Technische
Universität
München

Walther-
Meißner-
Institut

Bayerische
Akademie der
Wissenschaften

Single-Shot Microwave Quantum Key Distribution

Master’s Thesis

Philipp Krüger

Supervisor: Prof. Dr. Rudolf Gross

Advisor: Dr. Kirill Fedorov

Garching, April 25, 2022

Fakultät für Physik

Technische Universität München

Quantum Cryptography

Alice said to her friend Eve,
"Why do you practice to deceive?
You know I need to talk to Bob.
Without that I won’t have a job.

"Bob can’t know where my note has been.
He thinks that you are listening in.
He wonders if it’s safe enough
For me to send him secret stuff.

"And Bob’s right not to trust you, Eve,
With quantum tricks stuffed up your sleeve.
But he thinks we can freeze you out,
With quantum tricks we’ve learned about.

"With quantum states, what we achieve
Defeats whatever you conceive.
So even Bob has to believe
That you can’t hear us, can you Eve?"

John Preskill (November 1, 2001)

Abstract

Quantum cryptography aims to exploit the laws of quantum mechanics to securely transmit data. Among different possible encryption methods, we focus on quantum key distribution (QKD). In this context, the no-cloning theorem limits the access of an eavesdropper to information communicated via a quantum channel between two parties. In this thesis, we implement a specific prepare-and-measure continuous-variable QKD protocol proposed by Cerf *et al.* [1], which encodes classical information in displacement amplitudes of squeezed coherent states of light. In our experimental implementation, we use propagating squeezed microwaves at the carrier frequency of $f_0 = 5.5231\,\mathrm{GHz}$. The detection of these microwave signals relies on cryogenic amplification chains. Here, state-of-the-art cryogenic high-electron mobility transistor amplifiers add $10 - 20$ noise photons, corresponding to a quantum efficiency of $\eta < 5\%$. These phase-insensitive amplifiers are ill-suited for QKD, as they typically reduce the signal-to-noise ratio (SNR) below a threshold required for the secure communication and are also bound by the standard quantum limit (SQL), $\eta = 50\%$. Therefore, we make use of superconducting phase-sensitive amplifiers which can even exceed the SQL to implement the aforementioned CV-QKD protocol with quantum microwaves in the single-shot regime.

As our main experimental result, we achieve a positive secret key for our microwave CV-QKD protocol implementation and analyze its robustness against an eavesdropping attack. To this end, we use a Josephson parametric amplifier (JPA) in the phase-sensitive regime at the beginning of the cryogenic amplification chain. With this modification, we demonstrate a significant improvement in the experimental quantum efficiency, $\eta = 38\%$. This step allows us to increase the SNR from 14% to 177% during the CV-QKD protocol sequence which results in the positive secret key. The current SNR is mainly limited by the dynamic range of our JPAs. In the future, the SNR can be further improved by exploiting traveling wave parametric amplifiers. Our results highlight the experimental feasibility of microwave CV-QKD protocols.

Contents

List of Figures

List of Tables

1 Introduction

Quantum information theory promises many novel applications in various fields, such as communication [2], computation [3], and metrology [4]. These applications often rely on the interplay between classical algorithms and features of quantum mechanics, such as quantum uncertainty [5], quantum superposition [6], and quantum entanglement [7]. Quantum information theory emerged from the success of quantum theories in physics [8] and the development of programmable digital computers [9]. Before the advent of modern computers, Claude Shannon demonstrated in 1940 that electrical circuits could perform any boolean logical operation [10]. Eight years later, he founded the field of information theory in his seminal paper *A Mathematical Theory of Communication* [11]. There, he quantified the ultimate compressibility of information and ultimate limit for transmitting information over a communication channel. Using these newly developed concepts, he provided an unconditional security proof of the one-time pad (OTP) method [12], where a message is encoded with a bit-by-bit XOR operation of a randomly generated set of bits (key) [13]. In order to achieve the absolute security, this secret shared key must be completely random and as long as the encoded message (plaintext). The OTP method is a symmetric encryption method, as both parties have access to the same key.

Many modern encryption methods use asymmetric encryption, where the shared key consists of a combination of private and public keys. The Diffie–Hellman key exchange [14] and the RSA scheme [15] are among the most prominent examples. Here, the public key is generated from the private key, which consists of a product of two large prime numbers and an auxiliary value. In contrast to the OTP method, its security is not unconditional. The impossibility to infer the private key from the public key relies on the assumption that factoring out two large unknown prime numbers requires computational resources that are not available to a potential eavesdropper. This assumption was challenged in 1994 by Peter Shor's algorithm [16]. This algorithm relies on quantum resources and allows for an efficient factorization of large integer numbers with polynomial scaling.

Prospects of quantum computing, first envisioned by Richard Feynman [17], were heavily doubted by William Unruh [18]. In response, Shor developed the first scheme for error-correction [19] and fault-tolerant quantum computation [20]. Afterwards, he showed that all cryptosystems which rely on general factorization, or discrete logarithm problems, are breakable in polynomial time on a quantum computer [21]. Consequently, the focus for post-quantum algorithms shifted back to symmetric encryption algorithms like the OTP method or the newly developed AES standard (2001) [22]. One of the cornerstones of these protocols is a secure distribution of keys between the communicating parties.

This goal can be achieved by using quantum key distribution (QKD), where a secret classical key is shared using quantum states. The usage of corresponding quantum communication channels instead of classical channels requires an adaptation of Shannon's information theory by taking into account new resources provided by quantum mechanics. These adaptations were largely influenced by the Russian physicist Alexander Holevo. He found that it is not possible to transmit more than one classical bit per transferred qubit state [23]. This proof was the main ingredient for evaluating the classical capacity of a noisy quantum channel by Holevo [24], and Schumacher and Westmoreland [25].

The first practical QKD protocol was proposed by Bennett and Brassard in 1984 and is known under the acronym BB84 [26]. It was inspired by Wiesner's idea for conjugate coding [27]. In the BB84 protocol, a discrete-variable encoding is used via the preparation and measurement of photon polarization [28]. Any interference of an eavesdropper with the communication necessarily results in a disturbance of the statistics for the shared key due to the no-cloning theorem [29–31]. The first security proof of the BB84 protocol by Shor and Preskill [32] used the equivalence principle [26] between the entanglement-based E91 and BB84 protocols [33].

Timothy Ralph was first to consider the encoding of keys in continuous-variable (CV) quadratures of multi-photon states instead of the discrete-variable (DV) polarizations of single-photon states [34]. In 2001, Cerf *et al.* [1] proposed encoding symbols in the Gaussian-modulated amplitude of displaced squeezed vacuum states, which improved the bit-depth, as compared to DV [1]. Later, error correction and privacy amplification protocols were added for this protocol [35]. More CV-QKD protocols emerged in the following years [36, 37] and related security proofs for CV-QKD were provided by Pirandola *et al.* [38]. In 2015, a formal derivation of the secret key capacity (the maximal amount of secure bits transmitted per channel use) was found for CV-QKD protocols [39].

So far, experimental implementations of CV-QKD protocols have been demonstrated only for optical frequencies $\sim 4000\,\mathrm{THz}$. First laboratory demonstrations were made in 2003 [40]. Later on, experimental implementations were continuously improved to communication distances over 50 km in 2019 [41]. The communication at optical frequencies is possible over high distances due to low losses in optical fibers and practically absent noise photons.

However, modern computation and communication hardware like WiFi [42], or the 5G standard [43], operate at microwave frequencies ($300\,\mathrm{MHz} - 5\,\mathrm{GHz}$). This is also the case for superconducting quantum computers [44]. Recent advances in experiments with quantum microwaves [45, 46] allowed for first quantum microwave communication protocols like remote state preparation [47] or quantum teleportation [48]. Moreover, a theory analysis showed experimental feasibility of a fully microwave CV-QKD protocol using squeezed states [49]. There, propagating squeezed states are assumed to be generated using flux-driven Josephson parametric amplifiers (JPAs) [50].

This work builds on the advances which were made in Ref. 49 by building a corresponding experimental setup. We achieve a positive experimental secret key rate by averaging over the acquired samples with a heterodyne microwave detection scheme. However, careful analysis shows that averaging must be inherently prohibited in the QKD protocol, because it contradicts the security of the communication channel imposed by the no-cloning theorem. If each symbol of the quantum key can be obtained from multiple averages, an eavesdropper could potentially perform a precise tomography of the transmitted state and break the encryption. In this context, our main goal is to achieve a positive secret key for a single-shot readout of the propagating quantum microwaves at the bandwidth of our electronic readout components. We aim to achieve this task by employing an extra JPA as a phase-sensitive preamplifier. We improve a quadrature-dependent signal-to-noise ratio (SNR) and increase the readout quantum efficiency, so that a positive secret key within a single demodulation period becomes possible. In order to achieve our goal, we need to synchronize all setup components, and characterize the optimal working point for the squeezing JPA and the preamplifier JPA.

Chapter 2 starts with a theoretical description of properties and transformations of quantum microwave states. Afterwards, we introduce a framework for amplification noise and JPAs as a tool for phase-sensitive amplification. We introduce a particular CV-QKD protocol and outline how to calculate the secret key. Chapter 3 concerns experimental methods. Our implementation operates superconducting circuits in a cryogenic dilution refrigerator. We describe the implementation and characterization of the CV-QKD protocol in an experimental cryogenic microwave setup. Chapter 4 is dedicated to the comparison of experimental secret key measurements with and without phase-sensitive amplification. We compare our secret key with estimates from the calibration measurements and discuss our findings. Chapter 5 highlights main novel results and provides an outlook.

2 Theoretical Concepts

In this chapter, we provide a conceptual theory framework. First, we introduce propagating quantum microwaves and their description in phase-space using the Wigner quasi-probability distribution. We also use the covariance matrix formalism to represent Gaussian states and their transformations in a mathematically concise way. Later, we introduce theory of phase-preserving (nondegenerate) and phase-sensitive (degenerate) amplification. We show how phase-sensitive amplification can be implemented with a superconducting Josephson parametric amplifier (JPA). In the third section, we describe a specific quantum communication protocol which we study experimentally in this thesis. This protocol relies on a continuous-variable quantum key distribution (CV-QKD) using Gaussian-modulated displaced squeezed states. Our main goal is to investigate the security of this protocol. To this end, we define the units and amount of information that can be shared or eavesdropped by different communication parties over a quantum channel.

2.1 Propagating quantum microwaves

We start with a brief motivation for the phase-space representation of propagating quantum states. In particular, we are interested in Gaussian states and operations that preserve the Gaussian nature.

2.1.1 Quadratures of the quantized electromagnetic field

Microwaves are electromagnetic field oscillations in the frequency range ($300\,\mathrm{MHz} - 300\,\mathrm{GHz}$). A single-mode microwave field can be described by its amplitude A, angular frequency $\omega = 2\pi f$, and phase ϕ, as $A(t) = A\cos(\omega t + \phi)$. We obtain an equivalent formulation by decomposing the amplitude $A(t)$ into its in-phase, $I(t)$, and out-of-phase, $Q(t)$ quadrature components. In particular, we employ the angle sum identity, so that

$$\begin{aligned} A(t) &= A\cos(\omega t + \phi) \\ &= A\cos(\phi)\cos(\omega t) + A\sin(\phi)\sin(\omega t) \\ &= I(t)\cos(\omega t) + Q(t)\sin(\omega t)\,, \end{aligned} \tag{2.1}$$

where $I(t) = A\cos(\phi)$, $Q(t) = A\sin(\phi)$, $A = \sqrt{I(t)^2 + Q(t)^2}$ and $\phi = \arctan(Q(t)/I(t))$. However, this classical description is unable to reflect quantum features.

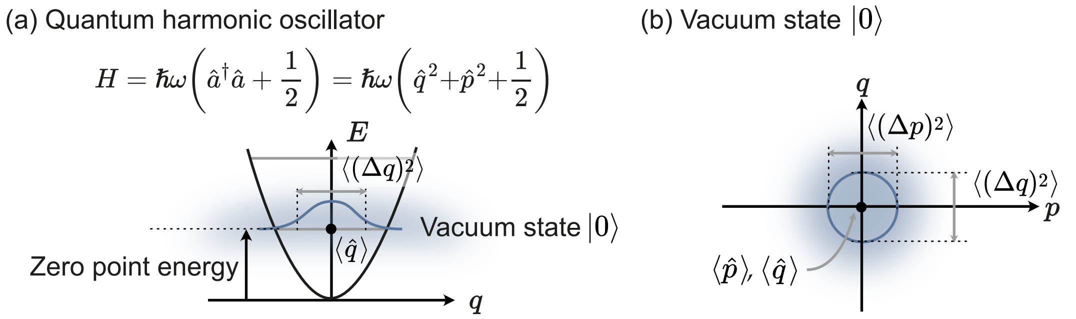
(a) Quantum harmonic oscillator
$H = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right) = \hbar\omega\left(\hat{q}^2+\hat{p}^2+\frac{1}{2}\right)$
E
$\langle(\Delta q)^2\rangle$
Vacuum state $|0\rangle$
$\langle\hat{q}\rangle$
Zero point energy
q
(b) Vacuum state $|0\rangle$
q
$\langle(\Delta p)^2\rangle$
$\langle(\Delta q)^2\rangle$
p
$\langle\hat{p}\rangle, \langle\hat{q}\rangle$

Figure 2.1: (a) Zero point energy of the quantum harmonic oscillator. The ground state energy is $E_0 = \hbar\omega/2$. (b) The vacuum state $|0\rangle$ is the lowest eigenstate of the quantum harmonic oscillator. The expectation values of the quadrature operators are $\langle\hat{p}\rangle = \langle\hat{q}\rangle = 0$; the variance of the quadratures is $\langle(\Delta\hat{p})^2\rangle = \langle(\Delta\hat{q})^2\rangle = 0.5$.

A quantum-mechanically accurate framework can be created via quantization of the electromagnetic field in free space. A thorough introduction to this topic can be found in Refs. 51, 52. In short, the Hamiltonian of a single-mode electromagnetic field is equivalent to a quantum harmonic oscillator [52]

$$H = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right), \tag{2.2}$$

with the Planck constant $\hbar$, the angular frequency ω and the bosonic creation, $\hat{a}^\dagger$, and annihilation, $\hat{a}$, operators. These operators obey the bosonic commutation relation $\left[\hat{a}, \hat{a}^\dagger\right] = 1$. Then, the single-mode solution $\hat{E}(t)$ is defined as [53]

$$\hat{E}(t) = E_0\left[\hat{a}e^{i\omega t} + \hat{a}^\dagger e^{-i\omega t}\right], \tag{2.3}$$

where E_0 contains dimensional prefactors. Here, $\hat{a}$ describes the forward propagating and $\hat{a}^\dagger$ the backwards propagating waves. Then, we can define the canonical quadrature operators $\hat{q}$ and $\hat{p}$ as

$$\hat{q} = \frac{\hat{a}+\hat{a}^\dagger}{2}, \quad \hat{p} = \frac{\hat{a}-\hat{a}^\dagger}{2i}, \quad [\hat{q},\hat{p}] = \frac{i}{2}. \tag{2.4}$$

Using this definition, we can rewrite the electric field in terms of the sine and cosine parts as [53]

$$\hat{E}(t) = 2E_0\left[\hat{q}\cos(\omega t) + \hat{p}\sin(\omega t)\right]. \tag{2.5}$$

This description of the propagating microwave field is compatible with quantum mechanics due to the nature of $\hat{q}$ and $\hat{p}$ quadrature operators. Unlike their classical counterparts I and Q, the precision of a simultaneous measurement of both q and p is bounded by the Heisenberg uncertainty relation [54]

$$\langle(\Delta q)^2\rangle\langle(\Delta p)^2\rangle \geq \frac{1}{4}\left|\langle[\hat{q},\hat{p}]\rangle\right|^2 = \frac{1}{16}, \tag{2.6}$$

where the variance of an observable $\hat{O}$ is defined as

$$\Delta\hat{O}^2 = \langle\hat{O}^2\rangle - \langle\hat{O}\rangle^2. \tag{2.7}$$

The quadrature operators and their minimal uncertainty are the central properties for quantum microwave signals.

2.1.2 Quadrature moments of Gaussian states

Quantum states are usually described by their density matrix $\hat{\rho} = \sum_i^{\mathrm{N}} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$, $\mathrm{Tr}(\hat{\rho}) = 1$, where p_i is the probability for a system to be in the pure state $\left|\psi_i\right\rangle$. An analogous description can be achieved by using a the quasi-probability distribution provided by the Wigner function. The Wigner function allows us to characterize a quantum state in the phase-space spanned by the quadrature components p and q. The Wigner function $W(q,p)$ can be directly obtained from the density matrix [55]

$$W(q,p) = \frac{1}{\pi\hbar}\int \left\langle q-y\right| \hat{\rho} \left|q+y\right\rangle e^{2ipy/\hbar} dy. \tag{2.8}$$

The Wigner function behaves like a classical probability distribution in terms of normalization (i.e., $\int W(q,p)dqdp = 1$) and marginal distributions (i.e., $\int W(q,p)dp = \left\langle q\right| \hat{\rho} \left|q\right\rangle$). However, the Wigner function (for example, for Fock states) can be negative, $W(q,p) < 0$, for a certain range of quadratures. Therefore, the Wigner function is often referred to as the quasi-probability distribution [56][1].

Gaussian states represent a subclass of general quantum states. Hudson's theorem states that the Wigner function of any pure quantum state is positive if and only if it follows a Gaussian distribution in phase space [60–62]. Gaussian states encompass coherent, thermal, squeezed states, and their linear superpositions. In this work, we focus on generation and exploitation of microwave Gaussian states. Therefore, we can introduce a more concise formalism limited to Gaussian states. In particular, the Wigner function of an N-mode Gaussian state (see Eq. 2.9) can be reformulated using its displacement vector $\bar{\mathbf{r}} = \langle\hat{r}\rangle$ (first-order statistical moment) and covariance matrix $\mathbf{V} = (V_{ij}) \in \mathbb{R}^{2N\times 2N}$ (second-order statistical moment) as [63, 64]

$$W(\hat{\mathbf{r}}) = \frac{1}{(2\pi)^{\mathrm{N}}\sqrt{\det\mathbf{V}}} \exp\left[-\frac{1}{2}(\hat{\mathbf{r}}-\bar{\mathbf{r}})\mathbf{V}^{-1}(\hat{\mathbf{r}}-\bar{\mathbf{r}})^{\mathrm{T}}\right]. \tag{2.9}$$

Here, the displacement vector is

$$\bar{\mathbf{r}} = (\langle\hat{q}_1\rangle, \langle\hat{p}_1\rangle, \ldots, \langle\hat{q}_N\rangle, \langle\hat{p}_N\rangle), \tag{2.10}$$

[1] This is due to the violation of Bochner's theorem for classical probability, which tells us that the Fourier transformation of a continuous positive-definite function on a locally compact Abelian group corresponds to a finite positive measure on the Pontryagin dual group. The interested reader is referred to Refs. 56–59.

and the covariance matrix $\mathbf{V}$ is given by

$$V_{ij} = \frac{1}{2}\langle\{\Delta\hat{r}_i, \Delta\hat{r}_j\}\rangle = \frac{\langle\hat{\boldsymbol{r}}_i\hat{\boldsymbol{r}}_j + \hat{\boldsymbol{r}}_j\hat{\boldsymbol{r}}_i\rangle}{2} - \langle\hat{\boldsymbol{r}}_i\rangle\langle\hat{\boldsymbol{r}}_j\rangle, \tag{2.11}$$

where $\Delta\hat{r}_i = \hat{r}_i - \langle\hat{r}_i\rangle$, $\{,\}$ is the anti-commutator, and $i, j = 1, \ldots, 2N$. The diagonal elements of the covariance matrix can be reduced to the variances of field quadratures [64]

$$V_{ii} = \langle(\Delta\hat{r}_i)^2\rangle = \langle\hat{r}_i^2\rangle - \langle\hat{r}_i\rangle^2. \tag{2.12}$$

The covariance matrix is constrained by the Heisenberg uncertainty principle so that $\det V^N \geq 1/16^N$ for an arbitrary N-mode state [53].

Purity is another important measure of quantum states indicating their mixedness. The purity, μ, of a Gaussian state depends on the covariance matrix as

$$\mu = \frac{1}{4^N\sqrt{\det(\mathbf{V})}}. \tag{2.13}$$

Equivalent to their description via quadrature moments, we can formulate the Gaussian Wigner function in terms of its measurable signal moments $\langle(\hat{a}^\dagger)^m\hat{a}^n\rangle$ with $m, n \in \mathbb{N}_0$, $m+n \leq 2$ [65]. This allows a full state tomography [66]. The Wigner function of a Gaussian state can be written as [65, 67]

$$\begin{aligned} W(\hat{a}, \hat{a}^\dagger) = & \frac{1}{\pi\sqrt{(\mathcal{N}+1/2)^2 - |\mathcal{M}|^2}} \\ & \times \exp\left[-\frac{(\mathcal{N}+1/2)|\alpha - \langle\hat{a}\rangle|^2 - (\mathcal{M}^*/2)(\alpha - \langle\hat{a}\rangle)^2 - (\mathcal{M}/2)(\alpha^* - \langle\hat{a}^\dagger\rangle)^2}{(\mathcal{N}+1/2)^2 - |\mathcal{M}|^2}\right], \end{aligned} \tag{2.14}$$

with the displacement amplitude $\alpha = q + ip$, and the measured central moments [68]

$$\begin{aligned} \langle\hat{a}^2\rangle^{(c)} \equiv & \mathcal{M} = \left\langle\hat{a}^2\right\rangle - \langle\hat{a}\rangle^2 \\ \langle\hat{a}^\dagger\hat{a}\rangle^{(c)} \equiv & \mathcal{N} = \left\langle\hat{a}^\dagger\hat{a}\right\rangle - |\langle\hat{a}\rangle|^2 \\ \mathcal{N} \geq 0,& \quad \mathcal{N}(\mathcal{N}+1) \geq |\mathcal{M}|^2. \end{aligned} \tag{2.15}$$

In conclusion, an arbitrary Gaussian state is completely described by its mean displacement $\bar{\mathbf{r}}$ and its covariance matrix $\mathbf{V}$, which are accessible through the measurements of signal moments.

2.1.3 Gaussian squeezing and displacement

Squeezing and displacement are Gaussian unitary operations. A quantum operation is Gaussian when it transforms Gaussian states into Gaussian states [64]. We can also introduce a Gaussian communication channel which can be viewed as a linear map that is completely positive and trace preserving [69]. A subset of these transformations can be represented by unitary transformations, such that $\hat{\rho} \rightarrow U\hat{\rho}U^{\dagger}$ is pure ($\mathrm{Tr}(\hat{\rho}^2) = 1$). This holds only in the absence of added noise. In Ref. 70, the reader can find a complete derivation showing that an affine symplectic map $(\mathbf{S}, \mathbf{d})$ can fully characterize a Gaussian unitary channel as [64, 71]

$$\begin{aligned} U(\mathbf{S}, \mathbf{d}): \quad \hat{\mathbf{r}} &\rightarrow \mathbf{S}\hat{\mathbf{r}} + \mathbf{d}, \\ \mathbf{V} &\rightarrow \mathbf{S}\mathbf{V}\mathbf{S}^T, \end{aligned} \tag{2.16}$$

where $\mathbf{S}$ is a symplectic matrix which fulfills

$$\mathbf{S}\boldsymbol{\Omega}\mathbf{S}^T = \boldsymbol{\Omega}, \quad \text{with} \quad \boldsymbol{\Omega} = \mathrm{diag}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{2.17}$$

Next, we describe the most important states in this work: vacuum, thermal, displaced, squeezed states and their linear superpositions.

Vacuum and thermal state

The vacuum state $|0\rangle$ has zero noise photons $n_{\mathrm{th}} = 0$, and minimum variance in the canonical variables $(\Delta q)^2 = (\Delta p)^2 = 1/4$ [64] (see Fig. 2.3 (a)). The vacuum state is then simply described by

$$\bar{\mathbf{r}}_{\mathrm{vac}} = 0 \quad \text{and} \quad \mathbf{V}_{\mathrm{vac}} = \frac{\mathbb{I}}{4}, \tag{2.18}$$

where $\mathbb{I}$ is the identity matrix. In practice, a non-zero temperature of the electromagnetic mode, $T > 0\,\mathrm{K}$, increases the uncertainty by adding a finite amount of thermal photons n_{th} in the bosonic mode, which can be computed with the Planck distribution [72]

$$n_{\mathrm{th}} = \frac{1}{\exp(\hbar\beta\omega) - 1}, \tag{2.19}$$

where $\beta = 1/(k_B T)$. As a consequence, the covariance matrix has to account for additional noise (see Fig. 2.3 (b)). The Gaussian Wigner function of a thermal state is defined by [64]

$$\bar{\mathbf{r}}_{\mathrm{th}} = 0 \quad \text{and} \quad \mathbf{V}_{\mathrm{th}} = (1 + 2n_{\mathrm{th}})\frac{\mathbb{I}}{4}. \tag{2.20}$$

However, often the condition $k_B T \ll hf$ is fulfilled, as it is also the case in many cryogenic microwave experiments ($f \simeq 5\,\mathrm{GHz}$, $T \simeq 40\,\mathrm{mK}$, $n_{\mathrm{th}} \leq 10^{-2}$), the vacuum state is a good approximation for the lowest energy state.

Displacement and coherent states

An arbitrary coherent state $|\alpha\rangle$ is the eigenstate of the annihilation operator $\hat{a}$ with an eigenvalue α [73]

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,. \tag{2.21}$$

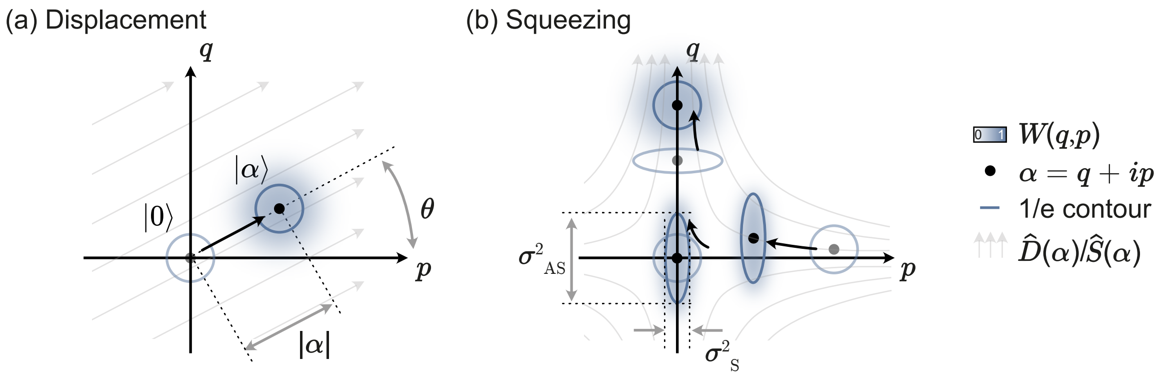

Figure 2.2: (a) Displacement operation. The vacuum state $|0\rangle$ is displaced to the coherent state $|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle$. The displacement amplitude is given by $\alpha = |\alpha|e^{i\theta} = q + ip$. (b) Squeezing operation. The p quadrature is squeezed. In the center, we depict a squeezed vacuum state. Off center, we plot displaced (coherent) squeezed states with different displacement amplitudes.

The coherent state $|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle$ can be decomposed in the number state basis [51]

$$|\alpha\rangle = \exp\!\left(-\frac{1}{2}|\alpha|^2\right)\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,. \tag{2.22}$$

If we substitute $|n\rangle = \left[(\hat{a}^\dagger)^n/\sqrt{n!}\right]|0\rangle$ in Eq. 2.22, we can obtain the definition of the displacement operator $\hat{D}(\alpha)$ (see also Sec. A.2)

$$\hat{D}(\alpha) = \exp\!\Big(\alpha\hat{a}^\dagger - \alpha^*\hat{a}\Big), \tag{2.23}$$

where $\alpha = q + ip$ is the complex displacement amplitude. The action of the displacement operator on the creation and annihilation operators $\hat{a}^\dagger$ and $\hat{a}$ is [51]

$$\begin{aligned}\hat{D}^\dagger(\alpha)\hat{a}\hat{D}(\alpha) &= \hat{a} + \alpha,\\ \hat{D}^\dagger(\alpha)\hat{a}^\dagger\hat{D}(\alpha) &= \hat{a}^\dagger + \alpha^*.\end{aligned} \tag{2.24}$$

The displacement operator $\hat{D}(\alpha)$ can be expressed using the symplectic map formalism, via the symplectic matrix $\mathbf{S}$ and displacement vector $\mathbf{d}$

$$\mathbf{S} = \mathbb{I}, \quad \mathbf{d} = \mathbf{d}_\alpha = \begin{pmatrix} q \\ p \end{pmatrix} = \begin{pmatrix} \mathrm{Re}\{\alpha\} \\ \mathrm{Im}\{\alpha\} \end{pmatrix}. \tag{2.25}$$

Respectively, the displacement transformation becomes [64]

$$\begin{aligned}\hat{D}(\alpha):\quad \hat{\mathbf{r}} &\mapsto \hat{\mathbf{r}} + \mathbf{d}_\alpha,\\ \mathbf{V} &\mapsto \mathbf{V}.\end{aligned} \tag{2.26}$$

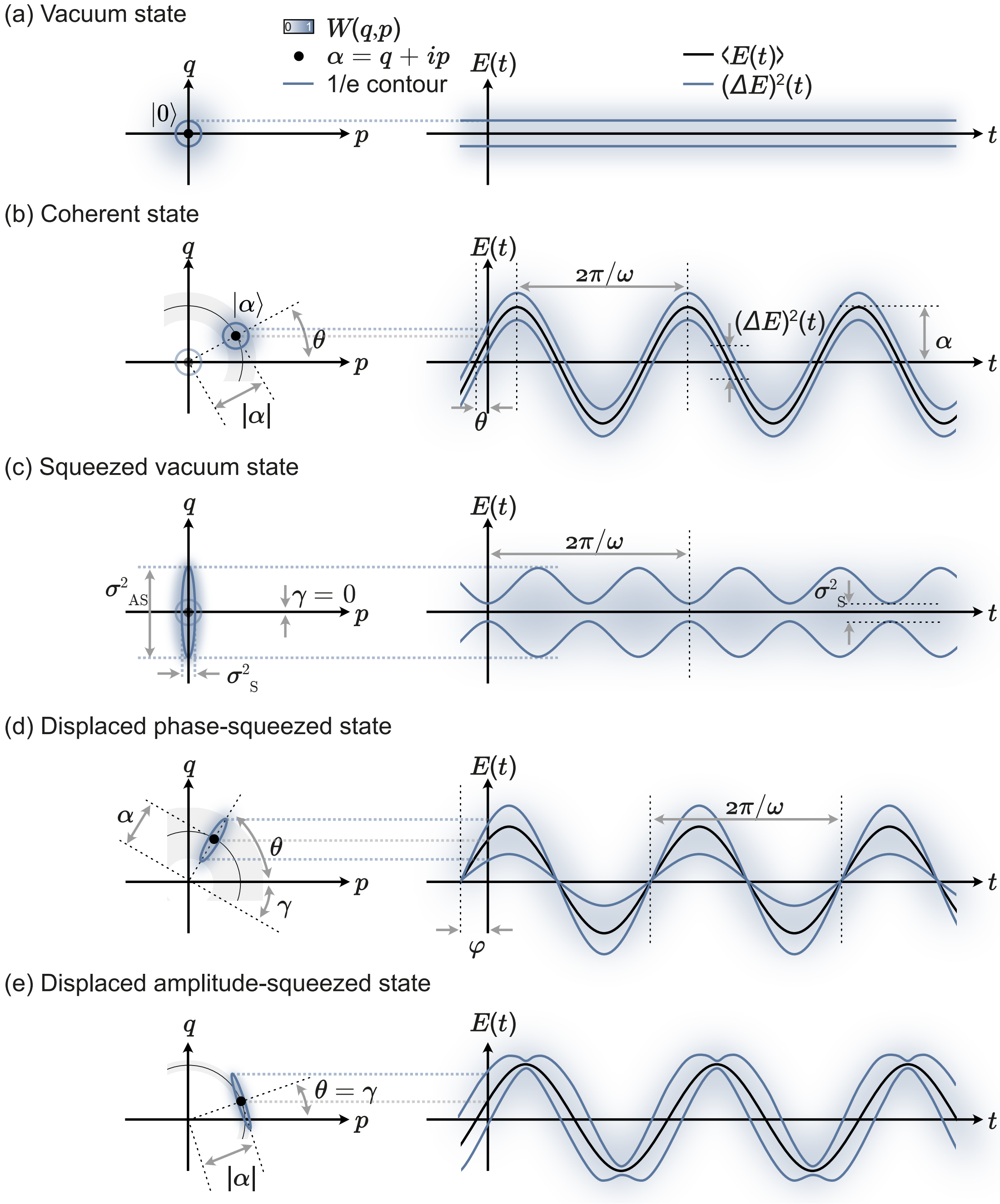

Figure 2.3: Wigner function $W(q,p)$ distributions of displaced and squeezed vacuum states in phase-space (left column) and its electric field $E(t)$ in the time domain (right column). (a) Vacuum state $|0\rangle$ with the minimal variance $1/4$ in p and q quadrature. (b) Coherent state $|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle$, where the displacement amplitude is $\alpha = |\alpha|e^{i\theta}$, with the displacement angle $\theta = 45°$. (c) Squeezed vacuum state $\hat{S}\,|0\rangle$ with squeezing angle $\gamma = 0°$. (d) Displaced squeezed state, with orthogonal squeezing angle and displacement angle $\gamma \perp \theta$. (e) Displaced squeezed state, where squeezing angle and displacement angle are parallel $\gamma \parallel \theta$.

The displacement operator is a Gaussian unitary operator. Since $\hat{D}^\dagger(\alpha) = \hat{D}(-\alpha) = \hat{D}(\alpha)^{-1}$, we note that the displacement operator is also unitary. The displacement operation is visualized in Fig. 2.2.

In quantum optics, the displacement operation is implemented using highly asymmetric (transmissivity $\tau \to 1$) beam splitters whose first (strongly coupled) input port $\hat{a}_{\mathrm{in}}$ is to be displaced and the second (weakly coupled) port is fed by a strong coherent state $\hat{b}_{\mathrm{coh}}$ [74]. The resulting bosonic output mode is [75]

$$\hat{a}_{\mathrm{out}} = \sqrt{\tau}\hat{a}_{\mathrm{in}} + \sqrt{1-\tau}\hat{b}_{\mathrm{coh}}. \tag{2.27}$$

By assuming that $\hat{b}_{\mathrm{coh}} \left|\tilde{\alpha}\right\rangle = \tilde{\alpha}\left|\alpha\right\rangle$, and in the limit $\tau \to 1$, the bosonic output mode of the directional coupler $\hat{a}_{\mathrm{out}}$ can be approximated as [74, 75]

$$\hat{a}_{\mathrm{out}} = \hat{a}_{\mathrm{in}} + \sqrt{1-\tau}\tilde{\alpha} = \hat{a}_{\mathrm{in}} + \alpha, \tag{2.28}$$

with $\alpha = \sqrt{1-\tau}\tilde{\alpha}$. In the microwave regime, the displacement operation can be efficiently implemented by using cryogenic directional couplers [46]. Here, the quantum nature of displaced states can be preserved even if the state is displaced by hundreds of photons [46].

Single-mode squeezing and squeezed vacuum states

The second important Gaussian operation is squeezing. It is defined by the action of a single-mode squeezing operator [52]

$$\hat{S}\left(\xi\right) = \exp\left(\frac{1}{2}\xi^*\hat{a}^2 - \frac{1}{2}\xi\left(\hat{a}^\dagger\right)^2\right), \tag{2.29}$$

where the complex squeezing parameter $\xi = re^{i\varphi}$ consists of the squeezing factor r and the squeezing phase, which describes the orientation in the phase space φ. The squeezing angle $\gamma = -\varphi/2$ is defined between the anti-squeezed quadrature and the p-axis (see Fig. 2.3 (d)). The squeezing factor r defines the squeezed ($\sigma_S^2 = e^{-2r}/4$) and anti-squeezed ($\sigma_A^2 = e^{2r}/4$) quadrature variances. Typically, we quantify using a squeezing level S and antisqueezing level A. Both quantities are usually measured in decibels

$$S = -10\log_{10}\left(\frac{\sigma_S^2}{0.25}\right) \qquad A = 10\log_{10}\left(\frac{\sigma_A^2}{0.25}\right), \tag{2.30}$$

where the variances are normalized to 0.25 corresponding to the vacuum state variance. Squeezed and anti-squeezed quadrature variances always have to balance the Heisenberg uncertainty relation such that $A - S \geq 0$. If the squeezed state is pure, $\mu = 1$, we expect $S = A = 20r\log_{10}\left(e\right)$. Squeezing can be also represented by the corresponding symplectic map with the symplectic matrix $\mathbf{S}$ and displacement vector $\mathbf{d}$

$$\mathbf{S}(\xi) = \begin{pmatrix} e^{-\xi} & 0 \\ 0 & e^{\xi} \end{pmatrix}, \quad \mathbf{d} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{2.31}$$

The corresponding transformation is given by

$$\begin{aligned} \hat{S}(\xi): \quad \hat{\mathbf{r}} &\mapsto \mathbf{S}(\xi)\hat{\mathbf{r}}, \\ \mathbf{V} &\mapsto \mathbf{S}(\xi)\mathbf{V}\mathbf{S}(\xi)^T. \end{aligned} \tag{2.32}$$

The operator transformation by the squeezing operator is given by the Bogoliubov transform [52]

$$\begin{aligned} \hat{S}^\dagger(\xi)\hat{a}\hat{S}(\xi) &= \hat{a}\cosh(r) - \hat{a}^\dagger e^{i\varphi}\sinh(r), \\ \hat{S}^\dagger(\xi)\hat{a}^\dagger\hat{S}(\xi) &= \hat{a}^\dagger\cosh(r) - \hat{a}e^{-i\varphi}\sinh(r). \end{aligned} \tag{2.33}$$

Respectively, we can compute the displacement and covariance matrices of a squeezed vacuum states to be [75]

$$\bar{\mathbf{r}}_{\text{sq}} = \mathbf{0} \quad \text{and} \quad \mathbf{V}_{\text{sq}} = \frac{1}{4}\begin{pmatrix} e^{-2r}\cos^2\frac{\varphi}{2} + e^{2r}\sin^2\frac{\varphi}{2} & \sin\varphi\left(e^{-2r} - e^{2r}\right)/2 \\ \sin\varphi\left(e^{-2r} - e^{2r}\right)/2 & e^{2r}\cos^2\frac{\varphi}{2} + e^{-2r}\sin^2\frac{\varphi}{2} \end{pmatrix}. \tag{2.34}$$

In our notation, positive values of S correspond to squeezing of vacuum fluctuations below the vacuum level. Experimentally, we generate squeezed microwave states with the help of Josephson parametric amplifiers. A summary of the Gaussian unitary operations that are discussed above, can be found in Fig. 2.3. In particular, the squeezing operation applied to the vacuum state (see Fig. 2.3 (a)) results in the squeezed vacuum state (see Fig. 2.3 (c)). Squeezing and displacement can also be applied consecutively as shown in Fig. 2.3 (d,e) for phase-squeezed and amplitude-squeezed states.

