Quantum key exchange using squeezed states

Poels, K.J.P.M.

Award date:
2004

TECHNISCHE UNIVERSITEIT EINDHOVEN
Department of Mathematics and Computing Science

MASTER'S THESIS

Quantum Key Exchange

using Squeezed States

by

K.J.P.M. Poels

Supervisors:

Dr. Ir. L. A. M. Schoenmakers
Technische Universiteit Eindhoven

Dr. P. Tuyls
Philips Research Eindhoven

Abstract

BB84 is a Quantum Key Exchange (QKE) protocol that works with qubits which are two-dimensional. Theoretically, this protocol is secure under certain conditions. Practically however, there are some implementation problems. These problems are partially solved by QKE using squeezed states, which are infinite-dimensional. Squeezed states have the nice property that the variance of one of the quadratures can be made arbitrary small, at the expense of the variance of the other quadrature which becomes very large. In this thesis, we study squeezed states in order to be able to study the QKE protocol GP00 that uses squeezed states and is presented in [23]. We show the resemblance between BB84 and GP00.

In [24], a general method is given to prove the security of QKE protocols. This method applies to for example BB84, but does not immediately apply to the infinite dimensional case. In this thesis we study this general method, and apply it to GP00.

Acknowledgements

First of all I want to thank Pim Tuyls and Berry Schoenmakers for providing me with a challenging problem and for the helpful suggestions and comments. It was fun developing two independent ears for listening to two information sources at the same time. I thank Pim and Philips for making it possible for me to do my master's thesis at Philips Research. I thank Philips Research for the financial support.

I thank Benne de Weger and Hans Cuypers for the effort they put in studying my thesis.

Then I thank Henk van Tilborg for his guidance and assistance during the master's phase of my studies. I also want to thank him for keeping my secret.

Then we want to thank Karin for the most schizophrenic period of my life. We had a lot of fun and spent so much time together that we became maximally entangled! Thanks for all the women talk and the mental support once in a while.

I also want to thank Peter. I call him the amazing living google machine. Ask him anything and he has an answer in two seconds. Thanks for answering all my questions so patiently.

Really precious were the numerous times Karin and I went doing sports at the FitLab. Thanks Philips Research and especially Mike for giving us this opportunity and the possibility to clear our minds.

Last, but certainly not least, I thank my parents for giving me the opportunity to do my studies in the first place.

Contents

Chapter 1

Introduction

A basic problem in Cryptography is *key exchange*. Key exchange is a protocol in which two parties, conventionally known as Alice and Bob, agree on a secret key to use for private communication over an insecure communication channel. The problem is to do the key exchange in such a way that a possible eavesdropper (Eve) has negligible information about the key such that the key is indeed secret.

A common solution to this problem is to use Diffie-Hellman [1] for the key exchange protocol. In Diffie-Hellman, Alice and Bob agree on a group G and an element $g \in G$ before the start of the protocol. Alice chooses $a \in \mathbb{N}$ and sends g^a to Bob over an insecure communication channel. Bob chooses $b \in \mathbb{N}$ and sends g^b to Alice over the same channel. Alice and Bob can both calculate g^{ab} which will serve as the secret key.
A problem of Diffie-Hellman is that the security of the protocol relies on the fact that, given g^a and knowing g, it is computationally hard for an attacker to calculate a. This is also known as the discrete log problem. A different problem is the so called man-in-the-middle attack. A malicious third party can interfere in the key exchange protocol in such a way that it can read and modify all messages communicated between Alice and Bob.

The problem of key exchange is possibly solved by the fundamental principles of quantum mechanics.

> Quantum mechanics was developed to explain certain phenomena in Nature, like the photo-electric effect (which was explained by Einstein in [2]) and the Stern-Gerlach experiment [3], which could not be explained using only "classical physics". Classical physics is only applicable up to atomic level but to make predictions at atomic level or beyond quantum mechanics has to be applied. With this new set of physical theories, open questions like the structure of the stars [4], the behavior of solid states [6] and superconductivity [5] were answered. Even today quantum mechanics is being applied to new problems and new situations. We are exploring untouched regimes of Nature in the hope to discover new and unexpected phenomena.

... what is proved by impossibility proofs is lack of imagination.
- John Bell

> By regarding a wall not as a whole but as a collection of atoms, there is a very small probability that for two seconds certain atoms of the wall move in a certain direction so that I can walk through it.
> Quantum mechanics states that we know things because we measure them. We know the world because we measure it with our eyes and ears, what the world really is, is not necessarily what we measure. It may be clear that quantum mechanics has drawn the attention of many philosophers [7, 8].

There are algorithms known based on quantum mechanics that can solve the discrete log problem [9] (but also other problems like prime factorization [9]) in polynomial time. This means that if these quantum algorithms can be implemented, key exchange protocols of which the security is based on the intractability assumption are not secure anymore.

Quantum key exchange (QKE) protocols are key exchange protocol based on the laws of quantum mechanics. They are provably secure because, instead of on intractability assumptions, the security relies on fundamental laws of quantum mechanics. Those fundamental properties are first, the no-cloning theorem; Eve cannot copy the message Alice sent to Bob. Second, in any attempt to distinguish between two non-orthogonal quantum states, information gain is only possible at the expense of introducing disturbance in the system. Because of these properties Eve cannot gain information about the messages sent from Alice to Bob without disturbing the system.

Theoretically, this means that QKE protocols can be made in which Alice and Bob can determine whether Eve has more than negligible information about the key they agreed on. As a consequence, Alice and Bob can determine whether the key is secret or not. In other words, QKE protocols based on fundamental laws of quantum mechanics can be made that are perfectly secure. Practically however, it is still a big challenge to implement these protocols.

In 1984 Charles H. Bennett and Gilles Brassard introduced the first workable quantum key exchange scheme known as BB84 [10] by which a perfectly secure secret common key between Alice and Bob is established. The protocol works with single photon states that are polarized in one out of two non-orthogonal bases. The security of the protocol depends on the fact that Alice sends single photons, polarized in a certain basis, to Bob. However, the main practical weakness is that preparing single photon states is extremely difficult. Instead of just a single photon, often a beam of two or three photons polarized in the same basis is sent. This means that an adversary can split the beam of photons such that he obtains a photon identically polarized as the photon Bob receives. In these cases Eve extracts the same bit value as Bob extracts. This attack is called a "beam splitter" attack. With this attack Eve gains information about the secret key whereas Alice and Bob do not notice the interference.

In 2000 Daniel Gottesman and John Preskill presented a key exchange protocol (GP00) [23] that resembles BB84 but works with squeezed states instead of single photons.
Squeezed states are quantum states of which the uncertainty of one observable can be made arbitrarily small ("squeezed") at the expense of the uncertainty of a conjugate variable, that becomes very large. Squeezed states can be made by a laser and are more easy to prepare than single-photon states. Key exchange protocols that work with squeezed states solve the prac-

tical problem of BB84 but at the same time introduce other problems. Preparing a squeezed state is difficult but yet not as difficult as preparing a single photon. The more squeezing is needed the more difficult it is to prepare the squeezed state. Therefore it is important to determine the amount of squeezing needed for the protocol to be secure.
Single photons are elements of a two-dimensional Hilbert space whereas squeezed states are elements of an infinite-dimensional Hilbert space. This is one of the reasons that squeezed states are difficult to work with. Although GP00 resembles BB84, results from BB84 are not easily translated into results in GP00. In this thesis we study the concept of the squeezed state to be able to analyze GP00. We do this among others by computing the probability distribution of the position and momentum with respect to squeezed states, showing that squeezed states cannot be cloned and giving the time evolution of a squeezed state in free space.
With these calculations we fully analyze the squeezed state version of BB84, GP00. Before we study GP00, we analyze BB84. We analyze the two protocols in a similar way, from which the resemblance of the two protocols will follow straightforwardly.

The security of the QKE protocols relies theoretically on the fundamental principles of quantum mechanics. Practically however, known security proofs of quantum key exchange protocols are non trivial and are usually restricted in their applicability to specific protocols. In [24],Matthias Chrisandl, Renato Renner and Artur Ekert present a generic proof of security with which security proofs of a class of QKE protocols can be made in a direct, intuitive way. This generic proof of security however does not immediately apply to the infinite-dimensional case.
We analyze the security of BB84 and GP00 in two different ways. First, we apply the traditional approach, that is, try a number of attacks and verify whether Alice and Bob will detect Eve. Specific attacks however do not exclude the possible existence of better attacks and therefore this proof of security is not complete. We apply the method presented in [24] to BB84 to find the well known threshold for the bit error rate. If the bit error rate of BB84 is smaller than the threshold, then the protocol is secure. Using the similarity of GP00 with BB84 we apply the method presented in [24] to the infinite-dimensional case GP00. We therefore prove the security of GP00 in a direct way.

In Chapter 2 the basic principles of quantum mechanics are presented that are used in this thesis. To make squeezed states mathematically more comprehensible the concept of the squeezed state is studied in Chapter 3 and 4 of this paper. Because squeezed states are "made of" coherent states which can also be made with a laser, these states are also explained in Chapter 3.

The squeezed state protocol GP00 approaches BB84 with respect to structure and security. We study both protocols in Chapter 5.

In Chapter 7 we explain how to apply the generic proof to BB84. A more complex problem is how to apply the generic proof to GP00, moreover because of the infinite dimensionality of the squeezed states. Using the similarity between BB84 and Gp00, we apply the method to GP00.

The conclusions are presented in Chapter 8.

Chapter 2

Preliminaries on Quantum Mechanics

In this chapter, the basic principles of quantum mechanics are presented that are needed in this thesis. We gathered this information from [21] and [22]. For more information about quantum mechanics we refer to these books.

2.1 The Schrödinger equation

In classical physics, given a specified force $F(x,t)$ working on a particle of mass m that is not of atomic level moving along the x-axis, we can calculate its position $x(t)$ at any given time t. We do this by applying Newton's second law $F = ma$.

In quantum mechanics we cannot calculate the exact position of a particle at a given time t. However, we can calculate a probability distribution that gives the probability for a particle to have position x at time t. This probability distribution is determined by a certain wave function $\Psi(x,t)$ belonging to a particle. This wave function can be found by solving the *Schrödinger equation*:

$$i\hbar\frac{\partial\Psi(x,t)}{\partial t} = -\frac{\hbar^2}{2m}\frac{\partial^2\Psi(x,t)}{\partial x^2} + V\Psi(x,t)$$

where Planck's constant is $\hbar = \frac{h}{2\pi} = 1.054573\times10^{-34}Js$ and V is the potential of the particle. The probability of finding the particle at position x at time t is given by $|\Psi(x,t)|^2$. Because $|\Psi(x,t)|^2$ is a probability distribution it has to be normalized, so

$$\int_{-\infty}^{\infty}|\Psi(x,t)|^2dx = 1.$$

The Schrödinger equation can be solved by the method of separation of variables if the potential V is separable, that is, V is independent of t. This is done by substituting $\Psi(x,t) = \psi(x)f(t)$ in the Schrödinger equation. The equation can then be separated into two equations, one for $f(t)$ and one for $\psi(x)$:

$$\frac{df(t)}{dt} = -\frac{iE}{\hbar}f(t) \quad \wedge \quad -\frac{\hbar^2}{2m}\frac{d^2\psi(x)}{dx^2} + V(x)\psi(x) = E\psi(x) \tag{2.1}$$

where E is called the separation constant. It is the total energy of the particle.
The general solution to the left equation is

$$f(t) = e^{-iEt/\hbar}$$

and the right equation is called the time-independent Schrödinger equation.

For every possible energy (or separation constant) E_i of the particle there is a different wave function solution of the Schrödinger equation $\Psi_i(x,t) = f_i(t)\psi_i(x) = e^{-iE_it/\hbar}\psi_i(x)$. Any linear combination (superposition) of possible solutions is again a solution, so the general solution to the Schrödinger equation is given by the wave packet

$$\Psi(x,t) = \sum_{n=1}^{\infty} c_n \psi_n(x) e^{-iE_nt/\hbar} \tag{2.2}$$

where $c_n \in \mathbb{C}$ such that $\sum_{n=1}^{\infty} |c_n|^2 < \infty$.

Every particle has a certain wave function, that is, a certain probability distribution. If we measure for example the position of a particle then $|\Psi(x,t)|^2$ gives us the probability to measure position x at time t. Upon measurement, the wave function collapses to a spike at the measured position value so if we make a second measurement right after the first one, we find the same value we found in the first measurement. Soon after the measurement the wave function will spread out again according to the Schrödinger equation.

2.2 Representation of Quantum states

A Hilbert space is an inner product space that is complete with respect to the norm defined by the inner product. The space L^2 is the set of all square-integrable functions over $\mathbb{R}$. This means all functions $h : \mathbb{R} \to \mathbb{C}$ with $\int_{-\infty}^{\infty} |h(x)|^2 dx < \infty$ such that the function can be normalized. The space L^2 is complete and is thus a Hilbert space. A wave function $\Psi : \mathbb{R} \times \mathbb{R}^* \to \mathbb{C}$ must be normalizable. Every wave function $\Psi(x,t)$ can be written as in Eq. 2.2 and therefore, if $\psi_n(x) \in L^2$ for all $n \geq 1$ then $\Psi(x,t)$ is normalizable. Let $L^{2'}$ be the function space that contains the functions $\Psi : \mathbb{R} \times \mathbb{R}^* \to \mathbb{C}$ with this property such that every $\Psi(x,t) \in L^{2'}$ is normalizable. It holds that $L^{2'}$ is a Hilbert space as well and $L^2 \subset L^{2'}$. Note that every wave function $\Psi(x,t)$ is a time-dependent linear combination of functions in L^2.

From now on we focuss on wave functions in the Hilbert space $L^{2'}$ and therefore we assume that every wave function $\Psi(x,t) \in L^{2'}$. If we talk about the time independent part of the wave function, $\psi(x)$, we assume that $\psi(x) \in L^2$. The state of the particle with wave function $\Psi(x,t) \in L^{2'}$ will be represented by $|\Psi\rangle$.

The inner product of two wave functions $\Psi(x,t)$ and $\Phi(x,t)$ is defined by the integral

$$\langle \Psi | \Phi \rangle = \int_{-\infty}^{\infty} \Psi^*(x,t)\Phi(x,t)dx$$

where $\Psi^*(x,t)$ is the complex conjugate of $\Psi(x,t)$. It holds that $\langle \Psi|\Phi\rangle = \langle \Phi|\Psi\rangle^*$.

2.3 Operators applied to quantum states

Let T be a linear operator that maps a function in $L^{2'}$ to a function in W. Here W is a function space over $\mathbb{R}$. If we apply T to a wave function $\Psi(x,t) \in L^{2'}$, then the expectation value of T is denoted by $\langle T \rangle$ and calculated by

$$\langle T \rangle = \langle \Psi | T\Psi \rangle = \int_{-\infty}^{\infty} \Psi^*(x,t) T\Psi(x,t) dx$$

The Hermitian conjugate of an operator T is the operator $T^\dagger$ such that

$$\langle T^\dagger f | g \rangle = \langle f | Tg \rangle$$

for all $f, g \in L^{2'}$.

An operator T is *unitary* if $TT^\dagger = I$. A unitary operator T preserves inner products between quantum states because

$$(T|f\rangle, T|g\rangle) = \langle f | T^\dagger T | g \rangle = \langle f | g \rangle$$

for every $f, g \in L^{2'}$.

An operator T is *Hermitian* if $\langle f | Tg \rangle = \langle Tf | g \rangle$ for all $f, g \in L^{2'}$. It holds that $T^\dagger = T$. The Hermitian operator T has the following properties:

1. The eigenvalues are real. Eigenvalues of T are values $\lambda \in \mathbb{R}$ such that there is a function h with $Th = \lambda h$. The function $h \in L^{2'}$ is called an eigenfunction of T.

2. The eigenfunctions belonging to distinct eigenvalues are orthogonal. The eigenfunctions belonging to identical eigenvalues can be chosen orthogonal.

3. The eigenfunctions span the space $L^{2'}$ if the eigenvalues of T form a discrete spectrum.

2.4 Fundamental Principles of Quantum mechanics

We present the fundamental principles of quantum mechanics to improve our intuition about the subject. These principles are presented in the form of a number of postulates. Recall that if A is a bounded linear operator over a Hilbert space V then A is positive if and only if $\langle Ax | x \rangle \geq 0$ for every $x \in V$.

1. The state of a particle is represented by a normalized function $|\Psi\rangle$ in the Hilbert space L^2.

2. The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ at time t_2 by a unitary operator U which depends only on the times t_1, t_2,

$$|\psi'\rangle = U|\psi\rangle.$$

3. • General measurements
Quantum measurements are described by a collection $\{M_m\}_{m=1}^k$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the system is $|\Psi\rangle$ immediately before the measurement then the probability that result m occurs is given by

$$p(m) = \langle\Psi|M_m^\dagger M_m|\Psi\rangle$$

and the state of the system right after the measurement is

$$\frac{M_m|\Psi\rangle}{\sqrt{\langle\Psi|M_m^\dagger M_m|\Psi\rangle}}.$$

The measurement operators satisfy the completeness equation

$$\sum_{m=1}^{k} M_m^\dagger M_m = I.$$

A set $\{M_m\}_{m=1}^k$ that satisfies this property is in the literature often called a partition of unity of size k.

• A set of positive operators $\{P_m\}_{m=1}^k$, with $P_m > 0$ and satisfying

$$\sum_{m=1}^{k} P_m = 1$$

is called a POVM which stands for Positive Operator Valued Measure. The index m refers to the measurement outcomes that may occur in the experiment. The probability that result m occurs is

$$p(m) = \langle\Psi|P_m|\Psi\rangle.$$

POVM's are a special case of the general measurement. They provide a means to study the measurement statistics without the necessity for knowing the state of the system right after the measurement which makes them very important in quantum information theory.

• Projective measurements
A projective measurement is described by an observable M that is a Hermitian operator on the state space of the system being observed. The observable has a spectral decomposition,

$$M = \sum_m mP_m.$$

If the Hermitian operator M has a continuous spectrum then the spectral decomposition becomes

$$M = \int mP_m dm,$$

where P_m is the projector onto the eigenspace of M with eigenvalue m in V. The possible outcomes of the measurement correspond to the eigenvalues m of the

observable M. Upon measuring the state $|\Psi\rangle$, the probability of getting result m is given by

$$p(m) = \langle\Psi|P_m|\Psi\rangle.$$

Given that outcome m occurred, the state of the quantum system immediately after the measurement is

$$\frac{P_m|\Psi\rangle}{\sqrt{\langle\Psi|P_m|\Psi\rangle}}.$$

The expectation value of M, $\langle M\rangle$, is given by

$$\langle M\rangle = \langle\Psi|M|\Psi\rangle.$$

Projective measurements are a special case of the POVM.

4. The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\Psi_i\rangle$, then the joint state of the total system is the composite state

$$|\Psi_1\rangle \otimes |\Psi_2\rangle \otimes \cdots \otimes |\Psi_n\rangle = |\Psi_1\Psi_2 \ldots \Psi_n\rangle.$$

A composite system can be in a superposition of composite states. If this superposition is such that the state cannot be written as a product of n states, then the composite state is entangled. An entangled state has the important property that if a measurement is made in system i, then the state of system j is changed by this measurement.

