Technische Universität München | Walther-Meißner Institut | Bayerische Akademie der Wissenschaften

Microwave cryptography with propagating quantum tokens

Valentin Weidemann

Thesis submitted 12.12.2023
within the Master's Program Condensed Matter

Supervisor: Prof. Dr. Rudolf Gross
Advisor: Dr. Kirill Fedorov

December 12, 2023

Thesis advisor: Dr. Kirill Fedorov *Valentin Weidemann*

Microwave cryptography with propagating quantum tokens

ABSTRACT

In quantum cryptography, we aim to exploit the fundamental laws of quantum mechanics to guarantee secure transfer of data between two parties. In particular, we use that any information gained by an eavesdropper disturbs the received state by an amount quantifiable by both parties, therefore enabling us to bound the maximum eavesdropper information by measuring this perturbation. In this thesis, we implement a microwave continuous-variable quantum key distribution (CV-QKD) protocol based on Gaussian modulation of squeezed microwave states, which encodes information in the displacement of squeezed states. In our experimental implementation, we use a cryogenic microwave amplification chain consisting of a preamplifier Josephson-parametric-amplifier (JPA) and a phase-insensitive high-electron-mobility-transistor (HEMT) amplifier. As the main experimental result, we show that we can achieve a significant repetition rate increase by controllably modulating the input displacement power. This allows us to increase the secret key frequency by a factor of 6. In addition, we use the finite-size analysis outlined by Pirandola et al. [1] to show the expected channel uses required for secure key generation under the collective attack. In this regard we discuss possible further improvements leading to an increased repetition rate in order to reach channel uses on the order of one million in an experimental setting.

Contents

Chapter 1

Introduction

Within the past century, quantum information processing, a subfield of quantum theory, has attracted a great interest from both science and industry. Applications in this field, such as quantum computing [2], sensing [3], and communication [4] utilize fundamental features of quantum mechanics, such as quantum entanglement, the Heisenberg uncertainty, and superposition principle in order to gain an advantage over competing classical approaches and protocols. In this work we focus on quantum communication, in particular quantum cryptography. In modern classical communication, asymmetric algorithms, such as the RSA algorithm [5] use mathematical problems which are asymmetric, i.e., significantly more difficult to solve for an eavesdropper than for an authorized communication party. The implicit premise in this context is that classical algorithms are inefficient in solving these mathematical challenges. As a consequence, the restricted computational capacity of the eavesdropper ensures security. However it is often difficult to prove that such efficient classical algorithms do not exist. Moreover in the case of the RSA, there are algorithms utilizing quantum computers which can potentially solve the RSA underlying mathematical problem of the prime number factorization, namely, the Shor algorithm [6]. Since the RSA algorithm remains widely used in modern cryptography, the ongoing development of quantum computing represents a real threat to secure communication. For this reason, there has been a growing interest in the field of quantum cryptography. Here, secrecy of communication is guaranteed by quantum-mechanical laws. In particular, in quantum key distribution (QKD) schemes, one aims to distribute keys between two parties while a potential eavesdropper tries to gain information about the key. These schemes can achieve unconditional security even under assumption of unlimited computational power of the eavesdropper. One of the properties of quantum states enabling for this unconditional security is the no-cloning theorem that prohibits ideal copying of unknown quantum states. This implies that in order for the eavesdropper to gain information about the key, they would necessarily have to interact with the sent quantum states. This renders the eavesdropper presence detectable and quantifiable by the original communication parties. QKD protocols have many hardware platforms. However, historically, most QKD protocols have been implemented in the optical regime [7][8]. However, many modern classical communication protocols and platforms operate in the microwave GHz frequency range, making it important to implement QKD with propagating microwaves. In this work, we experimentally implement a CV-QKD protocol utilizing propagating squeezed microwave states by encoding classical key elements in displacement amplitudes of these squeezed states. We generate the squeezed states using Josephson parametric amplifiers (JPAs) and displace them using a highly asymmetric microwave beam splitter, known as a directional coupler. The resulting displaced squeezed states are sent along low-loss superconducting cables to another JPA acting as a single-shot quadrature measurement device. We extend this protocol further by implementing a displacement time-modulation scheme to controllably and quickly change the displacement amplitude during each measurement run to significantly speed

up the protocol and increase the secret key generation. In chapter 2, we introduce theoretical concepts, such as propagating quantum microwaves and a Josephson parametric amplifier, relevant to our experiments. Next, we also discuss a specific implementation of our CV-QKD protocol. In chapter 3, we present a related experimental setup, including a cryogenic apparatus needed to use our superconducting circuits. In addition we discuss calibration measurements necessary to choose optimal working conditions and fully characterize our quantum states. In chapter 4, we analyze the CV-QKD measurements in terms of signal-to-noise ratio, mutual information, and the Holevo bound. Finally, chapter 5 provides a summary of our results and gives an outlook of future improvements.

Chapter 2

Theory

In this chapter we discuss fundamental theory elements necessary for a QKD protocol. First, we discuss propagating quantum microwaves and Gaussian states. Secondly, we introduce a Josephson parametric amplifier (JPA). We additionally present the concept of a macroscopic wave function, a direct current superconducting quantum interference device (dc-SQUID), and the use of the JPA as an amplifier. In the next part, we introduce our quantum key distribution (QKD) protocol and discuss the principle of QKD with its corresponding underlying security analysis. We apply the security analysis to our specific QKD protocol and compare its performance with other common protocols. Finally, we discuss finite-size effects in our QKD protocol, arising from the finite amount of quantum states used during our QKD protocol implementation.

2.1 Propagating quantum microwaves

In this section we discuss a quantum-mechanical description of electromagnetic fields. First, we introduce electromagnetic fields. Secondly, we discuss a special type of quantum states called Gaussian states, as defined by their Gaussian Wigner function.

2.1.1 Quantized electromagnetic field

Microwaves are electromagnetic field oscillations with corresponding eigenfrequencies ranging from 300 MHz ($\approx$ 1 m wavelength) to 100 GHz ($\approx$ 3 mm wavelength). We can represent a single-mode electromagnetic field by $A(t) = A_0 \cos(\omega t + \varphi)$, with the amplitude A_0, the angular frequency ω, and the phase φ. Equivalently, we can write $A(t) = I(t)\cos(\omega t) + Q(t)\sin(\omega t)$, with the in-phase quadrature I and the out-of-phase quadrature Q. The single-mode quantized electromagnetic field is given by

$$\hat{E}(t) = E_0 \left(\hat{a}e^{i\omega t} + \hat{a}^\dagger e^{-i\omega t}\right) = 2E_0 \left(\hat{q}\cos(\omega t) + \hat{p}\sin(\omega t)\right), \tag{2.1}$$

with the bosonic annihilation and creation operators, $\hat{a}$ and $\hat{a}^\dagger$, the amplitude E_0, and the quadrature operators

$$\hat{q} = \frac{\hat{a} + \hat{a}^\dagger}{2}, \quad \hat{p} = \frac{\hat{a} - \hat{a}^\dagger}{2i}. \tag{2.2}$$

The corresponding quantum harmonic oscillator Hamiltonian is given by [9]

$$\hat{H} = \hbar\omega(\hat{a}^\dagger\hat{a} + \frac{1}{2}), \tag{2.3}$$

with the reduced Planck's constant $\hbar$. The creation and annihilation operators follow the bosonic commutation relation, $[\hat{a}, \hat{a}^\dagger] = 1$, and act on the Fock states, the eigenstates $|n\rangle$ with $n \in \mathbb{N}$ of

the quantum harmonic oscillator, as

$$\hat{a}^\dagger |n\rangle = \sqrt{n+1}\,|n+1\rangle\,, \quad \hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle\,. \tag{2.4}$$

From the bosonic commutation relation we compute that $[\hat{q}, \hat{p}] = i/2$, which implies for the Heisenberg uncertainty relation [10]

$$\mathrm{Var}(\hat{q})\,\mathrm{Var}(\hat{p}) \geq \frac{1}{16}, \tag{2.5}$$

with the variance defined as $\mathrm{Var}(\hat{O}) = \langle \hat{O}^2 \rangle - \langle \hat{O} \rangle^2$. Thus, it is not possible to measure both quadratures of the single-mode electromagnetic field simultaneously with an arbitrary precision.

2.1.2 Gaussian states

Wigner function The density matrix of a given quantum state is defined as

$$\hat{\rho} = \sum_i^N p_i\,|\psi_i\rangle\,\langle\psi_i|\,, \tag{2.6}$$

where p_i is the probability of the system being in the corresponding pure state $|\psi_i\rangle$ and N is the Hilbert space dimension. In this work we primarily deal with a subclass of quantum states, called Gaussian states. Gaussian states have a continuous eigenspectrum and, as such, are described in an infinite-dimensional Hilbert space. Consequently, the density matrix formalism is not the most suitable formalism for manipulation or computation based on Gaussian states. In the following we introduce a more intuitive formalism that consists of the Wigner function $W(q,p)$, defined for a given density matrix $\hat{\rho}$ as [11]

$$W(q,p) = \frac{1}{\pi\hbar}\int \langle q-y|\hat{\rho}|q+y\rangle\, e^{2ipy/\hbar}\mathrm{d}y. \tag{2.7}$$

One can show that the following holds:

$$\int W(q,p)\,\mathrm{d}q\,\mathrm{d}p = 1, \tag{2.8}$$

$$\int W(q,p)\,\mathrm{d}q = \langle p|\hat{\rho}|p\rangle\,, \quad \int W(q,p)\,\mathrm{d}p = \langle q|\hat{\rho}|q\rangle\,. \tag{2.9}$$

The Wigner function exhibits similar properties of a joint probability distribution of q and p. However the Wigner function, in general, is not positive, $W(q,p) > 0$. For this reason, the Wigner function is called a quasi-probability distribution and allows for efficient computation of quantum operator actions on quantum states.

Statistical moments and Gaussian states A N-mode Gaussian state has a Wigner function of the form [12]

$$W(\mathbf{r}) = \frac{1}{(2\pi)^N\sqrt{\det(\boldsymbol{V})}}\exp\left(-\frac{1}{2}(\mathbf{r}-\bar{\mathbf{r}})\boldsymbol{V}^{-1}(\mathbf{r}-\bar{\mathbf{r}})^T\right), \tag{2.10}$$

with the number of modes N, the covariance matrix $\boldsymbol{V} = (V_{ij}) \in \mathbb{R}^{2N\times 2N}$, with $i,j = 1...2N$, the phase-space vector $\mathbf{r} = (\hat{q}_1, \hat{p}_1, ..., \hat{q}_N, \hat{p}_N)$, and the displacement vector $\langle\bar{\mathbf{r}}\rangle = (\langle\hat{q}_1\rangle, \langle\hat{p}_1\rangle, ..., \langle\hat{q}_N\rangle, \langle\hat{p}_N\rangle)$. The covariance matrix elements are given by

$$V_{ij} = \frac{\langle\hat{\mathbf{r}}_i\hat{\mathbf{r}}_j + \hat{\mathbf{r}}_j\hat{\mathbf{r}}_i\rangle}{2} - \langle\hat{\mathbf{r}}_i\rangle\langle\hat{\mathbf{r}}_j\rangle . \tag{2.11}$$

The knowledge of the covariance matrix and displacement vector is sufficient to fully describe any N-mode Gaussian quantum state. We can express the purity of a Gaussian stateas:

$$\mu = \mathrm{Tr}(\hat{\rho}^2) = \frac{1}{4^N\sqrt{\det(\boldsymbol{V})}}. \tag{2.12}$$

The purity is an indicator for the "mixedness" of a quantum state, with $\mu = 1$ indicating a pure state and $\mu = 0$ meaning that the quantum state is a fully mixed state. For Gaussian states, such state would correspond to a thermal state (see Fig. 2.1(b)) with infinite amount of noise.

Average states In this work we deal with quantum states $|\psi_i\rangle$ that are drafted from a fixed probability distribution p_i, with $i = 1...M$. The corresponding average density matrix is defined as

$$\hat{\rho}_{\text{avg}} = \sum_{i=1}^{M} p_i\hat{\rho}_i, \tag{2.13}$$

with the density matrix $\hat{\rho}_i$ corresponding to the probability p_i. We compute the average signal moments associated with the average density matrix $\hat{\rho}_{\text{avg}}$ as

$$\langle(\hat{a}^\dagger)^m\hat{a}^n\rangle_{\text{avg}} = \mathrm{Tr}\left((\hat{a}^\dagger)^m\hat{a}^n\hat{\rho}_{\text{avg}}\right) = \sum_{i=1}^{M} p_i\,\mathrm{Tr}\left((\hat{a}^\dagger)^m\hat{a}^n\hat{\rho}_i\right) = \sum_{i=1}^{M} p_i\,\langle(\hat{a}^\dagger)^m\hat{a}^n\rangle_i , \tag{2.14}$$

with $m,n \in \mathbb{N}_0^2$ and the signal moments $\langle(\hat{a}^\dagger)^m\hat{a}^n\rangle_i$ associated to the individual state $\hat{\rho}_i$. Using Eq. 2.14 we can compute the average signal moments with the individual signal moments and, therefore, the average covariance matrix, which will be used in later sections.

Vacuum and thermal states The vacuum state, with its Wigner function shown in Fig. 2.1(a), is the lowest energy state of a bosonic mode and saturates the uncertainty relation. This state is described by

$$\bar{\mathbf{r}}_{\text{vac}} = 0, \quad \mathbf{V}_{\text{vac}} = \frac{\mathbb{1}}{4}, \tag{2.15}$$

with the identity matrix $\mathbb{1}$. Since the vacuum state is the lowest energy state, it corresponds to a field mode with temperature $T = 0$ K. In reality, we always have a finite non-zero temperature in our physical systems with an associated finite number of thermal noise photons $\overline{n}_{\text{th}}$ that follow the Bose-Einstein statistics [13]

$$\overline{n}_{\text{th}} = \frac{1}{\exp(\hbar\omega\beta) - 1}, \tag{2.16}$$

with $\beta = 1/(k_{\text{B}}T)$. The Wigner function of an exemplary thermal state is shown in Fig. 2.1(b) and the state is described by [12]

$$\bar{\mathbf{r}}_{\text{th}} = 0, \quad \mathbf{V}_{\text{th}} = (1 + 2\overline{n}_{\text{th}})\frac{\mathbb{1}}{4}. \tag{2.17}$$

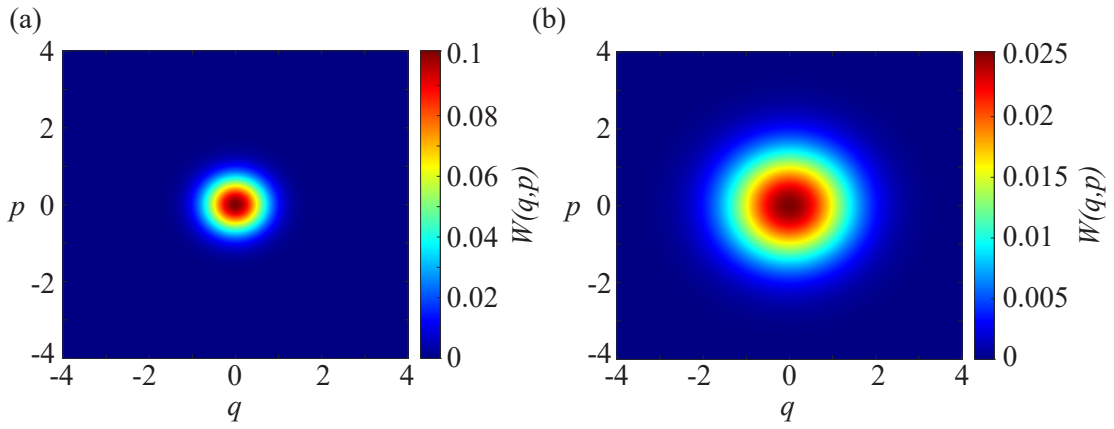

Figure 2.1: Wigner functions of the vacuum state (a) and the thermal state (b) with $\overline{n}_{\text{th}} = 1.5$. We observe a rotational symmetry in phase space for these states and the expected increase in quadrature variance with added thermal noise photons.

However, for $\hbar\omega\beta \gg 1$, we can approximate a thermal state as the vacuum state. In our experiments, we operate frequencies of $\omega/2\pi \sim 5$ GHz in a cryogenic environment at $T \sim 15$ mK. We compute $\hbar\omega\beta \sim 16 \gg 1$, which justifies the approximation of the thermal state as the vacuum state.

Coherent states Coherent states $|\alpha\rangle$ are defined as eigenstates of the annihilation operator $\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle$, for a given complex number α, commonly referred to as a displacement complex amplitude. [14]. An exemplary coherent state Wigner function is shown in Fig. 2.2(a). With the displacement operator

$$\hat{D}(\alpha) = \exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a}), \tag{2.18}$$

one can show that $|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle$. A coherent state is described by [12]

$$\bar{\mathbf{r}}_{\text{coh}} = (\text{Re}(\alpha), \text{Im}(\alpha)), \quad \mathbf{V}_{\text{coh}} = \frac{\mathbb{1}}{4}, \tag{2.19}$$

meaning that it can be viewed as the vacuum state which has been displaced in the quadrature phase space. The phase of the displacement complex α amplitude corresponds to the displacement angle, while the magnitude of α gives the length of the displacement in the phase space. Experimentally, we obtain coherent states with a directional coupler, which acts as a highly asymmetric microwave beamsplitter, where a strong coherent state is sent to the weakly-coupled port. The output signal is then [15][16]

$$\hat{a}_{\text{out}} = \sqrt{\tau}\hat{a}_{\text{in}} + \sqrt{1-\tau}\hat{a}_{\text{coh}}. \tag{2.20}$$

For $\tau \to 1$ and for coherent states with large amplitudes, this transforms to

$$\hat{a}_{\text{out}} = \hat{a}_{\text{in}} + \sqrt{1-\tau}\tilde{\alpha} = \hat{a}_{\text{in}} + \alpha, \tag{2.21}$$

where $\tilde{\alpha}$ is the displacement complex amplitude of the strong coherent state and α the resulting output displacement.

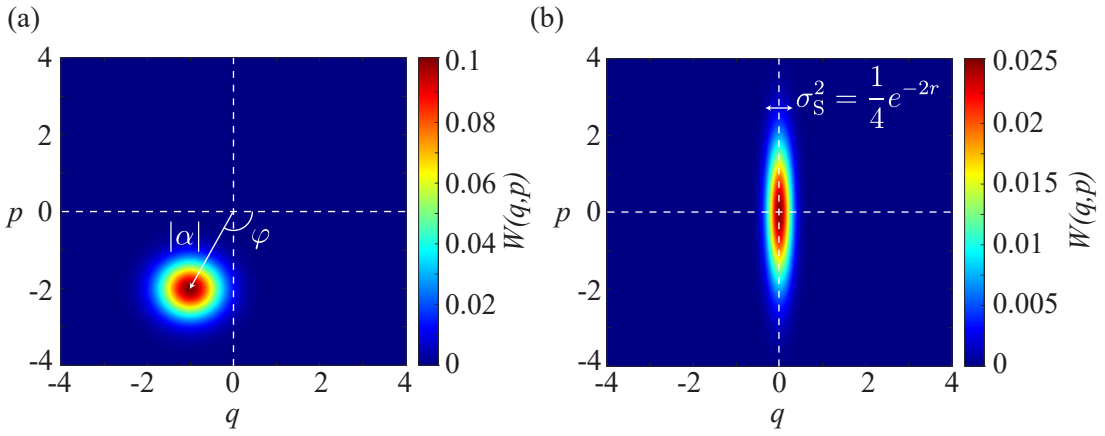

Figure 2.2: Wigner functions of the coherent and squeezed states. (a) Coherent state with $\alpha = -1 - 2i$. We observe the shifted expectation value of the quadratures, $\langle q \rangle = -1$, $\langle p \rangle = -2$. (b) Squeezed state with the squeezing level of $S = 8$ dB and squeezing angle of $\varphi = 0°$. We observe the decrease in the squeezed quadrature variance q and increase in the antisqueezed quadrature variance p.

Single-mode squeezed states The single-mode squeezing operator is defined as [9]

$$\hat{S}(\xi) = \exp\left[\frac{1}{2}(\xi^* \hat{a}^2 - \xi(\hat{a}^\dagger)^2)\right]. \tag{2.22}$$

The complex squeezing factor $\xi = re^{i\varphi}$ describes the squeezing effect with a magnitude r and the orientation in phase space with the phase φ. The single-mode squeezing operator is a mathematical tool to describe the effectively observed squeezed state but is not fully physical since it does not consider bandwidth effects. The single-mode squeezed state is then described by [16]

$$\bar{\mathbf{r}}_S = 0, \quad \mathbf{V}_S = \frac{1}{4}\begin{pmatrix} e^{-2r}\cos^2(\frac{\varphi}{2}) + e^{2r}\sin^2(\frac{\varphi}{2}) & \sin(\varphi)\sinh(2r) \\ \sin(\varphi)\sinh(2r) & e^{2r}\cos^2(\frac{\varphi}{2}) + e^{-2r}\sin^2(\frac{\varphi}{2}) \end{pmatrix}. \tag{2.23}$$

The Wigner function of an exepmlary squeezed state is shown in Fig. 2.2(b). In our use case, we restrict ourselves during some measurements to $\varphi \in \{0, \pi\}$, which simplifies the covariance matrix to $\mathrm{diag}(\sigma_S^2, \sigma_{AS}^2)$ for $\varphi = 0$, with $\sigma_S^2 = e^{-2r}/4$ and $\sigma_{AS}^2 = e^{2r}/4$. To characterize squeezed states, one commonly uses the squeezing level S and antisqueezing level A, defined as

$$S = -10\log_{10}\left(\frac{\sigma_S^2}{0.25}\right), \quad A = 10\log_{10}\left(\frac{\sigma_{AS}^2}{0.25}\right), \tag{2.24}$$

where 0.25 corresponds to the vacuum state variance.

Two-mode squeezed states The two-mode squeezed (TMS) states are entangled states that are related to the Einstein-Podolsky-Rosen states, in the context for continuous variables quantum states. The TMS states are used in optimal collective attacks from an eavesdropper, as discussed in Sec. 2.3.1. The two-mode squeezing operator is defined as [9]

$$\hat{S}_{1,2}(\xi) = \exp(\xi^* \hat{a}_1 \hat{a}_2 - \xi \hat{a}_1^\dagger \hat{a}_2^\dagger), \tag{2.25}$$

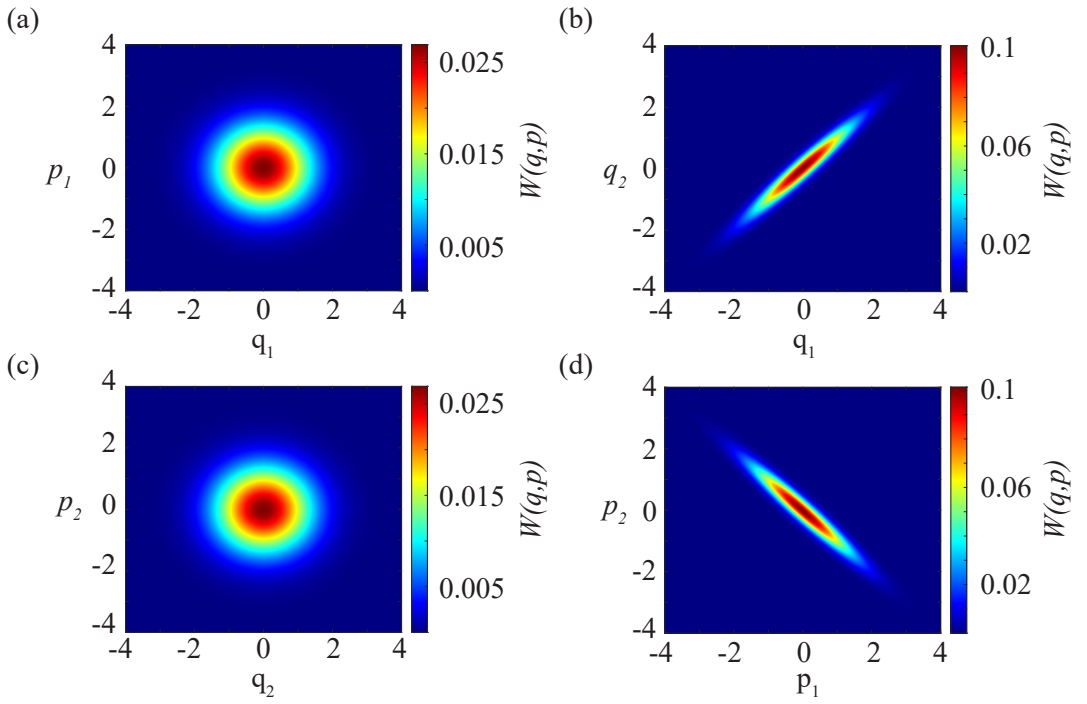

Figure 2.3: Marginal Wigner function distributions $W(q_1, p_1)$ in panel (a), $W(q_1, q_2)$ in panel (b), $W(q_2, p_2)$ in panel (c), and $W(p_1, p_2)$ in panel (d).

with the annihilation operators $\hat{a}_1, \hat{a}_2$ for the first and second modes. The TMS state in the Fock basis is given by [12]

$$|\nu\rangle = \sum_n \frac{(e^{-i\varphi}\tanh(r))^n}{\cosh(r)} |n, n\rangle\,, \tag{2.26}$$

where $\xi = re^{i\varphi}$. A TMS vacuum state can be represented by [12]

$$\bar{\mathbf{r}}_{\text{TMSVS}} = 0, \quad \mathbf{V}_{\text{TMSVS}} = \frac{1}{4}\begin{pmatrix} \cosh(2r) & 0 & \sinh(2r) & 0 \\ 0 & \cosh(2r) & 0 & -\sinh(2r) \\ \sinh(2r) & 0 & \cosh(2r) & 0 \\ 0 & -\sinh(2r) & 0 & \cosh(2r) \end{pmatrix}. \tag{2.27}$$

We observe that when $\cosh(2r) = (1 + 2\overline{n}_{\text{th}})/4$, each mode exhibits characteristics akin to a local thermal state. The marginal distributions of a TMS state are shown in Fig. 2.3. We observe a local thermal state for each mode and positive covariance between q_1 and q_2 and negative covariance between p_1 and p_2. The Pearson correlation coefficient of two random variables X, Y is related to the covariance and variance as

$$r_{xy} = \frac{\text{Cov}(X, Y)}{\sqrt{\text{Var}(X)\,\text{Var}(Y)}}, \tag{2.28}$$

and takes values from -1 to 1, where -1 or 1 indicates a linear relation between X and Y with incline -1 or 1, respectively. For the TMS state we compute

$$r_{q_1q_2} = \frac{\sinh(2r)}{\cosh(2r)}, \quad r_{p_1p_2} = -\frac{\sinh(2r)}{\cosh(2r)}. \tag{2.29}$$

For $r \to \infty$ we observe that $r_{q_1 q_2} \to 1$ and $r_{p_1 p_2} \to -1$, i.e. the quadratures are perfectly correlated in the limit of infinite two-mode squeezing.

Gaussianity check Given data samples $\{x_i\}_{i=1...N}$, we check whether or not measured data is Gaussian or not within a given confidence level α. To this end we introduce three test statistics in this work. First, we discuss the Jarque-Bera test [17]. Its test quantity, which maps the data to a single number with a certain distribution, is defined as

$$JB = \frac{N}{6}\left(S^2 + \frac{1}{4}(K-3)^2\right), \tag{2.30}$$

with the skewness S and kurtosis K defined as

$$S = \frac{\mu_3}{\sigma^3} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \overline{x})^3}{\left(\frac{1}{N}\sum_{i=1}^{N}(x_i - \overline{x})^2\right)^{3/2}}, \tag{2.31}$$

$$K = \frac{\mu_4}{\sigma^4} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \overline{x})^4}{\left(\frac{1}{N}\sum_{i=1}^{N}(x_i - \overline{x})^2\right)^{2}}. \tag{2.32}$$

The test quantity was obtained by a maximum-likelyhood approach [17]. If the data samples follow a Gaussian distribution, the skewness is 0 and the kurtosis is 3 in the asymptotic case, resulting in $JB = 0$ with a chi-square distribution with two degrees of freedom, with its probability density function

$$\chi^2(x) = \frac{1}{2}e^{-x^2/2}. \tag{2.33}$$

We note that for a small number of samples ($N < 2000$) the chi-square distribution is an insufficient approximation of the distribution of the JB test quantity and in this case the critical value is computed via Monte-Carlo simulations. In Monte-Carlo simulations with simulation size k the critical test quantity JB_{C} for a given sample size N is computed by computing the test quantity for k data sets that are drafted from the Gaussian distribution. We end up with k test quantities $\{JB_i\}_{i=1...k}$. The critical test quantity for a confidence level of $\tilde{\alpha}$ is then given by the interval $[0, JB_{\mathrm{C}}]$ which contains $1-\tilde{\alpha}$ of the computed test quantities $\{JB_i \mid JB_i < JB_{\mathrm{C}}\}$. In other words, $\tilde{\alpha}$ gives the probability of the test quantity exceeding the criticial quantity even when the dataset was drafted from the Gaussian distribution $\tilde{\alpha} = P(JB > JB_{\mathrm{C}}|H)$, i.e. the probability of a false rejection of the gaussianity hypothesis H. Secondly, we introduce the Anderson-Darling test [18]. The Anderson-Darling test quantity A assesses if the data is sampled from a distribution with a cumulative distribution function (CDF) F and is defined as

$$A^2 = -N - \sum_{i=1}^{N}\frac{2i-1}{N}\left[\ln(F(x_i)) + \ln(1 - F(x_{n+1-i}))\right], \tag{2.34}$$

where the data samples must be sorted, i.e. $x_1 < ... < x_N$. For a given theoretical distribution with CDF F, the values of A^2 is compared to critical values associated with a chosen confidence parameter $\tilde{\alpha}$ given some confidence interval. If the computed value A^2 falls above the critical value $A^2_{\tilde{\alpha}}$ for the chosen confidence level, then the null hypothesis that the data is drafted from the probability distribution with CDF F is rejected. For example, the critical value for $\tilde{\alpha} = 0.05$

is $A^2_{0.05} = 0.683$ in the case of the Gaussian distribution with an unknown variance and mean [19]. Lastly, we introduce the Shapiro-Wilk test [20]. Its test quantity is defined as

$$W = \frac{\left(\sum_{i=1}^{N} a_i x_{(i)}\right)^2}{\sum_{i=1}^{N}(x_i - \overline{x})^2}, \tag{2.35}$$

where $x_{(i)}$ is the i-th order statistic, i.e. the i-th smallest value of $\{x_i\}_{i=1...N}$ and

$$(a_1, ..., a_N) = \frac{m^T V^{-1}}{C}, \tag{2.36}$$

where $m = (m_1, ..., m_N)^T$ is the expected values of the order statistics of the standard normal distribution and V is the corresponding covariance matrix of those normal order statistics [21]. The cutoff values for W are calculated using Monte Carlo simulations.

2.2 Josephson parametric amplifier

In this section, we discuss flux-driven Josephson parametric amplifiers (JPAs). JPAs are commonly operated in the phase-sensitive regime, which is used for generation of microwave squeezed vacuum states and for quantum state readout. First, we discuss the working principle of a JPA. We explain basics about Josephson junctions and a direct current superconducting quantum interference device (dc-SQUID) that acts as a flux-tuneable inductance. Then, we discuss parametric amplification in the form of non-degenerate and degenerate amplification.

