TECHNISCHE UNIVERSITÄT MÜNCHEN

WALTHER-MEISSNER-INSTITUT

BAYERISCHE AKADEMIE DER WISSENSCHAFTEN

# Demonstration of microwave single-shot quantum key distribution

Dissertation

Florian Fesquet

TECHNISCHE UNIVERSITÄT MÜNCHEN

TUM School of Natural Sciences

# Demonstration of microwave single-shot quantum key distribution

Florian Fesquet

Vollständiger Abdruck der von der TUM School of Natural Sciences der Technischen Universität München zur Erlangung des akademischen Grades eines

**Doktors der Naturwissenschaften (Dr. rer. nat.)**

genehmigten Dissertation.

Vorsitz: _____

Prüfer*innen der Dissertation: 1. Prof. Dr. Rudolf Gross

2. _____

Die Dissertation wurde am _____ bei der Technischen Universität München eingereicht und durch die TUM School of Natural Sciences am _____ angenommen.

# Abstract

Quantum mechanics with the associated applications and development over the past decades hold the promise of pushing the boundaries of modern technologies. Along quantum computing and quantum sensing, the field of quantum communication has seen tremendous progress, appearing as one of the most mature quantum technology. In quantum communication, quantum properties and quantum laws are harnessed to provide security thresholds that outperform classical bounds. In particular, a great interest has emerged with the concept of quantum computers and its potential associated threat to established classical security algorithms. Among the variety of competing hardware platforms that have flourished, superconducting quantum circuits presents itself as a prime candidate for the advent of a fault-tolerant quantum computer. As a result, the need to further develop quantum computation operated at microwave frequencies has been motivated. In this thesis, we focus on the quantum key distribution (QKD), a type of communication protocol aiming at exchanging information between remote parties with the potential to demonstrate unconditional security. Here, theoretical investigations and practical experiments are so far lacking. As the first central result of this work, we present a theoretical study of the feasibility of QKD in the microwave regime and relying on continuous-variable (CV) states. We focus on a realistic experimental implementation with cryogenic systems, making use of the decades of demonstrated expertise at the Walther-Meissner-Institut in low temperature physics. We find that microwave CV-QKD should be experimentally possible and predict open-air communication distances over hundred of meters in ideal conditions. There, we unravel many experimental limitations, ranging from state preparation to state detection. Additionally, we highlight a robustness of microwave CV-QKD to weather imperfections, in strong contrast to conventional CV-QKD operated at optical frequencies. As the second main result of this thesis, we demonstrate the first microwave CV-QKD proof-of-principle implementation. The chosen protocol relies on displaced squeezed states which we obtain using notably Josephson parametric amplifiers (JPAs) combined with cryogenic directional couplers. In this experiment, we explain how JPAs can realize single-shot single quadrature measurements, an analog process to conventional homodyne detection for optical signals. Relying on state-of-the-art security proofs, we demonstrate an achievable unconditional security in the asymptotic regime. Additionally, we investigate finite-size effects, arising from limitations in practical experiments, that are found to be successfully mitigated at the cost of more demanding, but feasible, experimental requirements. Based on the presented results, we extrapolate long-range communication over a kilometer as well as open-air communication for dozens of meters. Lastly, as the third main result of this work, we present experiments of coupling microwave signals to a spin ensemble. Specifically, we investigate its coupling to propagating squeezed microwave states, which we treat as a quantum memory for quantum communication applications. Our analysis reveals a partial storage, even at the single photon regime, of incoming microwave signals to the spin ensemble, where we find the efficiency of the coupling to be determined by the system cooperativity. The novel insights based on these investigations allows for successful experiments aiming at demonstrating the retrieval of the stored states.

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

Due to its accurate theoretical formulation and successful experimental verification, quantum mechanics is firmly established as a fundamental concept of modern physics. Many concepts in quantum physics challenge the classical view of reality. In particular, they lead to non-trivial, exotic properties, such as quantum entanglement and state superposition [1, 2, 3]. The latter play a crucial role in quantum algorithms, offering powerful tools to achieve a quantum advantage of quantum systems over their classical counterparts. Notably, the concept of quantum entanglement and its implications of nonlocality have been extensively investigated over the past few decades, providing a more complete understanding of modern physics [4, 5]. These properties can also be harnessed to advance quantum technology, with particular interest in the field of information science [6, 7]. There, harnessing quantum properties has led to the emergence of the fields of quantum information theory and quantum communication. Interestingly, the laws of quantum physics can allow for a variety of improvements over classical systems, such as in efficiency and security of communication protocols [8]. Quantum algorithms also allow certain computational problems to be solved several orders of magnitude more efficiently than by their best-known classical counterparts. Recently, quantum supremacy has been demonstrated in quantum computing [9]. These advancements in quantum information processing have driven the development of various competing hardware platforms, such as systems based on trapped ions [10], spin systems [11], neutral atoms [12], nitrogen-vacancy centers [13], and superconducting circuits [14].

In this thesis, we focus on superconducting circuits, particularly in the context of signal amplification. Superconducting circuits are considered one of the most promising candidates for developing quantum processors, with the long-term goal of creating the world's first practical quantum computers. Recently, significant breakthroughs have been achieved using this hardware platform by, for example, demonstrating the aforementioned quantum supremacy and achieving quantum error correction beyond the break-even point [15]. Although some of these results are still debated [16, 17], they represent important steps towards fault-tolerant quantum computers, i.e., systems capable of operating correctly even in the presence of substantial or non-negligible errors in quantum operations [18]. In this context, it is particularly relevant to investigate the exchange of information between different communicating parties, aiming at enabling efficient, secure, and superconducting-circuit-based communication protocols.

At the moment, among various applications of quantum information processing, quantum communication stands out as one of the fields that is most advanced. Traditionally, the exchange of information between two parties is established by securely encrypting data before transmission, ensuring that a third party attempting to intercept the communication cannot decrypt and recover the original information. In part, security systems commonly rely on computationally hard-to-solve asymmetrical problems. A well-known example is the RSA encryption protocol [19], which exploits the fact that prime factorization of large integers is

computationally exponentially demanding. For a product of large prime numbers (modern RSA often uses encryption private keys, for the purpose of data encoding, that are of 2048 bits or more), the factorization task is effectively impossible within a reasonable period of time, limited by the present efficiency of classical prime factorization algorithms and power of available classical computing systems. This picture has been changed with the development of quantum algorithms designed to run on quantum computers, most notably Shor's algorithm [20]. Using a sufficiently powerful quantum computer, this algorithm reduces the unfavorable exponential complexity of prime number factorization to a polynomial one [21, 22], thus challenging the security of RSA-based algorithms. This particular example illustrates that upcoming quantum computational methods may drastically change modern secure communication protocols.

One potential solution to the aforementioned problem is to perform communication using quantum states. This allows to achieve efficient and secure communication between remote parties where security would be guaranteed by the laws of quantum physics. In particular, quantum resources such as entanglement can be used to provide security in nonclassical methods and perform nonclassical operations. In this context, quantum teleportation is one of the most fundamental protocols in quantum communication [23, 24], demonstrating the ability to transfer information encoded into a quantum state from one place to another [25]. Since its introduction, quantum teleportation has been studied across various platforms, with continuous-variable (CV) quantum communication being a particularly active area of research. Here, numerous experiments have shown advantages of using quantum correlations for communication [8, 24, 26, 27]. Alongside quantum teleportation, several other quantum communication protocols have been studied and experimentally implemented, including dense coding [28] and remote state preparation [27, 29].

In the context of secure quantum communication, the field of quantum cryptography has made significant advances over the past few decades, particularly in the development of quantum key distribution (QKD) protocols. These protocols enable secure information exchange between two remote parties, ensuring that a potential eavesdropper cannot gain information about the transmitted data. The key distinction that provides the security of QKD protocols, as compared to classical encryption, is based on the no-cloning theorem of quantum physics [30, 31]. This fundamental theorem states that it is impossible to create two perfect copies of an unknown given quantum state through a unitary transformation applied to the original state and any additional ancilla states. As a result, quantum information cannot be perfectly duplicated and requires interactions with quantum systems. A malicious eavesdropper, attempting to intercept the communication, would inevitably disturb the transmission in a detectable way. By analyzing the impact of this disturbance, it is possible to estimate the amount of information that may leak during the communication. This principle is the basis of QKD protocols, which take advantage of these effects to offer the promise of reaching unconditionally secure communication. The latter indicates that even the availability of unlimited computational power of a third party, including quantum computing, can compromise the security of such communication. However, practical implementations are more complex and contain various imperfections, such as (un)trusted preparation and measurement devices [32, 33], which could compromise their security. Despite these challenges, many QKD protocols have been experimentally implemented in various scenarios [8]. The ongoing development in this field focuses on security proofs for increasingly complex and relevant communication cases [34, 35, 36, 37].

The first quantum key distribution (QKD) protocol was proposed by Bennett and Brassard in 1984 [38]. It relies on using different polarizations of single photons to encode and communicate classical bits of information. Security proofs have since been extended to meet modern security requirements [39, 40]. This particular QKD protocol is often classified as a discrete-variable (DV) protocol, which involves description in finite-dimensional Hilbert spaces [8, 36, 41]. DV-QKD has been implemented successfully with a variety of quantum states,

particularly using left/right circular polarized light [8]. Reliable and fast information rates over long distances have been demonstrated using DV-QKD protocols as well as compatibility with modern communication platforms [42, 43]. Alternatively, CV protocols imply an infinite-dimensional Hilbert space and represent a conjugate approach to the DV one. Among important advantages of CV protocols are less stringent experimental requirements and potentially significantly higher communication rates. Additionally, CV systems can also be easily integrated into existing classical communication platforms, taking advantage of direct technological compatibility [8].

Historically, QKD protocols have been studied and implemented in the optical regime. In the context of the rapid development of modern superconducting quantum circuits operated at GHz frequencies as mentioned previously, it becomes crucial to study avenues of QKD in the microwave regime, corresponding to the frequency range of 1-10 GHz. Unfortunately, the large energy difference between microwave and optical photons, on the order of $10^5$, makes it very difficult to achieve an efficient conversion between these two frequency regimes. Best currently-available optical-to-microwave transducers achieve single-photon efficiencies of $\sim 10^{-5}$ for single photons [44, 45, 46]. As a result, converting microwave quantum signals into optical photons for communication purposes is experimentally very challenging and still an unsolved task. Therefore, in our approach, we rely on direct implementations with microwave carrier frequencies. This implementation possesses both certain fundamental drawbacks and useful benefits. Due to their low energy scale, thermal microwave noise is significant with quantum microwave experiments requiring cryogenic cooling to millikelvin temperatures in order to suppress undesired thermal photons [47]. Here, we build on the longstanding expertise of the Walther-Meißner-Institut in cryo-engineering, which has led to the implementation of many milestone quantum microwave experiments, including microwave Planck spectroscopy [48], dual-path Wigner tomography of microwave signals [49], the realization of displacement and squeezing operations [50, 51], and the demonstration of path entanglement [52].

In this thesis, we study and, for the first time, realize a CV-QKD protocol in the microwave regime. We demonstrate its potential for unconditionally secure communication, based on state-of-the-art security proofs [53]. The primary resource in our experiments is the Josephson parametric amplifier (JPA) [54, 55]. JPAs can be operated as both phase-sensitive and phase-insensitive amplifiers with noise properties approaching the standard quantum limit [56]. JPAs are widely used in various microwave quantum experiments, ranging from single-shot qubit readout to enhancing spin-echo experiments [57, 58, 59]. In our work, we experimentally show that JPAs can be utilized to perform single-shot quadrature measurements. Using this detection method, we experimentally realize a particular CV-QKD protocol with propagating squeezed displaced microwaves [53]. From the analysis of the received key, we extract a nonzero secret key rate and confirm the reachability of unconditionally secure communication. As an extension of this work, we derive that microwave CV-QKD should be feasible under open-air conditions with experimentally accessible parameters [60]. Our analysis further reveals that microwave signals could be particularly suitable for short-range communication, compatible with existing 5G and future 6G mobile communication standards, offering strong resilience to weather imperfections. Finally, we discuss how to couple and store microwave quantum states in a spin ensemble. We present our experimental progress in this direction by demonstrating squeezed states coupling to the spin ensemble. These results represent an important step towards the integration of long-lived quantum memories in secure quantum communication protocols such as the investigated CV-QKD one, which is an important milestone for using microwave CV states in quantum information processing.

This thesis is structured as follows. In chapter 2, we introduce a fundamental theoretical description of JPAs and general quantum states. In particular, we focus on Gaussian states, quasi-probability Wigner functions, entanglement properties, and Gaussian quantum chan-

nels. We develop a theoretical description of squeezing and displacement operations, which are needed for CV-QKD. Based on this formalism, we discuss QKD fundamentals in the next chapter 3 with general notions of QKD. There, we compare DV- and CV-QKD protocols and show that the latter are better suited for the microwave regime. Due to their sensitivity to the presence of thermal noise in the communication, we show the relevance and advantage of squeezed-state-based protocols over coherent-state-based ones for microwave signals, representing a striking contrast to CV-QKD implementations in the optical domain. In chapter 4, we present the experimental setup implementing the chosen displaced squeezed CV-QKD protocol with Gaussian modulation. There, we detail calibration measurements that are essential to support our findings and comment on various technical aspects of our experiments. Additionally, we introduce a novel analysis for determining the Gaussianity of measured states based on their experimentally reconstructed moments up to the fourth order. As the culminating point of this work, in chapter 5, we demonstrate a successful experimental proof-of-principle realization of the studied CV-QKD protocol. There, we prove the Gaussianity of our measured states and use state-of-the-art security proofs to demonstrate the accessibility of unconditional security of our experimental quantum communication. We also incorporate finite-size effects in our analysis and highlight the robustness of the implemented CV-QKD protocol under more realistic conditions. This allows us to extrapolate a faithful upper bound on secure communication rates that can be achieved in the microwave regime. Lastly, our investigation of microwave CV-QKD is extended in chapter 6 to include quantum memories in the form of a spin ensemble coupled to a superconducting resonator. In our experiments, we succeeded in coupling and storing microwave squeezed states to the spin ensemble. Chapter 7 concludes this thesis with a summary and outlook of the presented results.

# Chapter 2

# Quantum information with microwave states

In this chapter, we introduce the theoretical foundations required to describe the experiments performed in this work. Our theoretical description is based on textbook knowledge where we provide corresponding relevant sources. First, section 2.1 is dedicated to theory and circuit models of Josephson parametric amplifiers (JPAs), which serve as fundamental building blocks in our experiments. There, we derive the JPA Hamiltonian and the necessary assumptions to operate JPAs in a linear amplification regime. Then, section. 2.2 presents the properties of Gaussian quantum states and their associated representations. There, we detail the transfer of Gaussian states through Gaussian quantum channels and their associated physical interpretation. We conclude with a measurement theory based approach to link squeezed states to single quadrature measurements.

## 2.1 Josephson parametric amplifier

In this section, we focus on the general theory of JPAs and parametric amplification. In Sec. 2.1.1, we describe Josephson junctions and direct current superconducting quantum interference devices. In Sec. 2.1.2, we first describe the derivation of the JPA Hamiltonian. In Sec. 2.1.3 we then introduce the input-output formalism of an undriven JPA. Finally, in Sec. 2.1.4, we present the mechanism of parametric amplification obtained by applying a magnetic flux drive to the JPA and comment on the related amplification efficiency.

### 2.1.1 Josephson junctions and dc-SQUIDs

One of the most significant properties of superconductors is the Meißner-Ochsenfeld effect, describing the expulsion of magnetic flux from the interior of a superconductor below its critical temperature. This property is valid only up to a material-dependent critical magnetic field. Whereas for type I superconductors there is only a single critical field marking the boundary to the normal state, there is a lower and upper critical field for type II superconductors. In the phase diagram of type II superconductors, the Meißner state is present below the lower and the normal state above the upper critical field, whereas a mixed state with partial flux penetration is established in between the two critical fields.

Within the macroscopic quantum model of superconductivity, the whole entity of superconducting electrons is described by a macroscopic wave function $\Psi(\boldsymbol{r},t) = \sqrt{n_\mathrm{s}}\exp(\imath\theta(\boldsymbol{r},t))$. Its amplitude is given by the Cooper pair density $\sqrt{n_\mathrm{s}}$ and $\theta(\boldsymbol{r},t)$ represents its phase [61]. By weakly coupling two bulk superconductors, described by the macroscopic wave functions

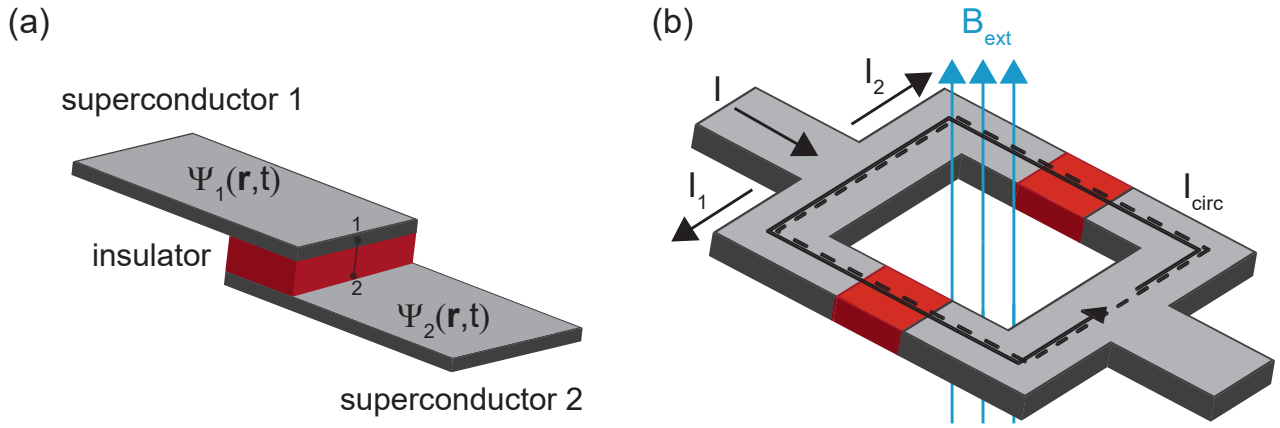


Figure 2.1: Schematics of a Josephson junction and a dc-SQUID. As depicted in panel (a), a Josephson junction is formed by two superconductors shown in grey separated by an insulator, shown in red, acting as a tunnel barrier. Each superconductor is characterized by its macroscopic wave function $\Psi_i$. The line represents the integration path used to define the gauge-invariant phase difference. Two Josephson junctions can be assembled in a superconducting loop to form a dc-SQUID, as shown in panel (b). There, a bias current $I$ splits into the two arms, $I_1$ and $I_2$, leading to a circulating current $I_{\mathrm{circ}}$. An external magnetic field, $B_{\mathrm{ext}}$, is threading through the dc-SQUID loop. The dashed line represents the contour line used to obtain Eq. (2.11) and is displayed purposely with a slight offset for visibility.

$\Psi_1(\boldsymbol{r},t)$ and $\Psi_2(\boldsymbol{r},t)$, using a thin layer of non-superconducting material such as an insulator one obtains a structure known as a Josephson junction. A schematic representation of a Josephson junction is shown in Fig. 2.1. Due to the finite coupling between the two superconductors, the phases $\theta_1$ and $\theta_2$ of the coupled wave functions are no longer independent. The phase difference between the two junction electrodes is given by the gauge-invariant expression [62]

$$\varphi(\boldsymbol{r},t) = \theta_2(\boldsymbol{r},t) - \theta_1(\boldsymbol{r},t) - \frac{2\pi}{\Phi_0}\int_1^2 \mathbf{A}(\boldsymbol{r},t)d\boldsymbol{l}, \tag{2.1}$$

where $\mathbf{A}$ is the magnetic vector potential, $\Phi_0$ the flux quantum, and the integral is along a path from superconductor 1 to superconductor 2 across the junction barrier. The Josephson current density accross the junction is related to the phase difference by the first Josephson equation, also known as the current-phase relation [61]

$$J_{\mathrm{s}}(\boldsymbol{r},t) = J_{\mathrm{c}}(\boldsymbol{r})\sin(\varphi(\boldsymbol{r},t)), \tag{2.2}$$

where $J_{\mathrm{c}}$ is the junction critical current density. Eq. (2.2) also implies that the current density is a nonlinear function of the phase. In the following, we only consider spatially homogeneous junctions ($J_{\mathrm{c}}(\boldsymbol{r}) = \text{const.}$) and junctions with spatial dimensions much smaller than the Josephson penetration depth so that $\varphi(\boldsymbol{r}) = \text{const.}$ In this case, we can replace Eq. (2.2) by

$$I_{\mathrm{s}}(t) = I_{\mathrm{c}}\ \sin(\varphi(t)). \tag{2.3}$$

For a single Josephson junction, the phase difference $\varphi$ is related to the voltage across the junction via the second Josephson equation as [61]

$$\frac{\partial\varphi}{\partial t} = \frac{2\pi}{\Phi_0}V(t). \tag{2.4}$$

By using the definition of an inductance

$$L_{\mathrm{s}}\frac{\mathrm{d}I_s}{\mathrm{d}t} = V(t), \tag{2.5}$$

one can define the Josephson inductance $L_\mathrm{s}$ of a Josephson junction as

$$L_\mathrm{s} = \frac{\Phi_0}{2\pi I_c \cos(\varphi)}. \tag{2.6}$$

This result is remarkable, as it means that a Josephson junction corresponds to a nonlinear inductor which can be changed by a bias current. The nonlinear tunable properties of the Josephson junction make it a central element for superconducting quantum circuits such as superconducting qubits, parametric amplifiers, or magnetic sensors [61, 62].

Based on the first and second Josephson equation, one can estimate the binding energy, $E_\mathrm{J}$, associated with a Josephson junction as

$$E_\mathrm{J}(\varphi) = \int_0^t I_\mathrm{s}(t')V(t')\mathrm{d}t' = \frac{\Phi_0}{2\pi} I_c(1-\cos(\varphi)) = E_{\mathrm{J},0}(1-\cos(\varphi)). \tag{2.7}$$

Obviously, this coupling energy depends only on the phase difference $\varphi$.

One can draw an analogy with a mechanical system by associating $\varphi$ with the coordinate $x$ of a particle inside a potential landscape described by $E_\mathrm{J}$. As for a mechanical system, one can define the Lagrangian of the Josephson junction as the difference between the kinetic term, $T$, and a potential term, $E_\mathrm{pot}$. Without damping components, the Josephson junction Lagrangian takes the form

$$\mathcal{L}(\varphi,\dot{\varphi}) = T(\dot{\varphi}) - E_\mathrm{pot}(\varphi) = \frac{\hbar^2\dot{\varphi}^2}{4E_\mathrm{C}} - E_{\mathrm{J},0}(1-\cos(\varphi)), \tag{2.8}$$

where $E_\mathrm{C} = (2e)^2/2C$ is the charging energy associated with the charge $2e$ of a Cooper pair stored on the junction capacitance $C$. The classical dynamics can be derived using the Euler-Lagrange equation

$$\frac{\mathrm{d}}{\mathrm{d}t}\frac{\partial\mathcal{L}}{\partial\dot{\varphi}}(\varphi,\dot{\varphi}) - \frac{\partial\mathcal{L}}{\partial\varphi}(\varphi,\dot{\varphi}) = 0. \tag{2.9}$$

To provide a quantum mechanical description of the Josephson junction, one has to replace the classical variables by their quantum-mechanical operator counterparts. Additionally, in this work, devices are operated in the deep phase regime, where the Josephson energy is much larger than the charging energy ($E_\mathrm{J}/E_\mathrm{C} \simeq 10^3$) [54]. Consequently, the phase, or the magnetic flux, is a good quantum number for the description of Josephson dynamics.

Using two Josephson junctions, one can build another important superconducting device - a direct current superconducting quantum interference device (dc-SQUID). The two Josephson junctions must be arranged in a loop, as shown in Fig. 2.1(b). For simplicity, we assume junctions with identical critical current. Other devices using Josephson junctions designed with different critical currents exist, such as SNAILs [63] or asymmetric SQUIDs. Applying an external magnetic field, $\mathbf{B}_\mathrm{ext}$, perpendicular to the SQUID loop results in the magnetic flux $\Phi_\mathrm{ext} = A_\mathrm{loop}\cdot\mathbf{B}_\mathrm{ext}$ through the SQUID loop. Here, $A_\mathrm{loop}$ is the loop area of the dc-SQUID. Within the macroscopic quantum model of superconductivity, one can derive the following expression for the gauge-invariant phase gradient in a bulk superconductor [61]:

$$\boldsymbol{\nabla}\theta = \frac{2\pi}{\Phi_0}(\Lambda\mathbf{J_s} + \mathbf{A}). \tag{2.10}$$

Here, $\Lambda$ is the London coefficient [61] and $\mathbf{J_s}$ is the supercurrent density. By integrating along a closed contour line $\mathcal{C}$, as shown in Fig. 2.1(b), the phase differences $\varphi_1$ and $\varphi_2$ across the two junctions can be related to the total magnetic flux $\Phi$ threading the loop by

$$\varphi_2 - \varphi_1 = 2\pi\,\frac{\Phi}{\Phi_0}. \tag{2.11}$$

Here, we have used the fact that the total phase change accumulated along the closed contour path $\mathcal{C}$ is given by $2\pi n$ with $n$ being an integer (fluxoid quantization). We also assumed thick superconducting electrodes, what allows us to choose an integration path deep inside the superconductor where $\mathbf{J_s} = 0$.

The total magnetic flux $\Phi$ is composed of two components, namely the flux $\Phi_{\text{ext}}$ generated by the applied magnetic field and the self-generated flux $\Phi_{\text{L}} = L_{\text{loop}} I_{\text{circ}}$ due to a current circulating in the SQUID loop of geometric inductance $L_{\text{loop}}$. Then, the total flux can be written as $\Phi = \Phi_{\text{ext}} + L_{\text{loop}} I_{\text{circ}}$. The circulating current $I_{\text{circ}}$ can be expressed using the first Josephson equation applied to each junction, resulting in the expression

$$I_{\text{circ}} = \frac{I_1 - I_2}{2} = I_c \cos\left(\frac{\varphi_1 + \varphi_2}{2}\right) \sin\left(\frac{\varphi_1 - \varphi_2}{2}\right) = -I_c \cos(\varphi_+) \sin(\varphi_-), \tag{2.12}$$

where $I_i$ is the current in the branch $i$ of the dc-SQUID. Here, one defines two new phase variables

$$\varphi_+ = \frac{\varphi_1 + \varphi_2}{2} \quad \text{and} \quad \varphi_- = \frac{\varphi_2 - \varphi_1}{2}, \tag{2.13}$$

in order to simplify Eq. (2.12) to a similar structure as Eq. (2.3). Using these definitions, we obtain [64]

$$\frac{\Phi}{\Phi_0} = \frac{\Phi_{\text{ext}}}{\Phi_0} - \frac{\beta_{\text{L}}}{2} \cos(\varphi_+) \sin(\varphi_-) \quad \text{with} \quad \beta_{\text{L}} = \frac{2 L_{\text{loop}} I_{\text{c}}}{\Phi_0}. \tag{2.14}$$

From Eq. (2.14), we observe that the total magnetic flux threading a dc-SQUID shows a hysteric behavior which is quantified using the dimensionless parameter $\beta_{\text{L}}$, referred to as the screening parameter. This parameter relates the maximally self-induced magnetic flux $\Phi_{\text{L}} = L_{\text{loop}} I_{\text{circ}}$ to half of a flux quantum, $\Phi_0/2$. As a result, a large screening parameter indicates a strong hysteretic behavior of the dc-SQUID. In this case, the magnetic flux cannot be explicitly determined analytically. Instead, one extracts it by numerically solving the system of equations given by Eq. (2.14) and the total current $I_1 + I_2 = 2I_{\text{c}} \sin(\varphi_+) \cos(\varphi_-)$. In the limit of negligible loop inductance, the self-induced field becomes negligible as compared to the applied field, corresponding to a screening parameter $\beta_{\text{L}}$ close to 0. Here, the total magnetic flux is given by the external magnetic flux, $\Phi \simeq \Phi_{\text{ext}}$. Consequently, one can obtain explicit expressions for maximal supercurrent and inductance of the dc-SQUID [65]

$$I_{\text{s}}^{\max} = 2I_{\text{c}} \left| \cos\left(\pi \frac{\Phi_{\text{ext}}}{\Phi_0}\right) \right| \quad \text{and} \quad L_{\text{s}}(\Phi_{\text{ext}}) = \frac{\Phi_0}{4\pi I_{\text{c}} \left| \cos\left(\pi \frac{\Phi_{\text{ext}}}{\Phi_0}\right) \right|}. \tag{2.15}$$

From Eq. (2.15), it can be seen that the dc-SQUID behaves similarly to a single Josephson junction. In general, the maximum supercurrent and inductance of the dc-SQUID are related to the external magnetic flux as

$$I_{\text{s}}^{\max} = 2I_{\text{c}} j_{\text{c}}(\Phi_{\text{ext}}) \quad \text{and} \quad L_{\text{s}}(\Phi_{\text{ext}}) = \frac{\Phi_0}{4\pi I_{\text{c}} j_{\text{c}}(\Phi_{\text{ext}})}. \tag{2.16}$$

Following our previous discussion on Lagrangian mechanics, one can derive the general Lagrangian for the dc-SQUID with a given screening parameter, $\beta_{\text{L}}$, as [66]

$$\mathcal{L} = \frac{\hbar^2(\dot{\varphi}_+^2 + \dot{\varphi}_-^2)}{2E_{\text{C}}} - 2E_{\text{J},0}(1 - \cos(\varphi_+)\cos(\varphi_-) - j_{\text{tr}}\varphi_+) - \frac{2E_{\text{J},0}}{\pi\beta_{\text{L}}} \left(\varphi_- - \pi \frac{\Phi_{\text{ext}}}{\Phi_0}\right)^2. \tag{2.17}$$

where $j_{\text{tr}} = (I_1 + I_2)/(2I_{\text{c}})$. We note that this Lagrangian does not incorporate any dissipative terms. It is also important to remind that the Lagrangian of the dc-SQUID given in Eq. (2.17) can be used to derived the general dynamics of a phase particle with coordinates $(\varphi_+, \varphi_-)$ in the dc-SQUID potential however one must also account for the fluxoid quantization defined by Eq. (2.11) to obtain the full dynamics of a dc-SQUID [67].

### 2.1.2 Josephson parametric amplifier

We consider a flux-driven Josephson parametric amplifier which consists of a coplanar waveguide (CPW) and is shorted to ground via the dc-SQUID as illustrated in Fig. 2.2. In this work, we consider the CPW as a one-dimensional microwave transmission line that is made of a superconducting Nb thin film. In order to analytically describe the CPW, we use a distributed element model of a chain of LC resonators. An electromagnetic wave propagating in such a medium is described using Telegrapher's equations [68]. For an ideal lossless transmission line, the characteristic impedance is given by $Z = \sqrt{L_0/C_0}$ with $L_0$ and $C_0$ being the inductance and capacitance per unit length of the transmission line, respectively. In order to create a CPW resonator, one imposes specific boundary conditions. On one CPW end, we use a coupling capacitor with the value, $C_\mathrm{c}$, which serves as an input port to the resonator. The opposite boundary condition corresponds to a galvanic short to the ground plane through the dc-SQUID. The CPW resonator length $d_\mathrm{r}$ is designed to be a quarter of the wavelength $\lambda_\mathrm{r}$ of the fundamental mode of a targeted frequency [69]

$$\frac{\omega_\mathrm{r}}{2\pi} = \frac{1}{4d_\mathrm{r}\sqrt{L_0 C_0}}. \tag{2.18}$$

The CPW resonator Lagrangian is written using a distributed element model consisting of a series of $N$ LC resonators as shown in Fig. 2.2(a). We account for the dc-SQUID at the boundary of the resonator and rewrite the magnetic flux at a position $i$ as $\Phi_i = (\Phi_0/2\pi)\varphi_i$, using a phase variable $\varphi_i$. The resulting CPW resonator Lagrangian takes the form

$$\mathcal{L}_\mathrm{r} = \sum_{i=1}^{N-1} \left(\frac{\Phi_0}{2\pi}\right)^2 \left(\frac{C_i \dot{\varphi_i}^2}{2} - \frac{(\varphi_{i+1}-\varphi_i)^2}{2L_i}\right) + \left(\frac{\Phi_0}{2\pi}\right)^2 \left(\frac{C_N \dot{\varphi_N}^2}{2} - \frac{(\varphi_{N+1}-\varphi_N)^2}{2L_N}\right), \tag{2.19}$$

where the phase $\varphi_{N+1}$ at the end position $i = N+1$ is related to the gauge invariant phase differences of the dc-SQUID. Using values of capacitance and inductance per unit length of the CPW resonator, we write $C_i = C_0\Delta x$, $L_i = L_0\Delta x$, with $\Delta x$ the space between two consecutive LC circuits. We obtain in the limit of $\Delta x \to 0$

$$\mathcal{L}_\mathrm{r} = \int_0^{d_\mathrm{r}} \left(\frac{\Phi_0}{2\pi}\right)^2 \left(\frac{C_0\dot{\varphi}^2}{2} - \frac{1}{2L_0}\left(\frac{\partial\varphi}{\partial x}\right)^2\right) \mathrm{d}x, \tag{2.20}$$

where we introduce a phase variable $\varphi$. From the Euler-Lagrange equation shown in Eq. (2.9), we obtain the equation of motion for the phase

$$\frac{\partial^2\varphi}{\partial t^2} - \nu_0^2 \frac{\partial^2\varphi}{\partial x^2} = 0, \tag{2.21}$$

with the phase velocity $\nu_0 = 1/\sqrt{L_0 C_0}$. A fundamental solution to this wave equation is given by

$$\varphi(x,t) = \varphi_0 \sin(k\nu_0 t)\cos(kx), \tag{2.22}$$

where the phase velocity $\nu_0$ is related to the wavevector $k$ via the linear dispersion relation $k\nu_0 = \omega_0$, and $\varphi_0$ is a constant phase amplitude. Assuming $\beta_\mathrm{L} \ll 1$, the dc-SQUID can be described as an effective single Josephson junction using Eq. (2.15). Using Eqs. 2.11 and 2.17, in the limiting case of a fixed external dc magnetic flux, one derives the dc-SQUID Lagrangian [70]

$$\mathcal{L}_\mathrm{SQUID} = \left(\frac{\Phi_0}{2\pi}\right)^2 \frac{C_\mathrm{s}\dot{\varphi}_\mathrm{s}^2}{2} + \tilde{E}_\mathrm{J}(\Phi)\cos(\varphi_\mathrm{s}), \tag{2.23}$$

where $\tilde{E}_\mathrm{J}(\Phi) = 2E_{\mathrm{J},0}\cos(2\pi\Phi/\Phi_0)$ and $C_\mathrm{s}$ is the capacitance of each branch of the dc-SQUID. We denote the phase variable $\varphi_\mathrm{s} = \varphi_+$ to illustrate that the dc-SQUID behaves more like a

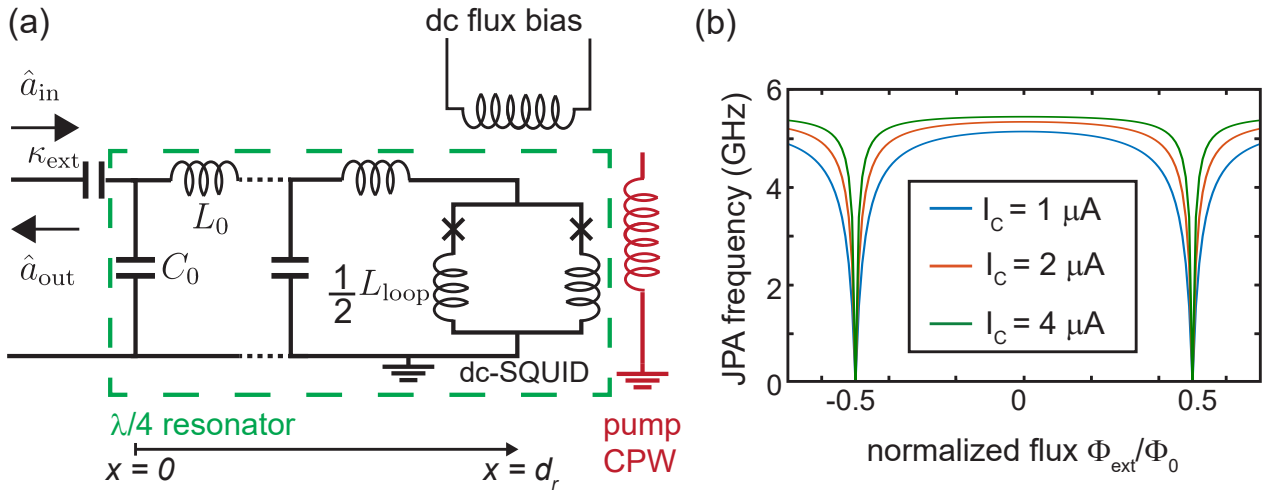


Figure 2.2: Schematic of a JPA circuit and its associated flux-dependent frequency response. (a) JPA circuit consisting of a $\lambda/4$ resonator modelled with a distributed element circuit, characterized by a capacitance per unit length, $C_0$, and inductance per unit length, $L_0$. The resonator is coupled to input modes $\hat{a}_{\rm in}$ via a coupling capacitor with the coupling rate $\kappa_{\rm ext}$. A dc-SQUID with an inductance $L_{\rm loop}$ short-circuits the resonator to ground. An external dc-bias magnetic flux is applied using an external magnetic coil while an ac magnetic flux is induced via an inductively coupled pump line. The bottom axis indicates the spatial coordinate along the circuit. (b) Flux-dependent JPA frequency response for different values of the dc-SQUID critical current. These plots are made using Eq. (2.27) for the particular value of resonator inductance $L_{\rm r} = 2\,{\rm nH}$ and loop inductance $L_{\rm loop} = 50\,{\rm pH}$.

single junction. We note that this Lagrangian is effectively describing only the boundary of the JPA circuit at the position $x = d_{\rm r}$ such that $\varphi(d_{\rm r}, t) = \varphi_{\rm s}(t)$. To account for the dc-SQUID effect, we write the total circuit Lagrangian $\mathcal{L}_{\rm tot} = \mathcal{L}_{\rm r} + \mathcal{L}_{\rm SQUID}$ and minimize the action $S$ over a time interval $T$

$$S = \int_0^T \mathcal{L}_{\rm tot}(t){\rm d}t. \tag{2.24}$$

The condition $\delta S = 0$ results in a new equation of motion for the CPW resonator with the dc-SQUID, using the principle of least action, i.e., $\delta\varphi(x,0) = \delta\varphi(x,T) = 0$ at any position $x$ in the resonator. This equation of motion reads as

$$\left(\frac{\Phi_0}{2\pi}\right)^2 \frac{1}{L_0}\frac{\partial\varphi_{\rm s}}{\partial x} + \left(\frac{\Phi_0}{2\pi}\right)^2 C_{\rm s}\frac{\partial^2\varphi_{\rm s}}{\partial t^2} - \tilde{E}_{\rm J}(\Phi)\varphi_{\rm s} = 0. \tag{2.25}$$

Using the solution from Eq. (2.22), one obtains a transcendental equation relating the JPA resonance frequency, $\omega_{\rm J}$, and the bare resonator frequency, $\omega_{\rm r}$. Denoting the effective resonator capacitance $C_{\rm r} = d_{\rm r}C_0$ and resonator inductance $L_{\rm r} = d_{\rm r}L_0$, the transcendental equation can be analytically written as [70, 71]

$$\left(\frac{\pi}{2}\frac{\omega_{\rm J}}{\omega_{\rm r}}\right)\tan\left(\frac{\pi}{2}\frac{\omega_{\rm J}}{\omega_{\rm r}}\right) = -\left(\frac{2\pi}{\Phi_0}\right)^2 L_{\rm r}\tilde{E}_{\rm J}(\Phi) + \frac{C_{\rm s}}{C_{\rm r}}\left(\frac{\pi}{2}\frac{\omega_{\rm J}}{\omega_{\rm r}}\right)^2. \tag{2.26}$$

A general solution of Eq. (2.26) requires numerical calculations. However, in some particular cases, analytical solutions can be computed. In the limit of $\omega_{\rm J} \simeq \omega_{\rm r}$ [70], i.e., for a small modulation of the JPA resonance frequency, a Taylor expansion of the tangent term in Eq. (2.26) near $\omega_{\rm J}/\omega_{\rm r} = 1$ leads to the simplified expression

$$\omega_{\rm J}(\Phi) = \omega_{\rm r}\left(\frac{L_{\rm r}}{L_{\rm r} + L_{\rm s}(\Phi) + L_{\rm loop}/4}\right), \tag{2.27}$$

where we account for the loop inductance. The flux-dependent JPA resonance frequency according to Eq. (2.27) is shown in Fig. 2.2(b).

In the following, we derive the JPA Hamiltonian which enables parametric amplification effects. In order to treat the JPA circuit from a quantum mechanical point of view, we first consider the fundamental mode solution written in the form $(\Phi_0/2\pi)\varphi(x,t) = \phi(t)\cos(kx)$. Next, we quantize the flux variable $\phi$ by replacing it with an operator $\hat{\phi}$, and similarly, $\varphi$ is switched to the operator $\hat{\varphi}$. Next, we introduce the Hamiltonian of the system based on the Legendre transformation by setting the potential term $V = -\tilde{E}_\mathrm{J}\cos(\varphi_\mathrm{s})$. We obtain the Hamiltonian

$$\hat{H} = \int_0^{d_\mathrm{r}} (\cos(kx)^2 \frac{C_0}{2}\frac{\mathrm{d}\hat{\phi}}{\mathrm{d}t}^2 + \sin(kx)^2\frac{k^2}{2L_0}\hat{\phi}^2)\mathrm{d}x + \left(\frac{\Phi_0}{2\pi}\right)^2 \frac{C_\mathrm{s}}{2}\frac{\mathrm{d}\hat{\varphi}}{\mathrm{d}t}^2(d_\mathrm{r},t) - \tilde{E}_\mathrm{J}(\Phi_\mathrm{ext})\cos(\hat{\varphi}(d_\mathrm{r},t)). \tag{2.28}$$

For the purpose of parametric amplification, we consider a small phase modulation corresponding to a small current flowing through the Josephson junctions. Therefore, we expand the cosine potential term in Eq. (2.28) outside of the integral term and keep the first term proportional to $\varphi^2$. This approach leads to the simplified Hamiltonian

$$\hat{H} = \int_0^{d_\mathrm{r}} (\cos(kx)^2 \frac{C_0}{2}\frac{\mathrm{d}\hat{\phi}}{\mathrm{d}t}^2 + \sin(kx)^2\frac{k^2}{2L_0}\hat{\phi}^2)\mathrm{d}x + \left(\frac{\Phi_0}{2\pi}\right)^2 \frac{C_\mathrm{s}}{2}\frac{\mathrm{d}\hat{\varphi}}{\mathrm{d}t}^2(d_\mathrm{r},t) + \frac{\tilde{E}_\mathrm{J}(\Phi_\mathrm{ext})}{2}\hat{\varphi}(d_\mathrm{r},t)^2. \tag{2.29}$$

We note that the structure of the simplified Hamiltonian is that of a harmonic oscillator with an additional nonlinear term coming from the dc-SQUID. In other words, the Hamiltonian of the JPA has in first order the structure of a harmonic oscillator with a flux-tunable frequency. As a result, the system dynamics could be described similarly to that of a pendulum with a parametrically modulated fundamental frequency. This parametric modulation leads to a parametric amplification process. To unravel this underlying structure of the simplified Hamiltonian, we introduce an effective capacitance and inductance of the circuit as

$$C = C_0\int_0^{d_\mathrm{r}}\cos(kx)^2\mathrm{d}x + C_\mathrm{s}\cos(kd_\mathrm{r})^2, \quad \frac{1}{L} = \frac{k^2}{L_0}\int_0^{d_\mathrm{r}}\sin(kx)^2\mathrm{d}x + \left(\frac{2\pi}{\Phi_0}\right)^2\tilde{E}_\mathrm{J}(\Phi_\mathrm{ext})\cos(kd_\mathrm{r})^2, \tag{2.30}$$

which, based on the definition of $\hat{\varphi}$ and $\hat{\phi}$, allows to write the simplified Hamiltonian in the form of a harmonic oscillator

$$\hat{H} = E_\mathrm{C}\left(\frac{C}{2e}\frac{\mathrm{d}\hat{\phi}}{\mathrm{d}t}\right)^2 + E_\mathrm{L}\left(\frac{\hat{\phi}}{\Phi_0}\right)^2 \tag{2.31}$$

with the charging energy $E_\mathrm{C} = (2e)^2/(2C)$ and the inductive energy $E_\mathrm{L} = \Phi_0^2/(2L)$. Since we consider a flux-induced parametric amplification, we additionally take into account that the magnetic flux is composed of two components, a fixed dc flux bias and an alternating ac flux, i.e., $\Phi_\mathrm{ext}(t) = \Phi_\mathrm{dc} + \Phi_\mathrm{ac}(t)$. As mentioned earlier, we consider the case of small ac excitation $\Phi_\mathrm{ac} \ll \Phi_0$. Under this assumption, we perform a Taylor expansion of $\tilde{E}_\mathrm{J}$ for the ac flux term around the dc flux bias, truncating the expansion to the first term since the JPA nonlinearity is relatively small [72], and obtain

$$\tilde{E}_\mathrm{J}(\Phi_\mathrm{ext}) = \tilde{E}_\mathrm{J}(\Phi_\mathrm{dc}) + \Phi_\mathrm{ac}\left.\frac{\partial\tilde{E}_\mathrm{J}}{\partial\Phi_\mathrm{ext}}\right|_{\Phi_\mathrm{ext}=\Phi_\mathrm{dc}}. \tag{2.32}$$

Lastly, based on the law of induction, $Q = -C\mathrm{d}\phi/\mathrm{d}t$, we introduce the charge operator $\hat{Q}$ which fulfils the commutation relation $[\hat{\phi},\hat{Q}] = i\hbar$. Using this definition in combination with

Eqs. 2.31 and 2.32, we derive the flux-modulated Hamiltonian of the JPA [73]

$$\hat{H} = E_{\mathrm{C}} \left(\frac{\hat{Q}}{2e}\right)^2 + E_{\mathrm{L}^\star} \left(\frac{\hat{\phi}}{\Phi_0}\right)^2 + \left(\frac{2\pi}{\Phi_0}\right)^2 \cos(k d_{\mathrm{r}})^2 \frac{\Phi_{\mathrm{ac}}}{2} \frac{\partial \tilde{E}_{\mathrm{J}}}{\partial \Phi_{\mathrm{ext}}} \hat{\phi}^2. \tag{2.33}$$

where we define $L^\star \coloneqq L(\Phi_{\mathrm{ext}} = \Phi_{\mathrm{dc}})$. Finally, we introduce the annihilation and creation operators as

$$\hat{a} = \left(\frac{C}{4\hbar^2 L^\star}\right)^{\frac{1}{4}} \hat{\phi} + i \left(\frac{L^\star}{4\hbar^2 C}\right)^{\frac{1}{4}} \hat{Q}, \quad \hat{a}^\dagger = \left(\frac{C}{4\hbar^2 L^\star}\right)^{\frac{1}{4}} \hat{\phi} - i \left(\frac{L^\star}{4\hbar^2 C}\right)^{\frac{1}{4}} \hat{Q}, \tag{2.34}$$

which we use in combination with Eq. (2.33) to obtain the final Hamiltonian of the JPA

$$\hat{H} = \hbar \omega_{\mathrm{J}} \left(\Phi_{\mathrm{dc}}\right) \left[\hat{a}^\dagger \hat{a} + \frac{\Phi_{\mathrm{ac}}}{2\omega_{\mathrm{J}}} \frac{\partial \omega_{\mathrm{J}}}{\partial \Phi_{\mathrm{ext}}} (\hat{a} + \hat{a}^\dagger)^2\right]. \tag{2.35}$$

We consider the case that a pump signal $s_{\mathrm{p}}$ induces the ac flux term $\Phi_{\mathrm{ac}}$ via a mutual inductance between the dc-SQUID and the additional pump line antenna in the JPA circuit, located next to the dc-SQUID. We assume that the pump tone takes the form $s_{\mathrm{p}}(t) = s_0 \cos(\alpha \omega_{\mathrm{J}}(\Phi_{\mathrm{dc}}) t)$, where $s_0$ is the pump amplitude and $\alpha$ is a proportionality constant relating the pump frequency to the JPA resonance frequency, $\omega_{\mathrm{p}} = \alpha \omega_{\mathrm{J}}(\Phi_{\mathrm{dc}})$. Thus, we reformulate the Hamiltonian of the JPA as [74]

$$\hat{H}_{\mathrm{JPA}} = \hbar \omega_{\mathrm{J}} \left(\Phi_{\mathrm{dc}}\right) \left[\hat{a}^\dagger \hat{a} + \epsilon \cos(\alpha \omega_{\mathrm{J}}(\Phi_{\mathrm{dc}}) t)(\hat{a} + \hat{a}^\dagger)^2\right], \tag{2.36}$$

where the parameter $\epsilon$ contains the pump amplitude and relevant geometric parameters. We note that $\epsilon$ depends on the JPA resonance frequency and can be tuned depending on the dc flux bias. Additionally, the modulation depends on the slope of the frequency vs. flux dependence of the JPA at the dc flux bias point as seen from Eq. (2.35). This implies that for practical implementations, it is preferable to operate JPAs at relatively small slopes in order to reduce the sensitivity of the JPA resonance frequency to random variation of the applied magnetic flux. However, the smaller the slope, the larger the required amplitude of the pump tone to achieve the desired parametric amplification effects, implying that both effects must be balanced. We note that the Hamiltonian in Eq. (2.35) is only valid up to a certain pump tone amplitude, beyond which previously neglected higher-order terms must be taken into account [73].

### 2.1.3 Input-output formalism

The input-output formalism of the JPA is derived by considering the coupling of the previously described system to input signals. To this end, we we assume that the JPA is coupled to an input transmission line with the coupling rate $\kappa_{\mathrm{ext}}$ and to a bosonic thermal bath with the coupling rate $\kappa_{\mathrm{int}}$ [75]. Both the input line and thermal bath are described as a continuum of bosonic modes [74]

$$\begin{aligned} \hat{H}_{\mathrm{ext}} &= \hbar \int \left[\omega_k \hat{b}_k^\dagger \hat{b}_k + i \sqrt{\frac{v_k \kappa_{\mathrm{ext}}}{2\pi}} \left(\hat{b}_k^\dagger \hat{a} - \hat{b}_k \hat{a}^\dagger\right)\right] \mathrm{d}k, \\ \hat{H}_{\mathrm{int}} &= \hbar \int \left[\omega_k \hat{c}_k^\dagger \hat{c}_k + i \sqrt{\frac{v_k \kappa_{\mathrm{int}}}{2\pi}} \left(\hat{c}_k^\dagger \hat{a} - \hat{c}_k \hat{a}^\dagger\right)\right] \mathrm{d}k, \end{aligned} \tag{2.37}$$

where $k$ is the wavevector of the mode $k$ with a linear dispersion, $k v_k = \omega_k$. Here, $\omega_k$ and $v_k$ are the corresponding frequency and phase velocity, respectively. The annihilation operator $\hat{b}_k$ ($\hat{c}_k$) corresponds to the external (internal) bath mode $k$ and follows the bosonic commutation

relation $[\hat{b}_k, \hat{b}_{k'}] = \delta(k-k')$ ($[\hat{c}_k, \hat{c}_{k'}] = \delta(k-k')$). The external coupling rate, $\kappa_\mathrm{e}$, depends on the coupling capacitance, $C_\mathrm{c}$, and on the JPA frequency. The internal coupling rate, $\kappa_\mathrm{i}$, is related to internal loss mechanisms. In the case of an undriven JPA, the total Hamiltonian of the system, $\hat{H}_\mathrm{tot} = \hat{H}_\mathrm{JPA}(\epsilon = 0) + \hat{H}_\mathrm{ext} + \hat{H}_\mathrm{int}$, corresponds to the following equations of motion:

$$\begin{aligned}\frac{\mathrm{d}\hat{a}}{\mathrm{d}t} &= -\frac{i}{\hbar}\left[\hat{a}, \hat{H}_\mathrm{tot}\right] = -i\omega_\mathrm{J}\hat{a} + \sqrt{\frac{v\kappa_\mathrm{ext}}{2\pi}}\int \hat{b}_k \mathrm{d}k + \sqrt{\frac{v\kappa_\mathrm{int}}{2\pi}}\int \hat{c}_k \mathrm{d}k, \\ \frac{\mathrm{d}\hat{b}_k}{\mathrm{d}t} &= -\frac{i}{\hbar}\left[\hat{b}_k, \hat{H}_\mathrm{tot}\right] = -i\omega_k\hat{b}_k - \sqrt{\frac{v\kappa_\mathrm{ext}}{2\pi}}\hat{a}.\end{aligned} \tag{2.38}$$

Here, we assume frequency-independent phase velocities, $v_k = v$. Furthermore, we denote the JPA resonance frequency as $\omega_\mathrm{J} = \omega_\mathrm{J}(\Phi_\mathrm{dc})$. We also do not explicitly state the equation for the modes $\hat{c}_k$. However, we note that any result obtained for the modes $\hat{b}_k$ can be directly applied to the modes $\hat{c}_k$ by substituting $\kappa_\mathrm{ext}$ with $\kappa_\mathrm{int}$. First, we solve the equation of motion for $\hat{b}_k$ and obtain

$$\hat{b}_k = e^{-i\omega_k t}\hat{b}_k(0) - \sqrt{\frac{v\kappa_\mathrm{ext}}{2\pi}}\int_0^t e^{-i\omega_k(t-t')}\hat{a}(t')\mathrm{d}t', \tag{2.39}$$

where we set the time reference for the system to $t = 0$. Using Eq. (2.39), one typically defines an input mode $\hat{b}_\mathrm{in}$ describing a signal incoming at the JPA input as [74]

$$\hat{b}_\mathrm{in}(t) = \int_{-\infty}^{+\infty} e^{-i\omega_k t}\hat{b}_k(0)\mathrm{d}k, \tag{2.40}$$

which can be linked to an output mode $\hat{b}_\mathrm{out}$ describing an outgoing signal from the JPA input. This results in the JPA input-out relation [74]

$$\hat{b}_\mathrm{out}(t) = \hat{b}_\mathrm{in}(t) - \sqrt{\frac{\kappa_\mathrm{ext}}{v}}\hat{a}(t). \tag{2.41}$$

We note that the relations are suited for any single-port lossy harmonic oscillator. Inserting Eqs. 2.39 and 2.40 into Eq. (2.38), we obtain the final equation of motion for the JPA intra-resonator mode

$$\frac{\mathrm{d}\hat{a}}{\mathrm{d}t} = -i\omega_\mathrm{J}\hat{a} - \frac{\kappa}{2}\hat{a}(t) + \sqrt{v\kappa_\mathrm{ext}}\hat{b}_\mathrm{in}(t) + \sqrt{v\kappa_\mathrm{int}}\hat{c}_\mathrm{in}(t), \tag{2.42}$$

where $\kappa = \kappa_\mathrm{ext} + \kappa_\mathrm{int}$ is the total coupling rate. The structure of Eq. (2.42) shows that $\kappa$ corresponds to an overall loss rate of the JPA mode $\hat{a}$. Although classically valid, on their own, these losses of the JPA mode $\hat{a}$ are insufficient from a quantum point of view, as the mode $\hat{a}$ satisfying Eq. (2.42) would no longer fulfil the bosonic commutation relation. Modes $\hat{b}_\mathrm{in}$ and $\hat{c}_\mathrm{in}$ are required to allow the bosonic commutation relation to be fulfilled at any time $t$. The steady-state solution of Eq. (2.42) can be obtained by transforming it into the frequency domain via Fourier transformation. Using the resulting equation with the input-output relation from Eq. (2.41), we can derive the magnitude and phase of a reflected signal using the scattering matrix formalism. For the scattering parameter, $S_{11} = \langle\hat{b}_\mathrm{out}\rangle / \langle\hat{b}_\mathrm{in}\rangle$, we obtain for a given signal frequency $\omega$, such that $\Delta = \omega - \omega_\mathrm{J}$

$$\begin{aligned}\left|S_{11}(\Delta)\right|^2 &= 1 - \frac{4\kappa_\mathrm{ext}\kappa_\mathrm{int}}{\Delta^2 + 2\kappa^2}, \\ \arg(S_{11}(\Delta)) &= \mathrm{atan2}(-4\Delta\kappa_\mathrm{ext}, 4\Delta^2 + \kappa^2 - 2\kappa_\mathrm{ext}\kappa).\end{aligned} \tag{2.43}$$

Here, we use the 2-argument arctangent function atan2. Furthermore, we define an external quality factor, $Q_\mathrm{ext}$, an internal quality factor, $Q_\mathrm{int}$, and a loaded quality factor, $Q_\mathrm{l}$. These quality factors determine the ratio between the total energy stored in the JPA and energy lost

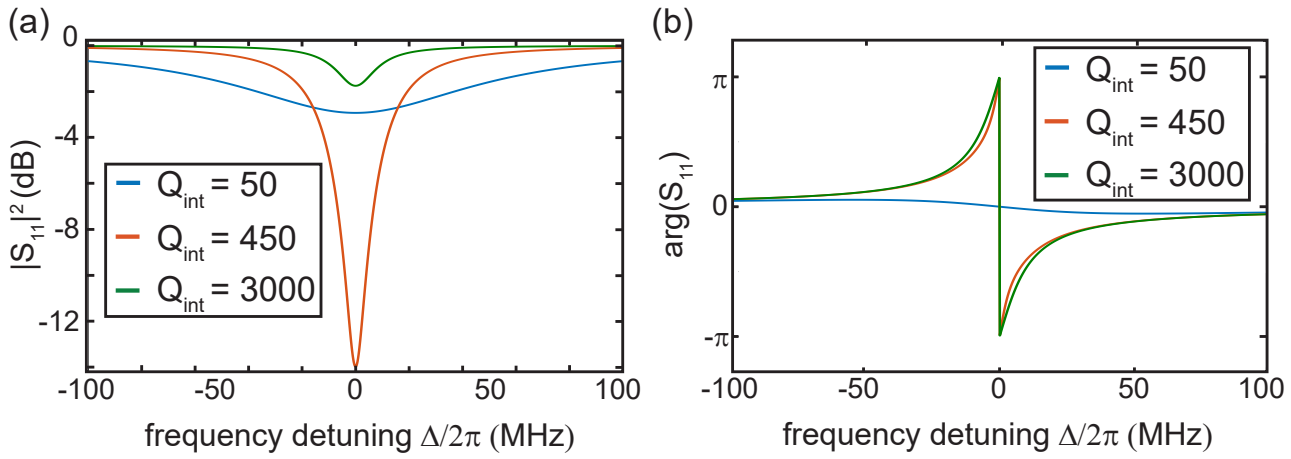


Figure 2.3: Frequency dependence of the scattering parameter $S_{11}$ of an undriven JPA. The magnitude of the scattering parameter, $|S|^2_{11}$, is shown in panel (a) while the phase of the scattering parameter $\arg(S_{11})$, is plotted in panel (b). The data are obtained with Eq. (2.43) for a fixed quality factor $Q_{\text{ext}} = 300$. The green, red, and blue curves correspond to the overcoupled, critically coupled, and undercoupled regimes, respectively.

per oscillation of the signal inside the JPA to the respective loss channel. As such, a large quality factor is equivalent to small losses relative to the stored energy. From this perspective, a practical fabrication of JPA would aim at having an internal quality factor as high as possible. The quality factors are related to the respective coupling rates as follows:

$$Q_{\text{ext}} = \frac{\omega_{\text{J}}}{\kappa_{\text{ext}}}, \quad Q_{\text{int}} = \frac{\omega_{\text{J}}}{\kappa_{\text{int}}}, \text{ and } \quad Q_{\text{l}} = \frac{\omega_{\text{J}}}{\kappa}. \tag{2.44}$$

The magnitude and the phase of the scattering parameters according to Eq.2.43 are plotted versus frequency in Fig. 2.3. We see that the quality factors play a significant role in the JPA response. Typically, one defines three corresponding regime, overcoupled ($Q_{\text{ext}} > Q_{\text{int}}, Q_{\text{l}} \simeq Q_{\text{ext}}$), undercoupled ($Q_{\text{ext}} < Q_{\text{int}}, Q_{\text{l}} \simeq Q_{\text{int}}$), and critically coupled regime ($Q_{\text{ext}} \simeq Q_{\text{int}}, Q_{\text{l}} \simeq 2Q_{\text{ext}}$). As illustrated in Fig. 2.3(a), the frequency dependence of the magnitude is quite similar in the overcoupled and undercoupled regimes. For this reason, it is favorable to use the phase response to distinguish between these two regimes, as shown in Fig. 2.3(b). In contrast, in the critically coupled regime a strong amplitude response is observed while the phase response is close to that of the undercoupled regime.

Lastly, we consider the case of the flux-driven JPA with $\epsilon \neq 0$. The total Hamiltonian reads $\hat{H}_{\text{tot}} = \hat{H}_{\text{JPA}}(\epsilon) + \hat{H}_{\text{ext}} + \hat{H}_{\text{int}}$ and the equations of motion remain the same as previously described, except for an added drive term $\propto \cos(\alpha\omega_{\text{p}}t)(\hat{a} + \hat{a}^\dagger)^2$ as seen in Eq. (2.36). The flux modulation is obtained by setting the pump frequency to twice the JPA resonance frequency, $\omega_{\text{p}} = 2\omega_{\text{J}}$, as illustrated in Fig. 2.4(a). In this case, we expand the cosine term $\cos(\alpha\omega_{\text{p}}t)$ in its exponential form according to Euler's formula and apply a rotating wave approximation to the term $\cos(\alpha\omega_{\text{p}}t)(\hat{a} + \hat{a}^\dagger)^2$, keeping only expressions proportional to $e^{2i\omega_{\text{J}}t}\hat{a}^2 + e^{-2i\omega_{\text{J}}t}(\hat{a}^\dagger)^2$. This transformation leads to the new equation of motion

$$\frac{\mathrm{d}\hat{a}}{\mathrm{d}t} = -i\omega_{\text{J}}\hat{a} - \frac{\kappa}{2}\hat{a}(t) - i\epsilon\omega_{\text{J}}e^{-2i\omega_{\text{J}}t}\hat{a}^\dagger + \sqrt{v\kappa_{\text{ext}}}\hat{b}_{\text{in}}(t) + \sqrt{v\kappa_{\text{int}}}\hat{c}_{\text{in}}(t). \tag{2.45}$$

Here, we apply the stiff pump approximation, which assumes no energy depletion in the pump mode [76].

### 2.1.4 JPA amplification and standard quantum limit

In our experiments, JPAs are operated in a steady-state regime where they are driven with a pump tone at twice the JPA resonance frequency with a fixed amplitude, implying $\epsilon = const.$ From Eq. (2.42), we determine the steady-state regime of the JPA by shifting to a frame rotating at the frequency $\omega_\mathrm{J}$. In this frame, we denote the rotated operators with corresponding capital letters, e.g., $\hat{A} = e^{i\omega_\mathrm{J} t}\hat{a}$, resulting in the equation

$$\frac{\mathrm{d}\hat{A}}{\mathrm{d}t} + \frac{\kappa}{2}\hat{A}(t) - i\epsilon\omega_\mathrm{J}\hat{A}^\dagger = \hat{F}(t), \tag{2.46}$$

where we define the operator $\hat{F} = \sqrt{v\kappa_\mathrm{ext}}\hat{B}_\mathrm{in} + \sqrt{v\kappa_\mathrm{int}}\hat{C}_\mathrm{in}$. We find a transient solution of Eq. (2.46) by using the ansatz $\hat{A}_\mathrm{hom}(t) = e^{\lambda_\mathrm{hom} t}\hat{C}_\mathrm{hom}$, where $\hat{C}_\mathrm{hom}$ is a bosonic operator. This leads to the solutions

$$\lambda_{\mathrm{hom},\pm} = -\frac{\kappa}{2} \pm \epsilon\omega_\mathrm{J}. \tag{2.47}$$

In particular, we observe that $\lambda_{\mathrm{hom},+}$ becomes positive for $\epsilon > \epsilon_\mathrm{c} = \kappa/(2\omega_\mathrm{J})$, meaning that convergence to a steady-state regime is possible only for $\epsilon \leq \epsilon_\mathrm{c}$ for this ansatz. Above that critical threshold, the JPA enters a parametric oscillating behavior [77] and is no longer suited for linear parametric amplification. In the rest of this thesis, we only consider the case $\epsilon \leq \epsilon_\mathrm{c}$ and obtain a steady-state solution using the Fourier transform applied to both Eq. (2.46) and its complex conjugate. Similarly, we perform the Fourier transform of Eq. (2.41) in the frame rotating with the frequency $\omega_\mathrm{J}$, resulting in the equation

$$\hat{B}_\mathrm{out}(\delta\omega) = \hat{B}_\mathrm{in}(\delta\omega) - \sqrt{\frac{\kappa_\mathrm{ext}}{v}}\hat{A}(\delta\omega), \tag{2.48}$$

where $\omega$ is the signal frequency and $\delta\omega = \omega - \omega_\mathrm{J}$ is the frequency detuning. Combining Eq. (2.46) with Eq. (2.48), we derive the final input-output relation in the frequency domain

$$\hat{B}_\mathrm{out}(\delta\omega) = M_\mathrm{in}(\delta\omega)\hat{B}_\mathrm{in}(\delta\omega) + L_\mathrm{in}(\delta\omega)\hat{B}^\dagger_\mathrm{in}(-\delta\omega) + M_\mathrm{n}(\delta\omega)\hat{C}_\mathrm{in}(\delta\omega) + L_\mathrm{n}(\delta\omega)\hat{C}^\dagger_\mathrm{in}(-\delta\omega), \tag{2.49}$$

with the scalar amplitudes of the corresponding bosonic modes

$$\begin{aligned} M_\mathrm{in}(\delta\omega) &= 1 + \kappa_\mathrm{ext}\frac{\kappa/2 - i\delta\omega}{(\delta\omega + i\kappa/2)^2 + \epsilon^2\omega_\mathrm{J}^2}, \quad L_\mathrm{in}(\delta\omega) = -\frac{i\epsilon\kappa_\mathrm{ext}\omega_\mathrm{J}}{(\delta\omega + i\kappa/2)^2 + \epsilon^2\omega_\mathrm{J}^2}, \\ M_\mathrm{n}(\delta\omega) &= \sqrt{\kappa_\mathrm{ext}\kappa_\mathrm{int}}\frac{\kappa/2 - i\delta\omega}{(\delta\omega + i\kappa/2)^2 + \epsilon^2\omega_\mathrm{J}^2}, \quad L_\mathrm{n}(\delta\omega) = -\frac{i\epsilon\sqrt{\kappa_\mathrm{ext}\kappa_\mathrm{int}}\omega_\mathrm{J}}{(\delta\omega + i\kappa/2)^2 + \epsilon^2\omega_\mathrm{J}^2}. \end{aligned} \tag{2.50}$$

The structure of Eq. (2.49) shows that the final output signal leaking out of the JPA consists of the input signal scaled by a factor $M_\mathrm{in}$, an additional noise term $M_\mathrm{n}\hat{C}_\mathrm{in} + L_\mathrm{n}\hat{C}^\dagger_\mathrm{in}$ corresponding to the internal losses, and the term $L_\mathrm{in}\hat{B}^\dagger_\mathrm{in}$, presenting a negative frequency detuning. As a result, the parametric amplification process of an input signal at a given frequency, $\omega = \omega_\mathrm{s}$, necessarily involves an additional mode, commonly referred to as the *idler* mode, at a frequency $\omega_\mathrm{i} = 2\omega_\mathrm{J} - \omega_\mathrm{s}$. This result can be understood in the framework of a three-wave mixing where the amplification of an input signal at frequency $\omega_\mathrm{s} = \omega_\mathrm{J} + \delta\omega$ involves an idler signal at frequency $\omega_\mathrm{i} = \omega_\mathrm{J} - \delta\omega$ as illustrated in Fig. 2.4(c) Intuitively, it corresponds to the frequency conversion process $\omega_\mathrm{p} = \omega_\mathrm{s} + \omega_\mathrm{i}$, where $\omega_\mathrm{p}$ is the frequency of the applied pump signal. In the case of finite detuning $\delta\omega \neq 0$, we compute the signal and idler gain values using $G_\mathrm{s} = |M_\mathrm{in}|^2$ and $G_\mathrm{i} = |L_\mathrm{in}|^2$, respectively. For small detuning, $\delta\omega \ll \omega_\mathrm{J}$, we find

$$G_\mathrm{s}(\delta\omega) = 1 + \frac{4\epsilon^2\epsilon_\mathrm{c}^2\omega_\mathrm{J}^4}{(\epsilon_\mathrm{c}^2 - \epsilon^2)^2\omega_\mathrm{J}^4 + 2\omega_\mathrm{J}^2(\epsilon^2 + \epsilon_\mathrm{c}^2)(\delta\omega)^2 + (\delta\omega)^4} \simeq 1 + \frac{2\epsilon^2\epsilon_\mathrm{c}^2\omega_\mathrm{J}^2/(\epsilon^2 + \epsilon_\mathrm{c}^2)}{\frac{(\epsilon_\mathrm{c}^2 - \epsilon^2)^2\omega_\mathrm{J}^2}{2(\epsilon^2 + \epsilon_\mathrm{c}^2)} + (\delta\omega)^2}. \tag{2.51}$$

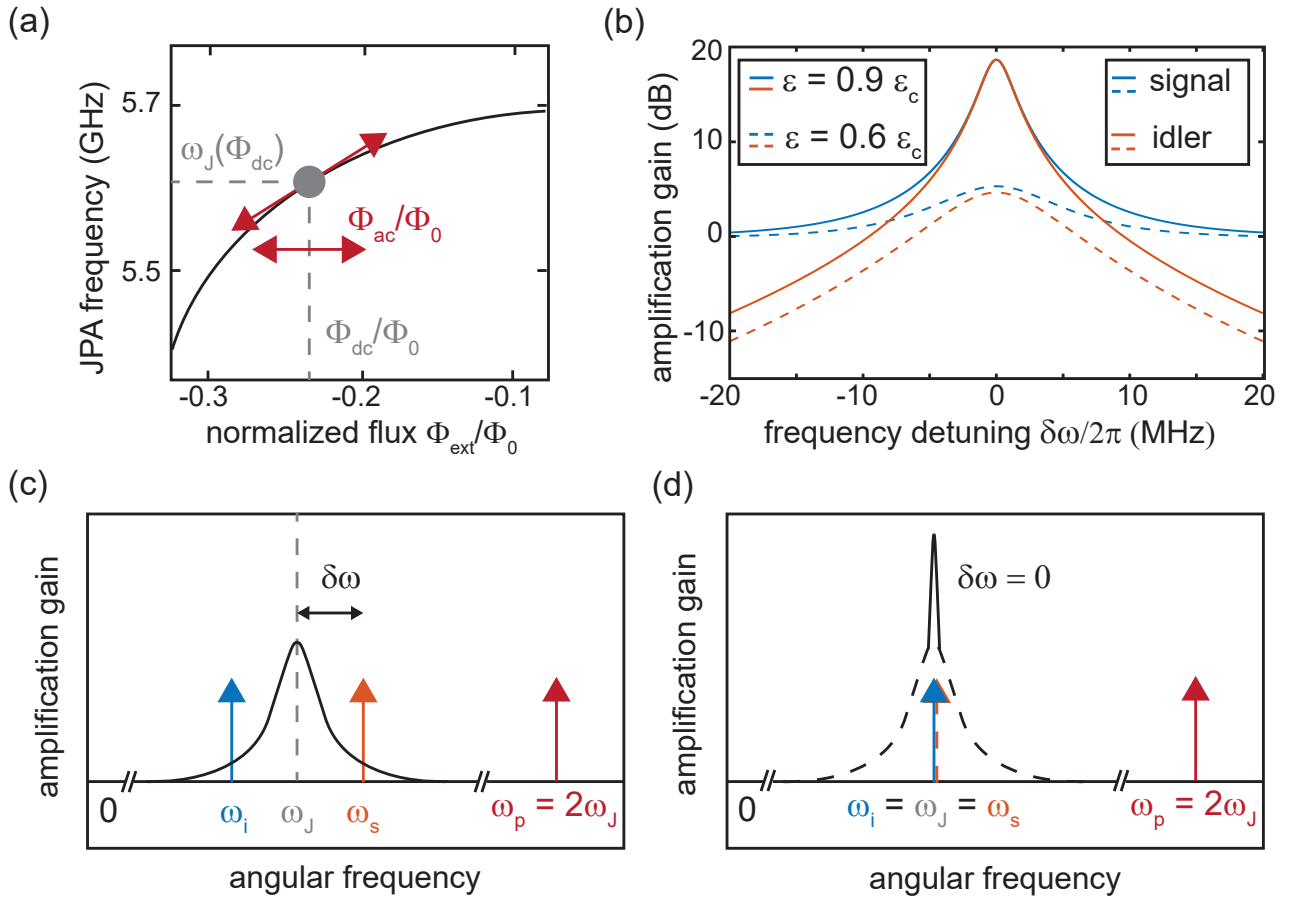


Figure 2.4: Priciple of parametric amplification principle and gain response of a flux-driven JPA. (a) Working principle of a flux-driven JPA. The JPA resonance frequency $\omega_J(\Phi_{dc})$ is adjusted by changing the dc magnetic flux bias while a parametric amplification is induced using an ac flux drive $\Phi_{ac}$ by applying a pump signal at the frequency $\omega_p = 2\omega_J$. (b) Signal and idler gain of the flux-driven JPA operated in the nondegenerate regime. This plot is obtained using Eq. (2.51) for the quality factors $Q_{ext} = 250$ and $Q_{int} = 2500$ at the resonance frequency of $\omega_J = 5.5\,\text{GHz}$ and different pump strengths $\epsilon$. (c) Scheme of the nondegenerate parametric amplification, characterized by a nonzero detuning $\delta\omega \neq 0$, signal frequency $\omega_s = \omega_p/2 + \delta\omega$, and idler frequency $\omega_i = \omega_p/2 - \delta\omega$. (d) Scheme of the degenerate parametric amplification obtained in the case of $\delta\omega = 0$. In this case, the amplification gain depends on the signal phase. In the panel, we illustrate the case of maximal amplification gain.

We note that Eq. (2.51) implies gain values necessarily greater than or equal to one, meaning that the amplitude of the input signal is unchanged or amplified. The signal and idler gain values are shown in Fig. 2.4(b). From Eq. (2.51), we note that the gain profile presents a Lorentzian shape with a full width half maximum $\Gamma_J = (\epsilon_c^2 - \epsilon^2)\omega_J/\sqrt{2(\epsilon_c^2 + \epsilon^2)}$ and a corresponding maximal gain $G_{max} = 4\epsilon_c^2\epsilon^2/(\epsilon_c^2 - \epsilon^2)^2$. We compute a gain-bandwidth product (GBP) $\tau_J$ of the JPA given by [50]

$$\tau_J = \sqrt{G_J}\Gamma_J = \frac{\epsilon_c\omega_J}{2}\left(1 + \frac{\epsilon_c}{\epsilon}\right) + o\left(\frac{\epsilon_c}{\epsilon}\right). \tag{2.52}$$

Here, we see that the GBP approaches a constant value of $\kappa/2$ as the pump power gets closer to the critical pump value, $\epsilon_c$. This result implies that the amplification gain is inversely proportional to the amplification bandwidth. In this work, we operate the JPA in the overcoupled regime where $\kappa_{ext} \gg \kappa_{int}$, resulting in a GBP of $\tau_J = \kappa_{ext}/2$. In the case of no detuning, $\delta\omega = 0$, the signal and idler mode are degenerate in frequency and can coherently interfere with each other [78]. We refer to this regime as *degenerate* amplification as shown in Fig. 2.4(d). Contrary to the nondegenerate amplification regime, the degenerate amplification gain is sensitive to the

phase $\theta_\mathrm{s}$ of the input signal. The degenerate gain is given by [74]

$$\begin{aligned} G_\mathrm{s}(\theta_\mathrm{s}) &= \left| M_\mathrm{in}(0)e^{i\theta_\mathrm{s}} + L_\mathrm{in}(0)e^{-i\theta_\mathrm{s}} \right|^2 \\ &= \frac{(\frac{\kappa_\mathrm{ext}^2-\kappa_\mathrm{int}^2}{2} + \epsilon^2\omega_\mathrm{J}^2)^2 + \kappa_\mathrm{ext}^2\epsilon^2\omega_\mathrm{J}^2 - 2\kappa_\mathrm{ext}\epsilon\omega_\mathrm{J}\left(\frac{\kappa_\mathrm{ext}^2-\kappa_\mathrm{int}^2}{4} + \epsilon^2\omega_\mathrm{J}^2\right)\sin(2\theta_\mathrm{s})}{\left(\frac{\kappa^2}{4} - \epsilon^2\omega_\mathrm{J}^2\right)^2}. \end{aligned} \tag{2.53}$$

Here, it is possible to reach a regime where $G_\mathrm{s} < 1$ for a certain input signal phase, resulting in a deamplification of the input signal. In particular, we obtain the maximal gain for $\theta_\mathrm{s} = 3\pi/4 + z\pi$ for $z \in \mathbb{Z}$ and the minimal gain for $\theta_\mathrm{s} = \pi/4 + z\pi$. The corresponding maximal and minimal gains are given by

$$G_{s,\max} = \left(\frac{\epsilon\omega_\mathrm{J} - \frac{\kappa_\mathrm{ext}-\kappa_\mathrm{int}}{2}}{\epsilon\omega_\mathrm{J} + \frac{\kappa_\mathrm{ext}+\kappa_\mathrm{int}}{2}}\right)^2, \quad G_{s,\min} = \left(\frac{\epsilon\omega_\mathrm{J} + \frac{\kappa_\mathrm{ext}-\kappa_\mathrm{int}}{2}}{\epsilon\omega_\mathrm{J} - \frac{\kappa_\mathrm{ext}+\kappa_\mathrm{int}}{2}}\right)^2. \tag{2.54}$$

In the limit of a strongly overcoupled JPA, $\kappa_\mathrm{ext} \gg \kappa_\mathrm{int}$, we find that $G_{s,\max}\, G_{s,\min} = 1$, meaning that for a certain phase the input signal is maximally amplified, while it is maximally deamplified for the input phase value changed by 90°. As explained later in Sec. 2.2.1, the phase-sensitive amplification is closely related to the squeezing operation that can be implemented with overcoupled JPAs.

**Standard quantum limit.** In the following, we briefly comment on the quantum mechanical description of linear amplification. The fundamental difference to a classical treatment is the necessity that all involved quantum bosonic modes obey the bosonic commutation relation. This has crucial implications for the noise properties of the amplification process. In particular, the Haus-Caves [79, 80] theorem states that it is not possible to perform a noiseless linear phase-preserving amplification. Therefore, to ensure that both the input mode $\hat{a}$ and its corresponding output mode $\hat{a}'$ after phase-preserving amplification are bosonic modes, the input-output relation must take the form [81]

$$\hat{a}' = \sqrt{G_\mathrm{s}}\hat{a} + \sqrt{G_\mathrm{s} - 1}\hat{h}^\dagger, \tag{2.55}$$

where $G_\mathrm{s}$ is the phase-preserving amplification gain and $\hat{h}$ is a bosonic noise operator reflecting that the input modes are coupled to a thermal bath [81]. It can be straightforwardly verified that the output mode operator fulfills the bosonic commutation relation. A total, average number of photons $N$ in the amplified mode can be computed as

$$N = \frac{\left\langle \hat{a}'(\hat{a}')^\dagger + (\hat{a}')^\dagger\hat{a}' \right\rangle}{2} = G_\mathrm{s}\frac{\left\langle \hat{a}\hat{a}^\dagger + \hat{a}^\dagger\hat{a} \right\rangle}{2} + (G_\mathrm{s} - 1)\frac{\left\langle \hat{h}\hat{h}^\dagger + \hat{h}^\dagger\hat{h} \right\rangle}{2}, \tag{2.56}$$

where we use that the signal and noise operators commute. The last equation indicates that the output power is composed of both amplified input photons and added noise photons. From Eq. (2.56), the average added noise in units of photons, $A_\mathrm{amp}$, referred to the input the amplifier is calculated as [80]

$$A_\mathrm{amp} = \frac{(G_\mathrm{s} - 1)}{G_\mathrm{s}}\frac{\left\langle \hat{h}\hat{h}^\dagger + \hat{h}^\dagger\hat{h} \right\rangle}{2} = \frac{(G_\mathrm{s} - 1)}{G_\mathrm{s}}\left(\left\langle \hat{h}^\dagger\hat{h} \right\rangle + \frac{1}{2}\right) \geq \frac{1}{2}\left(1 - \frac{1}{G_\mathrm{s}}\right). \tag{2.57}$$

The last inequality is obtained by noticing that $\langle \hat{h}^\dagger\hat{h} \rangle$ is the average noise photon number and is bounded from below by 0. The inequality in Eq. (2.57) is commonly known as the standard

quantum limit (SQL) of linear amplification [80, 82]. This fundamental limit implies that any nondegenerate amplification process adds at least the vacuum variance to output signal variances. This result is rooted in the Heisenberg uncertainty relation. The added noise can be evaluated using the quantum efficiency $\eta$ [73], defined as the ratio between the input and output signal-to-noise ratios. The corresponding expression can be simplified to

$$\eta = \frac{1}{1 + 2A_{\mathrm{amp}}}. \tag{2.58}$$

According to the SQL, the quantum efficiency of any degenerate linear amplifier is at most 1/2. Conversely, in the degenerate amplification regime, the SQL can be violated. As shown in Eq. (2.54), noiseless amplification is allowed in this regime, as expected from the Heisenberg uncertainty. This fundamental difference can be illustrated in the input-output relation obtained in Eq. (2.55) by replacing the mode $\hat{h}$ by the signal mode, $\hat{a}^\dagger$, representing the interference with the idler mode. The resulting transformation can also be described as a squeezing operation, as explained later in Sec. 2.2.2. Furthermore, one can derive a more general expression for the SQL using the Haus-Caves theorem. With respective gain values $G_1$ and $G_2$, the average noise $A_1$ and $A_2$ in units of photons added to orthogonal signal quadratures, follows the inequality [80, 81]

$$A_1 A_2 \geq \frac{1}{16}\left|1 - \frac{1}{\sqrt{G_1 G_2}}\right|^2, \tag{2.59}$$

Here, we observe that under the condition $G_1 G_2 = 1$, noiseless, phase-sensitive amplification is possible. Lastly, we can define a quadrature-dependent quantum efficiency, $\eta_\theta$, similarly to the nondegenerate amplification case [73]

$$\eta_\theta = \frac{1}{1 + 2A_\theta}, \tag{2.60}$$

where $A_\theta$ is the average noise in units of photons added to the signal quadrature defined by the signal phase $\theta$. In this thesis, we refer to the quadrature quantum efficiency as $\eta_{\mathrm{X}}$, where $X$ stands for either the $q$- or the $p$-quadrature. Since a degenerate amplification can be fundamentally noiseless, the quadrature-dependent quantum efficiency is limited to 1.

## 2.2 Continuous-variable quantum information

In this section, we focus on continuous-variable quantum states and their associated physical properties. In Sec. 2.2.1, we present a general formalism for quantum states which is particularly suited to describe Gaussian states. In Sec. 2.2.2, we introduce such Gaussian states as well as Gaussian channels which are used in communication protocols. In Sec. 2.2.3, general expressions for quantum entanglement and the entropy of quantum states are presented.

### 2.2.1 Representation of quantum microwave signals

In this work, we measure microwave signals with carrier frequencies in the range of 4-6 GHz. Classically, a signal mode is described using a mode at angular frequency $\omega_{\mathbf{k}}$ with an associated electric field at the position $\mathbf{r}$ as

$$E_{\mathbf{k}}(\mathbf{r}, t) = I(t)\cos(\omega_{\mathbf{k}} t - \mathbf{r}\cdot\mathbf{k} + \theta_{\mathrm{ref}}) + Q(t)\sin(\omega_{\mathbf{k}} t - \mathbf{r}\cdot\mathbf{k} + \theta_{\mathrm{ref}}), \tag{2.61}$$

where $\mathbf{k}$ is the corresponding wave vector and $I$ ($Q$) is the in-phase (out-of-phase) quadrature component of the field. Additionally, $\theta_{\mathrm{ref}}$ is the phase reference. Similarly, one defines the

quantized electric field using bosonic annihilation and creation operators, $\hat{a}_{\mathbf{k}}$ and $\hat{a}_{\mathbf{k}}^{\dagger}$, as [26]

$$\begin{aligned}\hat{E}_{\mathbf{k}}(\mathbf{r},t) &= E_0(\hat{a}_{\mathbf{k}}e^{i(\omega_{\mathbf{k}}t-\mathbf{r}\cdot\mathbf{k}+\theta_{\text{ref}})} + \hat{a}_{\mathbf{k}}^{\dagger}e^{-i(\omega_{\mathbf{k}}t-\mathbf{r}\cdot\mathbf{k}+\theta_{\text{ref}})}) \\ &= 2E_0(\hat{q}_{\mathbf{k}}^{\theta_{\text{ref}}}\cos(\omega_{\mathbf{k}}t-\mathbf{r}\cdot\mathbf{k}+\theta_{\text{ref}}) + \hat{p}_{\mathbf{k}}^{\theta_{\text{ref}}}\sin(\omega_{\mathbf{k}}t-\mathbf{r}\cdot\mathbf{k}+\theta_{\text{ref}})),\end{aligned} \tag{2.62}$$

where we have introduced the rotated quadratures $\hat{q}_{\mathbf{k}}^{\theta_{\text{ref}}}$ and $\hat{p}_{\mathbf{k}}^{\theta_{\text{ref}}}$ which are the quantum counterpart of the in-phase and out-of-phase classical quadratures $I$ and $Q$. Additionally, $E_0$ defines the field amplitude. The rotated quadratures are defined as

$$\hat{q}_{\mathbf{k}}^{\theta_{\text{ref}}} = \frac{\hat{a}_{\mathbf{k}}e^{-i\theta_{\text{ref}}} + \hat{a}_{\mathbf{k}}^{\dagger}e^{i\theta_{\text{ref}}}}{2} \quad \text{and} \quad \hat{p}_{\mathbf{k}}^{\theta_{\text{ref}}} = \frac{\hat{a}_{\mathbf{k}}e^{-i\theta_{\text{ref}}} - \hat{a}_{\mathbf{k}}^{\dagger}e^{i\theta_{\text{ref}}}}{2i}. \tag{2.63}$$

The reference phase is conventionally set to zero which leads to $\hat{q}_{\mathbf{k}} \coloneqq \hat{q}_{\mathbf{k}}^{0}$ and $\hat{p}_{\mathbf{k}} \coloneqq \hat{p}_{\mathbf{k}}^{0}$ with the commutation relation $[\hat{q}_{\mathbf{k}}, \hat{p}_{\mathbf{k}}] = 1/2i$. The quadratures fulfil the Heisenberg uncertainty relation

$$(\Delta\hat{q}_{\mathbf{k}})^2(\Delta\hat{p}_{\mathbf{k}})^2 = (\langle\hat{q}_{\mathbf{k}}^2\rangle - \langle\hat{q}_{\mathbf{k}}\rangle^2)(\langle\hat{p}_{\mathbf{k}}^2\rangle - \langle\hat{p}_{\mathbf{k}}\rangle^2) \geq \frac{1}{4}\left|\langle[\hat{q}_{\mathbf{k}}, \hat{p}_{\mathbf{k}}]\rangle\right|^2 = \frac{1}{16}. \tag{2.64}$$

The relation in Eq. (2.64) is at the core of this work and represents the basis for protocols presented in later sections. Remarkably, the quadrature operators form a continuum of observables and, as a result, have a continuous spectrum of eigenvalues and corresponding eigenvectors living in a Hilbert space of infinite dimension. Therefore, one commonly speaks of continuous-variable states. Here, these quantum states can be described using a density matrix in the form

$$\hat{\rho} = \sum_i \langle\psi_i|\hat{\rho}|\psi_i\rangle|\psi_i\rangle\langle\psi_k| = \sum_i p_i|\psi_i\rangle\langle\psi_i|, \tag{2.65}$$

where $p_i$ is the probability of the state to be measured in the state $i$ for a given basis $\{|\psi_i\rangle\}_i$. The coefficients $p_i$ are positive real numbers which are normalized by $\sum_i p_i = 1$, meaning $\text{Tr}(\hat{\rho}) = 1$. Here, a commonly used basis is the Fock state basis $\{|n\rangle\}_{n\in[0,+\infty]}$ corresponding to eigenvectors of the photon number operator, $\hat{n} \coloneqq \hat{a}^{\dagger}\hat{a}$. The expectation value of a given operator $\hat{A}$ can be computed using the Born rule, $\langle\hat{A}\rangle = \text{Tr}(\hat{\rho}\hat{A})$. In particular, the purity of a state is computed as $\text{Tr}(\hat{\rho}^2)$ and is either one or less than one. A purity of one implies that the quantum state is pure meaning that it is possible to find a certain ket $|\psi^{\star}\rangle$ such that the associated density matrix $\hat{\rho}^{\star} = |\psi^{\star}\rangle\langle\psi^{\star}|$. Conversely, when a state cannot be described using only a single ket, it is referred to as a *mixed* state with a purity strictly less than one. A general structure of a mixed state is given by Eq. (2.65).

In the framework of continuous variable states, it is convenient to introduce a mapping from the space of density matrices to complex-valued multidimensional functions. Such a mapping allows for an easier and more intuitive representation of quantum states. A particular mapping approach is provided by the Wigner function formalism, although we note that other approaches exist, such as $P$ or $Q$-functions [83, 84]. All these mappings are equivalent to each another. For a given single mode associated with a density matrix $\hat{\rho}$, the Wigner function is defined as [85]

$$W_{\hat{\rho}}(q,p) = \frac{2}{\pi}\int_{-\infty}^{+\infty} e^{4iyp}\langle q-y|\hat{\rho}|q+y\rangle \mathrm{d}y. \tag{2.66}$$

The classical variables, $q$ and $p$, are associated with the $\hat{q}$ and $\hat{p}$ quadrature operators, respectively. Here, we explicitly highlight the dependence of $W$ on $\hat{\rho}$, which is useful for further derivations in this chapter. This definition can also be straightforwardly extended to $N$ modes. The Wigner function possesses properties similar to a classical probability distribution. It is normalized to unity and can be used to obtain marginal distribution probabilities, meaning that

$$\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} W_{\hat{\rho}}(q,p)\mathrm{d}q\mathrm{d}p = 1, \ \int_{-\infty}^{+\infty} W_{\hat{\rho}}(q,p)\mathrm{d}p = \langle q|\hat{\rho}|q\rangle, \ \int_{-\infty}^{+\infty} W_{\hat{\rho}}(q,p)\mathrm{d}q = \langle p|\hat{\rho}|p\rangle. \tag{2.67}$$

We note, however, that the Wigner function lacks the positivity property. This implies that it can become negative locally and, therefore, is commonly denoted as a quasi-probability distribution. Remarkably, the Wigner function can be used to compute an expectation value of a given operator $\hat{A}$,

$$\langle \hat{A} \rangle = \mathrm{Tr}(\hat{\rho}\hat{A}) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} W_{\hat{\rho}}(q,p)\tilde{A}(q,p)\mathrm{d}q\mathrm{d}p, \tag{2.68}$$

where the function $\tilde{A}$ is related to the operator $\hat{A}$ via the Weyl transformation [26, 86]

$$\tilde{A}(q,p) = \int_{-\infty}^{+\infty} e^{4iyp}\langle q-y|\hat{A}|q+y\rangle \mathrm{d}y = \frac{\pi}{2} W_{\hat{A}}(q,p). \tag{2.69}$$

Using Eq. (2.69) and the integral identity $\int e^{4iyp}\mathrm{d}p = (\pi/2)\delta(y)$, the following relation is obtained for the operators $\hat{A}$ and $\hat{B}$

$$\mathrm{Tr}(\hat{A}\hat{B}) = \frac{4}{\pi} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \tilde{A}(q,p)\tilde{B}(q,p)\mathrm{d}q\mathrm{d}p. \tag{2.70}$$

Using Eq. (2.68), one further can derive for integers $m, n \in \mathbb{N}$ the important expression [26]

$$\mathrm{Tr}(\hat{\rho}\mathcal{S}(\hat{q}^m\hat{p}^n)) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} W_{\hat{\rho}}(q,p) q^m p^n \mathrm{d}q\mathrm{d}p, \tag{2.71}$$

where $\mathcal{S}$ denotes the symmetrization superoperator, e.g., $\mathcal{S}(\hat{q}^2\hat{p}) = (\hat{q}^2\hat{p}+\hat{q}\hat{p}\hat{q}+\hat{p}\hat{q}^2)/3$ [87]. This expression is particularly relevant for computing moments of averaged density matrices, since the Wigner function is a linear mapping. Additionally, we define the characteristic function (CF), $\chi$, of the normally ordered moments $\langle (\hat{a}^\dagger)^m \hat{a}^n \rangle$, with $(m,n) \in \mathbb{N}^2$, where we consider a single mode leading to

$$\chi(x,y) = \langle \exp(x\hat{a}^\dagger)\exp(-y\hat{a})\rangle. \tag{2.72}$$

This definition can also be straightforwardly extended to $N$ modes. From Eq. (2.72) one derives that

$$\langle (\hat{a}^\dagger)^m \hat{a}^n \rangle = (-1)^n \frac{\partial^{n+m}\chi}{\partial x^n \partial y^m}(x,y)\Big|_{x=0,y=0}. \tag{2.73}$$

Computation of the CF for a given density matrix $\hat{\rho}$ provides a direct analytical expression of normally ordered moments to any order and is particularly relevant to compare high order moments measured in experiments to theoretical expressions. Lastly, for a given $N$-mode quantum state, it is useful to introduce two quantities that describe the underlying statistics of this quantum state. First, we introduce a vector of quadratures $\hat{x} = (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_N, \hat{p}_N)$ and define the associated displacement vector, $\mathbf{d} = \langle \hat{x} \rangle$, containing the expectation values of all individual quadratures. Then, we introduce the covariance matrix, $\mathbf{V}$, of the quantum state which components are defined as

$$(\mathbf{V})_{i,j} = \frac{\langle \hat{x}_i\hat{x}_j + \hat{x}_j\hat{x}_i \rangle}{2} - \langle \hat{x}_i \rangle \langle \hat{x}_j \rangle \quad \text{for } (i,j) \in [1,N]^2. \tag{2.74}$$

Note that for any $N$-mode quantum state, the resulting covariance matrix is a square $2N \times 2N$ matrix.

