Technische Universität München

Walther-Meißner-Institut für Tief-Temperaturforschung

Bayerische Akademie der Wissenschaften

Experimental implementation of a quantum key distribution with squeezed microwaves

Master's thesis

Florian Fesquet

Supervisor: Prof. Dr. Rudolf Gross

Advisor: Dr. Kirill Fedorov

Garching – October 8, 2020

Contents

Chapter 1

Introduction

Over the last century, quantum theory has lead to many technological advances and physical discoveries which have promoted an ever growing interest for both research and industries. Among them, the field of quantum information has become a noticeable center of attention. In particular, it includes topics such as quantum computing [1], quantum sensing [2, 3], quantum communication [4, 5] and cryptography [6]. In these fields, fundamental quantum mechanical effects such as superposition or entanglement are considered to be key resources to gain advantage over classical systems in terms of efficiency, computing power, or security of communication.

Exchange of information is at the heart of our current society and thus, it is especially relevant to make possible confidential communication, where any undesired party has no access to communicated messages. Classically, information can be encrypted and exchanged in a perfectly secure manner using classical algorithms such as the well-known one-time pad [7]. The main issue with the latter algorithm is that the data is encrypted using a key, i.e., a string of numbers, which is required to be as long as the data itself. This already limits the usage of the one-time pad for communication involving large amounts of data. Modern communication security algorithms, such as RSA [8] and its derivatives, are based on a different approach which relies on asymmetrically difficult mathematical problems. These problems are easy to solve in a direct way, such as multiplication of two large prime numbers, but difficult to reverse on a classical computer - i.e., to find the prime number multipliers of a single large number (factorization problem). In other words, the limitations on our current computing power is the main factor which guaranties secrecy in modern communications. However this picture has been changed with the arrival of quantum algorithms which make use of quantum effects. Noticeably, the now very well-known Shor algorithm [9] in principle allows for a much more efficient factorization of large numbers in comparison with the classical algorithms. This jeopardizes the security of the widely used cryptographic schemes.

For these and other reasons, the field of quantum cryptography has seen a tremendous

development over the past decades. This field investigates the secrecy of possible communication protocols using physical properties of quantum states. A particular sub-field dealing with secure distribution of keys is the field of quantum key distribution (QKD) [10]. There, the goal is to exchange a key between two parties while an external eavesdropper tries to gain information about the key. Very interestingly, such schemes can achieve unconditional security meaning an absolute security of the key, no matter how much of computational power is available to the eavesdropper [11]. One of the fundamental reasons for this security comes from the no-cloning theorem [12] which prohibits ideal copying of quantum states, meaning that the eavesdropper would necessarily have to interfere with the communicated quantum states, rendering this interaction detectable and quantifiable.

In general, QKD protocols can be experimentally implemented with any carrier of information such as electrons or molecules. However, historically, QKD protocols have been invented and extensively studied in the optical regime with optical photons [13, 11, 14]. One of the central advantages to use optical photons is a possibility for a straightforward long-distance quantum communication. However, nowadays all computational and communication hardware operates at microwave frequencies of few GHz. This is also true for most advanced up-to-date superconducting quantum computers [15]. This makes it extremely important to study QKD protocols in the aforementioned microwave range. Here, we focus on continuous variable QKD (CV-QKD) where information is stored in quantum states with a continuous spectrum of eigenstates [16]. In our experimental setups, such quantum states manifest as propagating quantum microwaves, which are generated by superconducting circuits. Among these quantum states, squeezed and displaced states [16] are particularly useful resources for CV-QKD protocols.

In our work, squeezed microwave states are generated by a flux-driven Josephson parametric amplifier (JPA) [17] composed of a superconducting resonator short-circuited to ground by a direct-current superconducting quantum interference device (dc-SQUID). The dc-SQUID is a nonlinear flux-sensitive device which can be exploited for parametric amplification of microwave signals incoming to the resonator. Furthermore, parametric amplification can be extended into the phase-sensitive regime which allows one to achieve deamplification, or *squeezing*, below the fundamental threshold of vacuum noise, thus, generating squeezed microwave states [18]. By coupling the JPA to the transmission lines, the squeezed states may leak out and propagate along a low-loss superconducting cables without losing their quantum properties. In our work, we focus on a specific CV-QKD protocol [19] implemented in the microwave regime. In this protocol, we start by generating the previously introduced squeezed states which are afterwards displaced using a highly asymmetric directional coupler [20]. The key is

encoded within the displacements of the squeezed states.

The thesis is structured as follows. In chapter 2, we present a theoretical description of propagating quantum microwaves and introduce important Gaussian states. Additionally, we discuss the physics of Josephson parametric amplifiers as well as their working principle. Furthermore, the generation of squeezed states from flux-driven JPAs is discussed. In Chapter 3, we explain the basics of quantum key distribution and discuss a specific protocol based on displaced squeezed states. In Chapter 4, we present experimental techniques including cryogenic measurement setups which are used to experimentally implement the microwave QKD protocol. Next, in Chapter 5, we study secret key measurements and discuss various aspects limitations of our experiments. Finally, Chapter 6 gives a summary of the thesis and a brief outlook.

Chapter 2

Theory of quantum microwaves

In this chapter, we present theoretical elements necessary for our work. First, we introduce a theory basis to describe propagating quantum microwaves and characterize them. For this purpose, we present a quasi-probability distribution known as the Wigner function. We discuss certain important states which are vacuum, thermal, coherent, and squeezed states. Then, we introduce Josephson parametric amplifiers (JPAs). We discuss the elements which compose them, namely, a coplanar waveguide (CPW) and a direct current superconducting quantum interference device (dc-SQUID). To this end, we briefly present the theory of Josephson junctions and their relevant properties. Then, we discuss about how JPA can perform parametric amplification and squeezing of microwave signals.

2.1 Propagating quantum microwaves

In this section, we discuss the theory of propagating microwaves. In a first step, a general quantum mechanical representation of propagating microwaves is introduced. In particular, a focus is given to Wigner functions, a class of quasiprobability distributions. These are used to highlight differences with classical representations. In a second step, we present general Gaussian states and explain in more details vacuum, thermal, coherent, and squeezed states. Especially, the mean and the covariance matrix of each individual state are shown.

2.1.1 Representation of quantum microwaves

In this work, we study electromagnetic signals in the frequency range of 4-6 GHz which propagate along coaxial cables or coplanar waveguides. Such signals $A(t)$ can be described classically by two components, $I(t)$ and $Q(t)$, the in-phase quadrature and out-of-phase quadrature, respectively. In this way, we can express a propagating signal

$A(t)$ at a frequency $f = \omega/2\pi$ using the following expression

$$A(r,t) = I(t)\cos(\omega t - \mathbf{k}\cdot\mathbf{r}) + Q(t)\sin(\omega t - \mathbf{k}\cdot\mathbf{r}), \tag{2.1}$$

where $\mathbf{k}$ is the wave vector of the propagating waves and $\mathbf{r}$ denotes the position of interest in space. From Eq. 2.1, we see that the quadratures allow us to fully describe signals at a given time t and position $\mathbf{r}$ if we know the frequency f and the wave vector $\mathbf{k}$. By introducing a quantization of the electromagnetic field, one arrives to an equivalent quantum description of the signal which encompasses the effects imposed by quantum mechanics. The amplitude operator for a one-dimensional, single-mode electrical field reads [21]

$$\hat{A}(r,t) = C\left[\hat{a}e^{i(\omega t-\mathbf{k}\cdot\mathbf{r})} + \hat{a}^{\dagger}e^{-i(\omega t-\mathbf{k}\cdot\mathbf{r})}\right] = 2C\left[\hat{q}\cos(\omega t - \mathbf{k}\cdot\mathbf{r}) + \hat{p}\sin(\omega t - \mathbf{k}\cdot\mathbf{r})\right]. \tag{2.2}$$

where C is a normalization constant. Here, we have introduced the annihilation and creation operators of a bosonic mode, $\hat{a}$ and $\hat{a}^{\dagger}$, respectively. They obey the bosonic commutation relation $[\hat{a},\hat{a}^{\dagger}] = 1$ and are related to the quadrature components

$$\hat{q} = \frac{\left(\hat{a} + \hat{a}^{\dagger}\right)}{2}, \quad \hat{p} = \frac{\left(\hat{a} - \hat{a}^{\dagger}\right)}{2i}. \tag{2.3}$$

The latter obey the commutation relation $[\hat{q},\hat{p}] = i/2$ and are the quantum counterparts of the classical quadratures I and Q. Due to the non-zero commutation relation between the quadratures, the corresponding Heisenberg uncertainty implies that

$$\Delta q \cdot \Delta p \geq \frac{1}{4}, \tag{2.4}$$

where the standard deviation ΔO of an observable $\hat{O}$ is defined as $(\Delta O)^2 = \left\langle(\Delta\hat{O})^2\right\rangle \equiv \left\langle\hat{O}^2\right\rangle - \left\langle\hat{O}\right\rangle^2$. In other words, it is not possible to measure simultaneously both quadratures with absolute precision. This represents a radical difference to the classical description where it is possible to assign a precise value to both I and Q. Thus, a propagating quantum wave needs to be described in a way which includes the appropriate Heisenberg uncertainty relation.

Density matrix

A general way of describing a quantum system is to use the density matrix formalism. A arbitrary density matrix $\hat{\rho}$ can be written as

$$\hat{\rho} = \sum_{i}^{N} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|, \tag{2.5}$$

where p_i represents the probability that the system is in the state $|\psi_i\rangle$ and N is the dimension of the Hilbert space describing the system. If the space is infite dimentional then the summation goes to infinity. It satisfies the property

$$\begin{aligned} \mathrm{Tr}\left(\hat{\rho}^2\right) = 1 &\iff \hat{\rho} \text{ is pure,} \\ \mathrm{Tr}\left(\hat{\rho}^2\right) < 1 &\iff \hat{\rho} \text{ is mixed.} \end{aligned} \tag{2.6}$$

Furthermore, it is a positive operator normalized as

$$\mathrm{Tr}\left(\hat{\rho}\right) = 1. \tag{2.7}$$

Although a density matrix gives the full information on a state, it is more suited for Hilbert space of small or finite dimensions. For infinite dimensions, the state is mathematically more complex to handle since the summation goes to infinity. In particular, the propagating electromagnetic fields are described by infinite-dimensional Hilbert spaces. For this reason, we use a different formalism for the description of such states using quasi-probability distribution, known as the Wigner function. It gives an equivalent description to the density matrix but is easier and more intuitive for infinite-dimensional bosonic quantum states.

Wigner functions

Wigner functions have been introduced by Eugene Wigner [22] as a way to link density matrix of states to real phase-space functions. For the propagating waves, we can assign a probability distribution to each individual quadrature. However, we need a full quasiprobability distribution of the system in order to describe both of the quadratures simultaneously due to the Heisenberg uncertainty. In our case, this quasiprobability distribution is given by the Wigner function. It corresponds to an extension of classical probability distributions to quantum systems. In general, the

Wigner function of a state with the density matrix $\hat{\rho}$ is defined as [22, 23]

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

Wigner functions are real-value functions and their marginal distributions give the probability distribution for each quadrature:

$$\begin{aligned}\int_{-\infty}^{+\infty} W(q,p)dp &= \langle q|\,\hat{\rho}\,|q\rangle\,,\\ \int_{-\infty}^{+\infty} W(q,p)dq &= \langle p|\,\hat{\rho}\,|p\rangle\,.\end{aligned} \tag{2.9}$$

In addition, if the Wigner function of a state is a Gaussian function, the state is referred to as a Gaussian state. A Gaussian function is a function f which can be expressed as

$$f(x) = a\exp\left(-\frac{(x-b)^2}{2c^2}\right), \tag{2.10}$$

where a, b are real constants and c is a real non-zero constant. Gaussian Wigner functions allow for a simplified description of propagating waves while preserving the majority of respective quantum properties. This stems from the fact that a general quantum state can be fully characterized by its signal moments $\left\langle(\hat{a}^\dagger)^m\hat{a}^n\right\rangle$ with m, $n \in \mathbb{N}_0$ [24]. The complete set of these moments provide the same information as the density matrix. For a Gaussian state, it is sufficient to obtain the signal moments up to the second order, $m+n \leq 2$, as higher order can be built from them [25]. Therefore, the Wigner function of a Gaussian state can be written as [25, 26]

$$\begin{aligned}W(q,p) = &\frac{1}{\pi\sqrt{(\nu+1/2)^2-|\mu|^2}}\\ &\times\exp\left[-\frac{(\nu+1/2)|\zeta-\langle\hat{a}\rangle|^2-(\mu^*/2)(\zeta-\langle\hat{a}\rangle)^2-(\mu/2)(\zeta^*-\left\langle\hat{a}^\dagger\right\rangle)^2}{(\nu+1/2)^2-|\mu|^2}\right],\end{aligned} \tag{2.11}$$

where $\zeta = q+ip$, $\mu = \left\langle\hat{a}^2\right\rangle - \langle\hat{a}\rangle^2$, and $\nu = \left\langle\hat{a}^\dagger\hat{a}\right\rangle - |\langle\hat{a}\rangle|^2$.

Statistical moments

From the signal moments, it is possible to define statistical moments of the quadratures. It is a suitable description for experiments and we will use this formalism throughout this work to characterise our states. For a general N-mode Gaussian state, we define a vector

$$\hat{\boldsymbol{r}} = (\hat{q}_1,\hat{p}_1,\ldots,\hat{q}_N,\hat{p}_N,), \tag{2.12}$$

containing all quadratures of each mode. Quadratures of different modes commute with each others. The first-order statistical moment is then the mean $\bar{\mathbf{r}} = \langle \hat{\boldsymbol{r}} \rangle$. The second-order statistical moments are the covariances

$$V_{ij} = \frac{\left\langle \hat{\boldsymbol{r}}_i \hat{\boldsymbol{r}}_j + \hat{\boldsymbol{r}}_j \hat{\boldsymbol{r}}_i \right\rangle}{2} - \langle \hat{\boldsymbol{r}}_i \rangle \langle \hat{\boldsymbol{r}}_j \rangle \, . \tag{2.13}$$

The second-order moments form the covariance matrix $\mathbf{V} = (V_{ij}) \in \mathbb{R}^{2N \times 2N}$. From the previous subsection, we know that the knowledge of the statistical moments up to the second order, which is equivalent to the knowledge of the mean values and covariance matrix, gives full information about an arbitrary quantum Gaussian state [27]. The corresponding Wigner function can be written as

$$W(x) = \frac{\exp\left[-\frac{1}{2}(\mathbf{x} - \bar{\mathbf{r}})\mathbf{V}^{-1}(\mathbf{x} - \bar{\mathbf{r}})^{\mathrm{T}}\right]}{(2\pi)^{\mathrm{N}} \sqrt{\det \mathbf{V}}}, \tag{2.14}$$

where $\mathbf{x} = (q,p)$ is a vector in the phase-space.

Average states

Throughout this work, we have to consider density matrices that are defined as the average of other density matrices. A general average density matrix $\hat{\rho}_{\mathrm{avg}}$ is expressed as

$$\hat{\rho}_{\mathrm{avg}} = \sum_{\mathrm{i}=1}^{\mathrm{M}} p_{\mathrm{i}} \cdot \hat{\rho}_{\mathrm{i}}, \tag{2.15}$$

where M is the number of state in the sum and p_{i} is a probability associated with a state $\hat{\rho}_{\mathrm{i}}$. The set of discrete probabilities $\{p_{\mathrm{i}}\}_{\mathrm{i} \in [1,\mathrm{M}]}$ can correspond to any discrete probability distribution. The set of density matrices $\{\hat{\rho}_{\mathrm{i}}\}_{\mathrm{i} \in [1,\mathrm{M}]}$ can correspond to any density matrices. In particular, for such average density matrices, we have a very useful property for signal moments

$$\left\langle (\hat{a}^\dagger)^m \hat{a}^n \right\rangle_{\mathrm{avg}} = \mathrm{Tr}\left((\hat{a}^\dagger)^m \hat{a}^n \, \hat{\rho}_{\mathrm{avg}} \right) = \sum_{\mathrm{i}=1}^{\mathrm{M}} p_{\mathrm{i}} \cdot \mathrm{Tr}\left((\hat{a}^\dagger)^m \hat{a}^n \, \hat{\rho}_{\mathrm{i}} \right) = \sum_{\mathrm{i}=1}^{\mathrm{M}} p_{\mathrm{i}} \cdot \left\langle (\hat{a}^\dagger)^m \hat{a}^n \right\rangle_{\mathrm{i}}, \tag{2.16}$$

where $m, n \in \mathbb{N}_0$, $\left\langle (\hat{a}^\dagger)^m \hat{a}^n \right\rangle_{\mathrm{avg}}$ corresponds to a signal moment for the average state $\hat{\rho}_{\mathrm{avg}}$, and $\left\langle (\hat{a}^\dagger)^m \hat{a}^n \right\rangle_{\mathrm{i}}$ corresponds to the same signal moment for the individual state $\hat{\rho}_{\mathrm{i}}$.

Importantly, using Eq. 2.16, one can show that

$$\begin{aligned}(\Delta q)^2_{\mathrm{avg}} \equiv \left\langle \hat{q}^2 \right\rangle_{\mathrm{avg}} - \langle \hat{q} \rangle^2_{\mathrm{avg}} &= \sum_{\mathrm{i}=1}^{\mathrm{M}} p_{\mathrm{i}} \cdot \left\langle \hat{q}^2 \right\rangle_{\mathrm{i}} - \left(\sum_{\mathrm{i}=1}^{\mathrm{M}} p_{\mathrm{i}} \cdot \langle \hat{q} \rangle_{\mathrm{i}} \right)^2 \\ &\neq \sum_{\mathrm{i}=1}^{\mathrm{M}} p_{\mathrm{i}} \cdot \left(\left\langle \hat{q}^2 \right\rangle_{\mathrm{i}} - \langle \hat{q} \rangle^2_{\mathrm{i}} \right),\end{aligned} \tag{2.17}$$

where $\langle \hat{q}^{\mathrm{n}} \rangle_{\mathrm{avg}}$ is the n-th moments of the operator $\hat{q}^{\mathrm{n}}$ for the average state $\hat{p}_{\mathrm{avg}}$ and $\langle \hat{q}^{\mathrm{n}} \rangle_{\mathrm{i}}$ is the n-th moments of the operator $\hat{q}^{\mathrm{n}}$ for the individual state $\hat{p}_{\mathrm{i}}$ More generally, this means that one cannot add up the covariance matrices to get the covariance matrix of the average state

$$\mathbf{V}_{\mathrm{avg}} \neq \sum_{\mathrm{i}}^{\mathrm{M}} p_{\mathrm{i}} \cdot \mathbf{V}_{\mathrm{i}}, \tag{2.18}$$

where $\mathbf{V}_{\mathrm{avg}}$ correspond to the covariance matrix of the state $\hat{\rho}_{\mathrm{avg}}$ and $\mathbf{V}_{\mathrm{i}}$ corresponds to the covariance matrix of the state $\hat{\rho}_{\mathrm{i}}$. Instead, one needs to compute the average signal moments of the average state from Eq. 2.16. Then, one can compute the covariance matrix $\mathbf{V}_{\mathrm{avg}}$ from the average moments.

Purity Gaussian states

We define purity μ of an N-mode Gaussian state as

$$\mu = \frac{1}{4^{\mathrm{N}} \sqrt{\det \mathbf{V}}}, \tag{2.19}$$

where $\mathbf{V}$ is the covariance matrix of the N-mode Gaussian state introduced in Eq. 2.13. Purity is unity for any pure state. For single-mode states ($N = 1$), it corresponds to states that saturate the Heisenberg uncertainty relation given in Eq. 2.4. For mixed states, purity is below 1.

2.1.2 Gaussian states

In this subsection, we introduce all generic Gaussian states as well as their relevant properties. Additionally, we present their statistical moments and Wigner function description.

Vacuum and thermal states

The first Gaussian state of interest corresponds to the lowest energy state. It saturates the single-mode Heisenberg uncertainty relation $(\Delta q)^2 = (\Delta p)^2 = 1/4$. This means that even for the lowest energy state, both quadratures present fluctuations. Since it corresponds to the lowest energy, the equilibrium temperature $T = 0$ is assigned to it. For this reason, this state is known as the vacuum state and denoted by $|0\rangle$, representing a ground state of a bosonic mode. In reality, temperatures are always non-zero however we can approximate the lowest energy state in our experiment as the vacuum state as long as $k_B T \ll hf$. This approximation is fulfilled for our frequency range (around 5 GHz) and our temperature range (around 40 mK).

For an equilibrium temperature $T > 0$, if the previously mentioned approximation is not used or is not valid, one has to consider so-called thermal states. They are characterised by their mean photon number n_{th}. The latter follows the Bose-Einstein statistics [28]

$$n_{\text{th}} = \frac{1}{\exp\left(\frac{hf}{k_B T}\right) - 1}. \tag{2.20}$$

The density matrix of the corresponding state is given by [21]

$$\hat{\rho}_{\text{th}} = \sum_n \frac{\langle \hat{n} \rangle^n}{(1 + \langle \hat{n} \rangle)^{n+1}} |n\rangle \langle n| , \tag{2.21}$$

where $\langle \hat{n} \rangle = \left\langle \hat{a}^\dagger \hat{a} \right\rangle$ From quantum theory, we can find $n_{\text{th}} = \text{Tr}\left(\hat{n}\, \hat{\rho}_{\text{th}}.\right)$. The mean and the covariance matrix are given by

$$\bar{\mathbf{r}}_{\text{th}} = \mathbf{0} \quad \text{and} \quad \mathbf{V}_{\text{th}} = (1 + 2n_{\text{th}}) \frac{\mathbb{I}}{4}, \tag{2.22}$$

where $\mathbb{I}$ is the identity matrix. Fig. 2.1 represents the Wigner functions of a vacuum state and thermal state with $n_{\text{th}} = 3$.

Coherent states

The third class of states of interest is represented by a coherent, or displaced, state $|\alpha\rangle$. It is defined as an eigenstate of the annihilation operator, $\hat{a} |\alpha\rangle = \alpha |\alpha\rangle$. Coherent states are theoretically obtained by applying the displacement operator

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

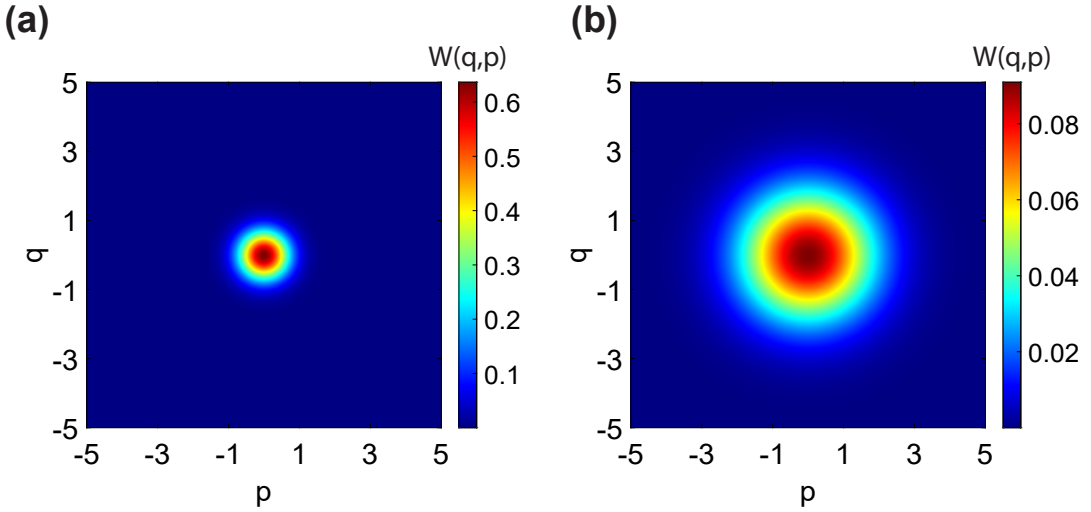


Figure 2.1: (a) Wigner function of a vacuum state. (b) Wigner function of a thermal state with $n_{\mathrm{th}} = 3$.

to the vacuum state $|\alpha\rangle = \hat{D}(\alpha)|0\rangle$. The corresponding mean and variance matrix are then given by

$$\bar{\mathbf{r}}_{\mathrm{coh}} = (\mathrm{Re}(\alpha), \mathrm{Im}(\alpha)) \quad \text{and} \quad \mathbf{V}_{\mathrm{coh}} = \frac{\mathbb{I}}{4}, \tag{2.24}$$

where $\alpha = |\alpha|e^{i\theta}$ is the complex displacement amplitude. This means that the coherent states Wigner function corresponds to the one of the vacuum with its center displaced in the phase space to coordinates $(\mathrm{Re}(\alpha), \mathrm{Im}(\alpha))$. Coherent states also saturate the Heisenberg uncertainty relation as the vacuum state. To characterise the displacement, we use the complex the displacement amplitude α with magnitude $|\alpha|$ and displacement angle $\Theta = \pi/2 - \theta$ as it can be seen in Fig. 2.2. They are often considered as the most classical of all Gaussian quantum states [16].

To implement the displacement operator in our experiments, we use a directional coupler acting as highly asymmetric beam splitter in the microwave regime [20]. An incoming signal $\hat{a}_{\mathrm{in}}$ is sent to a port of the directional coupler with transmissivity τ while a strong coherent state $|\alpha_{\mathrm{coh}}\rangle$ is sent to a weakly-coupled port of the directional coupler. In such case, the output signal $\hat{a}_{\mathrm{out}}$ is expressed as [29]

$$\hat{a}_{\mathrm{out}} = \sqrt{\tau}\hat{a}_{\mathrm{in}} + \sqrt{1-\tau}\,\hat{a}_{\mathrm{coh}}. \tag{2.25}$$

In the limit of $\tau \to 1$ and for a strong coherent signal $|\alpha_{\mathrm{coh}}| \gg 1$ sqtisfzing the condition $\sqrt{1-\tau}|\alpha_{\mathrm{coh}}| = \alpha$, one can show that the directional coupler implements the

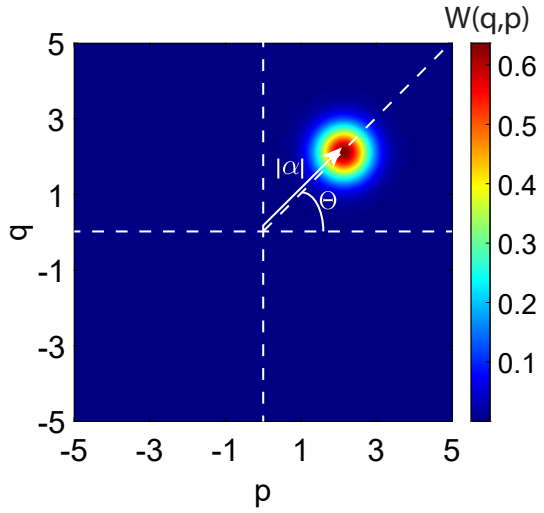


Figure 2.2: Wigner function of a coherent state. Here, $|\alpha| = 3$ and $\theta = \pi/4$, resulting in $\Theta = \pi/4$.

transformation

$$\hat{a}_{\text{out}} \approx \hat{a}_{\text{in}} + \alpha \hat{1}, \tag{2.26}$$

where $\hat{1}$ is the identity operator. The output state is a displaced state.

Squeezed state

The last class of Gaussian states of interest is the squeezed state $|\xi\rangle$. It can be described by applying the squeeze operator

$$\hat{S}(\xi) = \exp\left(\frac{1}{2}\xi^* \hat{a}^2 - \frac{1}{2}\xi \left(\hat{a}^\dagger\right)^2\right), \tag{2.27}$$

to the vacuum state $|\xi\rangle = \hat{S}(\xi)|0\rangle$. Here, we parametrise squeezing with the squeeze parameter $\xi = re^{i\varphi}$, where r is the squeezing factor and φ is the squeezing angle. Furthermore, we define $\gamma = -\varphi/2$ as the angle between the antisqueezed quadrature and the p-axis as shown in Fig. 2.3. The mean and the covariance matrix are given by

$$\bar{\mathbf{r}}_{\text{sq}} = \mathbf{0} \quad \text{and} \quad \mathbf{V}_{\text{sq}} = \frac{1}{4}\begin{pmatrix} e^{-2r}\cos^2\frac{\varphi}{2} + e^{2r}\sin^2\frac{\varphi}{2} & \sin\varphi\left(e^{-2r} - e^{2r}\right)/2 \\ \sin\varphi\left(e^{-2r} - e^{2r}\right)/2 & e^{2r}\cos^2\frac{\varphi}{2} + e^{-2r}\sin^2\frac{\varphi}{2} \end{pmatrix}. \tag{2.28}$$

The Wigner function of squeezed states has an ellipsoidal form. The amount of squeezing and antisqueezing is characterized by the squeezed variance $\sigma_S^2 = e^{-2r}/4$ and the anti-squeezed variance $\sigma_A^2 = e^{2r}/4$, respectively. In our experiments, we also

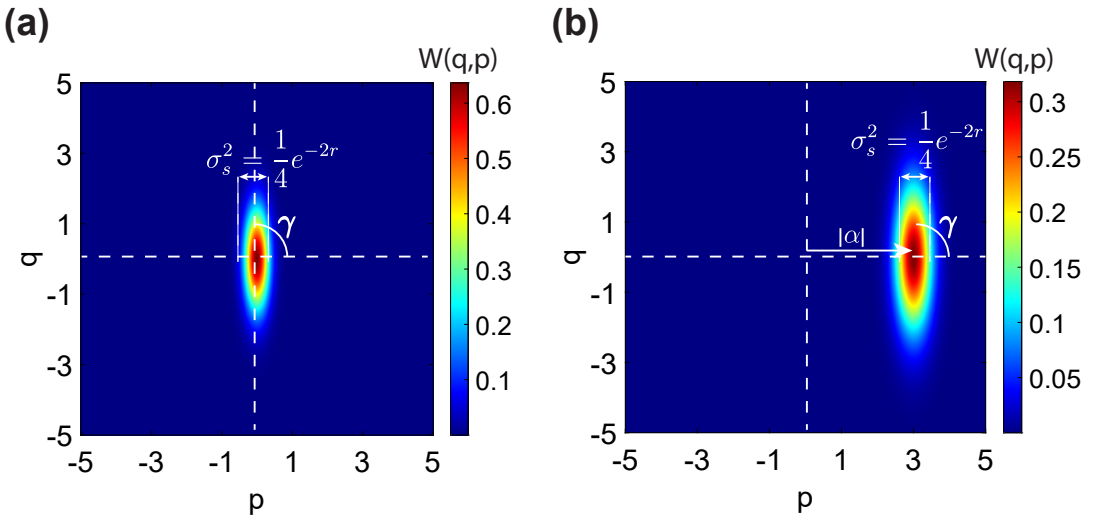


Figure 2.3: (a) Wigner function of a squeezed state. Here, $\gamma = \pi/2$ and $r = 0.7$, corresponding to the squeezing level of $S = 6.1$ dB. (b) Wigner function of a displaced squeezed thermal state for $\gamma = \pi/2$, $r = 0.7$, $|\alpha| = 3$, and $\Theta = 0$. Here, $n_{\text{th}} = 1$.

use the squeezing level S and antisqueezing level A as quantifiers

$$S = -10\log_{10}\left(\frac{\sigma_S^2}{0.25}\right) \quad \text{and} \quad A = 10\log_{10}\left(\frac{\sigma_A^2}{0.25}\right), \tag{2.29}$$

where 0.25 in both S and A refers to the quadrature variance of the vacuum state. Therefore, positive values of S corresponds to a squeezing of vacuum fluctuations below the vacuum level. For a pure squeezed state, we get $S = 20r\log_{10}(e)$. Experimentally, we generate squeezed microwave states with the help of Josephson parametric amplifiers (see Sec. 2.2 below).

Displaced squeezed thermal states

It is important to note that all states presented in the previous sections can be combined together. For this, one can consider displaced squeezed thermal states. They can be described by applying the squeeze operator $\hat{S}(\xi)$, then the displacement operator $\hat{D}(\alpha)$ to a thermal state $\hat{\rho}_{\text{th}}$

$$\hat{\rho}_{DS} = \hat{D}(\alpha)\hat{S}(\xi)\hat{\rho}_{\text{th}}\hat{S}(\xi)^{\dagger}\hat{D}(\alpha)^{\dagger}, \tag{2.30}$$

where $\hat{\rho}_{DS}$ is the density matrix of the displaced squeezed thermal state with $\xi = re^{i\varphi}$, and $\alpha = |\alpha|e^{i\theta}$. We stress that the order of the operators is important since the squeeze and displacement operators generally do not commute [30]. With the order presented here (squeeze before displacement), the squeezing of the final state is solely character-

ized by the squeeze factor r and squeeze angle φ as for Sec. 2.1.2. The displacement of the final state is independent of the squeeze parameter r and angle φ and depends only on α as in Sec. 2.1.2. We refer the reader to Ref.[21] for a theoretical description of squeezed displaced states and to Ref. [18] for an experimental implementation in the microwave regime. The mean and the covariance matrix of a displaced squeezed thermal state are given by

$$\begin{aligned} \bar{\mathbf{r}}_{\mathrm{DS}} &= (\mathrm{Re}(\alpha), \mathrm{Im}(\alpha)), \\ \mathbf{V}_{\mathrm{DS}} &= \frac{(1+2n_{\mathrm{th}})}{4} \begin{pmatrix} e^{-2r}\cos^2\frac{\varphi}{2} + e^{2r}\sin^2\frac{\varphi}{2} & \sin\varphi\left(e^{-2r}-e^{2r}\right)/2 \\ \sin\varphi\left(e^{-2r}-e^{2r}\right)/2 & e^{2r}\cos^2\frac{\varphi}{2} + e^{-2r}\sin^2\frac{\varphi}{2} \end{pmatrix}, \end{aligned} \tag{2.31}$$

where n_{th} is the mean photon number of the thermal state $\hat{\rho}_{\mathrm{th}}$. An example of the displaced squeezed thermal state is presented in Fig. 2.3.

2.2 Josephson parametric amplifier (JPA)

Josephson parametric amplifiers (JPAs) represent the central building blocks in our experiments with propagating squeezed microwaves [31, 32, 33]. In the current work, we exclusively employ flux-driven JPAs [17]. A flux-driven JPA consists of a superconducting microwave resonator fabricated in a coplanar waveguide (CPW) geometry. By short-circuiting the resonator to ground via a direct current superconducting quantum interference device (dc-SQUID), one can tune the resonant frequency of the resonator with an external magnetic flux through the dc-SQUID loop. Additionally, the flux-driven JPA employs an on-chip pump antenna inductively coupled to the dc-SQUID loop. By applying a strong coherent pump tone via this antenna, we can achieve parametric amplification of signal incident to the JPA. Notably, this can be used to generate squeezed vacuum states.