2.2.1 Josephson junctions and dc-SQUID

Macroscopic wave function Josephson junctions are crucial for the JPA nonlinear properties. They are made of two superconductors weakly coupled together with, typically, an insulating layer in between. To describe these junctions, we introduce a macroscopic wavefunction $\psi(\mathbf{r}, t) = \sqrt{n(\mathbf{r}, t)}e^{i\theta(\mathbf{r},t)}$ where n denotes the Cooper pair density in the superconductors [22] and θ is the phase of the macroscopic wavefunction. With this, we can write the first and second Josephson equations [22][23]

$$I_S = I_C \sin(\varphi), \quad \frac{\partial \varphi}{\partial t} = \frac{2\pi}{\Phi_0} V(t), \tag{2.37}$$

with the Josephson junction critical current I_C, the flux quantum $\Phi_0 = h/2e$, the voltage across the junction $V(t)$, and the gauge-invariant phase difference

$$\varphi = \theta_2(\mathbf{r}, t) - \theta_1(\mathbf{r}, t) - \frac{2\pi}{\Phi_0}\int_1^2 \mathbf{A}(\mathbf{r}, t) \cdot \mathrm{d}\mathbf{l}, \tag{2.38}$$

with the vector potential $\mathbf{A}$. An exemplary Josephson junction is shown schematically in Fig. 2.4(a), where two superconductors S_1 and S_2 are coupled through an insulating barrier I. With the definition of the inductance L as $V = LdI/dt$ and by inserting the first Josephson equation, we compute [22]

$$L_S = \frac{L_C}{\cos(\varphi)}, \tag{2.39}$$

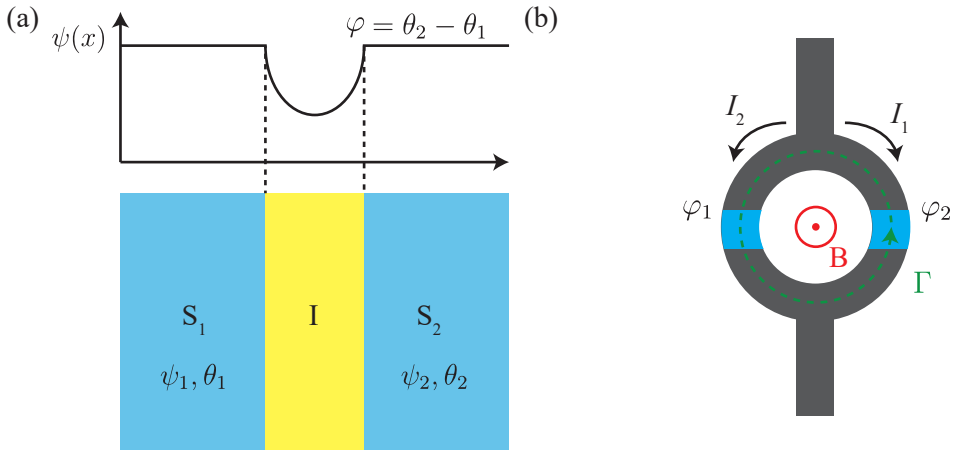

Figure 2.4: (a) Schematic of a Josephson junction with superconductors S_1 and S_2 weakly coupled via an insulator I. (b) Schematic of an exemplary dc-SQUID with one Josephson junction in each arm with the corresponding phase differences φ_1, φ_2 and currents I_1, I_2. The integral contour Γ, which we use in the derivation of equation Eq. 2.42, is shown in green.

where $L_C = \Phi_0/(2\pi I_C)$. In addition, with the macroscopic wavefunction, one can find for the supercurrent density:

$$\mathbf{J}_S = 2e\, n(\mathbf{r},t) \left(\frac{\hbar}{m_e} \nabla\theta(\mathbf{r},t) - \frac{2e}{m_e} \mathbf{A}(\mathbf{r},t) \right), \tag{2.40}$$

with the electron mass m_e.

dc-SQUID A typical dc-SQUID configuration can be seen in Fig. 2.4(b). Such a device is composed of two Josephson junctions in a ring made of superconducting material. If we assume the thickness of this ring to be greater than the London penetration depth [22], the superconducting current density will be vanishingly small in the middle of the superconducting leads. We further approximate a constant Cooper pair density n_S along this ring. With this, we can approximate equation Eq. 2.40 to [22]

$$\nabla\theta = \frac{2\pi}{\Phi_0} \mathbf{A}. \tag{2.41}$$

Then, by integrating along the inner ring contour Γ, shown in green in Fig. 2.4(b), we compute

$$\varphi_2 - \varphi_1 = \frac{2\pi\Phi}{\Phi_0} + 2\pi n, \tag{2.42}$$

where $\varphi_{1,2}$ is the gauge-invariant phase difference across the respective Josephson junction in the ring. We decompose the total flux Φ into an external flux and a self-induced flux caused by circulating currents

$$\Phi = \Phi_{\text{ext}} + L_{\text{loop}} I_{\text{cir}}, \tag{2.43}$$

with the circulating current $I_{\text{cir}} = (I_1 - I_2)/2$, and the geometric loop inductance L_{loop}. We can insert equation Eq. 2.43 in equation Eq. 2.42. By inserting the first Josephson equation for both

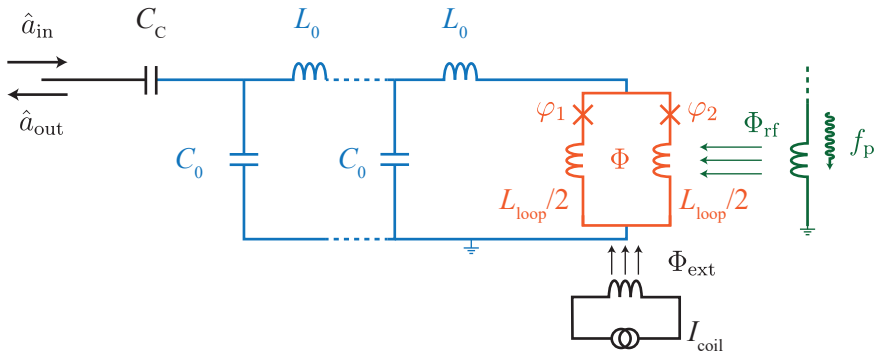

Figure 2.5: Circuit schematic of a Josephson parametric amplifier. A coupling capacitance C_{C} couples the input signal to the CPW (blue) with a unit inductance and capacitance L_0, C_0. The CPW is shorted to ground with a dc-SQUID (orange). The flux Φ in the dc-SQUID can be controlled with an external bias flux Φ_{ext} provided by a coil. The parametric amplification effect is induced by an inductively coupled pump line modulating the flux in the dc-SQUID by Φ_{rf}.

I_1 and I_2, we find:

$$\frac{\Phi}{\Phi_0} = \frac{\Phi_{\text{ext}}}{\Phi_0} - \frac{\beta_L}{2}\cos\left(\frac{\varphi_1+\varphi_2}{2}\right)\sin\left(\frac{\varphi_1-\varphi_2}{2}\right), \tag{2.44}$$

with the screening parameter $\beta_L = 2L_{\text{loop}}I_C/\Phi_0$. Here, we also assume that both junctions have the same critical currents. In the case of $\beta_L \approx 0$, we can obtain $\Phi = \Phi_{\text{ext}}$. The dc-SQUID acts like one effective Josephson junction with a flux-dependent maximum supercurrent:

$$I_s^m = 2I_C\left|\cos\left(\pi\frac{\Phi_{\text{ext}}}{\Phi_0}\right)\right|. \tag{2.45}$$

From here, we calculate an associated nonlinear inductance:

$$L_S(\Phi_{\text{ext}}) = \frac{\Phi_0}{4\pi I_C\left|\cos\left(\frac{\Phi_{\text{ext}}}{\Phi_0}\right)\right|}. \tag{2.46}$$

We see that the dc-SQUID acts like a flux-tuneable inductance in the case of $\beta_L \approx 0$. For $\beta_L \geq 1$, one needs to numerically simulate the system since an analytical expression cannot be found due to non-negligible self-induced flux, which causes the resulting equation to become transcendental.

Josephson parametric amplifier A particular design of flux-driven JPA is schematically shown in Fig. 2.5. It consists of a coupling capacitor, a coplanar waveguide (CPW) resonator and a dc-SQUID. The CPW can be treated as a quasi one-dimensional lossless transmission line [24] with a characteristic impedance $Z = \sqrt{L_0/C_0}$, where L_0 and C_0 are the inductance and capacitance per unit length. The CPW is capacitively coupled to the input line at one end and shorted to the ground by the dc-SQUID on the other end, the distance between them defining an electric length d of the CPW. The total inductance and capacitance are given by $L_r = d \cdot L_0$ and $C_r = d \cdot C_0$. Resonators are characterized by their internal and external coupling rates, which are

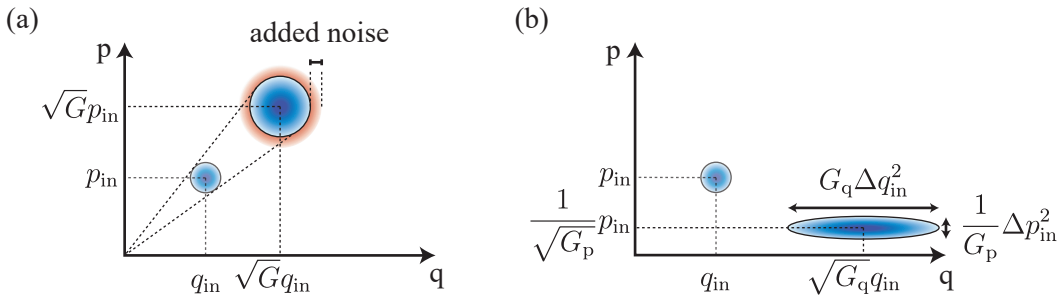

Figure 2.6: Illustration of amplification of signals using linear amplifiers. (a) Non-degenerate, or phase-insensitive, amplification. Both quadratures are amplified equally and, at least, half a noise photon is added in the limit of large amplification gain, $G \gg 1$. (b) Degenerate, or phase-sensitive, amplification. One quadrature is amplified with the gain G_{q}, the other is deamplified with the gain G_{p}. For $G_{\mathrm{p}}G_{\mathrm{q}} = 1$, the amplification is noiseless.

related to internal losses and external losses, respectively. Typically, one aims at minimizing the internal loss rate, κ_{int}. We note that even with superconducting materials, two-level fluctuations [25], surface resistance [26], and eddy currents [27] cause finite internal losses. Probing the $d = \lambda/4$ resonator with a microwave tone results in the complex reflection coefficient [28]

$$\Gamma = \frac{(\omega-\omega_0)^2 + i\kappa(\omega-\omega_0) + (\kappa_{\mathrm{ext}}^2 - \kappa_{\mathrm{int}}^2)/4}{((\omega-\omega_0) + i(\kappa_{\mathrm{ext}}+\kappa_{\mathrm{int}})/2)^2}, \tag{2.47}$$

with the internal and external loss rates $\kappa_{\mathrm{int}}, \kappa_{\mathrm{ext}}$, and the angular resonance frequency ω_0. The total resonance frequency, $\omega_0/2\pi$, of the CPW is

$$\frac{\pi\omega_0}{2\omega_{\mathrm{res}}}\tan\left(\frac{\pi\omega_0}{2\omega_{\mathrm{res}}}\right) = \frac{8\pi^2}{\Phi_0^2}L_{\mathrm{res}}E_{\mathrm{s}}(\Phi_{\mathrm{ext}}) - 2\frac{C_{\mathrm{s}}}{C_{\mathrm{res}}}\left(\frac{\pi\omega_0}{2\omega_{\mathrm{res}}}\right)^2, \tag{2.48}$$

where $\omega_{\mathrm{res}}/2\pi$, L_{res}, and C_{res} are the frequency, inductance, and capacitance of the CPW resonator without the SQUID, respectively, and C_{s} is the capacitance of the single Josephson junction. Additionally $E_{\mathrm{s}}(\Phi_{\mathrm{ext}})$ is the flux-dependent energy of the dc-SQUID given by [16]

$$E_{\mathrm{s}}(\Phi_{\mathrm{ext}}) = \frac{\Phi_0^2}{(2\pi)^2}\frac{1}{L_{\mathrm{s}}(\Phi_{\mathrm{ext}} + L_{\mathrm{loop}}/4)}. \tag{2.49}$$

2.2.2 Non-degenerate and degenerate amplification

Non-degenerate amplification The effect of non-degenerate amplification is schematically shown in Fig. 2.6(a). We show that the non-degenerate, or phase-insensitive, amplification adds at least half a noise photon to the input signal, referred to as the standard quantum limit (SQL). The Caves theorem [29] asserts that the bosonic commutation relation, $\left[\hat{a}_{\mathrm{out}}, \hat{a}_{\mathrm{out}}^\dagger\right] = 1$, of output modes $\hat{a}_{\mathrm{out}}$ is satisfied only when an extra idler mode $\hat{b}_{\mathrm{in}}$ is introduced. With this, the amplification relation is given by

$$\hat{a}_{\mathrm{out}} = \sqrt{G}\,\hat{a}_{\mathrm{in}} + \sqrt{G-1}\,\hat{b}_{\mathrm{in}}^\dagger. \tag{2.50}$$

The input-output relation of any bosonic amplifier is thus composed of two different modes: the signal and the idler. With this, the lower bound for the added noise referred to the input is given by

$$\overline{n} = \sqrt{1 - \frac{1}{G}}\,\langle \hat{b}_{\text{in}}^{\dagger}\hat{b}_{\text{in}}\rangle \geq \frac{1}{2}\left|1 - \frac{1}{G}\right|, \tag{2.51}$$

with the amplifier gain G and the average added noise photon number $\overline{n}$. A typical phase-insensitive amplifier, such as a high-electron-mobility-transistor (HEMT), adds 10-20 noise photons referred to the input.

Degenerate amplification Degenerate amplification is schematically shown in Fig. 2.6(b). Unlike phase-insensitive amplification, phase-sensitive amplification has the potential to noiselessly amplify input signals. We show that a significant advantage can obtained by using such amplifiers at the first stage in an amplification chain. We discuss here a 3-wave mixing process in the flux-driven JPAs which are presented above. We adjust the pump frequency to twice the signal frequency, $\omega_{\text{p}} = 2\omega_{\text{s}}$, to produce degenerate frequencies for both the signal and the idler mode $\omega_{\text{s}} = \omega_{\text{i}}$. In this case, the idler mode can be expressed as a phase-shifted signal mode, which enables constructive or destructive interferences. We obtain the input-output relation for phase-sensitive amplification [30]

$$\hat{a}_{\text{out}} = \sqrt{G}\,\hat{a}_{\text{in}} + e^{-i\varphi}\sqrt{G-1}\,\hat{a}_{\text{in}}^{\dagger}, \tag{2.52}$$

with the phase shift between the signal and the idler modes, φ. From Eq. 2.52, one can derive that it is possible to reduce the uncertainty in one quadrature phase below the vacuum level. The resulting added noise in the phase-sensitive amplification is [29]

$$\overline{n}_{\text{q}}\overline{n}_{\text{p}} \geq \frac{1}{16}\left|1 - \frac{1}{\sqrt{G_{\text{q}}G_{\text{p}}}}\right|^2, \tag{2.53}$$

where $\overline{n}_{\text{q}}$ ($\overline{n}_{\text{p}}$) is the added noise photon number to the amplified (deamplified) quadrature with the gain G_{q} (G_{p}). We observe that for $G_{\text{q}}G_{\text{p}} = 1$, we get $\overline{n}_{\text{q}}\overline{n}_{\text{p}} = 0$, implying noiseless phase-sensitive amplification.

Parametric amplification with the JPA In the flux-driven JPA, a pump tone at twice the JPA resonance frequency, $\omega_{\text{p}}/2\pi$, is inductively coupled to the dc-SQUID loop and periodically modulates the magnetic flux, leading to a periodic modulation of the dc-SQUID inductance. This causes a periodic modulation of the resonance frequency, $\omega_0/2\pi$, of the JPA circuit. This periodic modulation induces a three-wave mixing process that amplifies a signal mode with the angular frequency, $\omega_{\text{s}} = \omega_{\text{p}}/2 + \Delta\omega$, and detuning, $\Delta\omega$, and also creates an idler mode with the angular frequency, $\omega_{\text{i}} = \omega_{\text{p}}/2 - \Delta\omega$. This process can be illustrated as a pump photon splitting into one signal photon and one idler photon under the conservation of energy, $\omega_{\text{p}} = \omega_{\text{s}} + \omega_{\text{i}}$. To describe the flux-driven JPA analytically, we start with the classical harmonic oscillator with a periodically modulated resonance frequency, $\omega_0 \rightarrow \omega_0(1 + \epsilon/2\cos(\alpha\omega_0 t))$, with the modulation amplitude $\epsilon/2$, and the modulation frequency, $\alpha\omega_0$. The classical equation of motion is given by [28]

$$\frac{\mathrm{d}^2x}{\mathrm{d}t^2} + \omega_0^2(1 + \epsilon\cos(\alpha\omega_0 t)), \tag{2.54}$$

where we neglected terms $O(\epsilon^2)$ since we assume the modulation amplitude to be weak. The corresponding Hamiltonian reads

$$\hat{H} = \hbar\omega_0 \left(\hat{a}^\dagger \hat{a} + \frac{1}{2} + \epsilon \cos(\alpha\omega_0 t)(\hat{a} + \hat{a}^\dagger)^2 \right). \tag{2.55}$$

By introducing a signal and loss port, the Heisenberg equation of motion can be solved analytically in a frame rotating with $\alpha\omega_0$, for which we refer to Ref. [28]. We first discuss the non-degenerate operation mode of the JPA, with the input signal frequency, $\omega_\mathrm{s} = \omega_\mathrm{p}/2 + \Delta\omega$. In this case, the signal and idler power gain is given by [28]

$$G_\mathrm{s}(\Delta\omega) = \frac{\kappa_\mathrm{int}^2 \Delta\omega^2 + \left[(\kappa_\mathrm{int}^2 - \kappa_\mathrm{ext}^2)/4 - \epsilon^2\omega_0^2 - \Delta\omega^2\right]^2}{\kappa^2\Delta\omega^2 + \left(\kappa^2/4 - \epsilon^2\omega_0^2 - \Delta\omega^2\right)^2}, \tag{2.56}$$

$$G_\mathrm{i}(\Delta\omega) = \frac{\kappa^2\epsilon^2\Delta\omega^2}{\kappa^2\Delta\omega^2 + \left(\kappa^2/4 - \epsilon^2\omega_0^2 - \Delta\omega^2\right)^2}, \tag{2.57}$$

with the sum of internal and external loss rates, $\kappa = \kappa_\mathrm{int} + \kappa_\mathrm{ext}$. This derivation is only valid for low modulation amplitudes, $\epsilon \leq \kappa/2\omega_0$. In the degenerate case, $\omega_\mathrm{s} = \omega_\mathrm{p}/2$, i.e. $\Delta\omega = 0$, the signal and idler mode can destructively or constructively interfere depending on their relative phase, θ, and the degenerate signal gain is given by [28]

$$G_\mathrm{d} = \frac{\left[(\kappa_\mathrm{ext}^2 - \kappa_\mathrm{int}^2)/4 + \epsilon^2\omega_0^2\right]^2 + \epsilon^2\kappa_\mathrm{ext}^2\omega_0^2 - 2\epsilon\kappa_\mathrm{ext}\omega_0\left[(\kappa_\mathrm{ext}^2 - \kappa_\mathrm{int}^2)/4 + \epsilon^2\omega_0^2\right]\sin(2\theta)}{(\kappa^2/4 - \epsilon^2\omega_0^2)^2}, \tag{2.58}$$

for low modulation amplitudes,$\epsilon \leq \kappa/2\omega_0$. Under the assumption of an over-coupled JPA, i.e. $(\kappa_\mathrm{ext}^2 - \kappa_\mathrm{int}^2)/4 - \epsilon^2\omega_0^2 > 0$, one can show that the maxmimum and minimum degenerate gain is given by

$$G_\mathrm{d}^\mathrm{min} = \left(\frac{\epsilon\omega_0 - (\kappa_\mathrm{ext} - \kappa_\mathrm{int})/2}{\epsilon\omega_0 + (\kappa_\mathrm{ext} + \kappa_\mathrm{int})/2}\right)^2, \tag{2.59}$$

$$G_\mathrm{d}^\mathrm{max} = \left(\frac{\epsilon\omega_0 + (\kappa_\mathrm{ext} - \kappa_\mathrm{int})/2}{\epsilon\omega_0 - (\kappa_\mathrm{ext} + \kappa_\mathrm{int})/2}\right)^2. \tag{2.60}$$

The corresponding relative phases are $\theta^\mathrm{min} = \pi/4 + n\pi$, and $\theta^\mathrm{max} = 3\pi/4 + n\pi$, for minimum and maximum degenerate gain, respectively. Thus, the difference in phase between the maximum and minimum gain is $\pi/2$, i.e. maximally amplified and deamplified quadratures are orthogonal. For no internal losses, $\kappa_\mathrm{int} = 0$, we obtain $G_\mathrm{d}^\mathrm{min} G_\mathrm{d}^\mathrm{max} = 1$, i.e. noiseless amplification in the JPA for vanishing internal losses.

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

In this section we describe the general framework of continuous-variable quantum key distribution (CV-QKD) protocols and introduce metrics for assessing the performance of these protocols. Throughout this work, we refer to Alice, Bob, and Eve as placeholders for the sender, receiver, and eavesdropper, respectively.

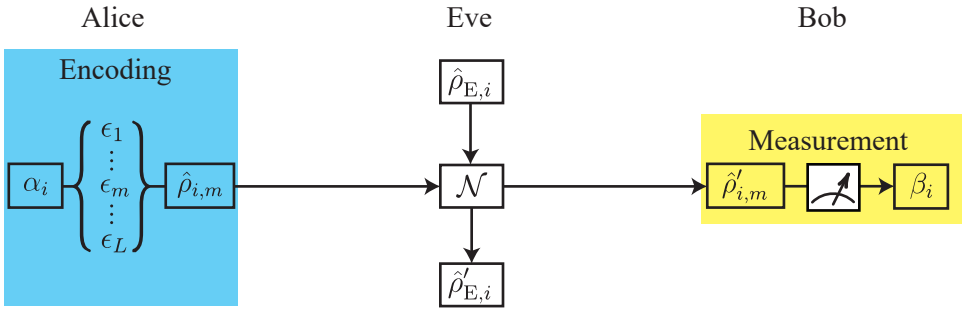

Figure 2.7: General schematic of a QKD protocol. Alice encodes her symbols $\{\alpha_i\}$ in an ensemble of states $\hat{\rho}_{i,m}$ and sends it to Bob over a quantum channel $\mathcal{N}$. Eve interacts with Alice's states, receiving her states $\hat{\rho}'_{\mathrm{E},i}$. Bob performs a measurement on his received states to extract corresponding symbols $\{\beta_i\}$. The security of the protocol depends on the implementation of Eve's attack, Alice's encoding, and Bob's measurement.

2.3.1 General QKD protocol

Quantum key distribution (QKD) is a technique to securely exchange a key between two parties, typically referred to as Alice and Bob. We consider a key to consist of multiple numerical components, key elements. A typical QKD protocol can be divided into two parts: (i) quantum communication and (ii) classical post-processing. The second part is further divided into information reconciliation and privacy amplification steps.

Exchange of states During the first part (i), Alice encodes each key element $\{\alpha_i\}_{i=1}^{N_{\mathrm{key}}}$ into a corresponding quantum state $\hat{\rho}_i$, which propagates through a quantum channel $\mathcal{N}$ to Bob. Eve interacts with Alice's sent state through this quantum channel, receiving her output states $\hat{\rho}'_{\mathrm{E},i}$. Bob receives the output state $\hat{\rho}'_i$ and measures it, obtaining a decoded element β_i. This is repeated until all N_{key} key elements are encoded and sent. Alice and Bob also share an authenticated classical channel. Authenticated messages allow eavesdropping of communicated information over the classical channel, however an eavesdropper, Eve, is unable to change the message themselves. In the most general framework, the eavesdropper is assumed to be limited by the laws of quantum mechanics. By transmitting non-orthogonal states, the transmitted states are protected by the no-cloning theorem and, therefore, limit the information Eve receives on our encoded key elements where Eve's best approach is to interact with the states sent by Alice. A general quantum communication protocol is shown in Fig. 2.7. Here, for each key element, Alice chooses randomly between L different encoding ensembles $\epsilon_m = \{p_{i,m}, \hat{\rho}_{i,m}\}$ [31], with $p_{i,m}$ the probability for Alice to encode the key element α_i onto the quantum state $\hat{\rho}_{i,m}$ given the chosen ensemble $m = 1...L$. Since the no-cloning theorem is valid only for pure states and in practice we often deal with mixed states, we introduce the no-broadcasting theorem, a generalization of the no-cloning theorem. The no-broadcasting theorem [32] states that, given a unknown state in the Hilbert space H_{A} drafted from the set $\{\hat{\rho}_i\}_{i=1,2}$ with $[\hat{\rho}_1, \hat{\rho}_2] \neq 0$, there is no process to create a state $\hat{\rho}_{\mathrm{AE}}$ in a Hilbert space $H_{\mathrm{A}} \otimes H_{\mathrm{E}}$ such that $\rho_i = \mathrm{Tr}_{\mathrm{A}}\, \rho\hat{_{\mathrm{AE}}}$ or $\rho_i = \mathrm{Tr}_{\mathrm{E}}\, \rho\hat{_{\mathrm{AE}}}$. In other words, this means that one can not take a single copy of an unkown state and create a state such that either partial traces result in the original unkown state. With this we require the chosen encoded states $\rho_{i,m}$ to be non-commuting: $[\hat{\rho}_{i,m}, \hat{\rho}_{i,m'}] \neq 0$ for all i and

$m \neq m'$. In this work we further require

$$\int p_m(\alpha)\hat{\rho}_m(\alpha)\mathrm{d}\alpha = \hat{\rho}_{\text{avg}}, \quad \forall m, \tag{2.61}$$

with the average density matrix $\hat{\rho}_{\text{avg}}$ introduced in Sec. 2.1.2. This implies that any measurement by Eve will render her unable to deduce which encoding ensemble is used. After the transmission of states, Bob performs a measurement on his received state, obtaining the decoded key element β_i. There are no restrictions on the type of measurement Bob can perform as long as it is physical, however there are optimal measurements which maximize the shared information between Alice and Bob, discussed in section Sec. 2.3.3.

Classical post-processing After completing the quantum communication, Alice and Bob progress to the extraction of a shared key from the information they have exchanged. This one-way post-processing involves a classical communication step between Alice and Bob through the public authenticated channel. We distinguish between direct reconcilation (DR) and reverse reconciliation (RR). In the DR case, the point of reference for information is the sender of quantum states (Alice) and we aim to correct Bob's data according to Alice's. Conversely, in the RR case, the receiver of quantum states is the reference and we correct Alice's data according to Bob's. Depending on the QKD protocol, Alice and Bob may initially need to discard portions of their respective data, a process known as sifting. This post-processing can be divided into two stages: error correction, also commonly called information reconciliation, and privacy amplification. In this discussion, we initially focus on the information reconciliation. After the protocol we get two partially correlated lists of symbols, or key elements, each of length n. Then, we aim to generate a perfectly correlated list of elements of length l, with $l \leq n$. The Shannon limit [33] shows that an upper bound to the number of perfectly correlated symbols that can be extracted is given by the mutual information I between Alice and Bob. In practice this upper bound is not reached and the deviation from this upper bound defines the reconciliation efficiency $\beta = I_{\text{A:B,p}}/I_{\text{A:B,S}}$, where $I_{\text{A:B,p}}$ is the extracted mutual information during the chosen reconcilation protocol and $I_{\text{A:B,S}}$ is the Shannon limit. Using low-density parity-check (LDPC) codes reconciliation efficiencies of over 90% can be reliably achieved [34]. These reconciliation protocols work in the discrete domain, which implies that the measured data in our protocol, stemming from continuous variables, needs to be discretized. During the privacy amplification, we assume that Alice and Bob share a common key after the reconciliation. However Eve is assumed to possesses correlated information on this key since she can eavesdrop on the classical channel during the reconciliation step. Privacy amplification algorithms remove the compromised key elements, further reducing the final key length. Alice and Bob can estimate the amount of eavesdropping information Eve gets after the exchange of states by disclosing key elements, which is further discussed in Sec. 2.4.3. Using this, they can use a two-universal hash function to remove the information that Eve possesses at the cost of further reducing the length of the key [8].

Eve's attack An important step of QKD is to describe Eve's attack. In this regard, we show three types of attacks that are known as individual, collective, and coherent attacks. The security analysis relies on the assumptions that: (i) Eve has full control over the quantum channel (ii) Eve has unlimited classical and quantum computation power (iii) Eve can eavesdrop on the classical channel without being detected (iv) Eve cannot access Alice's or Bob's experimental setups.

Class	Canonical Form $C(\tau, r, \overline{n})$	$\boldsymbol{T}$	$\boldsymbol{N}$
A_1	$C(0, 0, \overline{n})$	0	$(2n+1)\mathbb{1}$
A_2	$C(0, 1, \overline{n})$	$(\mathbb{1}+\sigma_z)/2$	$(2n+1)\mathbb{1}$
B_1	$C(1, 1, 0)$	$\mathbb{1}$	$(\mathbb{1}-\sigma_z)/2$
B_2	$C(1, 2, \overline{n})$	$\mathbb{1}$	$\overline{n}\mathbb{1}$
L	$C(\tau \in (0,1), 2, \overline{n})$	$\sqrt{\tau}\mathbb{1}$	$(1-\tau)(2\overline{n}+1)\mathbb{1}$
A	$C(\tau > 1, 2, \overline{n})$	$\sqrt{\tau}\mathbb{1}$	$(\tau-1)(2\overline{n}+1)\mathbb{1}$

Table 2.1: Canonical classes [12] with their respective parameters $\tau, r, \overline{n}$. $\mathbb{1}$ is the identity matrix and $\sigma_z = \mathrm{diag}(1, -1)$ the Pauli z matrix.

In the most powerful attack, the coherent attack, Eve sends possibly different states to interact with Alice's signals in the quantum channel and stores each output state in a perfect quantum memory. Then, once Eve listened to all classical communication, she performs an optimal joint measurement on the states in her quantum memory. Finding an optimal coherent attack is challenging since Eve is able to freely interact with Alice's states, i.e. she can choose arbitrary input states $\hat{\rho}_{\mathrm{E},i}$ to the quantum channel $\mathcal{N}$. However, with the quantum de Finetti theorem, the security against coherent attacks can be restricted to security against collective attacks [35][36]. This proof relies on the invariance of the total system $\{\hat{\rho}_{i,m}\}$ under permutations of the subsystems $\hat{\rho}_{i,m}$. In QKD protocols we send a number of symbols sequentially, however the order of those sent states is often irrelevant, so the permutation symmetry is fulfilled. In addition, the proof needs the Hilbert space dimension of the individual subsystem to be smaller than the number of transferred states. However in the continuous variable case, where the Hilbert space of the individual subsystem is infinite dimensional, this proof only works in the case of an infinite amount of transferred states, the so-called asymptotic case. In collective attacks, Eve uses identical independent states that interact with Alice's signals in the quantum channel. After the exchange of states, Eve is assumed to perform an ideal joint measurement on the stored output states in her quantum memory. Lastly, in individual attacks, Eve is assumed to use identical independent states to interact with and perform an individual measurement on each of these incoming signals before the classical post-processing step.