### 2.2.2 Gaussian states and Gaussian channels

In this section, we focus on a subset of quantum states called Gaussian states. This category of quantum states is beneficial for many quantum communication protocols [6, 24, 88, 89]. Gaussian states are fully described by their displacement vector $\mathbf{d}$ and covariance matrix $\mathbf{V}$. The Wigner function of a Gaussian state is a multidimensional Gaussian function, written in the form [6]

$$W_{\hat{\rho}}(\mathbf{X}) = \frac{1}{(2\pi)^N\sqrt{\det(\mathbf{V})}}\exp\left(-\frac{1}{2}(\mathbf{X}-\mathbf{d})\mathbf{V}^{-1}(\mathbf{X}-\mathbf{d})^T\right), \tag{2.75}$$

where $N$ is the number of modes in the state and $\mathbf{X} = (q_1, p_1, \ldots, q_N, p_N)$ is a vector of variables each corresponding to one pair of quadrature operators. Using Eq. (2.70) and Eq. (2.75), we derive the expression of the purity, $\mu \coloneqq \mathrm{Tr}(\hat{\rho}^2)$, for Gaussian states

$$\mu = \pi^N \int W_{\hat{\rho}}(\mathbf{X})^2 \mathrm{d}\mathbf{X} = \frac{1}{4^N\sqrt{\det(\mathbf{V})}}. \tag{2.76}$$

From Eqs, 2.64 and 2.76, we obtain that a pure state, for which $\mu = 1$, saturates the Heisenberg inequality, as in that case $\sqrt{\det(\mathbf{V})} = 4^{-N}$. Conversely, a maximally mixed state is obtained for $\mu \to 0$ when $\det(\mathbf{V}) \to +\infty$.

The most fundamental Gaussian state is the vacuum state, which is defined as the ground state of a quantum harmonic oscillator satisfying the Heisenberg uncertainty relation. As such, we can ascribe the temperature $T = 0$ to the vacuum state. This state is associated with a finite amount of fluctuations corresponding to the energy of half a photon at the chosen mode frequency. These fluctuations correspond to quadrature variances of $(\Delta\hat{q})^2 = (\Delta\hat{p})^2 = 1/4$. The corresponding Wigner function plot is shown in Fig. 2.5(a). For a finite temperature $T > 0$, there will be a nonzero number of thermal noise photons in the mode, which gives rise to a thermal state. Its density matrix can be computed using the canonical partition sum [90]

$$\hat{\rho}_{\mathrm{th}} = \sum_{n=0}^{+\infty} \frac{\bar{n}_{\mathrm{th}}^n}{(1+\bar{n}_{\mathrm{th}})^{1+n}}|n\rangle\langle n|, \quad \bar{n}_{\mathrm{th}}(\omega, T) = \mathrm{Tr}(\hat{\rho}_{\mathrm{th}}\hat{a}^\dagger\hat{a}) = \frac{1}{\exp\left(\hbar\omega/(k_{\mathrm{B}}T)\right) - 1}. \tag{2.77}$$

The thermal state displacement vector $\mathbf{d}$ is equal to zero, while its covariance matrix can be written as $\mathbf{V} = (1 + 2\bar{n}_{\mathrm{th}})\mathbf{I}_2/4$, where $\mathbf{I}_N$ is the identity matrix of dimension $N$. In Fig. 2.5(b), we plot the Wigner function of the thermal state with the photon number $\bar{n}_{\mathrm{th}} = 2$. The Wigner function of a thermal state and its purity reads

$$W_{\mathrm{th}}(q,p) = \frac{2}{\pi(1+2\bar{n}_{\mathrm{th}})}\exp\left(-\frac{2(q^2+p^2)}{1+2\bar{n}_{\mathrm{th}}}\right) \quad \text{and} \quad \mu_{\mathrm{th}} = \frac{1}{1+2\bar{n}_{\mathrm{th}}}. \tag{2.78}$$

From Eq. (2.78) we note that the Wigner function of a thermal state is invariant under rotation around the origin of the Wigner space, meaning that thermal noise is distributed equally among quadratures. The purity coincides with the definition of the quantum efficiency and is a good measure of the average number of thermal photons.

The next type of a Gaussian state is a coherent state, $|\alpha\rangle$, where $\alpha = q + ip$ is a complex amplitude. A coherent state is defined as an eigenvector of the annihilation operator, $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$. An intuitive picture of coherent states can be obtained by considering the fact that the displacement operator $\hat{D}$ applied to the vacuum state results in $\hat{D}(\alpha)|0\rangle = |\alpha\rangle$ [51]. The corresponding Wigner function and is shown in Fig. 2.6(a). From the definition of the displacement operator [91]

$$\hat{D}(\alpha) = \exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a}), \tag{2.79}$$

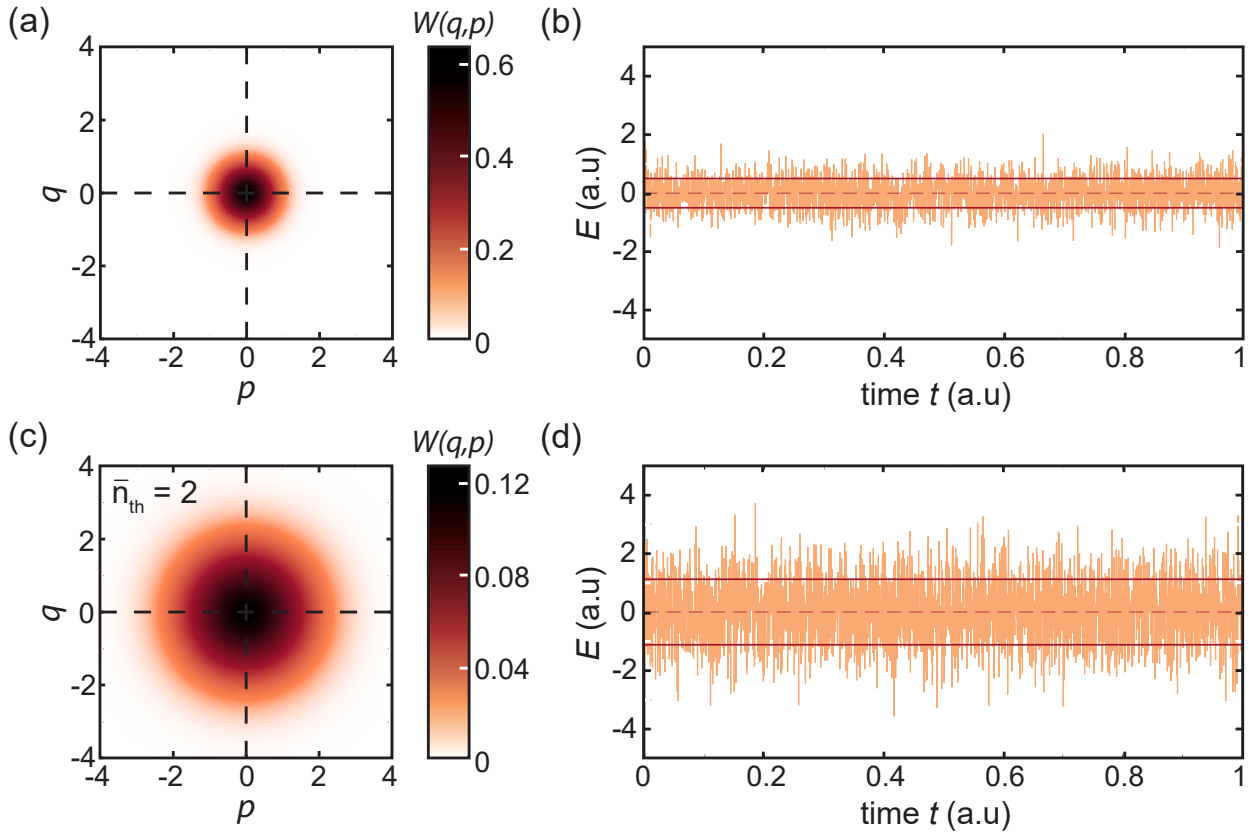


Figure 2.5: Wigner function and time evolution of its associated electric field amplitude for the vacuum state (panels $(a)$ and $(b)$) and a thermal state (panels $(c)$ and $(d)$) with the photon number $\bar{n}_{\mathrm{th}} = 2$. The points shown in orange are 3000 random samplings of the multivariate Gaussian distribution describing the $\hat{q}$- and $\hat{p}$-quadratures associated with the Gaussian state. The dashed line corresponds to the mean field amplitude, while the solid line represents the $1\sigma$ confidence interval of field fluctuations.

one can derive the important property, $\hat{D}^\dagger(\alpha)\hat{a}\hat{D} = \hat{a} + \alpha$. This means that any coherent state can be obtained by displacing the vacuum state in phase space, corresponding to a displacement vector $\mathbf{d} = |\alpha|^2 (\cos(\theta_\alpha), \sin(\theta_\alpha))$ with $\theta_\alpha = \arg(\alpha)$. At the same time, the displacement operation leaves the covariance matrix of the vacuum state unchanged. As the displacement operator is unitary, this also implies that coherent states are pure states.

Finally, we consider squeezed vacuum state. There are another kind of minimum-uncertainty states, with a corresponding purity $\mu = 1$, obtained by reducing the variance of one quadrature below vacuum fluctuations, while the conjugate quadrature variance is correspondingly increased. In this case, one commonly says that one quadrature is *squeezed* while its corresponding conjugate quadrature is *antisqueezed*. More precisely, the induced unitary transform is modelled using the squeezing operator [92]

$$\hat{S}(\xi) = \exp\left[\frac{1}{2}\xi^*\hat{a}^2 - \frac{1}{2}\xi(\hat{a}^\dagger)^2\right], \tag{2.80}$$

where $\xi = re^{i\varphi}$ parametrizes the properties of the squeezing operator, namely the squeezing factor $r = |\xi|$ and phase $\varphi = \arg(\xi)$. Squeezed states are obtained by applying the squeezing operator to the vacuum state, $|\xi\rangle = \hat{S}(\xi)|0\rangle$.

The Wigner function of a squeezed state is shown in Fig. 2.6(c). The squeezing factor $r$ defines an amplitude of variance squeezing while the phase $\varphi$ determines the orientation of the squeezed state in phase space [93]. Commonly, the squeezing direction is parametrized via the squeezing angle, $\gamma = -\varphi/2$, which can be understood as the angle between the antisqueezed

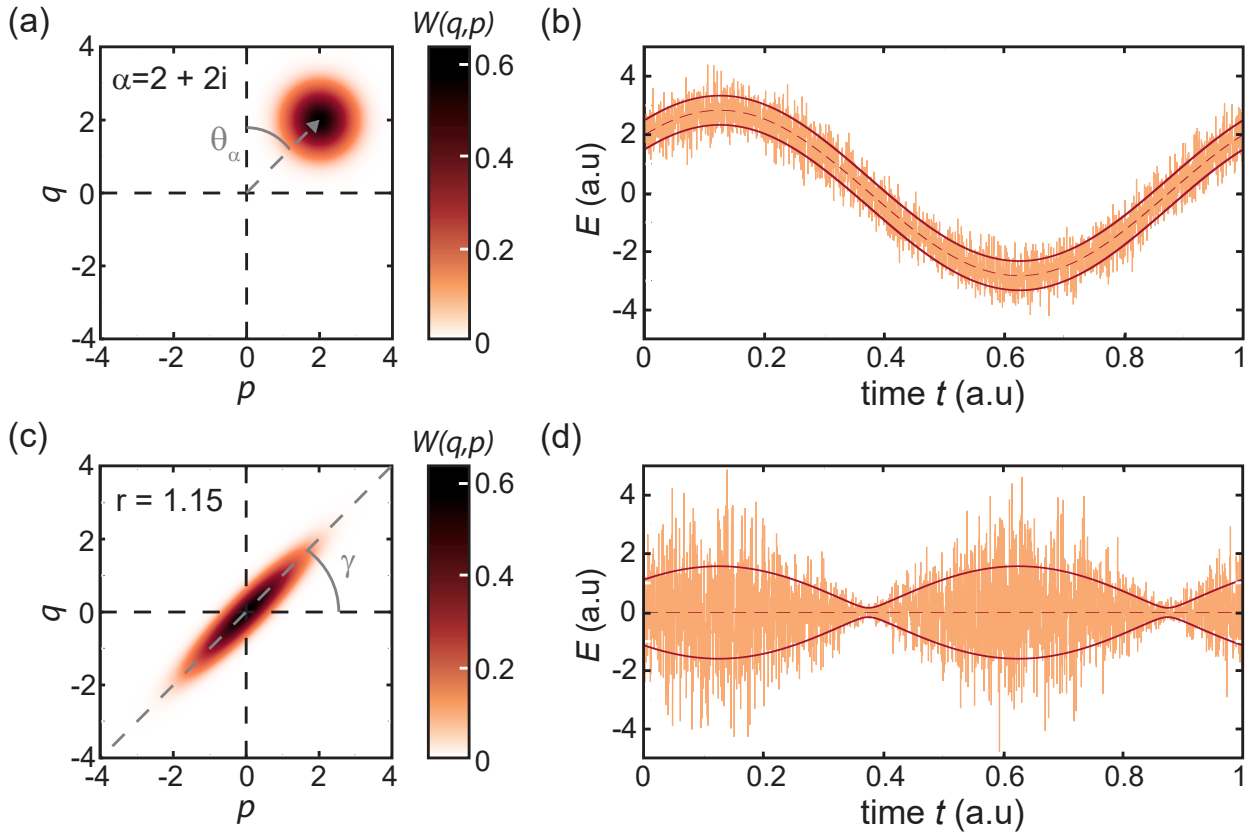


Figure 2.6: Wigner function of a coherent state (a) and a squeezed state (c) together with the time traces [(b) and (d)] of the associated electric fields. For the coherent state (panels (a) and (b)) we assumed a complex displacement amplitude $\alpha = 2 + 2i$ (corresponding to the displacement angle $\theta_\alpha$). For the squeezed state (panels (c) and (d)) we assumed a squeezing angle $\gamma = \pi/4$ and squeezing factor $r = 1.15$, resulting in a squeezing level of $S = 10\,\mathrm{dB}$ below vacuum. The points in orange represent 3000 random samplings of the multivariate Gaussian distribution describing the $\hat{q}$- and $\hat{p}$-quadratures associated with the Gaussian state. The dashed line corresponds to the mean field amplitude, while the solid line represents the $1\sigma$ confidence interval of field fluctuations.

quadrature and the $p$-axis of phase space. The squeezing operator induces the following transformation of the annihilation operator

$$\hat{S}^\dagger \hat{a} \hat{S} = \cosh(r)\hat{a} - e^{i\varphi}\sinh(r)\hat{a}^\dagger. \tag{2.81}$$

We note that Eq. (2.81) is structurally similar to Eq. (2.55) with the difference that no additional mode $\hat{h}$ appears. Interestingly, any squeezed state can be decomposed in the Fock basis as [92]

$$|\xi\rangle = \sum_{n=0}^{+\infty} (-1)^n \frac{\sqrt{(2n)!}}{2^n n!} \frac{(e^{i\varphi}\tanh(r))^n}{\sqrt{\cosh(r)}} |2n\rangle, \tag{2.82}$$

meaning that a pure squeezed state only contains an even number of photons, corresponding to the signal and idler modes. This fact hints at the possibility of using squeezed states for generating quantum entanglement. The displacement vector of a squeezed vacuum state is $\mathbf{d}_{\mathrm{sq}} = \mathbf{0}$ and its corresponding covariance matrix can be written as

$$\mathbf{V}_{\mathrm{sq}} = \frac{1}{4}\begin{pmatrix} e^{-2r}\cos^2(\gamma) + e^{2r}\sin^2(\gamma) & -\sinh(2r)\cos(2\gamma) \\ -\sinh(2r)\cos(2\gamma) & e^{2r}\cos^2(\gamma) + e^{-2r}\sin^2(\gamma) \end{pmatrix}. \tag{2.83}$$

From a practical point of view, it is convenient to define a squeezing (antisqueezing) level, $S$ ($AS$), comparing the variance $\sigma_{\mathrm{s}}^2$ ($\sigma_{\mathrm{as}}^2$) of the squeezed (antisqueezed) quadrature to that of the

vacuum state, yielding [50]

$$S = -10\log_{10}\left(\frac{\sigma_{\mathrm{s}}^2}{1/4}\right), \quad AS = 10\log_{10}\left(\frac{\sigma_{\mathrm{as}}^2}{1/4}\right). \tag{2.84}$$

Using Eq. (2.84), we can reformulate the Heisenberg uncertainty relation as $AS - S \geq 0$.

Using the previously introduced states, we can describe an arbitrary Gaussian state. More precisely, according to the Williamson theorem, any Gaussian state can be written as [94]

$$\hat{\rho} = \hat{D}(\alpha)\hat{S}(\xi)\hat{\rho}_{\mathrm{th}}\hat{S}^{\dagger}(\xi)\hat{D}(\alpha)^{\dagger}. \tag{2.85}$$

This implies that any Gaussian state can be viewed as a displaced squeezed thermal state, which is entirely characterized by the complex numbers $\xi$, $\alpha$, and thermal population $\bar{n}_{\mathrm{th}}$. Additionally, although the displacement and squeezing operators do not commute, the general decomposition of a Gaussian state can also be performed with the sequence of these operators reversed. This means that the same density matrix as in Eq. (2.85) can be written as

$$\hat{\rho} = \hat{S}(\xi')\hat{D}(\alpha')\hat{\rho}_{\mathrm{th}}\hat{D}(\alpha')^{\dagger}\hat{S}^{\dagger}(\xi'), \tag{2.86}$$

where $\xi = re^{i\varphi}$ is chosen such that

$$\alpha = \cosh(r)\alpha' - e^{i\varphi}\sinh(r)(\alpha')^{*}. \tag{2.87}$$

The last state of interest is the two-mode squeezed (TMS) state, which is commonly regarded as the continuous-variable equivalent to Bell states [95]. The TMS state is generated using two modes, $\hat{a}_1$ and $\hat{a}_2$, by applying the two-mode squeezing operator $\hat{S}_{\mathrm{TMS}} = \exp(\xi^{*}\hat{a}_1\hat{a}_2 - \xi\hat{a}_1^{\dagger}\hat{a}_2^{\dagger})$ to the two-mode vacuum, $|0\rangle_{12} = |0\rangle_1|0\rangle_2$. Here, the complex number $\xi = re^{i\varphi}$ has a similar decomposition as for squeezed states. The resulting decomposition of the TMS state in the Fock basis is comparable to that of a squeezed state given in Eq. (2.82) [92]

$$|\mathrm{TMS}\rangle = \sum_{n=0}^{+\infty} \frac{(e^{-i\varphi}\tanh(r))^n}{\cosh(r)}|n\rangle_1|n\rangle_2, \tag{2.88}$$

implying that also pairs of photons are created, albeit in the different modes. The TMS vaccum state has a zero displacement vector and its covariance matrix can be written as

$$\mathbf{V}_{\mathrm{TMS}} = \frac{1}{4}\begin{pmatrix} \cosh(2r)\mathbf{I}_2 & \sinh(2r)(\boldsymbol{\sigma}_{\mathrm{z}}\cos(\varphi) + \boldsymbol{\sigma}_{\mathrm{x}}\sin(\varphi)) \\ \sinh(2r)(\boldsymbol{\sigma}_{\mathrm{z}}\cos(\varphi) + \boldsymbol{\sigma}_{\mathrm{x}}\sin(\varphi)) & \cosh(2r)\mathbf{I}_2. \end{pmatrix}, \tag{2.89}$$

where $\boldsymbol{\sigma}_{\mathrm{z}}$ ($\boldsymbol{\sigma}_{\mathrm{x}}$) is the z (x) Pauli matrix. For simplicity, the phase $\varphi$ is often assumed to be zero. Defining the nonlocal quadratures as $q_{\pm} \coloneqq (q_1 \pm q_2)/\sqrt{2}$ and $p_{\pm} \coloneqq (p_1 \pm p_2)/\sqrt{2}$, one can use a compact form for the TMS Wigner function [92, 96]

$$W_{\mathrm{TMS}}(q_+, q_-, p_+, p_-) = \frac{4}{\pi^2}\exp\left[-\frac{2(q_+^2 + p_-^2)}{e^{2r}} - \frac{2(q_-^2 + p_+^2)}{e^{-2r}}\right]. \tag{2.90}$$

The corresponding TMS Wigner function is shown in Fig. 2.7. In the limit of $r \to +\infty$, Eq. (2.90) implies that $W_{\mathrm{TMS}} \propto \delta(q_-)\delta(p_+)$, indicating that the pairs of quadratures $(q_1, q_2)$ and $(p_1, p_2)$ become perfectly correlated (anticorrelated), similarly to the property of ideal Bell states [3]. Interestingly, the local Wigner function of an ideal TMS state always resembles the thermal state with average thermal photon number $\bar{n}_{\mathrm{th}} = \sinh^2(r)$. However, the nonlocal quadrature correlations in the TMS states represent an extremely useful resource for quantum information processing tasks, including quantum communication and sensing.

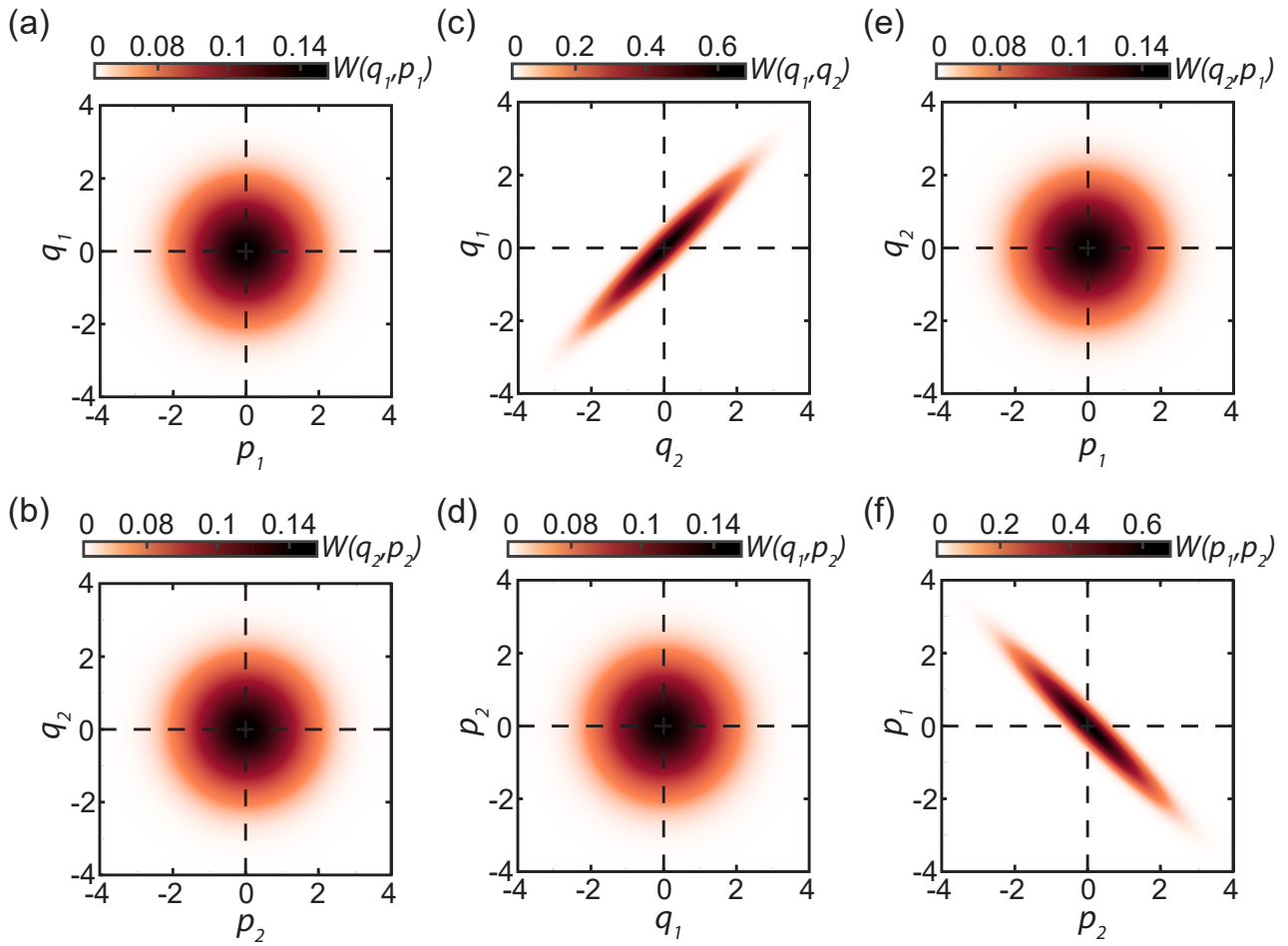


Figure 2.7: Marginal distributions of the Wigner function of a TMS state. The local marginal Wigner functions are shown in panels (a) and (b), resembling local thermal states. The nonlocal marginal Wigner functions are shown in panels (c) - (f). They resemble either a thermal state or a squeezed state. Here, the TMS state is obtained from Eq. (2.88) for the squeezed factor $r = 1$ and phase $\varphi = 0$, resulting in a correlated quadrature pair $(q_1, q_2)$ and anticorrelated quadrature pair $(p_1,p_2)$.

**Gaussian channels.** A quantum channel is said to be Gaussian if it maps Gaussian states to Gaussian states [97]. By this definition, a composition of Gaussian channels is again a Gaussian channel. A general channel $\mathcal{G}$ acting on a Gaussian state $\hat{\rho}_{\mathrm{G}}$ transforms its corresponding displacement vector $\mathbf{d}$ and covariance matrix $\mathbf{V}$ as [98]

$$\mathbf{d} \to \mathbf{T}\mathbf{d} + \mathbf{r} \quad \text{and} \quad \mathbf{V} \to \mathbf{T}\mathbf{V}\mathbf{T}^T + \mathbf{N}, \tag{2.91}$$

where $\mathbf{T}$ and $\mathbf{N}$ are two real matrices describing a physical transformation implemented by the channel. We refer to the matrix $\mathbf{N}$ as the noise matrix. The vector $\mathbf{r}$ represents an induced displacement. The channel itself can be further decomposed into [98]

$$\mathcal{G}(\mathbf{T}, \mathbf{N}, \mathbf{r}) = \mathcal{U}_2 \circ \mathcal{C}(\mathbf{T}_{\mathrm{C}}, \mathbf{N}_{\mathrm{C}}) \circ \mathcal{U}_1, \tag{2.92}$$

where $\mathcal{U}_{1(2)}$ is a unitary mapping and $\mathbf{T}_{\mathrm{C}}$ and $\mathbf{N}_{\mathrm{C}}$ are two real diagonal matrices. Here, the symbol $\circ$ denotes a composition of two mappings, meaning that one is applied after the other. The Gaussian channel $\mathcal{C}$ is referred to as a canonical map and always has a zero induced displacement. In the case of the noise matrix being zero, a Gaussian mapping becomes unitary. This unitary mapping describes a displacement or squeezing operation and the matrix $\mathbf{T}$ becomes a symplectic matrix, meaning that

$$\mathbf{T}\boldsymbol{\Omega}\mathbf{T}^T = \boldsymbol{\Omega}\,, \quad \boldsymbol{\Omega} = \begin{pmatrix} 0 & \mathbf{I}_M \\ -\mathbf{I}_M & 0 \end{pmatrix}, \tag{2.93}$$

where $M$ is the dimension of the covariance matrix $\mathbf{V}$. A displacement map of a single-mode Gaussian state corresponds to the transformation in Eq. (2.91) with $\mathbf{T} = \mathbf{I}_2$ and $\mathbf{r} = (|\alpha|\cos(\theta), |\alpha|\sin(\theta))$ for $\alpha = |\alpha|\, e^{i\theta}$. Similarly, a squeezing map is obtained from the transformation in Eq. (2.91) with the parameters $\mathbf{r} = \mathbf{0}$ and

$$\mathbf{T} = \begin{pmatrix} \cos(\varphi/2) & \sin(\varphi/2) \\ \sin(\varphi/2) & \cos(\varphi/2) \end{pmatrix} \begin{pmatrix} \exp(-r) & 0 \\ 0 & \exp(r) \end{pmatrix}, \tag{2.94}$$

where $re^{i\varphi} = \xi$ parametrizes the squeezing operation. There exist 7 physically possible canonical maps denoted with the letters $A$ to $D$, each letter having two subscripts $1, 2$ for the letters $A$ to $C$ [98]. Here, we focus on classes $B_1, B_2, C_1$, and $C_2$. Canonical maps are parametrized using a generalized transmission coefficient $\tau \in [-\infty, +\infty]$ and a noise photon number $\bar{n}$. We focus on some of these classes for single-mode Gaussian states that are of particular interest for quantum communication. The extension to multimode Gaussian states is done by repeating the transformation induced by the matrices $\mathbf{T}_\mathrm{C}$ and $\mathbf{N}_\mathrm{C}$ to each mode.

**Noise channels.** Classes $B_1$ and $B_2$ both represent additive noise channels, implying that the displacement vectors of input Gaussian states are left unchanged by these channels. The channel $B_1$ represents adding vacuum fluctuations to only the $p$- quadrature and is characterized by the matrices

$$\mathbf{T}_\mathrm{C} = \mathbf{I}_2, \quad \mathbf{N}_\mathrm{C} = \frac{1}{4}\frac{\mathbf{I}_2 - \boldsymbol{\sigma}_\mathrm{Z}}{2}, \tag{2.95}$$

where $\boldsymbol{\sigma}_\mathrm{Z}$ is the z-Pauli matrix. Conversely, the second channel $B_2$ represents addition of noise to both quadratures and is modelled using the matrices

$$\mathbf{T}_\mathrm{C} = \mathbf{I}_2, \quad \mathbf{N}_\mathrm{C} = \frac{\bar{n}}{4}\mathbf{I}_2. \tag{2.96}$$

These channels can be used to model the average total number of noise photons added during amplification of signals. In particular, we can use this type of channel to describe the number of noise photons added during phase-sensitive amplification.

**Attenuation channel.** Channel $C_1$ represents an attenuation channel which has the effect of decreasing the amplitude of the displacement vector of an input Gaussian state by the transmission coefficient, $\tau$, with $\tau \in (0, 1)$. In order to fulfil the Heisenberg uncertainty, the canonical map takes the form [92]

$$\mathbf{T}_\mathrm{C} = \sqrt{\tau}\mathbf{I}_2, \quad \mathbf{N}_\mathrm{C} = (1-\tau)\frac{1+2\bar{n}}{4}\mathbf{I}_2. \tag{2.97}$$

From Eq. (2.97), we observe that an attenuation channel corresponds physically to coupling an input Gaussian state to a thermal background with a mean photon number $\bar{n}$. This coupling is described as a beam splitter type of interaction, which involves two modes $\hat{a}_1$ and $\hat{a}_2$ coupled together via the beam splitter operator

$$\hat{B}_{12}(\theta_\mathrm{b}) = \exp\left[i\theta_\mathrm{b}(\hat{a}_1^\dagger \hat{a}_2 + \hat{a}_1 \hat{a}_2^\dagger)\right]. \tag{2.98}$$

Here, $\theta_\mathrm{b}$ is a free parameter that determines the balancing between two modes, i.e., we construct $\tau$ such that $\sqrt{\tau} = \cos(\theta_\mathrm{b})$ and $\sqrt{1-\tau} = \sin(\theta_\mathrm{b})$. Additionally, we note that the attenuation channel can also be implemented by coupling of an input Gaussian state to one local mode of a TMS state with $\cosh(r) = 1 + 2\bar{n}$. This result implies that it is impossible to locally distinguish coupling an input state to either a thermal background or to a TMS state. One needs to exploit nonlocal measurements for this task.

**Amplification channel.** Channel $C_2$ is an amplification channel which has the effect of increasing the amplitude of the displacement vector of an input Gaussian state by the transmission coefficient, $\tau$, with $\tau > 1$. This channel represents the physical amplification of a Gaussian state corresponding to the process of nondegenerate amplification, due to the fact that the channel adds at least half a noise photon to input states. Similarly to the described channel $C_1$, this transformation is characterized via

$$\mathbf{T}_{\mathrm{C}} = \sqrt{G}\mathbf{I}_2, \quad \mathbf{N}_{\mathrm{C}} = (G-1)\frac{1+2\bar{n}}{4}\mathbf{I}_2, \tag{2.99}$$

where we set $G = \tau$ for convenience to illustrate the amplification process. This transformation corresponds to the input-output formalism introduced in Eq. (2.55) and involves the coupling of an input state to a thermal background with a mean photon number $\bar{n}$. As a result, an amplifier (such as the JPA) operated in the nondegenerate regime implements a Gaussian amplification channel. It is interesting to note that the two previously mentioned channels can be used to implement the noise channel $B_2$. It can be observed that in the limit of $\tau \to 1$ the single attenuation channel $C_1$ results in the noise channel $B_2$ for which the added mean noise photon number $\bar{n}_2 = (1-\tau)(1+2\bar{n}_1)$. Here, $\bar{n}_{1(2)}$ is the mean noise photon number of the channel $C_1$ ($B_2$). However, this description implies that for a fixed mean noise photon number $\bar{n}_2$, the noise photon number $\bar{n}_1$ diverges. A more physically realistic description is to obtain the $B_2$ channel as the composition of the amplification channel $C_1$ and the attenuation channel $C_2$. Then one obtains the noise channel $B_2$ using the following matrices

$$\mathbf{T}_{\mathrm{C}}^{C_1} = \sqrt{1/G}\mathbf{I}_2, \quad \mathbf{T}_{\mathrm{C}}^{C_2} = \sqrt{G}\mathbf{I}_2, \quad \mathbf{N}_{\mathrm{C}}^{C_1} = (1-1/G)\frac{1+2\bar{n}_1}{4}\mathbf{I}_2, \quad \text{and} \quad \mathbf{N}_{\mathrm{C}}^{C_2} = (G-1)\frac{1+2\bar{n}_2}{4}\mathbf{I}_2, \tag{2.100}$$

where we choose $G\tau = 1$. From Eq. (2.100), we compute that the total added noise is described by the matrix

$$N_{\mathrm{C}}^{\mathrm{tot}} = \frac{1}{2}(G-1)(1+(\bar{n}_1+\bar{n}_2))\mathbf{I}_2 \coloneqq \bar{n}\mathbf{I}_2. \tag{2.101}$$

From Eq. (2.101), any noise photon number $\bar{n} \in [0, +\infty)$ can be obtained by choosing a suitable values for $G$, $\bar{n}_1$, and $\bar{n}_2$. We note that in experiments one commonly has only partial control of the mean noise photon numbers $\bar{n}_1$ and $\bar{n}_2$ (in particular, one often is not able to set them to exactly zero), but a more complete control of gain values in the range of $G > 1$.

### 2.2.3 Quantum entanglement and quantum entropy

Entanglement is a purely quantum phenomenon that emerges from a specific types of quantum correlations and expresses the nonseparability of multipartite quantum systems. For the bipartite case with subsystems $A$ and $B$, the joint system is described using a joint density matrix $\hat{\rho}_{\mathrm{AB}}$. The bipartite system is said to be separable if there exists two ensembles of $\{\hat{\rho}_{i,\mathrm{A}}\}_i$ and $\{\hat{\rho}_{i,\mathrm{B}}\}_i$ such that the density matrix of the state can be written as

$$\hat{\rho}_{\mathrm{AB}} = \sum_i p_i \hat{\rho}_{i,\mathrm{A}} \otimes \hat{\rho}_{i,\mathrm{B}}, \tag{2.102}$$

where $\{p_i\}_i$ are probabilities. As illustrated in Fig. 2.8 (a), each local subsystem $A$ and $B$ can be fully described using the ensemble sets, $\{\hat{\rho}_{i,\mathrm{A}}\}_i$ and $\{\hat{\rho}_{i,\mathrm{B}}\}_i$, respectively. Equation 2.102 indicates that the separable joint system can be represented by its respective individual parts. In general, quantifying separability in a multipartite quantum system is not a straightforward task and, often, relies on so-called witness functions, which may, fully or partially, capture the presence of nonseparability of systems. For bipartite systems, there exists a deterministic witness function relying on the positive partial transpose (PPT) criterion [99]. In general, an

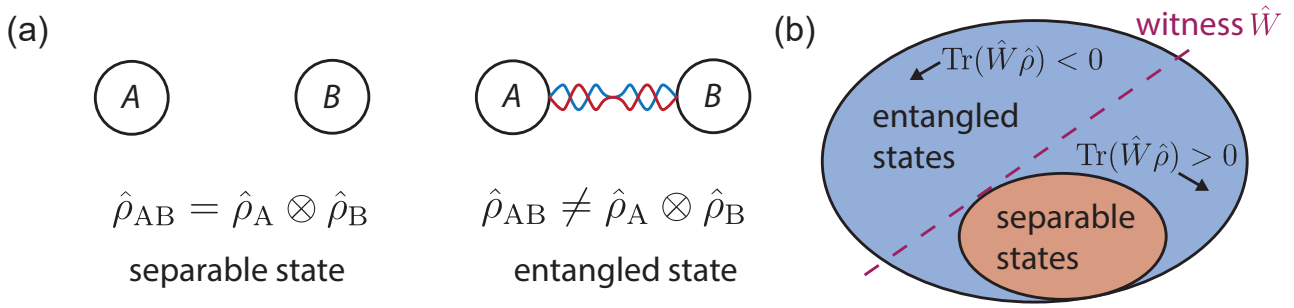


Figure 2.8: Representation of entangled states. (a) Illustration of a separable bipartite system where we consider for simplicity that the subsystem $A$ ($B$) is fully described using one density matrix, $\hat{\rho}_A$ ($\hat{\rho}_B$). Conversely, an entangled state cannot be decomposed into such tensor product of local states. (b) An entanglement witness is capable of distinguishing between some entangled states and separable states. Every separable states lead to a positive outcome, $\mathrm{Tr}(\hat{W}\hat{\rho}) \geq 0$ while an entangled state results in $\mathrm{Tr}(\hat{W}\hat{\rho}) < 0$. However, there can be entangled states that are not detected by the chosen witness. In the case of two-mode systems, one can construct a witness based on the PPT criterion which detects all entangled cases.

entanglement witness is a Hermitian operator $\hat{W}$ for which $\mathrm{Tr}(\hat{W}\hat{\rho})$ is positive for a separable state $\hat{\rho}$, and negative if the state is entangled as shown in Fig. 2.8 (b). In the context of Gaussian states, a suitable monotonic witness function can be obtained using the so-called negativity $N_{\mathrm{eg}}$. The latter is a monotonic measure of quantum entanglement, implying that the more a given state $\hat{\rho}_{AB}$ is entangled, the larger the negativity is. For a two-mode Gaussian state, the negativity relies on the state's symplectic eigenvalues. These eigenvalues are defined as the eigenvalues of $i\mathbf{\Omega V}$, where $\mathbf{\Omega}$ is the symplectic matrix defined in Eq. (2.93) and $\mathbf{V}$ is the covariance matrix of the two-mode Gaussian state. The corresponding covariance matrix is

$$\mathbf{V} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}, \tag{2.103}$$

where submatrix $\mathbf{A}$ ($\mathbf{B}$) is the covariance matrix of the subsystem $A$ ($B$) while submatrix $\mathbf{C}$ determines the nonlocal correlations between $A$ and $B$. Using Eq. (2.103), one defines the symplectic invariants of the covariance matrix [6]

$$\tilde{I}_1 = \det \mathbf{A}, \quad \tilde{I}_2 = \det \mathbf{B}, \quad \tilde{I}_3 = \det \mathbf{C}, \quad \tilde{I}_4 = \det \mathbf{D}. \tag{2.104}$$

These invariants do not change under symplectic transformations, i.e., according to Sec.,2.2.2, under a local unitary Gaussian transformation in the form of squeezing or displacement operations. With the four symplectic invariants, one can derive the corresponding symplectic eigenvalues to [100]

$$\nu_{\pm} = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4\tilde{I}_4}}{2}}, \tag{2.105}$$

where $\Delta = \tilde{I}_1 + \tilde{I}_2 + 2\tilde{I}_3$. Similarly, one can compute the symplectic eigenvalues of the partially transposed density matrix. The resulting symplectic eigenvalues $\tilde{\nu}_{\pm}$ are the same symplectic eigenvalues as in Eq. (2.105) but with $\Delta$ replaced by $\tilde{\Delta} = \tilde{I}_1 + \tilde{I}_2 - 2\tilde{I}_3$. Then, the negativity for a two-mode state reads as

$$N_{\mathrm{eg}} = \max\left(0, \frac{1 - 4\tilde{\nu}_-}{8\tilde{\nu}_-}\right), \tag{2.106}$$

which is greater or equal to zero. It can be shown that a positive negativity value indicates that the state is entangled in agreement with the PPT criterion. The state is maximally entangled

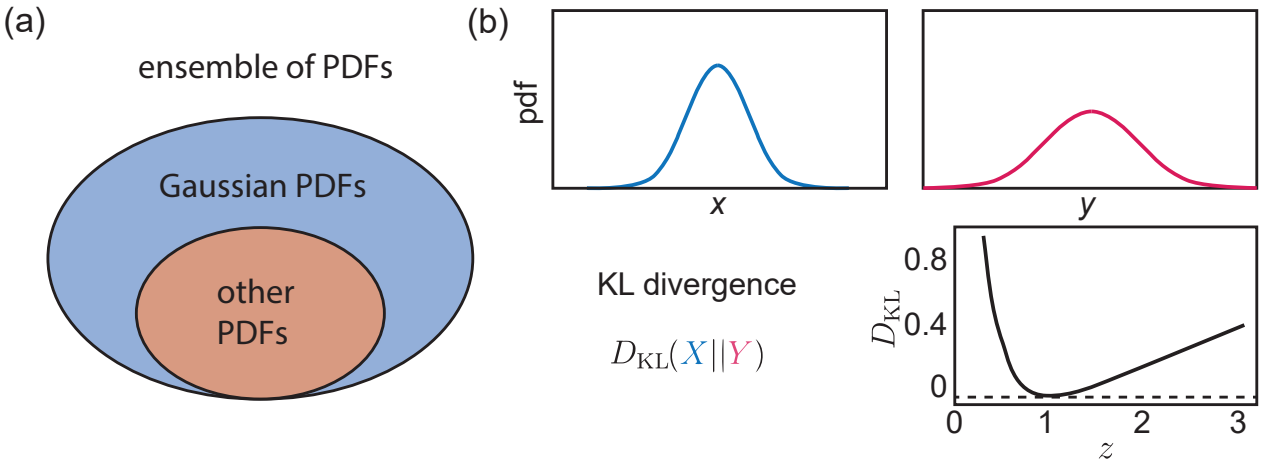


Figure 2.9: Entropy of states. (a) Visualization of the differential entropy $h$ of a continuous function representing a PDF associated with a classical random variable. The entropy is defined up to an arbitrary offset constant. Gaussian probability density functions (PDFs) maximize the differential entropy as compared to any other PDF with a given mean value $\mu$ and variance $\sigma^2$. (b) Kullback-Leibler (KL) divergence between two Gaussian PDFs with the same mean value but different variances. We observe that the KL divergence measures the closeness of the two distributions and is minimal for $z = \sigma_1^2/\sigma_2^2 = 1$. As such, the differential entropy is relevant to evaluate the relative information between two distributions.

in the limit of $N_{\mathrm{eg}} \to +\infty$. Computing the negativity for the TMS state defined in Sec. 2.2.2 results in the value

$$N_{\mathrm{eg,TMS}} = \max\left(0, \frac{1}{2}\left(e^{2r} - 1\right)\right). \tag{2.107}$$

As a consequence, the vacuum TMS state is entangled for any squeeze factor $r > 0$, and becomes maximally entangled in the limit of $r \to +\infty$.

**Entropy of quantum states.** The entropy of a quantum state measures the statistical ordering of a physical system. For the case of classical systems where the system state would be described by a classical random variable $X$, which takes values $x_i$ with associated probabilities $p_i$, the entropy can be measured using the Shannon entropy $H(X) = -\sum_i p_i \log p_i$ [101]. The Shannon entropy estimates the minimal number of classical bits required to describe the system's information content. The Shannon entropy is defined for discrete variables, but can be extended to continuous-variables using the differential entropy

$$h(X) = -\int_{\mathcal{X}} f_X(x) \log(f_X(x)) \mathrm{d}x, \tag{2.108}$$

for the continuous random variable $X$ with a density probability function $f_X$ that is defined over a domain $\mathcal{X}$. The differential entropy can be defined for conditional variables as

$$\begin{aligned} h(X|Y) &= -\int_{\mathcal{X}}\int_{\mathcal{Y}} f_Y(y) f_{X|Y}(x,y) \log(f_{X|Y}(x,y)) \mathrm{d}x\, \mathrm{d}y \\ &= -\int_{\mathcal{X}}\int_{\mathcal{Y}} f_{(X,Y)}(x,y) \log\left(\frac{f_{(X,Y)}(x,y)}{f_Y(y)}\right) \mathrm{d}x\, \mathrm{d}y, \end{aligned} \tag{2.109}$$

where $X|Y$ is a continuous random variable expressing values of the continuous random variable $X$ conditioned on the values taken by the continuous random variable $Y$. The function $f_Y$ defined over a domain $\mathcal{Y}$ is the density probability function of the random variable $Y$, while

$f_{(X,Y)}$ is the joint probability density function (PDF) of $X$ and $Y$. It is tempting to consider the differential entropy as the continuous limit of the Shannon entropy. However, this is not the case as the differential entropy is ill-defined, since it is not invariant under a linear invertible map $\mathbf{A}$

$$h(\mathbf{AX}) = h(\mathbf{X}) + \log(\left|\det(\mathbf{A})\right|) \tag{2.110}$$

for a random variable vector $\mathbf{X} = (X_1, \ldots, X_n)$. The differential entropy of a random vector is computed using the conditional differential entropy

$$h(\mathbf{X}) = \sum_{i=1}^{n} h(X_i|X_1, \ldots, X_{i-1}). \tag{2.111}$$

As a consequence of Eq. (2.110), the differential entropy is not invariant under a change of variables. It can also take negative values depending on the basis of the logarithm and the probability distribution chosen. Nevertheless, the differential entropy is a useful tool to compute information-related quantities for random variables. Most importantly, as illustrated in Fig. 2.9 (a), for a random variable vector $\mathbf{X}$ of dimension $n$ with a classical covariance matrix $\mathbf{V}$, one can show that [102]

$$h(\mathbf{X}) \leq \frac{1}{2} \log\left[(2\pi e)^n \det(\mathbf{V})\right], \tag{2.112}$$

where the right hand side of Eq. (2.112) corresponds to a Gaussian random variable vector with the same covariance matrix $\mathbf{V}$. This result implies that the differential entropy of a Gaussian random variable can be analytically computed and that Gaussian random variables maximize the differential entropy. One can construct a statistical distance between probability density functions called the Kullback-Leibler (KL) divergence. For two PDFs $f$ and $g$, associated with a continuous random variable $X$ and $Y$, respectively, and defined on a common domain $\mathcal{X}$, the KL divergence reads

$$D_{\mathrm{KL}}(X||Y) = \int_{\mathcal{X}} f(x) \left( \log\left(\frac{f(x)}{g(x)}\right)\right) \mathrm{d}x = -h(f) - \int_{\mathcal{X}} f(x) \log(g(x)) \mathrm{d}x, \tag{2.113}$$

The KL divergence circumvents many issues of the differential entropy as it is always positive and invariant under a change of variable from $x$ to another $y(x)$. These properties suggest that it is more relevant to evaluate the difference between differential entropies rather than only differential entropies themselves. For the KL divergence, a nonzero value can be interpreted as a measure of the closeness between PDFs. As an example, the KL divergence between two Gaussian distributions with zero mean value but different variances gives

$$D_{\mathrm{KL}}(X||Y) = \frac{1}{2}\left( \log\left(\frac{\sigma_1^2}{\sigma_2^2}\right) + \frac{\sigma_2^2}{\sigma_1^2} - 1\right) = \frac{1}{2}\left(\log(z) + z^{-1} - 1\right), \tag{2.114}$$

where we define $z = \sigma_1^2/\sigma_2^2$. In Fig. 2.9 (b), we show the resulting KL divergence and observe that it is zero for $z = 1$, reflecting that the two PDFs are identical at this point.

Lastly, in analogy to the Shannon entropy, one can define a measure of the entropy of quantum states, known as the von Neumann entropy. For a general density matrix, $\hat{\rho}$, the von Neumann entropy is defined as the Shannon entropy of the set of eigenvalues $\{\lambda_i\}_{i\in[1,M]}$ of the density matrix [6]

$$S_M(\hat{\rho}) = -\sum_{i=1}^{M} \lambda_i \log(\lambda_i), \tag{2.115}$$

where similarly to the Shannon entropy and the differential entropy, the logarithm can use different bases. For the case of an $M$-mode Gaussian state, the von Neumann entropy can be directly computed using the symplectic eigenvalues $\{\nu_i\}_{i\in[1,M]}$ [26]

$$S_M(\hat{\rho}) = \sum_{i=1}^{M} g(\nu_i), \quad g(x) = \frac{1}{2}\left[(4x+1)\log(4x+1) - (4x-1)\log(4x-1) - 2\log(2)\right]. \tag{2.116}$$

For the case of $M = 2$, the von Neumann entropy simplifies to $S_2(\hat{\rho}) = g(\nu_+) + g(\nu_-)$, where $\nu_\pm$ are the symplectic eigenvalues defined in Eq. (2.105).

## 2.3 Gaussian single-shot measurement formalism

In a quantum system, physical quantities are measured as eigenvalues of certain operators, which are defined as observables. These measurements can be described in a general framework using positive operator valued measure (POVM) operators, acting on a Hilbert space $\mathcal{H}$ that describes the physical system under study. The POVM consists of a set of positive semi-definite Hermitian operators $\{\hat{E}_i\}_{i\in[1,N]}$ having the properties

$$\hat{E}_i = \hat{E}_i^\dagger, \;\; \langle\phi|\hat{E}_i|\phi\rangle \geq 0, \text{ for any state } |\phi\rangle, \;\; \sum_{i=1}^{N} \hat{E}_i = \hat{\mathbb{1}}, \tag{2.117}$$

where $\hat{\mathbb{1}}$ is the identity operator. This property guarantees that the POVM operators form a complete set of measurements, i.e., are able to describe all possible values for measurable physical quantities in experiments. In other words, this property implies that probabilities describing the measurement results can be associated with the set of operators. The construction of such probabilities relies on the aforementioned properties of the POVM operators. In general, these operators are not orthogonal to each other. As such, a measurement with an outcome $i$ can be associated to a POVM element $\hat{E}_i$ with a probability given by the Born rule as

$$P(i) = \mathrm{Tr}(\hat{\rho}\hat{E}_i), \tag{2.118}$$

where the density matrix $\hat{\rho}$ describes the physical system. A particular set of POVM operators are called projection-valued measure (PVM) operators. These operators have an added property of being projectors meaning that these operators are pairwise orthogonal to each other and, for a PVM $\{\hat{\Pi}_i\}_{i\in[1,N]}$, the operators fulfil the relation

$$\hat{\Pi}_i^2 = \hat{\Pi}_i \quad \text{and} \quad \hat{\Pi}_i\hat{\Pi}_j = \delta_{ij}\hat{\Pi}, \text{ for } i,j \in [1,N], \tag{2.119}$$

where $\delta_{ij}$ the Kronecker delta symbol. More generally, any POVM can be associated with another PVM operator using Naimark's dilation theorem [103]. This theorem indicates that any POVM in a Hilbert space $\mathcal{H}$ can be linked to a PVM in a different higher-dimensional Hilbert space $\mathcal{H}'$ via an isometry transformation. This result implies that any POVM in experiments can be performed by finding suited PVMs in a larger Hilbert space. A famous example is the problem of unambiguous quantum state discrimination, i.e., the task of distinguishing two possible given states of a quantum system from measurements with the highest probability [104]. We note that from Eq. (2.119) a measurement described by PVMs projects an input system into a unique subsystem perfectly distinguishable from other possible outcomes. As a results, one can write the resulting density matrix after a PVM measurement as

$$\hat{\rho}' = \frac{\hat{\Pi}_i\hat{\rho}\hat{\Pi}_i}{\mathrm{Tr}(\hat{\rho}\hat{\Pi}_i)}. \tag{2.120}$$

The orthogonality property of PVMs ensures that the resulting state in Eq. (2.120) remains in the projected subspace.

The PVM operator can be built by choosing a set of eigenvectors $|\psi_i\rangle$ which are suited to describe a physical system under study. PVM operators can be obtained as $\hat{\Pi}_i = |\psi_i\rangle\langle\psi_i|$, where the operators $\hat{\Pi}_i$ are projectors since $\hat{\Pi}_i\hat{\Pi}_j = \delta_{ij}$. For instance, in the case of photon counting, a well-suited set of eigenvectors is the Fock basis, meaning that $\hat{\Pi}_n = |n\rangle\langle n|$, with $n \in [0, +\infty]$. In the context of continuous variables, the states of interest are the eigenvectors of the quadrature operators of the electric field introduced in Eq. (2.63). Based on our experimental measurement setup described in Chap. 4, measurements in our experiments can be described using these states. Here, an appropriate set of PVMs is given by the set of coherent states $\{|\alpha\rangle\}_{\alpha\in\mathbb{C}}$. Additionally, one can use the set of eigenvectors of the quadrature operators, $\hat{q}$ and $\hat{p}$, namely $\{|q\rangle\}_{q\in\mathbb{R}}$ and $\{|p\rangle\}_{p\in\mathbb{R}}$, respectively. For the last two sets, one can use Eq. (2.66) to compute the Wigner function of a given projector $\hat{\Pi}_{q^\star} = |q^\star\rangle\langle q^\star|$ and $\hat{\Pi}_{p^\star} = |p^\star\rangle\langle p^\star|$

$$W_{\hat{\Pi}_{q^\star}}(q,p) = \delta(q-q^\star) \quad \text{and} \quad W_{\hat{\Pi}_{p^\star}}(q,p) = \delta(p-p^\star). \tag{2.121}$$

Here, $q^\star, p^\star \in \mathbb{R}$ and $\delta$ is the delta-Dirac function. Using the definitions in Eq. (2.118) and Eq. (2.121), for a single-mode Gaussian state we obtain the probability of measuring an outcome $q^\star$ as

$$P(q^\star) = \mathrm{Tr}(\hat{\rho}\hat{\Pi}_{q^\star}) = \pi\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} W_{\hat{\rho}}(q,p)W_{\hat{\Pi}_{q^\star}}(q,p)\mathrm{d}q\mathrm{d}p = \frac{1}{\sqrt{2\pi\sigma_q^2}}\exp\left[-\frac{(q^\star-\bar{q})^2}{2\sigma_q^2}\right]. \tag{2.122}$$

Here, the displacement vector of the Gaussian state is $\mathbf{d} = (\bar{q}, \bar{p})$, while $\sigma_q^2$ is the variance of the $q$-quadrature. We note that the same result can be derived for the $p$-quadrature by interchanging the roles of $q$ and $p$, while replacing $q^\star$ with $p^\star$. The result in Eq. (2.122) indicates that the outcome of a PVM measurement is described by the underlying Gaussian distribution of the quadratures, as it would be intuitively expected. In general, PVM measurements based on the quadrature operators are well-suited for Gaussian states. However, in experimental implementations, we must additionally account for noise, arising from multiple sources, e.g., measurement devices or thermal fluctuations. Following the same formalism as above, we account for the noise in PVM measurements by modifying the projectors

$$\hat{\Pi}^{\mathrm{n}}_{q^\star} = \int_{-\infty}^{+\infty}\frac{1}{\sqrt{2\pi\sigma_{\mathrm{n}}^2}}\exp\left[-\frac{(y-q^\star)^2}{2\sigma_{\mathrm{n}}^2}\right]|y\rangle\langle y|\mathrm{d}y, \tag{2.123}$$

where $\sigma_{\mathrm{n}}^2 = n$ is the added variance due to the noise in the measurement, $n$ being a positive real number. The previous operator is an integral of the PVM operators, $|y\rangle\langle y|$, weighted by a Gaussian envelope with a mean value of $q^\star$ and variance $\sigma_{\mathrm{n}}^2$. One can derive that

$$W_{\hat{\Pi}^{\mathrm{n}}_{q^\star}}(q,p) = \frac{1}{\sqrt{2\pi\sigma_{\mathrm{n}}^2}}\exp\left[-\frac{(q-q^\star)^2}{2\sigma_{\mathrm{n}}^2}\right], \tag{2.124}$$

resulting in the final outcome probability

$$P(q^\star) = \frac{1}{\sqrt{2\pi\sigma_{\mathrm{tot}}^2}}\exp\left[-\frac{(q^\star-\bar{q})^2}{2\sigma_{\mathrm{tot}}^2}\right], \tag{2.125}$$

with $\sigma_{\mathrm{tot}}^2 = \sigma_q^2 + \sigma_{\mathrm{n}}^2$. Remarkably, Eq. (2.125) means that a noisy PVM measurement gives the same result as a noiseless PVM measurement but with the noise variance added to the

quadrature variance. In particular, the final probability is still Gaussian with only an enlarged variance. From a practical perspective, these results motivate an implementation of the PVM measurements with the quadrature operators while simultaneously minimizing the induced measurement noise. An insight into possible implementations of such measurements can be obtained by considering the following quantum state

$$|q^\star, r\rangle \coloneqq \hat{D}(q^\star)\hat{S}(re^{i\pi/2})|0\rangle. \tag{2.126}$$

This state corresponds to a $q$-squeezed state (with the associated squeezing factor $r$) displaced along the $q$-quadrature by an amplitude $q^\star$. Here, $\hat{D}$ and $\hat{S}$ are respectively the displacement operator and squeezing operator introduced in Eq. (2.79) and Eq. (2.80). We compute the action of the operator $\hat{q}$ on this state

$$\hat{q}|q^\star, r\rangle = q^\star|q^\star, r\rangle + e^{-r}\frac{1}{2}\hat{D}(q^\star)\hat{S}(re^{i\pi/2})|1\rangle. \tag{2.127}$$

From the previous equation, it can be shown that $|q^\star, r\rangle \to |q^\star\rangle$ for $r \to +\infty$ [86]. Therefore, the PVM measurements with the quadrature operators can be potentially implemented with the squeezing operation and, by extension, with phase-sensitive amplifiers, such as JPAs.

# Chapter 3

# Continuous-variable quantum key distribution with microwaves

Historically, the first QKD protocols have been implemented in the optical regime with signal wavelengths around $\lambda = 860\,\mathrm{nm}$ and $\lambda = 1550\,\mathrm{nm}$. In these experiments, the unconditional security of a variety of discrete-variable (DV) protocols has been demonstrated with a particular focus on coherent state protocols due to their practical simplicity. As a brief introduction, we present the basics of DV-QKD protocols in Sec. 3.1 and then focus on CV-QKD protocols, most relevant for our experiments. The latter offers a less cumbersome experimental implementation with direct compatibility to existing classical communication platforms. Here, it becomes relevant to investigate the potential of propagating quantum microwave signals as an alternative to optical signals due to their frequency compatibility with superconducting circuits. In particular, in Sec. 3.2 we emphasize the fact that squeezed state CV-QKD protocols represent a more relevant choice for experimental implementations of CV-QKD protocols in the microwave domain than coherent states. To demonstrate the potential of CV-QKD protocols for unconditionally secure communication, we present a security analysis in Sec. 3.4. Furthermore, in Sec. 3.5 the advantages of a microwave CV-QKD open-air communication are discussed, especially in comparison with optical counterparts operated at the telecom wavelength of $\lambda = 1550\,\mathrm{nm}$. We show that microwave signals can potentially offer larger secret key rates (SKRs) in combination with a remarkable resilience to weather imperfections in strong contrast with the telecom signals. These results have been published in Ref. 60. Figures and text have been adapted from this publication.

## 3.1 From discrete-variable to continuous-variable quantum key distribution

QKD protocols exist in a variety of forms that can be classified into two large families, depending on the type of states used as a resource to encode information. One refers to the DV-QKD protocols when the corresponding quantum states can be described by a Hilbert space of finite dimension. Historically, this type of protocol was first implemented in practice. However, DV-QKD protocols rely on technically demanding resources such as Fock states that are challenging to generate and control in a scalable manner. Alternatively, CV-QKD has been developed, making use of the compatibility with already existing classical communication platforms. In Sec. 3.1.1, we introduce generic notions of QKD protocols in order to discuss DV-QKD in Sec. 3.1.2. There, secure communication and security threshold can be intuitively derived, where we give some associated experimental performances. Then, in Sec. 3.1.3, we shift to CV-QKD and point out potential advantages of this type of protocol over DV-QKD. Depending

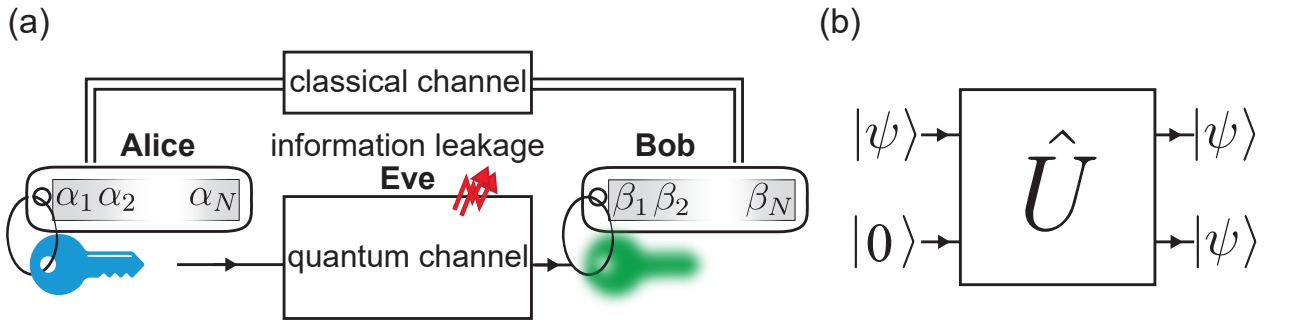


Figure 3.1: General concept of quantum key distribution. (a) A transmitter named Alice sends a classical key $\mathcal{K}_\mathrm{A} = \{\alpha_i\}_{i\in[1,N]}$, encoded into quantum states, over an untrusted quantum channel, which is assumed to be under the control of an external eavesdropper Eve. The latter induces an information leak in the communication by interfering with Alice's key. A disturbed key signal is received by Bob. Upon measuring these signals, Bob obtains a distorted version of Alice's key and forms a corresponding ensemble $\mathcal{K}_\mathrm{B} = \{\beta\}_{i\in[1,N]}$. Alice and Bob also have a classical channel at their disposal, which allows them, after authentication, to classically communicate in order to perform various tasks related to information reconciliation and privacy amplification. (b) An impossible cloning machine illustrating the no-cloning theorem. The latter implies that no unitary transformation, $\hat{U}$, exists that could generate a perfect copy of an input state $|\psi\rangle$.

on the level of security, the former can be classified into three subtypes, which we present in Sec. 3.1.4.

### 3.1.1 General notions of QKD protocols

QKD aims at exchanging classical information (a key) in a secure manner between two remote parties. A generic QKD scheme is presented in Fig. 3.1(a). The sender side is commonly referred to as Alice, while the receiver side is denoted Bob. In this context, a key is an ensemble of numbers or digits that typically have been generated randomly according to a random distribution that varies depending on the chosen QKD protocol. Security of this key exchange is addressed by assuming the presence of a malicious eavesdropper, Eve, who interferes with the communication between Alice and Bob. Eve's goal is to maximize the amount of information that can be extracted from her interactions alone about the key. In this work, we focus on "preparing and measuring" CV-QKD protocols, meaning that the communication between Alice and Bob consists of Alice preparing quantum states, encoding the key, and sending it through a quantum channel to Bob. On his side, Bob performs quantum measurements of the incoming states. Considering an ensemble of $N$ real numbers $\{\alpha_i\}_{i\in[1,N]}$, we write Alice's key as a collection of numbers $\mathcal{K}_\mathrm{A} = \{\alpha_i\}_{i\in[1,N]}$ and refer to each number as a *symbol*. Each of these individual symbols, $\alpha_i$, is encoded in a quantum state and sent through a quantum channel. The state at the output of the channel is measured by Bob, resulting in a corresponding measured symbol $\beta_i$. After repeating this procedure for each symbol of Alice, Bob has a measured key $\mathcal{K}_\mathrm{B} = \{\beta_i\}_{i\in[1,N]}$. In practical implementations, one commonly considers that the quantum channel induces losses and adds noise to the incoming signals. One cannot differentiate whether observed nonidealities in the data exchanged between Alice and Bob are induced by uncorrelated independent sources (e.g., due to the presence of background noise), in which case the information is lost, or whether these disturbances originate from Eve interfering with the quantum states propagating through the channel. To certify unconditional security, one considers a worst-case scenario where all imperfections in communication between Alice and Bob are attributed to Eve. As a result, Eve is assumed to have full control over the quantum channel.

One important restriction on Eve is imposed by the no-cloning theorem [30]. This theorem forbids Eve from producing perfect copies of unknown quantum states, as illustrated in Fig. 3.1(b). This feature represents a striking difference between quantum and classical states, where the latter can be perfectly copied without any disturbance of the original data. Additionally, Alice's key is encoded into a certain state basis, which is selected to provide orthogonality of the corresponding quantum states. The encoding basis is constructed to prevent any possibility of distinguishing which basis is used to encode a given symbol. Under these conditions, one can certify that Eve can only get partial information about the original key while necessarily disturbing the quantum states sent by Alice [105]. These induced disturbances of Alice's states represent the main difference between QKD protocols and classical key distribution protocols. No matter which strategy Eve uses, one can estimate the maximal effect of her actions on the key information content and derive a security threshold that separates the unconditional security regime and insecure one.

### 3.1.2 Discrete-variable quantum key distribution.

Before introducing the CV-QKD protocols, we briefly discuss certain DV-QKD protocols in a general context, irrespective of the particular frequency regime. These types of protocols also correspond to the first experimental realizations of QKD protocols as well as the earliest proposed QKD protocols. They rely on quantum states living in a Hilbert space of finite dimension. Commonly, these protocols use qubits (or qubit-like states) that can be implemented in a variety of physical systems. Here, we mention that in the optical domain, a common choice are the polarization states of electromagnetic fields. They provide a natural encoding basis using linearly polarized light or left/right circularly polarized light [8]. For comparison, in the microwave domain, many different types of superconducting qubits, e.g., transmon, fluxonium, cat-qubits, have been successfully realized [14]. For DV-QKD protocols, a common encoding basis is the computational basis $\{|0\rangle, |1\rangle\}$ (the Z-basis) with associated states $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ (X-basis), leading to a an indistinguishability condition between both bases

$$|0\rangle\langle 0| + |1\rangle\langle 1| = \hat{1} = |+\rangle\langle +| + |-\rangle\langle -|, \tag{3.1}$$

where $\hat{1}$ is the identity operator. This implies that, on average, measurements in one basis or another yield the same ensemble of results. In other words, it is not possible, on average, to deduce which encoding basis has been used from measurements performed randomly in the Z-basis or the X-basis.

The most well-known DV-QKD protocol is the BB84 protocol [106, 107, 108]. In this protocol, as shown in Fig. 3.2(a), Alice assigns a logical bit 0 to the two non-orthogonal states, $|0\rangle$ and $|+\rangle$, and a logical bit 1 the two non-orthogonal states, $|1\rangle$ and $|-\rangle$. Since the states assigned to each logical bit are nonorthogonal with each other, perfect copies of them cannot be made by Eve according to the no-cloning theorem. It follows that Eve needs to interact with Alice's states to obtain information, rendering her presence detectable by Alice and Bob. The protocol relies on Bob performing measurements, switching randomly between the Z-basis or the X-basis. If Bob's measurement basis coincides with the encoding basis, ideally, Bob obtains the same logical bit as Alice. In case the bases do not coincide, Bob obtains a random result, corresponding to 0 in 50% of cases and 1 in the other 50%. The procedure of the protocol is to disclose, after Alice's entire key has been sent through the quantum channel, which encoding and measurement bases have been used, and to discard measurements for which the bases do not agree. This part of the protocol is commonly known as *sifting*. In an ideal scenario, Bob's sifted key would exactly coincide with Alice's sifted key. In a nonideal case, the presence of Eve would necessarily imply that some measured data of Bob does not match Alice's data even after sifting. This deviation can be quantified by Alice and Bob using a part of their data

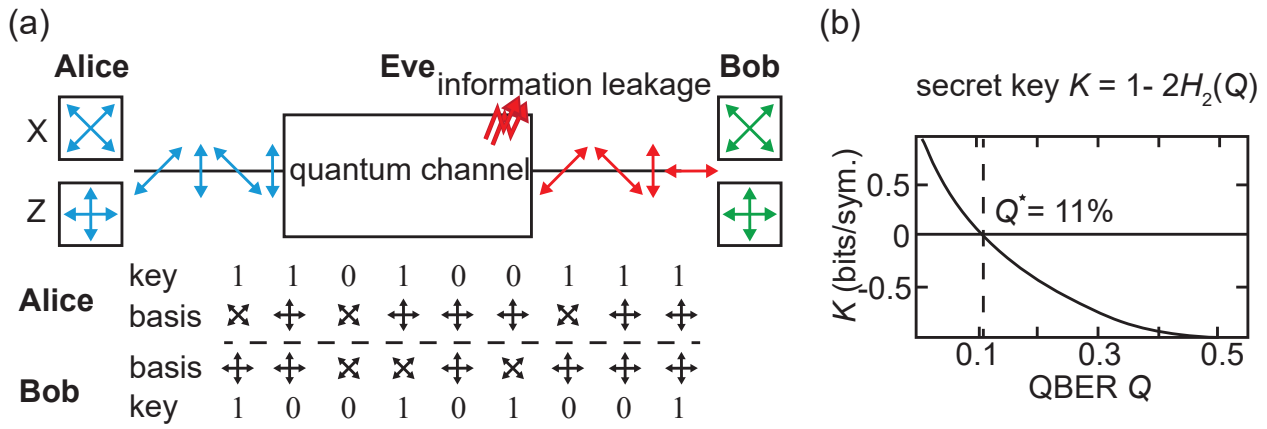


Figure 3.2: General concept of the BB84 protocol. (a) First, Alice chooses an encoding basis, either the X-basis or the Z-basis. Each basis contains two states to which Alice can assign a logical bit as described in the main text. These states encode a bit of information and are sent through a quantum channel to Bob. Eve obtains some information about Alice's key by interfering with the propagating quantum states. The resulting states at the quantum channel outputs are received by Bob, who performs a measurement in a random basis. (b) The secret key $K$ from Eq. (3.3) of the BB84 protocol as a function of the QBER, $Q$. A security threshold, defined as $K = 0$, corresponds to a maximal QBER of 11%.

and computing an average error between their respective keys. Here, the maximal security assumption implies that any non-idealities in measurements resulting in errors for Bob are attributed to Eve. The figure of merit associated to this error is the quantum bit error rate (QBER), defined as

$$\begin{aligned} Q &= \text{Prob(mismtach between Alice's and Bob's key)} \\ &= \frac{\text{number of mismatch between Alice's and Bob's bits}}{\text{total number of bits}}. \end{aligned} \tag{3.2}$$

Using the above definition, the protocol security simplifies to determining the maximum tolerable QBER in the considered communication. Different security proofs have been established [8] with the possibility to map the protocol to an entanglement-based version, in which Alice and Bob would perform the communication of the key using entangled states. Using quantum error correction codes, Shor and Preskill [106] have demonstrated a lower bound on the rate at which a key can be securely generated. This lower bound is given in bits per symbol by

$$K = 1 - H_2(\epsilon_z) - H_2(\epsilon_x), \tag{3.3}$$

where $H_2$ is the binary entropy function, i.e. $H_2(x) = -x\log(x) - (1-x)\log(1-x)$. Here, $\epsilon_z$ is the bit-flip error rate (errors in the Z-basis) and $\epsilon_x$ is the phase-flip error rate (errors in the X-basis). Based on our previous discussion, one can qualify the communication to be *unconditionally* secure in the case of $K > 0$, as this implies that in a worst-case scenario, Eve does not possess enough information to prevent Alice and Bob from sharing a finite number of secret bits. One can show, as shown in Fig. 3.2(b), that $K$ remains positive for a QBER, $Q \leq 11\%$, such that $\epsilon_z = \epsilon_x = Q$ [106], providing a threshold QBER value number for practical implementations. Although the experimental realization of such protocols can be challenging due to stringent requirements on state preparation and measurements, variations of the BB84 protocol have been demonstrated. First demonstrations of this protocol have been performed with SKRs of about $\sim$ 10bits/s by using polarized laser light with wavelengths of $\lambda = 850\,\text{nm}$ and $\lambda = 1550\,\text{nm}$ [109, 110]. It is noteworthy to mention that a simplified version of the BB84 protocol has been used to demonstrate secure communication over 421 km [43], highlighting the potential of QKD protocols for long-distance secure communication.

### 3.1.3 Continuous-variable quantum key distribution

During the last decades, a different type of QKD protocols based on CVs has been proposed as an alternative to DV-QKD protocols. The large interest in CV-QKD protocols stems from the possibility of increasing secure key rates (originally, by taking advantage of fast communication rates in existing optical fibres) [111, 112]. At the same time, CV-QKD protocols rely on quantum states, which are easier to use in experiments as compared to DV-QKD, while being compatible with standard telecommunication techniques and platforms. These aspects greatly simplify the implementation of practical QKD. Instead of (ideal) single-photon detection for signal readout in DV-QKD, CV-QKD encodes information in quadratures of the quantized electromagnetic field. As discussed in Sec. 2.2, quadrature operators are described by an infinite-dimensional Hilbert space with associated continuous eigenvalue spectra. Readout of such field quadratures can be performed with reliable and efficient methods based on $I/Q$ demodulation in the microwave regime and, equivalently, using homodyne or heterodyne detection in the optical regime [113]. These readout methods circumvent the complexity of implementing single-photon detectors and are able to achieve high detection efficiency in both optical and microwave regimes [114, 115, 116]. On the other hand, local conjugate field quadrature measurements are fundamentally limited by the SQL. To some extent, one can avoid this limitation by measuring only one of the field quadratures and considering relevant CV-QKD schemes.

In CV processes, many algorithms can be implemented using solely Gaussian states, a specific subclass of CV states introduced in Sec. 2.2. In the optical domain, multiple protocols and experiments have been demonstrated. The first successful implementation of a CV-QKD has been performed by Grosshans et al. [117] using a protocol relying only on coherent states generated with a laser diode at the wavelength of 780 nm. There, the resulting SKRs, including data post-processing, have reached 75 kbits/s, demonstrating the potential of CV-QKD for secure communication with high data rates. Remarkably, large rates up to 25 Mbit/s [118] and 30 Mbits/s [119] have been achieved with more advanced post-processing methods. Based on the aforementioned advantages of CV-QKD and with the recent advent of the field of superconducting circuits operated at microwave frequencies, it is interesting to investigate the potential of microwave signals for secure quantum communication. To this end, we strongly benefit from the frequency and technology compatibility with existing classical communication platforms, such as WiFi, Bluetooth, or 5G technologies.

### 3.1.4 CV-QKD protocols classification

Due to the large variety of existing CV-QKD protocols, we start by discussing some general aspects and, in particular, the classification of potential attacks by an eavesdropper. In this context, it is essential to distinguish between the two cases of discrete and continuous modulation. The former means that Alice's symbols are mapped onto a discrete codebook in a finite-dimensional Hilbert space. Nonetheless, the communication itself is performed with CV states and this mapping is only used during post-processing. As such, this type of protocol retains the advantages of CV-QKD. The main challenge for practical implementations of this particular scheme is related to the existing but limited security analysis, which is not as advanced as for other types [120, 121]. Alternatively, one can use a continuous modulation where symbols of Alice are represented as points in the phase space associated with the field quadrature $\hat{q}$ and $\hat{p}$ as defined in Sec. 2.2. For instance, in coherent state-based protocols the displacement vectors of encoding states generally can point along any axis in phase space, whereas in squeezed state-based protocols, the displacement vectors are commonly restricted to be along a few axes. For the both coherent and squeezed states, the security analysis is mostly complete with many experimental limitations taken into account, such as the finite number of communicated symbols [122], parameter estimation of the quantum channel [123],

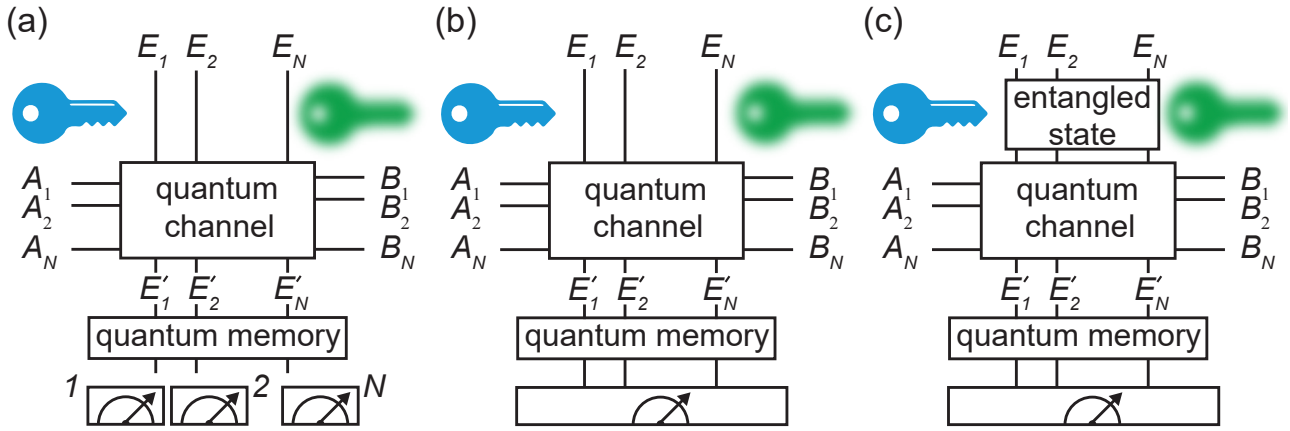


Figure 3.3: Classification of attacks performed by the eavesdropper Eve. (a) Individual attacks. Alice sends individual states $A_i$ one after the other through a quantum channel, which are received by Bob, who then performs individual measurements, corresponding to the outcomes $B_i$. Eve individually probes states, $E_1$, to the channels and retrieves outcomes $E_i'$ that are stored in a quantum memory. Finally, Eve performs individual measurements on her stored states. (b) Collective attacks. Similarly to individual attacks, Eve interacts with each incoming state of Alice, stores the outcomes in a quantum memory, but performs a joint measurement over the entire ensemble of outcomes. (c) Coherent attacks. Similarly to collective attacks, Eve performs a joint measurement. However, in this case, Eve's probe state is a fully entangled multimode state.

measurement device independence [124], and composable security [125]. The main drawback of continuous modulation is related to the necessity of data post-processing. Since symbols can take continuous values, digitization of Alice's and Bob's keys (which is necessary for final key generation as shown later in Sec. 5.3.4) requires a potentially large number of symbols depending on the chosen precision during discretization. This aspect can severely limit achievable practical SKRs [126].

The attack of an eavesdropper, Eve, can be classified into three different categories as illustrated in Fig. 3.3. The simplest form of attacks is referred to as *individual* attacks. There, Eve couples an ancillary state to each individual incoming state from Alice and stores the resulting outcome state in a quantum memory, waiting for Bob to perform the corresponding individual measurement. Eve is assumed to have perfect quantum memories where information can be ideally stored and retrieved from. A generalisation of this type of attack is referred to as *collective* attacks. There, Eve performs the same individual interaction as for individual attacks. However, she proceeds with an optimal joint measurement on the entire ensemble of states stored in her quantum memories to maximise the amount of information on Alice's and Bob's keys. Finally, the most powerful type of attack is called *coherent* attacks. There, Eve uses a multimode entangled state that is coupled to all incoming states from Alice and stores the resulting multimode state in a corresponding quantum memory. Once Bob has performed all individual measurements, Eve implements an optimal joint measurement on the quantum memories. Coherent attacks are more difficult to implement in practical settings due to their experimental requirements as compared to collective attacks. However, it can be shown that optimal coherent attacks do not yield more information to Eve than optimal collective attacks based on the de Finetti theorem applied to infinite-dimensional systems [127]. Moreover, the security against coherent attacks can be restricted to security against collective Gaussian attacks, where Eve is restricted to Gaussian channels (see Sec. 2.2.2) [128, 129]. The remarkable optimality of Gaussian attacks allows for a direct computation of SKRs [98, 130]. This allows for further limiting Eve's quantum channel to a noisy attenuation channel that can be fully parametrized by an amount of losses $\varepsilon$, or equivalently a transmissivity $\tau$, and a

coupled mean noise photon number $\bar{n}$.

Importantly, security proofs are often performed under the assumption that Alice sends an infinite amount of states, a regime referred to as the *asymptotic limit*. In practice, only a finite number of states can be communicated, implying that further security analysis is required to account for this additional limitation. Corresponding effects on the secret keys are discussed in Sec. 3.5.2. Lastly, at the end of their communication using the quantum channel, Alice and Bob need to post-process their data to obtain an exactly identical common secret key. In particular, during an error correction step, or reconciliation, a classical algorithm is used in order to generate a common key based on Alice's initial key and the corresponding key measured by Bob. This algorithm requires a key to be used as a reference, meaning that two options are possible. Either Alice's key is used as a reference and Bob's key is corrected accordingly, or the opposite is done and Bob's key is used as a reference. The former case is called the *direct reconciliation* (DR) case, while the latter is the *reverse reconciliation* (RR) case. The choice of reconciliation greatly influences the sensitivity of secret keys to the parameters of the quantum channel. More precisely, the specific choice of the quantum channel that Eve controls has a large influence on the performance of the CV-QKD protocol, independent of whether it is operated in the DR or RR case. We also mention that protocols considered in this work are classified as *one-way* quantum communication, meaning that Alice sends her states to Bob and there is no return quantum communication by Bob. However, there exists *two-way* communication protocols where Bob initially sends reference states to Alice through the quantum channel. Then, Alice applies a unitary transformation to generate new states to be sent back to Bob. Due to the necessity of Eve to attack both the forward and backward signals, this mode of communication can possess improved robustness to the presence of noise in the quantum channel. Thus, two-way CV-QKD can be particularly relevant for microwave CV-QKD. Nevertheless, both its experimental implementations and security analysis are more complex than for one-way communication. Proofs have been derived for the asymptotic limit, where protocols with Gaussian states are shown to tolerate more noise in the quantum channel as compared to their one-way implementation counterpart [98, 131]. This branch of CV-QKD protocols is beyond the scope of this thesis, where we focus on the potential of one-way CV-QKD and its experimental implementation in the microwave regime.

## 3.2 Coherent and squeezed state based protocols

Following the discussion in the previous section, we consider CV-QKD protocols that can be implemented using Gaussian states as a resource. The majority of these protocols rely on coherent and squeezed states, although it is also possible to use thermal coherent states as information carriers [132]. This possibility extends the application of CV-QKD to communication in a noisy environment while offering potentially simpler state preparation. Thermal states can also be used in the context of open-air or satellite communication [133]. In particular, García-Patrón et al. studied in Ref. 134 the impact of noise on the preparation and detection side for the DR and RR case. It is shown that noise is not necessarily detrimental to the security of the communication between Alice and Bob. In the RR case, an added trusted (i.e., not under Eve's control) noise on the detection side improves the protocol performance in terms of tolerable losses and noise in the quantum channel. One way of understanding this effect is to consider the RR case, where Bob is used as a reference. Here, the presence of an additional trusted noise on Bob's side only deteriorates the correlations between Eve and Bob since Eve's joint measurements are based on Bob's results. The additional trusted noise on Bob's side degrades Eve's information, as the latter measurements also become noisier. Conversely, a symmetric situation is also possible, where the trusted preparation noise is added on Alice's side in the DR case.

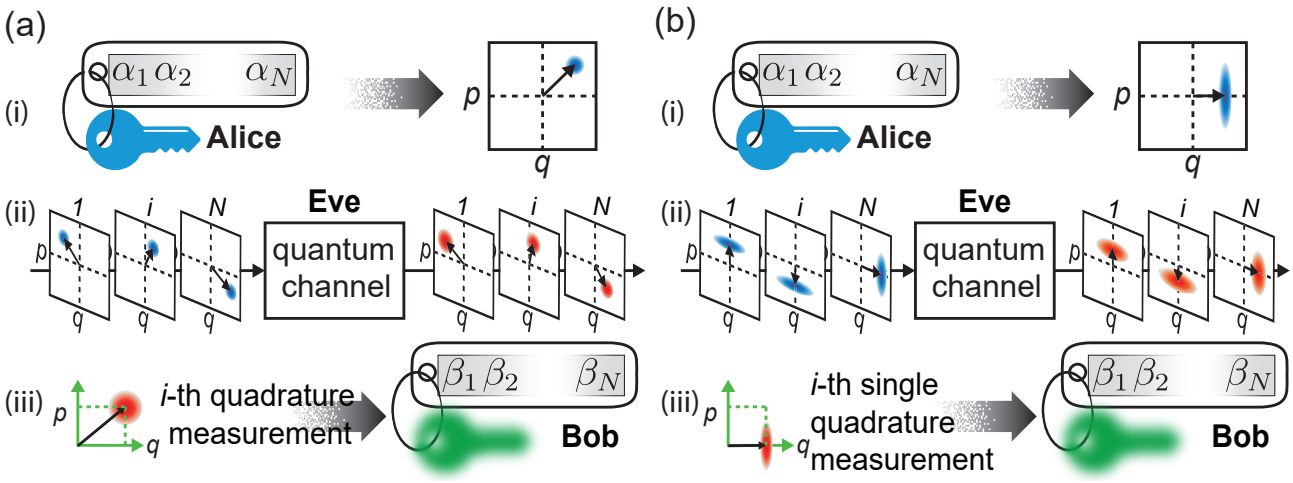


Figure 3.4: Overview of coherent state protocols in comparison to squeezed state protocols. (a) Generic coherent state protocol. Symbols of Alice's key are encoded in step (i) within coherent states whose displacement in phase space is given by two symbols (one for each quadrature axis). In step (ii), the prepared signals from Alice are sent through the quantum channel, where they can be distorted by losses and coupled noise. In step (iii), Bob performs quadrature measurements to obtain his key. (b) Generic squeezed state protocol. In step (i), similar to coherent state protocols, Alice encodes one symbol in a displaced squeezed state before sending them through the quantum channel in step (ii). In step (iii), Bob performs single quadrature measurements to obtain his key. In comparison with coherent state protocols, here, one only encodes one symbol at a time.

As a result, one can use the added trusted noise to increase the maximum tolerable amount of noise that can be present in the quantum channel as demonstrated in Refs. 134, 135. We note that the mutual information (MI) between Alice and Bob decreases when adding trusted noise. However, Eve's information decreases faster than the mutual information, resulting in a net gain in terms of security.

At optical frequencies, coherent states as encoding states are commonly preferred in experiments over squeezed states. Here, we investigate the potential of displaced and squeezed states using the secret key as an indicator in the microwave regime. In the DR case, it is a well-known fact that CV-QKD is limited to a maximum tolerable amount of losses of 3 dB [8]. This fundamental limit can intuitively be understood as Eve is obtaining more than 50% of Alice's input signals and thereby effectively replacing Bob in the communication. This implies that no security between Alice and Bob is possible. For this reason, it is in general more favourable to use DR for noisy rather than lossy quantum channels [135]. Additionally, one needs to consider limitations arising from realistic experimental conditions (e.g., limited experimental signal-to-noise ratios, imperfect post-processing). As a remedy to the limit on losses, RR has been introduced in Ref. 136. RR has the remarkable property of having no limit in tolerable losses in the quantum channel, i.e., secure communication can be potentially established for any amount of losses. Interestingly, the squeezed state protocols can outperform the coherent state protocols for tolerable losses and noise in the quantum channel for ideal and practical conditions. However, coherent state protocols can exhibit higher SKRs and are a prime choice for CV-QKD in the optical regime where the main limitations stem from losses due to large communication distance over several kilometres [8, 137, 138]. One can also compare coherent states and squeezed states by extending the analysis to satellite-based communication [139], restricting protocols to using only one phase-space quadrature [140], or relying on entangled states [141]. In all of these applications, squeezed states can offer an advantage over coherent states in terms of tolerable coupled noise in the quantum channel. In certain cases, squeezed states are shown to offer an advantage in terms of maximal communication distances, increasing

them by one order of magnitude [141]. As such, it appears that no clear preference can be made between coherent and squeezed states in a general sense and must rather be studied depending on properties of a particular protocol, frequency regime, and other experimental limitations. In Fig. 3.4, we present a general overview of coherent and squeezed state protocols. Squeezed states are not often used in optical CV-QKD mainly due to extra difficulties in generating squeezed light in this frequency domain in comparison to coherent states. Optical squeezing requires a nonlinear medium, such as a PPTK crystal with a dedicated setup for precise control [142]. Coherent states can be generated and controlled using commercial, off-the-shelf, modern lasers. However, in the microwave regime, one can routinely use nonlinear parametric amplifiers such as JPAs, which are straightforward to fabricate and control, for the generation of microwave squeezed signals. Nowadays, various JPA devices can also be purchased from many start-up companies. In contrast to optics, the readout of microwave states is mainly limited by amplification noise originating from cryogenic detection chains. For this reason, coherent states, where classical information is encoded in two field quadratures, perform significantly worse than squeezed states, where only one quadrature needs to be measured at a time. This implies that there will be twice more noise in the protocols with microwave coherent states as with the squeezed ones (see Sec. 3.4.4). This extra noise degrades the performance of the coherent state protocols and makes the squeezed state ones a more attractive choice in the microwave regime.

## 3.3 Protocols implementation and key distribution

We focus on a CV-QKD protocol with microwave squeezed states. We use a particular scheme originally proposed by Cerf et al. [105] with a Gaussian modulation. A schematic diagram of this protocol is shown in Fig. 3.5.

1. Alice initially generates a random key using a zero-mean Gaussian distribution with a fixed variance $\sigma_{\mathrm{A}}^2$, representing the codebook variance in the protocol. The key consists of a string of numbers, $\mathcal{K}'_{\mathrm{A}} = \{\alpha_i\}_{i\in\{1,\ldots,L\}}$, randomly chosen according to the zero-mean Gaussian distribution. The codebook variance is chosen such that the ensemble statistics is indistinguishable between the $q$-quadrature and the $p$-quadrature. For the squeezed states with a squeezed variance $\sigma_{\mathrm{s}}^2$ and antisqueezing variance $\sigma_{\mathrm{as}}^2$, the indistinguishability condition is
$$\sigma_{\mathrm{as}}^2 = \sigma_{\mathrm{A}}^2 + \sigma_{\mathrm{s}}^2 \Rightarrow \sigma_{\mathrm{A}}^2 = \sinh(2r)^2/2, \tag{3.4}$$
where $r$ is the squeezing factor of Alice's squeezed states.

2. For each symbol $\alpha_i$, Alice randomly chooses an encoding basis by selecting the squeezing and displacement operation along either the $q$- or the $p$-direction in phase space.

3. For each symbol $\alpha_i$, Alice generates a squeezed state along the chosen quadrature. The squeezed state is displaced along the same quadrature with a displacement amplitude given by the complex amplitude $\alpha_i$.

4. Alice sends each displaced squeezed state through the quantum channel, which is assumed to be under Eve's control. The quantum channel is a noisy loss channel, characterized by its transmissivity $\tau$ and a coupled noise photon number $\bar{n}$. Bob receives corresponding distorted states at the output of the quantum channel.

5. For each incoming displaced squeezed state, Bob decides on a measurement basis by randomly choosing either to measure along the $q$- or the $p$-quadrature. Each quadrature is chosen with equal probability.