If we make measurement M_i on system i then we apply $M_1 \otimes M_2 \otimes \cdots \otimes M_n$ to the composite system.

If a variable is represented by an Hermitian operator then we call that variable an *observable*.

Example 2.4.1 *Let $|0\rangle, |1\rangle$ be orthonormal quantum states independent of t. That means $|0\rangle, |1\rangle \in L^2$. A measurement in the basis $\{|0\rangle, |1\rangle\}$ is a projective measurement (see Appendix B). Let λ_0 be the eigenvalue belonging to $|0\rangle$ and λ_1 be the eigenvalue belonging to $|1\rangle$. Let Λ be the Hermitian operator belonging to this measurement. We have*

$$\Lambda = \lambda_0 P_{\lambda_0} + \lambda_2 P_{\lambda_1} = \lambda_0 |0\rangle\langle 0| + \lambda_2 |1\rangle\langle 1|.$$

Suppose that the joint state of two systems is $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$. This state is not entangled because

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right).$$

This means that system 1 is in quantum state $|0\rangle$ and system 2 is in the normalized quantum state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. A consequence of the non-entanglement is that a measurement of the observable Λ in system 1 does not influence the state of system 2. To illustrate this we

note that a measurement of Λ in system 1 will always return the value λ_0. The state of the composite system after this measurement is

$$\begin{aligned}(P_{\lambda_0} \otimes I)|\psi\rangle &= (|0\rangle\langle 0| \otimes I)\left(|0\rangle \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)\right) \\ &= |0\rangle \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)\end{aligned}$$

Suppose that the joint state of two systems is $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ which is known as a Bell state. This state is entangled because it cannot be written as a product of two quantum states. A measurement of Λ in system 1 does influence the state of system 2. We illustrate this by a measurement of Λ on the state $|\psi\rangle$. The probability namely that λ_0 is measured in system 1 is

$$\begin{aligned}p(\lambda_0) = \langle\psi|(P_{\lambda_0} \otimes I)|\psi\rangle &= \frac{1}{\sqrt{2}}\langle\psi|(|0\rangle\langle 0| \otimes I)\,(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \\ &= \frac{1}{\sqrt{2}}\langle\psi|00\rangle \\ &= \frac{1}{2}.\end{aligned}$$

The state of the system after measurement of λ_0 is

$$\begin{aligned}\frac{(P_{\lambda_0} \otimes I)|\psi\rangle}{\sqrt{P(\lambda_0)}} &= (|0\rangle\langle 0| \otimes I)\,(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \\ &= |00\rangle \\ &= |0\rangle \otimes |0\rangle.\end{aligned}$$

In the same way we find that if λ_1 is measured then the state after the measurement is $|11\rangle$. We conclude that if λ_i is measured in system 1, then in system 2 the same value is found with a measurement of Λ.

2.5 Position and momentum

Let the operator $\hat{x}$ represent the observable position x. In this introductory part, to avoid confusion, we place a hat on the observable to denote the operator representing the observable.

The operator $\hat{x}$ is Hermitian because

$$\langle f|\hat{x}|g\rangle = \int_{-\infty}^{\infty} f^\dagger(x,t)\hat{x}g(x,t)dx = \int_{-\infty}^{\infty} (\hat{x}f(x,t))^\dagger g(x,t)dx = \langle \hat{x}f|g\rangle$$

for all $f, g \in L^{2'}$. In [21], Griffiths shows that the operator $\hat{p} = \frac{\hbar}{i}\frac{\partial}{\partial x}$ represents the observable momentum p.

If we restrict ourselves to functions which go to zero when x goes to infinity so $f(x,t) \to 0$

when $|x| \to \infty$ then we see that the operator $\hat{p}$ is Hermitian;

$$\begin{aligned}
\langle f|\hat{p}|g\rangle &= \int_{-\infty}^{\infty} f^{\dagger}(x,t)\frac{\hbar}{i}\frac{\partial g(x,t)}{\partial x}dx \\
&= -\int_{-\infty}^{\infty} \frac{\hbar}{i}\frac{\partial f^{\dagger}(x,t)}{\partial x}g(x,t)dx + f^{\dagger}(x,t)g(x,t)|_{-\infty}^{\infty} \\
&= \int_{-\infty}^{\infty} \left(\frac{\hbar}{i}\frac{\partial f(x,t)}{\partial x}\right)^{\dagger} g(x,t)dx \\
&= \langle \hat{p}g|g\rangle
\end{aligned}$$

Griffiths also proves that the commutator of $\hat{x}$ and $\hat{p}$ is $[\hat{x},\hat{p}] = [x, \frac{\hbar}{i}\frac{\partial}{\partial x}] = i\hbar$.

All observables can be written in terms of position x and momentum p. This means that the operator representing the observable $M(x,p,t)$ is given by $M(x, \frac{\hbar}{i}\frac{\partial}{\partial x}, t)$.

Because the canonical observables x, p are very important in Quantum Mechanics, it is important to know the eigenfunctions of the Hermitian operators $\hat{x} = x$ and $\hat{p} = \frac{\hbar}{i}\frac{\partial}{\partial x}$.

- We take $\delta(x)$ as the usual Dirac function. The Dirac function $\delta(x)$ is defined as

$$\delta(x) = \begin{cases} 0 & \text{if } x \in \mathbb{R}, x \neq 0 \\ \infty & \text{if } x = 0 \end{cases} \quad \text{with} \int_{-\infty}^{\infty} \delta(x)dx = 1$$

  Suppose $x_n \in \mathbb{R}$. Then

$$x\delta(x - x_n) = \begin{cases} 0 & \text{if } x \neq x_n \\ x_n\delta(0) & \text{if } x = x_n \end{cases}$$

  This gives us that $x\delta(x - x_n) = x_n\delta(x - x_n)$. We find that $|x_n\rangle = \delta(x - x_n)$ is the eigenfunction of the operator $\hat{x}$ belonging to the eigenvalue x_n for every $x_n \in \mathbb{R}$. This gives us the spectral decomposition for x:

$$\hat{x} = \int_{x_n} x_n P_{x_n} dx_n = \int_{x_n} x_n |x_n\rangle\langle x_n| dx_n.$$

- Suppose $p_n \in \mathbb{R}$. It holds that

$$\frac{\hbar}{i}\frac{\partial}{\partial x}\frac{1}{\hbar}e^{ip_n x} = p_n e^{ip_n x}.$$

  We can say that $|p_n\rangle = \frac{1}{\hbar}e^{ip_n x}$ is the eigenfunction of the operator $\hat{p}$ belonging to the eigenvalue x_n for every $x_n \in \mathbb{R}$. We have that the spectral decomposition of $\hat{p}$ is

$$\hat{p} = \int_{p_n} p_n P_{p_n} dp_n = \int_{p_n} p_n |p_n\rangle\langle p_n| dp_n$$

2.6 The Hamiltonian

The total energy (kinetic plus potential) of a system is called the *Hamiltonian*:

$$H(x,p) = \frac{p^2}{2m} + V(x)$$

and the corresponding Hamiltonian operator is given by

$$\hat{H} = -\frac{\hbar^2}{2m}\frac{d^2}{dx^2} + \hat{V}(x)$$

where $\hat{V}(x)$ is a multiplication operator. That is, $\hat{V} : L^2 \to L^2$, $\hat{V} : f \mapsto Vf$ with $Vf(x) = V(x)f(x)$.

From the time independent Schrödinger equation (2.1) we see that

$$\hat{H}\psi(x) = E\psi(x)$$

such that the solution of the time independent Schrödinger equation is an eigenfunction of the Hamiltonian with eigenvalue equal to the total energy of the system. For finding the total energy of a system we therefore apply the Hamiltonian to the wave function of a system.

2.7 Uncertainty principles

Suppose $\hat{A}$ and $\hat{B}$ are Hermitian operators representing the observables A and B. For the variances of A and B it then holds that

$$\sigma_A^2\sigma_B^2 \geq \left(\frac{1}{2i}\langle[\hat{A},\hat{B}]\rangle\right)^2.$$

This is the general uncertainty principle. If $A = x$ and $B = p$ then we know that $[\hat{x},\hat{p}] = i\hbar$ and $\sigma_x^2\sigma_p^2 \geq \left(\frac{1}{2i}i\hbar\right)^2 = \frac{\hbar^2}{4}$ and thus

$$\sigma_x\sigma_p \geq \frac{\hbar}{2}.$$

This inequality is better known as the Heisenberg uncertainty principle.

2.8 Density matrix

If a quantum system is in the state $|\Psi\rangle$, then that state is pure. It is also possible that with probability p_i the quantum system is in the state $|\Psi_i\rangle$. We then say that the state is mixed.

A convenient means for describing quantum systems whose state is not completely known is the *density matrix*. It is defined by

$$\rho = \sum_i p_i|\Psi_i\rangle\langle\Psi_i|.$$

The density matrix is also known as the density operator. The third postulate is changed in the following way.

- Suppose we perform a measurement described by measurements operators $\{M_m\}_{m=1}^k$ with $\sum_{m=1}^k M_m^\dagger M_m = I$. The probability of obtaining result m is

$$p(m) = tr(M_m^\dagger M_m \rho)$$

where $tr(.)$ is the usual trace function. After a measurement that yields the result m the density matrix becomes

$$\rho_m = \frac{M_m \rho M_m^\dagger}{tr(M_m^\dagger M_m \rho)}.$$

- Suppose the measurement is given by a POVM, a set of positive operators $\{P_m\}_{m=1}^k$, with $P_i > 0$ and satisfying $\sum_{m=1}^k P_m = 1$. The probability that result m occurs is

$$p(m) = tr(P_m \rho).$$

- If the measurement operator is Hermitian, then the observable has spectral decomposition $M = \sum_m m P_m$ defined as in Postulate 3. The probability of measuring eigenvalue m is

$$p(m) = tr(P_m \rho).$$

After a measurement that yields the result m the density matrix becomes

$$\rho_m = \frac{P_m \rho P_m}{tr(P_m \rho)}.$$

2.9 Qubits

The bit is the fundamental concept of classical computation and classical information. A bit can be in the state 0 or 1. In quantum computation and quantum information there is an analogous concept called the quantum bit or *qubit*. The classical bits 0 and 1 correspond in the quantum world to respectively the quantum state $|0\rangle$ and $|1\rangle$, where $|0\rangle$ and $|1\rangle$ are orthonormal wave functions.

Whereas a bit can only be in two different states, a qubit can also be in a superposition of the basis states. If the basis states are $|0\rangle$ and $|1\rangle$ then, in general, a qubit is in the state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where $|\alpha|^2 + |\beta|^2 = 1$. In this view, the state of a qubit is a vector in a 2-dimensional vector space with basis $\{|0\rangle, |1\rangle\}$ also known as the rectilinear or computational basis. Another possible basis is the diagonal basis consisting of $\{|+\rangle, |-\rangle\} = \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ where $|+\rangle$ correspond with a classical bit 0 and $|-\rangle$ with a classical bit 1. In this basis a qubit is in the general state

$$|\psi\rangle = \alpha|+\rangle + \beta|-\rangle.$$

Obviously there are many more possible bases.

Chapter 3

Introduction to Coherent States and Squeezed States

This thesis mainly deals with squeezed states but because squeezed states are "made from" coherent states we introduce both squeezed and coherent state in this chapter.

Very briefly, *coherent* and *squeezed states* are states that satisfy the Heisenberg uncertainty relation (see 2.7) with equality for certain observable pairs x' and p' so $\sigma_{x'}\sigma_{p'} = \hbar/2$. For coherent states the uncertainty in x' and p' is equal so $\sigma_{x'} = \sigma_{p'} = \sqrt{\hbar/2}$. For squeezed states one of the uncertainties can be made arbitrarily small while the other becomes arbitrarily large in order to keep the product constant at $\hbar/2$.

As a coherent state is a special case of a squeezed state, the coherent state was the first of these minimum uncertainty states that was fully analyzed [11]. This was done for the first time by Schrödinger [12]. A coherent state is important because it mimics a classical field. A squeezed state is important because there is no lower bound for the uncertainty in one variable anymore and this can be very beneficial, for example when a precise measurement is needed.

Before we introduce these states, we give some background information about the harmonic oscillator.

3.1 Harmonic oscillator

A *harmonic oscillator* describes a mass m attached to a spring of a certain force constant k. The potential energy is $V(x) = \frac{1}{2}kx^2$.
In classical mechanics, the motion is governed by Hooke's law, $F = -kx$. In quantum mechanics, the wave function is calculated by solving the Schrödinger equation for the potential $V(x) = \frac{1}{2}kx^2$. The possible solutions to this equation correspond to the possible separation (energy) constants. The possible solutions are given in [21]:

$$\phi_n(x) = |n\rangle \quad f_n(t) = e^{-iE_n\frac{t}{\hbar}} \quad E_n = \left(n + \tfrac{1}{2}\right)\hbar\omega$$

where $\omega = \sqrt{k/m}$ and $n \in \mathbb{N}$. This gives us that the general solution to the time-dependent Schrödinger equation is

$$\Psi(x,t) = \sum_{n=0}^{\infty} c_n f_n(t)|n\rangle = \sum_{n=0}^{\infty} c_n e^{-iE_n \frac{t}{\hbar}}|n\rangle$$

with $c_n \in \mathbb{C}$. The state $|n\rangle \in L^2$ represents the solution to the time-independent Schrödinger equation with separation constant E_n. These states are also called *number states* because the index n in $|n\rangle$ represents the number of photons in the system.

There are so called *creation* and *annihilation operators* with which the representation of and the calculations involving the harmonic oscillator are simplified. A simple expression for the number states can be given. Also, the Hamiltonian becomes very easy in terms of these operators. For a more simple representation of the creation and annihilation operators, we choose $k = m = 1$. The creation and annihilation operators are defined in the following definition.

Definition 3.1.1 *The creation operator $a^\dagger$ and annihilation operator a are defined by*

$$a^\dagger = \frac{x - ip}{\sqrt{2\hbar}} \quad \textit{and} \quad a = \frac{x + ip}{\sqrt{2\hbar}}$$

where $a^\dagger$ is the Hermitian conjugate of a. The number states are defined as the eigenfunctions of $a^\dagger a$ in the following way

$$a^\dagger a|n\rangle = n|n\rangle.$$

It was proved in [21] that the creation and annihilation operators respectively raise and lower the energy of a number state such that the state is changed in a higher number state or lower number state;

$$a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle \quad \textit{and} \quad a|n\rangle = \sqrt{n}|n-1\rangle$$

and $a|0\rangle = 0$. The state $|0\rangle$ is called the vacuum.

Before we can give an expression of the number states in terms of the creation operators, we give an explicit expression of the time independent wave function of the vacuum state $|0\rangle$ that follows from Definition 3.1.1.

Corollary 3.1.2 *The time-independent wave function of the normalized vacuum $|0\rangle$ is given by*

$$|0\rangle = (\pi\hbar)^{-\frac{1}{4}} e^{-\frac{x^2}{2\hbar}}$$

Proof. The vacuum $|0\rangle$ is an element of the nullspace of the annihilation operator a. We use $p = \frac{\hbar}{i}\frac{\partial}{\partial x}$ (see 2.5) to see that:

$$\begin{aligned} \frac{x + ip}{\sqrt{2\hbar}}|0\rangle &= 0 \\ \left(x + \hbar\frac{\partial}{\partial x}\right)|0\rangle &= 0 \\ \frac{\partial|0\rangle}{|0\rangle} &= \frac{-x}{\hbar}\partial x \end{aligned}$$

Integrating both parts gives

$$\begin{aligned}\int \frac{\partial|0\rangle}{|0\rangle} &= \int \frac{-x\partial x}{\hbar} \\ \ln|0\rangle &= -\frac{x^2}{2\hbar} + c \ , \ c \in \mathbb{C} \\ |0\rangle &= Ce^{-\frac{x^2}{2\hbar}} \ , \ C \in \mathbb{C}\end{aligned}$$

According to the normalization condition (see 2.1) it has to hold that $\int ||0\rangle|^2 dx = 1$. With the standard integral $\int e^{-ax^2}dx = \sqrt{\pi/a}$ we find

$$\begin{aligned}|C|^2 \int e^{-\frac{x^2}{\hbar}} dx &= 1 \\ |C|^2 = (\pi\hbar)^{-\frac{1}{2}}\end{aligned}$$

We choose $C = (\pi\hbar)^{-\frac{1}{4}}$ such that $|0\rangle = (\pi\hbar)^{-\frac{1}{4}} e^{-\frac{x^2}{2\hbar}}$. □

The vacuum evolves in time as $\Psi(x,t) = e^{-iE_0\frac{t}{\hbar}}|0\rangle = e^{-\frac{it}{2}}|0\rangle$. How the number state $|n\rangle$ can be written in terms of the creation operator $a^\dagger$ and the vacuum $|0\rangle$ is presented in the following lemma.

Lemma 3.1.3 *Let $n \in \mathbb{N}$ and let $|0\rangle$ be the vacuum as defined in Lemma 3.1.2. The number state $|n\rangle$ is expressed in terms of the creation operator $a^\dagger$ and the vacuum in the following way*

$$|n\rangle = \frac{(a^\dagger)^n}{\sqrt{n!}}|0\rangle.$$

Proof. We have that

$$\begin{aligned}|n\rangle &= \frac{a^\dagger}{\sqrt{n}}|n-1\rangle \\ &= \frac{(a^\dagger)^2}{\sqrt{n(n-1)}}|n-2\rangle \\ &\vdots \\ &= \frac{(a^\dagger)^n}{\sqrt{n!}}|0\rangle.\end{aligned}$$

□

The Hamiltonian H has a very easy expression in terms of the creation and annihilation operators. This expression is given in the following corollary.

Corollary 3.1.4 *The Hamiltonian operator H corresponding to the harmonic oscillator is given by*

$$H = \hbar\left(a^\dagger a + \frac{1}{2}\right).$$

It gives the total energy of a quantum state in a harmonic oscillator.

PROOF. We chose $k = m = 1$. With this assumption we find

$$\begin{aligned} H &= -\frac{\hbar^2}{2m}\frac{d^2}{dx^2} + V(x) \\ &= -\frac{\hbar^2}{2}\frac{d^2}{dx^2} + \frac{1}{2}x^2 \\ &= \frac{1}{2}\left(x^2 + \left(\frac{\hbar}{i}\frac{d}{dx}\right)^2\right) \\ &= \frac{1}{2}\left(x^2 + p^2\right) \\ &= \hbar\frac{(x-ip)}{\sqrt{2\hbar}}\frac{(x+ip)}{\sqrt{2\hbar}} - \frac{1}{2}(ixp - ipx) \\ &= \hbar a^\dagger a - \frac{i}{2}[x,p] \\ &= \hbar\left(a^\dagger a + \frac{1}{2}\right) \end{aligned}$$

□

With this expression for H we see that for the solutions of the time-independent Schrödinger equation (the number states ($|n\rangle$) it holds that

$$\begin{aligned} H|n\rangle &= E_n|n\rangle \\ \hbar\left(a^\dagger a + \frac{1}{2}\right)|n\rangle &= \left(n + \frac{1}{2}\right)\hbar\omega|n\rangle \\ \left(a^\dagger a + \frac{1}{2}\right)|n\rangle &= \left(n + \frac{1}{2}\right)|n\rangle \\ a^\dagger a|n\rangle &= n|n\rangle. \end{aligned}$$

From this we see that a number state is defined as the eigenfunction of the number operator $a^\dagger a$.