Canonical form of a Gaussian quantum channel Eve's collective attack can be shown to be optimal if she uses a Gaussian attack [37]. In the Gaussian attack, the quantum channel is replaced with a single-mode Gaussian channel G that preserves Gaussianity of input states. In the case of single-mode states, the output Gaussian states are given by

$$\overline{\mathbf{r}}' = \boldsymbol{T}\overline{\mathbf{r}} + \mathbf{d}, \tag{2.62}$$

$$\boldsymbol{V}' = \boldsymbol{T}\boldsymbol{V}\boldsymbol{T}^T + \boldsymbol{N}, \tag{2.63}$$

where $\boldsymbol{T}, \boldsymbol{N} \in (\mathbb{R}^{2\times 2})^2$, $\mathbf{d} \in \mathbb{R}^2$, and $\boldsymbol{V}$ and $\overline{\mathbf{r}}$ are the input covariance matrix and displacement vector of the input Gaussian state, respectively. We follow Ref. [12] to simplify the action of this channel. The Gaussian channel can be decomposed to $G = W \circ C \circ U$, where W, C, and U are physical maps applied one after the other. U, W are called Gaussian unitaries, and C is called the canonical form. A Gaussian unitary is defined by its action on a Gaussian state with mean $\overline{\mathbf{r}}$ and covariance matrix $\boldsymbol{V}$:

$$\overline{\mathbf{r}}' = \boldsymbol{S}\overline{\mathbf{r}} + \mathbf{d}, \quad \boldsymbol{V}' = \boldsymbol{S}\boldsymbol{V}\boldsymbol{S}^T, \tag{2.64}$$

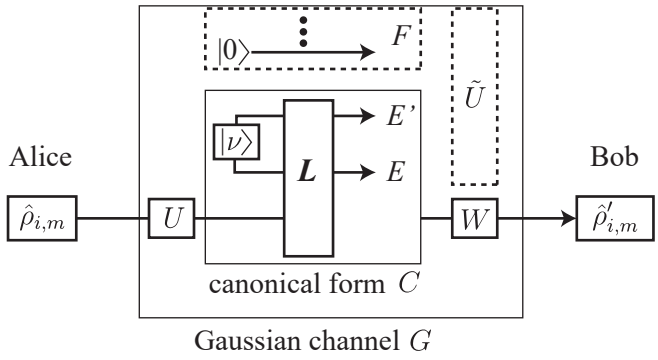

Figure 2.8: Schematic of a collective Gaussian attack [12]. The Gaussian channel G is reduced to a canonical form C and two Gaussian unitaries U, W. The canonical form C can be extended to a symplectic transformation $\boldsymbol{L}$ mixing a TMS state with Alice's input state. This extension is unique up to a unitary $\tilde{U}$ combining the TMS output modes E, E' with a countable set of vacuum modes F. Eve stores the output of $\tilde{U}$ in a quantum memory until the state transfer is complete and the side information has been released by Alice and Bob.

where $\boldsymbol{S}$ is a symplectic matrix:

$$\boldsymbol{S}\boldsymbol{\Omega}\boldsymbol{S}^T = \boldsymbol{\Omega}, \text{with} \quad \boldsymbol{\Omega} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{2.65}$$

The canonical form C is a Gaussian channel with no displacement $\mathbf{d} = 0$, and diagonal entries in $\boldsymbol{T}, \boldsymbol{N}$. The canonical form can be parameterized by the transmittivity τ, the channel rank r, and the thermal number $\overline{n}$, with

$$\tau = \det(\boldsymbol{T}) \tag{2.66}$$

$$r = \min(\operatorname{rank}(\boldsymbol{T}), \operatorname{rank}(\boldsymbol{N})) \tag{2.67}$$

$$\overline{n} = \begin{cases} \frac{\sqrt{\det(\boldsymbol{N})} - (1-\tau)}{2|1-\tau|} & \text{for } \tau \neq 1, \\ \sqrt{\det(\boldsymbol{N})} & \text{otherwise.} \end{cases} \tag{2.68}$$

Table Tab. 2.1 shows the different canonical classes. A_1 replaces the input state with a thermal state, A_2 replaces a quadrature with Gaussian noise, B_1 adds Gaussian noise to one quadrature, B_2 adds Gaussian noise to both quadratures. L is a loss channel with losses $\tau \in (0, 1)$ and A is an amplification channel with $\tau > 1$. With this decomposition of the general Gaussian channel into the canonical form and two Gaussian unitaries, we have taken the first step to describing the most effective attack by Eve.

Extension of Gaussian canonical forms We use the Stinespring dilation theorem to represent the canonical form as a three-mode canonical unitary $U_{\boldsymbol{L}}$ with the corresponding symplectic matrix $\boldsymbol{L}$. This unitary couples the input state σ with mode A to an environmental TMS state $|\nu\rangle$ with modes E and E' [12] and corresponding variance $\nu = (1 + 2\overline{n})/4$. The matrix $\boldsymbol{L}$ is determined by the canonical class, $\boldsymbol{L} = \boldsymbol{L}(\tau, r)$. Excluding the canonical class B_2, shown in table Tab. 2.1, for which the matrix $\boldsymbol{L}$ is more complex, $\boldsymbol{L}$ can be decomposed as

$\boldsymbol{L}(\tau, r) = \boldsymbol{M}(\tau, r) \oplus \mathbb{1}_{E'}$, where $\mathbb{1}_{E'}$ is the identity operator on mode E' and $\boldsymbol{M}(\tau, r)$ is a two-mode unitary acting on modes A and E. By tracing out the environmental mode E', we get a thermal state in the mode E and see that the canonical forms of all classes except B_2 are simply a thermal state with $\overline{n}$ photons combining with the input mode A. For all the different unitaries $\boldsymbol{M}(\tau, r)$ that describe how the TMS state combines with the input mode we refer to [12]. In particular, we get for the loss channel L:

$$\boldsymbol{M}(\tau \in (0,1), 2) = \begin{pmatrix} \sqrt{\tau}\mathbb{1} & \sqrt{1-\tau}\sigma_z \\ -\sqrt{1-\tau}\sigma_z & \sqrt{\tau}\mathbb{1} \end{pmatrix}, \tag{2.69}$$

which corresponds to the beam splitter matrix coupling mode E of the TMS state to the input mode A.

Eve's entangling cloner attack For Eve's attack, we restrict our considerations to losses and coupled noise describing a typical communication channel, which is fully described by a lossy and noisy channel. Considering one can show that attacks of Eve are invariant under isometric operations [38], we choose $W = U = \mathbb{1}$. Then, the output of the Gaussian channel is

$$\overline{\mathbf{r}}' = \sqrt{\tau}\overline{\mathbf{r}}, \quad \boldsymbol{V}' = \tau\boldsymbol{V} + \frac{1}{4}(1-\tau)(1+2n)\mathbb{1}. \tag{2.70}$$

We can further define the coupled noise $\overline{n}$ such that

$$(1-\tau)\frac{n}{2} = \overline{n}. \tag{2.71}$$

This transforms the covariance matrix of the output of the Gaussian channel to

$$\boldsymbol{V}' = \tau\boldsymbol{V} + \overline{n}\mathbb{1} + \frac{1}{4}(1-\tau)\mathbb{1}. \tag{2.72}$$

This attack known as the universal Gaussian entangling cloner attack [12].

2.3.2 Entropy of quantum states

In order to mathematically quantify the information exchanged in our CV-QKD implementation, we define entropies within the framework of classical information theory.

Shannon entropy and differential entropy First, we introduce the Shannon entropy, defined for discrete variables. Given a discrete random variable X with the total number of outcomes N, the Shannon entropy H is given by

$$H(X) = -\sum_{x \in X} p(x) \log p(x), \tag{2.73}$$

where $p(x)$ is the probability distribution over X. The most common bases for the logarithm are bits (basis 2) and nats (basis e). For a continuous variable, Shannon defined the differential entropy as

$$h(X) = -\int_{\mathbb{D}} f(x) \log f(x) \mathrm{d}x, \tag{2.74}$$

where $\mathbb{D}$ is the domain of the probability density function f of the continuous random variable X. Intuitively this seems to correspond to a continuous extension of the discrete definition above, but there are some important differences. First, for $N \to \infty$, the Shannon entropy for the discrete variable does not coincide with the differential entropy in some cases [39] and the differential entropy can also take negative values. In addition, the differential entropy is only defined up to a constant. One can show that with $Y = aX$

$$h(Y) = h(X) + \log |a|. \tag{2.75}$$

The differential entropy still remains a useful quantity however since in the security analysis we are only interested in a difference of differential entropies, where the offset $\log |a|$ disappears.

Von Neumann entropy The von Neumann entropy S_N of a quantum state with density matrix $\hat{\rho}$ is defined as

$$S_N(\hat{\rho}) = -\operatorname{Tr}(\hat{\rho} \log \hat{\rho}), \tag{2.76}$$

where $\log$ denotes the natural logarithm. This can be rewritten in terms of the eigenvalues $\hat{\rho}$ as

$$S_N(\hat{\rho}) = -\sum_i \lambda_i \log \lambda_i, \tag{2.77}$$

We observe a similarity to the Shannon entropy, where λ_i has replaced $p(x)$. For pure states we get $S_N = 0$. In this work we mostly work with Gaussian states and their moment matrices. The von Neumann entropy of a N-mode Gaussian state can be calculated from the covariance matrix $\boldsymbol{V}$ as [7]

$$S_N(\hat{\rho}) = \sum_i g(\nu_i), \tag{2.78}$$

with the symplectic eigenvalues ν_i of $\boldsymbol{V}$ and

$$g(x) = \left(2x + \frac{1}{2}\right) \log \left(2x + \frac{1}{2}\right) - \left(2x - \frac{1}{2}\right) \log \left(2x - \frac{1}{2}\right). \tag{2.79}$$

The symplectic eigenvalues of a covariance matrix $\boldsymbol{V}$ are given by the eigenvalues of

$$\tilde{\boldsymbol{V}} = i\boldsymbol{\Omega}\boldsymbol{V}, \tag{2.80}$$

where

$$\boldsymbol{\Omega} = \bigoplus_{i=1}^{N} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{2.81}$$

with the matrix direct sum is defined as

$$\boldsymbol{A} \bigoplus \boldsymbol{B} = \begin{pmatrix} \boldsymbol{A} & 0 \\ 0 & \boldsymbol{B} \end{pmatrix}. \tag{2.82}$$

2.3.3 Mutual information and Holevo's bound

Mutual information The mutual information defines the amount of shared information between two parties with a correlated set of variables. For two random variables (X, Y) with their

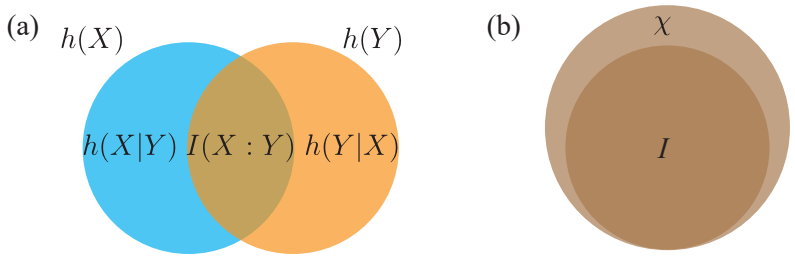

Figure 2.9: (a) Illustration of differential entropies $h(X)$ (blue) and $h(Y)$ (orange) and their corresponding conditional entropies $h(X|Y)$ and $h(Y|X)$. The mutual information is given by the overlap of $h(X)$ and $h(Y)$, i.e., $I(X:Y) = h(Y) - h(Y|X) = h(X) - h(X|Y)$. (b) The mutual information is bounded from above by the Holevo bound χ.

corresponding domain $\mathbb{D}_X \times \mathbb{D}_Y$ and joint probability density function $p(x, y)$, we define the mutual information between X and Y as

$$I(X:Y) = \int_{\mathbb{D}_X} \int_{\mathbb{D}_Y} p(x,y) \log \frac{p(x,y)}{p(x)p(y)}, \tag{2.83}$$

with the marginal distributions for X and Y being $p(x)$ and $p(y)$, respectively. We define the conditional entropy $H(Y|X)$

$$H(Y|X) = -\int_{\mathbb{D}_X} \int_{\mathbb{D}_Y} p(x,y) \log p(y|x), \tag{2.84}$$

with the probability density function $p(y|x)$ of the random variable Y conditioned on $X = x$. With this, the mutual information becomes

$$I(X:Y) = H(Y) - H(Y|X), \tag{2.85}$$

which is illustrated in Fig. 2.9. In this work, we work with Gaussian random variables, for which the mutual information has a simple form. The differential entropy of a Gaussian random variable X with the variance σ^2_{X} is given by [31]

$$h(X) = \frac{1}{2} \log(2\pi e \sigma^2_{\mathrm{X}}) + C, \tag{2.86}$$

where C is a constant. The conditional entropy is [31]

$$h(Y|X) = \frac{1}{2} \log(2\pi e \sigma^2_{\mathrm{Y|X}}) + C, \tag{2.87}$$

with the conditional variance $\sigma^2_{\mathrm{Y|X}}$ defined as

$$\sigma^2_{\mathrm{Y|X}} = \sigma^2_{\mathrm{Y}} - \frac{\mathrm{Cov}(X,Y)^2}{\sigma^2_{\mathrm{X}}}. \tag{2.88}$$

Then, the mutual information is given by

$$I(X:Y) = \frac{1}{2} \log \left(\frac{\sigma^2_{\mathrm{Y}} \sigma^2_{\mathrm{X}}}{\sigma^2_{\mathrm{Y}} \sigma^2_{\mathrm{X}} - \mathrm{Cov}(X,Y)^2} \right). \tag{2.89}$$

This value can be calculated directly from experiments and is invariant under linear rescaling of either datasets X or Y.

Holevo information We consider the information accessible to Eve she obtains from interacting with Alice's states by coupling her own TMS states to them. The maximum accessible information that can be extracted from any measurement, illustrated in Fig. 2.9(b), is defined as

$$I_{\text{acc}}(\epsilon_{\text{E}}) = \max I(X:E)_{M_{\text{E}}}, \tag{2.90}$$

with Eve's measurements M_{E}, the mutual information between Alice ($X = A$, in the DR case) or Bob ($X = B$, in the RR case) and Eve. Here, $\epsilon_{\text{E}} = \{p_i, \hat{\rho}_{\text{E},i}\}$ denotes the ensemble of states obtained by Eve after the attack with their associated probabilities. The computation of I_{acc} is generally difficult since any possible measurement M_{E} can be considered. However, Holevo's theorem provides an upper bound to the information Eve gains on the key regardless of her measurement which is given by [40]

$$I_{\text{acc}}(\epsilon_{\text{E}}) \leq \chi(\epsilon_{\text{E}}), \tag{2.91}$$

where

$$\chi(\epsilon_{\text{E}}) = S_N\left(\int p(x)\hat{\rho}_{\text{E}}(x)\mathrm{d}x\right) - \int p(x) S_N(\hat{\rho}_{\text{E}}(x))\mathrm{d}x. \tag{2.92}$$

2.3.4 Asymptotic security

We recall that the exponential de Finetti reduction theorem allows us to consider that Eve's attack is a collective attack in the asymptotic case of infinite number of exchanged states, for which Gaussian attacks are proven to be optimal. Using the previously shown Stinespring dilation we can further reduce the Gaussian channel to a TMS coupling to Alice's input mode via a beamsplitter, as described in Sec. 2.3.1. The asymptotic secret key is given by [31][8]

$$K = \beta I(A:B) - \chi_{\text{E}}, \tag{2.93}$$

with the reconciliation efficiency β, the mutual information between Alice and Bob $I(A:B)$, and the Holevo bound on Eve's information χ_{E}. The secret key rate is given in bits per channel use. With the repetition rate, or channel use rate f_r, and the sifting factor $D \in (0,1)$, we define the secret key rate as

$$R = f_r D K. \tag{2.94}$$

The sifting factor D is protocol-dependent and is the result of postselection while the repetition rate is mostly defined by the experimental setup. We discuss the effect of a finite amount of exchanged symbols in Sec. 2.4.3.

2.4 Gaussian modulated coherent- and squeezed-state CV-QKD protocols

In this section, we apply the introduced framework for the security analysis of two different Gaussian modulated CV-QKD protocols. First, we show the Gaussian-modulated coherent-state CV-QKD protocol with both homodyne and heterodyne detection on Bob's side. Following this, we introduce the Gaussian-modulated squeezed-state CV-QKD protocol with homodyne detection and compare its performance to the coherent-state protocol.

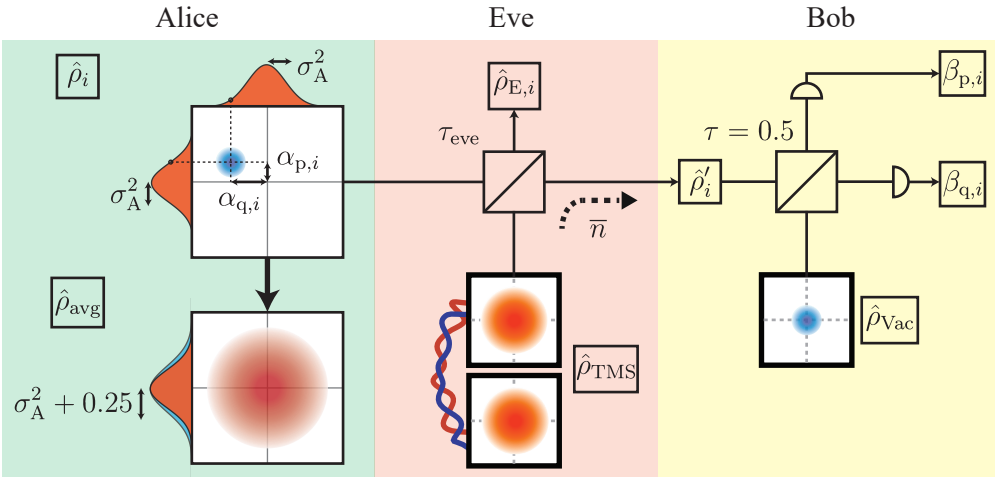

Figure 2.10: Schematic of the coherent state CV-QKD protocol with heterodyne detection. Alice encodes her symbols $\alpha_{q,i}$ and $\alpha_{p,i}$, drawn from a Gaussian distribution with the variance σ_A^2, in displaced vacuum states. The resulting average state has the variance of $\sigma_A^2 + 0.25$. This state is sent to Bob over the Gaussian channel where it couples to one mode of Eve's TMS state. At Bob's side, a heterodyne measurement yields the measured symbols, $\beta_{q,i}$ and $\beta_{p,i}$.

2.4.1 Gaussian-modulated coherent state CV-QKD protocol

In the Gaussian-modulated coherent state CV-QKD protocol, Alice uses coherent states to encode her key elements. The experimental accessibility of coherent states, as opposed to single-photon states required for discrete-variable protocols, such as BB84 [41], makes this CV-QKD protocol easier to implement experimentally. In particular, in the microwave regime, since microwave single-photon sources and detectors are still ongoing research topics, discrete-variable protocols are more complex to realize. Therefore, we first discuss encoding of the key elements in coherent states and consider corresponding possible measurements (decoding) on Bob's side. Following this, we calculate the mutual information based on a quantum-limited readout on Bob's side. Finally, we compute Eve's average and individual states with its associated Holevo bound.

Coherent state protocol encoding In the Gaussian-modulated coherent state protocol shown in Fig. 2.10, Alice encodes her key elements drawn from a Gaussian distribution, $\mathcal{N}(0, \sigma_A)$, in displacement of vacuum states. Alice draws two numbers from the Gaussian distribution, $\alpha_{q,i}$ and $\alpha_{p,i}$, and displaces her vacuum state by the complex displacement amplitude, $\alpha_i = \alpha_{q,i} + i\alpha_{p,i}$, resulting in the Gaussian state

$$\bar{\mathbf{r}}_A = \begin{pmatrix} \alpha_{q,i} \\ \alpha_{p,i} \end{pmatrix}, \quad \boldsymbol{V}_A = \frac{1}{4}\mathbb{1}. \tag{2.95}$$

In the limit of infinite number of sent states, $N \to \infty$, the average Gaussian channel input state is given by

$$\bar{\mathbf{r}}_{A,coh,avg} = (0,0), \quad \boldsymbol{V}_{A,coh,avg} = \frac{1+\sigma_A^2}{4}\mathbb{1}, \tag{2.96}$$

which is identical to a thermal state with the photon number $1 + 2\overline{n}_{\text{th}} = (1 + \sigma_{\text{A}}^2)/4$. This state propagates through the Gaussian channel with transmission τ_{Eve} and coupled noise $\overline{n}$ to Bob, who receives the state

$$\overline{\mathbf{r}}_{\text{B}} = \sqrt{\tau_{\text{Eve}}} \begin{pmatrix} \alpha_{\text{q},i} \\ \alpha_{\text{p},i} \end{pmatrix}, \quad \boldsymbol{V}_{\text{B}} = \tau_{\text{Eve}} \boldsymbol{V}_{\text{A}} + \overline{n}\mathbb{1} + \frac{1 - \tau_{\text{Eve}}}{4}\mathbb{1}. \tag{2.97}$$

Bob performs either a homodyne measurement in the randomly chosen basis $x \in \{q, p\}$, or a heterodyne measurement. He measures either a single displacement $\beta_{x,i}$ in the homodyne case or both displacements $\beta_{q,i}$ and $\beta_{p,i}$ in the heterodyne case. In the case of N transmitted states and heterodyne detection, the measurements results in $L_{\text{het}} = 2N$ correlated key elements $\{\alpha_{x,i}, \beta_{x,i}\}_{x\in\{q,p\},i=1\ldots N}$. In the case of homodyne detection, Bob communicates his chosen measurement basis x via the authenticated classical channel. Alice discards the corresponding conjugate basis key element and the measurements results in $L_{\text{hom}} = N$ correlated key elements $\{\alpha_{x,i}, \beta_{x,i}\}_{i=1\ldots N}$.

Mutual information We discuss first the case of homodyne detection on Bob's side. From the Gaussian loss channel introduced in Sec. 2.3.1, we know that Bob's output key element is given by

$$\beta_{x,i} = \sqrt{\tau_{\text{Eve}}}\alpha_{x,i} + z, \quad z \in Z, \tag{2.98}$$

with the Gaussian noise variable Z and its variance $\sigma_{\text{Z}}^2 = \tau_{\text{Eve}}/4 + \overline{n} + (1 - \tau_{\text{Eve}})/4$. Here, we assume the minimum readout noise $n_q = n_p = 0$ for homodyne detection on Bob's side from Sec. 2.2.2. A more realistic protocol model that is closer to experimental reality is discussed later in Sec. 4.1.1. Then, we compute $\sigma_{\text{B}}^2 \equiv \text{Var}(\{\beta_{x,i}\}_{i=1\ldots N}) = \tau\sigma_{\text{A}}^2 + \sigma_{\text{Z}}^2 + \text{Cov}(A, Z)$ and $\text{Cov}(A, B) = \text{Cov}(A, \sqrt{\tau}A) + \text{Cov}(A, Z)$. We note that the Gaussian noise introduced by Eve is uncorrelated to Alice's key elements, resulting in $\text{Cov}(A, Z) = 0$. The mutual information between Bob's measured key elements $\beta_{x,i}$ and Alice's sent key elements $\alpha_{x,i}$ is given by Eq. 2.89:

$$I(A : B)_{\text{coh,hom}} = \frac{1}{2}\log_2\left(\frac{\sigma_{\text{B}}^2\sigma_{\text{A}}^2}{\sigma_{\text{B}}^2\sigma_{\text{A}}^2 - \text{Cov}(A, B)^2}\right) = \frac{1}{2}\log_2\left(1 + \frac{\tau_{\text{Eve}}\sigma_{\text{A}}^2}{\sigma_{\text{Z}}^2}\right). \tag{2.99}$$

In a second step, we discuss the case of heterodyne detection. In this case, Bob first uses a symmetric beam splitter with a vacuum state at the second input. As a result, the input state before Bob's measurement is described by a Gaussian two-mode state described by

$$\overline{\mathbf{r}}_{\text{B,het}} = \sqrt{\frac{\tau_{\text{Eve}}}{2}} \begin{pmatrix} \alpha_{\text{q},i} \\ \alpha_{\text{p},i} \\ \alpha_{\text{q},i} \\ \alpha_{\text{p},i} \end{pmatrix}, \quad \boldsymbol{V}_{\text{B,het}} = \frac{1}{2}\left(\boldsymbol{V}_{\text{B}} \oplus \boldsymbol{V}_{\text{B}} + \frac{1}{4}\mathbb{1}_4\right), \tag{2.100}$$

where $\mathbb{1}_4$ is the 4-dimensional identity matrix. Now, Bob performs a homodyne measurement in q-basis on the first mode and a homodyne measurement in p-basis on the second mode. Bob's output key element is given by

$$\beta_{x,i} = \sqrt{\frac{\tau_{\text{Eve}}}{2}}\alpha_{x,i} + z, \quad z \in Z, \tag{2.101}$$

where the variance of the Gaussian noise variable Z is

$$\sigma^2_{\mathrm{Z,het}} = \frac{\sigma^2_{\mathrm{Z}} + 0.25}{2}. \tag{2.102}$$

The corresponding mutual information is given by

$$I(A:B)_{\mathrm{coh,het}} = \log_2\left(1 + \frac{\tau_{\mathrm{Eve}}\sigma^2_{\mathrm{A}}}{\sigma^2_{\mathrm{Z}} + \frac{1}{4}}\right), \tag{2.103}$$

where the factor $\frac{1}{2}$ is missing, since Bob measures twice the key elements per channel use as with homodyne detection. We observe the minimum added noise of half a noise photon from the heterodyne detection, also mentioned in Sec. 2.2.2. It is important to note that even though the mutual information is increased by a factor 2 in comparison with the homodyne detection case, as shown in Eq. 2.99, there is a decrease in the signal-to-noise ratio due to the elevated noise level. Therefore, it is not straightforward to find which regime performs better. One approach can outperform another depending on actual experimental parameters (see Sec. 4.1.3).

Holevo bound Eve's Holevo bounds for direct reconcilation (DR) and reverse reconcilation (RR) are given by

$$\chi^{\mathrm{DR}}_{\mathrm{E}} = S_N\left(\int p(\alpha)\hat{\rho}_{\mathrm{E}}(\alpha)\mathrm{d}\alpha\right) - \int p(\alpha)S_N(\hat{\rho}_{\mathrm{E}}(\alpha)), \tag{2.104}$$

$$\chi^{\mathrm{RR}}_{\mathrm{E}} = S_N\left(\int p(\beta)\hat{\rho}_{\mathrm{E}}(\beta)\mathrm{d}\beta\right) - \int p(\beta)S_N(\hat{\rho}_{\mathrm{E}}(\beta)). \tag{2.105}$$

To compute this quantity, we need to calculate Eve's state $\hat{\rho}_{\mathrm{E}}(\alpha)$ after the Gaussian channel for a given key element α. The corresponding input state of Eve is a TMS state with the variance $\Sigma_{\mathrm{TMS}} = \cosh(2r)/2 = (1 + 2n_{\mathrm{Eve}})/4 = 1/4 + \overline{n}/(1 - \tau_{\mathrm{Eve}})$ and corresponding covariance matrix

$$\boldsymbol{V}_{\mathrm{E}} = \begin{pmatrix} \Sigma_{\mathrm{TMS}} & 0 & \Delta_{\mathrm{TMS}} & 0 \\ 0 & \Sigma_{\mathrm{TMS}} & 0 & -\Delta_{\mathrm{TMS}} \\ \Delta_{\mathrm{TMS}} & 0 & \Sigma_{\mathrm{TMS}} & 0 \\ 0 & -\Delta_{\mathrm{TMS}} & 0 & \Sigma_{\mathrm{TMS}} \end{pmatrix}, \text{ with } \Delta_{\mathrm{TMS}} = \sqrt{\Sigma^2_{\mathrm{TMS}} - \frac{1}{16}}. \tag{2.106}$$

This state has a zero mean vector $\overline{\mathbf{r}}_{\mathrm{E}} = 0$. At the output of the Gaussian channel, Eve's state $\hat{\rho}_{\mathrm{E}}(\alpha_{\mathrm{q}}, \alpha_{\mathrm{p}})$ transforms to

$$\boldsymbol{V}_{\mathrm{E'},\mathrm{coh}} = \begin{pmatrix} \Sigma_{\mathrm{TMS,coh}} & 0 & \sqrt{\tau_{\mathrm{Eve}}}\Delta_{\mathrm{TMS}} & 0 \\ 0 & \Sigma_{\mathrm{TMS,coh}} & 0 & -\sqrt{\tau_{\mathrm{Eve}}}\Delta_{\mathrm{TMS}} \\ \sqrt{\tau_{\mathrm{Eve}}}\Delta_{\mathrm{TMS}} & 0 & \Sigma_{\mathrm{TMS}} & 0 \\ 0 & -\sqrt{\tau_{\mathrm{Eve}}}\Delta_{\mathrm{TMS}} & 0 & \Sigma_{\mathrm{TMS}} \end{pmatrix}, \tag{2.107}$$

with $\Sigma_{\mathrm{TMS,coh}} = \tau_{\mathrm{Eve}}\Sigma_{\mathrm{TMS}} + (1 - \tau_{\mathrm{Eve}})/4$ and the mean vector $\overline{\mathbf{r}}_{\mathrm{E,coh}} = \sqrt{1 - \tau_{\mathrm{Eve}}}(\alpha_{\mathrm{q}}, \alpha_{\mathrm{p}}, 0, 0)$. By taking into account that the key elements from Alice are distributed according to the Gaussian distributions with variance σ^2_{A}, we can compute the average state for Eve in the asymptotic limit, $N \to \infty$, as

$$\hat{\rho}_{\mathrm{E,avg}} = \int_{-\infty}^{\infty}\mathrm{d}\alpha_{\mathrm{q}}\int_{-\infty}^{\infty}\mathrm{d}\alpha_{\mathrm{p}}\frac{1}{2\pi\sigma^2_{\mathrm{A}}}\exp\left(-\frac{\alpha^2_{\mathrm{q}} + \alpha^2_{\mathrm{p}}}{2\sigma^2_{\mathrm{A}}}\right)\hat{\rho}_{\mathrm{E}}(\alpha_{\mathrm{q}}, \alpha_{\mathrm{p}}). \tag{2.108}$$

Since this state is an integral of Gaussian states, only differing in a prefactor, the resulting state is also Gaussian with the mean zero and the covariance matrix

$$\boldsymbol{V}_{\text{E,avg}} = \begin{pmatrix} \Sigma_{\text{TMS,coh}} + (1-\tau_{\text{Eve}})\sigma_{\text{A}}^2 & 0 & \sqrt{\tau_{\text{Eve}}}\Delta_{\text{TMS}} & 0 \\ 0 & \Sigma_{\text{TMS,coh}} + (1-\tau_{\text{Eve}})\sigma_{\text{A}}^2 & 0 & -\sqrt{\tau_{\text{Eve}}}\Delta_{\text{TMS}} \\ \sqrt{\tau_{\text{Eve}}}\Delta_{\text{TMS}} & 0 & \Sigma_{\text{TMS}} & 0 \\ 0 & -\sqrt{\tau_{\text{Eve}}}\Delta_{\text{TMS}} & 0 & \Sigma_{\text{TMS}} \end{pmatrix}. \tag{2.109}$$

We note here that the average state of Eve defines the first term of the Holevo bound and does not depend on the reconcilation method (DR vs RR) or on the measurement method (homodyne vs. heterodyne). The Holevo bound for homodyne detection is given by

$$\chi_{\text{E,hom}}^{\text{DR}} = S_N(\hat{\rho}_{\text{E,avg}}) - \sum_{x\in\{q,p\}} \frac{1}{2}\int_{-\infty}^{\infty} \mathrm{d}\alpha_x f(\alpha_x, \sigma_{\text{A}}) S_N(\hat{\rho}_{\text{E}}(\alpha_x)), \tag{2.110}$$

$$\chi_{\text{E,hom}}^{\text{RR}} = S_N(\hat{\rho}_{\text{E,avg}}) - \sum_{x\in\{q,p\}} \frac{1}{2}\int_{-\infty}^{\infty} \mathrm{d}\beta_x f(\beta_x, \sigma_{\text{B}}) S_N(\hat{\rho}_{\text{E}}(\beta_x)), \tag{2.111}$$

with $x \in \{q,p\}$ and the Gaussian probability distribution function $f(x,\sigma)$

$$f(x,\sigma) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{x^2}{\sigma^2}\right). \tag{2.112}$$

For heterodyne detection, we account for both quadratures resulting in

$$\chi_{\text{E,het}}^{\text{DR}} = S_N(\hat{\rho}_{\text{E,avg}}) - \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \mathrm{d}\alpha_{\text{q}}\mathrm{d}\alpha_{\text{p}} f(\alpha_{\text{q}}, \sigma_{\text{A}}) f(\alpha_{\text{p}}, \sigma_{\text{A}}) S_N(\hat{\rho}_{\text{E}}(\alpha_{\text{q}}, \alpha_{\text{p}})), \tag{2.113}$$

$$\chi_{\text{E,het}}^{\text{RR}} = S_N(\hat{\rho}_{\text{E,avg}}) - \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \mathrm{d}\beta_{\text{q}}\mathrm{d}\beta_{\text{p}} f(\beta_{\text{q}}, \sigma_{\text{B}}) f(\beta_{\text{p}}, \sigma_{\text{B}}) S_N(\hat{\rho}_{\text{E}}(\beta_{\text{q}}, \beta_{\text{p}})). \tag{2.114}$$

We compute the von Neumann entropy by computing the symplectic eigenvalues of the covariance matrix (see Eq. 2.78).