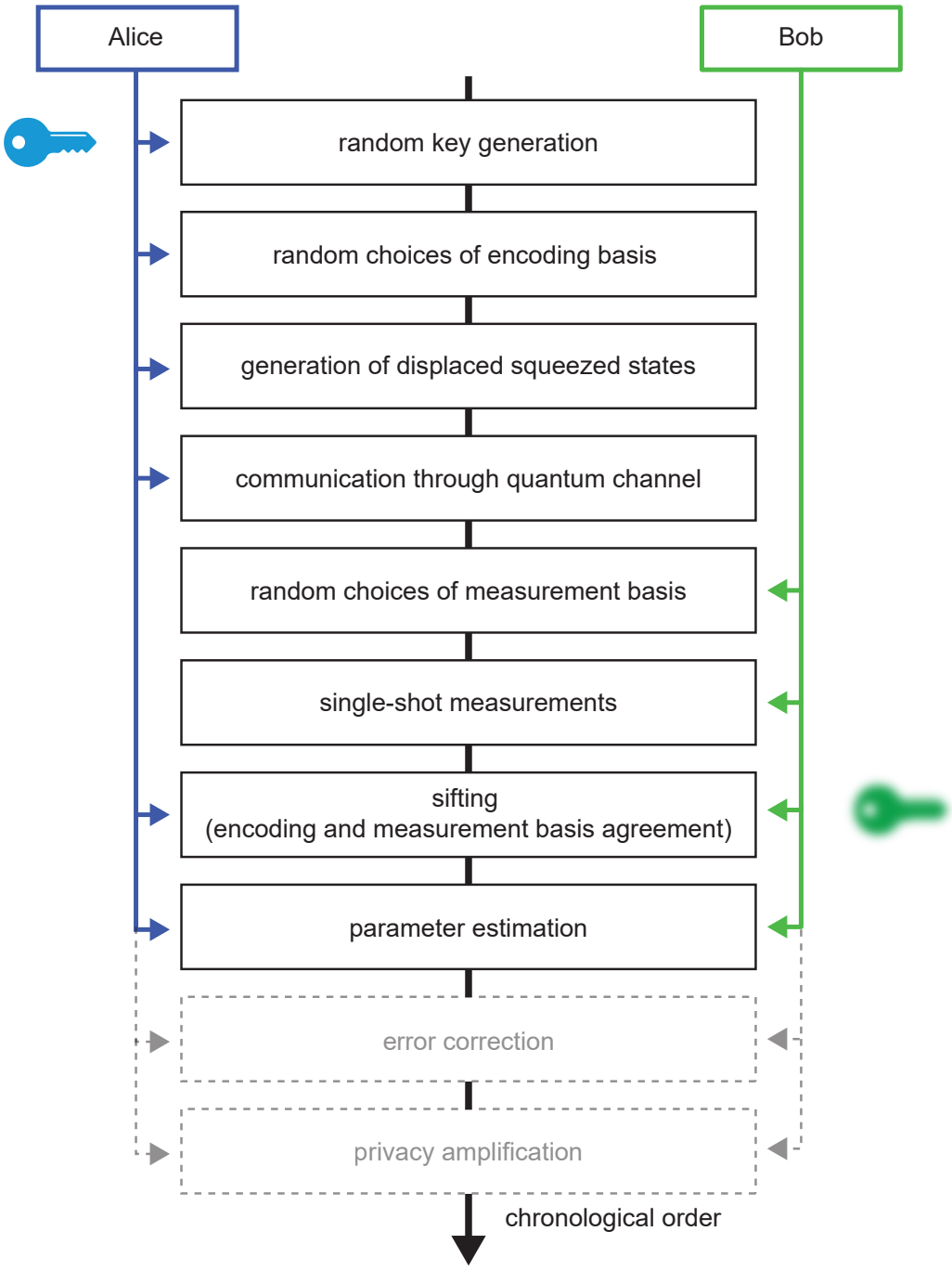


Figure 3.5: Schematic diagram of a CV-QKD protocol with squeezed microwave states. Each step is labelled with its corresponding task which are implemented in a chronological order. Alice's steps are indicated by a blue arrow, and those of Bob are indicated by a green arrow. For the sake of completeness, error correction and privacy amplification, post-processing steps are shown. However, they are not implemented in this work.

6. For each incoming displaced squeezed state, Bob implements a single-shot quadrature measurement according to the measurement basis chosen in the previous step. This operation results in the measured displacement amplitude, $\beta_i$, for each state. The whole ensemble of measured amplitudes forms a measured key.

7. Once Bob has obtained the measured key $\mathcal{K}'_{\mathrm{B}} = \{\beta_i\}_{i\in\{1,\ldots,L\}}$, Alice discloses the original encoding basis and Bob discards the measured symbols, where his measurement basis does not agree with Alice's encoding basis, representing the *sifting* step. This step results

in Alice's prepared key $\mathcal{K}_{\mathrm{A}} = \{\alpha_i\}_{i\in\{1,\dots,N\}}$ and Bob's measured key $\mathcal{K}_{\mathrm{B}} = \{\beta_i\}_{i\in\{1,\dots,N\}}$. Security analysis is performed based on these two keys.

8. Alice and Bob characterize the correlations between their keys using the MI, $I(A\colon B)$. Based on the channel parameters, Alice and Bob compute an upper bound on the information leaked to Eve using the Holevo quantity, $\chi_{\mathrm{E}}$, [143] and define the asymptotic raw secret key as
$$K = I(A\colon B) - \chi_{\mathrm{E}}. \tag{3.5}$$

9. Since only a finite number of symbols can be communicated, Alice and Bob do not have exact knowledge of the parameters of the quantum channel and must instead estimate those values. To do so, Alice and Bob use $N - n_{\mathrm{ec}}$ of their symbols to calculate worst-case estimators for the transmissivity $\tau$ and coupled noise photon number $\bar{n}$ of the quantum channel. Using these parameters, they compute a finite-size secret key (see Sec. 3.4). If this secret key is lower than zero (insecure), they abort the communication. In the limit of an infinite number of exchanged symbols, the estimators converge to the exact value of the channel parameters, and the finite-size secret key converges to the asymptotic secret key.

10. If the asymptotic secret key or the finite-size secret key is nonzero, Alice and Bob continue with further post-processing of their data. They implement a classical error correction algorithm to obtain a common key. The length of this key is less than that of the initial key. During this step, Alice's key can be used as a reference (DR case) or Bob's key can be used as a reference (RR case). The data of Alice and Bob is discretized, since their key has been obtained from continuous-variable measurements. The efficiency of the error correction algorithm is commonly denoted as $0 \leq \beta \leq 1$. Experimental works demonstrate that this coefficient can be made close to unity [144, 145]. There, low-density parity check codes are very helpful, capable of handling communication with a rather low SNR around 1 or below [146, 147, 148]. For the computation of the finite-size secret key, one can show that the optimal information of Eve is related to the smoothed min-entropy [149]. The Holevo quantity can also be used, but at a certain bit cost that depends notably on the success probability of the error correction algorithm [149, 150].

11. Finally, Alice and Bob implement an additional classical algorithm to remove the remaining information that Eve possesses on their common key [8, 151]. This step is commonly referred to as *privacy amplification*. It can be performed using random hash functions that map Alice's and Bob's data to a dataset of fixed values. Remarkably, this procedure works even if Eve has access to a perfect quantum memory [152]. One can show that using the random hash functions, Alice and Bob can generate a common string of bits for which each bit is independent of Eve's acquired information. In other words, Eve cannot do better than guessing the value of these bits, thus resulting in a secure key between Alice and Bob. This method relies on the generation of random seeds, where the specific choice of a seed and a random process does not influence the final security [152]. Additionally, note that this procedure typically produces a secret key of reduced size compared to the initial size of Alice's and Bob's common key at the end of the error correction step.

## 3.4 Security analysis

This section is dedicated to a theoretical security analysis of CV-QKD protocols with a Gaussian modulation. For a detailed analysis of our experimental implementation, we refer to Chap. 5.

Here, we provide useful tools to prove the unconditional security of the protocol introduced in previous Sec. 3.3. In Sec. 3.4.1, we start with the description of the MI, which captures the correlations between Alice's and Bob's keys. Following this step, we introduce the Holevo quantity as a bound on Eve's accessible information in Sec. 3.4.2. We analyze the secret key in the context of DR and RR for different channel parameters in Sec. 3.4.3. Based on these results, Sec. 3.4.4 shows that squeezed state protocols are inherently more promising for microwave signals, as compared to coherent state protocols due to limitations imposed by detection noise. Sec. 3.4.5 concludes this section with a short introduction to non-Gaussian operations, as a possible additional step to improve the performance of CV-QKD protocols.

### 3.4.1 Mutual information between Alice and Bob

Correlations between Alice's and Bob's key can be measured using entropy quantities, the precise choice of which depends on whether a DV or CV protocol is considered. In the case of CV-QKD, the entropy of continuous variables can be measured using the differential entropy introduced in Sec. 2.2.3. In this section, we denote by $A$ Alice's classical random variable representing a prepared key $\mathcal{K}_{\mathrm{A}}$. Similarly, we denote by $B$ Bob's classical random variable describing a measured key $\mathcal{K}_{\mathrm{B}}$. Note that even though Bob's key is described classically, it is obtained via measurements performed on quantum states. In this context, the MI between Alice and Bob is defined as the difference

$$I(A\colon B) = h(A) - h(A|B) = \int_{\mathcal{A}}\int_{\mathcal{B}} f_{(\mathrm{A,B})}(\alpha,\beta)\log\left(\frac{f_{(\mathrm{A,B})}(\alpha,\beta)}{f_{\mathrm{B}}(\beta)}\right)\mathrm{d}\alpha\,\mathrm{d}\beta, \tag{3.6}$$

with $f_{(\mathrm{A,B})}$ being the joint probability density function of $A$ and $B$, and $f_{\mathrm{A}}$ and $f_{\mathrm{B}}$, with respective domain of definition $\mathcal{A}$ and $\mathcal{B}$, are the marginal probability density functions of $A$ and $B$, respectively. In Eq. (3.6), $h$ is the differential entropy defined by Eq. (2.108) of Sec. 2.2.3 and $h(\cdot|\cdot)$ is the conditional differential entropy defined in Eq. (2.109). Since the MI is defined as a difference, the problem with absolute values of the differential entropy is circumvented, similarly to the KL divergence in Sec. 2.2.3. Additionally, by definition, the MI is symmetric $I(A\colon B) = I(B\colon A)$, as expected for a measure of correlations between Alice and Bob. Furthermore, using Jensen's inequality [153], we find

$$I(A\colon B) \geq \log\left(\int_{\mathcal{A}}\int_{\mathcal{B}} f_{(\mathrm{A,B})}(\alpha,\beta)\frac{f_{\mathrm{B}}(\beta)}{f_{(\mathrm{A,B})}(\alpha,\beta)}\mathrm{d}\alpha\,\mathrm{d}\beta\right) = 0, \tag{3.7}$$

The equality holds if, and only if, $f_{(\mathrm{A,B})} = f_{\mathrm{A}}\, f_{\mathrm{B}}$, meaning that $A$ and $B$ are completely uncorrelated. This property allows to interpret the MI as a measure of reduction in uncertainty on Alice's information given Bob's information. If their datasets are uncorrelated, revealing Bob's information provides no knowledge of Alice's information, and their MI is zero. For continuous variables, there is no upper bound on the MI, and the latter can diverge. For CV-QKD protocols, the random variable A is a Gaussian random variable centred on zero with a fixed codebook variance $\sigma_{\mathrm{A}}^2$. Once again, the quantum channel under Eve's control is a noisy loss channel with a transmissivity $\tau$ and an average coupled noise photon number $\bar{n}$. We note that in literature it is common to quantify the channel noise as excess noise, $\epsilon \coloneqq \bar{n}/\tau$. However, this definition is less suited for our experiments in the microwave regime and, in the remainder of this thesis, we instead use the coupled noise photon number, $\bar{n}$. The states measured by Bob at the output of the quantum channel are modelled using an attenuation channel $C_1$ (see Eq. (2.97)) with a transmissivity $\tau$ followed by a noise channel $B_2$ (see Eq. (2.96)) with the same added noise photon number $\bar{n}$. For our chosen protocol of Ref. 105, Alice relies on displaced squeezed states as the information carrier. For a given symbol $\alpha_i$ of Alice and a corresponding

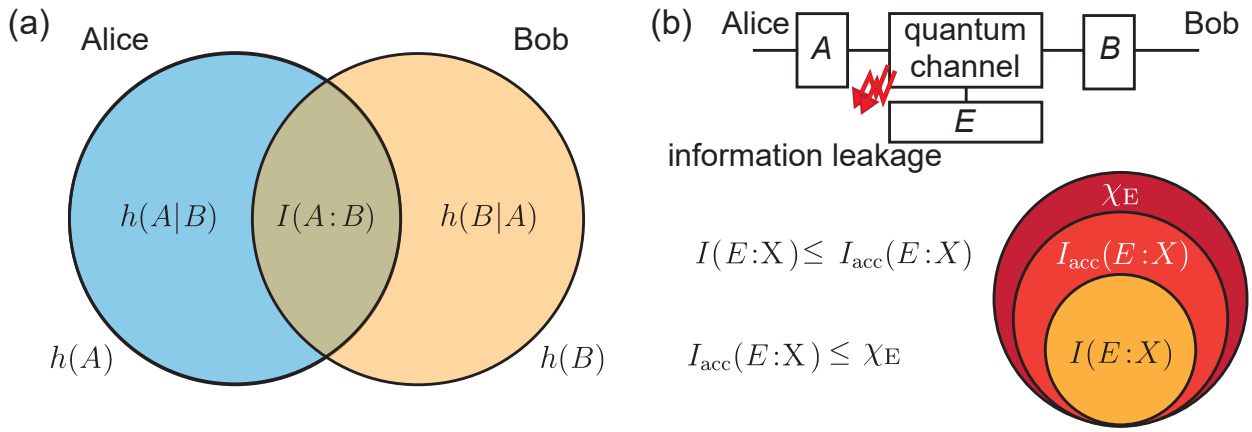


Figure 3.6: Representation of entropy quantities. (a) MI between Alice and Bob. Schematically, it corresponds to the intersection between Alice's differential entropy, $h(A)$, and Bob's differential entropy, $h(B)$. The remaining entropies are conditional entropies, $h(A|B)$ and $h(B|A)$, respectively. (b) Eve performs an attack through the quantum channel, resulting in the ensemble of states described by a random variable $E$. Eve's MI, $I(E\colon X)$, with Alice's random variable $X = A$ (DR case) or Bob's random variable $X = B$ (RR case) is bounded from above by her accessible information, $I_{\mathrm{acc}}(E\colon X)$. The latter is bounded from above by Eve's Holevo quantity, $\chi_{\mathrm{E}}$, computed directly using Eve's ensemble of states.

measured symbol $\beta_i$ by Bob, the classical random variable, $B$, is a Gaussian random variable centered on $\alpha_i$ with a variance

$$\sigma^2_{\mathrm{B|A}} = \tau\sigma^2_{\mathrm{s}} + \frac{(1-\tau)}{4} + \bar{n}. \tag{3.8}$$

The probability density function of the random variable $B$ can be derived using Eq. (3.8) combined with the indistinguishability condition from Eq. (3.4). For protocols, where symbols are modulated according to a Gaussian distribution $f_{\mathrm{A}}$, the resulting ensemble state of Bob is also described by a Gaussian random variable with the probability density function

$$f_{\mathrm{B}}(\beta) = \int_{-\infty}^{+\infty} f_{\mathrm{B|A}=\alpha}(\beta) f_{\mathrm{A}}(\alpha)\mathrm{d}\alpha = \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{B}}} \exp\left(\frac{-\beta^2}{2\sigma^2_{\mathrm{B}}}\right), \; \sigma^2_{\mathrm{B}} = \tau\sigma^2_{\mathrm{as}} + \frac{(1-\tau)}{4} + \bar{n}. \tag{3.9}$$

Using Eq. (2.112) to compute the differential entropy of a Gaussian random variable, we find the MI between Alice and Bob from the definition in Eq. (3.8) and based on Eqs. 3.9, resulting in

$$I(A\colon B) = h(B) - h(B|A) = \frac{1}{2}\left[\log_2(2\pi e)\sigma^2_{\mathrm{B}} - \log_2(2\pi e)\sigma^2_{\mathrm{B|A}}\right] = \frac{1}{2}\log_2\left(1 + \frac{\tau\sigma^2_{\mathrm{A}}}{\tau\sigma^2_{\mathrm{s}} + \frac{(1-\tau)}{4} + \bar{n}}\right). \tag{3.10}$$

Note that in the previous equation, we choose the unit of bits and express accordingly the MI in the $\log_2$ basis. The argument of the logarithm in the last expression in Eq. (3.10) can be interpreted as $1 + \mathrm{SNR}$, where SNR is the signal-to-noise ratio at Bob. A visual representation of the MI is given in Fig. 3.6 (a). We observe that the noise in the SNR depends on the coupled noise $\bar{n}$ from the quantum channel, a parameter not under Alice's and Bob's control, but also on the squeezed variance $\sigma^2_{\mathrm{s}}$, a parameter that can be reduced to zero (or closed to zero) in theory. Therefore, SNRs in squeezed state protocols can be improved by directly reducing the noise floor of the communication, a striking difference to coherent state protocols.

### 3.4.2 Holevo quantity of Eve

Thanks to her attacks during Alice and Bob's communication via the quantum channel, Eve obtains states that are partially correlated to their shared information. In general, the precise amount of information depends on the exact measurement performed by Eve. One can define the *accessible information* as the maximum information that Eve can extract from a given measurement. The possible physical measurements to consider depend on the type of attack Eve implements. In the context of a collective attack, we write the accessible information of Eve as

$$I_{\mathrm{acc}}(A\colon E) = \max\{I(A\colon E)|M_{\mathrm{E}}\}, \tag{3.11}$$

where $M_{\mathrm{E}}$ is any physically possible measurement performed by Eve. Given that Alice's codebook is described by the probability density function $f_{\mathrm{A}}$, the accessible information can be bounded from above by the Holevo quantity [143]

$$\chi_{\mathrm{E}} = S_M\left(\int_{\mathcal{A}} f_{\mathrm{A}}(\alpha)\hat{\rho}_{\mathrm{E}|\alpha}\mathrm{d}\alpha\right) - \int_{\mathcal{A}} f_{\mathrm{A}}(\alpha) S_M\left(\hat{\rho}_{\mathrm{E}|\alpha}\right)\mathrm{d}\alpha \geq I_{\mathrm{acc}}(A\colon E), \tag{3.12}$$

where $S_M$ is the von Neumann entropy of a $M$-mode state with the integration performed over a codebook ensemble $\mathcal{A}$. The hierarchy between different entropy quantities is illustrated in Fig. 3.6 (b). The states of Eve, conditioned on a chosen symbol $\alpha$ from Alice, are denoted as $\hat{\rho}_{\mathrm{E}|\alpha}$. Note that the Holevo quantity in Eq. (3.12) is shown for the DR case. In the RR case, the same results can be obtained by interchanging Alice with Bob, and correspondingly, $\alpha$ must be replaced by $\beta$. We note that the Holevo quantity is independent of any specific measurements performed by Eve. According to Eq. (3.12), one needs to compute Eve's ensemble state

$$\hat{\rho}_{\mathrm{E,ens}} \coloneqq \int_{\mathcal{A}} f_{\mathrm{A}}(\alpha)\hat{\rho}_{\mathrm{E}|\alpha}\mathrm{d}\alpha, \tag{3.13}$$

in order to obtain the Holevo quantity. Using the linearity of the trace operator and Eq. (3.13), the statistical moments of Eve's ensemble state can be expressed as

$$\langle \hat{q}^n \hat{p}^m \rangle_{\mathrm{E,ens}} = \mathrm{Tr}\left(\hat{q}^n \hat{p}^m \hat{\rho}_{\mathrm{E,ens}}\right) = \int_{\mathcal{A}} f_{\mathrm{A}}(\alpha)\left\langle \hat{q}^n \hat{p}^m \right\rangle \mathrm{d}\alpha \tag{3.14}$$

for integers $(n, m) \in \mathbb{N}^2$. For instance, we can derive

$$\left\langle \hat{q}^2 \right\rangle_{\mathrm{E,ens}} - \langle \hat{q} \rangle^2_{\mathrm{E,ens}} = \int_{\mathcal{A}} f_{\mathrm{A}}(\alpha)\left\langle \hat{q}^2 \right\rangle \mathrm{d}\alpha - \left(\int_{\mathcal{A}} f_{\mathrm{A}}(\alpha)\left\langle \hat{q} \right\rangle \mathrm{d}\alpha\right)^2. \tag{3.15}$$

Based on our general description of Gaussian channels in Sec. 2.2.2, a general Gaussian noisy loss channel can be formulated as a local interaction with one mode of a TMS state combined with an additional unitary transformation applied before and after the interaction [98]. Since the von Neumann entropy is invariant under any unitary transformation, only the canonical form of the Gaussian channel introduced in Eq. (2.92) is relevant for the computation of the Holevo quantity. It means that the assumed collective attack of Eve can be restricted to an entangling cloner attack [154]. Here, for each incoming state of Alice, Eve starts with a TMS state and couples any one mode of its state to that of Alice. The local variance of Eve's TMS state is chosen as $\cosh(2r_{\mathrm{TMS}}) = (1 + 2\bar{n}_{\mathrm{E}})$, for a mean photon number $\bar{n}_{\mathrm{E}}$. The value of the latter is defined by the condition

$$(1-\tau)(1+2\bar{n}_{\mathrm{E}}) = 4\bar{n} + (1-\tau), \tag{3.16}$$

with $\tau$ and $\bar{n}$ the corresponding quantum channel parameters. Considering that Alice starts with a displaced squeezed state, with displacement along the $q$- or $p$-quadrature, Eve's individual state $\hat{\rho}_{\mathrm{E}|\alpha}$ after her interaction through the quantum channel has the following covariance matrix

$$\mathbf{V}_{\mathrm{E}|\alpha} = \frac{1}{4}\begin{pmatrix} V_{\mathrm{E},11} & 0 & \sqrt{\tau}\sinh(2r_{\mathrm{TMS}}) & 0 \\ 0 & V_{\mathrm{E},22} & 0 & -\sqrt{\tau}\sinh(2r_{\mathrm{TMS}}) \\ \sqrt{\tau}\sinh(2r_{\mathrm{TMS}}) & 0 & \cosh(2r_{\mathrm{TMS}}) & 0 \\ 0 & -\sqrt{\tau}\sinh(2r_{\mathrm{TMS}}) & 0 & \cosh(2r_{\mathrm{TMS}}) \end{pmatrix}, \quad (3.17)$$

where $V_{\mathrm{E},11} = \tau\cosh(2r_{\mathrm{TMS}}) + (1-\tau)\exp(-2r)$ and $V_{\mathrm{E},22} = \tau\cosh(2r_{\mathrm{TMS}}) + (1-\tau)\exp(2r)$. This expression is valid for the case of Alice sending displaced squeezed states along the $q$-quadrature. For the $p$-quadrature, the same expression is obtained for $V_{\mathrm{E},11}$ being interchanged with $V_{\mathrm{E},22}$. Using the definition of moments of Eve's ensemble state in Eq. (3.14), we compute the covariance matrix of Eve's ensemble state

$$\mathbf{V}_{\mathrm{E,ens}} = \frac{1}{4}\begin{pmatrix} V_{\mathrm{E,ens}} & 0 & \sqrt{\tau}\sinh(2r_{\mathrm{TMS}}) & 0 \\ 0 & V_{\mathrm{E,ens}} & 0 & -\sqrt{\tau}\sinh(2r_{\mathrm{TMS}}) \\ \sqrt{\tau}\sinh(2r_{\mathrm{TMS}}) & 0 & \cosh(2r_{\mathrm{TMS}}) & 0 \\ 0 & -\sqrt{\tau}\sinh(2r_{\mathrm{TMS}}) & 0 & \cosh(2r_{\mathrm{TMS}}) \end{pmatrix}, \quad (3.18)$$

where $V_{\mathrm{E,ens}} = \tau\cosh(2r_{\mathrm{TMS}}) + (1-\tau)\exp(2r)$. Note that this derivation is based on the indistinguishability condition from Eq. (3.4). In the RR case, the roles of Alice and Bob are reversed. This means that Eve's ensemble state is unchanged, but her individual states now depend on the results of Bob's measurements. To compute the covariance matrix of Eve's individual state conditioned by Bob's measured symbols, we use the conditional covariance matrix formalism for Gaussian variables. This formalism can be viewed as the inverse mapping of the integration operation introduced in Eq. (3.13). To this extent, we consider Bob's ensemble state given by

$$\hat{\rho}_{\mathrm{B,ens}} \coloneqq \int_{\mathcal{A}} f_{\mathrm{A}}(\alpha)\hat{\rho}_{\mathrm{B}|\alpha}\mathrm{d}\alpha, \quad (3.19)$$

where $\hat{\rho}_{\mathrm{B}|\alpha}$ is an originally displaced squeezed state sent by Alice (corresponding to a symbol $\alpha$) after interaction with Eve through the quantum channel. Based on the derivation in Eq. (3.9), we write its covariance matrix as $\mathbf{V}_{\mathrm{B,ens}} = \mathrm{diag}(\sigma_{\mathrm{B}}^2, \sigma_{\mathrm{B}}^2)$. The covariance matrix of Eve's individual state conditioned on a measurement of Bob is given by [154]

$$\mathbf{V}_{\mathrm{E}|\beta} = \mathbf{V}_{\mathrm{E,ens}} - \frac{1}{\sigma_{\mathrm{B}}^2}\mathbf{D}\mathbf{\Pi}\mathbf{D}^T, \quad (3.20)$$

where $\mathbf{\Pi}$ represents a quadrature projection depending on the measured quadrature by Bob, i.e., $\mathbf{\Pi} = \mathrm{diag}(1,0)$ for a measured $q$-quadrature and $\mathbf{\Pi} = \mathrm{diag}(0,1)$ for a measured $p$-quadrature. Here, the matrix $\mathbf{D}$ represents correlations between Eve's ensemble state and Bob's ensemble state. It can be derived using a beam splitter operation between Eve's TMS coupled mode and Bob's states. To show this result, we derive a fully analytical model and we express the displacement vector of Bob's mode (Eve's modes) $\mathbf{d}_{\mathrm{B}}$ ($\mathbf{d}_{\mathrm{E}}$), as well as the covariance matrix of Bob's mode (Eve's modes) $\mathbf{V}_{\mathrm{B}}$ ($\mathbf{V}_{\mathrm{E}}$), as

$$\begin{aligned} \left(\mathbf{d}_{\mathrm{B}}, \mathbf{d}_{\mathrm{E}}\right)^{\mathrm{T}} &= \mathbf{\Sigma}\cdot\left(\bar{\mathbf{0}}, \mathbf{d}_{\mathrm{E,in}}\right)^{\mathrm{T}} + \mathbf{\Sigma}_{\mathrm{E}}\cdot\left(\mathbf{d}_{\mathrm{A}}, \bar{\mathbf{0}}_{\mathrm{E,in}}\right)^{\mathrm{T}}, \\ \begin{pmatrix} \mathbf{V}_{\mathrm{B}} & \mathbf{C}_{\mathrm{BE}} \\ \mathbf{C}_{\mathrm{BE}}^{\mathrm{T}} & \mathbf{V}_{\mathrm{E}} \end{pmatrix} &= \mathbf{\Sigma}\cdot\left(\mathbf{V}_0 \oplus \mathbf{V}_{\mathrm{E,in}}\right)\cdot\mathbf{\Sigma}^{\mathrm{T}}, \end{aligned} \quad (3.21)$$

with

$$\mathbf{\Sigma}_{\mathrm{E}} = \mathcal{B}\left(\tau_{\mathrm{E}}\right) \oplus \mathbf{I}_2, \mathbf{\Sigma}_{\mathrm{A}} = \mathbf{R}\left(\varphi/2\right)\cdot\mathbf{S}_{\mathrm{sq}}\left(r\right) \oplus \mathbf{I}_4, \text{ and } \mathbf{\Sigma} = \mathbf{\Sigma}_{\mathrm{E}}\cdot\mathbf{\Sigma}_{\mathrm{A}}. \quad (3.22)$$

Here, $\mathbf{I}_n$ is the identity matrix of dimension $n$. Note that the dot symbol $\cdot$ represents a matrix multiplication and $\bar{\mathbf{0}}$ ($\mathbf{V}_0$) corresponds to the mean displacement vector (covariance matrix) of the vacuum state. Furthermore, $\mathbf{d}_{\mathrm{A}}$ represents Alice's mean displacement vector, and $\mathbf{d}_{\mathrm{E,in}}$ represents Eve's initial mean displacement vector of her TMS state. Additionally, $\varphi$ corresponds to the squeezing angle of Alice's squeezed states. Correlations between Bob's and Eve's individual states are described by the submatrix $\mathbf{C}_{\mathrm{BE}}$. The matrix $\mathcal{B}$ represents the beam splitter operation and can be expressed as

$$\mathcal{B}(\tau) = \begin{pmatrix} \sqrt{\tau}\,\mathbf{I}_2 & \sqrt{1-\tau}\,\mathbf{I}_2 \\ -\sqrt{1-\tau}\,\mathbf{I}_2 & \sqrt{\tau}\,\mathbf{I}_2 \end{pmatrix}. \tag{3.23}$$

Finally, $\mathbf{R}$ corresponds to a 2D rotation matrix while $\mathbf{S}_{\mathrm{sq}}$ is a 2×2 matrix

$$\mathbf{R}\left(\varphi/2\right) \cdot \mathbf{S}_{\mathrm{sq}}(r) = \begin{pmatrix} \cos\left(\varphi/2\right) & \sin\left(\varphi/2\right) \\ -\sin\left(\varphi/2\right) & \cos\left(\varphi/2\right) \end{pmatrix} \cdot \begin{pmatrix} \exp(-r) & 0 \\ 0 & \exp(r) \end{pmatrix}. \tag{3.24}$$

Using Eq. (3.21) and the definition of the quantum channel parameter in Eq. (3.16), we retrieve the expression of the variance of Bob established in Eq. (3.8)

$$\mathbf{V}_{\mathrm{B}} = \tau_{\mathrm{E}}\mathbf{V}_{\mathrm{A}} + (1-\tau_{\mathrm{E}})\,\frac{1}{4}\,(1+2n_{\mathrm{E}})\,\mathbf{I}_2 = \tau_{\mathrm{E}}\mathbf{V}_{\mathrm{A}} + \left[\frac{1}{4}\,(1-\tau_{\mathrm{E}}) + \bar{n}\right]\mathbf{I}_2. \tag{3.25}$$

Here, $\mathbf{V}_{\mathrm{A}}$ represents Alice's state variance, corresponding for our studied protocol to the squeezed variance of Alice's squeezed states. Based on the multimode covariance matrix derived in Eq. (3.21), we can straightforwardly express the correlation matrix $\mathbf{D}$ as

$$\mathbf{D} = \begin{pmatrix} D_{11} & 0 \\ 0 & D_{22} \\ D_{31} & 0 \\ 0 & -D_{42} \end{pmatrix}, \; D_{ij} = \frac{1}{2}\langle \hat{X}_{\mathrm{E},i}\hat{X}_{\mathrm{B},j} + \hat{X}_{\mathrm{B},j}\hat{X}_{\mathrm{E},i}\rangle - \langle \hat{X}_{\mathrm{E},i}\rangle\langle \hat{X}_{\mathrm{B},j}\rangle \tag{3.26}$$

where $\hat{X}_{\mathrm{E},i}$ corresponds to the $i$th element in $\{\hat{q}_{\mathrm{E},1}, \hat{p}_{\mathrm{E},1}, \hat{q}_{\mathrm{E},2}, \hat{p}_{\mathrm{E},2}\}$ and $\hat{X}_{\mathrm{B},j}$ corresponds to the $j$th element in $\{\hat{q}_{\mathrm{B}}, \hat{p}_{\mathrm{B}}\}$. Note that in the previous expressions, we have dropped the subscript "ens" for compactness. Moreover, the subscript "1" indicates the coupled mode of Eve's TMS state, while the subscript '2" refers to the idler uncoupled mode. After calculations, we find

$$D_{11} = D_{22} = -\sqrt{\tau}\sqrt{1-\tau}(e^{2r} - \cosh(2r_{\mathrm{TMS}}))/4\;, \;\; D_{31} = D_{42} = \sqrt{1-\tau}\sinh(2r_{\mathrm{TMS}})/4. \tag{3.27}$$

One way to physically interpret Eqs. 3.20 and 3.26 is to consider that after Eve's attack, we have correlated three-mode states. A local measurement of Bob on his subsystem projects the idler subsystem onto a new state. This new state is determined by the correlations between Bob's and Eve's modes, which are described by the correlation matrix $\mathbf{D}$. The resulting state after measuring of the $q$- or $p$-quadrature is a Gaussian state with a covariance matrix given by Eq. (3.20).

### 3.4.3 Secret key

From a practical point of view, it is required to evaluate the security of CV-QKD protocols. This security is quantified by the secret key $K_{\mathrm{exp}}$, which represents the amount of secure information per communicated symbol through the quantum channel. The secret key is bounded from below by

$$K_{\mathrm{exp}} \geq K = \beta\, I(A{:}B) - \chi_{\mathrm{E}}. \tag{3.28}$$

Here, in contrast to the naive original expression given by Eq. (3.5), we include the error correction efficiency $\beta$. As previously mentioned, experimental values $\beta > 0.9$ can be achieved with current classical post-processing error correction algorithms [37]. Therefore, within a first analysis step, we can omit this term to estimate the performance of our CV-QKD protocol. We recall that a positive value of $K$ indicates a secure communication, as Alice and Bob share more information than Eve can in principle obtain. In order to take into account the finite size of the communicated key between Alice and Bob, the secret key expression must be modified as [150]

$$K_{\text{exp}} \geq K_N = \frac{n_{\text{ec}}\, p_{\text{ec}}}{N} \left( K\left(\hat{\tau}^{\star}, \hat{\bar{n}}^{\star}\right) - \Delta\left(n_{\text{ec}}\right) \right), \tag{3.29}$$

where $n_{\text{ec}} \leq N$ denotes a number of symbols needed to be kept for the reconciliation algorithm, leaving $m = N - n_{\text{ec}}$ symbols to be used for the parameter estimation. Additionally, the error correction step is assumed to succeed with a probability of $p_{\text{ec}}$. The additional term $\Delta\left(n_{\text{ec}}\right)$ corresponds to a correction term due to the finite key size. As explained in Sec. 3.3, it represents the cost of using the Holevo quantity instead of Eve's smoothed min-entropy. Lastly, $\hat{\tau}_{\text{E}}^{\star}\left(\hat{\bar{n}}^{\star}\right)$ is a worst-case scenario statistical estimator of the channel parameter $\tau_{\text{E}}\left(\bar{n}\right)$. It can be built using Alice and Bob data block of length $m$, where one computes a square root transmissivity estimator using the following construction

$$\hat{T} = \frac{\sum_{i=1}^{m}\left(\alpha_i - \bar{A}\right)\left(\beta_i - \bar{B}\right)}{\sum_{i=1}^{m}\left(\alpha_i - \bar{A}\right)^2}, \tag{3.30}$$

with the statistical average of Alice and Bob individual data defined as

$$\bar{A} = \sum_{i=1}^{m} \alpha_i \quad \text{and} \quad \bar{B} = \sum_{i=1}^{m} \beta_i. \tag{3.31}$$

From this estimator, one defines $\hat{\tau} \coloneqq \hat{T}^2$, which satisfies by construction that $\langle\hat{\tau}\rangle = \tau$. To derive a noise estimator, one starts by building a total noise photon number estimator [150]

$$\hat{\bar{n}}_{\text{tot}} = \frac{1}{m}\sum_{i=1}^{m}\left(\beta_i - \sqrt{\hat{\tau}}\,\alpha_i\right)^2, \tag{3.32}$$

which has the property $\left\langle\hat{\bar{n}}_{\text{tot}}\right\rangle = \bar{n}_{\text{tot}} = \tau\,\sigma_s^2 + (1-\tau)/4 + \bar{n}$. Given a statistical confidence parameter $w$, worst-case scenario unbiased estimators can be built by underestimating the transmissivity and overestimating the amount of coupled noise leading to the definitions

$$\begin{aligned} \hat{\tau}^{\star} &\coloneqq \hat{\tau} - w\sqrt{\text{var}\left(\hat{\tau}\right)} \simeq \hat{\tau} - 2w\sqrt{\left(\frac{\bar{n}_{\text{tot}}}{\sigma_{\text{A}}^2} + 2\tau\right)\frac{\tau}{m}}, \\ \hat{\bar{n}}_{\text{tot}}^{\star} &\coloneqq \bar{n}_{\text{tot}} + w\sqrt{\text{var}\left(\bar{n}_{\text{tot}}\right)} \simeq \bar{n}_{\text{tot}} + w\sqrt{\frac{\bar{n}_{\text{tot}}^2}{2\,m}}. \end{aligned} \tag{3.33}$$

An important note based on the previous equation is that the worst-case scenario estimators converge slowly, as $1/\sqrt{m}$, to the value of the actual quantum channel parameters. This aspect implies that keys of large length are necessarily required from any protocol for the error of estimators to become tolerable. In the case of random variables with a normal distribution, the confidence parameter $w$ reduces to

$$w = \sqrt{2}\,\text{erf}^{-1}\left(1 - 2\varepsilon_{\text{ec}}\right), \tag{3.34}$$

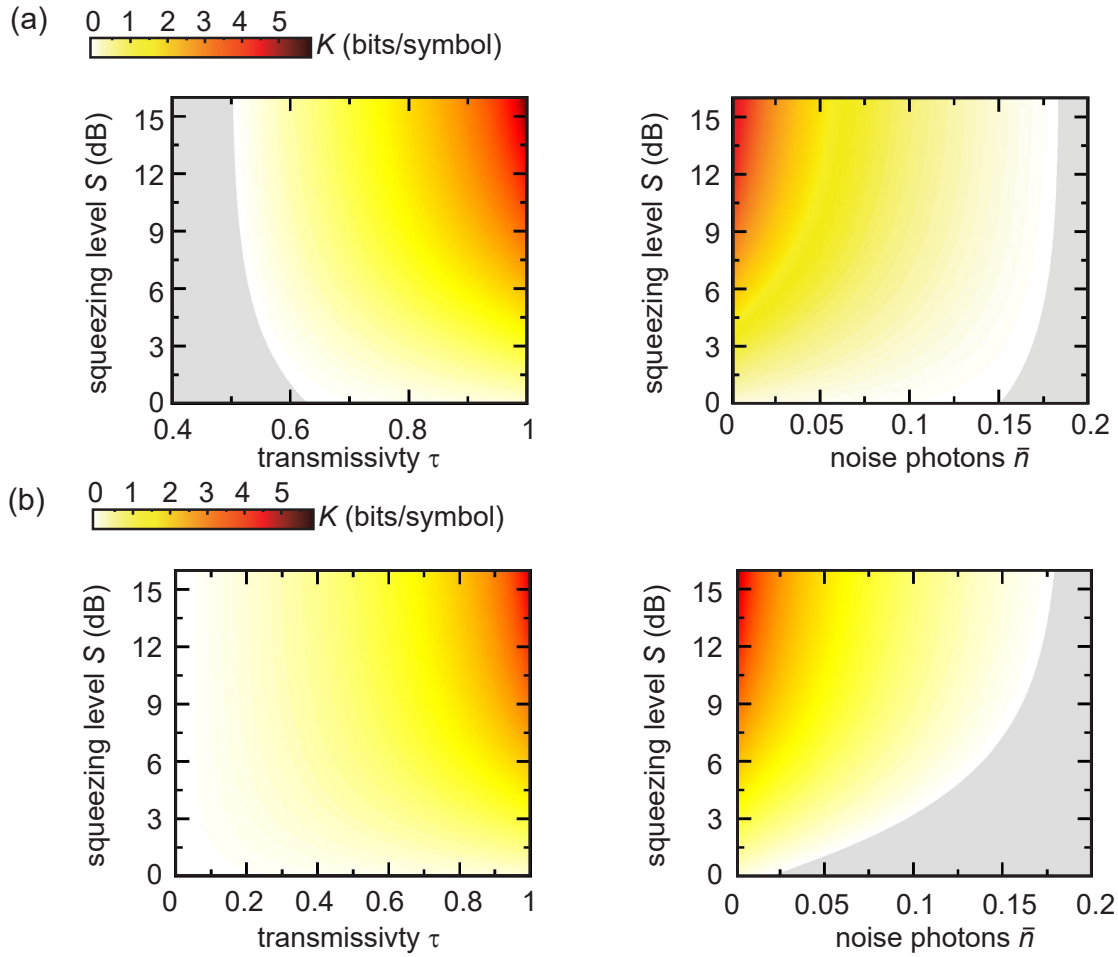


Figure 3.7: Secret key $K$ of the CV-QKD protocol plotted as a function of the squeezing level $S$ (measured in dB below the vacuum limit), transmissivity $\tau$ and average noise photon number $\bar{n}$ for ideal reconciliation efficiency $\beta = 1$, according to Eq. (3.28). Panels (a) and (b) show the cases of DR and RR, respectively. Grey areas represent the regions of negative keys, i.e., insecure communication.

with $\varepsilon_{\text{ec}}$ defined as an error probability, i.e., the confidence interval that is considered for the worst-case estimators. For practical applications, CV-QKD protocols are commonly implemented with error probabilities around $10^{-10}$, resulting from Eq. (3.34) in $w \simeq 6.34$. From the previous total noise estimator, a coupled noise photon number unbiased estimator can be naturally defined as

$$\hat{\bar{n}}^{\star} = \hat{\bar{n}}^{\star}_{\text{tot}} - \frac{(1-\hat{\tau}^{\star})}{4} - \hat{\tau}^{\star}\,\sigma_{\text{s}}^2. \tag{3.35}$$

In Fig. 3.7, we show results of a numerical evaluation of the secret key as a function of the transmissivity $\tau$ and noise photon number $\bar{n}$ in the quantum channel. Remarkably, in the DR case a secure communication cannot exist when $\tau$ exceeds a threshold value of 0.5, which illustrates the well-known result that secure CV-QKD communication in DR schemes is limited by 3 dB of losses [136, 155]. As discussed previously, the reason for this fact is that communication with DR cannot be secure when Eve receives more than 50% of Alice's signal. In this scenario, Eve effectively replaces Bob as the communication partner. As illustrated in Fig. 3.7, this limit can be entirely circumvented by using the RR scheme, where Bob is used as a reference. For RR, if we imagine that Eve only induces losses during the quantum communication, Alice always has more information than Eve on Bob's measured key. This is because Eve is assumed to cause losses on Alice's signals modeled by a beam splitter operation. As a result, Eve can only obtain a fraction of Alice's information. Furthermore, in the case of

very large losses ($\tau_E \to 0$), Bob receives only a tiny fraction of the signal coming from Alice, meaning that the original signal is largely uncorrelated with Eve's eavesdropped information. As a consequence, Eve's information reveals very little about Bob's measured key, making the communication secure. If Eve couples noise photons in addition to the losses, the correlations between the key sent by Alice and that measured by Bob decrease. At the same time, Eve gains more information on the key measured by Bob. In particular, the communication is secure up to a coupled noise photon threshold value $\bar{n}$ of 0.183 for both reconciliation cases. This result is consistent with the well-known Pirandola-Laurenza-Ottaviani-Banchi (PLOB) upper bounds for Gaussian channels [156]. The PLOB noise threshold corresponds to the crossover of a quantum channel capacity from finite values to zero. It is also important to note that these noise numbers do not account for noise photons, which can be added by Bob during the measurements. Finally, we observe that an increase in the squeezing level results in an increase in the secret key. This increase can be understood as a decrease of the displacement uncertainty encoding the symbols, while also allowing for higher displacement amplitudes according to the indistinguishability condition imposed in Eq. (3.4).

### 3.4.4 Coherent vs squeezed states comparison

As discussed in Sec. 3.2, CV-QKD protocols in the optical domain often rely on coherent states. These coherent states can be readily generated with modern lasers and are well-suited for CV-QKD at optical frequencies. Additionally, efficient homodyne (heterodyne) detection setups [157, 158] allow for direct single (double) quadrature measurements required by these protocols. For these reasons, CV-QKD in this frequency regime is mainly limited by losses in the quantum channel, for instance, originating from fiber optic losses or atmospheric absorption losses. As a result, one could initially consider coherent states as a first candidate for CV-QKD protocol implementation in the microwave regime. However, protocols in this regime are primarily limited by coupled communication and detection-induced noise photons. To demonstrate this aspect, we consider the same communication scenario between Alice and Bob, as previously explained in Sec. 3.3, where we now account for additional noise induced by Bob's measurements. As presented in Sec. 2.2.2, the total added noise is quantified using the quadrature quantum efficiency, since Bob is required to measure single quadratures. Here, we only consider cases where a single quadrature is amplified. This requirement results in Bob having an additional noise contribution $A_{\mathrm{det}} = 0.5(\eta_X^{-1} - 1)$ in the variance of the individual conditional random variable $B|A$, which is transposed to the variance of the random variable $B$ representing the measured ensemble. Interestingly, this additional detection noise does not affect Eve in the DR case, since Eve's information depends solely on Alice's states here. As a result, we expect a strict decrease of the maximum tolerable coupled noise photon number, $\bar{n}$. In our work, superconducting JPA devices possess quadrature quantum efficiencies on the order of 60% to 70%, meaning that in experiments, one expects around 0.26 to 0.33 detection noise photons for every measured quadrature value. This additional amplification noise changes the variance of Bob's individual states to

$$\sigma^2_{B|A} = \tau\sigma^2_{\mathrm{in}} + \frac{1}{4}(1-\tau) + \bar{n} + A_{\mathrm{det}}, \tag{3.36}$$

where $\sigma^2_{\mathrm{in}}$ is the variance of Alice's input states. According to our discussion in Sec. 2.1.4, this photon number depends strongly on whether a single or both quadratures are measured. For both DR and RR, the MI between Alice and Bob's is decreased, which results in a degradation of the security of the protocol. For the RR case, we must consider the added noise contribution in Bob's variance $\sigma^2_B$, as Eve's Holevo quantity is affected by the detection noise. The covariance matrix of Eve's state after Bob performs his noisy readout can be computed using Eqs. 3.20

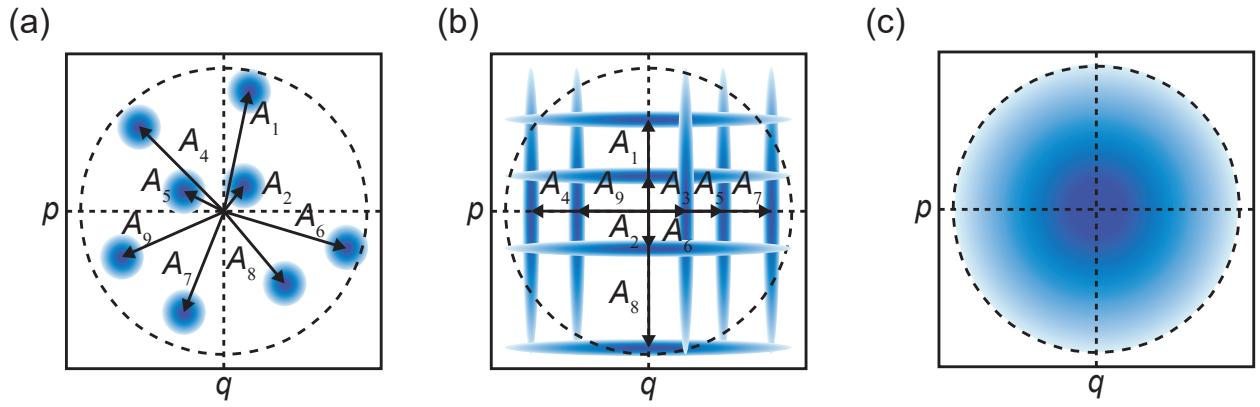


Figure 3.8: Symbol modulation for coherent and squeezed state protocols. (a) For a generic coherent state protocol, multiple coherent states are prepared, with displacement complex amplitudes distributed according to a Gaussian distribution in phase space. For illustration, we show an example of 9 randomly chosen states with their corresponding Wigner function. The circular dashed line marks the threshold of $p \leq 99\%$. (b) Same illustration as in panel (a) using displaced squeezed states with squeezing along either the $q$- or $p$-quadrature. (c) The Wigner function of the average ensemble of states for the CV-QKD protocol with Gaussian modulation. This ensemble is constructed to coincide with a thermal state in both cases, erasing information about chosen encoding bases.

and 3.26

$$\sigma_{\mathrm{B}}^2 = \tau(\sigma_{\mathrm{in}}^2 + \sigma_{\mathrm{A}}^2) + \frac{1}{4}(1-\tau) + \bar{n} + A_{\mathrm{det}}, \tag{3.37}$$

Next, we perform secret key computations, assuming that Alice relies only on coherent states. To compare this protocol to its squeezed state-based counterpart, we consider that the codebook size of both protocols is the same, meaning that $\sigma_{\mathrm{A,coh}}^2 = \sigma_{\mathrm{A,sq}}^2$. Note that for the coherent state protocol, the information of each symbol is encoded into two quadratures instead of one for the squeezed state. This effectively implies that the symbol rate is doubled compared to the squeezed state protocol. Furthermore, if no restrictions are imposed on displacement angles, we choose displacement complex amplitudes such that any quadrature is statistically indistinguishable from another, similarly to the squeezed state protocol, as illustrated in Fig. 3.8.

Two main properties distinguish coherent state protocols from squeezed state ones. Firstly, the doubling of symbol rate, using two quadratures instead of only one, results in an increase by a factor of two in the MI between Alice and Bob. Secondly, the amplification noise is significantly larger for coherent state protocols because measurements of both quadratures are limited by the SQL. Therefore, detection noise in this case amounts to at least half a photon. In the optical domain, such a measurement scheme is commonly performed using heterodyne detection. There, incoming signals are split using a 50/50 beam splitter before performing a single quadrature measurement in each output mode of the beam splitter. In the microwave domain, a similar procedure can be considered with a cryogenic hybrid ring serving as a microwave 50/50 beam splitter. Then, a single conjugate quadrature can be measured using an amplifier operated in the degenerate regime of amplification. One can note that a nondegenerate amplification can also be used to measure both quadratures simultaneously. To compare both approaches, we consider an experimental setup consisting of an ideal cryogenic hybrid ring and perform a degenerate amplification at each of its outputs. The variance of these output states can be estimated using a beam splitter channel with the transmissivity $\tau_{\mathrm{HR}} = 0.5$ and adding a noise contribution of $A_1$ ($A_2$) to the measured quadrature at the first (second) output port of the hybrid ring. Assuming $A_2 = A_1$, i.e., the degenerate amplification efficiency does not depend on the specific measured quadrature. In this case we obtain the quantum

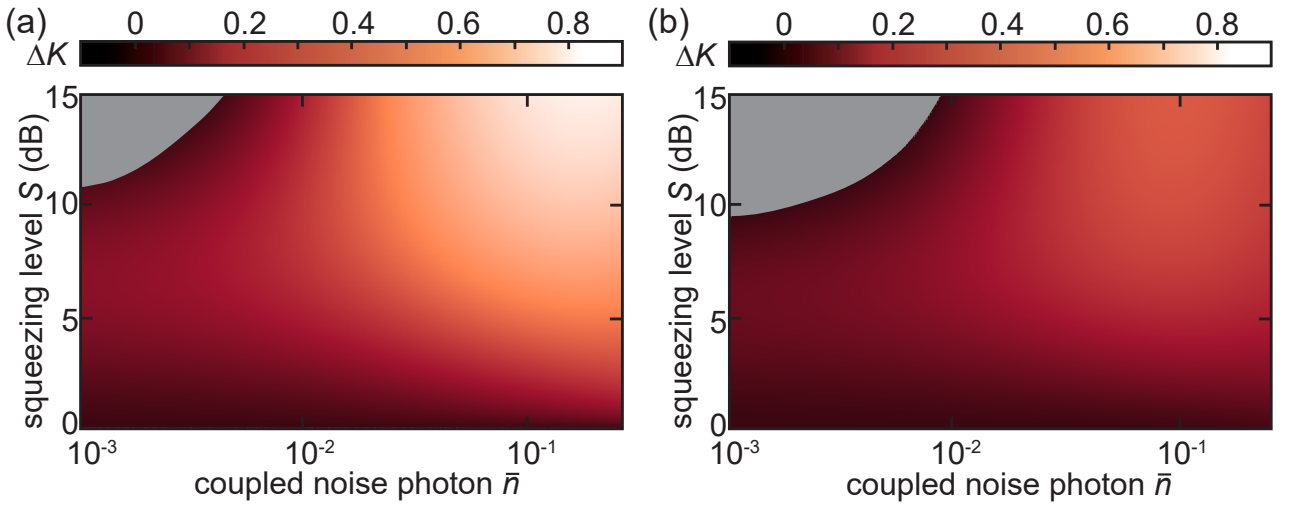


Figure 3.9: Comparison between coherent and squeezed state CV-QKD protocols. (a) Difference $\Delta K$ between the DR secret key obtained with squeezed states and coherent states. For the latter, the MI is computed using Eq. (3.40). The region of $\Delta K < 0$, corresponding to a worse QKD performance for squeezed states compared to coherent states, is highlighted in grey. The quadrature quantum efficiency of $\eta_{\mathrm{X}} = 65\%$ and an equivalent quantum efficiency $\eta = 24\%$ are used in these estimations. (b) Same scenario as in panel (a) but for the case of RR with the Holevo quantity based on Eq. (3.39). Here, as for the DR case, we observe a small region of negative $\Delta K$ for low coupled noise photon numbers, $\bar{n} \leq 0.017$, and for large squeezing levels, $S \gtrsim 10\,\mathrm{dB}$.

efficiency by measuring both quadratures as

$$\eta = \frac{1}{1 + 2\left(\frac{1}{2} + 4A_1\right)} \leq 50\%. \tag{3.38}$$

For an exemplary quadrature quantum efficiency of $\eta_{\mathrm{X}} = 65\%$, or equivalently $A_1 = 0.27$, we obtain $\eta = 24\%$. Comparatively, when relying on JPAs, we commonly observe the quantum efficiency values for non-degenerate amplification in excess of $\eta = 25\%$ [82]. Therefore, these two measurement approaches are physically equivalent and only differ in their experimental implementation. Under these considerations, we compute the covariance matrices of Eve's individual states. Accounting for the measurement of two quadratures and using Eq. (3.20), one can show that [154]

$$\mathbf{V}_{\mathrm{E}|\beta} = \mathbf{V}_{\mathrm{E,ens}} - \frac{1}{(\sigma_{\mathrm{B}}^2 + 1)}\mathbf{D}\mathbf{D}^T, \tag{3.39}$$

where $\sigma_{\mathrm{B}}^2$ is given by Eq. (3.37). Similarly, the MI between Alice and Bob from Eq. (3.10) becomes

$$I(\mathrm{A}\colon \mathrm{B}) = h(\mathrm{B}) - h(\mathrm{B}|\mathrm{A}) = 2 \times \frac{1}{2}\log_2\left(1 + \frac{\tau\sigma_{\mathrm{A,coh}}^2}{\tau\frac{1}{4} + \frac{(1-\tau)}{4} + \bar{n} + \frac{1}{4} + 2A_1}\right). \tag{3.40}$$

In Fig. 3.9, we plot the difference between the secret key of the squeezed and the coherent state protocol as a function of the quantum channel parameters for the realistic quadrature quantum efficiency of $\eta_X = 65\%$ and the quantum efficiency of $\eta = 24\%$. Except for a very small noise photon number $\bar{n} \leq 0.08$, we observe that squeezed states outperform coherent states. This is explained by the influence of the detection noise. Even though the MI is seemingly doubled for the coherent state protocol, at the same time the measurement SNR is degraded. Additionally, due to compression effects in our JPAs, the protocol codebook variance in our experimental microwave CV-QKD implementations must follow $\sigma_{\mathrm{A}}^2 \lesssim 4$. This

limits experimentally feasible squeezing levels to $S \lesssim 10\,\mathrm{dB}$, where coherent states perform worse than squeezed states, as shown in Fig. 3.9. Remarkably, in the RR case, this discussion remains valid. It is important to note that for both protocols in RR, the tolerable coupled noise is enlarged for reduced quantum efficiencies as compared to the same protocols in RR but with a perfect quantum efficiency. This effect illustrates the benefit of adding trust on the receiver side in RR [134, 135]. In the microwave regime, this improved performance in terms of tolerable noise is very important, since photon noise originating from the quantum channel is the main limiting factor for a secure microwave communication. This analysis explains a larger potential of squeezed state CV-QKD protocols over coherent ones under realistic experimental parameters.

### 3.4.5 Non-Gaussian operations

Section 3.4.3 highlights the sensitivity of CV-QKD protocols to coupled noise in the quantum channel, which strongly limits performances in terms of secure bit rates, communication distances, and feasibility of practical implementations. A possible alternative, also allowing for an increase in the tolerance to coupled noise in the quantum channel, is to use non-Gaussian operations. Among them, there exists a subclass of non-Gaussian channels relying on photon counting operations. Such operations are known to potentially improve quantum properties of Gaussian states [159, 160]. As a result, it should be possible to use such operations as part of the post-processing of CV-QKD protocols, in order to increase secure communication distances or SKRs. In particular, we can consider non-Gaussian operations on Alice's preparation side or on Bob's receiving side. Here, either Alice's states (preparation side) or Bob's states (receiving side) are sent to one input of a beam splitter, parametrized by the transmissivity $\tau_{\mathrm{NG}}$. We consider that a Fock state $|m\rangle$ is sent to the other beam splitter input. The mode at the first output of the beam splitter is used in post-processing steps to generate a secret key. In parallel, the second output mode is measured using an ideal photon counter, providing a detected photon number $n$ associated with the Fock state $|n\rangle$. Three different cases are considered, as shown in Fig. 3.10

1. The detected photon number $n$ is such that $n < m$. In this case, the number of photons in the initial Fock state $|m\rangle$ is reduced, and the number of photons in the other input state is increased. This operation is commonly referred to as *photon addition*, and the resulting state is non-Gaussian.

2. The detected photon number $n$ is such that $n > m$. In this case, the number of photons in the initial Fock state $|m\rangle$ is increased, implying that the photon number of the other input state is reduced. This operation is called *photon subtraction*. Again, the resulting state is non-Gaussian.

3. The detected photon number $n$ is the same as the initial number $m$. This case is referred to as *photon catalysis* [161]. Even if photon numbers are unchanged in the output states, one can view the operation as a virtual exchange of photons between output states. As a result, this case also leads to non-Gaussian states.

Each operation is associated with a success probability that depends on the transmissivity $\tau_{\mathrm{NG}}$. This parameter can be optimized for a required operation given a chosen input state, i.e., given a chosen CV-QKD protocol. We note that this model can be relaxed to include single-photon detection, where the measurement would be described by the set of operators $\{|0\rangle\langle 0|, \hat{1} - |0\rangle\langle 0|\}$.

In Fig. 3.11, we show a summary of a possible implementations of non-Gaussian operations. Complete and exact computations of the secret keys after usage of non-Gaussian operations is in general a complex task. In the following, we restrict our discussion to only giving sufficient

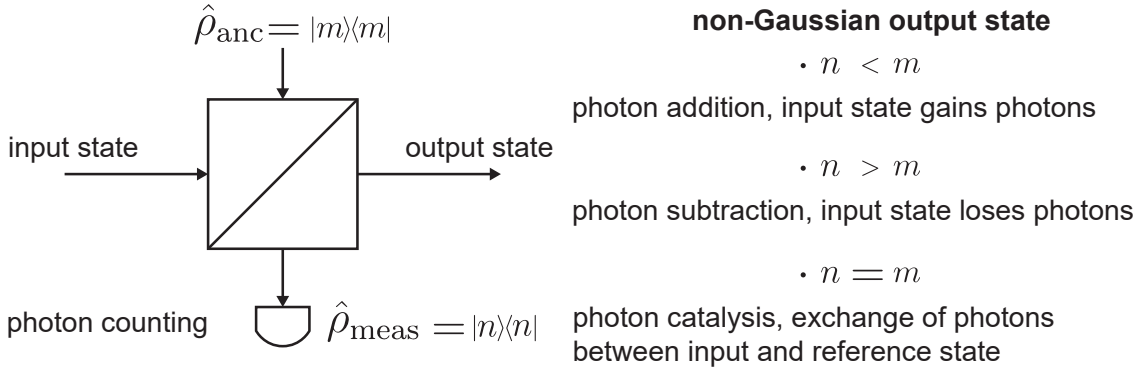


Figure 3.10: Non-Gaussian operation for a given input state, coming from either Alice or Bob. The operation is modelled using a beam splitter, where an input ancilla state $|m\rangle\langle m|$ is sent to one input port. At the output, a corresponding Fock state $|n\rangle\langle n|$ is measured using a photon counter. Depending on the value of $n$, as compared to $m$, one out of three non-Gaussian operations is implemented. In all cases, the initial Gaussian input state is transformed into a non-Gaussian output state.

elements for the estimation of a lower bound on secret keys. First, one uses the optimality of Gaussian states to simplify the analysis. This implies that we can consider a worst-case scenario where Eve's attack is modeled with a Gaussian channel. [129, 162]. Additionally, for a given protocol and quantum channel with any corresponding system state $\hat{\rho}$, an experimentally measurable secret key $K(\hat{\rho})$ is bounded from below by $K(\hat{\rho}_{\text{G}})$, where the Gaussian state $\hat{\rho}_{\text{G}}$ has the same first and second order quadrature moments as the state $\hat{\rho}$. Therefore, the main task is to compute the covariance matrix of Eve's individual and ensemble states from the corresponding attack in the DR and RR cases. Similarly, one needs to estimate the correlations between Alice and Bob after the non-Gaussian operations. A powerful tool that can be used in this case is to consider that Alice and Bob possess an input TMS state, instead of single-mode states considered earlier (prepare and measure protocols). Then, one part of the TMS entangled state is sent through the quantum channel, after which Alice and Bob perform local measurements on their local mode. This version of CV-QKD protocols is commonly referred to as *entanglement-based* protocols. It can be shown (see also Appendix A) that entanglement-based protocols are equivalent to prepare and measure protocols, meaning that the corresponding security analyses are interchangeable [154]. This way, either for Alice and Bob, or for Eve, one needs to compute quadrature moments from a two-mode state and apply transformations induced by the quantum channel and by the selected non-Gaussian operations. A powerful resource for these computations is the characteristic function (CF), $\chi$, defined in Eq. (2.72) from which quadrature moments can be derived. The CF of a TMS state reads

$$\chi_{\text{TMS}}(\alpha,\beta) = \exp\left(\frac{-\cosh(2r)}{2}(|\alpha|^2 + |\beta|^2) + \frac{\sinh(2r)}{2}(\alpha\beta + \alpha^*\beta^*)\right), \tag{3.41}$$

where $\alpha = q_1 + ip_1$ is a complex amplitude associated with the quadrature variable pair $(q_1, p_1)$ of the first local TMS mode, while $\beta = q_2 + ip_2$ is associated with the quadrature variable pair $(q_2, p_2)$ of the second local TMS mode. The quantum channel is considered again as a noisy loss channel, which is modelled as a beam splitter operation coupled to one mode of Eve's TMS state, mimicking a thermal environment. The effect of coupling one mode of a TMS state is described using the input-output relation as [163]

$$\chi_{\text{out}}(\alpha,\beta) = \exp\left(-\frac{2\bar{n}_{\text{E}}+1}{2}(1-\tau)|\beta|^2\right)\chi_{\text{in}}(\alpha,\sqrt{\tau}\beta), \tag{3.42}$$

where $\tau$ and $\bar{n}_{\text{E}}$ are the noisy loss channel parameters, defined in Eq. (3.16). Additionally, $\chi_{\text{in}}$ is the CF of the two-mode state at the input of the quantum channel, while $\chi_{\text{out}}$ is the CF of

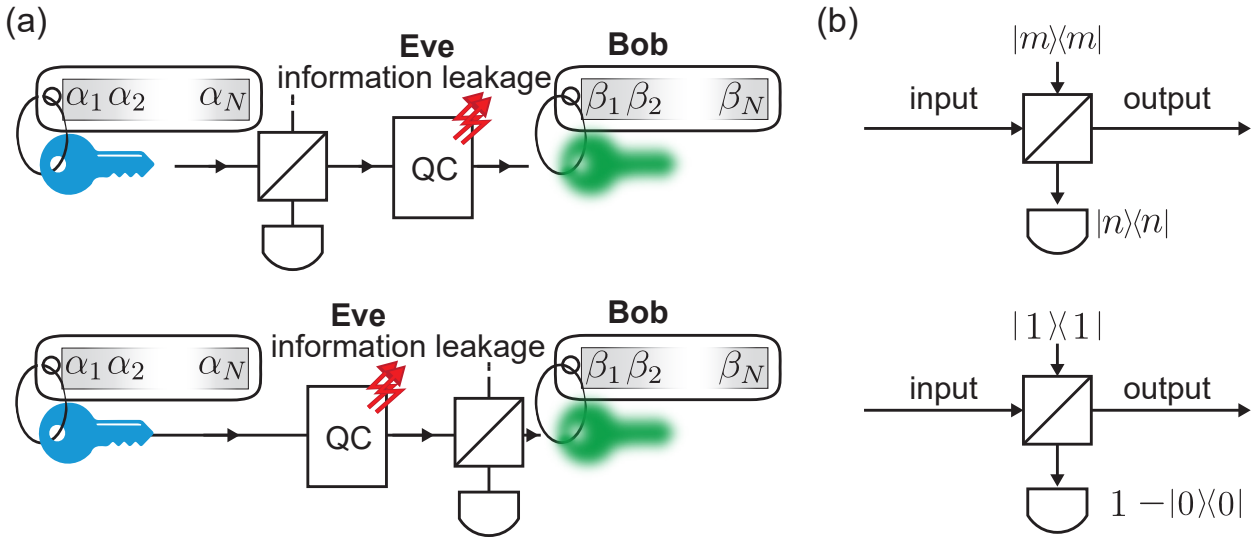


Figure 3.11: Implementation of non-Gaussian operations. (a) During the communication between Alice and Bob, a non-Gaussian operation is performed on the preparation side before sending the resulting non-Gaussian state to Bob through the quantum channel. As opposed to the situation depicted in the top part, the non-Gaussian operation can also be implemented on the receiving side, before Bob performs measurements, as shown in the bottom part. (b) Under ideal conditions, non-Gaussian operations are realized using a photon counter to accurately determine a measured state $|n\rangle\langle n|$. This condition can be relaxed in a more realistic case with single-photon detection, where the detector can capture only individual photons at a time.

the two-mode state at the output. Here, we consider that the second mode propagates through the quantum channel. Note that using this formalism, one can compute both the transformed CF of Eve's TMS state for prepare and measure protocols as well as the transformed CF of Alice and Bob's TMS for entanglement-based protocols.

Lastly, the non-Gaussian operation results in the following transformation of the CF of the input two-mode state [163]

$$\chi_{\text{out}}(\alpha,\beta) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} \chi_{\text{in}}(\alpha,\gamma)\chi_m(\gamma_1)\chi_n(\gamma_2)\frac{1}{\pi(1-\tau)}\mathrm{d}^2\gamma, \tag{3.43}$$

where $\gamma_1 = \beta/\sqrt{1-\tau} - \gamma\sqrt{\tau/(1-\tau)}$ and $\gamma_2 = \gamma/\sqrt{1-\tau} - \beta\sqrt{\tau/(1-\tau)}$. Furthermore, $\chi_k$ corresponds to the CF of the Fock state $|k\rangle$ [163]

$$\chi_k(z) = \exp(-\frac{1}{2}|z|^2)L_k(|z|^2), \tag{3.44}$$

where $L_k$ is the $k$th Laguerre polynomial with the complex number $z$. By extension of Eq. (2.73) for single-mode states, one computes the quadrature moments of a general two-mode state based on the following equations

$$\langle \hat{q}_1^m \hat{p}_1^n \hat{q}_2^k \hat{p}_2^l \rangle = (-1)^{m+k} \frac{\partial^{n+m+k+l}}{\partial q_1^n \partial p_1^m \partial q_2^l \partial p_2^k} \chi(q_1,p_1,q_2,p_2)\Big|_{q_1=p_1=q_2=p_2=0}, \tag{3.45}$$

with $m,n,k,l$ being integer numbers. To compute Eve's Holevo quantity in the DR case, Eq. (3.42),3.43, and 3.45 provide a direct access to the quadrature moments of Eve's individual states which, after integration over a chosen protocol codebook, result in the quadrature moments of Eve's ensemble state. The Holevo quantity under the worst-case scenario Gaussian attack is given by Eq. (3.12). For the RR case, one can use the Gaussian conditional covariance

matrix calculation of Gaussian states, depending on whether one quadrature is measured (see Eq. (3.20)) or two quadratures are measured by Bob (see Eq. (3.39)). The computation the MI between Alice and Bob can be done using the entanglement-based protocol formalism. Starting with Alice's and Bob's ensemble state, the same transformation as for Eve's TMS state can be applied to calculate their ensemble and conditional states after the non-Gaussian operations. Depending on the considered protocols, full analytical formulas can be derived [164].

Out of the three non-Gaussian operations presented in this section, photon catalysis has been reported as the most promising one, capable of extending tolerable excess noise as well as maximal secure communication distances for CV-QKD protocols. In Ref. 165, photon catalysis allows for a more than doubling of communication distances for a lossy quantum channel. This property is related to the ability of photon catalysis to undo effects of photon loss on entangled states [166]. As Alice, Bob, and Eve can all be viewed as having a TMS state in a generic CV-QKD protocol thanks to the equivalence between the entanglement-based and prepare-and-measure protocols, this property can be directly applied to the security analysis of CV-QKD. Remarkably, photon catalysis can also be extended to CV-QKD protocols relying on two-mode squeezed coherent states, i.e., the displaced TMS states, a class of Gaussian states relevant for measurement device-independent CV-QKD [167]. The latter aims at relaxing assumptions made to prove the security of CV-QKD by deriving a security analysis that does not depend on whether the measurement devices, used for state preparation and measurement, are trusted or not. As an alternative approach, photon subtraction is also known to increase secure communication distances, although to a lesser extent than photon catalysis. However, for microwave signals, such operations need to be performed on the Bob side, as non-Gaussian states are more sensitive to effects of noise in the quantum channel, as compared to Gaussian states [168]. Moreover, we note that the non-Gaussian operation performance is strongly affected by nonidealities in the photon number measurement methods used to implement them. Switching from photon counting to single-photon detection can lead to a severe reduction in communication distances. The success probability, as well as the efficiency of photon counting, needs to be optimized depending on the implemented CV-QKD protocol, where nontrivial optimal values of these parameters appear [168]. Interestingly, one can also implement classical data post-processing to achieve similar results. For instance, non-Gaussian functions can be used to postselect parts of Alice's and Bob's keys, implementing a virtual photon subtraction. One can optimize the reconciliation schemes to account for such non-Gaussian features and improve the performance of the CV-QKD protocols [169, 170].

## 3.5 Perspective of microwave quantum key distribution in open-air

In this section, we investigate the potential of microwave CV-QKD for open-air quantum communication and compare it to CV-QKD implementations at the telecom frequencies. The presented results are adapted from our published work [60]. Central components to realize such an open-air microwave quantum communication are introduced in Sec. 3.5.1. We analyze the generation and detection of propagating squeezed states at millikelvin temperatures. Detection is modelled by a homodyne quadrature measurement with the quantum efficiency $\eta$. Coupling of microwave squeezed states to the open-air environment (atmosphere) is modelled with two antennae with corresponding gain coefficients. The environment is assumed to be at ambient room temperature, $T = 300\,\mathrm{K}$, and is described by frequency-dependent absorption losses. The resulting secure communication distances are presented in Sec. 3.5.2 where we highlight the impact of a finite number of exchanged states in the CV-QKD protocol. In Sec. 3.5.3, we extrapolate that the microwave-based squeezed QKD protocol can potentially outperform

the telecom counterpart. This advantage becomes much more significant in the presence of weather imperfections, highlighting the resilience of microwaves to fog and rain, as discussed in Sec. 3.5.4.

### 3.5.1 Experimental scheme

Central components to realize an open-air microwave quantum communication are presented in an associated generic scheme in Fig. 3.12. We consider an experimental realization of the CV-QKD protocol from Sec. 3.3 which relies on propagating displaced squeezed states. In the microwave regime, flux-driven Josephson parametric amplifiers (JPAs) provide a well-established tool to generate squeezed states with tunable squeezing levels and angles [50, 54] as discussed in Sec. 4.2.2. Furthermore, at least one additional linear phase-sensitive amplifier is necessary on the detection side to perform single quadrature measurements. We recall that according to Cave's theory of noise in linear amplifiers [80], phase-insensitive bosonic amplifiers are quantum-limited, meaning that at least half a photon is added to amplified signals, as shown in Sec. 2.1.4. In contrast, a phase-sensitive amplifier can, in principle, achieve noiseless amplification. The JPAs operating in the GHz regime can reach noise levels well below the quantum limit, corresponding to 0.1 added noise photons in the phase-sensitive regime [24, 50, 82]. Presently, the noise performance of JPAs is known to be limited by fabrication imperfections, pump-induced noise [24, 82], and higher-order nonlinearities [73]. Lastly, the displacement operation required by our CV-QKD protocol can be experimentally realized by applying strong coherent drive tones to cryogenic directional couplers [51] (also see Sec. 4.3.4). Ultimately, the combination of the JPAs with the subsequent directional couplers allows one to generate the microwave displaced squeezed states with any desired displacement amplitude $\alpha$.

**Microwave antennae and amplification noise.** In order to couple propagating microwave states, generated at millikelvin temperatures, to the open-air quantum channel one requires a microwave interface such as a microwave antenna between the corresponding cryogenic environment and the open-air medium. This antenna may be modelled by a transmission line of spatially varying impedance connecting the $50\,\Omega$-matched cryogenic circuits to open-air channels with the characteristic impedance of $377\,\Omega$. Here, a central figure of merit of the transmitter and receiver antennae is their passive antenna gain, $G_{\mathrm{ant}}$. In general, for microwave antennae, the gain reads [68]

$$G_{\mathrm{ant}} = \eta_{\mathrm{rad}}\, D, \tag{3.46}$$

where $0 \leq \eta_{\mathrm{rad}} \leq 1$ is the radiation efficiency and accounts for the antenna losses, while $D$ represents the antenna directivity. The latter expresses the ability of the antenna to focus the emitted power into a specific direction and strongly depends on the antenna geometry. An antenna with a well-defined physical aperture area, $A$, has the directivity [68]

$$D = \frac{4\pi A}{\lambda^2}\, e_{\mathrm{A}}, \tag{3.47}$$

where $\lambda$ is the signal wavelength, and $e_{\mathrm{A}}$ is the aperture efficiency, defined as ratio between the effective and physical aperture areas. A realistic value of aperture efficiency is $e_{\mathrm{A}} = 0.67$. Cryogenic to open-air transmission of microwave signals is a current technological challenge, but first proposals already exist [171]. For communication distances of approximately 50 m, an open-air geometric attenuation of signals, also known as the path loss, is around 80 dB at the frequency of 5 GHz. In general, the path loss can be compensated by using transmitter and receiver antennae with sufficient gain values. For instance, a parabolic transmitter and receiver antenna with a diameter of around $D_{\mathrm{ant}} = 2\,\mathrm{m}$ could compensate for the aforementioned path loss. Discussions about the impact of an uncompensated path loss can be found in more detail

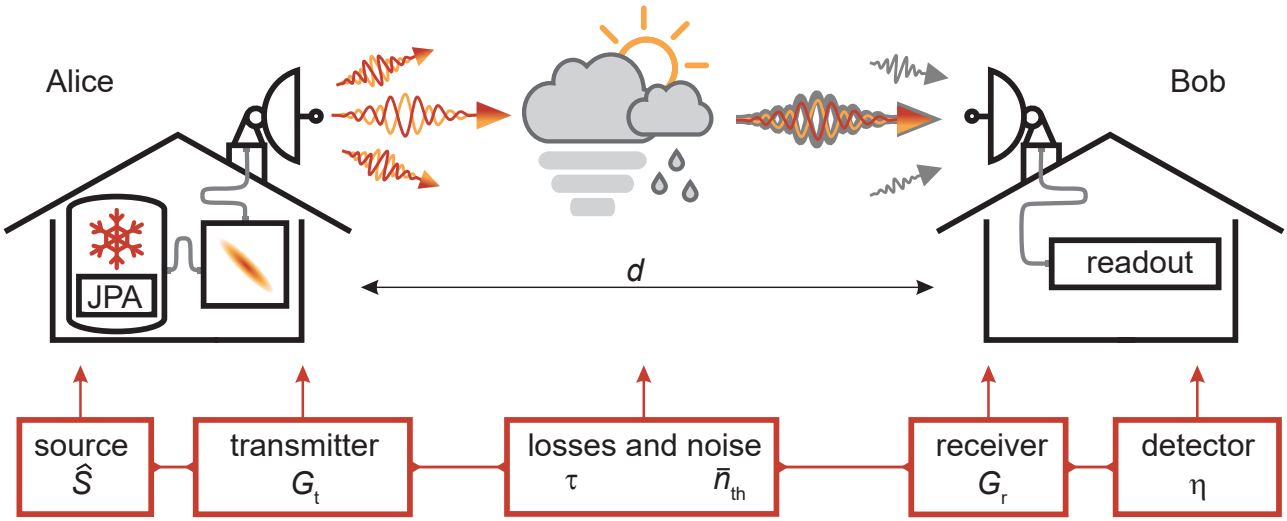


Figure 3.12: Schematic of main components for an open-air microwave quantum communication. Source denotes a squeezing generator, implemented with a JPA in a cryogenic environment. Transmitter and receiver represent corresponding microwave antennae with gains $G_t$ and $G_r$, respectively. These antennae belong to different communication parties, Alice and Bob, and are separated by a distance $d$. Atmospheric absorption losses are quantified using transmissivity $\tau$, which couples the quantum communication channel to the open-air environment with the thermal noise photon number $\bar{n}_{th}$. Readout is modelled as a homodyne detector with an overall quantum efficiency $\eta$.

in Refs. 126, 172. These works highlight the importance of geometric losses on open-air communication for microwave signals, potentially limiting secure communication distances. Here, we assume that the antenna gains fully compensate for the path loss and focus on unavoidable physical effects of atmospheric absorption losses as the main source of communication imperfections. As such, the SKRs derived in this section should be treated as upper bounds.

Additionally, the quantum efficiency of the detection chain represents a main limiting factor for optimizing the implementation of the prepare-and-measure CV-QKD protocol [82]. There, state-of-the-art travelling wave parametric amplifiers (TWPAs) allow for phase-insensitive amplification with high gain values ($\sim 20\,\mathrm{dB}$) and broad bandwidths ($\sim 3\,\mathrm{GHz}$) at cryogenic temperatures. These TWPAs are also potentially able to approach the quantum-limited regime characterized by $n_{amp} = 0.5$ for the phase-insensitive mode of operation [80]. Conversely, phase-sensitive linear amplifiers allow for (potentially noiseless) amplification of single quadratures, at the cost of deamplifying the conjugate quadrature. Such a detection scheme can be used to implement a microwave homodyne detection [173]. In cryogenic microwave experiments, one typically uses serially connected quantum-limited amplifiers followed by cryogenic high-electron-mobility transistor (HEMT) amplifiers. In this case, we can use the Friis formula [174] to estimate the total amplification noise $n_{amp}$ of the detection chain. This total noise $n_{amp}$ depends mainly on the noise properties of the first amplifier. As a comparison, for homodyne detectors at telecom wavelengths, the quantum efficiency is usually modeled by additional losses, introduced by a nonunity transmissivity with the beam splitter model. For the case of a purely lossy optical detector, both approaches are known to be equivalent, as described in Ref. 73. However, we emphasize that our definition of the quantum efficiency is well-suited for the study of microwave quantum communication, as the efficiency of signal readout is primarily limited by amplification noise in this case.

**Losses and noise budget.** We conclude this section with a brief analysis of losses and noise in open-air communication channels, where losses scale with the communication distance. We distinguish between two categories of losses: (i) the aforementioned path loss which represents

a geometric attenuation of propagating signals and (ii) absorption losses due to coupling to the environment, such as atmospheric absorption losses or weather-induced losses. For signals transmitted and received via a microwave antenna, the path loss $L_{\mathrm{p}}$, describing the fraction of the initial signal power lost during the communication, is commonly described using the Friis transmission formula [68]

$$L_{\mathrm{p}} = 10\log_{10}\left(G_{\mathrm{t}}G_{\mathrm{r}}\left(\frac{\lambda}{4\pi d}\right)^{2}\right). \tag{3.48}$$

Here, $G_{\mathrm{t}}$ ($G_{\mathrm{r}}$) is the transmitter (receiver) antenna gain, $\lambda$ the wavelength of the communication signals, and $d$ the propagation distance. The dependence of $L_{\mathrm{p}} \propto 1/d^2$ indicates a strong attenuation of the signal power due to isotropic emission of the signal in open air. This aspect makes the usage of the microwave antennae with very high directivity an absolute necessity for efficient communication. Note that in practice, high directivity microwave antennae exist and are commercially available [1], although optimized for classical communication. We model the absorption and scattering power losses via a single effective beam splitter with transmissivity $\tau$ given by

$$\tau = 10^{-\gamma d/10}, \tag{3.49}$$

where $\gamma$ is the total specific attenuation (dB/km) given by the sum of each specific attenuation $\gamma_i$ associated with a respective loss mechanism. Note that this model is equivalent to a more accurate description where the whole power losses are expressed as a chain of beam splitters coupled to local bath modes, which would describe a continuous loss of input signal power [175]. The equivalence holds if the chain of beam splitters is coupled to the same thermal bath, which is true for our analysis. In this case, we attribute the signal losses to atmospheric absorption and weather imperfections such as rain or haze. Empirical models show that for microwave frequencies around $\omega_{\mathrm{mw}}/(2\pi) \simeq 5\,\mathrm{GHz}$, these propagation losses mainly arise due to molecular oxygen absorption [176]. For the ideal case of dry weather, we estimate the corresponding specific attenuation to be around $\gamma_{\mathrm{mw}} = 6.3 \times 10^{-3}\,\mathrm{dB/km}$ [176]. To describe the coupling of the propagating quantum bosonic signal $\hat{a}$ to the noisy environmental modes, we use the input-output formalism. An output signal mode $\hat{a}'$ after interaction with the open-air thermal background can be expressed as

$$\hat{a}' = \sqrt{\tau}\,\hat{a} + \sqrt{1-\tau}\,\hat{h}_{\mathrm{env}}, \tag{3.50}$$

where $\hat{h}_{\mathrm{env}}$ corresponds to the environmental thermal mode. The latter may be a vacuum or thermal state, depending on the carrier frequency and the environmental temperature. For a thermal background, the average thermal noise photon number $\bar{n}_{\mathrm{th}}$ per mode is given by the Planck distribution as

$$\bar{n}_{\mathrm{th}} = \left[\exp\left(\frac{\hbar\,\omega}{k_{\mathrm{B}}T}\right) - 1\right]^{-1}, \tag{3.51}$$

where $\hbar$ is the reduced Planck constant, $k_{\mathrm{B}}$ the Boltzmann constant, $\omega/(2\pi)$ the signal frequency, and $T$ the background temperature in the open-air environment. From Eq. (3.50), the relation between the photon number $\bar{n}_{\mathrm{th}}$ and the coupled noise photon number $\bar{n}$ is expressed as

$$\bar{n} = \frac{1}{2}\,(1-\tau)\;\bar{n}_{\mathrm{th}}, \tag{3.52}$$

following the same model as introduced in Sec. 3.4.2. For comparison, we briefly describe the open-air losses at telecom wavelengths. In the optical frequency domain, $G_{\mathrm{t}}$ and $G_{\mathrm{r}}$ correspond to the effective passive gain of optical lenses used to focus and collect optical beams

[1] See for instance high directivity, high gain antennae available for purchase here (gain of 39 dBi for frequencies in $[5.15\,\mathrm{GHz}, 5.875\,\mathrm{GHz}]$ with an antenna diameter of 1.5 m).

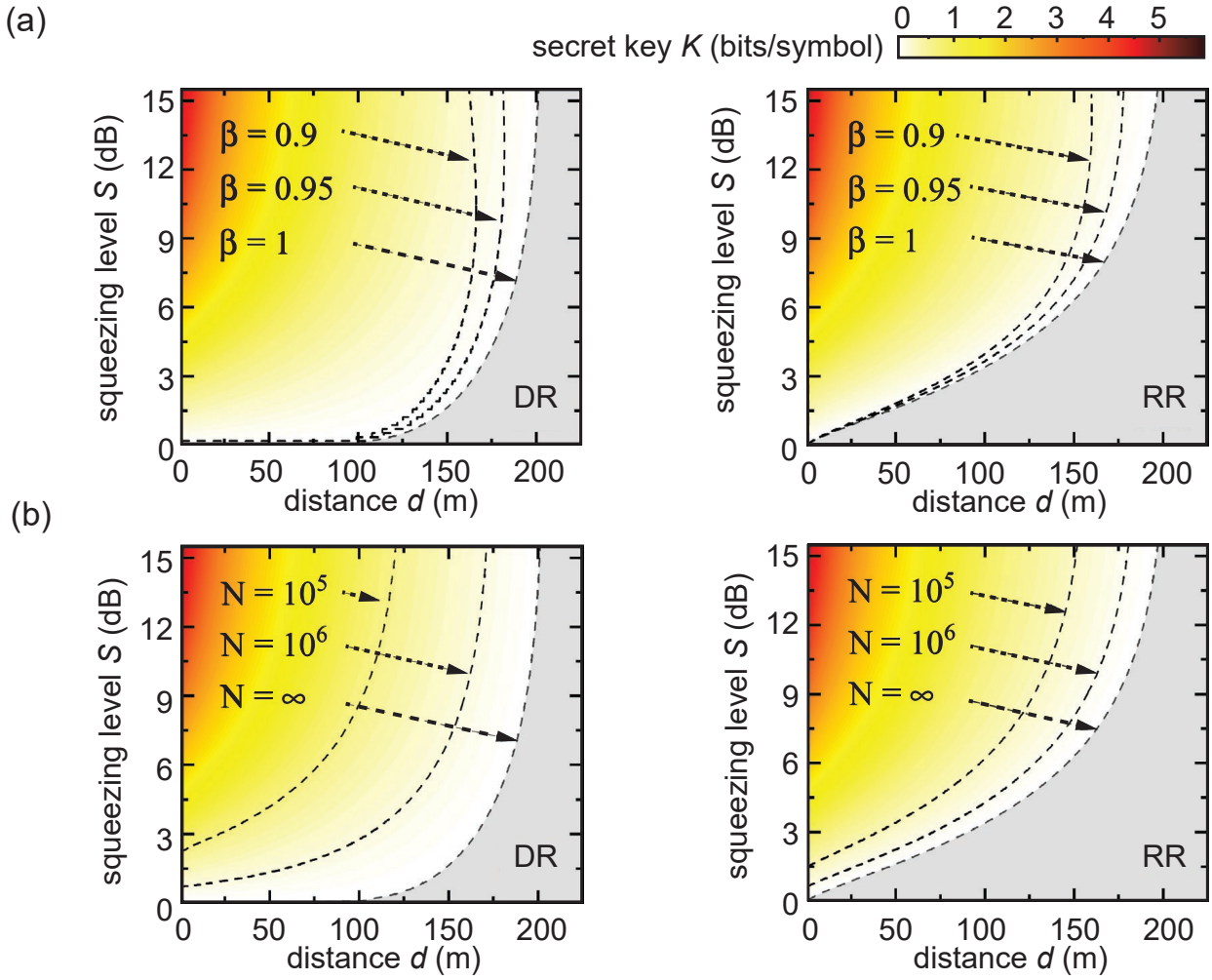


Figure 3.13: Secret key $K$ of the CV-QKD protocol as a function of its communication distance $d$ and squeezing level $S$. Left (right) plot corresponds to the DR (RR) cases, respectively. The dashed lines represent $K = 0$ for different values of $\beta$ in panel (**a**) and different values of $N$ in panel (**b**) according to Eq. (3.29). Squeezing is given in dB below the vacuum level. We assume the average environmental noise photon number $\bar{n}_{\mathrm{th}} = 1250$ and transmission losses $\gamma_{\mathrm{mw}} \simeq 6.3 \times 10^{-3}\,\mathrm{dB/km}$. Grey areas represent the regions of negative keys, i.e., insecure communication.

instead of the propagating microwave signals. Typical telecom wavelengths ($780-850\,\mathrm{nm}$ and $1520-1600\,\mathrm{nm}$) are chosen to benefit from windows of low atmospheric absorption losses or minimize the attenuation losses of optical fibres. At the telecom wavelength of $1550\,\mathrm{nm}$, optical fibre losses of less than $1.0 \times 10^{-2}\,\mathrm{dB/km}$ can be reached [177]. For this frequency, open-air attenuation is mainly caused by scattering losses, such as the Rayleigh or Mie scattering [177]. The corresponding open-air specific attenuation is $\gamma_{\mathrm{tel}} = 2.02 \times 10^{-1}\,\mathrm{dB/km}$. We discuss the additional attenuation due to rain and haze in more detail in Sec. 3.5.4.

### 3.5.2 Communication distance

First, we investigate maximal communication distances $d$ that could be achieved with the microwave CV-QKD protocol, for both DR and RR. To this end, we use Eq. (3.50) in combination with the specific attenuation given in Sec. 3.5.1 to convert communication distances $d$ into the corresponding quantum channel transmissivity $\tau$ using Eq. (3.49). We additionally consider the effects of imperfect reconciliation and finite-size effects, as mentioned in Sec. 3.4.3. The secret keys are computed using the MI in Eq. (3.10) and the Holevo quantity in Sec. 3.4.2 (see

Eq. (3.20) for DR and Eq. (3.39) for RR). The corresponding secret keys are shown in Fig. 3.13. Remarkably, we observe positive secret key values over communication distances of up to 200 m, in both DR and RR. These results suggest the experimental feasibility of microwave QKD in open-air conditions. No major distinction in communication distances is observed between the reconciliation cases, although one could intuitively expect RR to yield larger maximal secure distances. In fact, the RR case has been historically introduced to extend secure communication over the 50% loss limit of the DR case [136]. The similar behavior between DR and RR with respect to maximally achievable communication distances originates from the presence of a bright microwave thermal background, which couples to propagating states during the communication. Consequently, the effects of coupled noise largely outweigh the effects of losses and make the RR and DR cases reach similar maximal secure distances, a striking contrast to CV-QKD protocols operated at optical frequencies. Moreover, as shown in Fig. 3.13(a), we observe that an imperfect reconciliation with $0.9 \leq \beta \leq 1$ leads only to a slight decrease of the maximal secure communication distance with positive secret key values still up to 176 m (167 m) for $\beta = 0.95$ ($\beta = 0.9$). However, we note that finite-size effects have a more significant impact on the secret key values as presented in Fig. 3.13(b). Here, the total length $N$ of the key critically determines the secure communication distance, which is in agreement with the finite-size effects for other CV-QKD implementations [8]. For instance, a practical key length of $N = 10^5$ decreases the secure communication distance to 122 m (154 m) in the DR (RR) case. These effects can be overcome by extending the key length to larger values. A realistic but more demanding key length of $N = 10^6$ extends the secure communication distance to 172 m (183 m) in the DR (RR) case. We note that in a practical QKD realization, a very large key length is desirable to completely overcome any finite-size limitations, where key lengths of $N \simeq 10^9$ can be necessary [178].

Finally, we comment on the Gaussian modulation in our protocol, as compared to the discrete modulation regime. We consider the discrete modulation homodyne detection quadrature phase shift keying CV-QKD protocol [179, 180], which is similar to the one we analyze in this section. Here, instead of a continuous modulation of the key, symbols are generated by assigning quadrants of the quadrature phase space to bits, effectively discretizing any applied continuous displacement operations. Our preliminary analysis indicates that the CV-QKD protocol with such discrete modulation [180] could be realized in the microwave regime and, under ideal conditions, could achieve notably by a factor of 3 larger secure communication distances than for the protocols with Gaussian modulation. However, under more realistic conditions with noisy detectors, the discrete modulation protocols appear to quickly lose their advantage as a function of the detection noise, as compared to the Gaussian modulation protocols. We emphasize that this preliminary analysis requires further detailed investigations going beyond the scope of this section.

### 3.5.3 Comparison of telecom with microwave carriers

For a practical evaluation of the CV-QKD protocol, one additionally uses a SKR, $R_0$. The latter evaluates the amount of secure bits per second that can be obtained from the communication protocol. In the asymptotic case, one can express the SKR, $R_0$, in bits per second using the secret key as

$$R_0 = f_\mathrm{r}\, K, \tag{3.53}$$

where $f_\mathrm{r}$ represents the effective repetition rate (in symbols per second). This rate encompasses all information post-processing steps, such as sifting, parameter estimations [154, 181], and experimental bandwidths of the involved devices. We use an upper bound on the SKRs, $R$,

derived from the Shannon-Hartley theorem and the Nyquist rate [90]

$$R_0 \leq R = \frac{\Delta\omega}{\pi} K, \tag{3.54}$$

where $\Delta\omega/2\pi$ denotes the experimental detection bandwidth. This upper bound becomes especially useful when comparing different physical QKD platforms. We compare the microwave CV-QKD performance to that at telecom frequencies. For this purpose, we define and numerically compute a communication crossover distance $d_\mathrm{c}$, i.e., the maximal distance for which the microwave SKR is larger than the telecom SKR, expressed as

$$d_\mathrm{c} \coloneqq \max\{d|\, R_\mathrm{mw} \geq R_\mathrm{tel}\}, \tag{3.55}$$

where $d$ corresponds to communication distance, while $R_\mathrm{mw}$ and $R_\mathrm{tel}$ are the SKRs for the microwave and telecom carrier frequencies, respectively. Secret keys are computed in the asymptotic regime using Eq. (3.28). According to Eq. (3.54), it is relevant to optimize the detection bandwidth to achieve high SKRs. To this end, we assume an experimental broadband squeezing generation and detection at 1550 nm wavelength over a bandwidth of $\Delta\omega_\mathrm{tel}/2\pi = 1.2\,\mathrm{GHz}$ with a quantum efficiency of $\eta_\mathrm{tel} = 0.53$, as shown in [182]. In this experiment, the authors also report a measured squeezing level of 3 dB, which we will use as a reference level of vacuum squeezing for both the microwave and telecom regimes. We compute the corresponding crossover distance as a function of the microwave detection bandwidth $\Delta\omega_\mathrm{mw}/2\pi$. Here, we additionally account for a nonunity quadrature quantum efficiency $\eta_\mathrm{mw}$, as explained in Sec. 3.4.4 and modelled in Eqs. 3.36 ,3.37.