We can express the observables x and p in terms of a and $a^\dagger$. This is presented in the following corollary.

Corollary 3.1.5 *The observables x and p are expressed in terms of a and $a^\dagger$ as*

$$x = \sqrt{\frac{\hbar}{2}}(a^\dagger + a) \quad \textit{and} \quad p = i\sqrt{\frac{\hbar}{2}}(a^\dagger - a)$$

It further holds that

$$[a, a^\dagger] = 1.$$

PROOF. The first result follows in a straightforward way from Definition 3.1.1.

We use $[x,p] = i\hbar$ (see 2.5) to see that the commutator of a and $a^\dagger$ is

$$\begin{aligned}[a,a^\dagger] &= \frac{1}{2\hbar}[x+ip, x-ip] \\ &= \frac{i}{2\hbar}(-[x,p]+[p,x]) \\ &= -\frac{i}{\hbar}([x,p]) = 1.\end{aligned}$$

□

3.2 Coherent states

We first give the definition of coherent states. Then we state some important properties.

Definition 3.2.1 *Let $\alpha \in \mathbb{C}$ and $|0\rangle$ be the vacuum such that $a|0\rangle = 0$ and $\langle 0|0\rangle = 1$. The coherent state corresponding to the value α is represented by $|\alpha\rangle$ and is defined by*

$$|\alpha\rangle = D(\alpha)|0\rangle$$
$$D(\alpha) = e^{\alpha a^\dagger - \alpha^* a}.$$

$D(\alpha)$ is called the displacement operator.

A coherent state has some important properties. These are stated in the following theorem.

Theorem 3.2.2 *Let $\alpha \in \mathbb{C}$ and $|0\rangle$ be the vacuum. Then,*

$$|\alpha\rangle = e^{-|\alpha|^2/2} e^{\alpha a^\dagger}|0\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle.$$

A coherent state is therefore a superposition of number states. It also holds that

$$a|\alpha\rangle = \alpha|\alpha\rangle \text{ and } \langle\alpha|\alpha\rangle = 1.$$

This means that a coherent state is normalized and is an eigenstate of the annihilation operator.

Proof. We first proof the first part of the theorem.
We can use Lemma A.0.3 with $A = \alpha a^\dagger$ and $B = -\alpha^* a$ because $[A,B] = [\alpha a^\dagger, -\alpha^* a] = -|\alpha|^2[a^\dagger, a] = |\alpha|^2$ is independent of A and B and so $[A,[A,B]] = [B,[A,B]] = 0$. With this lemma we find

$$\begin{aligned}|\alpha\rangle &= e^{\alpha a^\dagger - \alpha^* a}|0\rangle \\ &= e^{-\frac{1}{2}|\alpha|^2} e^{\alpha a^\dagger} e^{-\alpha^* a}|0\rangle.\end{aligned}$$

Using $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ and the fact that $a^n|0\rangle = 0$ for $n > 0$ and $a^n|0\rangle = |0\rangle$ for $n = 0$ we find that

$$\begin{aligned}|\alpha\rangle &= e^{-\frac{1}{2}|\alpha|^2} e^{\alpha a^\dagger} \sum_{n=0}^{\infty} \frac{(-\alpha^*)^n}{n!} a^n|0\rangle \\ &= e^{-\frac{1}{2}|\alpha|^2} e^{\alpha a^\dagger}|0\rangle\end{aligned}$$

With the definition of a number state, $|n\rangle = \frac{(a^\dagger)^n}{\sqrt{n!}}|0\rangle$ we find that

$$\begin{aligned} e^{-\frac{1}{2}|\alpha|^2} e^{\alpha a^\dagger}|0\rangle &= e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{n!} \left(a^\dagger\right)^n |0\rangle \\ &= e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle \end{aligned}$$

We use this result to prove the second part of the theorem. With the linearity of a and $a|n\rangle = \sqrt{n}|n-1\rangle$ we find

$$\begin{aligned} a|\alpha\rangle &= e^{-\frac{1}{2}|\alpha|^2} \sum_{n=1}^{\infty} \frac{\alpha^n}{\sqrt{(n-1)!}}|n-1\rangle \\ &= e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^{n+1}}{\sqrt{n!}}|n\rangle \\ &= \alpha e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle \\ &= \alpha|\alpha\rangle \end{aligned}$$

We can use Lemma A.0.3 with $A = \alpha a^\dagger - \alpha^* a$ and $B = -\alpha^* a + \alpha a^\dagger$ to prove that $D(\alpha)$ is a unitary operator because the commutator

$$\begin{aligned} [A,B] &= [\alpha a^\dagger - \alpha^* a, -\alpha^* a + \alpha a^\dagger] \\ &= -|\alpha|^2[a^\dagger, a] + \alpha^2[a^\dagger, a^\dagger] + (\alpha^*)^2\,[a,a] - |\alpha|^2[a^\dagger, a] \\ &= -|\alpha|^2([a^\dagger, a] + [a^\dagger, a]) \\ &= -|\alpha|^2([a^\dagger, a] - [a, a^\dagger]) \\ &= 0 \end{aligned}$$

is independent of A and B and therefore $[A,[A,B]] = [B,[A,B]] = 0$. With the lemma we find

$$\begin{aligned} D(\alpha)D^\dagger(\alpha) &= e^{\alpha a^\dagger - \alpha^* a} e^{-\alpha^* a + \alpha a^\dagger} \\ &= e^{\alpha a^\dagger - \alpha^* a - \alpha^* a + \alpha a^\dagger} \\ &= I \end{aligned}$$

Because $D(\alpha)$ is unitary it preserves inner products between states. This means that the coherent state $|\alpha\rangle$ is normalized:

$$\begin{aligned} \langle\alpha|\alpha\rangle &= \langle 0|D^\dagger(\alpha)D(\alpha)|0\rangle \\ &= \langle 0|0\rangle = 1 \end{aligned}$$

□

3.3 Squeezed states

We first define squeezed states and then give some important properties.

Definition 3.3.1 *Let $\zeta, \alpha \in \mathbb{C}$ and $|0\rangle$ be the vacuum. The squeezed state corresponding to the values ζ, α is represented by $|\zeta, \alpha\rangle$ and is defined by*

$$|\zeta, \alpha\rangle = S(\zeta)D(\alpha)|0\rangle$$

$$S(\zeta) = e^{\frac{1}{2}\zeta(a^\dagger)^2 - \frac{1}{2}\zeta^* a^2} \text{ and } D(\alpha) = e^{\alpha a^\dagger - \alpha^* a}.$$

$S(\zeta)$ is called the squeezing operator and ζ the squeezing parameter.

It is obvious that the coherent state is a special case of the squeezed state because $|0, \alpha\rangle = S(0)D(\alpha)|0\rangle = D(\alpha)|0\rangle = |\alpha\rangle$.

In the following theorem we show that a squeezed state is normalized.

Theorem 3.3.2 *Let $\zeta, \alpha \in \mathbb{C}$ and $|0\rangle$ be the vacuum. It holds that*

$$\langle \zeta, \alpha | \zeta, \alpha \rangle = 1$$

so $|\zeta, \alpha\rangle$ is normalized.

Proof. We can use Lemma A.0.3 with $A = \frac{1}{2}\zeta(a^\dagger)^2 - \frac{1}{2}\zeta^* a^2$ and $B = \frac{1}{2}\zeta^* a^2 - \frac{1}{2}\zeta(a^\dagger)^2$ to prove that $S(\zeta)$ is a unitary operator because the commutator

$$\begin{aligned}
[A, B] &= [\frac{1}{2}\zeta(a^\dagger)^2 - \frac{1}{2}\zeta^* a^2, \frac{1}{2}\zeta^* a^2 - \frac{1}{2}\zeta(a^\dagger)^2] \\
&= \frac{1}{2}|\zeta|^2([(a^\dagger)^2, a^2] + [a^2, (a^\dagger)^2]) \\
&= \frac{1}{2}|\zeta|^2([(a^\dagger)^2, a^2] - [(a^\dagger)^2, a^2]) \\
&= 0
\end{aligned}$$

is independent of A and B and therefore $[A, [A, B]] = [B, [A, B]] = 0$. With the lemma we find that the operator $S(\zeta)$ is unitary;

$$\begin{aligned}
S(\zeta)S^\dagger(\zeta) &= e^{\frac{1}{2}\zeta(a^\dagger)^2 - \frac{1}{2}\zeta^* a^2} e^{\frac{1}{2}\zeta^* a^2 - \frac{1}{2}\zeta(a^\dagger)^2} \\
&= e^{\frac{1}{2}\zeta(a^\dagger)^2 - \frac{1}{2}\zeta^* a^2 + \frac{1}{2}\zeta^* a^2 - \frac{1}{2}\zeta(a^\dagger)^2} \\
&= I.
\end{aligned}$$

This gives us that

$$\begin{aligned}
\langle \zeta, \alpha | \zeta, \alpha \rangle &= \langle 0 | D^\dagger(\alpha) S^\dagger(\zeta) S(\zeta) D(\alpha) | 0 \rangle \\
&= \langle 0 | D^\dagger(\alpha) D(\alpha) | 0 \rangle \\
&= \langle 0 | 0 \rangle \\
&= 1
\end{aligned}$$

□

The following theorem tells us that there is another way to represent squeezed states and that the two possible representations are equivalent.

Theorem 3.3.3 *Let $\alpha \in \mathbb{C}$ and $\zeta = re^{i\phi}$ with $r > 0, \phi \in [0, 2\pi)$ and let $|0\rangle$ be the vacuum. Then*

$$S(\zeta)D(\alpha) = D(\gamma)S(\zeta)$$

with

$$\alpha = \gamma \cosh r - \overline{\gamma} e^{i\phi} \sinh r.$$

PROOF. This lemma will be proved in Section 4.1. □

Theorem 3.3.3 implicates that there are two representations of a squeezed state. For one representation, we first apply the displacement and then the squeezing operator to the vacuum, for the other representation vice versa. The order of D and S is just a matter of agreement. In this thesis we will represent squeezed states as $|\zeta, \alpha\rangle = S(\zeta)D(\alpha)|0\rangle$.

Chapter 4

Statistics of Squeezed States

In this chapter we will study some important properties of squeezed states. In Section 4.1 we will calculate the expectation and the variance of a class of variables for squeezed states. From the results of these calculations we give for each squeezed state $|\zeta, \alpha\rangle$ a generalized position and momentum pair x', p' such that the squeezed state has minimum uncertainty with respect to this variable pair.
In Section 4.2 we will calculate the time-independent wave function of the squeezed states that has minimum uncertainty with respect to the observables position x and momentum p. From this wave function we will deduce the probability distributions that give us the probability to measure a certain value of x or p.
In Section 4.3 we will prove that squeezed states cannot be copied and in Section 4.4 we will study the time evolution of squeezed states in free space. This gives us the time-dependent wave function of squeezed states that have minimum uncertainty with respect to x and p.
In Section 4.5 we will show how to choose the parameters of a squeezed state such that a squeezed state is squeezed in x or in p. The section also serve as a general summary of this chapter.

Because a coherent state is a special case of a squeezed state, we find the analogous results for coherent states by substituting $\zeta = 0$.

4.1 Expectation and variance of generalized position and momentum

We calculate the expectation and the variance of the canonical observables x_β and p_β for squeezed states. These generalized position and momentum operators are defined in the following definition.

Definition 4.1.1 *Let $\beta \in [0, 2\pi)$. The canonical observables x_β and p_β are defined by*

$$x_\beta = \sqrt{\frac{\hbar}{2}}\left(a^\dagger e^{i\beta} + a e^{-i\beta}\right) \text{ and } p_\beta = i\sqrt{\frac{\hbar}{2}}\left(a^\dagger e^{i\beta} - a e^{-i\beta}\right).$$

From the definition we easily see that these operators are Hermitian operators. The well known position variable x and momentum variable p are special cases of these variables x_β and p_β and they are found by substituting $\beta = 0$.

The uncertainty relation for x_β and p_β equals that for x and p, i.e. the Heisenberg uncertainty relation. We find this result in the following lemma.

Lemma 4.1.2 *Let $\beta \in [0, 2\pi)$. It holds that*

$$\sigma_{x_\beta}\sigma_{p_\beta} \geq \frac{\hbar}{2}.$$

This relation is a Heisenberg uncertainty relation for the Hermitian operators x_β, p_β.

Proof. The commutator of x_β and p_β is

$$\begin{aligned}
[x_\beta, p_\beta] &= i\frac{\hbar}{2}[a^\dagger e^{i\beta} + ae^{-i\beta}, a^\dagger e^{i\beta} - ae^{-i\beta}] \\
&= i\frac{\hbar}{2}(-[a^\dagger e^{i\beta}, ae^{-i\beta}] + [ae^{-i\beta}, a^\dagger e^{i\beta}]) \\
&= i\frac{\hbar}{2}(-[a^\dagger, a] + [a, a^\dagger]) \\
&= i\hbar.
\end{aligned}$$

This means that the uncertainty relation for x_β and p_β is given by

$$\begin{aligned}
\sigma^2_{x_\beta}\sigma^2_{p_\beta} &\geq \left(\frac{1}{2i}\langle[x_\beta, p_\beta]\rangle\right)^2 \\
&= \frac{\hbar^2}{4}
\end{aligned}$$

This completes the proof of this corollary. □

The following lemma helps us to calculate the expectation and variances of x_β and p_β for a squeezed state.

Lemma 4.1.3 *Let $\zeta = re^{i\phi}$ with $r > 0$ and $\phi \in [0, 2\pi)$. Then*

$$S^\dagger(\zeta)aS(\zeta) = a\cosh r + a^\dagger e^{i\phi}\sinh r$$

and

$$S^\dagger(\zeta)a^\dagger S(\zeta) = a^\dagger\cosh r + ae^{-i\phi}\sinh r.$$

Proof. We have that

$$\begin{aligned}
S^\dagger(\zeta)aS(\zeta) &= e^{\frac{1}{2}\zeta^* a^2 - \frac{1}{2}\zeta(a^\dagger)^2} a e^{\frac{1}{2}\zeta(a^\dagger)^2 - \frac{1}{2}\zeta^* a^2} \\
&= e^{\frac{1}{2}\zeta^* a^2 - \frac{1}{2}\zeta(a^\dagger)^2} a e^{-(\frac{1}{2}\zeta^* a^2 - \frac{1}{2}\zeta(a^\dagger)^2)}.
\end{aligned}$$

We can apply Lemma A.0.2 with $A = \frac{1}{2}\zeta^* a^2 - \frac{1}{2}\zeta(a^\dagger)^2$ and $B = a$. Using Lemma A.0.4 we find that

$$\begin{aligned}
[A, B] &= [\frac{1}{2}\zeta^* a^2 - \frac{1}{2}\zeta(a^\dagger)^2, a] \\
&= -\frac{1}{2}\zeta[(a^\dagger)^2, a] \\
&= -\frac{1}{2}\zeta(a^\dagger[a^\dagger, a] + [a^\dagger, a]a^\dagger) \\
&= \zeta a^\dagger
\end{aligned}$$

From this we see that

$$[A_{(1)},[A_{(2)},\ldots,[A_{(n)},B]]\ldots] = \begin{cases} \zeta^{\frac{n}{2}}(\zeta^*)^{\frac{n}{2}}\,a = |\zeta|^n a = r^n a & \text{if } n \text{ is even} \\ \zeta^{\frac{n+1}{2}}(\zeta^*)^{\frac{n-1}{2}}a^\dagger = \zeta r^{n-1}a^\dagger = e^{i\phi}r^n a^\dagger & \text{if } n \text{ is odd} \end{cases}$$

Lemma A.0.2 gives us that

$$\begin{aligned} S^\dagger(\zeta)aS(\zeta) &= \sum_{n=0}^{\infty}\frac{1}{n!}[A_{(1)},[A_{(2)},\ldots,[A_{(n)},B]]\ldots] \\ &= \sum_{n=0}^{\infty}\left(a\frac{r^{2n}}{(2n)!} + a^\dagger e^{i\phi}\frac{r^{2n+1}}{(2n+1)!}\right) \\ &= a\sum_{n=0}^{\infty}\left(\frac{r^{2n}}{(2n)!}\right) + a^\dagger e^{i\phi}\sum_{n=0}^{\infty}\left(\frac{r^{2n+1}}{(2n+1)!}\right) \\ &= a\cosh r + a^\dagger e^{i\phi}\sinh r. \end{aligned}$$

Taking the Hermitian conjugate we immediately see that

$$(S^\dagger(\zeta)aS(\zeta))^\dagger = S^\dagger(\zeta)a^\dagger S(\zeta) = a^\dagger\cosh r + ae^{-i\phi}\sinh r$$

□

We deduce the following useful corollary from Lemma 4.1.3 that helps us to calculate the expectations and variances of x_β and p_β for a squeezed state.

Corollary 4.1.4 *Let $\zeta = re^{i\phi}$ with $r > 0$ and $\phi \in [0, 2\pi)$. Then*

$$\begin{aligned} S^\dagger(\zeta)aaS(\zeta) &= a^2\cosh^2 r + (a^\dagger)^2 e^{2i\phi}\sinh^2 r + a^\dagger a e^{i\phi}\sinh(2r) + \frac{1}{2}e^{i\phi}\sinh(2r) \\ S^\dagger(\zeta)a^\dagger a^\dagger S(\zeta) &= a^2 e^{-2i\phi}\sinh^2 r + (a^\dagger)^2\cosh^2 r + a^\dagger a e^{-i\phi}\sinh(2r) + \frac{1}{2}e^{-i\phi}\sinh(2r) \\ S^\dagger(\zeta)a^\dagger aS(\zeta) &= \frac{1}{2}a^2 e^{-i\phi}\sinh(2r) + \frac{1}{2}(a^\dagger)^2 e^{i\phi}\sinh(2r) + a^\dagger a\cosh(2r) + \sinh^2 r \\ S^\dagger(\zeta)aa^\dagger S(\zeta) &= \frac{1}{2}a^2 e^{-i\phi}\sinh(2r) + \frac{1}{2}(a^\dagger)^2 e^{i\phi}\sinh(2r) + a^\dagger a\cosh(2r) + \cosh^2 r. \end{aligned}$$

Proof. The squeezing operator $S(\zeta)$ is a unitary operator so $S^\dagger(\zeta)S(\zeta) = I$. With this we find

$$\begin{aligned} S^\dagger(\zeta)aaS(\zeta) &= S^\dagger(\zeta)aS(\zeta)S^\dagger(\zeta)aS(\zeta) \\ &= \Big(a\cosh r + a^\dagger e^{i\phi}\sinh r\Big)^2. \end{aligned}$$

Using linearity, the formula $\frac{1}{2}\sinh(2r) = \sinh r\cosh r$ and the commutator $[a^\dagger, a] = -1$ we find

$$S^\dagger(\zeta)aaS(\zeta) = a^2\cosh^2 r + (a^\dagger)^2 e^{2i\phi}\sinh^2 r + a^\dagger a e^{i\phi}\sinh(2r) + \frac{1}{2}e^{i\phi}\sinh 2r.$$

Taking the Hermitian conjugate on both sides gives us that

$$S^\dagger(\zeta)a^\dagger a^\dagger S(\zeta) = (a^\dagger)^2\cosh^2 r + a^2 e^{-2i\phi}\sinh^2 r + a^\dagger a e^{-i\phi}\sinh(2r) + \frac{1}{2}e^{-i\phi}\sinh 2r.$$

Using the same argumentations we find that

$$\begin{aligned} S^\dagger(\zeta)a^\dagger aS(\zeta) &= S^\dagger(\zeta)a^\dagger S(\zeta)S^\dagger(\zeta)aS(\zeta) \\ &= \left(a^\dagger \cosh r + ae^{-i\phi}\sinh r\right)\left(a\cosh r + a^\dagger e^{i\phi}\sinh r\right) \\ &= \frac{1}{2}a^2e^{-i\phi}\sinh(2r) + \frac{1}{2}(a^\dagger)^2e^{i\phi}\sinh(2r) + a^\dagger a\cosh(2r) + \sinh^2 r. \end{aligned}$$

The operator $S^\dagger(\zeta)a^\dagger aS(\zeta)$ is Hermitian so we calculate $S^\dagger(\zeta)aa^\dagger S(\zeta)$ in the direct way.

$$\begin{aligned} S^\dagger(\zeta)aa^\dagger S(\zeta) &= S^\dagger(\zeta)aS(\zeta)S^\dagger(\zeta)a^\dagger S(\zeta) \\ &= \left(a\cosh r + a^\dagger e^{i\phi}\sinh r\right)\left(a^\dagger \cosh r + ae^{-i\phi}\sinh r\right) \\ &= \frac{1}{2}a^2e^{-i\phi}\sinh(2r) + \frac{1}{2}(a^\dagger)^2e^{i\phi}\sinh(2r) + a^\dagger a\cosh(2r) + \cosh^2 r \end{aligned}$$

□

We are now able to prove Theorem 3.3.3. We give this proof before we go further with our calculations in this section.