2.2.1 Josephson junctions and dc-SQUID

Both the JPA resonator and dc-SQUID consist of superconducting materials such as niobium or aluminum. Superconductors allows one to achieve low losses at cryogenic temperatures which is particularly important in order to preserve quantum properties of squeezed microwave states. In combination with low losses, superconductors provide another useful effect, the Josephson effect [34] which is used to enable the dc-SQUIDs. This effect appears when two superconductors are weakly coupled to each other (for instance, via an insulating layer). In order to describe the Josephson effect, we assign a macroscopic wavefunction $\Psi_{\mathrm{k}}(\mathbf{r},t) = \sqrt{n_{\mathrm{k}}(\boldsymbol{r},t)}e^{i\theta_{\mathrm{k}}(\mathbf{r},t)}$ to each superconductor, where

$k = 1,2$ for superconductor 1 or 2. Here, $n_\mathrm{k}(\mathbf{r},t)$ refers to the Cooper pairs density in the superconductors and $\theta_k(\boldsymbol{r},t)$ to the phase of the macroscopic wavefunction of Cooper pairs. A representation is given in Fig. 2.4 (a). Furthermore, we introduce a gauge-invariant phase difference expressed as [35]

$$\varphi(\boldsymbol{r},t) = \theta_2(\boldsymbol{r},t) - \theta_1(\boldsymbol{r},t) - \frac{2\pi}{\Phi_0}\int_1^2 \boldsymbol{A}(\boldsymbol{r},t)\cdot \mathrm{d}\boldsymbol{l}, \tag{2.32}$$

which will be used to describe the Josephson effect. Here, $\Phi_0 = h/2e$ is the magnetic flux quantum and $\boldsymbol{A}$ is the vector potential. The integral path from 1 to 2 refers to a path from superconductor 1 to superconductor 2 across the tunnel barrier. In our experiments, we consider lumped Josephson junctions where we neglect spatial variations of the Cooper pairs. Furthermore, two equations are used to describe the Josephson effect. These are known as the first Josephson equation and the second Josephson equations, respectively [35]

$$I_\mathrm{s}(\varphi) = I_\mathrm{c}\sin(\varphi) \quad \text{and} \quad \frac{\partial\varphi}{\partial t} = \frac{2\pi}{\Phi_0}V(t), \tag{2.33}$$

where I_s is the Josephson supercurrent, I_c is the Josephson critical current, and V is the voltage across the Josephson junction. It can be seen from the Josephson equations that a constant voltage across the junction will induce a sinusoidal supercurrent. In addition, by using the definition of inductance as $V = L\,\mathrm{dI/dt}$, one can obtain a nonlinear inductance of the Josephson junction

$$L_\mathrm{s} = L_\mathrm{c}\frac{1}{\cos(\varphi)}, \tag{2.34}$$

where $L_\mathrm{c} = \Phi_0/(2\pi I_\mathrm{c})$. This nonlinear inductance is in the central element of the absolute majority of quantum superconducting circuits.

Moreover, Josephon junctions can be used to build more complex devices. In particular, dc-SQUIDs are also based on lumped element Josepshon junctions. In general, a dc-SQUID consists of two Josephson junctions in a superconducting loop as shown in Fig. 2.4 (b). In the following, we assume for simplicity that critical currents of the Josephson junctions are identical. To describe dynamics of the dc-SQUID, we want to look at the gauge invariant phase difference. The first important dc-SQUID relation can be obtained by considering the total phase change over a closed contour C around the dc-SQUID. Due to nature of the phase, we have to demand $\oint_C \nabla\theta\cdot \mathrm{d}r = 2\pi n$ with $n \in \mathbb{N}_0$. One can see that the phase θ_k in each superconductor is defined in an interval

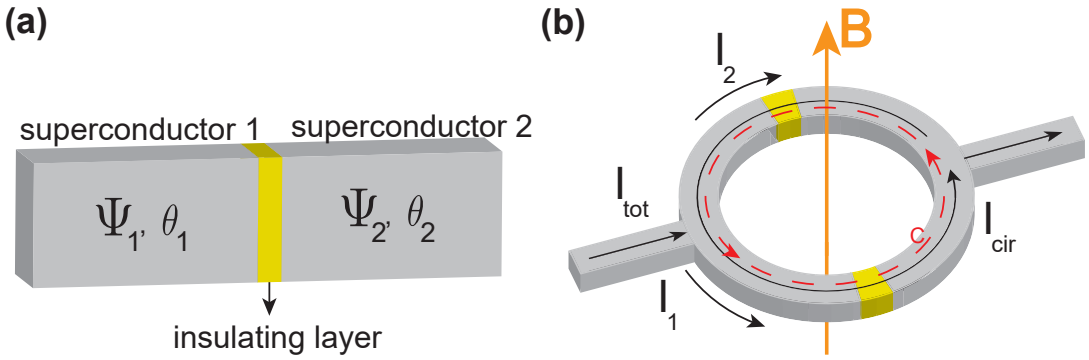


Figure 2.4: (a) Schematic of a Josephson junction. Superconductors 1 and 2 are represented by gray color while the insulating layer between them is depicted by yellow color. (b) Schematic of a dc-SQUID. The total current is given by $I_{\text{tot}} = I_1 + I_2$. Circulating current is defined as $I_{\text{cir}} = I_1 - I_2$. The broken line represents the closed contour C.

of 2π. One can also express the phase gradient as [35]

$$\nabla\theta = \frac{2\pi}{\Phi_0}\left(\Lambda \boldsymbol{J}_s + \boldsymbol{A}\right), \tag{2.35}$$

where Λ is the London parameter, $\boldsymbol{J}_s$ is the supercurrent density, and $\boldsymbol{A}$ is the vector potential. If we integrate Eq. 2.35 along a path inside the superconductor where the supercurrent density $\boldsymbol{J}_s$ is close to zero, we obtain

$$\varphi_2 - \varphi_1 = \frac{2\pi\Phi}{\Phi_0} + 2\pi n. \tag{2.36}$$

This expression connects the phase difference $\varphi_2 - \varphi_1$ between the dc-SQUID Josephson junctions to the total magnetic flux through the loop. The latter can be decomposed written as $\Phi = \Phi_{\text{ext}} + L_{\text{loop}} I_{\text{cir}}$. The second contribution comes from a geometric inductance of the superconducting loop and a non-zero circulating current. The latter is $I_{\text{cir}} = (I_1 - I_2)/2$. Using the previous expression for the total magnetic flux and Eq. 2.36, one can then write

$$\frac{\Phi}{\Phi_0} = \frac{\Phi_{\text{ext}}}{\Phi_0} - \frac{\beta_L}{2}\cos\left(\frac{\varphi_1 + \varphi_2}{2}\right)\sin\left(\frac{\varphi_1 - \varphi_2}{2}\right), \tag{2.37}$$

where we have introduced the screening parameter $\beta_{\text{L}} = 2L_{\text{loop}} I_{\text{c}}/\Phi_0$ [36]. Here, we can distinguish two characteristic regimes of the dc-SQUIDs. If we consider $\beta_{\text{L}} \approx 0$, the screening effect is small. In this case, we can neglect the self-induced flux and assume that $\Phi \approx \Phi_{\text{ext}}$. In this case, the dc-SQUID can be regarded as a single Josephson junction whose maximal supercurrent is modulated by the external applied flux. One

can then define a nonlinear flux-dependent inductance of the dc-SQUID [37]

$$L_s\left(\Phi_{\text{ext}}\right) = \frac{\Phi_0}{4\pi I_c \left|\cos\left(\pi \frac{\Phi_{\text{ext}}}{\Phi_0}\right)\right|}. \tag{2.38}$$

The dc-SQUID becomes a nonlinear element in superconducting circuits which can be tuned by the external flux. If we consider $\beta_L > 1$, the self inductance of the loop contribution is not negligible anymore. Analytical expression cannot be derived in this case and one needs to use the expression in Eq. 2.37 for a numerical simulation of the system.

2.2.2 CPW resonator short-circuited by a dc-SQUID

Another important element of the JPAs is a coplanar waveguide (CPW) resonator made of superconducting materials. To describe such the CPW resonator, we first consider a CPW acting as a quasi one-dimensional transmission line. The lateral dimension of our CPW is in the order of few millimetres, corresponding to resonant frequencies on the order of few GHz. For a more detailed description, we adopt a distributed element model where the waves propagating through the CPW are described by the telegrapher's equations [38]. A representation is given in Fig. 2.5. Since our CPW is made of superconducting materials, we can approximate it with a lossless transmission line. These assumptions allow us to write the characteristic impedance of the CPW as [38]

$$Z = \sqrt{\frac{L_0}{C_0}}, \tag{2.39}$$

where L_0 and C_0 are respectively, the inductance and capacitance per unit length of the transmission line (see Fig. 2.5). In order to estimate a resonant frequency of this system, we apply a set of boundary conditions to the propagating microwaves on the transmission line. To this end, an input line is capacitively coupled at one end of the CPW via a capacitance C_{c}, while the other end of the CPW is short-circuited to ground so that the electric length of the CPW is equal to d. This creates a reflection type resonator. The frequency of the fundamental resonant mode is then given by [39]

$$f_{\text{res}} = \frac{1}{4d\sqrt{L_0 C_0}} = \frac{1}{4\sqrt{L_{\text{res}} C_{\text{res}}}}, \tag{2.40}$$

where $L_{\text{res}} = d\,L_0$ and $C_{\text{res}} = d\,C_0$ are the total inductance and capacitance of the resonator, respectively. The wavelength of this fundamental resonant mode λ is linked

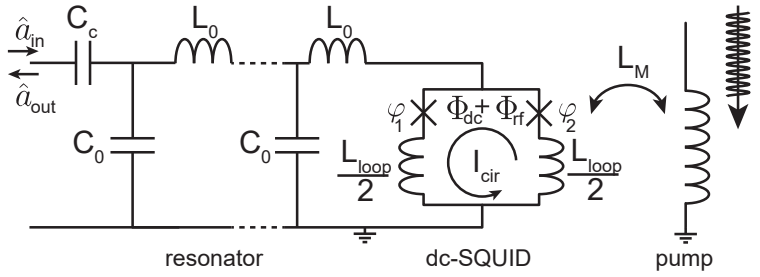


Figure 2.5: Distributed element model of a CPW resonator. Here, L_0 and C_0 are the inductance and capacitance per unit length, respectively. On the top left, C_c is the coupling capacitance. It describes the coupling of an incoming signal $\hat{a}_{in}$ to the resonator. The resonator is short-circuited to ground with a dc-SQUID. An external magnetic flux Φ_{dc} is inductively coupled to the dc-SQUID. Additionally, an oscillating flux Φ_{rf} can applied via an external pump tone sent to the pump line represented on the right hand side. Inductance coupling between the pump line and the dc-SQUID is shown via the mutual coupling coefficient L_M.

to the size of the resonator d as $\lambda = 4d$. For this reason, this type of resonator is called quarter-wavelength $\lambda/4$ resonator. From Eq. 2.40 , we see that changing the inductance of the resonator due to the additional flux-dependent dc-SQUID inductance will induce a change in the resonant frequency. It can be shown that the dependency of the resonant frequency f_0 on the external flux is given by [40, 41, 42]

$$\left(\frac{\pi f_0}{2f_{res}}\right)\tan\left(\frac{\pi f_0}{2f_{res}}\right) = 2\frac{(2\pi)^2}{\Phi_0^2}L_{res}E_s\left(\Phi_{ext}\right) - \frac{2C_s}{C_{res}}\left(\frac{\pi f_0}{2f_{res}}\right)^2, \tag{2.41}$$

where L_{res}, C_{res} and f_{res} are the total inductance, capacitance, and resonant frequency of the bare resonator. Additionally, C_s corresponds to the capacitance of a single Josephson junction. Here, $E_s\left(\Phi_{ext}\right)$ represents the flux-dependent energy of the dc-SQUID [43]. From Eq. 2.41, one can see how the resonant frequency depends on the introduced dc-SQUID. For a zero dc-SQUID energy, $f_0 \to 0$ and one obtains an open transmission line. Conversely, for an infinite dc-SQUID energy, $f_0 \to f_{res}$. In that case, one obtains the previously introduced $\lambda/4$ resonator.

2.2.3 Generation of squeezed states with flux driven JPAs

JPAs are parametric amplifiers that have been experimentally used many times in literature for various purposes [44, 18, 45]. In this work, we work with a flux-driven JPA [17] in order to generate squeezed states. Flux-driven JPAs consist of a $\lambda/4$ resonator acting as an oscillator whose resonant frequency is tuned by a dc-SQUID via an external flux. The pump line allows to induce an additional alternating flux Φ_{rf} through the dc-SQUID loop (see Fig. 2.5), enabling oscillations of the resonant frequency. Parametric

amplification is achieved when the pump frequency is set to $f_{\text{pump}} = 2f_0$. To this extent, one first needs to tune the resonant frequency to a desired frequency f_0 by applying a dc flux Φ_{dc} to the dc-SQUID. The power of the pump tone modulates the magnitude of the amplification. The whole parametric amplification process can be described as a non-linear interaction between three modes, a pump mode at frequency f_{pump}, a signal mode at frequency f_{signal}, and an idler mode at frequency f_{idler}. More precisely, in the case of the flux-driven JPA, one has to consider the three-wave mixing process, characterized by the condition [31]

$$f_{\text{pump}} = f_{\text{signal}} + f_{\text{idler}}. \tag{2.42}$$

If $f_{\text{pump}} \neq 2f_{\text{signal}}$, one talks about phase-insensitive or non-degenerate amplification. If $f_{\text{pump}} = 2f_{\text{signal}}$, one talks about phase-sensitive or degenerate amplification. The amplification process can be described by the power gain G for each quadrature component. For both type of amplification regimes (non-degenerate or degenerate), it is important to consider is the noise performance, that is, the number of noise photons added to amplified signals. For a phase-insensitive amplifier, C.Caves [46] showed that this number of added noise photons η_{amp} has a fundamental lower bound. If we consider η_{amp} as the noise photon number referred to the input of the amplifier, we can express this lower bound as

$$\eta_{\text{amp}} \geq \frac{1}{2}\left|1 - G_{\text{s}}\right|, \tag{2.43}$$

where G_{s} refers to the signal mode power gain. So even in the limit of very large gain G_{s}, a minimal amount of $1/2$ noise photons is added to the signal.

For a phase-sensitive amplifier, the situation is different. For this type of amplifiers, one quadrature is amplified, while another one is deamplified. For each quadrature ($\text{i} = \{1, 2\}$), we can assign an individual gain G_{i} and a respective number of added noise photons η_{i}. According to Caves [46], these quantities are related as

$$\eta_1\eta_2 \geq \frac{1}{16}\left|1 - \frac{1}{\sqrt{G_1 G_2}}\right|^2, \tag{2.44}$$

The interesting outcome of Eq. 2.44 is that under condition $G_1G_2 = 1$ a noiseless amplification can be achieved. In other words, in this regime, one quadrature of the signal can be amplified with gain G_1 without adding additional noise, while the conjugate quadrature will be deamplified with gain G_2. This process corresponds to the squeezing operation. More precisely, using a flux driven JPA in the phase-sensitive regime where $f_{\text{pump}} = 2f_{\text{signal}}$, we can generate a squeezed state using a vacuum state

as an input. In fact, it is possible to show that the JPA Hamiltonian in the interaction picture corresponds to the squeeze operator. Following Ref. [16], one can indeed derive that the unitary evolution of the system is described by

$$\hat{U}(t) = \exp\left[-\frac{i}{\hbar}\hat{H}_{\text{int}}t\right] = \exp\left(\frac{1}{2}\xi^{*}\hat{a}^{2} - \frac{1}{2}\xi\left(\hat{a}^{\dagger}\right)^{2}\right), \tag{2.45}$$

where $\xi = re^{i\varphi}$ and $\hat{H}_{\text{int}}$ is the JPA Hamiltonian in the interaction picture. Here, we define $r = \lambda t$ with λ the effective frequency modulation and φ is related to the pump tone phase. We invite the reader to Ref. [43] for a more detailed derivation. In other words, the unitary transformation in the JPA under the parametric degenerate drive coincides with the squeezing operator defined in Eq. 2.27. Furthermore, Yamamoto *et al*. [47] used an input-output formalism to investigate the gain in the phase-sensitive and phase-insensitive regime. It can be shown that in the phase-sensitive regime, one obtains the following signal gain [48]

$$G_{\text{d}}(\theta) = \frac{\left(\frac{\kappa_{\text{ext}}^{2}-\kappa_{\text{int}}^{2}}{4} - 4\delta^{2}\omega_{0}^{2}\right)^{2} + 4\delta^{2}\kappa_{\text{ext}}^{2}\omega_{0}^{2} - 4\delta\kappa_{\text{ext}}\omega_{0}\left(\frac{\kappa_{\text{ext}}^{2}-\kappa_{\text{int}}^{2}}{4} - 4\delta^{2}\omega_{0}^{2}\right)\sin(2\theta)}{\left(\frac{(\kappa_{\text{ext}}+\kappa_{\text{int}})^{2}}{4} - 4\delta^{2}\omega_{0}^{2}\right)^{2}}, \tag{2.46}$$

where θ is the phase difference between the signal mode and pump tone, δ is the pump tone amplitude and $\omega_0 = 2\pi f_0$ is the resonance angular frequency. Furthermore, we define $\kappa_{\text{int}} = \omega_0/Q_{\text{int}}$ and $\kappa_{\text{ext}} = \omega_0/Q_{\text{ext}}$ as the internal and external loss rates, respectively. Now, one can obtain from this expression values for the minimal and maximal gains describing the amplification and deamplification in the flux-driven JPA

$$\begin{aligned} G_{\text{d}}^{\min} &= \left(\frac{2\delta\omega_0 - (\kappa_{\text{ext}} - \kappa_{\text{int}})/2}{2\delta\omega_0 + (\kappa_{\text{ext}} + \kappa_{\text{int}})/2}\right)^{2}, \quad \text{for}\,\theta \equiv \frac{\pi}{4}\,(\text{mod}\,\pi), \\ G_{\text{d}}^{\max} &= \left(\frac{2\delta\omega_0 + (\kappa_{\text{ext}} - \kappa_{\text{int}})/2}{2\delta\omega_0 - (\kappa_{\text{ext}} + \kappa_{\text{int}})/2}\right)^{2}, \quad \text{for}\,\theta \equiv \frac{3\pi}{4}\,(\text{mod}\,\pi), \end{aligned} \tag{2.47}$$

where we assume $\kappa_{\text{ext}} > \kappa_{\text{int}}$. Remarkably, we obtain the condition $G_{\text{d}}^{\min}G_{\text{d}}^{\max} = 1$ (i.e., potentially noiseless phase-sensitive amplification) under the condition $\kappa_{\text{int}} = 0$.

Additionally, it is important to note that our JPA does not produce pure squeezed states. More precisely, for an ideal JPA operating in the phase-sensitive regime, sending the vacuum as an input state can produce a pure squeezed state. However, experimentally, additional noise is added by our JPAs to both quadratures even in the degenerate regime. This happens due to various imperfections of practical JPAs, finite ambient temperatures, photon noise uncertainty in the pump tones, among other reasons. In the

end, the output JPA states can be effectively modelled as a squeezed thermal states. Using a similar approach as in Sec. 2.1.2, we can describe these squeezed thermal states $\hat{\rho}_{\mathrm{J}}$ as

$$\hat{\rho}_{\mathrm{J}} = \hat{S}\left(\xi\right)\hat{\rho}_{\mathrm{th}}\hat{S}^{\dagger}\left(\xi\right), \tag{2.48}$$

where $\hat{\rho}_{\mathrm{th}}$ describes a thermal state with a fixed mean photon number n_{th}. The latter is directly related to the added noise photon number of the JPA.

Chapter 3

Quantum Key Distribution

In this chapter, we present concepts of quantum key distribution (QKD) which are used throughout this work. First, we introduce a general framework of QKD. We focus on a possible way to generate a common key, which usually can be represented by a string of numbers, between two parties. In order to investigate the security of such protocols, we present a model used to describe an external eavesdropper attack whose purpose would be to gain information on the key. Second, we explain possible ways to quantify information in classical approaches and quantum. For this, we consider different notions of entropy to quantitatively describe information content and correlations between the different parties at stake. Additionally, we introduce the notion of security in QKD protocols. In the end of this chapter, we focus on a specific QKD protocol based on displaced squeezed states. We investigate a secret key of this protocol based on numerical simulations under the direct and reverse reconciliation.

3.1 QKD Concepts

In this section, we discuss general concepts of QKD protocols in addition to a description of eavesdropping attacks we consider in this work.

3.1.1 QKD principle and general framework

Quantum Key Distribution (QKD) is a method used to exchange secretly a key between two parties, which are often denoted as Alice and Bob. More specifically, we consider a key made of several numbers which we call key elements. A general QKD protocol can be split into two main steps. The first step corresponds to a quantum communication between Alice and Bob and the second step corresponds to the secret key distillation from the information exchanged during the first part. This last step is itself decomposed into two main parts, known as information reconciliation (error correction) and privacy amplification. For the quantum communication step, the purpose

is to encode a classical key into quantum states and to send those to the receiver. A general representation is given in Fig. 3.1. To do so, Alice and Bob agree on a communication protocol. Alice encodes each key element into a quantum state which propagates through a quantum channel. On the other end of the channel, Bob receives the state and measures it, obtaining an estimation of the key element. They repeat the procedure until every key element has been encoded and communicated. Alice and Bob also have access to a generally insecure classical channel. This channel is needed to implement classical algorithms to distil the secret key. In order to prevent any man-in-the-middle attack on this classical channel, the messages are authenticated. This means that the messages can be eavesdropped but not changed by an external attacker [49]. Since this classical procedure already requires a shared secret key between Alice and Bob, QKD falls more into the key-growing category. During the quantum communication step, a third party, often denoted as Eve, is assumed to eavesdrop the communication (both the authenticated classical and quantum channel) and gain information on the key. The security of the protocol depends on what information Eve gains. As we mentioned before, QKD can theoretically achieve unconditional security. This implies that in the most general framework, Eve is considered to be limited in her actions over the communicated quantum state only by the laws of quantum physics. In particular, when the QKD protocol relies on non-orthogonal states, the no-cloning theorem [12] forbids Eve from creating perfect copies of the state. Only imperfect cloners exist [50] which can only produce noisy copies of arbitrary quantum states. More generally, it is important that Eve disturbs the quantum states as this makes her interaction detectable. One can then estimate from this disturbance the amount of information gained by Eve on the communicated key.

One of a possible eavesdropping attacks is the intercept-resend attack. Here, Eve intercepts each quantum state sent by Alice and measures it in a way she chooses. Then, she prepares a quantum state based on her measurements and sends this state to Bob. Once again, if Alice and Bob chose to use non-orthogonal states, the no-cloning theorem again assures that Eve is not able to gain information without disturbing the states. Let us now explain how a general quantum communication protocol is built to force Eve to interact with and disturb the states sent by Alice. A general quantum communication protocol consists in Alice randomly choosing, for each key element k_i, a quantum state from an ensemble $\mathcal{E}_\mathrm{m}$. This ensemble is itself randomly chosen among L possible ensemble of states [51]. Such ensemble $\mathcal{E}_\mathrm{m}$ is defined as

$$\mathcal{E}_\mathrm{m} = \left\{ p_{\mathrm{i,m}}, \left|\psi_{\mathrm{i,m}}\right\rangle \left\langle\psi_{\mathrm{i,m}}\right| \right\}, \tag{3.1}$$

where $p_{\mathrm{i,m}}$ is the probability of sending the state $\left|\psi_{\mathrm{i,m}}\right\rangle \left\langle\psi_{\mathrm{i,m}}\right|$ when the ensemble $\mathcal{E}_\mathrm{m}$

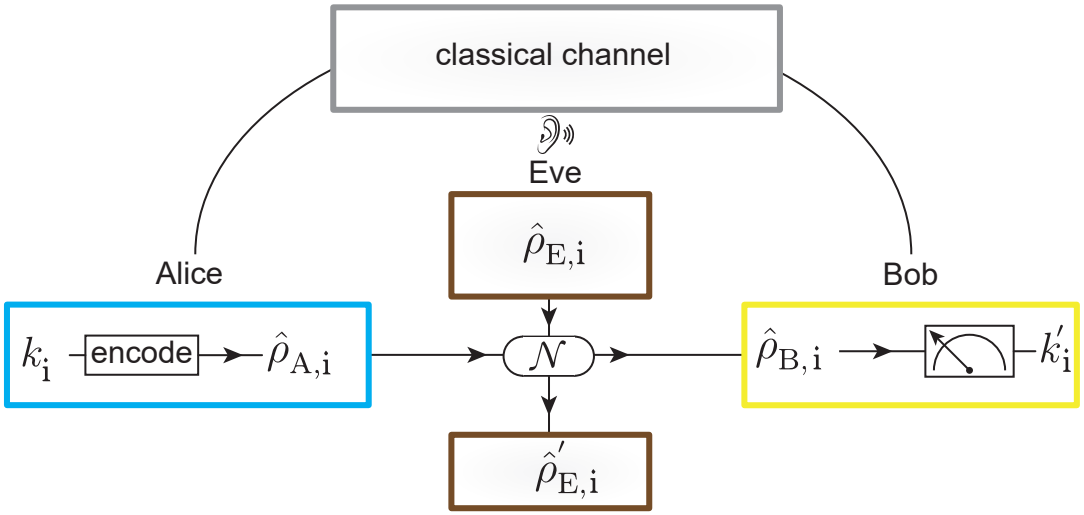


Figure 3.1: Scheme a general QKD protocol. Alice starts by getting a random number k_{i} which she encodes in a state $\hat{\rho}_{\mathrm{A,i}}$. The latter state propagates through a quantum channel $\mathcal{N}$. There, in order to get information on k_{i}, Eve probes the quantum communication channel with a state $\hat{\rho}_{\mathrm{E,i}}$. The second communication party, Bob, receives the state $\hat{\rho}_{\mathrm{B,i}}$. He performs a measurement of the received state which results into a number k'_{i}. The number represents an estimation of k_{i}. Eve also obtains a state $\hat{\rho}'_{\mathrm{E,i}}$ which may contain finite information on k_{i}. Finally, Alice and Bob can communicate classically over an authenticated classical channel which Eve can only listen to.

has been chosen. In order to protect information encoded in the sent quantum states, we need that the states in the different ensembles are non-orthogonal. It is sufficient to impose that $\left|\psi_{\mathrm{i,m}}\right\rangle\left\langle\psi_{\mathrm{i,m}}\right|$ and $\left|\psi_{\mathrm{i,m'}}\right\rangle\left\langle\psi_{\mathrm{i,m'}}\right|$ are non-orthogonal states for all i and for $m \neq m'$. Additionally, we require that

$$\forall m : \sum_i p_{\mathrm{i,m}} \left|\psi_{\mathrm{i,m}}\right\rangle\left\langle\psi_{\mathrm{i,m}}\right| = \hat{\rho}_{\mathrm{avg}}, \tag{3.2}$$

where $\hat{\rho}_{\mathrm{avg}}$ is an average density matrix that depends on the QKD protocol chosen. Since $\hat{\rho}_{\mathrm{avg}}$ is the same for every ensemble $\mathcal{E}_{\mathrm{m}}$, Eve cannot deduce from her measurement which ensemble was chosen. This way, the optimal strategy for Eve is to interact with the states sent by Alice. This interaction will then disturb the states which is detectable and quantifiable by Alice and Bob. The knowledge on the amount of information extracted by Eve determines whether or not the communication is secure.

From this general description, two groups of QKD protocols are of particular interest. The first group is represented by discrete-variable (DV) QKD protocols. The information here is encoded in discrete bases. One of the most famous protocols in DV-QKD is the BB84 protocol. For this protocol, two discrete bases are used. The first basis is the computational basis $\{|0\rangle, |1\rangle\}$ where each state has an equal probability $p = 0.5$ to

be chosen. The second discrete basis is $\left\{|+\rangle = (|0\rangle + |1\rangle) / \sqrt{2}, |-\rangle = (|0\rangle - |1\rangle) / \sqrt{2}\right\}$ where each state also has an equal probability $p = 0.5$ to be chosen. With the formalism presented in Eq. 3.2 and denoting the identity operator as $\hat{1}$, we have

$$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| = \frac{1}{2}\hat{1} = \hat{\rho}_{\text{avg}}. \tag{3.3}$$

The second group is represented by continuous variable (CV) QKD protocols where a continuous basis is used to encode the key elements. The most common choice of the basis here is the one using coherent states and squeezed states introduced in Sec. 2.1.2. Here the information is carried by the two conjugate field quadratures. The results of measurements of these quadratures are continuous values. Finally, CV protocols which use exclusively Gaussian states, such as coherent states or squeezed states, are known as Gaussian CV-QKD protocols. They are frequently employed in literature and experiments as the analysis of security of these protocols is much more accessible than for general states.

3.1.2 Information reconciliation and privacy amplification

Once Alice and Bob finish their quantum communication step, they must proceed to the distillation of a common key from the information they exchanged. This step can be classified as classical information postprecessing. Among various possible classical information postprocessing procedures, the most common one is the one-way postprocessing. It consists of a one-way classical communication between Alice and Bob through a public classical channel. Here, a distinction must be introduced. If during the procedure, the reference of information is the same as the the sender of quantum states during the quantum communication step (i.e., Alice in our case), we speak of *direct reconciliation* (DR). If the reference is the receiver of the quantum states (i.e., Bob in our case), we speak of *reverse reconciliation* (RR). Depending on the QKD protocol used, Alice and Bob may need first to discard parts of their respective data. This step is called *sifting*. One-way postprocessing is split into two steps: first an error correction step, also called *information reconciliation*, and a *privacy amplification* step.

We first focus on the information reconciliation step. This process takes two partially correlated list of symbols, key elements, of length n and generates an output a perfectly correlated list of length $l \leq n$ shared by Alice and Bob. Shannon [52] proved that the number of perfectly correlated symbols that can be extracted is theoretically limited by mutual information between Alice and Bob (see Sec. 3.2.2). For practical implementations, low-density parity-check (LDPC) codes are typically employed [53, 10]. Practical codes do not reach the bound derived by Shannon and are less efficient. The efficiency

of reconciliation algorithms in general is characterised by an efficiency parameter β. For a given reconciliation algorithm, it quantifies how close the information in the correlated symbols at the output of the algorithm to the Shannon limit. The efficiency of the codes depends generally on the problem and the available devices. A trade-off between performance/complexity also needs to be respected. Practical efficiencies achieved are usually above $\beta = 80\,\%$. Furthermore, the codes used generally work integer entries. This means that depending on the type of quantum communication step implemented, digitization of the data may be needed, which may decrease the available information. A more detailed analysis is done by Lodewyck et al. in Ref.[53]. Remarkably, they reported an efficiency of $\beta = 0.898$ for their experimental implementation of a CV-QKD protocol in the optics regime.

We now focus on the privacy amplification step. After Alice and Bob performed information reconciliation, they share a common key. However, since Eve is assumed to be able to freely eavesdrop the classical communication channel, she still has correlated information this new key. Privacy amplification algorithms have to get rid of the compromised key elements which Eve possesses at the cost of further reducing the length of the key. This procedure is often implemented by using two-universal symmetric hash functions [11]. For these functions, one defines a security parameter corresponding to the number of bits used for the implementation of the algorithm [11]. If this security parameter is large enough, Eve does not have any knowledge on the final key with high probability. The amount of information Eve has determines how large the security parameter needs to be. Therefore, the choice between direct reconciliation or reverse reconciliation is also essential for that step as Eve's information can vary significantly depending on which reconciliation was chosen.

3.1.3 Eavesdropping attacks and implementation

Another important aspect of QKD deals with how to describe and quantify Eve's possible attacks. This is necessary to be able to quantify the amount of information Eve extracted from the quantum communication step and is a crucial number for the security of the protocols. For a general description, Eve is free to interact with the states sent by Alice as she wants. As a consequence, it is a complex task to model an attack by Eve. To this extent, we first start by introducing three classes of attacks which classify Eve's possible attacks from the weakest to the strongest. In a general setup, Eve is assumed to have an ancilla, which can be simply the environment, which she uses to interfere with the quantum communication between Alice and Bob.

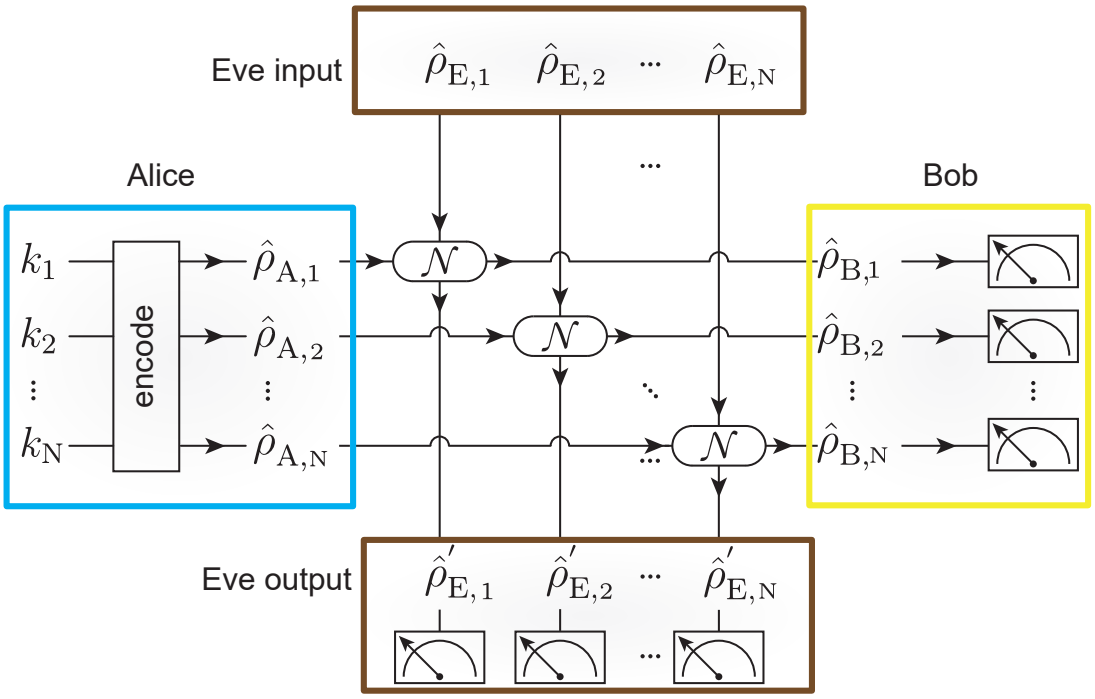


Figure 3.2: Schematic of a general individual attack. On her side, Alice encodes each of her N key elements into a quantum state $\hat{\rho}_{A,i}$. These states propagate through the quantum channel $\mathcal{N}$, assumed to be under Eve's control. Eve interacts individually with each of Alice's states. Each interaction is the same and does not depend on $\hat{\rho}_{A,i}$. At the output of the quantum channel, Bob receives a state $\hat{\rho}_{B,i}$ for each state sent by Alice. He performs individual measurement on his received states. Finally, Eve receives a state $\hat{\rho}'_{E,i}$ for each state sent by Alice. She also measures them individually.

Individual attacks

Individual attacks (see Fig. 3.2) is a family of attacks described as the most constrained one [10]. They are defined by two properties. The first one states that Eve is assumed to interact with the incoming states from Alice individually and independently using the same approach and strategy. The second property is that Eve measures her ancilla before Alice and Bob proceed to classical information postprocessing, i.e., to information reconciliation and privacy amplification steps. Therefore, at this stage, Alice, Bob, and Eve both share classical elements. The previously introduced intercept-resend attack falls into this category, as Eve interacts individually and independently with each signal using this strategy. For a general protocol, an upper bound of Eve's information is found by performing an optimization over all possible measurements which Eve can implement. The resulting upper bound of Eve's information depends on the type of protocol used.