The corresponding results are shown in Fig. 3.14 for both DR and RR. Interestingly, we observe that the microwave CV-QKD protocol can outperform the telecom counterpart for realistic values of $\Delta\omega_\mathrm{mw}/2\pi$ and $\eta_\mathrm{mw}$. A clear distinction can be seen between the two reconciliation cases. For the DR case, it is beneficial to aim at a quantum efficiency close to unity and large detection bandwidths. The situation is noticeably different in RR. For the latter, we observe that above a certain detection bandwidth the optimal quantum efficiency is no longer unity. Instead, there exists an optimal detection noise added by Bob, which maximizes the SKR depending on the detection bandwidth. The existence of an optimal quantum efficiency is a remarkable feature of RR, which arises when Bob couples additional (trusted) noise during his measurements [134], as discussed in Sec. 3.2. To illustrate the influence of the quantum efficiency and the detection bandwidth, we envision two different microwave homodyne detection cases implemented by a phase-sensitive amplifier. First, we choose a high detection bandwidth $\Delta\omega_\mathrm{mw}/2\pi = 3\,\mathrm{GHz}$ with the quantum efficiency of $\eta_\mathrm{mw} = 0.345$. This case is motivated by the existing state-of-the-art superconducting TWPA devices operated in the phase-insensitive regime [183, 184]. The second case considers the detection bandwidth of $\Delta\omega_\mathrm{mw}/2\pi = 1.2\,\mathrm{GHz} = \Delta\omega_\mathrm{tel}/2\pi$, and the quantum efficiency of $\eta_\mathrm{mw} = 0.695$, such that both cases yield the same DR crossover distance. These parameters originate from recent results on broadband squeezing in the microwave regime [185, 186]. By using this set of already experimentally feasible parameters, we can reach the crossover distance of $d_\mathrm{c} = 16\,\mathrm{m}$ for both cases. For RR, we observe that the crossover distance can be increased to $d_\mathrm{c} = 25\,\mathrm{m}$. The reason is that RR benefits from quantum efficiencies below unity as stated before. Remarkably, high SKRs, $R$, of a few Gbits per second can be reached for all of the previously mentioned sets of parameters. However, we stress that the computed SKRs $R$ are merely upper bounds for realistically achievable rates. Existing telecom QKD implementations reach secure key rates up to a few Mbits per second [187, 188, 189]. Aside from finite quantum detection efficiencies and bandwidths, practical SKRs are also limited by various factors, such as actual experimental repetition rates [154], device-induced noise [188], finite-size effects [149], or post-processing [190]. Nevertheless, microwave quantum communication looks clearly relevant for short-distance classical communication situations compatible with the Wifi 802.11 standard (communication range

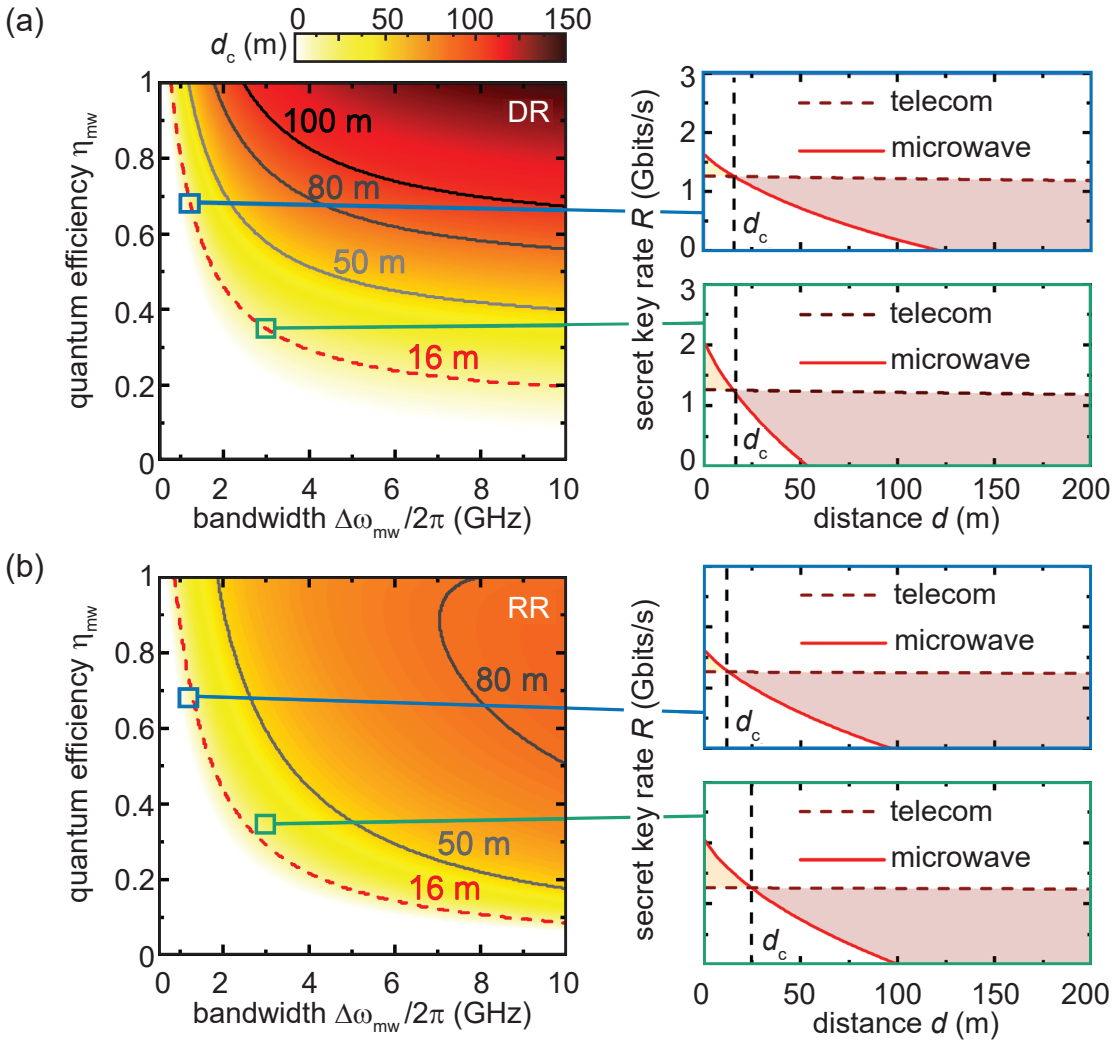


Figure 3.14: Crossover distance $d_c$ between microwave and telecom CV-QKD. Panels (**a**) and (**b**) illustrate the DR and RR cases, respectively. SKRs are computed according to Eq. (3.29) combined into Eq. (3.54). For the telecom and microwave wavelengths, we assume transmission losses $\gamma_{tel} \simeq 2.02 \times 10^{-1}$ dB/km, and $\gamma_{mw} \simeq 6.3 \times 10^{-3}$ dB/km, respectively. For both DR and RR, the SKRs, $R$, of both detection cases are shown on the right column as a function of the communication distance $d$. The top blue (bottom green) inset represents a comparison between microwave and telecom SKRs for the quantum efficiency $\eta_{mw} = 0.695$ ($\eta_{mw} = 0.345$) and detection bandwidth $\Delta\omega_{mw}/2\pi = 1.2$ GHz ($\Delta\omega_{mw}/2\pi = 3.0$ GHz).

$\simeq 70$ m), Bluetooth 5.0 ( $\simeq 240$ m), or more recent technologies, such as 5G ($\simeq 300$ m) because of their matching frequency ranges, distances, and technological infrastructure.

### 3.5.4 Weather induced loss effects

So far, we have investigated open-air CV-QKD under ideal weather conditions. We extend our analysis by investigating the effects of weather conditions on secure open-air quantum communication. It is well-known that realistic, non-optimal weather conditions may drastically affect absorption losses for propagating signals. Such effects are especially prominent in the telecom frequency range. In fact, both telecom and microwave classical communication approaches are known to suffer differently from weather imperfections such as rain or haze, whereas microwave signals are more resilient to such perturbations as compared to telecom signals. Here, we focus on how these properties translate to the quantum regime.

| losses (dB/km) / frequency | ideal | rain light/heavy | light haze/ haze |
|---|---|---|---|
| microwave | $6.3 \cdot 10^{-3}$ | $7 \cdot 10^{-3}/1.22 \cdot 10^{-2}$ | $6.4 \cdot 10^{-3}/6.7 \cdot 10^{-3}$ |
| telecom | $2.02 \cdot 10^{-1}$ | 1.91/4.17 | $1.55 \cdot 10^{-2}/17$ |

Table 3.1: Absorption losses for microwave and telecom signals under different weather conditions. For ideal conditions, we assume a visibility of 23 km, for light (heavy) rain a rain rate of 7 mm/h $\left(2\,\mathrm{mm/h}\right)$, and for light haze (haze) a visibility of 1 km (4 km).

**Non-optimal weather conditions.** We focus on two non-ideal weather scenarios: rain and haze. In the context of microwave communication, the International Telecommunication Union (ITU)-R P. 838-3 [191] and ITU-R P. 840-6 [192] recommendations provide empirical prediction models for the induced attenuation on propagating microwave signals due to rainfall and haze, respectively. More precisely, the specific attenuation $\gamma_{\mathrm{mw,r}}$ due to rain along a horizontal path can be expressed as [193]

$$\gamma_{\mathrm{mw,r}} = k\left(\omega\right)\, R_{\mathrm{r}}^{\alpha(\omega)}, \tag{3.56}$$

where $k$ and $\alpha$ are coefficients which depend on the communication microwave frequency $\omega/2\pi$, while $R_{\mathrm{r}}$ (mm/h) is the rain rate. The haze specific attenuation $\gamma_{\mathrm{h}}$ can be obtained from the liquid water concentration $M$ (g/cm$^3$) using a linear relationship as [194]

$$\gamma_{\mathrm{mw,h}} = K_{\mathrm{l}}\left(\omega, T\right)\, M, \tag{3.57}$$

where $K_{\mathrm{l}}$ ((dB/km) / (g/cm$^3$)) is the linear attenuation that depends on the considered microwave frequency $\omega/2\pi$ and water temperature $T$ in the atmosphere. The liquid water concentration can be related to a physically more intuitive quantity, the so-called visibility $V$ (km). The latter represents the distance at which the light intensity from an object drops to 2% of its initial value [177]. For a non-polluted environment, one can link two aforementioned quantities as [195]

$$M = \left(\frac{a}{V}\right)^{b}, \tag{3.58}$$

where $a = -\log\left(0.02\right)/99$ and $b = 0.92^{-1}$. For the telecom frequencies, rain causes a wavelength-independent attenuation. The specific attenuation $\gamma_{\mathrm{tel,r}}$ can be expressed for a horizontal path as [177]

$$\gamma_{\mathrm{tel,r}} = k\, R_{\mathrm{r}}^{\alpha}, \tag{3.59}$$

where $R_{\mathrm{r}}$ is the rain rate, $k = 1.076$, and $\alpha = 0.67$. The haze-specific attenuation is empirically derived similarly to the microwave case. Once again, visibility determines the specific attenuation $\gamma_{\mathrm{tel,r}}$. Empirical models for the Mie scattering show that [177, 196]

$$\gamma_{\lambda,\mathrm{h}} = \frac{C}{V}\left(\frac{\lambda}{550}\right)^{-p(V)}, \tag{3.60}$$

where $C = 39.1\log\left(e\right)$, $\lambda$ (nm) corresponds to the selected telecom wavelength, and $p$ is a scattering coefficient that depends on the considered visibility range and varies from 0 to 1.6 [177, 196].

**Effects of weather conditions.** In order to study the effect of non-optimal weather conditions on the CV-QKD secure key rates, we consider following specific situations: (i) light (heavy) rain with the rain rate $R_{\mathrm{r}} = 2\,\mathrm{mm/h}$ $\left(R_{\mathrm{r}} = 7\,\mathrm{mm/h}\right)$ and (ii) light haze (haze) with a visibility $V = 4\,\mathrm{km}$ ($V = 1\,\mathrm{km}$). We compare the telecom and microwave SKRs in Fig. 3.15. For the detection bandwidth and quantum efficiency, we stick to the previously analyzed set

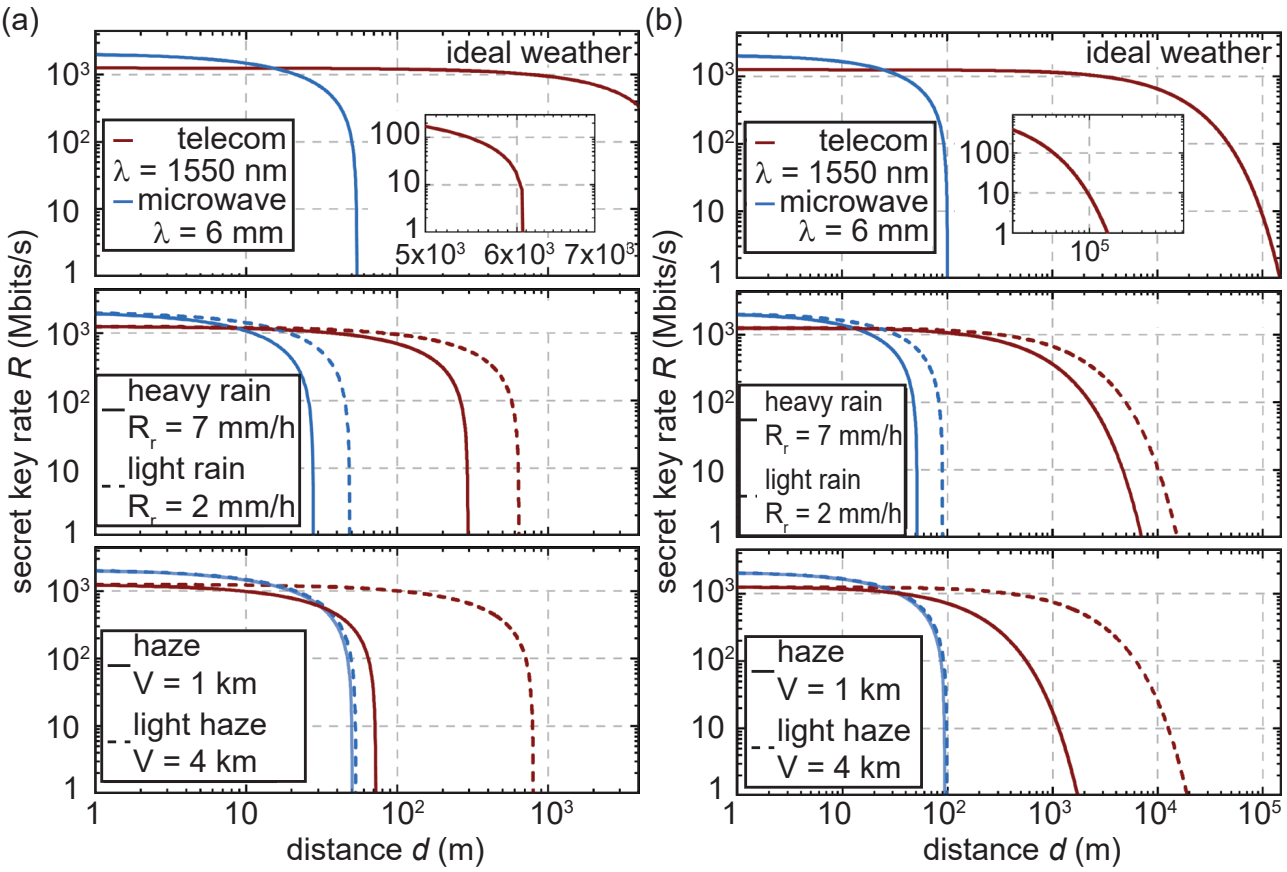


Figure 3.15: SKRs of the CV-QKD protocol for various weather conditions. Telecom (brown lines) and microwave (blue lines) SKRs, $R$, are computed for DR in panel $(a)$ and for RR in panel $(b)$ as a function of the communication distance $d$ for the squeezing levels of $S_{\text{tel}} = S_{\text{mw}} = 3\,\text{dB}$. The insets correspond to a zoom for the telecom SKRs. Three different weather conditions are considered: ideal weather conditions (visibility of 23 km), light rain (heavy rain) with a rain rate of 2 mm/h (7 mm/h), and light haze (haze) with a visibility of 4 km (1 km). The choice of quantum efficiency and detection bandwidth is the same as for the ideal weather conditions.

of parameters ($\Delta\omega_{\text{tel}}/2\pi = 1.2\,\text{GHz}$, $\eta_{\text{tel}} = 0.53$ and $\Delta\omega_{\text{mw}}/2\pi = 3\,\text{GHz}$, $\eta_{\text{mw}} = 0.345$). For completeness, we show in Tab. 3.1, the specific attenuations for microwave and telecom signals depending on the considered weather conditions. We find that short-distance microwave QKD for our parameter choices could potentially yield higher SKRs than the telecom case. The reason is that microwave QKD benefits primarily from higher experimental bandwidths, further enhanced by lower losses at imperfect weather. We note that telecom QKD allows for secure communication over much larger distances, up to $d \simeq 140\,\text{km}$ using RR. This result is expected as optical CV-QKD is known to reach kilometre-long secure communication [137, 144]. These distances are significantly reduced when the effects of rain and haze are taken into account. For these weather conditions, the maximum secure telecom communication distances is strongly reduced to $\simeq 300\,\text{m}$ (7 km) and $\simeq 70\,\text{m}$ (1.7 km), for DR (RR), respectively. Conversely, for microwave frequencies, the maximum secure communication distance is almost unchanged in both reconciliation cases compared to that obtained for the optimal weather conditions, highlighting the robustness of microwave CV-QKD to weather effects. The most significant difference arises when considering the effect of light haze. Remarkably, haze induces little-to-no extra microwave losses. Even strong haze and fog only weakly disturb microwave signals by causing a small additional attenuation of around $1 \times 10^{-3}\,\text{dB/km}$. The latter holds even when visibility is reduced to less than 500 m. In contrast, reducing the visibility below 1 km would generate large losses (more than $\sim 20\,\text{dB/km}$) for the telecom signal frequencies, preventing any possibility

of a long-distance secure quantum communication with a meaningful SKR. These results indicate that an ideal quantum open-air communication network could consist of a combination of microwave-based channels for short distances ($d \leq 200\,\mathrm{m}$) and telecom-based channels for long distances ($d > 200\,\mathrm{m}$). It would also be important to develop microwave open-air CV-QKD for short-range applications, such as building-to-building communication, where the microwave signals are mostly undisturbed by any change in weather conditions.

### 3.5.5 Summary on open-air CV-QKD in the microwave regime

In conclusion, we have performed a comprehensive analysis of microwave CV-QKD and demonstrated its potential for applications in open-air conditions. We have shown that quantum microwaves can yield positive SKRs for short-distance communication for both the DR and RR cases. Our calculations rely on empirical models for microwave and telecom atmospheric absorption losses. We have estimated the related microwave and telecom-specific attenuation values for optimal weather conditions to be $6.3 \times 10^{-3}\,\mathrm{dB/km}$ and $2.02 \times 10^{-1}\,\mathrm{dB/km}$, respectively. In our analysis, we have assumed microwave homodyne detection based on state-of-the-art TWPAs. Our model for the CV-QKD protocol predicts positive SKRs for the microwave regime over distances of around 200 m. We have extended our analysis to include imperfect reconciliation and finite-size effects. Here, we have found that an imperfect reconciliation only marginally limits the communication distance and that finite-size effects can be overcome using a key length of $N \geq 10^6$. We have employed this model to compare the microwave and telecom cases for different detection quantum efficiencies and bandwidths. Our results show that, based on parameters of state-of-the-art technology, the microwave CV-QKD can potentially outperform the telecom implementations for short distances of around 30 m in terms of the SKRs. From our analysis, it appears that both reconciliation scenarios are relevant. In particular, DR is favored for high quantum efficiencies and offers a better robustness to coupled noise from the quantum channel compared to RR, while the latter allows for applications with rather lower detection quantum efficiencies $\eta$. The RR case also exhibits a nontrivial dependence of the SKR, $R$, on $\eta$, which can be explained by the positive impact of detection noise on the protocol security.

Finally, we have considered the open-air CV-QKD protocol under nonideal weather conditions of rain and haze. We have found that these nonidealities strongly reduce the secure communication distance for the telecom regime, from 140 km to several hundred meters. Remarkably, the microwave open-air CV-QKD protocol appears to be largely immune to these weather imperfections, with its secure communication distances staying mostly unchanged. These results encourage first prototypes of secure microwave quantum local area networks and lay the foundations for hybrid networks, where short-distance secure communication is carried out by microwave quantum signals. Such a hybrid quantum network offers the advantage of providing potential high SKRs and robustness to weather imperfections, while relying on telecom setups for long-distance communication. Short-distance microwave quantum communication secure platforms could also complement current classical microwave communication technologies, such as Wifi, Bluetooth, and 5G due to the intrinsic frequency and range compatibilities.

# Chapter 4

# Experimental techniques

Experimental implementation of quantum communication at gigahertz frequencies requires cryogenic systems with associated room-temperature electronics allowing for precise control and measurement of microwave signals. In Sec. 4.1, we introduce the main cryogenic system used in this thesis with a corresponding room-temperature detection chain. In our experiments, we perform Wigner function tomography based on measured, digitized, and filtered signals. Our analysis relies on a reference state reconstruction method from which we extract signal moments up to the fourth order. In the case of ideal Gaussian states, the knowledge of moments up to the second order is sufficient. In Sec. 4.2, we present the JPA chip packaging with additional characterization measurements to determine experimentally relevant properties. Finally, in Sec. 4.3, we discuss calibration measurements which provide all necessary experimental parameters for our CV-QKD protocol. These calibrations are based on an advanced 2D Planck spectroscopy [197], serving as a novel and precise technique to extract the amount of losses present at the sample stage of our cryogenic setup.

## 4.1 Experimental setup

In this section, we focus on our experimental setup, which includes both the cryogenic system and the associated room-temperature signal detection chain. First, Sec. 4.1.1 introduces a $^3$He/$^4$He cryogenic dilution refrigerator unit. The dilution fridge houses experimental components required for our CV-QKD protocol implementation. All relevant room temperature devices used in our measurements are presented in Sec. 4.1.2, where we discuss signal processing steps including digital filtering of measured signals, followed by a digital $I/Q$ demodulation. This signal processing relies on measurements of microwave signals outgoing from our cryogenic system using a field programmable gate array (FPGA). The corresponding FPGA detection setup processes the aforementioned signals, performing both filtering and down-converting them to the intermediate frequency of 11 MHz. Details about this setup are shown in Sec. 4.1.3. Lastly, in Sec. 4.1.4, we explain the reference state tomography method and computation of signal moments up to the fourth order.

### 4.1.1 Cryogenic setup

Our experiments are based on superconducting microwave circuits, which allow for the engineering of quantum states necessary for the CV-QKD protocol implementation. The quantum properties of these circuits are extremely susceptible to the presence of noise photons. For instance, quantum entanglement degrades rapidly as a function of noise and completely disappears at 1 coupled noise photon, a process known as the sudden death of entanglement [198].

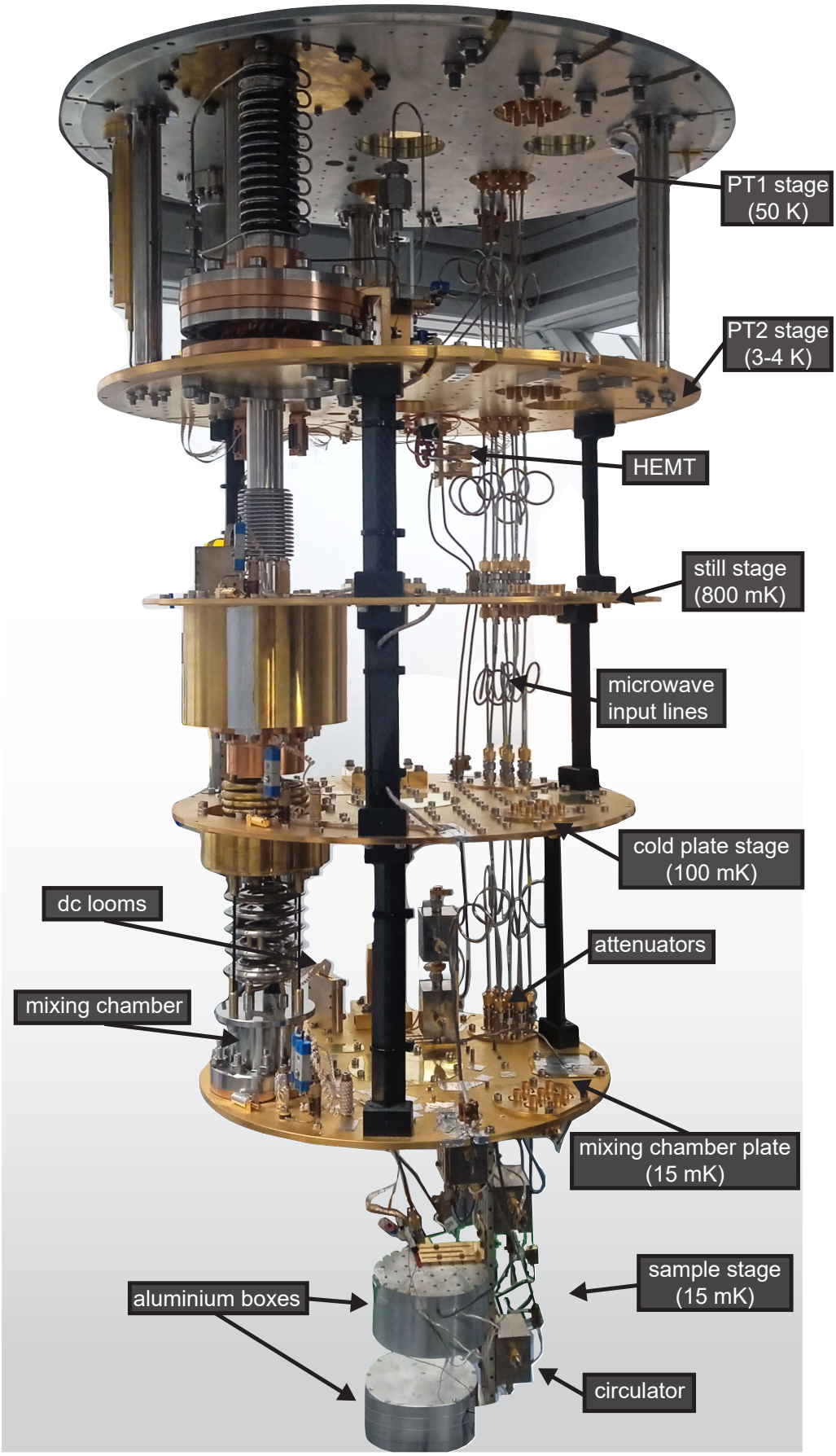


Figure 4.1: Photograph of the dilution cryostat with labelled temperature stages, and selected microwave components. The aluminium boxes contain the JPA samples used in our experiments.

Similarly, squeezing is strongly sensitive to the presence of noise [27]. More generally, superconducting devices require the use of cryogenic techniques to cool them well below the liquid helium temperature of 4.2 K. At the same time, in the microwave regime, the energy scale of microwave photons at a frequency around 5 GHz is about 5 orders of magnitude smaller than for optical photons at frequencies around 190 THz. As a result, it is important to ensure a low mean noise photon number, $\bar{n} \ll 1$, in experiments. As a results of working with commonly low power signals, one must additionally strongly amplify these signals for them to be detected and measured. A conventional method of amplification of microwave signals in cryogenic setups relies on the use of cryogenic high-electron-mobility transistors (HEMTs) with typical gain values of $G_{\mathrm{H}} \simeq 40\,\mathrm{dB}$. These amplifiers also add around 10 noise photons referred to their input during the amplification, which represents a major limitation for measurements of microwave quantum signals [173]. Based on Sec. 2.2.1, HEMTs are limited by the SQL and necessarily add at least half a noise photon per quadrature (see Sec. 2.1.4). This added noise implies that many essential quantum correlations, such as entanglement or vacuum squeezing, are lost after the HEMT amplification. However, the original quantum information arising from these quantum properties is contained within in the amplified signals.

The cryostat system used in the experiments presented in Chap. 5 is a commercial Triton system from Oxford Instruments [199]. We use this cryogenic unit to cool down our experimental components to the base cryogenic temperature of $T \simeq 15\,\mathrm{mK}$. The refrigerator is composed of several temperature stages, highlighted in Fig. 4.1. The different temperature stages are precooled using a small part of a $^3$He / $^4$He mixture, extracted from a 810 mbar mixture tank, representing a few millibar of pressure loss in the tank. The precooling is achieved notably via a two-stage pulse tube refrigerator (PTR). During this step, the small amount of mixture is pumped and circulates inside the precooling circuits, allowing for precooling of the cryostat. This small amount of mixture is pressurized to roughly 2.5 bar at a compressor provided with the Triton system. The first two temperature stages, labelled "PT1" and "PT2" respectively, are designed to be eventually cooled to working temperatures of $T \simeq 50\,\mathrm{K}$ and $T \simeq 4\,\mathrm{K}$. Three additional temperature stages are present, labelled in order "still", "cold plate", and "mixing chamber" (MC). Once the still and MC stages reach temperatures below 10 K, the precooling mixture is evacuated back into the mixture tank using a turbo-molecular pump (TMP) with a scroll backing pump. Then, a full condensation of the entire mixture is started. The coldest temperature of the refrigerator is obtained at the MC, with a minimum temperature as low as $T \simeq 15\,\mathrm{mK}$ in our experiments. At this temperature, there are two phases of the $^3$He / $^4$He mixture in equilibrium, namely a concentrated phase (nearly 100%) of $^3$He and a dilute phase (about 6.6% of $^3$He and 93.4% of $^4$He). These two phases are separated by a phase boundary with the lighter concentrated phase sitting on top of the heavier dilute phase. By pumping on the dilute phase, mostly $^3$He is removed from this phase and has to be continuously transferred from the concentrated to the dilute phase across the phase boundary to keep the minimum $^3$He concentration in the dilute phase. The enthalpy of $^3$He in the dilute phase is higher than in the concentrated phase and additional energy is required to allow $^3$He to cross the phase boundary. This energy is extracted in the form of heat from the environment thus making the dilution an endothermic process [200, 201]. As a result, the flow rate of $^3$He directly determines the cooling power. In the dilute phase, $^3$He is pulled by an osmotic pressure gradient to the still. On its way up, the cold dilute $^3$He additionally cools, through heat exchangers, the $^3$He circulating downward towards the MC. Considering there is a finite pumping power in the system, heat is supplied at the still stage to increase the vapor pressure of $^3$He, higher than the one of $^4$He, in order to maintain a steady $^3$He flow. However, the still cannot be excessively heated because $^4$He would start to evaporate significantly. Therefore, we commonly operate with a still temperature of $T \simeq 800\,\mathrm{mK}$ to compromise for both effects. For more technical details about cryogenic dilution refrigerators, we invite the reader to consult Ref. [202].

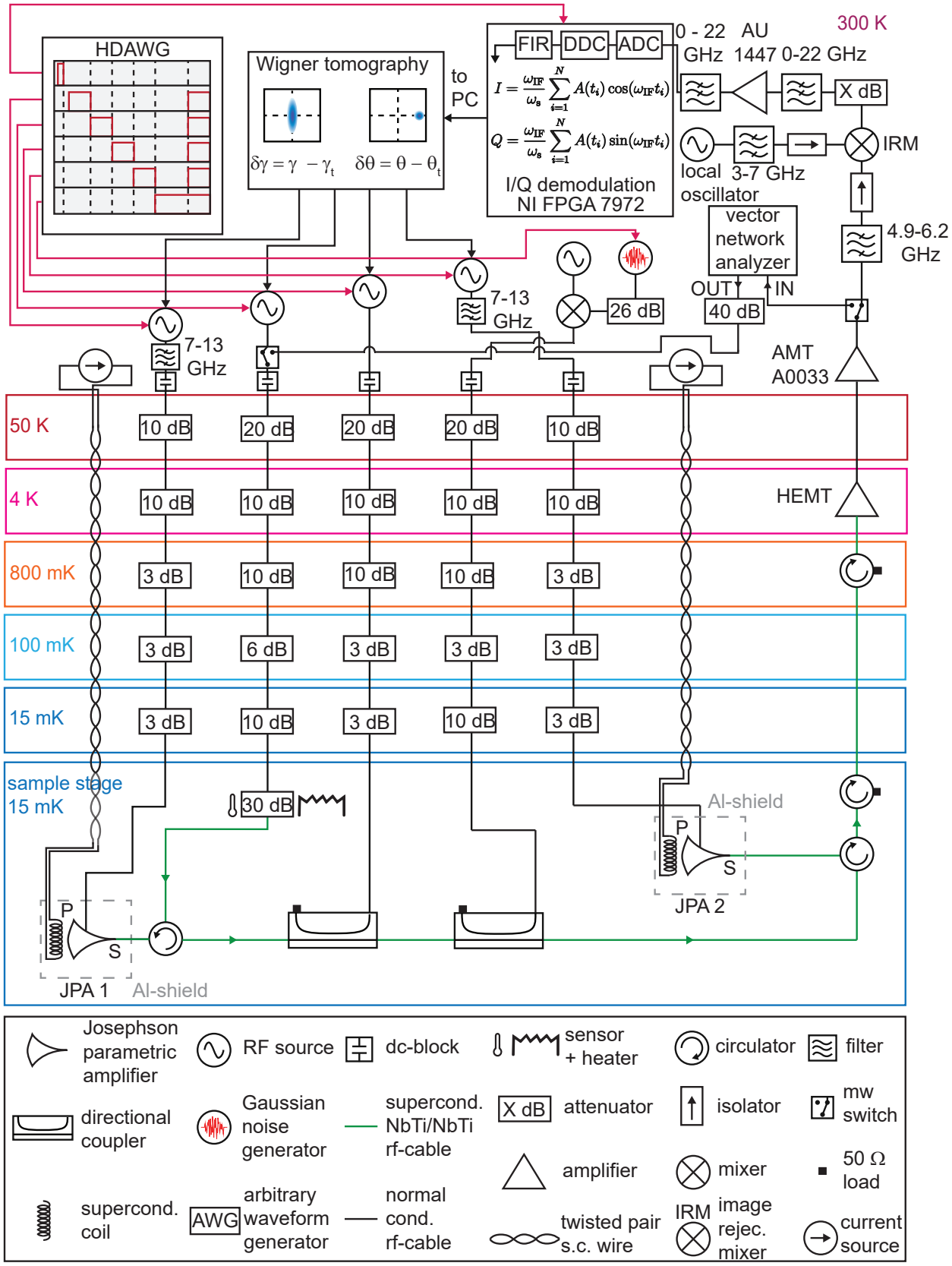


Figure 4.2: Experimental scheme of our CV-QKD implementation with propagating microwave states. The superconducting magnetic solenoids are located on top of the JPAs. All microwave signal sources are modulated using an AWG, and all devices are referenced to a 10 MHz clock signal. The noise generator is an AFG 81160A from Keysight, and the AWG is a HDAWG from Zurich Instruments. The current sources are 6241A sources from ADCMT.

In the cryogenic system, input radio-frequency (RF) lines are installed through all temperature stages using stainless steel (SS) cables. These cables are mechanically stable and robust at cryogenic temperatures, possessing low thermal conductivity as desired for efficient thermal decoupling of the cryostat stages [201]. However, these cables are characterized by significant losses of several dB/m at gigahertz frequencies. This property is not a critical limitation for the input lines, as long as the cooling power of the dilution cryostat at each temperature stage is sufficient to sustain the heat load induced by signal dissipation. Additionally, we attenuate the input lines using microwave attenuators in order to suppress incoming thermal noise, bringing it into equilibrium with millikelvin temperatures [203]. We commonly use attenuation of 20 dB for the first PTR stage (PT1, see above), 10 dB for the second PTR (PT2) and still stages, and 6 dB for the cold plate and MC stage. For the input lines which we use for sending the pump signals to our JPA samples, we use lower attenuation values, as we require strong, on the order of $-50$ dBm, signals in order to enable desirable parametric amplifications. At the sample stage, we use NbTi superconducting cables with low microwave losses at cryogenic temperatures of $5 \times 10^{-2}$ dB/m [204]. These low losses are important in our experiment to preserve the quantum properties of propagating microwave quantum states before amplification. The inner and outer conductors of our superconducting coaxial cables are made of NbTi and are manufactured by CoaxCo (Japan). These cables are terminated at each end with crimped SMA connectors. We ensure that all microwave connectors have a low impedance mismatch from the desired target of $Z = 50\,\Omega$. We determine this impedance mismatch using a time domain reflectometer (TDR) and target mismatch values around $2\,\Omega$. At the sample stage, cables and microwave components of our experimental setup are thermally and mechanically anchored to a silver rod, which is itself connected directly to the MC stage. To ensure good thermalization, we use additional silver ribbons attached to each component and the silver rod. After bending these ribbons in a desired shape, we anneal them at 900°C for one hour in vacuum, in order to improve their thermal conductivity. To provide electric currents to flux-bias JPAs, we rely on dc looms running through the cryostat. The looms are connected to several pin connectors that house twisted pairs of thin superconducting wires. These wires connect to various experimental components such as thermometers, heaters, or superconducting coils. We mention that further technical details about the cryostat can be found in Ref. [205].

### 4.1.2 Experimental setup

In this section, we discuss the experimental setup used in this work, as shown in Fig. 4.2. The setup is composed of two JPAs connected in series with two cryogenic directional couplers in between. Both JPAs are pumped individually with microwave signals generated by room temperature microwave sources (SGS 100A from Rohde & Schwarz). During measurements with one of the single JPA, the other JPA is detuned far from resonance in order to avoid unwanted interferences. Typically, this detuning is around several tens of megahertz and is implemented by changing the magnetic flux controlled by individual JPA magnetic coils. Additionally, each JPA is encapsulated in an aluminium box to prevent magnetic flux crosstalk between them and shield them from stray fields. The first directional coupler is used to perform the displacement operation of quantum states and is connected to another microwave source (SGS 100A from Rohde & Schwarz). The second directional coupler is used to controllably couple Gaussian noise to prepared quantum states. The noise coupled to the second directional coupler is generated by an arbitrary function generator (AFG 81160A from Keysight) acting as a quasi-Gaussian noise source with a crest factor of 7, meaning that the noise signal is limited by a $\pm 7\sigma$ window, with $\sigma$ being the standard deviation of the corresponding Gaussian distribution. This Gaussian noise has a spectral bandwidth of 200 MHz and is up-converted to carrier frequencies around 5 GHz using a mixer driven by an additional microwave source (SGS 100A from Rohde & Schwarz).

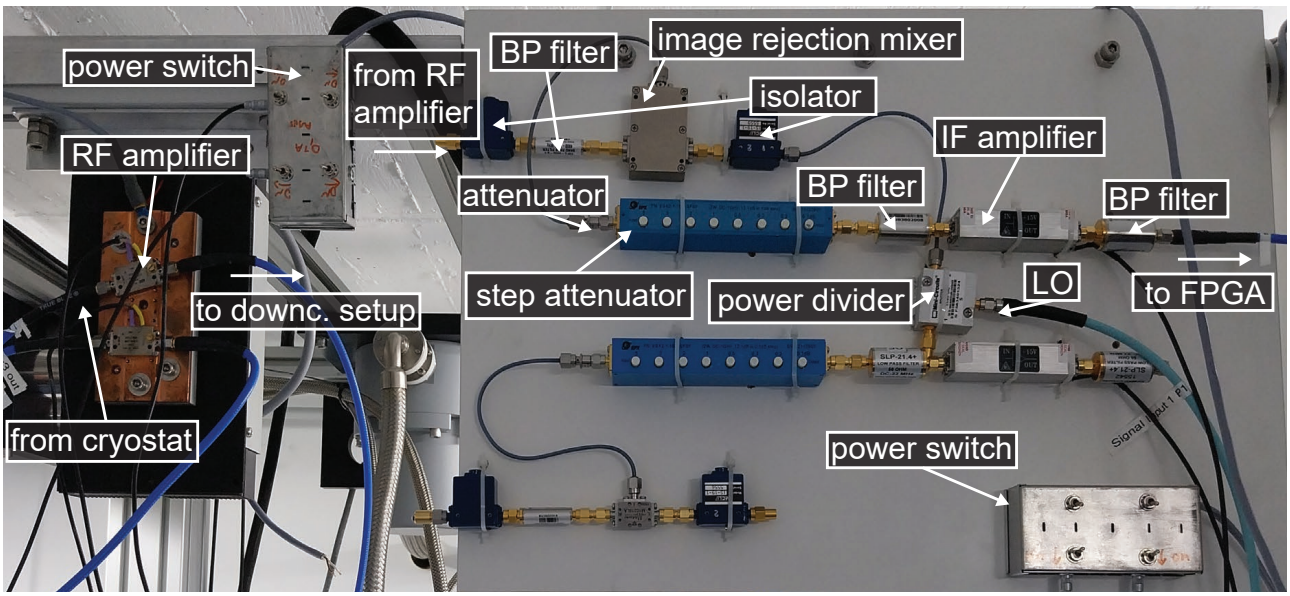


Figure 4.3: Photograph of the room temperature down-conversion setup. A signal from our cryostat is amplified by an RF amplifier before down-conversion in the image-rejection mixer, driven by the external LO, to the intermediate frequency range. An additional RF and IF amplifiers are used to further amplify signals.

The output signal after the HEMT (LNF-LNC4_8F from Low Noise Factory) is amplified by a room-temperature RF amplifier (AMT-A0033 from Agile MwT). We use a vector network analyzer (VNA) for spectroscopic measurements of both JPAs in order to characterise their flux-dependent frequency response. Amplified signals are filtered around a center frequency using a bandpass filter before being down-converted to the IF frequency of 12.5 MHz with the image rejection mixer driven by a local oscillator (LO) signal originating from an additional SGS source.

The data processing, resulting in $I/Q$ sampled data points, consists of a digital down-conversion (DDC) and a filtering using a digital finite-impulse response (FIR) filter with a full measurement bandwidth of 400 kHz. We compute the quadrature moments $\langle I^k Q^l \rangle$ for $k + l \leq 4$ $\left((n, m) \in \mathbb{N}^2\right)$ from $2.475 \times 10^8$ filtered $I/Q$ points. Using the reference state reconstruction method (Sec. 4.1.4 below), we experimentally extract the phase of measured signals and adjust the corresponding phase of the signal generators in order to stabilize the aforementioned angles around desired target values during hours-long measurements. The angle drift in our experiments is typically on the order of 1°/h and varies depending on the used room temperature sources, stability of magnetic fields, and other imperfections. For state tomography measurements, the angles are continuously adjusted. For single-shot measurements, where no data averaging is performed, we restrict the data analysis to single $I/Q$ points and do not continuously adjust the phase of the signal sources. Knowing the signal phase drift, we adapt measurement times such that all signal phases remain stable within less than 1 degree from their corresponding desired values. For state tomography measurements, we switch on measurement devices only during specific time windows. This is achieved using an arbitrary waveform generator (AWG) (HDAWG from Zurich Instruments), which generates square pulse trains to trigger measurement devices for a specific, tailored time window. For calibration measurements, we split this time window into $N$ identical intervals, where $N$ is the number of involved quantum states, which depends on the specific calibration measurement (see Sec. 4.3 for details).

We note that for state tomography purposes, one of these intervals necessarily corresponds to a measurement with all signal generator devices switched off. The HDAWG additionally

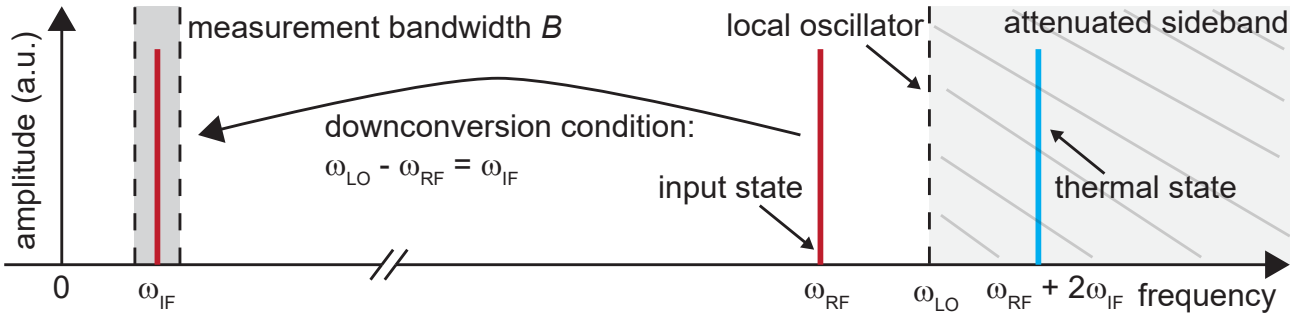


Figure 4.4: Down-conversion principle. An input signal at the frequency $\omega_{\mathrm{RF}}$ is down-converted to the intermediate frequency $\omega_{\mathrm{IF}}$ within a full measurement bandwidth $B = 400\,\mathrm{kHz}$ using an image rejection mixer with a LO at the frequency $\omega_{\mathrm{LO}} = \omega_{\mathrm{RF}} + \omega_{\mathrm{IF}}$. Such a mixer strongly attenuates the blue sideband signal at a frequency $\omega_{\mathrm{rf}} + 2\omega_{\mathrm{IF}}$, which would otherwise be down-converted to the IF frequency as well, inducing additional noise that could limit detected squeezing levels.

provides a 1.6 V rectangular trigger signal for the FPGA card to start signal recording and for a proper synchronization of the data acquisition as well as of the devices. The VNA, HDAWG, FPGA, and LO are synchronized by a 10 MHz reference signal from a S725 rubidium frequency standard from Stanford Research Systems. The microwave signal sources are daisy-chained to the LO using the 1 GHz reference signal for better phase stability.

### 4.1.3 Heterodyne detection setup

Our measurement setup is based on a heterodyne detection setup with the purpose of computing $I/Q$ quadratures of signals coming from our cryostat. These quadratures can be used for the computation of their statistical moments and Wigner tomography. Radio frequency (RF) signals at the output of our cryostat are amplified by a room-temperature RF amplifier (AMT-003 from Agile MwT) with a gain of 28 dB. Signals are processed through the down-conversion setup shown in Fig. 4.3. There, a first bandpass filter has a bandwidth from 4.9 GHz to 6.2 GHz (VPFZ-5500-S+ from Mini-Circuits) before an image rejection mixer (IRM4080B from Polyphase). The latter down-converts RF signals at a frequency, $\omega_{\mathrm{rf}}$, to a desired intermediate frequency (IF), $\omega_{\mathrm{IF}}$, using a microwave source (SGS 100A from Rohde & Schwarz) that acts as a LO. The frequency of the LO signal is chosen according to $\omega_{\mathrm{LO}} = \omega_{\mathrm{RF}} + \omega_{\mathrm{IF}}$. Note that the use of an image rejection mixer is critical to avoid the presence of down-converted signals from a mirror frequency $\omega_{\mathrm{RF}} + 2\omega_{\mathrm{IF}}$. The IF frequency is chosen to be commensurable with the signal sampling frequency of $\omega_{\mathrm{s}} = 125\,\mathrm{MHz}$ and is set to $\omega_{\mathrm{IF}} = 12.5\,\mathrm{MHz}$.

The overall down-conversion principle is illustrated in Fig. 4.4. This IF frequency is also advantageous, because it is sufficiently detuned from the clock reference frequency of 10 MHz. This clock signal (provided by the S725 rubidium frequency standard) also allows for a proper phase synchronization of all experimental devices. Down-converted signals are strongly amplified by an IF amplifier (AU-1447-R amplifiers from Miteq) with a gain of 58 dB. We note that this process introduces additional noise in the amplified signals. However, the noise properties are primarily determined by the first amplifier in our amplification chain and are not limited by this noise. Resulting signals are guided to the FPGA device, where analog signals are digitized and processed. The digitization is performed based on the National Instruments NI-5782 transceiver module with an analog-to-digital converter (ADC) with a 14-bit resolution, while the connected National Instruments PXIe-7972R FPGA processes the recorded data in parallel. The FPGA sampling frequency of $\omega_{\mathrm{s}} = 125\,\mathrm{MHz}$ is seemingly doubled in our experiment as two recording channels of the FPGA are used in parallel and combined in data analysis. Recorded data points $\{A(t_i)\}_{i\in[1,N]}$ are used to perform a digital $I/Q$ demodulation of a measured signal

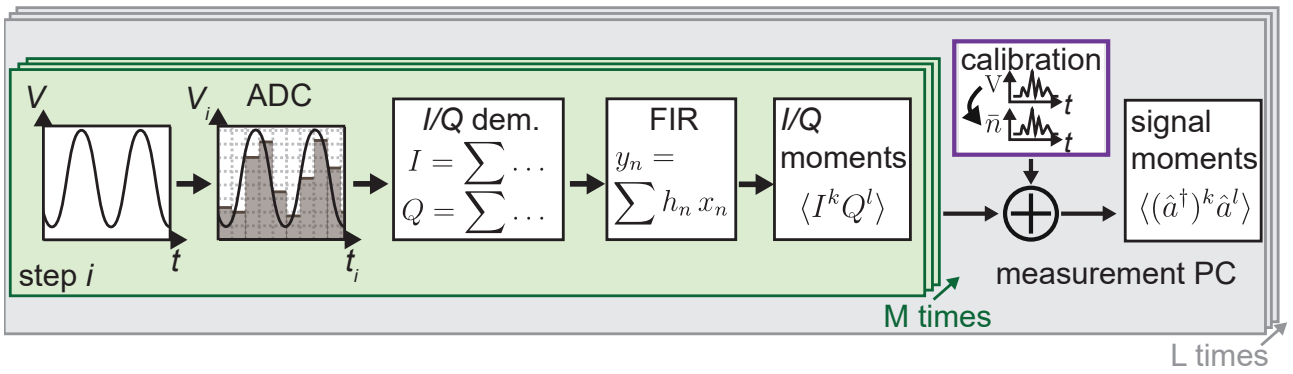


Figure 4.5: Schematic for the data acquisition and processing of our FPGA. An input signal is digitized by an ADC and subsequently digitally demodulated, resulting in pairs of $I/Q$ points. They are digitally filtered using a FIR with 90 coefficients from which $I/Q$ moments up to the fourth order are computed. The data is then sent to a measurement PC for further post-processing. There, using a photon number calibration factor, $I/Q$ moments are converted into signal moments from which experimental parameters are extracted. The moments are calculated over $M$ measured traces before being sent to the measurement PC. The overall process is repeated $L$ times.

$A$ as

$$\begin{aligned} I(t) &= \frac{\omega_{\mathrm{IF}}}{\pi}\int_{t}^{t+\frac{2\pi}{\omega_{\mathrm{IF}}}} A(\tau)\cos(\omega_{\mathrm{IF}}\tau)\mathrm{d}\tau \simeq \frac{\omega_{\mathrm{IF}}}{\omega_{\mathrm{s}}}\sum_{i=1}^{N} A(t_i)\cos(\omega_{\mathrm{IF}}t_i), \\ Q(t) &= \frac{\omega_{\mathrm{IF}}}{\pi}\int_{t}^{t+\frac{2\pi}{\omega_{\mathrm{IF}}}} A(\tau)\sin(\omega_{\mathrm{IF}}\tau)\mathrm{d}\tau \simeq \frac{\omega_{\mathrm{IF}}}{\omega_{\mathrm{s}}}\sum_{i=1}^{N} A(t_i)\sin(\omega_{\mathrm{IF}}t_i), \end{aligned} \tag{4.1}$$

where the digitization times are chosen as $t_i = t_0 + 2\pi i/\omega_{\mathrm{s}}$ and $N$ corresponds to an integer such that the integration time corresponds to exactly one IF period. It is computed as $N = \lfloor \omega_{\mathrm{s}}/\omega_{\mathrm{IF}} \rfloor = 10$, with $\lfloor\cdot\rfloor$ being the floor function. The initial time, $t_0$, corresponds to the beginning of the measurement while the index $i$ is such that the time $t$ fits in the interval $[t_i, t_{i+1}]$. For completeness, we mention that each $I/Q$ at a time $t$ is obtained from the average of both recording channels. In order to reduce the detection noise after demodulation, we use a digital finite impulse response (FIR) filter which sets the measurement bandwidth to a single-sideband value of $B = 200\,\mathrm{kHz}$.

The digital filtering operation is implemented using a sequence of coefficients $h_n$, referred to as an impulse response sequence, within a window of $N$ points. A filtered point at a time $t_n$, as defined in Eq. (4.1) with the convention $t_0 = 0$, is denoted $y_n \coloneqq y(t_n)$ and computed according to

$$y_n = \sum_{k=0}^{N} h_n\, x(t_n - t_k) = \sum_{k=0}^{N} h_n\, x_{n-k}. \tag{4.2}$$

Here, $x_{n-k}$ denotes an input signal digitized at a time $t_n - t_k$. In our experiments, we use $N = 90$ points to compute the filtered signal points, $y_n$. For each subsequent computation, this window of points is shifted by one input data point to the right. For instance, the ensemble of input data points $\{x_{n-N+1}, \ldots, x_n\}$ is used to compute the filtered data point $y_n$, while the ensemble $\{x_{n-N+2}, \ldots, x_{n+1}\}$ is used to compute the data point $y_{n+1}$. To guarantee a finite response time and design a desired frequency response of the filter, the impulse response sequence is multiplied by a weighting window sequence, $w_n$. These weighting coefficients are chosen according to a Hamming window centred around the IF frequency $\omega_{\mathrm{IF}}$ with the cutoff frequency of 200 kHz. The filter coefficients are obtained using the Filter Designer interface of MATLAB, provided by its DSP system toolbox. We note that smaller filtering bandwidths below 200 kHz

are possible but more computationally demanding, limited in practice by the available memory in the FPGA. We refer to Ref. 206 for technical details about this signal data processing and associated FPGA implementation. Subsequently, filtered $I/Q$ points are used to compute $I/Q$ moments $\langle I^k Q^l \rangle$, with $(k,l) \in \mathbb{N}^2$, such that $k+l \leq 4$. Using a calibration measurement as explained in Sec. 4.1.4, we convert the computed $I/Q$ moments into corresponding signal moments $\langle (\hat{a}^\dagger)^k \hat{a}^l \rangle$. The data acquisition chain is shown in Fig. 4.5. Processed $I/Q$ moments are recorded within the first-in-first-out memory, which transfers the data to a host PC. Both the FPGA image programming and data processing measurement code on the host PC are implemented in the LABVIEW 2019 programming language. The host PC establishes a transmission control protocol (TCP) channel with the FPGA, where data can be communicated in a synchronized manner. Considering the previously mentioned aspects, each measurement cycle is structured as follows. First, we record 1650 digitized and filtered $I/Q$ points, using 96.4% of the available 16.02 Mbit block memory (BRAM) of the FPGA, at the digitization frequency of $\omega_\mathrm{s} = 125\,\mathrm{MHz}$. Each filtered $I/Q$ point corresponds to $10 \times 1/(125 \times 10^6) = 80\,\mathrm{ns}$ of signal trace, implying a total time trace of $1650 \times 80\,\mathrm{ns} = 132\,\mu\mathrm{s}$. Each time trace is repeated $M$ times for each measurement, with the final recorded $I/Q$ moments averaged over these $M$ traces. Note that the described implementation implies that filtered $I/Q$ points are completely statistically independent from each other in time windows separated by 90 input digitized points $x_n$, resulting in a time separation of $90 \times 80\,\mathrm{ns} = 7.2\,\mu\mathrm{s}$. This aspect of our data processing is relevant for the later data analysis of CV-QKD measurements, where processed data points, corresponding to filtered $I/Q$ points, are required to be independent samplings.

### 4.1.4 State tomography

In this section, we describe a state reconstruction method for data analysis. We rely on the reference state reconstruction [52, 207]. Its main idea is to use a known state as a reference to calibrate the photon statistics of the amplification chain. Assuming that these properties remain constant during measurements, this calibration allows the extraction of statistical moments of cryogenic quantum signals from measured noisy data at room temperature. In the microwave cryogenic experiments, the HEMT noise dominates the noise figure of the amplification chain. According to the Friis formula [174], the added noise photon number from the amplification chain, referred to its input, can be expressed as

$$\bar{n}_\mathrm{tot} = \sum_{i=1}^{N} \frac{\bar{n}_i}{\prod_{j=1}^{i-1} G_j} = \bar{n}_1 + \frac{\bar{n}_2}{G_1} + \frac{\bar{n}_3}{G_1\,G_2} + \cdots, \tag{4.3}$$

where each subsequent amplifier gain is denoted as $G_i$ with its associated noise $\bar{n}_i$. If the HEMT is the first amplifier in the chain, we see from Eq. (4.3) that the following noise contributions can be neglected, owing to the large HEMT gain values of around 40 dB. For instance, typical commercial room-temperature amplifiers add a mean noise photon number on the order of $\bar{n} \lesssim 10$ for microwave signals with a frequency between 4 to 8 GHz. As such, we can consider that our amplification is limited by the HEMT noise.

The principle of the reference state tomography method is shown in Fig. 4.6. A general signal envelope $\hat{S}$ mode at the output of our amplification chain, and normalized by the amplification chain gain $G$, can be written using the amplification Gaussian channel from Eq. (2.99)

$$\hat{S} = \frac{1}{\sqrt{G}}(\sqrt{G}\hat{a} + \sqrt{G-1}\hat{h}_1^\dagger) = \hat{a} + \hat{h}^\dagger, \tag{4.4}$$

where modes $\hat{h}_1$ and $\hat{h} = \sqrt{1-1/G}\,\hat{h}_1$ are noise (bosonic) modes. Note that with this convention, $\hat{h}$ is only a bosonic mode in the limit $G \gg 1$. Here, the mode $\hat{a}$ represents a quantum state

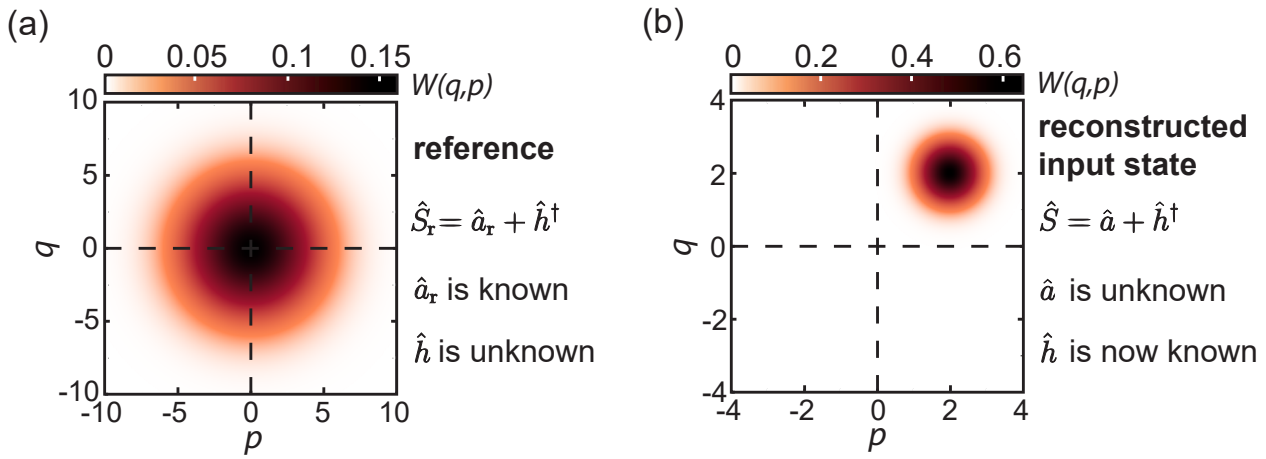


Figure 4.6: Principle of the reference state tomography. (a) A known reference state, $\hat{a}_\mathrm{r}$, a weak thermal state, is used to determine the properties of our amplification chain, characterized by a noise operator $\hat{h}$. (b) An unknown input state $\hat{a}$ is deduced from our measurement, assuming that the amplification chain properties remain similar to those during the measurement of the reference state. In our experiments, these two steps are typically measured back to back over a few dozen microseconds.

before amplification. From Eq. (4.4), we can express any signal envelope moments $\langle(\hat{S}^\dagger)^i\,(\hat{S})^j\rangle$, with integers $(i,j)$, such that $i+j \leq 4$, as a function of the signal moments $\langle(\hat{a}^\dagger)^i\,(\hat{a})^j\rangle$ and noise moments $\langle(\hat{h}^\dagger)^i\,(\hat{h})^j\rangle$. For instance, one can derive

$$\langle\hat{S}\rangle = \langle\hat{a}\rangle + \langle\hat{h}^\dagger\rangle\,, \quad \langle\hat{S}^\dagger\hat{S}\rangle = \langle\hat{a}^\dagger\hat{a}\rangle + \langle\hat{h}^\dagger\hat{h}\rangle + 1 + 2\mathrm{Re}(\langle\hat{a}\rangle\langle\hat{h}^\dagger\rangle), \tag{4.5}$$

where we use the fact that the modes $\hat{a}$ and $\hat{h}$ commute, as they are uncorrelated. Accounting for the fact that the noise mode, $\hat{h}$, is assumed to be a thermal state, equations for signal envelope moments can be further simplified. As shown in Eq. (4.5), equations of second-order signal envelope moments involve first-order signal and noise moments. In general, the equation of signal envelope moments of order $m$ uses signal and noise moments of order $l \leq m$. In the reference state reconstruction method, we first measure signal envelope moments $\langle(\hat{S}_\mathrm{r}^\dagger)^i\,(\hat{S}_\mathrm{r})^j\rangle$ based on Eq. (4.4) assuming a known input mode $\hat{a} = \hat{a}_\mathrm{r}$, serving as a reference. In our measurements, this reference state is a weak thermal state obtained by switching off all signal generator devices. The temperature of this thermal mode can be extrapolated to be the cryostat measured (photonic) temperature, which is about $T = 68\,\mathrm{mK}$ in the experiments discussed in this chapter and Chap. 5. Having knowledge of the photon number conversion factor (PNCF), $\kappa$, and reference signal moment values, we extract noise moment values $\langle(\hat{h}^\dagger)^i\,(\hat{h})^j\rangle$. Here, we additionally treat these noise moments as constant within a given reference state measurement. After measurements using the reference mode $\hat{a}_\mathrm{r}$, we repeat the same signal envelope moment measurements with an unknown, to-be-reconstructed signal mode $\hat{a}$. More precisely, we solve for unknown signal moments $\langle(\hat{a}^\dagger)^i\,(\hat{a})^j\rangle$ in signal envelope moment equations such as in Eq. (4.5). A full set of general solutions can be found in Ref. 208. In our experiments, signal envelope moments are extracted from measured quadrature moments $\langle I^k Q^l\rangle$, with $\{(k,l)|k+l \leq 4\}$ where $I/Q$ coincides with the in-phase and out-of-phase quadratures introduced in Sec. 2.2. These moments are related as

$$\hat{S} = \frac{\hat{I} + i\hat{Q}}{\sqrt{\kappa}}\,, \;\; \langle\hat{S}^k(\hat{S}^\dagger)^l\rangle = \frac{\left\langle(\hat{I}+i\hat{Q})^k(\hat{I}-i\hat{Q})^l\right\rangle}{(\sqrt{\kappa})^{k+l}}, \tag{4.6}$$

where $\kappa$ is the PNCF, which is introduced in Sec. 4.3.1. Based on this technique, any moments of an unknown signal mode $\hat{a}$ can be computed. However, this method is not suited for the

reconstruction of an arbitrary quantum state. This originates from the fact that the full tomography of an arbitrary quantum state requires knowledge of order signal moments up to infinity [209], whereas experiments are limited to measurements of a finite number of moments [24, 210]. However, this limitation can be circumvented for the case of Gaussian states as mentioned in Sec. 2.2.2, where the information about first and second moments is necessary and sufficient to fully reconstruct any unknown Gaussian state. Additionally, to verify the Gaussianity of our states, we compute moments up to the fourth order in our experiments. As explained in Sec. 4.3.2, moments up to the fourth order are enough to estimate when reconstructed quantum states are no longer Gaussian. For a given Gaussian state, we write its Wigner function, giving all information about the Gaussian state, using Eq. (2.75) as a function of first and second order signal moments

$$W(q,p) = \frac{1}{\pi M} \exp\left\{ -\frac{1}{M^2}\left( (\nu + 1/2)\left|\xi - \langle\hat{a}\rangle^2\right| - 2\,\mathrm{Re}[(\mu^*/2)(\xi - \langle\hat{a}\rangle)^2] \right) \right\}, \tag{4.7}$$

where $\xi = q + ip$, $\mu = \langle\hat{a}^2\rangle - \langle\hat{a}\rangle^2$, $\nu = \langle\hat{a}^\dagger\hat{a}\rangle - \left|\langle\hat{a}\rangle\right|^2$, and $M^2 = (\nu + 1/2)^2 - |\mu|^2$.

We note that there exist other tomography techniques for microwave quantum states. An alternative is the dual-path reconstruction method [49], which uses two signal paths and their corresponding correlations to extract signal moments. It presents the advantage of not relying on a reference state. However, its implementation necessitates an additional 50 : 50 hybrid ring and two output channels (instead of one with the reference state method). Alternatively, one can employ a qubit-based Wigner tomography of an arbitrary quantum state. This method has been extensively used in many experiments, representing an efficient and robust method for state reconstruction [211, 212, 213]. The main drawback of this method is its complexity and requirement to have an efficiently coupled qubit system, which is not always possible. Lastly, we comment that there is the possibility to perform state tomography of quantum states based on histogram measurements using a parametric amplifier such as a JPA. This method is discussed in more detail in Chap.5.

## 4.2 JPA characterization

In this section, we present information on the JPA sample packaging, flux tunability, gain characteristics, and characteristic measurements. Section 4.2.1 details the JPA sample preparation and shows a typical JPA chip in our experiments. In Sec. 4.2.2, we focus on characteristic measurements to determine the frequency range of measured devices. Additionally, we measure amplification gains of JPAs in the cases of both nondegenerate and degenerate regime of parametric amplification.

### 4.2.1 Sample preparation

In our experiments, we use JPA chips fabricated in the Institute of Physical and Chemical Research (RIKEN) in Japan. Each JPA chip consists of a $\lambda/4$ microwave resonator in the coplanar waveguide (CPW) geometry. The resonator is short-circuited to ground via a dc-SQUID. The dc-SQUID is made using a shadow evaporation technique to produce Aluminium superconducting electrodes with a thickness of 50 nm. The resonator and pump CPW lines are fabricated using a sputtering technique and consist of a 50 nm thick layer of niobium [50, 54]. In Fig. 4.7, we show a microscope image of the JPA chip. Each chip is packaged into a customized sample box, shown in Fig. 4.8 (a). These boxes are made from an oxygen-free high thermal conductivity (OFHC) copper and are gold-plated. The chip is glued in the center of the box using a GE varnish glue. The signal and pump JPA inputs are interfaced using K-connectors

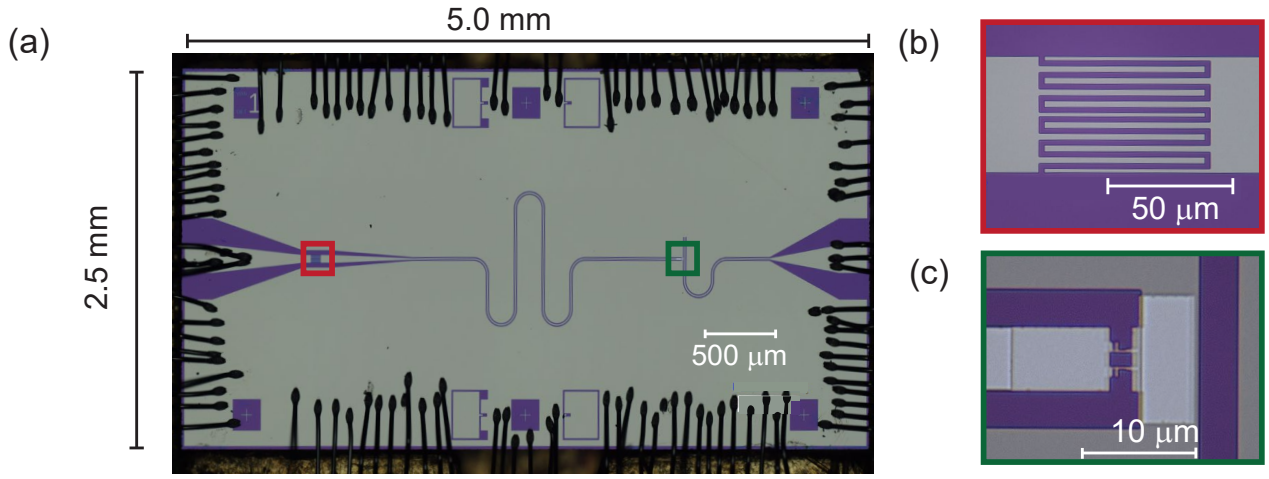


Figure 4.7: Optical micrograph of a JPA sample. An overview of the chip is given in panel (a) with aluminium (black) bonding wires. The signal port corresponds to the left CPW, while the pump port designates the right CPW. The coupling capacitance is highlighted in the red box and is shown in panel (b). The dc-SQUID that provides flux tunability to the JPA resonance frequency is indicated by the green box. A close-up of the dc-SQUID area is shown in panel (c).

(K102F-R connectors from Anritsu), which are soldered to glass beads (K-100 glass beads from Anritsu) located inside the copper housing. The connection between the glass beads and the JPA chip is mediated through a custom printed circuit board (PCB) with a 50 Ω matched CPW. Aluminium bonds are used to connect ground planes and CPW lines of the JPA and PCBs. To ensure better grounding of the PCBs, we add small quantities of silver glue between the sample holder walls and the PCB edges. The resulting boxes typically have ±3 Ω characteristic impedance mismatches from the desired target of 50 Ω impedance. In order to avoid parasitic magnetic crosstalks between different JPAs and protect those from stray magnetic fields, each sample box is installed inside a custom-made aluminium box, which is superconducting below the critical temperature of $T = 1.2\,\mathrm{K}$. On top of each sample box, we mount a custom-made superconducting coil. The coil holder is made of gold-plated OFHC copper where a superconducting NbTi-wire is wound around, resulting in a magnetic field typically on the order of a few $\mu$T. We fix the superconducting wire to the copper matrix using GE varnish glue, which ensures reliable usage of the coils over many cryogenic cool-downs. A final assembly of the sample box with the mounted coil is shown in Fig. 4.8 (b). Here, proper thermalization of all components of the sample holder is important at millikelvin temperatures. To this end, we add two thermally annealed silver ribbons, one positioned between the JPA box and the coil and another between the JPA sample box and the aluminium box. The pump sample holder output is connected to a flexible microwave cable (Minibend cables from Huber+Suhner) since the JPA operation requires high pump powers, where extra microwave losses are not critical.

On the other hand, propagating squeezed states are very sensitive to even to small microwave losses. To this end, we use a low-loss NbTi superconducting cable [204] to guide signals in and out of the JPA sample holders. As our JPAs are measured in reflection, we use circulators (CTH1184-KS18 from Quinstar) to separate incoming from outcoming signals. These circulators generate stray magnetic fields and must be spatially separated from the JPAs to avoid trapping magnetic flux before the aluminium magnetic shieldings become superconducting. Additionally, magnetic shields are provided with the circulators which greatly reduce the magnetic field seen by other surrounding components. In order to minimize the pump crosstalk between different JPAs, we use broadband circulators, with effective bandwidth of $4 - 12\,\mathrm{GHz}$. Additionally, we mount the circulators such that their main magnetic field component aligns

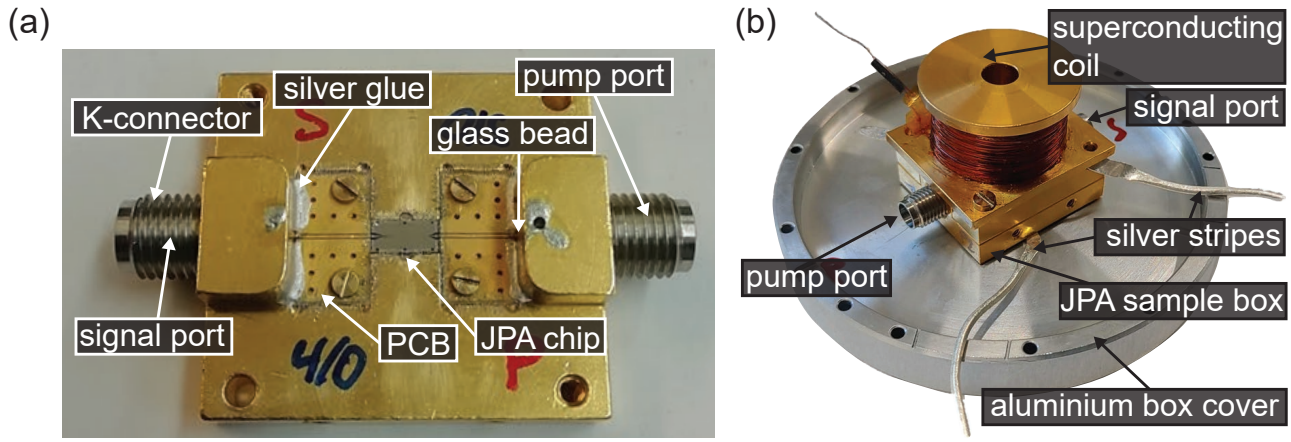


Figure 4.8: JPA sample box. (a) Photograph of the JPA sample box with a JPA chip at the center. The signal and pump ports are connected via a K-connector. The latter leads to a glass bead soldered to a PCB. Aluminium bonds are used to connect both PCBs and the chip. (b) Photograph of an assembled JPA sample box with a superconducting coil mounted on top of it. Silver stripes are used to ensure good thermalization of the sample box and the coil. The box is fixed with brass screws to the aluminium shielding box with an additional silver stripe placed in-between them.

in parallel to dc-SQUID loops of JPAs.

### 4.2.2 JPA characterization measurements

**JPA flux response.** As a first step, we measure the frequency response of our JPAs as a function of applied magnetic flux through the dc-SQUID loop. To this end, we use a vector network analyzer (VNA) to obtain the frequency response of one of our JPAs, during which we set the magnetic flux of the other JPA to zero. The scheme of the measurement is shown in Fig. 4.9 (a). We sweep the magnetic field by varying the coil current generated using a dc current source (6241A source from ADCMT). In our measurements, we commonly use currents in the range of $\pm 300\,\mu\text{A}$. In Fig. 4.9 (b), we show a measurement of the phase response of the scattering parameter $S_{21}$ as a function of the applied magnetic flux (proportional to the current through the coil). This parameter is defined as the ratio between input and output voltages at the ports of the VNA. The magnitude and phase response of the JPA reflection can be fitted using Eq. (2.43) for each measured flux point. The JPAs are designed to be in the overcoupled regime, with the target external quality factor of $Q_{\text{ext}} = 200$. As a result, the JPA has a weak magnitude response and strong phase one. The latter is shown in Fig. 4.9 (b). An accurate fitting of internal quality factors from the JPA response according to Sec. 2.1.3 is difficult due to a potential Fano interference, leading to large uncertainty for overcoupled resonators [214]. We note that for the used JPA circuit design, the presence of a separate pump port is known to be a limiting element for the internal quality factor, as input signals can leak via the inductively coupled pump line. Additional filtering of the pump line can partially prevent such a leakage [215]. Lastly, we observe that our model prediction in Eq. (2.27) is in agreement with the measured JPA resonance frequency shown in Fig. 4.9.

**Nondegenerate gain.** The amplification properties of the JPA are of crucial importance in this work. We measure nondegenerate gain profiles of our JPAs using the VNA, using the identical experimental setup as for the flux-dependence JPA response measurements. The VNA input and output ports are connected to the cryogenic system and used to measure microwave reflection from the JPA input. Using the VNA, we perform a frequency sweep

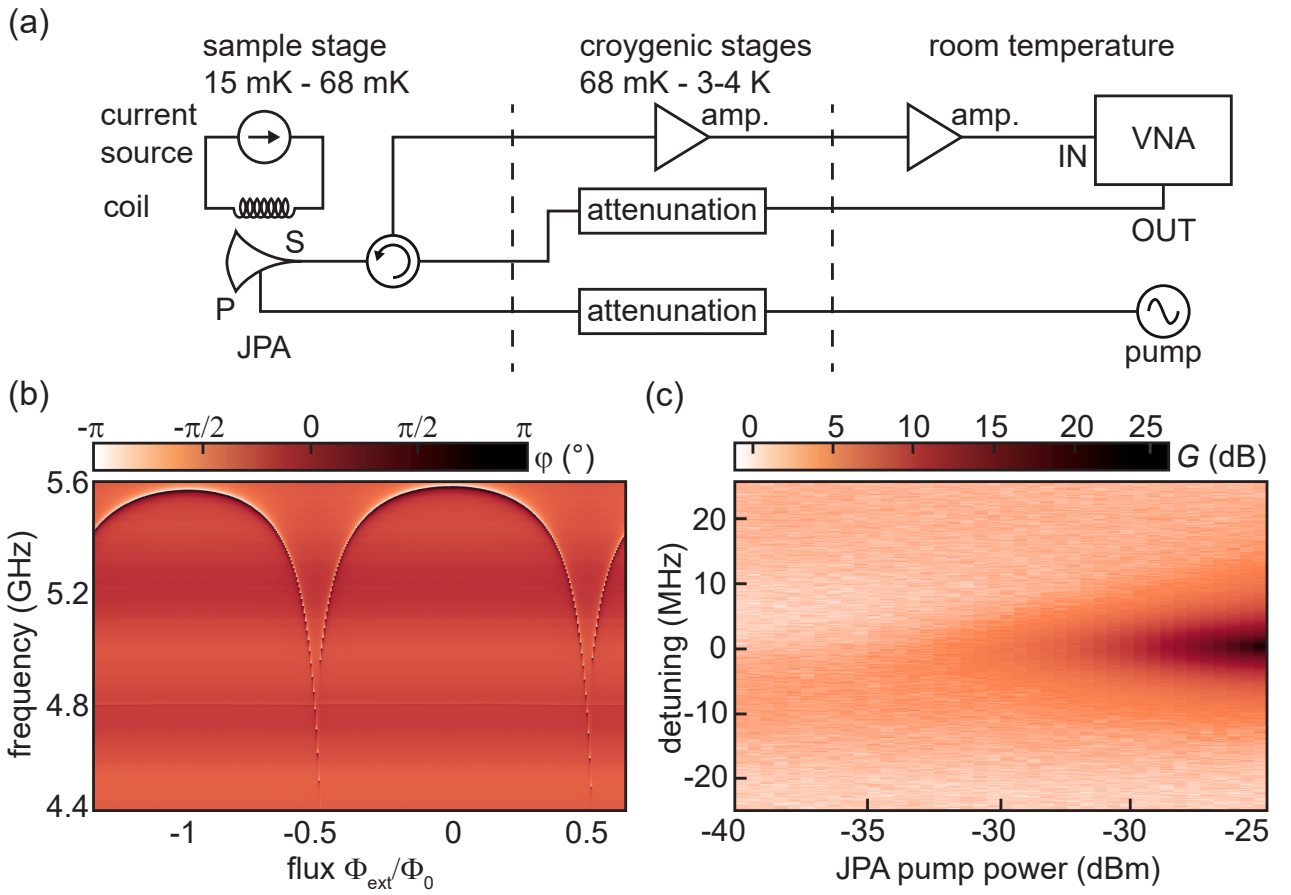


Figure 4.9: JPA characterization measurements. (a) General scheme for JPA characterization with the VNA. A circulator separates incoming from outgoing signals at the JPA. A current source controls the magnetic flux threading the JPA. (b) Phase $\varphi$ of the complex scattering parameter $S_{21}$ plotted as a function of the applied magnetic flux and probe frequency. We observe a periodic modulation of the JPA resonance frequency in agreement with the model in Sec. 2.1.4. The magnetic flux is generated using a home-made superconducting coil mounted on top of the JPA. (c) Exemplary measurement of the nondegenerate gain $G$ as a function of the JPA pumping power. Lorentzian gain profiles, $G(\omega)$ (vertical cuts), are observed in agreement with the theory model presented in Sec. 2.1.4.

around a selected JPA resonance frequency. This frequency choice depends on the frequency-dependent properties of all other microwave devices involved in the CV-QKD implementation, where a frequency compatibility must be ensured. For this reason, the JPAs are designed with nominally identical target frequencies around 5.7 GHz. Additionally, we choose to work close to the JPA maximal resonance frequency. This approach is primarily motivated by the sensitivity of the JPA to magnetic flux, which rapidly increases when detuning the JPA closer to $\Phi_0/2$ and results in extra noise. At the same time, frequencies in the close vicinity of the zero magnetic flux JPA resonance frequency present low sensitivity to applied magnetic flux. As shown in Eq. (2.35), parametric amplification effects are proportional to the derivative, $\partial\omega_\mathrm{J}/\partial\Phi_\mathrm{ext}$, of the JPA resonance frequency as a function of the applied external magnetic flux. For resonance frequencies close to the zero flux resonance frequency, this derivative is comparatively small. As a result, higher pump powers are required to obtain the same amplification gain as compared to resonance frequencies with a corresponding larger sensitivity to magnetic flux. For higher pump powers, we also introduce larger pump-induced noise, which degrades the JPA performance. Additionally, a higher pump power implies a larger heat load on the MC of the cryostat, leading potentially to elevated equilibrium temperatures in our experiments. For these reasons, a good compromise between these two extremes must be preserved, which typically corresponds

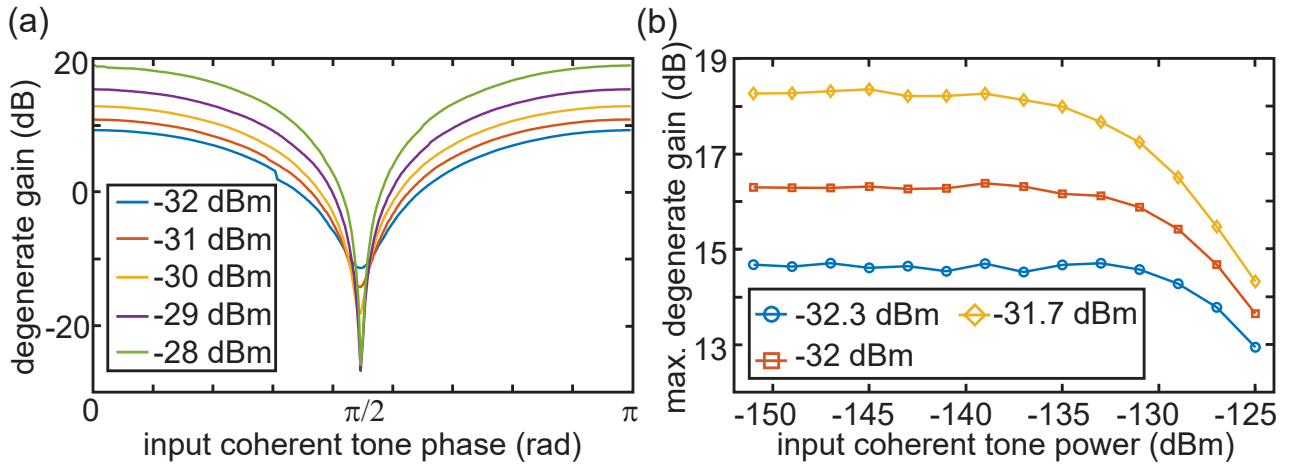


Figure 4.10: Degenerate gain measurements. (a) Degenerate gain measurements of the JPA 2 pumped at the frequency $\omega_\mathrm{p} = 2\omega_\mathrm{J}$. The gain is determined as the ratio between an input coherent tone and the corresponding amplified coherent tone power. The gain is measured as a function of the input coherent tone phase and for different pump powers. (b) Exemplary 1−dB compression point measurements. Degenerate gains are shown as a function of the input coherent tone power for different pump powers. The 1−dB compression is determined as the input power for which the measured gain is 1 dB below its maximal, low-power value.

to the JPA working frequencies detuned on the order of $\sim 100\,\mathrm{MHz}$ from the JPA zero flux resonance frequency. In Fig. 4.9 (c), we show an exemplary nondegenerate measurement of the measurement JPA, labelled JPA 2 in Fig. 4.2. In this measurement, we choose the resonance frequency to be $\omega_\mathrm{J}/2\pi = 5.52\,\mathrm{GHz}$ and apply the pump tone at the frequency $\omega_\mathrm{p} = 2\omega_\mathrm{J}$. Using the VNA, we send a probe signal at a frequency $\omega_\mathrm{s} = \omega_\mathrm{p}/2 + \delta\omega$, with $\delta\omega$ a frequency offset, and measure a corresponding scattering parameter magnitude, $|S_{21}|^2_\mathrm{on}$. Switching off the pump tone, we additionally repeat the measurement of the scattering parameter magnitude and use the corresponding measured value, $|S_{21}|^2_\mathrm{off}$, as a reference. The nondegenerate amplification gain at a given signal frequency is defined as $G = |S_{21}|^2_\mathrm{on}\,/|S_{21}|^2_\mathrm{off}$. We obtain a large amplification gain with a maximal value of 25 dB, which is a good gain value for our experiments. The observed Lorentzian gain profile is also in good agreement with the formalism presented in Sec. 2.1.4.

**Degenerate gain.** Another crucial property of the JPA is its degenerate gain. As explained in Sec. 2.1.4, this gain regime is achieved by pumping the JPA at twice its resonance frequency and measuring the gain at the JPA resonance frequency. As amplification is phase-sensitive in this regime, we send a coherent tone with a well-defined phase to the input of the measured JPA and vary the phase of the coherent tone. We perform two measurements where the pump tone is first switched off, providing a reference power, computed as $P_\mathrm{ref} = (\langle I\rangle^2_\mathrm{off} + \langle Q\rangle^2_\mathrm{off})/Z_0$, with $Z_0$ being the characteristic $50\,\Omega$ impedance in our circuits. A second measurement is performed with the pump turned on, resulting in degenerate amplification. Here, we compute the amplified signal power by using the second-order moments $P_\mathrm{amp} = (\langle I\rangle^2_\mathrm{on} + \langle Q\rangle^2_\mathrm{on})/Z_0$. According to Sec. 2.1.4, we expect the gain value to vary as a function of the coherent tone phase, $\theta$.

In Fig. 4.10 (a), we display exemplary measurements of the degenerate gain for the measurement JPA 2 at the frequency of $\omega_\mathrm{J}/2\pi = 5.48\,\mathrm{GHz}$. We observe a change in the gain from a maximal value for a phase at $\theta = 0$ and $\theta = \pi$, with a minimal value for a phase at $\theta = \pi/2$. We note that the maximal and minimal gain values are separated by the phase difference of $\Delta\theta = \pi/2$, as predicted by our theory in Sec. 2.1.4. For the phase of $\theta = \pi/2$, we note that gain

values are negative, meaning that the input signal is attenuated. This aspect is closely related to the generation of squeezed states, where the precise nomenclature depends on whether the output variance of the state for the deamplified quadrature is below the vacuum limit or not. In the case where this variance is above that of vacuum fluctuations, one speaks about *squashed* states. We measure degenerate gain values up to 20 dB, as shown in Fig. 4.10 (b). We note that larger degenerate gain values can still be obtained with our devices by further increasing the pump power. Large degenerate gain values are particularly important to enable efficient single-shot quadrature measurements as detailed in Chap. 5. Using the same measurement approach, we can investigate the 1-dB compression point of the JPA. This quantity is a common figure of merit for linear amplifiers, where the output power of an amplifier saturates for large enough input signal powers. In our JPAs, compression effects set on due to effects of pump depletion and higher-order nonlinearities [73]. The 1-dB compression point is defined as the characteristic input signal power for which the amplifier gain is 1 dB below its maximal value. Therefore, we can obtain this quantity by varying the power of the coherent tone at fixed pump power values. For each coherent tone power, we extract a corresponding maximal degenerate gain by sweeping the phase of the coherent tone from 0 to $\pi$. Our results for the JPA 2 are shown in Fig. 4.10 (b). We observe that for gain values above 20 dB, the 1-dB compression point strongly decreases, limiting the applicability of JPAs in actual protocols. Based on the noise properties of our JPAs (see Sec. 4.3.3) and compression effects, a good gain optimum, typically, lies around 20 dB for our type of JPA devices.

## 4.3 Calibration measurements

In this section, we present calibration measurements that are required for the experimental implementation and subsequent data analysis of our CV-QKD protocol. In Sec. 4.3.1, we discuss our photon number calibration based on the 2D Planck spectroscopy [197], serving as a novel loss calibration method. Section 4.3.2 is dedicated to the verification of the Gaussianity of measured quantum states. There, we introduce a novel approach to determine non-Gaussian features in measured microwave signals based on the analysis of signal moments up to the fourth order. Quantum efficiency, a quantity defining the noise properties of all JPAs of paramount importance for the CV-QKD protocol, is discussed in Sec. 4.3.3. In Sec. 4.3.4, we focus on squeezed states measurements and their characteristic quantities, such as purity, cumulants, and squeezing level. In this same section, we discuss about calibration of displacement operations, the latter representing an essential resource for practical realizations of the CV-QKD protocol. We conclude by discussing the calibration of induced Gaussian noise in Sec. 4.3.5, which is the key for emulating CV-QKD performance under realistic conditions, simulating the presence of a bright thermal background.

### 4.3.1 Two-dimensional Planck spectroscopy

As explained in Sec. 4.1.3, our heterodyne detection setup allows for the computation of quadrature moments $\langle I^k Q^l \rangle$. These moments are converted into normally ordered signal moments $\langle (\hat{a}^\dagger)^i \hat{a}^j \rangle$ using a PNCF, $\kappa$. The latter is obtained using the two-dimensional (2D) Planck spectroscopy [197], which is an extension of the conventional Planck spectroscopy, commonly used in previous experiments [24, 27, 216, 217]. To distinguish these two methods, we refer to the conventional Planck spectroscopy as one-dimensional Planck spectroscopy. During this measurement, both JPAs are far detuned from a chosen frequency mode to prevent any interference effects. To implement a one-dimensional Planck spectroscopy, we use a heatable 30 dB attenuator at the input of our cryogenic setup, as shown in Fig. 4.2. This attenuator serves as a self-calibrated thermal photon reference source, which can be viewed as a quasi-black body

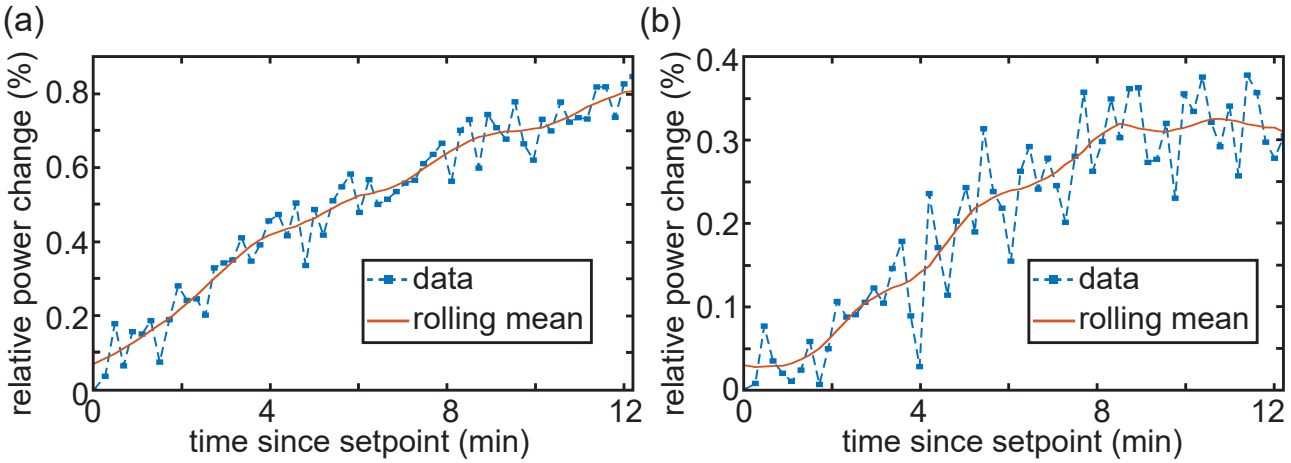


Figure 4.11: Temperature stability measurements. (a) Relative change in measured power after increasing the temperature of the heatable input attenuator from the base temperature of 68 mK to the target temperature of 500 mK. The reference time, $t = 0$, on the $x$-axis is defined as the moment the attenuator reaches the target temperature on the AVS temperature bridge, with the measured power at $t = 0$ treated as the reference for the computation of relative power change. (b) Measured relative power variations after the heatable input attenuator, first heated up to the target temperature of 400 mK, is stabilized to the target temperature of 300 mK. These measurements are performed immediately following the ones in panel (a). For both panels, we show a smoothed rolling mean over 7 consecutive points as a guide to the eye.

radiator, controllably stabilized at a desired temperature, $T_{\mathrm{att}}$. This is achieved using a small heater, made from a thin silver stripe, that is clamped to the heatable attenuator. This attenuator is weakly thermally anchored to the MC stage of our dilution refrigerator using a long, thin silver stripe.

The idea of the 2D Planck spectroscopy is to consider that the sample stage is thermally coupled to the MC stage thermal bath via the total losses present in the experimental setup. As a result, we can estimate these losses by varying the MC temperature $T_{\mathrm{mc}}$, using a proportional-integral-derivative (PID) controller, provided by Oxford Instruments. For such measurements, it is important to account for a thermalization time after the MC stage has been heated. We typically wait a time of $t = 30$ mins to ensure that a thermal equilibrium is reached. For each MC temperature, $T_{\mathrm{mc}}$, we sweep the temperature of our heatable attenuator in a range varying from the base temperature, slightly above $T_{\mathrm{mc}}$, to the final temperature, $T_{\mathrm{att}} = 440$ mK. Additionally, to estimate the time needed to wait at each attenuator temperature for the setup to reach a thermal equilibrium, we perform another set of measurements. For these, we start by heating the heatable attenuator to $T_{\mathrm{att}} = 500$ mK. This temperature is subsequently lowered by steps of 100 mK, while we record the total emitted power from the hot radiator at a selected frequency as $P = \langle I^2 + Q^2 \rangle / Z_0$. The power is recorded once the target temperature is reached. The measurement of the temperature of the heatable attenuator is performed using a temperature bridge (AVS-48 from Picowatt), which offers a PID controller to stabilize the temperature during Planck spectroscopy measurements. Ideally, one would expect no power fluctuations. However, due to the thermal inertia of the different components in our setup, a waiting time is required before reaching a final thermal equilibrium. Two exemplary power variations are shown in Fig. 4.11, where we observe slow power changes before converging to a steady regime, indicating that the thermal equilibrium has been reached. Note that even though the displayed relative power changes appear small, there are comparable to power variations measured during PNCF measurements. From these measurements, we extrapolate that the additional average waiting time of $t \simeq 8$ mins guarantees power fluctuations of less

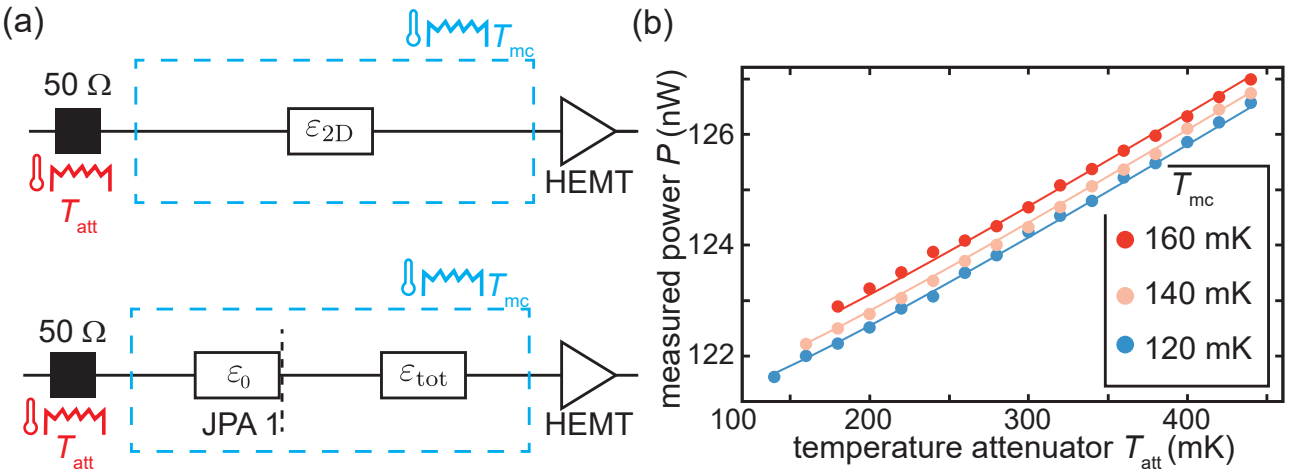


Figure 4.12: Photon number calibration. (a) Scheme of repartition of losses. The losses, $\varepsilon_{2D}$, between the attenuator (black square box) and the HEMT can be decomposed into two components before and after JPA1, denoted $\varepsilon_0$ and $\varepsilon_{tot}$, respectively. (b) Experimental 2D Planck spectroscopy as a function of the attenuator temperature $T_{att}$. Symbols depict experimental data for different mixing chamber temperature $T_{mc}$ and solid lines are corresponding fits according to Eq. (4.8).

than 0.1% for a given attenuator temperature. For all subsequent Planck spectroscopies, we use this waiting time in the measurements.