Two-mode squeezed vacuum states

Two-mode squeezed vacuum (TMSV) states are entangled states. They were used to realize the Einstein-Podolsky-Rosen (EPR) paradox [76] for continuous position and momentum observables [77]. A TMSV can be created by applying a two-mode squeezing operator to the vacuum state. The two-mode squeezing operator is defined as [52]

$$\hat{S}_{1,2} = \exp\left(\xi^*\hat{a}_1\hat{a}_2 - \xi\hat{a}_1^\dagger\hat{a}_2^\dagger\right), \tag{2.35}$$

where $\hat{a}_1$ ($\hat{a}_2$) is the annihilation operator of the 1st (2nd) mode. The complex squeezing parameter $\xi = re^{i\varphi}$ is defined by the squeezing factor r and phase φ. If we set the phase to

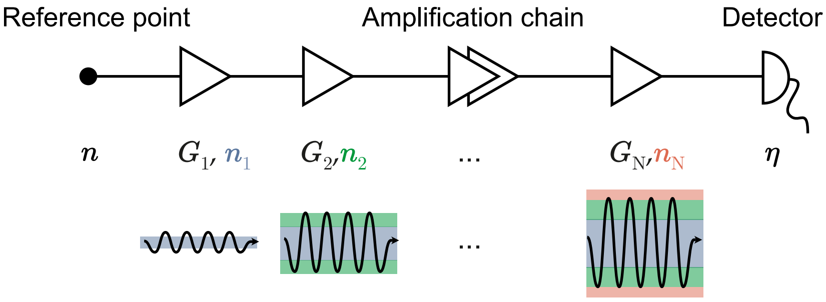

Figure 2.4: Scheme of noise in an amplification chain consisting of N amplifiers, $i = \{1, 2, 3, \ldots, N\}$, with noise number n_i referred to their input and gain G_i. The added noise by the first amplifier n_1 (blue) dominates the total photon noise number , n_{th}, as the noise gets amplified by the complete amplification chain. Even a high noise number of the last amplifier (red) weakly affects the output signal.

$\varphi = 0$, the mean $\bar{\mathbf{r}}_{\text{TMSV}}$ and covariance matrix $\mathbf{V}_{\text{TMSV}}$ are given as [53]

$$\bar{\mathbf{r}}_{\text{TMSV}} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \quad \mathbf{V}_{\text{TMSV}} = \frac{1}{4} \begin{pmatrix} \cosh(2r) & 0 & \sinh(2r) & 0 \\ 0 & \cosh(2r) & 0 & -\sinh(2r) \\ \sinh(2r) & 0 & \cosh(2r) & 0 \\ 0 & -\sinh(2r) & 0 & \cosh(2r) \end{pmatrix}. \tag{2.36}$$

We can express the quadrature variances as $\cosh(2r) = (1 + 2n_{\text{th}})$. Physically, it means that each mode looks locally like a thermal state with an average noise photon number n_{th} [49].

2.2 Phase-sensitive amplification of quantum microwaves

In this section, we want to discuss the limitations of different quadrature detection strategies for microwave signals. We introduce a quantum efficiency quantity and its limits for phase-insensitive and phase-sensitive amplification. At the end of the section, we show the working principle of a Josephson parametric amplifier, which is able to implement both amplification regimes in the microwave regime.

2.2.1 Quantum efficiency of quantum state tomography

At optical frequencies ($\sim 4000\,\text{THz}$), the high energy of single photons enables efficient single-photon detectors and optical homodyne detection [78]. In optics, the quantum efficiency is defined as the ratio of incident photons to converted electrons. Optical detectors can achieve high quantum efficiencies of $\eta \geq 90\%$ [79].

At microwave frequencies ($300\,\text{MHz} - 300\,\text{GHz}$), the realization of single-photon detectors is still an active research challenge [80, 81]. More often, researchers still rely on linear amplification chains for microwave state detection [82]. The quantum efficiency η of such an amplification chain can be defined as [83]

$$\eta = \frac{1}{1+2n}, \quad 0 < \eta < 1, \tag{2.37}$$

where n is the total added noise. The total noise for chained amplification (see Fig. 2.4) can be expressed by the Friis noise formula with the noise photon number referred to the input of the amplifiers, n_i, with the corresponding gain factors, G_i [84]

$$n = n_1 + \frac{n_2}{G_1} + \frac{n_3}{G_1 G_2} + \cdots + \frac{n_N}{\prod_{i=1}^{N-1} G_i}. \tag{2.38}$$

This equation demonstrates that the overall added noise is dominated by the noise level of the first amplifier in the limit of large amplifier gains, $G_i \gg 1$.

2.2.2 Parametric amplification

For cryogenic amplification in microwave circuits, there are two commonly used options: linear amplification with a HEMT, or parametric amplification with a Josephson parametric amplifier. HEMT amplifiers rely on field effect transistors, where a small input voltage induces a large output current due to an engineered high carrier mobility [85]. The source for the added 10-20 noise photons is the HEMT's non-vanishing phase-insensitive resistance in the direct current [86]. Instead of a phase-insensitive dc resistance, parametric amplifiers are characterized by their impedance. This impedance consists of resistance and a reactance, which can store energy and return it to the circuit after a quarter oscillation (as in an LC oscillator) [87]. Common mechanical analogues of parametric amplification are the periodic variation of the pendulum length, or the pumping of a swing [88] at twice the signal frequency ω_s.

We briefly motivate the effect of a frequency-doubled pump signal in an undamped toy model. A more detailed introduction into parametric amplification and driven oscillators can be found in Refs. 88, 89. Parametric amplification can be studied by variation of the intrinsic resonance frequency of an unperturbed harmonic oscillator. There, the resonance frequency ω_r is periodically modulated as $\omega_r \to \omega_r\,(1 + f(t)/2)$, with $f(t) = A\cos(2\omega_r t)$. The classical equation of motion for the response $q(t)$ is then [89]

$$\frac{d^2 q(t)}{dt^2} + \omega_r^2\,(1 + f(t))\,q(t) = 0. \tag{2.39}$$

Here, the A^2 term was neglected by assuming small pump amplitudes. We can write the system as a driven harmonic oscillator with a static resonance frequency and a response-modulated pumping signal $f(t)$ as driving force

$$\frac{d^2 q(t)}{dt^2} + \omega_r^2 q(t) = -\omega_r^2 f(t) q(t). \tag{2.40}$$

In general, a harmonic oscillator is driven in resonance for a $\pi/2$ phase-shifted signal at the resonance frequency. We assume an initial resonant oscillation $q(t) = \cos(\omega_r t)$ and apply a trigonometric identity on the right hand side of Eq. 2.40

$$\begin{aligned} f(t)q(t) &= A\sin(2\omega_r t)\cos(\omega_r t) \\ &= \frac{A}{2}\left[\sin(\omega_r t) + \sin(3\omega_r t)\right]. \end{aligned} \tag{2.41}$$

We see that the effective driving signal consist of an off-resonant (therefore attenuated) signal at $3\omega_r$ and a signal in resonance ω_r with the oscillator. As a result the amplitude of the oscillation increases exponentially. An analogue principle of signal pumping can be exploited for a corresponding quantum mechanical Hamiltonian

$$H = \hbar\omega_0 \left[\hat{a}^\dagger\hat{a} + \frac{1}{2} + A\cos(2\omega_r t)(\hat{a} + \hat{a}^\dagger)^2\right]. \tag{2.42}$$

By introducing a signal and loss port to the Hamiltonian, the equation of motion can be solved in a reference frame rotating with ω_r. The resulting output field is the expression for the output of Josephson parametric amplifiers, which we discuss in more detail in Sec. 2.2.5. There, parametric down-conversion splits a pump photon into two photons, called signal and idler, with frequencies $\omega_s = \omega_p/2 + \delta\omega$, and $\omega_i = \omega_p/2 + \delta\omega$. JPAs can be employed both for nondegenerate, $\omega_p \neq 2\omega_s$, and degenerate amplification, $\omega_p = 2\omega_s$ [90].

2.2.3 Nondegenerate amplification

In the following, we show that a nondegenerate (phase-insensitive) amplification adds at least half a noise photon to the signal, referred to the amplifier input. Respective limits of bosonic phase-preserving amplifiers were originally developed by Haus and Mullen (1962) [91] and later extended by Caves (1982) [92].

In this context, we should consider general limitations on input and output modes. Let $\hat{a}_{\text{in}}$ be the input and $\hat{a}_{\text{out}}$ the output modes of a bosonic amplifier. The Caves theorem states that the output modes commutation relation $\left[\hat{a}_{\text{out}}, \hat{a}_{\text{out}}^\dagger\right] = 1$ is only fulfilled if an additional idler mode $\hat{b}_{\text{in}}$ is added. A more detailed motivation is shown in the Appendix A.3. Then, the bosonic scattering relation for phase-preserving amplification is [44, 86]

$$\hat{a}_{\text{out}} = \underbrace{\sqrt{G}\hat{a}_{\text{in}}}_{\text{Amplification}} + \underbrace{\sqrt{G-1}\hat{b}_{\text{in}}^\dagger}_{\text{Added idler noise}}. \tag{2.43}$$

Therefore, any bosonic amplifier input-output relation is composed of at least two different signals: the signal and idler mode. When considering the lower bound for noise in the output mode [86], one can retrieve the fundamental theorem for phase-insensitive linear

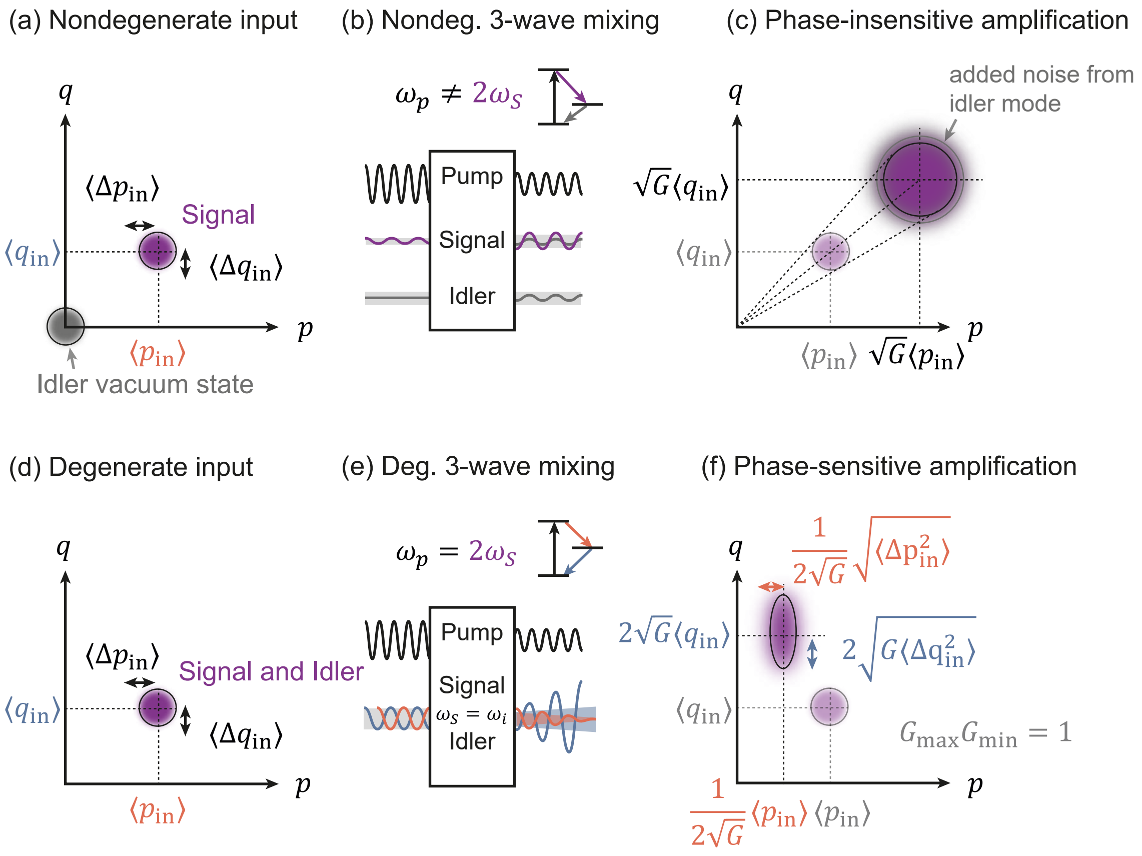
(a) Nondegenerate input
(b) Nondeg. 3-wave mixing
(c) Phase-insensitive amplification
q
$\langle \Delta p_{\mathrm{in}} \rangle$
Signal
$\langle q_{\mathrm{in}} \rangle$
$\langle \Delta q_{\mathrm{in}} \rangle$
p
$\langle p_{\mathrm{in}} \rangle$
Idler vacuum state
$\omega_p \neq 2\omega_S$
Pump
Signal
Idler
added noise from
idler mode
$\sqrt{G}\langle q_{\mathrm{in}} \rangle$
$\langle p_{\mathrm{in}} \rangle$ $\sqrt{G}\langle p_{\mathrm{in}} \rangle$
(d) Degenerate input
(e) Deg. 3-wave mixing
(f) Phase-sensitive amplification
Signal and Idler
$\omega_p = 2\omega_S$
$\omega_S = \omega_i$
$\frac{1}{2\sqrt{G}}\sqrt{\langle \Delta p_{\mathrm{in}}^2 \rangle}$
$2\sqrt{G}\langle q_{\mathrm{in}} \rangle$
$2\sqrt{G\langle \Delta q_{\mathrm{in}}^2 \rangle}$
$G_{\mathrm{max}}G_{\mathrm{min}} = 1$
$\frac{1}{2\sqrt{G}}\langle p_{\mathrm{in}} \rangle$ $\langle p_{\mathrm{in}} \rangle$

Figure 2.5: Schematic of 3-wave mixing during degenerate and nondegenerate amplification of a (a) coherent input state with the respective noise represented by the radii of the circles along the real and imaginary axes. Idler mode (grey) at idler frequency $\omega_i \neq \omega_s$. (b) Schematic representation of nondegenerate 3-wave mixing. (c) For phase-preserving amplification both quadratures are amplified with the gain $\sqrt{G}$, while (for a perfect vacuum state in the idler mode) half a photon of noise is added to the input distribution (grey halo in the output state). (d) Coherent input state with the idler and signal mode at the same frequency $\omega_i = \omega_s$. (e) Schematic representation of degenerate ($f_{\mathrm{pump}} = 2f_{\mathrm{signal}}$) 3-wave mixing. (f) During phase-sensitive amplification, noise along one quadrature is suppressed and added on the conjugate one according to the amplifier uncertainty principle.

amplifiers as formulated by Caves [92]

$$n \geq \frac{1}{2}\left|1 - \frac{1}{G}\right|, \tag{2.44}$$

where G is the amplifier's photon number gain, and n the average number of added noise photons. Even in the limit of $G \to \infty$, the added noise is at least half a photon $\hbar\omega/2$ (visualized in Fig. 2.5 (c)). If we consider half a noise photon for the definition of the quantum efficiency (see Eq. 2.37), this limit results in the standard quantum limit (SQL) of $\eta = 1/(1+2n) = 50\%$. State-of-the-art low-noise microwave amplifiers fall far behind this limit. Typical high-electron mobility transistor (HEMT) amplifiers add 10-20 noise photons to the signal [86].

2.2.4 Degenerate amplification

In contrast to the phase-insensitive amplification, phase-sensitive amplification can be ideally noiseless. Therefore, it is highly beneficial to use it at the very first stage of an amplification chain. In the following, we discuss added noise during the phase-sensitive amplification process, which can be realized by a 3-wave mixing process in nonlinear resonators.

In particular, we can tune the pump frequency to twice the signal frequency, $\omega_p = 2\omega_s$, so that the photon energy conservation yields the degenerate frequencies for signal and idler modes, $\omega_s = \omega_i$. Therefore, we can identify the idler mode as a phase-shifted signal mode $\hat{b}^\dagger_{\text{in}} = e^{-i\phi}\hat{a}^\dagger_{\text{in}}$ in the relation Eq. 2.45. Here, $\phi \in [0, 2\pi]$ is related to the phase shift between the two degenerate quadratures of the input and idler modes. As a result, these modes can interfere constructively and destructively, depending on their relative phase. Then, the input-output relation for phase-sensitive amplification is [44]

$$\hat{a}_{\text{out}} = \underbrace{\sqrt{G}\hat{a}_{\text{in}}}_{\text{Amplification}} + \underbrace{e^{-i\phi}\sqrt{G-1}\hat{a}^\dagger_{\text{in}}}_{\text{Phase dep. noise}}. \tag{2.45}$$

The striking result is that the uncertainty in one quadrature can be suppressed below the vacuum level without violating Heisenberg's uncertainty relation. This process is known as single-mode squeezing and was first observed experimentally by Yurke *et al.* [90]. Considering the lower bounds for the noise in the quadratures, we can see that a reduction of noises added to one quadrature phase requires an increase in noise added on the other phase. This relation was coined as the amplifier uncertainty principle [92]

$$n_{\text{q}} n_{\text{p}} \geq \frac{1}{16}\left|1 - \frac{1}{\sqrt{G_{\text{q}} G_{\text{p}}}}\right|^2, \tag{2.46}$$

where G_{q}, G_{p} are the individual gains and n_q, n_p are the noise numbers for conjugate quadratures. In the case $G_{\text{q}} = G_{\text{p}}$, this equation reduces to the fundamental theorem for phase-insensitive linear amplifiers (see Eq. 2.44). In the case $G_{\text{q}} G_{\text{p}} = 1$, noise numbers can be zero which corresponds to the maximum quantum efficiency of $\eta = 100\%$.

2.2.5 Josephson parametric amplifiers (JPA)

In this work, the squeezing operation (see Sec. 3.3.2) and phase-sensitive amplification (see Sec. 2.2.4) are performed using flux-driven Josephson parametric amplifiers [50]. Josephson parametric amplifiers (JPAs) can be employed in a number of different applications, such as qubit readout [93–95] or quantum communication [82, 96, 97]. A flux-driven JPA consists of three parts: a superconducting microwave resonator, a pump antenna, and a tunable direct-current superconducting quantum interference device (dc-SQUID). The superconducting microwave resonator is short-circuited by the dc-SQUID to ground. The JPA resonant frequency can be tuned by applying an external magnetic flux through the dc-SQUID. The pump antenna can also induce a high frequency magnetic flux through the dc-SQUID which induces parametric amplification in the JPA. The inductance of the dc-SQUID loop depends on the flux-dependent current across two parallel Josephson junctions.

In the following, we present a basic physical description of the Josephson effect and corresponding dc-SQUID behavior. Then, we analyze the JPA structure using an equivalent circuit. We discuss how interaction between signals incident to the JPA and the pump tone may result in the 3-wave mixing process which gives rise to various amplification regimes.

Josephson equations and nonlinear inductance

A superconductor is characterized by its perfect diamagnetism [98] and resulting perfect conductivity. These properties are typically observed below a certain critical temperature, T_C. Most of the superconducting circuits used in this work are made from superconducting materials, such as niobium ($T_C \simeq 9.2\,\mathrm{K}$), niobium-titanium alloy ($T_C \simeq 10\,\mathrm{K}$) [99], or aluminum ($T_C = 1.2\,\mathrm{K}$) [100]. In these materials, microwave losses are greatly reduced in comparison with normal metals. This low-loss microwave environment is one of the keys for preserving the fragile nature of quantum signals.

Another advantage of using superconducting circuits is the Josephson effect [101], which appears when two superconductors are weakly coupled to another. Figure 2.6 (a) shows a schematic of a Josephson junction, where two macroscopic wave functions $\Psi_\mathrm{k}(\mathbf{r},t) = \sqrt{n_\mathrm{k}(\boldsymbol{r},t)}e^{i\theta_\mathrm{k}(\mathbf{r},t)}$ of two superconductors $k = 1, 2$ overlap in a thin layer of non-superconducting material (insulator). Here, the density of superconducting Cooper pairs is given by $n_\mathrm{k}(\mathbf{r},t)$, and the phase of the macroscopic wave function is denoted by $\theta_k(\boldsymbol{r},t)$.

The gauge-invariant phase difference of the macroscopic wave function across the Josephson junction is given by [102]

$$\varphi(\boldsymbol{r},t) = \theta_2(\boldsymbol{r},t) - \theta_1(\boldsymbol{r},t) - \frac{2\pi}{\Phi_0}\int_1^2 \boldsymbol{A}(\boldsymbol{r},t)\cdot \mathrm{d}\boldsymbol{l}, \tag{2.47}$$

where $\Phi_0 = h/2e$ is the magnetic flux quantum and $\boldsymbol{A}$ is the vector potential. The integral path crosses the tunnel barrier from superconductor 1 to superconductor 2.

When we neglect spatial variations of the Cooper pairs, we can characterize the current across the junction by the lumped Josephson equations. The first Josephson equation (current-phase relation) [102]

$$I_\mathrm{s}(\varphi) = I_\mathrm{c}\sin(\varphi) \tag{2.48}$$

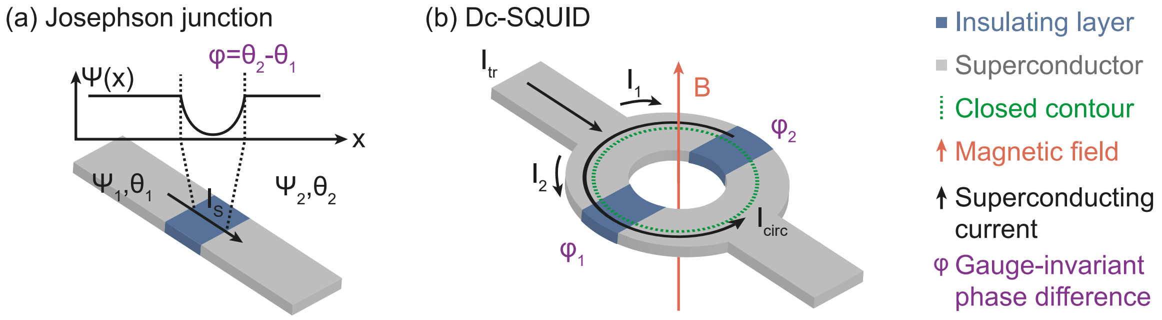

Figure 2.6: (a) Schematic of a Josephson junction with superconductors in gray and an insulating layer in blue. (b) Schematic of the dc-SQUID with one Josephson junction in each arm of the superconducting loop. Each Josephson junction is associated with the phase differences φ_1, φ_2.

describes the dependence of the supercurrent I_s on the gauge invariant phase difference ϕ and the critical current I_c. The second Josephson equation (voltage-phase relation) [102]

$$\frac{\partial \varphi}{\partial t} = \frac{2\pi}{\Phi_0} V\left(t\right), \tag{2.49}$$

describes the time evolution of the phase difference ϕ when a voltage V is applied across the Josephson junction. In presence of a constant voltage, the time-dependent phase leads to a sinusoidal supercurrent according to Eq. 2.48.

The process of parametric amplification relies on the nonlinear inductance of the Josephson junctions. This can be seen by using the conventional definition of inductance, $V = L\,dI/dt$, in combination with Eq. 2.48 in order to obtain the equation for a nonlinear Josephson inductance

$$L_\mathrm{s} = \frac{\Phi_0}{(2\pi I_\mathrm{c})}\frac{1}{\cos\left(\varphi\right)} = L_\mathrm{c}\frac{1}{\cos\left(\varphi\right)}, \tag{2.50}$$

where L_c is the minimal Josephson junction inductance. This nonlinearity is exploited to engineer the energy potential in many different superconducting circuits and is also the key component for the development of superconducting qubits [103].

Flux-dependent inductance of a dc-SQUID

A dc-SQUID consists of two Josephson junctions with critical currents I_c in a superconducting loop as shown in Fig. 2.6 (b). For simplicity, we assume that the critical currents of the Josephson junctions are identical, which is not a necessary condition. The external magnetic field **B** induces a magnetic flux Φ_ext through the dc-SQUID loop.

Here, the effect on the gauge invariant phase difference can be understood when we consider that the total phase change over a closed contour C around the dc-SQUID (green dotted line) is quantized, $\oint_C \nabla\theta \cdot \mathrm{d}r = 2\pi n$ with $n \in \mathbb{N}_0$. This is a direct result of underlying nature of the macroscopic wave function of superconducting electrons. The phase gradient $\nabla\theta$ can be expressed in terms of the supercurrent density $\boldsymbol{J}_s$, and the vector potential $\boldsymbol{A}$ as

[102]

$$\nabla\theta = \frac{2\pi}{\Phi_0}\left(\Lambda \boldsymbol{J}_s + \boldsymbol{A}\right), \tag{2.51}$$

where Λ is the London parameter. The evaluation of the phase difference in a closed contour becomes easier when we choose an integration path deep inside the superconductor, where the supercurrent density $\boldsymbol{J}_s$ is close to zero. Then we can neglect the supercurrent and obtain the condition for the phase differences φ_1 and φ_2

$$\varphi_2 - \varphi_1 = \frac{2\pi\Phi}{\Phi_0} + 2\pi n. \tag{2.52}$$

This result links the phase differences to the total magnetic flux Φ through the dc-SQUID loop. The total magnetic flux consists of the externally applied flux Φ_{ext} and a self-induced flux, $\Phi_{\mathrm{loop}} = L_{\mathrm{loop}} I_{\mathrm{circ}}$, where $I_{\mathrm{circ}} = (I_1 - I_2)/2$ is the circulating supercurrent, and L_{loop} the self-inductance of the superconducting loop. We can rewrite the supercurrent I_{cir} with the help of Eq. 2.52 so that the total flux through the dc-SQUID loop Φ is

$$\begin{aligned}\frac{\Phi}{\Phi_0} &= \frac{\Phi_{\mathrm{ext}}}{\Phi_0} + \frac{L_{\mathrm{loop}} I_{\mathrm{cir}}}{\Phi_0} \\ &= \frac{\Phi_{\mathrm{ext}}}{\Phi_0} - \frac{\beta_L}{2}\cos\left(\frac{\varphi_1+\varphi_2}{2}\right)\sin\left(\frac{\varphi_1-\varphi_2}{2}\right),\end{aligned} \tag{2.53}$$

where the magnitude of the screening parameter $\beta_{\mathrm{L}} = 2L_{\mathrm{loop}}I_{\mathrm{c}}/\Phi_0$ [104] is indicating whether the screening effect is negligible ($\beta_{\mathrm{L}} \approx 0$) or whether the self-induced flux can no longer be neglected ($\beta_{\mathrm{L}} > 1$).

If we can neglect the screening effect ($\beta_{\mathrm{L}} \approx 0$), the dc-SQUID can be treated as a single Josephson junction, where the total flux approximately coincides with the external one, $\Phi \approx \Phi_{\mathrm{ext}}$, and modulates the maximal supercurrent $I_{\mathrm{S}}^{\max}$ as [105]

$$I_{\mathrm{S}}^{\max}(\Phi_{\mathrm{ext}}) = 2I_{\mathrm{c}}\left|\cos\left(\pi\frac{\Phi_{\mathrm{ext}}}{\Phi_0}\right)\right|. \tag{2.54}$$

Then, the nonlinear flux-dependent inductance of the dc-SQUID can be reduced to the inductance of the Josephson junction (analogous to Eq. 2.50) [106]

$$L_s\left(\Phi_{\mathrm{ext}}\right) = \frac{\Phi_0}{4\pi I_c\left|\cos\left(\pi\frac{\Phi_{\mathrm{ext}}}{\Phi_0}\right)\right|}. \tag{2.55}$$

If we cannot neglect the screening effect ($\beta_L > 1$), we need to find a self-consistent solution to Eq. 2.53. However, it is not possible to find an analytical solution in general. For a numerical analysis, the reader is referred to Ref. 75.

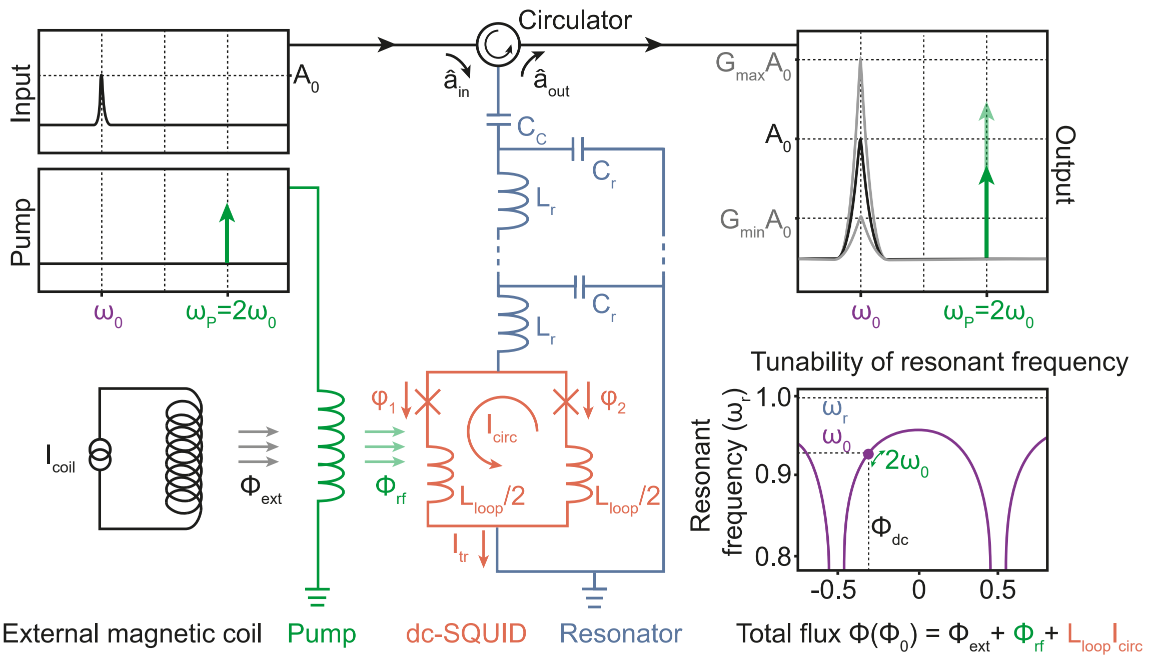

Figure 2.7: Circuit schematic and pump scheme for phase-sensitive amplification with a Josephson parametric amplifier. The device consists of a quarter-wavelength CPW resonator (blue), shorted to ground with a dc-SQUID (red). The pump antenna (green) induces the high frequency flux oscillations Φ_{rf} in the dc-SQUID around a static point determined by Φ_{dc}. The flux pump frequency is chosen $\omega_p = 2\omega_s$ to enable the 3-wave mixing process and parametric amplification.

Tunable resonance frequency of a Josephson parametric amplifier

The JPA circuit schematic is shown in Fig. 2.7. Here, the resonator (blue in Fig. 2.7) is made from a coplanar waveguide (CPW), which can be treated as a quasi one-dimensional transmission line [84]. The wave propagation in the CPW is described by the telegrapher's equation, which relies on the use of a distributed inductance L_0 and capacitance C_0 per unit length [84]. Since the CPW is made from a superconducting material, we assume the characteristic impedance for a lossless transmission line

$$Z = \sqrt{\frac{L_0}{C_0}}. \tag{2.56}$$

The CPW can be used as a quarter-wavelength resonator by introducing appropriate boundary conditions. The CPW resonator (blue) in Fig. 2.7 is coupled to the signal line via the coupling capacitance C_c on one end, while the other end is shorted to ground via the dc-SQUID. The total resonator inductance and capacitance, $L_r = d\,L_0$, and $C_r = d\,C_0$, are defined by the electric length d of the CPW. The resonant frequency ω_r corresponding to the quarter wavelength resonance is given by [89, 107]

$$\omega_r = \frac{2\pi}{4d\sqrt{L_0 C_0}} = \frac{2\pi}{4\sqrt{L_r C_r}}. \tag{2.57}$$

Resonators are typically characterized by their internal and external coupling strengths. Typically, resonator designs aim at a low internal loss rate κ_{int}. However, two-level fluctuations [108], surface resistance [109], and eddy currents [110] always lead to finite loss contributions even when using superconducting materials. The $\lambda/4$ resonator can be characterized by probing it with a external microwave tone and, then, measuring the frequency-dependent reflection coefficient Γ [89]

$$\Gamma = \frac{(\omega - \omega_0)^2 + i\kappa_{\text{int}}(\omega - \omega_0) + (\kappa_{\text{ext}}^2 - \kappa_{\text{int}}^2)/4}{((\omega - \omega_0) + i(\kappa_{\text{ext}} + \kappa_{\text{int}})/2)^2}, \tag{2.58}$$

where ω_0 is the resonant frequency and κ_{int} and κ_{ext} are internal and external loss rates, respectively. The internal quality factor is defined as $Q_{\text{int}} = \omega_0/\kappa_{\text{int}}$ and the external quality factor is $Q_{\text{ext}} = \omega_0/\kappa_{\text{ext}}$ [75].

The resonant frequency in Eq. 2.57 depends on the inductance of the resonator L_r. In order to correctly estimate the JPA total inductance, we take into account the effect of the dc-SQUID: the resonant frequency of the resonator-SQUID system ω_0 depends also on the nonlinear inductance of the dc-SQUID, which in turn depends on the external flux [111–113]

$$\left(\frac{\pi\omega_0}{2\omega_r}\right)\tan\left(\frac{\pi\omega_0}{2\omega_r}\right) = 2\frac{(2\pi)^2}{\Phi_0^2}L_r E_{\text{s}}\left(\Phi_{\text{ext}}\right) - \frac{2C_{\text{s}}}{C_r}\left(\frac{\pi\omega_0}{2\omega_r}\right)^2, \tag{2.59}$$

where L_r, C_r and ω_r are the total inductance, capacitance, and flux-dependent resonance frequency of the JPA. Additionally, C_{s} corresponds to the capacitance of a single Josephson junction, and ω_r to the resonant frequency of the bare resonator. Here, $E_{\text{s}}\left(\Phi_{\text{ext}}\right)$ represents the flux-dependent energy of the dc-SQUID [75]

$$E_{\text{s}}(\Phi_{\text{ext}}) = \frac{\Phi_0^2}{(2\pi)^2}\frac{1}{L_s(\Phi_{\text{ext}} + L_{\text{loop}}/4)} \tag{2.60}$$

We see from Eq. 2.59 that the resonance frequency ω_0 has two limits that depend on the energy of the dc-SQUID. For zero dc-SQUID energy E_s, the circuit is equivalent to an open transmission line as $\omega_0 \to 0$. For an infinite dc-SQUID energy, $\omega_0 \to \omega_r$ we obtain the $\lambda/4$-resonator [49].

Squeezing and parametric amplification with flux-driven JPAs

In the flux-driven JPAs used in this work [50], the pump tone induces an additional alternating flux Φ_{rf} through the dc-SQUID loop, which drives the parametric amplification. The amplification gain depends on the power of the pump signal.

In the interaction picture, the Hamiltonian of a flux-driven JPA $\hat{H}_{\text{int}}$ corresponds to the squeezing operator (see Appendix A in Ref. 75). The corresponding unitary evolution

$\hat{U} = \exp\left(-\frac{i}{\hbar}\hat{H}_{\text{int}}t\right)$ of the intraresonator JPA field is given by [53]

$$\hat{U}(t) = \exp\left(\frac{1}{2}\xi^{*}\hat{a}^{2} - \frac{1}{2}\xi\left(\hat{a}^{\dagger}\right)^{2}\right), \tag{2.61}$$

where $\xi = re^{i\varphi}$.

The phase-sensitive amplification gain G_{deg} of the degenerate JPA can be computed using the input-output formalism developed by Yamamoto *et al.* [89]

$$G_{\text{deg}}(\theta) = \frac{\left(\frac{\kappa_{\text{ext}}^{2}-\kappa_{\text{int}}^{2}}{4} - 4\delta^{2}\omega_{0}^{2}\right)^{2} + 4\delta^{2}\kappa_{\text{ext}}^{2}\omega_{0}^{2} - 4\delta\kappa_{\text{ext}}\omega_{0}\left(\frac{\kappa_{\text{ext}}^{2}-\kappa_{\text{int}}^{2}}{4} - 4\delta^{2}\omega_{0}^{2}\right)\sin(2\theta)}{\left(\frac{(\kappa_{\text{ext}}+\kappa_{\text{int}})^{2}}{4} - 4\delta^{2}\omega_{0}^{2}\right)^{2}}, \tag{2.62}$$

where 2θ is the relative phase of the signal mode, δ is the pump tone amplitude, and ω_0 is the resonance angular frequency. The internal loss rate $\kappa_{\text{int}} = \omega_0/Q_{\text{int}}$ and external loss rate $\kappa_{\text{ext}} = \omega_0/Q_{\text{ext}}$ are linked to the internal and external quality factors. For an overcoupled JPA ($\kappa_{\text{ext}} > \kappa_{\text{int}}$), we can compute the minimal and maximal gains $G_{\text{deg}}^{\text{min}}$, $G_{\text{deg}}^{\text{max}}$, which describe the amplification and de-amplification of the signal quadratures as follows [89]

$$\begin{aligned} G_{\text{deg}}^{\text{min}} &= \left(\frac{2\delta\omega_0 - (\kappa_{\text{ext}} - \kappa_{\text{int}})/2}{2\delta\omega_0 + (\kappa_{\text{ext}} + \kappa_{\text{int}})/2}\right)^{2}, \quad \text{for } \theta \equiv \frac{\pi}{4} \,(\text{mod}\,\pi), \\ G_{\text{deg}}^{\text{max}} &= \left(\frac{2\delta\omega_0 + (\kappa_{\text{ext}} - \kappa_{\text{int}})/2}{2\delta\omega_0 - (\kappa_{\text{ext}} + \kappa_{\text{int}})/2}\right)^{2}, \quad \text{for } \theta \equiv \frac{3\pi}{4} \,(\text{mod}\,\pi). \end{aligned} \tag{2.63}$$

Since noiseless phase-sensitive amplification is only possible when $G_{\text{deg}}^{\text{min}}G_{\text{deg}}^{\text{max}} = 1$, we can can notice from Eq. 2.63 that this is only possible when $\kappa_{\text{int}} = 0$. Another limitation to the noiseless phase-sensitive amplification might be that the to-be-squeezed input state is not a perfect vacuum state, but rather a thermal state with a finite thermal photon number due to finite environment temperatures. As a result, the purity of the produced squeezed vacuum state decreases below unity, $\mu < 1$. Furthermore, additional noise is introduced via other loss channels, such as the pump line. These pump photon uncertainties may lead to an effective noise contribution to the total JPA noise.

2.3 Continuous-variable quantum key distribution (CV-QKD) protocol

In this section, we describe continuous-variable quantum key distribution (CV-QKD) protocols. We define measures which can be used to estimate the performance of communication protocols. The communication parties are the sender Alice, the receiver Bob, and the eavesdropper Eve. Throughout this work, Alice, Bob, and Eve serve as metasyntactic variables for the sending, receiving and eavesdropping parties. This choice is a convenient standard in the field of cryptography and was first used in Ref. 15.