Proof of Theorem 3.3.3
Let $\alpha, \gamma, \zeta \in \mathbb{C}$ with $\zeta = re^{i\phi}$ where $r > 0$ and $\phi \in [0, 2\pi)$. We want to prove that

$$S(\zeta)D(\alpha) = D(\gamma)S(\zeta)$$

holds for $\alpha = \gamma\cosh r - \overline{\gamma}e^{i\phi}\sinh r$. Because $S(\zeta)$ is unitary this equality is equivalent to

$$D(\alpha) = S^\dagger(\zeta)D(\gamma)S(\zeta).$$

Using the unitarity of $S(\zeta)$ and Lemma 4.1.3 we find that

$$\begin{aligned} S^\dagger(\zeta)D(\gamma)S(\zeta) &= S^\dagger(\zeta)e^{\gamma a^\dagger - \overline{\gamma}a}S(\zeta) \\ &= S^\dagger(\zeta)\sum_{n=0}^{\infty}\frac{(\gamma a^\dagger - \overline{\gamma}a)^n}{n!}S(\zeta) \\ &= \sum_{n=0}^{\infty}\frac{(S^\dagger(\zeta)(\gamma a^\dagger - \overline{\gamma}a)S(\zeta))^n}{n!} \\ &= \sum_{n=0}^{\infty}\frac{(\gamma S^\dagger(\zeta)a^\dagger S(\zeta) - \overline{\gamma}S^\dagger(\zeta)aS(\zeta))^n}{n!} \\ &= \sum_{n=0}^{\infty}\frac{(a^\dagger\gamma\cosh r + a\gamma e^{-i\phi}\sinh r - a\overline{\gamma}\cosh r - a^\dagger\overline{\gamma}e^{i\phi}\sinh r)^n}{n!} \\ &= \sum_{n=0}^{\infty}\frac{(a^\dagger(\gamma\cosh r - \overline{\gamma}e^{i\phi}\sinh r) - a(\overline{\gamma}\cosh r - \gamma e^{-i\phi}\sinh r))^n}{n!} \\ &= e^{a^\dagger(\gamma\cosh r - \overline{\gamma}e^{i\phi}\sinh r) - a(\overline{\gamma}\cosh r - \gamma e^{-i\phi}\sinh r)} \\ &= D(\gamma\cosh r - \overline{\gamma}e^{i\phi}\sinh r) \end{aligned}$$

This completes the proof of Theorem 3.3.3. □

We present the theorem in which we give the expectation and variance of x_β and p_β.

Theorem 4.1.5 *Let $|\zeta,\alpha\rangle = S(\zeta)D(\alpha)|0\rangle$ be a squeezed state with $\zeta = re^{i\phi}$ and $\alpha = se^{i\theta}$ where $r,s>0$ and $\phi,\theta\in[0,2\pi)$. The expectation and variances of the observables x_β and p_β for the squeezed state $|\zeta,\alpha\rangle$ are*

$$\begin{aligned}
\langle x_\beta\rangle &= \sqrt{2\hbar}s(\cos(\theta-\beta)\cosh r+\cos(\theta-\phi+\beta)\sinh r)\\
\langle p_\beta\rangle &= \sqrt{2\hbar}s(\sin(\theta-\beta)\cosh r-\sin(\theta-\phi+\beta)\sinh r)\\
\sigma^2_{x_\beta} &= \frac{\hbar}{2}(\cosh(2r)+\cos(\phi-2\beta)\sinh 2r)\\
\sigma^2_{p_\beta} &= \frac{\hbar}{2}(\cosh(2r)-\cos(\phi-2\beta)\sinh 2r)
\end{aligned}$$

Proof. Because x_β and p_β are Hermitian operators, measurement of these observables are projective measurements. According to Postulate 3 (see 2.4), the expectations are respectively $\langle x_\beta\rangle = \langle\zeta,\alpha|x_\beta|\zeta,\alpha\rangle$ and $\langle p_\beta\rangle = \langle\zeta,\alpha|p_\beta|\zeta,\alpha\rangle$. We use Lemma 4.1.3 and the relation $a|\alpha\rangle = \alpha|\alpha\rangle$. We find

$$\begin{aligned}
\langle x_\beta\rangle &= \sqrt{\frac{\hbar}{2}}\langle\zeta,\alpha|(a^\dagger e^{i\beta}+ae^{-i\beta})|\zeta,\alpha\rangle\\
&= \sqrt{\frac{\hbar}{2}}\langle\alpha|S^\dagger(\zeta)(a^\dagger e^{i\beta}+ae^{-i\beta})S(\zeta)|\alpha\rangle\\
&= \sqrt{\frac{\hbar}{2}}\langle\alpha|e^{i\theta}S^\dagger(\zeta)a^\dagger S(\zeta)+e^{-i\beta}S^\dagger(\zeta)aS(\zeta)|\alpha\rangle\\
&= \sqrt{\frac{\hbar}{2}}\langle\alpha|a^\dagger e^{i\beta}\cosh r+ae^{-i\phi+i\beta}\sinh r+ae^{-i\beta}\cosh r+a^\dagger e^{i\phi-i\beta}\sinh r|\alpha\rangle\\
&= \sqrt{\frac{\hbar}{2}}\left(\alpha^* e^{i\beta}\cosh r+\alpha e^{-i\phi+i\beta}\sinh r+\alpha e^{-i\beta}\cosh r+\alpha^* e^{i\phi-i\beta}\sinh r\right)\\
&= \sqrt{\frac{\hbar}{2}}\left(s\left(e^{i(\theta-\beta)}+e^{-i(\theta-\beta)}\right)\cosh r+s\left(e^{i(\theta-\phi+\beta)}+e^{-i(\theta-\phi+\beta)}\right)\sinh r\right)\\
&= \sqrt{2\hbar}s\left(\cos(\theta-\beta)\cosh r+\cos(\theta-\phi+\beta)\sinh r\right)
\end{aligned}$$

The calculation of $\langle p_\beta\rangle$ works in a similar way. We find

$$\begin{aligned}
\langle p_\beta\rangle &= i\sqrt{\frac{\hbar}{2}}\langle\zeta,\alpha|(a^\dagger e^{i\beta}-ae^{-i\beta})|\zeta,\alpha\rangle\\
&= \sqrt{2\hbar}s\left(\sin(\theta-\beta)\cosh r-\sin(\theta-\phi+\beta)\sinh r\right)
\end{aligned}$$

To calculate the variances, we note that x_β^2 and p_β^2 are Hermitian operators. The calculation of $\langle x_\beta^2\rangle$ and $\langle p_\beta^2\rangle$ follow the line of reasoning of the calculation of $\langle x_\beta\rangle$. As an illustration we show some steps of the calculation of $\langle x_\beta^2\rangle$.

We use Corollary 4.1.4, $a|\alpha\rangle = \alpha|\alpha\rangle$ and some trigonometric relations. We find

$$\begin{aligned}
\langle {x_\beta}^2\rangle &= \frac{\hbar}{2}\langle\zeta,\alpha|(a^\dagger e^{i\beta} + ae^{-i\beta})^2|\zeta,\alpha\rangle \\
&= \frac{\hbar}{2}\langle\alpha|S^\dagger(\zeta)\left(a^\dagger a^\dagger e^{2i\beta} + a^\dagger a + aa^\dagger + aae^{-2i\beta}\right)S(\zeta)|\alpha\rangle \\
&= \frac{\hbar}{2}\langle\alpha|\left(e^{2i\beta}S^\dagger(\zeta)a^\dagger a^\dagger S(\zeta) + S^\dagger(\zeta)a^\dagger aS(\zeta) + S^\dagger(\zeta)aa^\dagger S(\zeta) + e^{-2i\beta}S^\dagger(\zeta)aaS(\zeta)\right)|\alpha\rangle \\
&= \frac{\hbar}{2}\langle\alpha|(a^\dagger)^2\left(e^{2i\beta}\cosh^2 r + \frac{1}{2}e^{i\phi}\sinh(2r) + \frac{1}{2}e^{i\phi}\sinh(2r) + e^{i(2\phi-2\beta)}\sinh^2 r\right)|\alpha\rangle + \\
&\quad \frac{\hbar}{2}\langle\alpha|a^\dagger a\left(e^{i(-\phi=2\beta)}\sinh(2r) + \cosh(2r) + \cosh(2r) + e^{i(\phi-2\beta)}\sinh 2r\right)|\alpha\rangle + \\
&\quad \frac{\hbar}{2}\langle\alpha|a^2\left(e^{i(-2\phi+2\beta}\sinh^2 r + \frac{1}{2}e^{-i\phi}\sinh(2r) + \frac{1}{2}e^{-i\phi}\sinh(2r) + e^{-2i\beta}\cosh^2 r\right)|\alpha\rangle + \\
&\quad \frac{\hbar}{2}\langle\alpha|\left(\frac{1}{2}e^{-i(\phi-2\beta)}\sinh(2r) + \sinh^2 r + \cosh^2 r + \frac{1}{2}e^{i(\phi-2\beta)}\sinh 2r\right)|\alpha\rangle \\
&= \frac{\hbar\,(\alpha^*)^2}{2}\left(e^{2i\beta}\cosh^2 r + e^{i\phi}\sinh(2r) + e^{i(2\phi-2\beta)}\sinh^2 r\right) + \\
&\quad \frac{\hbar|\alpha|^2}{2}\left(2\cos(\phi-2\beta)\sinh(2r) + 2\cosh(2r)\right) + \\
&\quad \frac{\hbar\alpha^2}{2}\left(e^{-i\phi}\sinh(2r) + e^{-2i\beta}\cosh^2 r + e^{-i(2\phi-\beta)}\sinh^2 r\right) + \frac{\hbar}{2}\left(\cosh(2r) + \cos(\phi-2\beta)\sinh 2r\right) \\
&= 2s^2\hbar\left(\cos(\theta-\beta)\cosh r + \cos(\theta-\phi+\beta)\sinh r\right)^2 + \frac{\hbar}{2}\left(\cosh(2r) + \cos(\phi-2\beta)\sinh 2r\right) \\
&= \langle x_\beta\rangle^2 + \frac{\hbar}{2}\left(\cosh(2r) + \cos(\phi-2\beta)\sinh 2r\right)
\end{aligned}$$

The variance of x_β follows easily from $\langle x_\beta^2\rangle$;

$$\begin{aligned}
\sigma_{x_\beta}^2 &= \langle {x_\beta}^2\rangle - \langle x_{beta}\rangle^2 \\
&= \langle x_\beta\rangle^2 + \frac{\hbar}{2}\left(\cosh(2r) + \cos(\phi-2\beta)\sinh 2r\right) - \langle x_\beta\rangle^2 \\
&= \frac{\hbar}{2}\left(\cosh(2r) + \cos(\phi-2\beta)\sinh 2r\right)
\end{aligned}$$

The argumentation of the calculation of $\langle p_\beta^2\rangle$ is similar to that of $\langle x_\beta^2\rangle$. We find

$$\begin{aligned}
\langle p_\beta^2\rangle &= -\frac{\hbar}{2}\langle\zeta,\alpha|(a^\dagger e^{i\beta} - ae^{-i\beta})^2|\zeta,\alpha\rangle \\
&= \langle p_\beta\rangle^2 + \frac{\hbar}{2}\left(\cosh(2r) - \cos(\phi-2\beta)\sinh 2r\right)
\end{aligned}$$

The variance of p_β is

$$\begin{aligned}
\sigma_{p_\beta}^2 &= \langle p_\beta^2\rangle - \langle p_\beta\rangle^2 \\
&= \langle p_\beta\rangle^2 + \frac{\hbar}{2}\left(\cosh(2r) - \cos(\phi-2\beta)\sinh 2r\right) - \langle p_\beta\rangle^2 \\
&= \frac{\hbar}{2}\left(\cosh(2r) - \cos(\phi-2\beta)\sinh 2r\right)
\end{aligned}$$

□

For a particular choice of β we find that the squeezed state $|\zeta, \alpha\rangle$ has minimum uncertainty with respect to x_β and p_β, i.e. x_β and p_β satisfy the Heisenberg uncertainty principle with equality. This result is presented in the next theorem.

Theorem 4.1.6 *Let $|\zeta, \alpha\rangle$ be a squeezed state with $\zeta = re^{i\phi}$ and $\alpha = se^{i\theta}$ where $r \in \mathbb{R}, s > 0$ and $\phi, \theta \in [0, 2\pi)$. This state has minimum uncertainty with respect to the observables x_β and p_β if and only if $2\beta = \phi$. This means that the observable pair $x_{\phi/2}$ and $p_{\phi/2}$ satisfies the Heisenberg uncertainty principle with equality:*

$$\sigma_{x_{\frac{\phi}{2}}} \sigma_{p_{\frac{\phi}{2}}} = \frac{\hbar}{2}.$$

Further, for the coherent state $|\alpha\rangle$ every observable pair x_β, p_β satisfies Heisenberg's uncertainty principle with equality.

Proof. From Theorem 4.1.5 we see that

$$\begin{aligned}
\sigma_{x_\beta}\sigma_{p_\beta} &= \frac{\hbar}{2}\sqrt{(\cosh(2r) + \cos(\phi - 2\beta)\sinh 2r)(\cosh(2r) - \cos(\phi - 2\beta)\sinh(2r))} \\
&= \frac{\hbar}{2}\sqrt{\cosh^2(2r) - \cos^2(\phi - 2\beta)\sinh^2 2r} \\
&= \frac{\hbar}{2}\sqrt{1 + \sinh^2(2r) - \cos^2(\phi - 2\beta)\sinh^2(2r)} \\
&= \frac{\hbar}{2}\sqrt{1 + \sin^2(\phi - 2\beta)\sinh^2(2r)}
\end{aligned}$$

Heisenberg's uncertainty principle is satisfied with equality if

$$\begin{aligned}
\sqrt{1 + \sin^2(\phi - 2\beta)\sinh^2(2r)} &= 1 \\
\sin^2(\phi - 2\beta)\sinh^2(2r) &= 0 \\
r = 0 \quad \text{or} \quad &\sin(\phi - 2\beta) = 0.
\end{aligned}$$

If $r = 0$ then $\zeta = 0$ so $S(\zeta) = 1$. This means that $|\zeta, \alpha\rangle = |\alpha\rangle$ is a coherent state. We can conclude from the solution $r = 0$ that every coherent state satisfies Heisenberg's uncertainty relation with equality for the observable pair x_β, p_β.

The solutions to $\sin(\phi - 2\beta) = 0$ are $\phi - 2\beta = k\pi$ so $\phi = 2\beta + k\pi$ where $k \in \mathbb{N}$. This means that the squeezed states $|re^{i(2\beta+2k\pi)}, \alpha\rangle = |re^{2i\beta}, \alpha\rangle$ and $|re^{i(2\beta+(2k+1)\pi)}, \alpha\rangle = |-re^{2i\beta}, \alpha\rangle$ have minimum uncertainty with respect to the observable pair x_β, p_β. If we take $r \in \mathbb{R}$ instead of $r > 0$ then we can say that the state $|re^{i\phi}, \alpha\rangle$ has minimum uncertainty with respect to the pair x_β, p_β if and only if $\phi = 2\beta$. □

For coherent states ($r = 0$) the expectation and variance of x_β and p_β easily follow from Theorem 4.1.5 by substituting $r = 0$. They are presented in the following corollary.

Corollary 4.1.7 *Let $|\alpha\rangle = D(\alpha)|0\rangle$ be a coherent state with $\alpha = se^{i\theta}$ where $s > 0$ and $\theta \in [0, 2\pi)$. Then*

$$\begin{aligned}
\langle x_\beta \rangle &= \sqrt{2\hbar} s \cos(\theta - \beta) \\
\langle p_\beta \rangle &= \sqrt{2\hbar} s \sin(\theta - \beta) \\
\sigma^2_{x_\beta} &= \frac{\hbar}{2} \\
\sigma^2_{p_\beta} &= \frac{\hbar}{2}
\end{aligned}$$

As we already proved in Theorem 4.1.6 a coherent state has minimum uncertainty for all values $\beta \in [0, 2\pi)$.

The statistical properties of coherent states with respect to the observables x and p can be found by substituting $\beta = 0$ in Corollary 4.1.7.

The statistical properties of minimum uncertainty squeezed states with respect to the variables $x_\beta = x_{\phi/2}$ and $p_\beta = p_{\phi/2}$ follow from Theorem 4.1.5 and are presented in the following corollary.

Corollary 4.1.8 *Let $|\zeta, \alpha\rangle$ be a squeezed state with $\zeta = re^{i\phi}$ and $\alpha = se^{i\theta}$ where $r \in \mathbb{R}, s > 0$ and $\phi, \theta \in [0, 2\pi)$. This squeezed state has minimum uncertainty with respect to the variables $x_{\phi/2}$ and $p_{\phi/2}$. The expectation and variance of these variables are:*

$$\begin{aligned}
\langle x_{\frac{\phi}{2}} \rangle &= \sqrt{2\hbar} s \cos\left(\theta - \frac{\phi}{2}\right) e^r \\
\langle p_{\frac{\phi}{2}} \rangle &= \sqrt{2\hbar} s \sin\left(\theta - \frac{\phi}{2}\right) e^{-r} \\
\sigma^2_{x_{\frac{\phi}{2}}} &= \frac{\hbar}{2} e^{2r} \\
\sigma^2_{p_{\frac{\phi}{2}}} &= \frac{\hbar}{2} e^{-2r}
\end{aligned}$$

PROOF. Substitute $\beta = \frac{\phi}{2}$ in the results from Theorem 4.1.5. □

In this thesis we will mainly work with the observables position x and momentum p. The squeezed states with minimum uncertainty with respect to x and p have $\beta = \phi/2 = 0$ such that $\zeta = r \in \mathbb{R}$. From now on with a minimum uncertainty squeezed state we mean a squeezed state that has minimum uncertainty with respect to x and p. The expectations and variances of such a minimum uncertainty state easily follow from Theorem 4.1.5 by substituting $\beta = \phi = 0$ and are given in the following corollary.