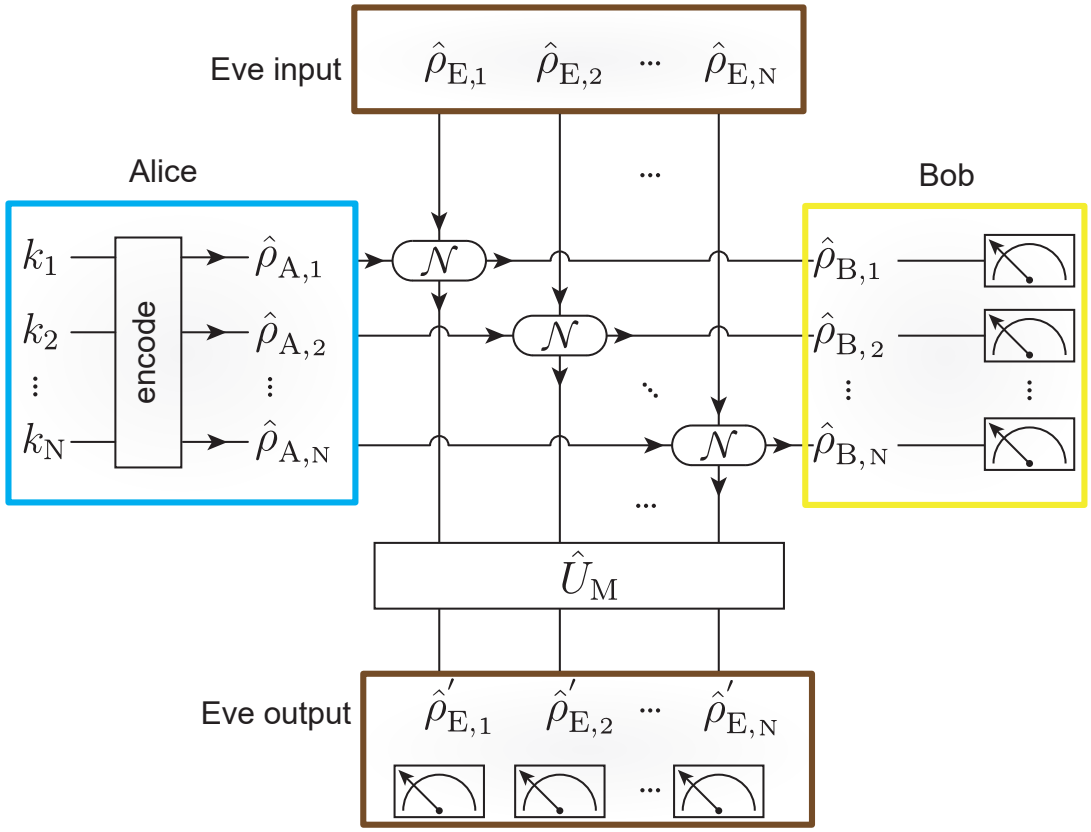


Figure 3.3: Schematic of a general collective attack. On her side, Alice encodes each of her N key elements into a quantum state $\hat{\rho}_{\mathrm{A,i}}$. These states propagate through the quantum channel $\mathcal{N}$, assumed to be under Eve's control. Eve interacts individually with each of Alice's states. Each interaction is the same and does not depend on $\hat{\rho}_{\mathrm{A,i}}$. At the output of the quantum channel, Bob receives a state $\hat{\rho}_{\mathrm{B,i}}$ for each state sent by Alice. He performs individual measurement on his received states. Finally, Eve receives a state $\hat{\rho}'_{\mathrm{E,i}}$ for each state sent by Alice. Contrary to individual attacks, Eve is free to perform an optimal collective measurement by applying a unitary $\hat{U}_\mathrm{M}$ to her ensemble of states.

Collective attacks

Collective attacks (see Fig. 3.3) is another family of attacks [10]. As for individual attacks, they are defined by two properties. First, Eve is assumed again to interact individually and independently with each incoming states from Alice using the same strategy. Second, Eve can now store her ancilla into a quantum memory until the end of the classical information postporcessing step. Then, she performs an optimal collective measurement on her ancilla. For instance, she can apply a joint unitary $\hat{U}_\mathrm{M}$ to her entire ancilla and measures each state individually.

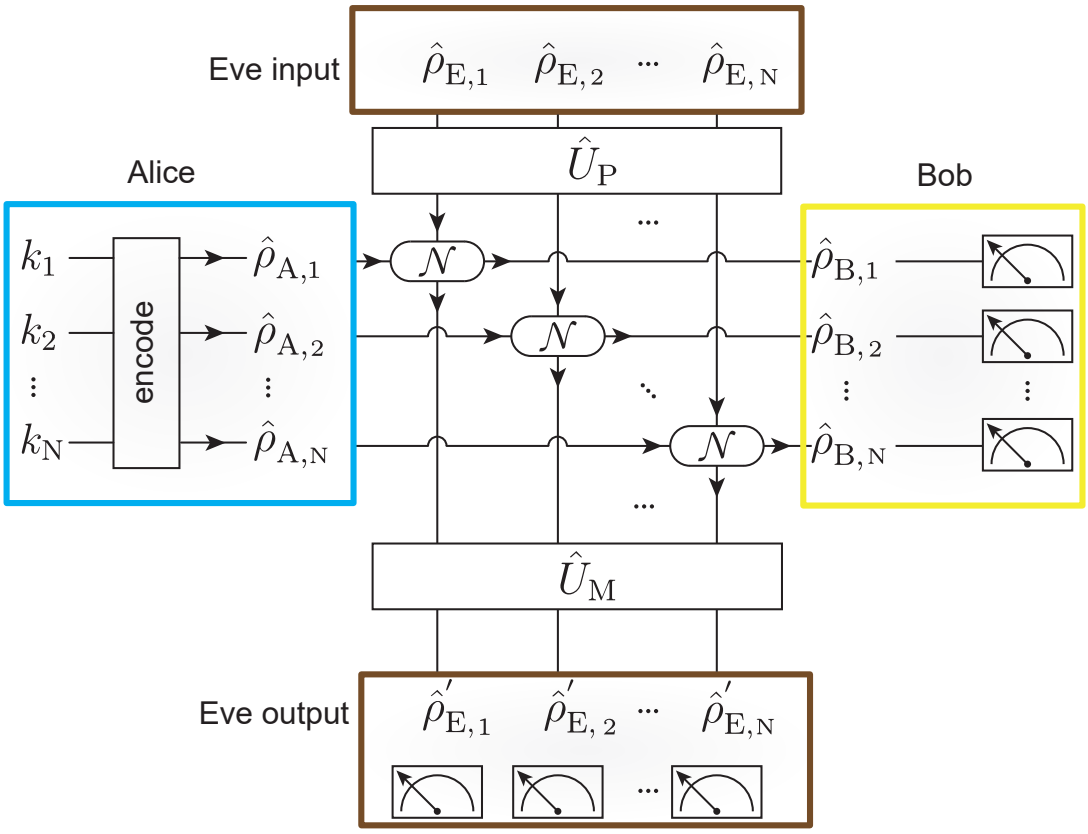


Figure 3.4: Schematic of a general coherent attack. On her side, Alice encodes each of her N key elements into a quantum state $\hat{\rho}_{\mathrm{A,i}}$. These states propagate through the quantum channel $\mathcal{N}$, assumed to be under Eve's control. This time, Eve is free to prepare her ensemble in any possible manner by applying a unitary $\hat{U}_{\mathrm{P}}$ to her ensemble. Each mode of her newly formed ensemble interacts, through the quantum channel $\mathcal{N}$, with the states $\hat{\rho}_{\mathrm{A,i}}$ sent by Alice. At the output of the quantum channel, Bob receives a state $\hat{\rho}_{\mathrm{B,i}}$ for each state sent by Alice. He performs individual measurement on his received states. Finally, Eve receives a state $\hat{\rho}'_{\mathrm{E,i}}$ for each state sent by Alice. Once again, Eve is free to perform a optimal collective measurement by applying a unitary $\hat{U}_{\mathrm{M}}$ to her ensemble of states.

Coherent attacks

Coherent attacks (see Fig. 3.4) describe Eve's most general and powerful attack [10]. By definition, it is not limited by any technical restrictions. This means that Eve is able to interact freely and in any possible way allowed by the laws of physics with the states sent by Alice. Finding the optimal coherent attack is very challenging to implement as coherent attacks cannot be precisely parametrized. However, some simplifications can be achieved. The central argument is provided by the de Finetti theorem [54]. Thanks to this theorem, coherent attacks can be reduced to collective attacks [55, 54]. In other words, the theorem is used to argue that collective attacks can be as powerful as coherent attacks. This statement relies on the assumption that the

classical postprocessing step is symmetric. This proof only works when we consider the so-called asymptotic case, or in the asymptotic scenario, where the number of exchange key elements goes to infinity. If one consider a realistic scenario where this number is finite, the claim does not hold. However, one can argue that in a realistic scenario, a large number of states is typically communicated which brings us very close to the asymptotic case. For these reasons, we limit our analysis in this thesis to the asymptotic case and collective attacks.

Two-mode squeezed vacuum state

In Sec. 3.1.3 to Sec. 3.1.3, we introduced different categories of possible attacks. We now focus on the implementation of Eve's attack. To this extent, we briefly describe another state that is needed to describe this attack. Until now, the Gaussian states introduced in Chapter 2 were single-mode states which are local to one party. In the context of CV-QKD, the two-mode squeezed vacuum (TMSV) state is a non-local state which possesses finite quantum entanglement and is related to the Einstein-Podolsky-Rosen (EPR) state [56]. A TMSV state is obtained by applying to the vacuum state a two-mode squeeze operator [57]

$$\hat{S}_{1,2} = \exp\left(\xi^* \hat{a}_1 \hat{a}_2 - \xi \hat{a}_1^\dagger \hat{a}_2^\dagger\right), \tag{3.4}$$

where $\hat{a}_\mathrm{i}$ is the annihilation operator of the i-th mode. Similarly to a single-mode squeezed state, we define $\xi = re^{i\varphi}$ where r corresponds to the amount of squeezing and determines, with the phase φ, the correlations between quadratures of each mode. For $\varphi = 0$, we can express the mean $\bar{\mathbf{r}}_\mathrm{TM}$ and covariance matrix $\mathbf{V}_\mathrm{TM}$ as [16]

$$\bar{\mathbf{r}}_\mathrm{TM} = \mathbf{0} \quad \text{and} \quad \mathbf{V}_\mathrm{TM} = \frac{1}{4}\begin{pmatrix} \cosh(2r) & 0 & \sinh(2r) & 0 \\ 0 & \cosh(2r) & 0 & -\sinh(2r) \\ \sinh(2r) & 0 & \cosh(2r) & 0 \\ 0 & -\sinh(2r) & 0 & \cosh(2r) \end{pmatrix}. \tag{3.5}$$

Remarkably, we can see from Eq. 3.5 and Eq. 2.22 that locally each mode looks like thermal states with a noise photon n_th such that $\cosh(2r) = (1 + 2n_\mathrm{th})$.

Eve's attack implementation

Since we would like to consider collective attacks, we need to optimize Eve's attack over possible physical attacks to maximize information she obtains. It is possible to simplify this approach. This stems from the fact that Gaussian attacks are proven to be optimal attacks among collective attacks [58]. This optimality of the Gaussian attacks

refers to the security of the protocol. In other words, if a protocols is proven secure for this type of attack, then it is secure from any general collective attack. Therefore, we can restrict ourselves to considering Gaussian collective attacks for Eve. A Gaussian attack is implemented via a one-mode Gaussian quantum channel which is used to interact with the states sent by Alice. Such quantum channel is defined as a completely positive map acting on a single bosonic mode and preserves Gaussian statistics of the channel input states. So, if the input states are Gaussian states, a Gaussian attack produces also Gaussian states. Furthermore, this thesis investigates a CV-QKD protocol using Gaussian states. Therefore, we consider from now on, that the input states sent by Alice are Gaussian states.

The following is a description of a general Gaussian collective attack and based on [59]. As mentioned above, such an attack is modelled as a Gaussian channel acting on single modes. For a Gaussian state with mean $\bar{\mathbf{r}}$ and covariance matrix $\mathbf{V}$, as defined in Eq. 2.12 and Eq. 2.13, a Gaussian channel G outputs another Gaussian state with mean $\bar{\mathbf{r}}'$ and covariance matrix $\mathbf{V}'$ given by

$$\begin{aligned} \bar{\mathbf{r}}' &= \mathbf{T}\bar{\mathbf{r}} + \mathbf{d}, \\ \mathbf{V}' &= \mathbf{T}\mathbf{V}\mathbf{T}^T + \mathbf{N}. \end{aligned} \tag{3.6}$$

where $\mathbf{d} \in \mathbb{R}^2$ and $\mathbf{T}$,$\mathbf{N} \in \mathbb{R}^{2\times 2}$. These two matrices parametrize any physical map acting on the input Gaussian states. In particular, $\mathbf{T} = \sqrt{\tau}\mathbb{I}$ where $\mathbb{I}$ is the identity matrix represents physically the action of a beamsplitter of transmissivity τ. This can be used to represent adding losses on a physical system. Additionally, $\mathbf{N} = n\mathbb{I}$ represents adding n photons to the input Gaussian states. This is can be used to represent adding noise on a physical system. We can use this formalism to describe a lossy noise quantum channel. The interesting point is that G can be further decomposed as $G = U_{\mathrm{B}} \circ C \circ U_{\mathrm{A}}$. Here, U_{B}, U_{A}, and C are individually physical maps and $\circ$ indicates that there are composed one after another (i.e., they are applied one after the other). Additionally, U_{A},U_{B} are called Gaussian unitaries and C is called the canonical form. A Gaussian unitary is defined in Ref.[59] as a unitary $\hat{U}$ acting on a Gaussian state $\hat{\rho}$ with mean $\bar{\mathbf{r}}$ and covariance matrix $\mathbf{V}$. This unitary action can be characterized by the following transformations

$$\begin{aligned} \hat{\rho}' &= \hat{U}\hat{\rho}\hat{U}^{\dagger}, \\ \bar{\mathbf{r}}' = \mathbf{S}\bar{\mathbf{r}} + \mathbf{d}, \quad &\text{and} \quad \mathbf{V}' = \mathbf{S}\mathbf{V}\mathbf{S}^T. \end{aligned} \tag{3.7}$$

where $\mathbf{S}$ is a symplectic matrix meaning that

$$\text{for } \mathbf{\Omega} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathbf{S}\mathbf{\Omega}\mathbf{S}^T = \mathbf{\Omega}. \tag{3.8}$$

The canonical form C is a Gaussian channel G for which $\mathbf{d} = \mathbf{0}$ and $\mathbf{T} = \mathbf{T}_C, \mathbf{N} = \mathbf{N}_C$ are diagonal. For Eve's Gaussian collective attack implementation, it is modelled as Eve replacing Alice and Bob quantum channel by her own quantum channel. The latter is then described as a lossy noise channel. This means that Eve's quantum channel induces losses and couples noise to an input state. This encompasses all losses to the states sent by Alice such as losses from cables or coming from Eve's devices. This also includes any noise coupled to the states sent by Alice such as thermal noise, noise coming from Eve's devices, or noise added due to Eve specific attack. We parametrize Eve's Gaussian collective attack with two parameters, the transmissivity τ of the channel and the noise η. The transmissivity τ ranges from 0 to 1 and the noise η corresponds to a photon number which is always positive.

Now, we describe a specific practical implementation. We start by splitting the attack into two parts, the action of the attack on the states and the collective measurement performed by Eve.

Regarding the action of the attack, we have to implement the transformation described by Eq. 3.6. Thanks to Stinespring's dilution theorem [60], every Gaussian channel can be seen as a unitary operation coupling the input state to the environment. This representation is unique up to isometries. In our case, the environment is under control of Eve. As explained in [59], we look first at the canonical form C of the Gaussian channel and apply again Stinespring's dilution theorem. One obtains that the canonical form can be uniquely represented by a symplectic transformation $\mathbf{L}$ up to an isometry. This symplectic transformation $\mathbf{L}$ acts on the input states sent by Alice. It couples them with a TMSV state (see Sec. 3.1.3) with a variance parametrized by a squeezing factor r as given by Eq. 3.5 and such that $\cosh(2r) = (1 + 2n_{\text{Eve}})$. Therefore, Eve's ancilla can be considered to be a TMSV state. There are eight possible different transformations which depend on how the coupling with the TMSV state is done. For a complete characterization of each possible transformations, we refer the reader to the table presented in [59]. This concludes the description of the canonical form C. Then, in order to describe the full quantum channel, one needs to consider additionally the two Gaussian unitaries, U_A and U_B.

Regarding the collective measurement, one normally has to consider the optimal collective measurement that Eve could apply. Nevertheless, it is possible to also circumvent this task by using upper bounds on Eve's information. Such bounds allowed us to disregard the precise collective measurement Eve performs. Out of the available bounds, we used the so-called Holevo bound, which we explain further in Sec. 3.2.2. This bound is invariant under isometric operation. This means that the environment unitary can be disregarded as well. We briefly explain what we consider an isometric operation. An operation on a quantum state with a density matrix $\hat{\rho}$ is called isometric

transformation if there an isometry $\hat{V}$ such that $\hat{\rho}$ is transformed as

$$\hat{\rho} \rightarrow \hat{V}\hat{\rho}\hat{V}^{\dagger}. \tag{3.9}$$

For our description of Eve's attack, we consider only losses and coupled noise. It turns out that this can be fully described by the canonical form of the Gaussian channel. Fig. 3.5 illustrates the implementation of Eve's attack. More specifically, for $0 \leq \tau < 1$, we get

$$\begin{gathered} U_{\mathrm{A}} = U_{\mathrm{B}} = \hat{1}, \\ \mathbf{T}_{\mathrm{C}} = \sqrt{\tau}\mathbb{I}, \quad \mathbf{N}_{\mathrm{C}} = \frac{1}{4}(1-\tau)(1+2n_{\mathrm{Eve}})\,\mathbb{I}, \end{gathered} \tag{3.10}$$

where $\hat{1}$ is the identity operator and $\mathbb{I}$ is the identity matrix. We keep these two last notations for the remaining of this section. The canonical form corresponds physically to a beam splitter with transmissivity τ [16] coupling one mode of the TMSV state. This mode locally looks like a thermal state with a thermal noise photon n_{Eve}. Considering an input Gaussian state $\hat{\rho}$ with mean $\bar{\mathbf{r}}$ and covariance matrix $\mathbf{V}$, we obtain the following transformation

$$\begin{aligned} \bar{\mathbf{r}}' &= \sqrt{\tau}\,\bar{\mathbf{r}}, \\ \mathbf{V}' &= \tau\mathbf{V} + \frac{1}{4}(1-\tau)(1+2n_{\mathrm{Eve}})\,\mathbb{I}, \end{aligned} \tag{3.11}$$

where we see that the transmissivity τ and the input noise n_{Eve} are coupled together. In order to have two separate parameters, we parametrize the coupled noise as

$$(1-\tau)(1+2n_{\mathrm{Eve}}) = \eta' + (1-\tau). \tag{3.12}$$

Inserting Eq. 3.12 in Eq. 3.11, we then get

$$\bar{\mathbf{r}}' = \sqrt{\tau}\bar{\mathbf{r}} \quad \text{and} \quad \mathbf{V}' = \tau\mathbf{V} + \eta\mathbb{I} + \frac{1}{4}(1-\tau)\,\mathbb{I}, \tag{3.13}$$

where we defined $\eta = \eta'/4$. Now τ and η are two independent parameters and correspond exactly to the losses and noise of Eve's quantum channel that we defined above. This specific attack is known as the entangling cloner attack [61]. Unfortunately, for $\tau = 1$ and $\eta \neq 0$, this model cannot be strictly implemented. Indeed, in this case, we have

$$\begin{gathered} U_{\mathrm{A}} = U_{\mathrm{B}} = \hat{1} \quad , \quad \mathbf{T}_{\mathrm{C}} = \mathbb{I}, \quad \mathbf{N}_{\mathrm{C}} = \eta\mathbb{I}, \\ \bar{\mathbf{r}}' = \bar{\mathbf{r}} \quad \text{and} \quad \mathbf{V}' = \mathbf{V} + \eta\mathbb{I}. \end{gathered} \tag{3.14}$$

Instead, one can view this case as the asymmetric limit of the entangling cloner attack

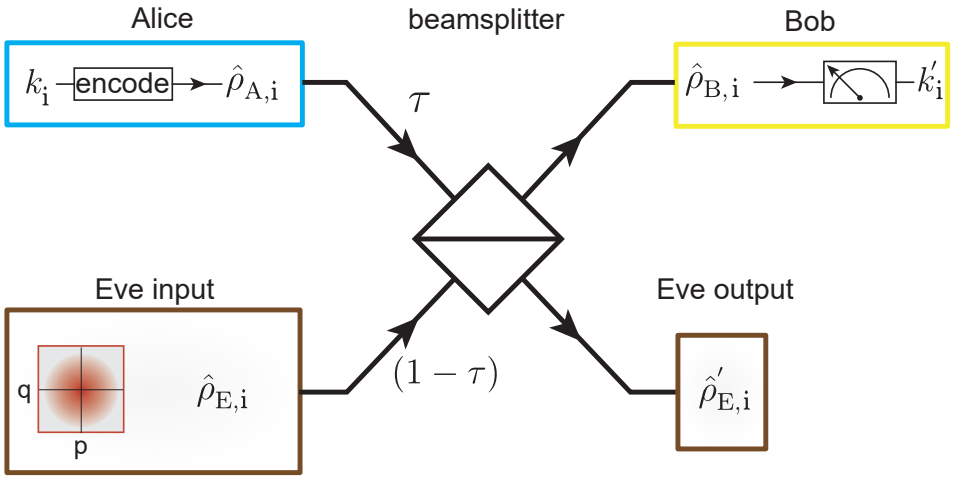


Figure 3.5: Schematic of Eve's entangling cloner attack. Alice encodes each key element k_{i} into a quantum state $\hat{\rho}_{\mathrm{A,i}}$. Individually, each of these states are coupled through a beamsplitter of transmissivity τ to one mode of Eve's TMSV which locally looks like a thermal state. This is represented by the red Wigner function. One output of the beamsplitter is kept by Eve while another is sent to Bob.

where $\tau \to 1$ as seen from Eq. 3.13. The attack in itself is known as the universal Gaussian cloner attack [62].

3.2 Gaussian quantum information and security

In this section, we investigate different notions of entropy and the security of QKD protocols. First, we look at different entropy quantities which are useful to characterise information exchanged in our QKD protocol. We focus in particular on the differential entropy to characterize classical correlations. The Von Neumann entropy allows us to evaluate general quantum information content. In the second step, we introduce important *mutual information* and *Holevo quantities*. The former is used to quantify general correlations between Alice and Bob and the latter is used to obtain an upper bound on Eve's information. Using these quantities, we define two central quantifiers of CV-QKD, the *secret key K* and the *secret key rate R*. The positivity of the secret key determines whether the communication between Alice and Bob is secure or not.

3.2.1 Entropy of quantum states

In this section, we focus on entropy quantities for classical and quantum systems. To this end, we present the well-known Shannon entropy for DV systems before presenting the differential entropy for CV systems. Then, we consider at the Von Neumann entropy which is the equivalent entropy for quantum systems. Furthermore, we present the

so-called mutual information which is used to characterize the information shared between Alice and Bob at the end of the QKD protocol. One finds an upper bound on Eve's information by introducing the Holevo quantity which is defined using the Von Neumann entropy. This useful upper bound simplifies the analysis of possible Eve's attacks. From it, we define the secret key K and secret key rate R.

Shannon entropy

In classical information theory, the Shannon entropy is an important tool to quantify information content of a system. Considering a discrete random variable X which takes its values in the set $\{x_1, \ldots, x_N\}$, its Shannon entropy H is defined by

$$H(X) = -\sum_{i}^{N} p_i \log_b(p_i), \tag{3.15}$$

where p_i is the probability of X being x_i. The logarithm used here is in base b. The common bases are $b = 2$ and $b = e$ which in term of units correspond to bits and nats, respectively. The Shannon entropy H can be interpreted in different ways. On the one hand, it can be seen as the amount of uncertainty about X. For a classical system, one can view it as the information required to describe such system. This comes from the Shannon's source coding theorem [52] used in data compression. In this context, one obtain from the theorem that the Shannon entropy gives the minimum number of bits required to describe the full information about the system.

Differential entropy

The previously introduced Shannon entropy deals with classical discrete random variables. In this work, we are interested in continuous random variables. To measure the entropy of such random variables, we have to introduce another quantity called the differential entropy h. For a continuous random variable X with probability density function f, we define

$$h(X) = -\int_{\mathcal{D}} f(x) \log_b(f(x)) \, \mathrm{d}x. \tag{3.16}$$

where $\mathcal{D}$ is the domain of definition of f. This quantity intuitively seems to correspond to the continuous extension of the Shannon entropy but it is not exactly the case. First, the limit of the Shannon entropy when $n \to +\infty$ does not coincide with the differential entropy [63]. Second, the differential entropy can take negative values for certain variables. Lastly, it is only defined up to an arbitrary constant. For instance, if one

defines $Y = aX$, one can show that

$$h(Y) = h(X) + \log_{\mathrm{b}} |a|. \tag{3.17}$$

Nevertheless, it remains a useful quantity which is used throughout this work because we are interested in difference between differential entropies where the problems mentioned just above disappear.

Von Neumann entropy

To measure the entropy of quantum states, we need to use a quantum version of entropy which is the Von Neumann entropy S. For an arbitrary quantum state described by a density matrix $\hat{\rho}$, the Von Neumann entropy is defined as

$$S(\hat{\rho}) = -\mathrm{Tr}\left(\hat{\rho}\log(\hat{\rho})\right), \tag{3.18}$$

where log is the natural matrix logarithm. One can rewrite the Von Neumann entropy of a density matrix $\hat{\rho}$ using the eigenvalues λ_{i} of $\hat{\rho}$ as

$$S(\hat{\rho}) = -\sum_{\mathrm{i}} \lambda_{\mathrm{i}} \log(\lambda_{\mathrm{i}}), \tag{3.19}$$

where log is the natural logarithm. If we want to express the Von Neumann in terms of bits, we replace log in Eq. 3.19 by $\log_2$. This equation also draws a parallel with the Shannon entropy. For Gaussian states, the calculation simplifies as the Von Neumann entropy can be calculated from the covariance matrix of the state. In particular, for single-mode Gaussian states ($N = 1$), one obtains that [27]

$$S(\hat{\rho}) = g\left(\sqrt{\det \mathbf{V}}\right), \tag{3.20}$$

where

$$g(x) = \left(2x + \frac{1}{2}\right)\log\left(2x + \frac{1}{2}\right) - \left(2x - \frac{1}{2}\right)\log\left(2x - \frac{1}{2}\right). \tag{3.21}$$

For two-mode Gaussian states ($N = 2$), one first needs to rewrite the covariance matrix in the form

$$\mathbf{V} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^{\mathrm{T}} & \mathbf{B} \end{pmatrix}, \tag{3.22}$$

where $\mathbf{A} \in \mathbb{R}^{2\times2}$ locally describes one mode, $\mathbf{B} \in \mathbb{R}^{2\times2}$ locally describes the other mode, and $\mathbf{C} \in \mathbb{R}^{2\times2}$ describes the correlation between the modes. One can define

$$\Delta = \det \mathbf{A} + \det \mathbf{B} + 2 \det \mathbf{C}, \tag{3.23}$$

to obtain that [64]

$$S(\hat{\rho}) = g(\nu_+) + g(\nu_-), \tag{3.24}$$

where

$$\nu_\pm = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4\det \mathbf{V}}}{2}} \tag{3.25}$$

are symplectic eigenvalues of $\mathbf{V}$, with Δ defined as in Eq. 3.23. Lastly, the Von Neumann entropy is invariant under isometric operations. In other words, for any density matrix $\hat{\rho}$ and any isometric operator $\hat{V}$, we have

$$S\left(\hat{V}\hat{\rho}\hat{V}^\dagger\right) = S(\hat{\rho}). \tag{3.26}$$

3.2.2 Mutual information and Holevo quantity

Another important aspect we need for our analysis is the way to describe correlations between two parties. To this extent, we introduce two crucial quantities which are the mutual information and the Holevo quantity. Their description relies on the previously introduced entropies.

Mutual information

For a pair of discrete random variables (X,Y) defined over a domain of definition $\mathcal{D}_\mathrm{X} \times \mathcal{D}_\mathrm{Y}$ ($\mathcal{D}_\mathrm{X}$ being the domain of definition for X and $\mathcal{D}_\mathrm{Y}$ being the domain of definition for Y) with a joint probability distribution $p_{(\mathrm{X,Y})}$, we can define their mutual information as

$$I(X{:}Y) = \sum_{(x,y)\in\mathcal{D}_\mathrm{X}\times\mathcal{D}_\mathrm{Y}} p_{(\mathrm{X,Y})} \log_\mathrm{b} \frac{p_{(\mathrm{X,Y})}(x,y)}{p_\mathrm{X}(x)\, p_\mathrm{Y}(y)}. \tag{3.27}$$

where p_X and p_Y are the probability distribution of X and Y, respectively. This quantifies the amount of correlation between the two variables X and Y. A useful representation can be obtained by introducing the the conditional entropy $H(Y|X)$. It can be seen as the Shannon entropy of Y conditioned by the values taken by X. The latter is defined as

$$H(Y|X) = -\sum_{x\in\mathcal{D}_\mathrm{X}} \sum_{y\in\mathcal{D}_\mathrm{Y}} p_{(\mathrm{X,Y})}(x,y) \log_\mathrm{b}\left(p_{\mathrm{Y|X}}(y|x)\right), \tag{3.28}$$

where $p_{\mathrm{Y|X}}$ is the probability density of the random variable Y conditioned on $\{X = x\}$. Then we can rewrite the mutual information as

$$I(X{:}Y) = H(Y) - H(Y|X). \tag{3.29}$$

This way, we can see the mutual information as the reduce in uncertainty on Y knowing X. From Eq. 3.28 and Eq. 3.16, we see that for independent variables, we have $H(Y|X) = H(Y)$ so $I(X{:}Y) = 0$.

Interestingly, this definition can be extended to continuous random variables. We can indeed define the conditional differential entropy

$$h(Y|X) = -\int_{\mathcal{D}_{\mathrm{X}}} \int_{\mathcal{D}_{\mathrm{Y}}} f_{(\mathrm{X,Y})}(x,y) \log_{\mathrm{b}} \left(f_{\mathrm{Y|X}}(y|x) \right) \mathrm{d}x, \tag{3.30}$$

where $f_{(\mathrm{X,Y})}$ is joint probability density function of (X,Y), $f_{\mathrm{Y|X}}$ is joint probability density function of Y conditioned on $\{X = x\}$. It is the continuous counterpart to the discrete conditional entropy defined above. One can then define a corresponding mutual information

$$I(X{:}Y) = h(Y) - h(Y|X). \tag{3.31}$$

Regarding the discussion on the differential entropy in Sec. 3.2.1, the problem that the differential entropy is defined up to a constant vanishes, since the mutual information is defined as a difference. In Fig. 3.6, we give a visual representation of the quantities introduced. Remarkably, for continuous random variables with Gaussian distributions, which we refer as Gaussian random variables in the remaining, the mutual information can be expressed in a simple form. To show this, we use some intermediate results. First, the differential entropy of a Gaussian random variable X with variance σ_X^2 reads [51]

$$h(X) = \frac{1}{2} \log_{\mathrm{b}} \left[(2\pi e)\, \sigma_X^2 \right] + C, \tag{3.32}$$

where C is a reference constant. Then, for a given pair of random variables (X,Y), we define the following classical covariance matrix

$$\Sigma_{XY} = \begin{pmatrix} \sigma_X^2 & \mathrm{Cov}(X,Y) \\ \mathrm{Cov}(X,Y) & \sigma_Y^2 \end{pmatrix}, \tag{3.33}$$

where σ_Y^2 is the variance of Y and $\mathrm{Cov}(X,Y)$ is the covariance of X and Y. The condi-

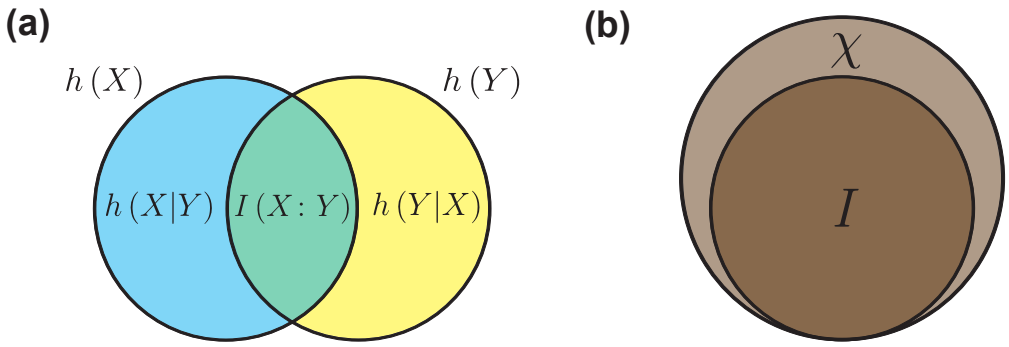


Figure 3.6: (*a*) Representation of different entropies for a pair of random variables (*X*,*Y*) and the relation between them. The blue circle represents the entropy of *X* while the yellow represents the entropy of *Y*. The overlap of the two circles represents $I(X{:}Y)$ while the remaining none overlapping parts of the circles are the conditional entropies. (*b*) Representation of mutual information, denoted as *I* which is bounded from above by the Holevo quantity, denoted as χ.

tional differential entropy in Eq. 3.28 becomes [51]

$$h(Y|X) = \frac{1}{2}\log_{\mathrm{b}}\left[(2\pi e)\,\sigma^2_{Y|X}\right] + C, \tag{3.34}$$

where C is the same as in Eq. 3.32 and $\sigma^2_{Y|X}$ is the variance of Y knowing X, defined as

$$\sigma^2_{Y|X} = \frac{\det(\Sigma_{XY})}{\sigma^2_X} = \sigma^2_Y - \frac{\mathrm{Cov}(X,Y)^2}{\sigma^2_X}. \tag{3.35}$$

From this results, one can express the mutual information as

$$I(X{:}Y) = \frac{1}{2}\log_{\mathrm{b}}\left[\frac{\sigma^2_Y}{\sigma^2_{Y|X}}\right] = \frac{1}{2}\log_{\mathrm{b}}\left[\frac{\sigma^2_Y\,\sigma^2_X}{\sigma^2_Y\,\sigma^2_X - \mathrm{Cov}(X,Y)^2}\right]. \tag{3.36}$$

The last expression is particularly useful as it can be calculated directly from experiments.

Accessible information and Holevo bound

During the quantum communication step, we consider that Alice communicates to Bob encoded key elements. Each key element is encoded in a state randomly taken from the ensemble of states $\mathcal{E}_{\mathrm{k}}$ (see Sec. 3.1.1 and Eq. 3.1). The ensemble of states communicated by Alice and received by Bob can be formulated as

$$\mathcal{E}_{\mathrm{B}} = \left\{p_{\mathrm{k_i}}, \hat{\rho}_{\mathrm{B,k_i}}\right\}, \tag{3.37}$$

where p_{k_i} is the probability that Bob receives the state $\hat{\rho}_{B,k_i}$ which encodes a key element k_i. The length of the ensemble $\mathcal{E}_B$ is the number of states measured by Bob. The amount of classical information on what Alice communicated that Bob gets from his measurements on this ensemble $\mathcal{E}_B$ is given by their mutual information $I(A{:}B)$. Here, A stands for the set of key elements of Alice and B for the set of key elements of Bob. This quantity depends on the measurement performed by Bob. To address this point, a useful quantity is the accessible information I_{acc}. For a given ensemble $\mathcal{E}_B$, it represents the maximum value of the mutual information $I(A{:}B)$ over all possible measurements performed by Bob. It is defined as

$$I_{acc}(\mathcal{E}_B) = \max_{M_B} I(A{:}B). \tag{3.38}$$

where M_B corresponds to Bob's measurements. This quantity gives the maximum obtainable correlations between Alice and Bob. However, it turns out that it is very challenging to calculate in practice due to a very large variety of implementable measurements for Bob. Fortunately, there exist an upper bound for I_{acc} such as the Holevo bound.

For a given ensemble $\mathcal{E}_B = \left\{p_{k_i}, \hat{\rho}_{B,k_i}\right\}$, the Holevo bound χ, also called the Holevo quantity, is defined as

$$\chi(\mathcal{E}_B) = S\left(\sum p_{k_i}\hat{\rho}_{B,k_i}\right) - \sum p_{k_i} S\left(\hat{\rho}_{B,k_i}\right), \tag{3.39}$$

where S is the Von Neumann entropy defined in Eq. 3.18. Due to the concavity of the Von Neumann entropy, it is always a positive quantity. Furthermore, it has the following crucial property [65]

$$I_{acc}(\mathcal{E}_B) \leq \chi(\mathcal{E}_B). \tag{3.40}$$

Since $I(A{:}B) \leq I_{acc}(\mathcal{E}_B)$, the mutual information is bounded from above by the Holevo quantity as visualized in Fig. 3.6. As we can see, the Holevo quantity does not depend on the type of measurements but only on the states used for the communication.

Similarly, if we consider Eve, her ensemble of states obtained individually at the output of her attack can be written as

$$\mathcal{E}_E = \left\{p_{k_i}, \hat{\rho}_{E,k_i}\right\}, \tag{3.41}$$

where p_{k_i} is the probability that Eve receives the state $\hat{\rho}_{E,k_i}$ at the output of her attack,

which encodes a key element k_i. We can write also that

$$I_{acc}(\mathcal{E}_E) \leq \chi(\mathcal{E}_E). \tag{3.42}$$

This allows us to bound the information obtained by Eve without having to consider what measurements she would implement.