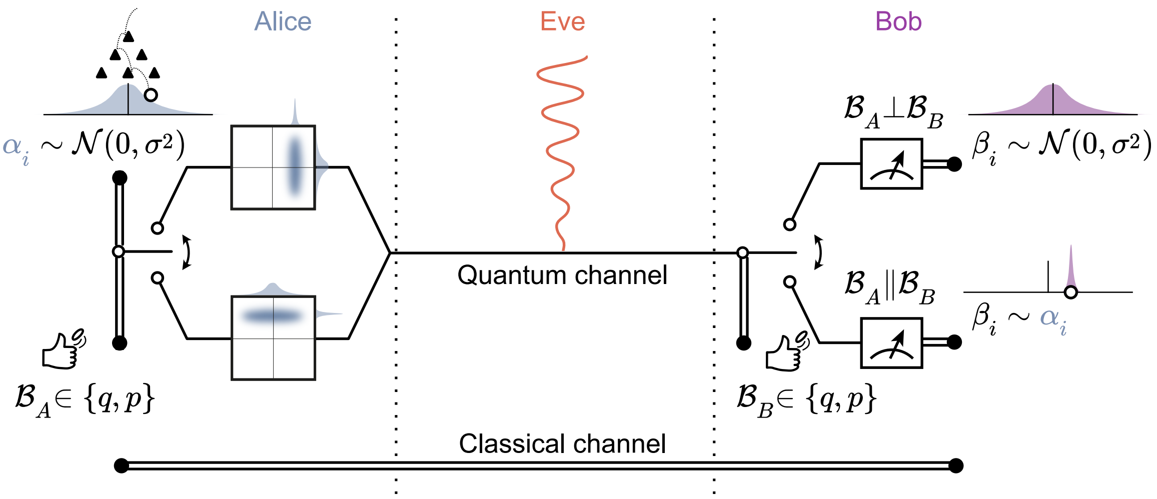
Alice
Eve
Bob
$\alpha_i \sim \mathcal{N}(0,\sigma^2)$
$\mathcal{B}_A \in \{q,p\}$
Quantum channel
Classical channel
$\mathcal{B}_A \perp \mathcal{B}_B$
$\beta_i \sim \mathcal{N}(0,\sigma^2)$
$\mathcal{B}_A \| \mathcal{B}_B$
$\beta_i \sim \alpha_i$
$\mathcal{B}_B \in \{q,p\}$

Figure 2.8: Scheme of a general Gaussian CV-QKD protocol. The sender Alice draws a random number α_i, a symbol, from a Gaussian distribution $\mathcal{N}(0,\sigma^2)$. After choosing a random basis $\mathcal{B}_\mathrm{A}$, she encodes the symbol into the corresponding expectation value $\langle q\rangle$, or $\langle p\rangle$ of a Wigner function, which is first squeezed and then displaced by the symbol magnitude $\hat{D}(\alpha_i)$. Then, the eavesdropper Eve performs an attack on the quantum channel. The receiver Bob chooses a random measurement basis $\mathcal{B}_B$ to perform a measurement of a state arrived through the quantum channel. Alice and Bob agree on two orthogonal bases. Depending on whether his basis was identical to Alice's ($\mathcal{B}_A \parallel \mathcal{B}_B$) or orthogonal ($\mathcal{B}_A \perp \mathcal{B}_B$), he obtains either a low-noise estimation of the true key $\beta_i \sim \alpha_i$, or a random value $\beta_i \sim \mathcal{N}(0,\sigma^2)$, which is uncorrelated to the initial symbol.

2.3.1 General aspects of a squeezed-state CV-QKD protocol

CV-QKD protocols exist in a number of different flavors. They can differ by the type of quantum state that carries information (coherent states, squeezed states), the classical encoding map (continuous Gaussian modulation, discrete alphabet), and the measurement type (homodyne or heterodyne detection) [114]. In the following, we focus on the protocol proposed by Cerf *et al.* [1]. We denote the elements of a shared key as symbols. In this implementation, the symbols are encoded in the displacement amplitude α of Gaussian-modulated squeezed states.

The CV-QKD protocol consists of two main steps: quantum communication and classical post-processing. First, the sender (Alice) encodes random classical variables α_i in the displacement amplitude of Gaussian quantum states. These variables α_i are sampled from a zero-mean Gaussian distribution (see Sec. 2.3.3). The states are encoded equiprobably in q- or p-displacement amplitudes with vacuum squeezing along q or p quadratures, respectively. Then, Alice sends the newly obtained displaced squeezed states over a quantum channel, characterized by its transmissivity τ and added thermal noise $\bar{n}$. This quantum channel is controlled by an eavesdropper (Eve) who tries to listen in on the message sent by Alice to Bob. The encoded information is protected by the no-cloning theorem [29–31]. However, Eve can get information by interfering with the channel (see Sec. 2.3.5 or imperfect cloners in Ref. 115). At the output of the quantum channel, the receiver (Bob) obtains a corresponding random classical variable β_i by using a projective measurement on a received state. After transmitting the complete key, either Alice communicates her measurement bases $\mathcal{B} \in \{q, p\}$ over a generally insecure classical channel to Bob (direct reconciliation) or vice versa (reverse reconciliation). They keep the symbols that were sent and measured in the identical bases, $\mathcal{B}_\mathrm{A} = \mathcal{B}_\mathrm{B}$. This process is called sifting. Classical post-processing consists of two steps: reconciliation of the key, and privacy amplification. During the reconciliation step, the correlated set of variables is distilled to an error-corrected shared set of identical variables. During the privacy amplification, Alice and Bob eliminate the threat imposed by stolen information by Eve. Any interaction by Eve with the quantum states induces a detectable disturbance on the quantum channel. The remaining shared variables represent the secret key k_i. This secret key can be used to encode one-time pad ciphertext over a classical channel.

The security of the CV-QKD protocol depends on the condition whether the shared information between Alice and Bob is larger than the information content obtained by the eavesdropper Eve. This information game can be summarized by a mathematical condition for information-theoretic quantities. The protocol is secure if and only if the secret key is positive, $K \geq 0$ (bits/channel use). The secret key is defined as

$$K = \eta_\mathrm{rec} I(\alpha{:}\beta) - \chi_\mathrm{E}, \tag{2.64}$$

where $\eta_\mathrm{rec} \in (0, 1)$ is the reconciliation efficiency (see classical post-processing in Sec. 2.3.6), $I(\alpha{:}\beta)$ is the mutual information shared between the sifted variables α_i and β_i (see Sec. 2.3.4), and χ_E is Eve's Holevo information (see Sec. 2.3.5) on Alice or Bob's secret key. This definition of the secret key is an upper bound for the asymptotic secret key under the requirement for strict unconditional security.

2.3.2 Units of classical and quantum information

Now, we need to mathematically quantify the amount of information that is stored in a continuous variable. In order to do so, we begin with the definition of entropy in the framework of classical information theory. A related quantity is the Shannon entropy [11]. The Shannon entropy is defined for discrete variables, whereas the differential entropy is used for continuous variables. Later, we present the von Neumann entropy as a measure of information in quantum states. Finally, we discuss how to calculate this entropy from the covariance matrix of a Gaussian state.

Differential Shannon entropy

We start with the definition of Shannon entropy H of a discrete random variable X with the possible outcomes $\{x_1, \ldots, x_\mathrm{N}\}$ in a system of size N. The probability of each variable

X being x_{i} is given by p_{i}. The Shannon entropy is defined as [11]

$$H\left(X\right) = -\sum_{i}^{N} p_{\mathrm{i}} \log_{\mathrm{b}}\left(p_{\mathrm{i}}\right), \tag{2.65}$$

where the choice for base b depends on the computational units. Common computational units are bits ($b = 2$) and nats ($b = e$). Initially, the measure was developed to quantify the compression limit for information communication over an arbitrary channel in Shannon's source coding theorem [11].

Shannon tried to extend the concept to continuous variables and assumed that the equivalent differential entropy for a continuous random variable X with probability density function f can be defined as

$$h\left(X\right) = -\int_{\mathcal{D}} f\left(x\right) \log_{\mathrm{b}}\left(f\left(x\right)\right) \mathrm{d}x, \tag{2.66}$$

where $\mathcal{D}$ is the domain of definition of f. However, it has not the same properties as the discrete variable version, as it is not strictly positive, and not invariant under a change of variables. In particular, one can show that the variable change $Y = aX$ leads to an additional constant [116]

$$h\left(Y\right) = h\left(X\right) + \log_{\mathrm{b}}|N|. \tag{2.67}$$

Lastly, in the limit of $N \to +\infty$ variables an additional term of $\log(N)$ appears which is infinitely large. This limit does not coincide with the differential entropy [117]. While a mathematically more advanced measure developed by Jaynes (1968) can recover the validity of these conditions [116], a relative difference between Shannon's differential entropies is still a valid measure where these previously mentioned limitations are irrelevant.

Von Neumann entropy

The entropy of an arbitrary quantum state with density matrix $\hat{\rho}$ is defined by the von Neumann entropy S [118]

$$S\left(\hat{\rho}\right) = -\mathrm{Tr}\left(\hat{\rho}\log\left(\hat{\rho}\right)\right), \tag{2.68}$$

where $\log$ is the natural matrix logarithm. This quantity can be rewritten with respect to its eigenvalues λ_{i} as

$$S\left(\hat{\rho}\right) = -\sum_{\mathrm{i}} \lambda_{\mathrm{i}} \log_{\mathrm{b}}\left(\lambda_{\mathrm{i}}\right), \tag{2.69}$$

where n represents a variable choice of the logarithm base. We note a similarity with the Shannon entropy, where we had in probabilities p_i in the place of eigenvalues λ_i. The von Neumann entropy is minimal ($S(\hat{\rho}) = 0$) if the state is pure, and maximal ($S(\hat{\rho}) = \log n$) for a maximally mixed state $\hat{\rho} = \mathbb{I}/n$ [119, 120].

In this thesis, we are mostly interested in Gaussian states which can be described with the covariance matrix formalism. Therefore, we should compute the von Neumann entropy from the covariance matrix $\mathbf{V}$. For a single-mode Gaussian states ($N = 1$), one obtains [64]

$$S\left(\hat{\rho}\right) = g\left(\sqrt{\det \mathbf{V}}\right), \tag{2.70}$$

where

$$g\left(x\right) = \left(2x + \frac{1}{2}\right)\log\left(2x + \frac{1}{2}\right) - \left(2x - \frac{1}{2}\right)\log\left(2x - \frac{1}{2}\right). \tag{2.71}$$

The von Neumann entropy is invariant under isometric operations (linear and distance preserving). This includes also unitary operations, as they are isometric isomorphisms. For any density matrix $\hat{\rho}$ and any isometric operator $\hat{V}$, the von Neumann entropy S is invariant [121],

$$S\left(\hat{V}\hat{\rho}\hat{V}^{\dagger}\right) = S\left(\hat{\rho}\right). \tag{2.72}$$

For two-mode Gaussian states ($N = 2$), the invariant von Neumann entropy S depends on the symplectic eigenvalues ν_- and ν_+ of $\mathbf{V}$ [122]

$$S\left(\hat{\rho}\right) = g\left(\nu_+\right) + g\left(\nu_-\right), \quad \nu_\pm = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4\det \mathbf{V}}}{2}}, \tag{2.73}$$

where Δ is the abbreviation of the sum of determinants of submatrices of $\mathbf{V}$

$$\Delta = \det \mathbf{A} + \det \mathbf{B} + 2\det \mathbf{C}, \quad \mathbf{V} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^{\mathrm{T}} & \mathbf{B} \end{pmatrix}, \tag{2.74}$$

where $\mathbf{A} \in \mathbb{R}^{2\times 2}$ describes the first mode locally, $\mathbf{B} \in \mathbb{R}^{2\times 2}$ describes the second mode locally, and $\mathbf{C} \in \mathbb{R}^{2\times 2}$ describes the correlation between the two modes [64]. A pedagogic introduction to the entropy for continuous-variable quantum states can be found in Ref. 122.

2.3.3 Alice's preparation of squeezed displaced cipher states

In this section, we describe how Alice encodes the Gaussian-sampled classical variable α_i into a microwave state and describe the quantum-cryptographic protection of this classical data.

Indistinguishable encoding bases

In this section, we want to discuss why Eve cannot infer the basis that Alice used to encode the symbol in the CV-QKD described above. Alice encodes each variable α_i in an ensemble

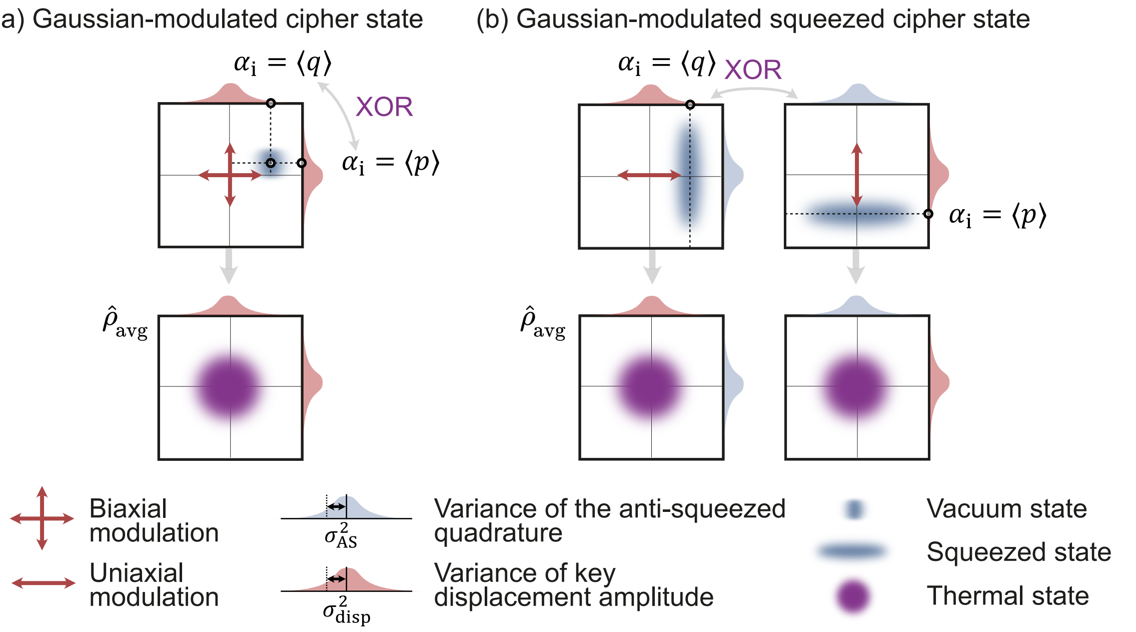
(a) Gaussian-modulated cipher state
(b) Gaussian-modulated squeezed cipher state
$\alpha_i = \langle q \rangle$
XOR
$\alpha_i = \langle p \rangle$
$\hat{\rho}_{avg}$
Biaxial modulation
Uniaxial modulation
σ^2_{AS}
σ^2_{disp}
Variance of the anti-squeezed quadrature
Variance of key displacement amplitude
Vacuum state
Squeezed state
Thermal state

Figure 2.9: Gaussian encoding schemes for indistinguishable bases. (a) Biaxial Gaussian modulation of a coherent state with variance $\sigma^2 = 0.25$ with random displacements drawn from the classical distribution $\mathcal{N}(0, \sigma^2_{\text{disp}})$. (b) Uniaxial Gaussian modulation of squeezed states with variance of the antisqueezed quadrature $\sigma^2_{\text{AS}} - \sigma^2_{\text{S}} = \sigma^2_{\text{disp}}$. In both encoding schemes, the average state $\hat{\rho}_{\text{avg}}$ is a thermal state.

$\mathcal{E}_{\text{m}}$ which is randomly chosen from N ensembles defined as [49]

$$\mathcal{E}_{\text{m}} = \{p_{\text{i,m}}, |\psi_{\text{i,m}}\rangle \langle\psi_{\text{i,m}}|\}\,, \tag{2.75}$$

where each state $|\psi_{\text{i,m}}\rangle \langle\psi_{\text{i,m}}|$ is sent with the probability $p_{\text{i,m}}$. Let us assume that the states in different N ensembles $\mathcal{E}_{\text{m}}$ are non-orthogonal. Let $\mathcal{E}_{\text{n}}$ be an arbitrary different ensemble $m \neq n$. If $|\psi_{\text{i,m}}\rangle \langle\psi_{\text{i,m}}|$ and $|\psi_{\text{i,n}}\rangle \langle\psi_{\text{i,n}}|$ are non-orthogonal states, and the the sum over i yields for any m the same identical average state $\hat{\rho}_{\text{avg}}$, then Eve can't know which ensemble was initially chosen. More precisely, [49]

$$\forall m : \sum_{i}^{N} p_{\text{i,m}} |\psi_{\text{i,m}}\rangle \langle\psi_{\text{i,m}}| = \hat{\rho}_{\text{avg}}, \tag{2.76}$$

where $\hat{\rho}_{\text{avg}}$ is an average density matrix of a thermal state. As a result, Eve has to interact with Alice's states. Alice and Bob can quantify this disturbance and quantify the amount of information extracted by Eve by analyzing the statistics in their error corrected shared secret key. Alice and Bob can then determine whether the communication is secure or not.

In Fig. 2.9, two different CV-QKD modulation schemes are shown. Fig. 2.9 (a) shows the coherent modulation scheme [37]. Here, the symbols are encoded either in the p or q quadrature, while the other quadrature gets a random value which encodes no useful information. The resulting average state has the same probability distribution as a thermal state if $\sigma^2_{\mathrm{disp,q}} = \sigma^2_{\mathrm{disp,p}}$.

The Gaussian-modulated squeezed state protocol is shown in Fig. 2.9 (b). We use it for our implementation of the CV-QKD protocol. Here, the symbols are also encoded either in the p or q quadrature. However, the uncertainty distribution on the other quadrature is not achieved with random classical sampling, but by using squeezed states with a matching variance so that the antisqueezed quadrature matches the sum of the displacement variance and the variance of the squeezed quadrature $\sigma^2_{\mathrm{AS}} = \sigma^2_{\mathrm{disp}} + \sigma^2_{\mathrm{S}}$.

In Fig. 2.9 (c,d), we can see that both schemes result in the same average state. The symbol encoding is also identical. The two approaches only differ in their approach to provide the required randomness to a achieve an average thermal state. From the perspective of the receiver Bob and the eavesdropper Eve they are equivalent.

Squeezed displaced states

Alice's goal is to provide a displaced squeezed state with a displacement amplitude α_i, where the squeezing angle and displacement angle are parallel to each other in p- or q-bases as follows

$$\bar{\mathbf{r}}_{\mathrm{q}} = \begin{pmatrix} \alpha_{\mathrm{i}} \\ 0 \end{pmatrix}, \quad \mathbf{V}_{\mathrm{q}} = \begin{pmatrix} \sigma^2_{\mathrm{S}} & 0 \\ 0 & \sigma^2_{\mathrm{AS}} \end{pmatrix}, \tag{2.77}$$

$$\bar{\mathbf{r}}_{\mathrm{p}} = \begin{pmatrix} 0 \\ \alpha_{\mathrm{i}} \end{pmatrix}, \quad \mathbf{V}_{\mathrm{p}} = \begin{pmatrix} \sigma^2_{\mathrm{AS}} & 0 \\ 0 & \sigma^2_{\mathrm{S}} \end{pmatrix}. \tag{2.78}$$

To achieve this goal with microwave states, we propose to squeeze a vacuum state using a Josephson parametric amplifier (JPA) (see Sec. 2.2.5) and displace an intermediate propagating squeezed state with a directional coupler coupled to a strong coherent tone (see Sec. 2.1.3). In the following, we account for a finite thermal noise added by the JPA and use a squeezed thermal state model with a noise photon number n_{JPA}.

For the i-th symbol, the random variables consisting of basis b_i and the displacement amplitude α_{i} are drawn from their respective distributions. In particular, the random variable b_i is defined as $b_{\mathrm{i}} \in \{q, p\}$, where the probabilities for the different bases are equally $P(\{q\}) = P(\{p\}) = 0.5$. The random variable α_{i} is drawn from $\mathcal{N}(0, \sigma^2_{\mathrm{disp}})$, which is a classical Gaussian distribution of mean 0 and displacement variance σ^2_{disp} that matches the anti-squeezing variance that can be realistically achieved by Alice's JPA. In particular, we can compute the average states for the limit of infinite number of symbols α_{i}

$$\bar{\mathbf{r}}_{\mathrm{avg,q}} = \mathbf{0}, \quad \mathbf{V}_{\mathrm{avg,q}} = \frac{1}{4}\begin{pmatrix} (1+2n_{\mathrm{JPA}})\,e^{-2r} + 4\sigma^2_{\mathrm{disp}} & 0 \\ 0 & (1+2n_{\mathrm{JPA}})\,e^{2r} \end{pmatrix}, \tag{2.79}$$

$$\bar{\mathbf{r}}_{\mathrm{avg,p}} = \mathbf{0}, \quad \mathbf{V}_{\mathrm{avg,p}} = \frac{1}{4}\begin{pmatrix} (1+2n_{\mathrm{JPA}})\,e^{2r} & 0 \\ 0 & (1+2n_{\mathrm{JPA}})\,e^{-2r} + 4\sigma^2_{\mathrm{disp}} \end{pmatrix}. \tag{2.80}$$

The condition for indistinguishable basis encoding from Eq. 2.76 requires that each of the average states has the same variance in both quadratures. For both average states in q and p, we require that

$$\frac{1}{4}\left(1+2n_{\mathrm{JPA}}\right)e^{-2r}+\sigma_{\mathrm{disp}}^{2}=\frac{1}{4}\left(1+2n_{\mathrm{JPA}}\right)e^{2r}. \tag{2.81}$$

Now Alice's average state can be fomulated as a thermal state with a uniform variance depending on the photon number $(1+2n_{\mathrm{th}})=(1+2n_{\mathrm{JPA}})\,e^{2r}$. The three needed steps are:

(i) Alice samples α_{i} from $\mathcal{N}(0,\sigma_{\mathrm{disp}}^{2})$, and b_{i} from $\{q,p\}$.

(ii) Squeezing of the vacuum state.

   (a) If $b_i=p$, Alice's JPA squeezing angle is set to $\gamma=0$.

   (b) If $b_i=q$, Alice's JPA squeezing angle is set to $\gamma=90°$.

(iii) Displacement of the squeezed vacuum state.

   (a) If $b_i=p$, Alice's displacement angle is set to $\theta=0°$the displacement amplitude is $\bar{\mathbf{r}}=(0,\alpha_{\mathrm{i}})^{T}$.

   (b) If $b_i=q$, Alice's displacement angle is set to $\theta=90°$. The displacement amplitude is $\bar{\mathbf{r}}=(\alpha_{\mathrm{i}},0)^{T}$.

Finally the displaced squeezed state is sent to the quantum channel.

2.3.4 Bob's homodyne detection

Alice's state (see Eq. 2.77) is sent through a noisy quantum channel. Bob is the receiver at the end of this quantum channel. In this section, we characterize the amount of mutual information shared between Alice and Bob over the quantum channel by their two sets of variables, $\alpha_i\in A$ and $\beta_i\in B$. We present two approaches to obtain the mutual information between a sender (Alice) and a receiver (Bob).

The first approach is based on the differential entropy of the classical input (α_i) and output (β_i) of the channel. We reformulate the differential entropy in terms of measurable variances and covariances. The second approach is motivated by Shannon's noisy channel coding theorem for discrete memoryless channels [123]. In contrast to the mutual information of a finite key, the capacity of a channel can provide an asymptotic measure for the mutual information which is dependent only on the average signal and noise powers. This provides us with an upper bound estimation for the mutual information and it can be computed by using a related signal-to-noise ratio (SNR) in the considered channel. The SNR is accessible from calibration measurements that characterize the signal and noise powers in the amplification chain. Finally, we present the scaling of the SNR as a function of averages in an additive white Gaussian noise (AWGN) channel. This allows us to scale the expected mutual information with a number of averages.

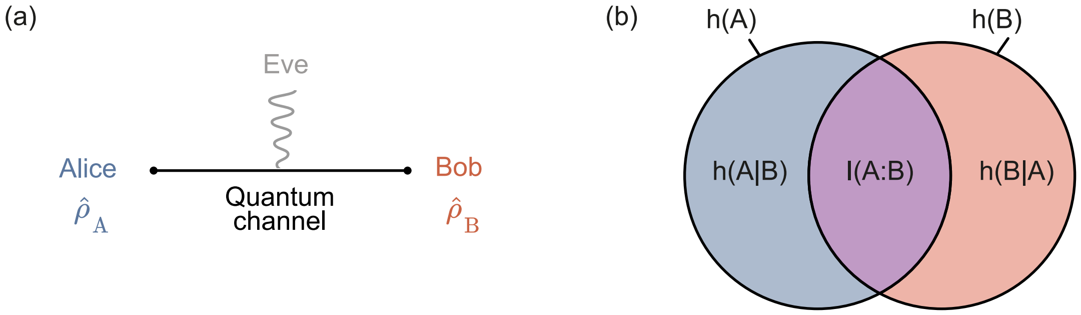

Figure 2.10: (a) Quantum channel between Alice and Bob with the input state $\hat{\rho}_A$ and the output state $\hat{\rho}_B$. (b) Venn diagram for the mutual information between Alice and Bob as the intersection of differential entropies h.

Mutual information continuous variables

The mutual information $I(A{:}B)$ quantifies the shared information between two sets, by the correlation of their two sets of variables: Alice's key A, Bob's key B, which consists of N symbols $\alpha_i \in A$, $\beta_i \in B$. We can define the mutual information $I(A{:}B)$ for continuous variables with the joint probability distribution $p_{A,B}(\alpha, \beta)$ as [49, 124]

$$\begin{aligned} I(A{:}B) &= h(A) - h(A|B) \\ &= h(B) - h(B|A) \\ &= h(A) + h(B) - h(A,B) \\ &= h(A,B) - h(A|B) - h(B|A), \end{aligned} \tag{2.82}$$

where $h(A)$ is the marginal differential Shannon entropy, and $h(A|B)$ is the conditional differential Shannon entropy. The relation can be understood from the standing point of Alice and Bob: the general uncertainty about Alice's key, $h(A)$, is reduced by Bob's information gain on Alice's key based on his own key, $h(A|B)$ [124]. An illustration of the involved quantities is shown in Fig. 2.10 (b). In this work, both encoded and decoded keys follow Gaussian distributions $\mathcal{N}(\mu_A, \sigma_A^2)$, $\mathcal{N}(\mu_B, \sigma_B^2)$, as Alice samples her key from a Gaussian distribution. Then, we assume that Bob's measurement of Alice's key is in itself a Gaussian sampling process consistent with the choice of an additive white Gaussian noise channel model. The covariance matrix of the two Gaussian-distributed sets A, B is defined as [125]

$$\Sigma_{AB} = \begin{pmatrix} \sigma_A^2 & \mathrm{Cov}\,(A,B) \\ \mathrm{Cov}\,(A,B) & \sigma_B^2 \end{pmatrix}, \tag{2.83}$$

with σ_A^2 being the variance of A and $\mathrm{Cov}\,(A,B)$ being the covariance of A and B. The variances σ_A^2, σ_B^2 and the covariance $\mathrm{Cov}\,(A,B)^2$ are computed from the key of finite length N by Alice's symbols $\alpha_i \in A$ and the measured symbols $\beta_i \in B$ by Bob. We use the variance and covariance in their Bessel-corrected form [125]

$$\sigma_A^2 = \frac{1}{N-1}\sum_{i=1}^{N}(\alpha_i - \mu_A)^2, \qquad \mu_A = \frac{1}{N}\sum_{i=1}^{N}\alpha_i, \tag{2.84}$$

$$\sigma_B^2 = \frac{1}{N-1}\sum_{i=1}^{N}(\beta_i - \mu_B)^2, \qquad \mu_B = \frac{1}{N}\sum_{i=1}^{N}\beta_i, \tag{2.85}$$

$$\mathrm{Cov}(A,B) = \frac{1}{N-1}\sum_{i=1}^{N}(\alpha_i - \mu_A)\cdot(\beta_i - \mu_B). \tag{2.86}$$

The conditional variance can be computed as [49]

$$\sigma_{B|A}^2 = \frac{\det\left(\Sigma_{AB}\right)}{\sigma_A^2} = \sigma_B^2 - \frac{\mathrm{Cov}\left(A,B\right)^2}{\sigma_A^2}. \tag{2.87}$$

Next, we find an explicit formulation for $h(A)$ and $h(B|A)$ to calculate the mutual information as in Eq. 2.82. For a Gaussian variable B, we can find from Eq. 2.66 the result for the marginal differential entropy [126]

$$h(A) = \frac{1}{2}\log_2\left((2\pi e)\sigma_B^2\right) + C, \tag{2.88}$$

where C is a reference constant and we chose the unit of bits. Similarly, the conditional differential entropy $h\left(B|A\right)$ is given by

$$h\left(B|A\right) = \frac{1}{2}\log_2\left[(2\pi e)\,\sigma_{B|A}^2\right] + C. \tag{2.89}$$

Here we made use of the earlier defined conditional variance $\sigma_{B|A}^2$. We compute the mutual information (see Eq. 2.82) by using the marginal differential entropy (see Eq. 2.88) and the conditional differential entropy (see Eq. 2.89) as [49]

$$\begin{aligned} I\left(A{:}B\right) &= \frac{1}{2}\log_2\left((2\pi e)\sigma_B^2\right) + C - \left(\frac{1}{2}\log_2\left[(2\pi e)\,\sigma_{B|A}^2\right] + C\right) \\ &= \frac{1}{2}\log_2\left[\frac{\sigma_B^2}{\sigma_{B|A}^2}\right] \\ &= \frac{1}{2}\log_2\left[\frac{\sigma_B^2\,\sigma_A^2}{\sigma_B^2\,\sigma_A^2 - \mathrm{Cov}\left(A,B\right)^2}\right]. \end{aligned} \tag{2.90}$$

Our initial concern about constant offsets in the differential entropy vanishes, as we note that the constant C cancels out for the final expression for mutual information in terms of differential entropies.

Shannon channel capacity

In this section, we consider bounds on the classical mutual information which are set by the channel capacity. The Shannon limit gives a definition for the channel capacity if the signal power is bounded, the noise is Gaussian, and the signal and noise powers are known for a classical channel [123]. The theorem states that the channel capacity C bounds the maximum information rate as (see theorem 2 in Ref. 123)

$$C(\mathcal{G}_{\text{class}}) \leq \Delta f \log_2 (1 + \text{SNR}) \, , \tag{2.91}$$

where Δf is the channel bandwidth, $\text{SNR} = P_{\text{S}}/P_{\text{N}}$ is the signal-to-noise ratio with the average signal power P_{S} and noise power P_{N}, $\mathcal{G}_{\text{class}}$ is an arbitrary white Gaussian noise channel, and the basis $n = 2$ defines bits as the units here.

To retrieve the corresponding maximum information transfer rate through the channel, we have to divide the capacity by the Nyquist rate $2\Delta f$, which can be interpreted as the symbol bandwidth in terms of bits ($n = 2$) per second (Δf) (see Nyquist sampling theorem 1 in Ref. 123). We refer to the maximum mutual information possible to achieve through our channel as the Shannon capacity

$$I_{\max}(\mathcal{G}_{\text{class}}) = \frac{1}{2} \log_2 (1 + \text{SNR}) \, . \tag{2.92}$$

This result is useful, as it gives an upper bound even for the asymptotic case of infinite keylength. The Shannon capacity holds only for classical channels. However, we can treat the symbol displacement amplitude at the input of the output line as classical variables.

Characterization of the output line with sample averages

The maximal mutual information $I(A{:}B) < I_{\max}$ on the output channel (bits per channel use) can be rewritten in terms of the signal powers at the end of the quantum channel $\text{SNR} = P_{\text{S}}/P_{\text{N}}$. Interestingly, the signal-to-noise ratio (SNR) is experimentally accessible with low error due to the well-known scaling of the SNR in Gaussian processes. Let Bob's i-th sample be $\beta_i = \alpha + n_i$, where Bob is repeatedly measuring a single symbol sent by Alice α and n_i represents random Gaussian noise. For the i-th sample of this averaging process, the SNR can be defined in terms of the expectation values of random variables for the signal S and the noise N as

$$\text{SNR}_i = \frac{E\left[s^2\right]}{E\left[n^2\right]}, \tag{2.93}$$

where E is the expectation operator. If the random variable β is averaged M times for a constant symbol of Alice α, the noise contribution is reduced. We can write for the averaged random variable $\bar{\beta}$

$$\bar{\beta} = \alpha + \frac{1}{M} \sum_{i=1}^{M} n_i. \tag{2.94}$$

For the M samples, the SNR is then

$$\mathrm{SNR_M} = \frac{E\left[\alpha^2\right]}{M^{-2} E\left[\left(\sum_{i=1}^{M} n_i\right)^2\right]} = M \frac{E\left[\alpha^2\right]}{E\left[\left(n_i^2\right)\right]} = M \cdot \mathrm{SNR_i}. \tag{2.95}$$

We can use this result to estimate the SNR more precisely using averaging measurements.

2.3.5 Eve's Holevo information

In this section, we discuss the strongest eavesdropping attack possible on the quantum channel. We dilate the attack on the channel into a canonical form with a beam splitter. This model allows us to calculate the information that Eve can extract by her attack. Finally, we discuss the theoretical limitations of the quantum channel. The following analysis is based on the asymptotic assumption of an infinite keylength. For composable security proofs and other security threats like quantum hacking, we refer to Ref. 114. The final result of a CV-QKD protocol, as described in Sec. 2.3.1, are the secret symbols k_i. It is obtained from the classical post-processing of the shared correlated variables of Alice (α_i) and Bob (β_i). The secret key K defines the how many bits per symbol were transmitted securely during one channel use.

Holevo information bound on accessible information for Eve

In the last section, we quantified the information between the two communicating parties Alice and Bob with the mutual information $I(A{:}B)$. Here, we consider attacks on the communication channel by an eavesdropper, Eve. Eve interacts with the communication channel by coupling her own states to propagating states coming from Alice and reading them out.

In practice, one can implement a number of different eavesdropping attacks. The maximally accessible information obtainable by Eve is defined for an optimal measurement [124]

$$I_{\mathrm{acc}}\left(\mathcal{E}_{\mathrm{E}}\right) = \max_{M_{\mathrm{E}}} I\left(X{:}E\right), \tag{2.96}$$

where M_{E} corresponds to Eve's measurements, and $I\left(X{:}E\right)$ is the mutual information between Alice ($X = A$, direct reconciliation) or Bob ($X = B$, reverse reconciliation). The ensemble $\mathcal{E}_{\mathrm{E}}$ denotes the states which Eve obtains by performing the attack on the commu-

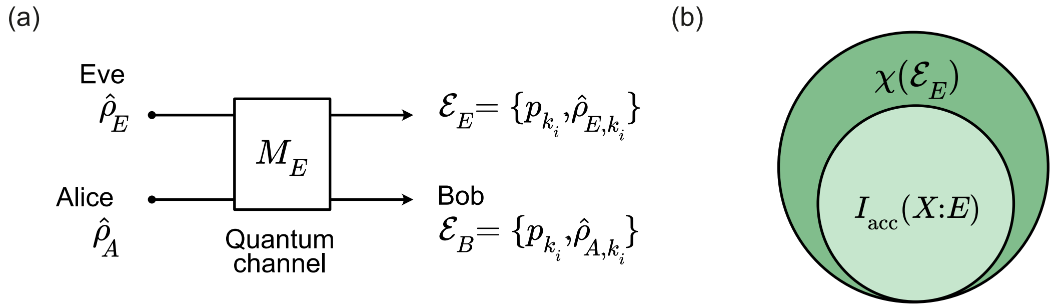

Figure 2.11: (a) Eavesdropping on the quantum channel through an optimal unitary measurement M_{E}. (b) Holevo information bound on Eve's accessible information.

nication channel as [124]

$$\mathcal{E}_{\mathrm{E}} = \{p_{\mathrm{k_i}}, \hat{\rho}_{\mathrm{E,k_i}}\}\,, \tag{2.97}$$

where Eve measures with the probability $p_{\mathrm{k_i}}$ a corresponding state $\hat{\rho}_{\mathrm{E,k_i}}$ corresponding to the key element k_{i}. More precisely, the ensemble $\mathcal{E}_{\mathrm{E}}$ is the environment output for the Stinespring dilation [127] of the bosonic quantum channel between Alice and Bob, as shown in Fig. 2.11. The corresponding output for Bob is computed by tracing out the environment controlled by Eve [64]

$$\mathcal{E}_{\mathrm{B}} = \mathrm{Tr}_{\mathrm{E}}\left[U\left(\hat{\rho}_{\mathrm{A}} \otimes |\Phi\rangle_{\mathrm{E}}\,\langle\Phi|_{\mathrm{E}}\right)U^{\dagger}\right], \tag{2.98}$$

where $\hat{\rho}_A$ is Alice's input state, U is the unitary interaction between Alice's state and Eve's pure state $|\Phi\rangle_{\mathrm{E}}$. Conversely, the system can be traced out to retrieve Eve's output ensemble $\mathcal{E}_{\mathrm{E}}$. Eve's input state can always be chosen to be a multi-mode vacuum state $|\Phi\rangle_{\mathrm{E}} = |0\rangle_{\mathrm{E}}$, as the Stinespring dilation is unique up to partial isometries [128].

In practice, the possibilities for the different measurements M_{E} are not mathematically tractable. However, Holevo's theorem states that the upper limit for the maximal mutual information is the Holevo information $\chi(\mathcal{E}_{\mathrm{E}})$ as [23]

$$I_{\mathrm{acc}}\left(\mathcal{E}_{\mathrm{E}}\right) \leq \chi\left(\mathcal{E}_{\mathrm{E}}\right). \tag{2.99}$$

The Holevo information $\chi(\mathcal{E}_{\mathrm{E}})$ is defined by

$$\chi\left(\mathcal{E}_{\mathrm{E}}\right) = S\left(\sum p_{\mathrm{k_i}}\,\hat{\rho}_{\mathrm{E,k_i}}\right) - \sum p_{\mathrm{k_i}} S\left(\hat{\rho}_{\mathrm{E,k_i}}\right) \geq 0, \tag{2.100}$$

where S is the von Neumann entropy (see Eq. 2.68). A detailed outline of the proof can be found in Ref. 120. In conclusion, the Holevo information is the upper bound for Eve's information on the key for any possible measurement implementation by Eve.

Eavesdropping strategies

In this section, we want to show three types of attacks on CV-QKD protocols, which are known as individual, collective, and coherent attacks [129]. Unconditional security proofs of QKD protocols rely on the following assumptions [64]:

(i) Eve has full access to the quantum channel.

(ii) Eve has unlimited computational power.

(iii) Eve can monitor the authenticated classical channel while staying undetected.

(iv) Eve has no access to Alice or Bob's setups.

The most powerful attack is the so-called coherent attack. Eve prepares a global input ancillary system that interacts with all signals on the quantum channel, and stores the output ancillary system into a quantum memory. After Eve has listened to all classical communication over the authenticated classical channel, she performs an optimal joint measurement on the quantum memory [64].

However, the security analysis of coherent attacks is very complex. By proving the quantum de Finetti theorem, Renner [130] enabled an equivalent proof for unconditional asymptotic security with the simpler collective attack for continuous variables [131]. The main point of the proof is that one can assume permutation symmetry in the classical post-processing. In a collective attack, Eve prepares a set of independent and identically prepared ancillas. Now, each of these ancillas interact individually with single signals in the quantum channel instead of the global interaction with all signals (coherent attack). Similar to the coherent attack, Eve stores the output states in quantum memory and applies an optimal measurement after listening in on the classical channel between Alice and Bob [64].

Dilation of Gaussian quantum channels to canonical forms

Noise in quantum communication protocols is typically characterized by using the framework of Gaussian channels [64, 132, 133]. Gaussian channels $\mathcal{G}$ can be decomposed with the help of unitary transformations to the canonical forms $\mathcal{C}$ consisting of simple diagonal matrices. In this section, we characterize different canonical forms $\mathcal{C}$ for unitary channels, amplification channels, quadrature-dependent noise channels, and classical noise channels. Later, we use these canonical forms to characterize the quadrature-dependent signal-to-noise ratio in transmission lines.