Corollary 4.1.9 *Let $|r, \alpha\rangle = S(r)D(\alpha)|0\rangle$ be a minimum uncertainty squeezed state with $r \in \mathbb{R}$ and $\alpha = se^{i\theta}$ where $s > 0$ and $\theta \in [0, 2\pi)$. The expectation and variance of x and p are*

$$\begin{aligned}
\langle x \rangle &= \sqrt{2\hbar} s \cos\theta e^r \\
\langle p \rangle &= \sqrt{2\hbar} s \sin\theta e^{-r} \\
\sigma^2_x &= \frac{\hbar}{2} e^{2r} \\
\sigma^2_p &= \frac{\hbar}{2} e^{-2r}
\end{aligned}$$

4.2 Probability distributions of minimum uncertainty squeezed states

In the previous section we did some algebraic calculations on squeezed states. These calculations showed us that the squeezed state $|re^{i\phi}, \alpha\rangle$ where $r \in \mathbb{R}, \alpha \in \mathbb{C}$ and $\phi \in [0, 2\pi)$ has minimum uncertainty with respect to the observable pair $x_{\phi/2}, p_{\phi/2}$. Because from now on we only work with the observable pair x, p we choose $\phi = 0$ to obtain the squeezed state $|r, \alpha\rangle$ that has minimum uncertainty with respect to x and p .

In this section we calculate the probability distributions that give us the probability to measure a certain position value or a certain momentum value for the minimum uncertainty squeezed state $|r, \alpha\rangle$ with $r \in \mathbb{R}$ and $\alpha \in \mathbb{C}$.

There is a lemma from Appendix A that we use very often in the following lemma's, preceding the theorem that presents the probability distributions. We present the result of this lemma before we go further. The proof of the lemma can be found in Appendix A.

Lemma A.0.3 *Let A, B be linear operators. If $[A, [A, B]] = [B, [A, B]] = 0$ then*

$$e^{A+B} = e^{-\frac{1}{2}[A,B]} e^A e^B$$

This is a descendent of the Baker-Campbell-Hausdorff formula, presented in Lemma A.0.2.

In the following two lemma's we give explicit expressions for $D(\alpha)$ and $S(r)$ with $\alpha \in \mathbb{C}$ and $r \in \mathbb{R}$. These lemma's help us to find the time-independent wave function of a coherent state and a minimum uncertainty squeezed state.

Lemma 4.2.1 *Let $\langle x \rangle$ and $\langle p \rangle$ be the expectation for the minimum uncertainty squeezed states as defined in Corollary 4.1.9 such that $e^{-r}\langle x \rangle$ and $e^r \langle p \rangle$ are the expectations for a coherent state as defined in Corollary 4.1.7 . Let $\alpha = se^{i\theta}$ where $s > 0$ and $\theta \in [0, 2\pi)$. A more explicit representation for the displacement operator is given by*

$$D(\alpha) = e^{-\frac{i}{2\hbar}\langle x \rangle \langle p \rangle} e^{\frac{i}{\hbar} e^r \langle p \rangle x} e^{-e^{-r}\langle x \rangle \frac{\partial}{\partial x}}$$

Proof. First, we express $D(\alpha)$ in terms of x and p instead of in a and $a^\dagger$.

$$\begin{aligned}
D(\alpha) &= e^{\alpha a^\dagger - \alpha^* a} \\
&= \exp\left(se^{i\theta} \left(\frac{x - ip}{\sqrt{2\hbar}} \right) - se^{-i\theta} \left(\frac{x + ip}{\sqrt{2\hbar}} \right) \right) \\
&= \exp\left(\frac{s}{\sqrt{2\hbar}} \left(x \left(e^{i\theta} - e^{-i\theta} \right) \right) - \frac{is}{\sqrt{2\hbar}} \left(p \left(e^{i\theta} + e^{-i\theta} \right) \right) \right) \\
&= \exp\left(is\sqrt{\frac{2}{\hbar}} \sin(\theta) x - is\sqrt{\frac{2}{\hbar}} \cos(\theta) p \right)
\end{aligned}$$

We can Lemma A.0.3 with $A = is\sqrt{\frac{2}{\hbar}}\sin(\theta)x$ and $B = -is\sqrt{\frac{2}{\hbar}}\cos(\theta)p$ because

$$\begin{aligned}[A,B] &= [is\sqrt{\frac{2}{\hbar}}\sin(\theta)x, -is\sqrt{\frac{2}{\hbar}}\cos(\theta)p] \\ &= \frac{2s^2}{\hbar}\sin(\theta)\cos(\theta)[x,p] \\ &= 2is^2\sin(\theta)\cos(\theta)\end{aligned}$$

is independent of A and B and therefore $[A,[A,B]] = [B,[A,B]] = 0$. Lemma A.0.3 gives us that

$$\begin{aligned}D(\alpha) &= e^{-is^2\sin\theta\cos\theta}e^{is\sqrt{\frac{2}{\hbar}}\sin(\theta)x}e^{-is\sqrt{\frac{2}{\hbar}}\cos(\theta)p} \\ &= e^{-\frac{i}{2\hbar}\langle x\rangle\langle p\rangle}e^{\frac{i}{\hbar}e^r\langle p\rangle x}e^{-e^{-r}\langle x\rangle\frac{\partial}{\partial x}}\end{aligned}$$

□

The following lemma gives a convenient representation for $S(r)$ with $r \in \mathbb{R}$.

Lemma 4.2.2 *Let $r \in \mathbb{R}$. A more convenient representation of the squeezing operator $S(r)$ is given by*

$$S(r) = e^{-\frac{r}{2}}e^{-rx\frac{\partial}{\partial x}}$$

Proof. Because $r \in \mathbb{R}$ the squeezing operator becomes

$$S(r) = e^{\frac{1}{2}r\left((a^\dagger)^2 - a^2\right)}.$$

By expressing $S(r)$ in terms of x and p, we complete the proof of this lemma:

$$\begin{aligned}S(r) &= e^{\frac{r}{4\hbar}\left((x-ip)^2-(x+ip)^2\right)} \\ &= e^{-\frac{ir}{2\hbar}(xp+px)} \\ &= e^{-\frac{ir}{2\hbar}(xp+(xp-ih))} \\ &= e^{-\frac{r}{2}}e^{-rx\frac{\partial}{\partial x}}\end{aligned}$$

□

We are now able to calculate the time-independent wave function of coherent and minimum uncertainty squeezed states. The next theorem gives the time-independent wave function of a coherent state.

Theorem 4.2.3 *Let $\alpha = se^{i\theta}$ with $s > 0$ and $\theta \in [0, 2\pi)$. Let $|\alpha\rangle$ denote a coherent state. Let $\langle x\rangle$ and $\langle p\rangle$ be the expectations for the minimum uncertainty squeezed states as defined in Corollary 4.1.9 such that $e^{-r}\langle x\rangle$ and $e^r\langle p\rangle$ are the expectations for a coherent state as defined in Corollary 4.1.7. The time-independent wave function of the coherent state $|\alpha\rangle$ is*

$$|\alpha\rangle = (\pi\hbar)^{-\frac{1}{4}}\exp\left(-\frac{1}{2\hbar}\left(x - e^{-r}\langle x\rangle\right)^2 + \frac{i}{\hbar}e^r\langle p\rangle x\right)$$

PROOF. Applying the time-independent wave function of the vacuum presented in Lemma 3.1.2, the representation of $D(\alpha)$ in Lemma 4.2.1 and the operator formulae in Lemma A.0.5 we find

$$\begin{aligned} D(\alpha)|0\rangle &= (\pi\hbar)^{-\frac{1}{4}} e^{-\frac{i}{2\hbar}\langle x\rangle\langle p\rangle} e^{\frac{i}{\hbar}e^r\langle p\rangle x} e^{-e^{-r}\langle x\rangle\frac{\partial}{\partial x}} e^{-\frac{x^2}{2\hbar}} \\ &= (\pi\hbar)^{-\frac{1}{4}} e^{-\frac{i}{2\hbar}\langle x\rangle\langle p\rangle} e^{\frac{i}{\hbar}e^r\langle p\rangle x} e^{-\frac{1}{2\hbar}\left(x-e^{-r}\langle x\rangle\right)^2} \\ &= (\pi\hbar)^{-\frac{1}{4}} e^{-\frac{i}{2\hbar}\langle x\rangle\langle p\rangle} e^{-\frac{1}{2\hbar}\left(x-e^{-r}\langle x\rangle\right)^2+\frac{i}{\hbar}e^r\langle p\rangle x} \end{aligned}$$

This state is not normalized yet. We have

$$\begin{aligned} \int_{-\infty}^{\infty} |D(\alpha)|0\rangle|^2 dx &= (\pi\hbar)^{-\frac{1}{2}} e^{-\frac{i}{\hbar}\langle x\rangle\langle p\rangle} \int_{-\infty}^{\infty} e^{-\frac{1}{\hbar}\left(x-e^{-r}\langle x\rangle\right)^2} d(x-e^{-r}\langle x\rangle) \\ &= (\pi\hbar)^{-\frac{1}{2}} e^{-\frac{i}{\hbar}\langle x\rangle\langle p\rangle} (\pi\hbar)^{\frac{1}{2}} \\ &= e^{-\frac{i}{\hbar}\langle x\rangle\langle p\rangle} \end{aligned}$$

This gives us that a normalized coherent state has as time-independent wave function

$$|\alpha\rangle = \frac{D(\alpha)|0\rangle}{e^{-\frac{i}{2\hbar}\langle x\rangle\langle p\rangle}} = (\pi\hbar)^{-\frac{1}{4}} \exp\left(-\frac{1}{2\hbar}\left(x-e^{-r}\langle x\rangle\right)^2 + \frac{i}{\hbar}e^r\langle p\rangle x\right)$$

□

With the result from Theorem 4.2.3 we can find the time-independent wave function of a minimum uncertainty squeezed state. It is presented in the following theorem.

Theorem 4.2.4 *Let $r \in \mathbb{R}$ and $\alpha = se^{i\theta}$ with $s > 0$ and $\theta \in [0, 2\pi)$. Let $|r, \alpha\rangle$ be a minimum uncertainty squeezed state. Let $\langle x\rangle$ and $\langle p\rangle$ be the expectations of the minimum uncertainty squeezed state as defined in Corollary 4.1.9. The time-independent wave function of $|r, \alpha\rangle$ is given by*

$$|r, \alpha\rangle = \left(\pi\hbar e^{2r}\right)^{-\frac{1}{4}} \exp\left(-\frac{e^{-2r}}{2\hbar}\left(x-\langle x\rangle\right)^2 + \frac{i}{\hbar}\langle p\rangle x\right)$$

PROOF. Using the representation of $S(r)$ in Theorem 4.2.2, the time-independent wave function of the coherent state $|\alpha\rangle$ given in Theorem 4.2.3 and the operator formulae given in Lemma A.0.5 we find that

$$\begin{aligned} S(r)|\alpha\rangle &= (\pi\hbar)^{-\frac{1}{4}} e^{-\frac{r}{2}} e^{-rx\frac{\partial}{\partial x}} e^{-\frac{1}{2\hbar}\left(x-e^{-r}\langle x\rangle\right)^2+\frac{i}{\hbar}e^r\langle p\rangle x} \\ &= (\pi\hbar)^{-\frac{1}{4}} e^{-\frac{r}{2}} e^{-\frac{1}{2\hbar}\left(xe^{-r}-e^{-r}\langle x\rangle\right)^2+\frac{i}{\hbar}e^r\langle p\rangle xe^{-r}} \\ &= (\pi\hbar)^{-\frac{1}{4}} e^{-\frac{r}{2}} e^{-\frac{e^{-2r}}{2\hbar}(x-\langle x\rangle)^2+\frac{i}{\hbar}\langle p\rangle x} \end{aligned}$$

This state is already normalized:

$$\begin{aligned} \int_{-\infty}^{\infty} |S(r)|\alpha\rangle|^2 dx &= (\pi\hbar)^{-\frac{1}{2}} e^{-r} \int_{-\infty}^{\infty} e^{-\frac{e^{-2r}}{\hbar}(x-\langle x\rangle)^2} d(x-\langle x\rangle) \\ &= (\pi\hbar)^{-\frac{1}{2}} e^{-r} \sqrt{\frac{\pi\hbar}{e^{-2r}}} \\ &= 1 \end{aligned}$$

This completes the proof of this theorem. □

Knowing the time-independent wave function of the minimum uncertainty squeezed state we can determine the probability distributions that give us the probability to measure a certain position value or momentum value.

We define the x-basis to be the set of position eigenfunctions as explained in Section 2.5

$$x = \{|x_n\rangle : x_n \in \mathbb{R}\}$$

where $|x_n\rangle = \delta(x - x_n)$. We define the p-basis to be the set of momentum eigenfunctions as explained in Section 2.5

$$p = \{|p_n\rangle : p_n \in \mathbb{R}\}$$

where $|p_n\rangle = e^{ip_n x}$. The probability distributions are presented in the next theorem.

Theorem 4.2.5 *Let $r \in \mathbb{R}$ and $\alpha = se^{i\theta}$ with $s > 0$ and $\theta \in [0, 2\pi)$. Let $|r, \alpha\rangle$ be a minimum uncertainty squeezed state. Let $\langle x\rangle$ and $\langle p\rangle$ be the expectations of this state as presented in Corollary 4.1.9.*
The probability of measuring position value x when we measure in the x-basis for the squeezed state $|r, \alpha\rangle$ is denoted by $P_X^{|r,\alpha\rangle}(x)$. The probability of measuring position value p when we measure in the p-basis for the squeezed state $|r, \alpha\rangle$ is denoted by $P_P^{|r,\alpha\rangle}(p)$. These probability distributions are given by

$$P_X^{|r,\alpha\rangle}(x) = \frac{e^{-r}}{\sqrt{\pi\hbar}} e^{-\frac{e^{-2r}}{\hbar}(x-\langle x\rangle)^2}$$

This is a Gaussian distribution with mean $\mu = \langle x\rangle$ and variance $\sigma_x^2 = \frac{\hbar}{2}e^{2r}$.

$$P_P^{|r,\alpha\rangle}(p) = \frac{e^{r}}{\sqrt{\pi\hbar}} e^{-\frac{e^{2r}}{\hbar}(p-\langle p\rangle)^2}$$

This is a Gaussian distribution with mean $\mu = \langle p\rangle$ and variance $\sigma_p^2 = \frac{\hbar}{2}e^{-2r}$.

Proof. In Section 2.5 we found that the measurement of the position x is a projective measurement because the operator x is Hermitian. The probability to measure position value x_n for the squeezed state $|r, \alpha\rangle$ is therefore given by

$$P(x_n) = \langle r, \alpha|x_n\rangle\langle x_n|r, \alpha\rangle = |\langle x_n|r, \alpha\rangle|^2.$$

We calculate $\langle x_n|r, \alpha\rangle$.

$$\begin{aligned}\langle x_n|r, \alpha\rangle &= (\pi\hbar e^{2r})^{-\frac{1}{4}} \int_{-\infty}^{\infty} \delta(x - x_n) \exp\left(-\frac{e^{-2r}}{2\hbar}(x - \langle x\rangle)^2 + \frac{i}{\hbar}\langle p\rangle x\right) dx \\ &= (\pi\hbar e^{2r})^{-\frac{1}{4}} \exp\left(-\frac{e^{-2r}}{2\hbar}(x_n - \langle x\rangle)^2 + \frac{i}{\hbar}\langle p\rangle x_n\right)\end{aligned}$$

This implicates that

$$|\langle x_n|r, \alpha\rangle|^2 = \frac{e^{-r}}{\sqrt{\pi\hbar}} e^{-\frac{e^{-2r}}{\hbar}(x_n-\langle x\rangle)^2}$$

This is already a normalized probability distribution because

$$\int_{-\infty}^{\infty} |\langle x_n|r,\alpha\rangle|^2 dx_n \quad = \quad \frac{e^{-r}}{\sqrt{\pi\hbar}}\sqrt{\frac{\pi\hbar}{e^{-2r}}} = 1$$

This completes the proof of the first part of the theorem.

The measurement of the momentum p is a projective measurement because the operator p is Hermitian. The probability to measure momentum value p_n is therefore given by

$$P(p_n) = |\langle p_n|r,\alpha\rangle|^2.$$

First, we calculate $\langle p_n|r,\alpha\rangle$.

$$\begin{aligned}\langle p_n|r,\alpha\rangle &= (\pi\hbar e^{2r})^{-\frac{1}{4}} \int_{-\infty}^{\infty} e^{-ip_n x} \exp\left(-\frac{e^{-2r}}{2\hbar}(x-\langle x\rangle)^2 + \frac{i}{\hbar}\langle p_n\rangle x\right)dx \\ &= (\pi\hbar e^{2r})^{-\frac{1}{4}} \int_{-\infty}^{\infty} \exp\left(-\frac{e^{-2r}}{2\hbar}(x-\langle x\rangle)^2 - \frac{i}{\hbar}(p_n-\langle p\rangle)x\right)dx \qquad (4.1)\end{aligned}$$

To solve the integral from Eq. 4.1 we use a method called "completing the square". We use the fact that

$$\begin{aligned}-\frac{e^{-2r}}{2\hbar}(x-\langle x\rangle)^2 - \frac{i}{\hbar}(p_n-\langle p\rangle)x = \\ -\frac{e^{-2r}}{2\hbar}((x+(ie^{2r}(p_n-\langle p\rangle)-\langle x\rangle))^2 + 2ie^{2r}\langle x\rangle(p_n-\langle p\rangle) + e^{4r}(p_n-\langle p\rangle)^2).\end{aligned}$$

Eq. 4.1 now becomes

$$\langle p_n|r,\alpha\rangle \quad = \quad (\pi\hbar e^{2r})^{-\frac{1}{4}} K \exp\left(-\frac{i}{\hbar}\langle x\rangle(p_n-\langle p\rangle) - \frac{e^{2r}}{2\hbar}(p_n-\langle p\rangle)^2\right)$$

with

$$K \quad = \quad \int_{-\infty}^{\infty} \exp\left(-\frac{e^{-2r}}{2\hbar}(x+(ie^{2r}(p_n-\langle p\rangle)-\langle x\rangle))^2\right)dp_n.$$

This gives that

$$|\langle p_n|r,\alpha\rangle|^2 = (\pi\hbar e^{2r})^{-\frac{1}{2}}|K|^2 \exp\left(-\frac{e^{2r}}{\hbar}(p_n-\langle p\rangle)^2\right).$$

This probability distribution is not normalized because

$$\begin{aligned}(\pi\hbar e^{2r})^{-\frac{1}{2}}|K|^2 \int_{\infty}^{\infty} e^{-\frac{e^{2r}}{\hbar}(p_n-\langle p\rangle)^2} d(p_n-\langle p\rangle) &= (\pi\hbar e^{2r})^{-\frac{1}{2}}|K|^2\sqrt{\frac{\pi\hbar}{e^{2r}}} \\ &= e^{-2r}|K|^2.\end{aligned}$$

We may conclude that the probability distribution for measuring the momentum value p for the state $|r,\alpha\rangle$ is given by

$$P_P^{|r,\alpha\rangle}(p) = \frac{|\langle p|r,\alpha\rangle|^2}{e^{-2r}|K|^2} = \frac{e^r}{\sqrt{\pi\hbar}} e^{-\frac{e^{2r}}{\hbar}(p-\langle p\rangle)^2}.$$

□

4.3 Squeezed states cannot be cloned

In the early 1980's the no-cloning theorem was presented [13]. It says that in general, quantum states cannot be copied. In the exceptional case that the input states are all orthogonal to each other, a quantum copying machine can be made that copies the input states.