3.2.3 Security of QKD protocol

In this section, we look into the security of QKD protocols, focused on CV-QKD. The security analysis for QKD protcols is a complex topic which is an active research field nowadays. Furthermore, we recall that the notion of "unconditionally secure" previously mentioned refers to no limitations being put on Eve's devices.

To investigate the security, it is very useful to look at the number of secure bits exchanged between Alice and Bob during the protocol. If N states are sent by Alice to Bob, the communicating parties have at their disposal a list of $n \leq N$ key elements after the sifting step. Once they finish the classical postprocessing step, they are left with a fully secure key with the length $l \leq n$. The word "secure" in this context refers to the fact that Eve does not hold any information about the final key with high probability. It is meaningful to define a quantity which we call in this work the secret key K'. It quantifies the amount of secret bits per usage of the channel. This number refers to the number of secure bits obtained at the end of the QKD protocol, so at the end of the classical postprocessing in our case. As mentioned in Sec. 3.1.3, when $N \to \infty$, we are in the aymptotic case and we therefore speak of asymptotic secret key. If one consider classical postprocessing with information reconciliation and privacy amplification, the asymptotic secret key can be expressed as[51, 11]

$$K' = \beta \cdot I(A{:}B) - I_E, \tag{3.43}$$

where β is the efficiency of the information reconciliation, $I(A{:}B)$ is the mutual information between Alice and Bob at the quantum communication step and I_E represents the information Eve has at the end of the information reconciliation step.

The secret key is expressed in bits per use of quantum channel. From this, we can define another quantity which we call the secret key rate R. It can be defined as

$$R = f_r \left(1 - D_{\text{sifting}}\right) K', \tag{3.44}$$

where f_r is called the repetition rate and is expressed in the number of states sent (i.e., the number of channel usage) per second and $\left(1 - D_{\text{sifting}}\right) \in [0,1]$ represents the

fraction of bits which are not discarded during the sifting step. Therefore, the secret key rate has the unit of bits per second and quantities the speed of the QKD protocol. These quantities (secret key and its rate) can be modified to encompass additional effects, called finite size effects, when N is finite. This adds terms to K' which are decreasing functions of N. In other words, these effects vanish when $N \to \infty$. However, it is a complex task to describe these effects. Some analysis have been done [66, 67]. The available analysis suggests that these effects reduce significantly the secret key rates. Moreover, a different description for security has been formulated when the exchanged keys have a finite number of key elements. The purpose is to parametrize the deviation of final key shared by Alice and Bob from a so-called perfect key, which is a uniformly distributed bit string on which Eve has no information [68]. However this analysis is again quite involved and complex. Details for different protocols can be found in Ref.[14]. Analysis in the asymptotic case is still useful as it allows to study the behaviour of the protocol against losses and noise. Furthermore, as emphasized in 3.1.3, one can consider that in realistic QKD protocols, N will be large enough so that we can be in the asymptotic case. For these reasons, we limit our security analysis to the asymptotic case. For CV-QKD with collective attacks, the secret key is bounded from below by [69]

$$K' \geq K = \beta I(A{:}B) - \chi_{\mathrm{E}}, \tag{3.45}$$

where χ_{E} is the Holevo quantity of Eve which represents an upper bound of her information content on the transmitted key. It depends on the information reconciliation step, whether direct reconciliation or reverse reconciliation is considered. Additionally, using the optimality of Gaussian states, we can further find an upper bound χ_{E} by assuming that all the states used for the protocol are Gaussian states. With these elements, a CV-QKD protocol is deemed secure against collective attacks if, and only if,

$$K \geq 0. \tag{3.46}$$

If $K \leq 0$ then the protocol is insecure and secure communication between Alice and Bob is impossible.

3.3 QKD protocol with squeezed states and simulations of secret key

Here, we focus now on a specific QKD protocol implementation. We investigate the secret key of such a protocol by simulating the direct reconciliation and reverse reconciliation cases. The effects of the squeezing level as well as the transmissivity τ

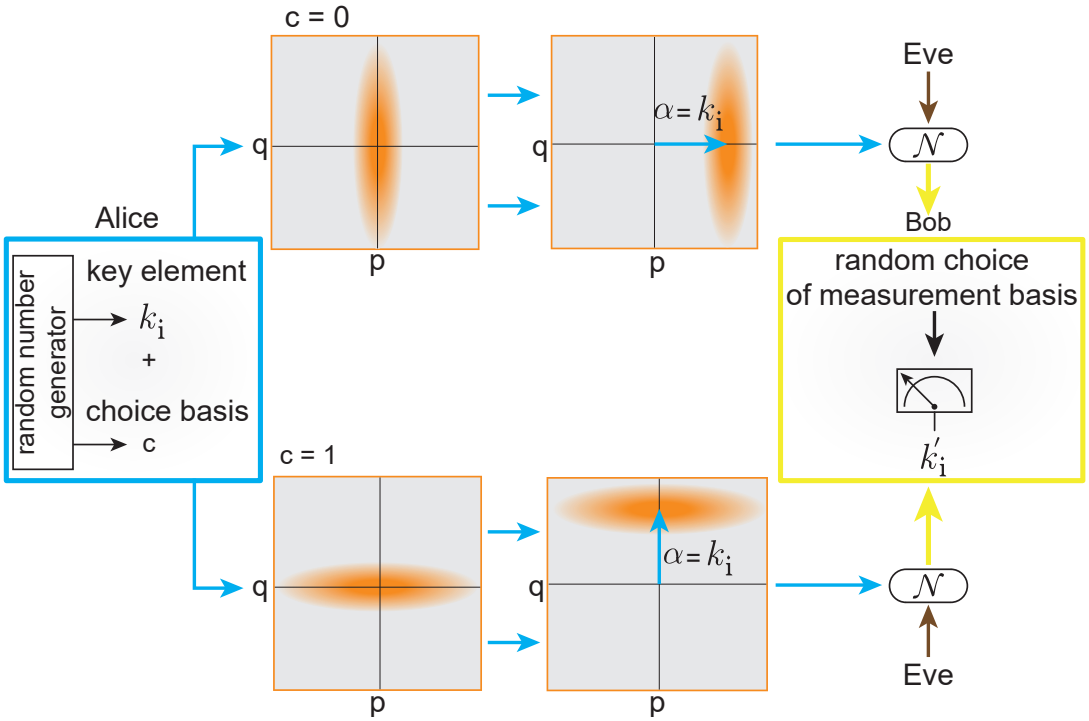


Figure 3.7: Schematic of our QKD protocol. Alice starts by generating two random numbers: a continuous number k_i from a Gaussian distribution and a number c from a binary distribution. The first one corresponds to Alice's key element and the second one corresponds to a choice of basis. If $c = 0$, Alice squeezes the q quadrature and displaces the squeezed state along the q quadrature. The displacement amplitude is given by k_i. If $c = 1$, Alice squeezes the p quadrature and displaces the squeezed state along the p quadrature. The displacement amplitude is given again by k_i. Then, the generated displaced squeezed state is sent through the quantum channel $\mathcal{N}$, which is assumed to be under control of Eve. There, Eve implements her attack. At the output of the channel, Bob receives a state which he measures in order to obtain a number k_i'. This number is an estimation of k_i. The whole procedure is then repeated N times.

and noise η on the secret key are studied for this protocol.

3.3.1 QKD with displaced squeezed microwave states

In this work, we investigate a CV-QKD protocol proposed by Cerf et al. in Ref.[19] for the optical regime. We translate this protocol to the microwave range and focus on the communication part. It is based on displaced squeezed states and can be viewed as the continuous-variable extension of the BB84 protocol. An ideal extension would require states infinitely squeezed states which are not physical. In this thesis, we consider squeezed states with a finite squeezing level S. These squeezed states are produced experimentally by using JPAs as explained in Sec. 2.2.3. Since these JPAs are

noisy, we adapt the protocol proposed by Cerf et al. by encompassing the noise n_{JPA} of the JPAs. The quantum communication part consists in the following steps (also see Fig. 3.7):

1. Alice decides on a squeezing level $S = (1 + 2n_{\mathrm{JPA}})\, e^{-2r}/4$.
2. Alice generates a random number k_{i} taken from a Gaussian distribution of a variable A with a zero mean and variance $\sigma_{\mathrm{A}}^2 = (1 + 2n_{\mathrm{JPA}}) \sinh(2r)/2$. She also generates a random bit c which can be 0 or 1 with the same probability.
3. If $c = 0$, Alice produces a displaced squeezed state (q quadrature squeezed) of squeezing level S as fixed in step 1 and mean $\bar{\mathbf{r}} = (k_{\mathrm{i}},0)$. If $c = 1$, she instead produces a displaced squeezed state (p quadrature squeezed) of mean $\bar{\mathbf{r}} = (0,k_{\mathrm{i}})$ with the same squeezing level S.
4. Alice sends the prepared state to Bob through a quantum channel controlled by Eve. Bob upon receiving the state randomly measures either the q or p quadrature with the same probability.
5. They repeat step 2 to 4 N times. The communicated key is then $\mathcal{K} = \{k_1, \ldots, k_{\mathrm{N}}\}$.
6. At the end of the communication, Alice tells to Bob through the authenticated classical channel which basis she chose to encode each key element. Eve is assumed to listen to this communication. Bob then discards the elements where he measured in the wrong basis. This ends the sifting step.

With the formalism introduced in Sec. 3.1.1, the previous quantum communication procedure makes Alice choose with same probability between two ensembles of states $\mathcal{E}_1$ and $\mathcal{E}_2$ corresponding to squeezed states (q quadrature squeezed) displaced along the q quadrature and to squeezed states (p quadrature squeezed) displaced along the p quadrature, respectively. We use the results of Sec. 2.1.1 and Eq. 3.2 for $\mathcal{E}_1$ to compute the average state $\hat{\rho}_{\mathrm{avg},1}$. It is another Gaussian state with mean $\bar{\mathbf{r}}_{\mathrm{avg},1}$ and covariance matrix $\mathbf{V}_{\mathrm{avg},1}$ given by

$$\bar{\mathbf{r}}_{\mathrm{avg},1} = \mathbf{0} \quad \text{and} \quad \mathbf{V}_{\mathrm{avg},1} = \frac{1}{4}\begin{pmatrix} (1 + 2n_{\mathrm{JPA}})\, e^{-2r} + 4\sigma_{\mathrm{A}}^2 & 0 \\ 0 & (1 + 2n_{\mathrm{JPA}})\, e^{2r} \end{pmatrix}. \tag{3.47}$$

For $\mathcal{E}_2$, we similarly get an average Gaussian state $\hat{\rho}_{\mathrm{avg},2}$ whose mean $\bar{\mathbf{r}}_{\mathrm{avg},2}$ and covariance matrix $\mathbf{V}_{\mathrm{avg},2}$ are given by

$$\bar{\mathbf{r}}_{\mathrm{avg},2} = \mathbf{0} \quad \text{and} \quad \mathbf{V}_{\mathrm{avg},2} = \frac{1}{4}\begin{pmatrix} (1 + 2n_{\mathrm{JPA}})\, e^{2r} & 0 \\ 0 & (1 + 2n_{\mathrm{JPA}})\, e^{-2r} + 4\sigma_{\mathrm{A}}^2 \end{pmatrix}. \tag{3.48}$$

The indistinguishable condition from Eq. 3.2 requires that $\hat{\rho}_{\text{avg},1} = \hat{\rho}_{\text{avg},2}$ which gives the final condition

$$\frac{1}{4}\left(1 + 2n_{\text{JPA}}\right) e^{-2r} + \sigma_{\text{A}}^2 = \frac{1}{4}\left(1 + 2n_{\text{JPA}}\right) e^{2r}. \tag{3.49}$$

This explains the choice made for the squeezing level. Thus, the ensemble of states sent by Alice on average looks like a thermal state with a photon number n_{th} such that $(1 + 2n_{\text{th}}) = (1 + 2n_{\text{JPA}})\, e^{2r}$. After the quantum communication part, Alice and Bob proceeds to the classical postprocessing with information reconciliation and privacy amplification. Nonetheless, it is important to note that usual algorithms require discrete data as inputs. In contrast, the measured key elements by Bob and the generated key elements by Alice are drawn from continuous variables and needs for this reason to be discretized. A possible procedure is proposed in Ref.[70].

3.3.2 Simulation of secret key in direct reconciliation case

We are now interested in the secret key of the protocol. We investigate the direct reconciliation case where Alice is used as a reference. The reverse reconciliation case is studied in Sec. 3.3.3. From Eq. 3.45, we have to investigate two quantities which are the mutual information between Alice and Bob $I(A{:}B)$ and Eve's Holevo quantity $\chi_{\text{E,DR}}$. We recall that we consider Gaussian collective attacks for Eve which are practically implemented with an entangling cloner attack.

Full model

The calculations for this section are based on Ref. [27, 71, 13]. For each key element k_{i}, Alice produces a displaced squeezed state either in the q or p quadrature as explained in the step 2 and 3 of Sec. 3.3.1. For Eve's attack, we consider the Gaussian collective attack that we implement as an entangling cloner attack following the description made in Sec. 3.1.3. For the entangling cloner attack, Eve starts with a TMSV state of variance $\cosh(2r) = (1 + 2n_{\text{Eve}})$. She couples one mode to the state sent by Alice with a beamsplitter of transmissivity τ where one output is sent to Bob and the other is kept by her. After the beamsplitter transformation, Bob receives a Gaussian state with mean $\bar{\mathbf{r}}_{\text{B}}^{k_{\text{i}}}$ and covariance matrix $\mathbf{V}_{\text{B}}^{k_{\text{i}}}$. Using Eq. 3.11 and Eq. 3.13, we can show that if $c = 0$ (q quadrature squeezed)

$$\begin{aligned} \bar{\mathbf{r}}_{\text{B}}^{k_{\text{i}}} &= (k_{\text{i}}, 0)\,, \\ \mathbf{V}_{\text{B}}^{k_{\text{i}}} &= \begin{pmatrix} \mathbf{V}_{\text{B,q}_1}^{k_{\text{i}}} & 0 \\ 0 & \mathbf{V}_{\text{B,p}_1}^{k_{\text{i}}} \end{pmatrix}, \end{aligned} \tag{3.50}$$

where $\mathbf{V}_{\mathrm{B},\mathrm{q}_1}^{k_\mathrm{i}} = \tau\left(1+2n_{\mathrm{JPA}}\right)e^{-2r}/4 + \eta + (1-\tau)/4$ and $\mathbf{V}_{\mathrm{B},\mathrm{p}_1}^{k_\mathrm{i}} = \tau\left(1+2n_{\mathrm{JPA}}\right)e^{2r}/4 + \eta + (1-\tau)/4$. If $c = 1$ (p quadrature squeezed)

$$\begin{aligned} \bar{\mathbf{r}}_{\mathrm{B}}^{k_\mathrm{i}} &= (0, k_\mathrm{i}), \\ \mathbf{V}_{\mathrm{B}}^{k_\mathrm{i}} &= \begin{pmatrix} \mathbf{V}_{\mathrm{B},\mathrm{q}_1}^{k_\mathrm{i}} & 0 \\ 0 & \mathbf{V}_{\mathrm{B},\mathrm{p}_1}^{k_\mathrm{i}} \end{pmatrix}, \end{aligned} \tag{3.51}$$

where $\mathbf{V}_{\mathrm{B},\mathrm{q}_1}^{k_\mathrm{i}} = \tau\left(1+2n_{\mathrm{JPA}}\right)e^{2r}/4 + \eta + (1-\tau)/4$ and $\mathbf{V}_{\mathrm{B},\mathrm{p}_1}^{k_\mathrm{i}} = \tau\left(1+2n_{\mathrm{JPA}}\right)e^{-2r}/4 + \eta + (1-\tau)/4$. For Eve, we can show that her two-modes Gaussian state $\hat{\rho}_{\mathrm{E}}^{k_\mathrm{i}}$ has the following covariance matrix if $c = 0$

$$\mathbf{V}_{\mathrm{E}}^{k_\mathrm{i}} = \begin{pmatrix} \mathbf{V}_{\mathrm{E},\mathrm{q}_1}^{k_\mathrm{i}} & 0 & \frac{1}{4}\sqrt{\tau}\Delta_\eta & 0 \\ 0 & \mathbf{V}_{\mathrm{E},\mathrm{p}_1}^{k_\mathrm{i}} & 0 & -\frac{1}{4}\sqrt{\tau}\Delta_\eta \\ \frac{1}{4}\sqrt{\tau}\Delta_\eta & 0 & \eta & 0 \\ 0 & -\frac{1}{4}\sqrt{\tau}\Delta_\eta & 0 & \eta \end{pmatrix}, \tag{3.52}$$

where $\mathbf{V}_{\mathrm{E},\mathrm{q}_1}^{k_\mathrm{i}} = (1-\tau)\left(1+2n_{\mathrm{JPA}}\right)e^{-2r}/4 + \eta + \tau/4$, $\mathbf{V}_{\mathrm{E},\mathrm{p}_1}^{k_\mathrm{i}} = (1-\tau)\left(1+2n_{\mathrm{JPA}}\right)e^{2r}/4 + \eta + \tau/4$ and $\Delta_\eta = \sqrt{(4\eta)^2 - 1}$. If $c = 1$, we get the same expression but with $\mathbf{V}_{\mathrm{E},\mathrm{q}_1}^{k_\mathrm{i}}$ and $\mathbf{V}_{\mathrm{E},\mathrm{p}_1}^{k_\mathrm{i}}$ swapped. The next step is to compute the average state of Eve. Since Alice's key elements are obtained from a continuous variable, we have to adapt the definition from Eq. 3.2 to encompass probability density functions. In our case, the average state reads

$$\hat{\rho}_{\mathrm{avg,E}} = \sum_{\mathrm{c}=0,1} \frac{1}{2} \int_{-\infty}^{\infty} f_{\mathrm{A}}\left(k_\mathrm{i}\right) \hat{\rho}_{\mathrm{E}}^{k_\mathrm{i}} \mathrm{d}k_\mathrm{i}. \tag{3.53}$$

where the summation represents the choice for c, $1/2$ corresponds to the probability of getting $c = 0$ or 1, and f_{A} is the Gaussian probability density function of Alice's random variable. With the notation introduced, we have

$$f_{\mathrm{A}}\left(x\right) = \frac{1}{\sqrt{2\pi\sigma_{\mathrm{A}}^2}} \exp\left(-\frac{x^2}{2\sigma_{\mathrm{A}}^2}\right). \tag{3.54}$$

Similarly as for Eq. 3.47 and Eq. 3.48, by using Sec. 2.1.1, we can show that the covariance matrix of Eve's average state is given by

$$\mathbf{V}_{\mathrm{avg,E}} = \begin{pmatrix} \mathbf{V}_{\mathrm{avg,E},\mathrm{q}_1} & 0 & \frac{1}{4}\sqrt{\tau}\Delta_\eta & 0 \\ 0 & \mathbf{V}_{\mathrm{avg,E},\mathrm{p}_1} & 0 & -\frac{1}{4}\sqrt{\tau}\Delta_\eta \\ \frac{1}{4}\sqrt{\tau}\Delta_\eta & 0 & \eta & 0 \\ 0 & -\frac{1}{4}\sqrt{\tau}\Delta_\eta & 0 & \eta \end{pmatrix}. \tag{3.55}$$

where $\mathbf{V}_{\mathrm{avg,E,q_1}} = \mathbf{V}_{\mathrm{avg,E,p_1}} = (1-\tau)(1+2n_{\mathrm{JPA}})\,e^{2r}/4 + \eta + \tau/4$ corresponds to Eve's one-mode at the output of the beamsplitter and $\Delta_\eta = \sqrt{(4\eta)^2 - 1}$.

Mutual information and Holevo quantity

We use the previous expressions to compute the mutual information between Alice and Bob and Eve's Holevo quantity. Following the quantum communication step, we assume that Bob performs a projective measurement, either $|q\rangle\langle q|$ or $|p\rangle\langle p|$. Different measurement bases have the same probability $p = 1/2$ to be chosen. We can further consider that Bob measures only in the basis of squeezed quadratures, since measurements in the basis of antisqueezed quadratures are discarded during the sifting step. Using Eq. 3.50 as well as 3.51, we can describe Bob's measurement by a Gaussian classical conditional random variable $B|A$. It is conditioned on Alice's key element k_{i}. Furthermore, its mean is given by $\sqrt{\tau}\,k_{\mathrm{i}}$ and its variance by

$$\sigma^2_{B|A} = \frac{1}{4}\tau\,(1+2n_{\mathrm{JPA}})\,e^{-2r} + \eta + \frac{1}{4}\,(1-\tau)\,. \tag{3.56}$$

Then, Bob's overall measurement probability density function f_{B} is given by

$$f_{\mathrm{B}}\,(y) = \int_{-\infty}^{\infty} f_{\mathrm{B|A}}\,(y|x)\,f_{\mathrm{A}}\,(x)\,\mathrm{d}x, \tag{3.57}$$

where $f_{\mathrm{B|A}}$ is the probability density function of the random conditional variable $B|A$ introduced above. This gives that Bob's overall measurement is described by a conditioned Gaussian classical random variable B of mean 0 and variance

$$\begin{aligned}\sigma^2_B &= \frac{1}{4}\tau\,(1+2n_{\mathrm{JPA}})\,e^{-2r} + \tau\sigma^2_{\mathrm{A}} + \frac{1}{4}\,(1-\tau) + \eta \\ &= \frac{1}{4}\tau\,(1+2n_{\mathrm{JPA}})\,e^{2r} + \frac{1}{4}\,(1-\tau) + \eta.\end{aligned} \tag{3.58}$$

where we use Eq. 3.49. Using the first equation in Eq. 3.36, we can calculate that the mutual information between Alice and Bob expressed in bits is given by

$$I\,(A{:}B) = \frac{1}{2}\log_2\left(\frac{\tau\,(1+2n_{\mathrm{JPA}})\,e^{2r} + 4\eta + (1-\tau)}{\tau\,(1+2n_{\mathrm{JPA}})\,e^{-2r} + 4\eta + (1-\tau)}\right). \tag{3.59}$$

One can verify that this expression coincides with the second equation in Eq. 3.36. Here, we derive another very useful result for this mutual information. If we use Eq. 3.58 in

combination with Eq. 3.59, we can write that

$$\begin{aligned} I(A{:}B) &= \frac{1}{2}\log_2\left(\frac{\tau(1+2n_{\mathrm{JPA}})\,e^{2r}+4\eta+(1-\tau)}{\tau(1+2n_{\mathrm{JPA}})\,e^{-2r}+4\eta+(1-\tau)}\right) \\ &= \frac{1}{2}\log_2\left(\frac{\tau(1+2n_{\mathrm{JPA}})\,e^{-2r}+4\tau\sigma_{\mathrm{A}}^2+(1-\tau)+4\eta}{\tau(1+2n_{\mathrm{JPA}})\,e^{-2r}+4\eta+(1-\tau)}\right) \\ &= \frac{1}{2}\log_2\left(1+\frac{4\tau\sigma_{\mathrm{A}}^2}{\tau(1+2n_{\mathrm{JPA}})\,e^{-2r}+4\eta+(1-\tau)}\right) \\ &= \frac{1}{2}\log_2\left(1+\mathrm{SNR}\right). \end{aligned} \tag{3.60}$$

where we defined the so-called *signal-to-noise ratio* (SNR) as

$$\mathrm{SNR} = \frac{\tau\sigma_{\mathrm{A}}^2}{\frac{1}{4}\tau(1+2n_{\mathrm{JPA}})\,e^{-2r}+\eta+\frac{1}{4}(1-\tau)}. \tag{3.61}$$

This is a very practical result as it means that we can compute an experimental SNR from the mutual information when this QKD protocol is implemented experimentally. This is a crucial point in Chapter. 5.

The derivation of $\chi_{\mathrm{E,DR}}$ is more straightforward. From the definition of the Holevo quantity from Eq. 3.39 adapted to encompass continuous variables and by using Eq. 3.53, we can write

$$\chi_{\mathrm{E,DR}} = S\left(\hat{\rho}_{\mathrm{avg,E}}\right) - \sum_{\mathrm{c}=0,1}\frac{1}{2}\int_{-\infty}^{\infty} f_{\mathrm{A}}(k_{\mathrm{i}})\; S\left(\hat{\rho}_{\mathrm{E}}^{k_{\mathrm{i}}}\right)\,\mathrm{d}k_{\mathrm{i}}. \tag{3.62}$$

where S is the von Neumann entropy which is computed using Eq. 3.24. To this extent, we use the covariance matrix of Eve's states formulated in Eq. 3.52 and Eq. 3.55.

Simulation secret key

We numerically calculate the secret key in the optimal reconciliation case where $\beta = 1$ from the definition in Eq. 3.45. We investigate effects of the losses and noise individually. As seen in Fig. 3.8, the secret key versus is plotted against the transmissivity τ (corresponding to losses $1-\tau$) and squeezing level of the JPA. Here, we set the noise $\eta = 0$. For the noise photon of the JPA, we assigned a typical value of $n_{\mathrm{JPA}} = 0.1$. We observe that the secret key increases with the squeezing level. On the contrary, it decreases with the losses. Interestingly, we see that no matter the squeezing level, the secret key becomes negative when $\tau \leq 0.5$. This limit has an important implication physically since the wires and cables have increased losses with their length. Therefore, it ultimately limits the distance over which the communication is possible. Furthermore,

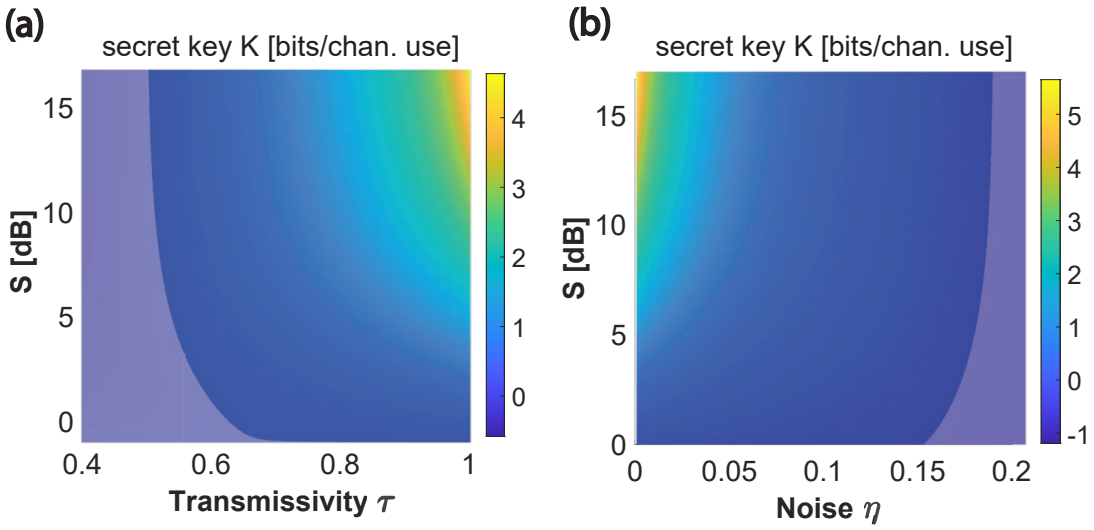


Figure 3.8: (*a*) Secret key in DR case versus squeezing level S and transmissivity τ with $n_{\text{JPA}} = 0.1$ and $\eta = 0$. The secret key is negative in the purple area and positive otherwise. (*b*) Secret key in DR case versus squeezing level S and noise η with $n_{\text{JPA}} = 0.1$ and $\tau \to 1$. The secret key is negative in the purple area and positive otherwise.The secret key is negative in the purple area and positive otherwise.

in the current direct reconciliation, Eve and Bob have a similar weight in the communication. If Eve takes more than 50% of the signal coming from Alice, she effectively replaces Bob and the communication becomes insecure.

In Fig. 3.8, the secret key is also plotted versus the noise η and squeezing level of the JPA. We set τ close to 1 and keep the same noise photon for the JPA. We observe similarly that the secret key increases with the squeezing level and decreases with the noise. We further note that a threshold for the noise appears as well at roughly $\eta_{\text{thresh}} = 0.184$. This implies that no matter the squeezing level, the communication becomes insecure above a certain noise value. Therefore, one can view this threshold as the maximal tolerable noise over the quantum channel such that the communication can still be secure. This also means that no matter Eve's actions, she is not allowed to introduce more noise than η_{thresh}. Otherwise, as we mentioned, the communication is inevitably insecure and is simply aborted by Alice and Bob, preventing Eve from gaining any information. This implies that Alice and Bob can detect this excess noise η. In optics QKD, this corresponds to the step called parameter estimation of the quantum channel [13, 11]. In our microwave implementation, we obtain the noise η from calibration measurements (see Sec. 5.1.1). Additionally, this noise threshold limits the noise coming from Eve's devices or the attack she implements. This physically limits for instance the universal Gaussian cloner attack [62] as this attacks produces noisy clones.

3.3.3 Simulation of secret key in reverse reconciliation case

In this section, we consider the secret key of the protocol in the reverse reconciliation case. We keep the same considerations as for the direct reconciliation case, only that now Bob is the reference. We investigate again the mutual information now between Bob and Alice, $I(B{:}A)$, and Eve's new Holevo quantity $\chi_{\mathrm{E,RR}}$. Fortunately, since the mutual information is symmetric, $I(B{:}A)$ is the same as $I(A{:}B)$. Our analysis can be restrained to the Holevo quantity.

Full Model

The analysis done in this part is notably based on Ref.[51, 71, 13]. The main difference with the direct reconciliation case is that Eve's Holevo quantity $\chi_{\mathrm{E,RR}}$ is now conditioned on Bob's measurement. This means that we need to consider the effect of Bob's measurement and what individual state Eve possesses after it. Fortunately, the average state of Eve stays the same as in the direct reconciliation case. Its covariance matrix is given by Eq. 3.55. This reduces the analysis to Eve's individual states. We denote as k'_{i} a result of Bob's individual measurement. First, we note that Eve's individual state conditioned on Bob's measurement result k'_{i} is still a Gaussian state. Second, adopting a similar method as in to [71], its covariance matrix $\mathbf{V}_{\mathrm{E}}^{k'_{\mathrm{i}}}$ is calculated individually as

$$\mathbf{V}_{\mathrm{E}}^{k'_{\mathrm{i}}} = \mathbf{V}_{\mathrm{avg,E}} - \frac{1}{\sigma_{\mathrm{B}}^2}\mathbf{D}\,\mathbf{\Pi}\,\mathbf{D}^T, \tag{3.63}$$

where

$$\begin{aligned} \sigma_{\mathrm{B}}^2 &= \frac{1}{4}\tau\,(1+2n_{\mathrm{JPA}})\,e^{2r} + \frac{1}{4}\,(1-\tau) + \eta, \\ \mathbf{\Pi} &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ if Bob measured the q quadrature,} \\ \mathbf{\Pi} &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \text{ if Bob measured the p quadrature,} \end{aligned} \tag{3.64}$$

Here, $\mathbf{D} \in \mathbb{R}^{4\times 2}$ is a matrix representing the quantum correlations Eve's average state and Bob's average state. The whole derivation is rather lengthy. Here, we merely gives the main elements useful to compute such matrix D. First, we note that Eve's average state has already been calculated in Sec. 3.3.2. We recall that it corresponds to a Gaussian state whose covariance matrix is given by Eq. 3.55. For later purpose, we simply re-write the covariance matrix from Eq. 3.55 as

$$\mathbf{V}_{\mathrm{avg,E}} = \begin{pmatrix} \mathbf{E}_{\mathrm{avg},1} & \mathbf{C}_{\mathrm{E}} \\ \mathbf{C}_{\mathrm{E}} & \mathbf{E}_{\mathrm{avg},2} \end{pmatrix}. \tag{3.65}$$

where $\mathbf{E}_{\text{avg,1}}$ is the covariance matrix of the average first mode of Eve's average state, $\mathbf{E}_{\text{avg,2}}$ is the covariance matrix of the average first mode of Eve's average state, and $\mathbf{C}_{\text{E}}$ describes the correlation between these two modes. To calculate Bob's average state, we use the same approach as for the calculation of Eve's average state. Therefore, we obtain that Bob's average state reads

$$\hat{\rho}_{\text{avg,B}} = \sum_{\text{c=0,1}} \frac{1}{2} \int_{-\infty}^{\infty} f_{\text{A}}(k_{\text{i}}) \hat{\rho}_{\text{B}}^{k_{\text{i}}} \text{d}k_{\text{i}}, \tag{3.66}$$

where the summation represents the choice for c, $1/2$ corresponds to the probability of getting $c = 0$ or 1, and f_{A} is again given by Eq. 3.54. Furthermore, $\hat{\rho}_{\text{B}}^{k_{\text{i}}}$ corresponds to the Gaussian state given by Eq. 3.50 if the q quadrature is squeezed ($c = 0$) and to the Gaussian state given by Eq. 3.51 if the p quadrature is squeezed ($c = 1$). Using Eq. 3.66 and results from Sec. 2.1.1, one can then show that Bob's average state is a Gaussian state whose covariance matrix is given by

$$\mathbf{V}_{\text{avg,B}} = \begin{pmatrix} \sigma_B^2 & 0 \\ 0 & \sigma_B^2 \end{pmatrix}, \tag{3.67}$$

where $\sigma_B^2 = \frac{1}{4}\tau(1 + 2n_{\text{JPA}})e^{2r} + \frac{1}{4}(1 - \tau) + \eta$. From these results, we can finally calculate that D is given by

$$\mathbf{D} = \frac{1}{4} \begin{pmatrix} D_1 & 0 \\ 0 & D_2 \\ D_3 & 0 \\ 0 & -D_4 \end{pmatrix}, \tag{3.68}$$

where

$$\begin{aligned} D_1 &= \frac{1}{2} \left\langle \hat{q}_{\text{avg,B}} \hat{q}_{\text{E,1}} + \hat{q}_{\text{E,1}} \hat{q}_{\text{avg,B}} \right\rangle - \left\langle \hat{q}_{\text{avg,B}} \right\rangle \left\langle \hat{q}_{\text{E,1}} \right\rangle, \\ D_2 &= \frac{1}{2} \left\langle \hat{p}_{\text{avg,B}} \hat{p}_{\text{E,1}} + \hat{p}_{\text{E,1}} \hat{p}_{\text{avg,B}} \right\rangle - \left\langle \hat{p}_{\text{avg,B}} \right\rangle \left\langle \hat{p}_{\text{E,1}} \right\rangle, \\ D_3 &= \frac{1}{2} \left\langle \hat{q}_{\text{avg,B}} \hat{q}_{\text{E,2}} + \hat{q}_{\text{E,2}} \hat{q}_{\text{avg,B}} \right\rangle - \left\langle \hat{q}_{\text{avg,B}} \right\rangle \left\langle \hat{q}_{\text{E,2}} \right\rangle, \\ D_4 &= \frac{1}{2} \left\langle \hat{p}_{\text{avg,B}} \hat{q}_{\text{E,2}} + \hat{p}_{\text{E,2}} \hat{p}_{\text{avg,B}} \right\rangle - \left\langle \hat{p}_{\text{avg,B}} \right\rangle \left\langle \hat{p}_{\text{E,2}} \right\rangle, \end{aligned} \tag{3.69}$$

.

Let us clarify the notation used. Here, $\hat{q}_{\text{avg,B}}$ represents the q quadrature of Bob's average state and $\hat{p}_{\text{avg,B}}$ represents the p quadrature of Bob's average state. Similarly, we use the same notations for Eve's average state. Only we have to consider her two

average modes individually. For this purpose, we denote with a subscript '1' the average first mode whose covariance matrix is given by $\mathbf{E}_{\text{avg},1}$. The two quadratures of this average mode are then denoted as $\hat{q}_{\text{E},1}$ and $\hat{p}_{\text{E},1}$. Likewise, we denote with a subscript '2', the second average mode whose covariance matrix is given by $\mathbf{E}_{\text{avg},2}$. The two quadratures of this mode are then denoted as $\hat{q}_{\text{E},2}$ and $\hat{p}_{\text{E},2}$. After calculations, one can derive that

$$\begin{aligned} D_1 = D_2 = &- \sqrt{\tau}\sqrt{1-\tau}\left[(1+2n_{\text{JPA}})\,e^{2r} - \left(\frac{4\eta}{1-\tau}+1\right)\right], \\ D_3 = D_4 = &\sqrt{1-\tau}\sqrt{\left(\frac{4\eta}{1-\tau}+1\right)^2 - 1}. \end{aligned} \tag{3.70}$$

To physically interpret those equations, a possible point of view to adopt is that at the output of the beamsplitter implemented by Eve, the two modes held by Eve and the single mode held by Bob form together a three modes system. In such case, a local measurement on one mode will project the system into a new state depending on the result of the measurement. Furthermore, the new state of the system depends on the correlation between the single mode onto which the measurement is performed and the remaining modes. Therefore, Bob's measurement on his single mode will affect the modes held by Eve since they are correlated after the beamsplitter implemented by Eve. In case of Gaussian states, the covariance matrix of the new state after measurement is then described by the set of equations given above.