2.4.2 Gaussian-modulated squeezed state CV-QKD protocol

Here, we introduce a similar protocol, as compared to the coherent state protocol, where we rely on the squeezed states and homodyne detection. The operation of the protocol with the squeezed states can be advantageous, since the noise contribution of the quantum state $\sigma_{\text{coh}}^2 = 1/4$ on Bob's side can be reduced below vacuum for the measured quadrature.

Squeezed state protocol encoding In the Gaussian-modulated squeezed state protocol shown in Fig. 2.11, Alice encodes her key element drawn from a Gaussian distribution, $\mathcal{N}(0,\sigma_{\text{A}})$, in the displacement of squeezed states. She chooses the squeezed quadrature $x \in \{q,p\}$ randomly and displaces the squeezed state in the same quadrature x. In the case of $x = q$, her input state is given by

$$\bar{\mathbf{r}}_{\text{A,sq}} = \begin{pmatrix} \alpha_i \\ 0 \end{pmatrix}, \quad \boldsymbol{V}_{\text{A,sq}} = \begin{pmatrix} \sigma_{\text{S}}^2 & 0 \\ 0 & \sigma_{\text{AS}}^2 \end{pmatrix}, \tag{2.115}$$

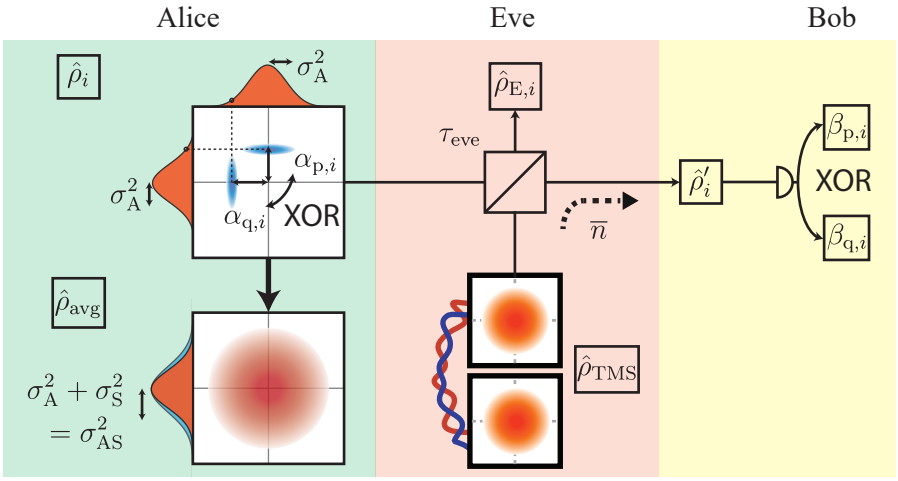

Figure 2.11: Schematic of the squeezed state protocol. Alice encodes her symbol $\alpha_{x,i}, x \in \{q, p\}$ in the displacement along quadrature x of a state squeezed in the quadrature x. To make the two encoding ensembles indistinguishable, the condition $\sigma^2_{\mathrm{A}} = \sigma^2_{\mathrm{AS}} - \sigma^2_{\mathrm{S}}$ needs to be fulfilled. This makes the average state look like a thermal state with the variance $\sigma^2_{\mathrm{A}} + \sigma^2_{\mathrm{S}} = \sigma^2_{\mathrm{AS}}$. Bob performs a homodyne measurement in a random basis $b \in \{q, p\}$. After the state transfer, Alice and Bob discard all symbols with mismatched encoding or measurement bases $x \neq b$.

with the squeezed variance $\sigma^2_{\mathrm{S}} = (1 + 2n_{\mathrm{JPA}})e^{-2r}/4$ and the antisqueezed variance $\sigma^2_{\mathrm{AS}} = (1 + 2n_{\mathrm{JPA}})e^{2r}/4$. In the case $x = p$, the squeezed and antisqueezed quadratures and the mean vector elements are swapped. We recall the condition that both ensembles must be indistinguishable, i.e., the average state $\hat{\rho}_{\mathrm{A,sq,avg}}$ should look like a thermal state. Alice's average input state in the case of $x = q$ is given by

$$\bar{\mathbf{r}}_{\mathrm{A,sq,avg}} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \quad \boldsymbol{V}_{\mathrm{A,sq,avg}} = \begin{pmatrix} \sigma^2_{\mathrm{S}} + \sigma^2_{\mathrm{A}} & 0 \\ 0 & \sigma^2_{\mathrm{AS}} \end{pmatrix}. \tag{2.116}$$

We observe that with the condition $\sigma^2_{\mathrm{A}} = \sigma^2_{\mathrm{AS}} - \sigma^2_{\mathrm{S}}$, the average state for both ensembles, $x = q$ and $x = p$, becomes

$$\bar{\mathbf{r}}_{\mathrm{A,sq,avg}} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \quad \boldsymbol{V}_{\mathrm{A,sq,avg}} = \sigma^2_{\mathrm{AS}}\mathbb{1}, \tag{2.117}$$

which resembles the thermal state with the variance σ^2_{AS}. Since the thermal state is invariant under rotation in phase space, the q- and p- quadratures are statistically indistinguishable from each other. This indistinguishability condition ties the squeezing level to the displacement variance, which can limit the performance of our protocol implementation, as discussed in Sec. 4.1.3. This state propagates through the Gaussian channel and Bob performs a homodyne measurement in a random basis $b \in \{q, p\}$, receiving his key element $\beta_{b|x,i}$. After the transmission of all N states, Alice and Bob release their encoding and decoding basis x, b over the classical channel and discard all states with mismatching basis $\{\beta_{b|x,i}\}_{b \neq x}$. On average $L_{\mathrm{sq}} = N/2$ key elements $\{\alpha_{x,i}, \beta_{x,i}\}_{i=1\ldots N/2}$ remain for the key generation.

Mutual information Following the same procedure as with the coherent state protocol in the case of homodyne detection, we get Bob's measured symbol

$$\beta_{x,i} = \sqrt{\tau_{\text{Eve}}}\alpha_{x,i} + z, \quad z \in Z, \tag{2.118}$$

with the Gaussian noise variable Z with variance $\sigma_{\text{Z,sq}} = \tau_{\text{Eve}}\sigma_{\text{S}}^2 + \overline{n} + (1 - \tau_{\text{Eve}})/4$. We note that the contribution of the quantum state to Bob's noise variance is smaller and below vacuum in the squeezed state protocol: $\sigma_{\text{S}}^2 < 1/4$. It follows that the mutual information is given by

$$I(A:B) = \frac{1}{2}\log_2\left(1 + \frac{\tau_{\text{Eve}}\sigma_{\text{A}}^2}{\sigma_{\text{Z,sq}}^2}\right). \tag{2.119}$$

Holevo bound In the case of $x = q$, Eve's output state is given by

$$\boldsymbol{V}_{\text{E,sq}} = \begin{pmatrix} \Sigma_{\text{TMS,S}} & 0 & \sqrt{\tau_{\text{Eve}}}\Delta_{\text{TMS}} & 0 \\ 0 & \Sigma_{\text{TMS,AS}} & 0 & -\sqrt{\tau_{\text{Eve}}}\Delta_{\text{TMS}} \\ \sqrt{\tau_{\text{Eve}}}\Delta_{\text{TMS}} & 0 & \Sigma_{\text{TMS}} & 0 \\ 0 & -\sqrt{\tau_{\text{Eve}}}\Delta_{\text{TMS}} & 0 & \Sigma_{\text{TMS}} \end{pmatrix}, \tag{2.120}$$

with $\Sigma_{\text{TMS,S}} = \tau_{\text{Eve}}\Sigma_{\text{TMS}} + (1 - \tau_{\text{Eve}})\sigma_{\text{S}}^2$, $\Sigma_{\text{TMS,AS}} = \tau_{\text{Eve}}\Sigma_{\text{TMS}} + (1 - \tau_{\text{Eve}})\sigma_{\text{AS}}^2$, and $\bar{\mathbf{r}}_{\text{E,sq}} = (\sqrt{1 - \tau_{\text{Eve}}}\alpha_{\text{q}}, 0, 0, 0)$. For the conjugate basis $x = p$, the variance and mean of the q and p quadratures of the first mode are swapped. The average state for Eve includes the basis swapping and becomes

$$\hat{\rho}_{\text{E,avg}} = \sum_{x\in\{q,p\}} \frac{1}{2}\int_{-\infty}^{\infty} \mathrm{d}\alpha_x f(\alpha_x, \sigma_A) \exp\left(-\frac{\alpha_x^2}{2}\right) \hat{\rho}_{\text{E}}(\alpha_x), \tag{2.121}$$

with the Gaussian probability distribution function $f(x, \sigma)$ already introduced before. We compute the covariance matrix of Eve's average state

$$\boldsymbol{V}_{\text{E,avg}} = \begin{pmatrix} \Sigma_{\text{TMS,avg}} & 0 & \sqrt{\tau_{\text{Eve}}}\Delta_{\text{TMS}} & 0 \\ 0 & \Sigma_{\text{TMS,avg}} & 0 & -\sqrt{\tau_{\text{Eve}}}\Delta_{\text{TMS}} \\ \sqrt{\tau_{\text{Eve}}}\Delta_{\text{TMS}} & 0 & \Sigma_{\text{TMS}} & 0 \\ 0 & -\sqrt{\tau_{\text{Eve}}}\Delta_{\text{TMS}} & 0 & \Sigma_{\text{TMS}} \end{pmatrix}, \tag{2.122}$$

with $\Sigma_{\text{TMS,avg}} = (1 - \tau_{\text{Eve}})\sigma_{\text{AS}}^2 + \tau_{\text{Eve}}\Sigma_{\text{TMS}} = (1 - \tau_{\text{Eve}})(\sigma_{\text{A}}^2 + \sigma_{\text{S}}^2) + \tau_{\text{Eve}}\Sigma_{\text{TMS}}$. Note that in the coherent protocol we get $\Sigma'_{\text{TMS,avg}} = (1 - \tau_{\text{Eve}})(\sigma_{\text{A}}^2 + (1 + 2\overline{n}_{\text{th}})/4) + \tau_{\text{Eve}}\Sigma_{\text{TMS}}$. This expression is similar except for the individual state variance, which is smaller for the squeezed state protocol. However, we can reduce the modulation variance in the coherent state protocol to make up for the state variance and get the same average state for Eve for both the squeezed state and the coherent state protocol. We compute

$$\Sigma'_{\text{TMS,avg}} = \Sigma_{\text{TMS,avg}} \tag{2.123}$$

$$\leftrightarrow \sigma_{\text{A,sq}}^2 = \sigma_{\text{A,coh}}^2 + (1 + 2\overline{n}_{\text{th}})/4 - \sigma_{\text{S}}^2 > \sigma_{\text{A,coh}}^2. \tag{2.124}$$

With this, the first expression in the Holevo bound for both squeezed state and coherent state protocol becomes identical and only Eve's individual states are different. The Holevo bound for

the squeezed state protocol then becomes

$$\chi_{\text{E,sq}}^{\text{DR}} = S_N(\hat{\rho}_{\text{E,avg}}) - \sum_{x\in\{q,p\}} \frac{1}{2}\int_{-\infty}^{\infty} \mathrm{d}\alpha_x f(\alpha_x, \sigma_{\text{A}}) S_N(\hat{\rho}_{\text{E}}(\alpha_x)), \tag{2.125}$$

$$\chi_{\text{E,q}}^{\text{RR}} = S_N(\hat{\rho}_{\text{E,avg}}) - \sum_{x\in\{q,p\}} \frac{1}{2}\int_{-\infty}^{\infty} \mathrm{d}\beta_x f(\beta_x, \sigma_{\text{B}}) S_N(\hat{\rho}_{\text{E}}(\beta_{x_i})), \tag{2.126}$$

For simulations and comparison of the performance of both protocols, we refer to Sec. 4.2.1.

2.4.3 Finite-size effects

In this section, we consider additional effects in the case of a finite number of exchanged states, N. We primarily consider the security in the case of collective attacks. The security of collective attacks can be extended to coherent attacks even in the finite case [35] [42] [43] under a decrease of a security parameter, ϵ. This security parameter is defined by the probability of the protocol being unsafe resulting from the failure of the classical algorithms in the post-processing steps. It can be made arbitrarily small at the cost of increased block sizes L during the key generation. The extension from the collective attack security to the coherent attack security is still an ongoing research topic and can be protocol-specific.

Parameter estimation In the case of infinite exchanged states and the Gaussian collective attacks, we can assume a negligible fraction of symbols are used to estimate the transmission losses and noise. This implies that Alice and Bob can get a perfect knowledge of the parameters of the quantum channel. However, in the case with a finite number, L, of quantum states are communicated over the quantum channel, we need to build a worst-case scenario statistical estimators of the transmission losses and total noise by constructing a confidence bound. We recall that in the introduced protocols, Alice's symbols $\{\alpha_i\}_{i=1\ldots L}$ are encoded in the displacement of quantum states and Bob receives a lossy and noisy version of the quantum state, so, he measures his symbols as

$$\beta_i = \sqrt{\tau_{\text{Eve}}}\alpha_i + z, \quad z \in Z, \tag{2.127}$$

where the Gaussian noise variable Z has the variance σ_{Z}^2, which depends on the coupled noise from Eve. If we assume that Alice and Bob use a number m of both symbols $\{\beta_i\}_{i=1\ldots m}$ and $\{\alpha_i\}_{i=1\ldots m}$, we can build estimators for τ_{Eve} and σ_{Z}^2. This requires releasing parts of their symbols that are now unusable for the key generation. We can build these estimators from the model in Eq. 2.127 such that [1]

$$\tilde{t}_{\text{Eve}} = \sqrt{\tilde{\tau}_{\text{Eve}}} = \frac{\sum_{i=1}^{m}\alpha_i\beta_i}{\sum_{i=1}^{m}\alpha_i^2} \approx \frac{\sum_{i=1}^{m}\alpha_i\beta_i}{m\sigma_{\text{A}}^2} \tag{2.128}$$

$$\tilde{\sigma}_{\text{Z}}^2 = \frac{1}{m}\sum_{i=1}^{m}(\beta_i - \tilde{t}_{\text{Eve}}\alpha_i)^2, \tag{2.129}$$

where $\tilde{t}$ and $\tilde{\sigma}_{\text{Z}}^2$ are the estimators for the square root transmission and total noise variance. We note that the estimator for the total noise variance depends on the estimator for transmissivity. For a large number of disclosed symbols m, the estimator $\tilde{t}_{\text{Eve}}$ is Gaussian and the variable

$Y = m\tilde{\sigma}_{\mathrm{Z}}^2/\sigma_{\mathrm{Z}}^2$ follows a chi-square distribution $\chi^2(m)$ with m degrees of freedom. Following Ref. [1] we compute

$$\sigma_t^2 \equiv \mathrm{Var}(\tilde{t}_{\mathrm{Eve}}) = \frac{\sum_{i=1}^{m} \mathrm{Var}(\beta_i \alpha_i)}{m^2 \sigma_{\mathrm{A}}^2} \approx \frac{\sigma_{\mathrm{Z}}^2}{m\sigma_{\mathrm{A}}^2} + \frac{2\tau_{\mathrm{Eve}}}{m}, \tag{2.130}$$

$$\sigma_\tau^2 \equiv \mathrm{Var}(\tilde{\tau}_{\mathrm{Eve}}) \approx \frac{4\tau_{\mathrm{Eve}}^2}{m}\left(2 + \frac{\sigma_{\mathrm{Z}}^2}{\tau_{\mathrm{Eve}}\sigma_{\mathrm{A}}^2}\right), \tag{2.131}$$

$$\sigma_N^2 \equiv \mathrm{Var}(\tilde{\sigma}_{\mathrm{Z}}^2) \approx \frac{\sigma_{\mathrm{Z}}^4}{8m}. \tag{2.132}$$

In an experimental setting, Alice and Bob can estimate the transmissivity τ_{Eve} and total noise variance σ_{Z}^2 using Eqs. 2.128 and 2.129 and then compute the expected estimator variance using the equations above. Since the estimators are Gaussian for sufficiently large m, we compute their standard deviation as the square root of their variance. With this, we define $w = \sqrt{2}\,\mathrm{erf}^{-1}(1 - 2\epsilon_{\mathrm{PE}})$, where ϵ_{PE} is the failure probability of the parameter estimation. We define the worst-case secnario estimators

$$\tau_{\mathrm{Eve,wc}} = \tilde{\tau}_{\mathrm{Eve}} - w\sigma_\tau \quad \sigma_{\mathrm{z,wc}}^2 = \tilde{\sigma}_{\mathrm{z}}^2 + w\sigma_N, \tag{2.133}$$

where ϵ_{PE} is the probability that the real transmissivity of the Gaussian channel lies below the worst-case scenario estimated transmissivity, $\tau_{\mathrm{Eve}} < \tau_{\mathrm{Eve,wc}}$, or that the actual total noise variance is larger than the estimated worst-case scenario total noise variance, $\sigma_{\mathrm{z}}^2 > \sigma_{\mathrm{z,wc}}^2$. This means that up to the probability of ϵ_{PE}, Alice and Bob can use the values of the estimators to infer the transmissivity and total noise of the quantum channel. Alice and Bob can compute the bound on Eve's information χ_{E} based on these worst-case scenario estimators, which yields the worst-case scenario asymptotic key rate, R_{wc}^{∞}. We note that ϵ_{PE} can be chosen arbitrarily low, resulting in a lower worst-case scenario key rate if the length of the disclosed dataset m is kept constant. For $m \to \infty$, the variance of the estimators vanishes and we recover the asymptotic case, $R_{\mathrm{wc}}^{\infty} \to R^{\infty}$.

Finite secret key rate In addition to the parameter estimation, we also have to consider an imperfect error correction and privacy amplification. Specific error correction and privacy amplification protocols are not discussed in this work, however, we characterize their performance by an error probability p_{ec} that is given by a probability of the successful error correction with an associated reconciliation efficiency β. In addition to ϵ_{pe} from the parameter estimation, there is an additional probability ϵ_{cor} that bounds the probability of obtaining different key strings even after error correction, and the probability ϵ_{sec} that bounds the distance between the key after privacy amplification and the ideal case where the eavesdropper holds no information on the key. One can decompose the latter probability as $\epsilon_{\mathrm{sec}} = \epsilon_{\mathrm{s}} + \epsilon_{\mathrm{h}}$, where ϵ_{s} is a smoothing parameter and ϵ_{h} is a hashing parameter [1]. In the case of collective attacks, the finite secret key rate is given by [1]

$$R^{\mathrm{fin}} \geq r\left(R_{\mathrm{wc}}^{\infty} - \Delta_{\mathrm{aep}} + \Theta\right), \tag{2.134}$$

where $r = \frac{np_{\mathrm{ec}}}{L}$, $n = L - m$, and

$$\Delta_{\mathrm{aep}} = \frac{4\log_2(2\sqrt{d}+1)\sqrt{\log_2\left(\frac{18}{p_{\mathrm{ec}}^2\epsilon_{\mathrm{s}}^4}\right)}}{\sqrt{n}}, \tag{2.135}$$

$$\Theta = \frac{\log_2\left(p_{\mathrm{ec}}(1-\epsilon_{\mathrm{s}}^2/3)\right) + 2\log_2\sqrt{2}\epsilon_{\mathrm{h}}}{n}, \tag{2.136}$$

where $d = 2^5$ for five bit digitization typically done in the case of digitization of data extracted from continuous variable states. We refer to Sec. 4.2.2 for simulations of the minimum exchanged states necessary to achieve a positive finite key rate for collective attacks.

Extension to security against coherent attacks The security analysis of QKD protocols in general works in two steps: first, we prove $\epsilon = 2p_{\text{ec}}\epsilon_{\text{PE}} + \epsilon_{\text{sec}} + \epsilon_{\text{cor}}$ security against the collective attacks, second, we apply the de Finetti reduction [44] to obtain ϵ' security against the coherent attacks, with $\epsilon' = C\epsilon$, $C = O(\text{poly}(n))$, with $n = L - m$, i.e,. the reduction of the security parameter is polynomial in the block size used for the key generation. This approach has successfully proven to be secure against general coherent attacks for DV protocols, such as the BB84 protocol [45] or the qudit protocol [46]. For CV protocols, we can follow the same steps as for DV protocols and prove security against the collective attacks, which are described above, and then apply the de Finetti reduction theorem. For continuous variable protocols, the underlying Hilbert space for each transmitted state is an infinite-dimensional Fock space, $\mathcal{H}$. This Hilbert space can be truncated via energy tests [47], but the truncated single-mode Hilbert space $\{\mathcal{H}'_i\}_{i=1\ldots n}$ grows logarithmically with n, which results in a superexponential $(\log(n)^{Cn}, C > 1)$ dimension for the total truncated Hilbert space $\mathcal{H}_{\text{tot}} = \bigotimes_i^n \mathcal{H}'_i$, with the tensor product $\bigotimes$. Following Ref. [44], this results in a significant loss of the security parameter $\epsilon' = \epsilon \cdot 2^{\text{polylog}(n)}$ [43]. This proves security for infinitely large block sizes against coherent attacks, but the drop in the security parameter is too significant for practical block sizes around $n \sim 10^6 - 10^9$. Protocol-specific approaches yield a practically useful extension for the coherent attack security for the coherent protocol with heterodyne detection [43], where we get $\epsilon' = C\epsilon$, $C = O(n^4)$. We note that this implies $\epsilon \sim 10^{-40}$ and, in particular, $\epsilon_{\text{PE}} \sim 10^{-40}$ is necessary to achieve $\epsilon' \sim 10^{-10}$ [1], which becomes extremely challenging to implement in experiments due to the required precision on the measurements. In addition, for the squeezed state protocol, a method based on entropic uncertainty relations for smooth entropies [48] can be used to prove the coherent attack security for block sizes of $n \sim 10^6 - 10^9$[49]. However, it should be mentioned that for $n \to \infty$, the key rate for the coherent attack security does not recover the key rate corresponding to the collective Gaussian attacks, which are expected to be optimal. In conclusion, the extension of security analysis to coherent attacks for squeezed state protocols with homodyne detection is an ongoing research topic. As a result, we focus on the ϵ security of the Gaussian collective attacks in this work.

Chapter 3

Experimental techniques

3.1 Experimental setup

In this section, we describe details of our experimental setup. In particular, we focus on a cryogenic setup, including a diulution fridge and room temperature devices.

3.1.1 Dry dilution refrigerator

Microwaves have a significant thermal spectral photon density, reaching an average thermal population per mode of 1250 photons at a typical frequency of 5 GHz at room temperatures. These photon numbers are significantly higher than the average photon population of our quantum signals, which lies around 1 photon. Therefore, in order to measure quantum effects, our systems are cooled down to temperatures of approximately 50 mK, where the corresponding thermal population is around 0.1 photons per mode. To achieve the millikelvin temperatures experimentally, we use a commercial "Triton" dry dilution refrigerator from Oxford Instruments. This refrigerator has several stages in a vacuum chamber which is pumped to a low pressure of 10^{-6} mbar in order to thermally decoupled the first stage of the cryostat from the room temperature environment. The first temperature stage consists of a PT1 stage at 50 K and is followed by a PT2 stage at 4 K. Both of these stages are cooled down by a pulse tube refrigerator working with ^{4}He gas. Additional radiation shields further thermally decouple each temperature stage. Lower temperatures are reached using the ^{3}He/^{4}He mixture. A still stage reaches temperatures of around 700 mK. At a temperature of $T = 860$ mK, there is a phase transition in the ^{3}He/^{4}He mixture and the mixture separates into a ^{3}He rich (concentrated phase) and a ^{3}He poor phase (diluted phase). The concentration of ^{3}He in each phase depends on the temperature and reaches 100% in the concentrated phase and $\approx 6.6\%$ in the diluted phase for temperatures near absolute zero. Since ^{4}He is almost inert at millikelvin temperature, the diluted phase can be seen as a ^{3}He gas and the concentrated phase as a ^{3}He liquid. The ^{3}He passing from the concentrated "liquid" to the diluted "gas" phase is similar to evaporation and, thus, endothermic [50]. This process continues to work even at very low temperatures since the ^{3}He concentration in the diluted phase remains almost constant and tends to $\approx 6.5\%$. The equilibrium temperature of the mixing chamber (MXC) in our cryostat further depends on a heat load and heat exchanger performance and lies around 50 mK for our cryostat. For further information on dilution cryostats we refer to Ref. [51].

3.1.2 Sample stage

Our experimental goal is to implement a microwave version of the protocol mentioned in Sec. 2.3.1. We already know from Sec. 2.3.1 that the optimum eavesdropping attack is the entangling cloner,

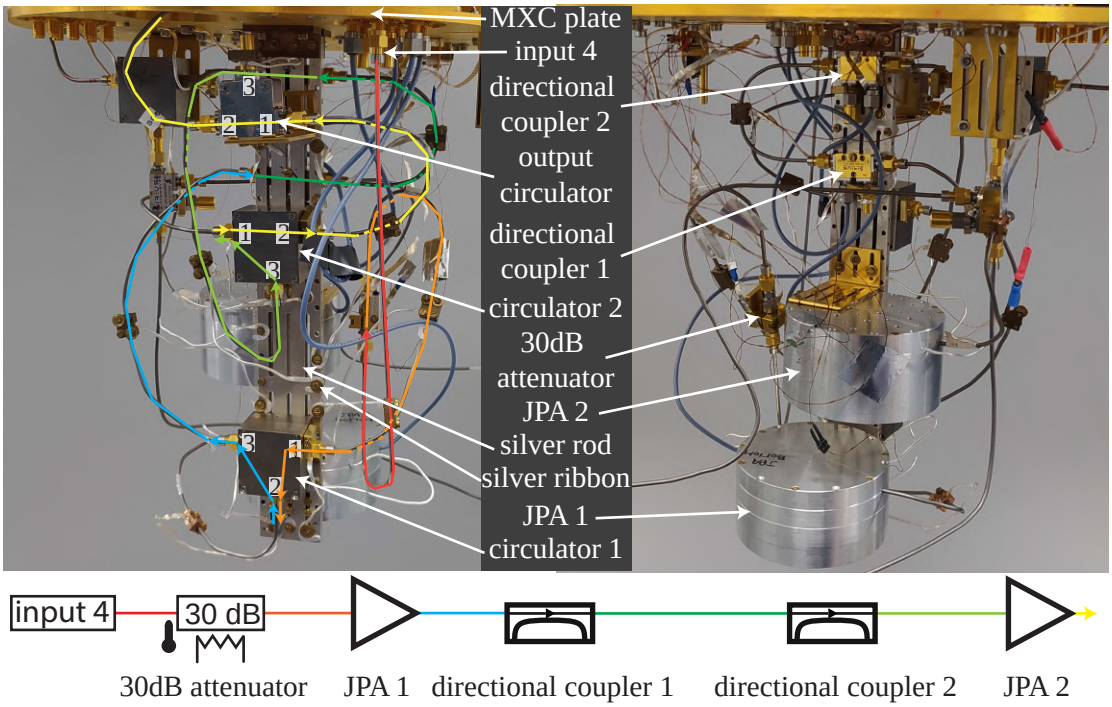

Figure 3.1: Photographs of the sample stage cryogenic setup. The squeezing JPA 1 is at the bottom, while the preamplifier JPA 2 is at the top, both inside of aluminum boxes. The JPA input signal line starts at input 4 (red) to the 30 dB heatable attenuator and continues to the circulator 1 (orange), then, from the squeezer JPA 1 (blue), through the directional coupler 1 (dark green) and directional coupler 2 (light green), and finally to the JPA 2 (yellow).

which couples one mode of a TMS state to Alice's state with a beam splitter. Bob then receives a lossy and noisy version of Alice's state. Knowing this, we add Gaussian noise via a directional coupler to our microwave quantum channel and, thus, emulate the equivalent coupled TMS corresponding to the same number of coupled noise photons. This allows us to simulate the discussed Gaussian quantum channel in an experimental setting. The setup is shown in Fig. 3.3, and the corresponding cryogenic components are shown in Fig. 3.1. In order to implement the protocol described in Sec. 2.4.2, we need to generate microwave displaced squeezed vacuum states. For the generation of microwave squeezed vacuum states, we use a JPA, as described in Sec. 2.2. This JPA is fabricated in-house at the Walter-Meißner institute. On top of the sample box holding the JPA, we mount a superconducting coil to control magnetic flux through the loop of the dc-SQUID of the JPA. Fig. 3.2 shows the JPA chip in the sample box. In addition, the assembled sample box is mounted inside a superconducting aluminum shield in order to prevent stray magnetic fields from affecting the JPA. This is important when using multiple JPAs, as the magnetic field from one JPA coil could affect another one. The squeezed vacuum state is generated by the first JPA in reflection, where we use a Quinstar circulator (OXE89) in order to decouple the incoming signals from the outgoing signals of the JPA, before subsequently going to a first directional coupler with transmittivity $\tau_{\mathrm{DC}} = 0.9885$. Here, a microwave source generates a strong coherent tone that is weakly coupled to our signal. As shown in Sec. 2.1.2,

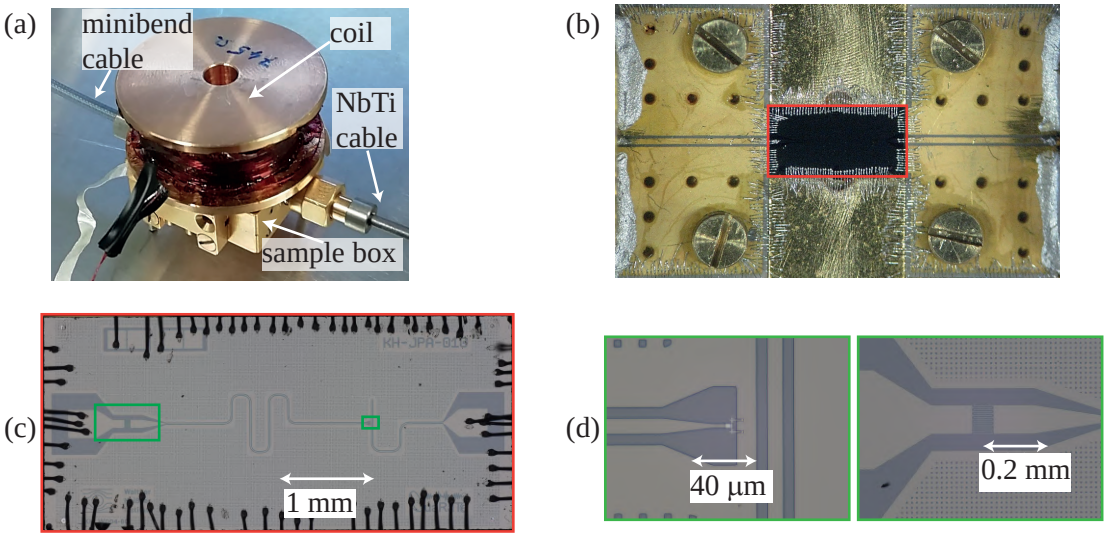

Figure 3.2: JPA sample box and chip photographs. (a) JPA sample box and its superconducting magnetic coil. The minibend cable provides the pump signal, the NbTi superconducting cable is connected to the input circulator. (b) Printed circuit board (PCB) and the JPA chip inside of the sample box. (c) The JPA chip with the coupling capacitor on the left, the CPW resonator in the middle and the DC-SQUID on the right. Black wires are aluminum wire bonds connecting both the PCB ground to the JPA ground plane, and the PCB CPW to the JPA CPW. (d) Optical images of the dc-SQUID and coupling capacitor areas.

since τ_{DC} is close to unity, this device implements the displacement operation for incoming microwave states. Then, the state propagates to a second directional coupler with transmission $\tau_{\mathrm{eve}} = 0.9885$, which couples artificial noise signals generated by an arbitrary function generator (AFG) to our state. The coupled noise photon number, $\overline{n}$, has to be independently calibrated, as described later in Sec. 3.2.6. After this, the state is strongly amplified by the second JPA, which is operated in the phase-sensitive regime in order to act as single-shot quadrature readout equivalent to an optical homodyne detection scheme [52]. Then, the signal propagates through two output circulators, one at the MXC stage and one at the still stage . These circulators function as passive components isolating the rest of the sample stage devices from the HEMT noise and reflected signals. Finally, our cryogenic amplification chain is concluded by a high electron mobility transistor (HEMT) amplifieroperated with the gain of roughly 40 dB. We use a heatable 30 dB attenuator connected to the input of the JPA 1 for a photon number calibration, as described in Sec. 3.2.3. We then use a temperature sensor to measure the temperature of the attenuator, which is combined with a local heater to create a temperature feedback loop and stabilize the heatable attenuator at a given temperature. In order to ensure that all the components of the setup are properly thermalized to the mixing chamber temperature, we thermally anchor each component with thin silver ribbons of roughly 1 mm of diameter to our sample stage silver rod. The rod is attached directly to the MXC plate using copper pieces, ensuring good thermal and mechanical contact between the rod and the MXC plate. These silver ribbons are additionally annealed at a temperature of 900° C to improve their thermal conductivity by removing crystal lattice defects.