In this section we prove that minimum uncertainty squeezed states cannot be copied. The proof of this fact is presented in Theorem 4.3.3 and it will follow the same line of reasoning as the proof of the original no-cloning theorem.

Before we present the theorem, we first give a few lemma's that will help us to prove that minimum uncertainty squeezed states cannot be copied.

The first lemma gives the inner product of two minimum uncertainty squeezed states.

Lemma 4.3.1 *Let $|r,\alpha\rangle$ and $|r',\alpha'\rangle$ be squeezed states with $r, r' \in \mathbb{R}$, $\alpha = se^{i\theta}$ and $\alpha' = s'e^{i\theta'}$ with $s, s' > 0$ and $\theta, \theta' \in [0, 2\pi)$. Let $\langle x\rangle$ and $\langle p\rangle$ be the expectations of $|r,\alpha\rangle$ and $\langle x\rangle'$ and $\langle p\rangle'$ be the expectations of $|r',\alpha'\rangle$. Then*

$$\langle r,\alpha|r',\alpha'\rangle = \sqrt{\frac{1}{\cosh(r-r')}}\exp\left(\frac{-1}{2\hbar}\left(\frac{(\langle x\rangle-\langle x\rangle')^2}{e^{2r}+e^{2r'}}+\frac{(\langle p\rangle-\langle p\rangle')^2}{e^{-2r}+e^{-2r'}}\right)\right)\cdot$$
$$\exp\left(\frac{-i}{\hbar\left(e^{-2r}+e^{-2r'}\right)}\left(e^{-2r}\langle x\rangle+e^{-2r'}\langle x\rangle'\right)\left(\langle p\rangle-\langle p\rangle'\right)\right).$$

Proof. We will not explain the proof step by step but mainly give the outline of the proof. With the time-independent wave function a minimum uncertainty squeezed state presented in Theorem 4.2.4 we find

$$\langle r,\alpha|r',\alpha'\rangle = \left(\pi\hbar e^{r+r'}\right)^{-\frac{1}{2}}\cdot$$
$$\int_{-\infty}^{\infty}\exp\left(-\frac{e^{-2r}}{2\hbar}(x-\langle x\rangle)^2-\frac{e^{-2r'}}{2\hbar}\left(x-\langle x\rangle'\right)^2-\frac{i}{\hbar}(\langle p\rangle-\langle p\rangle')x\right)dx. \quad (4.2)$$

The integral in Eq. 4.2 is solved by a method called "completing the square". If we make the substitutions

$$\begin{array}{lllllll} a & = & \frac{-e^{-2r}}{2\hbar} & & d & = & \langle x\rangle' \\ b & = & \langle x\rangle & & f & = & -\frac{i}{2\hbar}(\langle p\rangle-\langle p\rangle') \\ c & = & \frac{-e^{-2r'}}{2\hbar} & & & & \end{array}$$

then the exponent in Eq. 4.2 becomes

$$a(x-b)^2+c(x-d)^2+2fx = (a+c)\left(x-\left(\frac{ab+cd-f}{a+c}\right)\right)^2-\frac{(ab+cd-f)^2}{a+c}+ab^2+cd^2$$

The integral in Eq. 4.2 now becomes

$$\exp\left(-\frac{(ab+cd-f)^2}{a+c}+ab^2+cd^2\right)\int_{-\infty}^{\infty}\exp\left((a+c)\left(x-\left(\frac{ab+cd-f}{a+c}\right)\right)^2\right)dx =$$
$$\exp\left(-\frac{(ab+cd-f)^2}{a+c}+ab^2+cd^2\right)\sqrt{\frac{\pi}{-(a+c)}} \quad (4.3)$$

where

$$\begin{aligned} -\frac{(ab+cd-f)^2}{a+c}+ab^2+cd^2 &= \frac{-(ab+cd-f)^2+(a+c)(ab^2+cd^2)}{a+c} \\ &= \frac{ac(b-d)^2-f^2+2(ab+cd)f}{a+c} \\ &= \exp\left(\frac{-1}{2\hbar}\left(\frac{(\langle x\rangle-\langle x\rangle')^2}{e^{2r}+e^{2r'}}+\frac{(\langle p\rangle-\langle p\rangle')^2}{e^{-2r}+e^{-2r'}}\right)\right)\cdot \\ &\quad \exp\left(\frac{-i}{\hbar\left(e^{-2r}+e^{-2r'}\right)}\left(e^{-2r}\langle x\rangle+e^{-2r'}\langle x\rangle'\right)\left(\langle p\rangle-\langle p\rangle'\right)\right) \end{aligned}$$

and

$$\sqrt{\frac{\pi}{-(a+c)}} = \sqrt{\frac{2\pi\hbar}{e^{-2r}+e^{-2r'}}}.$$

We substitute Eq. 4.3 into Eq. 4.2. We find

$$\langle r,\alpha|r',\alpha'\rangle = \left(\pi\hbar e^{r+r'}\right)^{-\frac{1}{2}}\sqrt{\frac{2\pi\hbar}{e^{-2r}+e^{-2r'}}}\exp\left(\frac{-1}{2\hbar}\left(\frac{(\langle x\rangle-\langle x\rangle')^2}{e^{2r}+e^{2r'}}+\frac{(\langle p\rangle-\langle p\rangle')^2}{e^{-2r}+e^{-2r'}}\right)\right)\cdot$$
$$\exp\left(\frac{-i}{\hbar\left(e^{-2r}+e^{-2r'}\right)}\left(e^{-2r}\langle x\rangle+e^{-2r'}\langle x\rangle'\right)\left(\langle p\rangle-\langle p\rangle'\right)\right).$$

It holds that

$$\left(\pi\hbar e^{r+r'}\right)^{-\frac{1}{2}}\sqrt{\frac{2\pi\hbar}{e^{-2r}+e^{-2r'}}} = \sqrt{\frac{1}{\cosh\left(r-r'\right)}}.$$

This completes the proof of this lemma. □

The following lemma tells us that if we have two squeezed states with the same squeezing parameter r and they have the same expectation for x and p, then the squeezed states are the same.

Lemma 4.3.2 *Let $|r,\alpha\rangle$ and $|r',\alpha'\rangle$ be minimum uncertainty squeezed states with $r,r'\in\mathbb{R}$, $\alpha=se^{i\theta},\alpha'=s'e^{i\theta'}$ with $s,s'>0$ and $\theta,\theta'\in[0,2\pi)$. Let $\langle x\rangle$ and $\langle p\rangle$ be the expectations of $|r,\alpha\rangle$ and $\langle x\rangle'$ and $\langle p\rangle'$ be the expectations of $|r',\alpha'\rangle$.*

If $r=r'$ and $\langle x\rangle=\langle x\rangle'$ and $\langle p\rangle=\langle p\rangle'$ then $s=s'$ and $\theta=\theta'$ so that $|r,\alpha\rangle=|r',\alpha'\rangle$.

Proof. From Corollary 4.1.9 we find that if $r=r'$ then the relations $\langle x\rangle=\langle x\rangle'$ and $\langle p\rangle=\langle p\rangle'$ become

$$\begin{aligned} \sqrt{2\hbar}s\cos\theta e^{r} &= \sqrt{2\hbar}s'\cos\theta' e^{r} \\ s\cos\theta &= s'\cos\theta' \\ \tfrac{s'}{s} &= \tfrac{\cos\theta}{\cos\theta'} \end{aligned} \quad \text{and} \quad \begin{aligned} \sqrt{2\hbar}s\sin\theta e^{-r} &= \sqrt{2\hbar}s'\sin\theta' e^{-r} \\ s\sin\theta &= s'\sin\theta' \\ \tfrac{s'}{s} &= \tfrac{\sin\theta}{\sin\theta'}. \end{aligned}$$

From this we can conclude that

$$\begin{aligned}
\sin\theta\cos\theta' &= \cos\theta\sin\theta' \\
\left(e^{i\theta}-e^{-i\theta}\right)\left(e^{i\theta'}+e^{-i\theta'}\right) &= \left(e^{i\theta}+e^{-i\theta}\right)\left(e^{i\theta'}-e^{-i\theta'}\right) \\
e^{i(\theta+\theta')}+e^{i(\theta-\theta')}-e^{i(\theta'-\theta)}-e^{-i(\theta+\theta')} &= e^{i(\theta+\theta')}-e^{i(\theta-\theta')}+e^{i(\theta'-\theta)}-e^{-i(\theta+\theta')} \\
e^{i(\theta-\theta')} &= e^{i(\theta'-\theta)} \\
\theta &= \theta'
\end{aligned}$$

But then it also holds that

$$\frac{s'}{s}=\frac{\cos\theta}{\cos\theta'}=\frac{\cos\theta}{\cos\theta}=1$$

so $s=s'$. This concludes the proof of the lemma. □

We prove that it is impossible to copy squeezed states.

Theorem 4.3.3 *Let $r\in\mathbb{R}$ and $\alpha\in\mathbb{C}$. Copying machines to copy minimum uncertainty squeezed states $|r,\alpha\rangle$ can only be made to copy one single squeezed state. This means that it can only copy the squeezed state $|r,\alpha\rangle$ for a certain choice of the parameters r and α.*

Proof. Suppose we do have a copying machine that can perfectly copy minimum uncertainty squeezed states. This machine will work on the tensor product of two states, the squeezed state itself ($|r,\alpha\rangle$) and a so called ancilla ($|t\rangle$, with $\langle t|t\rangle=1$) which will change into the squeezed state during the copying. Postulate 2 from Section 2.5 tells us that the evolution of a closed quantum system is always described by a unitary transformation. From this it follows that the "copying machine" U_c is a unitary operator so $U_cU_c^\dagger=I$.

Suppose $|r,\alpha\rangle$ and $|r',\alpha'\rangle$ are two minimum uncertainty squeezed states with $\alpha=se^{i\theta},\alpha'=s'e^{i\theta'}$ where $r\in\mathbb{R}$ and $s,s'>0$ and $\theta,\theta'\in[0,2\pi)$. Let $|t\rangle$ be a normalized quantum state. Suppose U_c can copy both squeezed states. We then have the following equations for U_c,

$$U_c(|r,\alpha\rangle\otimes|t\rangle) = |r,\alpha\rangle\otimes|r,\alpha\rangle \tag{4.4}$$
$$U_c(|r',\alpha'\rangle\otimes|t\rangle) = |r',\alpha'\rangle\otimes|r',\alpha'\rangle. \tag{4.5}$$

Taking the inner product of the left sides of Eq. 4.4 and 4.5 we get

$$\begin{aligned}
(U_c(|r,\alpha\rangle\otimes|t\rangle),U_c(|r',\alpha'\rangle\otimes|t\rangle)) &= (U_c(|r,\alpha\rangle\otimes|t\rangle))^\dagger(U_c(|r',\alpha'\rangle\otimes|t\rangle)) \\
&= (\langle r,\alpha|\otimes\langle t|)U_c^\dagger U_c(|r',\alpha'\rangle\otimes|t\rangle) \\
&= (\langle r,\alpha|\otimes\langle t|)(|r',\alpha'\rangle\otimes|t\rangle) \\
&= \langle r,\alpha|r',\alpha'\rangle\langle t|t\rangle \\
&= \langle r,\alpha|r',\alpha'\rangle
\end{aligned}$$

Taking the inner product of the right sides of Eq. 4.4 and 4.5 we get

$$\begin{aligned}
(|r,\alpha\rangle\otimes|r,\alpha\rangle,|r',\alpha'\rangle\otimes|r',\alpha'\rangle) &= \langle r,\alpha|r',\alpha'\rangle\langle r,\alpha|r',\alpha'\rangle \\
&= \langle r,\alpha|r',\alpha'\rangle^2
\end{aligned}$$

These two inner products should be the same, so

$$\langle r,\alpha|r',\alpha'\rangle=\langle r,\alpha|r',\alpha'\rangle^2$$

This equation has as only solutions

$$\langle r, \alpha | r', \alpha' \rangle = 1 \text{ or } \langle r, \alpha | r', \alpha' \rangle = 0.$$

But then also

$$|\langle r, \alpha | r', \alpha' \rangle|^2 = 1 \text{ or } |\langle r, \alpha | r', \alpha' \rangle|^2 = 0. \tag{4.6}$$

At this point they can conclude that a copying machine can be made that can only copy states that are orthonormal. Our question however is for which minimum uncertainty squeezed states it holds that $|\langle r, \alpha | r', \alpha' \rangle|^2 = 1$ or $|\langle r, \alpha | r', \alpha' \rangle|^2 = 0$.

The value of $|\langle r, \alpha | r', \alpha' \rangle|^2$ follows from Lemma 4.3.1 and is given by

$$\begin{aligned} |\langle r, \alpha | r', \alpha' \rangle|^2 &= \langle r, \alpha | r', \alpha' \rangle^* \langle r, \alpha | r', \alpha' \rangle \\ &= \frac{1}{\cosh(r - r')} \exp\left(\frac{-1}{\hbar} \left(\frac{(\langle x \rangle - \langle x \rangle')^2}{e^{2r} + e^{2r'}} + \frac{(\langle p \rangle - \langle p \rangle')^2}{e^{-2r} + e^{-2r'}} \right) \right). \end{aligned}$$

Because $e^x > 0$ and $\cosh x \geq 1$ for every $x \in \mathbb{R}$ we see that $|\langle r, \alpha | r', \alpha' \rangle|^2 > 0$. We are left with the equation $|\langle r, \alpha | r', \alpha' \rangle|^2 = 1$;

$$\begin{aligned} 1 &= |\langle r, \alpha | r', \alpha' \rangle|^2 \\ \cosh(r - r') &= \exp\left(\frac{-1}{\hbar} \left(\frac{(\langle x \rangle - \langle x \rangle')^2}{e^{2r} + e^{2r'}} + \frac{(\langle p \rangle - \langle p \rangle')^2}{e^{-2r} + e^{-2r'}} \right) \right). \end{aligned} \tag{4.7}$$

We see that the left hand side of Eq. 4.7 is greater than or equal to 1 whereas the right hand side of Eq. 4.7 is smaller than or equal to 1 because the exponent is negative. Thus, the only solution to Eq. 4.7 is that both sides are equal to one so

$$\begin{aligned} \cosh(r - r') &= 1 \\ r &= r' \end{aligned} \tag{4.8}$$

and

$$\begin{aligned} \exp\left(\frac{-1}{\hbar} \left(\frac{(\langle x \rangle - \langle x \rangle')^2}{e^{2r} + e^{2r'}} + \frac{(\langle p \rangle - \langle p \rangle')^2}{e^{-2r} + e^{-2r'}} \right) \right) &= 1 \\ \frac{(\langle x \rangle - \langle x \rangle')^2}{e^{2r} + e^{2r'}} + \frac{(\langle p \rangle - \langle p \rangle')^2}{e^{-2r} + e^{-2r'}} &= 0 \\ \langle x \rangle = \langle x \rangle' \quad \text{and} \quad \langle x \rangle &= \langle x \rangle' \end{aligned} \tag{4.9}$$

Given Eq. 4.8 and 4.9, Lemma 4.3.2 tells us that it follows that $|r, \alpha\rangle = |r', \alpha'\rangle$.

We may conclude that the only solution to Eq. 4.7 is $|r, \alpha\rangle = |r', \alpha'\rangle$ and a copying machine U_c can only be made to copy minimum uncertainty squeezed states for one choice of the parameters r, α.

We note that the proof of the original no-cloning theorem [13] is the same until Eq. 4.6 but then with the difference that the state $|r, \alpha\rangle$ is changed into a general quantum state $|\psi\rangle$. The original no-cloning theorem states from this equation that a copying machine can only be made to copy orhonormal quantum states. □

4.4 The time evolution of minimum uncertainty squeezed states

In general, the time evolution of a minimum uncertainty squeezed state that is in the state $|r,\alpha\rangle$ at $t=0$ where $r \in \mathbb{R}$ and $\alpha \in \mathbb{C}$ is given by (see Section 2.1)

$$|r,\alpha\rangle_t = f(t)|r,\alpha\rangle = e^{-iEt/\hbar}|r,\alpha\rangle$$

where E is the total energy of a minimum uncertainty squeezed state. To find this energy we need an expression for the Hamiltonian operator H because $H|r,\alpha\rangle = E|r,\alpha\rangle$ (see Section 2.6). We study the time evolution of a minimum uncertainty squeezed state under the harmonic oscillator. A squeezed state under the harmonic oscillator evolves according to the Hamiltonian operator of the harmonic oscillator. This operator is given Corollary 3.1.4. We recall that

$$H = \hbar\left(a^\dagger a + \frac{1}{2}\right).$$

The time evolution of a minimum uncertainty squeezed state under the harmonic oscillator is now given by

$$|r,\alpha\rangle_t = e^{-iHt/\hbar}|r,\alpha\rangle = e^{-it\left(a^\dagger a+\frac{1}{2}\right)}|r,\alpha\rangle.$$

Before we can give the expectations and the variances of the observables x and p at time t we present the following lemma.

Lemma 4.4.1 *It holds that*

$$e^{ita^\dagger a}ae^{-ita^\dagger a} = ae^{-it}$$
$$e^{ita^\dagger a}a^\dagger e^{-ita^\dagger a} = a^\dagger e^{it}.$$

Proof. It holds that

$$\begin{aligned}[ita^\dagger a, a] &= it[a^\dagger a, a] \\ &= it[a^\dagger, a]a \\ &= -ita.\end{aligned}$$

With this and using the formula given in Lemma A.0.2 we find

$$\begin{aligned}e^{ita^\dagger a}ae^{-ita^\dagger a} &= \sum_{n=0}^{\infty}\frac{1}{n!}[ita^\dagger a_{(1)}, [ita^\dagger a_{(2)}, \ldots, [ita^\dagger a_{(n)}, a]]\ldots] \\ &= \sum_{n=0}^{\infty}\frac{1}{n!}(-it)^n a \\ &= a\sum_{n=0}^{\infty}\frac{(-it)^n}{n!} \\ &= ae^{-it}. \qquad (4.10)\end{aligned}$$

Taking the Hermitian conjugate of both sides of Eq. 4.10 we gives us

$$(e^{ita^\dagger a}ae^{-ita^\dagger a})^* = e^{ita^\dagger a}a^\dagger e^{-ita^\dagger a} = a^\dagger e^{it}$$

which completes the proof of this lemma. □

We are now able to give the expectations and the variances of x and p at time t for a minimum uncertainty squeezed state under the harmonic oscillator.