Mutual information and Holevo quantity

As previously explained, the mutual information is a symmetric function and therefore, the expression in Eq. 3.59 is still valid in this case. For the Holevo quantity, we use, similarly to the direct reconciliation case, the expression given in Eq. 3.62. The only difference is that we need to use the new state for Eve which now depends on Bob's measurement. To this extent, the von Neumann entropy $S\left(\hat{\rho}_{\text{E}}^{k_{\text{i}}}\right)$ in Eq. 3.62 is now replaced by $S\left(\hat{\rho}_{\text{E}}^{k'_{\text{i}}}\right)$. This last expression is calculated using the covariance matrix in equation Eq. 3.63 which corresponds to Eve's new individual state.

Simulation secret key

We numerically calculate the secret key again in the optimal reconciliation case $\beta = 1$. We investigate effects of losses and noise individually. We also keep the same value for the noise photon of the JPA to $n_{\text{JPA}} = 0.1$. In Fig. 3.9, the secret key is plotted against the transmissivity τ of Eve's beamsplitter (corresponding to losses $1-\tau$) and

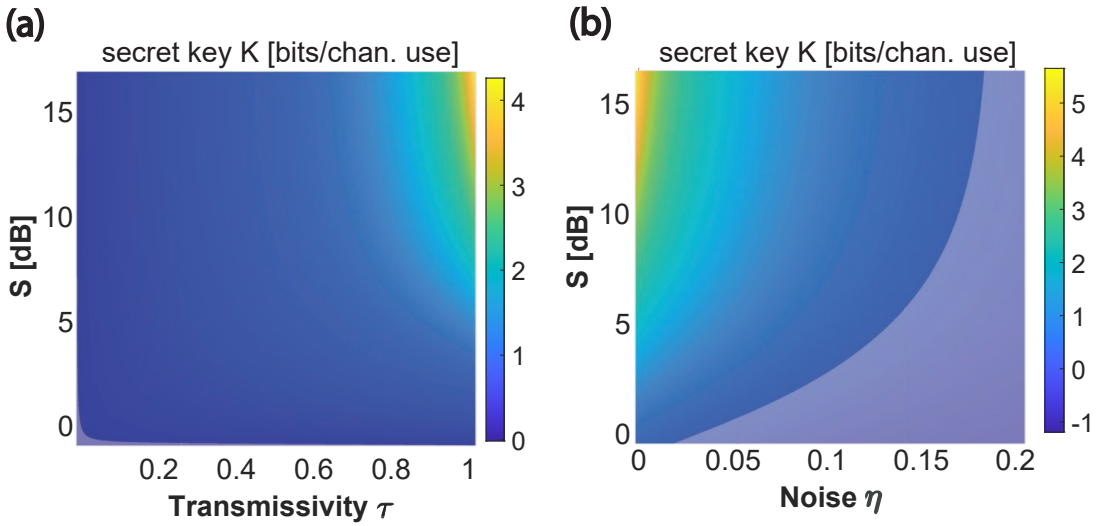


Figure 3.9: (*a*) Secret key in RR case versus squeezing level S and transmissivity τ with $n_{\text{JPA}} = 0.1$ and $\eta = 0$. The secret key is negative in the purple area and positive otherwise. (*b*) Secret key in RR case versus squeezing level S and noise η with $n_{\text{JPA}} = 0.1$ and $\tau \to 1$. The secret key is negative in the purple area and positive otherwise.

for no noise $\eta = 0$. We observe again that the secret key increases as a function of the squeezing level and decreases as a function of losses. However, it is very interesting to note that no threshold appears in this case. In other words, a lossy but noiseless channel will always produce a positive secret key, no matter what the losses are. In particular, this case is not limited by the distance alone, if we consider that the increase in distance only increases the losses. In realistic implementations, nonzero noise is present as well which limits the protocol to a finite distance. However, the communication is much more resilient to losses compared to the direct reconciliation case which limits the communication to 3 dB losses. This precise result of beating the 3 dB losses has been underlined in literature [53, 72, 71] and makes reverse reconciliation schemes particularly appealing.

On the other hand, Fig. 3.9 shows the effect of the noise η on the secret key with no losses $\tau = 1$. Similarly to the direct reconciliation case, the secret key increases with the squeezing level and decreases with the noise. Additionally, a secret key threshold also appears for the noise. It means that above a certain value of noise, the secret key is negative no matter the squeezing level. Numerically, we get a threshold noise value η_{thresh} of approximately $\eta_{\text{thresh}} = 0.181$. Similarly to the DR case (see Sec. 3.3.2), this noise threshold can be physically viewed as the maximal tolerable noise. In other words, no matter what Eve does, she is not allowed to add more than η_{thresh} noise photon. This includes her devices and whatever attack she chooses to implement. However, we can also remark that the secret key is less resilient to the noise compared to the direct

reconciliation case. More precisely, for a given and same squeezing level, the secret key can stay positive for higher noise values in the direct reconciliation case compared to the reverse reconciliation case. This means that a compromise need to be chosen between losses and noise if one wants to physically implement such QKD protocol.

Chapter 4

Experimental techniques

In this chapter, we are interested in experimental techniques used throughout this work to generate and detect weak quantum microwave states. More precisely, we focus on generation of relevant quantum states for the QKD protocol considered in this thesis.We start by describing a cryogenic experimental setup. The we focus on a microwave tomography setup. In the last sections, we present how important experimental parameters are chosen and controlled. In addition, we explain some important calibration measurements. These measurements are required to properly characterize the quantum states in the QKD protocol.

4.1 Cryogenic setup

In this section, we focus on an experimental implementation of the QKD protocol studied in this work. Very low temperatures are necessary to produce the desired quantum microwave states. To this extent, we present relevant experimental devices. In particular, a dilution cryostat is required to achieve low temperatures at which our quantum states are generated. Additionally, we describe our input and output lines. They are used to control and measure the quantum states we use throughout this work.

4.1.1 Cryostat

The quantum states used in this work require low temperatures to be generated. To this extent, we use a homemade cryostat which was designed and constructed at the Walther-Meißner-Institut. It is a ^{3}He/^{4}He wet dilution refrigerator which can reach temperatures around 40 mK. At these temperatures, the thermal population in the frequency range 4 to 6 GHz becomes roughly 10^{-5} to roughly 10^{-3}. This number depends on the used frequency and reached temperature. The cryostat is enclosed in a metallic dewar which is filled with liquid N_2 (77K) and liquid He (4.2K), isolated by vacuum layers. The cryostat contains five temperature stages to perform a gradual

cooling. The first stage is the 4K stage (temperature around 4.2 K) which is achieved by direct cooling with liquid He. The next temperature stage is the 1K stage (temperature around 1.3 K) enabled by evaporation cooling of ^{4}He in the 1K pot. The latter is connected to a Helium reservoir via a capillar. The last three temperature stages are the still (temperature around 700 mK), heat exchanger, and mixing chamber combined with the sample stage. The temperature reached at these two last stages is about 40 mK. To obtain such temperature, we use a ^{3}He/^{4}He mixture, composed of a ^{3}He rich phase (nearly 100 %) and a ^{3}He poor phase (6.4 % ^{3}He) that are in equilibrium and separated by a phase boundary. By removing ^{3}He from the diluted phase, ^{3}He from the concentrated phase crosses the phase boundary, going from the the concentrated phase to the diluted one. As this process is endothermic, heat is removed from the mixing chamber environment. For a detailed description of each temperature stages of the cryostat, we refer the reader to Ref.[73].

4.1.2 Experimental cryogenic implementation

In this section, we focus on the experimental microwave implementation of the QKD protocol introduced in Sec.3.3.1. Here, we implement a simplified version of this protocol. We do not implement straightforwardly the entangling cloner attack for Eve but rather emulate the effects of such attack. Therefore, we consider that Alice sends displaced squeezed states and measure the received states by Bob. However, we do not generate physically a TMSV state for Eve. A simplified experimental schematic is presented in Fig. 4.1.

We want to communicate a randomly generated key from Alice to Bob. The key is made of key elements that are randomly drawn from a fixed Gaussian distribution. This is done with a MATLAB random number generator. For each key element, we need to produce a displaced squeezed state. As indicated in step 1 in Fig. 4.1, we use a flux-driven JPA (see Sec.2.2) for generation of squeezed states as explained in Sec.2.2.3. At the sample stage, input states in the form of weak thermal states are squeezed by our JPA, which produces the output states. These incoming input states are separated from the output by a circulator. The resonant frequency of the JPA is controlled by a magnetic flux going through the dc-SQUID loop of the JPA. This magnetic flux is defined by a dc current, generated by an external current source, going through a magnetic coil mounted on top of the JPA. The squeezing level S and squeezing angle γ of the produced squeezed states are controlled by an external pump tone. Furthermore, we recall that our JPA also adds noise n_{JPA} to the outgoing squeezed states. Then, the squeezed states are sent through the first directional coupler implementing displacement as shown in Fig. 4.1. The directional coupler acts as a highly asymmetric beamsplitter.

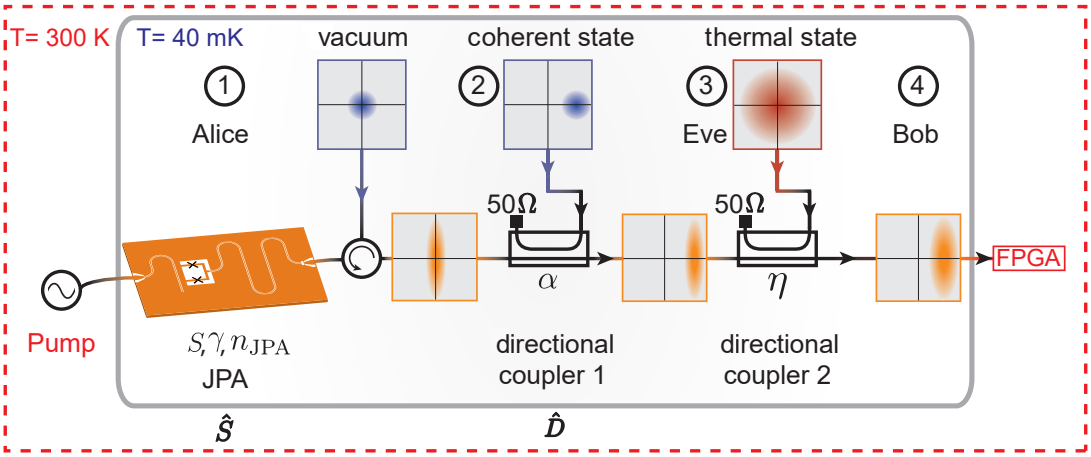


Figure 4.1: Schematic of the experimental cryogenic setup. The protocol is split into four steps indicated in the figure. In step 1, a JPA applies the squeeze operation $\hat{S}$ to an input vacuum resulting in a squeezed vacuum state, parametrized by the squeezing level S, the squeezing angle γ, and added noise n_{JPA}. These parameters are controlled by an external pump. In step 2, the displacement operator $\hat{D}(\alpha)$ is applied via the directional coupler 1 to the squeezed state resulting in a displaced squeezed state. The applied displacement is parametrized by a complex displacement amplitude α defined by the coherent tone. In step 3,external quasi-thermal noise η is coupled to the displaced squeezed state. This simulates the effects of Eve's attack. In step 4, Bob receives a noisy displaced squeezed state which is measured using a FPGA setup. Wigner functions of the generated states at each step are in colored insets. The reproduction of the JPA sketch from Ref.[43] is authorized by the author.

It applies the displacement operator by using a strong coherent signal incident at the coupled port [20]. The amplitude and phase of this coherent signal controls the complex displacement amplitude.

Like mentioned above, we only want to emulate Eve's attack effects which means that we want to add losses and noise to the states. While it is technically more difficult to vary losses, noise can be easily controlled in our experimental environment. Indeed, we can use Eq. 2.25 and replace the coupled strong coherent state by a thermal state with a mean photon number n_{th}. Then in the limit of $\tau \to 1$, we get that

$$\hat{a}_{\mathrm{out}} = \sqrt{\tau}\hat{a}_{\mathrm{in}} + \sqrt{1-\tau}\hat{V}_{\mathrm{th}}, \tag{4.1}$$

where $\hat{a}_{\mathrm{in}}$ corresponds to input states, $\hat{a}_{\mathrm{out}}$ describes output states, and $\hat{V}_{\mathrm{th}}$ describes thermal states. Depending on n_{th}, this effectively couples noise

$$\eta = \frac{1}{4}(1-\tau)(1+2n_{\mathrm{th}}) \tag{4.2}$$

to input states. This noise refers to the output of the directional coupler. Therefore, we

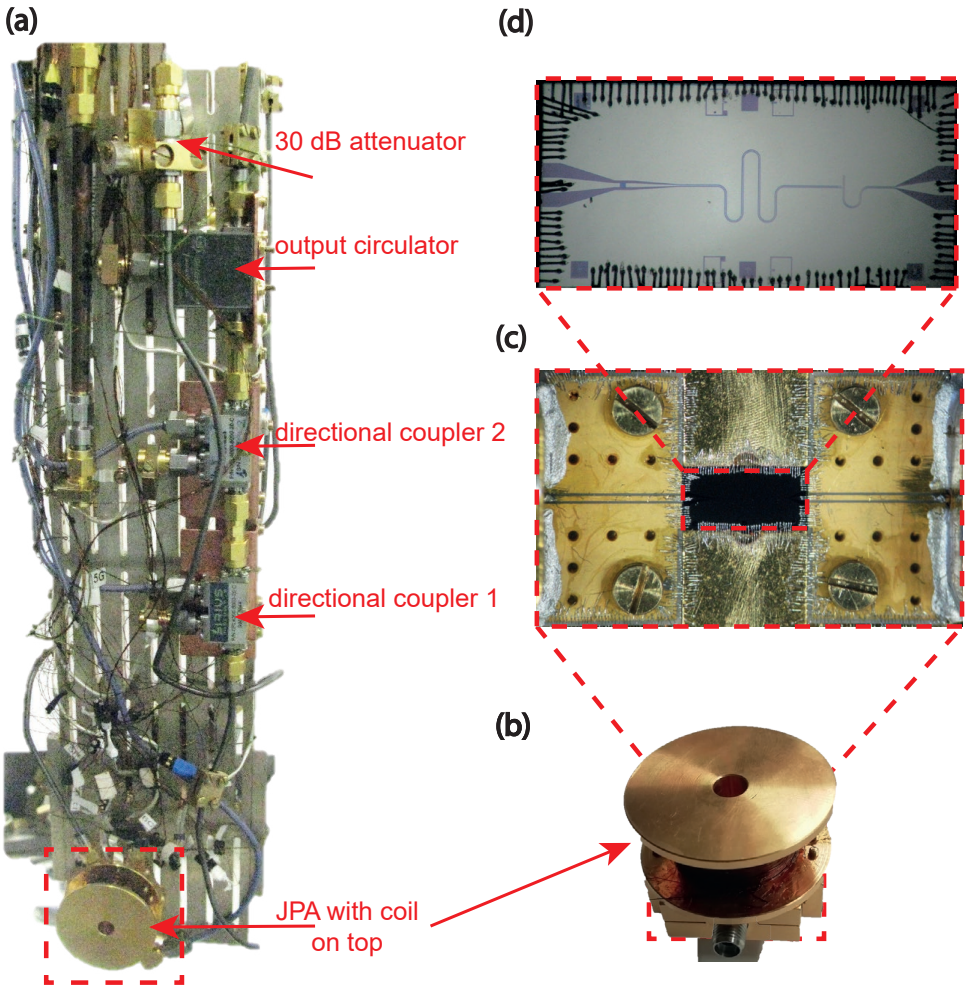


Figure 4.2: (a) Photograph of the experimental cryogenic setup presented in Sec. 4.1.2. (b) Photograph of the sample box of our JPA on which lies the magnetic coil. (c) Close-up of the JPA sample holder. Our JPA sits in the middle. (d) Photograph of our JPA chip.

use the second directional coupler directly connected to the first one to controllably inject noise into the communication channel. The thermal states $\hat{V}_{\text{th}}$ are produced by an arbitrary function generator (AFG) in the form of a quasi-Gaussian white noise. The signal corresponding to the output of this second directional coupler is then detected and measured. This step represents Bob in our protocol.

4.1.3 Sample stage

The overall experimental setup is presented in Fig. 4.3. In this section, we focus on the sample stage (T = 40 mK) shown at the bottom of the figure. For generation of squeezed states, we use a JPA chip fabricated at NEC Smart Energy Research Laboratories Japan and RIKEN, Japan. The chip sits in a sample box on top of which

lies a magnetic coil used to tune the flux going through the dc-SQUID loop of the JPA. In Fig. 4.2 (b), we show a photograph of our sample box with the JPA on top. Fig. 4.2 (c) and Fig. 4.2 (d) show a close-up of the JPA chip and the JPA sample box. The JPA is connected to the first directional coupler from Sirius Microwave (SN E16944) which is itself directly connected to the second directional coupler from Miteq (SN 15876). A photograph of the cryogenic setup is shown in Fig. 4.2 (a). Each directional coupler has an output of the coupling line port terminated by a 50 Ω load. An input line (input 2 in Fig. 4.3) is used for calibration purposes of the JPA as discussed in Sec.4.2.4. It contains a 30 dB INMET input attenuator connected to the signal port (labelled as S) of the JPA. We use a circulator (LNF-CIC4-8A from Low Noise Factory) to separate weak thermal states going inside the JPA from the outgoing squeezed states. Additionally, all the connections to this circulator are implemented by superconducting cables (SC-219/50-NbTi-NbTi) manufactured by Coax Co., Ltd with an outer conductor diameter of 2.19 mm. These cables have an inner conductor and outer conductor made of niobium titanium while the dielectric layer is made of polytetrafluoroethylene (PTFE). Such cables have low microwave losses at cryogenic temperatures due to the superconducting properties of NbTi alloy with the critical temperature T = 9.8 K. In order to ensure thermal connection of the cryogenic microwave components, we connect the directional couplers to the cryostat with a solid copper frame. The 50 Ω loads, the 30 dB attenuator, the superconducting cables, and the JPA sample box are additionally thermalized by using silver wires between these components and the mixing chamber. These wires are bent into suitable shapes and annealed at 900°C to reduce the defects in their crystal structure and improve their heat conductivity.

4.1.4 Input and output lines

Input lines

As shown in Fig. 4.3, we have four input lines in the setup. Up to the 4K stage, we use astrocobra-flex 31086S cables (from HUBER+SUHNER) for their flexibility and low losses. More precisely, the used cables present losses of 1.59 dB/m and 2.47 dB/m at 5 GHz and 10 GHz at room temperature, respectively. In our setup, this amounts to losses of 2.3 dB for input 1 and 1.4 dB for the other inputs for 90 cm long cables. Then, for the different temperature stages, we use thin coaxial cables manufactured by Coax Co., Ltd with outer conductor diameter of 1.19 mm. These cables have PTFE as a dielectric layer. The inner and outer conductors are made of, respectively, either silver-plated copper and oxygen-free copper (SC-119/50-SC) or niobium and cupronickel (SC-119/50-Nb-CN). The latter are partially superconducting due to the niobium used

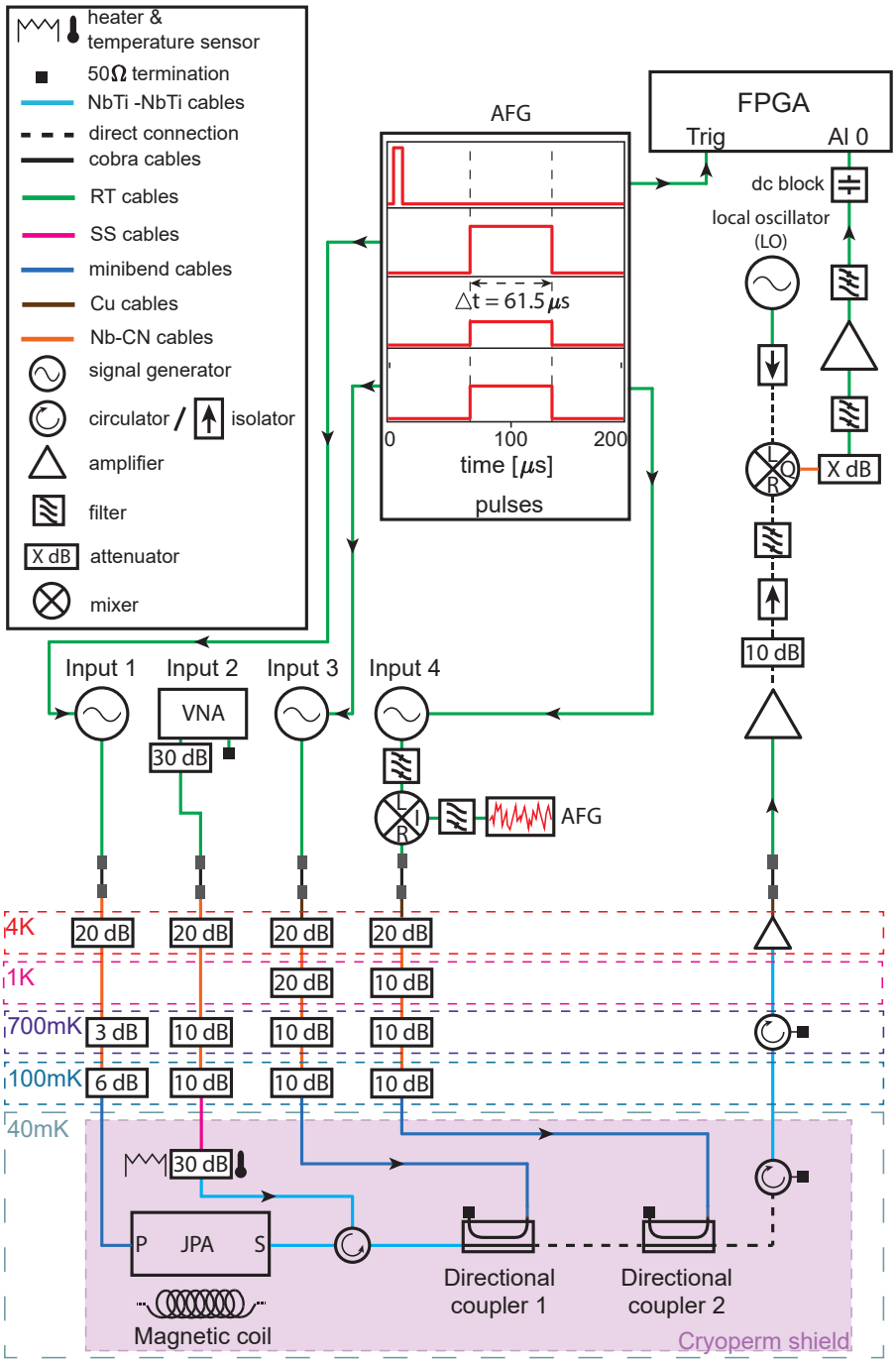


Figure 4.3: Full experimental setup for the microwave QKD protocol. All devices are referenced to a rubidium frequency standard (not shown). A magnetic coil sets on top of the JPA. It is connected to a dc line (not shown). The pulsing scheme is generated by the AFG (shown in the center). A vector network analyzer (VNA) is used for calibration purposes. During the quantum state reconstruction of microwave signals, the latter are first downconverted using a local oscillator to the IF frequency $f_{\mathrm{IF}} = 11$ MHz and then digitized by the FPGA card.

as the inner conductor. The copper/copper cables are used over short lengths so that the losses are small (less than 1 dB). Furthermore, from the 100 mK stage to the mixing chamber stage, we use minibend flexible cables (from HUBER+SUHNER). They have low losses of about 1 dB at 5 GHz. The only exception is the input to the heatable attenuator which is made with a fully stainless steel coaxial cable with PTFE as a dielectric layer from Coax Co., Ltd. At the sample stage, we use the Nb-Ti cables mentioned in Sec.4.1.3. We need to attenuate thermal radiation coming from the room temperature stages that destroy quantum effects. For this purpose, we use attenuators at the different temperature stages. If done correctly, this allows to suppress thermal photon population to approximately 10^{-3} at frequencies around 5 GHz, as limited by the temperature 40 mK of the mixing chamber. The choice of attenuation at each stage depends notably on the cooling power available and the temperature of each stage [74]. We note that the pump line of the JPA has less attenuation compared to the other lines. Here, we have sacrifice noise properties of our signals in order to reach high dynamic range of pump signals required to reach high squeezing levels in our JPAs. Lastly, the attenuators help to thermalize the inner conductors of the input cables.

Output lines

As shown in Fig. 4.3, the setup has only one output line. Since signals generated at the output of the microwave QKD protocol consist of very few photons, we use several amplifiers to amplify them. Up to the first amplifier stage, we want to minimize the losses. For this reason, we use the superconducting Nb-Ti coaxial cables. Theses cables are thermalized as well using silver wires which are annealed at 900°C. After our second directional coupler, we use two circulators in series (LNF-CIC4-8A from Low Noise Factory and CTH1368-K18-A from PAMTECH).

To this extent, one port of these circulators is terminated by a 50 Ω load which is itself thermalized to the corresponding temperature stages. In this way, signals can propagate from the low temperature stages to the upper ones while signals propagating in the opposite direction are suppressed by 42 dB (isolation due to the both circulators). After them, the first amplifier stage consists of a high-electron-mobility transistor (HEMT) amplifier (LNF-LNC4 8A from Low Noise Factory). It works in a bandwidth of 4 GHz (4-8 GHz). It has a specified amplification gain of 37 dB at our working frequencies and noise temperature 2.5 K when operating at a temperature of 8 K. At the 4K stage, the connections are assured by copper coaxial cables and astrocobra-flex 31086S cables similarly as for the input lines.

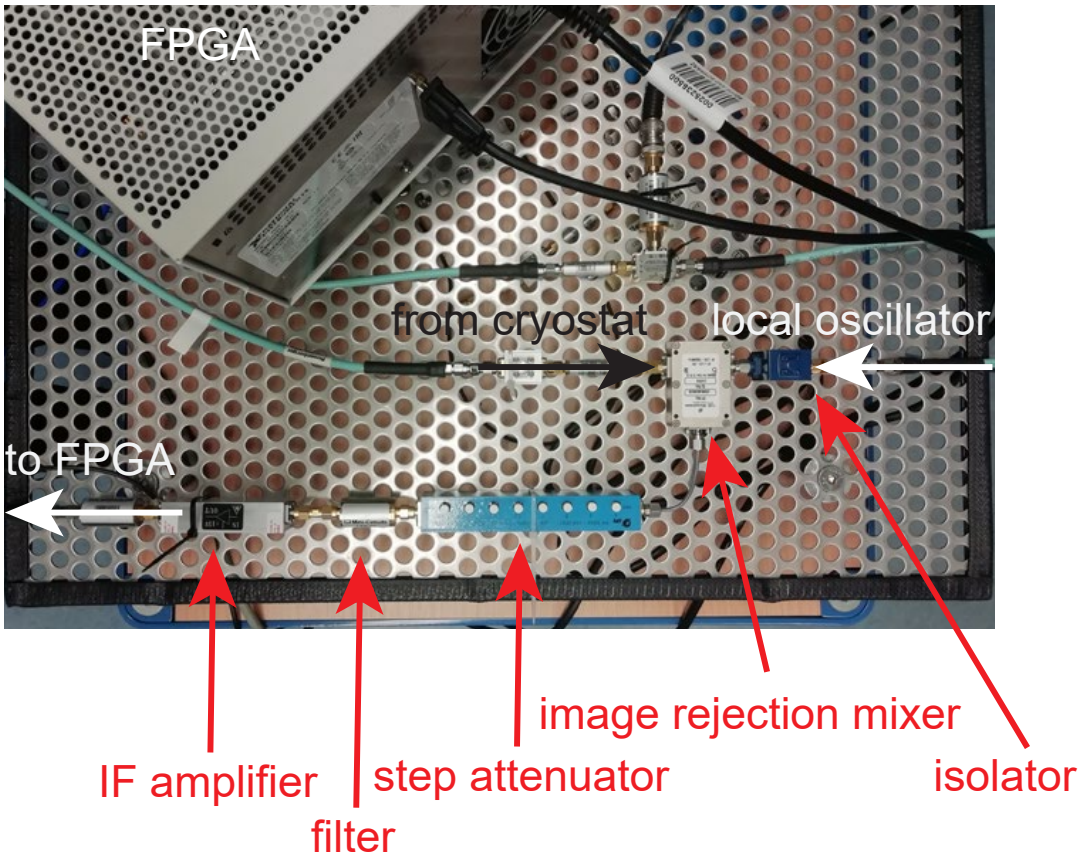


Figure 4.4: Photograph of part of the room temperature setup used to acquire signals coming from the cryostat. The photography corresponds to the right hand side of Fig. 4.3.

4.2 Data acquisition

In this section, we present the procedure used to perform tomography of microwave quantum states. First, we present our room temperature setup with the devices used to generate our quantum states as well as as devices used to detect them. To this end, we use a field programmable gate array (FPGA) setup to acquire and process measured data. Then, we present the reference state reconstruction method which is used in this work to reconstruct quantum states from measurements. Lastly, we introduce the notion of photon number conversion factor (PNCF) measurements. This measurement is essential as it allows us to convert measured voltages into photon numbers which is a key element for quantum states reconstruction.

4.2.1 Room temperature setup

As shown in Fig. 4.3, each of the four inputs lines of the setup are connected to a specific device. The pump line (input 1) is connected to a signal generator (SMF

100A from Rohde&Schwarz) that generates the pump signals for the JPA. Coherent signals for displacement are generated by a vector microwave signal generator SGS from Rohde&Schwarz (input 3). For the second directional coupler, we use an AFG generating a quasi-Gaussian noise as mentioned previously in Sec.4.1.2. We use an AFG fron Agilent Technologies (81160A). Such AFG can only generate noise in the maximum bandwidth of 500 MHz. For this reason, we up-convert the noise signal using a a harmonic mixer to the frequency of the squeezed signal $f \simeq 5\,\mathrm{GHz}$. The exact frequency targeted during the up-conversion depends on the chosen frequency for the squeezed states. Additionally, signals are filtered via a band pass filter. Finally, the input line of the JPA is also connected to a vector network analyzer (VNA) for calibration purposes.

The previously discussed devices allow us to generate the desired states (i.e.,displaced noisy squeezed states) inside the cryostat. In order to detect the outgoing signals, we use the setup presented in Fig. 4.3. A photograph is shown in Fig. 4.4. It consists of several steps. First, we amplify microwave signals coming from the cryostat by using the second amplifier (AFS5 from Miteq). This amplifier has a gain of 41.5 dB at our working frequencies. It is followed by an isolator (ECI04-5 from EPX microwave) and a bandpass filter (VBFZ-5500 from Mini-Circuits). This filter has a bandwidth of 1.4 GHz centred at 5.5 Ghz. It filters out the incoming signals around the relevant frequency f_{RF} which lies between 4-6 GHz. The next step consists in downconverting the signals to an intermediate frequency f_{IF} in the megahertz regime. This is done to match the sampling rate of the FPGA (see Sec.4.2.2) which we use to detect our signals. To perform the downconvertion, a strong signal at the frequency $f_{\mathrm{RF}} + f_{\mathrm{IF}}$ from a local oscillator (LO) is mixed to the incoming signals via an image rejection mixer (IRM4080B from Polyphase microwave). This mixer is necessary as otherwise an undesired signal at frequency $f_{\mathrm{RF}} + 2f_{\mathrm{IF}}$ which would also be down-converted at the frequency f_{IF}. After the downconversion, the signal can be attenuated by a step attenuator (ESA2-1-10/8-SFSF from EPX microwave) which is used to avoid compression effects. After going through a bandpass filter centred around f_{IF}, the signal is again amplified with an amplifier of gain 58.7 dB (AU 1447 from Miteq). The step attenuator is then used to regulate the amplitude of the signals measured at the FPGA after amplification. Finally, signals go through a lowpass filter and a DC block before being acquired by the FPGA. All the devices are referenced to a 10 MHz reference signal coming from a rubidium frequency standard. To avoid undesired interference with this 10 MHz reference, the IF frequency is fixed at $f_{\mathrm{IF}} = 11$ MHz.

4.2.2 FPGA data acquisition and processing

To digitize input signals, we use the NI 5782 transceiver adapter module operating at the sampling frequency $f_S = 250$ MHz which has a 14-bit analog input resolution. We use three channels on the front panel, one single-ended analog input channel (AI 0), a trigger input channel (TRIG), and a single-ended external reference input channel (CLK IN). This last channel is connected to an external reference clock, which is in our case another device of the room temperature setup. This way, the FPGA is synchronized with the other devices. The trigger input channel is used to trigger the measurement and is controlled via an applied pulse repeated at a fixed frequency f_{TRIG}.

IQ-Demodulation

As presented in Sec.2.1.1, our microwave propagating signals can be described by their I and Q quadratures. In order to measure them, input signals after digitization are mixed with a digital local oscillator operating at frequency f_d. In doing so, a down-converted input microwave signals A at frequency f_{IF} is demodulated into two components of frequency $f_d \pm f_{IF}$. These components are then used to perform a numerical integration over one period $T_{IF} = 1/f_{IF}$ which, after normalization, gives the quadratures values. By setting $f_d = f_{IF}$, the quadratures are obtained as

$$\begin{aligned} I &= 2f_{IF} \sum_{i=1}^{N} \cos\left(2\pi f_{IF} t_i\right) A\left(t_i\right) \Delta t, \\ Q &= 2f_{IF} \sum_{i=1}^{N} \sin\left(2\pi f_{IF} t_i\right) A\left(t_i\right) \Delta t, \end{aligned} \tag{4.3}$$

where $A(t_i)$ is the signal at the time t_i, $\Delta t = 1/f_S$ is the discret time step, f_S is the sampling frequency, and N is the number of points in the integration. The latter is defined as

$$N = \left\lfloor \frac{f_S}{f_{IF}} \right\rfloor. \tag{4.4}$$

In our case, $f_{IF} = 11$ MHz and $f_S = 250$ MHz, so we get $N = 22$. For each trigger signal, 1650 quadrature values are acquired which corresponds to a time trace with the duration 145.2 μs. Each trace is repeated a fixed number of times N_{avg}, which is also fixed for each measurement. Additionally, in order to guarantee no phase shift between the digital local oscillator and the digitized input signals over time, the intermediate frequency f_{IF} needs to be a multiple of the trigger frequency f_{TRIG}. In our experiments, f_{TRIG} is set to 5 kHz. Afterwards, we implement a digital finite impulse response (FIR)

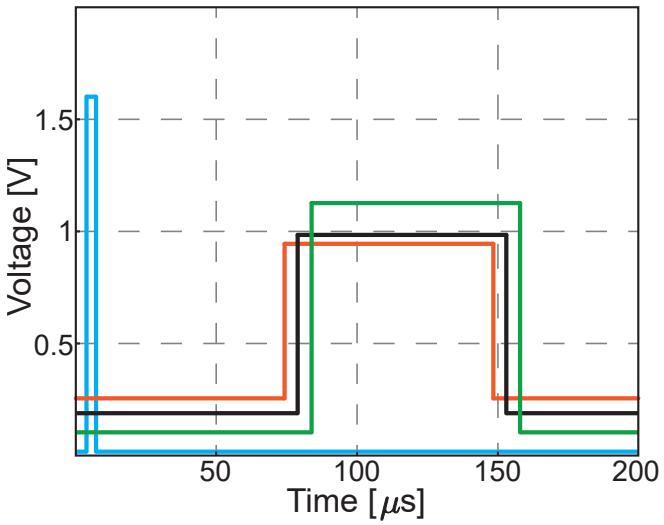


Figure 4.5: Experimental pulsing scheme. The FPGA trigger is shown in blue. It has an amplitude of 1.6 V. The pulse shown in orange is used to control the pump of the JPA. It has an amplitude of 800 mV. The pulse shown in black is used to control the SGS microwave source. It has an amplitude of 875 mV. Finally, the pulse shown in green is used to control the AFG 81160A. It has an amplitude of 1.13 V. For clarity, pulses are purposely depicted with a small offset of $\Delta V = 0.1\ V$ and $\Delta t = 10\ \mu$s. The trigger pulse has a width of $\Delta T_1 = 8$ ns. All the other pulses have the same width of $\Delta T_2 = 61.5\ \mu$s.

filter acting as a low pass filter with a single-sideband cutoff frequency f_c of 200 kHz. Finally, the quadrature moments $\langle I^n\, Q^m \rangle$ with $n + m \leq 4$ and $n, m \in \mathbb{N}_0$ are then calculated and averaged over the N_{avg} times repeated measurements.