The symplectic map formalism for Gaussian unitary operations is introduced in Sec. 2.1.3. However, Gaussian channels do not need to be locally unitary. That means, that an additional noise $\mathbf{N}$ can be introduced to the covariance matrix $\mathbf{V}$. Arbitrary single-mode Gaussian channels $\mathcal{G}(\mathbf{d}, \mathbf{T}, \mathbf{N})$ are completely described by the transformation map of the

Table 2.1: Canonical classes and their corresponding forms $\mathcal{C}$ parametrized by their transmissivity τ, rank r, and thermal number $\bar{n}$. Here, $\mathbf{I}$ is the identity matrix, $\mathbf{0}$ the zero matrix, and $\mathbf{Z} = \mathrm{diag}(1, -1)$. Adapted from Ref. 64.

Class	Form $\mathcal{C}(\tau, r, \bar{n})$	$\mathbf{T}_c$	$\mathbf{N}_c$
A_1	$\mathcal{C}(0, 0, \bar{n})$	$\mathbf{0}$	$(2\bar{n} + 1)\mathbf{I}$
A_2	$\mathcal{C}(0, 1, \bar{n})$	$(\mathbf{I} + \mathbf{Z})/2$	$(2\bar{n} + 1)\mathbf{I}$
B_1	$\mathcal{C}(1, 1, 0)$	$\mathbf{I}$	$(\mathbf{I} - \mathbf{Z})/2$
B_2	$\mathcal{C}(1, 2, \bar{n})$	$\mathbf{I}$	$\bar{n}\mathbf{I}$
$\mathcal{L}$	$\mathcal{C}(\tau \in (0, 1), 2, \bar{n})$	$\sqrt{\tau}\mathbf{I}$	$(1 - \tau)(2\bar{n} + 1)\mathbf{I}$
$\mathcal{A}$	$\mathcal{C}(\tau > 1, 2, \bar{n})$	$\sqrt{\tau}\mathbf{I}$	$(\tau - 1)(2\bar{n} + 1)\mathbf{I}$

first-order and second-order statistical moments [64, 71]

$$\begin{aligned} \mathcal{G}(\mathbf{d}, \mathbf{T}, \mathbf{N}): \quad \hat{\mathbf{r}} &\to \mathbf{T}\hat{\mathbf{r}} + \mathbf{d}, \\ \mathbf{V} &\to \mathbf{T}\mathbf{V}\mathbf{T}^T + \mathbf{N}, \end{aligned} \tag{2.101}$$

where the complete positivity (CP) condition of Gaussian unitaries (see Eq. 2.17) is extended to [64, 71]

$$\mathbf{N} + i\mathbf{\Omega} - i\mathbf{T}\mathbf{\Omega}\mathbf{T}^T \geq 0, \tag{2.102}$$

where $\mathbf{\Omega}$ is defined as in Eq. 2.17, $\mathbf{T}$ and $\mathbf{N} = \mathbf{N}^T$ are 2×2 real matrices in the case of a single mode. This CP condition can then be simplified to [64]

$$\mathbf{N} = \mathbf{N}^T \geq 0, \quad \det \mathbf{N} \geq (\det \mathbf{T} - 1)^2. \tag{2.103}$$

Gaussian channels characterize the (noisy) evolution of Gaussian states [64]. A single-mode Gaussian channel $\mathcal{G}$ can be decomposed to [134]

$$\mathcal{G} = W \left[\mathcal{C}(U \hat{\rho} U^\dagger) \right] W^\dagger, \tag{2.104}$$

where the canonical form $\mathcal{C} = \mathcal{C}(\mathbf{d}_c, \mathbf{T}_c, \mathbf{N}_c)$ is a Gaussian channel with zero displacement, $\mathbf{d}_c = 0$, and diagonal matrices $\mathbf{T}_c$ and $\mathbf{N}_c$. This constraint enables an additional parametrization of the canonical form with respect to a set of three invariants $\{\tau, r, \bar{n}\}$, where the channel transmissivity τ, the channel rank r, and the thermal number $\bar{n} \geq 0$ are defined by [64]

$$\tau = \det(\mathbf{T}), \quad \tau \in (-\infty, \infty), \tag{2.105}$$

$$r = \min\left[\mathrm{rank}(\mathbf{T}), \mathrm{rank}(\mathbf{N})\right], \quad r \in [0, 1, 2], \tag{2.106}$$

$$\bar{n} = \begin{cases} (\det(\mathbf{N}))^{1/2}, & \text{for} \quad \tau = 1, \\ \frac{(\det(\mathbf{N}))^{1/2}}{2|1-\tau|} - \frac{1}{2}, & \text{for} \quad \tau \neq 1. \end{cases} \tag{2.107}$$

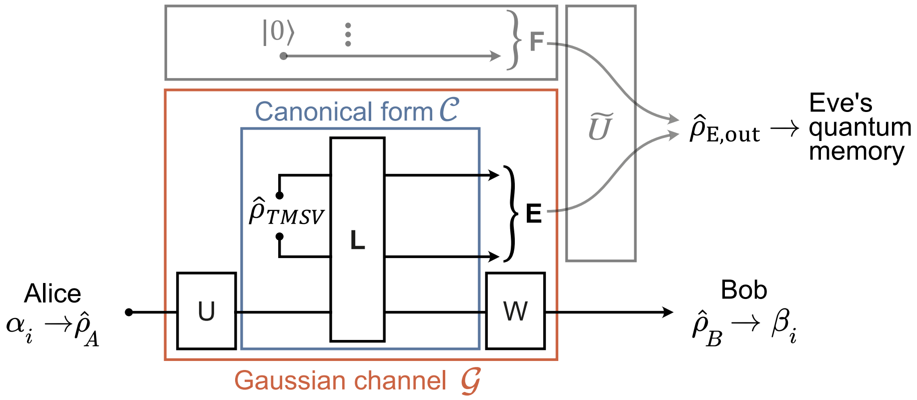
|0⟩
F
Canonical form $\mathcal{C}$
$\tilde{U}$
$\hat{\rho}_{\mathrm{E,out}} \rightarrow$
Eve's quantum memory
$\hat{\rho}_{TMSV}$
L
E
Alice
$\alpha_i \rightarrow \hat{\rho}_A$
U
W
Bob
$\hat{\rho}_B \rightarrow \beta_i$
Gaussian channel $\mathcal{G}$

Figure 2.12: Schematic of the canonical form and dilation of a collective attack on the quantum channel by an eavesdropper. The Gaussian channel $\mathcal{G}$ is reduced with the unitaries U and W to the canonical form $\mathcal{C}$. The canonical form $\mathcal{C}$ is dilated to a symplectic transformation $\mathbf{L}$ which takes as inputs Alice's state and the two-mode squeezed vacuum state $\hat{\rho}_{\mathrm{TMSV}}$ from Eve. $\tilde{U}$ transforms Eve's modes $\{\mathbf{E}, \mathbf{F}\}$ to a quantum memory.

This concludes the tool set needed to formulate canonical forms $\mathcal{C}(\tau, r, \bar{n})$ that satisfy the requirements for Gaussian channels. The classes of canonical forms differ in their three invariants $\{\tau, r, \bar{n}\}$ introduced above. Tab. 2.1 shows examples of these classes: Class A_1 replaces any input state with a thermal state; class A_2 replaces one quadrature of an input state with Gaussian noise $\bar{n}$; class B_1 adds classical Gaussian noise on one quadrature; class B_2 is a classical Gaussian noise channel for each quadrature; a loss channel $\mathcal{L}$ is defined for $0 < \tau < 1$; and the amplification channel $\mathcal{A}$ for $\tau > 1$ [64].

Canonical form of collective Gaussian attacks

As explained above, the collective Gaussian attack is the fundamental benchmark to test the security of continuous-variable QKD protocols. In this section, we present how this attack can be represented in the Gaussian communication channel (see Sec. 2.3.5) coupled to the environment controlled by Eve.

The following description is visualized in Fig. 2.12 and follows the description in Ref. 64. Let $\mathcal{G}$ be the Gaussian communication channel between Alice an Bob, characterized by its canonical form $\mathcal{C}(\tau, r, \bar{n})$ up to the unitary pair U and W. For an incoming state by Alice $\hat{\rho}_{\mathrm{A}}$, the canonical form can be dilated to the symplectic transformation $\mathbf{L}$, which includes Eve's two-mode squeezed vacuum (TMSV) state $\hat{\rho}_{\mathrm{TMSV}}$ with variance $\sigma_{\mathrm{E}}^2 = 1/4(1 + 2\bar{n})$. This TMSV state interacts through the symplectic transformation $\mathbf{L}$ with Alice's state. The resulting mode $\{\mathbf{E}\}$ is stored in a quantum memory by the transformation $\tilde{U}$. The unitary $\tilde{U}$ is dilated to an environment with the vacuum modes $\mathbf{F}$.

The canonical dilation $\mathcal{C}_{\mathbf{L}}(\tau, r, \bar{n}_{\mathrm{TMSV}})$ and the single-mode Gaussian unitaries U and W fully characterize the attack [38]. The attack is called canonical if the unitaries $U = W = \mathbb{I}$. This canonical dilation is modeled as a beam splitter $(0 < \tau < 1)$ [40].

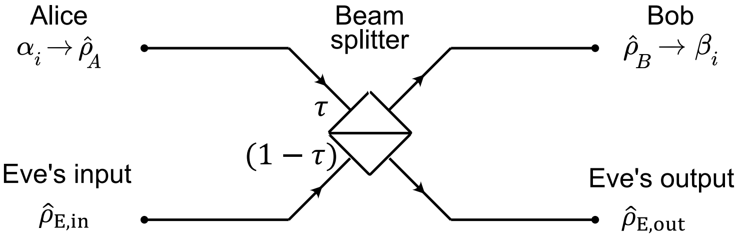
Alice
$\alpha_i \rightarrow \hat{\rho}_A$
Beam splitter
Bob
$\hat{\rho}_B \rightarrow \beta_i$
τ
$(1-\tau)$
Eve's input
$\hat{\rho}_{\mathrm{E,in}}$
Eve's output
$\hat{\rho}_{\mathrm{E,out}}$

Figure 2.13: Beam splitter representation of the entangling cloner eavesdropping attack. The beam splitter input consists of Alice's state $\hat{\rho}_{\mathrm{A}}$, encoding a classical variable α_i, and Eve's input state $\hat{\rho}_{\mathrm{E,in}}$. The transmissivity of the beam splitter is denoted as τ. At the output of the beam splitter are Bob's state $\hat{\rho}_{\mathrm{B}}$, which he uses to decode the classical variable β_i, and Eve's output state $\hat{\rho}_{\mathrm{E,out}}$.

Beam splitter model of the entangling cloner attack

In this section, we present how to model the entangling cloner attack with a beam splitter. This attack is a collective Gaussian attack, where an optimal collective measurement is required. However, the unitaries required to dilate the attack to an environment are not needed when we consider the Holevo bound (see Sec. 2.3.5), as the Holevo bound is invariant under isometric operations. Therefore, we can choose $U = W = \mathbb{I}$. The Gaussian channel of a beam splitter with transmissivity τ that couples noise from Eve $\mathcal{G}_{\mathrm{BS}}(\mathbf{d}, \mathbf{T}, \mathbf{N})$ can be characterized as [49]

$$\mathbf{d} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \quad \mathbf{T} = \sqrt{\tau}\mathbb{I}, \quad \mathbf{N} = \frac{1}{4}\left(1-\tau\right)\left(1+2n_{\mathrm{Eve}}\right)\mathbb{I}. \tag{2.108}$$

As a result, the transformation $\mathbf{L}$ of the beam splitter representation of the entangling-cloner attack can be written as

$$\begin{aligned} \mathcal{G}_{\mathrm{BS}}\{\mathbf{L}(\tau), \hat{\rho}_{\mathrm{E}}\}: \quad & \bar{\mathbf{r}} \mapsto \sqrt{\tau}\,\bar{\mathbf{r}}, \\ & \mathbf{V} \mapsto \tau\mathbf{V} + \frac{1}{4}\left(1-\tau\right)\left(1+2n_{\mathrm{Eve}}\right)\mathbb{I}, \end{aligned} \tag{2.109}$$

where we can parametrize Eve's coupled noise by the quantity $\bar{n}$ [49]

$$\frac{1}{4}\left(1-\tau\right)\left(1+2n_{\mathrm{Eve}}\right) = \bar{n} + \frac{1}{4}(1-\tau). \tag{2.110}$$

This leads to a modified symplectic map $\mathbf{L}$, that depends now on the losses $(1-\tau)$ and noise $(\bar{n})$ on Eve's channel [49]

$$\begin{aligned} \mathbf{L}(\tau, \bar{n}): \quad & \bar{\mathbf{r}} \mapsto \sqrt{\tau}\,\bar{\mathbf{r}}, \\ & \mathbf{V} \mapsto \tau\mathbf{V} + \bar{n}\mathbb{I} + \frac{1}{4}(1-\tau)\mathbb{I}. \end{aligned} \tag{2.111}$$

This representation is known as the universal Gaussian cloner attack [135]. We consider the entangling cloner attack in the limit of $\tau \rightarrow 1$, and $\bar{n} \neq 0$.

From here, we can show how Alice's and Eve's input states are transformed to Bob's state and Eve's output state. Let Alice's input state be $\hat{\rho}_{\mathrm{A}}$, Eve's input state is $\hat{\rho}_{\mathrm{E,in}}$, Bob's state is $\hat{\rho}_{\mathrm{B}}$, and Eve's output state is $\hat{\rho}_{\mathrm{E,out}}$. Alice's state is defined by her displacement amplitude, α_i, and the squeezing factor, r. For her input noise we assume a thermal state with noise n_{JPA}. We justify this, as the resulting squeezed state will be generated in the microwave circuit with a JPA that has in practice a non-zero noise contribution. We can write Alice's input state depending on her chosen encoding basis $\mathcal{B}_A \in \{q, p\}$ as

$$\bar{\mathbf{r}}_{\mathrm{A,q}} = \begin{pmatrix} \alpha_{\mathrm{i}} \\ 0 \end{pmatrix}, \quad \mathbf{V}_{\mathrm{A,q}} = \begin{pmatrix} V^{\mathrm{S}}_{\mathrm{A,q}} & 0 \\ 0 & V^{\mathrm{AS}}_{\mathrm{A,p}} \end{pmatrix} = \frac{1}{4}\begin{pmatrix} (1+2n_{\mathrm{JPA}})e^{-2r} & 0 \\ 0 & (1+2n_{\mathrm{JPA}})e^{2r} \end{pmatrix}, \tag{2.112}$$

$$\bar{\mathbf{r}}_{\mathrm{A,p}} = \begin{pmatrix} 0 \\ \alpha_{\mathrm{i}} \end{pmatrix}, \quad \mathbf{V}_{\mathrm{A,p}} = \begin{pmatrix} V^{\mathrm{AS}}_{\mathrm{A,q}} & 0 \\ 0 & V^{\mathrm{S}}_{\mathrm{A,p}} \end{pmatrix} = \frac{1}{4}\begin{pmatrix} (1+2n_{\mathrm{JPA}})e^{2r} & 0 \\ 0 & (1+2n_{\mathrm{JPA}})e^{-2r} \end{pmatrix}. \tag{2.113}$$

where α_i is the initial displacement amplitude chosen by Alice, and $V^{\mathrm{AS}}_{\mathrm{B,q}}$ is the antisqueezed (AS) variance of Alice's (A) q quadrature and $V^{\mathrm{S}}_{\mathrm{B,p}}$ is the squeezed (S) variance. Then, we can use the beam splitter model (see Eq. 2.111) which states that Bob's state has the same amplitude as Alice's in the limit of $\tau \to 1$. Respectively, we can write

$$\bar{\mathbf{r}}_{\mathrm{B,q}} = \begin{pmatrix} \sqrt{\tau}\alpha_{\mathrm{i}} \\ 0 \end{pmatrix}, \quad \mathbf{V}_{\mathrm{B,q}} = \begin{pmatrix} V^{\mathrm{S}}_{\mathrm{B,q}} & 0 \\ 0 & V^{\mathrm{AS}}_{\mathrm{B,p}} \end{pmatrix}, \tag{2.114}$$

$$\bar{\mathbf{r}}_{\mathrm{B,p}} = \begin{pmatrix} 0 \\ \sqrt{\tau}\alpha_{\mathrm{i}} \end{pmatrix}, \quad \mathbf{V}_{\mathrm{B,p}} = \begin{pmatrix} V^{\mathrm{AS}}_{\mathrm{B,q}} & 0 \\ 0 & V^{\mathrm{S}}_{\mathrm{B,p}} \end{pmatrix}, \tag{2.115}$$

where α_i is the initial displacement amplitude chosen by Alice and $V^{\mathrm{AS}}_{\mathrm{B,q}}$ is the antisqueezed (AS) variance of Bob's (B) q quadrature and $V^{\mathrm{S}}_{\mathrm{B,p}}$ is the squeezed (S) variance of p quadrature. The variances are defined as

$$V^{\mathrm{AS}}_{\mathrm{B,q}} = \tau\left(1+2n_{\mathrm{JPA}}\right)e^{2r}/4 + \bar{n} + (1-\tau)/4, \tag{2.116}$$

$$V^{\mathrm{S}}_{\mathrm{B,p}} = \tau\left(1+2n_{\mathrm{JPA}}\right)e^{-2r}/4 + \bar{n} + (1-\tau)/4. \tag{2.117}$$

Eve's input state $\hat{\rho}_{\mathrm{E,in}}$ is a two-mode squeezed vacuum state (see Eq. 2.36) with the variance $V_{\mathrm{TMSV}} = \cosh(2r) = 1 + 2n_{\mathrm{Eve}}$. If we assume that the encoding basis $\mathcal{B}_{\mathrm{A}} = q$, Eve's output state is then

$$\mathbf{V}_{\mathrm{E,q}} = \begin{pmatrix} V^{\mathrm{S}}_{\mathrm{E,q_1}} & 0 & \frac{1}{4}\sqrt{\tau}\Delta_{\bar{\mathrm{n}}} & 0 \\ 0 & V^{\mathrm{AS}}_{\mathrm{E,p_1}} & 0 & -\frac{1}{4}\sqrt{\tau}\Delta_{\bar{\mathrm{n}}} \\ \frac{1}{4}\sqrt{\tau}\Delta_{\bar{\mathrm{n}}} & 0 & \bar{n} & 0 \\ 0 & -\frac{1}{4}\sqrt{\tau}\Delta_{\bar{\mathrm{n}}} & 0 & \bar{n} \end{pmatrix}, \tag{2.118}$$

where $V^{\mathrm{S}}_{\mathrm{E,q_1}} = (1-\tau)\left(1+2n_{\mathrm{JPA}}\right)e^{-2r}/4 + \bar{n} + \tau/4$, $V^{\mathrm{AS}}_{\mathrm{E,p_1}} = (1-\tau)\left(1+2n_{\mathrm{JPA}}\right)e^{2r}/4 + \bar{n} + \tau/4$, and $\Delta_{\bar{\mathrm{n}}} = \sqrt{(4\bar{n})^2 - 1}$. If the encoding basis was $\mathcal{B}_{\mathrm{A}} = p$, only the variances $V^{\mathrm{S}}_{\mathrm{E,q_1}}$ and $V^{\mathrm{AS}}_{\mathrm{E,p_1}}$ are exchanged.

Calculation of Eve's Holevo information from the covariance matrix

In the previous section, we have presented the beam splitter model for the entangling cloner eavesdropping attack. Here, we can use this model to calculate the Holevo information analytically for direct (▶) and reverse reconciliation (◀) explicitly based on the methodology presented in Refs. 64, 136.

Eve's Holevo quantities for direct reconciliation $\chi_{\mathrm{E}}^{\blacktriangleright}$ and reverse reconciliation $\chi_{\mathrm{E}}^{\blacktriangleleft}$ are defined by using Eq. 2.100 as

$$\chi_{\mathrm{E}}^{\blacktriangleright} = S\left(\sum p_{\alpha_{\mathrm{i}}}\,\hat{\rho}_{\mathrm{E},\alpha_{\mathrm{i}}}\right) - \sum p_{\alpha_{\mathrm{i}}} S\left(\hat{\rho}_{\mathrm{E},\alpha_{\mathrm{i}}}\right), \tag{2.119}$$

$$\chi_{\mathrm{E}}^{\blacktriangleleft} = S\left(\sum p_{\beta_{\mathrm{i}}}\,\hat{\rho}_{\mathrm{E},\beta_{\mathrm{i}}}\right) - \sum p_{\beta_{\mathrm{i}}} S\left(\hat{\rho}_{\mathrm{E},\beta_{\mathrm{i}}}\right). \tag{2.120}$$

First, we note that due to the indistinguishable encoding schemes, the average state for all keys does not depend on the encoding basis (see Sec. 2.3.3) as

$$\hat{\rho}_{\mathrm{E,avg}} = \sum p_{\alpha_{\mathrm{i}}}\,\hat{\rho}_{\mathrm{E},\alpha_{\mathrm{i}}} = \sum p_{\beta_{\mathrm{i}}}\,\hat{\rho}_{\mathrm{E},\beta_{\mathrm{i}}}. \tag{2.121}$$

In general, the average density matrix $\hat{\rho}_{\mathrm{avg}} = \sum_{\mathrm{i}=1}^{\mathrm{M}} p_{\mathrm{i}}\hat{\rho}_{\mathrm{i}}$ can be computed as the p_{i}-weighted sum of states $\hat{\rho}_{\mathrm{i}}$. Therefore, we can write the average density matrix as

$$\hat{\rho}_{\mathrm{avg,E}} = \sum_{\mathcal{B}\in\{\mathrm{q,p}\}} \frac{1}{2}\int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma_{\mathrm{disp}}^2}} \exp\left(-\frac{x^2}{2\sigma_{\mathrm{disp}}^2}\right)\hat{\rho}_{\mathrm{E}}^{k_{\mathrm{i}}}\,\mathrm{d}k_{\mathrm{i}}. \tag{2.122}$$

where σ_{disp}^2 is the displacement variance, and $k_{\mathrm{i}} = \alpha_{\mathrm{i}}$ (▶) or $k_{\mathrm{i}} = \beta_{\mathrm{i}}$ (◀). The weighted probability of the encoding bases $\mathcal{B} \in \{q,p\}$ is assumed to be $1/2$.

We compute the von Neumann entropy by using the entropic function (see Eq. 2.71) of the symplectic eigenvalues of the covariance matrix (see Eq. 2.70). To obtain the average state in covariance matrix form, we use the property of the signal moments similar to average density matrices [49]

$$\left\langle(\hat{a}^\dagger)^m\hat{a}^n\right\rangle_{\mathrm{avg}} = \mathrm{Tr}\left((\hat{a}^\dagger)^m\hat{a}^n\,\hat{\rho}_{\mathrm{avg}}\right) = \sum_{\mathrm{i}=1}^{\mathrm{M}} p_{\mathrm{i}}\cdot\mathrm{Tr}\left((\hat{a}^\dagger)^m\hat{a}^n\,\hat{\rho}_{\mathrm{i}}\right) = \sum_{\mathrm{i}=1}^{\mathrm{M}} p_{\mathrm{i}}\cdot\left\langle(\hat{a}^\dagger)^m\hat{a}^n\right\rangle_{\mathrm{i}}, \tag{2.123}$$

where $\langle(\hat{a}^\dagger)^m\hat{a}^n\rangle_{\mathrm{avg}}$ is the $m,n\in\mathbb{N}_0$ signal moment for the average state $\hat{\rho}_{\mathrm{avg}}$, and $\langle(\hat{a}^\dagger)^m\hat{a}^n\rangle_{\mathrm{i}}$ is the same signal moment for the individual state $\hat{\rho}_{\mathrm{i}}$. Then, the covariance matrix of Eve's average state is

$$\mathbf{V}_{\mathrm{avg,E}} = \begin{pmatrix} V_{\mathrm{avg,E,1}} & 0 & \frac{1}{4}\sqrt{\tau}\Delta_{\bar{\mathrm{n}}} & 0 \\ 0 & V_{\mathrm{avg,E,1}} & 0 & -\frac{1}{4}\sqrt{\tau}\Delta_{\bar{\mathrm{n}}} \\ \frac{1}{4}\sqrt{\tau}\Delta_{\bar{\mathrm{n}}} & 0 & \bar{n} & 0 \\ 0 & -\frac{1}{4}\sqrt{\tau}\Delta_{\bar{\mathrm{n}}} & 0 & \bar{n} \end{pmatrix}, \tag{2.124}$$

where the variance for Eve's output mode of the beam splitter is quadrature independent $V_{\mathrm{avg,E,1}} = (1-\tau)\,(1+2n_{\mathrm{JPA}})\,e^{2r}/4 + \bar{n} + \tau/4$, with $\Delta_{\bar{\mathrm{n}}} = \sqrt{(4\bar{n})^2 - 1}$.

Finally, we have an analytical expression of the average covariance matrix (Eq. 2.124) and the quadrature-dependent covariance matrix. The information that Eve can maximally obtain is bounded by the Holevo information for direct ($\chi_{\mathrm{E}}^{\blacktriangleright}$) and reverse ($\chi_{\mathrm{E}}^{\blacktriangleleft}$) reconciliation as

$$\chi_{\mathrm{E}}^{\blacktriangleright} = S\left(\hat{\rho}_{\mathrm{E,avg}}\right) - \sum_{\mathcal{B}\in\{\mathrm{q,p}\}} \frac{1}{2}\int_{-\infty}^{\infty} f\left(\alpha_{\mathrm{i}}|0,\sigma_{\mathrm{disp}}^2\right)\, S\left(\hat{\rho}_{\mathrm{E},\mathcal{B}}^{\alpha_{\mathrm{i}}}\right)\, \mathrm{d}\alpha_{\mathrm{i}}, \tag{2.125}$$

$$\chi_{\mathrm{E}}^{\blacktriangleleft} = S\left(\hat{\rho}_{\mathrm{E,avg}}\right) - \sum_{\mathcal{B}\in\{\mathrm{q,p}\}} \frac{1}{2}\int_{-\infty}^{\infty} f\left(\beta_{\mathrm{i}}|0,\sigma_{\mathrm{disp}}^2\right)\, S\left(\hat{\rho}_{\mathrm{E},\mathcal{B}}^{\beta_{\mathrm{i}}}\right)\, \mathrm{d}\beta_{\mathrm{i}}, \tag{2.126}$$

where $f\left(\alpha_{\mathrm{i}}|0,\sigma_{\mathrm{disp}}^2\right)$ is the Gaussian probability density function distribution with the displacement variance σ_{disp}^2

$$f\left(\alpha_{\mathrm{i}}|0,\sigma_{\mathrm{disp}}^2\right) = \frac{1}{\sqrt{2\pi\sigma_{\mathrm{disp}}^2}} \exp\left(-\frac{\alpha_i^2}{2\sigma_{\mathrm{disp}}^2}\right). \tag{2.127}$$

2.3.6 Classical post-processing and secret key rate

The variables exchanged over the quantum channel need to be distilled to an error corrected, secure classical key. Classical post-processing is performed by Alice and Bob to meet this goal. The classical post-processing consists of three steps: sifting discards all symbols where Bob measured in a different basis than Alice's preparation basis; reconciliation uses the correlated information to distill a smaller, but error-corrected key based on Alice's sent key (direct reconciliation) or Bob's measured key (reverse reconciliation); privacy amplification discards a fraction of the key to limit the probability of successful eavesdropping attacks.

Sifting for matching bases

During the sifting, all measurements are discarded that were measured in the wrong basis $\mathcal{B} \in \{q, p\}$. This step is called sifting and has a typical efficiency of $\eta_{\mathrm{sift}} = 0.5$ for homodyne detection, as the probability is $1/2$ that Bob chooses randomly the same basis as Alice. Interestingly, it is in general not necessary to uniformly sample the bases $p_{\mathcal{B}_i} = 0.5$ [126]. Sifting is an active research field, where modern algorithms like the iterative sifting protocol are developed (see Ref. 137). The protocol with the currently highest sifting efficiency for a finite size key length was first proposed by Lo, Chau and Ardehali (LCA) [138]. The LCA sifting protocol relies on an asymmetric basis choice probability. A thorough security analysis for the LCA sifting protocol was performed by Pfister *et al.* [137], where it was found that a different parameter estimation subroutine is required to ensure perfect security. However, this protocol does not substantially exceed the Shor-Preskill efficiency $\eta_{\mathrm{sift}} = 0.5$

(first security proof for a QKD scheme in Ref. 32). Therefore, we assume in the following the lower bound $\eta_{\text{sift}} = 0.5$, which holds for asymptotic key length.

Information reconciliation of the noisy key

The information reconciliation processes the sifted noisy symbols that are shared between Alice and Bob and generates an error-corrected shared key of a smaller size. The reconciliation efficiency $\eta_{\text{rec}} = N_{\text{rec}}/N_{\text{noisy}}$ is the fraction between the original key size N_{noisy} and the reconciliated key N_{rec}. The number of error-corrected, correlated symbols over a noisy channel is limited by the mutual information [11]. In practice, common protocols like the low-density parity-check (LDPC) code achieve an efficiency of $\eta_{\text{rec}} = 86.7\,\%$ [139].

Privacy amplification

The last step of the classical post-processing is called privacy amplification. This process gets rid of compromised symbols by reducing the length of the key. From the estimated losses and noise in the quantum channel, Alice and Bob can estimate the amount of eavesdropping. This information is converted to a security parameter which reflects the risk that Eve obtained parts of the key [140]. Then, a two-universal symmetric hash function reduces the key and increases security [140].

Secret key rate

We define the secret key rate R (bits per symbol and second) as

$$R = f_{\text{r}} \eta_{\text{sift}} K, \tag{2.128}$$

where $K = \eta_{\text{rec}} I(\alpha{:}\beta) - \chi_{\text{E}}$ is the secret key, f_{r} is the repetition rate (number of channel usage per second), and and $\eta_{\text{sift}} \in [0, 1]$ is the sifting efficiency, which is the fraction of bits that are not discarded.

3 Experimental Techniques

In this chapter, we focus on technical requirements for a particular microwave CV-QKD protocol. In this context, a high fidelity single-shot microwave readout is one the central milestones.

This chapter starts with a description of our microwave CV-QKD protocol. Afterwards, we introduce a relevant cryogenic measurement setup, which includes a basic description of our dilution cryostat and microwave input and output lines. Later, we report on phase-sensitive amplification experiments with Josephson parametric amplifiers which serve as main building blocks of our investigations.

3.1 Implementation of squeezed-state CV-QKD protocol

A general goal of the microwave CV-QKD protocol is to communicate a secret key between the sender (Alice) and the receiver (Bob), which consists of a chain of symbols, i.e. continuous real numbers.

We implement the protocol presented in Sec. 2.3.1. This requires the implementation of Alice's preparation of squeezed displaced states (see Sec. 2.3.3), Bob's homodyne detection (see Sec. 2.3.4), and the effect of Eve's eavesdropping (see Sec. 2.3.5). A simplified schematic of our experimental setup is shown in Fig. 3.1. We use a first JPA to generate a propagating microwave squeezed state using a weak thermal state with an average temperature of $T = 40\,\mathrm{mK}$ as an input state. Then, we displace the previously squeezed state by applying a coherent tone to the weakly coupled port of directional coupler 1. The incident coherent tone is calibrated with respect to the induced displacement amplitude $|\alpha|$ and displacement angle $\theta = \arg(\alpha)$.

Instead of fully implementing the attacks as described in Sec. 2.3, we simulate its effect by inducing additional noise in Alice's cipher states. We achieve this, by coupling white Gaussian noise to the previous displaced squeezed states by using the second directional coupler. The coupled noise photon number, $\bar{n}$ is referenced to the output of directional coupler 2 and can be described with the highly asymmetric beam splitter model (see Eq. 2.1.3). Eve's thermal states are generated using an up-converted white Gaussian noise from an arbitrary function generator (AFG). Locally, such signal is equivalent to the entangling cloner eavesdropping attack, where Eve would couple a TMSV state to the cipher states. Using this local equivalence between the TMSV and thermal states, we can experimentally simulate the entangling cloner attack on our microwave CV-QKD protocol.

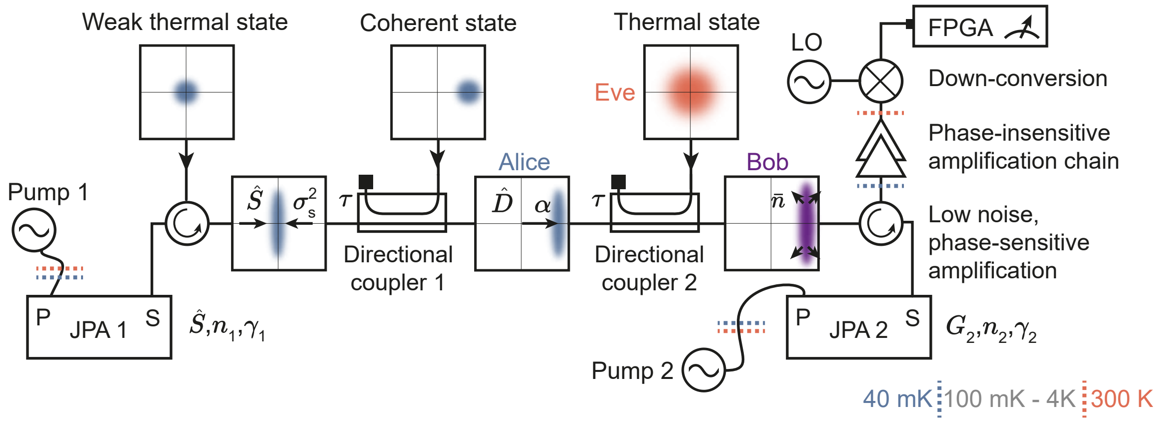

Figure 3.1: Signal flow in our experimental implementation of the microwave CV-QKD protocol. JPA 1 performs the squeezing operation, $\hat{S}$, with a squeezing angle γ_1. Directional coupler 1 implements the displacement operation $\hat{D}(\alpha)$ encoding a particular key element (symbol). The output state of directional coupler 1 represents Alice's cipher. In directional coupler 2, thermal noise $\bar{n}$ is coupled the cipher in order to simulate an eavesdropping attack by Eve. The resulting state is detected by the receiver, Bob. The detection chain consists of another JPA 2 with the gain G_2 and added noise n_2, followed by a cryogenic HEMT and room temperature amplifiers. Finally, the signal moments is down-converted and sampled by an FPGA. Colored boxes in the signal propagation line characterize Wigner functions of relevant microwave quantum states.

At the output of the second directional coupler, the signal can now be read out by Bob. The first step of the signal readout consists in a phase-sensitive amplification of the incoming signal in the same basis as the symbol was encoded. This phase-sensitive amplification is performed by driving JPA 2 with a strong coherent pump. The corresponding signal gain ($G_2 \sim 20\,\mathrm{dB}$) is large enough so that the signal-to-noise ratio is not significantly reduced by the noise of subsequent linear amplifiers. The microwave signals in the frequency range of around $5\,\mathrm{GHz}$ are down-converted to $11\,\mathrm{MHz}$ and subsequently sampled by an FPGA. The FPGA performs filtering and demodulation of the experimental signal, followed by calculation of statistical moments. The latter, in combination with a proper calibration (see Sec. 3.2.4), provide access to a partial or full tomography of the original microwave quantum state.

3.2 Cryogenic measurement setup

In order to operate superconducting microwave circuits in the quantum regime, we use a dilution cryostat to cool down our experimental set up to a temperature of 40 mK. In doing so, it also allows us to exploit superconducting coaxial NbTi cables with $T_\mathrm{c} = 9.8\,\mathrm{K}$ and characteristic losses around $1.0 \times 10^{-3}\,\mathrm{dB/m}$. More importantly, we need to consider the signal-to-noise ratio from a thermal point of view.

Our typical propagating microwave quantum states consist of a few photons. Assuming the named above frequency and temperature range, the Planck distribution can be used to

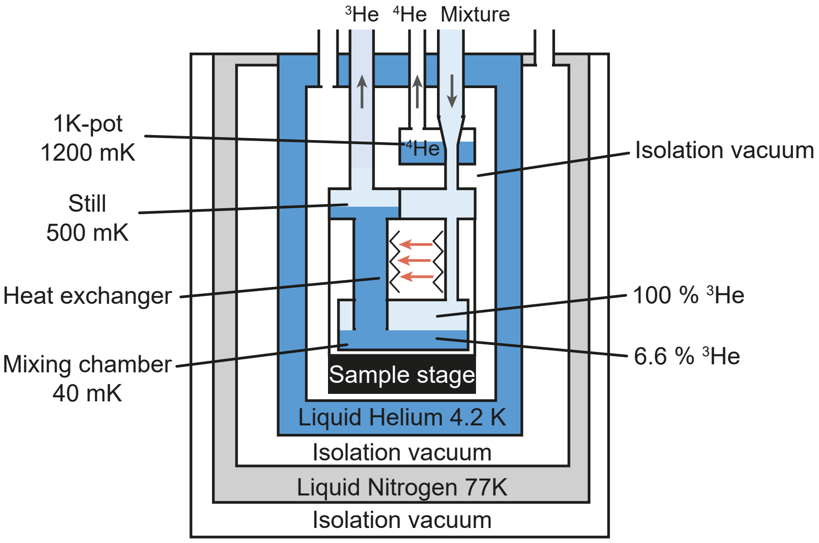

Figure 3.2: Schematic of a wet dilution refrigerator. The pre-cooled ^{3}He/^{4}He mixture enters the mixing chamber, where cooling to millekelvin temperatures is achieved by exploiting the dilution process of ^{3}He in the ^{3}He/^{4}He mixture.

estimate an average number of thermal photons per mode $\langle n \rangle$ as

$$\langle n \rangle = \frac{1}{\exp(\hbar\beta\omega) - 1}, \tag{3.1}$$

This results in a noise floor of $\langle n \rangle \leq 10^{-2}$ noise photons, where $\hbar$ is the Planck constant, ω is the frequency, $\beta = 1/(k_B T)$ is defined by the Boltzmann constant k_B and the temperature T.

In the following, we are going to present details of our cryogenic and room temperature microwave set up. Its central components are the dilution refrigerator, superconducting flux-driven JPAs, and room temperature microwave state reconstruction set up.

3.2.1 Wet dilution refrigerator

Here, we use a custom made wet dilution refrigerator based on the dilution process of ^{3}He in the ^{3}He/^{4}He mixture to achieve base temperatures around 10 mK. In particular, liquified nitrogen and helium pre-cool a mixing chamber, where ^{3}He is diluted in a ^{3}He/^{4}He phase.[1] As liquid Helium has a low latent heat [141], an efficient heat shielding from the room temperature environment is required. The cryostat used in this experiment was engineered at the Walther-Meißner-Institut. Its simplified schematic is shown in Fig. 3.2. It has several cooling stages. Each cooling stage limits the interaction with previous stages by making use of isolation vacuum. These insulation vacuum shields are formed by several nested dewars.

[1] Today's commercially available ^{3}He is as a byproduct of tritium generation in nuclear reactors:
$^6_3\text{Li} + ^1_0\text{n} \longrightarrow ^3_1\text{T} + ^4_2\text{He}$,
$^3_1\text{T} \xrightarrow{12.3\,\text{y}} ^3_2\text{He}^+ \; ^0_{-1}\text{e} + \nu$ [141]

The nitrogen dewar at $77\,\mathrm{K}$ pre-cools the helium dewar at $4.2\,\mathrm{K}$, which in turn contains the the third dewar (internal vacuum chamber) with the 1K-pot and ^{3}He/^{4}He mixing chamber.