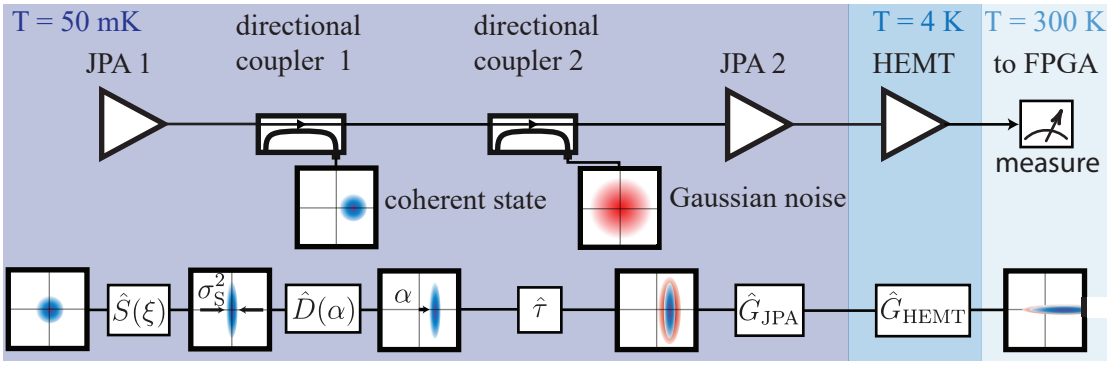

Figure 3.3: Schematic setup of the protocol. The top part shows crucial elements of our protocol implementation. The bottom part shows the corresponding evolution of the states Wigner functions ,$W(q,p)$, and operators for each respective element. Here, $\hat{S(\xi)}$ and $\hat{D}(\alpha)$ are the squeezing and displacement operators, respectively. The operators $\hat{G}_{\mathrm{JPA}}$ and $\hat{G}_{\mathrm{HEMT}}$ describe amplification by the preamplifier JPA 2 and the HEMT, respectively.

3.2 Data acquisition and processing

In this section, we describe a room temperature setup and a microwave tomography setup with an FPGA. Then, we explain gain measurements and different calibration steps.

3.2.1 Room temperature setup

Microwave input lines A complete room temperature setup schematic is shown in Fig. 3.4. In total, there are 5 input microwave lines. Input line 3 is used to generate displacement with the first directional coupler. Here, an SGS 100A signal generator from Rohde & Schwarz provides a coherent signal at the signal frequency of 5.856063 GHz. Input line 5 is used for sending artificial noise signals to the second directional coupler. This noise is generated by a Keysight 81160A AFG in the frequency band of 0-200 MHz with a quasi-Gaussian amplitude distribution. Since our signal frequency is around 5 GHz, we need to up-convert this noise signal. We achieve this by driving a harmonic mixer with a signal generated by an SMB 100A Rohde&Schwarz signal generator at a frequency of 5.848563 GHz. Input lines 6 and 7 are used for the pump tones for the JPA 1 and JPA 2, generated by individual SGS 100A signal sources. All input lines are attenuated at the different cryostat stages to suppress thermal noise coming from the room temperature environment. The attenuation distribution depends on the cooling power of different cryostat stages and must be optimized in order to reach millikelvin levels of the effective thermal noise photon numbers in resulting signals. Finally each device can be controllably triggered using a Zurich Instruments HDAWG arbitrary waveform generator (AWG), with the corresponding AWG waveform shown in Fig. 3.5. We also use the AWG to modulate the amplitude of the displacement source by using an in-built *I/Q* modulation port of the SGS source. For more details, we refer to Sec. 3.2.7.

Microwave output lines Output signals from the cryostat are routed to a room temperature attenuation and amplification setup shown in Fig. 3.5. Here, signals are first amplified by a room

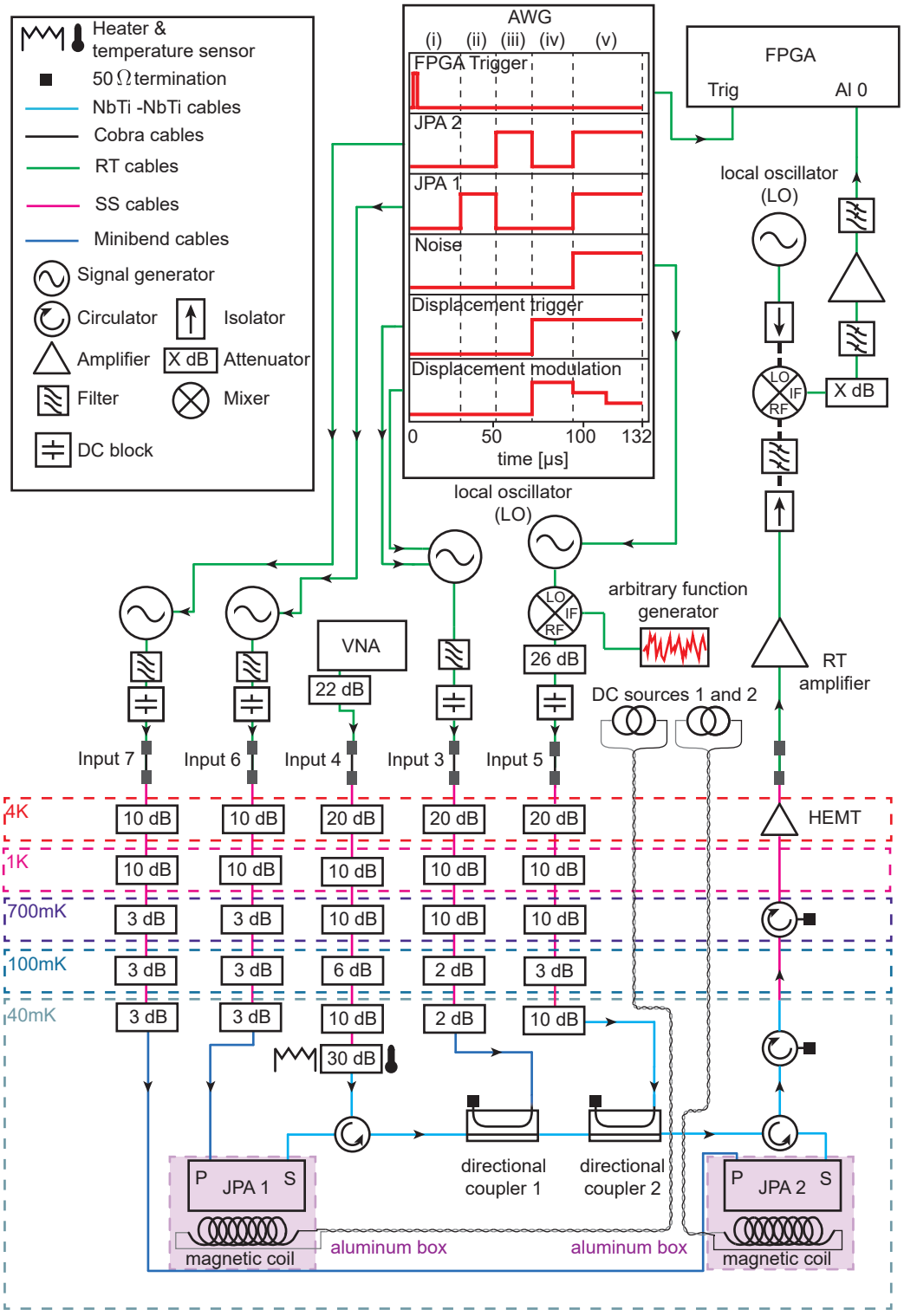

Figure 3.4: Microwave CV-QKD setup with displacement modulation. The superconducting JPA coils are connected via twisted pairs to the two ADCMT 6241A current sources. The vector network analyzer (VNA) is used primarily to calibrate the JPA working points. The AWG supplies tailored modulation envelopes to all microwave signal generators.

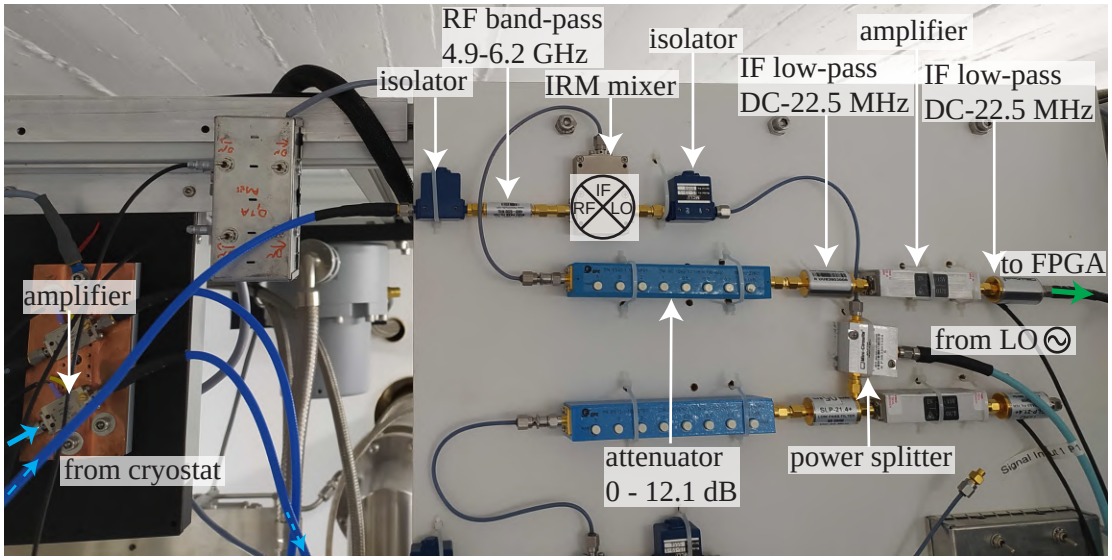

Figure 3.5: Photograph of the room temperature amplification and down-conversion setup between the cryostat output and the FPGA input. Signals are down-converted at the image rejection mixer to the intermediate frequency of $f_{\mathrm{IF}} = 12.5$ MHz. Two room temperature amplifiers increase the signal powers to a sufficiently high level for the FPGA sampling.

temperature AMT-A0033 amplifier with the gain of 28 dB. Signals are subsequently filtered using a 4.9-6.2 GHz bandpass filter (VBF Z-5500-S+ minicircuits). An image rejection mixer (IRM) mixes the RF signal with a local oscillator (LO) tone resulting in output signals at the carrier frequency $f_{\mathrm{IF}} = 12.5$ MHz. The LO is provided by an SGS 100A at the signal frequency of $f_{\mathrm{LO}} = 5.868563$ GHz. Further, the signals are attenuated using a step attenuator (ESA2-1-10/8-SFSF, EPX microwave) to avoid compression in a second stage room temperature amplifier. Signals are further filtered with a DC-22 MHz filter (SLP-21 from Mini-Circuits). To achieve a better signal-to-noise ratio, signals are additionally amplified by another room temperature amplifier (AU-1447 Miteq) with a gain of 58 dB. Finally, the signals are sampled by a FPGA through a NI 5782-02 transceiver unit, mounted to the FPGA NI PXIe-1073. In addition, a FS725 Rubidium frequency standard provides a steady 10 MHz reference for the FGPA, the SMB 100A, and one of the SGS 100A sources in order to provide all devices with a well-defined common phase reference. Other SGS sources are referenced to the first one using a daisy chain with the 1 GHz reference signal.

3.2.2 FPGA

Signal demodulation A NI adapter unit samples the input signal at a sampling frequency of $f_{\mathrm{S}} = 125$ MHz with the 14-bit vertical resolution. We use three different channels of this unit: an analog input channel (AI 0) for the signal, a trigger input (TRIG), and an external reference (CLK IN), which ensures that the FPGA is synchronized with other devices. Next, we perform an *I/Q* demodulation of incoming signals. To this end, the FPGA implements a digital *I/Q* demodulation of input signals $A(t)$ (at frequency f_{IF}) using a digital local oscillator at frequency $f_{\mathrm{IF,D}}$, which results in a digital *I/Q* demodulation of the input signals into two

components with frequency $f_{\mathrm{IF,D}} \pm f_{\mathrm{IF}}$. As a last step, the demodulated signals are integrated over one period $T_{\mathrm{IF}} = 1/f_{\mathrm{IF}}$

$$I = 2f_{\mathrm{IF}} \sum_{i=1}^{N} \cos(2\pi f_{\mathrm{IF}} t_i) A(t_i) \Delta t, \tag{3.1}$$

$$Q = 2f_{\mathrm{IF}} \sum_{i=1}^{N} \sin(2\pi f_{\mathrm{IF}} t_i) A(t_i) \Delta t, \tag{3.2}$$

where $A(t_i)$ is the digitized input signal at time t_i, $\Delta t = 8$ ns is the sampling period, and $N = f_{\mathrm{S}}/f_{\mathrm{IF}} = 10$ is the number of integration points. Then, we use a 200 kHz digital finite impulse response (FIR) filter to filter the extracted quadratures further. This filter uses a Hamming window with 90 coefficients, which leads to a ring-up time of the filter of about 7.2 μs. Each measurement trace contains 1650 of these quadrature values, for the total trace time length of 132 μs. Finally, the FPGA calculates the quadrature moments $\langle I^n Q^m \rangle$ with $n + m \leq 4$, with $n, m \in \mathbb{N}_0$. We repeat this process N_{avg} times in order to average these moments further.

Single shot measurements The aforementioned FPGA averages N_{avg} can be set to 1 to get into a single-shot regime. The individual I/Q points, extracted as described above, represent single-shot quadrature values of the microwave quantum state. In particular, without averages, all noise properties around the IF frequency are preserved, meaning that the HEMT noise is not averaged out.

Time modulation scheme The time modulation scheme is shown at the top of Fig. 3.4. In our experiments, we divide it into five sections. The first part (i) is used to trigger the FPGA to begin a measurement trace and record a vacuum state, where all other devices are switched off. The next part (ii) triggers the pump of the JPA1. From this measurement part, we extract a squeezing angle γ_{exp} using the reference state reconstruction, as explained in the next section. We change the phase of the JPA1 pump by $2\gamma_\Delta$ to adjust the squeezing angle according to $\gamma_{\mathrm{set}} = \gamma_{\mathrm{exp}} + \gamma_\Delta$. During part (iii), the pump for JPA2 is triggered to reproduce the same procedure as for the first JPA and to choose which quadrature is amplified by the phase-sensitive amplification by adjusting the squeezing angle of the second JPA to a desired value. In part (iv), the SGS source providing a coherent tone to the first directional coupler is triggered. Using the reference state reconstruction method, we extract a displacement angle ϕ_{exp} for each coherent tone. By adjusting the phase of the SGS source by $\phi_\Delta = \phi_{\mathrm{set}} - \phi_{\mathrm{exp}}$, we can controllably adjust the angle ϕ_{set} of the displacement operation mentioned in Sec. 2.1.2. Finally, in part (v), all devices are triggered, including the AFG providing the noise signal. This time window provides the actual measurement data for the QKD protocol.

Reference state reconstruction method In our experiments, propagating microwave signals are amplified using low-noise amplifiers in order to detect them at the FPGA. Typical phase-insensitive amplification adds at least half a noise photon referred to the input, as shown in Sec. 2.2.2. The advantage of using the phase-sensitive amplification is that it can be theoretically noiseless. However, we can only get meaningful information on a single quadrature at the cost of losing information on a deamplified conjugate quadrature in the case of single-shot measurements. Conversely, phase-insensitive amplifiers can detect both quadratures, limited by

the Heisenberg uncertainty relation. Best phase-insensitive amplifiers, such as the HEMT amplifiers, add around 10-20 noise photons to our signals. However if we use our JPA 2 as a low-noise phase-sensitive preamplifier, the overall amplification noise can be drastically reduced. According to the Friis formula [53], the total amplification noise would be composed of the noise added by the JPA2 and the noise of the HEMT scaled down by the gain of the JPA2

$$n_{\text{amp}} = n_{\text{JPA}} + \frac{n_{\text{H}}}{G} \tag{3.3}$$

In our experiments, this allows us to reach $n_{\text{amp}} < 1$. In the following, we describe how to extract a quantum state from noisy measurements by using a method called reference state reconstruction [54] [55]. As already mentioned, in the modulation scheme we have about 20 μs of a very weak ($T \approx 20$ mK) thermal state. From Sec. 2.1.2 we already know that we can reconstruct a Gaussian state completely with only up to second order moments. For the reference state reconstruction, we define the complex envelope function related to the measured signals as

$$\hat{\xi} = \frac{\hat{I} + i\hat{Q}}{\sqrt{\kappa}}, \tag{3.4}$$

with the measured quadratures $\hat{I}$ and $\hat{Q}$ and the photon number conversion factor (PNCF), κ. For our quantum states, the envelope function can be written as

$$\hat{\xi}_{\text{S}} = \sqrt{G}(\hat{a} + \hat{V}^{\dagger}), \tag{3.5}$$

with the gain of the JPA G, the signal annihilation operator $\hat{a}$, and the operator for the noise in the amplification path $\hat{V}$. The reference state envelope function is

$$\hat{\xi}_{\text{ref}} = \sqrt{G}(\hat{\nu} + \hat{V}), \tag{3.6}$$

with $\hat{\nu}$ describing the weak thermal state corresponding to our 20 μs pulse as mentioned above. First, we compute the noise moments, $\langle(\hat{V}^{\dagger})^m \hat{V}^n\rangle$, by using the measured moments from the reference state, $\langle(\hat{\xi}^{\dagger}_{\text{ref}})^m \hat{\xi}^n_{\text{ref}}\rangle$, and the weak thermal state, $\langle(\hat{\nu}^{\dagger})^m \hat{\nu}^n\rangle$. The latter are defined by the vacuum state moments, which is a good approximation for the weak thermal states. Then, using the computed noise moments $\langle(\hat{V}^{\dagger})^m \hat{V}^n\rangle$ and the measured moments of the signal envelope function $\langle(\hat{\xi}^{\dagger}_{\text{S}})^m \hat{\xi}^n_{\text{S}}\rangle$, we can compute $\langle(\hat{a}^{\dagger})^m \hat{a}^n\rangle$ by using equation Eq. 3.5. For more details we refer to [56] [57].

3.2.3 PNCF and temperature control

In order to convert voltages measured by the FPGA to a photon number, we use a PNCF calibration method, which relies experimentally on a Planck spectroscopy. The latter is performed using an attenuator that acts as a self-calibrated black body emitter in our setup. We heat the attenuator using a heater coupled to the attenuator. We use a PID feedback loop to ensure a stable temperature during our measurements. The spectral density of a black body emitter depending on its temperature is known from Planck's law, which can be used to derive a model for the detected signal power at the FPGA. This model is fitted to our data to extract both the PNCF κ and the total amplification noise n, stemming primarily from our HEMT. The detected power at the FPGA is [54] [55]

$$P = \frac{\langle I^2\rangle + \langle Q^2\rangle}{R} = \frac{\kappa G}{R}\left[\frac{1}{2}\coth\frac{hf_0}{2k_{\text{B}}T_{\text{att}}} + n\right], \tag{3.7}$$

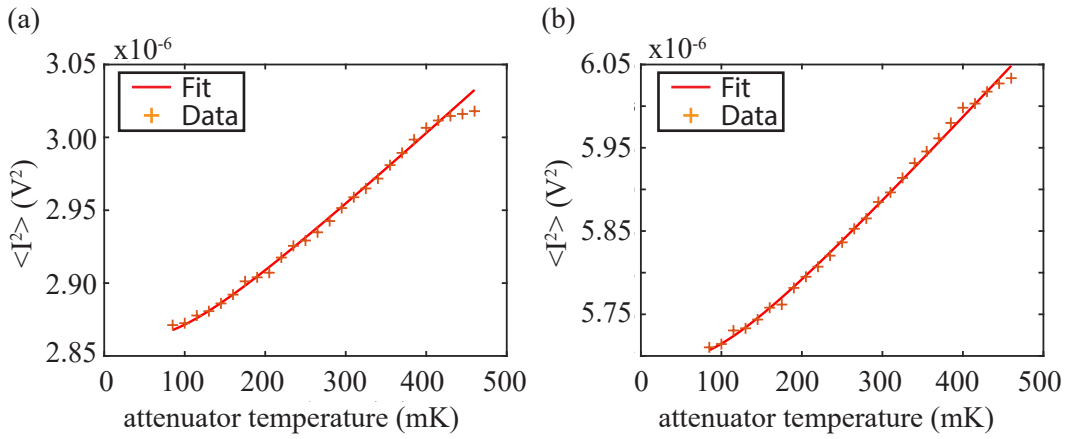

Figure 3.6: PNCF measurements with (a) 200 kHz and (b) 400 kHz FIR filter bandwidth with the carrier frequency of $f_0 = 5.856063$ GHz. The saturation for measurement points in the high temperature regime around 500 mK is likely due to the insufficient thermalization of the system.

FIR	Moment	κG [V^2/photon]	$n/2$ [photon]
200 kHz	$\langle I^2 \rangle$	$6.15 \cdot 10^{-7} \pm 1.264 \cdot 10^{-8}$	4.4 ± 0.1
200 kHz	$\langle Q^2 \rangle$	$6.25 \cdot 10^{-7} \pm 1.264 \cdot 10^{-8}$	4.3 ± 0.1
400 kHz	$\langle I^2 \rangle$	$1.28 \cdot 10^{-6} \pm 2.447 \cdot 10^{-8}$	4.2 ± 0.18
400 kHz	$\langle Q^2 \rangle$	$1.25 \cdot 10^{-6} \pm 2.447 \cdot 10^{-8}$	4.3 ± 0.18

Table 3.1: PNCF fitting results for the carrier frequency $f_0 = 5.856063$ GHz with both 200 kHz and 400 kHz FIR filter bandwidths. We note that the noise is fitted for each quadrature.

with the quadrature second order moments $\langle I^2 \rangle$ and $\langle Q^2 \rangle$, $R = 50\Omega$, the Planck constant h, the Boltzmann constant k_B, the carrier frequency f_0, and the noise and gain of the signal chain n and G, respectively. Lastly, $\kappa = R \cdot BW \cdot hf_0$ is the PNCF, where BW is the measurement bandwidth. We note that the PNCF depends on both the frequency and the measurement bandwidth. A typical PNCF measurement with the corresponding fit can be seen in Fig. 3.6. In these measurements, we measure from highest to lowest temperatures. Here, we perform a PNCF for two different FIR filter bandwidths, 200 kHz and 400 kHz. The extracted fit parameters in Tab. 3.1 for the HEMT noise is almost identical for both quadratures. The benefits of higher FIR filter bandwidth will be discussed in later sections. We note measurement points saturating in the higher temperature regime, near 500 mK, likely caused by an insufficient thermalisation of the system. These data points are discarded in our PNCF fit routines. Finally, we should note that these PNCF measurements are in general referenced to the output of the 30 dB attenuator. However, we often want states to be referred to a different position in our experimental setup. We can change the reference point by modifying the gain of the amplification chain during the data post-processing as

$$G_{\text{ref}} = G_{\text{att}} \cdot 10^{L/10}, \tag{3.8}$$

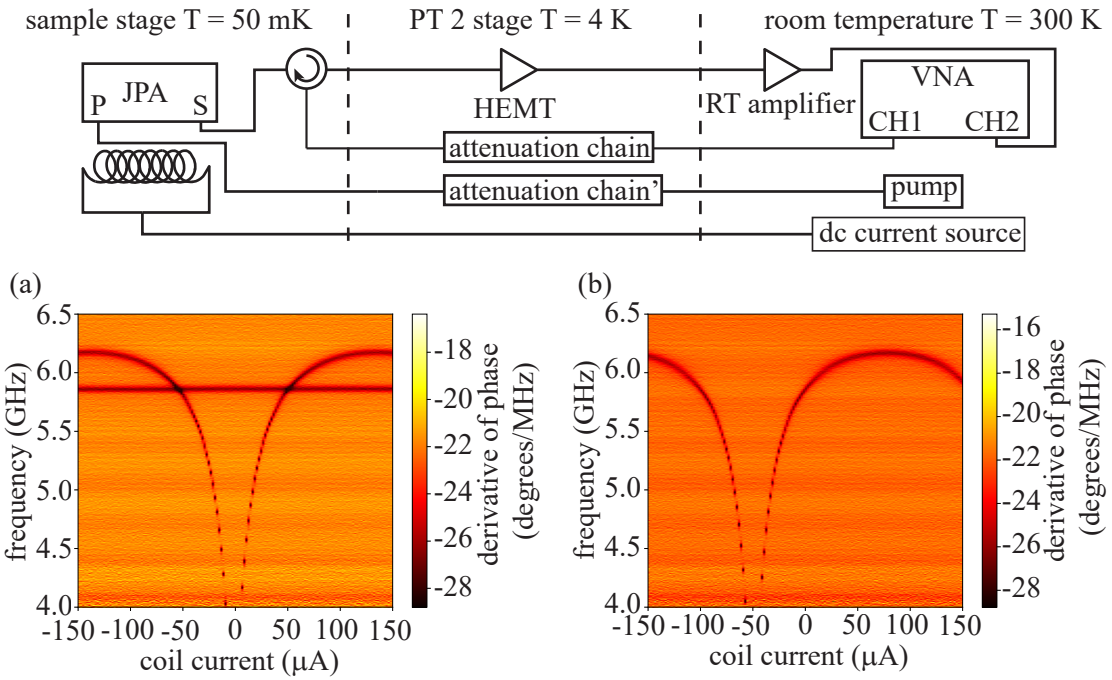

Figure 3.7: Figure at the top shows the measurement schematic. The JPA flux is controlled by a dc-current source which sends a dc-current through a magnetic coil. Flux sweeps for (a) JPA 1 and (b) JPA 2. We observe an offset of the maximal frequency with respect to the coil current for the JPA 2. This offset most probably originates from a trapped magnetic flux. The resonance line that we observe at roughly 5.9 GHz in panel (a) is caused by the zero-flux resonance frequency of the JPA 2.

where L are the losses between the 30 dB attenuator and the chosen reference point and G_{att} is the gain referenced to the 30 dB attenuator. The measurements shown in Fig. 3.6 are referenced to the input of the HEMT.

3.2.4 JPA flux response

We have shown already in Sec. 2.2 that we can tune the resonance frequency of our JPA by changing the magnetic flux ϕ that is enclosed in the dc-SQUID loop. In our setup, this is achieved by using a superconducting coil mounted on top of the JPA sample box. We use an ADCMT 6241A dc-source to send a specified current, typically in the 10-100 μA range, resulting in a specific magnetic flux threading through the dc-SQUID loop. In addition to this dc bias, we generate an RF signal with twice the resonance frequency that is inductively coupled to the dc-SQUID loop. This parametric amplification process, as described in Sec. 2.2.2, depends on the power, phase, and frequency of the pump tone. In order to operate our JPAs in the phase-sensitive regime, we need to measure its frequency-flux relation. We use a vector network analyzer (VNA, Keysight PNA N5222a) to perform transmission measurements. This corresponds to measuring our JPAs in the reflection configuration, since the signal couples through a circulator to the JPA signal port. Then, the JPA reflected signal goes back to the circulator, which further guides to an output port, different from the input one due to the non-reciprocal properties

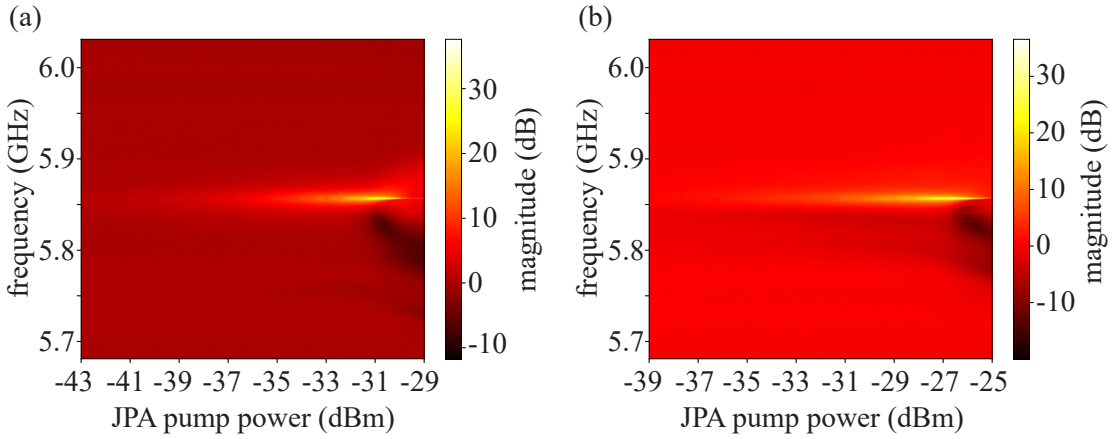

Figure 3.8: JPA nondegenerate gain measurements. Panel (a) corresponds to the JPA 1, while panel (b) corresponds to the JPA 2. The pump power values are referred to the JPA inputs. We observe non-degenerate gain values up to 30 dB for -31 dBm pump power for the JPA 1 and for -27 dBm for the JPA 2.

of the circulator. Finally, the response of our JPA is analysed using the S21 scattering parameter measured by the VNA, which simultaneously extracts the magnitude and phase responses of the JPA. We sweep the frequency of the probe signal, while also varying the coil current after each frequency sweep. Typically, we scan the frequency range of 4-6 GHz and the coil current range of -200 to 200 μA. One of our typical measurements can be seen in Fig. 3.7. We show the first derivative of the unwrapped phase for a better contrast of the JPA resonant response.

3.2.5 Non-degenerate and degenerate gain

Using the JPA we can perform both phase-insensitive and phase-sensitive amplification. In the following subsections, we explain related measurement results.