Timing

For the experiments and measurements, several pulses are needed in order to control when the different devices are operating. First, the trigger input channel of the FPGA is used to trigger the acquisition of input signals. A trigger pulse is generated by another AFG from Tektronix. The trigger pulse needs to have an amplitude of at least 1.6 V with a time width T_{TRIG} of a least $1/f_s$, which corresponds for the setup used to $T_{\text{TRIG}} \geq 8$ ns. Furthermore, for cryogenic experiments, pulse schemes are used to trigger devices at specific timing. To this extent, we generate trigger pulses with the same AFG in the form of square signals whose width and amplitude depend on the experiments and devices used. In Fig. 4.5, we present experimentally used pulse schemes. A representation of these pulses is also shown in Fig. 4.3.

4.2.3 Reference state reconstruction

Several methods are available to reconstruct quantum microwave states. In optics, homodyne and heterodyne direct detection methods are routinely used to detect and measure quantum signals [75, 51]. Such methods are efficient in optics because mean thermal photon numbers corresponding to room temperatures at optical frequencies is extremely small [76]. This means that ambient thermal noise does not influence optical quantum signals. In the microwave regime the situation is different. Due to the lack single-photon detectors for the microwave range, a common detection method is to use linear amplifiers to amplify the signals and, then, detect them at room temperatures. In particular, phase-sensitive linear amplifiers can be used to amplify only one quadrature of quantum states. The advantage is that such amplification can be theoretically noiseless as discussed in Sec.2.2.3 at the cost of loosing information about another (deamplified) quadrature. On the other hand, phase-insensitive linear amplifiers can be used to amplify both quadratures of quantum states but, due to the Heisenberg inequality, such amplification adds at least half a noise photon. Best among currently available linear amplifiers add around 10 to 15 noise photons making our quantum signals covered in noise. In this work, we use a method called the reference state reconstruction to reconstruct our quantum states from these noisy signals measured at room temperatures [77, 78].

In the reference state reconstruction method, a known signal is used as reference state. In our experiments, such reference state corresponds to a weak thermal state located in the cryostat at the mixing chamber stage. Considering the low temperatures of about $T = 40$ mk reached experimentally and the working frequency regime (around 5 GHz), these weak thermal states have a low photon number of about 0.01 photons which is experimentally taken into account for more precise measurements. The purpose of the method is to ultimately reconstruct the signal moments $\left\langle (\hat{a}^\dagger)^m \hat{a}^n \right\rangle$, with $m + n \leq 4$ of our propagating quantum states. From Sec.2.1.1, signal moments up to the second order are enough to reconstruct Gaussian states. The higher orders are used to control that the measured states are Gaussian. To calculate these signal moments, we use the complex envelope function $\hat{\xi}$ defined as

$$\hat{\xi} = \frac{\hat{I} + i\hat{Q}}{\sqrt{\kappa}}, \tag{4.5}$$

where we introduced κ, the so-called photon number conversion factor relating the voltage measurements of the quadratures to photon numbers (see Sec.4.2.4). Additionally, $\hat{I}$ and $\hat{Q}$ correspond to measured quadratures as explain in Sec. 4.2.2. From Eq. 4.5, the complex envelope function moments $\left\langle (\hat{\xi}^\dagger)^m \hat{\xi}^n \right\rangle$ can be computed from the quadrature

moments $\left\langle \hat{I}^{\mathrm{m}} \hat{Q}^{\mathrm{n}} \right\rangle$. The latter are calculated from the measured quadratures $\hat{I}$ and $\hat{Q}$. For our quantum states, the complex envelope function is written in the following form

$$\hat{\xi}_{\mathrm{s}} = \sqrt{G} \left(\hat{a} + \hat{\mathrm{V}} \right), \tag{4.6}$$

where $\hat{a}$ is the annihilation operator describing the quantum signal in the detection path, G is the amplification gain of the detection path, and $\hat{\mathrm{V}}$ is the operator describing the noise in the detection path. For the reference state, the complex envelope function reads

$$\hat{\xi}_{\mathrm{ref}} = \sqrt{G} \left(\hat{v} + \hat{\mathrm{V}} \right), \tag{4.7}$$

where now $\hat{v}$ describes the weak thermal state used as a reference. The first step is to use Eq. 4.7 to calculate the noise moments $\left\langle (\hat{V}^{\dagger})^{\mathrm{m}} \hat{V}^{\mathrm{n}} \right\rangle$ from the reference state moments $\left\langle (\hat{v}^{\dagger})^{\mathrm{m}} \hat{v}^{\mathrm{n}} \right\rangle$ and the complex envelope moments $\left\langle (\hat{\xi}_{\mathrm{ref}}^{\dagger})^{\mathrm{m}} \hat{\xi}_{\mathrm{ref}}^{\mathrm{n}} \right\rangle$. Then, using Eq. 4.6, we can similarly compute the signal moments $\left\langle (\hat{a}^{\dagger})^{\mathrm{m}} \hat{a}^{\mathrm{n}} \right\rangle$ from the complex envelope function $\left\langle (\hat{\xi}_{\mathrm{s}}^{\dagger})^{\mathrm{m}} \hat{\xi}_{\mathrm{s}}^{\mathrm{n}} \right\rangle$ and from the noise moments $\left\langle (\hat{V}^{\dagger})^{\mathrm{m}} \hat{V}^{\mathrm{n}} \right\rangle$, with $m + n \leq 4$. Additionally, we invite the reader to Ref.[44] for more details on the method.

4.2.4 PNCF calibration and temperature control

Photon number conversion factor

As explained in Sec.4.2.3, we need to calibrate the amplification chain to be able to convert the voltages measured during the experiment into photon numbers. This is done by using a photon source which emits a known photon number. To this extent, we use a 30 dB attenuator which behaves as a black body emitting thermal radiations with a power determined by the temperature of the attenuator [79]. The attenuator is placed in the input line of the JPA. We heat up the attenuator with a heater fixed to it while a thermometer monitors the temperature. We probe a temperature range of 40 mK to 600 mK. Additionally, a stainless steel cable is used as an input cable for the attenuator and a superconducting cable Nb-CN is used as an output cable in order to thermally decouple the attenuator from the cryostat. Since the thermal conductivity of the cables is low, we further weakly couple the attenuator to the mixing chamber stage via a thin silver ribbon. This is done so that the attenuator can be cooled down to low temperature (around 40 mK) while still being able to be heated up to higher temperatures (around 600 mK). Moreover, the superconducting cable is necessary to transmit the thermal radiations from the attenuator to the next components with as little losses as possible.

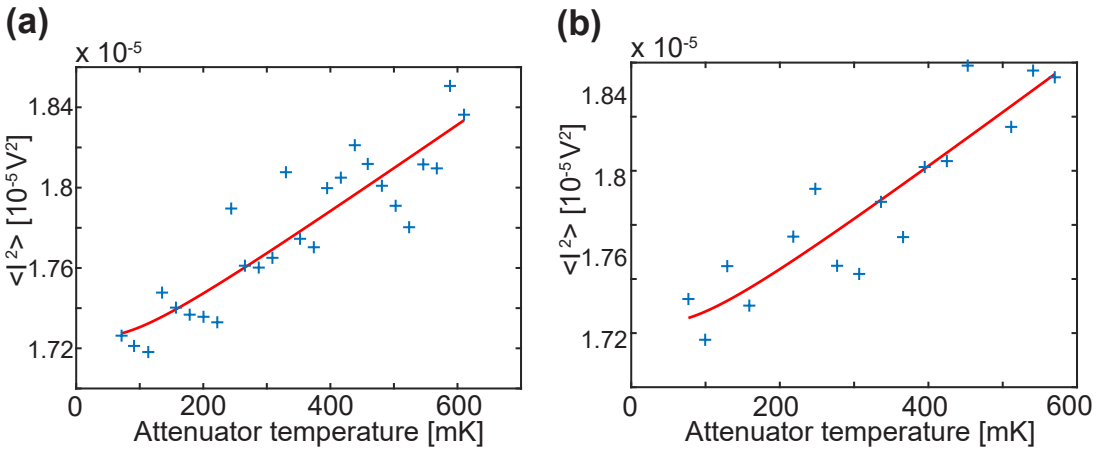


Figure 4.6: Measured $\langle I^2 \rangle$ versus the attenuator temperature. The markers represent measured data while the red line correpond to a data fit from Eq. 4.8. Qualitatively similar results are obtained for $\langle Q^2 \rangle$. (a) Fit obtained for the working point $f_0 = 5.35$ GHz. (b) Fit obtained for the working point $f_0 = 5.353$ GHz.

The detected power P of the amplification chain at the FPGA is given by [44, 79]

$$P = \frac{\langle I^2 \rangle + \langle Q^2 \rangle}{R} = \frac{\kappa G}{R} \left[\frac{1}{2} \coth \left(\frac{h f_0}{2 k_B T_{att}} \right) + n \right], \tag{4.8}$$

where $\langle I^2 \rangle$ and $\langle Q^2 \rangle$ are the quadrature second order moments. Additionally, $R = 50\ \Omega$, h is the Planck constant, k_B is the Boltzmann constant, and f_0 is the center of the detection bandwidth. Lastly, G and n denote the amplification and noise of the amplification chain, respectively. The photon number conversion factor (PNCF) is defined as $\kappa = R \cdot BW \cdot h f_0$ with BW being the detection bandwidth. It is used to convert the measured voltages into photon numbers. Based on Eq. 4.8, we can vary the temperature of the 30 dB attenuator and measure the corresponding the power in order to extract the product κG and the noise n by fitting the data. We note that from Eq. 4.5 and Eq. 4.6, this product κG can be directly used in the reference state reconstruction method and it is not required to compute κ and G separately. Moreover, we experimentally treat both quadrature moments $\langle \hat{I}^2 \rangle$ and $\langle \hat{Q}^2 \rangle$ separately. In Fig. 4.6, we display the fits of PNCF measurement made for the two working points ($f_0 = 5.35$ GHz and $f_0 = 5.353$ GHz). The results of the fits are shown in Tab. 4.1. As we can see from these results and Fig. 4.6, the parameters fitted present a quite large relative error. From measurements, we observe that a change in working frequency could lead to an improvement of the parameter fits. This behaviour is attributed to frequency-dependent interferences in the output microwave line that may lead to a degradation of the final signal-to-noise ratio. This explains the choice made for the second working point as the measured data points and the fit curved are more aligned than for the first working point.

Moments	κG $\left[\mathrm{V}^2/\mathrm{photon}\right]$	n $\left[\mathrm{photon}\right]$
$\left\langle I^2 \right\rangle$ (f_0 = 5.350 GHz)	$1.40 \cdot 10^{-6} \pm 2.83 \cdot 10^{-7}$	24.22 ± 5.16
$\left\langle Q^2 \right\rangle$ (f_0 = 5.350 GHz)	$1.40 \cdot 10^{-6} \pm 2.83 \cdot 10^{-7}$	24.26 ± 5.18
$\left\langle I^2 \right\rangle$ (f_0 = 5.353 GHz)	$1.30 \cdot 10^{-6} \pm 3.27 \cdot 10^{-7}$	27.86 ± 7.30
$\left\langle Q^2 \right\rangle$ (f_0 = 5.353 GHz)	$1.31 \cdot 10^{-6} \pm 3.27 \cdot 10^{-7}$	27.63 ± 7.19

Table 4.1: PNCF parameters values obtained from the fits for the two working points.

However, the errors on the fit parameters remain significant. After experimental tests, we attribute those errors to a faulty cryogenic thermalization of the 30 dB attenuator emulating the black body in our experiment. More precisely, if the attenuator is not properly mechanically connected to its support or to its silver ribbon, fluctuations in its temperature will occur. This problem could be easily solvable in future by a more careful re-building of the thermalization wires.

Change of reconstruction point

During PNCF calibration measurements, it is important to take into account effects of losses. If no losses were present, quantum states would be reconstructed as always appearing at the output of the 30 dB attenuator. However, cables and components physically add losses to input signals. Since we want to reconstruct quantum states at different position in the setup, we carefully estimate the losses introduced by all components from the 30 dB attenuator to the reconstruction point of interest. We denote by L the total losses between the 30 dB attenuator (ATT) to the new reconstruction point (R). Then, the amplification chain gain G_{ATT}, referenced at the attenuator, is related to the gain G_{R} at the reconstruction point by

$$G_{\mathrm{ATT}} = G_{\mathrm{R}} \cdot 10^{-\mathrm{L}/10}, \tag{4.9}$$

where $L > 0$ represents losses from ATT to R. Additionally, during shifts in reconstruction points, the gradient of temperature between the two points considered is taken into account during the data fitting.

4.3 Working point determination

In this section, we investigate measurements useful to determine working points of the setup. For the rest of this thesis, we define a working point of the setup as a selected

resonant frequency f_0 for our JPA. To this extent, we first look at the magnetic flux dependency of the JPA. This allows us to verify that the JPA used works properly in addition to determining a working frequency range. As the second step, once a working frequency has been chosen, we also investigate the nondegenerate gain of the JPA. This measurement helps to verify that the JPA behaves as expected. It also provides insights on achievable squeezing levels at the particular working frequency. It indicates the required pump power that we need to apply to the JPA.

4.3.1 Flux dependent JPA resonance frequency measurement

As discussed in the Sec.2.2, it is possible to tune the resonance frequency of a flux-driven JPA by generating a dc magnetic flux Φ_{dc} through the dc-SQUID loop. This is performed experimentally by applying an external magnetic field with a magnetic coil. This magnetic coil is mounted on top of the JPA as specified in Sec. 4.1.2. We use an external dc current source to send a specified electric current through the coil, and thus, control the dc magnetic acting on the JPA. Then, at a given JPA resonance frequency f_0, we obtain a parametric amplification effect by generating, via a microwave pump tone, an oscillating magnetic field at the frequency the $2f_0$, which induces an oscillating magnetic flux Φ_{rf}. Experimentally the parametric amplification is controlled by the frequency, power, and phase of the microwave pump tone. The JPA characteristics also influence the amplification performance. In order to operate the JPA as a squeezer at a desired work point,first, we need to perform calibration measurements to determine a working frequency and a characteristic range of pump powers.

The magnetic flux dependency of the JPA resonance frequency f_0 is described by Eq. 2.41. To determine it experimentally, we use the setup presented in Fig. 4.7. We probe the JPA with coherent input microwave signals and measure the output signals via a VNA. The input signals are sent from channel 2 of the VNA and the output signals are received at the channel 1. In this way, we measure the JPA reflection response as the S_{12} scattering parameter of the VNA. For these measurements, we sweep both the frequency of input signals as well as the coil current value I_{coil}. Changing the latter induces changes in the JPA resonance frequency. The frequency span Δf of the frequency sweep is set to $\Delta f = 1$ GHz and the coil current span ΔI is set to $\Delta I = 200\ \mu$A. Depending on the frequency and coil current probed, output signals have a different amplitude and phase from the input signals. These last two quantities are obtained from the measured signals with the VNA. From these results, a reference is chosen where no amplitude or phase changes are observed. In our case, we choose as a reference the measurements performed for $I_{\mathrm{coil}} = 84.5\ \mu$A. Measured values for this reference are then averaged and subtracted from the rest of measured data. Additionally,

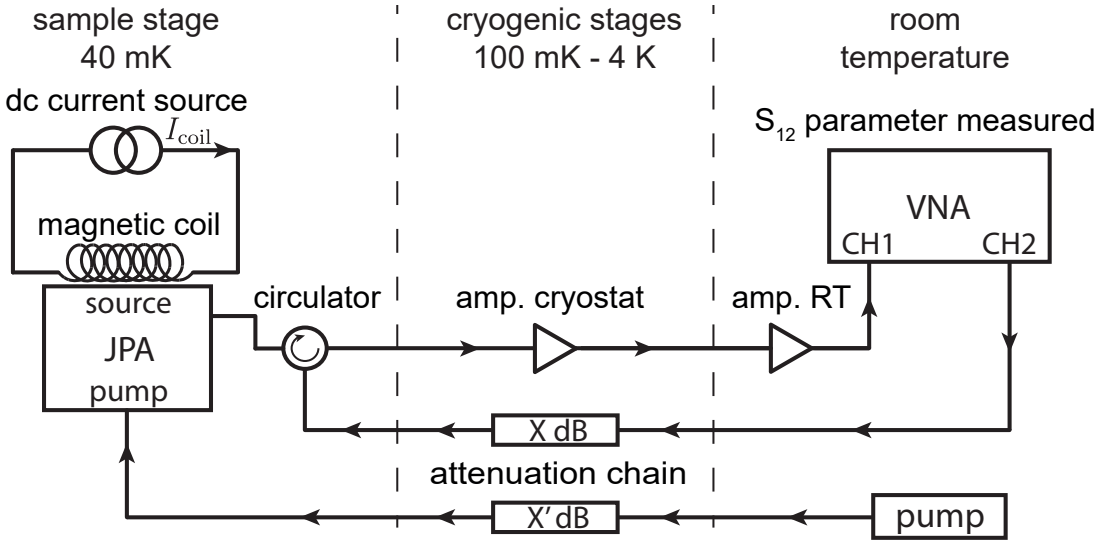


Figure 4.7: Schematic of the measurement setup for characterization of the JPA. Total attenuation numbers are represented by X dB and X' dB. This magnetic flux is controlled via a current source which sends a dc current through the magnetic coil.

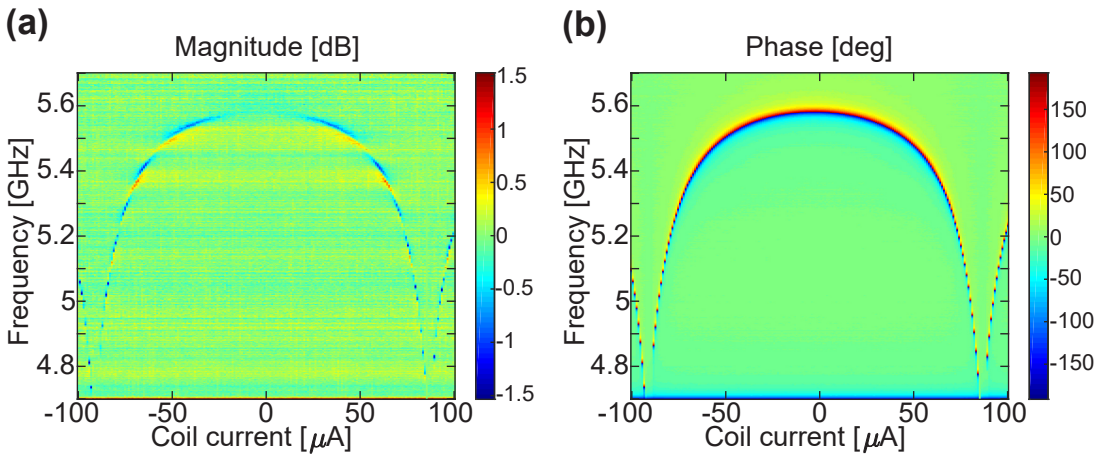


Figure 4.8: Magnetic flux dependence of the JPA microwave reflection. (a) Magnitude response of the reflected tone. (b) Phase response of the reflected tone.

the VNA records an unwrapped phase resulting in a linear phase increase with the frequency. This linear slope is subtracted from the data as well. The resulting plots are shown in Fig. 4.8. The plot of the phase shows an typical behaviour. Indeed, the phase of the measured signal is expected to undergo a 360° phase shift when crossing the JPA resonance frequency. Since the phase is plotted in a range of -180° to +180°, we obtain a dip in the phase response. In the magnitude response, we can observe an expected dip in the amplitude of the measured signals due to internal losses of the JPA. For some frequencies, small gain of about 1 dB are observed. We consider this behaviour to be an artefact of the calibration subtraction explained above. In the end, Fig. 4.7 provides

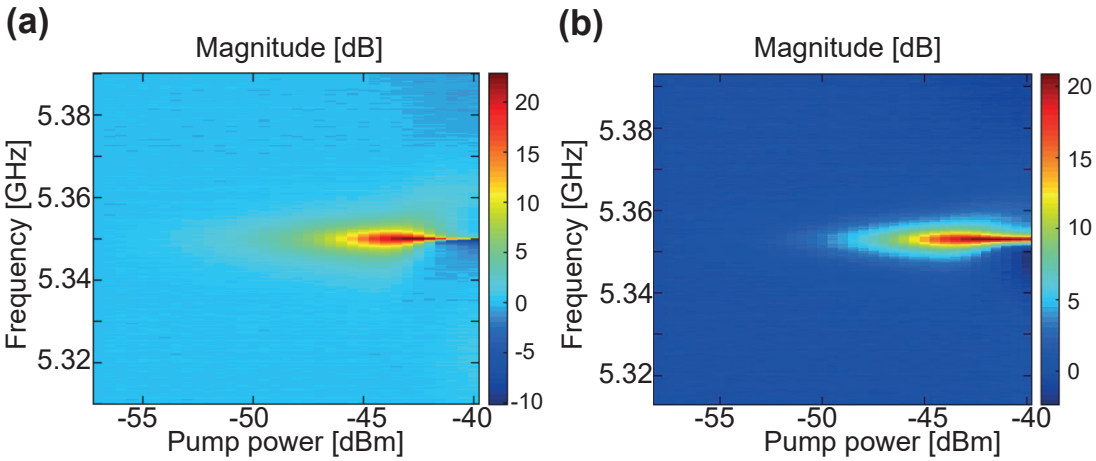


Figure 4.9: JPA nondegenerate gain measurements as a function of the pump power. (a) Magnitude response at the working point $f_0 = 5.35$ GHz. (b) Magnitude response for the working point $f_0 = 5.353$ GHz. Pump powers are referenced to the pump port of the JPA sample holder.

a calibration measurement for choosing a desired working frequency of the JPA by tuning the coil current to a respective value.

4.3.2 Nondegenerate gain measurement

To investigate the amplification of the JPA, we perform nondegenerate gain measurements, where the JPA acts as a phase insensitive parametric amplifier. Measurements are performed with the VNA as depicted in Fig. 4.7.

The slope of the JPA resonance frequency versus the coil current is an important factor. A working point where the slope is flat, or nearly flat, is not suitable for parametric amplification, as it makes the resonance frequency vary only weakly with magnetic flux. Thus, only a small amplification gain is obtained at these working points. On contrary, a working point with the steep slope makes the resonance frequency too sensitive to flux noise resulting in excessive noise during amplification or squeezing operations. Therefore, working points must be chosen to avoid both extreme situations. Once a frequency f_0 is determined, a corresponding coil current I_{coil} is selected. Afterwards, a pump tone of frequency $2f_0$ is applied to the JPA while input signals generated by the VNA are sent to the JPA. Measurements are performed with a sweep of the pump tone power and a sweep in frequency for the input signals. These frequencies are centred at $f = f_0$ with the frequency span of $\Delta f = 80$ MHz. We choose two working points at $f_0 = 5.350$ GHz and $f_0 = 5.353$ GHz for the coil currents $-70.9\ \mu$A and $-69.9\ \mu$A, respectively. The results of the respective gain measurement are shown in Fig. 4.9. We observe that the gain increases with the pump tone frequency up to a certain point.

The displayed pump power is referred to the input of the JPA. When the pump power becomes too high, around -42 dBm, higher order nonlinear effects [80, 81] starts to appear and reduces the amplification gain. We note that for input signals at exactly f_0 , the JPA acts as phase-sensitive amplifier. However, for the current measurements, these points are discarded. Furthermore, we want to be in a working regime where the gain profile in Fig. 4.9 is symmetric in frequency with respect to f_0 as this corresponds to the expected behaviour for a nondegenerate gain.

4.4 Calibration measurement

In this section, we present calibration measurements of different parts of the setup. Throughout this work, we use mainly two working different working points and focus on the results obtained for them. We present different calibration measurements necessary for us to produce quantum states in a controlled manner. To this extent, we investigate the production of squeezed states, displaced states, and noise in the form of thermal states.

4.4.1 Squeezing calibration measurement

In order to produce squeezed states in a controlled manner, we perform a squeezing calibration measurement. To this extent, we generate squeezed states at the JPA which propagates along microwaves cables and are acquired by the FPGA setup. After fixing a working point frequency f_0 and a corresponding coil current I_{coil}, we apply a pump tone at the frequency $2f_0$ to operate the JPA in the phase-sensitive regime. No input signals are sent to this JPA now. Instead, we use weak thermal states at the mixing chamber stage, whose temperature determines their thermal photon number. From the measured signals, we apply the reference state reconstruction method (see Sec.4.2.3) to reconstruct the quantum states. To this end, we apply two pulse schemes where the measurement time trace of 145.2 μs is split in half. This is represented in Fig. 4.5 by the orange pulse. During the first half, the microwave pump is inactive and this part of the trace produces the reference signal for state reconstruction. During the second half, we apply a pulse trigger to a microwave generator (SMF) in order to pump the JPA and squeeze the input signal. During the whole squeezing calibration measurement, we sweep the pump power. For each pump tone power, we repeat the pulsed measurement procedure presented above.

Several important quantities are then computed using the reconstructed moments

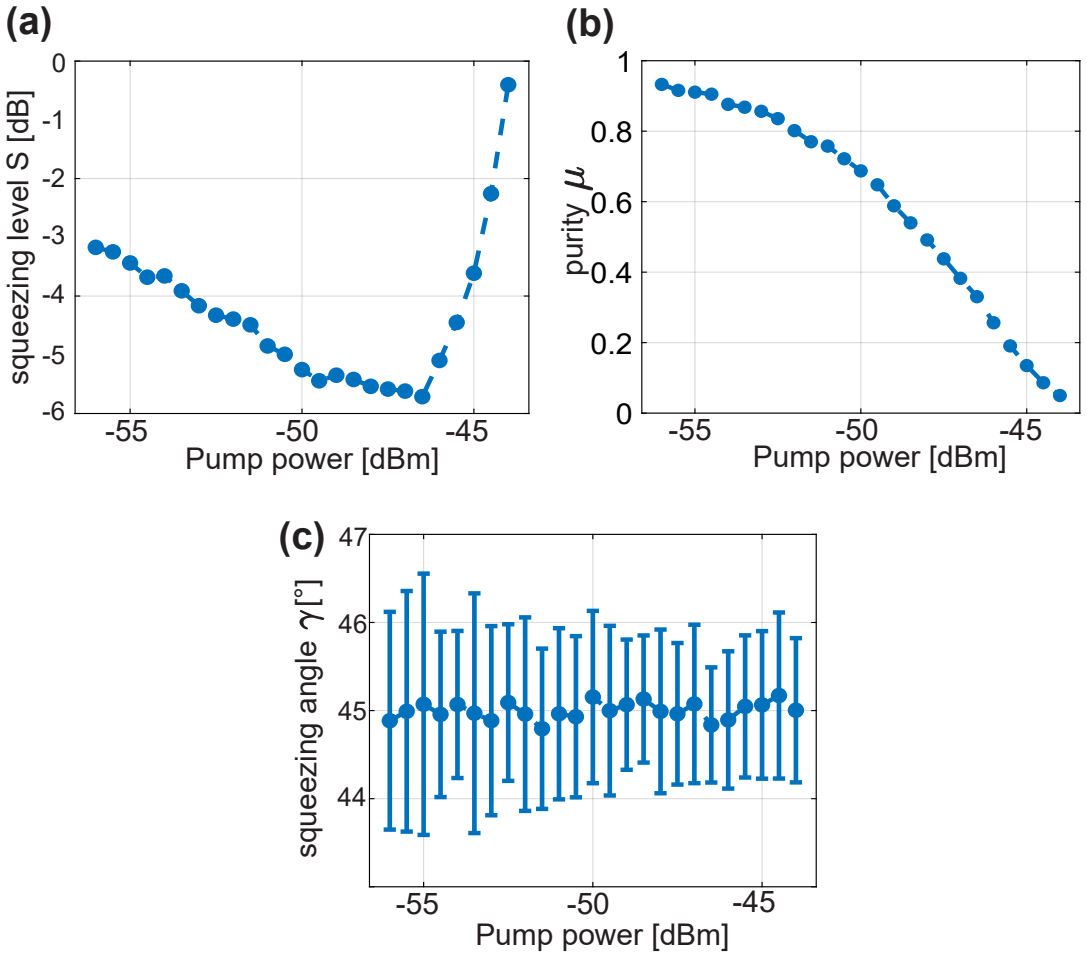


Figure 4.10: Squeezing calibration measurement for the second working point $f_0 = 5.353$ GHz. Pump powers are referenced to the pump port of the JPA sample holder. Markers represent measured data. If not shown, the error bars are smaller than the size of the markers. (a) Squeezing level versus the pump power. (b) Purity versus the pump power. (*c*) Squeezing angle versus the pump power.

from these measurements. First, we extract the squeezing level calculated here as

$$S = -10 \log_{10} \left(\frac{\sigma_S^2}{0.25} \right), \tag{4.10}$$

where 0.25 represents vacuum fluctuations and σ_S^2 is the reconstructed squeezed variance from measurements. In Fig. 4.10 (a), we show the squeezing level versus the pump power for the working point $f_0 = 5.353$ GHz. The other working point demonstrates similar results. We observe that the squeezing level increases with the pump power up to a certain threshold value. Above this value, the squeezing level starts to plummet which again is a sign of higher-order nonlinear effects [80, 81]. This defines the useful range of pump powers for generating of squeezed states. Second, we investigate the

purity μ (see Sec.2.1.1) of the reconstructed states. We reconstruct the purity of the measured quantum states under the assumption that these states are Gaussian, and display the results in Fig. 4.10 (b). We note that the purity is monotonously decreasing with the pump power. This behaviour can be explained by the JPA added noise. This added noise monotonously increases with the pump power leading to a decreasing purity with the pump power. Lastly, we also demonstrate control the squeezing angle γ of the states. In order to do so, we repeat each measurement two times for a given pump power. The first iteration of the measurement is used by a home made LabVIEW code to reconstruct a squeezing angle γ_{exp} and correct its deviation from a squeezing angle setpoint fixed γ_{target} at the beginning of the measurement. The correction is implemented by adjusting the phase of the applied pump signals. More precisely, we adjust the phase of the microwave pump by $2\delta\gamma = 2\left(\gamma_{\text{exp}} - \gamma_{\text{target}}\right)$. The second iteration of the measurement is then used to compute the quantities presented before. In Fig. 4.10 (c), we see that we can stabilize the squeezing phase to the setpoint phase of 45° with an error of roughly ±1.5°.

4.4.2 Displacement calibration measurement

In order to produce displaced states in a controlled manner, we perform displacement calibration measurement. As explained in Sec.2.1.2, we use a directional coupler acting as a highly asymmetric beamsplitter. A strong coherent signal is sent to a coupling port of the directional coupler. The states displaced are again weak thermal states coming from the mixing chamber stage to the input of the directional coupler. The power and phase of the coherent signal determines the amplitude of the displacement and the phase of the displacement, respectively. Similarly for squeezing calibration measurements, we apply a two pulse schemes where the measurement time trace of 145.2 μs is split in half. This is represented in Fig. 4.5 by the pulse in black. During the first half, no trigger pulse is applied to the SGS microwave source, so that no displacement is applied. During the second half, a trigger pulse is sent to the SGS which delivers a strong coherent signal to the coupling port of the directional coupler. The range of power for these signals is made large in order to cover small to large displacements of the states.

To calibrate the displacement, we plot the displacement photon number $n_{\text{d}} = |\langle\hat{a}\rangle|^2$ obtained from the reconstructed signal moments versus the power of the coherent signals. In Fig. 4.11 (a), we show the results for the working frequency $f_0 = 5.353$ GHz. The other working point has similar results. From the behaviour of the curves shown in the plots, we perform a linear regression fit of the curves, expressing the total photon

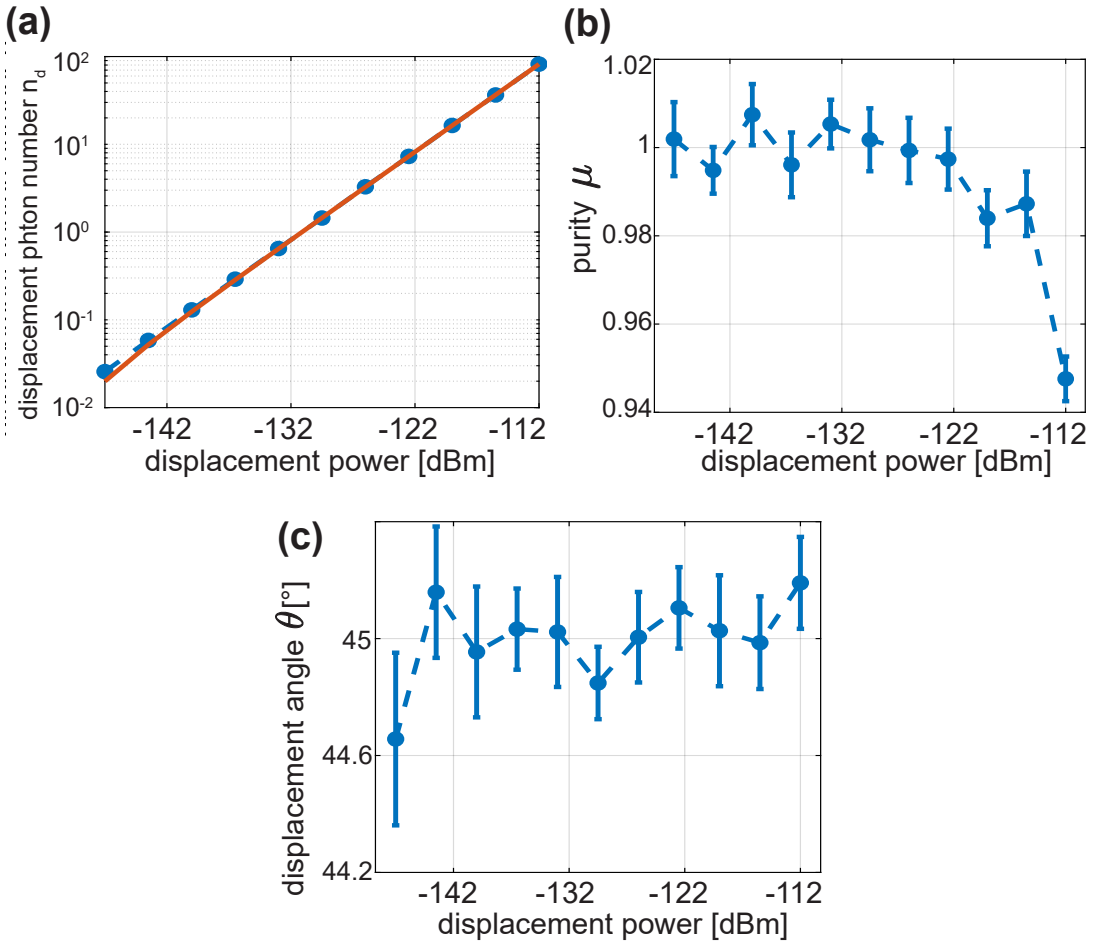


Figure 4.11: Displacement calibration measurement for the second working point $f_0 = 5.353$ GHz. Displacement power is referenced to the coupling port of the first directional coupler. Markers represent measured data. If not shown, the error bars are smaller than the size of the markers. (a) Displacement photon number versus displacement power. The blue markers correspond to measured data. The red line is a linear fit according to Eq. 4.11. (b) Purity versus displacement power. (c) Displacement angle versus displacement power.