Theorem 4.4.2 *Let $r \in \mathbb{R}$ and $\alpha = se^{i\theta}$ with $s > 0$ and $\theta \in [0, 2\pi)$. Let $|r, \alpha\rangle$ denote a minimum uncertainty squeezed state at time $t = 0$ under the harmonic oscillator. The expectation values and variances of the observables x and p with respect to the state $|r, \alpha\rangle$ at time $t \geq 0$ are given by*

$$\begin{aligned}
\langle x\rangle_t &= \sqrt{2\hbar}s(\cos(\theta - t)\cosh r + \cos(\theta + t)\sinh r) \\
\langle p\rangle_t &= \sqrt{2\hbar}s(\sin(\theta - t)\cosh r - \sin(\theta + t)\sinh r) \\
\sigma^2_{x,t} &= \frac{\hbar}{2}(\cosh(2r) + \cos(2t)\sinh 2r) \\
\sigma^2_{p,t} &= \frac{\hbar}{2}(\cosh(2r) - \cos(2t)\sinh 2r)
\end{aligned}$$

Proof. It holds that

$$\begin{aligned}
\langle x\rangle_t &= {}_t\langle r, \alpha|x|r, \alpha\rangle_t \\
&= \sqrt{\frac{\hbar}{2}}\langle r, \alpha|e^{it\left(a^\dagger a + \frac{1}{2}\right)}(a^\dagger + a)e^{-it\left(a^\dagger a + \frac{1}{2}\right)}|r, \alpha\rangle \\
&= \sqrt{\frac{\hbar}{2}}\langle r, \alpha|e^{ita^\dagger a}(a^\dagger + a)e^{-ita^\dagger a}|r, \alpha\rangle \\
&= \sqrt{\frac{\hbar}{2}}\langle r, \alpha|\left(e^{ita^\dagger a}a^\dagger e^{-ita^\dagger a} + e^{ita^\dagger a}ae^{-ita^\dagger a}\right)|r, \alpha\rangle \\
&= \sqrt{\frac{\hbar}{2}}\langle r, \alpha|\left(a^\dagger e^{it} + ae^{-it}\right)|r, \alpha\rangle \\
&= \langle x_\beta\rangle|_{\beta=t}.
\end{aligned}$$

In the same way we find

$$\langle p\rangle_t = \langle p_\beta\rangle|_{\beta=t}$$

where x_β and p_β are as defined in Definition 4.1.1. This means that the expectations and variances we are looking for are equal to the results presented in Theorem 4.1.5 with the substitutions $\beta = t$ and $\phi = 0$ for minimum uncertainty. This completes the proof of the theorem. □

The following corollary states that at given time instances the statistical properties of squeezed states are equal to the properties at $t = 0$. The theorem also gives a convenient property for the variances at time t.

Corollary 4.4.3 *Let $r \in \mathbb{R}$ and $\alpha = se^{i\theta}$ with $s > 0$ and $\theta \in [0, 2\pi)$. Let $|r, \alpha\rangle$ denote a minimum uncertainty squeezed state under the harmonic oscillator. Let $k \in \mathbb{N}$. For $t = 2k\pi$ it holds that*

$$\begin{aligned}
\langle x\rangle_t &= \langle x\rangle_0 \\
\langle p\rangle_t &= \langle p\rangle_0
\end{aligned} \quad \textit{and} \quad \begin{aligned}
\sigma^2_{x,t} &= \sigma^2_{x,0} \\
\sigma^2_{p,t} &= \sigma^2_{p,0}
\end{aligned}$$

Furthermore, for $t \geq 0$ and $r < 0$ it holds that

$$\sigma^2_{p,0} \geq \sigma^2_{x,t} \geq \sigma^2_{x,0} \leq \sigma^2_{p,t} \leq \sigma^2_{p,0}.$$

For $t \geq 0$ and $r > 0$ it holds that

$$\sigma^2_{x,0} \geq \sigma^2_{p,t} \geq \sigma^2_{p,0} \leq \sigma^2_{x,t} \leq \sigma^2_{x,0}.$$

PROOF. The first part of the theorem follows easily from Theorem 4.4.2 by substituting $t = 2k\pi$.

Now suppose $t \geq 0$. We use that $\cosh(2r) > 1$ for $r \in \mathbb{R}$.
If $r < 0$ then $\sinh(2r) < 0$ and we find the inequalities

$$\cosh(2r) - \sinh(2r) \geq \cosh(2r) + \cos(2t)\sinh 2r \geq \cosh(2r) + \sinh(2r)$$

and

$$\cosh(2r) + \sinh(2r) \leq \cosh(2r) - \cos(2t)\sinh 2r \leq \cosh(2r) - \sinh(2r).$$

These inequalities give us that

$$\sigma_{p,0}^2 \geq \sigma_{x,t}^2 \geq \sigma_{x,0}^2$$

and

$$\sigma_{x,0}^2 \leq \sigma_{p,t}^2 \leq \sigma_{p,0}^2.$$

If $r > 0$ then $\sinh(2r) > 0$ and we find the inequalities

$$\cosh(2r) - \sinh(2r) \leq \cosh(2r) + \cos(2t)\sinh 2r \leq \cosh(2r) + \sinh(2r)$$

and

$$\cosh(2r) - \sinh(2r) \geq \cosh(2r) - \cos(2t)\sinh 2r \geq \cosh(2r) - \sinh(2r).$$

From this we see that

$$\sigma_{p,0}^2 \leq \sigma_{x,t}^2 \leq \sigma_{x,0}^2$$

and

$$\sigma_{x,0}^2 \geq \sigma_{p,t}^2 \geq \sigma_{p,0}^2.$$

□

4.5 Squeezing in x or p

The advantage of squeezed and coherent states, as stated in the introductory part, is that these states can satisfy the Heisenberg uncertainty relation with equality for certain observable pairs x' and p'. Moreover, for a squeezed state the uncertainty in one variable can be made arbitrarily small while the uncertainty of the other becomes arbitrarily large in order to keep the product constant at $\hbar/2$. In the previous sections we showed how to choose the parameters of the squeezed and coherent states such that these properties hold.

The coherent state $|\alpha\rangle$ with $\alpha \in \mathbb{C}$ has minimum uncertainty for all observable pairs x_β and p_β. If $|re^{i\phi}, \alpha\rangle$ with $r \in \mathbb{R}, \theta \in [0, 2\pi\rangle$ represents a squeezed state then it has minimum uncertainty with respect to the observable pairs x_β and p_β if and only if $\phi = 2\beta$.

The uncertainty of $x_\beta = x_{\frac{\phi}{2}}$ and $p_\beta = p_{\frac{\phi}{2}}$ is given by (see Corollary 4.1.8).

$$\begin{aligned} \sigma_{x_{\frac{\phi}{2}}}^2 &= \frac{\hbar}{2}e^{2r} \\ \sigma_{p_\beta}^2 &= \frac{\hbar}{2}e^{-2r} \end{aligned}$$

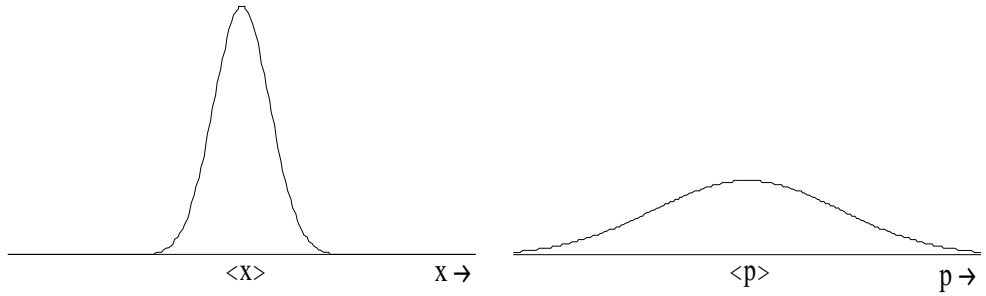


Figure 4.1: Probability distribution of measurement in x or p of a squeezed state squeezed in x.

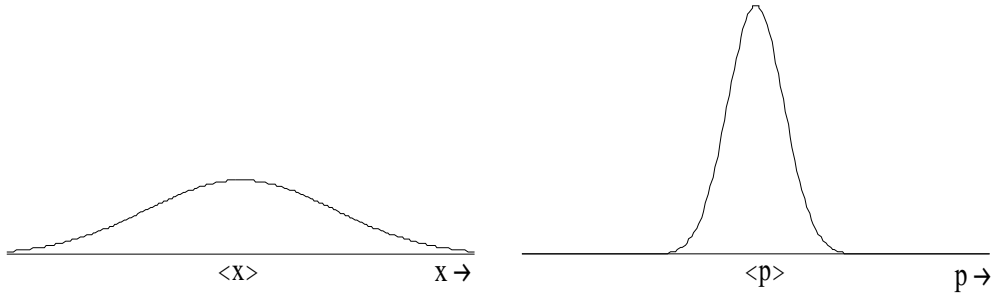


Figure 4.2: Probability distribution of measurement in x or p of a squeezed state squeezed in p.

If we choose $r < 0$ then $\sigma^2_{x_{\phi/2}} < \sigma^2_{p_{\phi/2}}$, and we say that the squeezed state is squeezed in $x_{\phi/2}$. The value of α is chosen such that the squeezed state has the desired expectation $\langle x_{\phi/2} \rangle$. When $r \to -\infty$ then the uncertainty in $x_{\phi/2}$ becomes arbitrarily small whereas the uncertainty in $p_{\phi/2}$ becomes arbitrarily large to keep the product constant. When $\beta = 0$, then the infinitely squeezed state has well defined position value and is therefore equal to the position eigenstate $\delta(x - \langle x \rangle)$.
The probability distributions for measuring the position value x and the momentum value p ($\phi = 0$) when $r < 0$ are normal distributions plotted in Figure 4.1. If we choose $r > 0$ then $\sigma^2_{x_{\phi/2}} > \sigma^2_{p_\beta}$ and we say that the squeezed state is squeezed in $p_{\phi/2}$. The value of α is chosen such that the squeezed state has the desired expectation $\langle p_{\phi/2} \rangle$. When $r \to \infty$ then the uncertainty in $p_{\phi/2}$ becomes arbitrarily small whereas the uncertainty in $x_{\phi/2}$ becomes arbitrarily large to keep the product constant. When $\beta = 0$, then the infinitely squeezed state has well defined momentum value and is therefore equal to the momentum eigenstate $e^{i\langle p \rangle x}$.

The probability distributions for measuring position value x and momentum value p ($\phi = 0$) when $r > 0$ are normal distributions plotted in Figure 4.2.

Chapter 5

Quantum Key Exchange

5.1 Introduction

First, we describe the settings of Quantum Key Exchange. There are two parties, Alice and Bob who want to agree on a secret key to use for encryption. To reach this they make use of a quantum communication channel to send the quantum states and an authenticated public channel on which they can exchange classical messages. Information on this public channel can be monitored but not altered. We assume that the quantum communication channel is a lossless channel, that is all states sent by Alice ultimately reach Bob.
There is a third, malicious party represented by an eavesdropper Eve. Eve tries to get as much information as possible about the secret key that Alice and Bob are agreeing on. We have to assume that Eve has unlimited quantum computational power.

Quantum key exchange (QKE) protocols can be provably secure because the security relies on fundamental laws of quantum mechanics instead of intractability assumptions. These fundamental laws are the no-cloning theorem and second, for every attempt to distinguish between two non-orthogonal quantum states, information gain is only possible at the expense of introducing disturbance in the system.

A QKE protocol makes use of this fact by transmitting non-orthogonal quantum states between Alice and Bob. Beforehand, Alice and Bob agree on a certain strategy to extract bit values from quantum states. After the transmission of the quantum states and the bit extraction Alice and Bob both have a key bit string. They check for disturbance in their bits by comparing a part of their bit strings (the so called check bits). If the disturbance (error rate) is lower than a certain threshold, then the security is guaranteed. When the error rate is indeed lower than the threshold, then Alice and Bob use the remaining bits as their key bits. To obtain a shared secret key, (classical) information reconciliation and privacy amplification are performed by Alice and Bob to distill a shared secret key bit string K. Information reconciliation and privacy amplification are described below. The threshold for the bit error rate is thus determined by the properties of the particular protocol and the efficiency of the information reconciliation and privacy amplification protocols.

In this way a private classical key can be created between two parties. The key can then be used to implement a (classical) private key cryptosystem to enable the parties to commu-

nicate securely.

Information reconciliation and Privacy amplification

After Alice sent quantum states to Bob and they both extracted a bit string, these two bit strings are highly correlated but are not identical. Suppose X is the bit string of Alice and Y is the bit string of Bob just before the information reconciliation. Both bit strings contain n bits. Information reconciliation reconciles errors between X and Y to obtain a shared bit string K' while giving away as less information as possible to Eve. The uncertainty Bob has about the bit string X is equal to $H(X|Y)$ (the conditional entropy of X given Y). This means that information reconciliation implies that Alice communicates in public to Bob approximately $H(X|Y)$ of her n bits. Then, with the information reconciliation, Alice and Bob find the same bit string K' with high probability. We will not elaborate on this subject, for more information see [15, 16].

After this step, Eve's information about Alice's string X consists of $H(X|Y)$ bits plus the information she gained in the previous steps of the protocol. This is information about the non-orthogonal quantum states Alice sent to Bob. We assume that Eve gained no more than t qubits of information about these quantum states. We say that Eve's information about X is no more than $H(X|Y)+t$ qubits because the information gained from classical information is never more than the information gained from quantum information.

It is proved by König, Maurer and Renner in [25] that no matter which observable on her quantum states Eve measures after the classical privacy amplification, she is no better off than she would be if she had $H(X|Y) + t$ classical bits of information about X before the privacy amplification. This means that (classical) privacy amplification can be applied to eliminate Eve's partial (quantum) information about the bit string Alice and Bob possess. The protocol creates a shorter string K of which Eve has negligible knowledge. Because the key bit string K is secret, it can subsequently be used for secure encryption. More about privacy amplification can be found in [17, 18].

In [24], a method for finding a threshold for t is given such that a quantum key exchange protocol is secure.

"Prepare and measure" and "entanglement based" protocols

In 1984 Bennett and Brassard proposed a quantum key exchange protocol known as BB84 [10]. It was the first quantum key exchange scheme by which a secret common key between Alice and Bob could be established. In BB84 Alice repeatedly sends to Bob non-orthogonal qubits and Bob measures them in one of two non-orthogonal bases.

Independently of the previous work, Ekert developed a different approach to quantum cryptography based on quantum entanglement. In his protocol E91 [14], entangled pairs of qubits are distributed to Alice and Bob who measure their qubits in non-orthogonal bases.

In general, quantum key exchange protocols can be divided into "prepare and measure" protocols such as BB84 and "entanglement based" protocols such as E91. In a "prepare

and measure" protocol, Alice encodes bits by preparing non-orthogonal quantum states. She sends the prepared states to Bob who extracts bit values by measuring every received state in one of the non-orthogonal bases. In an "entanglement based" protocol, Alice and Bob each receive a part of an entangled state from a dealer, which could be Alice herself. Alice and Bob extract bits by measuring every received state in one of the non-orthogonal bases agreed on beforehand.
Many interesting techniques for manipulating quantum entanglement have been discovered in the last few years and that is why it is sometimes convenient to interpret "prepare and measure" protocols in terms of "entanglement bases" protocols. We will do this with BB84 and GP00 in Section 7.

In Section 5.2 we will describe and analyze the firstly introduced key exchange protocol BB84. In Section 5.3 we will describe and analyze a "prepare and measure" key exchange protocol GP00 that works with squeezed states and resembles BB84. We will compare the two protocols.

In Chapter 7, we will deal with proofs of security of these two protocols.

5.2 BB84

Recall that a quantum key exchange protocol can be provably secure when Alice transmits non-orthogonal quantum states to Bob. In BB84 Alice transmits non-orthogonal qubits to Bob. The qubits are randomly chosen by Alice from two non-orthogonal qubit bases (see Section 2.9); the rectilinear basis RL = $\{|0\rangle, |1\rangle\}$ and the diagonal basis DG = $\{|+\rangle, |-\rangle\} = \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. This means that every time Alice wants to send a qubit to Bob, she randomly chooses (prepares) one of four qubits states: $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$. She then sends the states to Bob over a quantum communication channel.

Alice prepares a qubit by polarizing a photon in some direction. Qubits $|0\rangle$ and $|1\rangle$ correspond to a photon with respectively a horizontal and a diagonal polarization. Qubits $|+\rangle$ and $|-\rangle$ correspond to a photon with a diagonal polarization (respectively a plus 45 degree orientation and a minus 45 degree orientation).

Alice extracts bit values from the qubit states she sends to Bob. Bob extracts bit values from the measurement he makes on quantum states he receives. They extract bits according to some bit extraction strategy they agreed on beforehand. In Section 5.2.1 we will explain and study the bit extraction strategy used by Alice and Bob. We calculate the probability that Alice and Bob find the same bit value for different scenarios.

In Section 5.2.2 we describe the protocol BB84 and in Section 5.2.3 we list some possible attacks for Eve. In Section 5.2.4 we calculate the capacity of BB84 to find the maximal key rate.

5.2.1 Bit extraction: strategy and probabilities

Bit extraction strategy

The bit encoding scheme used by Alice is the following. Let $b \in \{0,1\}$ be the bit to be encoded.

b	encoded in RL-basis	encoded in DG-basis
0	$\|0\rangle$	$\|+\rangle$
1	$\|1\rangle$	$\|-\rangle$

Suppose that a bit value is encoded in the RL- or the DG-basis at random. The encoded bit is then sent to Bob. Suppose Bob receives the qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. He measures the state $|\psi\rangle$ in the RL-basis or the DG-basis at random. Bob decodes a measurement of state $|0\rangle$ or $|+\rangle$ to bit value 0 and a measurement of state $|1\rangle$ or $|-\rangle$ to bit value 1.

Bit extraction probabilities

In the following theorem we give the probabilities that Bob extracts a certain bit value if he measures a general qubit state $|\psi\rangle$ in the RL- or the DG-basis.

Theorem 5.2.1 *Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$. Let $RL = \{|0\rangle, |1\rangle\}$ be the rectilinear basis and $DG = \{|+\rangle, |-\rangle\}$ be the diagonal basis. Let a measurement of $|0\rangle$ or $|+\rangle$ correspond to a measurement of bit value 0 and let a measurement of $|1\rangle$ or $|-\rangle$ correspond to a measurement of bit value 1.*
The probability to extract bit value $b \in \{0,1\}$ from $|\psi\rangle$ when we measure in basis . is denoted by $P_{\cdot}^{|\psi\rangle}(b)$. These probabilities as well as the corresponding state after the measurement are given by

$$\begin{array}{lcll} P_{RL}^{|\psi\rangle}(0) & = & |\alpha|^2 & , \text{ state after the measurement is } \frac{\alpha}{|\alpha|}|0\rangle \\ P_{RL}^{|\psi\rangle}(1) & = & |\beta|^2 & , \text{ state after the measurement is } \frac{\beta}{|\beta|}|1\rangle \\ P_{DG}^{|\psi\rangle}(0) & = & \frac{|\alpha+\beta|^2}{2} & , \text{ state after the measurement is } \frac{\alpha+\beta}{|\alpha+\beta|}|+\rangle \\ P_{DG}^{|\psi\rangle}(1) & = & \frac{|\alpha-\beta|^2}{2} & , \text{ state after the measurement is } \frac{\alpha-\beta}{|\alpha-\beta|}|-\rangle \end{array}$$

Proof. Appendix B tells us that a measurement in basis RL is a projective measurement. The Postulates from Section 2.4 give us how to calculate with projective measurements.