Non-degenerate gain Here, we operate our JPAs in the phase-insensitive regime, as introduced in Sec. 2.2.2. The slope of the frequency-flux curve is relevant here, since when operating the JPA, we vary the flux threading through the dc-SQUID loop by applying a strong coherent pump tone at twice its resonance frequency. At a resonant frequency with a steep slope with respect to the magnetic flux, a given pumping tone usually induces a larger gain response than at a resonant frequency where the slope is more flat. However, a steep slope also implies that the JPA is more sensitive to flux noise, which can deteriorates the JPA gain and noise characteristics. Subsequently, operating the JPA at more flat slopes requires more pump power to achieve a desired gain and may lead to a larger heat load at the cryogenic system. This additional load can change the frequency response or the performance of the JPA, if the temperature of the JPA is significantly increased. Experimentally, these effects can be mitigated by making a good thermal contact between the JPA and the sample stage. In addition, at high enough pump powers the noise from the pump itself also becomes significant [58]. Therefore, we typically optimize our working point in terms of gain, squeezing, noise, and operate the JPA at a chosen frequency suitable for our desired measurements. For analyzing non-degenerate gain, we pump our JPAs

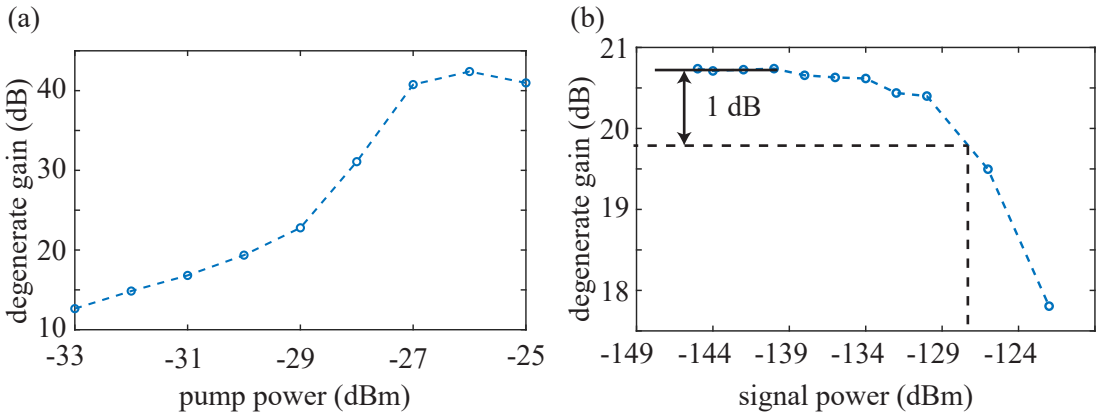

Figure 3.9: (a) Maximum degenerate gain for JPA 2. (b) Compression measurements for the JPA 2 pump power of -30 dBm. We observe a 1 dB compression point at roughly -127 dBm input power with approximately 20.7 dB gain.

with a frequency slightly offset from twice their resonance frequency, $f_\mathrm{p} = 2f_\mathrm{J} + \Delta\omega$, where we typically have $\Delta\omega = 10$ kHz for our devices. We vary the pump power and perform the VNA signal frequency sweep for each pump power. The resulting measurement can be seen in Fig. 3.8 for the JPA working frequency of 5.856063 GHz. We can see an increase in gain up to 28.4 dB of gain at -31 dBm pump power for the JPA 1.

Degenerate gain Here, the JPA is operated in the phase-sensitive regime, as discussed in the second part of Sec. 2.2.2. In our experiments, phase-sensitive amplification allows for readout measurement with an efficiency above the standard quantum limit ($\eta > 50\%$), as introduced in Sec. 2.2.2. In order to optimize the quantum efficiency, we first measure the degenerate gain of the JPA.To this end, we send a coherent tone through the first directional coupler, which is subsequently amplified by JPA 2. We sweep the phase of the coherent tone from 0 to 180° by varying the SGS source phase. As it can be seen from Sec. 2.2 and 2.1.2, the JPA realising the squeezing operator shows a two-fold rotational symmetry in the phase-space, making it sufficient to only consider a coherent tone phase in the range from 0 to 180°. At some phase ϕ_amp, the coherent state will get maximally amplified and for $\phi = \phi_\mathrm{amp} + 90°$ the coherent state will be maximally deamplified. We perform this measurement for different pump powers and extract the maximum gain, which can be seen on panel (a) in Fig. 3.9. We observe high degenerate gains of up to 40 dB at -26 dBm of the pump power. A high degenerate gain could lead to a high quantum efficiency but it also implies a low compression point, where higher-order nonlinearities start to manifest. Above this compression point, the JPA no longer acts as a linear amplifier and the resulting output states are no longer Gaussian. As the result, we need to find a compromise between high degenerate gains and high compression powers. Compression effects are characterized by the 1 dB compression point, which is defined as the signal power at which the degenerate gain is decreased by 1 dB from its maximal value. The resulting measurement can be seen in Fig. 3.9(b). Here, the 1 dB compression point is approximately -127 dBm of the input power for -30 dBm of the pump power. As described in Sec. 2.3.5., our analysis relies on the assumption that all quantum states remain Gaussian during the communication. In our protocol, displacements are drawn from a Gaussian distribution. As a result, we ensure that

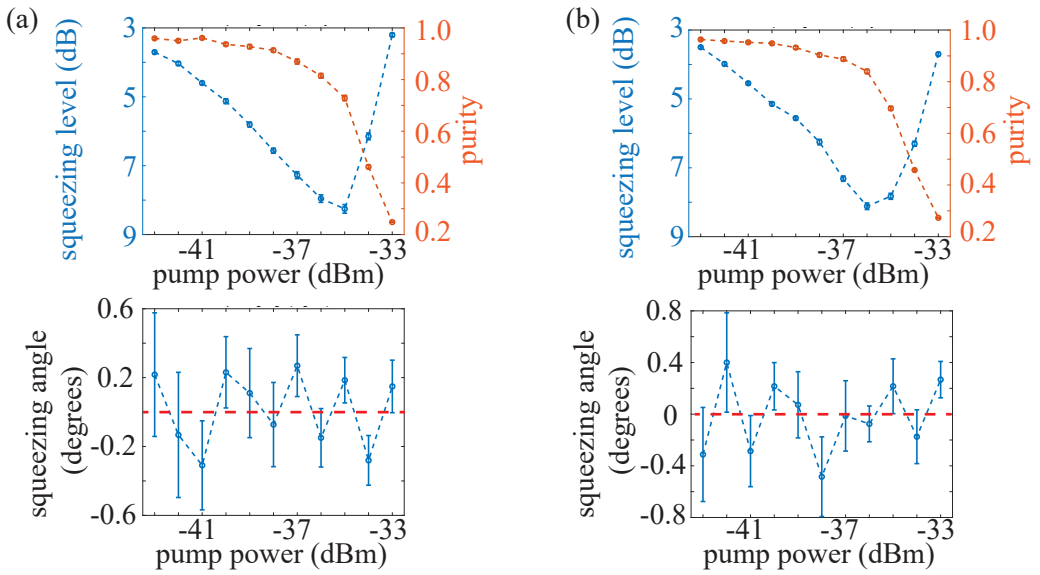

Figure 3.10: Squeezing level, purity, and squeezing angle measurements. For 200 kHz FIR filter bandwidth (panel (a)) and 400 kHz FIR filter bandwidth (panel (b)). Remarkably, the squeezing level and associated purity do not differ significantly from one bandwidth to another. As such, our calibration measurements can be made with the larger FIR filter bandwidth and as the result, with a faster displacement modulation (see Sec. 3.2.7)

the displacement powers are chosen such, that they dont drive the JPA 2 into compression. In our measurements we check that for displacement powers corresponding to a 3 σ_A interval are below the compression power of the JPA 2. This guarantees that no non-Gaussian contribution have to be taken into account later. We note here that during the protocol we can utilize the Gaussianity tests introduced in Sec. 2.1.2 to ensure Gaussianity of the measured data, implying linear amplification.

3.2.6 Calibration measurements

In this section we present all other necessary calibration steps in order to execute the microwave CV-QKD protocol. All of these measurements depend on the chosen working point.

Squeezing The experimental implementation of our protocol requires well-calibrated and controlled squeezed states. To measure the squeezed and antisqueezed variances of each squeezed states, we apply a pump tone at twice the chosen resonance frequency to operate the JPA in the phase-sensitive regime. Unlike with the degenerate gain measurements, we do not send a coherent input state to the JPAs, but instead amplify weak thermal states present in our sample stage at T =15 mK due to the finite temperature of our sample stage. These states serves as an input to our JPAs. Using the reference state reconstruction method, we reconstruct each quantum state propagating out of our JPAs. In order to get a reference state for the reconstruction method, we modulate the pump tone sent to the JPA in time. The modulation scheme consists of 2 parts, one where the JPA pump is off, and another where the JPA pump is on. This pattern is repeated for

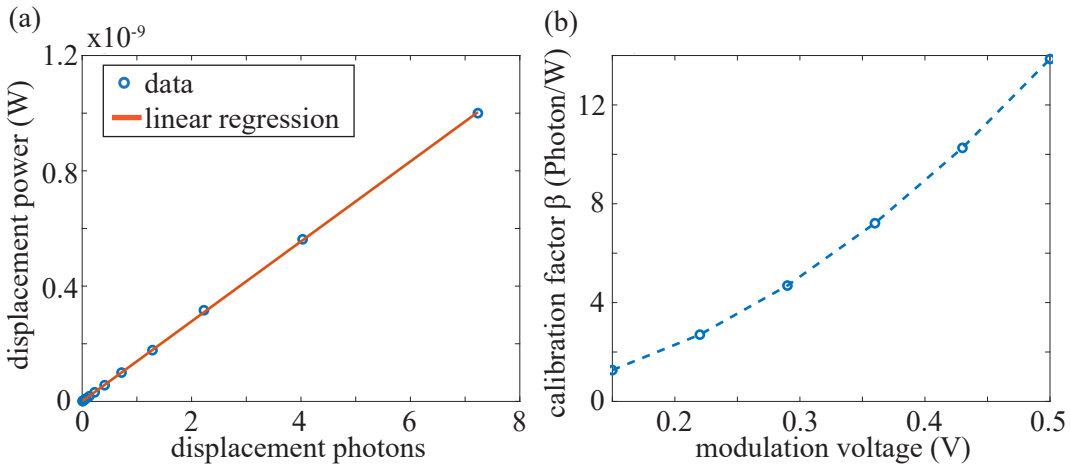

Figure 3.11: (a) Displacement power calibration for 0.36 V amplitude of the IQ modulation voltage. We observe the expected linear relation. (b) Linear regression slope coefficient as a function of the modulation voltage. With this we can predict the expected displacement both as a function of SGS power and SGS modulation voltage.

different pump powers. From these measurements, we extract the squeezing level S, defined as

$$S = -10 \log_{10} \left(\frac{\sigma_S^2}{0.25} \right), \tag{3.9}$$

where σ_S^2 is the squeezed variance and 0.25 is the vacuum variance. From the measurement shown in Fig. 3.10, we see that the squeezing level increases with the pump power up to a certain point, then, it decreases. We additionally calculate the purity from Sec. 2.1.2, which is monotonically decreasing with the pump power. This is due to the increased noise of the JPA with the increasing pump power. From the squeezing measurements, we observe that the squeezing angles can be reliably stabilized within a precision of less than 1°. For each data point, we perform at least two measurements. For the first measurement, we calculate the squeezing angle from the measured second order quadrature moment matrix by fitting it to the single-mode squeezed state covariance matrix introduced in Sec. 2.1.2. For subsequent measurements, we adjust the pump tone phase in order to change the squeezing angle to a target value, as mentioned in Sec. 3.2.2. As a result, we discard the first measurement in our analysis. This measurement also yields us the antisqueezed variance σ_{AS}^2m which defines the modulation variancem $\sigma_A^2 = \sigma_{\mathrm{AS}}^2 - \sigma_S^2$ and the variance for the subsequent displacement amplitudes encoding the Gaussian-distributed classical key. This makes the ensemble average state look like a thermal state, as seen in Sec. 2.4.2. The modulation variance also defines the corresponding $3\sigma_A$ interval which covers approximately 99.7% of the drawn displacement numbers.

Displacement power calibration Using the highly asymmetric directional coupler, we can displace quantum states, as discussed in Sec. 2.1.2. We send a strong coherent signal ($P_d \approx -120$ dBm) to the first directional coupler. The power and phase of the coherent tone define the number of the displacement photons, $n_{\mathrm{disp}} = |\alpha|^2$, and the displacement angle, ϕ, respectively. In order to find out the relation between the displacement power and displacement photons, we

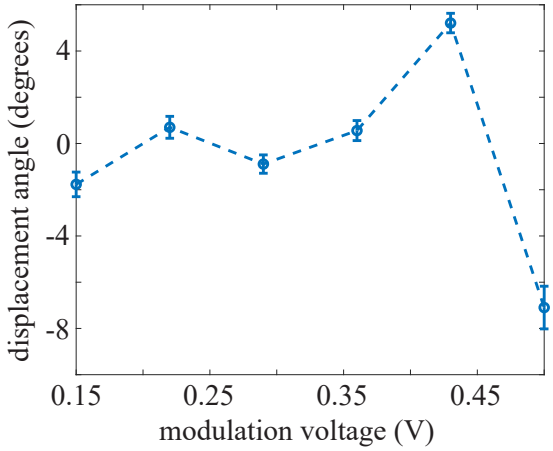

Figure 3.12: Displacement angle as a function of modulation voltage from 0.15 to 0.5 V. We observe stability of the angle within roughly 10°.

set up a time modulation scheme with two parts. The first part serves as a weak thermal state reference, when the coherent tone is switched off. In the second part, the coherent signal is ON. In addition, we modulate the SGS device power with six evenly spaced voltage amplitudes, in the range between 0.15 V and 0.5 V, implementing the time domain multiplexing in our CV-QKD protocol. Typically, we cover a large displacement power range to perform a better fit of the measured displacement amplitudes. In particular, we fit the displacement photon number, n_{disp}, as a function of the displacement power (in Watts) and modulation voltage with a linear function, $n_{\text{disp}} = cP_{\text{d}} + p_0$. Exemplary measurement results are shown in Fig. 3.11(a). From the fitted displacement photon number, we can convert any desired displacement photon number into a proper displacement power. Figure 3.11(b) shows the fitted displacement calibration factor as a function of the six modulation voltages. Figure Fig 3.12 shows the displacement angle during the displacement power modulation. We observe that the angle remains stable within 10° during the modulation.

Noise power calibration As discussed in Sec. 2.3.1, a quantum channel can be quantified by two parameters, losses and noise. Experimentally we can vary the noise, while keeping the losses constant. A controllable thermal noise can be generated by heating the input attenuator similarly to the PNCF measurements, but it would result in a large non-local heating over long times. Therefore, we generate our noise signals with an AFG at room tmperatures and couple it to the quantum channel via the second directional coupler. To calibrate the number of coupled noise photons to our signal, we use a two step modulation scheme, with a weak thermal state in the first part and the noise signal in the second. We reconstruct the noise photon, number $n_{\text{noise}} = \langle \hat{a}^\dagger \hat{a} \rangle$, which is fitted with a linear regression model, $n_{\text{noise}} = \alpha_{\text{n}} V_{\text{pp}}^2 + v_0$, with V_{pp} being the peak-to-peak voltage set at the AFG. An exemplary linear regressions is shown in Fig. 3.13.

Quantum efficiency We want to optimize the SNR in our protocol by minimizing the total added noise by both the pre-amplifier JPA 2 and the HEMT. We measure the quantum efficiency of our amplification using a 3 step modulation scheme. The first part is the reference

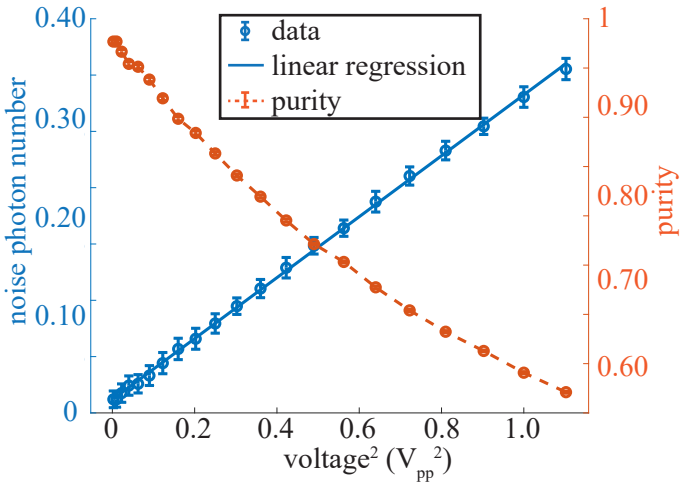

Figure 3.13: Noise photon number calibration for the AFG voltages of up to 1.1 V_{pp}^2. An expected decline in purity occurs, as more noise photons get coupled to signals propagating through the second directional coupler.

state, obtained when all devices are switched off, while the second part corresponds to the coherent displacement tone through the first directional coupler. This provides a well-calibrated reference displacement value, $|\alpha_{\mathrm{ref}}|^2$. In the third part, both the coherent tone and pump tone for the pre-amplifier JPA 2 are active, resulting in a corresponding amplified displacement, $|\alpha_{\mathrm{amp}}|^2 = G|\alpha_{\mathrm{ref}}|^2$. This procedure allows us to have an *in-situ* calibrated degenerate gain G for the preamplifier JPA. Additionally, we extract an amplification noise photon number, corresponding to the HEMT noise. Since our PNCF calibration does not include the preamplifier JPA gain, we rescale the measured quadrature variances by the gain G obtained from the first and second modulation steps. By combining variances measured at the different steps, we can extract the final amplification noise photon number n_{amp} as

$$n_{\mathrm{amp}} = n_{\mathrm{JPA}} + \frac{n_{\mathrm{H}}}{G} = \frac{\mathrm{Var}(\hat{q}_3)}{G} - \mathrm{Var}(\hat{q}_2) + \frac{n_{\mathrm{H}}}{G}, \tag{3.10}$$

where n_{JPA} and n_{H} are the noise photon numbers added to one quadrature at the input of the JPA 2 and the HEMT, respectively, and G is the JPA 2 gain. Also variances of $\hat{x}_2$ and $\hat{x}_3$ are the quadrature variances for the second and third part of the modulation scheme, respectively. Here, we use that the amplified coherent state variance is given by $\mathrm{Var}(\hat{x}_3) = G\,\mathrm{Var}(\hat{x}_2) + Gn_{\mathrm{JPA}}$. Then, finally we compute the quantum efficiency

$$\eta = \frac{1}{1 + 2n_{\mathrm{amp}}}. \tag{3.11}$$

An exemplary measurement of the quantum efficiency as a function of the JPA gain can be seen in Fig. 3.14. With increasing degenerate gain, the quantum efficiency increases, as long as the noise added by the JPA does not become larger than the HEMT noise scaled down by the JPA gain. However, with high enough pump powers, at the higher degenerate gain values, we can see a decrease in the quantum efficiency, when the noise of the JPA, scaled by the HEMT gain, outweighs the HEMT noise itself. Using the extracted quantum efficiency, we have to optimize for the choice of different pump powers for both of our JPAs: (i) the JPA 1 defines the

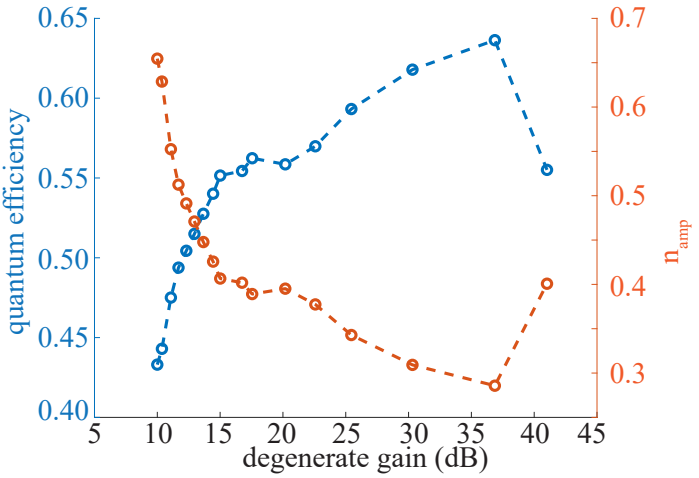

Figure 3.14: Quantum efficiency and corresponding partial amplification noise photons n_{amp} as a function of JPA 2 degenerate gain. The quantum efficiency is obtained from the amplification noise photon number n_{amp} added to a coherent state with -142 dBm input power by JPA 2. Quantum efficiencies of up to 63% at 36 dB of degenerate gain can be reached.

squeezing level and the modulation variance, which defines the $3\sigma_{\text{A}}$ interval, within which we expect 99.7% of the displacement photon numbers, (ii) the JPA 2 defines the quantum efficiency and the compression point, which ultimately limits the displacement modulation variance. The chosen pump powers are selected to optimize for the displacement photon number variance σ_{A} while accounting for constraints (i) and (ii). This results in a compromise choice. We can choose a lower JPA 2 pump power, resulting in a lower degenerate gain and quantum efficiency, but increases the compression power, allowing for a larger modulation variance.

3.2.7 Rapid displacement modulation

Displacement modulation in our protocol During the last part of our CV-QKD protocol we activate all of the aforementioned devices. We can use the IQ modulation ports of the SGS source that provides the coherent tone. By supplying a constant voltage to these ports, we effectively modulate the device power, resulting in a lower or higher displacement for lower or higher voltages, respectively. Based on the analysis described in Sec. 2.4.2, we measure multiple key elements within the pulse sequence, as shown in Fig. 3.15(a). For this, we use the HDAWG with a modulation voltage of up to 0.5 V. We use the displacement power calibrations for each of the modulation voltages, as presented in Fig. 3.11, and get corresponding displacement conversion factors c_i, where $i = 1, 2, ...N_{\text{disp}}$, N_{disp} being the number of modulated displacement values. The different conversion factors that we get for modulation voltages V_{mod} of 0.15 to 0.5 V are shown in Fig. 3.11(b). In order to obtain a key of longer length, we can combine all Gaussian key elements from each displacement modulation step. By merging N_{disp} Gaussian distributions together, each with an individual variance σ_i, we end up with a total variance of

$$\sigma_{\text{tot}}^2 = \frac{1}{N_{\text{disp}}} \sum_{i=1}^{N_{\text{disp}}} \sigma_i^2. \tag{3.12}$$

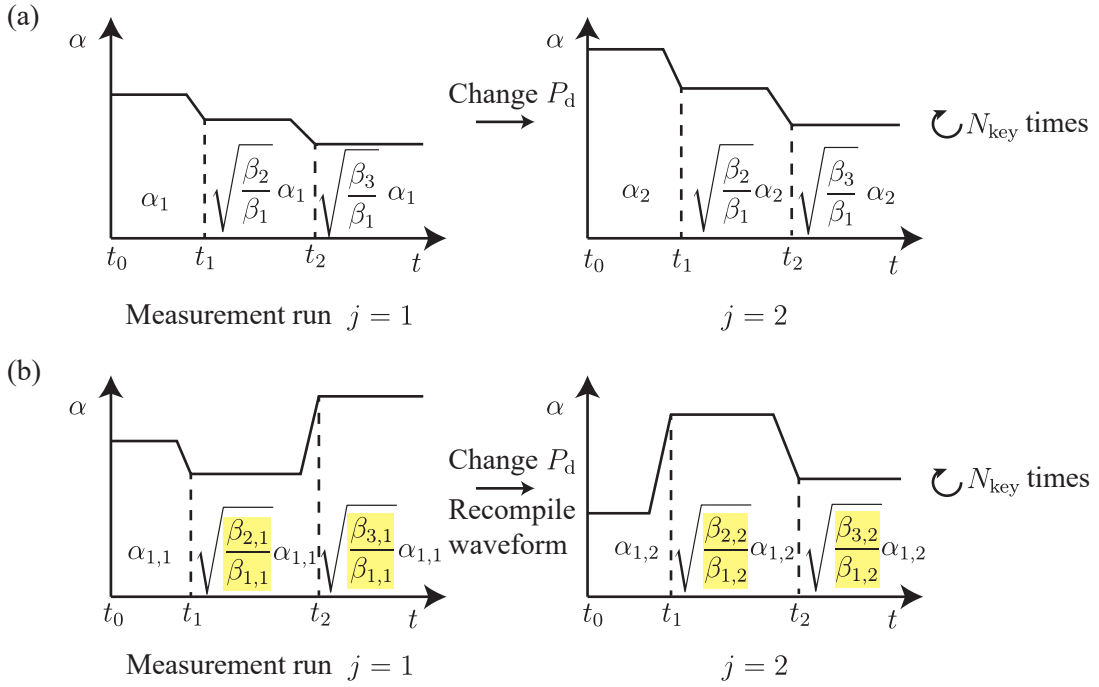

Figure 3.15: Illustration of two different displacement modulation schemes. The modulation times t_i can be arbitrarily placed as long as $\Delta t_i = |t_{i+1} - t_i| > 1/f_{\text{FIR}}$. (a) Displacement modulation for the constant modulation voltage for each measurement run. The ratio of displacement remains the same for each modulation step throughout the measurement. (b) Displacement modulation with the adapted modulation voltage, highlighted in yellow as $c_{i,j}$. Each measurement run requires different modulation voltages to generate the corresponding displacement $\alpha_{i,j}$.

Based on our experimental implementation of the protocol the total displacement modulation variance, σ^2_{tot}, must fulfill both the compression constraint and the CV-QKD protocol condition, $\sigma^2_{\text{tot}} = \sigma^2_{\text{AS}} - \sigma^2_{\text{S}}$. We can express the variances of the modulated Gaussian distributions, σ_i^2, with the relative conversion factors c_i: (i) for the first modulated symbol we set a device power $P_{\alpha_1} = |\alpha_1|^2/c_1$ to generate the displacement α_1 with the conversion factor c_1. Linear offsets in the displacement fits are not taken into account here, since all measured offsets are close to zero and orders of magnitude smaller than the displacement conversion factors. Then, (ii) with this constant device power P_{α_1}, we change the modulation voltage resulting in a conversion factor c_2. This implies that $|\alpha_2|^2 = c_2 P_{\alpha_1} = c_2/c_1|\alpha_1|^2$. Finally, (iii) the second displacement α_2 can be considered as drawn from a second Gaussian distribution. The variance of this second Gaussian distribution is given by $\sigma_2^2 = \text{Var}(\alpha_2) = \text{Var}(\sqrt{c_2/c_1}\alpha_1) = c_2/c_1\sigma_1^2$. This is only valid if $\arg(\alpha_2) = \arg(\alpha_1)$, i.e., if the phase of the coherent source remains stable within the modulation voltage change. We experimentally verify from the protocol measurements in Sec. 4.1.1 that the modulated variances fulfill this relation, proving that the phase remains stable during the modulation. This leads to a generalized expression:

$$\sigma_i^2 = \frac{c_i}{c_j}\sigma_j^2. \tag{3.13}$$

Based on this procedure, we express the total variance based on these individual variances as

$$\sigma_{\text{tot}}^2 = \frac{1}{N_{\text{disp}}}\sigma_1^2\left(1+\sum_{i=2}^{N_{\text{disp}}}\frac{c_i}{c_1}\right). \tag{3.14}$$

Therefore, by using the measured c_i, we can calculate the modulation variance σ_1^2 of the displacement photons for the first modulated symbol. From equation Eq. 3.14 we compute

$$\sigma_1^2 = \sigma_{\text{tot}}^2 N_{\text{disp}}\left(1+\sum_{i=2}^{N_{\text{disp}}}\frac{c_i}{c_1}\right)^{-1}. \tag{3.15}$$

We choose σ_1^2 to be the largest individual variance, i.e., that $c_1 > c_i\ \forall i \in [1, N_{\text{disp}}]$. In particular, we note that

$$\left(1+\sum_{i=2}^{N_{\text{disp}}}\frac{c_i}{c_1}\right) < 1+\left(1+\sum_{i=2}^{N_{\text{disp}}}1\right) = N_{\text{disp}}, \tag{3.16}$$

which implies that $\sigma_1^2 > \sigma_{\text{tot}}^2$ according to Eq. 3.15. So the maximum individual displacement variance is always larger than the total displacement variance. This is especially relevant when $c_i/c_1 \ll 1$, which is encountered when many modulation voltages ($N_{\text{disp}} \gg 1$) are used, as this leads to the case $\sigma_1^2 \gg \sigma_{\text{tot}}^2$. As a result the displacements obtained for the first variance σ_1 can be significant and exceed the power limit before the preamplifier JPA 2 enters the compression and, therefore, limits the maximum individual displacement variance that can be experimentally tolerated. This results in a limitation for the squeezing level and for the measurement SNR. As a result, the performance of our CV-QKD protocol depends strongly on the choice of the maximal individual variance σ_1^2. Respectively, we choose a compromise between a higher repetition rate or a lower key rate.

Alternatively, as it is shown schematically in Fig. 3.15(b), we can vary the modulation voltage during the measurement and consider N_{disp} Gaussian distributions with the same variance σ_{A}^2 and number of key elements N_{key}. In the following, we denote a displacement value $\alpha_{i,j}, i = 1...N_{\text{disp}}, j = 1...N_{\text{key}}$ as the displacement value for modulation step i drawn from Gaussian distribution number j. For each measurement run j we get the desired displacement values $\alpha_{i,j}$ for all modulation steps $i = 1...N_{\text{disp}}$ from a Gaussian distribution with the variance σ_{A}^2. Values of $\alpha_{i,j}$ can be linked to α_1, j using the relation $\alpha_{i,j}^2 = c_{i,j}P_{1,j}$ for $P_{1,j}$ being constant during the measurement trace j. This leads to $c_{i,j} = (\alpha_{i,j}/\alpha_{1,j})^2 c_{1,j}$ by using $\alpha_{1,j}^2 = c_{1,j}P_{1,j}$. The modulation voltage $V_{i,j}$ to get the corresponding conversion factor $c_{i,j}$ is set only during the modulation time t_i, corresponding to the displacement $\alpha_{i,j}$, and changes for each measurement run. However, this requires changing the modulation voltage for each modulation step for every displacement value $\alpha_{1,j}$ and requires recompiling the trigger pulse sequence N_{key} times which could induce an increased dead time. A possible approach would be to run a Matlab script to compute the correct pulse sequence and compile this new sequence for each measurement run j. Further tests are needed here in order to determine the stability and efficiency of this approach. Since now the N_{disp} Gaussian distributions would be independent and with the same variance, the total variance of the combined key elements remains unchanged: $\sigma_{\text{tot}}^2 = \sigma_A^2$ allowing for less measurement constraints as compared to the previous method.

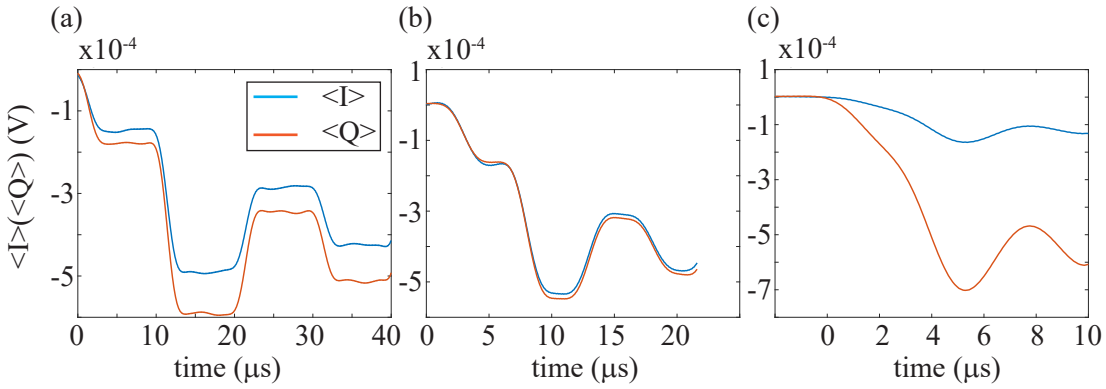

Figure 3.16: First order quadrature moments $\langle I \rangle$ and $\langle Q \rangle$, for four sequential displacement modulation voltages. The time between modulation voltage steps is (a) $\Delta t_{\text{mod}} = 10$ μs, (b) $\Delta t_{\text{mod}} = 5$ μs, and (c) $\Delta t_{\text{mod}} = 2.5$ μs. The total measurement trace time length is given by $4\Delta t_{\text{mod}}$. In panel (c) we observe smearing of the modulation steps once $\Delta t_{\text{mod}} < 1/f_{\text{FIR}} = 5$ μs for a 200 kHz FIR filter.