The 2D Planck spectroscopy allows for a precise extraction of the cryogenic losses, $\varepsilon_{2D}$, between the heatable attenuator and the input of the HEMT. According to Ref. 197 and using the transmissivity $\tau_{2D} = -10\log_{10}(\varepsilon_{2D})$, the measured power $P$ at the end of our detection chain reads

$$P = \frac{\kappa}{Z_0}\left[\frac{\tau_{2D}}{2}\coth\left(\frac{\hbar\omega}{2k_B T_{att}}\right) + \frac{1-\tau_{2D}}{2}\coth\left(\frac{\hbar\omega}{2k_B T_{mc}}\right) + A_{amp}\right], \tag{4.8}$$

where $\kappa$ (PNCF) relates the powers measured at the room temperature detector to corresponding photon numbers at the input of the HEMT. Here, $A_{amp}$ is the total noise (in units of photons) added by our amplification chain, with a HEMT being the first amplifier in the chain. Additionally, $Z_0$ is the characteristic 50 Ω impedance of our microwave waveguides. As shown in Fig. 4.12, we fit all individual Planck curves using Eq. (4.8) with $\tau_{2D}$, $\kappa$, and $A_{amp}$ as fitting parameters. We extract the parameters $\varepsilon_{2D} = 10^{-\tau_{2D}/10} = 3.06\,\text{dB}$, $\kappa = 4.7\times10^{-7}\,\text{V}^2/\text{photon}$, and $A_{amp} = 12.11$. We emphasize that in these measurements, the reference point is at the input of the HEMT, meaning that photon numbers obtained from $\kappa$ are referred to the input of the HEMT. To shift this reconstruction point to a different position, an estimation of the losses between the input of the HEMT and the reconstruction point of interest is required. This estimation can be made based on the datasheet values of different setup components and corresponding time domain reflectometry (TDR) measurements. However, both these measurements are performed in different conditions, namely at room temperatures and ambient pressures, as compared to cryogenic experiments. This uncertainty represents the main source of error for estimation of losses and influences final values of reconstructed signal moments. In our analysis, we need to consider losses in our setup from the first JPA to the input of the HEMT, $\varepsilon_{tot}$. As illustrated in Fig. 4.12 (a), we carefully estimate the losses between the heatable attenuator and the first JPA 1, $\varepsilon_0$, from which we compute $\varepsilon_{tot} = \varepsilon_{2D} - \varepsilon_0$, resulting in $\varepsilon_{tot} = 0.87\,\text{dB}$.

### 4.3.2 Gaussianity test

Our experiments rely on the assumption that reconstructed quantum states are Gaussian. Since we restrain our operations to Gaussian channels (see Sec. 2.2.2), we expect all states involved in our measurements to be Gaussian. We verify the Gaussianity of our states by computing cumulants from signal moments as [218, 219]

$$\kappa_{m,n} = \frac{\partial^m}{\partial x^m}\frac{\partial^n}{\partial y^n} \ln\left(\sum_{k=0}^{m}\sum_{l=0}^{n} \frac{\left\langle (\hat{a}^\dagger)^k \hat{a}^l \right\rangle}{k!l!} x^k y^l\right)\Bigg|_{x=y=0}, \tag{4.9}$$

giving, for instance, $\kappa_{11} = \left\langle a^\dagger a \right\rangle - \left\langle a^\dagger \right\rangle \langle a \rangle$. In theory, the cumulants of a Gaussian state are strictly zero for any order $m + n > 2$. However, in real experiments, this is not the case, as due to imperfections the experimental higher-order cumulants always have a residual nonzero value. A challenge here is to determine a threshold value for which cumulants with an order higher than two are considered significant or not. One possibility is to normalize the cumulants by the photon number value $\left\langle \hat{a}^\dagger a \right\rangle^{(m+n)/2}$. This mathematical operation is not ideal, as it does not provide a clear distinction between the Gaussian and non-Gaussian regimes. However, it allows to qualitatively estimate for which system parameters measured quantum states deviate from a Gaussian statistic. Alternatively, one can compare the values of the cumulants of lower orders (less than or equal to two) with those of higher orders (more than two). Assuming a smooth monotonic transition between the two regimes, a simple criterion to distinguish the Gaussian from non-Gaussian regime is to use experimental parameters for which the corresponding lower order cumulants are larger or comparable to higher order ones. In this context we note that we are limited by the FPGA memory in the calculation of cumulants up to the fourth order. Another method for Gaussianity detection, which is based on characteristic functions, is discussed in Sec. 4.3.6.

**Physicality checks.** Depending on the particular measurements, some reconstructed states can appear as unphysical, meaning that they violate one or several laws of quantum mechanics. This effect may originate from multiple sources, such as measurement instabilities, erroneous data discretization. Most often, it is related to an insufficient number of averages, resulting in statistical errors that can produce unphysical estimators, particularly for states containing a low number of photons. For our Gaussian states, an efficient physicality check is to verify that the measured states fulfil the Heisenberg uncertainty. Based on Eq. (2.64), we classify a state as physical if its measured covariance matrix, $\mathbf{V}$, satisfies the condition

$$\det(\mathbf{V}) \geq \frac{1}{16^d}\,, \text{ with } d = \frac{\dim(\mathbf{V})}{2}. \tag{4.10}$$

States that do not fulfil this are treated as unphysical and are removed from the data analysis. For states with low photon numbers, close to or less than one, one can observe that deviations from the inequality in Eq. (4.10) are not uncommon. This behavior is related to the insufficient SNR values while measuring these states and can be circumvented by increasing the number of sample averages at the cost of additional measurement time. As a result, one could consider including states that weakly violate the Heisenberg inequality, as those individual violations may still provide useful information about the original states. However, in our experiments, we disregard all reconstructed states which violate Eq. (4.10) for safety.

### 4.3.3 Quantum efficiency

A crucial figure of merit in our experiments is the noise added by amplifiers. In particular, CV-QKD protocols can only tolerate a finite amount of detection noise before losing unconditional

security. More precisely, any amount of detection noise significantly degrades the performance of QKD protocols, and as such, it is necessary to minimize the overall noise of our detection chain. In the context of quadrature measurements, we focus on the measurement of the quadrature-dependent quantum efficiency, $\eta_{\mathrm{X}}$, of our amplification chain, as defined in Eq. (2.60). The latter is measured with all setup devices active, except for the noise source, which is turned off during this measurement, and with both JPAs tuned in resonance. We observe that measured quantum efficiencies are different depending on whether a single or both JPAs are tuned in resonance. This is attributed to potential cross-interactions between the JPAs [205]. To measure the quantum efficiency, we generate displaced squeezed states that are subsequently phase-sensitively amplified by the measurement JPA 2. In Fig. 4.13, we plot the measured quantum efficiency $\eta_{\mathrm{X}}$ as a function of the JPA 2 degenerate amplification gain, $G_{\mathrm{J}}$. In this experiment, we choose to amplify the $q$-quadrature and record the measured power, $P_{\mathrm{amp}}$, for the amplified quadrature from first order signal moment

$$P_{\mathrm{amp}} = \frac{\kappa}{Z_0}\langle\hat{q}\rangle^2, \tag{4.11}$$

where $\kappa$ is the measured PNCF according to Sec. 4.3.1. As a power reference, we use the measured power, $P_{\mathrm{ref}}$, obtained by performing the same measurement without sending a pump tone to JPA 2. This provides an *in situ* degenerate gain calibration

$$G_{\mathrm{J}} = \frac{P_{\mathrm{amp}}}{P_{\mathrm{ref}}}. \tag{4.12}$$

At the same time, we extract from this measurement a value for the added noise variance, $A_{\mathrm{H}}$, where this noise, originating primarily from our HEMT amplifier, is added to the amplified quadrature variance. This photon number is measured during specific measurement windows, where no devices are active (labelled with the index "off") of the reference state reconstruction method. The recorded base power during these measurement windows provides a direct computation of the average HEMT noise per quadrature as

$$A_{\mathrm{H}} = \frac{\langle I^2 + Q^2\rangle_{\mathrm{off}}}{2\kappa}. \tag{4.13}$$

Note that the moments $\langle I^2\rangle$ and $\langle Q^2\rangle$ are expressed in unit of voltage squared and $A_{\mathrm{H}}$ is a noise variance, expressed in unit of number of photons. From these measurements, we find the noise variance of $A_{\mathrm{H}} = 6.05$. Setting the reference point of our tomography method at the input of the HEMT, we reconstruct the variance of the amplified quadrature as

$$\begin{aligned} \sigma^2_{\mathrm{tot}} &= G_{\mathrm{J}}\left[\tau_{\mathrm{tot}}\sigma^2_{\mathrm{s}} + (1-\tau_{\mathrm{tot}})(1+2\bar{n}_{\mathrm{th}})/4 + N_{\mathrm{X}}\right], \\ N_{\mathrm{X}} &= \tau_4\frac{\bar{n}_{\mathrm{J}}}{2} + \frac{A_{\mathrm{H}}}{G_{\mathrm{J}}}, \end{aligned} \tag{4.14}$$

where $\tau_{\mathrm{tot}}$ is the total transmissivity between the heatable input attenuator and the input of the HEMT, as obtained in Sec. 4.3.1 from the 2D Planck spectroscopy and related as $\tau_{\mathrm{tot}} = -10\log_{10}(\varepsilon_{\mathrm{tot}})$. Similarly, $\tau_4$ is the transmissivity between the measurement JPA 2 and the input of the HEMT. The quantity $\sigma^2_{\mathrm{s}}$ is the squeezed variance of the displaced squeezed state and $\bar{n}_{\mathrm{J}}$ is the added noise by the measurement JPA 2, referred to its input. The noise variance defines the quadrature quantum efficiency

$$\eta_{\mathrm{X}} = \frac{1}{1+2N_{\mathrm{X}}}. \tag{4.15}$$

The JPA noise depends on the JPA degenerate gain according to a polynomial function dependence [82]. As a result, increasing the JPA 2 gain also adds noise to the amplified states.

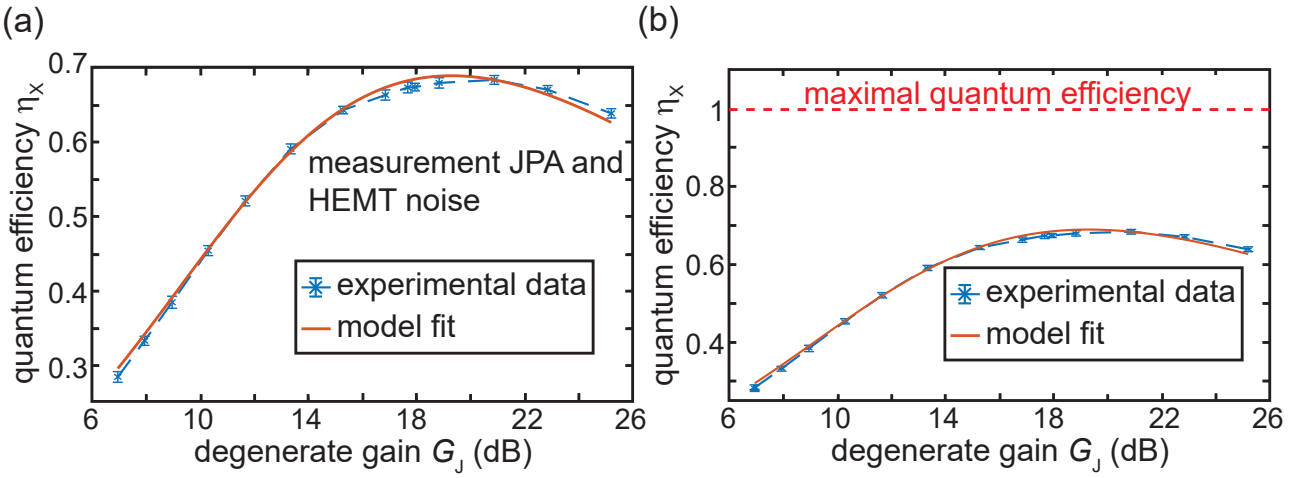


Figure 4.13: Experimental quantum efficiency accounting for the noise of the measurement JPA 2 and the HEMT noise. (a) The quantum efficiency is plotted as a function of the degenerate amplification gain $G_J$ of the measurement JPA 2. The measurement is performed for displaced squeezed states as input states to JPA 2. The blue symbols correspond to measured data, where the blue dashed line serves as a guide to the eye. The orange solid line is obtained from a model fit according to Eqs. 4.15 and 4.16. (b) Zoom-out version of panel (a), where the vertical scale is extended above the value $\eta_X = 1$, marked in red to illustrate its absolute limit.

At the same time, a larger degenerate gain results in a smaller contribution of the HEMT noise, as seen in Eq. (4.14). For this reason, there always exists a sweet spot in the degenerate gain, for which the total amplification noise is minimized. This optimal gain value depends on the JPA properties, the experimental setup, and the HEMT properties. We find that the JPA noise can be expressed as [82]

$$\bar{n}_J = \Xi_1 (G_J - 1)^{\Xi_2}, \tag{4.16}$$

with two phenomenological fitting parameters, $\Xi_1$ and $\Xi_2$. We fit the measured quadrature quantum efficiency according to Eqs. 4.14 and 4.16, showing corresponding results in Fig. 4.13. The fit is performed by minimizing the difference between the measured quantum efficiencies and their corresponding model predictions using a nonlinear solver under constraints of the Optimization Toolbox of MATLAB. The resulting fit values are $\Xi_1 = 0.049(2)$ and $\Xi_2 = 0.42(1)$.

### 4.3.4 Squeezing and displacement calibration

**Squeezing measurements.** As discussed in Sec. 2.1, we generate squeezed states using JPAs by driving them with the pump at a frequency twice the JPA resonance frequency. To characterize the microwave squeezed states, we follow a procedure similar to that for the degenerate amplification gain measurements. Here, we amplify weak thermal fluctuations originating from the heatable attenuator. We reconstruct the signal moments, $\langle (a^\dagger)^n a^m \rangle$, using the reference state reconstruction method. During these measurements, other devices, except for the JPA 1 pump, are not active. The pump tone is generated using a microwave source (SGS 100A from Rohde & Schwarz). We reconstruct a squeezing angle, $\gamma$, from the computed signal moments

$$\gamma = -\frac{\mathrm{Arg}(-\langle a^2 \rangle + \langle a \rangle^2)}{2}, \tag{4.17}$$

where we use the signal moment $\langle a^2 \rangle$ to account for a potential displacement of the measured squeezed state and arg is the argument of the complex function. We rotate the measured signal quadratures into a new frame with a rotation angle given by the squeezing angle. Signal quadratures are then rotated into a new frame with a rotation angle given by the previously

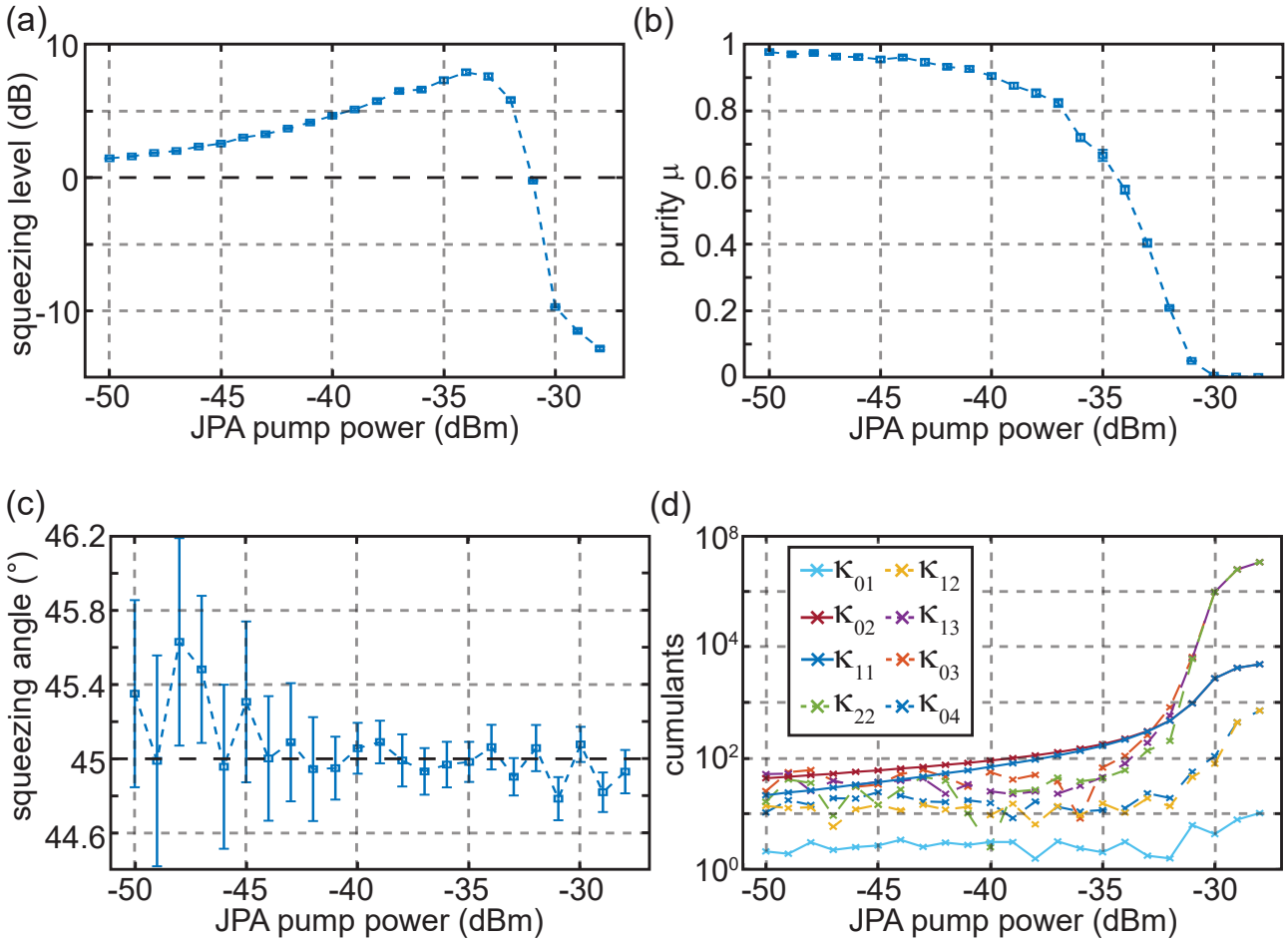


Figure 4.14: Characterization of squeezed states. (a) Measured squeezing level as a function of the JPA 1 pump power. The squeezing level is defined in Eq. (2.84), where positive values $S > 0$ indicate squeezing below vacuum. The dashed line at $S = 0$ serves as a reference. (b) Measured purity as a function of the JPA 1 pump power. (c) Experimental squeezing angle according to Eq. (4.17) for the target squeezing angle $\gamma_t = 45°$ as a function of the JPA 1 pump power. The dashed line represents the target value. (d) Experimental values of cumulants computed from signal moments as a function of the JPA 1 pump power. Cumulants are computed following Eq. (4.9). In all plots, error bars represent the standard deviation of the measured data.

computed squeezing angle. In this frame, we compute variances of the rotated $q$- and $p$-quadratures

$$\begin{aligned}\sigma_q^2 &= \frac{\langle \hat{a}^2 \rangle + \langle (\hat{a}^\dagger)^2 \rangle + 2\langle \hat{a}^\dagger \hat{a} \rangle + 1}{4} - \left( \frac{\langle \hat{a} \rangle^2 + \left\langle (\hat{a}^\dagger) \right\rangle^2 + 2\langle \hat{a}^\dagger \rangle \langle \hat{a} \rangle}{4} \right), \\ \sigma_p^2 &= \frac{-\langle \hat{a}^2 \rangle - \langle (\hat{a}^\dagger)^2 \rangle + 2\langle \hat{a}^\dagger \hat{a} \rangle + 1}{4} + \left( \frac{\langle \hat{a} \rangle^2 + \left\langle (\hat{a}^\dagger) \right\rangle^2 - 2\langle \hat{a}^\dagger \rangle \langle \hat{a} \rangle}{4} \right).\end{aligned} \tag{4.18}$$

From these equations, we obtain the squeezed quadrature variance as $\sigma_s^2 = \min(\sigma_q^2, \sigma_p^2)$. The anti-squeezed quadrature variance is similarly computed as $\sigma_{as}^2 = \max(\sigma_q^2, \sigma_p^2)$. The squeezing level $S$ and anti-squeezing level $AS$ are computed from these two variances according to Eq. (2.84). In Fig. 4.14, we display an exemplary squeezing measurement of JPA 1 at the frequency $\omega_J = 5.48\,\text{GHz}$. In addition to the squeezing level, we measure the purity of our

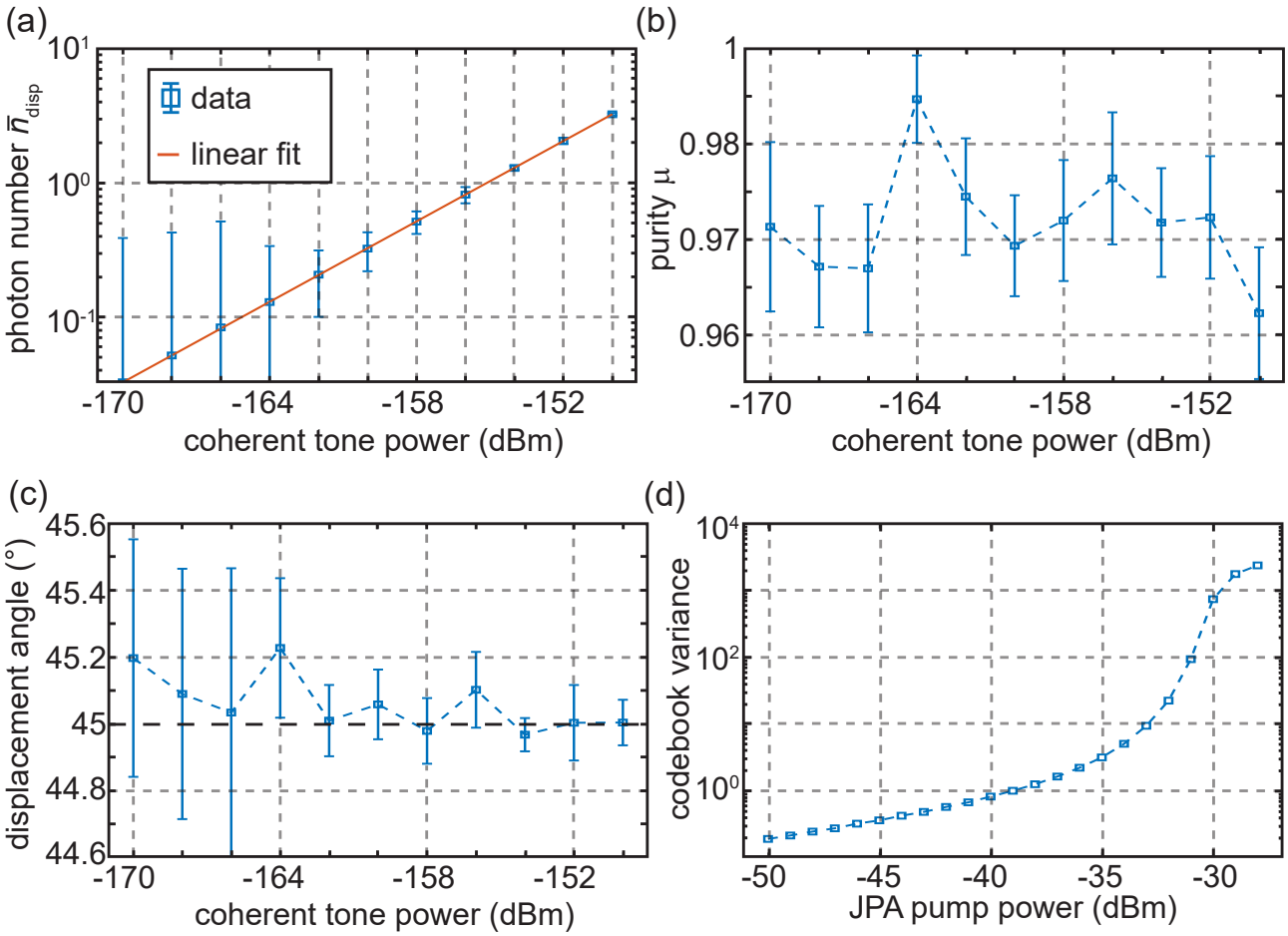


Figure 4.15: Characterization of coherent states. (a) Measurement of the photon number $\bar{n}_{\mathrm{disp}}$ generated by the coupling of a coherent tone to the first directional coupler with a weak thermal state at its input. The photon number is shown as a function of the coherent tone power and is fitted according to Eq. (4.21). (b) Corresponding purity of the displaced thermal states as a function of the coupled coherent tone power. (c) Reconstructed displacement angle $\theta$ following Eq. (4.20) for the target displacement angle $\theta_{\mathrm{t}} = 45°$. (d) Exemplary codebook variance $\sigma_{\mathrm{A}}^2 = \sigma_{\mathrm{as}}^2 - \sigma_{\mathrm{s}}^2$ following the squeezing measurement (as shown in Fig. 4.14) as a function of the JPA 1 pump power. We observe a decrease in the slope of the codebook variance for the pump powers above −30 dBm due to higher-order nonlinearities, resulting in non-Gaussian states. In all plots, error bars represent the standard deviation of the measured data.

squeezed state defined as $\mu = 1/4\sqrt{\det(\mathbf{V})}$, where $\mathbf{V}$ is the corresponding reconstructed covariance matrix. The purity is a direct measure of noise present in measured states. In Fig. 4.14 (a), we observe a monotonic increase in the squeezing level up until the pump power of −31 dBm. Above this point, the squeezing level decreases, as higher-order nonlinearity effects [73] set in, implying that the measured states become more and more non-Gaussian. The purity continuously decreases, indicating an increase in the noise of the squeezed states at the output of JPA 1.

Similarly to the measurement of JPA 2, this noise originates from fluctuations in the pump signal amplitude [82]. Based on the phase-locked loop, the squeezing angle is stabilized by adjusting the phase of the pump microwave source according to $2\delta\gamma = 2(\gamma - \gamma_{\mathrm{t}})$, for a target squeezing angle value $\gamma_{\mathrm{t}}$. In the CV-QKD experiments presented in Chap. 5, we keep a constant squeezing level $S = 3.6\,\mathrm{dB}$ corresponding to $\sigma_{\mathrm{s}}^2 = 0.11$. Simultaneously, the codebook variance, as defined in Sec. 3.3, is extracted according to $\sigma_{\mathrm{s}}^2 + \sigma_{\mathrm{A}'}^2 = \sigma_{\mathrm{as}}^2$.

| statistic \ values | slope $m$ | offset $p$ |
|---|---|---|
| linear fit value (photon/W) | $3.07 \cdot 10^{-11}$ | $2.3 \cdot 10^{-15}$ |
| error linear fit (photon/W) | $2.65 \cdot 10^{-14}$ | $< 10^{-15}$ |

Table 4.1: Summary table of the linear fit values, for induced displacements that are used in the CV-QKD protocol implementation. The linear fit values are shown with their associated error according to Eq. (4.21).

**Displacement measurement.** Displacement of input states is performed using a cryogenic directional coupler acting as a highly asymmetric beam splitter. A strong coherent tone is sent to the coupling port of the directional coupler, resulting in displacement of an input mode $\hat{a}$. In our experiments, we use cryogenic directional couplers from Sirius Microwave with the coupling coefficient of $C = 19.4\,\mathrm{dB}$ at the working frequency of $5.48\,\mathrm{GHz}$. Based on Eq. (2.97), we write the associated transmissivity $\tau = 1 - 10^{-C/10}$ with $\sqrt{1-\tau} = \alpha/\alpha_{\mathrm{coh}}$. The action of the directional coupler can be written as

$$\hat{a}' = \sqrt{\tau}\hat{a} + \sqrt{1-\tau}\hat{b} \simeq \hat{a} + \alpha, \tag{4.19}$$

where we use the approximation of the strong coherent tone, $\hat{b} \simeq \alpha_{\mathrm{coh}}$, in the limit of $\tau \to 1$. From Eq. (4.19), we observe that the directional coupler implements the displacement operation described in Eq. (2.79). The coherent tones are generated by a room temperature microwave source (SGS100A from Rohde & Schwarz). We vary the coherent tone power $P_{\mathrm{coh}}$ and reconstruct a displacement mean photon number, $\bar{n}_{\mathrm{disp}} = \langle \hat{a}^\dagger \hat{a} \rangle$, at the output of the first directional coupler using the reference state reconstruction method for each power value. During measurements at a fixed coherent tone power, the displacement angle $\theta$ is reconstructed from the measured moments via

$$\theta = \mathrm{Arg}(\langle a \rangle). \tag{4.20}$$

This angle is used in the phase-locked loop, where we periodically adjust the phase of the coherent tone source by $\delta\theta = \theta - \theta_{\mathrm{t}}$, where $\theta_{\mathrm{t}}$ is a target displacement angle value. This procedure allows for a stable displacement angle within $\pm 1°$. In Fig. 4.15, we show the displacement photon calibration, with the corresponding displacement angle, that we use in this work. For completeness, we additionally display the measured purity, similarly to the squeezed state measurements. We observe high purities, $\mu \geq 96\%$, indicating that little-to-no noise is present in the measured displaced states. The displacement photon number can be fitted as

$$\bar{n}_{\mathrm{disp}} = m\, P_{\mathrm{coh}} + p, \tag{4.21}$$

where $m$ and $p$ are two fit parameters. As shown in Fig. 4.15 $(a)$, we observe a very good agreement between the measurement and the theory with a statistical coefficient of determination, $R^2 > 99.999\%$, indicating an excellent matching of our model in Eq. (4.21) to the measured data. The latter is a measure of the quality of a linear data fit with $R \in [0, 1]$ [220]. The result of the fit with the associated errors is shown in Tab. 4.1. From this fit, we can reliably convert any desired symbol, $\alpha_i$, of Alice's key into a corresponding power $P_i$ to set for the coherent tone according to

$$P_i = \frac{|\alpha_i|^2 - p}{m}. \tag{4.22}$$

Lastly, the values of displacement chosen in our experiments are dependent on the codebook variance of Alice, which is related to the squeezed level chosen for our protocol implementation.

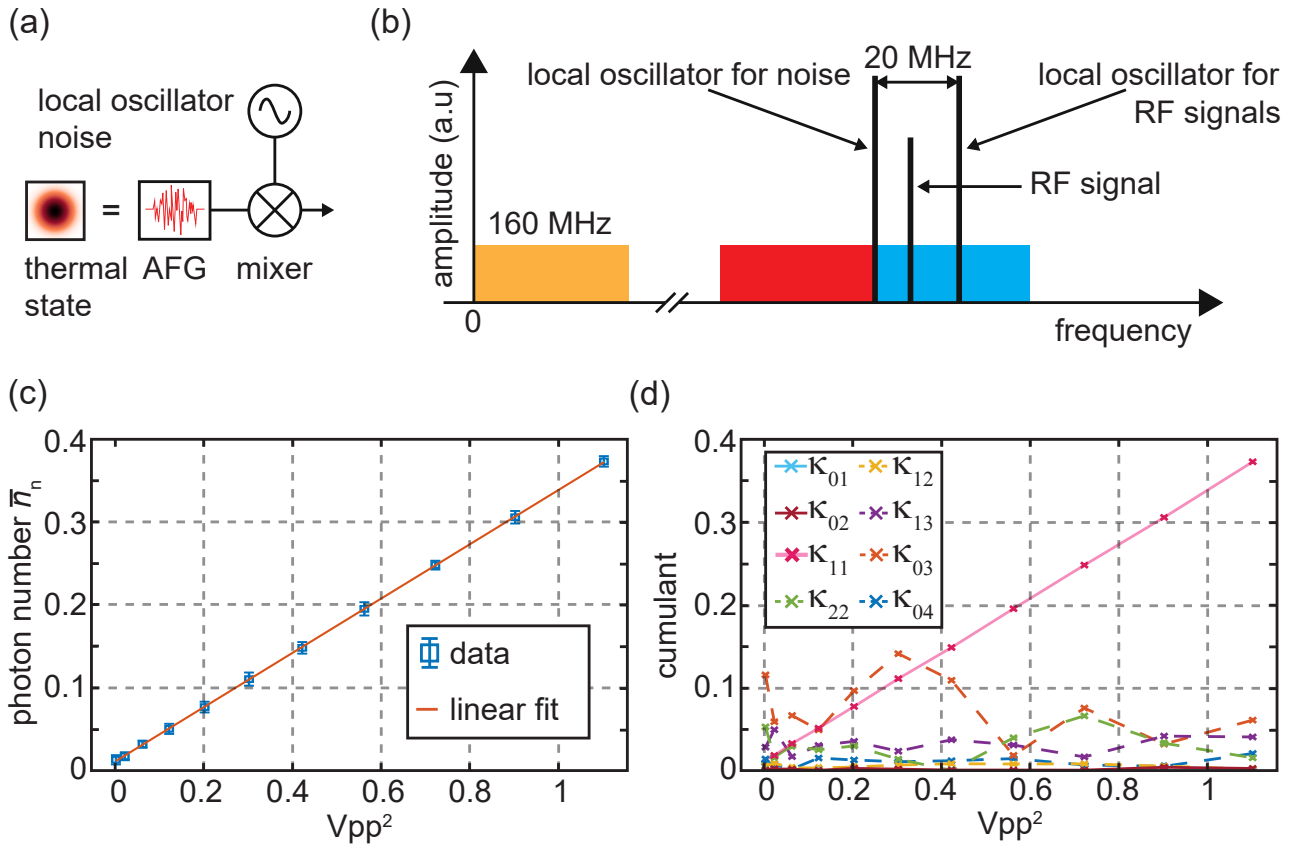


Figure 4.16: Experimental calibration of the coupled mean noise photon number $\bar{n}$. (a) Illustration of frequency up-conversion of noise. Artificially generated Gaussian noise, resembling a thermal state, is sent to a mixer driven by a LO. (b) Up-conversion of the 160 MHz noise bandwidth results in a red and blue sideband around the LO for noise. The latter is detuned by 20 MHz from the LO used during down-conversion of RF signals. Schematic not to scale. (c) Measured photon number $\bar{n}_n$ as a function of the square of the noise peak-to-peak voltage generated by the AFG. The data is fitted according to the linear fit in Eq. (4.28). (d) Cumulants computed from the measured signal moments up to the fourth order as a function of the square of the peak-to-peak voltage of the AFG. Cumulants are computed as in Eq. (4.9).

### 4.3.5 Calibration of coupled noise

We generate a quasi-Gaussian noise using an AFG source (81160A from Keysight) in a bandwidth of $0-160$ MHz. The noise signal is up-converted to a desired gigahertz frequency using a harmonic microwave mixer (M2-0218 from Marki microwave) driven by a strong tone, serving as a LO, from an additional SMB microwave source (SMB100A from Rohde&Schwarz), illustrated in Fig. 4.16 (a). The mixing process results in two sidebands according to $\omega_1 \pm \omega_2$ with $\omega_1$ being the LO microwave signal and $\omega_2$ a noise frequency in the noise bandwidth. We use the blue sideband, while the red sideband is filtered out by the down-conversion chain as shown in Fig. 4.16 (b). During noise calibration, all other devices are turned off. Both JPAs are detuned by more than 100 MHz, far from the chosen RF frequency point. The up-converted noise signal is sent to the coupling port of the second cryogenic directional coupler (see Fig. 4.2)). The corresponding operation is identical to the displacement operation

$$\hat{a}' = \sqrt{\tau}\hat{a} + \sqrt{1-\tau}\hat{f}, \tag{4.23}$$

where $\hat{f}$ is a noise mode, corresponding to the coupled noise within our measurement bandwidth. The transmissivity is given by the coupling of the directional coupler, $\tau = 1-10^{-C/10} = 0.9885$. We reconstruct a mean noise photon number using the reference state reconstruction method.

| values / statistic | slope $m'$ | offset $p'$ |
|---|---|---|
| linear fit value (photon/W) | $3.27 \cdot 10^{-1}$ | $1.21 \cdot 10^{-2}$ |
| error linear fit (photon/W) | $7.43 \cdot 10^{-14}$ | $< 10^{-4}$ |

Table 4.2: Summary of the parameters obtained from the linear fit according to Eq. (4.28) of the coupled noise used in the CV-QKD protocol implementation. The linear fit values are shown with their associated errors.

We relate the reconstructed photon number, $\bar{n}_{\mathrm{n}} = \langle \hat{a}^{\dagger}\hat{a} \rangle$, at the input of the HEMT to the noise photon number, $\bar{n}_{\mathrm{E}}$, at the input of the coupling port of the second directional coupler. Assuming that the final measured state corresponds to a thermal state, we derive the relation

$$(\tau_4\tau_3\tau_{\mathrm{E}} + 1 - \tau_3\tau_4)(1 + 2\bar{n}_{\mathrm{th}}) + \tau_3\tau_4\varepsilon_{\mathrm{E}}(1 + 2\bar{n}_{\mathrm{E}}) = (1 + 2\bar{n}_{\mathrm{n}}), \tag{4.24}$$

where $\tau_i$ with $i \in \{E, 3, 4\}$ describes transmissivity of the directional coupler, the path between the measurement JPA 2 and the directional coupler, and the path between the measurement JPA 2 and the HEMT, respectively. This equation can be reformulated to separate the losses and the noise contribution as

$$\frac{(\tau_4\tau_3\tau_{\mathrm{E}} + 1 - \tau_3\tau_4)(1 + 2\bar{n}_{\mathrm{th}}) + \tau_3\tau_4\varepsilon_{\mathrm{E}}}{4} + \tau_3\tau_4\bar{n} = \frac{(1 + 2\bar{n}_{\mathrm{n}})}{4}, \tag{4.25}$$

where we have defined the coupled noise photon number

$$\bar{n} = \frac{\varepsilon_{\mathrm{E}}\bar{n}_{\mathrm{E}}}{2}. \tag{4.26}$$

As a result, we can extract the following relation for the coupled noise photon number:

$$\bar{n} = \frac{\bar{n}_{\mathrm{n}} - (\tau_4\tau_3\tau_{\mathrm{E}} + 1 - \tau_4\tau_3)\bar{n}_{\mathrm{th}}}{2\tau_4\tau_3}. \tag{4.27}$$

To determine $\bar{n}$, we experimentally vary the total reconstructed photon number $\bar{n}_{\mathrm{n}}$ by sweeping the power of the AFG source $P_{\mathrm{n}}$. In Fig. 4.16 (c), we show the noise calibration used for our CV-QKD protocol implementations. The measured values can be linearly fitted according to

$$\bar{n}_{\mathrm{n}} = m' P_{\mathrm{n}} + p'. \tag{4.28}$$

Here, $m'$ and $p'$ are two fit parameters, similar to the displacement photon number calibration.

From Eqs. 4.27 and 4.28, we can reliably convert a desired photon number $\bar{n}$ into a corresponding power $P_{\mathrm{n}}$. The resulting fitting parameters with their associated error are shown in Tab. 4.2. We obtain the fit with a statistical coefficient of determination $R^2 > 99.99\%$, indicating that the data can be perfectly described by Eq. (4.28). Lastly, we show computed cumulants in Fig. 4.16 (d). Following our analysis in Sec. 4.3.2, we conclude that the generated noise follows Gaussian statistics.

### 4.3.6 Gaussianity verification based on characteristic functions

In this subsection, we propose an alternative approach to determine a threshold of Gaussianity in measured states. We use the characteristic function defined in Eq. (2.72) and consider a measurement for which only one experimental parameter is changed (typically the pump power). In the context of our experiments, we consider that there exist two regimes, one where the states are Gaussian and another where they deviate from the Gaussian statistics. We assume that

these two regimes are separated by a clear threshold across the chosen system parameter, such as pump power. For instance, in squeezing level measurements, the parameter is the pump power sent to the JPA. In the case of Gaussian states, one derives the general characteristic function of an arbitrary displaced squeezed thermal state as [221]

$$\chi(x,y) = -xy(\sinh(r)^2\coth(k/2)+f(k)) - \frac{\cosh(r)\sinh(r)\coth(k/2)}{2}(e^{-i\varphi}x^2+e^{i\varphi}y^2)+x\alpha^*-y\alpha, \tag{4.29}$$

where $r$ is the squeezing factor with the associated squeezing angle, $\gamma = -\varphi/2$. The displacement complex amplitude is given by $\alpha$, and $k = \hbar\omega/(k_\mathrm{B}T)$ with the temperature $T$ of the thermal state and its frequency $\omega$. The function $f$ is the Planck distribution,

$$f(k) = \frac{1}{\exp(k)-1}. \tag{4.30}$$

All these parameters can be extracted from reconstructed signal moments based on the assumption that the measured state is a Gaussian displaced squeezed thermal state. Note that according to Eq. (2.85), any Gaussian state can be described in this form. We find that

$$r = \frac{1}{2}\ln\left(\frac{\sigma_\mathrm{as}}{\sigma_\mathrm{s}}\right),\ \varphi = \mathrm{Arg}(\langle\hat{a}\rangle^2 - \langle\hat{a}^2\rangle),\ \bar{n}_\mathrm{JPA} = \frac{4\sigma_\mathrm{as}\sigma_\mathrm{s}-1}{2},\ T = \hbar\omega\left[k_\mathrm{B}\ln\left(1+\frac{1}{\bar{n}_\mathrm{JPA}}\right)\right]^{-1}, \tag{4.31}$$

where the squeezing variance $\sigma_\mathrm{s}$ and the anti-squeezing variance $\sigma_\mathrm{as}$ are defined by Eq. (4.18). Similarly, the displacement complex amplitude is computed as $\alpha = \langle\hat{a}\rangle$.

Based on these parameters, we compute the theoretical predictions of the signal moments from Eq. (4.29). Naturally, there is a good agreement between theory and measurements for moments of order two or less, since these are used to extract the system parameters. However, there is additional information that can be extracted from the moments of order three and four. In the case of the measured state being genuinely Gaussian, we expect a good agreement with theory, with a significant deviation once the states become non-Gaussian. The main difference with the cumulant measurements is that we use the theoretical prediction as a reference for comparison. Following this idea, we define a relative error as

$$\mathrm{err} = \left|\max_{i,j}\left\{\frac{M^{ij}_\mathrm{theo}-M^{ij}_\mathrm{exp}}{M^{ij}_\mathrm{theo}}\ \text{for}\ (i,j)|i+j\leq 4\right\}\right|, \tag{4.32}$$

where $M^{ij}_\mathrm{theo}$ is the signal moment $\left\langle(\hat{a}^\dagger)^i\hat{a}^j\right\rangle$ given by our theory prediction and $M^{ij}_\mathrm{exp}$ is the corresponding measured moment. We note that from this definition of the error, a large uncertainty can be obtained for the case of moments with near-zero or zero predicted values. When these cases appear, these moments are discarded in our analysis. Each measurement of the moments $M^{ij}_\mathrm{exp}$ is repeated $M$ times, which are used to build a histogram of the relative error as a function of the system parameter. Assuming that the error is distributed according to a Gaussian distribution for large data sets, we aim at comparing the different errors between them in order to find outliers. Ideally, we compare all errors to a reference error, which would be measured in ideal conditions. Taking into account that each error histogram has a finite sample size and that each individual measurement presents statistical fluctuations and errors, it is typically challenging to assign one specific measurement as a reference. To circumvent this problem, we compare each error distribution to each other by considering each error consecutively as the reference. For measurements using JPAs, where we vary pump power, we impose the additional restriction that a measurement $A$ can be considered as a reference for another measurement $B$ if and only if the pump power in measurement $A$ is strictly smaller

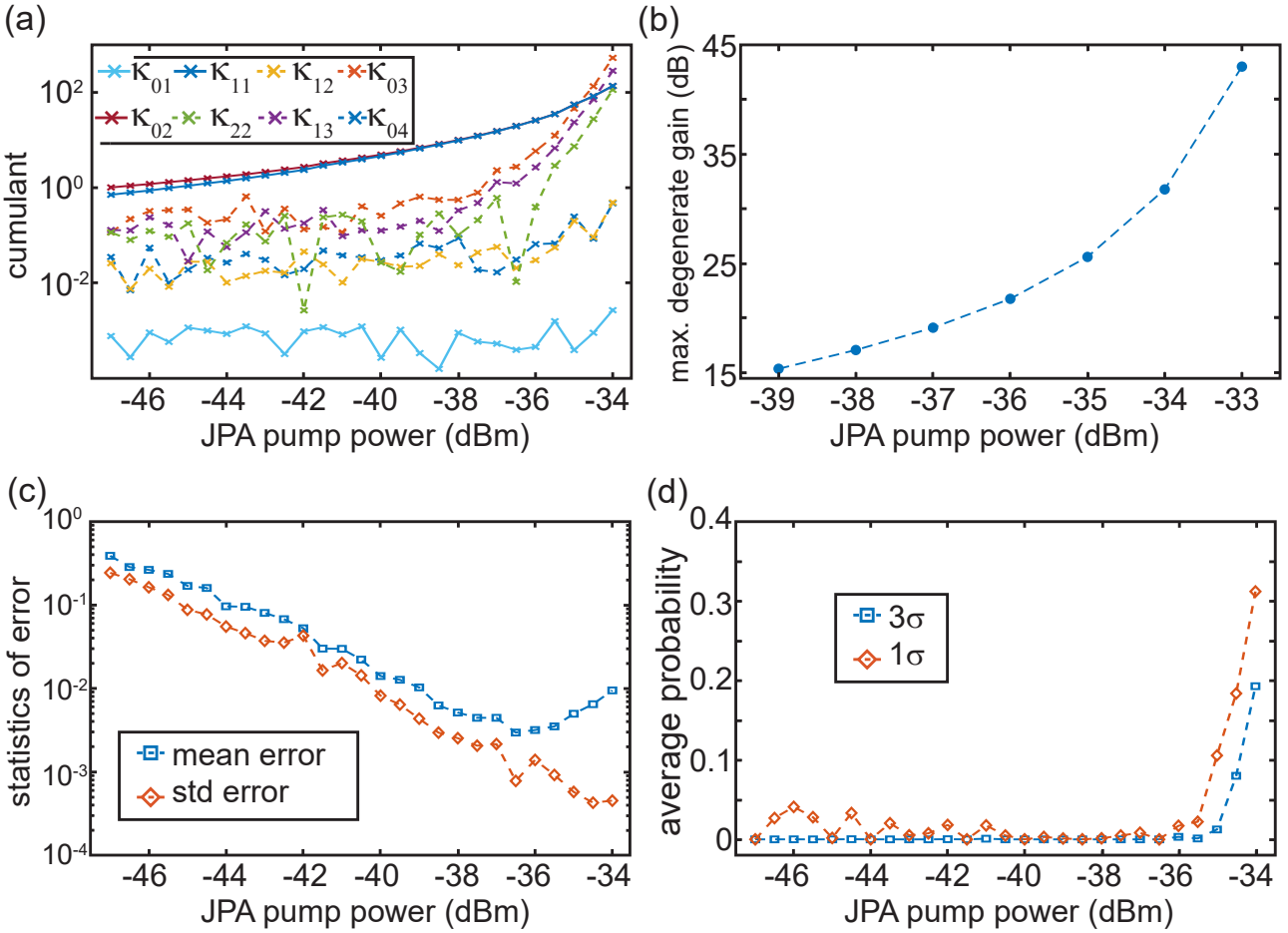


Figure 4.17: Exemplary Gaussianity verification. (a) Extracted cumulants for a squeezing measurement of JPA 1 as a function of the JPA pump power according to Eq. (4.9). (b) Measured maximal degenerate gain as a function of the JPA pump power. (c) Mean value and standard deviation of the relative error defined in Eq. (4.32) as a function of the JPA pump power. (d) Average probability that the observed statistics deviates from Gaussian statistics according to Eq. (4.34) as a function of the JPA pump power. The probability is computed for a 3-$\sigma$ threshold with $\mathrm{tr} = \mu_1 + 3\sigma_1$ and for a 1-$\sigma$ threshold with $\mathrm{tr} = \mu_1 + \sigma_1$.

than the one in measurement $B$. For instance, a squeezing measurement at a given pump power is used as a reference only for squeezing measurements with strictly higher pump powers. This restriction relies on the assumption that non-Gaussian features arise in a monotonic manner, meaning that, as we sweep the experimental parameter above a certain threshold value, the state becomes and remains non-Gaussian for higher pump powers.

In Fig. 4.17 (c), we show the relative error associated with a squeezing level measurement of JPA 1 at the frequency of $\omega_\mathrm{J} = 5.5\,\mathrm{GHz}$. Initially, we observe a decrease in the error as a function of the JPA pump power. This can be primarily understood as a relative increase in SNRs, as the signal amplitude increases with the pump power, reflected by the exponential dependency of the mean and standard deviation of the error. However, we note that above the pump power value, $P = -36.5\,\mathrm{dBm}$, the mean error starts to increase while the standard deviation continues to decrease. This behavior can be interpreted as an indication of non-Gaussian features emerging in the measured states, shifting from a squeezed state to a non-Gaussian one.

In order to compare the error distributions, we use a worst-case scenario, where we compute a probability $p$ that a tested distribution $P_2$ deviates strongly from a reference distribution $P_1$. Here, we are only interested in the cases of the mean value, $\mu_2$, of the distribution $P_2$ being larger than the mean value, $\mu_1$, of the reference distribution $P_1$. The opposite case indicates

that the error of the distribution $P_2$ is centered around a value smaller than for the reference $P_1$, and as such, the distribution $P_2$ cannot originate from non-Gaussian features. We take a one-sided 3-$\sigma$ deviation, which covers 99.88 % values of a Gaussian distributed random variable. The detection probability is defined as

$$p(P_2 \,\text{far from}\, P_1) = \int_{\text{tr}}^{+\infty} P_2(x)\mathrm{d}x = \frac{1}{2}\left(1 - \text{erf}\left(\frac{\text{tr} - \mu_2}{\sqrt{2}\sigma_2}\right)\right), \quad \text{tr} = \mu_1 + 3\sigma_1. \tag{4.33}$$

Here, $\mu_{1(2)}$ and $\sigma_{1(2)}$ are the expectation value and standard deviation of the distribution $P_1(2)$. Using different references $P_1$, we compute a matrix of probabilities $p_{i,j}$, where the index $i$ indicates the distribution chosen as the reference and the index $j$ refers to the tested distribution. To account for all the different individual probabilities $p_{i,j}$, we compute an ensemble probability for which each probability is weighed by a weight $w_{i,j}$ such that $\sum_{i=1}^{j-1} w_{i,j} = 1$ for a given $j$. A naive approach is to consider all distributions to have an equal chance of being representative of the error distribution for a Gaussian state. As such, we use a uniform distribution to assign the weights $w_{i,j} = 1/(j-1)$. We note that this approach is not optimal, since the mean error in Fig. 4.17 (c) presents a minimum value at a non-trivial pump power. Given these considerations and for a given tested distribution $P_j$ (except $P_1$), we compute the average detection probability as

$$\bar{p}_j = \frac{1}{j-1}\sum_{i=1}^{j-1} p_{i,j}. \tag{4.34}$$

In Fig. 4.17 (d), we display the average detection probability associated with the relative error shown in Fig. 4.17 (c). We observe a clear threshold behavior between two regimes: the first, where the average probability is negligible ($\bar{p}_j \ll 1\%$), and the second, showing a sudden increase for pump powers above $-36\,\text{dBm}$. For comparison, we also choose a 1-$\sigma$ deviation, which allows for a more refined distinction of the distributions, but only covers 79% of random outcomes. Remarkably, we find almost the same threshold as for the 3-$\sigma$ deviation, indicating robustness of the presented method. As the next step, one could potentially compute the propagated error of measurements above the threshold pump power under the (erroneous) assumption that the measured state is still Gaussian. For instance, one could estimate the propagated error on state fidelities [222].

It is insightful to compare the presented approach to the corresponding cumulants, computed from the same measured signal moments, as displayed in Fig. 4.17 (a). We observe a good agreement in terms of the assigned threshold pump power, where for the cumulants we use the criterion that cumulants of lower orders must be larger than cumulants of higher orders. Interestingly, we can compare this JPA pump power threshold with degenerate gain measurements. In Fig. 4.17 (b), we show the degenerate gain measurements of the same JPA, measured following the procedure in Sec. 4.2. Based on our analysis and with the deviation tolerance of $\bar{p}_j \leq 5\%$, we estimate that the measured states deviate significantly from a Gaussian distribution for pump powers above $-34.8\,\text{dBm}$, implying that the measured JPA behaves as a linear amplifier in very good approximation for degenerate gain values of $G_\text{J} \lesssim 26\,\text{dB}$.

## 4.4 Summary

In conclusion, we have presented the cryogenic setup with its associated room temperature down-conversion scheme and signal processing chain. We have explained the different steps involved in the measurement of the signal moments, including signal digitization, filtering, and $I/Q$ demodulation. Based on the novel technique of 2D Planck spectroscopy, we have detailed a precise method to experimentally reconstruct signal moments. From these moments,

the Wigner function of reconstructed states is obtained, giving full information about the associated quantum states. There, we have commented on Gaussianity tests based on the computation of cumulants up to the fourth order, which are enough to capture the presence of non-Gaussian features in measured signals. We have shown calibration measurements for squeezing, displacement, noise, and quantum efficiency in the experimental setup. Lastly, we have introduced a novel method for the Gaussianity test based on characteristic functions, where experimentally extracted signal moments can be compared to theoretical reference values. Using squeezing measurements, we have shown that clear thresholds can be decided to distinguish the transition from Gaussian to non-Gaussian regimes. Having presented these different elements, we can investigate the experimental implementation of the CV-QKD protocol and associated measurement results.

# Chapter 5

# Single-shot microwave quantum key distribution

In this chapter, we present experimental results of our implementation of the CV-QKD protocol in the microwave regime with squeezed states. First, in Sec. 5.1, we discuss the experimental implementation of single-shot single quadrature measurements in the microwave domain. Section 5.2 presents the experimental setup and associated quadrature measurement model. Then, in Sec. 5.2, we show corresponding measurement results, where we discuss details of our CV-QKD experiment, with associated experimental parameters and extracted information quantities, such as mutual information, Holevo quantity, and secret keys.

## 5.1 Single-shot measurements

Here, we focus on the experimental implementation of single-shot single quadrature measurements in the microwave domain. Section 5.1.1 presents possible considerations and experimental setups for the quadrature measurements. There, we show the usage of a single JPA to achieve the desired quadrature measurements. In Sec. 5.1.2, we explain that the statistics of measured quadratures are fully included in the measurements of $I/Q$ points and their corresponding moments, even when reaching the single-shot regime.

### 5.1.1 Quadrature measurements using parametric amplifiers

In quantum teleportation implemented in experiments based on continuous-variable states [24, 96], it has been established that phase-sensitive amplifiers combined with a directional coupler can be used to implement quadrature projectors in phase space. More precisely, we consider the case of an analog Bell-state measurement, as depicted in Fig. 5.1 (a). A detailed discussion on this topic can be found in Ref 205. There, the setup consists of two phase-sensitive amplifiers placed between two 50:50 beam splitters. An input signal is sent to one input of the first beam splitter. The output signal coming from the second beam splitter is sent to an asymmetric beam splitter. For continuous-variable states in the microwave regime, we use JPAs to perform phase-sensitive amplification. We note that the resulting setup of two JPAs and two hybrid rings can be used as a Josephson nonlinear interferometer, particularly relevant for quantum sensing or quantum radar applications [89, 217]. Lastly, the asymmetric beam splitter can be implemented using a directional coupler [51]. The phase-sensitive amplification of the JPAs is

described by the matrices

$$\mathbf{J} = \begin{pmatrix} \mathbf{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{J}_q & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{J}_p \end{pmatrix}, \quad \mathbf{J}_q = \begin{pmatrix} 1/\sqrt{G} & 0 \\ 0 & \sqrt{G} \end{pmatrix}, \text{ and } \quad \mathbf{J}_p = \begin{pmatrix} \sqrt{G} & 0 \\ 0 & 1/\sqrt{G} \end{pmatrix}. \tag{5.1}$$

Here, $\mathbf{0}_n$ is a quadratic matrix with zero entries and dimension $n$, and $G$ is the amplification gain of the JPAs. The directional coupler and hybrid rings are described by a beam splitter operator with $\tau = 1-\beta$ and $\tau = 1/2$, respectively, with $\beta \in [0,1]$. The Bell-state measurement can be modelled using the Gaussian channel formalism in Sec. 2.2.2 following Eq. (2.91) with [205]

$$\mathbf{T} = \frac{1}{2}\begin{pmatrix} 2\sqrt{1-\beta}\mathbf{I}_2 & \sqrt{\beta}(\mathbf{J}_q - \mathbf{J}_p) & \sqrt{\beta}(\mathbf{J}_q + \mathbf{J}_p) \\ -2\sqrt{\beta}\mathbf{I}_2 & \sqrt{1-\beta}(\mathbf{J}_q - \mathbf{J}_p) & \sqrt{1-\beta}(\mathbf{J}_q + \mathbf{J}_p) \\ \mathbf{0}_2 & -\mathbf{J}_q - \mathbf{J}_p & -\mathbf{J}_q + \mathbf{J}_p \end{pmatrix}, \mathbf{r} = \bar{\mathbf{0}}, \text{ and } \mathbf{N} = \mathbf{0}_6. \tag{5.2}$$

The zero displacement vector is denoted as $\bar{\mathbf{0}}$. In the projective limit, one can define a constant $k$ such that

$$\beta \to 0, \quad G \to +\infty, \text{ and } \quad k \coloneqq \frac{G\beta}{4} = \text{const.} \tag{5.3}$$

In the case of $k = 1$, one can show that the renormalized operators, $\sqrt{\beta}\mathbf{J}_q$ and $\sqrt{\beta}\mathbf{J}_p$, converge to quadrature projection operators as $\sqrt{\beta}\mathbf{J}_q \to 2\mathbf{\Pi}_q$ and $\sqrt{\beta}\mathbf{J}_p \to 2\mathbf{\Pi}_p$. Here, the matrices $\mathbf{\Pi}_q$ and $\mathbf{\Pi}_p$ are quadrature projectors in phase space for the $q$- and $p$-quadrature, respectively. The PVM measurement requirement is additionally fulfilled as $\mathbf{\Pi}^2_{q(p)} = \mathbf{\Pi}_{q(p)}$. As such, one could consider the JPAs acting as quadrature projectors in each branch of the setup. However, one derives that the final output state after the directional coupler is related to an input state at the first hybrid ring as

$$\mathbf{d}_{\text{out}} = \mathbf{d}_{\text{in}}, \quad \mathbf{V}_{\text{out}} = \mathbf{\Pi}\mathbf{V}_{\text{in}}\mathbf{\Pi}^T \quad \text{and} \quad \mathbf{\Pi} = \begin{pmatrix} \mathbf{I}_2 & \frac{-\boldsymbol{\sigma}_z}{2} & \frac{\mathbf{I}_2}{2} \end{pmatrix}, \tag{5.4}$$

where $\mathbf{V}_{\text{in}}$ is a 6x6 matrix describing the three modes involved in the Bell-state measurement, including the input mode. It can be shown that in the projective limit of $k = 1$ when using a TMS state as an input, one can recover $\mathbf{V}_{\text{out}} = \mathbf{V}_{\text{in}}$. The resulting states at the output of the directional coupler can ideally have no extra noise as compared to the initial state. However, the displacement vector is also left unchanged according to Eq. (5.4). This result is not surprising, as this setup is designed to perform quantum teleportation of an input state.

Nevertheless, a possible way to implement PVM measurements for quadrature operators is to consider only a single path of the previous setup, as shown in Fig. 5.1 (b). In this case, only a single mode is necessary to describe the overall transformation. The latter effectively consists of a unitary squeezing channel with $\exp(r) = \sqrt{G}$ according to Eq. (2.94) followed by an attenuation channel $C_1$ with $\tau = \beta$. Using the formalism presented in Sec. 2.2.2, we derive that this new setup results in a Gaussian channel with the following parameters:

$$\mathbf{T} = \sqrt{\beta}\begin{pmatrix} 1/\sqrt{G} & 0 \\ 0 & \sqrt{G} \end{pmatrix}, \quad \mathbf{r} = \bar{\mathbf{0}}, \text{ and } \quad \mathbf{N} = \frac{1}{4}(1+2\bar{n})\mathbf{I}_2. \tag{5.5}$$

One can take a similar projection limit by setting $k_0 = \beta G = 1$ with $\beta \to 0$ and $G \to +\infty$, then we recover the same projector limit $\sqrt{\beta}\mathbf{J}_q \to \mathbf{\Pi}_q$. However, according to the Gaussian channel formalism, an additional noise photon number, $\bar{n}$, is added to the input signal following Eq. (5.5). Since in the setup in Fig. 5.1 (b) one signal path containing one JPA has been removed

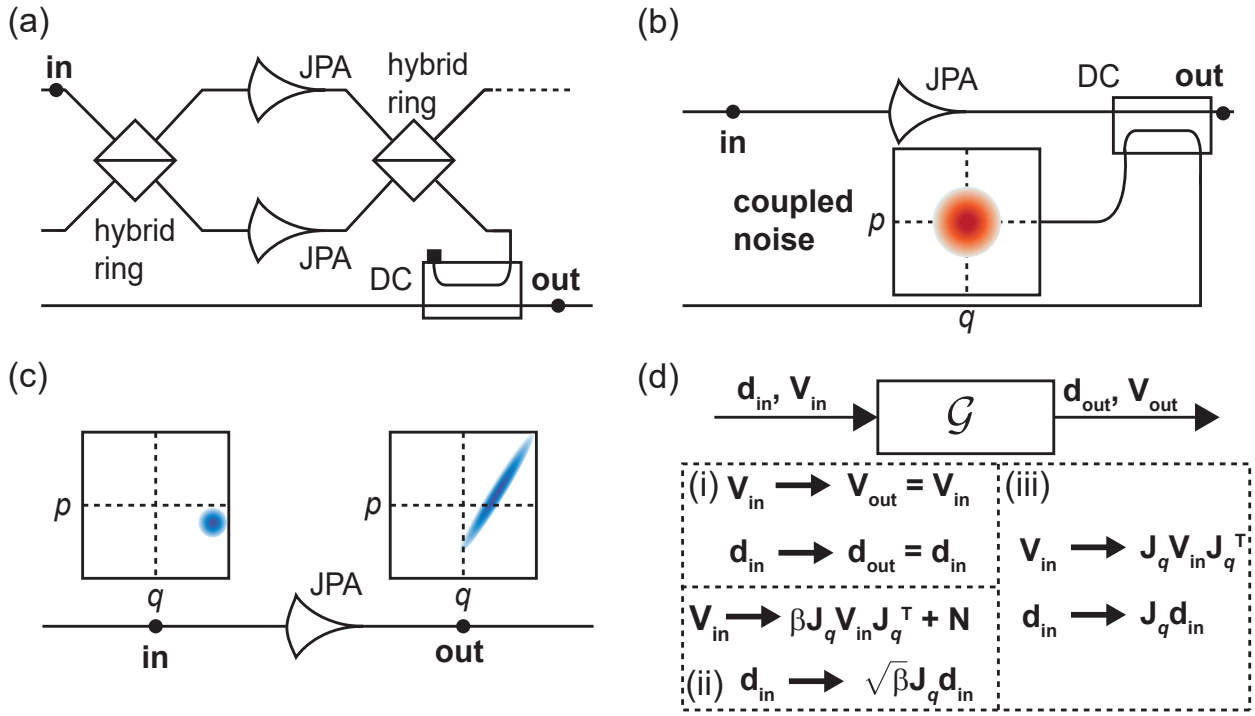


Figure 5.1: Schematic representation of quadrature measurements. The Bell-state measurement setup in panel (a) consists of two JPAs operated in the phase-sensitive regime and two hybrid rings acting as 50:50 beam splitters. The output (out) state is obtained at the output of a directional coupler (DC) for a corresponding input state (in) sent to one input of the first hybrid ring. A simplified setup is presented in panel (b), which consists of one JPA and a directional coupler. The noise coupled to the JPA is represented by its associated Wigner function. The last setup in panel (c) represents a strong phase-sensitive amplification performed by a single JPA. An exemplary amplified state is represented by its associated Wigner function. The overall transformations, according to Eqs. 5.2,5.5,5.6, of each measurement acting as a quantum channel $\mathcal{G}$ is shown in panel (d) where each transformation is indicated by a corresponding index. Here, (i) is for panel (a), (ii) for panel (b), and (iii) for panel (c).

as compared to that in Fig. 5.1 (a), an additional bath mode has to be introduced so that the final modes fulfil the bosonic relation. In other words, it is possible to construct a Gaussian channel that implements a quadrature projection at the cost of unavoidably adding noise to the input signal. Note that according to Eq. (5.5), at least vacuum fluctuations are added to the input signal. A possibility to achieve a reduction in noise as compared to the previous measurement techniques is to drop the directional coupler and to limit the measurement to only a single JPA operated in the phase-sensitive regime as shown in Fig. 5.1 (c). Ideally, a phase-sensitive amplification can be noiseless meaning that the PVM measurement would simply to a pure squeezing operation with a corresponding quantum channel that can be described using

$$\mathbf{T} = \begin{pmatrix} 1/\sqrt{G} & 0 \\ 0 & \sqrt{G} \end{pmatrix}, \quad \mathbf{r} = \bar{\mathbf{0}}, \text{ and } \quad \mathbf{N} = \mathbf{0}_2. \tag{5.6}$$

Using the squeezing operator, one obtains the interesting result that the amplified quadrature statistics can be retrieved while the deamplified quadrature eventually becomes inaccessible due to the inevitable presence of a noise floor in practical measurements. More precisely, a measurement of both quadratures, adding a finite noise photon number $\bar{n}$ to both quadratures, results in a final covariance matrix after the squeezing operation given by

$$\mathbf{V}_{\text{out}} = \begin{pmatrix} \frac{V_{11}}{G} + \frac{1+2\bar{n}}{4} & V_{12} \\ V_{21} & GV_{22} + \frac{1+2\bar{n}}{4} \end{pmatrix}. \tag{5.7}$$

Here, the entries of the initial Gaussian state are denoted $\{V_{ij}\}_{(i,j)\in[1,2]^2}$. Using Eq. (5.7), we straightforwardly obtain that the matrix entry $\mathbf{V}_{\text{out},22}$, upon rescaling by the gain $G$, converges to $V_{22}$ in the projective limit of $G \to +\infty$. Conversely, in this limit, noise only appears in the deamplified quadrature, reflected by the entry $\mathbf{V}_{\text{out},11}$. As a result, only the information about one quadrature remains accessible, coinciding with a projective measurement. However, this approach presents some limitations. First, one can note in Eq. (5.7) that off-diagonal terms are left unchanged as opposed to the case of a quadrature projection operator. This is not necessarily true in experiments. For a large enough amplification gain, the deamplified quadrature becomes extremely noisy (with a corresponding signal-to-noise ratio far less than 1). The measurement precision limits the achievable resolution of the measured deamplified quadrature, leading to a partial or total loss of original off-diagonal elements. As such, one JPA alone does not converge to a projection operator but provides similar results. Secondly, no rescaling is implemented, as it was previously the case using a directional coupler. Therefore, amplified signals acquire a large amplitude during experiments, which limits the range of experimental parameters that can be used, due to the limited saturation powers of other devices used in the experiment. Lastly, based on the formalism of Gaussian channels in Eq. (2.91), the initial displacement vector is also scaled by the matrix $\mathbf{T}$. This implies that measured displacements must be rescaled. This leads to an increased uncertainty originating from the uncertainty and instability in the amplification gain. In light of the previous discussion, we conclude that phase-sensitive amplification enables single-quadrature measurements to be made with a minimum of added noise, reaching a noiseless regime under ideal conditions.

### 5.1.2 Histogram based measurement and tomography

In Sec. 4.1, we have explained that our experiments utilize a heterodyne detection setup to measure both quadratures after amplification of the to-be-measured incoming signals. Based on the previous section, an ideal phase-sensitive amplification, resulting in a squeezing operation, allows the full information about a given amplified quadrature to be accessed with minimal disturbance at the cost of a corresponding deamplified quadrature. Therefore, by using a phase-sensitive preamplifier in the amplification chain, our experimental heterodyne detection setup effectively allows us to extract information about one quadrature, providing a measurement setup equivalent to a homodyne detection in the optical domain. To illustrate this aspect further, we focus on the procedure implemented during our heterodyne measurement. We recall that a given incoming signal, with a phase reference set to zero for convenience, is decomposed into two quadrature components

$$A(t) = I(t)\cos(\omega_{\text{IF}}t) + Q(t)\sin(\omega_{\text{IF}}t), \tag{5.8}$$

with an intermediate frequency $\omega_{\text{IF}}$. For continuous variable signals, the quadratures are defined as

$$I(t) = \frac{\omega_{\text{IF}}}{\pi}\int_t^{t+\frac{2\pi}{\omega_{\text{IF}}}} \cos(\omega_{\text{IF}}\tau)A(\tau)\mathrm{d}\tau \quad \text{and} \quad Q(t) = \frac{\omega_{\text{IF}}}{\pi}\int_t^{t+\frac{2\pi}{\omega_{\text{IF}}}} \sin(\omega_{\text{IF}}\tau)A(\tau)\mathrm{d}\tau. \tag{5.9}$$

In Sec. 4.1.3, we have explained that an RF signal at the output of our cryogenic setup is down-converted to an IF frequency with a narrow bandwidth determined by the FIR filters, typically of 400 kHz in our experiments. As a consequence, we approximate the associated quantum electric field as a single-mode field

$$\hat{E}(t) = 2E_0(\hat{q}\cos(\omega_{\text{IF}}t) + \hat{p}\sin(\omega_{\text{IF}}t)), \tag{5.10}$$

where $E_0$ is the amplitude of the field and the operators $\hat{q}$ and $\hat{p}$ are the quadrature operators of the associated quantum state. We consider that in a final step, the electric field is, at the

latest, projected onto some random eigenvectors $|\alpha = q + ip\rangle$ at times $t$ after amplification by a HEMT in our experiments. This means that we obtain some random value $q$ for the quadrature $\hat{q}$ and some random value $p$ for the quadrature $\hat{p}$. Following the laws of quantum mechanics, this random process is described by the underlying probability distribution of the measured quantum state. In addition, in the limit of a large amplification gain of the HEMT, at least vacuum fluctuations are added to the measured signal. The amplified signal is treated as a classical signal afterwards. Subsequent losses and added measurement noise can be straightforwardly accounted for by an additional amplification gain $\sqrt{G_{\mathrm{amp}}}$ and a noise signal $n_{\mathrm{m}}$. Under these considerations, we express the signal $A$ as

$$A(t) = \sqrt{G_{\mathrm{amp}}}(\langle\alpha|\hat{E}(t)|\alpha\rangle + 2E_0 n_{\mathrm{m}}(t)) = \sqrt{C_{\mathrm{amp}}}(q\cos(\omega_{\mathrm{IF}}t) + p\sin(\omega_{\mathrm{IF}}t) + n_{\mathrm{m}}(t)). \quad (5.11)$$

Here, we define $q = (\alpha + \alpha^*)/2$ and $p = (\alpha - \alpha^*)/2i$. The constant $\sqrt{C_{\mathrm{amp}}} = 2E_0 G_{\mathrm{amp}}$ is an overall scaling factor relating the amplitude of the signals at the output of the cryogenic setup to the signals measured at room temperature devices. The noise signal is assumed to be white Gaussian noise. The magnitude of this noise depends on the measurement bandwidth. Here, we decompose the noise signal picked up for the IF frequency as $n_{\mathrm{m}}(t) = \xi_1\cos(\omega_{\mathrm{IF}}t) + \xi_2\sin(\omega_{\mathrm{IF}}t)$ [223]. The classical random variables $\xi_1$ and $\xi_2$ are two independent zero-mean Gaussian variables with equal variance $\sigma^2_{\mathrm{GN}}/2$. Based on this result and with the definition of the quadrature operators, we compute the $I/Q$ quadrature expectation values as

$$\begin{aligned}\langle I(t)\rangle &= \frac{\omega_{\mathrm{IF}}}{\pi}\int_t^{t+\frac{2\pi}{\omega_{\mathrm{IF}}}} \cos(\omega_{\mathrm{IF}}\tau)\langle A(\tau)\rangle \mathrm{d}t \\ &= \frac{\omega_{\mathrm{IF}}\sqrt{C_{\mathrm{amp}}}}{\pi}\int_t^{t+\frac{2\pi}{\omega_{\mathrm{IF}}}} \cos(\omega_{\mathrm{IF}}\tau)\langle(\hat{q}\cos(\omega_{\mathrm{IF}}\tau) + \hat{p}\sin(\omega_{\mathrm{IF}}\tau) + n_{\mathrm{m}}(\tau))\rangle \mathrm{d}\tau \\ &= \sqrt{C_{\mathrm{amp}}}\langle\hat{q}\rangle.\end{aligned} \quad (5.12)$$

Here, we have used that $\langle q\rangle = \langle\hat{q}\rangle$ and $\langle p\rangle = \langle\hat{p}\rangle$. Similarly, we can derive that $\langle Q(t)\rangle = \sqrt{C_{\mathrm{amp}}}\langle\hat{p}\rangle$. We identify the scaling coefficient to be the PNCF in our measurements, i.e., $C_{\mathrm{amp}} = \kappa$. Additionally, using the linearity of the covariance, we can calculate the variance of the $I/Q$ quadratures as

$$\begin{aligned}\sigma^2_{\mathrm{I}} &= \mathrm{cov}(I(t), I(t)) \\ &= \left(\frac{\omega_{\mathrm{IF}}}{\pi}\right)^2 \int_t^{t+\frac{2\pi}{\omega_{\mathrm{IF}}}}\int_t^{t+\frac{2\pi}{\omega_{\mathrm{IF}}}} \cos(\omega_{\mathrm{IF}}\tau)\cos(\omega_{\mathrm{IF}}\tau')\mathrm{cov}(A(\tau), A(\tau'))\mathrm{d}\tau\mathrm{d}\tau' \\ &= C_{\mathrm{amp}}\left(\frac{\omega_{\mathrm{IF}}}{\pi}\right)^2 \int_t^{t+\frac{2\pi}{\omega_{\mathrm{IF}}}}\int_t^{t+\frac{2\pi}{\omega_{\mathrm{IF}}}} \cos(\omega_{\mathrm{IF}}\tau)\cos(\omega_{\mathrm{IF}}\tau')(\Delta\hat{q}^2\cos(\omega_{\mathrm{IF}}\tau)\cos(\omega_{\mathrm{IF}}\tau') + \\ &\qquad \Delta\hat{p}^2\sin(\omega_{\mathrm{IF}}\tau)\sin(\omega_{\mathrm{IF}}\tau') + (\langle\hat{q}\hat{p}\rangle - \langle\hat{q}\rangle\langle\hat{p}\rangle)\cos(\omega_{\mathrm{IF}}\tau)\sin(\omega_{\mathrm{IF}}\tau') + \\ &\qquad (\langle\hat{p}\hat{q}\rangle - \langle\hat{p}\rangle\langle\hat{q}\rangle)\sin(\omega_{\mathrm{IF}}\tau)\cos(\omega_{\mathrm{IF}}\tau') + \mathrm{cov}(n_{\mathrm{m}}(\tau), n_{\mathrm{m}}(\tau')))\mathrm{d}\tau\mathrm{d}\tau' \\ &= C_{\mathrm{amp}}(\Delta\hat{q}^2 + \sigma^2_{\mathrm{GN}}/2).\end{aligned} \quad (5.13)$$

Using a similar derivation, we can show that $\sigma^2_{\mathrm{Q}} = C_{\mathrm{amp}}(\Delta\hat{p}^2 + \sigma^2_{\mathrm{GN}}/2)$, and in general we find that $\langle I(t)^k Q(t)^l\rangle = C^{(k+l)/2}_{\mathrm{amp}}(\langle\hat{q}^k\hat{p}^l\rangle + \langle n_{\mathrm{m}}(t)^k n_{\mathrm{m}}(t)^l\rangle/2^{(k+l)/2})$ for $(k,l) \in \mathbb{N}^2$. In other words, the moments of the demodulated $I/Q$ points coincide exactly with those of their quantum operator counterpart, only scaled up by some coefficient $C_{\mathrm{amp}}$ and with an additional noise contribution. This property guarantees that each individual demodulated $I/Q$ point can be considered as a noisy sampling of the underlying probability distribution of the measured signal. Since the measured data points can always be rescaled by a properly determined PNCF, $\kappa$, the contribution of the amplification chain to the data statistics is the total amplification noise.

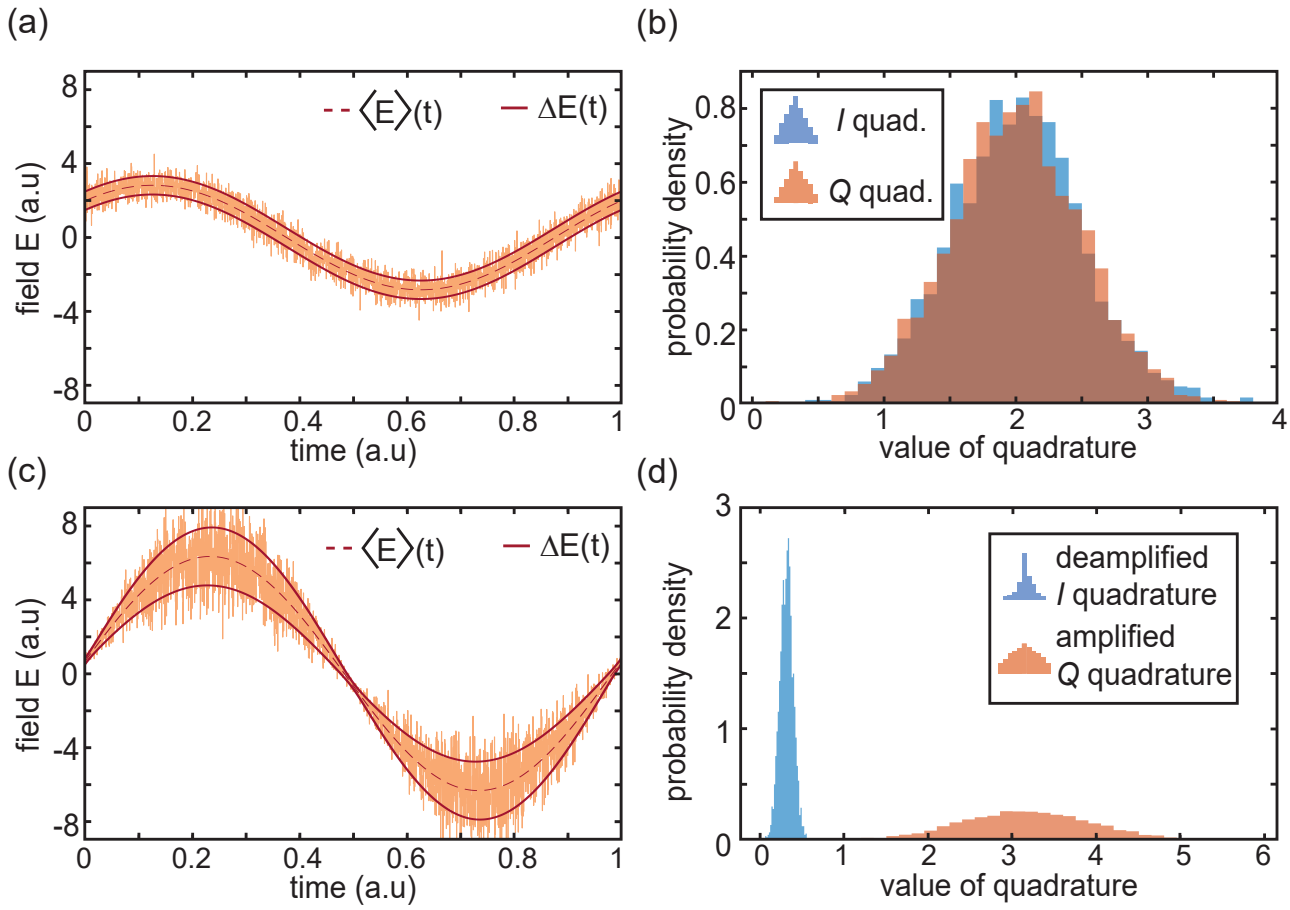


Figure 5.2: Time evolution and histogram of an exemplary coherent state with complex displacement amplitude $\alpha = 2 + 2i$, amplified using a JPA in the phase-sensitive regime. Panel (a) shows the time evolution of the associated electric field with mean value and standard deviation of the field. The corresponding Gaussian distribution of the $I/Q$-quadratures is shown in panel (b). The distributions are sampled with 3000 symbols. Histograms are shown with semitransparent colors to allow both distributions to be seen. Using a JPA, one quadrature of the initial coherent state is amplified, while the other quadrature is deamplified. The resulting electric field is shown in panel (c). Here, we assume that the $p$-quadrature is amplified with a gain of 10 dB. The resulting histogram of the $I/Q$-quadratures is shown in panel (d). The $I$-quadrature presents a narrower distribution with a reduced mean value, while the histogram of the $Q$-quadrature is broadened and has an enhanced mean value.

Each single $I/Q$ point extracted using the presented procedure can be referred to as a single-shot measurement, ideally, in noiseless conditions.

In light of our previous discussion, we consider a Gaussian state for which we aim to measure a single quadrature and obtain its corresponding statistics. Based on the setup introduced in Sec. 5.1.1, we use a JPA as a preamplifier in our amplification chain to strongly phase-sensitively amplify the to-be-measured quadrature, while the other quadrature is deamplified. An exemplary result is shown in Fig. 5.2, where the $p$-quadrature is strongly amplified. The corresponding histogram of the $I/Q$ quadratures illustrates the measurement principle. The statistics of amplified quadrature can be easily accessed from measurements, while the deamplified quadrature becomes much narrower and has a reduced mean value. From the previously introduced formalism, the corresponding measured $I/Q$ quadrature in the $I/Q$ plane presents exactly the same statistics up to an additional noise contribution and some scaling factor. For instance, if the $q$-quadrature is to be measured, we employ a preamplifier JPA to strongly amplify this quadrature. Based on Eqs. 5.7 and 5.13, we can express the measured $I$-quadrature

variance as

$$\sigma_{\mathrm{I}}^2 = \kappa \left( G_{\mathrm{J}} \sigma_q^2 + \frac{\sigma_{\mathrm{GN}}^2}{2} \right) = \kappa G_{\mathrm{J}} \left( \sigma_q^2 + \frac{\sigma_{\mathrm{GN}}^2}{2G_{\mathrm{J}}} \right). \tag{5.14}$$

Eq. (5.14) implies that in the limit of large amplification gain $G_{\mathrm{J}}$, the measured $I$-quadrature variance $\sigma_{\mathrm{I}}^2$ converges exactly to the quadrature variance $\sigma_q^2$ without any additional noise, only rescaled by a constant $\kappa G_{\mathrm{J}}$ that can be derived from calibration measurements. We note that in our experiments, we are limited by measurement-induced noise, e.g., a pump-induced noise of the preamplifier JPA, preventing an ideal noiseless single-shot measurement.

Lastly, we note that it is possible to reconstruct a Wigner function of an input quantum state from the introduced JPA-based quadrature measurement. Based on the description presented above, performing multiple quadrature measurements using a preamplifier JPA for a given quadrature $\hat{q}_\theta$ for $\theta \in [0, 2\pi)$ results in the measurement of the underlying probability density function associated with the measured quadrature. From Eq, 2.67, this function $f$ is related to the Wigner function of the measured quantum state $\hat{\rho}$ as [224]

$$f(q_\theta) = \mathrm{Tr}(\hat{\rho}\hat{q}_\theta) = \int_{-\infty}^{+\infty} W_{\hat{\rho}}(q_\theta, p_\theta) \mathrm{d}p_\theta. \tag{5.15}$$

In other words, each quadrature measurement with an angle $\theta$ provides a marginal distribution of the corresponding quadrature $\hat{q}_\theta$. This process can be viewed as performing a 2D cut at a given angle $\theta$ in the phase space of the Wigner function [224]. Repeating this procedure for $\theta \in [0, 2\pi)$ allows one to reconstruct the Wigner function, using for instance the Radon transform [225]. One can obtain the associated original density matrix via the Weyl transform [226], which corresponds to the inverse map of the Wigner function

$$\hat{\rho} = \left( \frac{1}{2\pi} \right)^2 \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} W_{\hat{\rho}}(q, p) \exp\left[ i(\alpha(\hat{q}_0 - q) + \beta(\hat{p}_0 - p)) \right] \mathrm{d}\alpha \mathrm{d}\beta \mathrm{d}q \mathrm{d}p. \tag{5.16}$$

In our experiments, this process is limited by the rate of number of points that can be measured for a given quadrature $\hat{q}_\theta$, the efficiency of quadrature measurements, and the rate at which the angle $\theta$ can be changed and stabilized. Additionally, we note that the derivations made above rely on the assumption that a given measured quantum state is stable throughout the measurements.

## 5.2 Continuous-variable quantum key distribution experimental implementation

In this section, we focus on the experimental implementation of the CV-QKD protocol. Sec. 5.2.1 presents the main components of the experimental setup as well as the experimental steps of the protocol implementation. In particular, we highlight practical considerations and limitations such as key sifting. In Sec. 5.2.2, we introduce a full quadrature measurement model that serves as the basis of all our data analysis of the protocol.

### 5.2.1 Protocol steps

Here, we consider the CV-QKD protocol with displaced squeezed states, following the protocol of Cerf et al. [105] explained in Sec. 3.3. Our CV-QKD protocol implementation relies on the generation of displaced squeezed microwave states to encode a key from Alice. Each squeezed state is generated by implementing a squeezing operation along the $q$- or $p$-quadrature, randomly chosen by Alice. These states are to be displaced in phase space to encode Alice's key. In

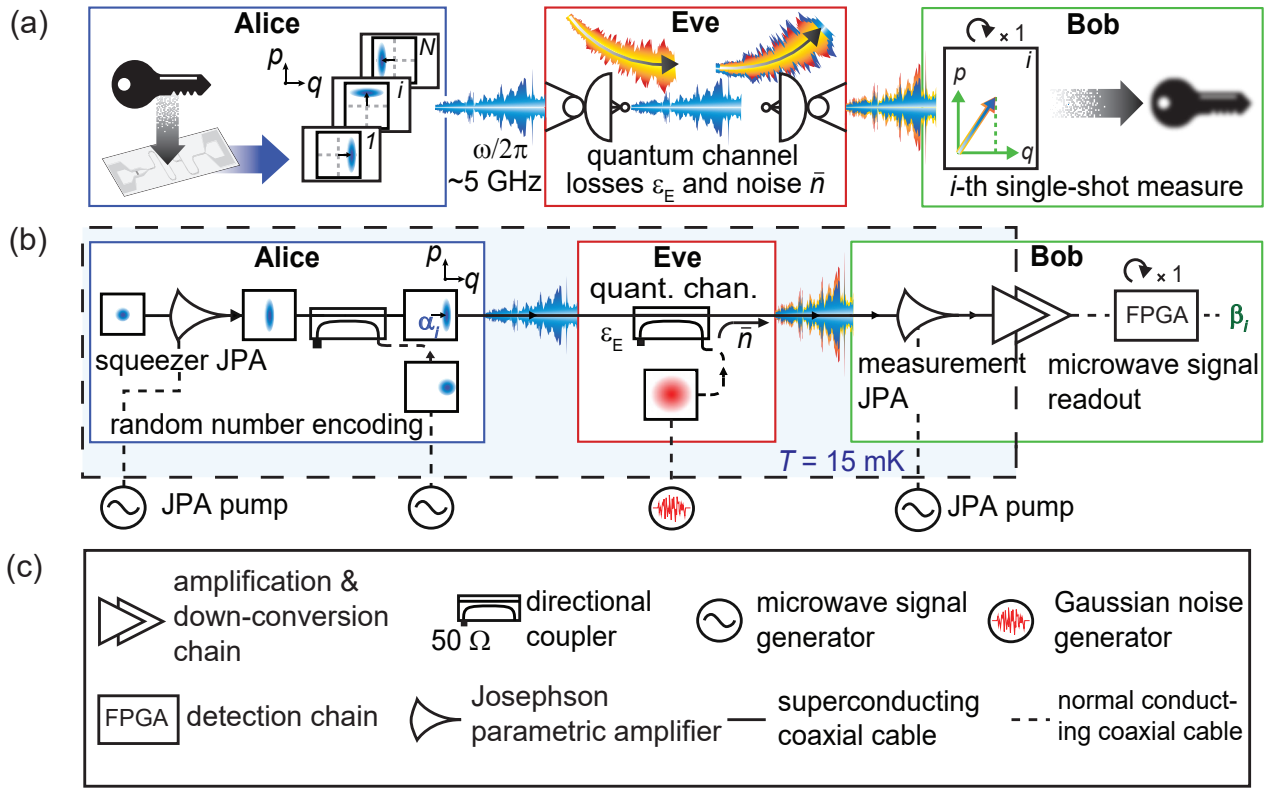


Figure 5.3: General concept of a prepare-and-measure CV-QKD protocol based on displaced squeezed states and its experimental implementation in the microwave regime. (a) In the CV-QKD protocol, Alice encodes her key in an ensemble of $q$- or $p$-displaced squeezed states. These states propagate as microwave signals through a quantum channel, which is assumed to be under Eve's control and is parametrized by power losses $\varepsilon_\mathrm{E}$ and an added noise photon number $\bar{n}$. Bob performs quadrature measurements to extract the displacement amplitude of each incoming state. (b) Experimental scheme of the microwave CV-QKD protocol with superconducting JPAs in the cryogenic environment. For each symbol, Alice generates a $q$- or $p$-squeezed state, which is subsequently displaced using a directional coupler coupled to a strong coherent signal. The resulting state propagates through a quantum channel consisting of a second directional coupler. This coupler is used to inject a variable number of noise photons $\bar{n}$. On Bob's side, a strong phase-sensitive amplification is performed using a second JPA. Color plots in boxes depict Wigner functions of quantum states in the quadrature phase space $(q, p)$. (c) Legend for various experimental components in panel (b).

Fig. 5.3, we illustrate its concept and present the scheme of our experimental implementation in the microwave regime.

We use a superconducting flux-driven JPA as presented in Sec. 2.1 for the generation of squeezed microwave states, which are characterized by a squeezing level $S$ below vacuum [51, 52]. Throughout this work, we refer to this JPA as the *squeezer* JPA. In this experiment, the JPAs and all other components are operated at the fixed frequency $\omega_\mathrm{J}/2\pi = 5.48\,\mathrm{GHz}$. We recall that a flux-driven JPA consists of a coplanar waveguide $\lambda/4$ resonator short-circuited to ground by a dc-SQUID (see Sec. 2.1.2). The dc-SQUID provides a flux-tunable inductance resulting in a flux-tunable JPA resonance frequency. For the generation of squeezed states, our JPAs are operated in the phase-sensitive regime by pumping them at twice their resonance frequencies, $\omega_\mathrm{p} = 2\omega$. The squeezed states are subsequently displaced in quadrature phase space using a cryogenic directional coupler [51]. Each displacement operation encodes a symbol $\alpha_j$ drawn from a codebook following a Gaussian distribution with the fixed variance $\sigma_\mathrm{A}^2$. These symbols constitute Alice's key $\mathcal{K}_\mathrm{A} = \{\alpha_i\}_{i\in\{1,\ldots,N\}}$. Displacement operations are performed either along

the $q$- or $p$-quadrature in phase space, chosen randomly for each symbol but always along the same direction as for the squeezing operations. In order to improve the efficiency and duty cycle of our experiment, we chose to implement the squeezing operation solely along the $q$-quadrature. This restriction is without loss of generality as the quadratures are made to be indistinguishable, i.e., the measured key statistics does not depend on which quadrature is used for squeezing operations.