The $^3\mathrm{He}/^4\mathrm{He}$ mixture is fed through all the aforementioned precooling stages and is gradually cooled down to temperatures below $1\,\mathrm{K}$, where the $^3\mathrm{He}$ evaporation cooling and dilution process start to take place. Below $0.87\,\mathrm{K}$, a ^{3}He/^{4}He mixture seperates into two phases: a ^{3}He-rich mixture, and a ^{3}He-poor phase. These phases are referred to as concentrated (near 100% ^{3}He) and dilute (6.6% ^{3}He) phase. In the mixing chamber, the ^{3}He rich mixture floats on top due to its lower density. The cooling power $\dot{Q}(T)$ is

$$\dot{Q}(T) = \dot{n}_3 \left[H_{3,d}(T) - H_{3,c}(T)\right], \tag{3.2}$$

where $\dot{n}_3$ (µmol/s) is the circulation rate of ^{3}He, and $H_{3,d}(T)$ and $H_{3,c}(T)$ the enthalpies of the diluted and concentrated phase. The resulting enthalpy difference is the energy required to transfer a ^{3}He atom from the concentrated into the dilute phase. This process is endothermic, as ^{3}He experiences a larger binding energy in the dilute phase due to a smaller zero point motion of ^{4}He atoms. This effect was experimentally quantified by Simon *et al.* [142, 143]. Unlike most two-phase liquids, there is a finite ^{3}He concentration in the dilute ^{3}He/^{4}He phase even at $T = 0\,\mathrm{K}$ [141].

The evaporating still has a higher temperature of $500\,\mathrm{mK}$. The resulting difference between the osmotic pressures of the mixing chamber and the ^{3}He evaporating still is sucking ^{3}He through the mixing chamber from the concentrated phase. This reflow of cold mixture is again used to pre-cool the diluted phase entering the mixing chamber over a heat exchanger. A detailed description of the cryostat can be found in Ref. 144. Further information on the physics of wet dilution refrigerators can be found in Pobell's book Ref. 141.

3.2.2 Cryogenic sample stage

In this section, we consider physical arrangement of components in the cryogenic setup. The sample stage is depicted in Fig. 3.3. There, the mixing chamber is providing cooling of the microwave set up to temperatures below $50\,\mathrm{mK}$. Microwave input and output lines are thermally anchored to all temperature stages in order to gradually thermalize related signals. The input line with a heatable attenuator is fed first into the circulator (Quinstar OXE89 SN 1603200002 from Low Noise Factory) at the bottom of the stage ①. There, it is connected to JPA 1 at the stage rear ②. Then, the signal line leads through two directional couplers ③ (Sirius Microwave SN E16944, Miteq SN E15876), where the first one is used for displacement of squeezed states, and the second one simulates Eve's entangling cloner attack by coupling a thermal signal. The top circulator ④ (Quinstar OXE89 SN 1519200003) interfaces with JPA 2 ⑤ with the output line ⑥ leading outside of the cryostat. Both JPAs were fabricated in RIKEN, Japan.

Our flux-driven JPAs are extremely magnetically sensitive devices and need to be shielded from stray magnetic flux. As JPA 1 sits back to back with the weakly magnetic circulator, an

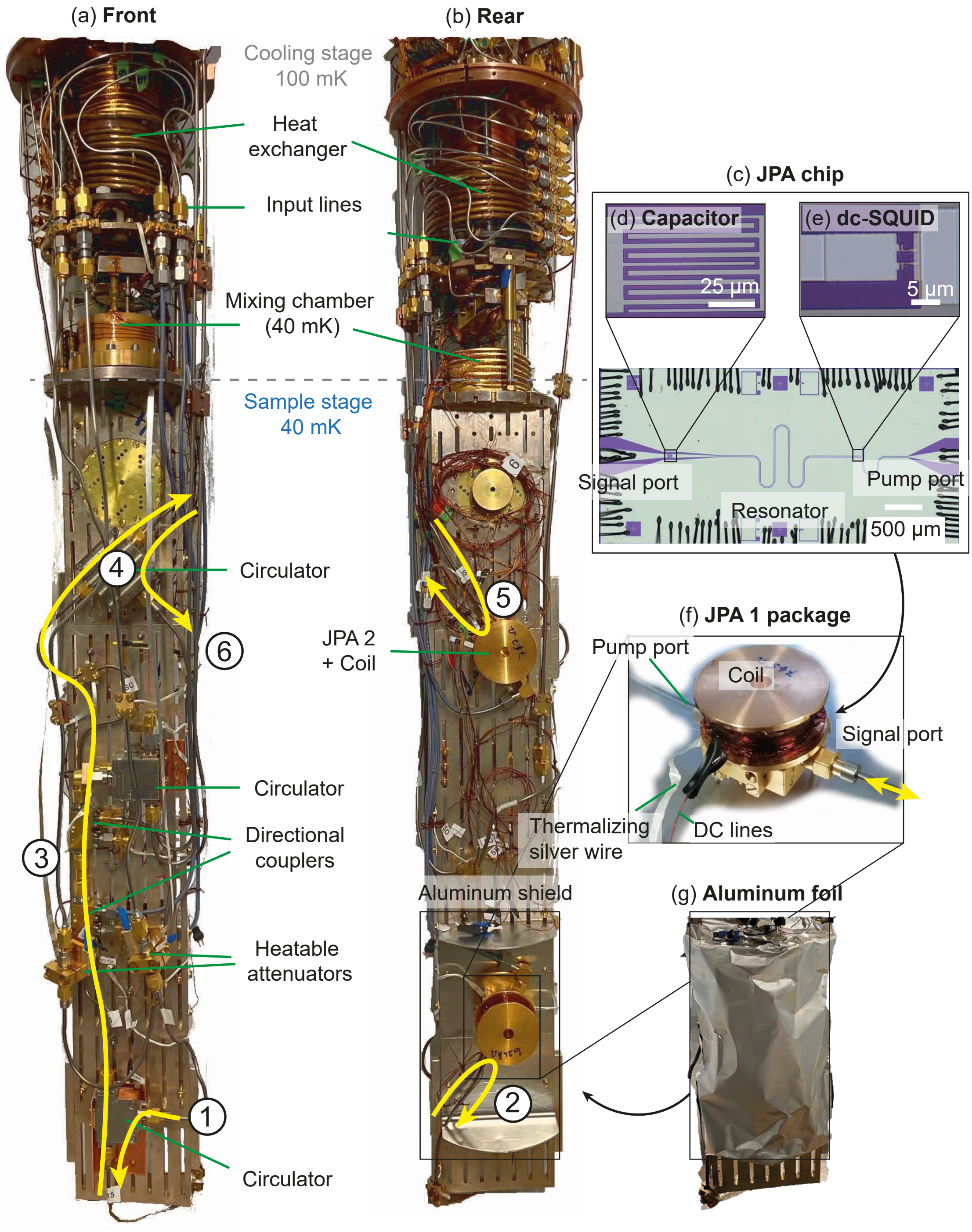

Figure 3.3: Photographs of the (a) rear sides and (b) back of the sample stage. (c) JPA chip with (d) the input capacitor and (e) dc-SQUID inside of the (f) JPA package, protected by the aluminum shield and (g) aluminum foil against stray magnetic fields.

aluminum shield is used in order to protect the JPA. This shield consists of a solid aluminum plate wrapped with an additional aluminum foil (see Fig. 3.3 (g)). The plate is mounted at the sample stage. The foil is wrapped around in order to leave small openings and allow for passing of incoming and outgoing microwave connections, as well as for a DC line for the JPA magnetic coil and the silver wires, which thermalize the JPA.

In our setup, we measure the JPAs in the reflection regime. Therefore, the signal port serves both as an input and output. The latter signals are separated by using a 3-port microwave nonreciprocal device (circulator). In Fig. 3.3 (f), the port to the left belongs to the pump line and introduces the pump tone to the JPA. A superconducting NbTi coil is mounted on top of the JPA sample box in order to provide stable and controllable magnetic flux, as required for the JPA frequency tuning.

Inside of the sample boxes, the JPA chips (see Sec. 2.2.5) are bonded to an internal printed circuit board (see Sec. 2.2.5 (c)) in order to provide a stable interface between the superconducting circuit and external coaxial cables. At the heart of the JPA chip, there is a CPW quarter-wavelength resonator short-circuited to ground with a dc-SQUID, as depicted in Fig. 3.3 (e).

3.2.3 Signal processing and data acquisition

Output microwave lines allow us to measure weak quantum signals coming from the sample stage. In particular, we are interested in the photon number of displaced squeezed states at the output of the second directional coupler (Bob's state). In Fig. 3.4, the upper half is showing the room temperature devices. The bottom part illustrates the cryogenic part.

Input microwave lines

Five input microwave lines lead into the cryostat. Input 4 is used to calibrate the working points of our JPAs. A coherent signal from a signal generator (SGS 100A, Rohde & Schwarz) through input 1 leads to the weakly coupled port of directional coupler 1; up-converted Gaussian white noise from an arbitrary function generator (81160A, Agilent Technologies) through input 3 leads to the weakly coupled port of directional coupler 2. The up-conversion is performed by using a harmonic mixer driven by a strong local oscillator (SGS 100A, Rohde & Schwarz) at the frequency around $5\,\mathrm{GHz}$. This step is necessary, as the AFG has a maximum bandwidth of $500\,\mathrm{MHz}$. Inputs 2 and 5 provide JPAs 1 and 2 with the pump tones.

All input lines are equipped with attenuators which are distributed across the different cooling stages. These attenuators function as power dividers and effectively allow to thermalize the intrinsic signal fluctuations to a temperature of the corresponding cryostat stage. This ultimately suppresses thermal noise population to around $n = 10^{-3}$ noise photons at the sample stage for signal frequencies of around $5\,\mathrm{GHz}$. In order to achieve this goal, one has to use high attenuation values, which correspond to high dissipated powers. Therefore, the bulk of this attenuation is placed above the $40\,\mathrm{mK}$ stage to avoid an excessive cryostat heating.

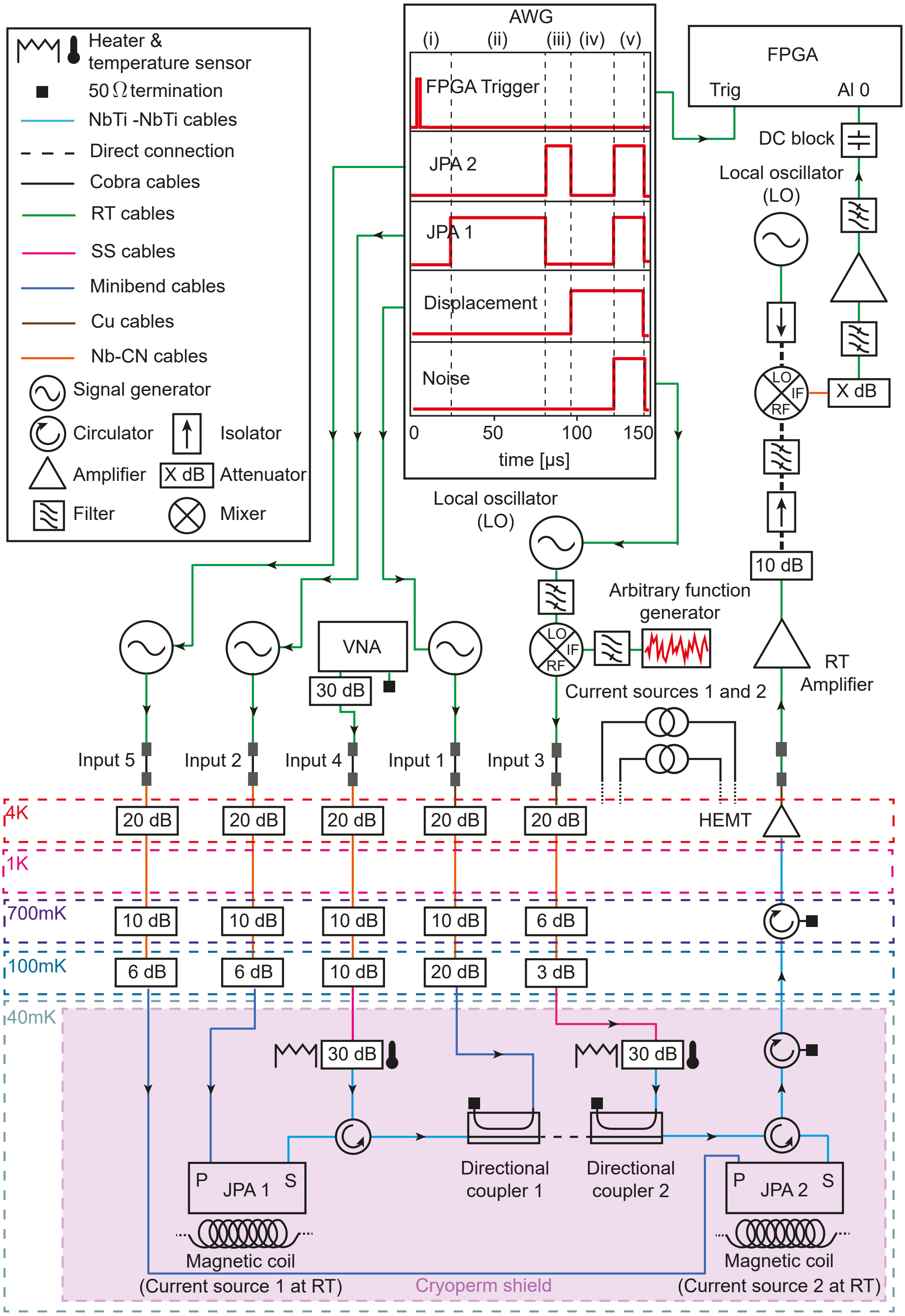

Figure 3.4: Microwave CV-QKD measurement setup. All microwave devices are referenced in chain to a rubidium 10 MHz clock. Magnetic coils on top of the JPAs are connected over dc lines to current sources 1 and 2. The Vector Network Analyzer (VNA) is used to calibrate the JPA working points. For quantum state reconstruction, the signal is down-converted to f_{IF}=11 MHz and digitized by the FPGA card.

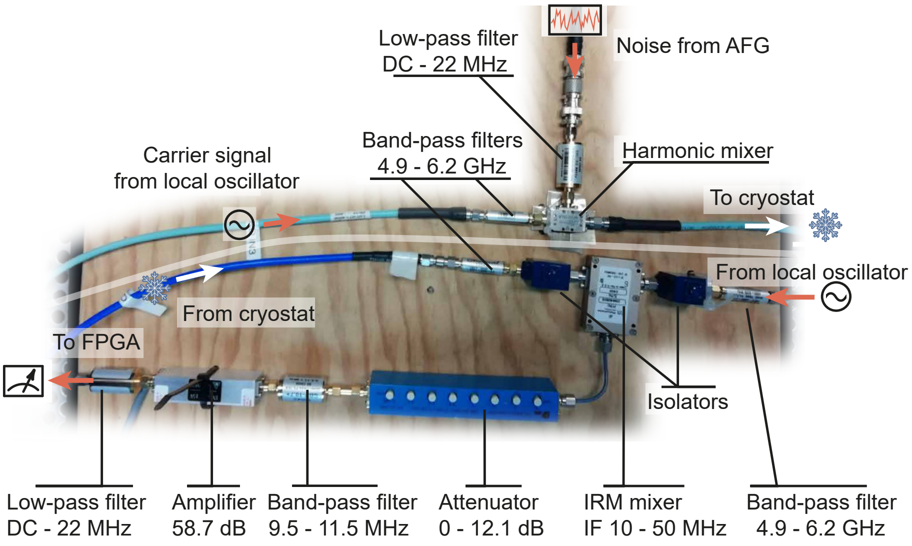

Figure 3.5: Room temperature microwave set up for the FPGA signal down-conversion & detection (bottom part) and the noise up-conversion (top part).

Output lines

In our experimental setup, we use a single output line, which is fed through two circulators mounted in series followed by a high-electron-mobility transistor (HEMT) amplifier (CLNA-C-0506-A TCA4003, TTI Inc.) with the average gain of $G_{\mathrm{H}} = 43\,\mathrm{dB}$ installed at the $4\,\mathrm{K}$ stage. Signals are subsequently amplifed by a room temperature amplifier with the gain of $G_1^{\mathrm{RT}} = 41.5\,\mathrm{dB}$ (AFS5, Miteq) to bring the signal power to a sufficiently high level for the FPGA sampling. The room temperature microwave set up can be seen in Fig. 3.5.The signal detection path goes through a band-pass filter of $4.9 - 6.2\,\mathrm{GHz}$ (VBFZ-5500+, Mini-circuits) is followed by an isolator (ECI04-5, EPX microwave). The filtered signal around $f_{\mathrm{RF}} = 5.5\,\mathrm{GHz}$ is down-converted using an image rejection mixer (IRM4080B, Polyphase microwave). This IRM mixer is driven by the local oscillator (SGS 100A, Rohde & Schwarz), which is set to the frequency $f_{\mathrm{LO}} = f_{\mathrm{RF}} + f_{\mathrm{IF}}$, such that $f_{\mathrm{IF}} = 11\,\mathrm{MHz}$. The IRM mixer is followed by a step attenuator (ESA2-1-10/8-SFSF, EPX microwave) to tune the resulting output power, if necessary, and avoid compression in the subsequent amplifier. After down-conversion, the signal carrier frequency is $f_{\mathrm{IF}} = 11\,\mathrm{MHz}$ and another band-pass filter (9.5 - 11.5 MHz) helps suppressing unwanted noise at the input of a low-frequency amplifier with the gain $G_2^{\mathrm{RT}} = 58.7\,\mathrm{dB}$ (AU 1447, Miteq). The step attenuator was also used to adjust the gain just below the maximum signal power $2.05\,\mathrm{Vpp}$ at the input of the FPGA to ensure the integrity of the device and to obtain the best dynamic range for the signal sampling. Finally, after passing through a low-pass filter, the signal is fed through a transceiver adapter module (NI 5782-02) which is mounted on the FPGA (NI PXIe 7975), where the signal is digitized.

Signal demodulation

The transceiver adapter module is sampling the down-converted ($11\,\mathrm{MHz}$) analog signal at the sampling rate of $f_\mathrm{S} = 250\,\mathrm{MHz}$ with the 14-bit vertical resolution. Three different channels are used: an analog input channel (AI 0) for the signal line, a trigger input (TRIG), which initiates the start of measurement traces, and an external reference channel (CLK IN) for the frequency synchronization. An arbitrary waveform generator (HDAWGG4, Zurich Instruments) supplies the trigger pulse for the FPGA and generates modulation waveforms for other devices as shown in Fig. 3.4.

The primary goal of the FPGA is to extract I and Q quadratures of the incoming signal. An internal digital local oscillator sitting at the same frequency $f_\mathrm{d} = f_\mathrm{IF}$ modulates the digitized IF signal $A(t_i)$ with numerically generated sine and cosine functions. The I and Q quadratures are the result of numerical integration of these functions

$$\begin{aligned} I &= 2f_\mathrm{IF}\sum_{\mathrm{i=1}}^{\mathrm{N}}\cos\left(2\pi f_\mathrm{IF}t_\mathrm{i}\right)A\left(t_\mathrm{i}\right)\Delta t,\\ Q &= 2f_\mathrm{IF}\sum_{\mathrm{i=1}}^{\mathrm{N}}\sin\left(2\pi f_\mathrm{IF}t_\mathrm{i}\right)A\left(t_\mathrm{i}\right)\Delta t. \end{aligned} \tag{3.3}$$

Here, $\Delta t = 8\,\mathrm{ns}$ is the sampling time, and the number of integration points is

$$N = \left\lfloor \frac{f_\mathrm{S}}{f_\mathrm{IF}} \right\rfloor, \tag{3.4}$$

which results in $N = 22$, considering that the FPGA samples at an effective sampling frequency of $f_\mathrm{S} = 250\,\mathrm{MHz}$. Then, the quadratures are filtered with a digital finite-impulse response (FIR) filter, which uses a Hamming window over 90 demodulated quadrature values. As a result, the ring-up time of the FIR filter is around $4\,\mathrm{ns} \times 22 \times 90 = 7.92\,\mathrm{\mu s}$, which determines the lower bound for the temporal length of our various modulation pulses, such as those used for JPAs, displacement, and noise.

Each triggering allows the FPGA to acquire 1650 quadrature values with a total duration of $145.2\,\mathrm{\mu s}$. After filtering and demodulation, the FPGA calculates the quadrature moments $\langle I^n Q^m \rangle$ with $n + m \leq 4, n, m \in \mathbb{N}_0$, as required for Gaussian quantum state tomography.

Pulse scheme

The pulse scheme can be seen at the top of Fig. 3.4. This scheme has four different calibration sections:

(i) Trigger the FPGA and aquire a well-calibrated **vacuum reference state** during the state when all other elements of the set up are switched off (see Sec. 2.1.3).

(ii) The second temporal window is used to measure a **squeezing angle** of the squeezed states generated by **JPA 1**. This squeezing angle can be stabilized around a predetermined value in subsequent measurements by adjusting the phase of the respective pump tone.

(iii) The same procedure is repeated for the **JPA 2 phase** stabilization to select which quadrature is amplified during the phase-sensitive amplification step.

(iv) The **displacement angle** of Alice's cipher state is measured. In the second measurement the angle is calibrated to align with the JPA's squeezing angles.

(v) All devices are operating. The samples acquired in this window provide measurement data for the CV-QKD protocol.

The trigger and modulation pulses are generated with an arbitrary waveform generator (HDAWGG4, Zurich Instruments). Except for the noise generation, all input signals are generated using SGS 100A microwave generators from Rohde & Schwarz. These devices are operated with a modulation voltage amplitude of $0.6\,\mathrm{V}$.

Reference state reconstruction

A well-defined vacuum reference state is crucial to analyze our signals and perform an accurate quantum state tomography. The method used here is based on the work from Ref. 145 and Ref. 146.

The reference state reconstruction uses a well-calibrated state as a reference measurement. In our experiments, this reference state corresponds to a weak thermal state emitted from a cold attenuator at the mean temperature of $T = 40\,\mathrm{mK}$. We define the complex envelope $\hat{\xi}_{\mathrm{ref}}$ of the amplified reference state as

$$\hat{\xi}_{\mathrm{ref}} = \sqrt{G}\left(\hat{v} + \hat{\mathrm{V}}\right), \tag{3.5}$$

where $\hat{V}$ describes the original thermal state, and G represents the gain of the amplification chain. The complex envelope function is calculated by using the measured quadratures $\hat{I}$ and $\hat{Q}$ (see Sec. 3.2.3), and κ, the photon number conversion factor (also see Sec. 3.2.4), as

$$\hat{\xi} = \frac{\hat{I} + i\hat{Q}}{\sqrt{\kappa}}. \tag{3.6}$$

We compute the moments $\left\langle (\hat{v}^{\dagger})^{\mathrm{m}}\hat{v}^{\mathrm{n}}\right\rangle$ of the weak thermal vacuum reference state $\hat{v}$, and the moments of the complex envelope function of the reference state $\left\langle (\hat{\xi}^{\dagger}_{\mathrm{ref}})^{\mathrm{m}}\hat{\xi}^{\mathrm{n}}_{\mathrm{ref}}\right\rangle$. After we have computed the amplification noise moments $\left\langle (\hat{V}^{\dagger})^{\mathrm{m}}\hat{V}^{\mathrm{n}}\right\rangle$, we can extract the signal moments from the complex envelope function of the signal. For our quantum states, the complex envelope function reads as

$$\hat{\xi}_{\mathrm{s}} = \sqrt{G}\left(\hat{a} + \hat{\mathrm{V}}\right), \tag{3.7}$$

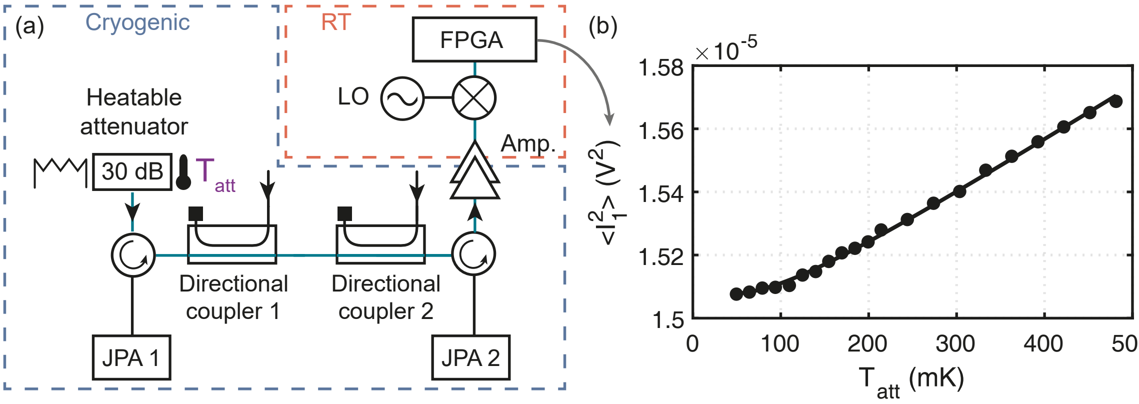

Figure 3.6: (a) Output line calibration measurement of the amplification chain. (b) Solid markers and black line represent experimental data and fit (Eq. 3.8) at the center frequency of $f_0 = 5.5231$ GHz with the detection bandwidth of 400 kHz.

where $\hat{a}$ represents a signal mode. From the complex envelope function moments $\langle (\hat{\xi}_s^\dagger)^m \hat{\xi}_s^n \rangle$ and the previously computed amplification noise moments $\langle (\hat{V}^\dagger)^n \hat{V}^m \rangle$, we can compute the signals moments $\langle (\hat{a}^\dagger)^n \hat{a}^m \rangle$. A detailed explanation can be found in Ref. 82.

3.2.4 Photon number conversion factor (PNCF)

We know only approximately by how much we amplify and attenuate the signal in our amplification chain. Therefore, we need a more precise method to associate an incoming signal power at the input of our FPGA with a specific photon number at a specific location of our cryogenic set up. Previously, we used the Planck distribution to calculate the average thermal photon number for a given temperature. We can use this knowledge by using a heatable attenuator which is set to a well-defined temperature. Then, this attenuator acts as a black-body emitter and generates a thermal signal with a well-defined average photon number, as shown in Fig. 3.6. This temperature and photon number are then related to the absolute output signal power measured at the FPGA. The result of this procedure is shown in Fig. 3.6 (b). The signal power is calculated from the quadrature second moments $\langle I^2 \rangle$ and $\langle Q^2 \rangle$, normalized to $R = 50\,\Omega$. When related to the predefined temperature at the 30-dB attenuator T_{att}, the signal power reads [82, 147]

$$P = \frac{\langle I^2 \rangle + \langle Q^2 \rangle}{R} = \frac{\kappa G}{R} \left[\frac{1}{2} \coth \left(\frac{h f_0}{2 k_B T_{\mathrm{att}}} \right) + n \right]. \tag{3.8}$$

The product between the photon number conversion factor and the gain κG defines the slope, while the total detection noise $n = n_I + n_Q$ corresponds to the offset in the I and Q quadrature. In this formula, h is the Planck constant, and f_0 is the center detection frequency. These two parameters can be determined by fitting the formula to the measured signal power while varying the temperature T_{att} of the attenuator. The resulting fit is shown in Fig. 3.6 (b). The resulting fitting parameters are shown in Tab. 3.1. From the

Moments	κG $[\mathrm{V}^2/\mathrm{photon}]$	n $[\mathrm{photon}]$
$\langle I^2 \rangle$	$1.490 \cdot 10^{-06} \pm 2.934 \cdot 10^{-08}$	9.868 ± 0.203
$\langle Q^2 \rangle$	$1.502 \cdot 10^{-06} \pm 2.934 \cdot 10^{-08}$	9.784 ± 0.199

Table 3.1: Fit parameters obtained from the exemplary PNCF measurement at the center frequency $f_0 = 5.5231\,\mathrm{GHz}$.

datasheet of the HEMT amplifier, we expect a total detection noise of around 20 noise photons. Evidently, our extracted noise photon number coincide well the expectations and are dominated by the HEMT noise. For these PNCF measurements, we can additionally take into account effects of losses along the signal path. If no losses are accounted for, the thermal signal power is referred directly to the output of the heatable attenuator, as well as the extracted PNCFs. However in our experiments, we need to reconstruct quantum states at various different points in the setup. To shift the reconstruction point, we have to estimate losses L (dB) between the output of the attenuator and the desired reconstruction point. Then, the effective gain referred to the output of the attenuator G_att is given by

$$G_\mathrm{att} = G_\mathrm{R} \cdot 10^{-\mathrm{L}/10}, \tag{3.9}$$

where G_R is referred to the desired reconstruction point. This procedure allows us to obtain an accurate estimation of PNCFs for an arbitrary point in our microwave cryogenic set up, provided that we can reliably estimate losses between this point and the heatable attenuator.

3.3 Working point

A working point is defined by the resonance frequency f_0 of the JPAs employed in the experiment. An optimal working point must allow for large squeezing levels with a purity close to unity for JPA 1. For JPA 2, we aim at obtaining high degenerate gain close to $20\,\mathrm{dB}$.

The JPA working point calibration consists of several steps. First, we start with the calibration of the JPAs by finding a possible resonance frequency for both our JPAs. This frequency should provide a high nondegenerate and degenerate gain. The frequency defines a center frequency for all other devices. Then, we calibrate the output line to relate the thermal noise temperature to a photon number (see Sec. 3.2.4). We calibrate the supplied power to the JPAs to analyze squeezing and purity. The power to the weakly coupled inputs of the directional couplers allow a calibration of Alice's cipher state displacement, Eve's added noise, and Bob's optimal amplification. Bob's detection efficiency is dependent on the signal power and pump power incident to JPA 2. In that regard, we characterize the quantum efficiency.

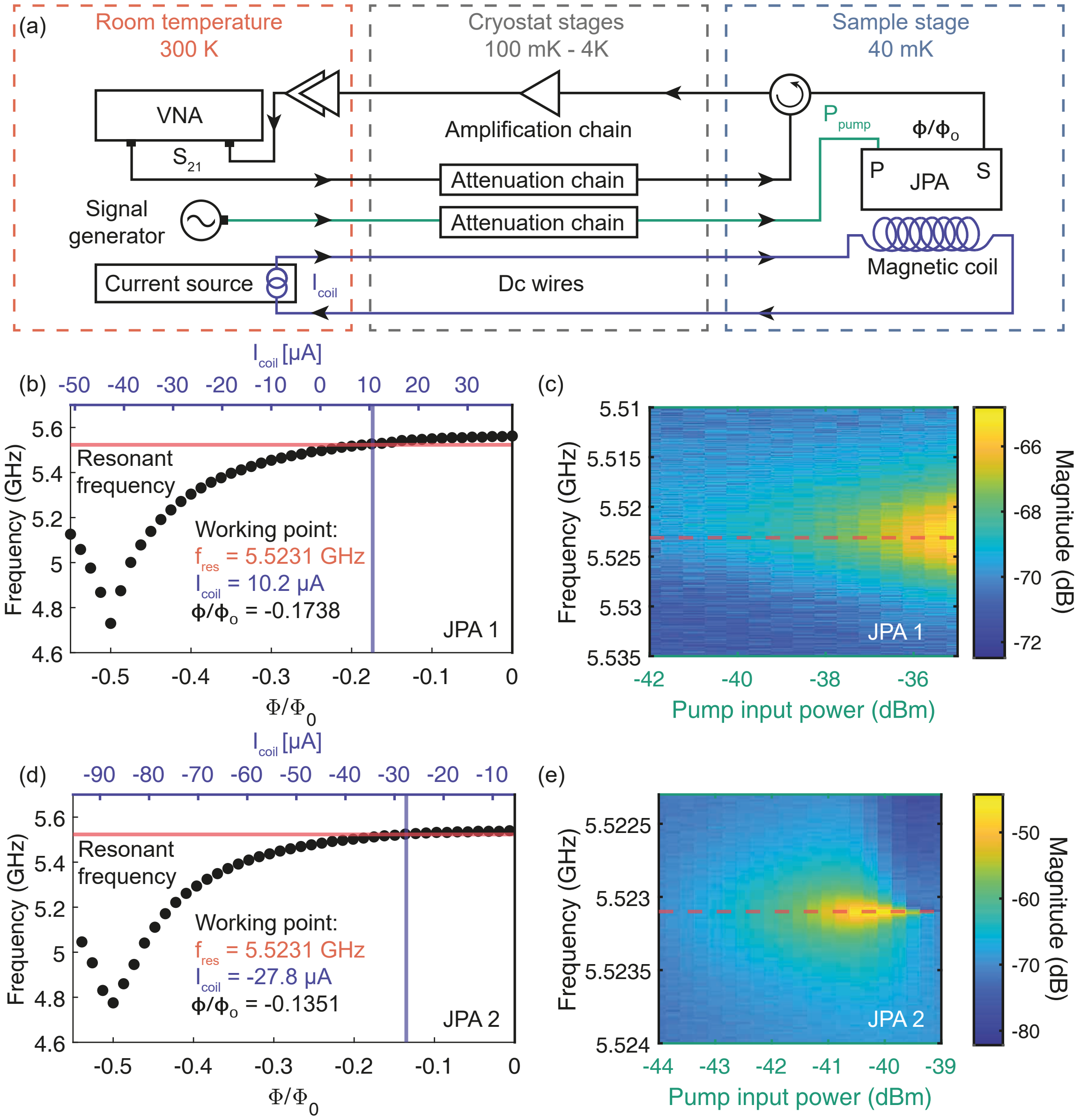

Figure 3.7: (a) JPA characterization scheme. The vector network analyzer (VNA) measures the magnitude and phase of the reflected signal from the JPA. (b) Flux-dependent resonant frequency of JPA 1. Solid markers represent resonant frequencies that are extracted from the frequency dependence of the reflection coefficient phase. (c) Pump power (green) sweep at the given working point for JPA 1 with a pump frequency of $f_{\text{pump}} = 11.0462\,\text{GHz}$ (d) Flux-dependent resonant frequency of JPA 2 tuned by the magnetic coil current (purple). (e) Pump power sweep at the given working point for JPA 2.

3.3.1 Flux-dependent JPA resonance frequency and nondegenerate gain

A systematic way to relate the dc magnetic flux Φ_{dc} to the applied coil current I_{coil} is to measure a frequency-dependent reflection coefficient from the JPA with a vector network analyzer (VNA) versus a varied coil current as depicted in Fig. 3.7 (a). By measuring a corresponding S-parameter, the JPA's resonant frequency can be identified by its induced phase shift and frequency dependent amplitude response. The flux dependence of the resonant frequency is shown in Fig. 3.7 (b) for JPA 1 and Fig. 3.7 (d) for JPA 2. On the lower x-axis, the total flux Φ/Φ_0 shows the characteristic periodicity that is expected for a dc-SQUID.

Next, for a given resonant frequency, the coil current is fixed to stabilize the JPA frequency at the chosen frequency f_0 and the pump tone is applied at the double frequency of $2f_0$. Then, the pump frequency is fine-tuned around $2f_0$ in order to achieve symmetric amplification response with up to 10 dB of gain. The only free parameter left after this procedure is the pump power, which is swept in a certain range of powers in order to verify the JPA gain response. Exemplary sweeps can be seen in Fig. 3.7 (c) for JPA 1 and (e) for JPA 2.

Finally, we need to fix the pump power $\mathrm{P}_{\mathrm{pump}}$. The JPA gain increases for higher pump powers, until nonlinear effects (see Ref. 148) start to manifest, preventing the JPA operation as a linear amplifier. This effect can be seen after $-39.5\,\mathrm{dBm}$ applied to the pump port of JPA 2 in Fig. 3.7 (e). The working point corresponding to the JPAs frequencies of $f_0 = 5.5231\,\mathrm{GHz}$ was used throughout the thesis and serves as a basis for further calibrations.

3.3.2 Squeezing and purity measurement

The calibration of the squeezing level in JPA 1 is important for the CV-QKD protocol, as the overall key variance depends both on the displacement amplitude and squeezing level. A high squeezing level enables high displacement amplitudes, and respectively, high secret key rates.

For the measurement, we use the working point $f_0 = 5.5231\,\mathrm{GHz}$, by tuning the coil current $I_{\mathrm{coil}} = -27.8\,\mu\mathrm{A}$ as described above and sweep the pump tone power, at the frequency of $2f_0$, between $-55\,\mathrm{dBm}$ and $-25\,\mathrm{dBm}$ referred to the JPA pump port. Instead of using the VNA for probing of the JPA, we send a weak thermal state from the mixing chamber attenuator to the JPA input, as illustrated in Fig. 3.8 (a). We use the reference state reconstruction method introduced in Sec. 3.2.3 to analyze the squeezed states. The squeezing level and purity is computed from the quadrature moments measured by the FPGA and are plotted in Fig. 3.8 (b). The target squeezing angle is set to $\gamma = 45°$, and shows a low variance of around $\pm 1°$ for the different pump powers. The squeezing level S and purity μ are calculated as [64]

$$S = 10 \log_{10} \left(\frac{\sigma_{\mathrm{S}}^2}{0.25} \right), \quad \mu = \frac{1}{4^N \sqrt{\det(\mathbf{V})}}, \tag{3.10}$$

where 0.25 represents the variance of vacuum fluctuations, σ_{S}^2 corresponds to the reconstructed squeezed variance, and $\mathbf{V}$ is the covariance matrix of the reconstructed state.

Higher-order nonlinear effects lead to a break down of the JPA squeezing operation, as observable at high pump powers, $P_{\mathrm{pump}} > -35\,\mathrm{dBm}$ in Fig. 3.8 (b). These effects force the JPA in a non-Gaussian regime of operation. For a more detailed description the reader is referred to Ref. 148 and Ref. 149.

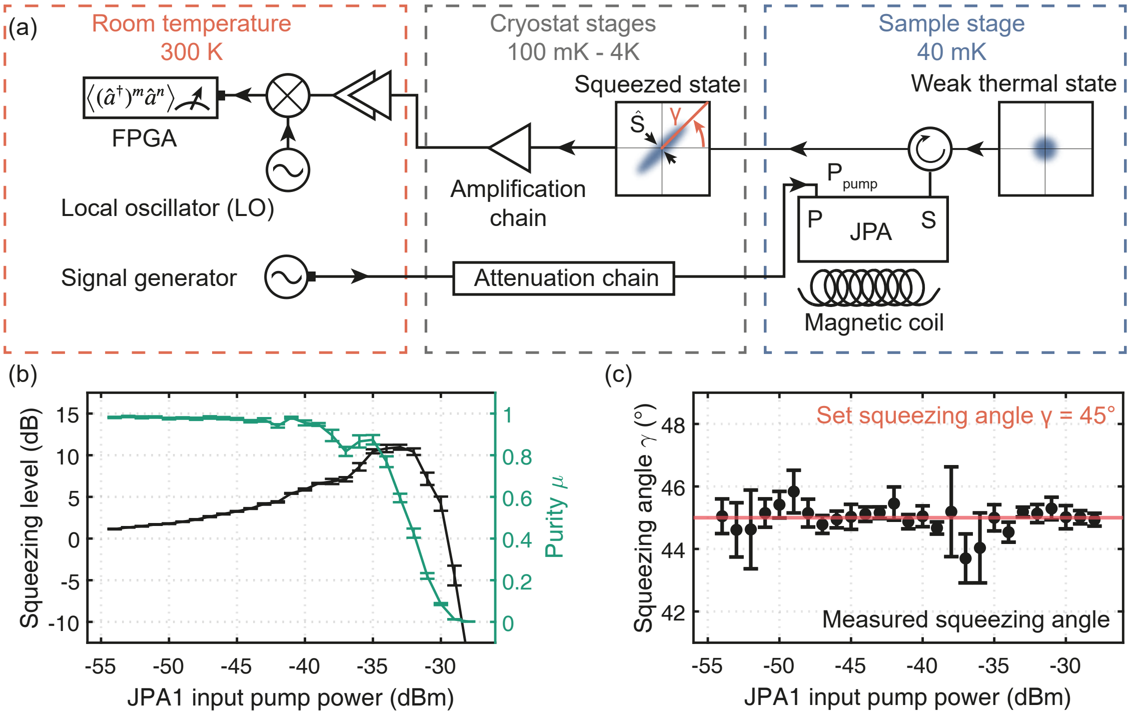

Figure 3.8: (a) Schematic for the squeezing measurements. A weak thermal state is squeezed by the pumped JPA. The FPGA extracts the output signal moments and, by using the PNCF calibration, converts them to the squeezed quadrature variance σ_s^2 and squeezing angle γ. (b) Exemplary squeezing and purity measurement versus the pump power referenced to the input of the JPA at the working point frequency $f_0 = 5.5231\,\text{GHz}$, and the pump frequency $f_\text{pump} = 11.0462\,\text{GHz}$. (c) Squeezing angle versus the pump power.