Limitations of displacement modulation frequency As discussed in Sec. 3.2.2, we use the FIR filter in the FPGA. This means that, while the HDAWG can reliably generate waveforms on a nanosecond scale, the FIR filter limits our modulation frequency, as illustrated in Fig. 3.16. We experimentally investigate an accessible modulation frequency by setting four displacement modulation voltage steps and reducing the time, Δt_{mod}, between them from 10 μs to 2.5 μs. With the 200 kHz FIR filter we expect to resolve temporal features which are longer or equal to $t_{\text{res}} \approx 1/f_{\text{FIR}} = 5$ μs. Reducing Δt_{mod} results in a smearing of the modulation steps. This smearing deteriorates the accuracy and stability of the measured displacements, as compared to their desired setpoints. This effect is particularly pronounced in the case of $\Delta_{\text{mod}} < t_{\text{res}}$. For this reason we test the performance of our system with different FIR bandwidths, as presented in Fig. 3.10. From these measurements, we infer that a doubling of the FIR bandwidth does not deteriorate the squeezing level or noise properties of our JPA, while allowing to double the symbol frequency and, ideally, the QKD secret key rate. This can be considered when optimizing for the final bit rate in our experimental implementation, $R_{\text{bit}} = R^{\text{fin}}_{\text{rate}} \cdot f_{\text{symbol}}$. Further increasing of the FIR filter bandwidth would lead to an increased rate up to a certain limit, where the JPA squeezing and noise properties would deteriorate due to an increasingly larger noise coupled via the larger bandwidth.

Chapter 4

Results and discussion

4.1 Protocol with displacement modulation

In this section we will analyze and discuss an executed microwave CV-QKD protocol measurement with 19996 exchanged displaced squeezed states at the carrier frequency of $f_r = 5.856063$ GHz. We first calculate the SNR and mutual information from the Shannon limit. Then, we calculate Eve's Holevo bound and estimate both the asymptotic and finite secret key rates.

4.1.1 SNR and mutual information

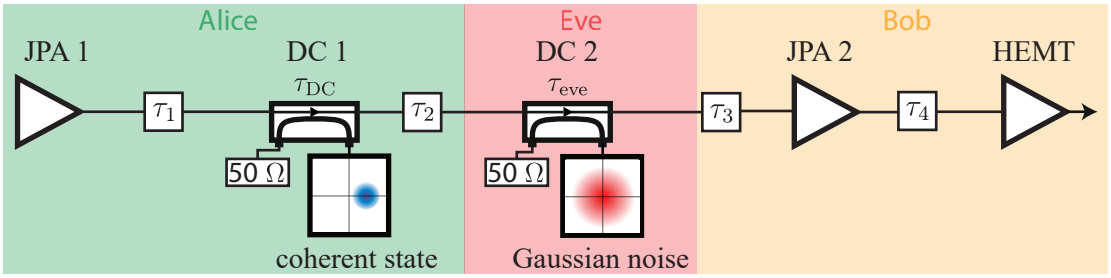

Figure 4.1: Schematic of the experimental setup. The transmissivity τ_i between the each functional part are the combined insertion losses and cable losses for each component. Eve (red) is assumed to be restricted to her directional coupler and unable to gain knowledge of Alice's (green) or Bob's (orange) signal before or after DC 2.

SNR The signal-to-noise ratio is defined as the ratio between signal and noise powers. The signal power is determined by the modulation variance at the HEMT, $\tau_{\text{eff}}\sigma_{\text{A}}^2$, with the transmissivity τ_{eff} between the first directional coupler and the HEMT. The noise power is determined by the variance of the received squeezed state measured at Bob's side, the coupled noise by Eve, and the added amplification noise of the cryogenic amplification chain. We note here that in the single shot measurement of Bob's symbols by the FPGA, we observe the noise of the entire amplification chain. However here we only consider the additional noise from the HEMT, since after this point the signal photon number is much larger than the noise photon number of further amplifiers. Figure 4.1 shows the transmissivity between the individual setup parts, taken from the respective part data sheets. With this, we compute the SNR

$$\text{SNR} = \frac{\tau_{\text{eff}}\sigma_{\text{A}}^2}{\sigma_{\text{B}}^2}, \tag{4.1}$$

with $\tau_{\text{eff}} = \tau_2\tau_3\tau_4\tau_{\text{eve}}$, the modulation variance σ_{A}^2, and the quadrature noise variance on Bob's

V_{mod} (amplitude)	0.15 V	0.22 V	0.29 V	0.36 V	0.43 V	0.5 V
σ_{i}^2 (photon number)	0.063	0.134	0.232	0.3577	0.508	0.686
SNR_{th}	0.1209	0.2495	0.3979	0.5867	0.8071	1.0232
SNR_{exp}	0.029(5)	0.053(4)	0.10(2)	0.14(2)	0.21(1)	0.27(2)

Table 4.1: Table showing the expected SNR for the corresponding modulation variance for each modulation voltage. The expected SNR is calculated with the previously shown calibration measurements and Eq. 4.1.

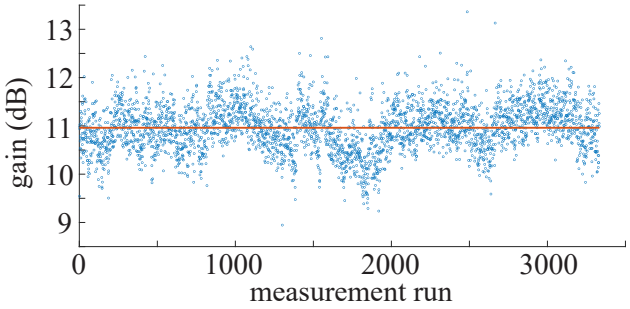

Figure 4.2: JPA 2 Gain extracted from the protocol phase stabilization, with the mean value plotted as the orange solid line. We observe the fluctuating degenerate gain. The mean gain value is 10.97 dB, noticeably lower than the expected 20.7 dB. The measured quantum efficiency from Fig. 3.14 at this gain is around 47%.

side σ_{Z}^2

$$\sigma_{\text{Z}}^2 = \tau_{\text{tot}}\sigma_{\text{S}}^2 + \tau_{\text{th}}\frac{1+2n_{\text{th}}}{4} + \tau_3\tau_4\left(\frac{1}{4}(1-\tau_{\text{eve}}) + \bar{n}\right) + n_{\text{amp}}, \tag{4.2}$$

with the total transmissivity $\tau_{\text{tot}} = \tau_1\tau_2\tau_{\text{DC}}\tau_{\text{eff}}$, with individual components in dB units $\tau_i = (0.5, 0.245, 0.31, 1.2182)$, the squeezed state variance σ_{S}^2, the coupled noise photons $\bar{n}$, the amplification noise n_{amp}, the thermal bath coupling $\tau_{\text{th}} = \tau_4\tau_3\tau_{\text{eve}}(1-\tau_1\tau_{DC}\tau_2) + (1-\tau_3\tau_4)$ and the thermal bath photon number $n_{\text{th}} \approx 3\cdot 10^{-4}$ at 50 mK. The measured SNR for all modulation voltages are shown in table 4.1. For this protocol measurement we use a constant modulation voltage modulation approach discussed in Sec. 3.2.7 and shown in Fig. 3.15(a). The number of exchanged states is 3333 for all, $N_{\text{disp}} = 6$, modulation voltages, resulting in the total symbol number of $m = 19996$. We observe the expected increase of the SNR with the modulation voltage, as the effective modulation variance increases with the modulation voltage (see Sec. 3.2.7). We operate the CV-QKD protocol with the squeezing level of $S = -7.96 \pm 0.11$ dB at the pump power of -36 dBm referred to the JPA 1 input. The total quadrature modulation variance, σ_{tot}^2, from Sec. 3.2.7 is 0.336. From the PNCF in Tab. 3.1 we obtain that the amplification chain adds 8.7 noise photons, which results in the total quantum efficiency of around 56% at the JPA 2 degenerate gain of 20.7 dB at -30 dBm pump power referred to the JPA 2 input. We measure the CV-QKD protocol with six different coupled noise photon numbers $\overline{n} \in \{0.074, 0.097, 0.156, 0.188, 0.215, 0.267\}$. With this we compute the expected noise variance on Bob's side and the expected SNR using Eq. 4.1. We observe that the measured SNR is about four times lower than the expected SNR. There are two most likely sources for this: (i) additional losses not considered in the PNCF reconstruction point from equation Eq. 3.8, (ii) lower quantum efficiency of the amplification chain due to a lower preamplifer gain. We provide

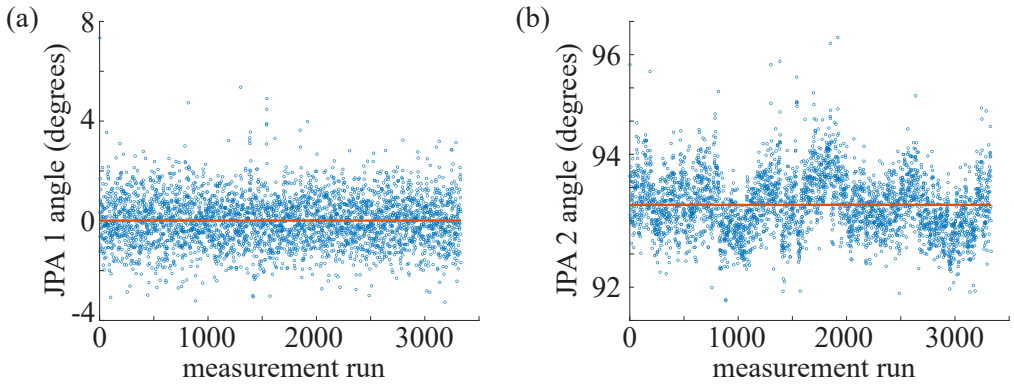

Figure 4.3: Squeezing and amplification phases extracted from the protocol phase stabilization, with the respective mean values shown with solid orange lines. We observe the stable phase of JPA 1 in panel (a) and JPA 2 in panel (b). This implies that the reduced mutual information is unlikely to be a phase stabilization problem.

V_{mod}	0.15 V	0.22 V	0.29 V	0.36 V	0.43 V
$r_{i,j}$	0.091	0.195	0.338	0.520	0.741
$\langle r_{i,j,\text{exp}} \rangle$	0.11(2)	0.20(2)	0.35(7)	0.53(6)	0.75(3)

Table 4.2: Measured SNR ratios, as defined in Eq. 4.3, extracted from the mean SNR over all coupled noise photon numbers versus expected variance ratios.

insights into the decrease of the SNRs by investigating the effects of transmissivity and coupled noise of the quantum channel obtained from statistical estimators (see Sec. 4.1.2).

SNR ratios From Eq. 4.1 We compute the ratio of the SNR for two modulation voltages V_i and V_j as

$$r_{i,j} \equiv \frac{\text{SNR}_i}{\text{SNR}_j} = \frac{\sigma^2_{\text{A},i}\sigma^2_{\text{Z},j}}{\sigma^2_{\text{A},j}\sigma^2_{\text{Z},i}} \approx \frac{\sigma^2_{\text{A},i}}{\sigma^2_{\text{A},j}} = \frac{c_i}{c_j}, \tag{4.3}$$

with the displacement power calibration factor c_i for modulation voltage V_i. We use that the noise on Bob's side should remain similar for all modulation voltages and Eq. 3.13 at the last step. Table 4.2 shows the SNR ratios for all modulated symbols. In this calculation, we took an average over all six different coupled noise photon number values to get the SNR ratio for two modulation voltages V_i and V_j with more statistics:

$$\frac{\langle \text{SNR}_i \rangle}{\langle \text{SNR}_j \rangle} = \frac{\sigma^2_{\text{A},i}\,\langle \sigma^2_{\text{Z},j} \rangle}{\sigma^2_{\text{A},j}\,\langle \sigma^2_{\text{Z},i} \rangle}, \tag{4.4}$$

where $\langle . \rangle$ denotes the mean over all six coupled noise photon numbers. We used here that $\sigma^2_{\text{A},i}$ does not depend on the coupled noise photon number. In addition, we divide the noise on Bob's side into two parts:

$$\sigma^2_{\text{Z}} = \sigma^2_{\alpha} + \sigma^2_{\bar{n}}, \tag{4.5}$$

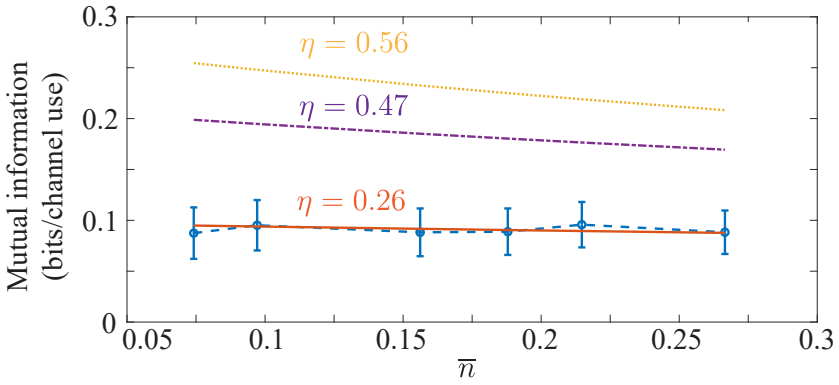

Figure 4.4: Measured mutual information (blue) of the combined symbols compared to the mutual information expected from the calibration with $\eta = 56\%$ at a JPA 2 gain of 20.7 dB (yellow) and $\eta = 47\%$ at a JPA 2 gain of 10.97 dB (purple) as a function of the coupled noise, $\overline{n}$. We also show the mutual information with $\eta = 26\%$ at a JPA 2 gain of 7 dB (orange).

where σ_α^2 contains all contributions in Eq. 4.2 except for the coupled noise variance $\sigma_{\overline{n}}^2$. With this, we express the mean of the SNR ratios as

$$\frac{\langle \mathrm{SNR}_i \rangle}{\langle \mathrm{SNR}_j \rangle} = \frac{\sigma_{\mathrm{A},i}^2(\sigma_{\alpha,j}^2 + \langle \sigma_{\overline{n},j}^2 \rangle)}{\sigma_{\mathrm{A},j}^2(\sigma_{\alpha,i}^2 + \langle \sigma_{\overline{n},i}^2 \rangle)} \approx \frac{c_i}{c_j}. \tag{4.6}$$

In the last step we used that $\sigma_{\alpha,i}^2$ and $\langle \sigma_{\overline{n},i} \rangle^2$ do not change with the modulation voltage, which implies that the ratio of the mean SNR remains c_i/c_j. We observe that the measured mean SNR ratio matches well with the predicted value from Sec. 3.2.7.

Mutual information Using the combined measured symbols, we compute the ensemble mutual information based on Eq. 2.119, which simplifies to

$$I(A:B) = \frac{1}{2}\log_2\left(1 + \frac{\tau\sigma_{\mathrm{A}}^2}{\sigma_{\mathrm{B}}^2}\right) = \frac{1}{2}\log_2\left(1 + \mathrm{SNR}\right), \tag{4.7}$$

We note that the last expression only depends on the measured SNR, which is independent of quadratures rescaling and, therefore, independent of the PNCF calibration. We observe from Fig. 4.4 that the measured mutual information does not align well with the expected mutual information calculated using a quantum efficiency of $\eta = 56\%$ at 20.7 dB of the JPA 2 degenerate gain. For further investigation we utilized a part of the protocol measurement used for the phase stabilization to calculate the degenerate gain of the JPA 2 and the squeezing and amplification phases of the JPA 1 and JPA 2, respectively, for each measurement run. Technically, the phase can drift between the phase stabilization and the protocol measurements, however, since the phase drift is rather slow on the order of minutes, the phase during the phase stabilization is a good approximation for the phase during the protocol measurement. If the amplification phase is unstable, the sent displacement would not get amplified along the correct quadrature axis, effectively resulting in a lower degenerate gain of the JPA 2, since we calculate the mutual information using only the real part of the displacement. However, we observe from Fig. 4.3 that the

amplification and squeezing phases are rather stable, implying that it is unlikely that the problem lies here. In addition to the amplification phase, the coherent tone phase could be unstable. The unstable coherent tone phase would change the displacement phase and could, therefore, reduce the modulation variance during the protocol. Unfortunately, in this case we cannot simply check the phase of the coherent tone pulse during the phase stabilization, as the coherent tone phase shows high instability when changing the coherent signal power. In this case, the previous assumption that the phase measured during phase stabilization is similar to the stabilized phase during the measurement run is invalid. Assuming that the displacement phase is slightly off by $\Delta\phi$, the output state after the preamplifier is given by

$$\bar{\mathbf{r}} = \left(\sqrt{G_{\text{JPA2}}}\cos(\Delta\phi)|\alpha|, \frac{\sin(\Delta\phi)|\alpha|}{\sqrt{G_{\text{JPA2}}}}\right), \quad \mathbf{\Sigma} = \begin{pmatrix} G_{\text{JPA2}}\sigma_{\text{S}}^2 & 0 \\ 0 & \frac{\sigma_{\text{AS}}^2}{G_{\text{JPA2}}} \end{pmatrix}, \tag{4.8}$$

with the JPA 2 gain, G_{JPA2}, the squeezed and antisqueezed quadratures $\sigma_{\text{S}}^2, \sigma_{\text{AS}}^2$ and the sent displacement $\alpha = e^{i\Delta\phi}|\alpha|$, where the encryption basis is $x = q$. Assuming that an error in the displacement phase is Gaussian-distributed with mean of 0 and variance σ_ϕ^2, this implies that the average real displacement along the q quadrature is $\sim \cos(\sigma_\phi)|\alpha|$. Since JPA 2 amplifies the displacement of the state along the q quadrature, this results in a reduced modulation variance by a factor of $\cos^2(\sigma_\phi) \approx 0.97$ for $\sigma_\phi \sim 10°$. Since the deviation from the expected SNR is much higher than a factor of 0.97, this is not likely to be the cause. To investigate the gain during the phase stabilization, we use the amplified vacuum state variances

$$\sigma_{\text{S}}^2 = (1 + 2n_{\text{JPA}})e^{-2r} = \tilde{n}G^{-1}, \tag{4.9}$$

$$\sigma_{\text{AS}}^2 = \tilde{n}G, \tag{4.10}$$

with the JPA noise photon number n_{JPA} and gain G. From this we compute the gain $G = \sqrt{\sigma_{\text{AS}}^2/\sigma_{\text{S}}^2}$. With this we compute the gain of the JPA 2. From Fig. 4.2, we observe that this degenerate gain is both fluctuating in time and lower than the expected 20.7 dB. We measure a mean degenerate gain of 10.97 dB averaged over all measurement runs. From the quantum efficiency calibration in Fig 3.14 we expect a quantum efficiency of around 47% at this gain. We observe from Fig. 4.4 that the mutual information computed with a gain of 10.97 dB and a quantum efficiency of 47% matches the data better, but still pretty badly. We should note here that during the protocol phase stabilization we use $8 \cdot 10^4$ FPGA averages, which is significantly lower than the typical FPGA averages of around $2 \cdot 10^5 - 4 \cdot 10^5$ we use for the degenerate gain calibration, which might impact the accuracy of this method. Still, we observe that the mutual information using this method matches with the result from the protocol measurement better than the expected gain of around 20 dB. Using the Gaussianity tests discussed in Sec. 2.1.2, we find that the Anderson-Darling and Shapiro-Wilk test both do not reject the null hypothesis of Bob's measured symbols being Gaussian with unknown mean and variance with a 5% confidence level for all noise voltages. This suggests that our measured CV-QKD protocol data is likely to be Gaussian. This excludes the amplifier compression effects as the underlying problem for the observed reduction in gain. The decrease in gain might be a result of trapped flux changing between the calibration measurements and the CV-QKD protocol measurement. This would effectively change the resonance frequency of the JPA and could cause the observed gain decrease. In addition, this resonance shift most likely also reduces the quantum efficiency.

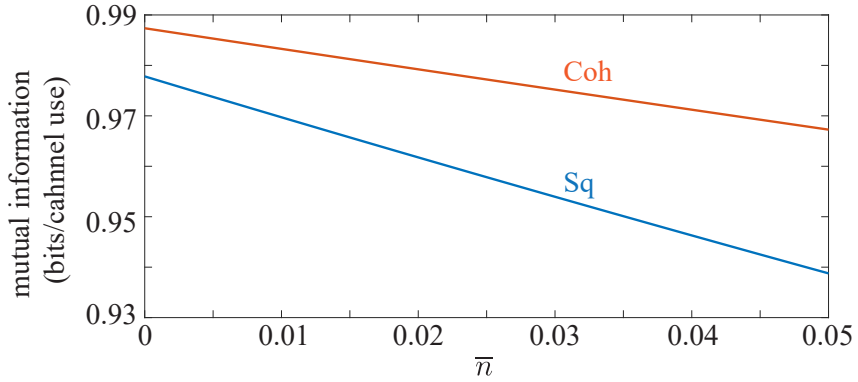

Figure 4.5: Computed mutual information for the squeezed and coherent protocol. We observe similar results for both protocols due to the increased effect of the amplification noise for the heterodyne detection in the coherent protocol.

4.1.2 Eve's Holevo information

Adaptations to theory regarding Alice's input state The experimental protocol deviates a bit from the discussed protocol in Sec. 2.4.2. We assume that the eavesdropper is restricted to its channel implemented with the second directional coupler, DC 2. All other transmissivities and noise beyond the second directional coupler are assumed to be trusted, i.e., do not affect the Holevo bound on Eve's information. In order to calculate the Holevo bound we need to know Alice's input state at the second directional coupler and the corresponding individual and average states of Eve at the output of DC 2. Alice's state at the JPA 1 output is a squeezed state that experiences the transmissivity τ_1 before reaching the first directional coupler, where the state gets displaced. At the input of the second directional coupler Alice's state is given by

$$\overline{\mathbf{r}}_{\mathrm{A,DC2}} = \begin{pmatrix} \sqrt{\tau_2}\alpha_{\mathrm{q},i} \\ 0 \end{pmatrix} \boldsymbol{\Sigma}_{\mathrm{A,DC2}} = \begin{pmatrix} \tau_1\tau_2\tau_{\mathrm{DC}}\sigma_{\mathrm{S}}^2 & 0 \\ 0 & \tau_1\tau_2\tau_{\mathrm{DC}}\sigma_{\mathrm{AS}}^2 \end{pmatrix}, \tag{4.11}$$

assuming the encoding basis $x = q$. The corresponding average state at the input of DC 2 is given by

$$\overline{\mathbf{r}}_{\mathrm{A,DC2}} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \boldsymbol{\Sigma}_{\mathrm{A,DC2}} = \begin{pmatrix} \tau_1\tau_2\tau_{\mathrm{DC}}\sigma_{\mathrm{S}}^2 + \tau_2\sigma_{\mathrm{A}}^2 & 0 \\ 0 & \tau_1\tau_2\tau_{\mathrm{DC}}\sigma_{\mathrm{AS}}^2 \end{pmatrix}. \tag{4.12}$$

From Eq. 4.12, we compute a modified indistinguishability condition of the encoding bases $\sigma_{\mathrm{A}}^2 = \tau_1\tau_{\mathrm{DC}}(\sigma_{\mathrm{AS}}^2 - \sigma_{\mathrm{S}}^2)$ that makes the average DC 2 input state look like a thermal state regardless of the chosen encoding basis x. This input state replaces the input displaced squeezed state from Sec. 2.4.2. The remaining calculation for Eve's average and individual states remains the same. This implies that only the transmissivity, τ_{eve}, and noise, $\overline{n}$, introduced by Eve affect the Holevo bound, χ_{E}. However, the signal line transmissivity and noise still affect the SNR and, therefore, the mutual information between Alice and Bob.

Computation of estimators from covariance matrix By using the measured symbols, α_i, β_i, from the protocol we compute the covariance matrix of Alice's and Bob's shared symbols

$$\begin{pmatrix} \sigma_{\mathrm{A}}^2 & \mathrm{Cov(A,B)} \\ \mathrm{Cov(A,B)} & \sigma_{\mathrm{B}}^2 \end{pmatrix}. \tag{4.13}$$

$\overline{n}$	0.074	0.097	0.156	0.188	0.215	0.267
$\tilde{\overline{n}}$	2.739	2.808	2.874	2.809	2.953	2.920
$\tilde{\tau}_{\text{eff}}$	0.970	1.069	1.006	0.999	1.107	1.017
$\tilde{\overline{n}}_{\text{opt}}$	0.067	0.102	0.135	0.103	0.174	0.158
$\tilde{\tau}_{\text{eff,opt}}$	0.605	0.667	0.628	0.624	0.691	0.634

Table 4.3: Transmission and noise estimators for all six coupled noise photon numbers assuming a degenerate gain of 10.97 dB and the expected quantum efficiency at this gain of 47%. We note that the estimators match badly. Also shown are the estimators $\tilde{\overline{n}}_{\text{opt}}, \tilde{\tau}_{\text{eff,opt}}$ for a degenerate gain of 13 dB and a quantum efficiency of $\eta = 26\%$, which matches the experimental values well, however this quantum efficiency does not match the expected quantum efficiency at this gain from the calibration, which is around 52%.

With this we can compute the estimators. However, we have to take the degenerate gain of JPA2 into account for Bob's measured symbols and rescale his symbols by $1/\sqrt{G_{\text{JPA2}}}$. In addition, the estimated transmissivity is not the total transmissivity between the JPA 1 and the HEMT, but rather the one between the first directional coupler and the HEMT, since the displacement photons are calibrated at the first directional coupler and the PNCF is referenced to the input of the HEMT. In the following, we denote an estimator for the corresponding channel parameter, x, as $\tilde{x}$. Using the adapted estimators from Sec. 2.4.3, we estimate the effective transmissivity and noise variance, $\tilde{\tau}_{\text{eff}} = \tilde{\tau}_{\text{eve}}\tau_2\tau_3\tau_4$ and $\tilde{\sigma}^2_{\text{Z}}$. With the expected contributions to transmissivity and noise from our trusted setup using the calibrations from Sec. 3.2.6, we compute the estimator $\tilde{\tau}_{\text{eve}}$ by inverting the equation for $\tilde{\tau}_{\text{eff}}$ and $\tilde{\overline{n}}$ by inverting Eq. 4.2. The estimators and their variance become

$$\tilde{\tau}_{\text{eve}} = \frac{\tilde{\tau}_{\text{eff}}}{\tau_2\tau_3\tau_4}, \quad \text{Var}(\tilde{\tau}_{\text{eve}}) = \frac{\text{Var}(\tilde{\tau}_{\text{eff}})}{(\tau_2\tau_3\tau_4)^2}, \tag{4.14}$$

$$\tilde{\overline{n}} = \frac{\tilde{\sigma}^2_{\text{Z}} - \tau_{\text{th}}n_{\text{th}} - n_{\text{amp}} - \tau_1\tau_{\text{DC}}\tilde{\tau}_{\text{eff}}\sigma^2_{\text{S}}}{\tau_3\tau_4} - \frac{1}{4}(1 - \tilde{\tau}_{\text{eve}}). \tag{4.15}$$

Under the assumption that the estimators for noise and transmissivity are independent, we compute the variance of the estimated coupled noise to

$$\text{Var}(\tilde{\overline{n}}) \approx \frac{1}{(\tau_3\tau_4)^2}\text{Var}(\tilde{\sigma}^2_{\text{Z}}) + \left(\tau_1\tau_2\tau_{\text{DC}}\sigma^2_{\text{S}} + \frac{1}{4}\right)^2 \text{Var}(\tilde{\tau}_{\text{eve}}). \tag{4.16}$$

With this we can compute the worst case estimator for the coupled noise and transmissivity, i.e., compute the standard deviation and build a sigma interval that contains the true coupled noise and transmissivity with a probability up to ϵ_{PE}. With this, we can construct Eve's TMS input state and compute the worst-case Holevo information based on Alice's and Bob's symbols. We observe from the estimators shown in Tab. 4.3 that our estimators match the experimental parameters rather poorly. We notice that to get close to the calibrated experimental parameters, we need to rescale the data with a gain of 13 dB and a quantum efficiency of 26%. However, this does not match both the protocol phase stabilization gain measurement from Fig. 4.2 and the quantum efficiency calibration from Fig. 3.14, since at a gain of 13 dB we expect around 52% quantum efficiency. In this regard, we continue with the computed Holevo bound obtained from Fig. 4.6.

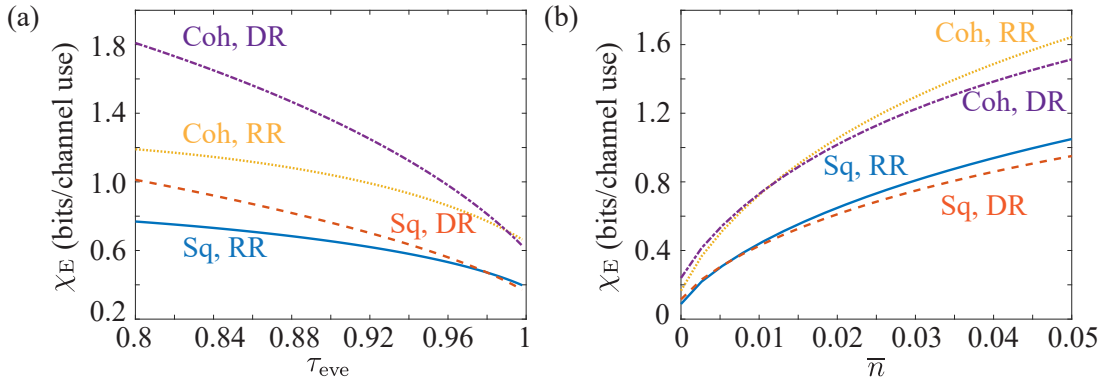

Figure 4.6: Computed Holevo bound per channel use with $\sigma_A^2 = 2.02$ as a function of (a) Eve's transmissivity with $\overline{n} = 0.01$ and (b) the coupled noise with $\tau_{Eve} = 0.9885$ for both the squeezed protocol (Sq) and the coherent protocol with heterodyne detection (Coh). The heterodyne detection is modeled as a beam splitter with two homodyne detectors. We observe that the Holevo bound per channel use is increased for the coherent state heterodyne protocol. In addition, higher coupled noise and lower transmissivity increase the Holevo bound. Direct reconciliation (DR) is more resistant to higher coupled noise, while reverse reconciliation (RR) is more resistant to a reduced transmissivity.

Holevo bound Figure 4.6 shows the computed Holevo bound using the experimental parameters for the individual transmissivities τ_i. We implemented the heterodyne detection as a beamsplitter with two homodyne detectors. As expected, we observe that the Holevo bound per channel use is increased for the coherent protocol with heterodyne detection. In the coherent protocol, Alice encodes two symbols in both q and p quadrature per transmitted state as opposed to the squeezed state protocol, which results in an increased information leakage to Eve, implying a higher Holevo bound. In addition we observe that direct reconciliation performs better with increased coupled noise, while reverse reconciliation performs better with reduced transmissivity. We note here that even with no coupled noise, $\overline{n} = 0$, the Holevo bound is non-zero, as a result of the sub-unity transmissivity. In addition, we note that the modulation variance for the coherent protocol with heterodyne detection in the simulation was adapted, so that the average state of the coherent state protocol at the input of directional coupler 2 is identical to the average of the squeezed state protocol, i.e.

$$\mathbf{\Sigma}_{A,coh,avg} = \left(\tau_2\sigma_{A,coh}^2 + \frac{1}{4}\right)\mathbb{1} = \mathbf{\Sigma}_{A,sq,avg} = \left(\tau_2\sigma_A + \tau_1\tau_2\tau_{DC}\sigma_S^2 + (1-\tau_1\tau_2\tau_{DC})/4\right)\mathbb{1}. \tag{4.17}$$

With this, we compute

$$\sigma_{A,coh}^2 = \sigma_A^2 + \tau_1\tau_{DC}\left(\sigma_S^2 - \frac{1}{4}\right). \tag{4.18}$$

With this, the Holevo bound between the two protocols is more comparable, since if Alice's average input state is the same for both protocols, then Eve's resulting average state is the same. This implies that the first contribution to the Holevo bound from Sec. 2.3.3 is the same.