The indistinguishability of both quadratures ensures a maximal security in our protocol and is obtained by imposing the condition $\sigma_{\mathrm{s}}^2 + \sigma_{\mathrm{A}}^2 = \sigma_{\mathrm{as}}^2$, where $(\sigma_{\mathrm{as}}^2)$ $\sigma_{\mathrm{s}}^2$ denotes the (anti-)squeezed quadrature variances. This condition ensures that Eve is prevented from extracting information on the encoding basis by averaging over the ensemble of Alice's states, forcing Eve to interact with each incoming individual state from Alice. Each displaced squeezed state propagates through the quantum channel under Eve's control, implemented in our experiment with a second cryogenic directional coupler, as illustrated in Fig. 5.3. This directional coupler adds a fixed amount of losses $\varepsilon_{\mathrm{E}}$ to incoming states and a tunable number of coupled noise photons $\bar{n}$. The tunability of the coupled noise is provided by the arbitrary waveform generator (AWG) capable of generating Gaussian noise in a 160 GHz bandwidth as explained in Sec. 4.3. This artificially generated noise is up-converted to the desired gigahertz frequency.

For signal readout, Bob uses a second JPA to perform single quadrature measurements according to the discussion in Sec. 5.1.1. In this work, we refer to this JPA as the *measurement* JPA. The quantum efficiency of the quadrature measurement depends primarily on the added JPA noise, as our JPA is a non-ideal device. This noise is related to intrinsic losses, pump-induced noise [24, 82], and higher-order nonlinearities [73]. Single-shot measurements, ideally implemented with quantum efficiency close to unity, are obtained with a quantum efficiency well above 50 % and without any averaging of measured signals. A single quadrature measurement is performed for each symbol encoded by Alice and results in a measured key for Bob $\mathcal{K}_{\mathrm{B}} = \{\beta_i\}_{i\in\{1,\dots,N\}}$.

In practical implementations, a CV-QKD protocol includes additional post-processing as mentioned in Sec. 3.3. In particular, Bob does not know the encoding basis chosen by Alice. Therefore, Alice and Bob proceed to an additional step, commonly referred to as *sifting*. In this step, Alice discloses which basis she chose once Bob performed all his quadrature measurements, resulting in half the data being discarded. In this work, we assume that Alice's and Bob's bases are always agreeing, which means that Alice squeezes states along the $q$-quadrature and Bob amplifies incoming states along the same quadrature. We account for the sifting using an additional factor 50% in the final secret key rates, a prefactor which is ideally achieved in the asymptotic limit or for a large number of symbols, $N \geq 10^4$. After the sifting step, Alice and Bob implement a classical error correction algorithm that uses either Alice's or Bob's keys as a reference to provide them with a common key. Here, we consider the direct reconciliation (DR) regime, where Alice's key is used as a reference, known to offer a better resilience to the coupled noise $\bar{n}$ as compared to reverse reconciliation, where Bob's key is taken as the reference [117, 227].

### 5.2.2 Quadrature measurement model

In this section, we provide a model describing a single-shot quadrature measurement (SQM) based on the experimental setup introduced in the previous section. This model is of paramount importance for the interpretation of our experiment and serves as the basis of the subsequent data analysis. The general scheme of our CV-QKD implementation setup is shown in Fig. 5.4 and represents a schematic representation of the experimental setup in Fig. 5.3. It consists of one main signal path and two additional paths to account for the signals sent to the two directional couplers. We divide our setup into multiple segments. For each segment, we introduce an

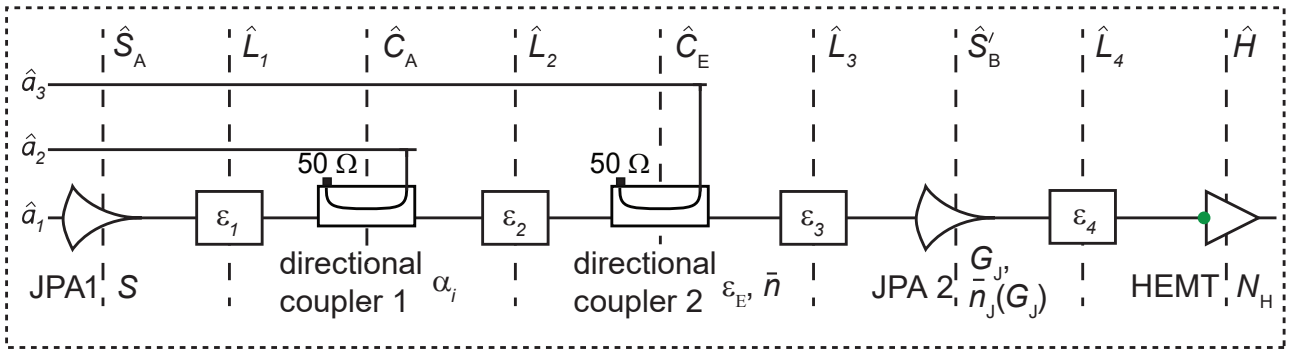


Figure 5.4: Schematic representation of the theoretical model used for describing the experimental implementation of the CV-QKD. For modelling, the experimental setup is split into several segments and consists of three paths. Each segment has either an operation on path signal ($\hat{S}_A$, $\hat{S}'_B$ with associated squeezing level $S$, amplification noise $\bar{n}_J$, and amplification gain $G_J$), between path signals ($\hat{C}_A$ with associated induced displacement $\alpha_i$, $\hat{C}_E$), path loss ($\hat{L}_1$, $\hat{L}_2$, $\hat{L}_3$, $\hat{L}_4$ with associated losses $\varepsilon_i$) or added noise ($\hat{H}$ with associated amplification noise $N_H$). The second directional coupler is characterized by the loss $\varepsilon_E$ and coupled noise photon number $\bar{n}$. For our model, the output state is effectively reconstructed at the input of the HEMT (while accounting for the HEMT noise), indicated by a green dot. Here, we do not show the modes corresponding to a path loss and HEMT noise.

operator acting on the signal modes, denoted $\hat{a}_i$. The modes for the main signal path are denoted $\hat{a}_1$, and the two other paths are denoted as $\hat{a}_2$ and $\hat{a}_3$, respectively. We consider a weak thermal background environment in each segment at a temperature $T$ and we model it as a bosonic mode with an average noise photon number

$$\bar{n}_{\text{th}} = \frac{1}{\exp(\frac{\hbar\omega}{k_B T}) - 1}. \tag{5.17}$$

The squeezing operation implemented by the first JPA, corresponding to Alice, is described by the squeeze operator $\hat{S}_A = \exp[(\xi^* \hat{a}_1^2 - \xi(\hat{a}_1^\dagger)^2)/2]$. This operator is parametrized by a squeezing factor $r_A = |\xi|$ and an angle $\varphi_A = \arg(\xi)$ (with a corresponding squeezing angle $\gamma_A = -\varphi_A/2$), which determines the amplitude and the direction of the squeezing operation. The action of the squeeze operator on a signal mode results in the transformation

$$\hat{S}_A^\dagger \hat{a}_1 \hat{S}_A = \hat{a}_1 \cosh(r_A) - \hat{a}_1^\dagger \sinh(r_A) e^{-2i\varphi_A}. \tag{5.18}$$

Alice performs this squeezing operation along the $q$-quadrature with $\varphi_A = 0$ while a squeezing along the $p$-quadrature would correspond to $\varphi_A = \pi$. For a given symbol $\alpha_i$, each squeezed state is displaced in quadrature phase space by applying the displacement operator $\hat{D}(\alpha_i) = \exp\left(\alpha_i \hat{a}_1^\dagger - \alpha_i^* \hat{a}_1\right)$ resulting in the transformation of an input signal mode $\hat{a}_1$ as

$$\hat{a}_1' = \hat{D}^\dagger(\alpha_i)\, \hat{a}_1 \hat{D}(\alpha_i) = \hat{a}_1 + \alpha_i. \tag{5.19}$$

This displacement operation is realized by the first cryogenic directional coupler, acting as a highly asymmetric beam splitter with a power transmissivity $\tau_A$, described as

$$\hat{C}_A^\dagger(\tau_A) \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix} \hat{C}_A(\tau_A) = \begin{pmatrix} \sqrt{\tau_A}\, \hat{a}_1 + \sqrt{1-\tau_A}\, \hat{a}_2 \\ -\sqrt{1-\tau_A}\, \hat{a}_1 + \sqrt{\tau_A}\, \hat{a}_2 \end{pmatrix}. \tag{5.20}$$

The coupling of $\bar{n}$ noise photons to Alice's signals is performed using the second cryogenic directional coupler which we model with a beam splitter of power transmissivity $\tau_E = 1 - \varepsilon_E$, resulting in

$$\hat{C}_E^\dagger(\varepsilon_E) \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix} \hat{C}_E(\varepsilon_E) = \begin{pmatrix} \sqrt{1-\varepsilon_E}\, \hat{a}_1 + \sqrt{\varepsilon_E}\, \hat{a}_2 \\ -\sqrt{\varepsilon_E}\, \hat{a}_1 + \sqrt{1-\varepsilon_E}\, \hat{a}_2 \end{pmatrix}. \tag{5.21}$$

A path loss in each section of the setup is modelled using a beam splitter model

$$\hat{L}_j^\dagger \hat{a}_1 \hat{L}_j = \sqrt{1-\varepsilon_j}\,\hat{a}_1 + \sqrt{\varepsilon_j}\,\hat{h}_j, \tag{5.22}$$

with $j \in \{1,2,3,4\}$. The bosonic modes $\hat{h}_j$ model the thermal environment with a mean thermal photon number $\bar{n}_{\mathrm{th}}$. Lastly, we describe the phase-sensitive amplification of the measurement JPA (second JPA) using a noisy squeezing operator to account for the amplification noise added by the JPA itself. We introduce a classical complex random variable $\zeta$ to model the added noise such that

$$(\hat{S}'_{\mathrm{B}})^\dagger \hat{a}_1 \hat{S}'_{\mathrm{B}} = (\hat{a}_1 + \zeta)\cosh(r_{\mathrm{B}}) - (\hat{a}_1^\dagger + \zeta^*)\sinh(r_{\mathrm{B}})e^{-2i\varphi_{\mathrm{B}}}, \tag{5.23}$$

where $\zeta$ satisfies $\langle |\zeta|^2 \rangle = \bar{n}_{\mathrm{J}}$, the added JPA noise. We assume an even splitting of the noise between the $q$- and $p$-quadrature, $\langle \mathrm{Re}\,(\zeta)^2 \rangle = \langle \mathrm{Im}\,(\zeta)^2 \rangle = \bar{n}_{\mathrm{J}}/2$, and that $\zeta$ has a zero-mean Gaussian distribution [27]. The noise of the JPA depends on the JPA gain $G_{\mathrm{J}}$ as

$$\bar{n}_{\mathrm{J}}\,(G_{\mathrm{J}}) = \Xi_1\,(G_{\mathrm{J}} - 1)^{\Xi_2}\,, \tag{5.24}$$

where $\Xi_1$ and $\Xi_2$ are phenomenological constants characterizing the noise properties of the JPA [82]. Since we are considering single-shot measurements, we account for the phase-insensitive amplification performed by the HEMT, which we describe as

$$\hat{H}^\dagger \hat{a}_1 \hat{H} = \sqrt{G_{\mathrm{H}}}\,\hat{a}_1 + \sqrt{G_{\mathrm{H}} - 1}\,\hat{h}_{\mathrm{H}}^\dagger. \tag{5.25}$$

Here, $\hat{h}_{\mathrm{H}}$ is a thermal mode describing the added HEMT noise and $G_{\mathrm{H}}$ is the HEMT amplification gain. We note that accounting for this gain would imply that signal moments are reconstructed at the output of the HEMT. In the measurements, we ultimately shift this reconstruction point to its input by rescaling the measured data with the amplification gain. The full protocol implementation is expressed by the operator $\hat{T}$ as

$$\hat{T} = \hat{H}\hat{L}_4\hat{S}'_{\mathrm{B}}\hat{L}_3\hat{C}_{\mathrm{E}}\hat{L}_2\hat{C}_A\hat{L}_1\hat{S}_{\mathrm{A}}. \tag{5.26}$$

We write the overall input state of our experimental setup as

$$\hat{\rho}_{\mathrm{in}} = \hat{\rho}_1 \otimes \hat{\rho}_2 \otimes \hat{\rho}_3, \tag{5.27}$$

where the states $\hat{\rho}_i$ describe the signal in path $i$, with $i \in \{1,2,3\}$. Here, the symbol $\otimes$ denotes a tensor product of density matrices. The input signal in path 1 is modelled as a weak thermal state with a thermal population $\bar{n}_{\mathrm{th}}$. The input signal in the path 2 is described as a strongly displaced thermal state to account for the induced displacement at the first directional coupler. Lastly, the input signal in path 3 corresponds to a strong Gaussian noise with an averaged photon number $\bar{n}_{\mathrm{E}}$, which couples to the second directional coupler. We note that a more complete description of our system would lead to

$$\hat{\rho}_{\mathrm{in}} = \hat{\rho}_1 \otimes \hat{\rho}_2 \otimes \hat{\rho}_3 \otimes \hat{\rho}_{\mathrm{th}}^{\otimes 4} \otimes \hat{\rho}_{\mathrm{H}}, \tag{5.28}$$

where $\hat{\rho}_{\mathrm{th}}$ is a thermal state with an average thermal population $\bar{n}_{\mathrm{th}}$ associated with the path loss operators $\hat{L}_j$ with $j \in \{1,2,3,4\}$. The term $\hat{\rho}_{\mathrm{th}}^{\otimes 4}$ denotes the tensor product of 4 copies of the density matrix $\hat{\rho}_{\mathrm{th}}$. Additionally, $\hat{\rho}_{\mathrm{H}}$ is a thermal state associated with the HEMT operator $\hat{H}$. In the following expressions for displacement vectors and covariance matrices, we implicitly do not consider these additional modes in our quantum model in order to keep the dimension of the system small. We emphasize that the results of our model remain entirely unchanged by this truncation. Therefore, we use Eq. (5.27) to describe our system.

The final output state after the HEMT can be expressed as

$$\hat{\rho}_{\mathrm{out}} = \hat{T}\hat{\rho}_{\mathrm{in}}\hat{T}^\dagger. \tag{5.29}$$

The moments of the output signals $\hat{b}_i$ (signals at the output of our device chain) can be calculated as

$$\begin{pmatrix} \langle (\hat{b}_1^\dagger)^n \hat{b}_1^m \rangle \\ \langle (\hat{b}_2^\dagger)^n \hat{b}_2^m \rangle \\ \langle (\hat{b}_3^\dagger)^n \hat{b}_3^m \rangle \end{pmatrix} = \begin{pmatrix} \mathrm{Tr}((\hat{a}_1^\dagger)^n \hat{a}_1^m \hat{\rho}_{\mathrm{out}}) \\ \mathrm{Tr}((\hat{a}_2^\dagger)^n \hat{a}_2^m \hat{\rho}_{\mathrm{out}}) \\ \mathrm{Tr}((\hat{a}_3^\dagger)^n \hat{a}_3^m \hat{\rho}_{\mathrm{out}}) \end{pmatrix}. \tag{5.30}$$

Experimentally, we restrict our measurements to the fourth order, i.e., $m+n \leq 4$ with $(m,n) \in \mathbb{N}^2$. With the complementary quadrature operators

$$\hat{q}_i = \frac{\hat{b}_i + \hat{b}_i^\dagger}{2}, \quad \hat{p}_i = \frac{\hat{b}_i - \hat{b}_i^\dagger}{2i}, \tag{5.31}$$

we define a vector $\hat{x} = (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2, \hat{q}_3, \hat{p}_3)^{\mathrm{T}}$. Considering that we use Gaussian states, we fully describe them using their displacement vector $\mathbf{d}$ and covariance matrix $\mathbf{V}$. According to Eqs. 5.27, 5.31, for the input state corresponding to $\hat{\rho}_{\mathrm{in}}$, we obtain

$$\begin{aligned} \mathbf{d}_{\mathrm{in}} &= \left(0, 0, \sqrt{\bar{n}_{\mathrm{d}}}\cos(\varphi_{\mathrm{d}}), \sqrt{\bar{n}_{\mathrm{d}}}\sin(\varphi_{\mathrm{d}}), 0, 0\right)^{\mathrm{T}}, \\ \mathbf{V}_{\mathrm{in}} &= \frac{1}{4}\begin{pmatrix} (1+2\bar{n}_{\mathrm{th}})\mathbf{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & (1+2\bar{n}_{\mathrm{th}})\mathbf{I}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{0}_2 & (1+2\bar{n}_{\mathrm{E}})\mathbf{I}_2 \end{pmatrix}. \end{aligned} \tag{5.32}$$

Here, $\bar{n}_{\mathrm{d}}$ is the displacement photon number and $\varphi_{\mathrm{d}}$ the corresponding displacement angle. For a given symbol of Alice, $\alpha_i$, we have $\bar{n}_{\mathrm{d}} = |\alpha_i|^2/(1-\tau_{\mathrm{A}})$ and $\varphi_{\mathrm{d}} = 0$ due to Alice choosing to encode the displacement along the $q$-quadrature. The squeezing operation for Alice's JPA is modelled by

$$\mathbf{J}_{\mathrm{A}} = \mathbf{R}_{\mathrm{A}}\mathbf{S}_{\mathrm{A}}\mathbf{R}_{\mathrm{A}}^{\mathrm{T}},\ \mathbf{S}_{\mathrm{A}} = \begin{pmatrix} e^{-r_{\mathrm{A}}} & 0 & 0 & 0 & 0 & 0 \\ 0 & e^{r_{\mathrm{A}}} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},\ \mathbf{R}_{\mathrm{A}} = \begin{pmatrix} \cos(\gamma_{\mathrm{A}}) & \sin(\gamma_{\mathrm{A}}) & 0 & 0 & 0 & 0 \\ -\sin(\gamma_{\mathrm{A}}) & \cos(\gamma_{\mathrm{A}}) & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{5.33}$$

The beam splitter operations are expressed as

$$\mathbf{C}_{\mathrm{A}} = \begin{pmatrix} \sqrt{\tau_{\mathrm{A}}}\,\mathbf{I}_2 & \sqrt{1-\tau_{\mathrm{A}}}\,\mathbf{I}_2 & \mathbf{0}_2 \\ -\sqrt{1-\tau_{\mathrm{A}}}\,\mathbf{I}_2 & \sqrt{\tau_{\mathrm{A}}}\,\mathbf{I}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{I}_2 \end{pmatrix},\ \mathbf{C}_{\mathrm{E}} = \begin{pmatrix} \sqrt{1-\varepsilon_{\mathrm{E}}}\,\mathbf{I}_2 & \mathbf{0}_2 & \sqrt{\varepsilon_{\mathrm{E}}}\,\mathbf{I}_2 \\ \mathbf{0}_2 & \mathbf{I}_2 & \mathbf{0}_2 \\ -\sqrt{\varepsilon_{\mathrm{E}}}\,\mathbf{I}_2 & \mathbf{0}_2 & \sqrt{1-\varepsilon_{\mathrm{E}}}\,\mathbf{I}_2 \end{pmatrix}. \tag{5.34}$$

The losses are described using two matrices

$$\mathbf{L}_j = \begin{pmatrix} \sqrt{1-\varepsilon_j}\,\mathbf{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{I}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{I}_2 \end{pmatrix},\ \mathbf{N}_j = \frac{1}{4}(1+2\bar{n}_{\mathrm{th}}) \begin{pmatrix} \varepsilon_j\mathbf{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{I}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{I}_2 \end{pmatrix}. \tag{5.35}$$

Lastly, the phase-sensitive amplification of the measurement JPA is described by

$$\mathbf{J}_{\mathrm{B}} = \mathbf{R}_{\mathrm{B}}\mathbf{S}_{\mathrm{B}}\mathbf{R}_{\mathrm{B}}^{\mathrm{T}},\ \mathbf{S}_{\mathrm{B}} = \begin{pmatrix} \frac{1}{\sqrt{G_{\mathrm{J}}}} & 0 & 0 & 0 & 0 & 0 \\ 0 & \sqrt{G_{\mathrm{J}}} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},\ \mathbf{R}_{\mathrm{B}} = \begin{pmatrix} \cos(\gamma_{\mathrm{B}}) & \sin(\gamma_{\mathrm{B}}) & 0 & 0 & 0 & 0 \\ -\sin(\gamma_{\mathrm{B}}) & \cos(\gamma_{\mathrm{B}}) & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \tag{5.36}$$

with the JPA added noise

$$\mathbf{N}_{\mathrm{J}} = \frac{\bar{n}_{\mathrm{J}}}{2}\begin{pmatrix} \mathbf{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 \end{pmatrix}. \tag{5.37}$$

The phase-insensitive amplification performed by the HEMT is modelled as

$$\mathbf{H} = \begin{pmatrix} \sqrt{G_{\mathrm{H}}}\mathbf{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{I}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{I}_2 \end{pmatrix}, \tag{5.38}$$

with the HEMT added noise

$$\mathbf{N}_{\mathrm{H}} = N_{\mathrm{H}}\begin{pmatrix} \mathbf{I}_2 & \mathbf{0}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{0}_2 & \mathbf{0}_2 \end{pmatrix}. \tag{5.39}$$

By defining the sequence

$$\mathbf{T} = \mathbf{H}\mathbf{L}_4\mathbf{J}_{\mathrm{B}}\mathbf{L}_3\mathbf{C}_{\mathrm{E}}\mathbf{L}_2\mathbf{C}_{\mathrm{A}}\mathbf{L}_1\mathbf{J}_{\mathrm{A}}, \tag{5.40}$$

the displacement vector and covariance matrix of the final state, $\hat{\rho}_{\mathrm{out}}$, can be expressed as

$$\mathbf{d}_{\mathrm{out}} = \mathbf{T}\mathbf{d}_{\mathrm{in}},\ \mathbf{V}_{\mathrm{out}} = \mathbf{T}\mathbf{V}_{\mathrm{in}}\mathbf{T}^{\mathrm{T}} + \mathbf{N}_{\mathrm{out}}. \tag{5.41}$$

Here, the matrix $\mathbf{N}_{\mathrm{out}}$ represents the total noise of the protocol implementation and can be calculated by chaining the different losses and amplification noise contributions. We find the expressions

$$\begin{aligned} \mathbf{N}_{\mathrm{out}} &= \mathbf{H}(\mathbf{N}_{\mathrm{H}} + \mathbf{N}_4)\mathbf{H}^{\mathrm{T}} + \mathbf{M}_4(\mathbf{N}_{\mathrm{J}} + \mathbf{N}_3)\mathbf{M}_4^{\mathrm{T}} + \mathbf{M}_3\mathbf{N}_2\mathbf{M}_3^{\mathrm{T}} + \mathbf{M}_2\mathbf{N}_1\mathbf{M}_2^{\mathrm{T}}, \\ \mathbf{M}_2 &= \mathbf{H}\mathbf{L}_4\mathbf{J}_{\mathrm{B}}\mathbf{L}_3\mathbf{C}_{\mathrm{E}}\mathbf{L}_2\mathbf{C}_{\mathrm{A}}, \\ \mathbf{M}_3 &= \mathbf{H}\mathbf{L}_4\mathbf{J}_{\mathrm{B}}\mathbf{L}_3\mathbf{C}_{\mathrm{E}}, \\ \mathbf{M}_4 &= \mathbf{H}\mathbf{L}_4\mathbf{J}_{\mathrm{B}}. \end{aligned} \tag{5.42}$$

Based on our model in Eq. (5.41), we can describe the result of individual SQMs performed by Bob by computing the mean value and variance of the quadrature amplified by phase-sensitive amplification. This quadrature can be readily extracted from the first two diagonal elements of $\mathbf{V}_{\mathrm{out}}$. For a symbol $\alpha_i$ of Alice, we obtain from our model that Bob's individual SQM, resulting in a measured symbol $\beta_i$, can be described by a Gaussian random variable with mean $\mu_{\mathrm{B|A}}$ and variance $\sigma^2_{\mathrm{B|A}}$. In order to write their expression in a compact analytical form, we introduce the notations

$$\tau_j = 1 - \varepsilon_j, \text{ for } j \in \{1,2,3,4\}, \text{ and } \alpha'_i = \alpha_i/\sqrt{\tau_1\,\tau_{\mathrm{A}}}. \tag{5.43}$$

Using Eqs. 5.41 and 5.43, we obtain

$$\mu_{\mathrm{B|A}} = \sqrt{G_{\mathrm{H}}}\sqrt{G_{\mathrm{J}}}\sqrt{\tau_{\mathrm{tot}}}\alpha'_i = \sqrt{G_{\mathrm{H}}}\sqrt{G_{\mathrm{J}}}\,\beta_i,\ \sigma^2_{\mathrm{B|A}} = G_{\mathrm{H}}\left[G_{\mathrm{J}}\left(\sigma^2_{\mathrm{n}} + N_{\mathrm{X}}\right)\right], \tag{5.44}$$

where we have defined

$$\begin{gathered} \sigma^2_{\mathrm{n}} = \tau_{\mathrm{tot}}\sigma^2_{\mathrm{s}} + \frac{1}{4}\tau_{\mathrm{th}}\left(1 + 2\bar{n}_{\mathrm{th}}\right) + \tau_3\tau_4\left(\frac{1}{4}\varepsilon_{\mathrm{E}} + \bar{n}\right), \\ N_{\mathrm{X}} = \tau_4\frac{\bar{n}_{\mathrm{J}}}{2} + \frac{N_{\mathrm{H}}}{G_{\mathrm{J}}},\ \tau_{\mathrm{tot}} = \tau_1\tau_{\mathrm{A}}\tau_2\tau_{\mathrm{E}}\tau_3\tau_4,\ \tau_{\mathrm{th}} = \tau_3\tau_4\tau_{\mathrm{E}}\left(1 - \tau_1\tau_{\mathrm{A}}\tau_2\right) + \tau_4\varepsilon_3, \text{ and } \bar{n} = \frac{\varepsilon_{\mathrm{E}}\bar{n}_{\mathrm{E}}}{2}. \end{gathered} \tag{5.45}$$

We note that during measurements, the value of $\beta_i = \sqrt{\tau_{\mathrm{tot}}}\,\alpha'_i$ can be computed by rescaling the measured symbols by $\sqrt{G_{\mathrm{H}}}\sqrt{G_{\mathrm{J}}}$. The individual values of $G_{\mathrm{H}}$ and $G_{\mathrm{J}}$ are obtained from

calibration measurements explained in Sec. 4.3. To compute the overall statistics of Bob's key, we write that the indistinguishability between the two quadratures imposes the condition

$$\tau_1\,\tau_\mathrm{A}\sigma_\mathrm{s}^2+\sigma_\mathrm{A}^2=\tau_1\,\tau_\mathrm{A}\sigma_\mathrm{as}^2 \quad\Longleftrightarrow\quad \sigma_\mathrm{s}^2+\sigma_{\mathrm{A}'}^2=\sigma_\mathrm{as}^2. \tag{5.46}$$

The mean and variance of the distribution of Bob's key can be viewed as a convolution between the Gaussian modulation of Alice's symbols and the Gaussian quadrature distribution of Bob's individual states. As such, we compute Bob's key probability density function $f_\mathrm{B}$ as

$$f_\mathrm{B}\left(\beta_i\right)=\int_{-\infty}^{\infty} f_{\mathrm{B|A}}\left(\beta_i|\alpha_i\right) f_\mathrm{A}\left(\alpha_i\right) d(\alpha_i), \tag{5.47}$$

where $f_{\mathrm{B|A}}$ is the the conditional probability density function of Bob's individual SQMs and $f_\mathrm{A}$ is the probability density function of Alice's Gaussian distribution. As a result, Bob's measured key has also a Gaussian distribution with a mean $\mu_\mathrm{B}$ and a variance $\sigma_\mathrm{B}^2$ given by

$$\mu_\mathrm{B}=0,\,\sigma_\mathrm{B}^2=G_\mathrm{H}\left[G_\mathrm{J}\left(\tau_\mathrm{tot}\sigma_\mathrm{as}^2+\frac{1}{4}\tau_\mathrm{th}\left(1+2\bar{n}_\mathrm{th}\right)+\tau_3\tau_4\left(\frac{1}{4}\varepsilon_\mathrm{E}+\bar{n}\right)+N_\mathrm{X}\right)\right]. \tag{5.48}$$

We emphasize that the experimentally measured values are rescaled by the gain values $G_\mathrm{H}$ and $G_\mathrm{J}$ during data analysis of Bob's keys.

## 5.3 Single-shot measurements and correlations

In this section, we present measurement results of our implementation of the squeezed-state CV-QKD protocol in the microwave domain. In Sec. 5.3.1, we show extracted mutual information from our communicated keys between Alice and Bob with their associated Holevo quantity, which we detail in Sec. 5.3.3. Sec. 5.3.2 additionally presents statistical tests performed to verify the Gaussianity of our measured data. The corresponding secret keys and the analysis of finite-size effects are presented in Sec. 5.3.4. Based on our measurement results, we investigate in Sec. 5.3.5 the maximal communication distance that could be achieved in a future practical implementations, making use of commercially available microwave technology for cryogenic and classical systems. In a second step, we discuss potential improvements and limitations of our protocol implementation in Sec. 5.3.6. Lastly, we mention two additional experiments of the CV-QKD protocol based on the same experimental setup. First, we investigate in Sec. 5.3.7 the relation between the mutual information and the signal-to-noise ratio and show that our experimental results agree well with our theoretical prediction. Second, in Sec. 5.3.8 we present a time multiplexing method that can significantly improve experimental secret key rates.

### 5.3.1 Mutual information measurement

In this section, we present our results regarding the mutual information (MI) extracted from our experiments. These results have been published in ref. 53. We use the SQM model presented in the previous section to describe the strong phase-sensitive amplification measurements performed by Bob. We expect a measured quadrature in the $I/Q$ phase space and a corresponding amplified quadrature in the $q/p$ phase space to be related via the total amplification gain with additional amplification noise. According to the formalism presented in Sec. 5.1.1, in the case of a JPA amplification gain $G_\mathrm{J}\gg 1$, the information about the deamplified quadrature becomes inaccessible from SQMs as opposed to the amplified quadrature. Experimentally, we characterize the quadrature amplification noise $N_\mathrm{x}$ using the quadrature quantum efficiency defined

| parameters / run | $\sigma_s^2$ | $\sigma_{as}^2$ | $\sigma_A^2$ | $\eta(\%)$ | $\varepsilon_0$ | $\varepsilon_1$ | $\varepsilon_2$ | $\varepsilon_3$ | $\varepsilon_4$ | $\tau_A$ |
|---|---|---|---|---|---|---|---|---|---|---|
| 1st run | 3.6 | 7.1 | 1.3 | 65 | 0.147 | 0.109 | 0.055 | 0.069 | 0.245 | 0.989 |
| 2nd run | 3.6 | 7.6 | 1.36 | 68 | 0.147 | 0.109 | 0.055 | 0.069 | 0.245 | 0.989 |

Table 5.1: Summary of the different experimental parameters used in both measurement runs. The values of the variances are given in dB, and the quantum efficiency is given in percent. The listed parameters are used in the SQM model in Eqs. 5.48,5.53.

as $\eta = 1/(1+2N_x)$ [73]. We operate the measurement JPA in the phase-sensitive regime with an amplification gain $G_J = 19.1(4)\,\mathrm{dB}$ and quadrature quantum efficiency $\eta = 65(2)$ %. For each encoded symbol of Alice $\alpha_i$, we select from our measured time trace a single filtered and demodulated $I_i$ quadrature point. This data point is related to the extracted symbol of Bob as $\beta_i = \kappa(I_i + n_i)$ with $\kappa$ the PNCF and $n_i$ a total measurement noise, according to our analysis in Sec. 5.1.2.

It is important to note that our digital FIR filters use a window of 90 $I/Q$ points to perform the digital filtering as mentioned in Sec. 4.1.3. This implies that completely statistically independent $I/Q$ points can be selected every 7.2 µs. All measured data points $\{\beta_i\}_{i\in[1,N]}$ form Bob's measured key. In Fig. 5.5 (b), we show an exemplary histogram of single-shot measurements of Bob's symbols, normalized to correspond to a probability density function. Superimposed to the histogram, we plot the quadrature distribution obtained from the model according to Eq. (5.48). We observe a good agreement between our model and the measured data. In order to precisely quantify the matching, we note, as explained in the previous section, that Bob's key is described with a zero mean Gaussian distribution which depends on the quantum channel losses $\varepsilon_e$ and coupled noise photons $\bar{n}$. However, additional experimental parameters play a role in the final measured variance $\sigma_B^2$, namely the squeezing (anti-squeezing) variance $\sigma_s^2$ ($\sigma_{as}^2$), the setup losses, and the amplification noise $N_X$. These quantities are extracted from calibration measurements according to Sec. 4.3 and are assumed to be known quantities in the remaining of our analysis. In Tab. 5.1, we provide a summary of the extracted parameters. Here, we also show the experimental parameters used for a 2nd run where we have improved the mutual information and associated security. We detail the changes from the 1st run in Sec. 5.3.4.

We perform our measurements for the constant squeezing level of $S = 3.6\,\mathrm{dB}$ corresponding to the squeezing variance of $\sigma_s^2 = 0.11$. For the setup losses, we perform a 2D Planck spectroscopy [197](see Sec. 4.3.1) and extract the experimental value of total losses $\varepsilon_{2D} = 3.06\,\mathrm{dB}$. In parallel, we carefully estimate the losses of our experimental setup, resulting in the loss estimation of $\varepsilon = 2.29\,\mathrm{dB}$. The observed discrepancy between our loss estimation and the extracted total losses is attributed to additional losses from our JPA sample box. Assuming a symmetric loss between the boxes, we consider an additional loss contribution of $\varepsilon_{box} = 0.39\,\mathrm{dB}$. The total estimated loss values are shown in Tab. 5.1. We note that during our measurements, we make sure that the measurement JPA does not enter compression for an interval of the Gaussian distribution of Alice of $3\sigma_A$, covering 99.73% of Alice's symbols. Additionally, the power corresponding to the outliers above this $3\sigma_A$ interval is primarily only slightly above the compression threshold of the measurement JPA. As a result, the fraction of symbols that results in a non-Gaussian state and statistics after amplification by the measurement JPA are not statistically significant. In addition, in Fig. 5.5 (a) we show an exemplary evolution of the Wigner function of a quantum state at different steps of our protocol. We observe that an initially displaced squeezed state generated on Alice's side is enlarged by the noise induced via the second directional coupler, representing Eve's quantum channel. Finally, the Wigner function is strongly amplified in the phase-sensitive regime, resulting in an elongated Wigner function along the $q$-quadrature. Note that the initial displacement, encoding a symbol $\alpha_i$ of

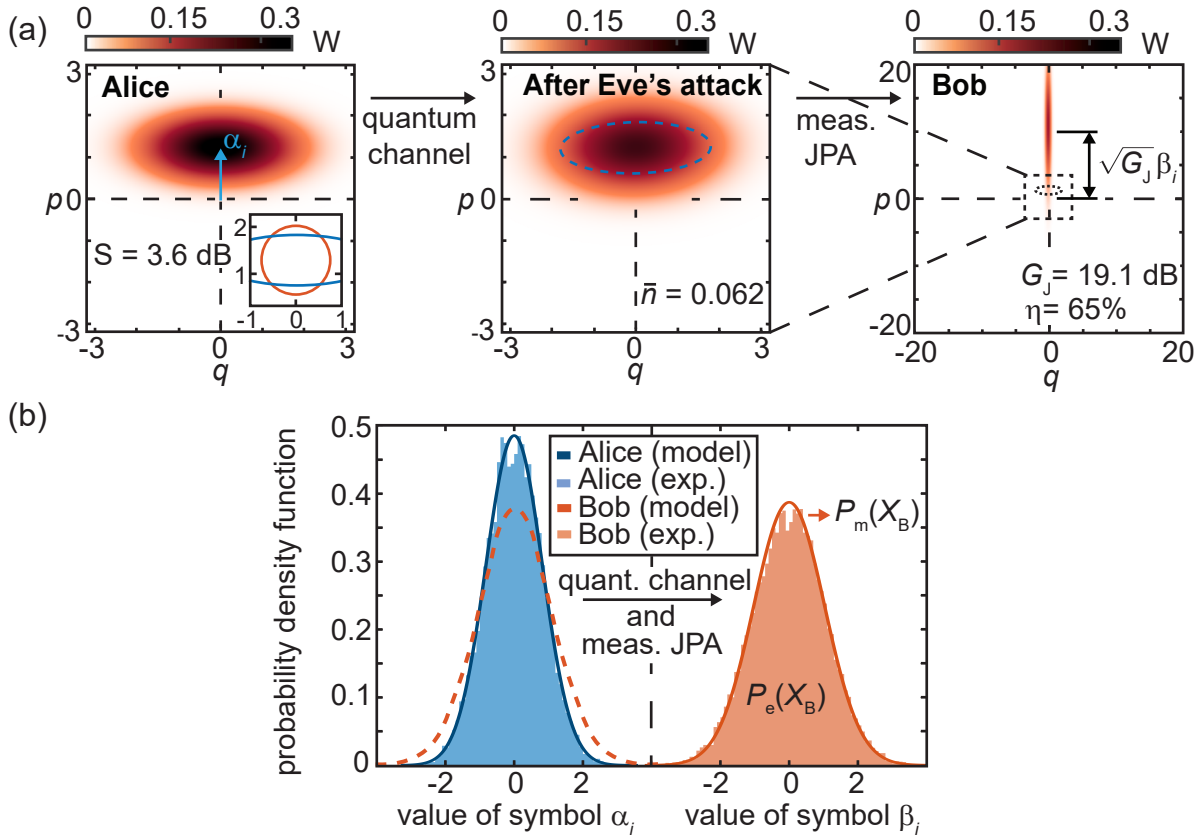


Figure 5.5: Tomography and single-shot measurement histograms of displaced squeezed microwave states. (a) Exemplary evolution of the reconstructed Wigner function of a quantum key symbol, starting from its preparation at Alice, followed by propagation through the quantum channel while being exposed to losses and noise (Eve's attack), finishing at Bob with a strong phase-sensitive amplification. The inset of the left Wigner function plot shows the 1/e contours for an ideal vacuum (red circle) and experimental squeezed state (blue ellipsoid), indicating squeezing below the level of vacuum fluctuations. (b) Exemplary measured histograms for Alice's and Bob's key symbols. For comparison with the measured probability distribution $P_{\mathrm{e}}(X_{\mathrm{B}})$, we plot the result of our quadrature model (solid lines). The latter results in a zero-mean Gaussian probability distribution $P_{\mathrm{m}}(X_{\mathrm{B}})$, whose variances are obtained from the calibration measurements presented in Sec. 4.3.

Alice, is strongly scaled by a factor $\sqrt{G_{\mathrm{J}}}$. This factor is removed during data analysis to rescale Bob's symbols.

Following these measurements, Bob possesses a set of symbols correlated to the initial set sent by Alice. Remarkably, the sifting step of the protocol leaves the measured mutual information and calculated Holevo quantity unchanged [154]. We characterize Alice's and Bob's correlations by computing the MI between Alice's encoded key $\mathcal{K}_{\mathrm{A}}$ and the corresponding key $\mathcal{K}_{\mathrm{B}}$ measured by Bob. For continuous-variable states, the mutual information between Alice's and Bob's keys can be written using the differential entropy defined in Eq. (2.108) as

$$I\left(\mathcal{K}_{\mathrm{A}}\colon \mathcal{K}_{\mathrm{B}}\right) = h\left(\mathcal{K}_{\mathrm{B}}\right) - h\left(\mathcal{K}_{\mathrm{B}}|\mathcal{K}_{\mathrm{A}}\right), \tag{5.49}$$

where $h$ is the differential entropy and $h\left(\mathcal{K}_{\mathrm{B}}|\mathcal{K}_{\mathrm{A}}\right)$ expresses the differential entropy of Bob's key conditioned on the values taken by Alice's key. Importantly, a zero MI indicates no correlations between the two keys $\mathcal{K}_{\mathrm{A}}$ and $\mathcal{K}_{\mathrm{B}}$. For a continuous variable system, the MI is unbounded in theory, but it is limited in practice by experimental parameters and the efficiency of our amplification chain. From Eq. (2.112), the differential entropy of a Gaussian variable $X$, in the units of bits, simplifies to

$$h\left(X\right) = \frac{1}{2}\log_2\left(2\pi e\,\sigma_{\mathrm{X}}^2\right), \tag{5.50}$$

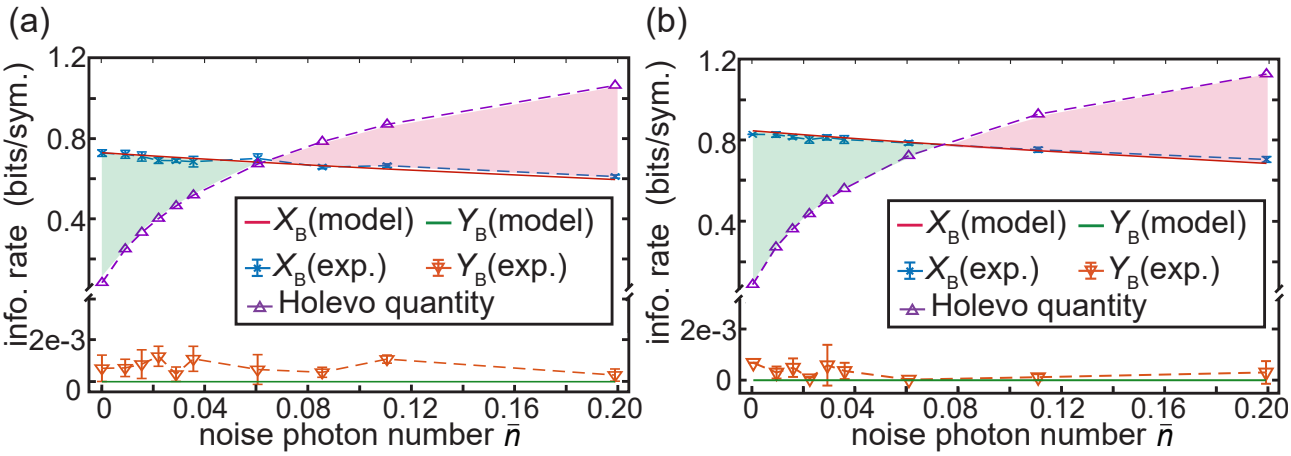


Figure 5.6: Single-shot measurements of the MI with associated Holevo quantity. The MI between Alice's and Bob's keys for the amplified (deamplified) quadrature $X_\mathrm{B}$ ($Y_\mathrm{B}$) as a function of the coupled noise photon number $\bar{n}$ is shown in panel (a) for the 1$^{\mathrm{st}}$ run and in panel (b) the 2$^{\mathrm{nd}}$ run. We additionally show the MI computed from our model according to Eq. (5.53) using the measured experimental parameters. Lastly, we show the corresponding Holevo quantity for both. The shaded green (red) area on the left (right) represents the region where the MI is larger (smaller) than the Holevo quantity, resulting in a unconditionally secure (insecure) communication. The error bars represent the standard deviation of the measurements. Lastly, we show the corresponding Holevo quantity.

where $\sigma^2_\mathrm{X}$ is the variance of the random variable $X$. Based on the formalism of conditional Gaussian variables [154], the variance of Bob's key conditioned on the values of Alice's key can be expressed as

$$\sigma^2_{\mathrm{B|A}} = \sigma^2_\mathrm{B} - \frac{\mathrm{cov}(\mathcal{K}_\mathrm{A}, \mathcal{K}_\mathrm{B})^2}{\sigma^2_\mathrm{A}}, \tag{5.51}$$

where $\mathrm{cov}(\mathcal{K}_\mathrm{A}, \mathcal{K}_\mathrm{B})$ is the classical covariance between Alice's key $\mathcal{K}_\mathrm{A}$ and Bob's key $\mathcal{K}_\mathrm{B}$. This results in an expression for the mutual information purely based on the statistics between Alice and Bob's key

$$I\left(\mathcal{K}_\mathrm{A} \colon \mathcal{K}_\mathrm{B}\right) = \frac{1}{2}\log_2\left(\frac{\sigma^2_\mathrm{A}\,\sigma^2_\mathrm{B}}{\sigma^2_\mathrm{A}\,\sigma^2_\mathrm{B} - \mathrm{cov}(\mathcal{K}_\mathrm{A}, \mathcal{K}_\mathrm{B})^2}\right) = \frac{1}{2}\log_2\left(1 + \frac{\mathrm{cov}(\mathcal{K}_\mathrm{A}, \mathcal{K}_\mathrm{B})^2}{\sigma^2_\mathrm{A}\,\sigma^2_\mathrm{B} - \mathrm{cov}(\mathcal{K}_\mathrm{A}, \mathcal{K}_\mathrm{B})^2}\right). \tag{5.52}$$

Here, we define the signal-to-noise ratio as $\mathrm{SNR} = \mathrm{cov}(\mathcal{K}_\mathrm{A}, \mathcal{K}_\mathrm{B})^2/(\sigma^2_\mathrm{A}\,\sigma^2_\mathrm{B} - \mathrm{cov}(\mathcal{K}_\mathrm{A}, \mathcal{K}_\mathrm{B})^2)$, representing the ratio between a signal variance and a noise variance. The last result offers a direct practical implementation as it provides a direct computation of the MI from our measured keys. We compute the classical variances and covariances between Alice's prepared keys and the corresponding keys measured by Bob. Using Eqs. 5.44 and 5.48, we obtain the corresponding mutual information from our quadrature distribution model

$$\begin{aligned} I\left(\mathcal{K}_\mathrm{A} \colon \mathcal{K}_\mathrm{B}\right) &= \frac{1}{2}\log_2\left(\frac{\sigma^2_\mathrm{B}}{\sigma^2_{\mathrm{B|A}}}\right) \\ &= \frac{1}{2}\log_2\left(1 + \frac{\tau_\mathrm{tot}\sigma^2_\mathrm{A}}{\tau_\mathrm{tot}\sigma^2_\mathrm{s} + \tau_\mathrm{th}\left(1 + 2\bar{n}_\mathrm{th}\right)/4 + \tau_3\tau_4\left(\varepsilon_\mathrm{E}/4 + \bar{n}\right) + \tau_4\bar{n}_\mathrm{J}/2 + N_\mathrm{H}/G_\mathrm{J}}\right). \end{aligned} \tag{5.53}$$

In Fig. 5.6, we plot the resulting MI extracted from measurements of the amplified quadrature. Additionally, we extract a MI for the deamplified quadrature. We note that the MI is insensitive to any linear rescaling of either Alice's or Bob's keys and, therefore, captures core

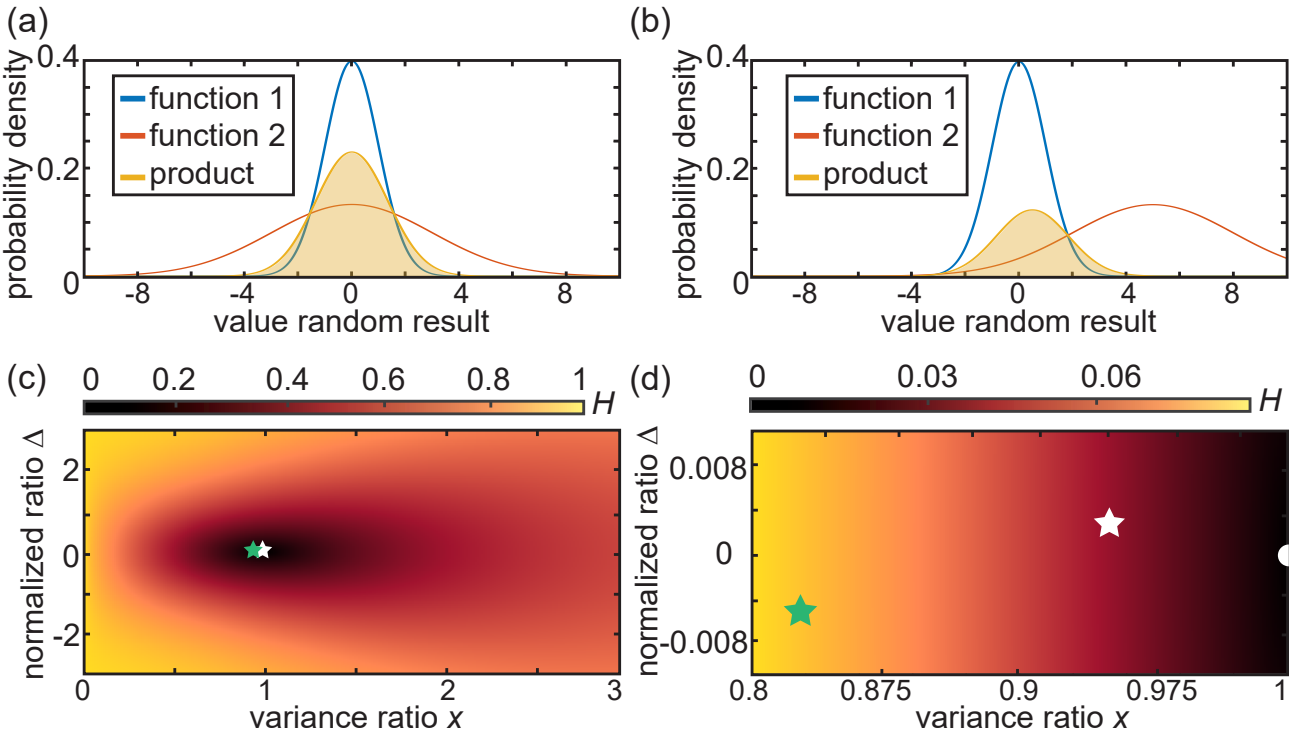


Figure 5.7: Illustration of the Bhattacharyya coefficient and experimentally computed Hellinger distances. Comparisons of exemplary Gaussian distributions are shown. In panel (a), a Gaussian distribution (blue) is used as a reference and is compared to a second similar distribution (orange), resulting in a large overlap depicted by the shaded area. In panel (b), the second distribution (orange) is less similar to the reference distribution (blue), resulting in a smaller shaded area. (c) Hellinger distance according to Eqs. 5.56 and 5.57 as a function of ratios $\Delta$ and $x$. The average values for the 1st run and 2nd run are shown by the star symbols. (d) Magnified view of the plot in panel (c). The yellow star corresponds to the 1st run with $\Delta = 0.003(5)$ and $x = 0.94(1)$. The green star corresponds to the 2nd run with $\Delta = -0.005(6)$ and $x = 0.84(1)$. The optimal point is shown with a white semicircle.

correlations between their datasets. More precisely, we write the SNR using Eq. (5.52) and imagine Alice would rescale her prepared key ensemble $\mathcal{K}_\mathrm{A}$ by a constant $C_\mathrm{A}$ and Bob would rescale his measured key ensemble $\mathcal{K}_\mathrm{B}$ by a constant $C_\mathrm{B}$. By linearity of the covariance, it follows that the rescaled SNR is given by

$$\mathrm{SNR}' = \frac{C_\mathrm{A}^2 C_\mathrm{B}^2 \,\mathrm{cov}(\mathcal{K}_\mathrm{A}, \mathcal{K}_\mathrm{B})^2}{C_\mathrm{A}^2 C_\mathrm{B}^2 \,\sigma_\mathrm{A}^2 \,\sigma_\mathrm{B}^2 - C_\mathrm{A}^2 C_\mathrm{B}^2 \,\mathrm{cov}(\mathcal{K}_\mathrm{A}, \mathcal{K}_\mathrm{B})^2} = \frac{\mathrm{cov}(\mathcal{K}_\mathrm{A}, \mathcal{K}_\mathrm{B})^2}{\sigma_\mathrm{A}^2 \,\sigma_\mathrm{B}^2 - \mathrm{cov}(\mathcal{K}_\mathrm{A}, \mathcal{K}_\mathrm{B})^2} = \mathrm{SNR}. \tag{5.54}$$

This result implies that computed SNR, and, in turn, the mutual information calculated from the measured symbols are independent of the constants $C_\mathrm{A}$ and $C_\mathrm{B}$. In particular, they are insensitive to any rescaling of the measured I/Q points by a specific value of the PNCF, $\kappa$. The latter is the largest source of uncertainty in our measurements. For the measured SNRs, the main uncertainty originates from statistical uncertainty (due to the finite number of symbols) and the stability of experimental devices. For the amplified quadrature, we observe a clearly nonzero MI, indicating strong correlations between Alice's and Bob's keys, in agreement with our quadrature model. Conversely, we observe a nearly zero MI for the deamplified quadrature, demonstrating an almost complete loss of information, as expected from the Heisenberg principle for conjugate variables. We note that from the SQM model, we expect a near-zero MI for the deamplified quadrature, as only noise can be measured for this quadrature.

The accuracy of our model is quantified using the Bhattacharyya coefficient, $\mathcal{B}$, [228], which evaluates the matching between measured quadrature distributions and our model predictions.

For continuous variables, the Bhattacharyya coefficient, $\mathcal{B}$, is defined as

$$\mathcal{B}(P_1, P_2) = \int_{\mathcal{D}} \sqrt{P_1(x)\, P_2(x)}\, dx, \tag{5.55}$$

where $P_1$ and $P_2$ are two probability density functions and $\mathcal{D}$ is a common domain of definition. In the case of Gaussian random variables where the domain of definition is the set of real numbers $\mathbb{R}$, the Bhattacharyya coefficient takes the simple form

$$\mathcal{B}(P_1, P_2) = \sqrt{\frac{2\sigma_1\sigma_2}{\sigma_1^2+\sigma_2^2}} \exp\left[-\frac{1}{4}\frac{(\mu_1-\mu_2)^2}{\sigma_1^2+\sigma_2^2}\right] = \sqrt{\frac{2}{x^2+x^{-2}}} \exp\left(\frac{-\Delta^2}{4(1+x^2)}\right), \tag{5.56}$$

where $\mu_1$ and $\mu_2$ are the mean values of the Gaussian distributions $P_1$ and $P_2$, respectively. Similarly, $\sigma_1$ and $\sigma_2$ are the standard deviations of the Gaussian distributions. To illustrate the behavior of the Bhattacharyya coefficient, we introduce the parameters $x \coloneqq \sigma_2/\sigma_1$ and $\Delta \coloneqq (\mu_1-\mu_2)/\sigma_1$. By definition, we have $0 \leq \mathcal{B} \leq 1$. implying that the coefficient $\mathcal{B}$ quantifies an overlap between the distributions $P_1$ and $P_2$. The Bhattacharyya coefficient can be used to define a proper metric for probability density functions, called the Hellinger distance

$$H(P_1, P_2) = \sqrt{1-\mathcal{B}(P_1, P_2)}, \qquad 0 \leq H \leq 1. \tag{5.57}$$

Since $H$ is a distance, it fulfils the triangular inequality and, in particular, we have the property $H(P_1, P_2) = 0 \Leftrightarrow P_1 = P_2$. It follows that the smaller the Hellinger distance, the more similar the probability density functions $P_1$ and $P_2$ are to each other. Equivalently, the Bhattacharyya coefficient close to unity indicates that the probability density functions $P_1$ and $P_2$ are similar. The principle of the Bhattacharyya coefficient with the associated measured Hellinger distances is shown in Fig. 5.7. Considering that our measured keys follow Gaussian distributions since all physical states and quantum channels involved in the experiment being Gaussian, we evaluate the relevant Bhattacharyya coefficients with the associated Hellinger distances using Eqs. 5.56 and 5.57. In this work, we obtain for the 1$^{\text{st}}$ run the coefficient $\mathcal{B}(P_{\text{e}}(X_{\text{B}}), P_{\text{m}}(X_{\text{B}})) = 99.98(1)\,\%$ with an associated $H(P_{\text{e}}(X_{\text{B}}), P_{\text{m}}(X_{\text{B}})) = 0.015(3)$ for $P_{\text{e}}(X_{\text{B}})$ the probability distribution of the experimentally measured amplified quadrature $X_{\text{B}}$ and $P_{\text{m}}(X_{\text{B}})$ its corresponding quadrature distribution predicted from our model. For the 2$^{\text{nd}}$ run, we compute the coefficients $\mathcal{B}(P_{\text{e}}(X_{\text{B}}), P_{\text{m}}(X_{\text{B}})) = 99.76(4)\,\%$ with $H(P_{\text{e}}(X_{\text{B}}), P_{\text{m}}(X_{\text{B}})) = 0.049(4)$. The $\mathcal{B}$ values close to unity indicate an excellent agreement between our model and experimental measurements, which can be interpreted as a proof of genuine SQMs in our experiments.

### 5.3.2 Test normality of measured datasets

Taking advantage of the histogram measurements of Bob's keys, we can verify the Gaussianity of the measured keys using classical statistical tests. These tests, alongside the measurements of cumulants up to the fourth order (see Sec. 4.3.2), assure that our measured data follows Gaussian statistics, i.e., the basic assumption made in all derivations in this work. We rely on well-known normality tests, namely the Shapiro–Wilk (SW) test, the Anderson–Darling (AD) test, and the Jarque–Bera (JB) test. Each test presents some robustness compared to the others. They are designed to test the validity of a null hypothesis, $H_0$, as compared to an alternative hypothesis (the negation of the null hypothesis most often). For these tests, the null hypothesis consists of stating that the observed data is normally distributed. For a given test, a so-called *p-value* is computed, which indicates the likelihood of the observed data to have occurred under the null hypothesis. In other words, the $p$-value represents the probability that we observe data as extreme as the measured ones given that the null hypothesis is true. To compute the $p$-value, a statistical quantity denoted $t$ (which depends on the performed

| test / keys | SW test | AD test | JB test |
|---|---|---|---|
| keys 1st run | $0.39 \pm 0.22$ | $0.43 \pm 0.29$ | $0.30 \pm 0.16$ |
| keys 2nd run | $0.40 \pm 0.21$ | $0.53 \pm 0.22$ | $0.39 \pm 0.14$ |

Table 5.2: Average $p$-value obtained for the various normality tests and for measured keys in the 1st and 2nd run. All $p$-values are well above the threshold $\alpha_{\text{thres}} = 0.05$.

test) is calculated for the unknown to-be-tested probability distribution $f$. The $p$-value is then expressed as

$$p = \Pr(f \geq t|H_0) \quad \text{or} \quad p = \Pr(f \leq t|H_0), \tag{5.58}$$

where the choice of the inequality depends on the test performed. One defines a confidence threshold $\alpha_{\text{thres}}$ and the null hypothesis $H_0$ can be rejected in the case of $p$-value $< \alpha_{\text{thres}}$. To reject the null hypothesis, the smaller the $p$-value, the more confident we are in rejecting the null hypothesis, as the probability of the observed data under the null hypothesis is small. One commonly considers that a $p$-value $\gtrsim 0.1$ does not provide statistical evidence against the null hypothesis. We note, however, that this result does not mean that the null hypothesis is corrected or that the alternative hypothesis is incorrect, but rather that the null hypothesis is not in contradiction with the observed data.

The SW test typically presents a high probability of rejecting the null hypothesis given that the alternative hypothesis is true [229]. It is computed using statistical estimators of the mean and the variance of the underlying random distribution. When applicable, this test is found to be efficient at capturing non-Gaussian characteristics of the observed data. Alternatively, the AD test is a commonly used test to evaluate observed data for any given probability distributions, not necessarily restricted to normal distributions [229]. It measures a weighted distance between the observed probability distribution and the assumed to-be-tested probability distribution. Similarly to the SW test, the AD test can capture non-Gaussian features efficiently when it is applied to a normal distribution. Lastly, the JB test can be used to test for normality of observed data by verifying whether or not the skewness and kurtosis of the data match a normal distribution [229]. The skewness measures the symmetry of the observed probability distribution and is zero for an ideal Gaussian distribution. The kurtosis is a statistical quantity that evaluates the significance of the tail of the distribution. For instance, a Poisson distribution has more outliers than a normal distribution and presents a corresponding higher kurtosis. Similarly to the SW test, the JB test presents a high probability of rejecting the null hypothesis under the assumption that the alternative hypothesis is true. The JB test is more suited than the SW test for a large data set of samples. More precisely, the SW test is recommended for a data set of less than 5000 samples. Since our sample size does not differ greatly from this threshold, we include both the SW and JB tests.

All tests are performed using the statistics toolbox of the programming language MATLAB®. Moreover, all tests are applied for the null hypothesis $H_0$ "The observed data has a Gaussian distribution". The computed average $p$-values of the tests for both measurement runs are listed in Tab. 5.2. The tests are performed with the common choice of $\alpha_{\text{thres}} = 0.05$ for all tests. We observe a high computed $p$-value for all three tests on average and for both measurement runs. The high standard deviation originates from the large fluctuations in $p$-values. However, all $p$-values are well above 0.1, except for one key for the first measurement run. Here, we obtain $p$-values around 0.05, which could indicate that the null hypothesis could be rejected. However, we recall that no experimental parameters are changed for this key compared to any other measured keys of the same measurement run. Moreover, none of the keys presents a low $p$-value for the second run. This seems to indicate that this particular key with a relatively low $p$-value is a statistical outlier and is not sufficient to confidently reject the null hypothesis. Thus, we

conclude that there is no statistical evidence to reject the null hypothesis and, as a result, we can assume that our measured keys are distributed according to Gaussian distributions. In addition, this result is in agreement with the assumption that all contributions of the variance of Bob presented in Eq. (5.48) have a Gaussian distribution, which we assume throughout all derivations in this work. More importantly, the assumption that our measured keys present a Gaussian distribution is in agreement with the fact that our measurement JPA, which we expect to perform phase-sensitive amplification, behaves as a linear amplifier throughout the measurements. In other words, it is in agreement with the assumption that all physical quantum operations taking place in our experimental setup are Gaussian and that we work exclusively with Gaussian channels.

### 5.3.3 Holevo quantity

In order to extract secret information from their datasets, Alice and Bob estimate an upper bound for the amount of information leaked during the quantum communication using the Holevo quantity $\chi_{\mathrm{E}}$. We rely on our calibration measurements to have an estimation of the channel losses $\tau_{\mathrm{E}}$ and coupled noise photon number $\bar{n}$. Without loss of generality [129, 230], we assume that Eve employs a collective Gaussian attack [98] with an optimal joint measurement, and we restrict her attack to an entangling cloner attack [227]. The entangling cloner attack consists of Eve coupling one mode of a TMS state to on incoming state of Alice, for each of Alice's states. The TMS is chosen such that $\cosh(r) = 1 + 2\bar{n}_{\mathrm{E}}$, for some apparent thermal photon number $\bar{n}_{\mathrm{E}}$. It is modelled using a density matrix encompassing the mode of Alice and the two modes of Eve. These modes are coupled together using a beam splitter model between Alice's incoming mode and one mode of Eve's TMS state. From the perspective of Alice and Bob, the signal coupled by Eve's attack appears as a thermal noise signal with $\bar{n}_{\mathrm{th}} = 2\bar{n}/\varepsilon_{\mathrm{E}}$. To compute the Holevo quantity, we define the ensemble state of Eve by averaging over Alice's codebook, which in this work takes the form

$$\hat{\rho}_{\mathrm{E,ens}} = \int_{\mathrm{A}} \mathrm{d}\alpha \, f(\alpha) \, \hat{\rho}_{\mathrm{E},\alpha}, \tag{5.59}$$

where $A$ is the codebook domain of Alice meaning the domain from which Alice chooses her symbols. Here, we consider $A = \mathbb{R}$. Note that a complete description would include a random change of basis, i.e., randomly switching between squeezing along the $q$- or $p$-quadrature. In our experiment, squeezing is restricted to the $q$-quadrature. The Holevo quantity is then given by [143]

$$\chi_{\mathrm{E}} = S_2\left(\int_{\mathrm{A}} d\alpha \, f(\alpha) \, \hat{\rho}_{\mathrm{E},\alpha}\right) - \int_{\mathrm{A}} d\alpha \, f(\alpha) \, S_2\left(\hat{\rho}_{\mathrm{E},\alpha}\right), \tag{5.60}$$

where $S_2$ is the von Neumann entropy for a two-mode states. We note that the second term inside the Holevo quantity represents an average of the von Neumann entropy of Eve's individual state. Even though these states individually depend on a given displacement amplitude $\alpha$, their corresponding von Neumann entropy does not. As a result, all individual states of Eve can be treated equally for the purpose of computing the Holevo quantity. As explained in Sec. 2.2.2, the von Neumann entropy of a Gaussian state is computed using its symplectic eigenvalues. The Holevo quantity as a function of experimental parameters is shown in Fig. 5.8. Since Eve is assumed to implement an entangling cloner attack and Alice uses a Gaussian codebook, all states involved in the protocol are Gaussian states. Following the derivations in Ref. [154], we can write the covariance matrix of an individual TMS state of Eve as

$$\mathbf{V}_{\mathrm{E,ind}} = \frac{1}{4}\begin{pmatrix} W\mathbf{I}_2 & \sqrt{W^2-1}\boldsymbol{\sigma}_{\mathrm{Z}} \\ \sqrt{W^2-1}\boldsymbol{\sigma}_{\mathrm{Z}} & W\mathbf{I}_2 \end{pmatrix}, \tag{5.61}$$

where $\boldsymbol{\sigma}_{\mathrm{Z}}$ is the $z$-Pauli matrix. The quantity $W$ represents the initial local variance of each mode of Eve's TMS state. We parametrize it as

$$W = 1 + \frac{4\bar{n}}{\varepsilon_{\mathrm{E}}} = 1 + 2\bar{n}_{\mathrm{E}}. \tag{5.62}$$

The interaction between Alice's and Eve's mode is modelled with a beam splitter operator $\hat{B}$ with a transmissivity $\tau = 1 - \varepsilon_{\mathrm{E}}$. After the interaction of an individual state of Eve with an incoming state from Alice, the covariance matrix in Eq.5.61 becomes

$$\mathbf{V}'_{\mathrm{E,ind}} = \frac{1}{4}\begin{pmatrix} (1-\varepsilon_{\mathrm{E}})W\mathbf{I}_2 + \varepsilon_{\mathrm{E}}\mathbf{V}_{\mathrm{A}} & \sqrt{(1-\varepsilon_{\mathrm{E}})}\sqrt{W^2-1}\boldsymbol{\sigma}_{\mathbf{Z}} \\ \sqrt{(1-\varepsilon_{\mathrm{E}})}\sqrt{W^2-1}\boldsymbol{\sigma}_{\mathbf{Z}} & W\mathbf{I}_2 \end{pmatrix}, \tag{5.63}$$

Here, the matrix $\mathbf{V}_{\mathrm{A}}/4$ is the covariance matrix of the incoming state of Alice at the input of the quantum channel (i.e., at the input of the second directional coupler in our implementation) and reads

$$\mathbf{V}_{\mathrm{A}} = 4\tau_2\tau_{\mathrm{A}}\tau_1\mathbf{V}_{\mathrm{sq}} + (1-\tau_2\tau_{\mathrm{A}}\tau_1)(1+2\bar{n}_{\mathrm{th}})\mathbf{I}_2, \tag{5.64}$$

with $\mathbf{V}_{\mathrm{sq}}$ the covariance matrix describing the squeezed state of Alice, i.e., for a $q$-squeezed state

$$\mathbf{V}_{\mathrm{sq}} = \begin{pmatrix} \sigma_{\mathrm{s}}^2 & 0 \\ 0 & \sigma_{\mathrm{as}}^2 \end{pmatrix}. \tag{5.65}$$

Using the indistinguishability condition in Eq.5.46, we derive the covariance matrix of the ensemble state of Eve as

$$\mathbf{V}'_{\mathrm{E,ens}} = \frac{1}{4}\begin{pmatrix} (1-\varepsilon_{\mathrm{E}})W\mathbf{I}_2 + \varepsilon_{\mathrm{E}}\tilde{V}_{\mathrm{A,ens}}\mathbf{I}_2) & \sqrt{(1-\varepsilon_{\mathrm{E}})}\sqrt{W^2-1}\boldsymbol{\sigma}_{\mathbf{Z}} \\ \sqrt{(1-\varepsilon_{\mathrm{E}})}\sqrt{W^2-1}\boldsymbol{\sigma}_{\mathbf{Z}} & W\mathbf{I}_2 \end{pmatrix}. \tag{5.66}$$

Here, we define

$$\tilde{V}_{\mathrm{A,ens}} = 4\tau_2\tau_{\mathrm{A}}\tau_1\sigma_{\mathrm{as}}^2 + (1-\tau_2\tau_{\mathrm{A}}\tau_1)(1+2\bar{n}_{\mathrm{th}}). \tag{5.67}$$

Using Eqs. 2.116 and 2.105, we derive the full analytical formula for the Holevo quantity

$$\chi_{\mathrm{E}} = g(\nu_1) + g(\nu_2) - g(\nu_3) - g(\nu_4), \tag{5.68}$$

where

$$\begin{aligned}
\nu_1 &= \frac{1}{8}\left(\sqrt{(W+(1-\varepsilon_{\mathrm{E}})W+\varepsilon_{\mathrm{E}}\tilde{V}_{\mathrm{A,ens}})^2 - 4(1-\varepsilon_{\mathrm{E}})(W^2-1)} + \left|\varepsilon_{\mathrm{E}}(\tilde{V}_{\mathrm{A,ens}} - W)\right|\right), \\
\nu_2 &= \frac{1}{8}\left(\sqrt{(W+(1-\varepsilon_{\mathrm{E}})W+\varepsilon_{\mathrm{E}}\tilde{V}_{\mathrm{A,ens}})^2 - 4(1-\varepsilon_{\mathrm{E}})(W^2-1)} - \left|\varepsilon_{\mathrm{E}}(\tilde{V}_{\mathrm{A,ens}} - W)\right|\right), \\
\nu_3 &= \frac{1}{4\sqrt{2}}\sqrt{\Delta_{\mathrm{A,s}}\Delta_{\mathrm{A,as}} + W^2 - 2(1-\varepsilon_{\mathrm{E}})(W^2-1) + \Delta_{\mathrm{E}}^2}, \\
\nu_4 &= \frac{1}{4\sqrt{2}}\sqrt{\Delta_{\mathrm{A,s}}\Delta_{\mathrm{A,as}} + W^2 - 2(1-\varepsilon_{\mathrm{E}})(W^2-1) - \Delta_{\mathrm{E}}^2},
\end{aligned} \tag{5.69}$$

with the following definitions

$$\begin{aligned}
\Delta_{\mathrm{E}}^4 &= (W^2 - \Delta_{\mathrm{A,s}}\Delta_{\mathrm{A,as}})^2 - 4(1-\varepsilon_{\mathrm{E}})(W^2-1)(W-\Delta_{\mathrm{A,s}})(W-\Delta_{\mathrm{A,as}}), \\
\Delta_{\mathrm{A,s}} &= (1-\varepsilon_{\mathrm{E}})W + \varepsilon_{\mathrm{E}}\tilde{V}_{\mathrm{A,s}}, \\
\Delta_{\mathrm{A,as}} &= (1-\varepsilon_{\mathrm{E}})W + \varepsilon_{\mathrm{E}}\tilde{V}_{\mathrm{A,as}}, \\
\tilde{V}_{\mathrm{A,s}} &= 4\tau_2\tau_{\mathrm{A}}\tau_1\sigma_{\mathrm{s}}^2 + (1-\tau_2\tau_{\mathrm{A}}\tau_1)(1+2\bar{n}_{\mathrm{th}}), \\
\tilde{V}_{\mathrm{A,as}} &= 4\tau_2\tau_{\mathrm{A}}\tau_1\sigma_{\mathrm{as}}^2 + (1-\tau_2\tau_{\mathrm{A}}\tau_1)(1+2\bar{n}_{\mathrm{th}}).
\end{aligned} \tag{5.70}$$

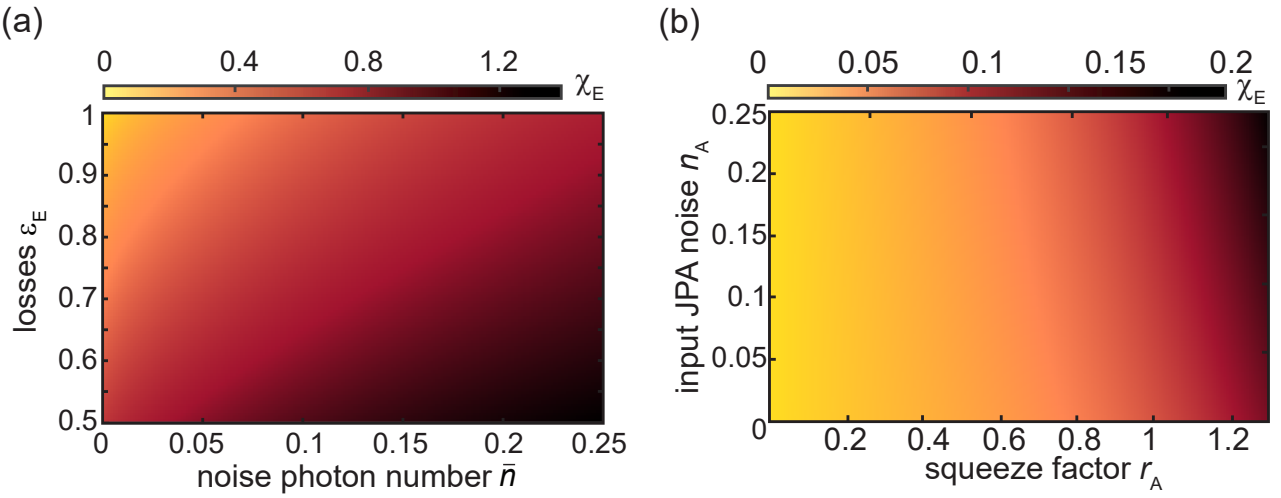


Figure 5.8: Holevo quantity $\chi_E$ calculated according to Eq. (5.68). (a) Holevo quantity as a function of the noise photon number $\bar{n}$ and loss $\varepsilon_E$ of the quantum channel. (b) Holevo quantity as a function of the squeezing factor $r_A$ and input JPA noise $\bar{n}_A$ of the first JPA used by Alice to prepare squeezed states. Here, we consider $\chi_E = 1 - 0.9885$ and the lowest coupled noise $\bar{n} \simeq 2 \times 10^{-6}$.

In our experiment, we use Eq. (5.68) to compute Eve's Holevo quantity. In the asymptotic case, we use the direct expression in Eq. (5.68) with the experimental parameters given in Tab. 5.1. The exact values of the channel parameters, $\varepsilon_E$ and $\bar{n}$, are used. In the case of finite-size effects as mentioned in Sec. 5.3.4, we follow the same procedure to compute the Holevo quantity, except that the values for the channel parameters are replaced by their worst-case scenario estimators. The resulting values for the asymptotic case are shown in Fig. 5.5. We observe a steady logarithm-like increase behavior of the Holevo quantity as a function of the coupled noise photon. This indicates that Eve gets more information from Alice as the coupled noise increases. Physically, this can be interpreted as Eve having more strongly correlated modes as the noise increases. Since one mode is coupled to Alice's mode, she can use her nonlocal correlations to extract information from Alice's symbol. In the limit of infinite noise, Eve has perfectly correlated modes and can extract exactly the symbol of Alice. Conversely, any noise on Alice's states decreases the final correlations measured by Bob. One can consider that information changes from flowing from Alice to Bob to flowing from Alice to Eve as the coupled noise increases, a notion that can be linked to quantum discord [216].

### 5.3.4 Security analysis

**Asymptotic key.** The security of communication in the asymptotic case is determined by bounding the number of secure bits communicated per symbol $K_{\text{exp}}$ with the secret key [181, 231]

$$K = I\left(\mathcal{K}_A : \mathcal{K}_B\right) - \chi_E \leq K_{\text{exp}}. \tag{5.71}$$

A more general formula would additionally include an efficiency coefficient $\beta$ related to the post-processing of the measured data. Here, we set $\beta = 1$ due to the fact that this coefficient depends on the efficiency of classical algorithms and represents rather a technical limitation. Instead, we focus on the efficiency of the communication from a quantum mechanical point of view. In Fig. 5.9, we show the secret key $K$ associated with the MI presented in Fig. 5.6. We observe a clear positive secret key, which indicates that Alice and Bob share more information than leaks to Eve. As a result, the communication is said to be *unconditional* secure in the asymptotic regime. However, it is important to remember that this statement is based on

several assumptions. The most important is related to the fact that Alice and Bob share a classical channel over which they can communicate and authenticate each other (see Sec. 3.1.4).

We observe that the asymptotic secret key remains positive up to 0.062(2) coupled noise photons. This noise represents the total tolerable noise that can be coupled from a noisy environment before the communication becomes insecure. Therefore, it is interesting to find ways of improving the protocol performance. To this end, we can increase the codebook size, squeezing level, or quantum efficiency of the measurement JPA. However, various limitations, such as compression effects of the JPAs, JPA noise performance, and experimentally achievable squeezing levels, must be taken into account. The codebook variance is such that the input measurement JPA power for Alice's symbols, in the worst-case scenario for a $3\sigma$ confidence interval, is almost reaching the compression level. Similarly, improving the quantum efficiency would imply using a larger gain, which would reduce the compression level. Lastly, in our experiments, we find that the squeezer JPA squeezing level reaches a plateau level of $S \sim 3.6\,\mathrm{dB}$, so it cannot be significantly increased.

However, it is possible to increase the codebook variance while keeping the squeezing level constant if the JPA input noise and squeeze factor increase such that they compensate each other. In our experiments, we enlarge the codebook variance $\sigma^2_{\mathrm{A}}$ by allowing for additional input noise from the first JPA (originating from a pump-induced noise and intrinsic losses) by increasing the pump tone amplitude of the measurement JPA. The increase in codebook variance can be explained by rewriting the indistinguishability condition from Eq. (5.46), taking into account that the squeezer JPA is actually not ideal but noisy in our experiments, similarly to the measurement JPA. We denote the noise of the first JPA as $\bar{n}_{\mathrm{A}}$ and derive

$$\sigma^2_{\mathrm{s}} + \sigma^2_{\mathrm{A}'} = \sigma^2_{\mathrm{as}} \Leftrightarrow \frac{1}{4}(1 + 2\bar{n}_{\mathrm{A}})\exp(-2r_{\mathrm{A}}) + \sigma^2_{\mathrm{A}'} = \frac{1}{4}(1 + 2\bar{n}_{\mathrm{A}})\exp(2r_{\mathrm{A}}). \tag{5.72}$$

Following this result, we can parametrize the squeezing level, $S$, and displacement (codebook) variance, $\sigma^2_{\mathrm{A}'}$, of Alice as

$$\begin{aligned} S &= -10\log_{10}(\sigma^2_{\mathrm{s}}/0.25) = 20r_{\mathrm{A}}\log_{10}(e) - 10\log_{10}(1 + 2\bar{n}_{\mathrm{A}}), \\ \sigma^2_{\mathrm{A}'} &= \frac{1}{2}(1 + 2\bar{n}_{\mathrm{A}})\sinh(2r_{\mathrm{A}}). \end{aligned} \tag{5.73}$$

From Eq. (5.73), we see that it is possible to enlarge the displacement variance while keeping the squeezing level the same if both the squeezing factor and the input JPA noise are increased. This results in an increase of the anti-squeezing level from 7.1 dB to 7.6 dB and, hence due to the constant squeezing level, in an enhancement of $\sigma^2_{\mathrm{A}}$ by $\sim 14\%$. As shown in Fig. 5.9 (b), this increased codebook variance leads to a higher secret key, extending the noise tolerance to 0.071(2) photons or a relative increase of the coupled noise tolerance by $\sim 14\%$.

During the 2$^{\mathrm{nd}}$ measurement run, we also obtain a slightly higher quantum efficiency of $\eta = 68(2)$ % as compared to the initial $\eta = 65(2)$ %. For both runs, we compute the expected MI and Holevo quantity according to Eqs. 5.53 and 5.68. As illustrated in Fig. 5.9 (b), we observe a good matching between the prediction of our model and the extracted secret keys. However, based on our quadrature model, the increased quantum efficiency in the 2$^{\mathrm{nd}}$ measurement run alone is insufficient to induce the observed higher secret keys. More precisely, this increase in quantum efficiency leads to a better SNR that alone would be insufficient to reach the measured SNR. The increase in secret key values with added preparation noise illustrates a general beneficial effect of adding trusted noise on the reference side of error correction [134, 135]. It is known from the literature that additional trusted noise on the reference side (Alice in DR and Bob in RR) results in an improved secret key. Here, the added noise originates from the increased anti-squeezed quadrature, and we consider this noise trusted, i.e., Eve does not have access to it. This assumption is a fair assumption in the framework of a lab experiment since the

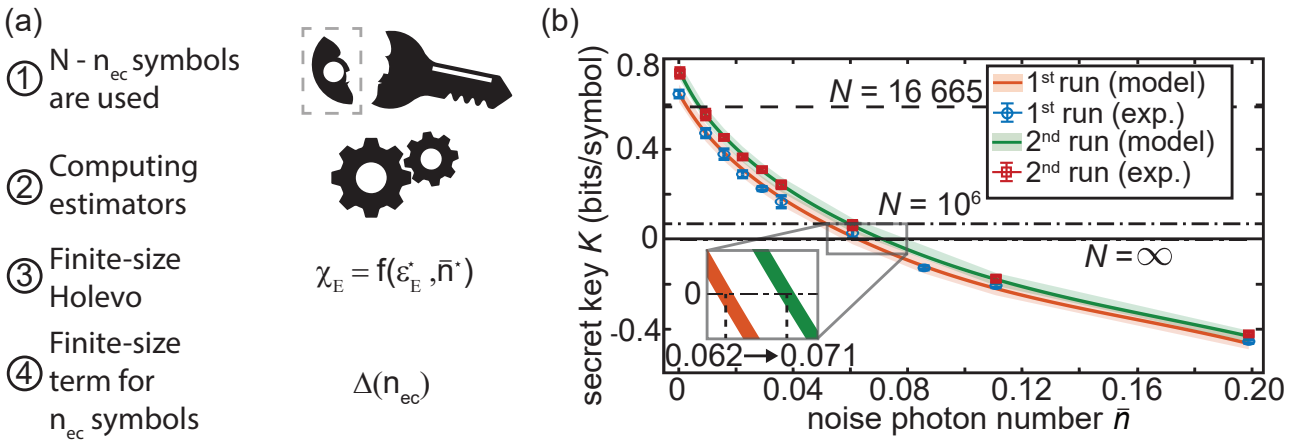


Figure 5.9: Secret key of the microwave CV-QKD protocol. (a) Principle of a finite-size estimators. A fraction of $m$ symbols of the key are used to build statistical estimators of the channel parameters. Using the remaining $N-m$ symbols, Alice and Bob compute a secret key bound using the statistical estimators and account for an additional finite-size term $\Delta$, which further reduces the secret key. (b) Measured secret key of the CV-QKD protocol for two experimental runs: 1st with squeezing (anti-squeezing) levels of 3.6 (7.1) dB and 2nd with squeezing (anti-squeezing) levels of 3.6 (7.6) dB. The dashed lines represent the finite-size terms $\Delta$, which impose upper limits for the noise tolerable for reaching the unconditional security. The error bars and shaded areas denote the standard deviation of the experimental data and model, respectively.

setup (or at least the two JPAs) is considered known and trusted. The enlarged codebook is a consequence of the indistinguishability condition $\sigma_{\mathrm{s}}^2 + \sigma_{\mathrm{A}'}^2 = \sigma_{\mathrm{as}}^2$ (see Eq. (5.72)), leading to a larger increase in MI than Holevo quantity, and thus, to an increase of the secret key rate. For the case of the lowest coupled noise, $\bar{n} \simeq 2 \times 10^{-6}$ (given by the coupling to our sample stage at $T \simeq 15\,\mathrm{mK}$), we measure a relatively high secret key up to 0.74 bits/symbol and a corresponding SNR of 2.16, similar to optical implementations in long-distance communication [232]. We note that this level remains lower than short-distance optical implementations, which typically work in a regime of SNRs $\geq 10$. The key point is that the optical implementation of CV-QKD protocols commonly relies solely on coherent states instead of squeezed states. In our work, it is not advantageous to use coherent state protocols in the microwave domain (see Ref. [233]). Instead, we profit from the straightforward implementation and control of squeezed states in our microwave setup.

**Finite-size effects.** Our security analysis can be extended to include limiting effects arising from the finite size of the transmitted key [149]. These finite-size effects, inducing a decrease of the secret key, are reflected by additional finite-size terms $\Delta$. Equally important, in practical QKD implementations, Alice and Bob are unaware of the exact quantum channel parameters and must estimate them using part of the communicated keys. To achieve maximal security, the channel parameters are obtained from worst-case-scenario statistical estimators $\varepsilon_{\mathrm{E}}^{\star}$ and $\bar{n}^{\star}$ for the channel losses $\varepsilon_{\mathrm{E}}$ and coupled noise $\bar{n}$, respectively. Alice and Bob build these statistically unbiased estimators from a publicly disclosed fraction of length $m = N - n_{\mathrm{ec}}$ of their exchanged key. The choice of length $m$ depends on the desired quality of the estimators. For practical implementations, an ideal number $m \geq 10^6$ is suitable. Based on Eq. (5.48), we first reformulate the random variable of Bob (resulting in his measured key) as

$$B = \sqrt{\tau_{\mathrm{tot}}} A + N, \tag{5.74}$$

with $A$ and $N$ the random variables describing Alice's key and the total added noise, respectively. Using the disclosed data, a square root transmissivity unbiased estimator can be

constructed as [126]

$$\hat{T}_{\text{tot}} = \frac{\sum_{i=1}^{m}\left(\alpha_i - \bar{A}\right)\left(\beta_i - \bar{B}\right)}{\sum_{i=1}^{m}\left(\alpha_i - \bar{A}\right)^2} \xrightarrow[m\to\infty]{} \frac{\text{Cov}(A,B)}{\text{Var}(A)}, \tag{5.75}$$

where we denote $\bar{A}$ as the average value of Alice's key $\mathcal{K}_{\text{A}} = \left\{\alpha_j\right\}_{j\in[1,N]}$ while $\bar{B}$ denotes the average value of Bob's key $\mathcal{K}_{\text{B}} = \left\{\beta_j\right\}_{j\in[1,N]}$. From this estimator, we define a new estimator $\hat{\tau}_{\text{tot}} = \hat{T}_{\text{tot}}^2$ which is unbiased since $\langle\hat{\tau}_{\text{tot}}\rangle = \tau_{\text{tot}}$, as a direct consequence of Eqs. 5.75 and 5.74. According to Eq. (5.45), we obtain an unbiased estimator of $\varepsilon_{\text{E}}$ as $\hat{\varepsilon}_{\text{E}} = 1 - \hat{\tau}_{\text{E}} = 1 - \hat{\tau}_{\text{tot}}/(\tau_1\tau_2\tau_{\text{A}}\tau_3\tau_4)$. From the previous result, we can construct an unbiased estimator for the quadrature total noise variance [126]

$$\hat{\sigma}_{\text{X}}^2 = \frac{1}{m}\sum_{i=1}^{m}\left(\beta_i - \hat{T}_{\text{tot}}\,\alpha_i\right)^2. \tag{5.76}$$

This estimator converges to the quadrature total noise variance, which we relate to the coupled noise photon number, $\bar{n}$, using that $\left\langle\hat{\sigma}_{\text{X}}^2\right\rangle \xrightarrow[m\to\infty]{} \sigma_{\text{X}}^2 = \tau_{\text{tot}}\sigma_{\text{s}}^2 + \tau_{\text{th}}\left(1+2\bar{n}_{\text{th}}\right)/4 + \tau_3\tau_4\left(\varepsilon_{\text{E}}/4 + \bar{n}\right) + N_{\text{X}}$. We compute a worst-case scenario unbiased estimator of the losses considering a confidence parameter $w$ such that

$$\varepsilon_{\text{E}}^{\star} = \hat{\varepsilon}_{\text{E}} + w\,\sigma_{\hat{\varepsilon}_{\text{E}}} \simeq \hat{\varepsilon}_{\text{E}} + 2w\sqrt{\left(\frac{\sigma_{\text{X}}^2}{\sigma_{\text{A}}^2} + 2\tau_{\text{tot}}\right)\frac{\tau_{\text{E}}}{\tau_1\tau_2\tau_{\text{A}}\tau_3\tau_4\,m}}. \tag{5.77}$$

For Gaussian random variables, the confidence parameter $w$ reduces to the simple form

$$w = \sqrt{2}\,\text{erf}^{-1}\left(1 - 2\varepsilon_{\text{ec}}\right), \tag{5.78}$$

with $\varepsilon_{\text{ec}}$ defined as an error probability, typically set in the range of $10^{-10}$ for CV-QKD protocols [126], giving the common value of $w \simeq 6.34$. In this work, we use a proof-of-principle value of $\varepsilon_{\text{ec}} = 10^{-3}$ giving a corresponding $w \simeq 3$. We note that this limitation is primarily motivated by the limited number of symbols $N = 16665$. For a larger $N$, one can decrease the value of $\varepsilon_{\text{ec}}$, improving the security. We can further extend this analysis to obtain a worst-case-scenario unbiased estimator of the coupled noise photon number $\bar{n}$. First, we define an unbiased coupled noise photon number estimator

$$\hat{\bar{n}} = \left(\hat{\sigma}_{\text{X}}^2 - \hat{\tau}_{\text{tot}}\,\sigma_{\text{s}}^2 - \tau_{\text{th}}\left(1+2\bar{n}_{\text{th}}\right)/4 - \tau_3\tau_4\frac{\varepsilon_{\text{E}}^{\star}}{4} - N_{\text{X}}\right)/(\tau_3\tau_4). \tag{5.79}$$

This results in the worst-case-scenario unbiased estimator for the coupled noise photon number

$$\bar{n}^{\star} = \hat{\bar{n}} + w\,\sigma_{\hat{\bar{n}}} \simeq \hat{\bar{n}} + w\sqrt{\frac{2\,\hat{\sigma}_{\text{X}}^4}{m}}. \tag{5.80}$$

Since a part of the secret key must be used for parameter estimation, Alice and Bob only preserve a key of finite size $n_{\text{ec}} = N - m$. In this work, we use the entirety of the key $m = N$ to optimize the precision of our worst-case scenario estimators. We note that this implies that no key remains for Alice and Bob. Simply, we aim at verifying the presented formalism of worst-case-scenario estimators. As a result, we use the built estimators and the communicated keys to gauge the impact of the finite size of the keys. This approach is equivalent to the case where keys would have been communicated with twice the current length ($N$ symbols for parameter estimations and $N$ remaining symbols for the finite-size keys) and is, therefore, valid since we

are focusing only on statistical quantities in this part. Additionally, we need to account for a finite-size term to obtain a finite-size secret key bound, which we calculate as [126]

$$\Delta\left(n_{\mathrm{exp}}\right) = \frac{\Delta_{\mathrm{fs}}}{\sqrt{n_{\mathrm{ec}}}} - \frac{\Theta}{n_{\mathrm{ec}}},$$
$$\Delta_{\mathrm{fs}} = 4\log_2\left(\sqrt{d}+2\right)\sqrt{\log_2\left(\frac{18}{p_{\mathrm{ec}}^2\varepsilon_{\mathrm{s}}^4}\right)},\ \Theta = \log_2\left[p_{\mathrm{ec}}\left(1-\frac{\varepsilon_{\mathrm{s}}^2}{3}\right)\right] + 2\log_2\left(\sqrt{2}\,\varepsilon_{\mathrm{h}}\right). \tag{5.81}$$

The inverse square root dependency of the $\Delta_{\mathrm{fs}}$ term is the main limitation in the previous equation, drastically increasing the necessary number of symbols to obtain a negligible finite-size term $\Delta$. Note that contrary to the channel parameter estimators, the finite-size term depends on $n_{\mathrm{ec}} = N - m$. Therefore, a compromise must be found in practical implementations. Here, the parameter $d$ represents the dimension of Alice's and Bob's effective codebooks after a discretization step during error reconciliation. This discretization is required to transform their data from a continuous set into a discrete set over which an existing classical optimized error correction algorithm can be run. We consider a typical value for CV-QKD protocols of $d = 2^5$ for a 5-bit discretization. The overall success of the protocol is limited by the tolerance error for the security of the protocol, reflected in a smoothing parameter $\varepsilon_{\mathrm{s}}$ and a hashing parameter $\varepsilon_{\mathrm{h}}$. These parameters determine the total error of the privacy amplification step, which follows the error correction step and depends on the choice of classical algorithm. The goal of privacy amplification is to remove the remaining information of Eve about Alice's and Bob's error-corrected key. In this work, we choose an illustrative value of $\varepsilon_{\mathrm{s}} = \varepsilon_{\mathrm{h}} = 10^{-3}$, although we note that conservative values of $\varepsilon_{\mathrm{s}} = \varepsilon_{\mathrm{h}} = 10^{-10}$ are typically chosen for CV-QKD protocols [126]. We emphasize that this point does not change our conclusions regarding the finite-size terms.

**Finite-size key.** Based on the previous considerations, we use the aforementioned finite-size term and parameter estimators to build a new bound on the secrete key in the finite-size case, which takes the form [126]

$$r\left[\beta I\left(\mathcal{K}_{\mathrm{A}}\colon\mathcal{K}_{\mathrm{B}}\right) - \chi_{\mathrm{E}}\left(\varepsilon_{\mathrm{E}}^{\star},\bar{n}^{\star}\right) - \Delta\left(n_{\mathrm{exp}}\right)\right] \leq K_{\mathrm{exp}}, \tag{5.82}$$

where $r = n_{\mathrm{ec}}\,p_{\mathrm{ec}}/N$ is a rescaling prefactor with $n_{\mathrm{ec}}$ denoting the fraction of the exchanged key not used for parameter estimation. The efficiency of the error correction protocol is denoted as before as $\beta$ and its success probability $p_{\mathrm{ec}}$, with an achievable $\beta > 90\,\%$ for an SNR around unity [178]. In this work, we set the success probability and efficiency coefficient $\beta$ to 0.95. As illustrated in Fig. 5.9 (a), if we account only for the finite-size terms $\Delta$ in Eq. (5.82) and keep the exact values of the channel losses and coupled noise, we can observe a region of positive secret key up to $\bar{n} = 0.004$ ($\bar{n} = 0.009$) for the 1$^{\mathrm{st}}$ run (2$^{\mathrm{nd}}$ run). This result shows a drastic decrease in secret key and coupled noise tolerance due to the finite-size term $\Delta$, scaling as $1/\sqrt{n_{\mathrm{ec}}}$ as in Eq. (5.81). This additional term $\Delta$ describes an information cost (in bits), induced by using the Holevo quantity in the finite case regime. The exact entropy term to use is related to the so-called *min-entropy*, a quantity tightly connected to the von Neumann entropy [234]. It expresses the maximal amount of information that Eve can extract under the additional constraint of being limited to a finite set of states.