Coefficient	Value fit [W/photon]	Error fit [W/photon]
m_d	$1.22 \cdot 10^{-9}$	$6.76 \cdot 10^{-13}$
p_d	$7.31 \cdot 10^{-12}$	$<10^{-14}$

Table 4.2: Linear fit results for the displacement photon versus the displacement power expressed in watts.

number as

$$n_d = m_d P_{coh} + p_d \tag{4.11}$$

where P_{coh} is the power in watts of the applied coherent signal and (m_d, p_d) are fitting

parameters representing the slope and the offset in the linear regression fit, respectively. They are used to power of the applied coherent signals into displacement photon numbers. In Tab. 4.2, the fitting parameters as well as the error for each parameters are displayed. The relative precision obtained is in the order of 10^{-3}. In Fig. 4.11 (b), we show the reconstructed purity μ. We observe that starting for higher powers (around -122 dBm) the purity begins to decrease. We attribute this behaviour to displacement phase fluctuations during the measurements as well as misestimations of the PNCF as discussed in Ref.[82]. Similarly to squeezing angles, we stabilize displacement angles θ by performing each measurement twice. The first iteration of each measurement permits to stabilize the reconstructed displacement angle θ to the displacement angle setpoint while the second iteration is used to reconstruct reconstruct quantum states.The results are shown in Fig. 4.11 (c).

4.4.3 Noise measurement calibration

In order to couple noise in a controlled manner, we use the setup discussed in Sec.4.2.1. A two pulses scheme is used again, where no trigger pulse is sent during the first half of the measurement time trace. Weak thermal states from the mixing chamber stage are used as a reference. During the second half of the measurement time trace, we trigger the noise generation from our AFG (81160A, Agilent Technologies). The measurement time trace is 145.2 μs long. This is represented in Fig. 4.5 by the pulse in green. The amplitude of the noise generated is related to the voltage peak-to-peak of the noise source. The generated noise is coupled via the second directional coupler to input signals. Voltage values of the AFG are swept in a broad range.

To calibrate the coupled noise, we plot the noise photon number $n_n = \langle \hat{a}^\dagger \hat{a} \rangle$ obtained from the reconstructed moments versus the voltage. From the observed behaviour of the curves in the plot, we perform a linear regression fit to express the total photon number as

$$n_\mathrm{n} = m_\mathrm{n} V_\mathrm{pp}^2 + p_\mathrm{n}, \tag{4.12}$$

where V_pp is the voltage peak-to-peak of the noise source and (m_n,p_n) are fitting parameters. They are used to convert the voltage peak-to-peak of the noise source into photon number. In Tab. 4.3, the fitting parameters as well as their error are shown. The relative precision obtained is in the order of 10^{-3}. Errors are of statistical nature, in particular for the offset p_n which is expected to be greater than or equal to 0.

Flux-dependent JPA resonance frequency measurements, as well as the nondegenerate gain measurement allow us to quantify the behaviour of our JPA. More precisely, from these measurements, we can determine a specific resonance frequency of our

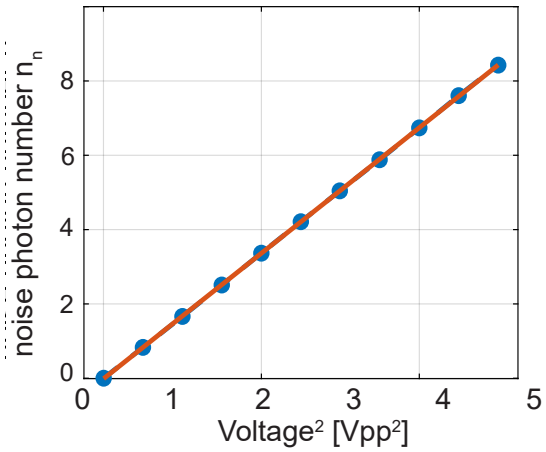


Figure 4.12: Noise calibration measurement for the second working point $f_0 = 5.353$ GHz. Markers represent measured data. If not shown, the error bars are smaller than the size of the markers. The blue markers correspond to measured data. The red line is a linear fit according to Eq. 4.12.

Coefficient	Value fit $[\text{photon}/\text{V}^2]$	Error fit $[\text{photon}/\text{V}^2]$
m_n	1.689	0.002
p_n	-0.015	0.006

Table 4.3: Linear fit results for the noise photon versus the voltage square. The voltage is expressed in peak-to-peak values.

JPA. Then, based on the calibration measurements, we are able to controllably generate noisy displaced squeezed states which are necessary for the implementation of our QKD protocol.

Chapter 5

Experimental results

In this chapter, we discuss an experimental implmenetation of the CV-QKD protocol. To this extent, we perform measurements at two working frequencies, $f_0 = 5.350$ GHz and $f_0 = 5.353$ GHz. These frequencies correspond to certain working points of our JPA (see Sec. 4.1.2). For both of these frequencies, we estimate an experimental secret key rate under various assumptions. For the first working point, we work at a fixed squeezing level $S = 3.7$ dB. From the measured data at this frequency, we investigate how to extract the mutual information and Eve's Holevo quantity. To complete the analysis, we study how the squeezing level influences the latter quantities by implementing the protocol for three different squeezing level ($S = 3.1$ dB, $S = 4.2$ dB, and $S = 5.1$ dB) for the second working point ($f_0 = 5.353$ GHz). In both cases, we analyze the effect of coupled noise η emulating Eve's Gaussian collective attack.

5.1 Protocol with fixed squeezing level

In this section, we discuss the quantum communication step of our protocol (see Sec. 3.3.1) applied for the first working point $f_0 = 5.350$ GHz. As mentioned above, this frequency corresponds to the resonance frequency of our JPA. First, we present measurements of the squeezing level S, squeezing angle γ, and purity μ. We discuss how retrieve the variance of Alice's random variable (see Sec. 3.3.1). In the second step, we calculate the secret key for the direct reconciliation case from our measured data. We assume that Eve's attack is a Gaussian collective attack in the asymptotic limit (see Sec. 3.1.3) emulated by the variable amount of noise coupled to the quantum channel. We present experimental results of the secret key rate dependence on this noise

5.1.1 Experimental realization and calibration of the protocol

For our measurements, we use all the pulses shown in Fig. 4.5 to trigger all of our devices synchronously. The idea remains the same as for calibrations measurements.

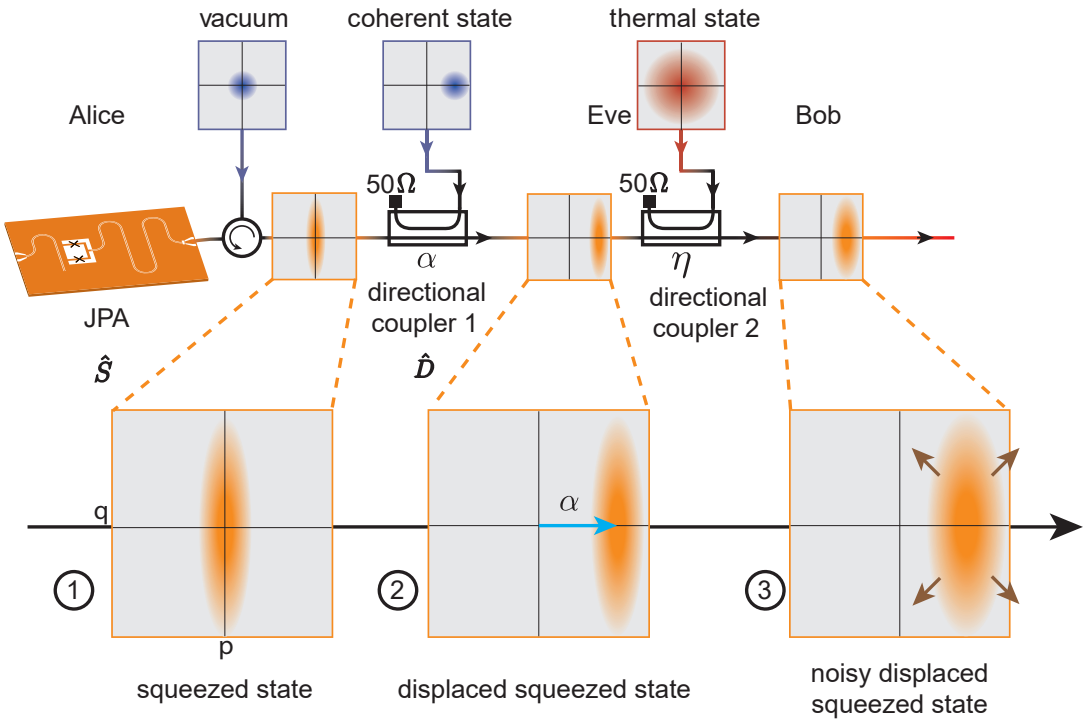


Figure 5.1: Wigner function plots of the propagating microwave state during our QKD protocol. First, at Alice's side, a JPA applies the squeeze operator $\hat{S}$ to an input vacuum generating a squeezed state. This is shown in step 1. Then in step 2, the first directional coupler implements displacement operator $\hat{D}$ to the squeezed state, using an input coherent state. Finally, using the second directional coupler, an external noise η is coupled to the displaced squeezed state. This represents the action of Eve's attack on the system. Finally, in step 3, the noisy displaced squeezed is received and measured by Bob.

In other words, we use weak thermal states as the reference states in the state reconstruction method (see Sec. 4.2.3). We remind that Alice is considered to be our JPA in combination with the first directional coupler. Eve's quantum channel is the second directional coupler. Finally, Bob is defined by a specific reference point at the output of the second directional coupler.

In order to implement the quantum communication part of our QKD protocol, we follow the steps explained in Sec. 3.3.1. However, we do not randomly change the squeezing angle of the generated squeezed states but rather work with a fixed squeezing angle throughout the experiment. This is done for two reasons. First, we reconstruct quantum states in our measurements with the reference state reconstruction method. This means in particular that we reconstruct the displacement angle and displacement photon number for each quantum states chosen by Alice. Second, if we experimentally fulfill the condition of indistinguishability indicated in Eq. 3.49, sending a key by randomly squeezing the q or p quadrature for each quantum states is equivalent to

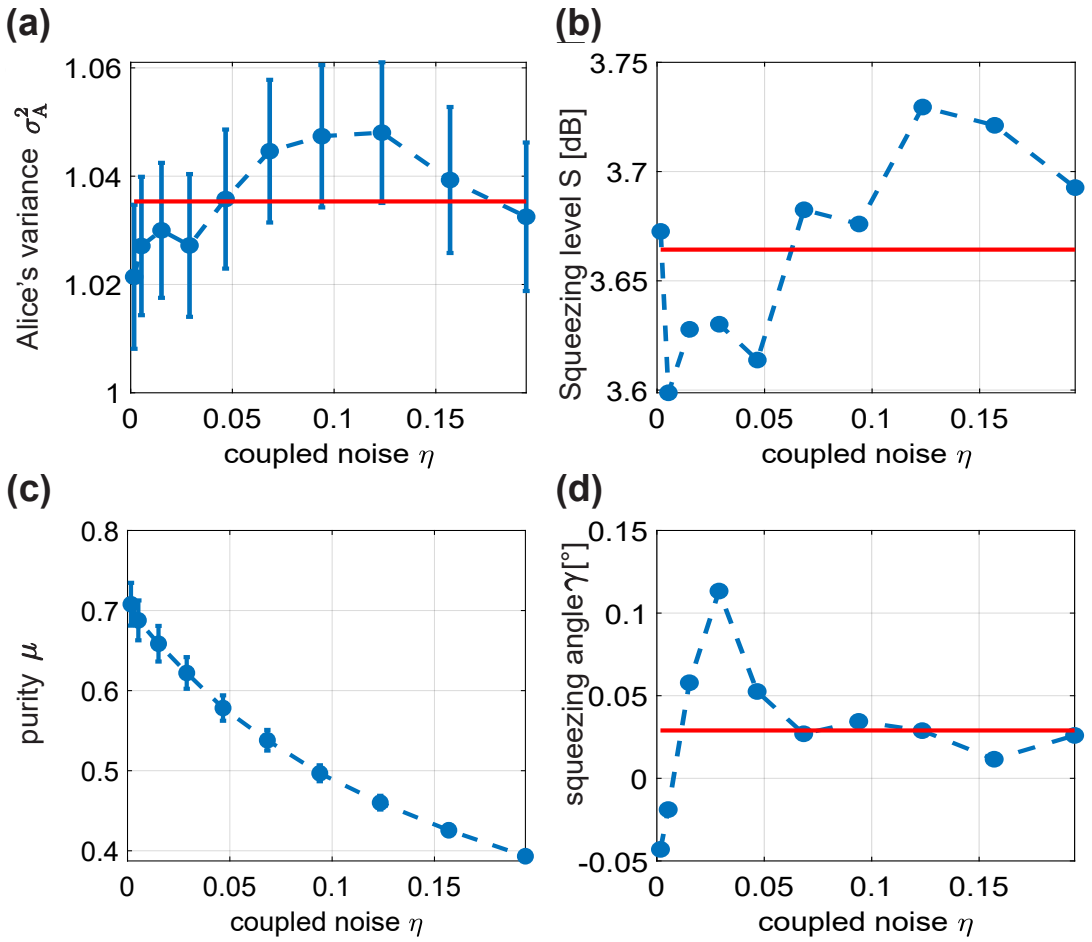


Figure 5.2: (a) Alice's average variance σ_A^2 reconstructed at the input of the second directional coupler versus the noise photon number η. The red line represents the mean value of the variance. (b) Average squeezing level reconstructed at the input of second directional coupler versus the noise photon number η. The red line represents the mean squeezing level. (c) Purity of output states reconstructed at the output of the second directional coupler versus the noise photon number η. (d) Average squeezing angle of output states reconstructed at the output of second directional coupler versus the noise photon number η. The red line represents the mean reconstructed squeezing angle. For all the plots, markers correspond to experimental data. If not shown, error bars are smaller than the size of the markers.

sending a key where the squeezed quadrature is fixed up to the fraction of discarded measurements during the sifting step. In other words, this equivalence holds if we account for the sifting fraction $\left(1 - D_{\text{sifting}}\right)$ in the secret key rate R. In our case, this involves adding a factor $1/2$ to our secret key rate since $\left(1 - D_{\text{sifting}}\right) = 1/2$ for our QKD protocol in the asymptotic case.

For this implementation of our QKD protocol, we choose the working point $f_0 = 5.350$ GHz and the corresponding coil current $I_{\text{coil}} = -69.9\ \mu$A. Additionally, we fix a squeezing level $S = 3.9$ dB $\pm$ 0.1 dB throughout the measurement by using the

corresponding pump power = -50.5 dBm. This squeezing level refers to the input of the second directional coupler (see Sec. 4.1.2). As discussed in the previous paragraph, we also fix the squeezing angle for all the quantum states and generated quantum state squeezed only in the q quadrature. Experimentally, we can rewrite the condition of indistinguishability as

$$\sigma^2_{\mathrm{AnSq}} = \sigma^2_{\mathrm{A}} + \sigma^2_{\mathrm{Sq}}, \tag{5.1}$$

where σ^2_{AnSq} corresponds to the reconstructed antisqueezed variance, σ^2_{Sq} corresponds to the reconstructed squeezed variance, and σ^2_{A} is the variance of Alice's Gaussian classical random variable that generates her key elements. This value σ^2_{A} is obtained using the squeezing calibration measurements performed at the frequency $f_0 = 5.35$ GHz in addition to Eq. 5.1. This variance is calculated at the input of the second directional coupler (see Sec. 4.1.2). For the squeezing level chosen, we experimentally get $\sigma^2_{\mathrm{A}} = 1.020 \pm 0.013$ for the variance of Alice's Gaussian classical random variable.

As mentioned above, we want to investigate the effects of coupled noise on the secret key. To this end, we start by generating $N = 150$ random key elements using a MATLAB script. They are individually drawn from a Gaussian distribution with zero mean and variance fixed to σ^2_{A}. This assures that the condition of indistinguishability is satisfied. We recall that for each key element, we generate a displaced squeezed using the JPA and the first directional coupler. This is represented by steps 1 and 2 in Fig. 5.1.

Noise is coupled to these displaced squeezed states through the second directional coupler. We use ten different values of coupled noise η. This is represented by the step 3 in Fig. 5.1. It ranges from $\eta = 0.0017$ corresponding to the lowest measured noise we can generate up to $\eta = 0.194$ noise photon. These photon numbers refer to the output of the second directional coupler (i.e., to Bob's states). For each coupled noise η, we use a key composed of $N = 150$ different key elements. This number N is a compromise between the asymptotic case $\mathrm{N} \rightarrow \infty$ and the duration of these measurements. In Fig. 5.2, we display useful reconstructed quantities from measurements. In Fig. 5.2(a), we observe the experimental variance σ^2_{A} calculated from Eq. 5.1. We note that the mean value $\sigma^2_{\mathrm{A}} = 1.035$ is in good agreement with the σ^2_{A} indicated above. Furthermore, it only varies on average as $\pm$ 0.01 from its mean value and those fluctuations are not correlated with the coupled noise η. In Fig. 5.2(b), we observe a similar behaviour for the squeezing level, which should ideally stay constant throughout the measurements. Here, we note a mean squeezing level of 3.7 dB. Furthermore, we also observe that the observed fluctuations seems not to be correlated with the coupled noise. We rather attribute them to statistical errors. In Fig. 5.2(c), we can see the effect of the coupled noise on the purity of quantum states. The decrease in purity is caused by the increased of the coupled noise which is an expected behaviour. Lastly in Fig. 5.2(d), we show

the reconstructed squeezing angle at the output of the second directional coupler versus the coupled noise. We observe a mean squeezing angle of 0.03° with a mean standard deviation of 0.043° which is in good agreement with our squeezing calibration measurements.

5.1.2 Mutual information and holevo quantity

In this section, we focus on the extraction of the mutual information and Eve's Holevo quantity from the measurements.

We start by considering Eve's Holevo quantity. To this extent, we use the results obtained in Sec. 3.3.2. In particular, we compute the different covariance matrices $\mathbf{V}_{\mathrm{E}}^{k_{\mathrm{i}}}$ describing the individual states of Eve for each key element k_{i} sent by Alice. For this, we use Eq. 3.52. From this equation, we can see that we need the covariance matrix describing Eve's mode of her TMSV state that interacted with incoming states of Alice. For a given noise n_{Eve} at the input of the second directional coupler and key element k_{i}, the covariance matrices of Alice's individual states $\mathbf{V}_{\mathrm{A}}^{k_{\mathrm{i}}}$ are transformed as

$$\mathbf{V}_{\mathrm{B}}^{k_{\mathrm{i}}} = \tau \mathbf{V}_{\mathrm{A}}^{k_{\mathrm{i}}} + (1-\tau)\,(1+2n_{\mathrm{Eve}})\,\frac{\mathbb{I}}{4}, \tag{5.2}$$

where $\mathbb{I}$ is the identity matrix, τ is the transmissivity of the second directional coupler, and $\mathbf{V}_{\mathrm{B}}^{k_{\mathrm{i}}}$ corresponds to the covariance matrix of Bob's state at the output of the second directional coupler. We see that we can get $\mathbf{V}_{\mathrm{A}}^{k_{\mathrm{i}}}$ from Eq. 5.2 considering that τ is known and n_{Eve} can be obtained from the noise calibration measurement. From there, we can calculate the covariance matrix of Eve's individual state as

$$\mathbf{V}_{\mathrm{E}}^{k_{\mathrm{i}}} = (1-\tau)\,\mathbf{V}_{\mathrm{A}}^{k_{\mathrm{i}}} + \tau\,(1+2n_{\mathrm{Eve}})\,\frac{\mathbb{I}}{4}. \tag{5.3}$$

Let us describe the connection between n_{Eve} and the noise calibration measurement. During this measurement, we effectively reconstruct thermal states whose thermal population depends on the input coupled noise n_{Eve}. We denote by n_{th} the thermal photon number of these thermal states. We can then write for this noise calibration measurement that

$$\tau\left(1+2n_{\mathrm{stage}}\right)\frac{\mathbb{I}}{4} + (1-\tau)\,(1+2n_{\mathrm{Eve}})\,\frac{\mathbb{I}}{4} = (1+2n_{\mathrm{th}})\,\frac{\mathbb{I}}{4}, \tag{5.4}$$

where n_{stage} is the thermal photon number corresponding to a weak thermal state at the mixing chamber stage and τ is still the transmissivity of the second directional coupler. Using this result and Eq. 3.12, we can additionally connect the coupled noise η of Eve's

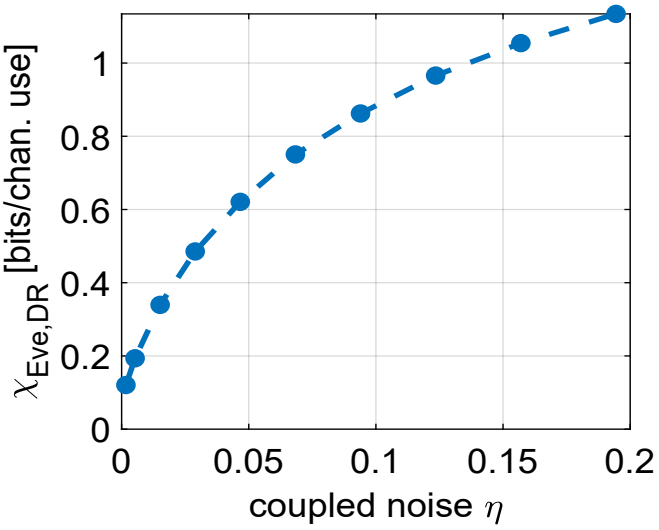


Figure 5.3: Eve's holevo quantity $\chi_{\text{Eve,DR}}$ obtained from the state tomography for each value of η in the DR case. Full circles correspond to the experimental data, dashed line is guide for eyes.

attack and the reconstructed photon number n_{th} as

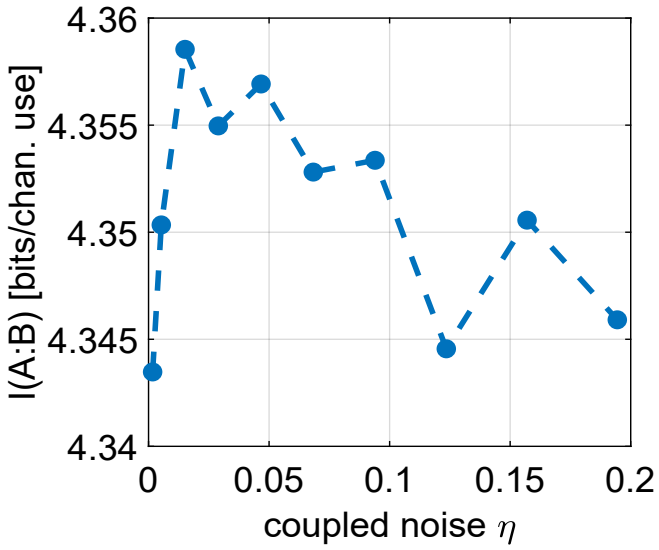
$$4\eta = 2\left(n_{\text{th}} - \tau\, n_{\text{stage}}\right). \tag{5.5}$$

From Eq. 5.3 and Eq. 5.5, we experimentally compute Eve's covariance matrix of her individual states as described in Eq. 3.52. Then, we calculate the average state $\hat{\rho}_{\text{E,avg}}$ of Eve as

$$\hat{\rho}_{\text{E,avg}} = \sum_{\text{i=1}}^{\text{N=150}} \frac{1}{150} \cdot \hat{\rho}_{\text{E}}^{k_{\text{i}}}, \tag{5.6}$$

where $\hat{\rho}_{\text{E}}^{k_{\text{i}}}$ corresponds to Eve's individual states whose covariance matrix is given by $\mathbf{V}_{\text{E}}^{k_{\text{i}}}$. These matrices are exactly given by the procedure explained above. We recall that N corresponds to the number of key elements sent by Alice. The experimental results are displayed in Fig. 5.3. The observed behaviour of the curve is similar to one obtained from theory. In particular, Eve's Holevo quantity increases with the coupled noise photon number η.

Now, we focus on extraction of the mutual information. We start by considering that on her side, Alice has a randomly generated key $\mathcal{K} = \{k_1, \cdots, k_{\text{N}}\}$, where each key element k_{i} is generated randomly based on a Gaussian distribution with the fixed variance as explained in Sec. 3.3.1. We remind that each key element is encoded in the displacement amplitude of the displaced squeezed states. From the reconstructed signal moments $\left\langle \hat{a}^n (\hat{a}^\dagger)^m \right\rangle$, we can extract a displacement photon number and angle for



.

Figure 5.4: Mutual information $I(A{:})$ from the measured data

each states. From this two last values, an estimation of each key element $k_{\mathrm{i}}^{'}$ is obtained. This provides Bob's estimate for the key $\mathcal{K}^{'} = \left\{k_1^{'}, \cdots, k_{\mathrm{N}}^{'}\right\}$. These two keys $\mathcal{K}$ and $\mathcal{K}^{'}$ are used to compute the mutual information between Alice and Bob. For a CV-QKD protocol using Gaussian states, the mutual information can be computed using Eq. 3.36. Applying this last equation in our case yields

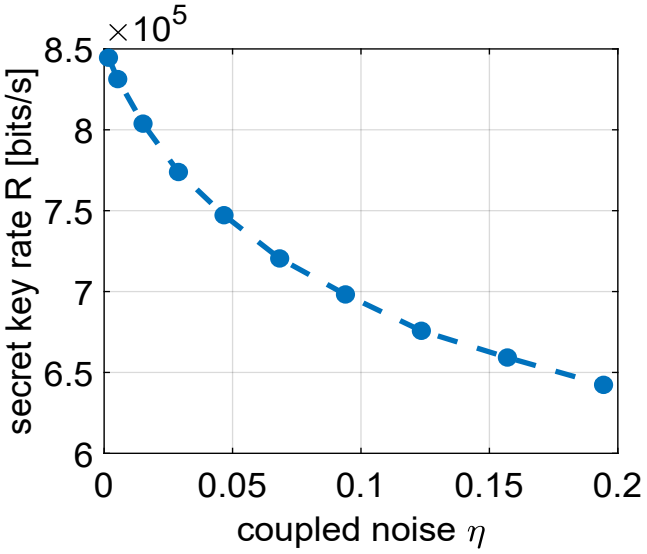
$$I(A{:}B) = \frac{1}{2}\log_2\left[\frac{\sigma_A^2\,\sigma_B^2}{\sigma_A^2\,\sigma_B^2 - \mathrm{Cov}(A,B)^2}\right]. \tag{5.7}$$

where $I(A{:}B)$ is the classical mutual information between Alice and Bob, A is Alice's key $\mathcal{K}$, and B is Bob's key $\mathcal{K}^{'}$. The measured variance of Alice's key and Bob's key is denoted σ_A^2 and σ_B^2, respectively. Finally, $\mathrm{Cov}(A,B)$ is the classical covariance between the two keys. In order to calculate those variances and covariances, we use statistical unbiased estimators. More precisely, for a set $X = \{x_1, \cdots, x_{\mathrm{N}}\}$ of N elements, the classical variance σ_X^2 of the set is defined as

$$\sigma_X^2 = \frac{1}{N-1}\sum_{\mathrm{i}=1}^{\mathrm{N}}(x_{\mathrm{i}} - \mu)^2\,, \tag{5.8}$$

where μ is the mean value of the set defined as

$$\mu = \frac{1}{N}\sum_{\mathrm{i}=1}^{\mathrm{N}} x_{\mathrm{i}}. \tag{5.9}$$



.

Figure 5.5: Secret key rate R calculated from the mutual information shown in Fig. 5.4 and Eve's Holevo quantity shown in Fig. 5.3 for a repetition rate of $f_r = 400\,kHz$ and a sifting rate $\left(1 - D_{\text{sifting}}\right) = 1/2$. Full circles correspond to the experimental data, dashed line is guide for eyes.

Additionally, for two sets $X = \{x_1, \cdots, x_N\}$ and $Y = \{y_1, \cdots, y_N\}$ of N elements each, the classical covariance Cov (X,Y) of the set is defined as

$$\text{Cov}\,(X,Y) = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \mu_X)\cdot(y_i - \mu_Y)\,, \tag{5.10}$$

where μ_X is the mean value of X and μ_Y is the mean value of Y. In Fig. 5.4, we show the mutual information $I\,(A{:}B)$ calculated from the measured set $\mathcal{K}$ and $\mathcal{K}'$ for each coupled noise η. From this figure, two important remarks can be made. First, we observe that the mutual information does not fluctuate significantly with the coupled noise η. Indeed, it varies by 0.01 around a mean value of 4.35 bits per channel usage. Second, we note that the calculated mutual information does not decrease significantly with the coupled noise like we expect from the simulations. To explain those observations, we have to take into account the number averages used during our reference state reconstruction method (see Sec. 4.2.2). In particular, each quadrature moment $\langle I^n Q^m \rangle$ measured are averaged in our case in total $M_{\text{avg}} = 2.094 \times 10^8$ times. In turn, this number of averages is included in the calculation of the signal moments $\left\langle \hat{a}^n (\hat{a}^\dagger)^m \right\rangle$. Therefore, if individually each measured key element has a statistical error of σ, then each averaged key element of Bob has a statistical error of $\sigma / \sqrt{M_{avg}}$. If this statistical error is attributed to noise during the measurements, the dominant noise contribution

comes from our first amplifier (HEMT). From our PNCF calibration measurement (see Sec. 4.2.4), we obtain a noise photon number of $n_{\mathrm{HEMT}} = 24.24$ and $n_{\mathrm{HEMT}} = 27.74$ for the working point at $f_0 = 5.350$ GHz and $f_0 = 5.353$ GHz, respectively. Therefore, we get $\sigma/\sqrt{M_{\mathrm{avg}}} < 0.01$ (i.e., the variance of the mutual information). From this approach, we can assume that the measured mutual information does not depend on the coupled noise η. However, it does not explain the variations observed. The latter are attributed to amplitude fluctuations over time of the coherent tone applied to our first directional coupler. Such fluctuations induce variations of the displacement of our generated displaced squeezed states. As a result, we also observe variations in the measured key elements over time.

Finally, we can use the obtained results for the mutual information and Eve's Holevo quantity to calculate the secret key rate R. To this end, we first calculate the secret key K from Eq. 3.43 where we assume a perfect reconciliation rate $\beta = 1$. Then, the secret key rate R is calculated from Eq. 3.44 and shown in Fig. 5.5. As discussed in Sec. 5.1.1, the sifting fraction is set to $\left(1 - D_{\mathrm{sifting}}\right) = 1/2$. Furthermore, we identify the repetition rate f_{r} with the measurement bandwidth Ω which experimentally limits the rate at which bits can be communicated. In our experiment, our measurement bandwidth is given by the bandwidth of the used FIR filters (see Sec. 4.2.2) which results in $f_{\mathrm{r}} = \Omega = 400\,\mathrm{kHz}$. Since the averages increase the calculated mutual information, we interpret this secret key rate R as an upper bound of the achievable secret key rate in our experimental setting.

The fact that our measurements contain many averages represent the main difference between our implementation of the QKD protocol and the theoretical analysis developed in Chapter. 3. In this analysis, we indeed consider that Bob only performs only one projective measurement for each quantum states he receives. In order to compare our experimental results with the theoretical calculations, we focus on a possible rescaling of the mutual information to emulate the effect of low number of averages $M_{\mathrm{avg}} \to 1$. To this extent, we make use of the expression of the mutual information derived from Eq. 3.60. Interestingly, this equation allows us to rescale our mutual information by rescaling our signal-to-noise (SNR) ratio. In our case, we can write that our measured $\mathrm{SNR_H}$ scales as

$$\mathrm{SNR_H} = M_{\mathrm{avg}} \cdot \mathrm{SNR_0}, \tag{5.11}$$

where $\mathrm{SNR_0}$ corresponds to the SNR obtained for no averages. Re-expressing Eq. 5.11 gives that

$$\mathrm{SNR_H} = 2^{2\,I(A:B)} - 1. \tag{5.12}$$

From Eq. 3.60 and Eq. 5.12, we can finally write the rescaled mutual information

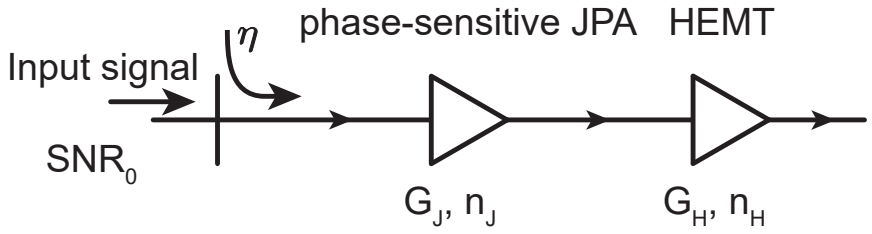


Figure 5.6: Modified amplification chain. On the left hand side, input signals have initially a SNR = SNR_0. This SNR is then reduced by the addition of a coupled noise η. This represents the noise coupled via the second direction coupler (see Fig. 5.1). A JPA is used as a first stage amplifier. It has a gain G_J and noise n_J referred to the input of the JPA. The HEMT is now the second stage amplifier. It has a gain G_H = 36.5 dB and a noise n_H referred to the input of the HEMT.

$I(A{:}B)_0$ as

$$I(A{:}B)_0 = \frac{1}{2}\log_2\left(1 + \frac{2^{2\,I(A:B)} - 1}{M_\mathrm{avg}}\right). \tag{5.13}$$

In Fig. 5.4, we display the rescaled mutual information. These values are significantly lower than the originally computed mutual information. This highlights the role of averaging in our detection setup. In such a setup, the noise from the first amplifier (HEMT) significantly affects the measurement SNR. However, this also means that the measurement SNR can be increased if we suppress the noise coming from our first amplifier. An interesting way to implement such strategy is to place a phase-sensitive amplifier before our HEMT amplifier. Experimentally, this can be done by an additional JPA the phase-sensitive regime. Remarkably, a JPA working in this regime can theoretically amplify input signals without adding any noise. To this extent, one quadrature is amplified while the orthogonal quadrature is deamplified. Therefore, we consider now an amplification chain where a JPA preamplifier operating in the phase-sensitive regime is placed before our HEMT amplifier. If we denote G_J and n_J the gain and noise referred to the input of such a JPA, we obtain using the Friis formula [38]

$$\frac{\mathrm{SNR_J}}{\mathrm{SNR}_0} = \frac{\mathrm{SNR_J}}{\mathrm{SNR_H}}\frac{1}{M_\mathrm{avg}} = \frac{n_\mathrm{H}}{n_\mathrm{J} + \frac{n_\mathrm{H}}{G_\mathrm{J}}}\frac{1}{M_\mathrm{avg}}, \tag{5.14}$$

where $\mathrm{SNR_J}$ is the measurement SNR if the first amplifier is a JPA working in the phase sensitive regime, $\mathrm{SNR_H}$ is the measurement SNR if the first amplifier is the previously HEMT, and n_H is the noise of the HEMT referred to the input. Since the measured SNR does not contain the effect of the coupled noise η as discussed above, it is added during the rescaling. This is done because the SNR for no averages should contain the coupled noise η. The final amplification chain we consider is shown in Fig. 5.6. Those

considerations allows us to write

$$\frac{\mathrm{SNR_J}}{\mathrm{SNR_0}} = \frac{n_\mathrm{H}}{n_\mathrm{J} + \frac{n_\mathrm{H}}{G_\mathrm{J}} + \eta} \frac{1}{M_\mathrm{avg}}. \tag{5.15}$$

More generally, if we consider that we allow for M instead of M_avg averages during the measurements, we can combine Eq. 5.11 and Eq. 5.15 to obtain the general rescaling

$$\frac{\mathrm{SNR_J}}{\mathrm{SNR_0}} = \frac{\mathrm{SNR_J}}{\mathrm{SNR_H}} \frac{1}{M_\mathrm{avg}} = \frac{n_\mathrm{H}}{n_\mathrm{J} + \frac{n_\mathrm{H}}{G_\mathrm{J}}} \frac{M}{M_\mathrm{avg}}, \tag{5.16}$$

In turn, this gives us a rescaled mutual information

$$I\left(A{:}B\right)_\mathrm{J} = \frac{1}{2} \log_2 \left(1 + \mathrm{SNR_J}\right). \tag{5.17}$$

Therefore, by varying the value of n_J and M, one can controllably rescale the mutual information. Depending on the values chosen, the mutual information can become greater than Eve's Holevo quantity. For numerical calculations, we consider a realistic implemetation of the phase sensitive amplifer by a JPA operating in the phase senstive regime. Thus, the achievable gain G_J is set to 40 dB which corresponds to a rather large gain for our JPAs. From Tab. 4.1, the noise photon number from the HEMT n_H is fixed to $n_\mathrm{H} = 24.25$. Fig. 5.7 shows parameter thresholds obtained for each squeezing level. The thresholds correspond to the minimum values of n_J and M required to reach the regime when the mutual information is equal to the Holevo quantity. According to Eq. 3.46, this translates into a threshold between positive and negative key rates, or between secure and insecure communication, respectively. From Fig. 5.7, we observe that the number of averages M can be significantly reduce. For a low coupled noise photon number $\eta = 0.0017$, we can go down to $M \simeq 17$.