During the CV-QKD protocol we stabilize the squeezing angle by establishing a feedback loop between a reconstructed angle based on relatively low averaging numbers. Within this feedback loop we adjust the phase of the JPA pump signal. The pump phase is changed by $\Delta\gamma = 2\,(\gamma_\text{set} - \gamma_\text{meas})$, where γ_set is the target phase and γ_meas is the measured phase. For the power calibration measurement shown in Fig. 3.10, we use the set angle of $\gamma_\text{set} = 45°$.

The measurement results displayed in Fig. 3.8 (b), (c) can be obtained when JPA 2 is detuned from the working point frequency f_0 to avoid its extra attenuation of signal transmission near its resonant frequency. However, the protocol for degenerate amplification requires a calibration of the squeezing angle of JPA 1, while both JPAs are tuned to the resonant frequency $f_0 = 5.5231\,\text{GHz}$. When not pumped, JPA 2 has a noticeable insertion loss of around $10\,\text{dB}$ which makes the squeezing angle stabilization more difficult, as it reduces the corresponding SNR and precision of angle stabilization. As a result, we have to adapt the pulse sequence and increase the JPA 1 pulse duration to compensate for the poor signal power due to attenuation by JPA 2. In Fig. 3.9, we demonstrate that we are able to stabilize the squeezing angle of JPA 1 by using 3×10^6 averaged traces N_avg to an accuracy of $\pm 2°$ even in this unfavorable regime.

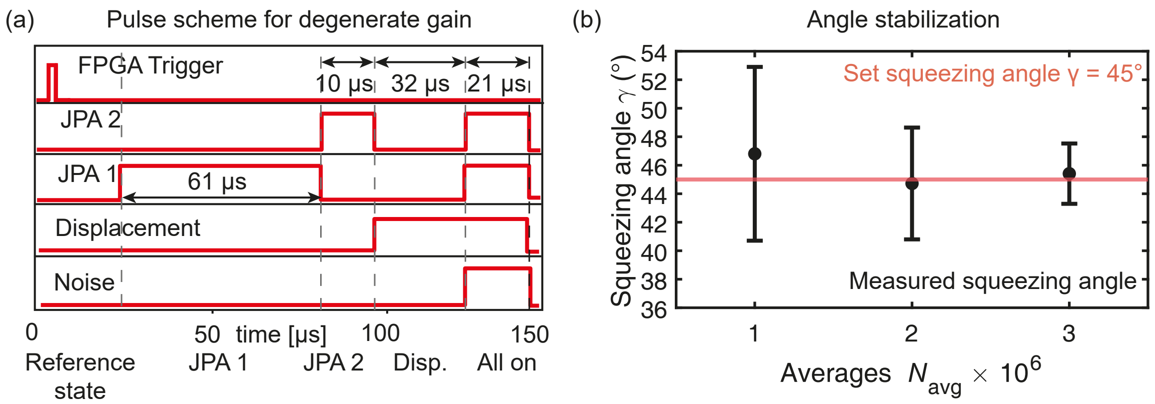

Figure 3.9: (a) Pulse scheme for the experimental implementation of the microwave CV-QKD protocol. Amplitude of each modulation pulse is set to $0.6\,\mathrm{V}$. (b) Angle stabilization measurement for JPA 1. The standard deviation for the squeezing angle of JPA 1 is sufficiently small for three million averages, reaching a deviation of $\pm 2^\circ$ around the setpoint.

3.3.3 Displacement calibration

In our CV-QKD protocol, we encode key symbols in the displacement amplitude of propagating displaced squeezed states. The displacement operator $\hat{D}(\alpha)$ (see Sec. 2.1.3) is implemented by coupling the squeezed state to a coherent tone via a cryogenic directional coupler. Hence, we need to calibrate how much input power is needed to displace the state by a certain number of photons. In the measurement displayed in Fig. 3.10 (a), we perform the displacement on an incident weak thermal state coming from the heatable attenuator. Similar to the squeezing stabilization measurements we have to stabilize the displacement angle in order to compensate for drifts in long measurements. This is achieved by introducing yet another feedback loop and changing the coherent tone phase by $\Delta\theta = \theta_{\mathrm{set}} - \theta_{\mathrm{meas}}$, where θ_{meas} is the reconstructed displacement phase from the previous iteration, and θ_{set} is the set point displacement phase (see Fig. 3.10 (c)).

Figure 3.10 (b) illustrates that in the range of displacement powers we need, the purity of the resulting displaced state remains close to 1, deviating only by $\sim 4\,\%$ from unity.The amount of displacement photons is computed via the reference state construction method, as described in Sec. 3.2.3. Corresponding data points are fitted with a linear noise model

$$n_{\mathrm{d}} = m_{\mathrm{d}}\, P_{\mathrm{coh}} + p_{\mathrm{d}}, \tag{3.11}$$

which we use to estimate the amount of displacement photons throughout the measurements.

Fig. 3.10 (c) shows that the measured displacement angles agree well with the target displacement angles. This ensures that the states can be displaced with the well-controlled displacement amplitude and displacement angle.

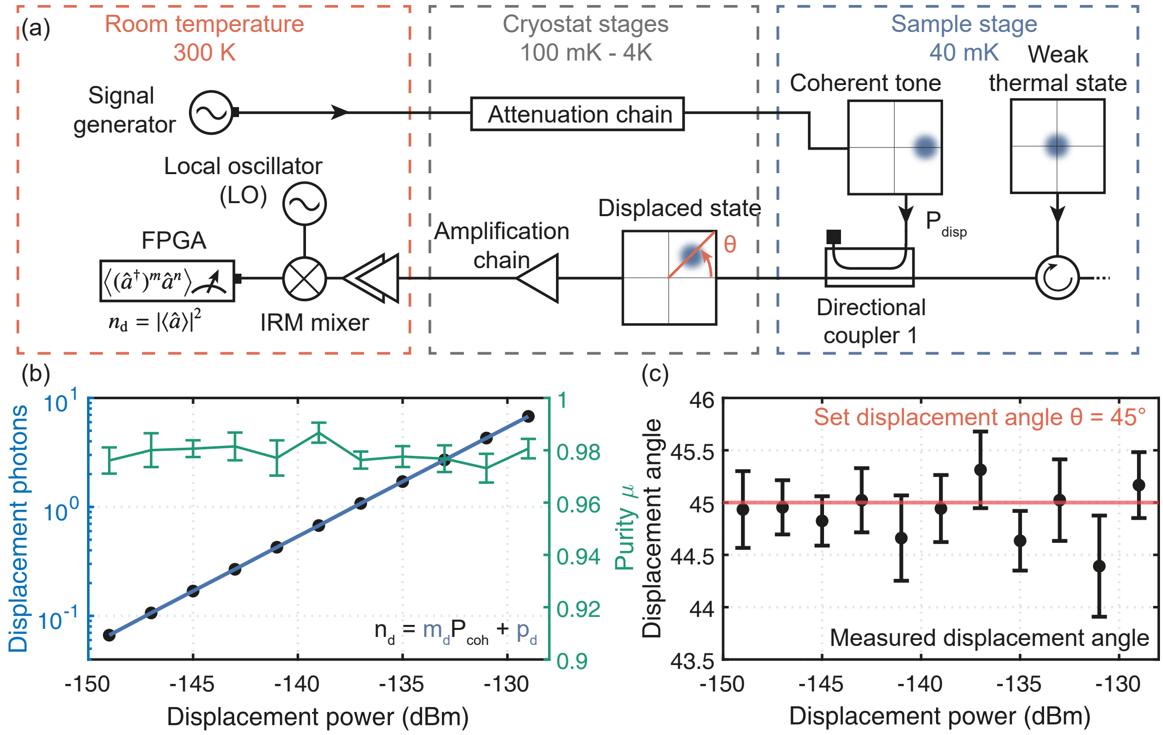

Figure 3.10: (a) Measurement scheme for displacement power calibration at the first directional coupler. (b) Displacement photon number $n_\mathrm{d} = |\langle\hat{a}\rangle|^2$ versus input power at the output of directional coupler 1. The fit parameters are $m_d = 4.66 \times 10^{-11} \pm 2.8^{-14}$, $p_d = 9.54 \times 10^{-15} \pm < 10^{-14}$. (c) Displacement angle for different powers.

3.3.4 Noise calibration

The second directional coupler simulates an eavesdropping attack as described in Sec. 2.3.5. To this end, we generate white Gaussian noise, approximating a thermal state, and couple it by a second cryogenic directional coupler to incoming propagating signals, as depicted in Fig. 3.11 (a). The artificial noise signal from an arbitrary function generator (81160A, Agilent Technologies) is up-converted to a carrier frequency of around 5 GHz by mixing the initial noise signal with a strong local oscillator at the harmonic mixer. The noise photon number, $n_n = \langle\hat{a}^\dagger\hat{a}\rangle$, is extracted from the signal moments measured at the FPGA. The purity of the noisy state rapidly decreases as the input voltage from the AFG is increased, as shown in Fig. 3.11 (b). The resulting noise photon dependency can be fitted with the linear model

$$n_\mathrm{n} = m_\mathrm{n}\, V_\mathrm{pp}^2 + p_\mathrm{n}, \tag{3.12}$$

where V_pp is the peak-to-peak voltage of the noise source and m_n, p_n are the fitting parameters. For plotting, the value of V_pp is converted to dBm units, referred to the weakly coupled port of the second directional coupler. The added variance to Alice's cipher state can be

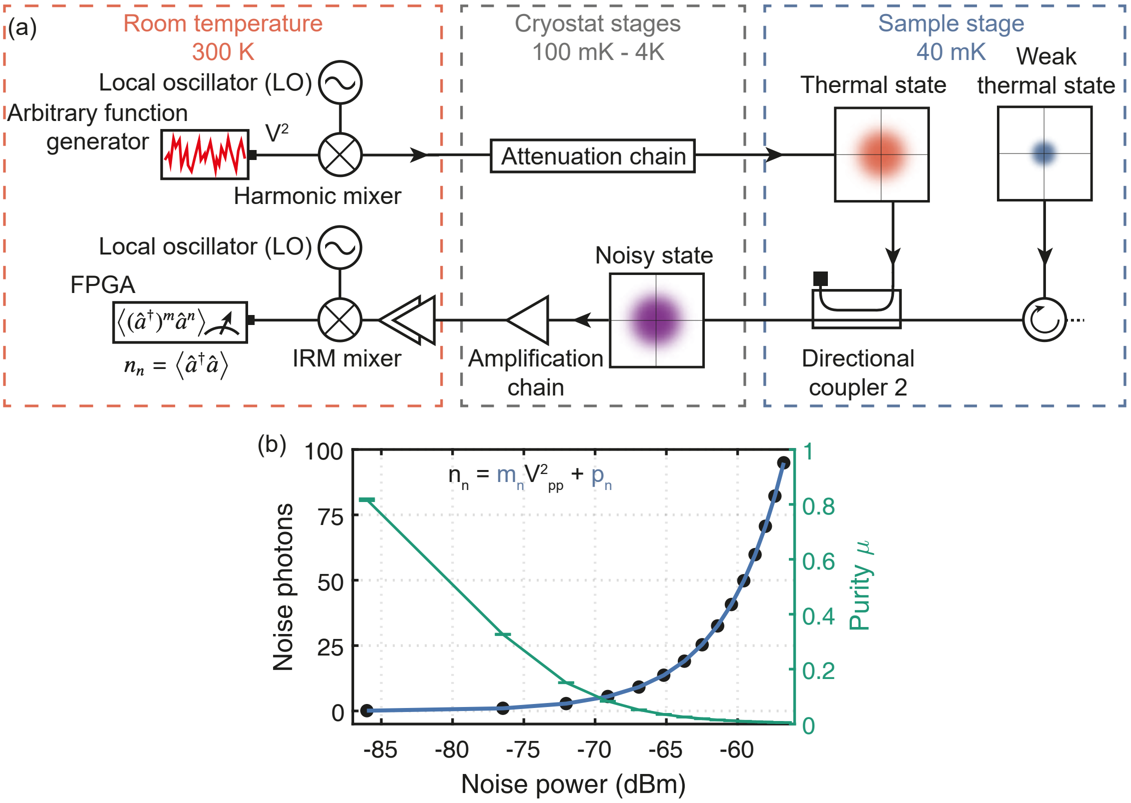

Figure 3.11: (a) Measurement scheme for the AWG noise calibration. (b) Exemplary calibration data of the average noise photon number versus the noise power (dBm) at the weakly coupled port of the directional coupler 2 and fitting parameters $m_n = 4.52 \times 10^1 \pm 2.22 \times 10^{-2}$, $p_n = -0.01 \pm 2.2 \times 10^{-2}$.

computed by using the relation

$$(1-\tau)V_E = (1-\tau)\frac{1}{4}(1+2n_{\mathrm{Eve}}) = \frac{1}{4}(1-\tau) + \bar{n}, \tag{3.13}$$

where n_{Eve} is average noise photon number, coming from Eve's side, and $\bar{n}$ is the effective coupled noise added to Alice's state.

3.3.5 Degenerate gain

The phase-sensitive amplification implemented at Bob's side is crucial to obtain a high signal-to-noise ratio and reach the single-shot readout regime. Fig. 3.12 (a) displays the schematic for the degenerate gain measurements of JPA 2.

In our implementation of the CV-QKD protocol, JPA 2 is used as a quantum-limited amplifier in the phase-sensitive regime. To study its degenerate gain, we use a coherent tone as an input signal and sweep the phase of the coherent tone from 0 to 180°. As shown in Fig. 3.12 (b), the JPA 2 response is a π-periodic function of the input coherent phase. The maxima for each pump power are visualized in Fig. 3.12 (c). Here, we achieve a maximum degenerate gain of up to 32 dB. However, this is possible only for the weak input signals with

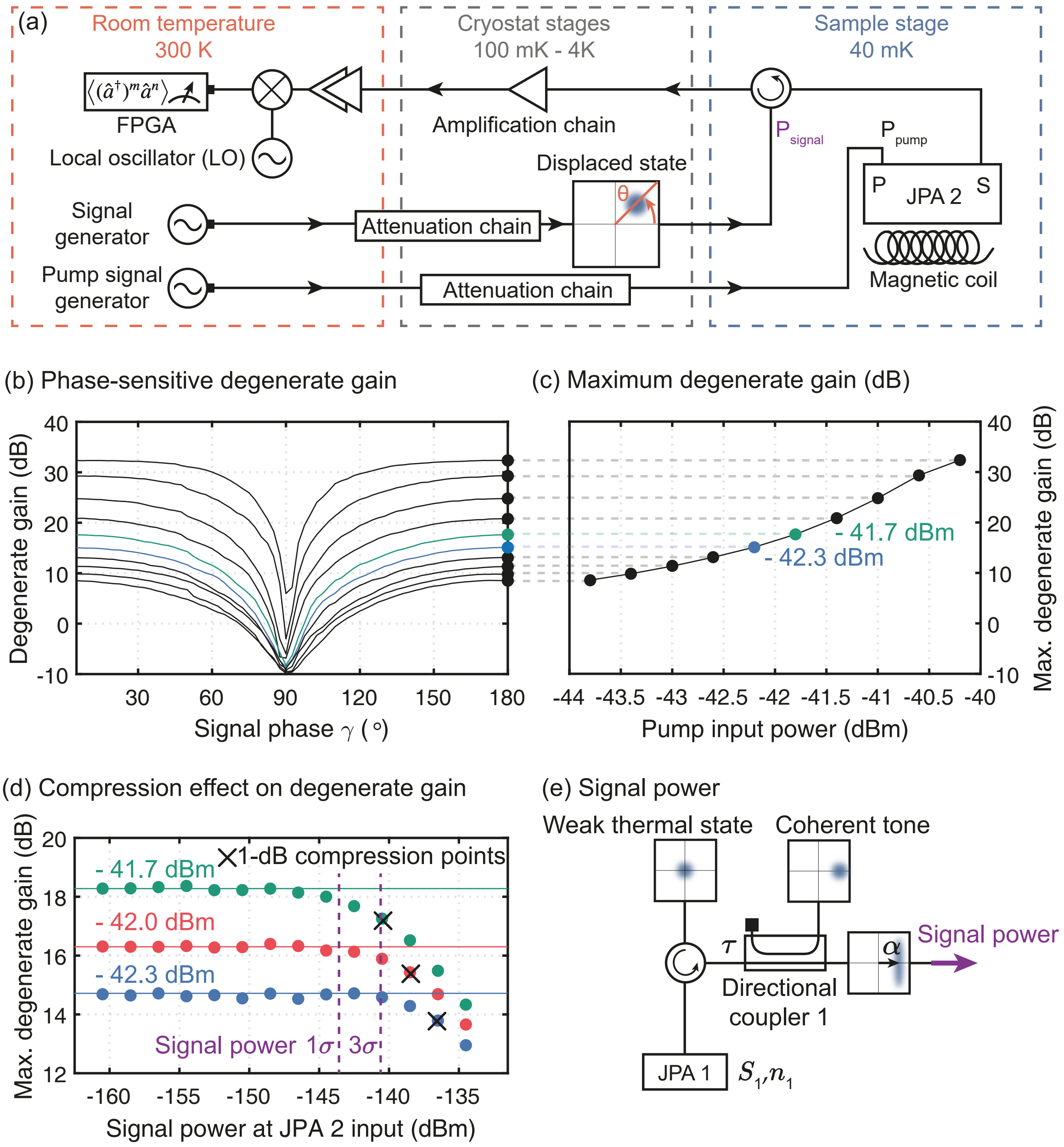

Figure 3.12: (a) Experimental scheme for JPA degenerate gain measurements. (b) Phase-sensitive degenerate gain. (c) Maximum degenerate gain. (d) Characterization of the JPA 1-dB gain compression in the degenerate regime. (e) Signal power of a cipher state by Alice, considering a displacement of 3σ.

less than $-140\,\mathrm{dB\,m}$ signal power. For higher powers, JPA 2 starts to slowly enter a nonlinear amplification regime and stops being useful for our purposes. This effect can be investigated by varying the input power and observing the resulting gain, as shown in Fig. 3.12 (d). Here, we use the 1-dB compression criterion which indicates that the signal gain decreased by $1\,\mathrm{dB}$ from its maximal value, in order to characterize maximally acceptable input powers for JPA 2. Finite 1-dB compression powers arise from higher-order nonlinear effects in JPAs which destroy Gaussianity of the incident states. Gaussianity implies that the third and fourth order cumulants ($n + m \geq 3$) are close to zero [145], which can be used as witness values to measure departure from the Gaussian character in amplified states. Also, the covariance matrix formalism, which we use to analyze displacements and variances of the microwave states, relies on the condition that our quantum states can be treated as Gaussian states, as the covariance matrix is only computed from second order moments. A detailed discussion of higher-order nonlinear effects leading to compression is presented in Ref. 148.

In order to identify an optimal pump power for JPA 2, we first need to estimate a maximum photon number in the incident states during the execution of our CV-QKD protocol. In Fig. 3.12 (e), a simplified circuit shows the signal line leading to the first directional coupler. As we sample the symbols from a Gaussian distribution $\mathcal{N}(0, \sigma^2_{\text{disp}})$, sometimes, the corresponding photon numbers and power will be very large, because Gaussian distributions have a infinite domain of definition. However, we can choose the variance of the Gaussian distribution such that 99.7% of the resulting displaced squeezed states incident to JPA 2 do not induce compression effects. This corresponds to a 3σ interval of a Gaussian distribution. Thus, the maximal tolerable displacement photons during the experiments are calculated by using a high-power cipher state at 3σ of the Gaussian distribution. We denote the corresponding signal photon number as $n_{3\sigma}$ and choose the circulator at JPA 2 as reference point. The average photon number of a squeezed displaced state is $n = |\alpha|^2 + \sinh^2(r)$. For the high-power cipher state, we set the displacement to 3σ, so that its photon number is $n_{3\sigma} = (3\tau\sigma_{\text{disp}})^2 + \sinh^2(r)$, where $\tau = 1 - 10^{-c/10} = 0.99$ and $c = 20\,\text{dB}$ is the coupling constant for the directional couplers, r is the squeezing factor, and σ^2_{disp} the sample variance of the Gaussian distribution from which the displacement amplitudes are sampled.

The displacement variance σ^2_{disp} corresponds to a squeezing level S, as these quantities need to fulfill the condition for indistinguishable bases, as discussed in Sec. 2.3.3. In the experiment, we decide for a squeezing level of $S = 5.2\,\text{dB}$. As a result, we have a corresponding displacement photon number sample variance of $\sigma^2_{\text{disp}} = 1.4$. As a result we need to choose a corresponding squeezing factor of $r = S/(20\log_{10}(e)) = 0.59$. This results in a total 3σ photon level $n_{3\sigma}$ of $n_{3\sigma} = 12.94$. Finally, we can compute the signal power P_{sig} for this photon number $n_{3\sigma}$ using

$$P_{\text{sig},3\sigma} = Bhfn_{3\sigma} = 6.087 \times 10^{-18}\text{W} = -142.16\,\text{dBm}, \tag{3.14}$$

with the bandwidth $B = 400\,\text{kHz}$, the Planck constant h, and the signal frequency $f = 5.5231\,\text{GHz}$. The resulting signal power of $-143.29\,\text{dBm}$ is marked by the dashed purple line in Fig. 3.12 (d). In conclusion, we are below the compression limit for the lowest pump power of $-42.3\,\text{dBm}$, which is indicated in blue. For the higher powers $-42.0\,\text{dBm}$ (red) and $-41.7\,\text{dBm}$ (green), the compression effect is already decreasing the degenerate gain.

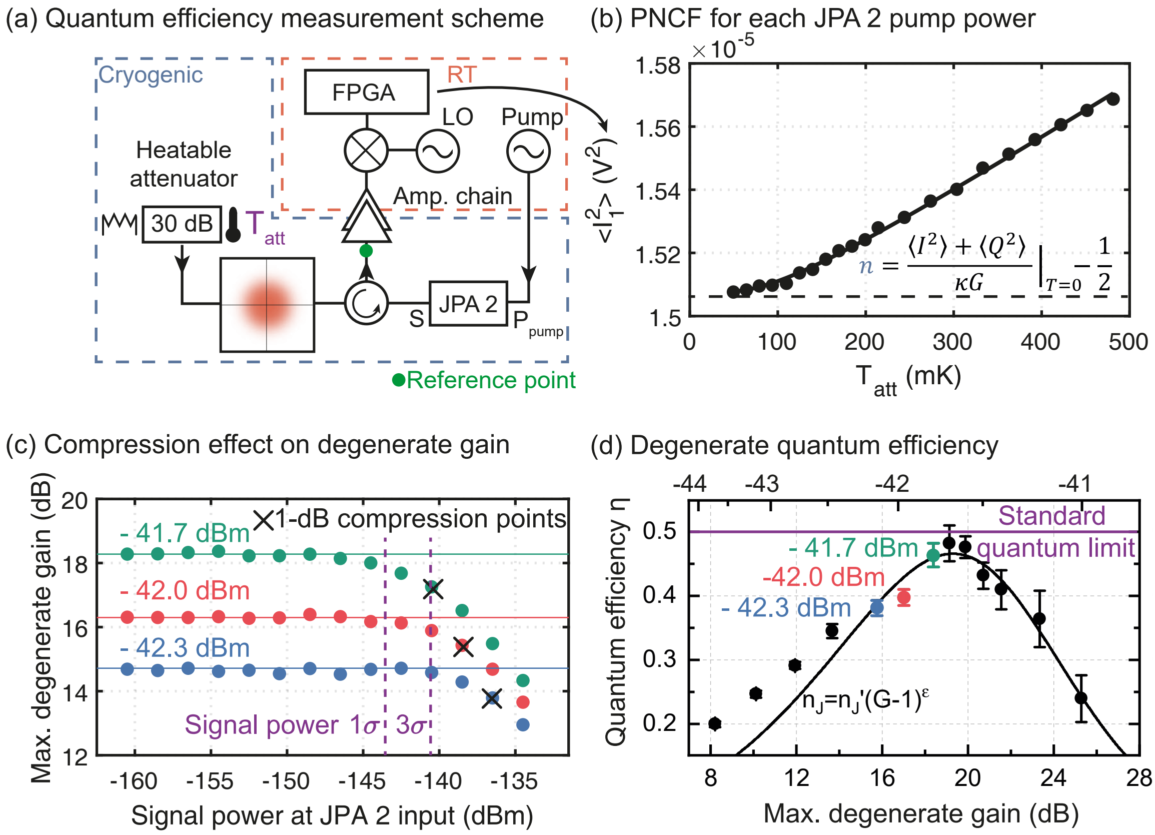

Figure 3.13: (a) Quantum efficiency measurement scheme. (b) Exemplary PNCF. The corresponding quantum efficiency η is computed by extracting the noise photon numbers n from Eq. 3.8. (c) Compression measurements. (d) Quantum efficiency measurement of JPA 2.

3.3.6 Quantum efficiency

In the last section, we showed how to estimate the signal power up to the input of JPA 2. In order to characterize the whole signal-to-noise ratio, we need to estimate the noise which is added by the subsequent degenerate (JPA 2) and nondegenerate amplifiers (HEMT and further linear amplifiers). To this end, we extract the total amplification noise referred to the input of JPA 2. The measurement configuration is shown in Fig. 3.13 (a). In contrast to the usual PNCF measurement (see Sec. 3.2.4), JPA 2 is active here and used in the degenerate regime. Then, we run individual PNCF calibration measurements for the individual JPA 2 pump powers, as shown in Fig. 3.13 (b), in order to extract the corresponding JPA 2 noise photon numbers and covert these to the quantum efficiency

$$\eta = \frac{1}{1+2n}, \tag{3.15}$$

where n are the total amplification noise photons. By applying the Friis formula (see Eq. 2.38), the total noise with reference to the input of the HEMT is given by

$$n = n_2 + \frac{n_\mathrm{H}}{G_2} + \cancelto{\simeq 0}{\frac{n_\mathrm{RT}}{G_\mathrm{H} G_2}} \quad , \tag{3.16}$$

where n_2 is the number of noise photons added by JPA 2 referred to its input, n_H is the noise added by the HEMT referred to its input, G_2 is the gain of JPA 2, and n_RT is the noise added by room temperature amplifiers referred to their inputs. From the known gain $G_2 \sim 20\,\mathrm{dB}$, HEMT noise in one quadrature $n_\mathrm{H} \sim 10$, and measured quantum efficiency η, we can estimate the added noise by JPA 2.

The resulting data points are shown in Fig. 3.13 (d), where the standard quantum limit (see Ref. 83) is indicated by the purple line at $\eta = 50\%$. In the plot, we notice two regimes: the low power regime below $-41.7\,\mathrm{dBm}$, where the quantum efficiency is increasing, and a high power regime above $-41.7\,\mathrm{dBm}$, where the quantum efficiency reaches its maximum at $\eta_\mathrm{JPA} = 48 \pm 3\%$ and starts decreasing. In comparison, the efficiency of phase-insensitive amplification, using only the HEMT amplifier, resulted in the quantum efficiency of $\eta_\mathrm{H} = (1 + 2n_\mathrm{H})^{-1} = 4.8\%$. Therefore, the phase-sensitive amplification JPA 2 increases η by a factor of ~ 10.

The observed behavior of the phase-sensitive quantum efficiency can be explained using the Friis formula for noise, Eq. 2.38. The quantum efficiency increases with the gain of JPA 2, G_2, as long as the noise of the HEMT dominates the overall noise, $n_\mathrm{H}/G_2 > n_2$. After reaching the maximum quantum efficiency, the pumped-induced noise and nonlinear effects (see Ref. 83) lead to an increase of n_2, which eventually leads to a degradation of the total noise, n.

4 Experimental Results and Discussion

In this chapter, we characterize the security of the microwave CV-QKD protocol in its experimental implementation as described in Sec. 3.1. The experiment is performed with and without phase-sensitive amplification by JPA 2. We expect that the improved quadrature-dependent signal-to-noise ratio increases the mutual information between Alice and Bob. This increase affects the secret key K (secure bits/channel use), which is defined as

$$K = \eta_{\mathrm{rec}} I_{\mathrm{AB}} - \chi_{\mathrm{E}}^{\blacktriangleright}, \tag{4.1}$$

where I_{AB} is the mutual information, $\eta_{\mathrm{rec}} \in (0,1)$ is the reconciliation efficiency, and $\chi_{\mathrm{E}}^{\blacktriangleright}$ Eve's Holevo information. In this analysis, we focus on the direct reconciliation case (▶ in Sec. 2.3.5).

Throughout all measurements, we stick to the working point frequency $f_0 = 5.5231\,\mathrm{GHz}$. Pre-characterization of this working point is provided in Sec. 3.3.1. JPA 1 is tuned in-resonance with f_0, to $I_{\mathrm{coil},1} = 10.2\,\mathrm{\mu A}$ $(-0.172\,\Phi/\Phi_0)$. For phase-sensitive amplification, JPA 2 is tuned to $I_{\mathrm{coil},2} = -27.8\,\mathrm{\mu A}$ $(-0.135\,\Phi/\Phi_0)$ and it is tuned off-resonance, when phase-sensitive amplification is not needed. In a first step, we compute the signal-to-noise ratio from calibration measurements and use it to calculate an expected limit for the mutual information $I_{\mathrm{AB}} = I_{\mathrm{max}}$ from the Shannon capacity (see Eq. 2.92). In a second step, we compare the Shannon limit with the measured mutual information $I_{\mathrm{AB}} = I(\alpha{:}\beta)$ between Alice's and Bob's variables, α and β (see Eq. 2.90), and calculate the secret key K. Then, we analyze whether our previous estimates for the secret key coincide with the measurements performed with a finite key length. Afterwards, we discuss the measured secret key rate. We conclude the chapter with an outlook directed towards possible improvements.

4.1 Preliminary calibrations and definitions

In this section, we compute the signal-to-noise ratio (SNR) for the phase-insensitive (PI) and phase-sensitive amplification (PS) regimes by using calibration measurements at the chosen working point. We use the Shannon limit $I_{\mathrm{max}} = \frac{1}{2}\log_2(1 + \mathrm{SNR})$ to estimate the maximal mutual information between Alice and Bob. Afterwards, we consider Eve's Holevo information $\chi_{\mathrm{E}}^{\blacktriangleright}$, which is obtained from a tomography of the average state of the CV-QKD protocol. Finally, we define the efficiencies and bandwidths needed to compute the secret key K and the corresponding secret key rate R in the PI and PS configurations.

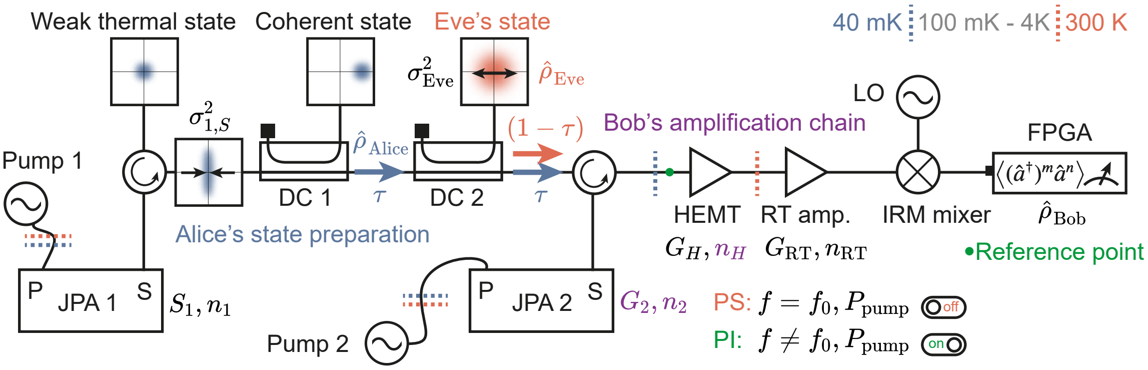
Weak thermal state
Coherent state
Eve's state
40 mK
100 mK - 4K
300 K
σ^2_{Eve}
$\hat\rho_{\mathrm{Eve}}$
LO
$\sigma^2_{1,S}$
$\hat\rho_{\mathrm{Alice}}$
$(1-\tau)$
Bob's amplification chain
FPGA
Pump 1
DC 1
τ
DC 2
τ
$\langle(\hat a^\dagger)^m \hat a^n\rangle$
HEMT
RT amp.
IRM mixer
$\hat\rho_{\mathrm{Bob}}$
Alice's state preparation
G_H, n_H
$G_{\mathrm{RT}}, n_{\mathrm{RT}}$
•Reference point
P
JPA 1
S
S_1, n_1
P
JPA 2
S
G_2, n_2
PS: $f = f_0, P_{\mathrm{pump}}$
off
PI: $f \neq f_0, P_{\mathrm{pump}}$
on
Pump 2

Figure 4.1: Simplified signal propagation path. The squeezed quadrature variance is $\sigma^2_{1,\mathrm{S}}$. The second directional coupler (DC 2) couples Eve's noise signal to the Alice cipher, simulating the entangling cloner attack. Afterwards, the signal is either phase-senitively amplified (PS), if JPA 2 is tuned in-resonance to f_0 and pumped, or passing through the circulator without any amplification, if the JPA 2 is detuned (PI). The rest of the amplification chain consists of the high-electron-mobility-transistor (HEMT) at 4 K and several subsequent amplifiers at room temperature. The input of the HEMT is chosen as the reference point (green) for the state tomography.

4.1.1 Shannon limit with and without phase-sensitive amplification

Here, we compare the signal-to-noise ratio and resulting for phase-insensitive (PI) and phase-sensitive amplification (PS) regimes. A simplified sketch of the noise in the experimental setup is shown in Fig. 4.1. The added noise of the room temperature amplifiers n_{RT} can be neglected, as explained in Sec. 3.3.6.

The signal-to-noise ratio relates the signal power to the total noise power present in the channel. The average signal power is determined by the variance of the sampled displacement amplitudes α drawn from the Gaussian distribution $\mathcal{N}(0, \sigma^2_{\mathrm{disp}})$. We denote this quantity as the displacement variance σ^2_{disp}. The latter is linked to the squeezing level of JPA 1, such that the average over all displaced squeezed states corresponds to a thermal state (see Sec. 2.3.3). The noise power is a sum of different contributions: the squeezed variance of Alice's state itself, the noise added by Eve, and the amplification noise. The amplification noise depends on the mode of operation of JPA 2. Either JPA 2 is detuned and not pumped (HEMT amplification, PI in Fig. 4.1), or JPA 2 is tuned in-resonance with f_0 and pumped (degenerate JPA amplification, PS in Fig. 4.1). The expected signal-to-noise ratio SNR can be written as

$$\mathrm{SNR} = \frac{\tau\sigma^2_{\mathrm{disp}}}{\underbrace{\tau^2\sigma^2_{1,\mathrm{S}}}_{\text{Alice}} + \underbrace{\bar n + 0.25(1-\tau)}_{\text{Eve}} + \underbrace{n_{\mathrm{amp}}}_{\text{Bob}}}, \tag{4.2}$$

where τ is the transmissivity of the first and second directional couplers, σ^2_{disp} is the displacement variance of the key, $\sigma^2_{\mathrm{S,JPA1}}$ is the variance in the squeezed quadrature of Alice's state, $\bar n + \frac{1}{4}(1-\tau)$ is Eve's added noise photons at the output of the second directional coupler (see Sec. 2.3.5), and n_{amp} is the total amplification noise added at Bob's side for one

S	σ^2_{disp}	$\mathrm{SNR_{PI}}$	$\mathrm{SNR_{PS}}$	$I_{\mathrm{max,PI}}$	$I_{\mathrm{max,PS}}$
3.5 dB	0.5	5%	63%	0.035	0.352
5.2 dB	1.4	14%	177%	0.095	0.734

Table 4.1: Expected signal-to-noise ratio SNR and Shannon capacity I_{max} (bits/channel use) with (PS) and without (PI) phase-sensitive amplification. For $\mathrm{SNR_{PI}}$, the amplification noise is $n_{\mathrm{amp}} = n_{\mathrm{H}}$; for $\mathrm{SNR_{PS}}$, the amplification noise is $n_{\mathrm{amp}} = n_2 + n_{\mathrm{H}}/G_2$. σ^2_{disp} denotes the sample variance of $N = 150$ symbols.

quadrature. Depending on the mode of operation, the total amplification noise is either dominated by the HEMT noise, $n_{\mathrm{amp}} = n_{\mathrm{H}}$ (PI), or by the JPA 2 noise, $n_{\mathrm{amp}} = n_2 + n_{\mathrm{H}}/G_2$ (PS).

We are using two different squeezing levels $S = 3.5\,\mathrm{dB}$, $S = 5.2\,\mathrm{dB}$ at the same working point $f_0 = 5.5231\,\mathrm{GHz}$. The purities for the squeezing levels are $\mu(S = 3.5\,\mathrm{dB}) = 96\%$ and $\mu(S = 5.2\,\mathrm{dB}) = 95\%$. The signal-to-noise ratio can be used to calculate the Shannon capacity of the channel between Alice and Bob (see Sec. 2.3.4). For a single channel use, the maximally obtainable mutual information is bound by $I_{\mathrm{max}} = \frac{1}{2}\log_2(1 + \mathrm{SNR})$. The squeezing level S dictates the displacement variance σ^2_{disp} through the condition for indistinguishable encoding bases, so that the antisqueezed variance of Alice's state is equal to the sum of the displacement variance and the squeezed variance. In the case of the squeezing level $S = 5.2\,\mathrm{dB}$, the displacement variance drawn from a distribution of variance $\sigma^2_{\mathrm{AS}} - \sigma^2_{\mathrm{S}} = \sigma^2_{\mathrm{disp}}$ was 1.4 photons. We draw 150 symbols from the corresponding distribution. We know from the earlier PNCF measurements (see Sec. 3.2.4) that the amplification noise in one quadrature is $n_{\mathrm{amp}} = n_{\mathrm{H}} \sim 10$ photons. In the degenerate case, a pump power of $-42.3\,\mathrm{dBm}$ results in $n_{\mathrm{amp}} = n_2 + n_{\mathrm{H}}/G_2 = 0.81$ noise photons. With an exemplary coupled noise of $\bar{n} = 0.05$ noise photons, and the known directional coupler transmissivity, $\tau = 0.99$, we can compute the expected signal-to-noise ratios for the squeezing levels $S = 3.5\,\mathrm{dB}$ and $S = 5.2\,\mathrm{dB}$, as shown in Tab. 4.1. As expected, the SNRs increase in the PS regime.