Only in the asymptotic case, $N \to +\infty$, the min-entropy term converges to the Holevo quantity. This effect can therefore be largely mitigated by extending the key length to a more demanding but realistic value of $N \geq 10^6$. In this case, we observe in Fig. 5.9 (b), that the secret key would be positive up to $\bar{n} = 0.053$ ($\bar{n} = 0.06$) for the 1$^{\mathrm{st}}$ run (2$^{\mathrm{nd}}$ run), nearly reaching the asymptotic values of tolerable coupled noise. In a second time, we compute using

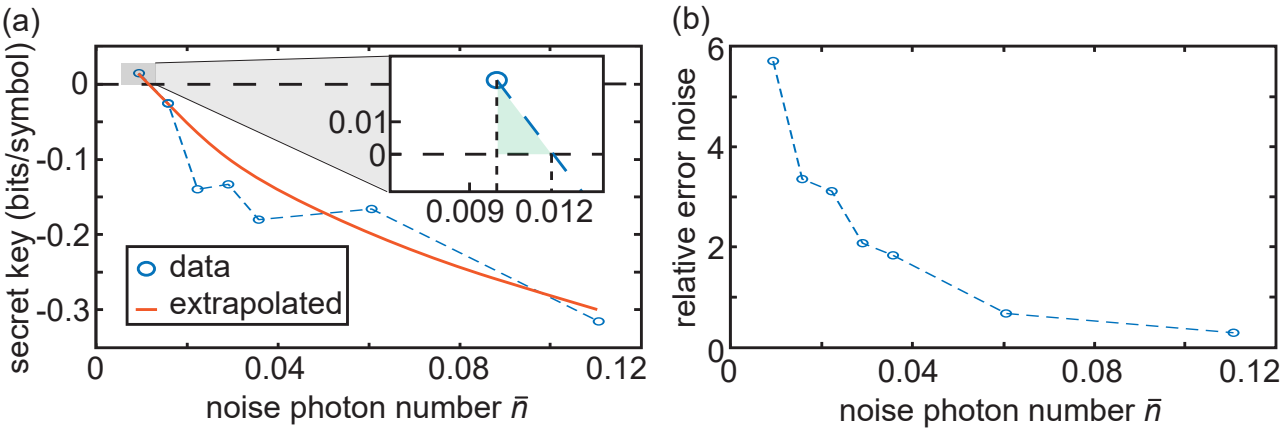


Figure 5.10: Results of the parameter estimation. (a) Secret key for the 1st run using the worst-case scenario channel estimators of the quantum channel parameters as a function of the exact value of the coupled noise $\bar{n}$. The estimators are built using $m = N$ symbols for maximal accuracy. We observe a strong reduction of the secret key as compared to the results in Fig. 5.9. The secret key conserves a comparable shape as depicted by the orange curve, which is extrapolated from the data and serves as a guide for the eye. We observe, as shown by a green shade in the zoom inset, a remaining region of positive secret key. (b) Relative error of the noise estimator. This estimator is the major reason for the reduction in secret key due to the large overestimation of the noise for small noise values. This result originates from the low absolute values of the noise and the inaccuracy of the estimator from the limited number of symbols. We note an exponential decrease, ranging from $\sim 600\%$ down to $\sim 11\%$, of the relative error as a function of the true coupled noise $\bar{n}$ due to an increase in the SNR of the noise estimator.

our whole measured keys the worst-case-scenario unbiased estimator for the losses and noise $\varepsilon_{\mathrm{E}}^{\star}$ and $\bar{n}^{\star}$ following Eqs. 5.77 and 5.80. As a consequence, we obtain the optimal estimators that can be built from our measured data. Recalling that we use an error of $e_{\mathrm{ec}} = 10^{-3}$ and not accounting for the finite-size terms $\Delta$, we compute the secret key bound from Eq. (5.82) and plot the resulting bound in Fig. 5.10 (a). We obtain a positive secret key bound up to roughly $\bar{n} = 0.012$ for the 1st run ($\bar{n} = 0.017$ for the same analysis in the 2nd run). We note a decrease in the coupled noise tolerance due to the estimators, reduced to a small region as highlighted in Fig. 5.10 (a). The secret key bound presents some irregularities due to the statistical imprecision of the parameter estimators. In particular, the main error originates from the estimation error of the noise as illustrated in Fig. 5.10 (b). The relative error in the noise estimator decreases as a function of the coupled noise due to lower relative statistical error. In general, the noise is typically largely overestimated, resulting in a significant decrease in the secret key bound. However, the general behaviour of the asymptotic secret key is preserved.

We conclude that it is possible to implement and verify experimentally the finite-size effects, including the finite-size term $\Delta$ and the parameter estimation. The overall effect of the worst-case scenario estimators is to reduce the tolerable coupled noise of the secret key due to the scaling of their intentional error, which is amplified by statistical errors. Since we are operating in a worst-case scenario, any deviation from the true channel parameters is noticeably detrimental to the secret key. However, for the same size $m$ of symbols used in finite-size effects, the reduction in tolerable coupled noise is less than the finite-size term $\Delta$. In light of these observations, we conclude that all finite-size effects can be straightforwardly solved by increasing the key length to $N \geq 10^6$, where the term $\Delta$ and the error of the parameter estimators become negligible, with both effects needing to be accounted for equally.

### 5.3.5 Secure communication distance investigation

In this section, we estimate the maximal secure communication distances that could be achieved with the microwave CV-QKD protocol based on the current experimental performance. To this end, we consider a communication protocol, where Alice and Bob keep the same experimental parameters as in the 2$^{\text{nd}}$ run (providing larger secret keys and tolerance to coupled noise), except that we treat the channel losses $\varepsilon_{\text{E}}$ as a system parameter for a given coupled noise photon number $\bar{n} = \bar{n}_{\text{th}}\varepsilon_{\text{E}}/2$. Here, we consider the quantum channel as a thermal environment that couples to the propagating signals provided by Alice. The photon number $\bar{n}_{\text{th}}$ is determined by the temperature of this thermal environment at a given frequency $\omega$. For each coupled noise photon number $\bar{n}$, the maximal tolerable losses are determined as

$$\varepsilon_{\text{E,max}} = \max\{\varepsilon_{\text{E}} |\, K(\varepsilon_{\text{E}}, \bar{n}) > 0\}. \tag{5.83}$$

In Fig. 5.11 (a), we show the maximally tolerable loss as a function of the photon number $\bar{n}_{\text{th}}$. We observe two regimes for the tolerable loss, where the maximal tolerable loss does not change significantly until about $\bar{n}_{\text{th}} \simeq 5 \times 10^{-2}$, corresponding to the temperature of $T \simeq 80\,\text{K}$ at the frequency of 5 GHz. Afterwards, the maximal tolerable loss shows an exponential decrease as a function of the thermal background noise. In a fully cryogenic environment at a temperature $T \simeq 30\,\text{mK}$, we assume the use of commercially available superconducting cables with characteristic losses of $L_{\text{sc}} \sim 10^{-3}\,\text{dB/m}$ [204] for frequencies around 5 GHz and parametrize the channel loss as $\varepsilon_{\text{E}} = L_{\text{sc}}\, d$, where $d$ is the communication distance. Based on the previous formalism, we find that an unconditionally secure microwave communication is feasible up to $d = 1190\,\text{m}$. This fairly long distance makes microwave CV-QKD relevant for secure local area quantum networks [235], where one could envision a cryogenic network of superconducting chips connected via superconducting cables, as depicted in Fig. 5.11 (b). In a cryogenic environment, proof-of-principle experiments can be implemented using several meter-long spools of superconducting cable or alternatively, one can rely on already existing cryogenic links [199, 236] to verify the CV-QKD microwave protocols over distances up to several tens of meters. There, it is also possible to employ microwave waveguides, which might offer even lower attenuation losses [204], as compared to superconducting coaxial cables, while not as flexible as the latter.

Remarkably, we also find that the unconditionally secure microwave communication could be feasible up to 84 m in the open-air room temperature environment with $\bar{n}_{\text{th}} \simeq 1250$ for signals at $\omega/2\pi \simeq 5\,\text{GHz}$. This finding results from considering the very low microwave atmospheric absorption losses of $6.3 \times 10^{-6}\,\text{dB/m}$ in clear weather conditions [60]. To obtain this result, we first estimate a path loss for the possible communication distance of $d = 84\,\text{m}$ of approximately 80 dB. A typical parabolic antenna with a diameter of around 2 m provides passive gain around 40 dB [60], implying that a pair (as an emitter and a receiver, representing respectively Alice and Bob) of such antennas would fully compensate the considered path loss. In this context, the implementation of a low-loss and sufficiently broadband interface between the cryogenic part and the antennae remains an important technological challenge for the future. Therefore, we focus on fundamentally unavoidable physical limitations due to absorption losses and treat the estimated communication distance as an upper bound for unconditionally secure microwave QKD based on the performance of our existing JPAs. We note that the presence of a finite uncompensated path loss does not necessarily prevent secure communication but may reduce the secure communication distances. Nonetheless, we stress that an actual implementation of such microwave antennas would most likely be limited by technical imperfections, as an ideal antenna would be challenging to obtain. These imperfections would manifest in the CV-QKD protocol as additional losses and noise on Alice's preparation side and Bob's measurement side. Depending on their values, the secure communication distance could be greatly affected. Such an open-air

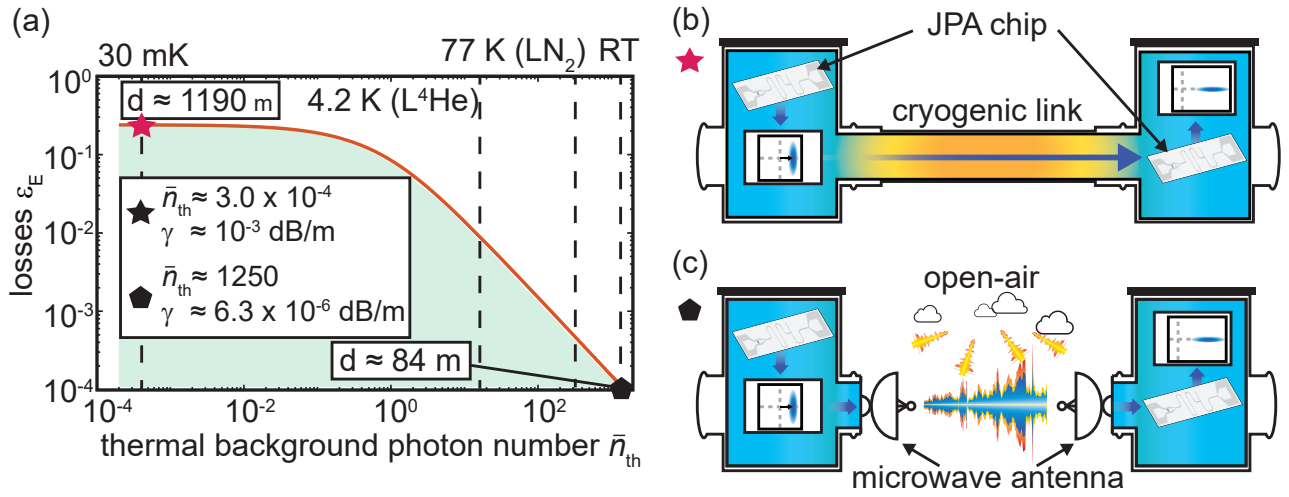


Figure 5.11: Extrapolated maximally tolerable loss in the quantum channel as a function of the thermal background photon number. (a) Estimation of maximally tolerable loss (solid line) for positive secret keys as a function of the photon number due to a thermal background, $\bar{n}_{\text{th}}$. This analysis is based on the experimental data from the 2$^{\text{nd}}$ run. The green shaded area indicates the region of positive secret keys. We emphasize two particular temperatures on this curve: the cryogenic temperature $\sim 30\,\text{mK}$ and room temperature (RT) $\sim 300\,\text{K}$. At millikelvin temperatures, we assume characteristic losses in superconducting cables of $\gamma = 1.0 \times 10^{-3}\,\text{dB/m}$ while for the open-air conditions, we restrict ourselves to atmospheric microwave losses $\gamma = 6.3 \times 10^{-6}\,\text{dB/m}$ due to pure absorption. (b) Schematic of the communication scenario at the point denoted by the red star symbol in panel (a). Here, a cryogenic link is considered between two cryostats, both at a temperature of $T \simeq 30\,\text{mK}$. The link represents the quantum channel, assumed in our calculations to be at the same temperature $T$ but potentially at a higher temperature (for higher coupled noise from Eve). (c) Schematic of the communication denoted by a pentagon symbol. Here, the background is assumed to be at room temperature and represents the quantum channel. The two cryostats send and receive the states via microwave antennae.

microwave system would be relevant for short-distance microwave applications such as WiFi or Bluetooth technology. Additionally, one can consider the case of short-distance communication between close buildings via antennas. As such, microwave CV-QKD demonstrates a notable potential for secure short-range open-air microwave communication, where microwave signals additionally benefit from a resilience to weather imperfections [60]. The latter are known to marginally interact with microwave signals, which are particularly impervious to small air particles (on the scale of $\sim 10\,\mu\text{m}$), for instance in the case of fog or haze.

### 5.3.6 Potential improvements and outlook

Our experiment reveals that the main limiting factor for the performance of the microwave CV-QKD protocol is the total noise in the measured keys, which is composed of the coupled noise $\bar{n}$ and the amplification noise. Here, the main aspect that can be improved is the quantum efficiency of the measurement JPA. We find that the measured SNRs and corresponding MIs are very sensitive to a change in quantum efficiency. Based on Eq. (5.53), we can extrapolate the influence of the change in amplification noise. Raising the quantum efficiency in the 2$^{\text{nd}}$ run from 68% to 88%, i.e., a relative change of $\sim 33\%$, results in doubling the measured SNRs and a relative increase in MI by $\sim 63\%$. Therefore, any increase in $\eta$ has a very positive impact on the secret key. Moreover, a decrease in the amplification noise means that more coupled noise photons can be tolerated in the communication, since the total noise is decreased, but the Holevo quantity stays unchanged (in the trusted noise scenario). Using the previous example, the maximum tolerable coupled noise would be increased to $\bar{n} = 0.13$ photons, nearly

doubling the value obtained in this work. This significant improvement would also largely improve the maximum tolerable communication distances, independent of a cryogenic or open-air environment.

We note, however, that increasing the quantum efficiency of present technology amplifiers to values above $\eta \simeq 70\%$ (as measured in Sec. 4.3.3) is a technical challenge. This is true also for flux-driven JPAs due to intrinsic limitations from internal losses. Another improvement of the MI can be made by further enlarging the codebook size, as is done in this work. We recall that this can be achieved by adding trusted noise on Alice's side or by increasing the initial squeezing level. Once again, the potential increase in MI would be very significant. It is more difficult to accurately gauge the impact of an increase in the squeezing level due to the increase in input noise from the squeezer JPA as well. Making the simple (but unrealistic) assumption that the noise would be unchanged and setting the squeezing level to $S = 10\,\mathrm{dB}$, we obtain from the indistinguishability condition in Eq. (5.73) that the codebook variance could reach $\sigma_{\mathrm{A}}^2 \simeq 6.24$. This impressive increase in codebook variance would result in a relative increase in MI of $\sim 150\%$. An actual implementation would be limited to a smaller value due to the aforementioned input JPA noise. More predominantly, this approach is limited by compression effects of our JPAs, which typically set in at input signal powers around $-130$ dBm, preventing the codebook variance from exceeding values around 10 photons. Traveling-wave parametric amplifiers [183] could serve as alternative phase-sensitive amplifiers in future experiments, commonly tolerating higher input powers with quantum efficiencies comparable to our JPAs. Their broadband amplification properties also enable the implementation of frequency multiplexing techniques, which deliver significantly higher secure bit rates. Lastly, the secret key rates could be largely improved by optimizing the symbol rates of our experimental implementation. Here, the main limitation is the phase stabilization of our JPAs, which could be minimized in future experiments by using better frequency filtering in our experimental setup and additional magnetic shielding. Increasing the measurement bandwidth results in an initial increase of the secret key rate at the cost of a larger background noise. To remedy this problem, multiplexing approaches, such as the time multiplexing approach explained in Sec. 5.3.8, can be used. There are also other multiplexing methods, for instance, frequency or code-division multiplexing.

Lastly, our experiments show that SQMs implemented with phase-sensitive amplifiers can be considered as a microwave equivalent of optical homodyne detection. More precisely, our experiment demonstrates the possibility of using these SQMs to unravel properties of quantum states, particularly relevant for quantum state tomography [224, 237]. This approach can be further extended to non-Gaussian state tomography and complements error correction codes by offering a single-shot quadrature detection technique [238, 239]. Our demonstrated results promote the ongoing development of local microwave networks [199, 235, 240], where short-distance secure microwave quantum communication platforms could complement current classical microwave communication technologies such as Wifi and Bluetooth due to the intrinsic frequency and range compatibilities. In this context, we extrapolate in our experiment a secret key rate of 42 kbit/s for our CV-QKD implementation. By using the Shannon-Hartley theorem with our measurement bandwidth of 400 kHz, we estimate an upper bound of our raw secret key rate up to 152 kbit/s for the 2$^{\mathrm{nd}}$ run, paving the way for secure high bit rate microwave CV-QKD communication.

### 5.3.7 Further investigation of mutual information

In this section, we present additional measurements aiming at a more thorough investigation of the MI. Details about these experiments can be found in the Master thesis of Philipp Krüger [241]. For these experiments, the same setup is used as the one presented in Sec. 5.2.1 to implement the same squeezed state CV-QKD protocol. Two different squeezing levels of $S =$

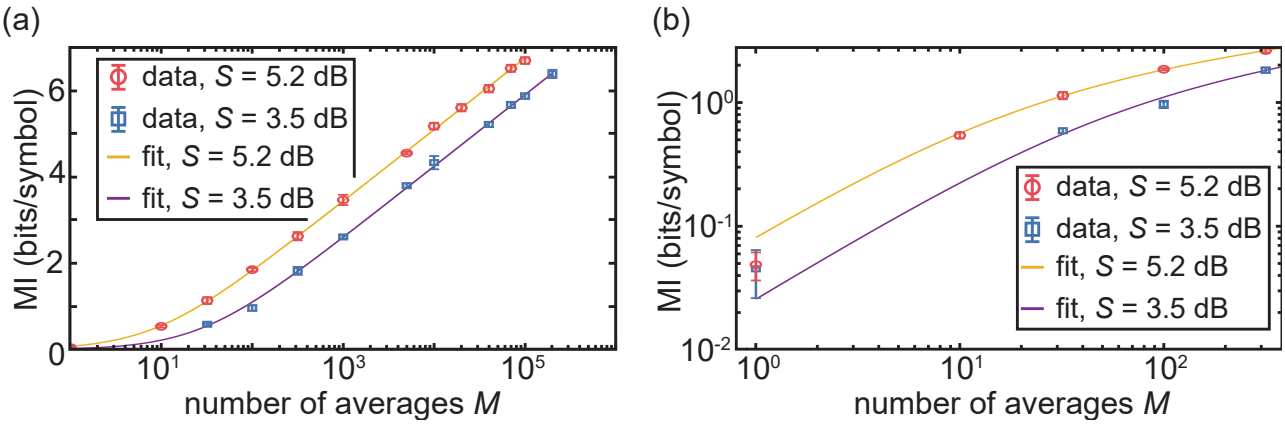


Figure 5.12: Extracted MI as a function of the number of measurement averages $M$ in the experiment for both squeezing levels. The solid lines represent fits of the MI according to the expression $I = \log_2(1 + M\,\mathrm{SNR})/2$ and serve as a guide to the eye. The panel (b) is a zoom of the results shown in panel (a) in the region of low numbers of averages. In particular, we observe a nonzero MI for $M = 1$, corresponding to no averages of the MI. We note an excellent agreement between our model and the measured MI for both squeezing levels.

3.5 dB and $S = 5.2$ dB are chosen for the squeezer JPA, operated at the frequency of $\omega_J/2\pi = 5.5231$ GHz. The resulting squeezed states are produced with the high purity of $\mu = 0.96$ and $\mu = 0.95$, respectively. This implies that little to no input noise is present on Alice's preparation side. Due to the indistinguishability condition $\sigma_A^2 = \sigma_{as}^2 - \sigma_s^2$, a direct approach to increase the codebook variance is to increase the squeezing level. We measure a resulting codebook variance of $\sigma_A^2 = 0.5\,(S = 3.5\,\mathrm{dB})$ and $\sigma_A^2 = 1.4\,(S = 5.2\,\mathrm{dB})$. The CV-QKD protocol is implemented with $N = 150$ different symbols drawn from a random Gaussian variable with zero mean and a variance $\sigma_A^2$ using the random number generation tool of the programming language MATLAB®. Based on Eq. (5.52), one can write the mutual information as $I(\mathcal{K}_A : \mathcal{K}_B) = \log_2(1 + \mathrm{SNR})/2$. This expression offers the important advantage of being independent of any rescaling of Alice's or Bob's key and captures core correlations between their datasets as explained in Sec. 5.3.1. Starting by modelling the measured symbols of Bob $\{\beta_i\}_{i\in[1,N]}$ as result of a Gaussian random variable $B$ related to the Gaussian random variable $A$ of Alice, from which she draws her symbols $\{\alpha_i\}_{i\in[1,N]}$, we write $B = \sqrt{\tau_{tot}}A + N$, Using this notation, the SNR can be expressed as

$$\mathrm{SNR} = \frac{\mathrm{Cov}(A,B)}{\mathrm{Var}(N)} = \frac{\sqrt{\tau_{tot}}\mathrm{Var}(A)}{\mathrm{Var}(N)}. \tag{5.84}$$

If the measurements of each symbol $\beta_i$ are repeated $M$ times for a fixed symbol $\alpha_i$ and averaged over these $M$ measurements, the new resulting SNR$'$ is computed as

$$\mathrm{SNR}' = \frac{\sqrt{\tau_{tot}}\mathrm{Var}(A)}{\mathrm{Var}(\frac{1}{M}\sum_{k=1}^{M} N_k)} = \frac{\sqrt{\tau_{tot}}\mathrm{Var}(A)}{\frac{1}{M^2}\sum_{k=1}^{M}\mathrm{Var}(N_k)} = M\frac{\sqrt{\tau_{tot}}\mathrm{Var}(A)}{\mathrm{Var}(N)} = M\,\mathrm{SNR}. \tag{5.85}$$

where each random variable $N_k$ represents the noise for a given symbol measurement $k \in [1, M]$. The main difference between the signal and the noise is that over the $M$-times repeated measurements of $\beta_i$, the corresponding symbol $\alpha_i$ of Alice is unchanged.

We observe that averaging over many measurements leads to a linear increase of the SNR and, therefore, the computed MI scales logarithmically with the number of averages. In these measurements, the coupled noise photon number is set to a low photon number $\bar{n} = 0.05$. The MI is computed using the formula in Eq. (5.52), and we show the results for both squeezing levels in Fig. 5.12. In these measurements, the amplifier JPA is not used and detuned from

the working frequency, implying that a large amplification noise is present. We observe an excellent agreement between our predicted scaling of the mutual information and the measured data for both squeezing levels. We distinguish two regimes, a linear regime (in logarithmic scale) when the number of averages is large enough, which agrees with our model in Eq. (5.85), and a second regime for a low number of averages. There, we note that for both squeezing levels we obtain a low but nonzero mutual information of $I(\mathcal{K}_\mathrm{A}\colon\mathcal{K}_\mathrm{B}) = 0.035\,(S = 3.5\,\mathrm{dB})$ and $I(\mathcal{K}_\mathrm{A}\colon\mathcal{K}_\mathrm{B}) = 0.095\,(S = 5.2\,\mathrm{dB})$ for the case $M = 1$, corresponding to noisy single-shot measurements.

### 5.3.8 Time multiplexing method

In this section, we investigate the implementation of a time-multiplexing method to improve the protocol's performance. In the previous experiments, during each measurement cycle, only one symbol was encoded and measured. This limits the rate of symbols that can be communicated during the measurements, as one full measurement cycle needs to be completed before another symbol can be sent. One possible approach to circumvent this limitation is to implement a time-multiplexing method. The idea is to divide the fraction of the time trace dedicated to the measurement of a given symbol from Alice into multiple ones, effectively encoding several symbols at once. This procedure allows for an increase in the symbol rate, which in turn allows for a significant improvement in the secret key rate during experiments. Details about this experiment can be found in the Master thesis of Valentin Weidemann [233]. The CV-QKD protocol is experimentally implemented as described in Sec. 5.2.1. The measurement time previously corresponding to one individual symbol is divided into $M$ sections, each ascribed to a different symbol. Such an implementation yields $M$ keys of $N$ symbols. The experimental implementation is illustrated in Fig. 5.13. One can merge all the different keys into one new, effective key. Combining all keys together provides one key with reduced finite-size effects originating from the finite number of symbols (see Sec. 5.3.4). The associated secret key rate is increased correspondingly. Naively, one would expect a linear increase by a factor $M$ in the secret key rate. However, in practice, a smaller effect is obtained due to experimental constraints as discussed in this section. In our experiments, $M$ keys are combined into one effective key, with each key being drawn from a zero-mean Gaussian distribution with a variance $\sigma^2_{\mathrm{A},k}$. The variance of the combined key reads

$$\sigma^2_\mathrm{ens} = \frac{1}{M}\sum_{k=1}^{M}\sigma^2_{\mathrm{A},k}. \tag{5.86}$$

In our experiments, during a single measurement cycle of one symbol of Alice, the power of each device involved in the measurements is set to a constant value. Here, to obtain different displacements within one cycle, we modulate the power of the microwave source we use to perform the displacement operations with $M$ different modulation voltages. This results in $M$ different modulation conversion factors $c_k$ relating an induced displacement complex amplitude $\alpha$ to a corresponding measured power $P_k$ as $P_k = c_k|\alpha|^2$. Initially, a key is randomly generated on Alice side providing $N$ symbols $\mathcal{K}_\mathrm{A} = \{\alpha_i\}_{i\in[1,N]}$ with a variance $\sigma^2_\mathrm{A}$. In the experiment, we set the first conversion factor to be the largest conversion factor. Discarding small negligible offsets in the calibration, we obtain $M$ new symbols $\alpha_{i,j}$ for each individual symbol $\alpha_i$ of Alice which are defined as

$$\left|\alpha_{i,k}\right|^2 = c_k P_i = c_k\frac{\left|\alpha_i\right|^2}{c_1},\ \text{for}\ (i,k)\in[1,N]\times[1,M], \tag{5.87}$$

The previous construction results in $M$ keys $\mathcal{K}_{\mathrm{A},k} = \{\alpha_{i,k}\}_{i\in[1,N]}$ with $k\in[1,M]$. Each key is described by a Gaussian random variable with zero mean and variance $\sigma^2_{\mathrm{A},k} = (c_k/c_1)\sigma^2_\mathrm{A}$.

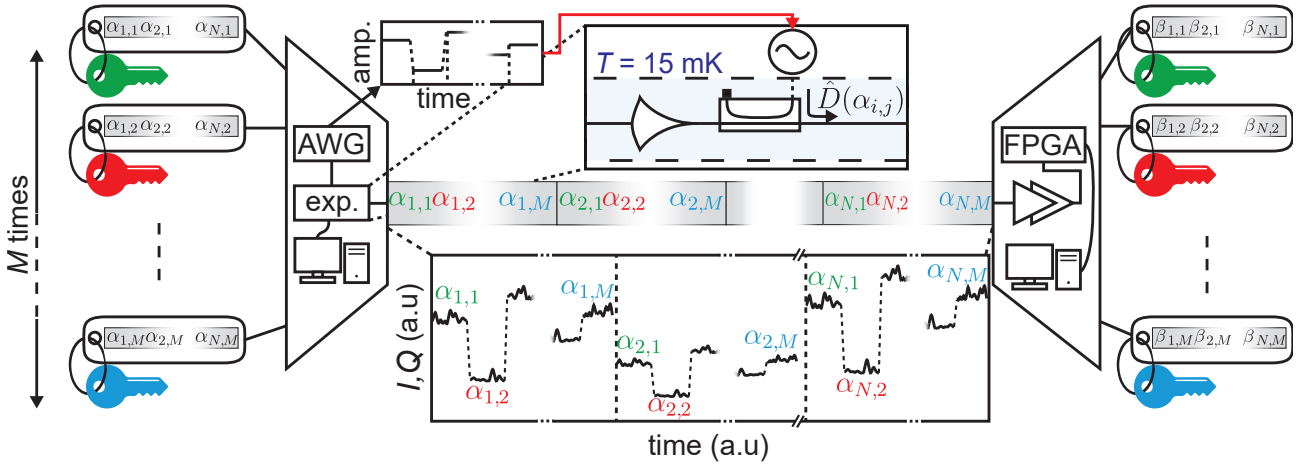


Figure 5.13: Schematic representation of the experimental implementation of the time-multiplexing method. $M$ keys are used in the experiment, each key is encoded using an AWG by modulating in time the displacement operation $\hat{D}(\alpha_{i,j})$ induced at the first directional coupler using an SGS source, as depicted in the inset. Each symbol of each key corresponds to a measured $I/Q$ data point. The symbols are subsequently measured after amplification by the measurement JPA, and the data is processed with our FPGA setup, resulting in $M$ measured keys.

We note that the definition of the displacement complex amplitudes in Eq. (5.87) implies a deterministic ratio between the different keys

$$\frac{\sigma^2_{\mathrm{A},k}}{\sigma^2_{\mathrm{A},k'}} = \frac{c_k}{c_{k'}}. \tag{5.88}$$

Since by construction, $c_1$ is larger than the other conversion factors, it results from the definition of the total variance in Eq. (5.86) that $\sigma_1^2 > \sigma^2_{\mathrm{ens}}$.

We experimentally verify the benefit of the modulated displacement approach using the same setup as presented in Sec. 5.2.1. In this experiment, we use the frequency of $\omega_{\mathrm{J}}/2\pi = 5.856\,\mathrm{GHz}$ and operate the squeezer JPA with a squeezing level of $S = 8.0(1)\,\mathrm{dB}$. The measurement JPA is operated with an amplification gain of $G_{\mathrm{J}} = 20.7(3)\,\mathrm{dB}$ and an expected quadrature quantum efficiency of $\eta = 0.56(4)$. Additionally, we generate $M = 6$ different keys using the modulated displacement approach, for $N = 3333$ symbols in each key. We extract the SNRs from the prepared keys of Alice and the measured keys of Bob according to Eq. (5.52). Since each key is generated only with a different modulation voltage from each other, the prime difference between each key is their codebook variance $\sigma^2_{\mathrm{A},k}$. According to Eq. (5.88), we expect to observe that

$$\frac{\mathrm{SNR}_k}{\mathrm{SNR}_{k'}} = \frac{\sigma^2_{\mathrm{A},k}}{\sigma^2_{\mathrm{A},k'}} = \frac{c_k}{c_{k'}}. \tag{5.89}$$

We note that this relation remains true if the measured SNRs are also averaged over the coupled noise photon, since additional noise by Eve does not change the codebook variance. In Fig. 5.14 (a), we show the measured SNR ratios, where all SNRs ratios are referenced to the largest SNR. We observe a good agreement between our model and the measurement, indicating the validity of our modulated displacement implementation. We note that these ratios are insensitive to any rescaling of measured data. Using the different keys with an associated codebook variance $\sigma^2_{\mathrm{A,k}}$, we additionally compute a corresponding MI using that $I(\mathcal{K}_{\mathrm{A},k}, \mathcal{K}_{\mathrm{B,k}}) = \log_2(1+\mathrm{SNR}_k)/2$ for three cases: (i) the key with the largest individual codebook variance $\sigma^2_{\mathrm{A},1}$, (ii) combining keys with the two largest codebook variances, $\sigma^2_{\mathrm{A},1}$ and $\sigma^2_{\mathrm{A},2}$, and (iii) combining all $M = 6$ keys together resulting in an effective ensemble codebook variance $\sigma^2_{\mathrm{ens}}$. We show

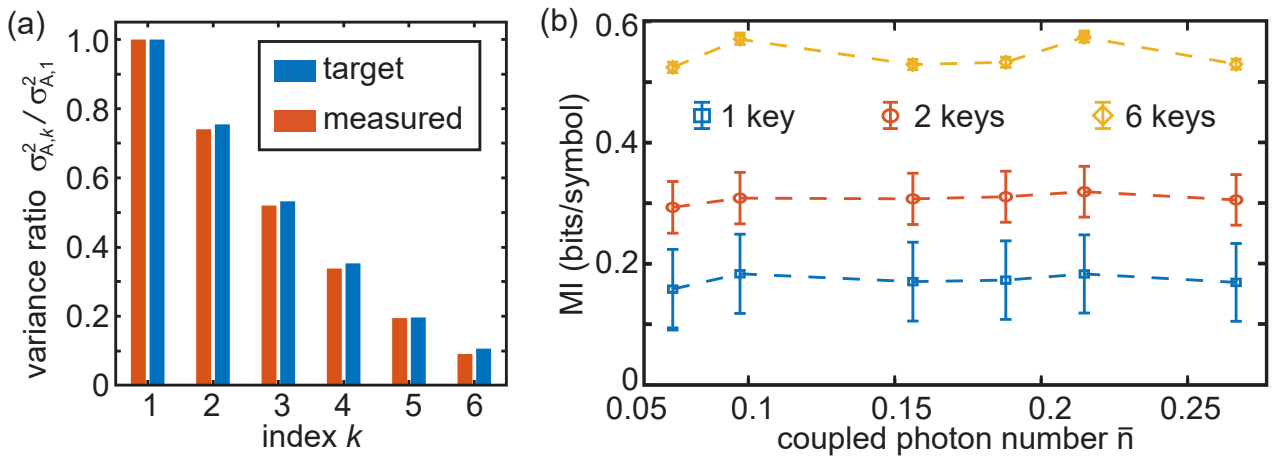


Figure 5.14: Time-multiplexing results. (a) Measured codebook variance ratios compared to the values expected according to Eq. (5.89). (b) Measured MI for the codebook with the largest individual codebook variance $\sigma^2_{\mathrm{A},1}$. Additionally, we show the extracted MI obtained by combining together the keys for the two largest codebooks ($\sigma^2_{\mathrm{A},1}$ and $\sigma^2_{\mathrm{A},2}$), labelled "2 keys". Lastly, we show the MI obtained by combining all keys together resulting in an average codebook variance given by $\sigma^2_{\mathrm{ens}}$ in Eq. (5.86), which we label as "6 keys".

the resulting values as a function of the coupled noise photon $\bar{n}$ in Fig. 5.14 (b). We note that the MIs appear not to depend on the noise photon number due to the presence of a larger detection noise as compared to the one predicted by our expected quadrature quantum efficiency, effectively rendering extracted MIs insensitive to the much weaker coupled photon number $\bar{n}$. By then merging all the keys together, we obtain a large key with the same signal noise as for the individual ones but with a new codebook variance given by $\sigma^2_{\mathrm{ens}}$. We obtain the ensemble MI and MI using the largest individual codebook variance as

$$I_{\mathrm{ens}} = \frac{M}{2}\log_2\left(1+\frac{\tau\sigma^2_{\mathrm{ens}}}{\sigma^2_{\mathrm{n}}}\right) > I_1 = \frac{1}{2}\log_2\left(1+\frac{\tau\sigma^2_1}{\sigma^2_{\mathrm{n}}}\right), \tag{5.90}$$

where the factor $M = 6$ is included to account for the increased symbol rate and $\sigma^2_{\mathrm{n}}$ is the noise variance in the measurements. Based on the formalism in Sec. 5.3.3, we compute the corresponding Holevo quantities for the merged key and individual key with the associated resulting secret key rates. Based on our measurement bandwidth of 400 kHz, we obtain a maximal secret key rate upper bound of $R = 21$ kbits/s for the secret key using only the individual key with the largest codebook variance $\sigma^2_{\mathrm{A},1}$ and of $R = 54$ kbits/s for the ensemble key, i.e., an increase by a factor $\sim 2.6$.

In conclusion, the time-multiplexing approach allows for a significant improvement of the secret key rates in our microwave CV-QKD. The main limitations arise from both the stability of the devices (e.g., stability of the measurement JPA) and technical limitations (e.g., modulation voltage implementation).

# Chapter 6

# Coupling microwave states to spin ensembles

In this chapter, we introduce a spin ensemble formed with phosphorus atoms embedded in a silicon matrix, with gigahertz Zeeman transition frequencies which are probed by coupling the spin ensemble to a niobium superconducting resonator. Such a hybrid system serves as a good quantum memory candidate for the storage of propagating microwave signals and in quantum communication protocols. In this chapter, we demonstrate that propagating microwave signals can be efficiently coupled to the spin ensemble, allowing for later retrieval of the stored signals. This part of the work was obtained with the support of *Prof. Dr. Hans Huebl* and *Patricia Oehrl*. We first present a brief modelling of spin ensembles in Sec. 6.1. Subsequently, we introduce the experimental setup in Sec. 6.2 that we use for characteristic measurements of the spin-resonator system. Using our room temperature detection setup, we additionally perform measurements of the squeezing level of quantum states, initially prepared as squeezed states using a JPA, before and after coupling to the spin-resonator system.

## 6.1 Spin ensemble concept

Over the last decades, spin systems have been intensively studied both in fundamental research and regarding applications, ranging from defect spectroscopy in semiconductor industries to biochemical applications [242, 243, 244]. Coupling of spin systems at millikelvin temperatures to propagating microwave signals has been demonstrated to achieve highly-sensitive, quantum-limited spectroscopy such as electron spin resonance spectroscopy [57]. There, a common method to control and read out a spin system is to use a superconducting resonator. However, individual spins present low coupling rates on the order of 10 Hz. These rates can be significantly increased using a spin ensemble − a collection of spins embedded into a host matrix [245, 246]. For quantum applications, phosphorus donors in silicon crystals are promising candidates due to their long spin coherence times, which are particularly relevant in the context of quantum memory applications. Storage of microwave signals in spin-based hybrid systems has been demonstrated, where nonlinear amplifiers such as JPAs have been used to improve the efficiency of spin readout [57, 247]. In this work, we aim to couple a spin ensemble to microwave signals. This offers the possibility of using spin systems as quantum memories in the microwave-based CV-QKD protocol presented in Chap. 5.

Here, we investigate the coupling of microwave signals to a spin ensemble which consists of phosphorus donors in a silicon host crystal at a doping concentration of $[P] = 10^{17}\,\mathrm{cm}^{-3}$. An extensive study of this system can be found in Ref. 248. In this section, we present a short overview of the system with associated theoretical models. We focus particularly on phosphorus donors in an isotopically purified $^{28}$Si: P crystal, with reported extremely long

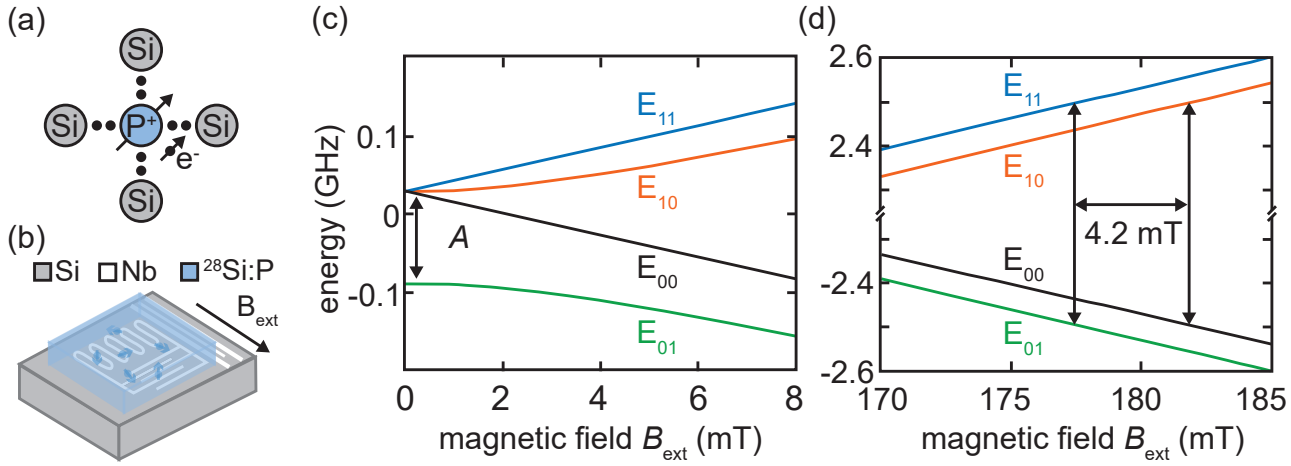


Figure 6.1: Spin energy levels. (a) Schematic of a phosphorus donor atom replacing a silicon atom in a silicon crystal lattice and providing one additional electron. (b) Schematic of the spin ensemble on top of the superconducting Nb resonator. The resonator is fabricated on a silicon substrate. An external magnetic field is applied in-plane, defining the z-axis of the system. (b) Energy levels from Eq. (6.2) for the phosphorus donor spin Hamiltonian in Eq. (6.1). At zero field, three levels are degenerate. (d) Same energy levels as panel (c) for larger magnetic fields. The energy transitions, shown as black arrows, sit in the gigahertz regime.

coherence times of $T_1 > 10\,\mathrm{s}$ [245, 246]. There, a phosphorus donor atom substituting a Si atom offers an additional electron with the associated electron spin, $S = 1/2$, as well as a nuclear spin, $I = 1/2$, from the nuclei of the phosphorus atoms as shown in Fig. 6.1 (a).

In presence of an externally applied magnetic field, $\mathbf{B}_{\mathrm{ext}}$, along the $z$-axis as shown in Fig. 6.1 (b), the spin Hamiltonian of a single phosphorus donor can be expressed as

$$\hat{H}_{\mathrm{s}} = g_{\mathrm{e}}\mu_{\mathrm{B}}\mathbf{S}\cdot\mathbf{B}_{\mathrm{ext}} - g_{\mathrm{n}}\mu_{\mathrm{n}}\mathbf{I}\cdot\mathbf{B}_{\mathrm{ext}} + A\mathbf{S}\cdot\mathbf{I}. \tag{6.1}$$

The g-factors are given by $g_{\mathrm{e}} = 1.9985$ [249] and $g_{\mathrm{n}} = 2.2632$ [250] with with the Bohr magneton $\mu_{\mathrm{B}}$ and the nuclear magneton $\mu_{\mathrm{n}}$. The first two terms in Eq. (6.1) represent the Zeeman interaction of the electron and nuclear spin with the external magnetic field. The hyperfine interaction between these two spins is described with a constant, $A/h = 117.53\,\mathrm{MHz}$ [249], with $h$ the Planck constant. Four eigenvectors can be built for the phosphorus donor spin Hamiltonian based on the state "up", denoted as"1", and "down", denoted as "0", of the electron and nuclear spins. The corresponding four eigenvalues of the phosphorus donor spin Hamiltonian are labelled $E_{ij}$, where the first index is the electron spin and the second is the nuclear spin. We find

$$\begin{aligned} &E_{00} = (A - 2\Delta_{\mathrm{B}})/4\,,\; E_{11} = (A + 2\Delta_{\mathrm{B}})/4, \\ &E_{01} = (-A - 2\sqrt{A^2 + \Sigma_{\mathrm{B}}^2})/4\,,\; E_{10} = (-A + 2\sqrt{A^2 + \Sigma_{\mathrm{B}}^2})/4, \\ &\Delta_{\mathrm{B}} = B_{\mathrm{ext}}g_{\mathrm{e}}\mu_{\mathrm{B}} - B_{\mathrm{ext}}g_{\mathrm{n}}\mu_{\mathrm{n}}\,,\; \Sigma_{\mathrm{B}} = B_{\mathrm{ext}}g_{\mathrm{e}}\mu_{\mathrm{B}} + B_{\mathrm{ext}}g_{\mathrm{n}}\mu_{\mathrm{n}}. \end{aligned} \tag{6.2}$$

At low magnetic fields, the eigenstates split into a spin singlet and triplet state, separated by the hyperfine energy $A$. For high magnetic fields, $B_{\mathrm{ext}} \gg 10\,\mathrm{mT}$, the degeneracy of the triplet state is lifted and typical transition frequencies between the different energy levels are in the gigahertz regime [248], enabling transitions between the levels with input microwave signals. The transitions of interest are between the energy levels $E_{01}$ and $E_{11}$ as well as the energy levels $E_{00}$ and $E_{01}$, as shown in Fig. 6.1 (b,c). These two energy transitions are separated by the hyperfine interaction term, resulting in a magnetic field spacing of 4.2 mT.

**Modelling of the spin ensemble coupled to a microwave resonator.** As indicated above, the spin ensemble is coupled to a superconducting microwave resonator. The coupling of a single spin 1/2 of a phosphorus donor (two-level system) to the modes of the microwave resonator can be described by the well-known James-Cumming Hamiltonian [251]. Here, we use an extension of this model referred to as the Tavis-Cumming Hamiltonian introduced by Tavis et al., describing the coupling of $N$ non-interacting spins to a resonator [252]

$$\hat{H}/\hbar = \omega_{\mathrm{r}}\hat{a}^{\dagger}\hat{a} + \frac{1}{2}\sum_{j=1}^{N}\omega_{\mathrm{s},j}\hat{\sigma}_{\mathrm{z},j} + \sum_{j=1}^{N} g_{0,j}(\hat{\sigma}_{+,j}\hat{a} - \hat{\sigma}_{-,j}\hat{a}^{\dagger}). \tag{6.3}$$

Here, $\hat{a}$ is the cavity mode at the frequency $\omega_{\mathrm{r}}$, coupled to the individual spins of the non-interacting spin ensemble via the coupling rates, $g_{0,j}$. The individual spins at the frequencies $\omega_{\mathrm{s},j}$ are described using the Pauli matrices $\hat{\sigma}_{\mathrm{z},j}$ and ladder operators $\hat{\sigma}_{-,j}$. Collective effects, such as superradiance [253], arise from the fact that the individual spins are linked to each other by their coupling to the resonator. The collective effects lead to a rich dynamics of the spin ensemble. Here, we take advantage of these collective effects to enhance the coupling rate of the spins to the resonator. To investigate the Hamiltonian in Eq. (6.3), it is common to introduce a collective spin operator. Additionally, we make the simplifying assumption that all individual couplings are equal and frequency independent, i.e., $g_{0,j} = g_0$, and introduce the notations

$$\hat{S}_{\pm} = \frac{1}{\sqrt{N}}\sum_{j=1}^{N}\hat{\sigma}_{\pm,j}\,,\ g_{\mathrm{eff}} = \sqrt{\sum_{j=1}^{N}|g_0|^2} = \sqrt{N}g_0. \tag{6.4}$$

Using the previous definitions, we write the Hamiltonian of the system in the frame rotating at a given signal frequency $\omega$ [254]

$$\hat{H}/\hbar = \Delta_{\mathrm{r}}\hat{a}^{\dagger}\hat{a} + \frac{1}{2}\sum_{j=1}^{N}\Delta_{\mathrm{s},j}\hat{\sigma}_{\mathrm{z},j} + g_{\mathrm{eff}}(\hat{S}_{+}\hat{a} - \hat{S}_{-}\hat{a}^{\dagger}). \tag{6.5}$$

The terms $\Delta_{\mathrm{r}} = \omega_{\mathrm{r}} - \omega$ and $\Delta_{\mathrm{s},j} = \omega_{\mathrm{s},j} - \omega$ are the detuning of the resonator and the individual spins, respectively. The dynamics of the system can be derived using equations of motion, similarly to Sec. 2.1.3. We account for the losses of the resonators using internal and external coupling rates, denoted $\kappa_{\mathrm{int}}$ and $\kappa_{\mathrm{ext}}$, respectively. As a result, we modify the Hamiltonian $\hat{H}$ to account for bosonic modes, $\hat{b}_{\mathrm{in}}$ and $\hat{c}_{\mathrm{in}}$, representing input signals to the resonator and internal resonator bath modes, respectively. Additionally, one needs to consider that the spins are not ideal, in particular, that they experience relaxation and dephasing rates $\gamma_1$ and $\gamma_2$ with the associated characteristic time constants $T_1 \propto 1/\gamma_1$ and $T_2 \propto 1/\gamma_2$, respectively. For phosphorus donors in silicon, dephasing effects largely dominate over relaxation mechanisms by several orders of magnitude. The different contributions can be modelled using quantum Lindblad superoperators $\hat{L}$ with collapse operators, $\hat{d}_j$, such that

$$\hat{d}_1 = \sqrt{\kappa/2}\hat{a}\,,\ \hat{d}_{2k} = \sqrt{\gamma_1}\hat{\sigma}_{-,2k}\,,\ \hat{d}_{2k+1} = \sqrt{\gamma_2}\hat{\sigma}_{\mathrm{z},2k+1}\,,\ \hat{L}(\hat{d}_k)\cdot = \hat{d}_k^{\dagger}\cdot\hat{d}_k - \frac{1}{2}\{\cdot,\hat{d}_k^{\dagger}\hat{d}_k\}. \tag{6.6}$$

Here, $\kappa = \kappa_{\mathrm{ext}} + \kappa_{\mathrm{int}}$ is chosen to be the full width at half maximum as in Chap. 2. Furthermore, the $\cdot$ symbol stands for an input operator, and $\{\cdot,\cdot\}$ is the anti-commutator between two operators. The first superoperator describes the physical coupling of the resonator to an outside bath. The even superoperators describe spin relaxation, and the odd superoperators model spin dephasing. Adding the operators $\hat{D}(\hat{d}_k)$ to the equations of motion, one can derive the full dynamics for resonator and spin modes. For the operators considered in this section, the full

equation of motion reads

$$\frac{\mathrm{d}\hat{O}}{\mathrm{d}t} = -\frac{i}{\hbar}[\hat{O}, \hat{H}] + \sum_{j=1}^{N} \hat{L}(\hat{d}_j)\hat{O}. \tag{6.7}$$

In general, one needs to account for different spin frequencies $\omega_{\mathrm{s},j}$ which may have different origins. First, according to Eq. (6.1) the energy levels of the spins are sensitive to spatial variations of the applied magnetic field. Second, we expect spatial variations of coupling rates and energy levels due to slight variations in the surroundings of the individual spins.

Based on the input-output derivations in Sec. 2.1.3 and using Eq. (6.7), we find that the equations of motion in the frequency domain can be expressed as

$$\begin{aligned} -i\omega\hat{a} &= -i\omega_{\mathrm{r}}\hat{a} - (\kappa/2)\hat{a} - ig_{\mathrm{eff}}\hat{S}_{-} + \sqrt{\kappa_{\mathrm{ext}}}\hat{b}_{\mathrm{in}} + \sqrt{\kappa_{\mathrm{int}}}\hat{c}_{\mathrm{in}}, \\ -i\omega\hat{\sigma}_{-,j} &= -(\gamma_2 + i\omega_{\mathrm{s},j})\hat{\sigma}_{-,j} - ig_0\hat{a}, \end{aligned} \tag{6.8}$$

Based on these equations, we can derive the complex scattering parameter $S_{21}$ using the expectation values of Eq. (6.8). We use the input mode $\hat{b}_{\mathrm{in}}$ as well as the output mode $\hat{b}_{\mathrm{out}}$ corresponding to modes at the input and output of the resonator, respectively. These last two modes are related via $\hat{b}_{\mathrm{out}} = \hat{b}_{\mathrm{in}} - \sqrt{\kappa_{\mathrm{ext}}}\hat{a}$ . We note that by convention, the dephasing rate, $\gamma_2$, is defined as the half-width at half maximum. From Eq. (6.8) we can derive the frequency dependence of the scattering parameter as

$$S_{21}(\omega) = \frac{\langle\hat{b}_{\mathrm{out}}\rangle}{\langle\hat{b}_{\mathrm{in}}\rangle} = 1 - \frac{\kappa_{\mathrm{ext}}}{i\Delta_{\mathrm{r}} + \kappa/2 + \kappa C(\omega)/2}\,, \text{ with } C(\omega) = \sum_{j=1}^{N} \frac{2g_{0,j}^2}{\kappa(\gamma_2 + i\Delta_{\mathrm{s},j}(\omega))}. \tag{6.9}$$

From Eq. (6.9), we expect an avoided crossing between the energy levels of the resonator and spin ensemble, illustrating a hybridization of the two systems which we confirm in our measurements (see Sec. 6.2.1). The level splitting between the hybridized modes is given by the effective coupling rate $g_{\mathrm{eff}}$. Therefore, the measurement of $S_{21}(\omega)$ provides direct information on the effective coupling strength of the resonator and the spin ensemble. The coupling rate of each individual spin to the resonator can then be derived from Eq. (6.4) by estimating the total number $N$ of coupled spins. Additionally, for large spin-resonator detuning, $\Delta_{\mathrm{r}} - \Delta_{\mathrm{s},j} \gg g_{\mathrm{eff}}$, the transmission spectrum of $S_{21}$ simplifies to that of the resonator alone. As a result, both the resonator and spin resonances can be seen in the $S_{21}$ spectra measured as a function of the externally applied magnetic field.

## 6.2 Experimental cryogenic setup

The experiments are performed in an Oxford Triton 400 dilution refrigerator, a similar system to that presented in Sec. 4.1.1. Details about this system can be found in Ref. 248. The main difference of this cryostat is the presence of a three-axis superconducting vector magnet, which allows for experiments in the microwave regime with magnetic fields applied in an arbitrary direction. The magnet offers a maximum field of 6 T along the $z$-axis. Importantly, additional coils are used to compensate for the magnetic field, ensuring that the field is primarily confined to the sample stage where the spin ensemble is located. The samples are mounted such that they are positioned at the center of the vector magnet, as shown in Fig. 6.2 (a). Additionally, thermalization of the sample is provided using silver wires. Thick, long silver wires thermally anchor the bottom of the sample stage directly to the mixing chamber. To preserve sensitive quantum properties, all devices at the sample stage are connected via superconducting coaxial NbTi cables (SC-219/50-NbTi-NbTi from Coax. Co). Attenuators are thermally clamped at each temperature stage of the cryostat to suppress incoming room temperature noise. The

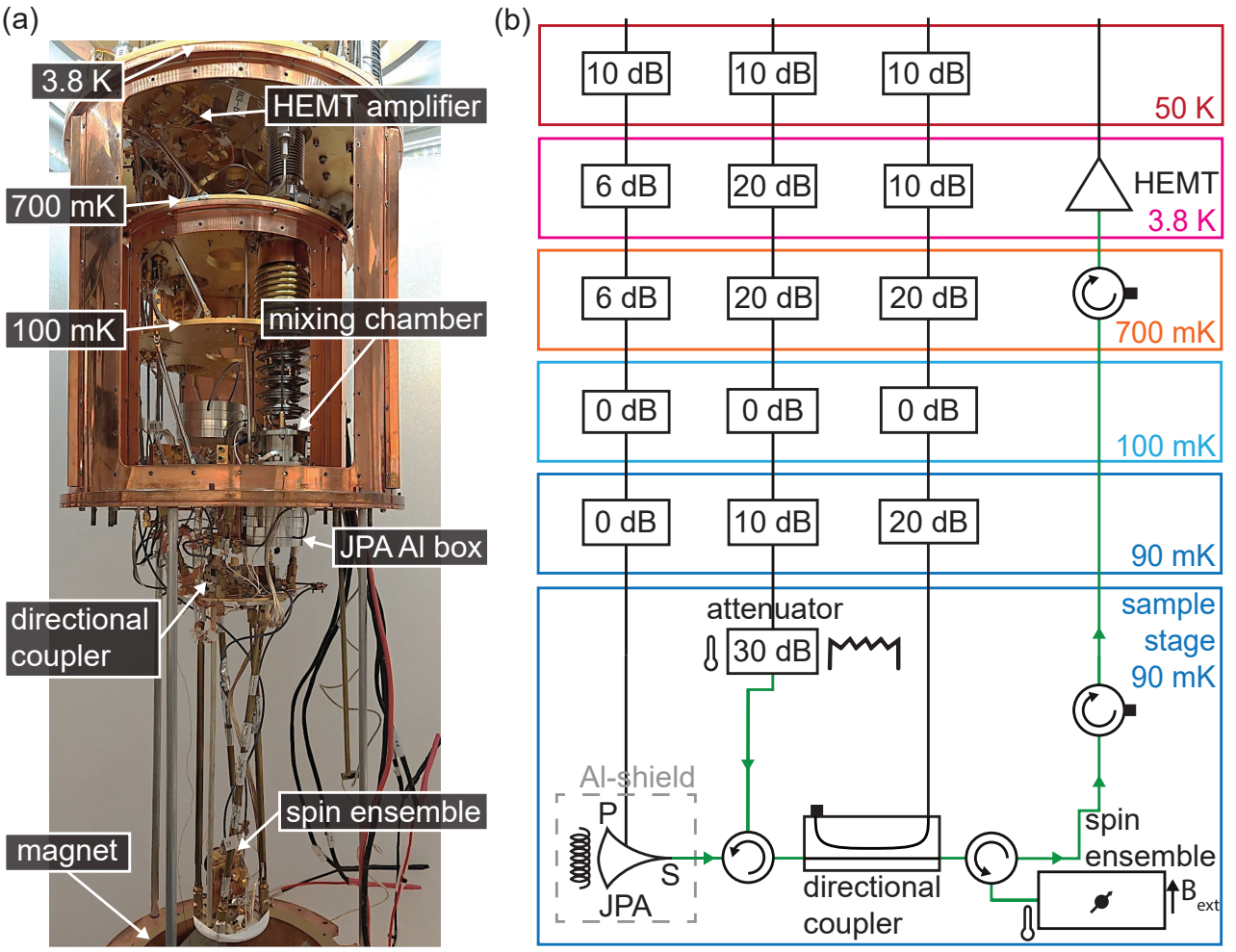


Figure 6.2: Experimental cryogenic setup. (a) Photograph of the Oxford Instruments Triton dilution refrigerator with different highlighted temperature stages. At the sample stage, we mount an aluminium box containing a JPA, which is connected to the spin ensemble positioned below it. The spin ensemble is placed in the center of the magnetic field generated by the 3D superconducting vector magnet (shifted down to a lower position in the photograph). (b) Schematic drawing of the measurement setup consisting of the JPA coupled to the spin ensemble. At the input line, an input 30 dB attenuator acts as a quasi-black body radiator to perform Planck spectroscopy measurements. The spin ensemble can be addressed alone via the directional coupler, bypassing the JPA. Green lines represent superconducting cables.

attenuator configuration used in the measurements is shown in Fig 6.2 (b). A circulator with a 50 Ω load is used to prevent backward propagating thermal noise from higher temperature stages.

Our experimental setup contains a JPA, which we use to generate squeezed states. This JPA is fabricated at the Walther-Meißner-Institut using a similar design as presented in Sec. 4.2 and with the same working principle. Fabrication details can be found in Ref. [255]. The JPA is connected to a heatable input attenuator, which we use for Planck spectroscopy measurements, in a configuration such as presented in Sec. 4.3.1. The JPA is enclosed in an aluminium box to shield external stray magnetic fields and prevent magnetic field crosstalk with other surrounding magnetic components. The spin ensemble has the dimensions $\sim 800\,\mu\text{m} \times 800\,\mu\text{m} \times 20\,\mu\text{m}$. It is fixed with a Marabu Fixo gum glue on top of the superconducting niobium resonator. The resonator is embedded into a sample box, mounted at the bottom of the sample stage. This sample box is connected to the JPA with a cryogenic directional coupler (CPL2000-18000-30-C from Sirius Microwave) in between. The latter allows for individual probing of the spin

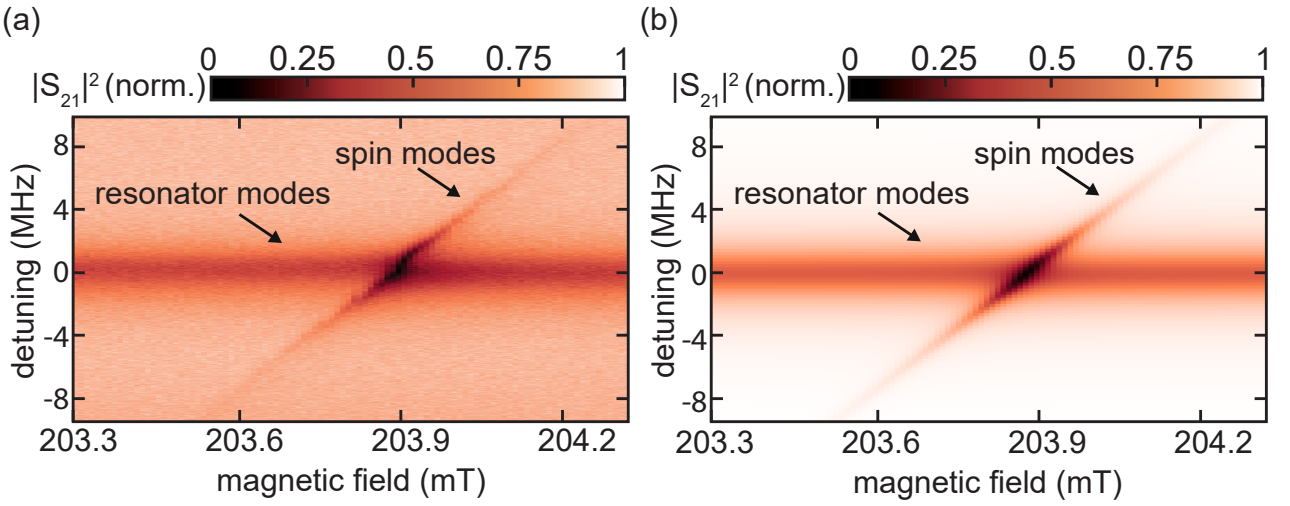


Figure 6.3: Avoided level crossing between resonator modes and spin ensemble modes. The avoided crossing is located at the frequency $\omega_s = 5.617\,24\,\mathrm{GHz}$. (a) VNA measurement of the $S_{21}$ scattering coefficient normalized by performing a background subtraction. The y-axis is the frequency detuning from the avoided crossing frequency, $\omega_s$. (b) Theoretical prediction of the scattering coefficient according to Eq. (6.9). The model is plotted for the parameters shown in Tab. 6.1 and is normalized similarly to the VNA measurement in panel (a).[1]

ensemble, bypassing the JPA. At the 3.8 K stage, a cryogenic HEMT (LNC4_8A from LNF) is used to amply signals with a gain of 39 dB and has datasheet noise temperature of 2 K.

### 6.2.1 Spin ensemble measurements

In order to study the coupling of propagating microwave signals to the spin ensemble, we experimentally extract the different system parameters introduced in Eq. (6.9). To this end, we use a VNA (ZVA8 from Rohde & Schwarz) which we connect to the input and output of the cryogenic unit and measure the scattering parameter $S_{21}$, computed as the ratio between input and output voltages at the ports of the VNA. Based on the theoretical description in Sec. 6.1, far from the resonance frequency at which the resonator and spin ensemble hybridize, the input signals from the VNA only probe resonator modes, whereas spins are not excited. In experiments, we measure at a frequency detuning between the resonator and spin modes of $\Delta_s/2\pi \simeq 20\,\mathrm{MHz}$. For the rest of this chapter, the frequency of each individual spins is assumed to be centered around a single frequency, $\omega_s = 5.617\,24\,\mathrm{GHz}$, with a narrow linewidth of $\Gamma/2\pi \ll 1\,\mathrm{MHz}$. Using the VNA, we measure the $S_{21}$ parameter as a function of signal frequency. The scattering parameter, when describing the resonator response, can be described using a complex function given by [256]

$$S_{21}(\omega) = S_0 e^{i\alpha_m} e^{-i\omega\tau_e} \left(1 - \frac{(Q_l/|Q_{ext}|)e^{i\phi}}{1 + 2iQ_l(\omega/\omega_r - 1)}\right), \tag{6.10}$$

where $S_0$ gives the amplitude of the signal with the measurement induced phase drift $\alpha_m$. [2] Similarly, the parameter $\tau_e$ accounts for the electrical delay due to a finite cable length. Overall impedance mismatch is reflected in the phase $\phi$. Here, $Q_l$ is the loaded quality factor and $Q_{ext}$ is the external quality factor defined as in Eq. (2.44). The measured spectrum, as compared to the theoretical mode of Eq. (6.10), is shown in Fig. 6.3. A widespread circle fit routine proposed

[2] We gratefully thank Patricia Oehrl, who performed this measurement and generated the corresponding model prediction.

| parameter / value parameter | $\kappa_{\mathrm{ext}}/2\pi$ | $\kappa_{\mathrm{int}}/2\pi$ | $\gamma_2/2\pi$ | $g_{\mathrm{eff}}^2/2\pi$ | $\omega_{\mathrm{s}}/2\pi$ | $\omega_{\mathrm{r}}/2\pi$ |
|---|---|---|---|---|---|---|
| rates (MHz) / frequencies (GHz) | 5.2 | 0.7 | 0.5 | 0.5 | 5.1724 | 5.6169 |

Table 6.1: Summary of the characteristic parameters of the coupled resonator-spin system. The internal quality factor of the resonator is obtained by fitting the data with Eq. (6.10) using an $S_{21}(\omega)$ measurement far detuned from the spin resonance, typically on the order of 20 MHz. The spin dephasing rate is obtained by fitting the data using an off-resonance response of the spin modes in Fig. 6.3 with a resonator-spin detuning of 10 MHz. The coupling between the spin ensemble and resonator is extracted from a fit of Eq. (6.9) to the measured VNA data in Fig. 6.3.

by Probst et al. [256] can be used to precisely fit the $S_{21}$ response according to Eq. (6.10). From this fit, we extract the resonator frequency with the associated loaded and external quality factors. We extrapolate the internal quality factor $Q_{\mathrm{int}}$, using the definition of quality factors in Eq. (2.44).

Based on our analysis in Sec. 6.1, the finite coupling between the resonator and spin-ensemble modes results in an exchange of excitations between the resonator and the spin modes at an effective rate $g_{\mathrm{eff}}$ when these two modes are tuned in resonance by the applied magnetic field. The resulting hybridized modes appear as an avoided level crossing in the measured $S_{21}(\omega)$ spectra. At frequencies far off-resonant from the resonator (spin) mode, only the spin-like (resonator-like) modes are excited as shown in Fig. 6.3. The average response of the spin-like modes at constant applied magnetic field (vertical cuts), far away from the resonance field, can be fitted according to the Lorentzian function

$$L(\omega) = \frac{C}{\pi} \frac{\gamma_{\mathrm{s}}}{(\omega - \omega_{\mathrm{s}})^2 + (\gamma_{\mathrm{s}})^2}, \tag{6.11}$$

where the half width at half maximum of the Lorentzian, defined by the spin ensemble dephasing rate, $\gamma_{\mathrm{s}}$, is used as a fitting parameter. Additionally, we fit the Lorentzian amplitude with a fitting parameter $C$. The detuning between the resonator frequency $\omega_{\mathrm{r}}$, and the spin mode frequency used in the Lorentzian function fit is set to 10 MHz.

Lastly, using the previously determined resonator coupling rates, $\kappa_{\mathrm{ext}}$ and $\kappa_{\mathrm{int}}$, as well as the spin dephasing rate, $\gamma_2$, as fixed parameters, we fit the full $S_{21}(\omega, B_{\mathrm{ext}})$ response given in Eq. (6.9) as a function of both signal frequency, $\omega$, and applied magnetic field, $B_{\mathrm{ext}}$. The mapping between applied field and corresponding spin frequency, $\omega_{\mathrm{s}}$, is given by the transition from energy level $E_{00}$ to energy level $E_{10}$. This energy transition is computed following Eq. (6.2). From this fit, we extract the collective spin coupling, $g_{\mathrm{eff}}$. Additionally, the fitted parameter values of the measurements described above are shown in Tab. 6.1.

### 6.2.2 Coupling of squeezed state to spin-ensemble

In this section, we investigate the coupling of propagating microwave squeezed states to the spin ensemble. We generate squeezed states using the JPA and measure the squeezing level as a function of applied pump power. Squeezing levels are extracted following the procedure described in Sec. 4.3.4. In order to enable the coupling of the squeezed states to the resonator-spin system, we use the external magnetic field, $B_{\mathrm{ext}}$, to tune the resonator frequency. More precisely, the superconducting resonator presents a non-negligible kinetic inductance due to the kinetic energy of superconducting charge carriers. One defines the kinetic inductance using the London penetration length, $\lambda_{\mathrm{l}}$, such that [257]

$$\frac{1}{2} L_{\mathrm{k}} I^2 = \frac{\mu_0 \lambda_{\mathrm{l}}^2}{2} \int_S J_{\mathrm{s}}^2 \mathrm{d}S, \tag{6.12}$$

where integration is performed over a cross-section, $S$, set by the design and dimension of the superconducting resonator. The associated supercurrent density, $J_\mathrm{s}$, leads to a supercurrent defined as $I = \int_S J_\mathrm{s} \mathrm{d}S$. To perform the integral, one takes into account that the supercurrent density is non-vanishing only in a penetration depth of characteristic length $\lambda_\mathrm{l}$. Importantly, this kinetic inductance is linked to the screening supercurrent, which is created at the surface of the superconductor when an external magnetic field is applied. Thus, the superconducting resonator presents a field-dependent kinetic inductance, which results in a tunable resonator frequency.

In our measurements, we first detune the resonator and spin ensemble far from the chosen JPA frequency, $\omega_\mathrm{J} = 5.616\,38\,\mathrm{GHz}$, by setting the applied external magnetic field to $B_\mathrm{ext} = 0\,\mathrm{T}$. The corresponding measured squeezing levels are displayed in Fig. 6.4. We treat these squeezing levels as a reference for the comparison with subsequently measured squeezing levels. Remarkably, we observe that for low pump powers, the squeezing levels reach a value of $S \simeq -0.4\,\mathrm{dB}$, indicating measured variances above vacuum fluctuations. This increased variance is attributed to a finite temperature of $T = 142\,\mathrm{mK}$ of our heatable input attenuator during this measurement. The finite associated variance due to weak thermal fluctuations explains the observed negative squeezing level for low pump powers. Then, we tune both the resonator and the JPA at the common frequency of $5.6169\,\mathrm{GHz}$, corresponding to the magnetic field of $B_\mathrm{ext} = 205\,\mathrm{mT}$. There, we repeat the measurement of squeezing levels. We expect a reduction in the observed squeezing levels due to the enabled coupling between the propagating microwave signals and the resonator. Note that even though the resonator is coupled to the spin ensemble, we do not expect, during these measurements, any contribution from the spins. This is due to the large frequency detuning between the spin ensemble and resonator of $\Delta\omega/(2\pi) \simeq 20\,\mathrm{MHz}$ for the applied magnetic field of $B_\mathrm{ext} = 205\,\mathrm{mT}$. As the last step, the spins, as well as the resonator and JPA, are tuned in resonance at the joint frequency of $5.617\,24\,\mathrm{GHz}$ which corresponds to high-field transition ($E_{00}$ and $E_{10}$ transition) of the Hamiltonian in Eq. (6.1) for the applied external magnetic field of $B_\mathrm{ext} = 203.92\,\mathrm{mT}$. The corresponding squeezing levels are shown in Fig. 6.3 (b). We note a reduction of squeezing levels as compared to the previous coupling with only the resonator, reflecting the contribution of the spin ensemble. To more precisely analyse these results, we construct a model Hamiltonian following the steps in Ref. 247. Here, it becomes crucial to consider additional bath modes $f_j$ to which the spin ensemble is coupled. These modes are associated with the dephasing effects of the spins, the latter being characterised by the dephasing time $T_2$. In general, one needs to additionally account for energy relaxation effects captured by a finite relaxation time $T_1$. However, in our system, relaxation effects are largely dominated by the dephasing of the spins, meaning that the decoherence time is in godd approximation given by the pure dephasing time. We use pulse sequence methods as described in Ref. 248 to extract the values of $T_1$ and $T_2$ of the spin ensemble, giving $T_1 = 22.7(7)\,\mathrm{s}$ and $T_2 = 126(2)\,\mu\mathrm{s}$, thus confirming the predominance of dephasing effects. A description of these pulse methods goes beyond the scope of this chapter. Instead, we refer to Ref 258 for technical details of the measurement methods.

The final Hamiltonian of the resonator-spin system in the frame rotating at the resonator frequency, $\omega_\mathrm{r}$, reads

$$\frac{\hat{H}_\mathrm{sr}}{\hbar} = \sum_j^N \left[ g_{0,j}(\hat{\sigma}_{-,j}\hat{a}^\dagger + \hat{\sigma}_{+,j}\hat{a}) + \frac{\Delta_{\mathrm{sr},j}}{2}\hat{\sigma}_{\mathrm{z},j} + i\sqrt{2\gamma_2}(\hat{\sigma}_{-,j}\hat{f}_j^\dagger - \hat{\sigma}_+^j\hat{f}_j) + \Delta_{\mathrm{f},j}\hat{f}_j^\dagger\hat{f}_j \right], \tag{6.13}$$

where $g_{0,j} = g_\mathrm{eff}/\sqrt{N}$ is the coupling of a single spin to the resonator mode $\hat{a}$, $\Delta_{\mathrm{sr},j} = \omega_{\mathrm{s},j} - \omega_\mathrm{r}$, is the detuning of the $j$-th spin to the resonator frequency and $\gamma_s$ is the spin dephasing rate, modelling spin decoherence with an associated noise mode $\hat{f}_j$. We write the $j$-th spin frequency detuning, $\Delta_{\mathrm{f},j}$. Additionally, we account for internal cavity losses with associated mode $\hat{c}_\mathrm{in}$ and

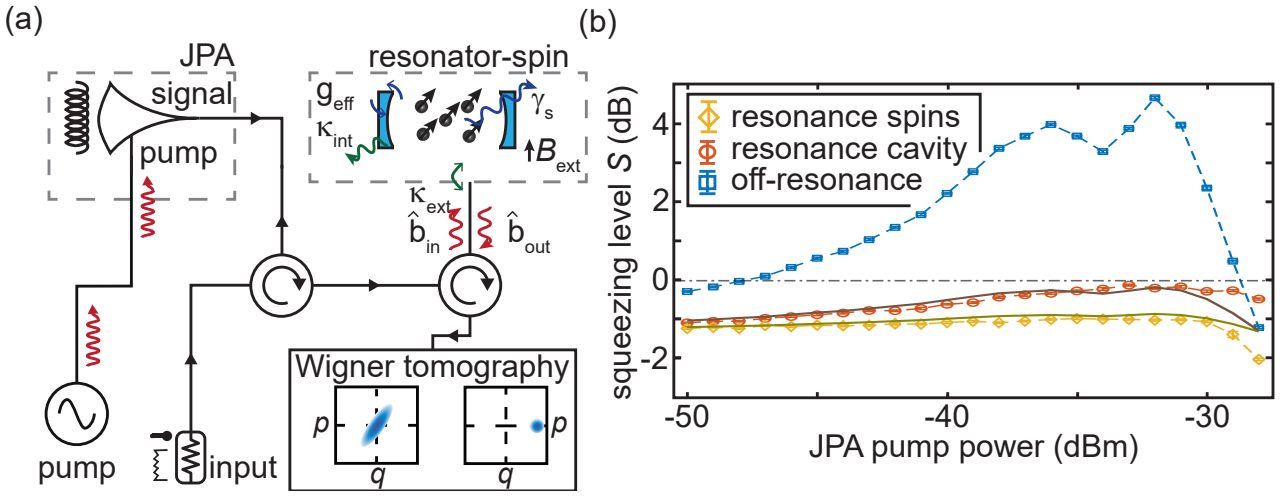


Figure 6.4: Coupling of propagating squeezed states to a coupled resonator-spin system. (a) Scheme of the experimental setup. System parameters are from the Hamiltonian in Eq. (6.13), which provides a detailed model for interactions between the external microwave signals and the resonator-spin system. For each output signal, we perform a Wigner tomography using the Planck spectroscopy, which is experimentally realized with the heatable input attenuator. Color plots depict exemplary Wigner functions. (b) Squeezing level as a function of the JPA pump power for the three different experimental scenarios, as described in the main text. The solid lines represent model predictions based on Eq. (6.15) using the off-resonance squeezing levels as an input.

rate $\kappa_{\mathrm{int}}$. The resonator-spin system is coupled to input microwave modes, $\hat{b}_{\mathrm{in}}$, via a coupling rate $\kappa_{\mathrm{ext}}$. Modes at the output of the resonator-spin system are labelled $\hat{b}_{\mathrm{out}}$. Similarly to Eq. (6.8), one derives the full equations of motion for the operators in the frequency domain as

$$\begin{aligned}
-i\omega\hat{a}(\omega) &= -(\kappa/2)\hat{a}(\omega) + \sqrt{\kappa_{\mathrm{int}}}\hat{c}_{\mathrm{in}}(\omega) + \sqrt{\kappa_{\mathrm{ext}}}\hat{b}_{\mathrm{in}}(\omega) - ig_{\mathrm{eff}}\hat{S}_{-}(\omega),\\
-i\omega\hat{\sigma}_{-,j}(\omega) &= -(\gamma_2 + i\Delta_{\mathrm{sr},j})\hat{\sigma}_{-,j}(\omega) - ig_0\hat{a}(\omega) + \sqrt{2\gamma_2}\hat{f}_j(\omega),\\
\hat{b}_{\mathrm{out}}(\omega) &= \hat{b}_{\mathrm{in}}(\omega) - \sqrt{\kappa_{\mathrm{ext}}}\hat{a}(\omega).
\end{aligned} \tag{6.14}$$

In Eq. (6.14), one can define a $q$-quadrature operator for each operator $\hat{O}$ as $\hat{q}_{\hat{O}} = (\hat{O} + \hat{O}^{\dagger})/2$. Following Ref. 247, we find a relation between the variance of the different $q$-quadrature operators. Here, the variance is defined as $\sigma^2_{\hat{O}} = \langle \hat{q}^2_{\hat{O}} \rangle$. In case of large spin-resonator detuning, $\Delta_{\mathrm{sr},j} > \kappa, \gamma_2$, as well as in resonance condition, $\Delta_{\mathrm{sr},j} = 0$, we obtain a simplified relation between the input signal variance and output signal variance

$$\sigma^2_{\hat{b}_{\mathrm{out}}} \simeq \mathrm{Re}(r(0))^2\sigma^2_{\hat{b}_{\mathrm{in}}} + \mathrm{Re}(l(0))^2\sigma^2_{\hat{c}_{\mathrm{in}}} + \mathrm{Re}(t(0))^2\sigma^2_{\hat{f}_j}, \tag{6.15}$$

with

$$\begin{aligned}
&r(\omega) = 1 - \frac{\kappa_{\mathrm{ext}}}{X(\omega)}\,,\; l(\omega) = \frac{\sqrt{\kappa_{\mathrm{ext}}\kappa_{\mathrm{int}}}}{X(\omega)}\,,\; t(\omega) = \frac{Y(\omega)}{X(\omega)},\\
&X(\omega) = -i\omega + \kappa/2 + \kappa C(\omega)/2\,,\; Y(\omega) = \sum_{j=1}^{N} \frac{\sqrt{2\gamma_2\,\kappa_{\mathrm{ext}}}g_0}{\gamma_2 + i(\Delta_{\mathrm{sr},j} - \omega)}\,,\; C(\omega) = \sum_{j=1}^{N} \frac{2g_0^2}{\kappa(\gamma_2 + i(\Delta_{\mathrm{sr},j} - \omega))}.
\end{aligned} \tag{6.16}$$

Here, we consider only operators with zero mean. Additionally, we assume that all noise modes $\hat{f}_j$ are identical, i.e., that all spins couple to the same bath. Physically, Eq. (6.15) means that microwave signals at the input of the resonator are coupled to resonator modes and spin ensemble modes. One can verify that $|r(\omega)|^2 + |l(\omega)|^2 + |t(\omega)|^2 = 1$, ensuring that the output mode, $\hat{b}_{\mathrm{out}}$, fulfils the bosonic commutation relation. Using the model in Eq. (6.15),

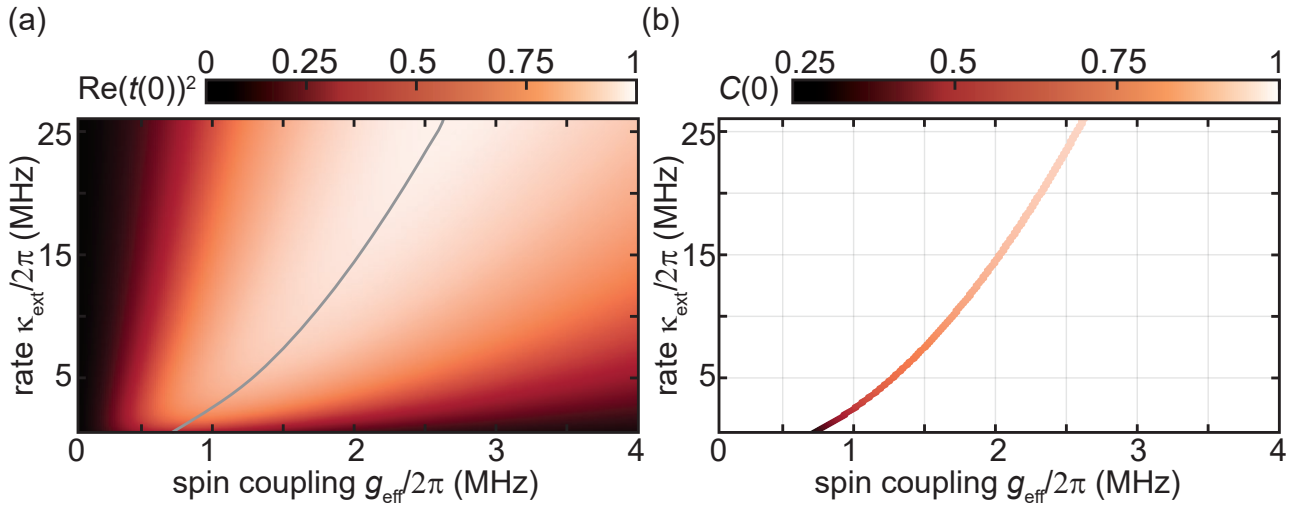


Figure 6.5: Numerical calculation of the coupling efficiency of squeezed microwave states to a spin ensemble. (a) Numerical computation of the coupling efficiency, $\mathrm{Re}(t(0))^2$, as a function of spin coupling rate, $g_{\mathrm{eff}}$, and external coupling rate, $\kappa_{\mathrm{ext}}$. The coupling efficiency is computed according to Eq. (6.15) for $\kappa_{\mathrm{int}}/2\pi = 1.5\,\mathrm{MHz}$ and $\gamma_2/2\pi = 0.5\,\mathrm{MHz}$. The grey line indicates the maximal value of coupling efficiency. (b) Cooperativity as a function of $g_{\mathrm{eff}}$ and $\kappa_{\mathrm{ext}}$ according to Eq. (6.17), with same parameter values as for panel (a). The two parameters ($g_{\mathrm{eff}}$ and $\kappa_{\mathrm{ext}}$) are chosen such that the coupling efficiency, $\mathrm{Re}(t(0))^2$, is maximized.

we investigate the coupling of input $q$-squeezed states to the coupled resonator-spin ensemble system. The measured final variance in our signals (corresponding to the mode $\hat{b}_{\mathrm{out}}$) is expected to be composed of a remaining squeezing contribution of the initial incoming microwave signals and contributions from two environmental baths, one from the resonator and another from the spin ensemble. These two baths are considered to be described by a thermal state [247]. Here, we assume that these thermal baths are at least at the finite temperature of $T = 142\,\mathrm{mK}$, measured at the input of the experimental chain. We fit our model prediction in Eq. (6.15) to measured squeezing levels displayed in Fig. 6.4 using the resonator internal coupling rate, $\kappa_{\mathrm{in}}$, as the sole fitting parameter and keeping all other system parameters as fixed values given from our measurements in Sec. 6.2.1 and in Tab. 6.1. We obtain the fitted value for the resonator internal losses of $\kappa_{\mathrm{int}}/2\pi = 1.5\,\mathrm{MHz}$. This fit value is in good agreement with the value given in Tab. 6.1, considering the large uncertainty of the circle fit routine in the case $\kappa_{\mathrm{int}} \ll \kappa_{\mathrm{ext}}$. We interpret these results as a successful coupling of the incoming squeezed states to the spin-ensemble. Based on our model, we estimate a coupling efficiency of $\mathrm{Re}(t(0))^2 \simeq 35\%$ to the spin ensemble. We note a good agreement between our model and squeezing level measurements as illustrated in Fig. 6.4 (b). However, for large pump powers above $-30\,\mathrm{dBm}$, the model starts to deviate from measured values. We attribute this deviation to higher-order nonlinearities in the JPA. To investigate the coupling of the squeezed states to the spin ensemble, we numerically evaluate Eq. (6.15) as a function of external coupling rate $\kappa_{\mathrm{ext}}$ and spin coupling rate $g_{\mathrm{eff}}$. We focus on the coupling efficiency, $\mathrm{Re}(t(0))^2$, and plot the resulting values in Fig. 6.5 (a). We observe a nontrivial maximum of the coupling efficiency, which reaches up to $\sim 95\%$. However, we find that the nonzero internal resonator losses prevent the coupling efficiency from increasing to unity.

It is insightful to numerically compute the values of spin coupling rate, $g_{\mathrm{eff}}$ and external coupling rate, $\kappa_{\mathrm{ext}}$ that maximise the coupling efficiency, $\mathrm{Re}(t(0))^2$. For each corresponding pair of parameters, we estimate the corresponding cooperativity, $C(0)$, defined as

$$C(0) = \frac{2g_{\mathrm{eff}}^2}{\kappa\,\gamma_2}. \tag{6.17}$$

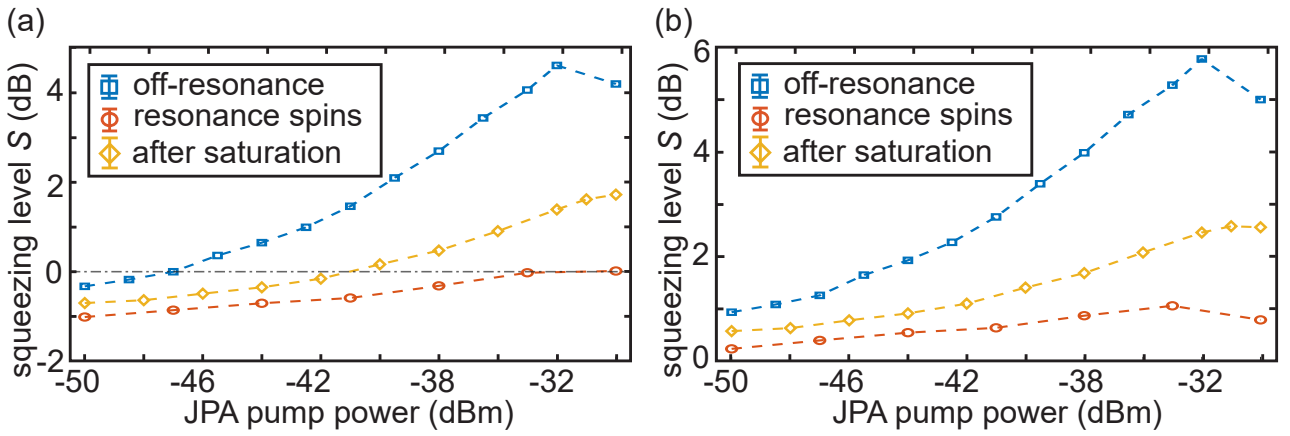


Figure 6.6: Saturation measurements of the spin ensemble. (a) Squeezing levels measured off-resonance, after coupling of the squeezed states to the resonator-spin system, and after saturation pulses applied for $t = 20\,\mathrm{ms}$ to the spin system. (b) Extrapolated squeezing levels as in panel (a) after removal of the squeezed variances of the noise contribution originating from the heatable attenuator.

and show the associated values in Fig. 6.5(b). The cooperativity is a measure of the coherent exchange of excitations in a coupled spin-cavity system. Here, we observe that the cooperativity, leading to maximal coupling efficiency, approaches unity for increasing values of both $\kappa_{\mathrm{ext}}$ and $g_{\mathrm{eff}}$. This result indicates that optimal coupling between squeezed states and the spin ensemble is achieved for the cooperativity $C(0) = 1$. Obviously, it is insufficient to increase only the spin coupling rate, $g_{\mathrm{eff}}$, but this increase has to be balanced with increased resonator and spin loss rates [259, 260, 261]. In the measurements presented in Fig. 6.5, we obtain the cooperativity $C(0) \simeq 0.15$, which explains the rather low coupling efficiency, $\mathrm{Re}(t(0))^2 \simeq 35\%$.

To confirm the coupling of the squeezed states to the spin ensemble, we repeat the squeezing level measurements. We start by tuning out of resonance both the resonator and the spin ensemble, by detuning the frequency from the resonator frequency and setting the external magnetic field to $B_{\mathrm{ext}} = 0\,\mathrm{T}$. In this setting, we measure the squeezing levels as a function of the applied pump power. Subsequently, we bring both the resonator and spin ensemble in resonance by setting $B_{\mathrm{ext}} = 203.92\,\mathrm{mT}$ and again measure corresponding squeezing levels. Additionally, we apply a strong, rectangular-shaped saturation pulse to the spin ensemble via the directional coupler. This pulse consists of a microwave signal with the magnitude of $-120\,\mathrm{dBm}$ at the resonator, with the duration of $t = 20\,\mathrm{ms}$. After this pulse, the spins relax over a measurement time $t_{\mathrm{re}}$ during which no pulse is applied. As a first-order approximation, we expect a fraction of excited spins $\propto \exp(-t_{\mathrm{re}}/T_1)$. We chose a $t_{\mathrm{re}} = 2\,\mathrm{s}$, resulting in an expected population of excited spins of $\sim 91.6\%$. During this time, we measured the squeezing levels at the output of the resonator-spin ensemble system. The corresponding values are plotted as a function of applied JPA pump power and are shown in Fig. 6.6. We observe a clear increase in squeezing levels as compared to the case where the squeezed states are in resonance with the spins or the values were measured after saturation pulses. We interpret this increase as a confirmation of the coupling between input squeezed states and the spin ensemble. However, the squeezing levels do not reach the original values measured off-resonance, due to the presence of the unsaturated resonator. Possibly, the results could also indicate a nonideal saturation process of the spin ensemble.

It is insightful to extract the corresponding squeezing levels in all three measurement cases (off-resonance, in resonance, after saturation pulse) without the parasitic input thermal noise contribution originating from the hot heatable attenuator. Modelling measured states as thermal squeezed states, we write the squeezed and anti-squeezed variances, denoted $\sigma_{\mathrm{s}}^2$ and $\sigma_{\mathrm{as}}^2$,

respectively, as

$$\sigma_{\mathrm{s}}^2 = \frac{1}{4}(1 + 2\bar{n}_{\mathrm{th}}) \exp(-2r)\,,\ \sigma_{\mathrm{as}}^2 = \frac{1}{4}(1 + 2\bar{n}_{\mathrm{th}}) \exp(2r). \tag{6.18}$$

Here, $\bar{n}_{\mathrm{th}}$ is the average thermal noise photon number present in the thermal squeezed states, with an associated squeezing factor $r$. We note that this noise photon number encompasses a contribution from the JPA itself. Based on Eq. (6.18), we see that both the photon number, $\bar{n}_{\mathrm{th}}$, and squeezing factors, $r$, can be straightforwardly computed from measured squeezed and anti-squeezed variances. One obtains squeezed states without the noise contribution from the heatable attenuator by replacing the noise photon number, $\bar{n}_{\mathrm{th}}$, with $\bar{n}_{\mathrm{th}} - \bar{n}_{\mathrm{th}}(T, \omega_{\mathrm{s}})$. Here, $\bar{n}_{\mathrm{th}}(T, \omega_{\mathrm{s}})$ is the estimated noise photon number emitted by the heatable attenuator for the temperature $T = 142\,\mathrm{mK}$ and spin frequency, $\omega_{\mathrm{s}}$. Additionally, we keep the same squeezing factor, $r$, and obtain the squeezing levels shown in Fig. 6.6 (b). We observe that off-resonance squeezing reaches nearly 6 dB below vacuum fluctuations and drops below 1 dB when in resonance with the spin ensemble, supporting our conclusions from the measurement results shown in Fig. 6.4. Lastly, the squeezing levels increase, after the saturation pulses, up to 2 dB, representing a significant increase as compared to measured levels without saturation pulse, which can be seen as a genuine proof of coupling of the squeezed states to the spin ensemble.

## 6.3 Conclusion

In conclusion, we have investigated a spin ensemble consisting of phosphorus donor atoms embedded in a silicon crystal, which is coupled to a superconducting Nb microwave resonator. A theoretical input-output model has been introduced, describing the interaction between the coupled spin ensemble-resonator system and the input microwave signals. Additionally, we have presented a cryogenic experimental setup, which enables precise control of the spin ensemble using microwave signals as well as external magnetic fields provided by a superconducting 3D vector magnet.

Using VNA measurements, we have demonstrated an avoided level crossing between the modes of the spin ensemble and the superconducting Nb resonator. This resonator allows for readout of the spin ensemble while also enabling coupling to external microwave signals. We have calibrated the resonator-spin system by performing complex scattering parameter measurements. From these measurements, we obtained the collective spin coupling rate of $g_{\mathrm{eff}}/2\pi = 0.5\,\mathrm{MHz}$, the spin dephasing rate of $\gamma_2/2\pi = 0.5\,\mathrm{MHz}$, and the total resonator coupling rate of $\kappa/2\pi = 5.9\,\mathrm{MHz}$.

Additionally, we have investigated the coupling of the spin ensemble to propagating squeezed microwave signals. Based on our theoretical model, we have estimated the coupling efficiency of squeezed signals to the spin ensemble to be $\mathrm{Re}(t(0))^2 \simeq 35\%$. Under ideal conditions, where the cooperativity reaches $C(0) = 1$, this efficiency can be increased to nearly unity, mainly limited by internal resonator losses. Experimental measurements using saturating microwave pulses sent to the spin ensemble further confirmed the coupling of microwave squeezed states. These pulses are rectangular shaped, with the duration of $t = 20\,\mathrm{ms}$ and the power of $-120\,\mathrm{dBm}$ at the spin ensemble.

Following the successful demonstration of squeezed state coupling, future experiments can aim at implementing spin-echo pulse sequences to retrieve the stored quantum states.