5.2 Protocol with different squeezing levels

In this section, we consider the quantum communication step of our protocol (see Sec. 3.3.1) applied for the second working point $f_0 = 5.353$ GHz. We calculate the secret key for the direct reconciliation case from the measured data. Additionally, we assume that Eve's attack is a Gaussian collective attack in the asymptotic limit (see Sec. 3.1.3). Furthermore, we experimentally focus on the noise influence by coupling different amount of noise to Alice's input states. Finally, we discuss relevant secret key rates as a function of noise and squeezing.

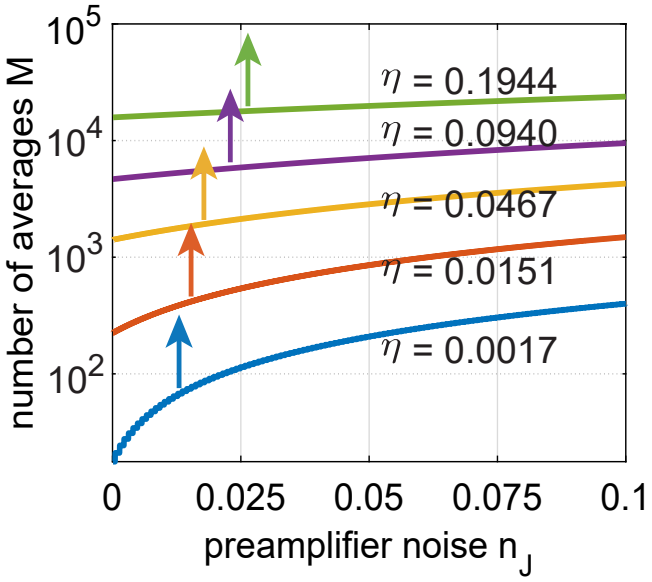


Figure 5.7: Thresold values of M and n_J such that the secret key K becomes positive. Each line corresponds to a different value coupled noise photon number η. For each line, a coloured arrow indicates that the parameters above the curve correspond to a positive secret key and secure communication. Only 5 coupled noise η are shown for clarity purpose.

5.2.1 Experimental realization and calibration of the protocol

Here, we investigate the protocol for different squeezing levels. We use the same measurement approach as explained in Sec. 5.1. The squeezing angle is fixed, so that the squeezed quadrature is always the q quadrature. This means that we need again to multiply our secret key by $\left(1 - D_{\text{sifting}}\right) = 1/2$ to obtain a secret key rate. For this implementation of our QKD protocol, the second working point $f_0 = 5.353$ GHz and coil current $I_{\text{coil}} = -70.9\ \mu$A are chosen. We use three different squeezing levels: $S = 3.5$ dB, $S = 4.5$ dB, and $S = 5.5$ dB. We measure experimentally three corresponding squeezing levels: $S = 3.1$ dB, $S = 4.2$ dB, and $S = 5.1$ dB with an error of ± 0.2 dB. Using Eq. 5.1, we can calculate the variance of Alice's Gaussian classical random variable. This is done using the results obtained from the squeezing calibration measurement performed for $f_0 = 5.353$ GHz. Similarly as for the previous section, we generate a random key composed of $N = 150$ key elements. Each key element is drawn from a normal distribution with a mean set to 0 and a variance set to σ_A^2. The value of σ_A^2 depends on the squeezing level according to Eq. 5.1. For each key element, we generate a displaced squeezed state using the JPA and the first directional coupler.

Noise is coupled to the displaced squeezed states using the second directional coupler. For each squeezing level, we use four different values of coupled noise η. It ranges from $\eta = 0.0017$ to $\eta = 0.2192$ corresponding to a value above the secure communication

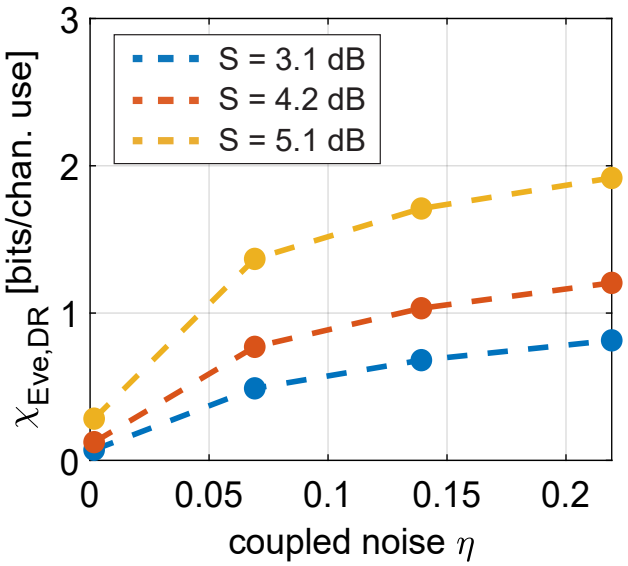


Figure 5.8: Eve's Holevo quantity $\chi_{\text{Eve,DR}}$ obtained from her reconstructed states for each coupled noise η in the DR case. Markers correspond to experimental data. Measurements for each squeezing level are shown.

threshold obtained from our numerical calculations (see Sec. 3.3.2). This noise photon number η is referred to the output of the second directional coupler. Since the procedure is exactly similar to the one presented in Sec. 5.1, we do not discuss in detail results measured for Alice's variance σ_A^2, the squeezing level, the squeezing angle and purity. We merely want to stress that similar precision as in Sec. 5.1 is achieved. This assures us that the protocol is well-calibrated.

5.2.2 Mutual information and Holevo quantity

We start by reminding that the coupled noise η is extracted from our measurement using Eq. 5.5, where n_{th} is the reconstructed photon number from the noise calibration measurement performed at the frequency f_0 (see results Sec. 4.3).

First, we consider Eve's Holevo quantity. We can straightforwardly use the previously derived expressions in Eq. 5.2 and Eq. 5.3, since we know the coupled noise value η from Eq. 5.5. The obtained results are displayed in Fig. 5.8. Like for the measurement with fixed squeezing level, Eve's Holevo quantity increases with the coupled noise η. In addition, we observe that Eve's Holevo quantity increases with the squeezing level. This is an expected behaviour as increasing the squeezing level increases the information obtained on the encoded key from Alice. To understand this effect, we recall that each key element k_{i} of Alice's key $\mathcal{K} = \{k_1, \cdots, k_{\text{N}}\}$ is encoded into the displacement of a displaced squeezed state. More precisely, it is encoded into the mean value of the squeezed quadrature. When the squeezing level increases, the uncertainty

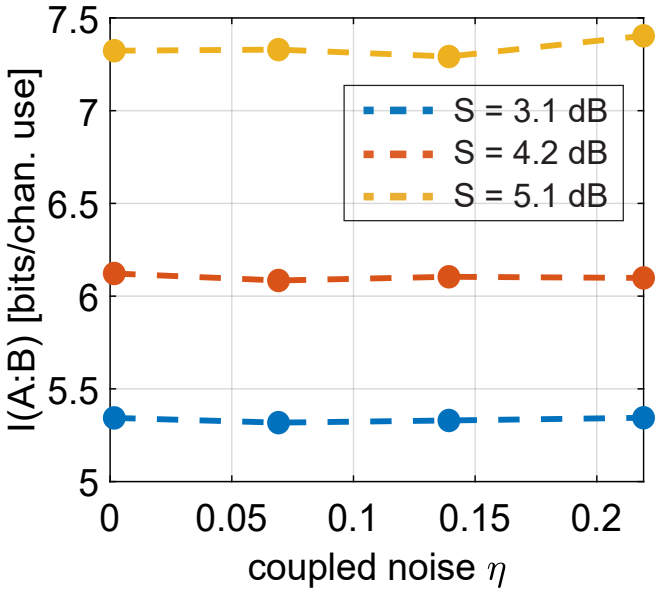


Figure 5.9: Mutual information $I(A{:}B)$ measured for each squeezing level. Full circles correspond to the measured data. Dashed lines are guides for eyes.

on the squeezed quadrature decreases meaning that the mean value of the squeezed quadrature is measured more precisely which also implies that the encoded key element k_i is measured more precisely.

To compute the mutual information between Alice and Bob, we implement the same procedure as described in Sec. 5.1.2. In particular, we consider again that Alice has a key $\mathcal{K} = \{k_1, \cdots, k_\mathrm{N}\}$ coming from her Gaussian random variable and Bob has a measured key $\mathcal{K}' = \left\{k'_1, \cdots, k'_\mathrm{N}\right\}$. We start by using Eq. 5.7 where σ^2_A and σ^2_B are the variance of Alice's key and Bob's key, respectively. Furthermore, $\mathrm{Cov}\,(A,B) = \mathrm{Cov}\left(\mathcal{K},\mathcal{K}'\right)$ is the classical covariance between the two keys. In Fig. 5.9, the mutual information for each squeezing level are shown. Once again, the mutual information is not dependent on the coupled noise. The fluctuations observed are attributed mainly to amplitude fluctuations over time of the coherent tone applied to the first directional coupler.

From the measured Holevo quantity shown in Fig. 5.8 and the mutual information shown in Fig. 5.9, we calculate the secret key rate R using Eq. 3.44 for each squeezing level where we assume a perfect reconciliation rate $\beta = 1$. The repetition rate is fixed by our measurement bandwidth to $f_\mathrm{r} = 400\,\mathrm{kHz}$ and the sifting rate is $\left(1 - D_\mathrm{sifting}\right) = 1/2$. In regard to our previous discussion in Sec. 5.1.2, the calculated mutual information does not depend on any experimental noise and is significantly increases by the averages M_avg. Therefore, we interpret the calculated secret key rates R as upper bounds on the achievable secret key rates for our experimental setup depending on the coupled noise η and the squeezing level. Remarkably, we observe that the latter increases the secret rate R which is in good agreement with our simulations in Sec. 3.8

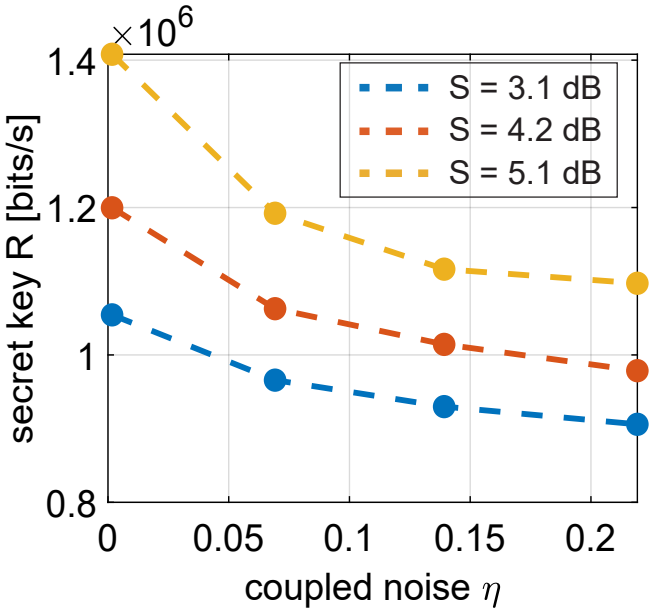


Figure 5.10: Secret key rate R calculated from the mutual information shown in Fig. 5.9 and Eve's Holevo quantity shown in Fig. 5.8 for a repetition rate of $f_r = 400\,\text{kHz}$ and a sifting rate $\left(1 - D_{\text{sifting}}\right) = 1/2$ for each squeezing level. Full circles correspond to the experimental data, dashed line is guide for eyes.

To complete this analysis, we rescale the mutual information using the calculated SNR. For this purpose, an additional phase-sensitive preamplifier is considered to be place before our HEMT amplifier. The rescaled SNR is extracted from Eq. 5.16 which is used to compute Eq. 5.17. Therefore, depending on the values of n_J and M, the mutual information can become greater than Eve's Holevo quantity. We assume a JPA preamplifier gain of $G_J = 40$ dB. From Tab. 4.1, the noise photon number from the HEMT n_H is fixed to $n_H = 27.74$. Fig. 5.11 shows the parameter thresholds obtained for each squeezing level. We recall that these thresholds correspond to the minimum values of n_J and M required such that the mutual information is greater than the Holevo quantiy. From Eq. 3.46, this translates into a positive secret key, and thus, a secure communication. The required number of averages increases with the coupled noise as expected. Indeed, an increased coupled noise means that more information from Alice and Bob is lost to Eve. Very interestingly, we observe that the required number of averages reach 1 or nearly 1 if we consider low coupled noise $\eta = 0.0017$ for each squeezing level. This represents a very promising result as it means that we can implement our QKD protocol in the single-shot regime. However, all squeezing levels, the maximal tolerable preamplifier noise n_J in order to have a positive secret key is quite small, being at most $n_J = 0.002$ noise photon. Furthermore, we notice that the required number of averages decreases with the squeezing level. This is an important effect, as this means that increasing the squeezing level can increase the

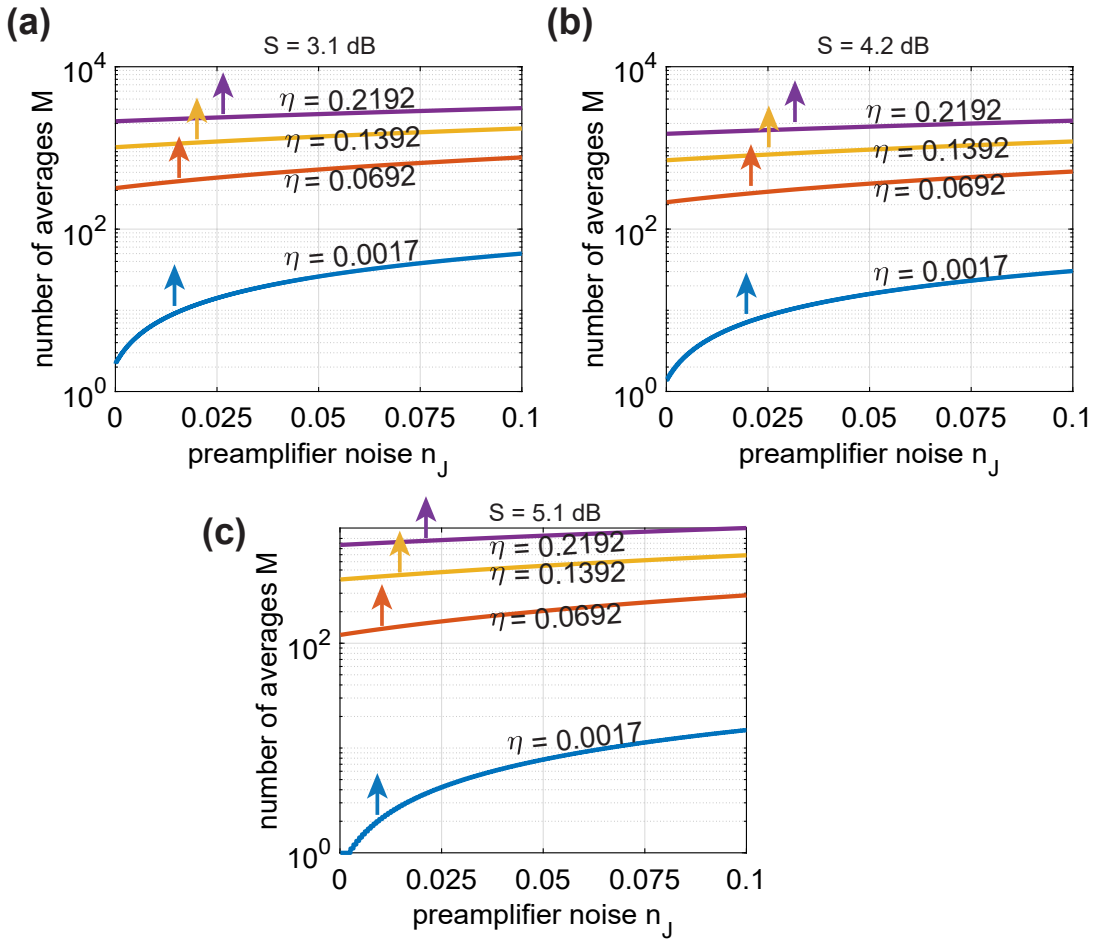


Figure 5.11: (a) Threshold values of M and n_J such that K becomes positive for $S = 3.1$ dB. Each line corresponds to a different coupled noise η. (b) Threshold values of M and n_J such that K becomes positive for $S = 4.2$ dB. Each line corresponds to a different coupled noise η. (c) Threshold values of M and n_J such that K becomes positive for $S = 5.1$ dB. Each line corresponds to a different coupled noise η. For each line, a coloured arrow indicates that the parameters above the curve correspond to a positive secret key and secure communication.

maximal tolerable preamplifer noise n_J. Therefore, we note in total three main ways to reduce the number of required averages M. First, as we mentioned, increase the squeezing level can be increased. Second, one can decrease the noise photon number n_J but Fig. 5.11 shows that this effect is limited and depends again on the squeezing level. Third, it is possible to increase the gain G_J. Indeed, the noise contribution of the HEMT enters as $n_\mathrm{H}/G_\mathrm{J} = 0.0027$ for the case $G_\mathrm{J} = 40\,\mathrm{dB}$ which is comparable to the coupled noise η.

Chapter 6

Conclusions and outlook

In this work, we have investigated, both theoretically and experimentally, a continuous-variable quantum key distribution (CV-QKD) protocol based on propagating displaced squeezed microwave states. To quantify security of this protocol, we have numerically calculated the secret key in the direct reconciliation (DR) and reverse reconciliation (RR) cases. The behaviour of the secret key rate versus the squeezing level S of the displaced squeezed states, as well as the transmissivity τ and noise η in the quantum channel, has been demonstrated. For the DR case, we have found that the communication is secure up to $\tau = 0.5$ and $\eta = 0.184$. This result can be interpreted that the protocol cannot be secure in the DR case if Eve gets more than 50 % of Alice's signals, because Eve substitutes Alice in this scenario. On the other hand, we have found that, in the RR case, the QKD protocol can remain secure up to infinitely large losses $\tau = 0$ and $\eta = 0.181$. This means that the RR case is not limited by losses.

Next, we have implemented and studied a simplified experimental realization of the aforementioned CV-QKD protocol in the microwave range. We have studied effects of the noise η in the quantum channel on the final secret key rate. This noise η has been used to emulate a collective attack from a potential eavesdropper Eve, which, in turn, allows for a flexible quantum experimental simulation of attacks with different strengths. Experimentally, propagating squeezed microwave states have been generated using a flux-driven Josephson parameter amplifiers (JPA), while the displacement, necessary for encoding of classical information, has been implemented with a cryogenic directional coupler. We have studied two different working points of our JPA (at the frequencies $f_0 = 5.350\,\mathrm{GHz}$ and $f_0 = 5.353\,\mathrm{GHz}$) which have demonstrated similar performance.

Main results of our experimental microwave QKD protocol have relied on the tomography of the propagating displaced squeezed states. From the corresponding tomography data, we have extracted both the mutual information between communication parties (Alice and Bob) in addition to Eve's Holevo quantity in the DR case. We have observed that Eve's Holevo quantity increases with the increasing coupled noise η, corresponding to a stronger eavesdropping attack and representing the increase of

information leaking to Eve. Surprisingly, we have observed that the measured mutual information between Alice and Bob does not depend on the coupled noise η but instead fluctuates around a mean value of 4.35 bits per channel usage. We explain this behaviour by a large averaging number $M_{\mathrm{avg}} = 2.094 \cdot 10^8$. These averages effectively suppress the noise in our signals, including the coupled noise η. Finally, the difference between the discussed mutual information and Eve's Holevo quantity allows us to estimate an upper bound of the secret key rate achievable in our experimental setting as a function of the coupled noise and squeezing level. These results are presented in Fig. 5.10 and provide a very promising perspective of microwave QKD protocols. To complete this analysis, we have repeated the measurements for the second working point $f_0 = 5.353$ GHz at different squeezing levels, $S = 3.1$ dB, $S = 4.2$ dB, and $S = 5.1$ dB. As the result, we have observed that Eve's Holevo quantity increases with both the squeezing level and coupled noise η. The respective secret key rate R increases with the increasing squeezing level S but decreases with the increasing coupled noise η, which underlines the fact that the mutual information between Alice and Bob grows with the increasing S than Eve's Holevo quantity. The same results have been obtained in theory (see Fig. 3.8 for more details).

In principle, excessive averaging number $M \gg 1$ must not be allowed in the QKD protocol due to its negative impact on the security. The impact of averaging on the measured Holevo quantity (and the final secret key rate) is not very well understood in theory at this moment. Therefore, we investigate our experimental setting by rescaling of the mutual information in order to estimate the protocol performance close to the single-shot readout regime $M \simeq 1$. To this end, we theoretically consider an additional JPA in the phase-sensitive regime acting as a low-noise preamplifier at Bob's side. This approach allows us to reduce the number of averages in our setup assuming large preamplifier gain G_{J} and low preamplifier noise n_{J}. Our results (see Fig. 5.11) shows that with a gain $G_{\mathrm{J}} = 40$ dB, we can already reduce the number of averages close to the single-shot regime $M \to 1$ for a noise n_{J} less than 0.025 noise photon. For the squeezing level $S = 5.1$ dB, we each the single-shot regime for a noise n_{J} less than 0.002 noise photon. Interestingly, higher squeezing levels alleviate conditions in terms of G_{J} and n_{J} required to reach the single-shot regime.

In the outlook, future experiments could include an additional JPA to perform a low-noise preamplification to reduce the number of averages M required for the secure communication. The ultimate goal would be to reduce M to one, while still being able to measure a positive secret key directly in the experimental setting. Furthermore, the current data analysis could be extended to the RR case in experiments. This could be done by applying the results of our current theory chapter. Overall, our experiments have demonstrated the potential of microwave quantum key distribution protocols and

will, hopefully, find its rightful place in quantum communication in the upcoming future.

Acknowledgments

In this part, I would like to thank all the people that contributed to this thesis.

To **Prof. Dr. Rudolf Gross**, for giving me the opportunity to do my master thesis in the qubit group at the Walther Meissner Institute. His impressive knowledge of Physics can only be rivalled by his general happy mood.

To **Dr. Kirill Fedorov**, for being my advisor throughout this work and providing a very useful proofreading of this thesis. He has always been there to answer my questions and to discuss with me, no matter how stubborn I could be. Many ideas in this thesis were born out of discussions with him. His numerous advices were particularly helpful for experimental work as well. I have learned a lot from him and he gave plenty of valuable knowledges, not only about Physics. I am ever so grateful of the attention and dedication he showed to my work. His commitment to work is nothing but inspiring.

To the PhD students, **Stefan Pogorzalek**, **Michael Renger**, and **Qi-Ming Chen**, for being very friendly and helpful throughout this work. They always helped me for whatever questions I had for them or for experimental work. In particular, I would like to thank Stefan very much for many discussions we had this year and all the help he provided. Many crucial problems in this thesis were also solved thanks to him. He also gave me plenty of practical help, let it be for the thesis or general advices. His always happy being makes him a great person to work with or to just be around.

To the qubit group in general, for being friendly and always pleasant to be with. Everyone was always open to talk or help, which made the atmosphere quite relaxing.

To the workshop team, for building various pieces that were necessary for this work and generally being always helpful.

To the everyone in WMI, for being generally nice people.

To my office collegue, **Manuel Müller**, **Leander Peis**, **Julia Lamprich**, **Stefan Trattnig**, **Christoph Scheuer**, **Carolina Lüthi**, **Elisabeth Meidinger** and all the other master students, for being always there and generally awesome. Their support has been amazing throughout this year. They personally cared and helped me many times when I needed and for that I truly thank them. I bow to Manuel, the meme God, for beating me at my own game and for being one of the most impressive persons I met in my life.

To my family, for always having my back and offering me the opportunity to do these studies. I would have been there without them. I love you all.

To my grand father, who past away during my studies.

Bibliography

[1] G. Wendin. Quantum information processing with superconducting circuits: a review. *Reports on Progress in Physics* **80**, 106001 (2017).

[2] S. Pirandola, B. R. Bardhan, T. Gehring, C. Weedbrook & S. Lloyd. Advances in photonic quantum sensing. *Nature Photonics* **12**, 724–733 (2018).

[3] S. Lloyd. Enhanced Sensitivity of Photodetection via Quantum Illumination. *Science* **321**, 1463–1465 (2008).

[4] N. Gisin & R. Thew. Quantum communication. *Nature Photonics* **1**, 165–171 (2007).

[5] L. Steffen, Y. Salathe, M. Oppliger, P. Kurpiers, M. Baur, C. Lang, C. Eichler, G. Puebla-Hellmann, A. Fedorov & A. Wallraff. Deterministic quantum teleportation with feed-forward in a solid state system. *Nature* **500**, 319–322 (2013).

[6] T. Koshiba. Quantum Cryptography **3-4**, 1521–1543 (2012).

[7] G. S. Vernam. Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications. *Transactions of the American Institute of Electrical Engineers* **XLV**, 295–301 (1926).

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

[9] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring 124–134 (2002).

[10] 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 & P. Wallden. Advances in Quantum Cryptography. *Advances in Optics and Photonics* 1–118 (2020).

[11] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus & M. Peev. The security of practical quantum key distribution. *Reviews of Modern Physics* **81**, 1301–1350 (2009).

[12] W. H. Zurek. [Letters to nature]. *Nature* **246**, 170 (1973).

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

[14] E. Diamanti & A. Leverrier. Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations. *Entropy* **17**, 6072–6092 (2015).

[15] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven & J. M. Martinis. Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019).

[16] L. S. Braunstein & P. Van Loock. Quantum information with continuous variables. *Reviews of Modern Physics* **77**, 513–577 (2005).

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

[18] L. Zhong, E. P. Menzel, R. Di Candia, P. Eder, M. Ihmig, A. Baust, M. Haeberlein, E. Hoffmann, K. Inomata, T. Yamamoto, Y. Nakamura, E. Solano, F. Deppe, A. Marx & R. Gross. Squeezing with a flux-driven Josephson parametric amplifier. *New Journal of Physics* **15**, 125013 (2013).

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

[20] K. G. Fedorov, L. Zhong, S. Pogorzalek, P. Eder, M. Fischer, J. Goetz, E. Xie, F. Wulschner, K. Inomata, T. Yamamoto, Y. Nakamura, R. Di Candia, U. Las Heras,

M. Sanz, E. Solano, E. P. Menzel, F. Deppe, A. Marx & R. Gross. Displacement of Propagating Squeezed Microwave States. *Physical Review Letters* **117**, 1–5 (2016).

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

[22] E. Wigner. On the quantum correction for thermodynamic equilibrium. *Physical Review* **40**, 749–759 (1932).

[23] M. Hillery, R. F. O'Connell, M. O. Scully & E. P. Wigner. Distribution functions in physics: Fundamentals. *Physics Reports* **106**, 121–167 (1984).

[24] 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**, 453–466 (1990).

[25] V. Bužek, G. Adam & G. Drobný. Quantum state reconstruction and detection of quantum coherences on different observation levels. *Physical Review A - Atomic, Molecular, and Optical Physics* **54**, 804–820 (1996).

[26] V. Bužek, G. Adam & G. Drobný. Reconstruction of wigner functions on different observation levels. *Annals of Physics* **245**, 37–97 (1996).

[27] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro & S. Lloyd. Gaussian quantum information. *Reviews of Modern Physics* **84**, 621–669 (2012).

[28] H. Nyquist. Thermal agitation of electric charge in conductors. *Physical Review* **32**, 110–113 (1928).

[29] M. G. Paris. Displacement operator by beam splitter. *Physics Letters, Section A: General, Atomic and Solid State Physics* **217**, 78–80 (1996).

[30] P. Yard. *Noncommutation and finite-timecorrelations with propagating quantummicrowave states*. Masters thesis, Technische Universität München (2016). URL `https://www.wmi.badw.de/publications/theses/Yard,Patrick_Masterarbeit_2016.pdf`.

[31] B. Yurke, L. R. Corruccini, P. G. Kaminsky, L. W. Rupp, A. D. Smith, A. H. Silver, R. W. Simon & E. A. Whittaker. Observation of parametric amplification and deamplification in a Josephson parametric amplifier. *Physical Review A* **39**, 2519–2533 (1989).

[32] E. A. Tholén, A. Ergül, E. M. Doherty, F. M. Weber, F. Grégis & D. B. Haviland. Nonlinearities and parametric amplification in superconducting coplanar waveguide resonators. *Applied Physics Letters* **90**, 253509 (2007).

[33] B. Abdo, O. Suchoi, E. Segev, O. Shtempluck, M. Blencowe & E. Buks. Intermodulation and parametric amplification in a superconducting stripline resonator integrated with a dc-SQUID. *EPL (Europhysics Letters)* **85**, 68001 (2009).

[34] B. D. Josephson. Possible new effects in superconductive tunnelling. *Physics Letters* **1**, 251–253 (1962).

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

[36] Michael Tinkham. Introduction to superconductivity / Michael Tinkham | National Library of Australia. URL `http://catalogue.nla.gov.au/Record/1834745` (1996).

[37] M. Sandberg, C. M. Wilson, F. Persson, T. Bauch, G. Johansson, V. Shumeiko, T. Duty & P. Delsing. Tuning the field in a microwave resonator faster than the photon lifetime. *Applied Physics Letters* **92**, 3–6 (2008).

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

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

[40] J. Bourassa, F. Beaudoin, J. M. Gambetta & A. Blais. Josephson-junction-embedded transmission-line resonators: From Kerr medium to in-line transmon. *Physical Review A - Atomic, Molecular, and Optical Physics* **86**, 1–13 (2012).

[41] M. Wallquist, V. S. Shumeiko & G. Wendin. Selective coupling of superconducting charge qubits mediated by a tunable stripline cavity. *Physical Review B - Condensed Matter and Materials Physics* **74**, 1–10 (2006).

[42] W. Wustmann & V. Shumeiko. Parametric resonance in tunable superconducting cavities. *Physical Review B - Condensed Matter and Materials Physics* **87**, 1–23 (2013).

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

[44] E. P. K. Menzel. *Propagating Quantum Microwaves: Dual-path State Reconstruction and Path Entanglement*. Diploma thesis, Technische Universität München (2013). URL https://www.wmi.badw.de/publications/theses/Menzel_Doktorarbeit_2013.pdf.

[45] S. Pogorzalek, K. G. Fedorov, L. Zhong, J. Goetz, F. Wulschner, M. Fischer, P. Eder, E. Xie, K. Inomata, T. Yamamoto, Y. Nakamura, A. Marx, F. Deppe & R. Gross. Hysteretic Flux Response and Nondegenerate Gain of Flux-Driven Josephson Parametric Amplifiers. *Physical Review Applied* **8**, 024012 (2017).

[46] C. M. Caves. Quantum limits on noise in linear amplifiers. *Physical Review D* **26**, 1817–1839 (1982).

[47] K. K. T. Yamamoto & Y. Nakamura. *Parametric Amplifer and Oscillator Based on Josephson Junction Circuitry* (Springer Japan, Tokyo, 2016). Edited by Y. Yamamoto and K. Semba.

[48] A. Baust. *Characterization of flux-driven Josephson parametric amplifiers*. Diploma thesis, Technische Universität München (2010).

[49] B. Bhushan, G. Sahoo & A. K. Rai. Man-in-the-middle attack in wireless and computer networking — A review 1–6 (2017).

[50] N. J. Cerf, A. Ipe & X. Rottenberg. Cloning of continuous quantum variables. *Physical Review Letters* **85**, 1754–1757 (2000).

[51] R. Garcia-Patron Sanchez. *Quantum Information with Optical Continuous Variables : from Bell Tests to Key Distributions*. Ph.D. thesis (2007). URL http://quic.ulb.ac.be/_media/publications/2007-thesis-raul.pdf.

[52] C. E. Shannon. A Mathematical Theory of Communication. *Bell System Technical Journal* **27**, 379–423 (1948).

[53] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin & P. Grangier. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Physical Review A - Atomic, Molecular, and Optical Physics* **76**, 1–10 (2007).

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

[55] R. Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics* **3**, 645–649 (2007).

[56] A. Einstein, B. Podolsky & N. Rosen. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Physical Review* **47**, 777–780 (1935).

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

[58] R. García-Patrón & N. J. Cerf. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Physical Review Letters* **97**, 1–4 (2006).

[59] S. Pirandola, S. L. Braunstein & S. Lloyd. Characterization of collective gaussian attacks and security of coherent-state quantum cryptography. *Physical Review Letters* **101**, 1–4 (2008).

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

[61] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri & P. Grangier. Virtual Entanglement and Reconciliation Protocols for Quantum Cryptography with Continuous Variables. *Quantum Information and Computation* **3**, 535–552 (2003).

[62] N. J. Cerf. Quantum Cloning with Continuous Variables **1**, 277–293 (2003).

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

[64] A. Serafini, F. Illuminati & S. D. Siena. Symplectic invariants, entropic measures and correlations of Gaussian states. *Journal of Physics B: Atomic, Molecular and Optical Physics* **37**, L21–L28 (2004).

[65] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii* **9**, 3–11 (1973).

[66] A. Leverrier, F. Grosshans & P. Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A* **81**, 062343 (2010).

[67] L. Ruppert, V. C. Usenko & R. Filip. Long-distance continuous-variable quantum key distribution with efficient channel estimation. *Physical Review A* **90**, 062310 (2014).

[68] R. Renner. Security of Quantum Key Distribution. *International Journal of Quantum Information* **06**, 1–127 (2008).

[69] I. Devetak & A. Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* **461**, 207–235 (2005).

[70] G. VanAssche, J. Cardinal & N. Cerf. Reconciliation of a Quantum-Distributed Gaussian Key. *IEEE Transactions on Information Theory* **50**, 394–400 (2004).

[71] C. Weedbrook, S. Pirandola & T. C. Ralph. Continuous-variable quantum key distribution using thermal states. *Physical Review A* **86**, 022318 (2012).

[72] R. García-Patrón & N. J. Cerf. Continuous-Variable Quantum Key Distribution Protocols Over Noisy Channels. *Physical Review Letters* **102**, 130501 (2009).

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

[74] S. Krinner, S. Storz, P. Kurpiers, P. Magnard, J. Heinsoo, R. Keller, J. Lütolf, C. Eichler & A. Wallraff. Engineering cryogenic setups for 100-qubit scale superconducting circuit systems. *EPJ Quantum Technology* **6**, 2 (2019).

[75] U. Leonhardt & M. Beck. Measuring the Quantum State of Light. *American Journal of Physics* **66**, 550–551 (1998).

[76] M. Sanz, K. G. Fedorov, F. Deppe & E. Solano. Challenges in Open-air Microwave Quantum Communication and Sensing 1–4 (2018).

[77] E. P. Menzel, R. Di Candia, F. Deppe, P. Eder, L. Zhong, M. Ihmig, M. Haeberlein, A. Baust, E. Hoffmann, D. Ballester, K. Inomata, T. Yamamoto, Y. Nakamura, E. Solano, A. Marx & R. Gross. Path Entanglement of Continuous-Variable Quantum Microwaves. *Physical Review Letters* **109**, 250502 (2012).

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

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

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

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

[82] S. Pogorzalek. *Displacement of squeezed propagating microwave states*. Masters thesis, Technische Universität München (2015). URL http://www.wmi.badw.de/publications/theses/Pogorzalek, Stefan_Masterarbeit_2015.pdf.