In conclusion, we observe a more than tenfold improvement of the signal-to-noise ratio by exploiting the degenerate pre-amplification by JPA 2. This should also lead to an increase by one order of magnitude for the maximally obtainable mutual information given by the Shannon limit.

4.1.2 Calculation of Holevo information for Eve's added noise photons

The computation of Eve's Holevo information $\chi_{\mathrm{E}}^{\blacktriangleright}$ relies on the approach introduced in Sec. 2.3.5. We estimate the Holevo information by using the covariance matrix formalism (see Sec. 2.3.5). In particular, we calculate the entropy of individual states $S\left(\hat{\rho}^{\alpha_{\mathrm{i}}}_{\mathrm{E},\mathcal{B}}\right)$ and the entropy of the average state $S\left(\hat{\rho}_{\mathrm{E,avg}}\right)$ with the encoding basis $\mathcal{B} \in \{q, p\}$ from their corresponding covariance matrices. The Holevo information is computed using the symplectic

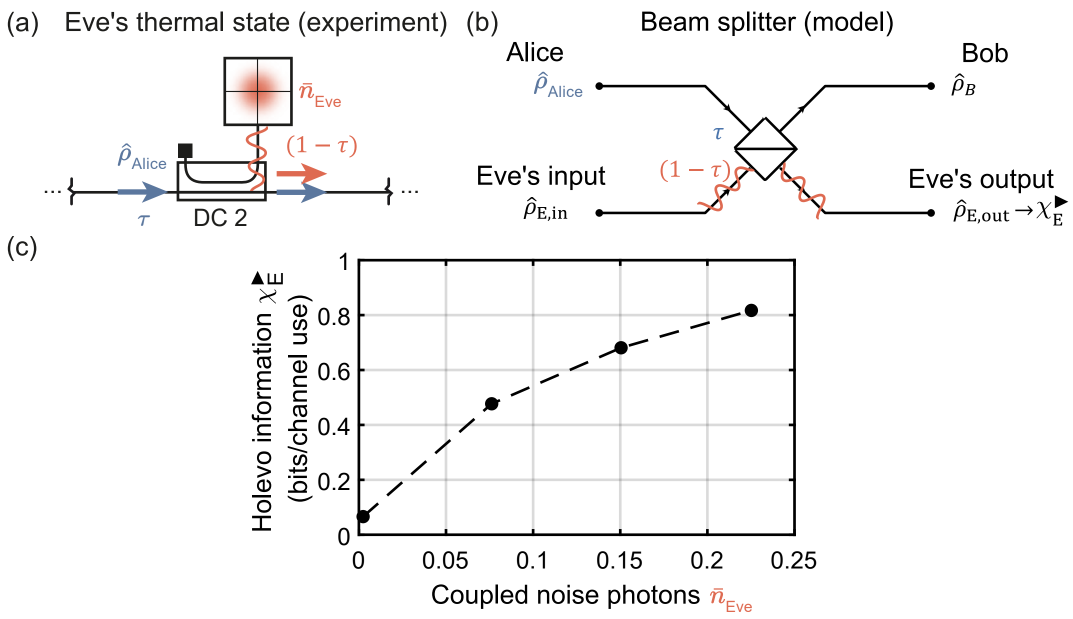

Figure 4.2: (a) Experimental simulation of the entangling cloner attack by Eve. (b) Beam splitter model. The Holevo information $\chi_{\mathrm{E}}^{\blacktriangleright}$ is the maximally attainable information possible based on a coupled state $\hat{\rho}_E$. (c) Eve's Holevo information for direct reconciliation depending on the average number of coupled noise photons.

eigenvalues $S(\mathbf{V}) = g(\nu_+) + g(\nu_i)$ so that

$$\chi_{\mathrm{E}}^{\blacktriangleright} = S\left(\mathbf{V}_{\mathrm{avg,E}}\right) - \sum_{\mathcal{B}\in\{\mathrm{q,p}\}} \frac{1}{2}\int_{-\infty}^{\infty} f\left(\alpha_{\mathrm{i}}|0,\sigma^2_{\mathrm{disp}}\right)\, S\left(\mathbf{V}^{\alpha_i}_{\mathrm{E},\mathcal{B}}\right) \mathrm{d}\alpha_{\mathrm{i}}, \tag{4.3}$$

where $\mathbf{V}_{\mathrm{avg,E}}$ is the covariance matrix of the average state as defined in Eq. 2.124, and $\mathbf{V}^{\alpha_i}_{\mathrm{E},\mathcal{B}}$ is the covariance matrix of an individual cipher state with the corresponding symbol α_i that is encoded in the basis $\mathcal{B}$, as defined in Eq. 2.118. The function $f\left(\alpha_{\mathrm{i}}|0,\sigma^2_{\mathrm{disp}}\right)$, is the probability density function at the symbol value α_i of the Gaussian distributed key with variance σ^2_{disp} and mean 0.

An accurate estimate of the covariance matrix of the average state and the covariance matrix of each individual cipher state relies on a precise tomography by Bob. Therefore, we measure each symbol with a high number of averages, $M = 10^5$. The computed Holevo quantities for the selected noise levels are shown in Fig. 4.2. The noise levels, $\bar{n} \in \{2.4\times10^{-3}, 7.6\times10^{-2}, 0.15, 0.23\}$ (photons), are purposefully chosen so that the Holevo information $\chi_{\mathrm{E}}^{\blacktriangleright}$ is close to the expected levels of mutual information as computed from the signal-to-noise ratios in Tab. 4.1.

4.1.3 Definition of the single-shot secret key

In this work, we define a single-shot secret key K as a single quadrature value that was acquired at the maximum bandwidth $B = 400\,\mathrm{kHz}$ of our readout setup (see Sec. 3.2.3). The secret key rate $R = f_{\mathrm{r}}\eta_{\mathrm{sift}}K$, as defined in Eq. 2.128, is the product of the secret key

$K = \eta_{\mathrm{rec}} I_{\mathrm{AB}} - \chi_{\mathrm{E}}$, the sifting efficiency η_{sift}, and the repetition rate f_{r}. For simplicity, we assume a perfect reconciliation efficiency of $\eta_{\mathrm{rec}} = 100\%$.

In our experimental setting, the repetition rate f_r of the protocol depends largely on the required time for phase stabilization. We stabilize the phase (see Sec. 3.3.2) of the involved JPAs and the coherent tone for each transmitted symbol to prohibit a loss of mutual information due to the phase drift. The experimental repetition rates for phase-insensitive amplification $\mathrm{f}_{\mathrm{r,PI}} = 0.17$ (symbols/s) exceeds the repetition rate $\mathrm{f}_{\mathrm{r,PS}} = 0.01$ (symbols/s) for phase-sensitive amplification due to extra attenuation when JPA 2 is not active and induced significant losses of around $-10\,\mathrm{dB}$ in the signal path. However, this limitation is not of fundamental nature and can be completely circumvented in the future by using fast flux lines for rapid tuning of the JPA resonant frequency. For now, we require a phase stabilization time for PS of around $7\,\mathrm{min}$. Our microwave signal detection operates at the bandwidth of $\Delta f = 400\,\mathrm{kHz}$. This sets an upper bound for the repetition rate, $f_r = 400\,\mathrm{kHz}$, and can be used to estimate the secret key rate. Similarly, we assume that Eve's Holevo information $\chi_{\mathrm{E}}^{\blacktriangleright}$ is obtained at the same bandwidth. However, the employed FPGA in our experiment lacks a port for synchronized digital data transmission during the runtime. Information can only be extracted at the beginning and the end of the runtime. This implies that in the current setup, only one symbol can be sent synchronously per runtime of the FPGA. In the experiment, the signal moments for a single symbol are stored in the memory of the FPGA and sent to the CPU after the synchronized measurement is completed. This also effectively limits the repetition rate to the latency of the communication between CPU and FPGA and the initialization time of the FPGA. This latency is on the order of one second per symbol. Therefore, a more practical implementation would require a FPGA with a digital bus.

The sifting efficiency $\eta_{\mathrm{sift}} = 50\%$ represents the fraction of symbols that are discarded due to non-matching quadrature bases $\mathcal{B} \in \{q, p\}$. In the current experimental implementation (see Sec. 3.1), we restrict ourselves to one encoding quadrature basis. This restriction is equivalent to an already applied sifting procedure. Therefore, the measured mutual information $I(\alpha{:}\beta)$ is already sifted with the efficiency of $\eta_{\mathrm{sift}} = 50\%$.

4.1.4 Definition of secret key capacity

We can define the secret key capacity $\mathcal{R}$ as the upper bound for the secret key rate R, so that $\mathcal{R} \geq R$

$$\begin{aligned} \mathcal{R} &= f_{\mathrm{r}} \eta_{\mathrm{sift}} \mathcal{K} \\ &= f_{\mathrm{r}} \eta_{\mathrm{sift}} (\eta_{\mathrm{rec}} I_{\mathrm{max}}(A{:}B) - \chi_{\mathrm{E,min}}^{\blacktriangleright}) \end{aligned} \tag{4.4}$$

where $\mathcal{K} \geq K$ is the maximum single-shot secret key. Since a sufficiently noisy eavesdropping attack can bring down any secret key rate to zero, this metric serves as a measure for the maximally possible secure communication rate. It is important to note that we typically introduce noise accessible to Eve in experimental settings. The fundamental result of non-zero losses in the signal path, which couple to environmental noise sources (controlled

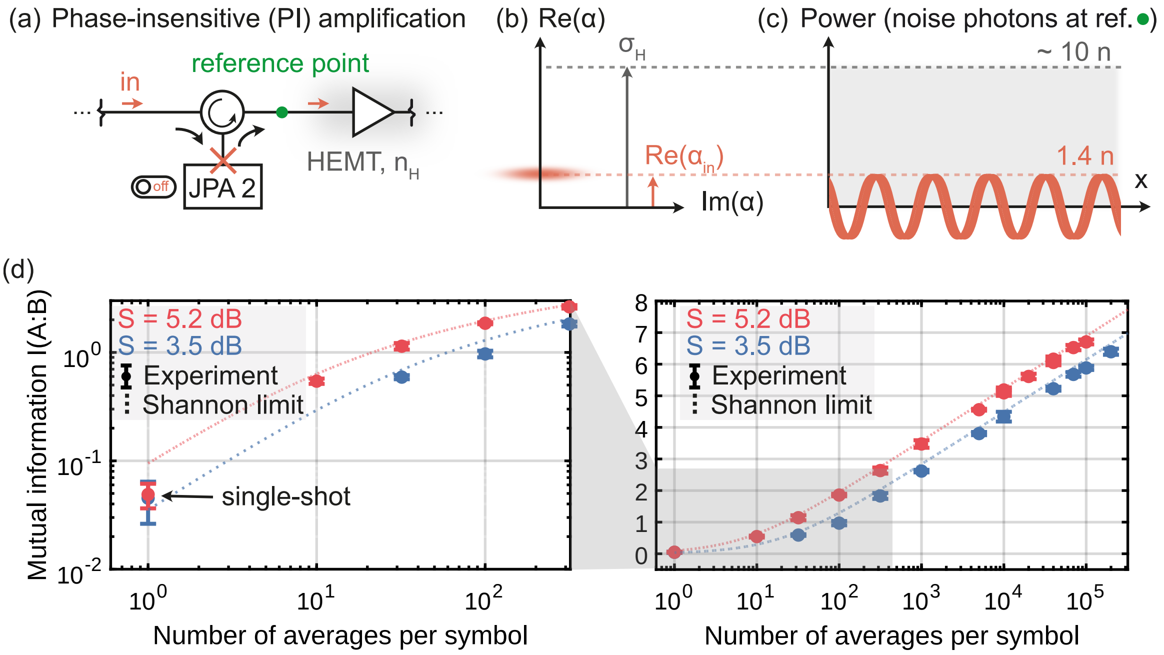

Figure 4.3: (a) Scheme for the phase-insensitive amplification with the detuned JPA 2. The amplification is performed by the HEMT and room temperature amplifiers. (b) Wigner function of an input signal (red) with the displacement amplitude $\alpha = \sigma_{\text{disp}}$. The standard deviation of the thermal state representing the HEMT input noise n_{H} is colored in grey. (c,d) Mutual information scaling with the number of performed averages. Subfigure (c) shows the scaling in the single-shot regime.

by Eve), lead to a finite Holevo quantity $\chi_E^{\blacktriangleright}$. We define the experimentally achievable maximum secret key rate $\mathcal{R}_{\text{exp}}$ correspondingly by using the measured secret key K_{exp}.

4.2 CV-QKD in the phase-insensitive (PI) regime

We measure the mutual information in the PI regime to allow for a later comparison with the PS regime. Furthermore, we are interested in how close the measured mutual information is to the Shannon limit. Our approach consists of three steps: key generation, synchronized measurements, and post-processing. First, the key corresponding to the squeezing level is drawn from a Gaussian distribution. Second, the measurement is conducted in the PI configuration (see Fig. 4.1). Third, we compute the mutual information from the measured keys (see Eq. 2.90). Lastly, we compute the secret key K from the mutual information between Alice and Bob and estimated Eve's Holevo information. The latter serves as a security criterion. The communication is secure if and only if $K > 0$.

Here, we compare the measured mutual information with the Shannon limit (see Sec. 4.1) for different amount of averages M. These two quantities are defined as (see Sec. 2.3.4)

$$\text{Shannon limit} \quad (\cdots \text{ in Fig. 4.3}) \qquad I_{\max} = \frac{1}{2}\log_2(1+\text{SNR}), \tag{4.5}$$

$$\text{Measured mutual information} \quad (\bullet \text{ in Fig. 4.3}) \qquad I(\alpha{:}\beta) = -\frac{1}{2}\log_2(1-\rho^2), \tag{4.6}$$

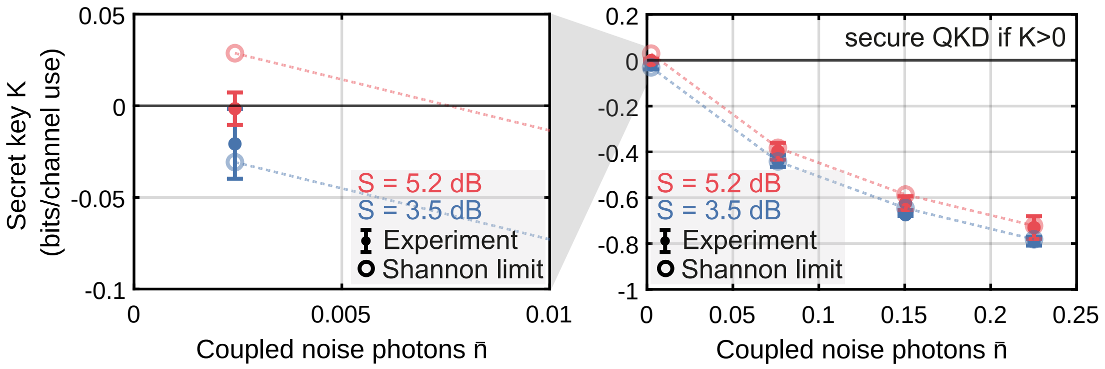

Figure 4.4: Single-shot secret key K (bits/channel use) versus the coupled noise photon number $\bar{n}$ without phase-sensitive amplification in the PI regime for the squeezing levels $S = 3.5\,\mathrm{dB}$ (blue) and $S = 5.2\,\mathrm{dB}$ (red) for $M = 1$. The left subfigure shows that the experimental secret key is negative even in the low-noise regime.

with the correlation coefficient $\rho = \mathrm{Cov}(\alpha, \beta)/(\sigma_\alpha \sigma_\beta)$ and M times averaged symbols α_i and β_i. The signal-to-noise ratio SNR improves linearly with M averages to $\mathrm{SNR_M} = \mathrm{SNR} \cdot M$ as shown in Eq. 2.95. We note that Eq. 4.1 for the secret key is only valid for $M = 1$. However, we are interested in the scaling of the measured mutual information to characterize the channel and to spot possible time dependent errors in the calibration. We expect from the computed Shannon limit in Tab. 4.1 that the signal-to-noise ratios are bound by $\mathrm{SNR}(S = 3.5\,\mathrm{dB}) = 5\%$, and $\mathrm{SNR}(S = 5.2\,\mathrm{dB}) = 14\%$.

4.2.1 Comparison of measured mutual information with the Shannon limit

Fig. 4.3 compares these bounds to the measured mutual information. The x-Axis scales the amount of averages logarithmically. We observe that the measured mutual information in both cases is following the expected logarithmic increase given by the Shannon limit and the linear scaling of the SNR with increasing averages. In particular, the measured mutual information is increasing logarithmically with the amount of averages per symbol. The single-shot mutual information for both squeezing levels is near the low expected mutual information of less than 0.1 bits. For the squeezing level $S = 3.5\,\mathrm{dB}$, the expected single-shot Shannon limit was $I_{\max} = 0.035$ bits. The experiment for $N = 150$ symbols and $n = 3$ runs yielded $I(\alpha{:}\beta) = 0.045 \pm 0.019$ bits. For $S = 5.2\,\mathrm{dB}$, the single-shot mutual information was $I_{\max} = 0.095$ bits, with an expected Shannon limit of $I_{\max} = 0.095$ bits. As the unit for mutual information is given in bits, the configuration is two orders of magnitude away from delivering binary information $I = 1$ bit.

4.2.2 Secret key for single-shot CV-QKD in the PI regime

When we consider that the Holevo information, as shown in Fig. 4.2, ranges from approximately 0.1 to 0.8 bits per channel use, we expect a negative secret key for any level of eavesdropping. Fig. 4.4 shows the secret key $K = \eta_{\mathrm{rec}} I_{\mathrm{AB}} - \chi_{\mathrm{E}}$ with an assumed reconciliation efficiency $\eta_{\mathrm{rec}} = 100\%$. We observe that the measured mutual information for both squeezing levels is not high enough to allow for a secure communication ($K > 0$).

In particular, the amplification noise $n_{\mathrm{amp}} = n_{\mathrm{H}}$ is so high that Bob is not able to gain enough information on Alice's key. We conclude, not very surprisingly, that a phase-insensitive amplification relying solely on the HEMT amplifier is not suited for the single-shot readout. An intuitive explanation of our observations is that the signal powers, corresponding to Alice's cipher states, are too low as compared to the HEMT noise level. As a result, the HEMT noise, $n_{\mathrm{H}} \sim 10$, is dominating the output signal.

4.3 CV-QKD in the phase-sensitive (PS) regime

In this section, we investigate the mutual information by using JPA 2 for phase-sensitive amplification (PS in Fig. 4.1) with the JPA 1 squeezing level $S = 5.2\,\mathrm{dB}$. We compare the results with the corresponding Shannon limit and measured mutual information in the PI regime. Alice sends an identical key in both configurations (PS and PI). We compute the mutual information from the measured keys (see Eq. 4.6) and compare it with the Shannon limit (see Eq. 4.5).

4.3.1 Comparison of measured mutual information with the Shannon limit

Similar to Sec. 4.2, we compare the measured mutual information with the Shannon limit for different numbers of averages M for the squeezing level $S = 5.2\,\mathrm{dB}$. From the estimated Shannon limit in Tab. 4.1, we expect that the signal-to-noise ratio is bound by $\mathrm{SNR}_{\mathrm{PS}} = 177\%$. This implies an expected increase by around twelve times in comparison to $\mathrm{SNR}_{\mathrm{PI}} = 14\%$. This expectation is based on our main hypothesis that the dominating factor in the SNR is the HEMT amplification noise n_{H}.

Figure 4.5 shows a comparison between the mutual information values experimentally obtained in the PI and PS regimes. The mutual information is measured for the real part (green) and the imaginary part (purple) of the displacement amplitude (see Fig. 4.5 (c)). We observe that the mutual information estimated from the amplified quadrature of the signal in the PS configuration is 13 times larger than the one in the PI configuration (PI) in the low-average regime $\leq 10^3$. As a result, we can achieve for a positive single-shot secret key in the PS regime (see Sec. 4.3.3), which was the main goal in this work. The measured single-shot mutual information, $I_{\mathrm{PS}} = 0.65 \pm 0.08$ bits, agrees well with the single-shot Shannon limit, $I_{\mathrm{max,PS}} = 0.73$ bits, that was computed from the improved quadrature-dependent quantum efficiency (see Sec. 4.1).The measured mutual information above 10^3 averages per symbol unexpectedly deviates from the Shannon limit and saturates at the mutual information value of $I(A{:}B) \simeq 5$ bits. This effect is irrelevant for the precision of the single-shot measurements. However, future protocols can increase their repetition rate f_{r} by reducing the amount of calibration runs per transmitted symbol. Therefore, we discuss this issue below.

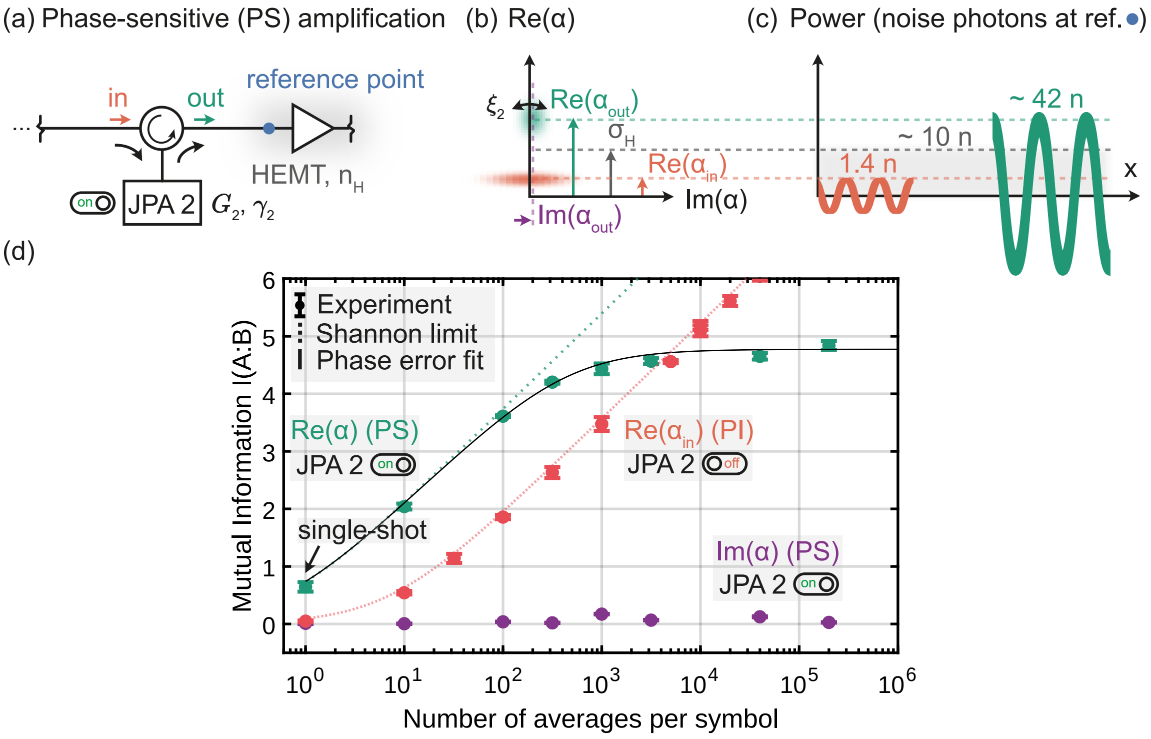

Figure 4.5: (a) Scheme for the phase-sensitive amplification with pumped JPA 2. One quadrature of the input signal (red) is amplified, so that the power of the output signal (green) is large in comparison to the HEMT noise (grey). (b) Wigner functions of the input signal (red) and output state (green). The real part of the input state is amplified to $\mathrm{Re}(\alpha_{\mathrm{out}}) = \sqrt{G_2}\mathrm{Re}(\alpha_{\mathrm{in}}) = 6.6$ photons. The degenerate gain of JPA 2 is $G_2 = 14.8\,\mathrm{dB}$. (c) Signal and noise powers referred to the input of the HEMT. (d) Mutual information $I(A{:}B)$ for the encoding quadrature of the phase-sensitively amplified state (green) and the orthogonal squeezed quadrature carrying no useful information.

4.3.2 Phase-drift impact on the signal-to-noise ratio

The most probable reason for the experimental decrease of the signal-to-noise ratio (SNR) is a dephasing during the averaging time, as indicated by ξ_2 in Fig. 4.5 (b). We note that most contributions to the SNR (see Eq. 4.2) are not prone to large deviations: the displacement variance σ^2_{disp} or the added noise $\bar{n}$ are stable during the measurements. The transmissivity of the directional coupler τ is also a well-fixed passive quantity. The only contribution that can be subject to large deviations over time is the phase noise in the amplification chain.

To calculate the effect of this dephasing on the amplification chain, we once again use the Friis formula, so that $n_{\mathrm{amp}} = n_2 + n_{\mathrm{H}}/G_2$ (see Eq. 2.38). We consider an extreme case of dephasing between the input signal and the JPA 2 squeezing angle of $\phi = 2\gamma = \pi$. Thus, JPA 2 actively adds amplified noise to the quadrature that carries the signal, so that $n_{\mathrm{amp}} = n_2 + G_2 n_{\mathrm{H}}$.

If we assume a first-order approximation for the JPA 2 phase drift, $\phi = \omega t$ as $\sin(\omega t) \simeq \omega t$, where ω (°/s) is the phase drift velocity, we can rewrite the total amplification noise n_{amp} as a sum of the suppressed noise and actively added noise dependent on the phase drift

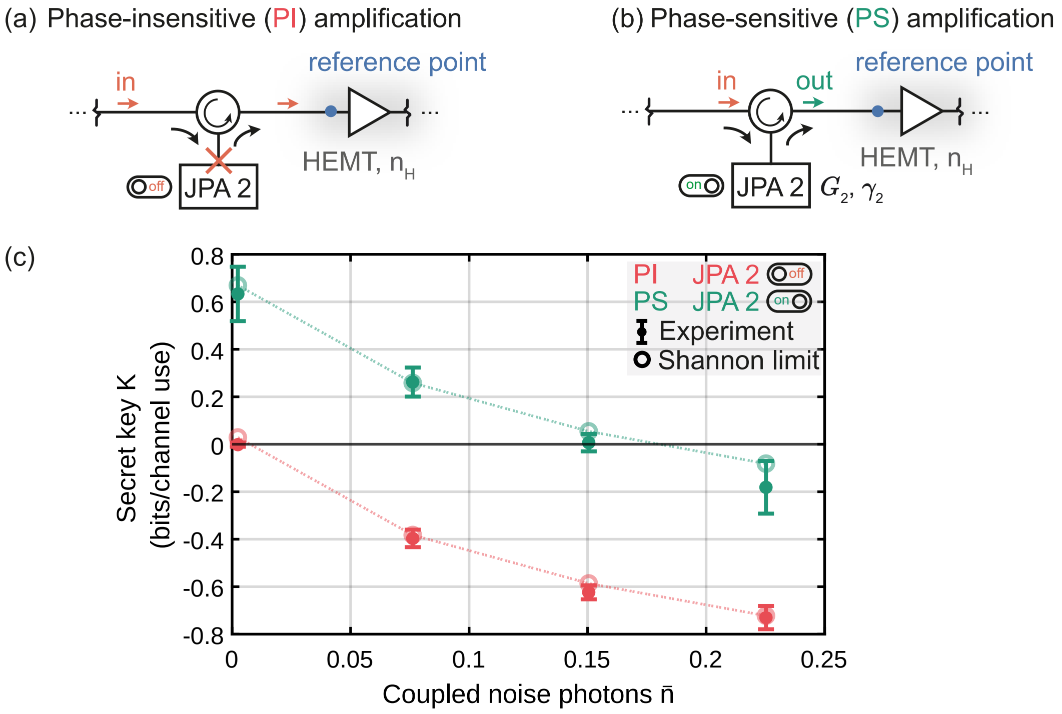

Figure 4.6: Single-shot secret key K (bits/channel use) versus the average coupled noise photon number $\bar{n}$ for the squeezing level $S = 5.2\,\mathrm{dB}$. (a) Phase-insensitive configuration. (b) Phase-sensitive configuration. (c) Secret key for the PI and PS regimes. The dashed line acts as a guide between the expected maximal secret key calculated from the Shannon limit.

$\phi(t)$ at time t as

$$n_{\mathrm{amp}} \simeq n_2 + n_{\mathrm{H}}/G_2 + G_2 n_{\mathrm{H}} \omega t \tag{4.7}$$

The solid black line in Fig. 4.5 (d) represents the fitted function using the Shannon limit on Eq. 4.2 with the adjusted the amplification noise Eq. 4.7. For the fit, we rescale the averages $M = Dt$ in terms of seconds, where the trace repetition rate (in averages M per second) is $D = 6.6\,\mathrm{kHz}$. This rate includes the minimal latency of the CPU generating and communicating the random symbols. The resulting phase drift is $\omega = 0.04\,\mathrm{rad}/s$. This model assumes a mean random phase error of $\gamma = \omega D^{-1} M = 0.35$ rad for the inflection point at $M = 10^3$. Therefore, the small angle approximation assumed for the first-order approximation holds in the regime of low averages at a time $\leq 0.15\,\mathrm{s}$. We note that a more advanced model needs to be developed for larger time scales and that the phase drift velocity is unusually high in our experiments.

4.3.3 Positive secret key for single-shot CV-QKD in the PS regime

As the measured single-shot mutual information for phase-sensitive amplification (PS) agreed with the Shannon limit, we immediately achieve a positive secret key in the limit of minimal eavesdropping. If we assume a small contribution of Eve's noise to the signal-to-noise ratio, we expect the threshold for secure key, $K = 0$, at a corresponding noise level for the Holevo information to be approximately 0.6 bits per channel use.

In Fig. 4.6, the estimated secret key for the PS regime is compared with the PI regime. The secret key is calculated from $K = \eta_{\text{rec}} I_{\text{AB}} - \chi_{\text{E}}$ with an assumed reconciliation efficiency $\eta_{\text{rec}} = 100\%$. The dashed line indicates the maximal mutual information $I_{\text{AB}} = I_{\max}$ due to the Shannon limit; the mutual information $I_{\text{AB}} = I(\alpha{:}\beta)$ represented by the solid markers is estimated using Eq. 4.6. We observe that the measured mutual information for $S = 5.2\,\text{dB}$ is high enough to allow for a secure communication ($K > 0$) below the coupled noise threshold of $\bar{n} = 0.15$ noise photons. This is a very important experimental milestone. It illustrates that the single-shot microwave CV-QKD is feasible even in the presence of significant external noise coupled to the quantum channel.

4.3.4 Calculation of secret key rate

Furthermore, we can estimate the secret key capacity $\mathcal{R} = f_{\text{r}} \eta_{\text{sift}} \mathcal{K}$ (bits/s) following the approach as defined in Sec. 4.1.3. The maximally achievable rate at the lowest noise level of $\bar{n} = 0.05$ enables the secret key capacity of $\mathcal{R}_{\text{exp}} = 3.1 \pm 0.6 \times 10^{-3}$ bits/s, where $f_{\text{r}} = 0.17\,\text{Hz}$ and $\eta_{\text{sift}} = 50\%$. Assuming an optimized protocol as proposed in Sec. 4.1.3 and setting our repetition rate to the upper limit defined by the detection bandwidth, $f_{\text{r}} = 400\,\text{kHz}$, we can obtain a secret key capacity of $\mathcal{R} = 1.3 \pm 0.23 \times 10^{5}$ bits/s, which illustrates a significant application potential for the near term future.

Let us make an estimation for the communication rate with a practical example: we can consider the binary UTF-8 encoding of *„Hello!“*). This 6 byte message requires the transmission of a quantum key of the same length. For the experimental secret key capacity $\mathcal{R}_{\text{exp}} = 3.1 \pm 0.6 \times 10^{-3}$ bits/s, the communication of a 6 byte quantum key takes $4.3\,\text{h}$. The optimized protocol that would solely require a digital bus (see Sec. 4.1.3 for details) can transmit the same message in a fraction of a second. Remarkably, one could communicate a secret key long enough to encode every word[1] in Shannon's article *A Mathematical Theory of Communication*, at the secret key capacity of $\mathcal{R} = 1.3 \pm 0.23 \times 10^{5}$ bits/s, in only 4.4 s [11].

4.4 Discussion of possible improvements and research directions

In Sec. 4.3.3, we demonstrate the positive secret key ($K > 0$) in the experimental setting by using the Josephson parametric amplifier for phase-sensitive amplification. We also successfully achieve the single-shot measurement for the microwave quantum states securely encoding classical key elements. Furthermore, we demonstrate that the Shannon limit, $I_{\max} = \frac{1}{2}\log_2(1 + \text{SNR})$, provides an accurate estimate for the channel capacity in the low-average regime below 10^3. The quantities determining the signal-to-noise ratio are obtained from the calibration measurements that does not rely on any key transmission.

[1] The 45 pages long article has approximately 15000 words. With an average of 4.7 characters per word in the english language, the total byte count in UTF-8 encoding (1 byte per character) is 70.5 kilobyte (564,000 bits).

Parameter	phase-insens.	phase-sensitive	improved components
n_{amp} (photons)	10	0.81 ($G_2 = 14.8\,\mathrm{dB}$)	0.51 ($G_2 = 25\,\mathrm{dB}$)
σ^2_{disp} (photons)	1.4	1.4 ($S_1 = 5.2\,\mathrm{dB}$)	39.6 ($S_1 = 10\,\mathrm{dB}$)
SNR	0.14	1.77	62.2
$\mathcal{K}_{\mathrm{exp}}$ (bits/ch. use)	< 0	0.63 ± 0.11	-
$\mathcal{K}$ (bits/ch. use)	0.028	0.67	2.99
$f_{\mathrm{r,max}}$ (symbols/s)	$400\,\mathrm{kHz}$	$400\,\mathrm{kHz}$	71.1×10^6 ($f_{\mathrm{S}} = 6.4\,\mathrm{GHz}$)
$\mathcal{R}_{\mathrm{exp}}$ (bits/s)	< 0	$3.1 \pm 0.6 \times 10^{-3}$	-
$\mathcal{R}$ (bits/s)	16.4×10^3	$1.3 \pm 0.23 \times 10^5$	1.06×10^8

Table 4.2: Parameters and results for an improved single-shot microwave CV-QKD. The parameters are presented both the PI and PS regimes. The third column shows the technically possible improvements discussed in Sec. 4.4.1, Sec. 4.4.2, and Sec. 4.4.3. For the calculation of maximal secret key rate $\mathcal{R}$, we assume the reconciliation efficiency $\eta_{\mathrm{rec}} = 100\%$, and $\eta_{\mathrm{sift}} = 50\%$.

The average signal power is $|\alpha|^2 = \sigma^2_{\mathrm{disp}} = 1.4$ photons. In the current configuration, an added noise of more than 10% leads to an unsecure connection. Therefore, the tolerance for maximally added noise can still be improved.

The main efforts for improving the secret key rate $\mathcal{R}$ should be directed towards increasing the mutual information $I(A{:}B)$, and the repetition rate f_{r}. As demonstrated, the mutual information depends on the signal-to-noise ratio which we define as

$$\mathrm{SNR} = \frac{\tau \sigma^2_{\mathrm{disp}}}{\tau^2 \sigma^2_{\mathrm{S,JPA1}} + \bar{n} + 0.25(1-\tau) + n_{\mathrm{amp}}}. \tag{4.8}$$

In general, we want to decrease the quantities in the denominator and increase the ones in the nominator. If we review the different contributions, we have three main levers for increasing the SNR (and the secret key rate R). We discuss below the limits for a reduced amplification noise n_{amp}, an increased signal power $|\alpha|^2 = \sigma^2_{\mathrm{disp}}$ equal to the displacement variance of the key, and a increased repetition rate f_{r}. The discussed improvements are summarized and contrasted with the current metrics in Tab. 4.2.

4.4.1 Reduction of amplification noise

We reduced the amplification noise by using the JPA 2 in the degenerate regime, from $n_{\mathrm{amp}} = n_{\mathrm{H}} = 10$ to $n_{\mathrm{amp}} = n_2 + n_{\mathrm{H}}/G_2 = 0.81$. However, the JPA 2 compression limit bounds the maximal gain (see Sec. 3.3.5). In particular, the maximum power ($P_{\mathrm{sig},3\sigma} = -142\,\mathrm{dBm}$) in a $3\sigma-$interval of the Gaussian distributed powers $\mathcal{N}(0, \sigma^2_{\mathrm{disp}})$, corresponding to the desired squeezing level $S = 5.2\,\mathrm{dB}$, allows only for the JPA 2 gain $G_2 = 14.8\,\mathrm{dB}$. Therefore, the contribution of the HEMT noise $n_{\mathrm{H}}/G_2 = 0.33$ is still significantly contributing to the total amplification noise. This becomes evident, when we review the low power regime in Fig. 3.13. An increased gain G_2 can reduce the contribution of the HEMT noise to the total amplification noise even further. Considering compression limits due to the signal power ($P_{\mathrm{signal}} = -143\,\mathrm{dBm}$), a realistically achievable gain is $G = 25\,\mathrm{dB}$. With a similar JPA input noise n_2, this would improve the amplification noise from $n_{\mathrm{amp}} = 0.81$ to $n_{\mathrm{amp}} = 0.51$.

4.4.2 Increased signal power

With an increased displacement variance σ^2_{disp}, we can achieve a higher SNR. We can see this effect in Sec. 4.2, where an increase of $1.7\,\mathrm{dB}$ resulted in a tripled single-shot Shannon limit. Traveling wave parametric amplifiers (TWPAs) can provide a higher dynamic range with input powers up to $P_{\mathrm{max}} = -92\,\mathrm{dBm}$ for the gain range similar to this work ($12-15\,\mathrm{dB}$) [150]. If we follow the procedure presented in Sec. 3.3.5, we can calculate the maximum displacement variance, so that the signal powers of 99.7% of the symbols are below the 1-dB compression point. From $P_{\mathrm{sig},3\alpha} = (\Delta f)hf(|3\alpha|^2 + \sinh^2(r))$, the resulting maximum displacement variance for $P_{\mathrm{sig},3\alpha} = P_{\mathrm{max}} = -92\,\mathrm{dBm}$, $\Delta f = 400\,\mathrm{kHz}$ at $f = 5.2\,\mathrm{GHz}$ is $\sigma^2_{\mathrm{disp}} = 5 \times 10^4$ photons.

However, the security of the protocol requires that the displacement variance agrees with the variance of the antisqueezed quadrature $\sigma^2_{\mathrm{disp}} + \sigma^2_{\mathrm{S}} = \sigma^2_{\mathrm{AS}}$ (see Sec. 2.3.3). Therefore, the maximally achievable squeezing level by the squeezing JPA S_{max} with a high purity μ determines the upper bound for the displacement variance. If we estimate from Fig. 3.8 a maximal squeezing level of $S_{\mathrm{max}} = 10\,\mathrm{dB}$, the maximal displacement variance is bound by $\sigma^2_{\mathrm{disp,max}} = \sigma^2_{\mathrm{A,max}} - \sigma^2_{\mathrm{S,min}} = 4 \cdot (10^{S_{\mathrm{max}}/10} - 10^{-S_{\mathrm{max}}/10}) = 39.6$ photons. A constant squeezing level for a displacement power of up to 160 photons was demonstrated in Ref. 46. Therefore, we can assume that it is possible to sample squeezed displaced states from a displacement variance of $\sigma^2_{\mathrm{disp}} = 39.6$. This would be a major increase considering that this work uses at most $\sigma^2_{\mathrm{disp}} = 1.4$.