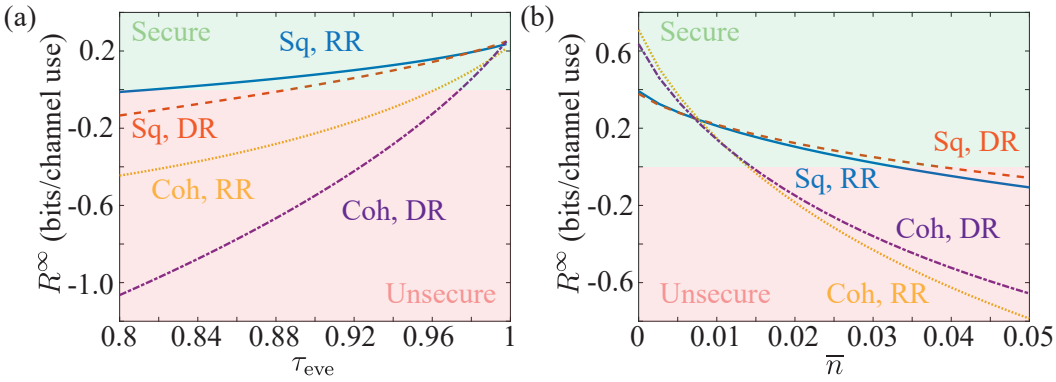

Figure 4.7: Computed asymptotic secret key rate for coherent (Coh) and squeezed (Sq) CV-QKD protocols with both reconciliation methods. For this simulation, we used $\sigma_{\text{A}}^2 = 2.02$ and $\eta = 56\%$. We observe increased resilience to the coupled noise and transmissivity for the squeezed state protocol, while the coherent protocol with has higher key rates for low coupled noise and transmissivity.

4.1.3 Asymptotic secret key rate

We note here that generating secure key rates with this protocol has already been experimentally demonstrated [59], however, it is not achieved in this work due to experimental difficulties. However, it should be mentioned that the main result here is the modulation approach working as intended, i.e. the measured SNR ratios matching theory, therefore, allowing for a significant increase in the repetition rate.

Comparison of secret key rate between two protocols We compare the performance of the squeezed state protocol with the coherent protocol with heterodyne detection. For this, we compute the coherent state protocol mutual information using Eq. 2.100, with the noise variance

$$\sigma_{\text{B}}^2 = \frac{1}{4} + \frac{1}{2}\tau_3\tau_4\left(\frac{1}{4}(1-\tau_{\text{eve}}) + \overline{n}\right) + n_{\text{amp}}. \tag{4.19}$$

For the mutual information this implies that the excess noise and measured symbols are essentially halved due to the beamsplitter on Bob's side. However, the added amplification noise remains the same for each quadrature. From Fig. 4.5 we observe that this has a significant impact on the resulting mutual information. Usually, for $\eta = 100\%$, the mutual information for the coherent state protocol is almost twice the mutual information for the squeezed state protocol, since twice the number of symbols are measured in the end. However, because of the significance of amplification noise in our protocol with imperfect homodyne detection, the mutual information for the coherent protocol is only marginally higher than for the squeezed protocol. In addition to this, the Holevo bound is increased for the coherent protocol with heterodyne detection, which makes the coherent protocol unfavourable when comparing the secret key rates shown in Fig. 4.7. We observe a comparatively higher maximum tolerable noise in the squeezed state protocol than in the coherent state protocol. However, we note that for the low coupled noise and transmissivities, the impact of sifting leaves the squeezed state protocol at a lower key rate. In total, with N transmitted states, the coherent protocol yields $2N$ symbols, while the squeezed state protocol , after sifting, yields $N/2$ symbols, on average. This could affect

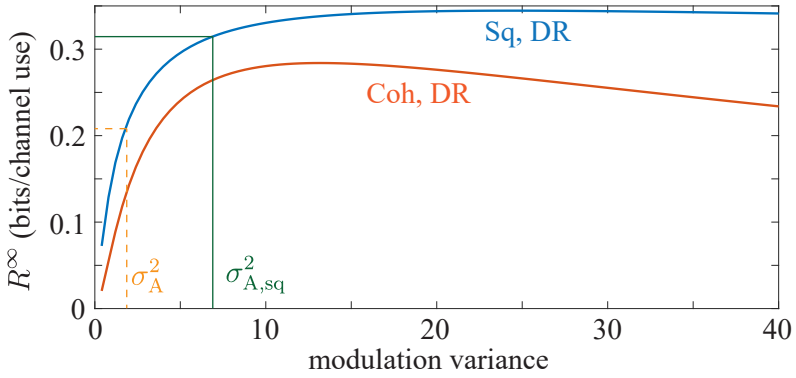

Figure 4.8: Asymptotic secret key rate with $\eta = 56\%$, reconciliation efficiency $\beta = 90\%$, and $\overline{n} = 0.01$ as a function of Alice's modulation variance σ^2_{A}. We observe that for the squeezed state protocol (Sq), the squeezing limited modulation variance, $\sigma^2_{\mathrm{A,sq}}$, beyond which the output states of the JPA 1 become non-Gaussian, is greater than the compression limited modulation variance, σ^2_{A}.

the finite-size performance of the squeezed state protocol, which is investigated in Sec. 2.4.3. In addition, the coherent state protocol has no thermal-state condition on the modulation variance, allowing free choice of the modulation variance. However, in our case, since the modulation variance is limited by the compression power of the JPA 2, the maximum modulation condition is typically easily reached with the relevant squeezing from the JPA 1. This justifies considering the same modulation variance for both protocols in the secret key simulations.

Optimal modulation variance and effect of preamplification From Fig. 4.8 we observe that the secret key rate as a function of the modulation variance exhibits a maximum, which implies there exists an optimum modulation variance, $\sigma^2_{\mathrm{A,opt}}$. This optimum modulation variance depends on the chosen protocol, the reconciliation efficiency, and the experimental parameters such as transmissivity. There are two experimental bounds on the modulation variance: (i) the compression of the preamplifier, limiting the maximum signal power at the input of the JPA 2, and (ii) the maximal squeezing level that can be obtained before the states at the output of our JPAs are no longer Gaussian. Since the indistingishibility condition of the encoding bases connect the squeezing level to the displacement modulation variance, such a limit in the squeezing level results in a limit on the achievable displacement modulation variance. From 3.10 we observe strong squeezing even at -33 dBm pump power, where the modulation variance is $\sigma^2_{\mathrm{A,sq}} = 7.11$. The signal photon number corresponding to the $3\sigma_{\mathrm{A,sq}}$ displacement is given by $9\sigma^2_{\mathrm{A,sq}} \approx 64$. Using the displacement calibration from Fig. 3.11, this implies a displacement power of $P_{\mathrm{d}} \approx -112$ dBm at the JPA 2, which is about 15 dB above the 1 dB compression point we observe in Fig. 3.9. From this we conclude that in our current experimental setup we are more limited by compression, rather than by squeezing. One could imagine that, perhaps, when not using a preamplifier, we can increase the modulation variance arbitrarily, or at least, until the compression power of the HEMT. However, one should note that this drastically reduces the secret key performance due to a quantum efficiency of around $\eta \approx 10\%$, with a HEMT noise of approximately 9 photons.

Without preamplification, the maximum modulation variance for the squeezed protocol would

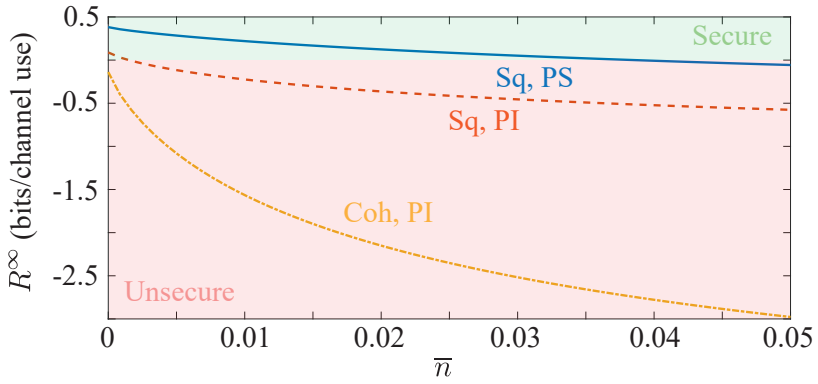

Figure 4.9: Secret key rate with the phase-sensitive amplification (PS) with the quantum efficiency of $\eta = 56\%$ and the modulation variance of $\sigma_{\text{A,PS}} = 2.02$ in comparison to the phase-insensitive amplification (PI) with $\eta = 10\%$ and $\sigma_{\text{A,PI}} = 13$ for the coherent protocol (Coh) and $\sigma_{\text{A,sq}} = 7.11$ for the squeezed protocol (Sq).

become $\sigma^2_{\text{A,sq,max}} = 7.11$, while for the coherent protocol it would be $\sigma^2_{\text{A,coh,opt}} = 13$, which in our case is larger than the maximum squeezed modulation variance, $\sigma^2_{\text{A,coh,opt}} > \sigma^2_{\text{A,sq,max}}$. Fig. 4.9 shows the performance of the squeezed protocol with the preamplifier (Sq,PS) in comparison with the squeezed and coherent protocol with no preamplifier (Sq,PI and Coh,PI, respectively). We observe significantly worsened performance without the preamplification, since the effect of the strong HEMT amplification noise outweighs the gained modulation variance increase, resulting in a lowered SNR in addition to a larger Holevo bound. From all of the above, we conclude that the maximum tolerable coupled noise with a positive asymptotic key rate with our experimental parameters is optimized for the squeezed state protocol.

4.2 Finite size effects

In this section, we consider finite size effects from Sec. 2.4.3 in the context of our CV-QKD protocol. We calculate the effect of the finite size effects on the secret key rate and compare simulations of the finite size performance for both the squeezed and coherent state protocols.

4.2.1 Finite key size effects in microwave CV-QKD protocol

Fig. 4.10 shows the difference between the worst-case estimator for transmissivity and coupled noise for $\epsilon_{\text{PE}} = 0.15\%$ as a function of m released symbols during the parameter estimation process, computed with the quantum efficiency of 56%. For the coupled noise and transmissivity we chose $\overline{n} = 0.01$ and $\tau_{\text{eve}} = 0.9885$, which is in line with what we expect in the QKD protocol. We observe that the relative error in transmissivity is low even for released symbols on the order of $m \sim 10^5$. However, we observe that even with a large number of released symbols on the order of $m \sim 10^6$, we get a significant relative error for the coupled noise, with a worst-case estimator of the coupled noise of $\overline{n}_{\text{est}} = 0.015$ for $m = 10^6$. In addition, we observe that the encoding in both quadratures and the missing sifting in the case of the coherent protocol with heterodyne detection makes for a better estimation of the transmissivity. However, the added effect of the higher amplification noise results in a worse estimation of the coupled

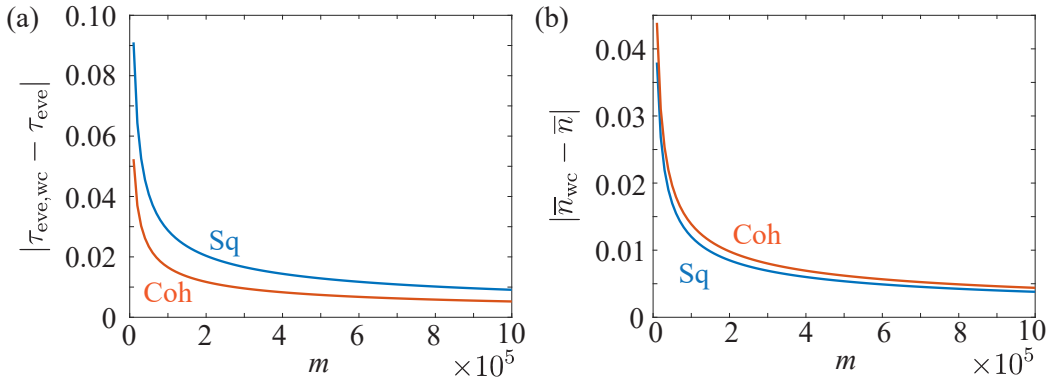

Figure 4.10: Simulation of the parameter estimation for the squeezed protocol (blue) and the coherent protocol (red). The difference between the worst-case estimator from the true transmissivity and the coupled noise is plotted, assuming $\epsilon_{\text{PE}} = 0.15\%$, which corresponds to the 3σ interval of certainty. We observe that while the transmissivity converges rather quickly to a genuine value, the coupled noise requires significantly more symbols to be correctly estimated.

noise even with more symbols. The overestimation of the coupled noise in addition to the lower transmissivity implies that the worst-case Holevo bound is a significant overestimation. We reformulate the final expression for the finite key rate from Eq. 2.134 to

$$R^{\text{fin}} \geq \frac{1}{2}\left(1 - \frac{m}{N}\right)\left(\beta I(A:B) - \delta_m\right), \tag{4.20}$$

where $\delta_m = \chi_{\text{E,m}} + 2\Delta_{\text{AEP}}(N-m)$. In addition, we approximate $\theta = O(1/n) \approx 0$ and assume a sifting factor of 0.5 for the squeezed protocol. Fig. 4.11(a) shows the mutual information and δ_m for $m_1 = 2 \cdot 10^5$, $m_2 = 10^6$, and the asymptotic case $\delta_\infty = \chi_{\text{E},\infty}$. Here, we assume that $\epsilon_H = \epsilon_S = 0.1075\%$, and $p_{\text{ec}} = 95\%$, such that $\epsilon = 2p_{\text{ec}}\epsilon_{\text{PE}} + \epsilon_{\text{H}} + \epsilon_{\text{S}} = 0.5\%$. In addition, the assumed total amount of symbols is five times larger than the number of symbols used for the parameter estimation, $N = 5m$. We observe that the maximum tolerable coupled noise is reduced from the asymptotic case of $\overline{n}_{\text{max},\infty} = 0.038$ to $\overline{n}_{\text{max},m_1} = 0.025$ for $m_1 = 2 \cdot 10^5$ and $\overline{n}_{\text{max},\infty} = 0.011$ for $m_2 = 10^6$. From this, we observe that with the key lengths on the order of $m \sim 10^5$, we achieve ϵ secure key generation in the finite case for the collective attacks, i.e. the generated key is secure up to a failure probability of $\epsilon = 0.5\%$. Fig. 4.11(b) shows the smoothing penalty Δ_{AEP} as a function of m, where we assume $N = 5m$. If we do not consider the effect of estimating the channel parameters, then, the difference between the asymptotic rate and Δ_{AEP} yields the secure key rate. We observe that even without parameter estimation, we need at least $m_{\text{min},\overline{n}_1} = 30000$ symbols to reach a positive key rate in this case. This analysis shows that the effect of the parameter estimation contributes primarily to the finite size key rate. For instance, for $m = 2 \cdot 10^5$, we get $2\Delta_{\text{AEP}} = 0.126$, which is a relatively small contribution when comparing the difference of δ_{m_1} to $\chi_{\text{E},\infty}$ in Fig. 4.11(a).

4.2.2 Maximum tolerable excess noise

The previous analysis allows us to compute the maximum tolerable excess noise as a function of the number of released symbols m. Fig. 4.12 shows the maximum coupled noise for two security

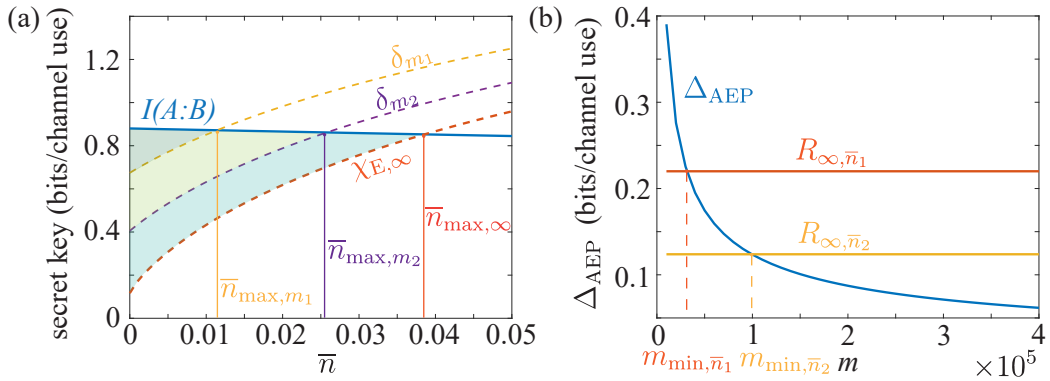

Figure 4.11: (a) Mutual information (blue) as a function of the coupled noise. We also plot $\delta_m = \chi_{\mathrm{E},m} + 2\Delta_{\mathrm{AEP}}(N-m)$ for $m_1 = 2 \cdot 10^5$ (yellow), $m_2 = 10^6$ (purple), and $m \to \infty$ (orange). The difference between the mutual information and different dashed lines representing δ_i yields the finite key rate up to the sifting factor of 0.5. We observe that the maximum tolerated noise drops with a smaller key length. (b) von-Neumann entropy correction Δ_{AEP} as a function of m, where we assume the total key length $N = 5m$. We also show the asymptotic key rate for $\overline{n}_1 = 0.01$ (orange) and $\overline{n}_2 = 0.02$ (yellow). We observe that without considering the parameter estimation, we need a minimum of $m \sim 30000$ symbols to generate a secure key for $\overline{n}_1 = 0.01$.

parameters $\epsilon = 0.5\%$ and $\epsilon_{\mathrm{PE}} = 0.15\%$ in panel (a), and $\epsilon = 2 \cdot 10^{-10}$ and $\epsilon_{\mathrm{PE}} = 10^{-10}$ in panel (b). We observe that the minimum transferred symbols changes from $m \sim 10^5$ to $m \sim 4 \cdot 10^5$. Symbol numbers on the order of $m \sim 10^5$ are currently achievable in experiments, benefitting from the modulation approach increasing the repetition rate by the modulation factor, N_{disp}.

4.3 Future improvements to repetition rate and protocol performance

In our current experimental setup, we encode $N_{\mathrm{disp}} = 6$ symbols during the final $t_{\mathrm{meas}} = 40$ μs long modulation pulse, resulting in 6 measured symbols every $t_{\mathrm{Tr}} = 132$ μs, or an effective repetition rate of $f_{\mathrm{R}} \approx 45.5$ kHz. This is already a significant improvement over the unmodulated approach with a six times lower repetition rate. However, to optimize this rate further, we can increase (i) the FIR filter bandwidth, allowing for a greater modulation rate (ii) increase the down-conversion IF frequency, f_{IF}, to increase the sampling frequency. The first approach (i) would require further studies of a higher FIR filter bandwidth on the noise performance of our setup. The already discussed improvement to $f_{\mathrm{FIR}} = 400$ kHz in 3.10(b) shows a promising result with no significant deterioration of the squeezing performance with the doubled FIR bandwidth. This suggests a potential doubling in the modulation rate, with higher FIR bandwidth increasing the repetition rate even further. The second approach (ii) would reduce the measurement trace acquisition time t_{Tr}. We note here that this alone does not increase the repetition rate, since the symbols per measurement trace are limited by the FIR filter bandwidth. However, the phase stabilization time would be reduced. While these two approaches result in a higher effective repetition rate, the real experimental repetition rate is limited by a measurement

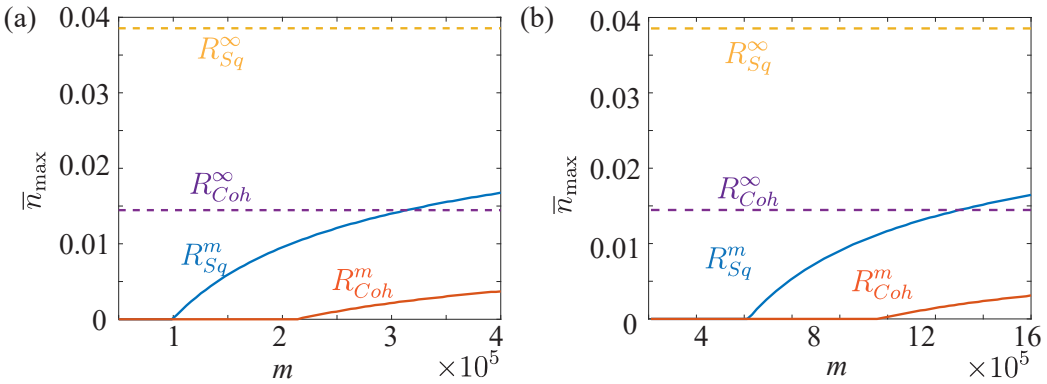

Figure 4.12: Maximum coupled noise as a function of the number of parameter estimation symbols, m, using $\tau_{\text{eve}} = 0.9885$ for the squeezed (blue) and coherent (orange) protocols with direct reconciliation. (a) Maximum tolerable noise for $\epsilon = 0.5\%$ and $\epsilon_{\text{PE}} = 0.15\%$. We observe the secure key generation for $m \sim 10^5$ for the squeezed protocol, with more than twice this number of symbols for the coherent protocol. (b) Maximum tolerable noise for $\epsilon = 2 \cdot 10^{-10}$ and $\epsilon_{\text{PE}} = 10^{-10}$. We observe the minimum of $m \sim 4 \cdot 10^5$ symbols for the secure key generation in the squeezed protocol.

dead-time between each measurement run. Here, depending on which modulation approach from Sec. 3.2.7 is chosen, setting a new displacement power or recompiling the AWG is significantly prolonging the dead-time. One could technically modulate the displacement power for more than one measurement trace by extending the AWG waveform to a multiple of t_{Tr} and choosing new displacement powers for each run. This approach would be limited by the maximum AWG waveform length. In addition, at some point the additional AWG recompilation time might exceed the gained repetition rate. The ideal solution to the dead-time problem would be a source giving random voltages according to a Gaussian distribution and keeping this voltage for the modulation time $\Delta t_{\text{mod}} = 1/f_{\text{FIR}}$. With this one could come close to the effective optimum repetition rate of $f_{\text{R}} = N_{\text{disp}}/t_{\text{Tr}} = t_{\text{meas}}/t_{\text{Tr}} f_{\text{FIR}}$.

Chapter 5

Conclusion and outlook

In this work we have experimentally investigated a CV-QKD protocol with rapidly-modulated displaced squeezed microwave states. We have analyzed this protocol with the calibrated experimental parameters and compared it to the coherent state protocol with heterodyne detection. Here, we have compared the asymptotic performance of both protocols and found that the squeezed state protocol is more resistant to losses and noise than the coherent state protocol due to the increased effect of detection noise when relying on heterodyne detection with the coherent state QKD approach. In addition, we have found that even when including the effect of sifting on the total symbol count, the squeezed protocol is more robust against the coupled noise, allowing for a higher maximum number of coupled noise photons with the same number of channel uses as the coherent protocol with heterodyne detection. We have observed that the number of symbols released during the parameter estimation for a positive key rate under collective attacks has to be on the order of $m \sim 10^5$.

In this regard, we have investigated a displacement modulation approach to increase the symbol repetition rate. To this end, we have used Josephson parametric amplifiers in the phase-sensitive regime to both generate the cipher states for the squeezed CV-QKD protocol and perform a single-shot quadrature measurement of these states with the phase-sensitive preamplifier to increase the readout quantum efficiency. We have found that the SNR ratios we obtained from the protocol for different modulation voltages should align with the ratio of the corresponding displacement calibration factors. From the protocol experiment, we have confirmed that the SNR ratios are indeed consistent with the SNR ratios we would expect from the displacement calibration. With this, we have shown that the modulation approach works as expected and we have successfully demonstrated an increased symbol repetition rate from 7.5 kHz to 45.5 kHz. With this increase, not only do the finite size effects become more manageable, but also the final secret key bit rate is also increased.

In conclusion, the microwave CV-QKD protocols have a large potential due to their frequency compatibility with both modern classical microwave networks, such as 4/5G, and superconducting quantum devices. In this regard, future experiments to optimize the CV-QKD repetition rates will be highly beneficial for the finite size security and our results offer a particular promising approach in this direction.

Bibliography

[1] S. Pirandola. Limits and security of free-space quantum communications. *Phys. Rev. Res.* **3**, 013279 (2021).

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

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

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

[5] R. L. Rivest, A. Shamir & L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* **21**, 120–126 (1978).

[6] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science* 124–134 (1994).

[7] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther & H. Hübel. Continuous-Variable Quantum Key Distribution with Gaussian Modulation—The Theory of Practical Implementations (Adv. Quantum Technol. 1/2018). *Advanced Quantum Technologies* **1**, 1870011 (2018).

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

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

[10] W. Heisenberg. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Physik* **43**, 172–198 (1927).

[11] E. Wigner. On the Quantum Correction For Thermodynamic Equilibrium. *Phys. Rev.* **40**, 749–759 (1932).

[12] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro & S. Lloyd. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621–669 (2012).

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

[14] R. J. Glauber. Coherent and Incoherent States of the Radiation Field. *Phys. Rev.* **131**, 2766–2788 (1963).

[15] M. G. Paris. Displacement operator by beam splitter. *Physics Letters A* **217**, 78–80 (1996).

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

[17] C. M. Jarque & A. K. Bera. Efficient tests for normality, homoscedasticity and serial independence of regression residuals. *Economics Letters* **6**, 255–259 (1980).

[18] T. W. Anderson & D. A. Darling. Asymptotic Theory of Certain "Goodness of Fit" Criteria Based on Stochastic Processes. *The Annals of Mathematical Statistics* **23**, 193 – 212 (1952).

[19] M. A. Stephens. EDF Statistics for Goodness of Fit and Some Comparisons. *Journal of the American Statistical Association* **69**, 730–737 (1974). Full publication date: Sep., 1974.

[20] S. S. Shapiro & M. B. Wilk. An Analysis of Variance Test for Normality (Complete Samples). *Biometrika* **52**, 591–611 (1965). Full publication date: Dec., 1965.

[21] M. A. S. C. S. Davis. The covariance matrix of normal order statistics. *Department of Statistics, Stanford University, Stanford, California. Technical Report No. 14* (1978).

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

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

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

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

[26] C. L. Holloway & E. F. Kuester. Edge shape effects and quasi-closed form expressions for the conductor loss of microstrip lines. *Radio Science* **29**, 539–559 (1994).

[27] J. Goetz, F. Deppe, M. Haeberlein, F. Wulschner, C. W. Zollitsch, S. Meier, M. Fischer, P. Eder, E. Xie, K. G. Fedorov, E. P. Menzel, A. Marx & R. Gross. Loss mechanisms in superconducting thin film microwave resonators. *Journal of Applied Physics* **119**, 015304 (2016).

[28] T. Yamamoto, K. Koshino & Y. Nakamura. *Principles and Methods of Quantum Information Technologies* (Springer Japan, 2016).

[29] C. M. Caves. Quantum limits on noise in linear amplifiers. *Phys. Rev. D* **26**, 1817–1839 (1982).

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

[31] R. G.-P. Sanchez. *Quantum Information with Optical Continuous Variables : from Bell Tests to Key Distributions*. Ph.D. thesis, Universit´e Libre de Bruxelles (2007).

[32] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa & B. Schumacher. Noncommuting Mixed States Cannot Be Broadcast. *Phys. Rev. Lett.* **76**, 2818–2821 (1996).

[33] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal* **27**, 379–423 (1948).

[34] X. Wen, Q. Li, H. Mao, X. Wen & N. Chen. An Improved Slice Reconciliation Protocol for Continuous-Variable Quantum Key Distribution. *Entropy (Basel)* **23** (2021).

[35] R. Renner & J. I. Cirac. de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography. *Phys. Rev. Lett.* **102**, 110504 (2009).

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

[37] R. García-Patrón & N. J. Cerf. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Phys. Rev. Lett.* **97**, 190503 (2006).

[38] Y. Li & P. Busch. Von Neumann entropy and majorization. *Journal of Mathematical Analysis and Applications* **408**, 384–393 (2013).

[39] G. E. Uhlenbeck, N. Rosenzweig, A. J. F. Siegert, E. T. Jaynes & S. Fujita. *Lectures in Theoretical Physics: Statistical Physics* (Benjamin, New York, 1963, 1962).

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

[41] C. Bennett & G. Brassard. WITHDRAWN: Quantum cryptography: Public key distribution and coin tossing (1984).

[42] R. RENNER. SECURITY OF QUANTUM KEY DISTRIBUTION. *International Journal of Quantum Information* **06**, 1–127 (2008).

[43] A. Leverrier. Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction. *Physical Review Letters* **118** (2017).

[44] M. Christandl, R. König & R. Renner. Postselection Technique for Quantum Channels with Applications to Quantum Cryptography. *Phys. Rev. Lett.* **102**, 020504 (2009).

[45] L. Sheridan, T. P. Le & V. Scarani. Finite-key security against coherent attacks in quantum key distribution. *New Journal of Physics* **12**, 123019 (2010).

[46] L. Sheridan & V. Scarani. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A* **82**, 030301 (2010).

[47] A. Leverrier, R. García-Patrón, R. Renner & N. J. Cerf. Security of Continuous-Variable Quantum Key Distribution Against General Attacks. *Phys. Rev. Lett.* **110**, 030502 (2013).

[48] M. Tomamichel & R. Renner. Uncertainty Relation for Smooth Entropies. *Phys. Rev. Lett.* **106**, 110506 (2011).

[49] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel & R. F. Werner. Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks. *Phys. Rev. Lett.* **109**, 100502 (2012).

[50] N. H. Balshaw. *Practical Cryogenics: An Introduction to Laboratory Cryogenics*. (Oxford Instruments (UK), Scientific Research Division, 1996).

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

[52] C. Eichler, D. Bozyigit & A. Wallraff. Characterizing quantum microwave radiation and its entanglement with superconducting qubits using linear detectors. *Phys. Rev. A* **86**, 032106 (2012).

[53] H. Friis. A Note on a Simple Transmission Formula. *Proceedings of the IRE* **34**, 254–256 (1946).

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

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

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

[57] R. D. Candia, E. P. Menzel, L. Zhong, F. Deppe, A. Marx, R. Gross & E. Solano. Dual-path methods for propagating quantum microwaves. *New Journal of Physics* **16**, 015001 (2014).

[58] M. Renger, S. Pogorzalek, Q. Chen, Y. Nojiri, K. Inomata, Y. Nakamura, M. Partanen, A. Marx, R. Gross, F. Deppe & K. G. Fedorov. Beyond the standard quantum limit for parametric amplification of broadband signals. *npj Quantum Information* **7**, 160 (2021).

[59] F. Fesquet, F. Kronowetter, M. Renger, W. K. Yam, S. Gandorfer, K. Inomata, Y. Nakamura, A. Marx, R. Gross & K. G. Fedorov. Demonstration of microwave single-shot quantum key distribution. 2311.11069 (2023).

List of Figures

List of Tables

Acknowledgements

In the following, I would like to thank the contributors to this thesis.
To *Prof. Dr. Rudolf Gross*, for giving me the oppurtunity to complete this Master's thesis at the Walther-Meißner-Institut. His lecture on low temperature physics inspired me to learn more about practical implementations of superconducting devices.
To *Dr. Kirill Fedorov*, for plenty of advice and playing a crucial role in enhancing the quality of this thesis through valuable proofreading. The lecture on applied superconductivity further motivated me to deepen my understanding of applications of superconducting quantum circuits. Dr. Fedorov's extensive expertise proved invaluable to this work.
To *Florian Fesquet*, for communicating crucial experimental and theoretical concepts of this project to me. Our numerous discussions, both theory and experimental, were indispensable towards extending my understanding about quantum key distribution and quantum information as a whole. I am very grateful for his everlasting patience and for his contributions of ideas and technical support to this work.
To *Michael Renger*, for significant help in running the cooldowns in Bob lab and extending my knowledge about dilution refrigeration.
To all the other students in the quantum communication and sensing group at WMI, for being very friendly and helpful during the experiments and in fruitful dicussions.