# Chapter 7

# Conclusion and outlook

In this thesis, we have investigated and developed techniques for the experimental realization of a microwave quantum key distribution (QKD) protocol. As a foundational step, we have introduced the concept of Gaussian states, along with their theoretical description. We have detailed the physical transformations of Gaussian channels that preserve Gaussian properties of quantum states, a crucial result for our experiments. Additionally, we have presented frameworks for the generation and manipulation of Gaussian states, with a particular focus on the Josephson parametric amplifier (JPA), which is employed as a source of propagating microwave squeezed light.

Historically, QKD protocols have been performed at optical frequencies, with first implementations relying on discrete-variable states. Over time, continuous-variable states have been shown to offer a powerful alternative, with more straightforward implementations based on less experimentally demanding systems. These approaches have blossomed into a modern field of secure quantum communication, based on sophisticated quantum key distribution protocols with direct practical applications and ever-growing security investigations. In parallel, tremendous progress in superconducting quantum circuit technologies operated at gigahertz frequencies has been achieved. Therefore, it has become of paramount importance to also consider the potential of QKD protocols in the microwave regime. Using the formalism of Gaussian states, we have analyzed the implementation of a specific QKD protocol using displaced squeezed states. We have found, in agreement with literature results, that in direct reconciliation (DR), the communication is secured for a maximum amount of $\tau = 50\%$ losses and a maximal tolerable coupled noise of $\bar{n} = 0.183$ photons. While the latter remains true, this 3 dB loss limit can been lifted by shifting to reverse reconciliation (RR). As an extension of these results, we have modified our analysis to additionally consider the presence of a detection noise on the receiving side. There, we have compared the newly found security bounds of the CV-QKD protocol to a hypothetical implementation, which would rely solely on coherent states. We have observed that coherent states perform significantly worse than squeezed states. More precisely, we have shown that coherent states can only produce slightly higher secret key rates than squeezed states for minimal amounts of coupled noise, $\bar{n} \leq 0.017$, and for large squeezing levels, $S \geq 10\,\mathrm{dB}$, accounting for the single quadrature quantum efficiency of $\eta_{\mathrm{X}} = 65\%$. Additionally, we have found these values to strongly depend on the presence of the detection noise, which quickly degrades the security performance of the protocols. For these reasons, we have focused on squeezed state CV-QKD, which also offers a significant advantage in resilience to coupled noise photons while being straightforwardly implemented in the microwave regime using nonlinear devices such as the aforementioned JPA. Here, we comment that better noise tolerance can be expected if one makes use of non-Gaussian operations, with a particular focus on photon catalysis standing as a promising tool to extend secure communication distances.

As one of the key results of this thesis, we have demonstrated that the CV-QKD protocol,

from a theoretical point of view, can be implemented in the microwave regime and under open-air conditions. This analysis relies on parameter values, known to be experimentally achievable from the expertise at the Walther-Meissner-Institut in cryogenic systems and superconducting circuits operated at microwave frequencies. We have found that microwave CV-QKD could provide, in ideal conditions, secure communication over distances up to 200 m, making it relevant for short-distance communication platforms that benefit from already existing classical technologies such as WiFi, Bluetooth, and 5G. Remarkably, we have observed that microwave signals could offer an advantage over more conventionally used optical frequencies, such as telecom signals, for short-range communication. In this context, it has become particularly interesting to consider the RR case, where added trusted noise, such as detection noise on the receiving side of the communication, can improve the security of the protocol. Additionally, we have shown that weather conditions, an important aspect to consider for open-air communication, only weakly affect microwave signals, as opposed to telecom ones. In fact, we have found that telecom signals are extremely sensitive to the presence of strong rain or fog, which rapidly induces large absorption losses, far exceeding 1 dB/km, and reducing secure communication distances by several orders of magnitude as compared to ideal weather conditions.

In the next step, we have presented experimental techniques for the practical implementation of the CV-QKD protocol in the microwave regime. First, we have introduced characteristic measurements of JPAs. Additionally, we have presented the room temperature setup used in our experiments with microwave signals. We have shown our post-processing steps to implement the reference state reconstruction method, which allows for a precise evaluation of quantum properties in measured signals. This process relies on a photon calibration which we implement with a novel two-dimensional Planck spectroscopy. Using these techniques, we have obtained reliable calibrations for microwave squeezed, displaced, and thermal states. Additionally, we have presented a new procedure to experimentally investigate the Gaussianity of quantum states based on signal moments up to the fourth order.

As the main milestone of this thesis, we have experimentally realized the displaced squeezed state CV-QKD protocol in the microwave regime using JPAs operated in the phase-sensitive regime. Here, we have demonstrated that unconditional security can be reached in the asymptotic limit, and that microwave CV-QKD could achieve secure communication distances of more than 1 km in a fully cryogenic environment as well as up to 84 m in ideal open-air conditions. This experiment represents the first successful experimental demonstration of microwave CV-QKD. The setup consists of a first JPA 1, which is used for generating microwave squeezed light, followed by two cryogenic directional couplers mounted in series. The first one serves to implement displacement operations on incoming states. The second directional coupler acts as the quantum channel in the communication, which we use to couple a controlled amount of noise to incoming signals, emulating both the presence of an eavesdropper and a potential bright thermal background. As part of our detection chain, we use a second JPA 2 operating as a strong phase-sensitive linear amplifier. Here, we have explained and modeled single quadrature measurements implemented by the JPA 2, providing an analogous measurement to homodyne detection of signals at optical frequencies. The associated quantum efficiency of the detection chain is shown to be primarily dependent on the noise of the measurement JPA 2, which has been measured to reach as high as $\eta_{\mathrm{X}} = 69\%$. In our experimental implementation of the CV-QKD protocol, we have worked with signals at the frequency of $\omega_{\mathrm{J}} = 5.48\,\mathrm{GHz}$ with the fixed squeezing level of $S = 3.6\,\mathrm{dB}$. The measurement JPA 2 has been operated with an amplification gain of $G_{\mathrm{J}} = 19.1\,\mathrm{dB}$ and quadrature quantum efficiency of $\eta_{\mathrm{X}} = 65\%$. Using this setup, we have measured a positive asymptotic secret key for a coupled noise photon number from the quantum channel up to $\bar{n} = 0.062$ in the DR case. The latter has performed better compared to RR due to the low amount of losses in the quantum channel of 0.05 dB, defined by the weak coupling of noise through the second directional coupler. Interestingly, we have

observed that adding trusted noise photons on the preparation side, while maintaining a constant squeezing level, leads to larger amounts of tolerable coupled noise photons in the quantum channel. This counterintuitive feature is a key aspect of CV-QKD protocols, potentially significantly extending communication distances. Additionally, we have included finite-size effects in our analysis and shown that a positive finite-size secret key can be achieved. Our results have proven that key lengths with $N \geq 10^6$ symbols would greatly reduce the impact of the aforementioned effects, ideally reaching $10^8$ or more symbols for practical implementations. Finally, based on our experimental bandwidth of 400 kHz, we have extracted a raw secure bit rate of 152 kbit/s.

Lastly, we have investigated the coupling of our propagating microwave states to a spin ensemble, which is coupled to a superconducting resonator. The spin ensemble presents Zeeman transition frequencies in the gigahertz regime. The interplay with such a hybrid system opens the possibility of adding quantum memories to our QKD protocol implementations. In collaboration with *Prof. Dr. Hans Huebl* and *Patricia Oehrl* from the Walther-Meissner-Institut, we have investigated the storage of squeezed states generated by a JPA, fabricated in-house, to a spin ensemble consisting of phosphorus donor atoms embedded in isotopically purified silicon crystal. Using a cryogenic dilution refrigerator equipped with a superconducting 3D vector magnet, we have shown that we can precisely tune the resonance frequency of the spin ensemble. There, we have first measured squeezing levels at the frequency of $\omega_\mathrm{J} = 5.616\,38$ GHz, which we treat as reference levels. Subsequently, we have shown a reduction in reference squeezing levels by coupling the squeezed states to the superconducting resonator at the frequency of 5.617 24 GHz. The amount of squeezing was further decreased by bringing the spin ensemble into resonance at the frequency of 5.6169 GHz, indicating storage of the squeezed states in the spin ensemble. Based on a modelling of the system and experimental parameters, we have extracted a coupling efficiency of $\sim 35\%$ of propagating microwave signals to the spin ensemble. To confirm our analysis, we have implemented saturation pulses on the spin ensemble. There, we have observed an expected increase in measured squeezing levels after the saturation pulses. However, we have noted that the squeezing level did not reach the reference values, potentially indicating a nonideal saturation of the spins during the measurements.

**Outlook.** The results achieved within this thesis pave the way for the development of QKD experiments at gigahertz frequencies. In future iterations, one could implement additional techniques to improve the performance of CV-QKD protocols, such as using non-Gaussian states and more advanced post-processing methods. Remarkably, having shown the possibility of long-distance secure cryogenic communication, one could integrate such microwave QKD systems in upcoming microwave quantum networks. Such networks are particularly relevant in the context of distributed superconducting quantum computing, where the feasibility of secure quantum communication could be highly beneficial. Here, an all microwave quantum platform offers a specific advantage over relying on optical frequencies. More precisely, motivated by the prospect of increasing communication distances, the development of efficient microwave-to-optics conversion has been an active field of research. However, best state-of-the-art frequency transduction techniques cannot yet provide a conversion efficiency of signals sufficient for long-distance quantum communication experiments.

Additionally, the prospects of theoretically feasible microwave secure communication in open-air conditions stimulates both a fundamental and technical research effort. There, novel technologies can be developed such as quantum microwave antennae serving as a medium between the cryogenic and open-air environments. At the same time, many experiments are to be conducted to investigate practical performances of CV-QKD protocols in the microwave regime with a quantum channel in room temperature conditions. Successful demonstrations of such system would propel the interest for secure microwave communication. Experimental

setups could be paired with the aforementioned non-Gaussian processes, for instance, relying on photon counting. Such techniques are expected to improve protocol performances and help extend communication distances, possibly as a way to combat detrimental effects of unwanted coupled noise during the communication. Lastly, as demonstrated in this thesis, quantum memories based on spin ensemble could be integrated in the currently demonstrated experimental realization. Future investigations would focus on achieving an on-demand retrieval of stored propagating quantum states, greatly relaxing time constrains in microwave CV-QKD protocols.

# Appendix

# Appendix A

# Prepare and measure & entanglement based protocol equivalence

We comment on the equivalence of prepare and measure (PM) CV-QKD protocols, such as the one studied in this work, with corresponding entanglement based (EB) CV-QKD protocols. Here, we focus on the displaced squeezed CV-QKD protocol with single quadrature measurements. Similar derivations can be performed for coherent-state protocols. In general, one finds that both approaches are equivalent and, thus, can attribute virtual entanglement to a PM protocol. That is to say, entanglement is not required to be physically generated for CV-QKD protocols to be secure.

In the studied displaced squeezed state PM protocol, Alice generates quantum states that are sent through a quantum channel to Bob. A symbol, $\alpha_i$, is drawn for each quantum state from a Gaussian distribution with a fixed variance $\sigma_{\mathrm{A}}^2$. Let us first consider that the quantum channel is a pure identity channel, i.e., no losses and noise are present during the communication. For a given state sent by Alice, Bob receives the exact same state corresponding to a displaced squeezed state, with a displacement complex amplitude $\beta_i = \alpha_i$. Without loss of generality, let us assume that Alice's states are squeezed only along the $q$-quadrature. Then, Bob's states have the corresponding displacement vector and covariance matrix

$$\mathbf{d}'_{\mathrm{B}} = (\alpha_i,\, 0)^{\mathrm{T}}\,,\; \mathbf{V}'_{\mathrm{B}} = \begin{pmatrix} \sigma_{\mathrm{s}}^2 & 0 \\ 0 & \sigma_{\mathrm{as}}^2 \end{pmatrix}. \tag{A.1}$$

where $\sigma_{\mathrm{s}}^2$ ($\sigma_{\mathrm{as}}^2$) is the (anti)squeezed variance. To build the EB protocol equivalent, let us consider that Alice and Bob start with sharing a TMS state with a local variance chosen as $\sigma_{\mathrm{as}}^2$ and zero displacement vector. For compactness, we denote $4\sigma_{\mathrm{as}}^2 = V$ and write the covariance matrix of the TMS as

$$\mathbf{V}_{\mathrm{AB}} = \frac{1}{4}\begin{pmatrix} V\mathbf{I}_2 & \sqrt{V^2-1}\boldsymbol{\sigma}_{\mathrm{z}} \\ \sqrt{V^2-1}\boldsymbol{\sigma}_{\mathrm{z}} & V\mathbf{I}_2 \end{pmatrix} = \frac{1}{4}\begin{pmatrix} \mathbf{V}_{\mathrm{A}} & \mathbf{V}_{\mathrm{C}} \\ \mathbf{V}_{\mathrm{C}} & \mathbf{V}_{\mathrm{B}} \end{pmatrix}. \tag{A.2}$$

Alice performs a local measurement where she measures the $q$-quadrature of her mode. Her measurement results in a random value $\alpha_i$. The covariance matrix of Bob's mode conditioned on Alice's measurement is calculated as [154]

$$\mathbf{V}_{\mathrm{B|A}} = \frac{\mathbf{V}_{\mathrm{B}}}{4} - \frac{1}{4V}\mathbf{V}_{\mathrm{C}}\boldsymbol{\Pi}\mathbf{V}_{\mathrm{C}}^{T} \text{ with } \boldsymbol{\Pi} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \tag{A.3}$$

Taken into account that $\sigma_{\mathrm{s}}^2\sigma_{\mathrm{as}}^2 = 1$, we derive

$$\begin{aligned}\mathbf{V}_{\mathrm{B|A}} &= \frac{V}{4}\mathbf{I}_2 - \frac{1}{4V}\begin{pmatrix} V^2-1 & 0 \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} \sigma_{\mathrm{s}}^2 & 0 \\ 0 & \sigma_{\mathrm{as}}^2 \end{pmatrix}\end{aligned}. \tag{A.4}$$

Therefore, the variance of Bob's state conditioned on Alice's measurement coincides with the variance of Bob's displaced squeezed states in the PM version of the protocol. Additionally, one can compute the conditioned displacement vector of Bob's state as [262]

$$\begin{aligned}\mathbf{d}_{\mathrm{B|A}} &= \mathbf{d}_{\mathrm{B}} + \frac{1}{V}\mathbf{V}_{\mathrm{C}}\mathbf{\Pi}((\alpha_i,\, 0)^{\mathrm{T}} - \mathbf{d}_{\mathrm{A}}) \\ &= (\frac{\sqrt{V^2-1}}{V}\alpha_i,\, 0)^{\mathrm{T}},\end{aligned} \tag{A.5}$$

where we use the fact that Alice and Bob start with a zero mean TMS state, implying that their local displacement vectors are $\mathbf{d}_{\mathrm{A}} = \mathbf{d}_{\mathrm{B}} = \bar{\mathbf{0}}_2$. From Eqs. (A.5), (A.4), we observe that Bob's conditional state is a displaced squeezed state with a displacement that differs from the PM case by a prefactor $\lambda = \sqrt{V^2-1}/V$. As a consequence, we consider additionally that, in the EB protocol, Alice rescales her data by the coefficient $\lambda$ resulting in the transformation of her quadrature operators

$$\hat{q}_{\mathrm{A}} \to \lambda\hat{q}_{\mathrm{A}}\ ,\ \hat{p}_{\mathrm{A}} \to \lambda\hat{p}_{\mathrm{A}} \tag{A.6}$$

In that case, one obtains that

$$\begin{aligned}\mathbf{d}_{\mathrm{B|A}} &= \mathbf{d}_{\mathrm{B}} + \frac{\lambda}{\lambda^2 V}\mathbf{V}_{\mathrm{C}}\mathbf{\Pi}((\alpha_i,\, 0)^{\mathrm{T}} - \mathbf{d}_{\mathrm{A}}) \\ &= \frac{1}{\lambda}(\frac{\sqrt{V^2-1}}{V}\alpha_i,\, 0)^{\mathrm{T}} \\ &= (\alpha_i,\, 0)^{\mathrm{T}}.\end{aligned} \tag{A.7}$$

Similarly, we can compute the conditional covariance matrix of Bob as

$$\begin{aligned}\mathbf{V}_{\mathrm{B|A}} &= \frac{V}{4}\mathbf{I}_2 - \frac{\lambda^2}{4\lambda^2 V}\begin{pmatrix} V^2-1 & 0 \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} \sigma_{\mathrm{s}}^2 & 0 \\ 0 & \sigma_{\mathrm{as}}^2 \end{pmatrix}\end{aligned}. \tag{A.8}$$

The results remain valid if we consider the losses, $\varepsilon = 1-\tau$, and coupled noise, $\bar{n}$, induced by the propagation of Alice's states through the quantum channel. In the PM case, the displacement vector and covariance matrix of Bob read

$$\mathbf{d}'_{\mathrm{B}} = (\sqrt{\tau}\alpha_i,\, 0)^{\mathrm{T}}\ ,\ \mathbf{V}'_{\mathrm{B}} = \tau\begin{pmatrix} \sigma_{\mathrm{s}}^2 & 0 \\ 0 & \sigma_{\mathrm{as}}^2 \end{pmatrix} + (1-\tau)(1/4+\bar{n})\mathbf{I}_2. \tag{A.9}$$

In the EB case, if Alice performs her local measurements before sending Bob's modes through the quantum channel, then the previous equivalence between the PM and EB protocols remain valid. If we consider that Bob's modes are sent through the quantum channel prior to Alice's local measurements, we obtain the covariance matrix of Alice's and Bob's TMS state as

$$\mathbf{V}_{\mathrm{AB}} = \frac{1}{4}\begin{pmatrix} V\mathbf{I}_2 & \sqrt{\tau}\sqrt{V^2-1}\boldsymbol{\sigma}_{\mathrm{z}} \\ \sqrt{\tau}\sqrt{V^2-1}\boldsymbol{\sigma}_{\mathrm{z}} & \tau V + (1-\tau)(1/4+\bar{n})\mathbf{I}_2 \end{pmatrix}. \tag{A.10}$$

Similar derivations as in Eqs. (A.5),(A.4) leads again to an equivalence between the PM and EB protocols under the rescaling of Alice's data by the coefficient $\lambda$ in the EB case.

# Appendix B

# Dissipative coupling to bath modes

Here, we investigate the (dissipative) coupling of a system to a bath environment. To this end, we consider a resonator coupled to a dissipative environment modelled as a continuum of modes with a coupling described by a coupling constant $g_0$. Therefore, we start with the following Hamiltonian of such a system

$$\frac{\hat{H}}{\hbar} = \omega_{\mathrm{r}}\hat{a}^{\dagger}\hat{a} + \int \omega_k \hat{b}_k^{\dagger}\hat{b}_k \mathrm{d}k + \int \left(g_k \hat{a}^{\dagger}\hat{b}_k + g_k^{*}\hat{a}\hat{b}_k^{\dagger}\right) \mathrm{d}k, \tag{B.1}$$

where $\omega_{\mathrm{r}}$ is the resonator frequency and $k$ is the wavevector of the bosonic mode $\hat{b}_k$ with a linear dispersion, $kv_k = \omega_k$. Here, mode $\hat{a}$ is the resonator bosonic mode. The different modes fulfil the bosonic commutation relation, meaning that $[\hat{b}_k, \hat{b}_{k'}^{\dagger}] = \delta(k - k')$ and $[\hat{a}, \hat{a}^{\dagger}] = 1$. Additionally, we consider a identical phase velocity for all modes, $v_k = v$, and wavevector-independent coupling, $g_k = g_k^{*} = g_0 = \sqrt{\gamma v/\pi}$. The dissipative mechanism is described with the associated rate $\gamma$ (e.g., internal cavity losses, $\gamma = \kappa_{\mathrm{int}}$, or spin dephasing rate, $\gamma = \gamma_{\mathrm{s}}$). Note that with the previous definitions, $\gamma$ is defined as a half width half maximum rate. Considering that the Hamiltonian has no explicit time-dependent part, the equations of motion for the involved modes read

$$\frac{\mathrm{d}\hat{O}}{\mathrm{d}t} = \frac{i}{\hbar}[\hat{H}, \hat{O}], \tag{B.2}$$

where $\hat{O}$ stands for either resonator mode $\hat{a}$ or a continuous mode $\hat{b}_k$. From Eq. (B.1), we find

$$\begin{aligned} \frac{\mathrm{d}\hat{a}}{\mathrm{d}t} &= -i\omega_{\mathrm{r}}\hat{a} - ig_0 \int \hat{b}_k \mathrm{d}k, \\ \frac{\mathrm{d}\hat{b}_k}{\mathrm{d}t} &= -i\omega_k \hat{b}_k - ig_0\hat{a}. \end{aligned} \tag{B.3}$$

The equation on the mode $\hat{b}_k$ can be directly solved, resulting in

$$\hat{b}_k(t) = e^{-i\omega_k t}\left[\hat{b}_k(0) - ig_0 \int_0^t e^{i\omega_k \tau}\hat{a}(\tau)\mathrm{d}\tau\right]. \tag{B.4}$$

Inserting Eq. (B.4) in Eq. (B.3) leads to the new equation of motion

$$\frac{\mathrm{d}\hat{a}}{\mathrm{d}t} = -i\omega_{\mathrm{r}}\hat{a} - ig_0 \int \hat{b}_k(0)e^{-i\omega_k t}\mathrm{d}k - g_0^2 \int_0^t \int e^{i\omega_k(\tau - t)}\hat{a}(\tau)\mathrm{d}\tau\mathrm{d}k. \tag{B.5}$$

The last term in the previous equation can be reformulated as

$$\begin{aligned} g_0^2 \int_0^t \int e^{i\omega_k(\tau-t)}\hat{a}(\tau)\mathrm{d}\tau\mathrm{d}k &= g_0^2 \int_0^t \mathrm{d}\tau\hat{a}(\tau)\int e^{ikv(\tau-t)}\mathrm{d}k \\ &= g_0^2 \int_0^t \mathrm{d}\tau\hat{a}(\tau)2\pi\delta(v(\tau-t)) \\ &= \frac{2\pi}{2v}g_0^2\,\hat{a}(t)\ (\delta(cx)=\delta(x)/|c| \text{ and } \int_0^t f(\tau)\delta(\tau-t)\mathrm{d}\tau = f(t)/2) \\ &= \gamma\hat{a}(t)\ (g_0^2=\gamma v/\pi). \end{aligned} \tag{B.6}$$

Therefore, the equation of motion on the resonator mode reads

$$\frac{\mathrm{d}\hat{a}}{\mathrm{d}t} = -i\omega_\mathrm{r}\hat{a} - ig_0\int \hat{b}_k(0)e^{-i\omega_k t}\mathrm{d}k - \gamma\hat{a} = -i\omega_\mathrm{r}\hat{a} - \gamma\hat{a} + \hat{R}(t). \tag{B.7}$$

The structure of Eq. (B.7) indicates that the coupling of the resonator to a dissipative medium (via a dissipative mechanism) results in a coupling term via the rate $\gamma$ as expected for this type of systems. However, one must consider an additional term, $\hat{R}$, emerging from the coupling. As detailed below, this term is necessary to preserve bosonic properties of the different modes. Solving Eq. (B.7) leads to

$$\hat{a}(t) = e^{(-i\omega_\mathrm{r}-\gamma)t}\left[\hat{a}(0) - ig_0\int_0^t\int e^{(i\omega_\mathrm{r}+\gamma)\tau}e^{-i\omega_k\tau}\hat{b}_k(0)\mathrm{d}k\,\mathrm{d}\tau\right]. \tag{B.8}$$

One can verify that bosonic properties are conserved with the solution in Eq. (B.8). For instance, one computes the commutator

$$\begin{aligned} [\hat{a}(t),\hat{a}^\dagger(t)] &= e^{-2\gamma t}\left([\hat{a}(0),\hat{a}^\dagger(0)] + g_0^2\int_0^t\int_0^t\int\int e^{(i\omega_\mathrm{r}+\gamma-i\omega_k)\tau}e^{(-i\omega_\mathrm{r}+\gamma+i\omega_k')\tau'}[\hat{b}_k(0),\hat{b}_{k'}^\dagger(0)]\mathrm{d}\tau\mathrm{d}\tau'\mathrm{d}k\mathrm{d}k'\right) \\ &= e^{-2\gamma t}\left(1 + g_0^2\int_0^t\int_0^t\int\int e^{(i\omega_\mathrm{r}+\gamma-i\omega_k)\tau}e^{(-i\omega_\mathrm{r}+\gamma+i\omega_k')\tau'}\delta(k-k')\mathrm{d}\tau\mathrm{d}\tau'\mathrm{d}k\mathrm{d}k'\right) \\ &= e^{-2\gamma t}\left(1 + g_0^2\int_0^t\int_0^t\int e^{i\omega_\mathrm{r}(\tau-\tau')+\gamma(\tau+\tau')}\mathrm{d}\tau\mathrm{d}\tau'\int e^{ikv(\tau'-\tau)}\mathrm{d}k\right) \\ &= e^{-2\gamma t}\left(1 + g_0^2\frac{2\pi}{v}\int_0^t e^{2\gamma\tau}\mathrm{d}\tau\right) \\ &= e^{-2\gamma t}\left(1+e^{2\gamma t}-1\right) \\ &= 1, \end{aligned} \tag{B.9}$$

ensuring that the mode $\hat{a}$ remains bosonic at all time. Therefore, two possible approaches can be use to describe the full physics of this kind of systems, e.g., a resonator coupled to a dissipative medium. The first approach is to explicitly include bath environment terms in a given system Hamiltonian as in Eq. (B.1) leading to an equation of motion as in Eq. (B.7). In that case, the bath term in the Hamiltonian, described by modes $\hat{b}_k$, appears in the equation of motion as the additional term $\hat{R}$. The second approach is to include the dissipative coupling by relying on the formalism of Lindblad superoperators, introducing the collapse operator $\hat{d} = \sqrt{\gamma}\hat{a}$ as in Sec. 6.1. Then, one additionally includes a coupling term, $\hat{H}_\mathrm{cpl}$, in the system Hamiltonian

$$\hat{H}_\mathrm{cpl} = i\hbar g_0(\hat{a}\hat{r}^\dagger - \hat{a}^\dagger\hat{r}) \text{ with } \hat{r}(t) = -i\int \hat{b}_k(0)e^{-i\omega_k t}\mathrm{d}k. \tag{B.10}$$

Note that it is common in literature to include the phase velocity in the bath modes as a normalization. This can be done by defining a new bath mode $\hat{f} = \sqrt{v/2\pi}\,\hat{r}$, ensuring that

$$\begin{aligned}[\hat{f}(t), \hat{f}^\dagger(t')] &= \frac{v}{2\pi}\int\int e^{-i\omega_k t} e^{i\omega_k' t'} [\hat{b}_k(0), \hat{b}_k^\dagger(0)] \mathrm{d}k \mathrm{d}k' \\ &= \frac{v}{2\pi}\int e^{i\omega_k (t'-t)} \mathrm{d}k \\ &= \delta(t-t').\end{aligned} \tag{B.11}$$

As a consequence, the coupling Hamiltonian is written as

$$\hat{H}_{\mathrm{cpl}} = i\hbar\sqrt{2\gamma}(\hat{a}\hat{f}^\dagger - \hat{a}^\dagger \hat{f}). \tag{B.12}$$

# Bibliography


[1] J. P. Dowling & G. J. Milburn. Quantum technology: the second quantum revolution. *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* **361**, 1655–1674 (2003).

[2] D. Griffiths. *Introduction to Quantum Mechanics*. Pearson international edition (Pearson Prentice Hall, 2005). URL `https://books.google.de/books?id=z4fwAAAAMAAJ`.

[3] M. A. Nielsen & I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2010).

[4] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe & D. J. Wineland. Experimental violation of a Bell's inequality with efficient detection. *Nature* **409**, 791–794 (2001).

[5] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau & R. Hanson. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **526**, 682–686 (2015).

[6] L. S. Braunstein & P. Van Loock. Quantum information with continuous variables. *Rev. Mod. Phys.* **77**, 513–577 (2005).

[7] M. H. Devoret & R. J. Schoelkopf. Superconducting Circuits for Quantum Information: An Outlook. *Science* **339**, 1169–1174 (2013).

[8] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi & P. Wallden. Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012–1236 (2020).

[9] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell *et al.* Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019).

[10] T. Monz, P. Schindler, J. T. Barreiro, M. Chwalla, D. Nigg, W. A. Coish, M. Harlander, W. Hänsel, M. Hennrich & R. Blatt. 14-Qubit Entanglement: Creation and Coherence. *Phys. Rev. Lett.* **106**, 130506 (2011).

[11] B. E. Kane. A silicon-based nuclear spin quantum computer. *Nature* **393**, 133–137 (1998).

[12] D. Bluvstein, S. J. Evered, A. A. Geim, S. H. Li, H. Zhou, T. Manovitz, S. Ebadi, M. Cain, M. Kalinowski, D. Hangleiter, J. P. Bonilla Ataides, N. Maskara, I. Cong, X. Gao, P. Sales Rodriguez, T. Karolyshyn, G. Semeghini, M. J. Gullans, M. Greiner, V. Vuletić

& M. D. Lukin. Logical quantum processor based on reconfigurable atom arrays. *Nature* **626**, 58–65 (2024).

[13] M. W. Doherty, N. B. Manson, P. Delaney, F. Jelezko, J. Wrachtrup & L. C. Hollenberg. The nitrogen-vacancy colour centre in diamond. *Physics Reports* **528**, 1–45 (2013). The nitrogen-vacancy colour centre in diamond.

[14] A. Blais, A. L. Grimsmo, S. M. Girvin & A. Wallraff. Circuit quantum electrodynamics. *Rev. Mod. Phys.* **93**, 025005 (2021).

[15] V. V. Sivak, A. Eickbusch, B. Royer, S. Singh, I. Tsioutsios, S. Ganjam, A. Miano, B. L. Brock, A. Z. Ding, L. Frunzio, S. M. Girvin, R. J. Schoelkopf & M. H. Devoret. Real-time quantum error correction beyond break-even. *Nature* **616**, 50–55 (2023).

[16] T. Begušić, J. Gray & G. K.-L. Chan. Fast and converged classical simulations of evidence for the utility of quantum computing before fault tolerance. *Sci. Adv.* **10** (2024).

[17] X.-H. Zhao, H.-S. Zhong, F. Pan, Z.-H. Chen, R. Fu, Z. Su, X. Xie, C. Zhao, P. Zhang, W. Ouyang, C.-Y. Lu, J.-W. Pan & M.-C. Chen. Leapfrogging Sycamore: Harnessing 1432 GPUs for 7× Faster Quantum Random Circuit Sampling. URL `https://arxiv.org/abs/2406.18889`. `2406.18889` (2024).

[18] P. Shor. Fault-tolerant quantum computation. In *Proceedings of 37th Conference on Foundations of Computer Science* 56–65 (1996).

[19] R. L. Rivest, A. Shamir & L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**, 120–126 (1978).

[20] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science* 124–134 (1994).

[21] D. Beckman, A. N. Chari, S. Devabhaktuni & J. Preskill. Efficient networks for quantum factoring. *Phys. Rev. A* **54**, 1034–1063 (1996).

[22] R. Jozsa & N. Linden. On the role of entanglement in quantum-computational speed-up. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* **459**, 2011–2032 (2003).

[23] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter & A. Zeilinger. Experimental quantum teleportation. *Nature* **390**, 575–579 (1997).

[24] K. G. Fedorov, M. Renger, S. Pogorzalek, R. Di Candia, Q. Chen, Y. Nojiri, K. Inomata, Y. Nakamura, M. Partanen, A. Marx, R. Gross & F. Deppe. Experimental quantum teleportation of propagating microwaves. *Sci. Adv.* **7**, 2–7 (2021).

[25] X.-M. Hu, Y. Guo, B.-H. Liu, C.-F. Li & G.-C. Guo. Progress in quantum teleportation. *Nat. Rev. Phys.* **5**, 339–353 (2023).

[26] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro & S. Lloyd. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621–669 (2012).

[27] S. Pogorzalek, K. G. Fedorov, M. Xu, A. Parra-Rodriguez, M. Sanz, M. Fischer, E. Xie, K. Inomata, Y. Nakamura, E. Solano, A. Marx, F. Deppe & R. Gross. Secure quantum remote state preparation of squeezed microwave states. *Nat. Commun.* **10**, 2604 (2019).

[28] S. L. Braunstein & H. J. Kimble. Dense coding for continuous variables. *Phys. Rev. A* **61**, 042302 (2000).

[29] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal & W. K. Wootters. Remote State Preparation. *Phys. Rev. Lett.* **87**, 077902 (2001).

[30] W. H. Zurek. A single quantum cannot be cloned. *Nature* **246**, 170–170 (1973).

[31] S. L. Braunstein, N. J. Cerf, S. Iblisdir, P. van Loock & S. Massar. Optimal Cloning of Coherent States with a Linear Amplifier and Beam Splitters. *Phys. Rev. Lett.* **86**, 4938–4941 (2001).

[32] F. Xu, X. Ma, Q. Zhang, H.-K. Lo & J.-W. Pan. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).

[33] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim & H. Weinfurter. A device-independent quantum key distribution system for distant users. *Nature* **607**, 687–691 (2022).

[34] J. Barrett, R. Colbeck & A. Kent. Memory Attacks on Device-Independent Quantum Cryptography. *Phys. Rev. Lett.* **110**, 010503 (2013).

[35] X. Zhang, Y. Zhang, Y. Zhao, X. Wang, S. Yu & H. Guo. Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **96**, 042334 (2017).

[36] M. Lucamarini, Z. L. Yuan, J. F. Dynes & A. J. Shields. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).

[37] C. Lupo, C. Ottaviani, P. Papanastasiou & S. Pirandola. Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks. *Phys. Rev. A* **97**, 052327 (2018).

[38] C. H. Bennett & G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (1984). Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[39] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers & J. Oppenheim. The Universal Composable Security of Quantum Key Distribution (2005). URL `http://link.springer.com/10.1007/978-3-540-30576-7_21`.

[40] H.-L. Yin, P. Liu, W.-W. Dai, Z.-H. Ci, J. Gu, T. Gao, Q.-W. Wang & Z.-Y. Shen. Experimental composable security decoy-state quantum key distribution using time-phase encoding. *Opt. Express* **28**, 29479–29485 (2020).

[41] F. Flamini, N. Spagnolo & F. Sciarrino. Photonic quantum information processing: a review. *Rep. Prog. Phys.* **82**, 016001 (2019).

[42] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.* Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47 (2017).

[43] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin & H. Zbinden. Secure Quantum Key Distribution over 421 km of Optical Fiber. *Phys. Rev. Lett.* **121**, 190502 (2018).

[44] A. Rueda, F. Sedlmeir, M. C. Collodo, U. Vogl, B. Stiller, G. Schunk, D. V. Strekalov, C. Marquardt, J. M. Fink, O. Painter, G. Leuchs & H. G. L. Schwefel. Efficient microwave to optical photon conversion: an electro-optical realization. *Optica* **3**, 597 (2016).

[45] M. Mirhosseini, A. Sipahigil, M. Kalaee & O. Painter. Superconducting qubit to optical photon transduction. *Nature* **588**, 599–603 (2020).

[46] X. Han, W. Fu, C.-L. Zou, L. Jiang & H. X. Tang. Microwave-optical quantum frequency conversion. *Optica* **8**, 1050–1064 (2021).

[47] R. Gross & A. Marx. *Festkörperphysik* (Oldenbourg Verlag, München, München, 2012).

[48] M. Mariantoni, E. P. Menzel, F. Deppe, M. A. Araque Caballero, A. Baust, T. Niemczyk, E. Hoffmann, E. Solano, A. Marx & R. Gross. Planck Spectroscopy and Quantum Noise of Microwave Beam Splitters. *Phys. Rev. Lett.* **105**, 133601 (2010).

[49] E. P. Menzel, F. Deppe, M. Mariantoni, M. A. Araque Caballero, A. Baust, T. Niemczyk, E. Hoffmann, A. Marx, E. Solano & R. Gross. Dual-Path State Reconstruction Scheme for Propagating Quantum Microwaves and Detector Noise Tomography. *Phys. Rev. Lett.* **105**, 100401 (2010).

[50] L. Zhong, E. P. Menzel, R. Di Candia, P. Eder, M. Ihmig, A. Baust, M. Haeberlein, E. Hoffmann, K. Inomata, T. Yamamoto, Y. Nakamura, E. Solano, F. Deppe, A. Marx & R. Gross. Squeezing with a flux-driven Josephson parametric amplifier. *New J. Phys.* **15**, 125013 (2013).

[51] K. G. Fedorov, L. Zhong, S. Pogorzalek, P. Eder, M. Fischer, J. Goetz, E. Xie, F. Wulschner, K. Inomata, T. Yamamoto, Y. Nakamura, R. Di Candia, U. Las Heras, M. Sanz, E. Solano, E. P. Menzel, F. Deppe, A. Marx & R. Gross. Displacement of Propagating Squeezed Microwave States. *Phys. Rev. Lett.* **117**, 020502 (2016).

[52] E. P. Menzel, R. Di Candia, F. Deppe, P. Eder, L. Zhong, M. Ihmig, M. Haeberlein, A. Baust, E. Hoffmann, D. Ballester, K. Inomata, T. Yamamoto, Y. Nakamura, E. Solano, A. Marx & R. Gross. Path Entanglement of Continuous-Variable Quantum Microwaves. *Phys. Rev. Lett.* **109**, 250502 (2012).

[53] F. Fesquet, F. Kronowetter, M. Renger, W. K. Yam, S. Gandorfer, K. Inomata, Y. Nakamura, A. Marx, R. Gross & K. G. Fedorov. Demonstration of microwave single-shot quantum key distribution. *Nat. Commun.* **15**, 7544 (2024).

[54] T. Yamamoto, K. Inomata, M. Watanabe, K. Matsuba, T. Miyazaki, W. D. Oliver, Y. Nakamura & J. S. Tsai. Flux-driven Josephson parametric amplifier. *Appl. Phys. Lett.* **93**, 042510 (2008).

[55] B. Yurke, L. R. Corruccini, P. G. Kaminsky, L. W. Rupp, A. D. Smith, A. H. Silver, R. W. Simon & E. A. Whittaker. Observation of parametric amplification and deamplification in a Josephson parametric amplifier. *Phys. Rev. A* **39**, 2519–2533 (1989).

[56] Z. R. Lin, K. Inomata, W. D. Oliver, K. Koshino, Y. Nakamura, J. S. Tsai & T. Yamamoto. Single-shot readout of a superconducting flux qubit with a flux-driven Josephson parametric amplifier. *Appl. Phys. Lett.* **103** (2013).

[57] A. Bienfait, J. J. Pla, Y. Kubo, M. Stern, X. Zhou, C. C. Lo, C. D. Weis, T. Schenkel, M. L. W. Thewalt, D. Vion, D. Esteve, B. Julsgaard, K. Mølmer, J. J. L. Morton & P. Bertet. Reaching the quantum limit of sensitivity in electron spin resonance. *Nat. Nanotechnol.* **11**, 253–257 (2016).

[58] C. Eichler, A. J. Sigillito, S. A. Lyon & J. R. Petta. Electron Spin Resonance at the Level of $10^4$ Spins Using Low Impedance Superconducting Resonators. *Phys. Rev. Lett.* **118**, 037701 (2017).

[59] S. Probst, A. Bienfait, P. Campagne-Ibarcq, J. J. Pla, B. Albanese, J. F. Da Silva Barbosa, T. Schenkel, D. Vion, D. Esteve, K. Mølmer, J. J. L. Morton, R. Heeres & P. Bertet. Inductive-detection electron-spin resonance spectroscopy with 65 spins/$\sqrt{\text{Hz}}$ sensitivity. *Appl. Phys. Lett.* **111** (2017).

[60] F. Fesquet, F. Kronowetter, M. Renger, Q. Chen, K. Honasoge, O. Gargiulo, Y. Nojiri, A. Marx, F. Deppe, R. Gross & K. G. Fedorov. Perspectives of microwave quantum key distribution in the open air. *Phys. Rev. A* **108**, 032607 (2023).

[61] R. Gross, A. Marx, D. Einzel & S. Geprägs. *Festkörperphysik* (De Gruyter Oldenbourg, 2023). URL `https://www.degruyterbrill.com/document/doi/10.1515/9783110782530/html`.

[62] W. Buckel & R. Kleiner. *Superconductivity* (Wiley, 2004). URL `https://onlinelibrary.wiley.com/doi/book/10.1002/9783527618507`.

[63] N. E. Frattini, U. Vool, S. Shankar, A. Narla, K. M. Sliwa & M. H. Devoret. 3-wave mixing Josephson dipole element. *Appl. Phys. Lett.* **110** (2017).

[64] M. Tinkham. *Introduction to Superconductivity.* International series in pure and applied physics (McGraw-Hill, 1975). URL `https://books.google.de/books?id=L0brob3Q9W4C`.

[65] M. Sandberg, C. M. Wilson, F. Persson, T. Bauch, G. Johansson, V. Shumeiko, T. Duty & P. Delsing. Tuning the field in a microwave resonator faster than the photon lifetime. *Appl. Phys. Lett.* **92**, 3–6 (2008).

[66] V. Lefevre-Seguin, E. Turlot, C. Urbina, D. Esteve & M. H. Devoret. Thermal activation of a hysteretic dc superconducting quantum interference device from its different zero-voltage states. *Phys. Rev. B* **46**, 5507–5522 (1992).

[67] S. Pogorzalek, K. G. Fedorov, L. Zhong, J. Goetz, F. Wulschner, M. Fischer, P. Eder, E. Xie, K. Inomata, T. Yamamoto, Y. Nakamura, A. Marx, F. Deppe & R. Gross. Hysteretic Flux Response and Nondegenerate Gain of Flux-Driven Josephson Parametric Amplifiers. *Phys. Rev. Appl.* **8**, 024012 (2017).

[68] D. M. Pozar. *Microwave engineering; 4th ed.* (Wiley, Hoboken, 2011). URL `https://www.wiley.com/en-us/Microwave+Engineering,+4th+Edition-p-9780470631553`.

[69] M. Göppl, A. Fragner, M. Baur, R. Bianchetti, S. Filipp, J. M. Fink, P. J. Leek, G. Puebla, L. Steffen & A. Wallraff. Coplanar waveguide resonators for circuit quantum electrodynamics. *J. Appl. Phys.* **104** (2008).

[70] M. Wallquist, V. S. Shumeiko & G. Wendin. Selective coupling of superconducting charge qubits mediated by a tunable stripline cavity. *Phys. Rev. B* **74**, 224506 (2006).

[71] W. Wustmann & V. Shumeiko. Parametric resonance in tunable superconducting cavities. *Phys. Rev. B* **87**, 184501 (2013).

[72] C. Eichler, Y. Salathe, J. Mlynek, S. Schmidt & A. Wallraff. Quantum-Limited Amplification and Entanglement in Coupled Nonlinear Resonators. *Phys. Rev. Lett* **113**, 110502 (2014).

[73] S. Boutin, D. M. Toyli, A. V. Venkatramani, A. W. Eddins, I. Siddiqi & A. Blais. Effect of Higher-Order Nonlinearities on Amplification and Squeezing in Josephson Parametric Amplifiers. *Phys. Rev. Appl.* **8**, 054030 (2017).

[74] K. K. T. Yamamoto & Y. Nakamura. *Parametric Amplifer and Oscillator Based on Josephson Junction Circuitry*, 495–513 (Springer Japan, Tokyo, 2016). Edited by Y. Yamamoto and K. Semba.

[75] J. Goetz, F. Deppe, M. Haeberlein, F. Wulschner, C. W. Zollitsch, S. Meier, M. Fischer, P. Eder, E. Xie, K. G. Fedorov, E. P. Menzel, A. Marx & R. Gross. Loss mechanisms in superconducting thin film microwave resonators. *J. Appl. Phys.* **119** (2016).

[76] A. Kamal, A. Marblestone & M. Devoret. Signal-to-pump back action and self-oscillation in double-pump Josephson parametric amplifier. *Phys. Rev. B* **79**, 184301 (2009).

[77] P. Krantz, A. Bengtsson, M. Simoen, S. Gustavsson, V. Shumeiko, W. D. Oliver, C. M. Wilson, P. Delsing & J. Bylander. Single-shot read-out of a superconducting qubit using a Josephson parametric oscillator. *Nat. Commun.* **7**, 11417 (2016).

[78] D. J. Parker, M. Savytskyi, W. Vine, A. Laucht, T. Duty, A. Morello, A. L. Grimsmo & J. J. Pla. Degenerate Parametric Amplification via Three-Wave Mixing Using Kinetic Inductance. *Phys. Rev. Appl.* **17**, 034064 (2022).

[79] H. A. Haus & J. A. Mullen. Quantum Noise in Linear Amplifiers. *Phys. Rev.* **128**, 2407–2413 (1962).

[80] C. M. Caves. Quantum limits on noise in linear amplifiers. *Phys. Rev. D* **26**, 1817–1839 (1982).

[81] C. M. Caves, J. Combes, Z. Jiang & S. Pandey. Quantum limits on phase-preserving linear amplifiers. *Phys. Rev. A* **86**, 063802 (2012).

[82] M. Renger, S. Pogorzalek, Q. Chen, Y. Nojiri, K. Inomata, Y. Nakamura, M. Partanen, A. Marx, R. Gross, F. Deppe & K. G. Fedorov. Beyond the standard quantum limit for parametric amplification of broadband signals. *Npj Quantum Inf.* **7**, 160 (2021).

[83] J. E. Harriman & M. E. Casida. Husimi representation for stationary states. *Int. J. Quantum Chem.* **45**, 263–294 (1993).

[84] E. C. G. Sudarshan. Equivalence of Semiclassical and Quantum Mechanical Descriptions of Statistical Light Beams. *Phys. Rev. Lett.* **10**, 277–279 (1963).

[85] E. Wigner. On the Quantum Correction For Thermodynamic Equilibrium. *Phys. Rev.* **40**, 749–759 (1932).

[86] V. Bužek, G. Adam & G. Drobný. Quantum state reconstruction and detection of quantum coherences on different observation levels. *Phys. Rev. A* **54**, 804–820 (1996).

[87] U. Leonhardt & H. Paul. Measuring the quantum state of light. *Prog. Quantum Electron.* **19**, 89–130 (1995).

[88] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble & E. S. Polzik. Unconditional Quantum Teleportation. *Science* **282**, 706–709 (1998).

[89] R. Assouly, R. Dassonneville, T. Peronnin, A. Bienfait & B. Huard. Quantum advantage in microwave quantum radar. *Nat. Phys* **19**, 1418–1422 (2023).

[90] H. Nyquist. Thermal Agitation of Electric Charge in Conductors. *Phys. Rev.* **32**, 110–113 (1928).

[91] M. O. Scully & M. S. Zubairy. *Quantum optics* (Cambridge University Press, Cambridge, 1997).

[92] D. F. Walls & G. J. Milburn. *Quantum optics* (Springer, Berlin Heidelberg, 2008).

[93] S. Pogorzalek. *Remote State Preparation of Squeezed Microwave States*. Phd thesis, Technische Universität München (2020). URL `https://www.wmi.badw.de/fileadmin/WMI/Publications/Pogorzalek_Stefan_Doktorarbeit_2020.pdf`.

[94] X. Wang, T. Hiroshima, A. Tomita & M. Hayashi. Quantum information with Gaussian states. *Phys. Rep.* **448**, 1–111 (2007).

[95] J.-W. Pan, D. Bouwmeester, H. Weinfurter & A. Zeilinger. Experimental Entanglement Swapping: Entangling Photons That Never Interacted. *Phys. Rev. Lett.* **80**, 3891–3894 (1998).

[96] R. Di Candia, K. Fedorov, L. Zhong, S. Felicetti, E. Menzel, M. Sanz, F. Deppe, A. Marx, R. Gross & E. Solano. Quantum teleportation of propagating quantum microwaves. *EPJ Quantum Technol.* **2**, 25 (2015).

[97] J. Eisert & M. M. Wolf. Gaussian Quantum Channels. In *Quantum Information with Continuous Variables of Atoms and Light* 23–42 (Published by Imperial College press and distributed by world scientific publishing Co., 2007). URL `http://www.worldscientific.com/doi/abs/10.1142/9781860948169_0002`.

[98] S. Pirandola, S. L. Braunstein & S. Lloyd. Characterization of collective gaussian attacks and security of coherent-state quantum cryptography. *Phys. Rev. Lett.* **101**, 1–4 (2008).

[99] A. Sergeevich & V. I. Man'ko. Scaling separability criterion: application to Gaussian states. *J. Russ. Laser Res.* **30**, 609–614 (2009).

[100] G. Adesso, A. Serafini & F. Illuminati. Determination of Continuous Variable Entanglement by Purity Measurements. *Phys. Rev. Lett.* **92**, 087901 (2004).

[101] C. E. Shannon. A Mathematical Theory of Communication. *Bell Syst. Tech. J.* **27**, 379–423 (1948).

[102] G. Adesso, S. Ragy & A. R. Lee. Continuous Variable Quantum Information: Gaussian States and Beyond. *Open Syst. Inf. Dyn* **21**, 1440001 (2014).

[103] M. A. N. I. M. Gelfand. On the imbedding of normed rings into the ring of operators in Hilbert space. *Mat. Sb.* **54**, 197–217 (1943).

[104] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden & N. Gisin. Unambiguous quantum measurement of nonorthogonal states. *Phys. Rev. A* **54**, 3783–3789 (1996).

[105] N. J. Cerf, M. Lévy & G. V. Assche. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* **63**, 052311 (2001).

[106] P. W. Shor & J. Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000).

[107] T. E. Chapuran, P. Toliver, N. A. Peters, J. Jackel, M. S. Goodman, R. J. Runser, S. R. McNown, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, C. G. Peterson, K. T. Tyagi, L. Mercer & H. Dardy. Optical networking for quantum key distribution and quantum communications. *New J. Phys.* **11**, 105001 (2009).

[108] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev & A. Zeilinger. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **19**, 10387–10409 (2011).

[109] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger & H. Weinfurter. Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. *Phys. Rev. Lett.* **98**, 010504 (2007).

[110] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam & J. E. Nordholt. Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber. *Phys. Rev. Lett.* **98**, 010503 (2007).

[111] N. J. Cerf & P. Grangier. From quantum cloning to quantum key distribution with continuous variables: a review (Invited). *J. Opt. Soc. Am. B* **24**, 324–334 (2007).

[112] Y. Zhang, Y. Bian, Z. Li, S. Yu & H. Guo. Continuous-variable quantum key distribution system: Past, present, and future. *Appl. Phys. Rev.* **11** (2024).

[113] N. Walk, T. C. Ralph, T. Symul & P. K. Lam. Security of continuous-variable quantum cryptography with Gaussian postselection. *Phys. Rev. A* **87**, 020303 (2013).

[114] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin & S. W. Nam. Detecting single infrared photons with 93efficiency. *Nat. Photonics* **7**, 210–214 (2013).

[115] K. Inomata, Z. Lin, K. Koshino, W. D. Oliver, J.-S. Tsai, T. Yamamoto & Y. Nakamura. Single microwave-photon detector using an artificial Λ-type three-level system. *Nat. Commun.* **7**, 12303 (2016).

[116] Y. Nojiri, K. E. Honasoge, A. Marx, K. G. Fedorov & R. Gross. Onset of transmon ionization in microwave single-photon detection. *Phys. Rev. B* **109**, 174312 (2024).

[117] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf & P. Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature* **421**, 238–241 (2003).

[118] D. Lin, D. Huang, P. Huang, J. Peng & G. Zeng. High performance reconciliation for continuous-variable quantum key distribution with LDPC code **13**, 1550010 (2015).

[119] T. Wang, P. Huang, Y. Zhou, W. Liu, H. Ma, S. Wang & G. Zeng. High key rate continuous-variable quantum key distribution with a real local oscillator. *Opt. Express* **26**, 2794 (2018).

[120] A. Leverrier & P. Grangier. Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation. *Phys. Rev. A* **83**, 042312 (2011).

[121] S. Ghorai, P. Grangier, E. Diamanti & A. Leverrier. Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation. *Phys. Rev. X* **9**, 021059 (2019).

[122] A. Leverrier, R. García-Patrón, R. Renner & N. J. Cerf. Security of Continuous-Variable Quantum Key Distribution Against General Attacks. *Phys. Rev. Lett.* **110**, 030502 (2013).

[123] L. Ruppert, V. C. Usenko & R. Filip. Long-distance continuous-variable quantum key distribution with efficient channel estimation. *Phys. Rev. A* **90**, 062310 (2014).

[124] P. Papanastasiou, C. Ottaviani & S. Pirandola. Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables. *Phys. Rev. A* **96**, 042332 (2017).

[125] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner & R. Schnabel. Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks. *Nat. Commun.* **6**, 8795 (2015).

[126] S. Pirandola. Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks. *Phys. Rev. Res.* **3**, 043014 (2021).

[127] A. Leverrier. Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction. *Phys. Rev. Lett.* **118**, 200501 (2017).

[128] M. Navascués, F. Grosshans & A. Acín. Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography. *Phys. Rev. Lett.* **97**, 190502 (2006).

[129] R. García-Patrón & N. J. Cerf. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **97**, 190503 (2006).

[130] F. Caruso, V. Giovannetti & A. S. Holevo. One-mode bosonic Gaussian channels: a full weak-degradability classification. *New J. Phys.* **8**, 310–310 (2006).

[131] C. Ottaviani, S. Mancini & S. Pirandola. Gaussian two-mode attacks in one-way quantum cryptography. *Phys. Rev. A* **95**, 052310 (2017).

[132] R. Filip. Continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A* **77**, 022310 (2008).

[133] Z. Wang, R. Malaney & J. Green. Inter-Satellite Quantum Key Distribution at Terahertz Frequencies. In *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)* 1–7 (2019).

[134] R. García-Patrón & N. J. Cerf. Continuous-Variable Quantum Key Distribution Protocols Over Noisy Channels. *Phys. Rev. Lett.* **102**, 130501 (2009).

[135] V. Usenko & R. Filip. Trusted Noise in Continuous-Variable Quantum Key Distribution: A Threat and a Defense. *Entropy* **18**, 20 (2016).

[136] F. Grosshans & P. Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett* **88**, 057902 (2002).

[137] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu & H. Guo. Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber. *Phys. Rev. Lett.* **125**, 010502 (2020).

[138] A. A. E. Hajomer, I. Derkach, N. Jain, H.-M. Chin, U. L. Andersen & T. Gehring. Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator. *Sci. Adv.* **10** (2024).

[139] I. Derkach & V. C. Usenko. Applicability of Squeezed- and Coherent-State Continuous-Variable Quantum Key Distribution over Satellite Links. *Entropy* **23**, 55 (2020).

[140] X. Wang, Y. Cao, P. Wang & Y. Li. Advantages of the coherent state compared with squeezed state in unidimensional continuous variable quantum key distribution. *Quantum Inf. Process.* **17**, 344 (2018).

[141] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip & U. L. Andersen. Continuous variable quantum key distribution with modulated entangled states. *Nat. Commun.* **3**, 1083 (2012).

[142] U. L. Andersen, T. Gehring, C. Marquardt & G. Leuchs. 30 years of squeezed light generation. *Physica Scripta* **91**, 053001 (2016).

[143] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Probl. Inf. Transm.* **9**, 177–183 (1973).

[144] D. Huang, P. Huang, D. Lin & G. Zeng. Long-distance continuous-variable quantum key distribution by controlling excess noise **6**, 19201 (2016).

[145] M. Mehic, M. Niemiec, H. Siljak & M. Voznak. Error Reconciliation in Quantum Key Distribution Protocols (2020). URL `https://link.springer.com/10.1007/978-3-030-47361-7_11`.

[146] X. Wang, Y. Zhang, Z. Li, B. Xu, S. Yu & H. Guo. Efficient rate-adaptive reconciliation for CV-QKD protocol **17**, 1123–1134 (2017).

[147] X. Wang, Y. Zhang, S. Yu & H. Guo. High speed error correction for continuous-variable quantum key distribution with multi-edge type LDPC code. *Sci. Rep.* **8**, 10543 (2018).

[148] M. Milicevic, C. Feng, L. M. Zhang & P. G. Gulak. Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography. *Npj Quantum Inf.* **4**, 21 (2018).

[149] A. Leverrier, F. Grosshans & P. Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **81**, 062343 (2010).

[150] S. Pirandola. Limits and security of free-space quantum communications. *Phys. Rev. Res.* **3**, 013279 (2021).

[151] G. Van Assche, J. Cardinal & N. Cerf. Reconciliation of a quantum-distributed Gaussian key. *IEEE Trans. Inf. Theory* **50**, 394–400 (2004).

[152] R. Renner. Security of Quantum Key Distribution. URL `https://arxiv.org/abs/quant-ph/0512258`. `quant-ph/0512258` (2006).

[153] T. M. Cover & J. A. Thomas. *Elements of Information Theory* (Wiley, 2005). URL `https://onlinelibrary.wiley.com/doi/book/10.1002/047174882X`.

[154] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther & H. Hübel. Continuous-Variable Quantum Key Distribution with Gaussian Modulation-The Theory of Practical Implementations. *Adv. Quantum Technol.* **1**, 1800011 (2018).

[155] C. Weedbrook, S. Pirandola & T. C. Ralph. Continuous-variable quantum key distribution using thermal states. *Phys. Rev. A* **86**, 022318 (2012).

[156] S. Pirandola, R. Laurenza, C. Ottaviani & L. Banchi. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).

[157] H. P. Yuen & V. W. S. Chan. Noise in homodyne and heterodyne detection. *Opt. Lett.* **8**, 177–179 (1983).

[158] H. Hansen, T. Aichele, C. Hettich, P. Lodahl, A. I. Lvovsky, J. Mlynek & S. Schiller. Ultrasensitive pulsed, balanced homodyne detector : application to time-domain quantum measurements. *Opt. Lett.* **26**, 1714–1716 (2001).

[159] A. I. Lvovsky & J. Mlynek. Quantum-Optical Catalysis: Generating Nonclassical States of Light by Means of Linear Optics. *Phys. Rev. Lett.* **88**, 250401 (2002).

[160] A. Ourjoumtsev, A. Dantan, R. Tualle-Brouri & P. Grangier. Increasing Entanglement between Gaussian States by Coherent Photon Subtraction. *Phys. Rev. Lett.* **98**, 030502 (2007).

[161] F. Jia, W. Ye, Q. Wang, L.-Y. Hu & H.-Y. Fan. Comparison of nonclassical properties resulting from non-Gaussian operations. *Laser Phys. Lett.* **16**, 015201 (2019).

[162] M. M. Wolf, G. Giedke & J. I. Cirac. Extremality of Gaussian Quantum States. *Phys. Rev. Lett.* **96**, 080502 (2006).

[163] L.-Y. Hu, F. Chen, Z.-S. Wang & H.-Y. Fan. Time evolution of distribution functions in dissipative environments. *Chin. Phys. B* **20**, 074204 (2011).

[164] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier & R. Tualle-Brouri. Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier. *Phys. Rev. A* **86**, 012327 (2012).

[165] L. Hu, M. Al-amri, Z. Liao & M. S. Zubairy. Continuous-variable quantum key distribution with non-Gaussian operations. *Phys. Rev. A* **102**, 012608 (2020).

[166] A. E. Ulanov, I. A. Fedorov, A. A. Pushkina, Y. V. Kurochkin, T. C. Ralph & A. I. Lvovsky. Undoing the effect of loss on quantum entanglement. *Nat. Photonics* **9**, 764–768 (2015).

[167] J. Singh & S. Bose. Non-Gaussian operations in measurement-device-independent quantum key distribution. *Phys. Rev. A* **104**, 052605 (2021).

[168] X. Chen, F. Jia, T. Zhao, N. Zhou, S. Liu & L. Hu. Continuous-variable quantum key distribution based on non-Gaussian operations with on-off detection. *Opt. Express* **31**, 32935–32952 (2023).

[169] H. Zhong, Y. Guo, Y. Mao, W. Ye & D. Huang. Virtual zero-photon catalysis for improving continuous-variable quantum key distribution via Gaussian post-selection. *Sci. Rep.* **10**, 17526 (2020).

[170] X. Wang, M. Xu, Y. Zhao, Z. Chen, S. Yu & H. Guo. Non-Gaussian Reconciliation for Continuous-Variable Quantum Key Distribution. *Phys. Rev. Appl.* **19**, 054084 (2023).

[171] T. Gonzalez-Raya & M. Sanz. Coplanar Antenna Design for Microwave Entangled Signals Propagating in Open Air. *Quantum* **6**, 783 (2022).

[172] M. Zhang, S. Pirandola & K. Delfanazari. Millimetre-waves to Terahertz SISO and MIMO Continuous Variable Quantum Key Distribution. URL `https://arxiv.org/abs/2301.04723`. `2301.04723` (2023).

[173] C. Eichler, D. Bozyigit & A. Wallraff. Characterizing quantum microwave radiation and its entanglement with superconducting qubits using linear detectors. *Phys. Rev. A* **86**, 032106 (2012).

[174] H. Friis. Noise Figures of Radio Receivers. *Proceedings of the IRE* **32**, 419–422 (1944).

[175] T. Gonzalez-Raya, M. Casariego, F. Fesquet, M. Renger, V. Salari, M. Möttönen, Y. Omar, F. Deppe, K. G. Fedorov & M. Sanz. Open-Air Microwave Entanglement Distribution for Quantum Teleportation. *Phys. Rev. Appl.* **18**, 044002 (2022).

[176] C. M. Ho, C. Wang, K. Angkasa & K. Gritton. Estimation of Microwave Power Margin Losses Due to Earth's Atmosphere and Weather in the Frequency Range of 3–30 GHz. *Jet Propulsion Laboratory* (2004).

[177] H. Kaushal, V. Jain & S. Kar. *Free Space Optical Communication*, Vol. 7 (Springer, New Delhi, 2018). URL `https://doi.org/10.1007/978-81-322-3691-7`.

[178] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier & E. Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **7**, 378–381 (2013).

[179] J. Lin, T. Upadhyaya & N. Lütkenhaus. Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution. *Phys. Rev. X* **9**, 041064 (2019).

[180] W.-B. Liu, C.-L. Li, Y.-M. Xie, C.-X. Weng, J. Gu, X.-Y. Cao, Y.-S. Lu, B.-H. Li, H.-L. Yin & Z.-B. Chen. Homodyne Detection Quadrature Phase Shift Keying Continuous-Variable Quantum key Distribution with High Excess Noise Tolerance. *PRX Quantum* **2**, 040334 (2021).

[181] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus & M. Peev. The security of practical quantum key distribution. *Rev. Mod. Phys* **81**, 1301–1350 (2009).

[182] S. Ast, M. Mehmet & R. Schnabel. High-bandwidth squeezed light at 1550 nm from a compact monolithic PPKTP cavity. *Opt. Express* **21**, 13572 (2013).

[183] C. Macklin, K. O'Brien, D. Hover, M. E. Schwartz, V. Bolkhovsky, X. Zhang, W. D. Oliver & I. Siddiqi. A near-quantum-limited Josephson traveling-wave parametric amplifier. *Science* **350**, 307–310 (2015).

[184] M. Perelshtein, K. Petrovnin, V. Vesterinen, S. H. Raja, I. Lilja, M. Will, A. Savin, S. Simbierowicz, R. Jabdaraghi, J. Lehtinen *et al.* Broadband continuous variable entanglement generation using Kerr-free Josephson metamaterial (2021).

[185] B. H. Schneider, A. Bengtsson, I. M. Svensson, T. Aref, G. Johansson, J. Bylander & P. Delsing. Observation of Broadband Entanglement in Microwave Radiation from a Single Time-Varying Boundary Condition. *Phys. Rev. Lett* **124**, 140503 (2020).

[186] J. Y. Qiu, A. Grimsmo, K. Peng, B. Kannan, B. Lienhard, Y. Sung, P. Krantz, V. Bolkhovsky, G. Calusine, D. Kim, A. Melville, B. M. Niedzielski, J. Yoder, M. E. Schwartz, T. P. Orlando, I. Siddiqi, S. Gustavsson, K. P. O'Brien & W. D. Oliver. Broadband squeezed microwaves and amplification with a Josephson travelling-wave parametric amplifier. *Nat. Phys* **19**, 706–713 (2023).

[187] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang & G. Zeng. Continuous-variable quantum key distribution with 1 Mbps secure key rate. *Opt. Express* **23**, 17511 (2015).

[188] X. Tang, R. Kumar, S. Ren, A. Wonfor, R. Penty & I. White. Performance of continuous variable quantum key distribution system at different detector bandwidth. *Opt. Commun.* **471**, 126034 (2020).

[189] S. Sarmiento, S. Etcheverry, J. Aldama, I. H. López, L. T. Vidarte, G. B. Xavier, D. A. Nolan, J. S. Stone, M. J. Li, D. Loeber *et al.* Continuous-Variable Quantum Key Distribution over 15 km Multi-Core Fiber (2022).

[190] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin & P. Grangier. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **76**, 042305 (2007).

[191] R. S. of International Telecommunication Union. Recommendation ITU-R P.838-3: Specific attenuation model for rain for use in prediction methods. URL `https://www.itu.int/rec/R-REC-P.838/en` (2005).

[192] R. S. of International Telecommunication Union. Recommendation ITU-R P.840-6: Attenuation due to clouds and fog. URL `https://www.itu.int/rec/R-REC-P.840/en` (2013).

[193] S. Shrestha & D.-Y. Choi. Rain Attenuation Study over an 18 GHz Terrestrial Microwave Link in South Korea. *Int. J. Antennas Propag* **2019**, 1–16 (2019).

[194] Z. Zhao & Z. Wu. Millimeter-wave attenuation due to fog and clouds. *J. Infrared Millim. Terahertz Waves* **21**, 1607–1615 (2000).

[195] J. Fišák, D. Řezáčová & J. Mattanen. Calculated and measured values of liquid water content in clean and polluted environments. *Stud. Geophys. Geod* **50**, 121–130 (2006).

[196] I. I. Kim, B. McArthur & E. J. Korevaar. Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications. *Proc. SPIE* **4214** (2001).

[197] S. Gandorfer, M. Renger, W. Yam, F. Fesquet, A. Marx, R. Gross & K. Fedorov. Two-dimensional Planck spectroscopy for microwave photon calibration. *Phys. Rev. Appl.* **23**, 024064 (2025).

[198] T. Yu & J. H. Eberly. Sudden Death of Entanglement. *Science* **323**, 598–601 (2009).

[199] W. K. Yam, M. Renger, S. Gandorfer, F. Fesquet, M. Handschuh, K. E. Honasoge, F. Kronowetter, Y. Nojiri, M. Partanen, M. Pfeiffer, H. van der Vliet, A. J. Matthews, J. Govenius, R. N. Jabdaraghi, M. Prunnila, A. Marx, F. Deppe, R. Gross & K. G. Fedorov. Cryogenic microwave link for quantum local area networks. *Npj Quantum Inf.* **11**, 87 (2025).

[200] A. T. A. M. de Waele. Basic Operation of Cryocoolers and Related Thermal Machines. *J. Low Temp. Phys.* **164**, 179–236 (2011).

[201] F. Pobell. *Matter and Methods at Low Temperatures* (Springer Berlin Heidelberg, 2007). URL `https://books.google.de/books?id=mRZ0uPfiWTQC`.

[202] C. Enss & S. Hunklinger. *Low-Temperature Physics*. SpringerLink: Springer e-Books (Springer Berlin Heidelberg, 2005). URL `https://books.google.de/books?id=ufM7sPMTGdAC`.

[203] S. Krinner, S. Storz, P. Kurpiers, P. Magnard, J. Heinsoo, R. Keller, J. Lütolf, C. Eichler & A. Wallraff. Engineering cryogenic setups for 100-qubit scale superconducting circuit systems. *EPJ Quantum Technol.* **6**, 2 (2019).

[204] P. Kurpiers, T. Walter, P. Magnard, Y. Salathe & A. Wallraff. Characterizing the attenuation of coaxial and rectangular microwave-frequency waveguides at cryogenic temperatures. *EPJ Quantum Technol.* **4**, 8 (2017).

[205] M. Renger. *Inter-lab Quantum Microwave Teleportation*. Phd thesis, Technische Universität München (2023). URL `https://www.wmi.badw.de/fileadmin/WMI/Publications/Renger_Michael_Doktorarbeit_2023.pdf`.

[206] R. Neagu. *FPGA-based Tomography of Propagating Quantum Microwaves*. Masters thesis, Technische Universität München (2019). URL `https://www.wmi.badw.de/fileadmin/WMI/Publications/Neagu%2CRobert_Masterarbeit_2019.pdf`.

[207] K. G. Fedorov, S. Pogorzalek, U. Las Heras, M. Sanz, P. Yard, P. Eder, M. Fischer, J. Goetz, E. Xie, K. Inomata, Y. Nakamura, R. Di Candia, E. Solano, A. Marx, F. Deppe & R. Gross. Finite-time quantum entanglement in propagating squeezed microwaves. *Sci. Rep.* **8**, 6416 (2018).

[208] E. P. K. Menzel. *Propagating Quantum Microwaves: Dual-path State Reconstruction and Path Entanglement*. Diploma thesis, Technische Universität München (2013). URL `https://www.wmi.badw.de/publications/theses/Menzel_Doktorarbeit_2013.pdf`.

[209] S. N. Filippov & V. I. Man'ko. Evolution of microwave quantum states in terms of measurable ordered moments of creation and annihilation operators. *Opt. Spectrosc.* **112**, 365–372 (2012).

[210] C. Eichler, D. Bozyigit, C. Lang, L. Steffen, J. Fink & A. Wallraff. Experimental State Tomography of Itinerant Single Microwave Photons. *Phys. Rev. Lett.* **106**, 220503 (2011).

[211] J. B. Altepeter, D. Branning, E. Jeffrey, T. C. Wei, P. G. Kwiat, R. T. Thew, J. L. O'Brien, M. A. Nielsen & A. G. White. Ancilla-Assisted Quantum Process Tomography. *Phys. Rev. Lett.* **90**, 193601 (2003).

[212] S. Filipp, P. Maurer, P. J. Leek, M. Baur, R. Bianchetti, J. M. Fink, M. Göppl, L. Steffen, J. M. Gambetta, A. Blais & A. Wallraff. Two-Qubit State Tomography Using a Joint Dispersive Readout. *Phys. Rev. Lett.* **102**, 200402 (2009).

[213] C. Schwemmer, G. Tóth, A. Niggebaum, T. Moroder, D. Gross, O. Gühne & H. Weinfurter. Experimental Comparison of Efficient Tomography Schemes for a Six-Qubit State. *Phys. Rev. Lett.* **113**, 040503 (2014).

[214] D. Rieger, S. Günzler, M. Spiecker, A. Nambisan, W. Wernsdorfer & I. Pop. Fano Interference in Microwave Resonator Measurements. *Phys. Rev. Appl.* **20**, 014059 (2023).

[215] W. Dai, G. Liu, V. Joshi, A. Miano, V. Sivak, S. Shankar & M. H. Devoret. Optimizing the pump coupling for a three-wave-mixing Josephson parametric amplifier. *Phys. Rev. Appl.* **23**, 054069 (2025).

[216] M. Renger, S. Pogorzalek, F. Fesquet, K. Honasoge, F. Kronowetter, Q. Chen, Y. Nojiri, K. Inomata, Y. Nakamura, A. Marx, F. Deppe, R. Gross & K. G. Fedorov. Flow of quantum correlations in noisy two-mode squeezed microwave states. *Phys. Rev. A* **106**, 052415 (2022).

[217] F. Kronowetter, F. Fesquet, M. Renger, K. Honasoge, Y. Nojiri, K. Inomata, Y. Nakamura, A. Marx, R. Gross & K. Fedorov. Quantum Microwave Parametric Interferometer. *Phys. Rev. Appl.* **20**, 024049 (2023).

[218] R. Schack & A. Schenzle. Moment hierarchies and cumulants in quantum optics. *Phys. Rev. A* **41**, 3847–3852 (1990).

[219] S.-H. Xiang, W. Wen, Y.-J. Zhao & K.-H. Song. Evaluation of the non-Gaussianity of two-mode entangled states over a bosonic memory channel via cumulant theory and quadrature detection. *Phys. Rev. A* **97**, 042303 (2018).

[220] Y. Dodge. *The Concise Encyclopedia of Statistics* (Springer New York, New York, NY, 2008). URL `http://link.springer.com/10.1007/978-0-387-32833-1`.

[221] H. Ezawa, A. Mann, K. Nakamura & M. Revzen. Characterization of thermal coherent and thermal squeezed states. *Ann. Phys.* **209**, 216–230 (1991).

[222] A. Uhlmann. The "transition probability" in the state space of a $*$-algebra. *Rep. Math. Phys.* **9**, 273–279 (1976).

[223] C. E. Rasmussen & C. K. I. Williams. *Gaussian Processes for Machine Learning* (The MIT Press, 2005). URL `https://direct.mit.edu/books/book/2320/Gaussian-Processes-for-Machine-Learning`.

[224] F. Mallet, M. A. Castellanos-Beltran, H. S. Ku, S. Glancy, E. Knill, K. D. Irwin, G. C. Hilton, L. R. Vale & K. W. Lehnert. Quantum State Tomography of an Itinerant Squeezed Microwave Field. *Phys. Rev. Lett.* **106**, 220502 (2011).

[225] J. Radon. On the determination of functions from their integral values along certain manifolds. *IEEE Trans. Med. Imaging* **5**, 170–176 (1986).

[226] G. B. Folland. *Harmonic Analysis in Phase Space. (AM-122)* (Princeton University Press, 1989). URL `https://www.degruyter.com/document/doi/10.1515/9781400882427/html`.

[227] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri & P. Grangier. Virtual Entanglement and Reconciliation Protocols for Quantum Cryptography with Continuous Variables. *Quantum Info. Comput.* **3**, 535–552 (2003).

[228] C. Fuchs & J. van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Trans. Inf. Theory* **45**, 1216–1227 (1999).

[229] M. Lovric. *International Encyclopedia of Statistical Science* (Springer, Berlin, 2011). URL https://doi.org/10.1007/978-3-642-04898-2.

[230] R. Renner & J. I. Cirac. de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography. *Phys. Rev. Lett.* **102**, 110504 (2009).

[231] I. Devetak & A. Winter. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A: Math. Phys. Eng. Sci.* **461**, 207–235 (2005).

[232] P. Jouguet, S. Kunz-Jacques & A. Leverrier. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A* **84**, 062317 (2011).

[233] V. Weidemann. *Microwave cryptography with propagating quantum tokens*. Masters thesis, Technische Universität München (2023). URL https://www.wmi.badw.de/fileadmin/WMI/Publications/Weidemann_Valentin_Masterarbeit_2023.pdf.

[234] M. Tomamichel, R. Colbeck & R. Renner. A Fully Quantum Asymptotic Equipartition Property. *IEEE Trans. Inf. Theory* **55**, 5840–5847 (2009).

[235] D. Awschalom *et al.* Development of Quantum Interconnects (QuICs) for Next-Generation Information Technologies. *PRX Quantum* **2**, 017002 (2021).

[236] P. Magnard, S. Storz, P. Kurpiers, J. Schär, F. Marxer, J. Lütolf, T. Walter, J.-C. Besse, M. Gabureac, K. Reuer, A. Akin, B. Royer, A. Blais & A. Wallraff. Microwave Quantum Link between Superconducting Circuits Housed in Spatially Separated Cryogenic Systems. *Phys. Rev. Lett.* **125**, 260502 (2020).

[237] E. Knyazev, K. Y. Spasibko, M. V. Chekhova & F. Y. Khalili. Quantum tomography enhanced through parametric amplification. *New J. Phys.* **20**, 013005 (2018).

[238] D. Gottesman, A. Kitaev & J. Preskill. Encoding a qubit in an oscillator. *Phys. Rev. A* **64**, 012310 (2001).

[239] F. Hanamura, W. Asavanant, S. Kikura, M. Mishima, S. Miki, H. Terai, M. Yabuno, F. China, K. Fukui, M. Endo & A. Furusawa. Single-shot single-mode optical two-parameter displacement estimation beyond classical limit. URL https://arxiv.org/abs/2308.15024 (2023).

[240] W. K. Yam. *Microwave quantum teleportation over a thermal channel*. Masters thesis, Technische Universität München (2022). URL https://www.wmi.badw.de/fileadmin/WMI/Publications/Yam_Wun_Kwan_Masterarbeit_2022.pdf.

[241] P. Krüger. *Single-Shot Microwave Quantum Key Distribution*. Masters thesis, Technische Universität München (2022). URL https://www.wmi.badw.de/fileadmin/WMI/Publications/Krueger_Philipp_Masterarbeit_2022.pdf.

[242] P. G. Baranov, H. J. von Bardeleben, F. Jelezko & J. Wrachtrup. *Magnetic Resonance of Semiconductors and Their Nanostructures*, Vol. 253 of *Springer Series in Materials Science* (Springer Vienna, Vienna, 2017). URL http://link.springer.com/10.1007/978-3-7091-1157-4.

[243] J. Štrancar. Advanced ESR Spectroscopy in Membrane Biophysics. In *ESR Spectroscopy in Membrane Biophysics* 49–93 (Springer US, Boston, MA, 2007). URL `http://link.springer.com/10.1007/978-0-387-49367-1_3`.

[244] M. Drescher & G. Jeschke (eds.) *EPR Spectroscopy, Applications in Chemistry and Biology*, Vol. 321 of *Topics in Current Chemistry* (Springer Berlin Heidelberg, Berlin, Heidelberg, 2012). URL `https://link.springer.com/10.1007/978-3-642-28347-5`.

[245] M. Steger, K. Saeedi, M. L. W. Thewalt, J. J. L. Morton, H. Riemann, N. V. Abrosimov, P. Becker & H.-J. Pohl. Quantum Information Storage for over 180 s Using Donor Spins in a 28 Si "Semiconductor Vacuum". *Science* **336**, 1280–1283 (2012).

[246] K. Saeedi, S. Simmons, J. Z. Salvail, P. Dluhy, H. Riemann, N. V. Abrosimov, P. Becker, H.-J. Pohl, J. J. L. Morton & M. L. W. Thewalt. Room-Temperature Quantum Bit Storage Exceeding 39 Minutes Using Ionized Donors in Silicon-28. *Science* **342**, 830–833 (2013).

[247] A. Bienfait, P. Campagne-Ibarcq, A. H. Kiilerich, X. Zhou, S. Probst, J. J. Pla, T. Schenkel, D. Vion, D. Esteve, J. J. L. Morton, K. Moelmer & P. Bertet. Magnetic Resonance with Squeezed Microwaves. *Phys. Rev. X* **7**, 041011 (2017).

[248] S. Weichselbaumer. *Spin Dynamics in Strongly Coupled Spin-Photon Hybrid Systems*. Phd thesis, Technische Universität München (2020). URL `https://www.wmi.badw.de/fileadmin/WMI/misc_uploads/Weichselbaumer_Stefan_Doktorarbeit_2020.pdf`.

[249] G. Feher. Electron Spin Resonance Experiments on Donors in Silicon. I. Electronic Structure of Donors by the Electron Nuclear Double Resonance Technique. *Phys. Rev.* **114**, 1219–1244 (1959).

[250] N. Stone. Table of nuclear magnetic dipole and electric quadrupole moments. *At. Data Nucl. Data Tables* **90**, 75–176 (2005).

[251] E. Jaynes & F. Cummings. Comparison of quantum and semiclassical radiation theories with application to the beam maser. *Proceedings of the IEEE* **51**, 89–109 (1963).

[252] M. Tavis & F. W. Cummings. Exact Solution for an $N$-Molecule—Radiation-Field Hamiltonian. *Phys. Rev.* **170**, 379–384 (1968).

[253] R. H. Dicke. Coherence in Spontaneous Radiation Processes. *Phys. Rev.* **93**, 99–110 (1954).

[254] J. H. Wesenberg, A. Ardavan, G. A. D. Briggs, J. J. L. Morton, R. J. Schoelkopf, D. I. Schuster & K. Mølmer. Quantum Computing with an Electron Spin Ensemble. *Phys. Rev. Lett.* **103**, 070502 (2009).

[255] K. E. Honasoge, M. Handschuh, W. K. Yam, S. Gandorfer, D. Bazulin, N. Bruckmoser, L. Koch, A. Marx, R. Gross & K. G. Fedorov. Fabrication of low-loss Josephson parametric devices. *Phys. Rev. B* – (2025).

[256] S. Probst, F. B. Song, P. A. Bushev, A. V. Ustinov & M. Weides. Efficient and robust analysis of complex scattering data under noise in microwave resonators. *Rev. Sci. Instrum.* **86** (2015).

[257] K. Yoshida, M. S. Hossain, T. Kisu, K. E. Keiji Enpuku & K. Y. Kaoru Yamafuji. Modeling of Kinetic-Inductance Coplanar Striplin with NbN Thin Films. *JJAP* **31**, 3844 (1992).

[258] P. Oehrl, T. Parvini, R. Gross & H. Huebl. Pulse shaping for optimal photon absoprtion into spin ensembles coupled to microwave resonators. Paper in preparation. (2025).

[259] M. Afzelius & C. Simon. Impedance-matched cavity quantum memory. *Phys. Rev. A* **82**, 022310 (2010).

[260] M. Afzelius, N. Sangouard, G. Johansson, M. U. Staudt & C. M. Wilson. Proposal for a coherent quantum memory for propagating microwave photons. *New J. Phys.* **15**, 065008 (2013).

[261] J. Z. Bernád, M. Schilling, Y. Wen, M. M. Müller, T. Calarco, P. Bertet & F. Motzoi. Analytical solutions for optimal photon absorption into inhomogeneous spin memories. *J. Phys. B: At., Mol. Opt. Phys.* **58**, 035501 (2025).

[262] J. Eisert & M. B. Plenio. Introduction to the basics of entanglement theory in continuous-variable systems. *Int. J. Quantum Inf.* **01**, 479–506 (2003).

# List of publications


1. F. Fesquet, F. Kronowetter, M. Renger, W. Yam, S. Gandorfer, K. Inomata, Y. Nakamura, A. Marx, R. Gross, K. G. Fedorov, "Demonstration of microwave single-shot quantum key distribution", *Nat. Commun.* **15**, 7544 (2024).

2. F. Fesquet, F. Kronowetter, M. Renger, Q. Chen, K. E. Honasoge, O. Gargiulo, Y. Nojiri, A. Marx, F. Deppe, R. Gross, K. G. Fedorov, "Perspectives of microwave quantum key distribution in open-air", *Phys. Rev. A* **108**, 032607 (2023).

3. S. Gandorfer, M. Renger, W. K. Yam, F. Fesquet, A. Marx, R. Gross, K. G. Fedorov, "Two-dimensional Planck Spectroscopy for Microwave Photon Calibration", *Phys. Rev. Appl.* **23**, 024064 (2025).

4. W. K. Yam, M. Renger, S. Gandorfer, F. Fesquet, M. Handschuh, K. E. Honasoge, F. Kronowetter, Y. Nojiri, M. Partanen, A. Marx, K. G. Fedorov, R. Gross, F. Deppe, "Cryogenic microwave link for quantum local area networks", *Npj Quantum Inf.* **11**, 87 (2025).

5. F. Kronowetter, F. Fesquet, M. Renger, K. Honasoge, Y. Nojiri, K. Inomata, Y. Nakamura, A. Marx, R. Gross, K. G. Fedorov, "Quantum microwave parametric interferometer", *Phys. Rev. Appl.* **20**, 024049 (2023).

6. M. Renger, S. Pogorzalek, F. Fesquet, K. E. Honasoge, F. Kronowetter, Q. Chen, Y. Nojiri, K. Inomata, Y. Nakamura, A. Marx, F. Deppe, R. Gross, K. G. Fedorov, "Flow of quantum correlations in noisy two-mode squeezed microwave states", *Phys. Rev. A* **106**, 052415 (2022).

7. T. Gonzalez-Raya, M. Casariego, F. Fesquet, M. Renger, V. Salari, M. Möttönen, Y. Omar, F. Deppe, K. G. Fedorov, M. Sanz1, "Open-Air Microwave Entanglement Distribution for Quantum Teleportation", *Phys. Rev. Appl.* **18**, 044002 (2022).

8. Q. Chen, M. Partanen, F. Fesquet, K. E. Honasoge, F. Kronowetter, Y. Nojiri, M. Renger, K. G. Fedorov, A. Marx, F. Deppe, R. Gross, "Scattering coefficients of superconducting microwave resonators. II. System-bath approach", *Phys. Rev. B* **106**, 214506 (2022).

9. Q. Chen, M. Pfeiffer, M. Partanen, F. Fesquet, K. E. Honasoge, F. Kronowetter, Y. Nojiri, M. Renger, K. G. Fedorov, A. Marx, F. Deppe, R. Gross, "Scattering coefficients of superconducting microwave resonators. I. Transfer matrix approach", *Phys. Rev. B* **106**, 214505 (2022).

10. Q. Chen, F. Kronowetter, F. Fesquet, K. E. Honasoge, Y. Nojiri, S. Pogorzalek, , Y. Nojiri, M. Renger, K. G. Fedorov, A. Marx, F. Deppe, R. Gross, "Tuning and amplifying the interactions in superconducting quantum circuits with subradiant qubits", *Phys. Rev. A* **105**, 012405 (2022).

# Acknowledgments

Over these last years, I have had the opportunity to interact with a large variety of people which greatly helped me throughout this work. Ranging from general physics discussions to tackling practical aspects such as screwing shields or installing devices in the labs, I am grateful to many that I would like to acknowledge in this section.

First, I would to thank my doctoral advisor *Prof. Dr. Rudolf Gross*, for giving me the chance to join the Wlather-Meißner-Institut and complete my thesis there. The quality of your work and valuable knowledge cannot be overstated. I am grateful for the many feedbacks you provided as well as a continuous support during the thesis.

I would like to thank *Dr. Kirill G. Fedorov* for being my everyday advisor. Thank you for your continuous help during the thesis with many insightful discussions. Plenty of ideas in this work result directly from our frequent exchanges. You have also guided me during lab work and showed a relentless desire to make things right. I greatly learned from your everyday perseverance and patience in science. I am particularly grateful for the many careful feedbacks given during all my thesis, that has constantly lifted me upwards. Additionally, I thank you for all the time and effort you spent helping me in my academic life, from scientific paper writing to this thesis.

A special thank to *Dr. Fabian Kronowetter* for the many hours we spent together in the lab. I am grateful for our long discussions trying to figure out lab problems, measurement plans, and data analysis. I am very glad of the results we have achieved. You have shown me a lot as a person and I very much admire your professionalism as well as your taste for life in general.

Additionally, my gratitude goes to *Dr. Michael Renger* who greatly helped me in the Bob lab or for general physics problems. One could also rely on you and be sure that you would come with a clever idea or a practical solution. I very much enjoyed our numerous trips together, either going to the US in Chicago or navigating the lands of my home country in Grenoble. It has been a pleasure to exchange with you, sharing our cultures and taste for physics together. Along these thoughts, I would like to warmly thank my co-workers *Simon Gandorfer* and *Wun Kwan Yam*. I greatly enjoyed our numerous discussions and work together. Whenever a lab related issue appeared or for some weird ideas about data analysis, I knew I could always rely on you and that if we put our minds together, we could (often) find a solution. I want to thank *Simon* for his calm demeanour and sharp mind, making that one always could count on you to help. His many ingenious ideas are hidden throughout this work, ranging from the development of the 2D Planck spectroscopy to physical model that are the backbone of this thesis data analysis. Likewise, *Wun Kwan* has shown remarkable expertise, especially through operating the cryolink system at WMI, always here if help is needed. I enjoyed our different discussions about secure communication and physics. I am impressed by your achievements and I have no doubt you will carry on this professionalism. I wish all of you all the best.

I would like to thank my colleague *Patricia Oherl* for the many time spent together, notably in the Abaqus lab. Thank you for introducing me to spin ensembles and their related physics.

I really appreciated our join efforts and discussions trying to figure out optimal measurements, exploring uncharted LabView code territories. Your kind and funny nature always made working with you a nice experience. I knew that I could rely on you at any time, for work-related problems or discussions about our daily life. I am proud of what we accomplished together and wish you a good continuity in your thesis. From her group, I would like to thank also *Korbinian Rubenbauer* for his help on numerous occasions in the Abaqus lab. I enjoyed our sessions together of screws and sample mounting while discussing about our music tastes. I applaud your devotion and integrity as a person, always trying to do the best you can, let it be in fabrication or volunteering as first aid. Similarly, I would like to thank *Dr. Thomas Luschmann* for his help in operating the Abaqus lab. I thank him for giving us access to high quality coffees which we very much make use of. I wish you all the best with Peak Quantum! Lastly, I would like to thank *Prof. Hans Huebl* for giving me the opportunity to work in the Abaqus lab and for the many discussions we had regarding spin ensemble physics. His constant involvement and support were greatly appreciated as well as his valuable inputs and help regarding data acquisition or data analysis.

I would like to thank all of our fabrication colleagues. In particular, I thank *Kedar Honasoge* and *Maria-Teresa Handschuh* for all of their efforts in the fabrication of JPAs that were used during spin ensemble measurements in this thesis. I am grateful to *Kedar* for all the help he provided with JPA measurements and the time we spent together in the labs. I appreciated all of our discussions and admire your problem-solving ingenuity. I enjoyed a lot all of our table tennis games and late evenings. Good luck with Peak Quantum as well! I am grateful to *Maria* as well for all her efforts in the fabrication of devices for the group. Your kindness and hard-working nature were very pleasant, reflected in the great quality of the work you provide. I wish you all the best with your own work in your thesis. I would like to thank *Daniil Bazulin* for his amazing personality. I have rarely seen someone as enjoyable to be around as you my good Monsieur. Thank you for your contribution to the fabrication team. I wish you good luck in your pursuit of JTWPA fabrication, if anyone can make it, it is you. I am also happy to have introduced you to the French delicacy of flans. I would also like to thank former WMI member, *Dr. Yuki Nojiri*, for his contribution as well to the fabrication team. I appreciate your kindness and I am happy that we could discuss about many common topic of interest. Je te souhaite le meilleur en France!

I would like to thank my Master students for their work. First, my gratitude goes to *Philipp Krüger*, with whom we got first promising QKD results. We spent a lot of time together in the labs and he contributed to the main results of this thesis. I have many fond memories working with you. Your happy nature and positive mental attitude made the work everyday more pleasant. Similarly, I would like to thank *Valentin Weidemann* for continuing the QKD project with me, to which he helped push to the final results presented in this work. I thank you for the many interesting physics discussions we had and for the work you provided. I greatly enjoyed the many measurements in Bob lab together. I appreciate your calmness and focused mindset as well as your determination. Lastly, I would like to thank *Sebastiano Covone* for the time we spent together in the qubit lab. We had many interesting and novel discussions about different aspects of quantum communication or quantum computing that I was not familiar with. I applaud your ingenuity and curious nature, always eager to seek and understand details of your topic. I wish you all the best for your future.

Importantly, I would like to thank office colleagues with whom I shared many great moments and made the daily life more enjoyable. First, I would like to thank my old colleague, *Dr. Manuel Müller*, for the awesome time we had at the institute. We shared many great experiences together, ranging from the late night at the institute discussing about various topics to the many

jogging sessions by the Isar. I sincerely admire your professionalism and undying commitment to any task assigned to you. I am very happy to have spent this time at the institute with you and can only look for more. Additionally, I would like to thank *Ivan Tsitsilin* for the many great discussions and funny demeanour. I learned quite a few things thanks to you, enjoying your sharp mind and cleverness. It is clear that people can rely on you, always finding smart practical solutions. My thanks go as well to Senior *Mathias Grammer* for his funny personality that made everyone happier and more relaxed. Last but not least, I would like to thank *Julius Feigl* for the discussions and exchanges we had together. I respect your eager-to-act nature and your many work efforts, even outside the institute such as your introduction to quantum computing at the Deutsches Museum.

I would like to thank *Ana Strinic* for the many great moments at the institute. I appreciate your cunning mind and integrity as a person, with a touch of cheekiness that we all know and like. I really enjoyed our table tennis games at the institute and hope to reiterate it one day if the circumstances present themselves. Additionally, I would like to thank *Shamil Erkenov*, my table tennis partner-in-crime. We had a great time together, notably thanks to your overall friendliness and support. I applaud your continuous commitment and seriousness in your work. I would like to thank also *Johannes Weber* for the many great moments together and being my gym bro. Monsieur, we had many laughs and funny interactions where we could exchange a lot about the French/German cultures. I enjoy your incredible kindness and happy-going, making it always a good time when you are around.

I would like to thank all the members of the quantum computing group for their help with lab-related questions, development of fabrication processes at the WMI, and being great people to be around. I applaud the quality of the work and great results you have obtained since the formation of the group. I am convinced that you will continue to do so in the future.

Similarly, I would like to thank everyone in the theoretical group of *Prof. Peter Rabl* for insightful physics discussions and great time to be around. I am grateful for the collaborations we have with the group and for the help with some of our theoretical models.

I would like to thank all members of the magnetism group as well as the group of *Dr. Nadezhda Kukharchyk* for their valuable feedbacks and help in the labs.

I would like to thank *Maria Botta* and *Sybilla Plöderl* for always making sure that the institute is clean. I enjoyed our small talks and wish you all the best too.

I would like to thank *Dr. Achim Marx* for his continuous support in the labs, especially when working in the Qubit lab. One could always rely on your help and great physics intuition. Your calm demeanour for any topics is not only very helpful but also very pleasant. I would like to thank the WMI workshop, *Alexander Rößl* and his team, for the fabrication of divers components that we needed in our experimental setups. In particular, I thank you all for the fabrication of the JPA sample boxes and their aluminium boxes. Additionally, I would like to thank *Andreas Russo* for his help with electrical components and electrical engineering expertise. Similarly, I would like to thank the helium liquefaction team, *Peter Binkert*, *Harald Schwaiger* and *Jan Naundorf* for proving liquid helium and nitrogen to all the students in the institute. Last but not least, I would like to thank the WMI administration, *Martina Meven*, *Carola Siegmayer*, *Andrea Person*, and especially *Emel Dönertas* who has provided a great administration support throughout the thesis.

I would like to thank my family and friends for their constant support during these years of thesis.