4.4.3 Increased repetition rate

Finally, the repetition rate f_{r} (symbols/s) can be improved. The current setup is limited by the phase stabilization time of the two JPAs and the communication latency between the CPU and the FPGA, since the FPGA has no synchronized digital bus during runtime (see Sec. 4.3.4).

For FPGAs that allow for synchronized digital signal transmission, the effective sampling rate is only limited by the window size of the finite impulse response (FIR) filter if we assume a slower random phase error drift in an optimal setup. In the FPGA unit (PXIe 7975), the FIR filter acts as a band-pass filter, where the signals are digitized at the sampling frequency $f_{\mathrm{S}} = 250\,\mathrm{MHz}$ with a vertical resolution of 14 bit (see Sec. 3.2.3). Recent FPGA models are capable of sampling frequencies of up to $f_{\mathrm{S,opt}} = 6.4\,\mathrm{GHz}$ (e.g. PXIe-5775 by National Instruments) with a vertical resolution of 12 bit. Most importantly, modern chassis (e.g. PXIe-1088) connect embedded controllers with the data acquisition unit over internal high-bandwidth digital bus connections (e.g. $8\,\mathrm{GB/s}$ for PXIe-8861). Hence, the synchronized measurement of statistically independent symbols is no longer limiting the repetition rate. We estimate an increased symbol sampling rate for a Hamming window size of $M = 90$ samplesof $f_{\mathrm{r,opt}} = f_{\mathrm{S,opt}}/M = 71.1\,\mathrm{MS/s}$.

4.4.4 Variable quantum channel transmissivity

In our experiments, we model the quantum channel (see Sec. 2.3.5) by the second directional coupler (see Sec. 3.3.4), with transmissivity $\tau = 0.99$. The ultimate bound for the secret key over a lossy channel with transmissivity τ is given by the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound for the secret key capacity $-\log_2(1-\tau)$ [39]. This bounds the maximal secret key from above by $\mathcal{K}_{\mathrm{max}} < 6.6$ bits per channel use. As it is the ultimate bound, it is not surprising that we fall below it. Future experiments with variable transmissivities τ could evaluate how the secret key capacity of the protocol relates to the PLOB bound.

5 Conclusion and Outlook

In this work, we have implemented a microwave ($f_0 = 5.5231\,\mathrm{GHz}$) continuous-variable quantum key distribution (CV-QKD) protocol which encodes classical information in the displacement amplitude of Gaussian-modulated propagating displaced squeezed states. The goal of this thesis has been to achieve the single-shot detection of the involved microwave quantum states and perform the aforementioned QKD protocol with it.

To this end, we have used a flux-driven Josephson parametric amplifier (JPA) in the phase-sensitive regime for an improved microwave readout. By using this approach, we have observed a significant reduction of the quadrature-dependent amplification noise, measured in terms of average number of added photons, from 10 ($\eta < 5\%$) to 0.81 ($\eta = 38\%$). This corresponds to an increase of the SNR from 14% to 177%. In the subsequent experiments, we have observed positive secret keys in the CV-QKD protocol, providing direct evidence for unconditional security in the microwave regime. These experiments have been performed with microwave signals with a power of up to 1.4 photons on average corresponding to the squeezing level of $S = 5.2\,\mathrm{dB}$ below the vacuum limit and a detection bandwidth of $400\,\mathrm{kHz}$. Furthermore, we have investigated and proved the robustness of our protocol to reasonable imperfections and eavesdropping in microwave quantum channels. The extracted secret key capacity, $\mathcal{K}_{\mathrm{exp}} = 0.63 \pm 0.11$ (bits/channel use) agrees well with the estimated Shannon capacity, $\mathcal{K} = 0.67$ (bits/channel use). With these positive secret keys, we have fulfilled our initial goal of single-shot microwave CV-QKD. Our experiments have demonstrated that microwave CV-QKD is experimentally feasible and possesses a large potential for future applications.

In perspective, microwave CV-QKD protocols can become an important part of future 5G/6G networks due to their frequency compatibility [151] and can even outperform optical counterparts [152]. In future experiments, the secret key can benefit from using more advanced superconducting quantum devices with high detection efficiencies, such as traveling wave parametric amplifiers or microwave single-photon detectors. Our results uncover and motivate a novel exciting field of microwave quantum key distribution.

A Appendix

A.1 Moyal equation in presence of harmonic forces

The phase-space formulation of the Liouville–von Neumann equation

$$i\hbar\frac{\partial\rho}{\partial t} = [H,\rho]. \tag{A.1}$$

is given by the Moyal equation [153]

$$\frac{\partial W(q,p,t)}{\partial t} = -\{\{W(q,p,t), H(q,p)\}\}, \tag{A.2}$$

where $\{\{\ ,\ \}\}$ is the Moyal bracket, and $\{\ ,\ \}$ the Poisson bracket. The analogy to the classical Liouville equation (see Ref. 154) is remarkable, when considering that the equation of motion for each point in the phase space is classical in presence of strictly harmonic forces [155]

$$\frac{\partial W(q,p)}{\partial t} = -p\frac{\partial W(q,p)}{\partial q}. \tag{A.3}$$

The solution is an oscillation around the center of the phase-space.

A.2 Displacement operator

A coherent state is defined as [52]

$$|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right)\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,. \tag{A.4}$$

The Fock state $|n\rangle$ can be obtained from consequent applications of the creation operator $\hat{a}^\dagger$ on the vacuum state $|0\rangle$ as [52]

$$|n\rangle = \left[(\hat{a}^\dagger)^n/\sqrt{n!}\right]|0\rangle\,. \tag{A.5}$$

We substitute $|n\rangle$, and rewrite the coherent state as [51]

$$|\alpha\rangle = e^{\alpha a^\dagger}\,|0\rangle\,e^{-|\alpha|^2/2}, \tag{A.6}$$

where the exponential on the left can be extended with the invariant term $\exp(-\alpha^* \hat{a})$, so that [51]

$$|\alpha\rangle = D(\alpha)\,|0\rangle \quad \text{with} \quad D(\alpha) = e^{-|\alpha|^2/2+\alpha\hat{a}^\dagger-\alpha^*\hat{a}}. \tag{A.7}$$

Using the Baker-Hausdorff formula $e^{A+B} = e^{-[A,B]/2}e^{A}e^{B}$ for two operators A, B it follows that [51]

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger-\alpha^*\hat{a}}. \tag{A.8}$$

A.3 Added noise mode in a nondegenerate bosonic amplifier

We briefly outline why an additional idler mode $\hat{b}_{\text{in}}$ is required to fulfill the commutation relation at the output of a phase-preserving amplifier following Refs. 86, 92. We start with defining a single-mode electric field in terms of the photon ladder operators $\hat{a}$ and $\hat{a}^\dagger$ as in Eq. 2.3

$$\hat{E}(t) = E_0\left[\hat{a}e^{i\omega t} + \hat{a}^\dagger e^{-i\omega t}\right]. \tag{A.9}$$

We describe the bosonic input mode of the amplifier as $\hat{a} = \hat{a}_{\text{in}}$. The output mode is $\hat{a} = \hat{a}_{\text{out}}$. The signals are described by the expectation values of input $\langle\hat{a}_{\text{in}}\rangle$ and output $\langle\hat{a}_{\text{out}}\rangle$ mode. The symmetrized noise for $\hat{a}$ is given by [86]

$$(\Delta a)^2 = \frac{1}{2}\langle\{\hat{a},\hat{a}^\dagger\}\rangle - |\langle\hat{a}\rangle|^2, \tag{A.10}$$

We have to fulfill two conditions [86]:

(i) Both modes have to obey the bosonic commutation relation $\left[\hat{a},\hat{a}^\dagger\right] = 1$.

(ii) The relation between the input and output modes must be linear, as the amplifier is phase-preserving. Therefore is has to hold that $\hat{a}_{\text{out}} = \sqrt{G}\hat{a}_{\text{in}}$ and $\hat{a}^\dagger_{\text{out}} = \sqrt{G}\hat{a}^\dagger_{\text{in}}$, where G is the dimensionless photon-number gain of the bosonic amplifier.

In the current input-output model, condition (ii) violates condition (i). We can see this by inserting (ii) into the commutation relation of the output mode [86]

$$\left[\hat{a}_{\text{out}},\hat{a}^\dagger_{\text{out}}\right] \overset{!}{=} 1 \tag{A.11}$$

$$\left[\hat{a}_{\text{out}},\hat{a}^\dagger_{\text{out}}\right] \overset{(i)}{=} \left[\sqrt{G}\hat{a}_{\text{in}},\sqrt{G}\hat{a}^\dagger_{\text{in}}\right] = G \quad ↯, \tag{A.12}$$

which is a contradiction. To account for the factor G while fulfilling the necessary condition (i), we have to add an additional noise operator $\hat{\mathcal{F}}$ to the phase-preserving amplification condition as [86]

$$\hat{a}_{\text{out}} = \sqrt{G}\hat{a}_{\text{in}} + \hat{\mathcal{F}}, \quad \hat{a}^\dagger_{\text{out}} = \sqrt{G}\hat{a}^\dagger_{\text{in}} + \hat{\mathcal{F}}^\dagger. \tag{A.13}$$

The minimum possible noise can be obtained by considering that $\hat{\mathcal{F}}$ is uncorrelated to the input signal. It follows that the noise operator commutes with the signal input mode $\left[\hat{\mathcal{F}}, \hat{a}\right] = \left[\hat{\mathcal{F}}, \hat{a}_{\text{in}}^\dagger\right] = 0$. Now, we can successfully enforce the bosonic commutation relation as

$$\begin{aligned}
&\left[\hat{a}_{\text{out}}, \hat{a}_{\text{out}}^\dagger\right] \overset{!}{=} 1 \\
&\left[\hat{a}_{\text{out}}, \hat{a}_{\text{out}}^\dagger\right] \overset{A.13}{=} \left[\sqrt{G}\hat{a}_{\text{in}} + \hat{\mathcal{F}}, \sqrt{G}\hat{a}_{\text{in}}^\dagger + \hat{\mathcal{F}}^\dagger\right] \\
&\qquad = G\underbrace{\left[\hat{a}_{\text{in}}, \hat{a}_{\text{in}}^\dagger\right]}_{=1} + \left[\hat{\mathcal{F}}, \hat{\mathcal{F}}^\dagger\right] + \underbrace{\sqrt{G}\left(\left[\hat{a}_{\text{in}}, \hat{\mathcal{F}}^\dagger\right] + \left[\hat{a}_{\text{in}}^\dagger, \hat{\mathcal{F}}\right]\right)}_{=0} \checkmark \\
&\Rightarrow \left[\hat{\mathcal{F}}, \hat{\mathcal{F}}^\dagger\right] = 1 - G.
\end{aligned} \tag{A.14}$$

We can find a lower bound for the noise of the output mode $(\Delta b)^2$ by using A.13 in A.10

$$\begin{aligned}
(\Delta\hat{a}_{\text{out}})^2 &= G(\Delta a_{\text{in}})^2 + \frac{1}{2}\langle\{\hat{\mathcal{F}}, \hat{\mathcal{F}}^\dagger\}\rangle \\
&\geq G(\Delta a_{\text{in}})^2 + \frac{1}{2}|\langle\{\hat{\mathcal{F}}, \hat{\mathcal{F}}^\dagger\}\rangle|.
\end{aligned} \tag{A.15}$$

We note that for no gain $G = 1$, no noise needs to be added. In the limit of large amplification ($G \gg$1), the gain is dominating the added noise $|G - 1| \simeq G$. Then we can write [86]

$$(\Delta a_{\text{out}})^2 \geq G\left((\Delta a_{\text{in}})^2 + \frac{1}{2}\right). \tag{A.16}$$

The contribution of $\frac{1}{2}$ is half an added noise quantum, which defines the standard quantum limit. It is convenient to write the noise operator in terms of an auxiliary bosonic mode $\hat{b}_{\text{in}}$ as

$$\hat{\mathcal{F}} = \sqrt{G-1}\hat{b}_{\text{in}}^\dagger, \quad \hat{\mathcal{F}}^\dagger = \sqrt{G-1}\hat{b}_{\text{in}}. \tag{A.17}$$

Bibliography

[1] N. J. Cerf, M. Lévy, and G. V. Assche, *Quantum distribution of Gaussian keys using squeezed states*, Physical Review A **63**, 052311 (2001).

[2] N. Gisin and R. Thew, *Quantum communication*, Nature Photonics **1**, 165 (2007).

[3] J. Preskill, *Quantum Computing in the NISQ era and beyond*, Quantum **2**, 79 (2018).

[4] V. Giovannetti, S. Lloyd, and L. Maccone, *Advances in quantum metrology*, Nature Photonics **5**, 222 (2011).

[5] O. Nairz, M. Arndt, and A. Zeilinger, *Experimental verification of the Heisenberg uncertainty principle for fullerene molecules*, Physical Review A **65** (2002).

[6] A. Zeilinger, *Experiment and the foundations of quantum physics*, Reviews of Modern Physics **71**, S288 (1999).

[7] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, *Quantum entanglement*, Reviews of Modern Physics **81**, 865 (2009).

[8] W. Heisenberg, in *The Physicist's Conception of Nature* (Springer Netherlands, 1973) pp. 264–275.

[9] K. Zuse, *The Computer - My Life* (Springer Berlin Heidelberg, 2010).

[10] C. E. Shannon, N. J. A. Sloane, and A. D. Wyner, *Claude Elwood Shannon: Collected Papers* (IEEE Press, 1993).

[11] C. E. Shannon, *A Mathematical Theory of Communication*, Bell System Technical Journal **27**, 379 (1948).

[12] S. M. Bellovin, *Frank Miller: Inventor of the One-Time Pad*, Cryptologia **35**, 203 (2011).

[13] C. E. Shannon, *Communication Theory of Secrecy Systems*, Bell System Technical Journal **28**, 656 (1949).

[14] W. Diffie and M. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory **22**, 644 (1976).

[15] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM **21**, 120 (1978).

[16] P. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, *Proceedings 35th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society Press , 124 (2002).

[17] R. P. Feynman, *Simulating physics with computers*, International Journal of Theoretical Physics **21**, 467 (1982).

[18] W. G. Unruh, *Maintaining coherence in quantum computers*, Physical Review A **51**, 992 (1995).

[19] P. W. Shor, *Scheme for reducing decoherence in quantum computer memory*, Physical Review A **52**, R2493 (1995).

[20] P. Shor, *Fault-tolerant quantum computation*, in *Proceedings of 37th Conference on Foundations of Computer Science* (IEEE Computer Society Press, 1996).

[21] P. W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM Journal on Computing **26**, 1484 (1997).

[22] Information Technology Laboratory (National Institute of Standards and Technology), *Announcing the Advanced Encryption Standard (AES)* (Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, MD, 2001).

[23] A. S. Holevo, *Bounds for the quantity of information transmitted by a quantum communication channel*, Problemy Peredachi Informatsii **9**, 3 (1973).

[24] A. Holevo, *The capacity of the quantum channel with general signal states*, IEEE Transactions on Information Theory **44**, 269 (1998).

[25] B. Schumacher and M. D. Westmoreland, *Sending classical information via noisy quantum channels*, Physical Review A **56**, 131 (1997).

[26] C. H. Bennett, G. Brassard, and N. D. Mermin, *Quantum cryptography without Bell's theorem*, Physical Review Letters **68**, 557 (1992).

[27] S. Wiesner, *Conjugate coding*, ACM SIGACT News **15**, 78 (1983).

[28] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Theoretical Computer Science **560**, 7 (2014).

[29] J. L. Park, *The concept of transition in quantum mechanics*, Foundations of Physics **1**, 23 (1970).

[30] W. H. Zurek, *A single quantum cannot be cloned*, Nature **246**, 170 (1973).

[31] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned*, Nature **299**, 802 (1982).

[32] P. W. Shor and J. Preskill, *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*, Physical Review Letters **85**, 441 (2000).

[33] A. K. Ekert, *Quantum cryptography based on Bell's theorem*, Physical Review Letters **67**, 661 (1991).

[34] T. C. Ralph, *Continuous variable quantum cryptography*, Physical Review A **61** (1999).

[35] G. VanAssche, J. Cardinal, and N. Cerf, *Reconciliation of a Quantum-Distributed Gaussian Key*, IEEE Transactions on Information Theory **50**, 394 (2004).

[36] D. Gottesman and J. Preskill, *Secure quantum key distribution using squeezed states*, Physical Review A **63** (2001).

[37] F. Grosshans and P. Grangier, *Continuous Variable Quantum Cryptography Using Coherent States*, Physical Review Letters **88** (2002).

[38] S. Pirandola, S. L. Braunstein, and S. Lloyd, *Characterization of collective gaussian attacks and security of coherent-state quantum cryptography*, Physical Review Letters **101**, 1 (2008).

[39] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Fundamental limits of repeaterless quantum communications*, Nature Communications **8** (2017).

[40] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, *Quantum key distribution using gaussian-modulated coherent states*, Nature **421**, 238 (2003).

[41] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu, and H. Guo, *Continuous-variable QKD over 50 km commercial fiber*, Quantum Science and Technology **4**, 035006 (2019).

[42] *IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012) , 1 (2016).

[43] R. Tafazolli, C.-L. Wang, and P. Chatzimisios, eds., *Wiley 5G Ref* (Wiley, 2019).

[44] P. Krantz, M. Kjaergaard, F. Yan, T. P. Orlando, S. Gustavsson, and W. D. Oliver, *A quantum engineer's guide to superconducting qubits*, Applied Physics Reviews **6**, 021318 (2019).

[45] M. A. Castellanos-Beltran, K. D. Irwin, G. C. Hilton, L. R. Vale, and K. W. Lehnert, *Amplification and squeezing of quantum noise with a tunable Josephson metamaterial*, Nature Physics **4**, 929 (2008).

[46] 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, and R. Gross, *Displacement of Propagating Squeezed Microwave States*, Physical Review Letters **117**, 1 (2016).

[47] 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, and R. Gross, *Secure quantum remote state preparation of squeezed microwave states*, Nature Communications **10** (2019).

[48] K. G. Fedorov, M. Renger, S. Pogorzalek, R. D. Candia, Q. Chen, Y. Nojiri, K. Inomata, Y. Nakamura, M. Partanen, A. Marx, R. Gross, and F. Deppe, *Experimental quantum teleportation of propagating microwaves*, Science Advances **7** (2021).

[49] F. Fesquet, *Experimental implementation of a quantum key distribution with squeezed microwaves*, Masters thesis, Technische Universität München (2020).

[50] T. Yamamoto, K. Inomata, M. Watanabe, K. Matsuba, T. Miyazaki, W. D. Oliver, Y. Nakamura, and J. S. Tsai, *Flux-driven Josephson parametric amplifier*, Applied Physics Letters **93**, 042510 (2008).

[51] M. O. Scully and M. S. Zubairy, *Quantum optics* (Cambridge University Press, Cambridge, 1997).

[52] D. F. Walls and G. J. Milburn, *Quantum optics* (Springer, Berlin Heidelberg, 2008).

[53] L. S. Braunstein and P. Van Loock, *Quantum information with continuous variables*, Reviews of Modern Physics **77**, 513 (2005).

[54] W. Heisenberg, *Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik*, Zeitschrift für Physik **43**, 172 (1927).

[55] E. Wigner, *On the quantum correction for thermodynamic equilibrium*, Physical Review **40**, 749 (1932).

[56] G. S. Agarwal and E. Wolf, *Calculus for Functions of Noncommuting Operators and General Phase-Space Methods in Quantum Mechanics. II. Quantum Mechanics in Phase Space*, Physical Review D **2**, 2187 (1970).

[57] E. Lukacs, *Characteristic functions* (Oxford University Press, 1987).

[58] W. Rudin, *Fourier Analysis on Groups* (John Wiley & Sons, Inc., 1990).

[59] N. Dangniam and C. Ferrie, *Quantum Bochner's theorem for phase spaces built on projective representations*, Journal of Physics A: Mathematical and Theoretical **48**, 115305 (2015).

[60] R. Hudson, *When is the wigner quasi-probability density non-negative?*, Reports on Mathematical Physics **6**, 249 (1974).

[61] F. Soto and P. Claverie, *When is the Wigner function of multidimensional systems nonnegative?*, Journal of Mathematical Physics **24**, 97 (1983).

[62] A. Mandilara, E. Karpov, and N. J. Cerf, *Extending Hudson's theorem to mixed quantum states*, Physical Review A **79**, 062302 (2009).

[63] A. Holevo, *Some statistical problems for quantum Gaussian states*, IEEE Transactions on Information Theory **21**, 533 (1975).

[64] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Gaussian quantum information*, Reviews of Modern Physics **84**, 621 (2012).

[65] V. Bužek, G. Adam, and G. Drobný, *Reconstruction of wigner functions on different observation levels*, Annals of Physics **245**, 37 (1996).

[66] A. Wunsche, *Reconstruction of operators from their normally ordered moments for a single boson mode*, Quantum Optics: Journal of the European Optical Society Part B **2**, 453 (1990).

[67] V. Bužek, G. Adam, and G. Drobný, *Quantum state reconstruction and detection of quantum coherences on different observation levels*, Physical Review A - Atomic, Molecular, and Optical Physics **54**, 804 (1996).

[68] C. W. Gardiner and P. Zoller, *Quantum noise : a handbook of Markovian and non-Markovian quantum stochastic methods with applications to quantum optics* (Springer, Berlin, 2000).

[69] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2009).

[70] A. S. Holevo, *Quantum systems, channels, information : a mathematical introduction* (De Gruyter, Berlin, 2012).

[71] A. S. Holevo and R. F. Werner, *Evaluating capacities of bosonic Gaussian channels*, Physical Review A **63**, 032312 (2001).

[72] H. Nyquist, *Thermal agitation of electric charge in conductors*, Physical Review **32**, 110 (1928).

[73] R. J. Glauber, *Coherent and Incoherent States of the Radiation Field*, Physical Review **131**, 2766 (1963).

[74] M. G. Paris, *Displacement operator by beam splitter*, Physics Letters, Section A: General, Atomic and Solid State Physics **217**, 78 (1996).

[75] S. Pogorzalek, *Remote State Preparation of Squeezed Microwave States*, Phd thesis, Technische Universität München (2020).

[76] A. Einstein, B. Podolsky, and N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Physical Review **47**, 777 (1935).

[77] Z. Y. Ou, S. F. Pereira, H. J. Kimble, and K. C. Peng, *Realization of the Einstein-Podolsky-Rosen paradox for continuous variables*, Physical Review Letters **68**, 3663 (1992).

[78] U. Leonhardt, *Measuring the Quantum State of Light* (Cambridge University Press, 2003).

[79] A. I. Lvovsky and M. G. Raymer, *Continuous-variable optical quantum-state tomography*, Reviews of Modern Physics **81**, 299 (2009).

[80] B. Royer, A. L. Grimsmo, A. Choquette-Poitevin, and A. Blais, *Itinerant Microwave Photon Detector*, Physical Review Letters **120** (2018).

[81] S. Kono, K. Koshino, Y. Tabuchi, A. Noguchi, and Y. Nakamura, *Quantum non-demolition detection of an itinerant microwave photon*, Nature Physics **14**, 546 (2018).

[82] E. P. K. Menzel, *Propagating Quantum Microwaves: Dual-path State Reconstruction and Path Entanglement*, Diploma thesis, Technische Universität München (2013).

[83] M. Renger, S. Pogorzalek, Q. Chen, Y. Nojiri, K. Inomata, Y. Nakamura, M. Partanen, A. Marx, R. Gross, F. Deppe, and K. G. Fedorov, *Beyond the standard quantum limit of parametric amplification*, (2020), arXiv:2011.00914v3 .

[84] D. M.Pozar, *Microwave Engineering, 4th Edition*, 4th ed. (Wiley, 2011).

[85] Y. Jin, Q. Dong, Y. X. Liang, A. Cavanna, U. Gennser, L. Couraud, and C. Ulysse, *Ultra-low noise HEMTs for high-impedance and low- frequency preamplifiers: realization and characterization from 4.2 K to 77 K*, Journal of Physics: Conference Series **568**, 032009 (2014).

[86] A. A. Clerk, M. H. Devoret, S. M. Girvin, F. Marquardt, and R. J. Schoelkopf, *Introduction to quantum noise, measurement, and amplification*, Reviews of Modern Physics **82**, 1155 (2010).

[87] P. Horowitz, *The art of electronics* (Cambridge University Press, Cambridge England New York, 1989).

[88] W. B. Case, *The pumping of a swing from the standing position*, American Journal of Physics **64**, 215 (1996).

[89] T. Yamamoto, K. Koshino, and Y. Nakamura, in *Principles and Methods of Quantum Information Technologies* (Springer Japan, 2016) pp. 495–513.

[90] B. Yurke, L. R. Corruccini, P. G. Kaminsky, L. W. Rupp, A. D. Smith, A. H. Silver, R. W. Simon, and E. A. Whittaker, *Observation of parametric amplification and deamplification in a Josephson parametric amplifier*, Physical Review A **39**, 2519 (1989).

[91] H. A. Haus and J. A. Mullen, *Quantum Noise in Linear Amplifiers*, Physical Review **128**, 2407 (1962).

[92] C. M. Caves, *Quantum limits on noise in linear amplifiers*, Physical Review D **26**, 1817 (1982).

[93] Z. R. Lin, K. Inomata, W. D. Oliver, K. Koshino, Y. Nakamura, J. S. Tsai, and T. Yamamoto, *Single-shot readout of a superconducting flux qubit with a flux-driven Josephson parametric amplifier*, Applied Physics Letters **103**, 132602 (2013).

[94] Z. Lin, K. Inomata, K. Koshino, W. Oliver, Y. Nakamura, J. Tsai, and T. Yamamoto, *Josephson parametric phase-locked oscillator and its application to dispersive readout of superconducting qubits*, Nature Communications **5** (2014).

[95] P. Krantz, A. Bengtsson, M. Simoen, S. Gustavsson, V. Shumeiko, W. D. Oliver, C. M. Wilson, P. Delsing, and J. Bylander, *Single-shot read-out of a superconducting qubit using a Josephson parametric oscillator*, Nature Communications **7** (2016).

[96] 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, and R. Gross, *Squeezing with a flux-driven Josephson parametric amplifier*, New Journal of Physics **15**, 125013 (2013).

[97] 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, and R. Gross, *Hysteretic Flux Response and Nondegenerate Gain of Flux-Driven Josephson Parametric Amplifiers*, Physical Review Applied **8**, 024012 (2017).

[98] W. Meissner and R. Ochsenfeld, *Ein neuer Effekt bei Eintritt der Supraleitfähigkeit*, Die Naturwissenschaften **21**, 787 (1933).

[99] Z. Charifoulline, *Residual Resistivity Ratio (RRR) Measurements of LHC Superconducting NbTi Cable Strands*, IEEE Transactions on Applied Superconductivity **16**, 1188 (2006).

[100] J. F. Cochran and D. E. Mapother, *Superconducting Transition in Aluminum*, Physical Review **111**, 132 (1958).

[101] B. D. Josephson, *Possible new effects in superconductive tunnelling*, Physics Letters **1**, 251 (1962).

[102] R. Gross and A. Marx, *Festkörperphysik* (Oldenbourg Verlag, München, München, 2012).

[103] Y. Makhlin, G. Schön, and A. Shnirman, *Quantum-state engineering with Josephson-junction devices*, Reviews of Modern Physics **73**, 357 (2001).

[104] Michael Tinkham, *Introduction to superconductivity* (1996).

[105] J. Clarke and A. I. Braginski, eds., *The SQUID Handbook* (Wiley, 2004).

[106] M. Sandberg, C. M. Wilson, F. Persson, T. Bauch, G. Johansson, V. Shumeiko, T. Duty, and P. Delsing, *Tuning the field in a microwave resonator faster than the photon lifetime*, Applied Physics Letters **92**, 3 (2008).

[107] M. Göppl, A. Fragner, M. Baur, R. Bianchetti, S. Filipp, J. M. Fink, P. J. Leek, G. Puebla, L. Steffen, and A. Wallraff, *Coplanar waveguide resonators for circuit quantum electrodynamics*, Journal of Applied Physics **104** (2008).

[108] D. S. Wisbey, J. Gao, M. R. Vissers, F. C. S. da Silva, J. S. Kline, L. Vale, and D. P. Pappas, *Effect of metal/substrate interfaces on radio-frequency loss in superconducting coplanar waveguides*, Journal of Applied Physics **108**, 093918 (2010).

[109] C. L. Holloway and E. F. Kuester, *Edge shape effects and quasi-closed form expressions for the conductor loss of microstrip lines*, Radio Science **29**, 539 (1994).

[110] 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, and R. Gross, *Loss mechanisms in superconducting thin film microwave resonators*, Journal of Applied Physics **119**, 015304 (2016).

[111] J. Bourassa, F. Beaudoin, J. M. Gambetta, and A. Blais, *Josephson-junction-embedded transmission-line resonators: From Kerr medium to in-line transmon*, Physical Review A - Atomic, Molecular, and Optical Physics **86**, 1 (2012).

[112] M. Wallquist, V. S. Shumeiko, and G. Wendin, *Selective coupling of superconducting charge qubits mediated by a tunable stripline cavity*, Physical Review B - Condensed Matter and Materials Physics **74**, 1 (2006).

[113] W. Wustmann and V. Shumeiko, *Parametric resonance in tunable superconducting cavities*, Physical Review B - Condensed Matter and Materials Physics **87**, 1 (2013).

[114] S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. Usenko, G. Vallone, P. Villoresi, and P. Wallden, *Advances in Quantum Cryptography*, Advances in Optics and Photonics , 1 (2020).

[115] N. J. Cerf, A. Ipe, and X. Rottenberg, *Cloning of continuous quantum variables*, Physical Review Letters **85**, 1754 (2000).

[116] E. Jaynes, *Prior Probabilities*, IEEE Transactions on Systems Science and Cybernetics **4**, 227 (1968).

[117] G. E. Uhlenbeck, N. Rosenzweig, A. J. F. Siegert, E. T. Jaynes, and S. Fujita, *Lectures in Theoretical Physics: Statistical Physics* (1962) p. 43.

[118] J. V. Neumann, *Mathematical Foundations of Quantum Mechanics* (Princeton University Press, 1996).

[119] A. Wehrl, *General properties of entropy*, Reviews of Modern Physics **50**, 221 (1978).

[120] J. Preskill, *Quantum Shannon Theory*, (2016), arXiv:1604.07450v3 .

[121] Y. Li and P. Busch, *Von Neumann entropy and majorization*, Journal of Mathematical Analysis and Applications **408**, 384 (2013).

[122] A. Serafini, F. Illuminati, and S. D. Siena, *Symplectic invariants, entropic measures and correlations of Gaussian states*, Journal of Physics B: Atomic, Molecular and Optical Physics **37**, L21 (2004).

[123] C. Shannon, *Communication in the Presence of Noise*, Proceedings of the IRE **37**, 10 (1949).

[124] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, 2016).

[125] A. C. Rencher and G. B. Schaalje, *Linear Models in Statistics* (John Wiley and Sons, 2007).

[126] R. Garcia-Patron Sanchez, *Quantum Information with Optical Continuous Variables: from Bell Tests to Key Distributions*, Ph.D. thesis (2007).

[127] W. F. Stinespring, *Positive Functions on C -Algebras*, Proceedings of the American Mathematical Society **6**, 211 (1955).

[128] V. Paulsen, *Completely Bounded Maps and Operator Algebras* (Cambridge University Press, 2003).

[129] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, *Direct and Reverse Secret-Key Capacities of a Quantum Channel*, Physical Review Letters **102** (2009).

[130] R. Renner, *Symmetry of large physical systems implies independence of subsystems*, Nature Physics **3**, 645 (2007).

[131] R. Renner and J. I. Cirac, *De Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography*, Physical Review Letters **102**, 110504 (2009).

[132] B. Demoen, P. Vanheuverzwijn, and A. Verbeure, *Completely positive maps on the CCR-algebra*, Letters in Mathematical Physics **2**, 161 (1977).

[133] G. Lindblad, *Cloning the quantum oscillator*, Journal of Physics A: Mathematical and General **33**, 5059 (2000).

[134] A. S. Holevo, *One-mode quantum Gaussian channels: Structure and quantum capacity*, Problems of Information Transmission **43**, 1 (2007).

[135] N. J. Cerf, *Quantum Cloning with Continuous Variables*, *Quantum Information with Continuous Variables*, **1**, 277 (2003).

[136] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, *Continuous-Variable Quantum Key Distribution with Gaussian Modulation-The Theory of Practical Implementations*, Advanced Quantum Technologies **1**, 1800011 (2018).

[137] C. Pfister, N. Lütkenhaus, S. Wehner, and P. J. Coles, *Sifting attacks in finite-size quantum key distribution*, New Journal of Physics **18**, 053001 (2016).

[138] H.-K. Lo, H. Chau, and M. Ardehali, *Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security*, Journal of Cryptology **18**, 133 (2004).

[139] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, *Quantum key distribution over 25 km with an all-fiber continuous-variable system*, Physical Review A - Atomic, Molecular, and Optical Physics **76**, 1 (2007).

[140] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The security of practical quantum key distribution*, Reviews of Modern Physics **81**, 1301 (2009).

[141] F. Pobell, *Matter and Methods at Low Temperatures* (Springer Berlin Heidelberg, 2007).

[142] F. Simon, *Behaviour of Condensed Helium near Absolute Zero*, Nature **133**, 529 (1934).

[143] *Thermodynamic properties and melting of solid helium*, Proceedings of the Royal Society of London. Series A. Mathematical and Physical Sciences **218**, 291 (1953).

[144] M. Á. A. Caballero, *A Setup for Quantum Signal Detection in a Circuit QED Architecture*, Diploma thesis, Technische Universität München (2008).

[145] 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, and R. Gross, *Path Entanglement of Continuous-Variable Quantum Microwaves*, Physical Review Letters **109**, 250502 (2012).

[146] C. Eichler, Y. Salathe, J. Mlynek, S. Schmidt, and A. Wallraff, *Quantum-Limited Amplification and Entanglement in Coupled Nonlinear Resonators*, Physical Review Letters **113**, 110502 (2014).

[147] M. Mariantoni, E. P. Menzel, F. Deppe, M. Á. Araque Caballero, A. Baust, T. Niemczyk, E. Hoffmann, E. Solano, A. Marx, and R. Gross, *Planck Spectroscopy and Quantum Noise of Microwave Beam Splitters*, Physical Review Letters **105**, 133601 (2010).

[148] S. Boutin, D. M. Toyli, A. V. Venkatramani, A. W. Eddins, I. Siddiqi, and A. Blais, *Effect of Higher-Order Nonlinearities on Amplification and Squeezing in Josephson Parametric Amplifiers*, Physical Review Applied **8**, 054030 (2017).

[149] B. A. Kochetov and A. Fedorov, *Higher-order nonlinear effects in a Josephson parametric amplifier*, Physical Review B **92**, 224304 (2015).

[150] T. C. White, J. Y. Mutus, I.-C. Hoi, R. Barends, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, E. Jeffrey, J. Kelly, A. Megrant, C. Neill, P. J. J. O'Malley, P. Roushan, D. Sank, A. Vainsencher, J. Wenner, S. Chaudhuri, J. Gao, and J. M. Martinis, *Traveling wave parametric amplifier with Josephson junctions using minimal resonator phase matching*, Applied Physics Letters **106**, 242601 (2015).

[151] C. D. Alwis, A. Kalla, Q.-V. Pham, P. Kumar, K. Dev, W.-J. Hwang, and M. Liyanage, *Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research*, IEEE Open Journal of the Communications Society **2**, 836 (2021).

[152] F. Fesquet, F. Kronowetter, M. Renger, Q. Chen, K. Honasoge, O. Gargiulo, Y. Nojiri, A. Marx, F. Deppe, R. Gross, and K. G. Fedorov, *Perspectives of microwave quantum key distribution in open-air*, (2022), arXiv:2203.05530 .

[153] J. E. Moyal, *Quantum mechanics as a statistical theory*, Mathematical Proceedings of the Cambridge Philosophical Society **45**, 99 (1949).

[154] H. Goldstein, C. Poole, and J. Safko, *Classical Mechanics* (Pearson Education Limited, 2013).

[155] M. te Vrugt, G. I. Tóth, and R. Wittkowski, *Master equations for Wigner functions with spontaneous collapse and their relation to thermodynamic irreversibility*, Journal of Computational Electronics **20**, 2209 (2021).

Acknowledgments

I had a lot of fun and learned many new things at the Walther-Meissner-Institute. This thesis would not have been possible without the help, knowledge, and support of several people accompanying me during the last year. In particular, I would like to thank:

Prof. Dr. Rudolf Gross for giving me the opportunity to complete my Master's thesis at the Walther-Meißner-Institut. I am thankful for his support and advice. His vast efforts in teaching solid-state physics inspired me at an early stage to learn more about superconductivity and devices that exploit the principles of quantum mechanics. Our conversations about interesting research projects in the field of quantum information processing widened my horizon.

Dr. Kirill Fedorov for interesting me in a topic at the Walther-Meißner-Institut through his exceptional lectures and his ability to communicate the joy of experimental physics. He offered me the best possible introduction through my working student job, and I am grateful for him trusting me with the topic of this thesis. I benefited from his vast laboratory experience, and I will always remember dearly the exciting breakthroughs in the projects we had together. Our numerous individual discussions and meetings were indispensable towards reaching the findings of this thesis. His dedication to the success of the project was inspiring. I could always approach him both for detailed feedback, and helpful general advice.

Florian Fesquet for his never-ending endurance to communicate experimental concepts to me. I am grateful for his contagious enthusiasm for science, and him providing emotional support throughout the ups and downs. His contribution of ideas and his technical support in the lab greatly improved the success of this thesis. Our final measurements together, were one of the most exciting things that happened to me.

Fabian Kronowetter for his resilience, humor, and for providing an intuitive approach to the physics of the set up. His ability to manage our resources in the best way possible was crucial for the success of this project. I am thankful for his advice and numerous contributions.

Michael Renger for his ability to find time for theoretical discussions while he handled one of the most difficult projects I have ever seen. His intuition and curiosity about quantum physics during the Qubit seminar inspired me to consider a working student position at WMI.

Yuki Nojiri and *Kedar Honasoge* not only for their admirable work culture and light-hearted talks during lunch, but also some common programming projects for JPA characterization.

Dr. Achim Marx for his technical advice and maintaining the functionality of the cryostat. This project would not have been possible without his experience and him pulling solutions out of his sleeve whenever we needed help.

The team of the Helium hall for keeping our cryostat cold, even when technical difficulties arose. Our most important measurements would not have been possible if not for their dedicated work and creative fixes.

The team of the workshop for manufacturing parts of the sample stage and offering their advice and knowledge.

Monika Scheufele for her emotional support during my most exciting measurement weeks.

Niklas Bruckmoser for teaching me the best practices for layout. He brought a steady flow of calmness, serenity and joy to our office.

Office 108 (*Elisabeth Meidinger*, *Korbinian Rubenbauer*, *Christopher Waas*, *William Yam*) and all the other students at WMI for creating an atmosphere of productivity and fun.

All my friends and family that supported me outside of work, especially *Max*, *Anni*, *Karina*, and my brother *Alexander*. I know that I can always count on you.

My parents, who supported me throughout the course of my studies. I am very grateful for their constant encouragement.