The probability to extract bit value 0 is

$$P_{RL}^{|\psi\rangle}(0) = \langle\psi|P_0|\psi\rangle = |\langle\psi|0\rangle|^2 = |\alpha|^2.$$

The state after this measurement is

$$\frac{P_i|\psi\rangle}{\sqrt{P_{|\psi\rangle}(0)}} = \frac{\alpha}{\sqrt{|\alpha|^2}}|0\rangle = \frac{\alpha}{|\alpha|}|0\rangle.$$

In the same way we find

$$P_{RL}^{|\psi\rangle}(1) = |\beta|^2$$

and the state after this measurement is

$$\frac{\beta}{|\beta|}|1\rangle.$$

Appendix B tells us that a measurement in the DG-basis is a projective measurement. The state $|\psi\rangle$ is written in the DG-basis in the following way.

$$\begin{aligned} |\psi\rangle = \alpha|0\rangle + \beta|1\rangle &= \left(\frac{\alpha+\beta}{\sqrt{2}}\right)\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) + \left(\frac{\alpha-\beta}{\sqrt{2}}\right)\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) \\ &= \left(\frac{\alpha+\beta}{\sqrt{2}}\right)|+\rangle + \left(\frac{\alpha-\beta}{\sqrt{2}}\right)|-\rangle. \end{aligned}$$

Using the Postulates presented in Section 2.4 and the representation of $|\psi\rangle$ in the DG-basis, the measurement probabilities and the states after the measurement in the DG-basis follow easily. □

The following theorem gives the probability that Alice and Bob extract the same bit value given that there is no eavesdropper. The theorem says that in this case, if Alice and Bob use the same basis then with probability 1 they find the same bit value. If the bases used are different then the extracted bit value by the receiver is random.

Theorem 5.2.2 *Let the bit to be encoded be $b \in \{0,1\}$. Suppose the bit is encoded into $|\psi\rangle$ according to the bit encoding strategy*

b	*encoded in RL-basis*	*encoded in DG-basis*
0	$\|0\rangle$	$\|+\rangle$
1	$\|1\rangle$	$\|-\rangle$.

Suppose a measurement of $|0\rangle$ or $|+\rangle$ corresponds to bit value 0, a measurement of $|1\rangle$ or $|-\rangle$ corresponds to bit value 1. If there is no eavesdropper, then

$$P_{RL}(b) = \begin{cases} 1 & \text{if } |\psi\rangle \in RL \\ \frac{1}{2} & \text{if } |\psi\rangle \in DG \end{cases}$$

and

$$P_{DG}(b) = \begin{cases} 1 & \text{if } |\psi\rangle \in DG \\ \frac{1}{2} & \text{if } |\psi\rangle \in RL \end{cases}$$

If $|\psi\rangle$ is measured in the correct basis then the state after the measurement is equal to $|\psi\rangle$. If $|\psi\rangle$ is measured in the incorrect basis then the state after the measurement is equally likely to be one of the basis states of this incorrect basis.

Proof. If $|\psi\rangle \in RL$, then $\alpha = 1$ and $\beta = 0$ or $\alpha = 0$ and $\beta = 1$. If $|\psi\rangle \in DG$, then $\alpha = 1/\sqrt{2}$ and $\beta = 1/\sqrt{2}$ or $\alpha = 1/\sqrt{2}$ and $\beta = -1/\sqrt{2}$. The results of the theorem easily follow from Theorem 5.2.1. □

Measuring in both bases gives no extra information

After a measurement of a qubit state $|\psi\rangle$ in the RL- or the DG-basis, a following measurement in the other basis does not give extra information about $|\psi\rangle$. This is because the outcome of the second measurement would be random. We illustrate why this is true.
For example, suppose the qubit $|\psi\rangle = \gamma|0\rangle + \delta|1\rangle$, with $|\gamma|^2 + |\delta|^2 = 1$, is measured in the RL-basis. Suppose bit value 1 is measured. Theorem 5.2.1 tells us that the state after the

measurement is equal to $(\delta/|\delta|)\,|1\rangle$. Suppose that this state is subsequently measured in the DG-basis. The probability that bit value 0 is measured is (substitute $\alpha = 0$ and $\beta = \delta/|\delta|$ in Theorem 5.2.1)

$$P_{DG}(0) = \frac{|\alpha + \beta|^2}{2} = \frac{|\delta|^2}{2|\delta|^2} = \frac{1}{2}$$

and the probability that bit value 1 is measured is

$$P_{DG}(1) = \frac{|\alpha - \beta|^2}{2} = \frac{|\delta|^2}{2|\delta|^2} = \frac{1}{2}.$$

5.2.2 Protocol

Now we explained which non-orthogonal quantum states are used in BB84 and the bit extraction strategy is studied, we can describe the protocol. Before we describe the protocol completely, we give a brief description of the protocol in which we explain some important steps.

Alice chooses a random bit string X'' of length $(4 + \delta)n$, where $\delta > 0$ and $n \in \mathbb{N}$. She encodes X'' using the encoding scheme described in the previous section. In this way she randomly prepares qubit states from the RL- and the DG-basis. Alice then sends the qubit states to Bob who measures them in the RL- or the DG-basis at random and extracts a bit string Y'' of length $(4 + \delta)n$.

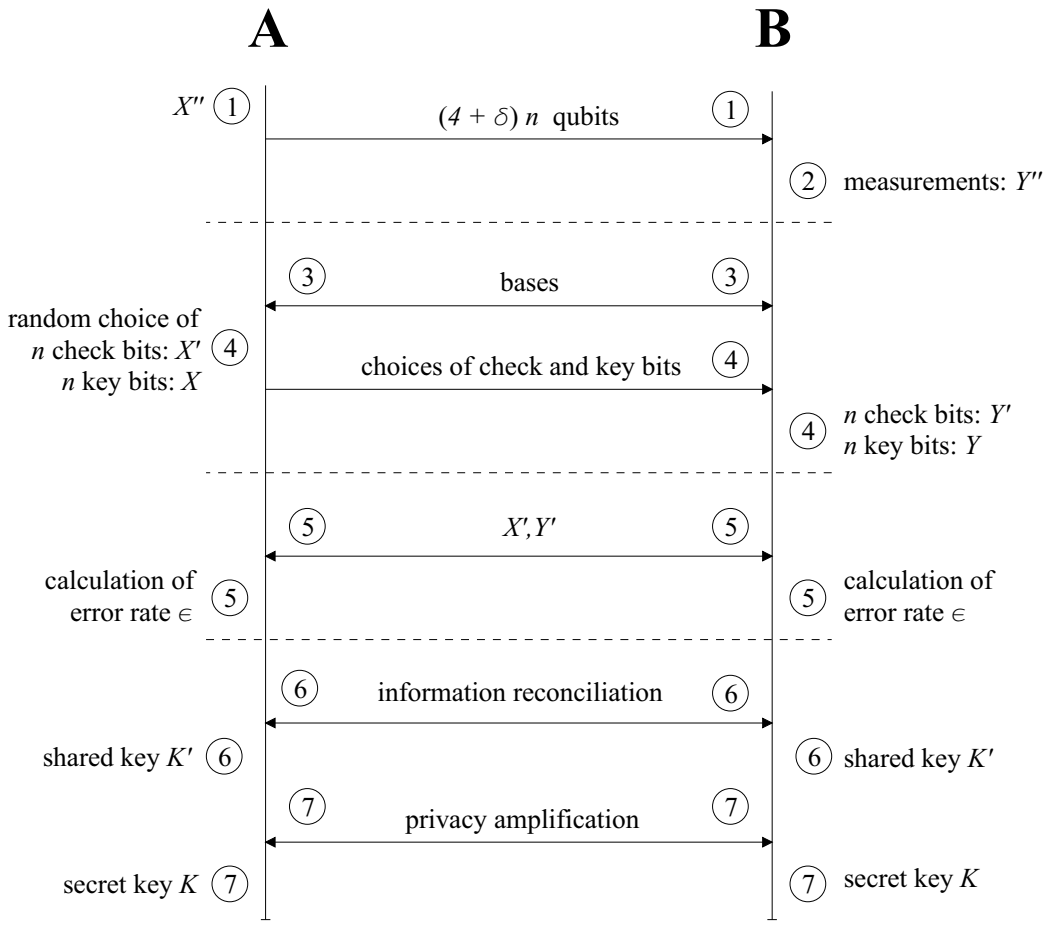
After Bob has measured all qubits, Alice and Bob can announce which bases they used. This is because of the following. Eve cannot clone the states sent by Alice (see Theorem 4.3.3) and therefore, once the qubits are received by Bob, Eve cannot gain information about the qubits anymore. This means that after Bob received the qubits, Alice and Bob are perfectly safe to announce which bases they used. Theorem 5.2.2 tells us that if Alice and Bob used the same basis then, if there is no eavesdropper, the extracted bit values from Alice and Bob are exactly the same. On the positions where they used a different basis the bit value Bob extracts is random. This means that Alice and Bob can discard the bits where they used a different basis without losing information they could have used to get a common secret key.

Next, if the number of positions where Alice and Bob used the same basis is at least $2n$, then Alice chooses from the corresponding bits n check bits (X') and n key bits (X). Alice announces the choice of these bits so that Bob can determine his check bit string (Y') and his key bit string (Y). Then Alice and Bob announce their check bits X', Y' such that they can estimate the bit error rate ϵ. Bit errors are introduced by the channel and by Eve who introduces disturbance in the system by trying to distinguish between the non-orthogonal states.
There are methods to find a threshold for the error rate ϵ. In Chapter 7 we will prove that this threshold is at $\epsilon = 0.11$ for BB84. We find this threshold with a method introduced in [24].

In our implementation of BB84, Alice uses half of the positions where they used the same basis as check bits. There are alternative methods, studied for example in [16], where Alice uses less bits for check bits. This might lead to a better rate but we will not explore that case, we will focuss on the case presented.

The reason that Alice starts with a bit string of length $(4+\delta)n$ with $\delta > 0$ and $n \in \mathbb{N}$ is that then, with high probability, Alice and Bob will have at least $2n$-bit positions where they used the same basis. How to choose δ such that the probability that Alice and Bob have at least $2n$ bit positions where they used the same basis is discussed in Appendix C. In practice, δ is small with respect to n; if $n > 1000$ for example, then δ can be chosen smaller than 1 such that with negligible probability, Alice and Bob have less than $2n$ values where they used the same basis.

The protocol is described below. The diagram displays the actions of Alice and Bob in the protocol. We see that X'', X and the qubits Alice sends are secret and only know by Alice. The bit strings Y'', Y are secret and only known by Bob. The strings K, K' are secret and known by Alice and Bob. The check bit strings X', Y' are public and after Bob has measured all qubits, the bases Alice and Bob used for all qubits are public as well.



Distribution, Measurement & Bit Extraction

1. Alice chooses a random bit string X'' of length $(4+\delta)n$, where $\delta > 0$. For each bit she decides at random to encode it in the RL-basis $\{|0\rangle, |1\rangle\}$ or in the DG-basis

$\{|+\rangle, |-\rangle\} = \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. The encoding scheme works in the following way.

bit value to encode	encoded in RL-basis	encoded in DG-basis
0	$\|0\rangle$	$\|+\rangle$
1	$\|1\rangle$	$\|-\rangle$

Alice sends the resulting $(4 + \delta)n$ qubits to Bob.

2. Bob receives the $(4 + \delta)n$ qubits and measures each of them in the RL- or DG-basis at random. From the result of each measurement he deduces a bit value 0 or 1. If he measures qubit $|0\rangle$ or $|+\rangle$ he deduces bit value 0 and if he measures qubit $|1\rangle$ or $|-\rangle$ he deduces bit value 1. Bob now has a bit string Y'' of length $(4 + \delta)n$.

Bases comparison & Determination of Key- and Check Bits

3. Bob confirms having received the qubits. Alice announces into which basis each bit in the bit string was encoded. Bob announces in which basis he measured each received qubit.

4. Alice and Bob discard the results in the cases where Alice encoded and Bob measured in a different basis. If there are less than $2n$ bits left, they abort the protocol. Alice decides randomly on a set of $2n$ bits to use for the protocol and selects at random n of these $2n$ bits that will serve as a check to Eve's interference. The other n bits will be key bits. Alice announces these choices. Alice and Bob now each have a check bit string and a key bit string of length n (respectively X' and X for Alice, Y' and Y for Bob).

Determination of error rate

5. Alice and Bob announce bit string X' and Y' and compare the values of these n check bits. If the error rate ϵ is greater than a certain threshold, they abort the protocol. If this is not the case, they know that Eve's interference is negligible.

Information Reconciliation & Privacy Amplification

6. Alice and Bob now have highly correlated bit strings that can be made identical with high probability by information reconciliation. For this Alice sends $H(X|Y) = nh(\epsilon)$ bits to Bob. With error correction Alice and Bob retrieve an equal bit string K' with high probability. We will not give further details about how the information reconciliation works because this is outside the scope of this thesis. For more information we refer to [15, 16].

7. Alice and Bob now have the same bit string but it is still possible that Eve has partial information about these bits. To eliminate this partial information Alice and Bob apply privacy amplification to their bit strings K'. The resulting $m < n$-bit string K is used as the secret key. We will not give further details about how the privacy amplification works because this is outside the scope of this thesis. For more information we refer to [17, 18].

5.2.3 Possible attacks by Eve

Because Eve cannot clone the state Alice sends to Bob, the only option for Eve is to intercept the state, measure it in some basis (she cannot measure in both bases) and send a state to Bob. Because Eve wants Bob to think that he received the state directly from Alice, Eve has to send such a state to Bob that the average probability that Alice and Bob find the same bit given that they both encode and measure in the same basis is as high as possible. In this section, we study some possible scenario's for Eve and see what the best strategy is for Eve.

We assume that Alice and Bob both encoded and measured in the same basis, because they discard the bits for which this is not the case.

Eve measures in the RL- or the DG-basis

In this scenario Eve intercepts the state sent by Alice, measures it in the RL- or DG-basis and sends a qubit state to Bob. We show that in this case, the probability that Eve finds the bit value encoded by Alice is always $\frac{3}{4}$ and the probability that Bob finds the same bit value as Alice with probability smaller or equal to $\frac{3}{4}$. The maximum $\frac{3}{4}$ is reached when Eve sends the state produced by her measurement to Bob.

Suppose Alice sends the state $|\psi\rangle$ with $|\psi\rangle \in \{|0\rangle, |1\rangle\}$ or $|\psi\rangle \in \{|+\rangle, |-\rangle\}$.

Eve sends the states produced by her measurements to Bob
Suppose first that Eve sends the state produced by her measurement to Bob. There are two possible situations.

- With probability $\frac{1}{2}$ Eve measures $|\psi\rangle$ in the correct basis. As we saw in Theorem 5.2.2 Eve finds the correct bit value with probability 1. The state of the qubit after the measurement in the correct basis is not altered so is equal to $|\psi\rangle$. Eve sends the unchanged qubit $|\psi\rangle$ to Bob who measures it in the correct basis as well. Bob will find the correct bit value with probability 1.
- With probability $\frac{1}{2}$ Eve measures $|\psi\rangle$ in the incorrect basis. As we saw in Theorem 5.2.2 the bit value Eve finds is random. The state of the qubit after the measurement is a random basis state of this incorrect basis. Eve sends a qubit from the incorrect basis to Bob who measures it in the correct basis. Bob will find a random bit.

The probability that Alice and Bob extract the same bit value in this scenario is $\frac{1}{2}\cdot 1 + \frac{1}{2}\cdot\frac{1}{2} = \frac{3}{4}$. Eve finds the correct bit value with the same probability.

We give an example of this scenario.

Example 5.2.3 *Suppose Alice sent the state $|\psi\rangle = |0\rangle$ to Bob. Suppose Eve measures in the RL-basis. She will measure bit value 0 with probability 1 and the state after the measurement is $|0\rangle$. Eve sends the state $|0\rangle$ to Bob who measures it in the RL-basis as well. He will measure bit value 0 with probability 1 (Theorem 5.2.2 is applied where Alice and Bob measured in the same basis).*

Suppose on the other hand that Eve measures in the diagonal basis. She will measure a random bit value and the state after the measurement is $|+\rangle$ or $|-\rangle$ each with probability $\frac{1}{2}$. Depending on the measurement result Eve sends $|+\rangle$ or $|-\rangle$ to Bob who measures it in the RL-basis. Theorem 5.2.2 says that Bob will find the correct bit value with probability $\frac{1}{2}$. (Theorem 5.2.2 is applied where Alice and Bob measured in different bases)

Eve sends different states than the states produced by her measurement to Bob
Now suppose that Eve sends a state to Bob different than the state produced by her measurement. We show that in this case Eve is worse off than in the previous case.

Suppose Eve measures the state sent by Alice. The probability that Eve measures the correct bit value is $\frac{3}{4}$ (see the previous scenario). Suppose Alice sends a state in the RL-basis. When Alice sends a state in the DG-basis the result of the calculations are the same. The scenario is the following.

- With probability 0.5 Alice sends qubit $|0\rangle$.
  - With probability 0.5 Eve measures in the correct basis. The state after the measurement is $|0\rangle$. Eve sends the state

    $$\sqrt{1-\gamma}|0\rangle + \sqrt{\gamma}|1\rangle$$

    to Bob where $0 < \gamma \leq 1/2$. By sending this state instead of sending $|0\rangle$ Eve hopes to cover the cases in which she measures in the incorrect basis. The probability that Bob measures bit value 0 is $1-\gamma$.
  - With probability 0.5 Eve measures in the incorrect basis. The state after the measurement is $|+\rangle$ with probability 0.5. Eve sends the state

    $$\sqrt{1-\gamma}|+\rangle + \sqrt{\gamma}|-\rangle$$

    to Bob. The probability that Bob measures bit value 0 in the RL-basis is

    $$\frac{|\sqrt{1-\gamma}+\sqrt{\gamma}|^2}{2} = \frac{1}{2} + \sqrt{(1-\gamma)\gamma}.$$

    The state after Eve's measurement can also be $|-\rangle$ with probability 0.5. Eve sends the state

    $$\sqrt{\gamma}|+\rangle + \sqrt{1-\gamma}|-\rangle$$

    to Bob and the probability that Bob measures the correct bit value 0 in the RL-basis is $\frac{1}{2} + \sqrt{(1-\gamma)\gamma}$ as well.

  We find that if Alice sends the state $|0\rangle$ then the probability that Bob measures bit value 0 is on average

  $$\frac{1}{2}(1-\gamma) + \frac{1}{2}\left(\frac{1}{2} + \sqrt{(1-\gamma)\gamma}\right)$$

- With probability 0.5 Alice sends qubit $|1\rangle$. The line of reasoning follows that of the case where Alice sent state $|0\rangle$.

– With probability 0.5 Eve measures in the correct basis. The state after the measurement is $|1\rangle$. Eve sends the state

$$\sqrt{\gamma}|0\rangle + \sqrt{1-\gamma}|1\rangle$$

to Bob where $\gamma > 0$. The probability that Bob measures bit value 1 is $1 - \gamma$.

– With probability 0.5 Eve measures in the incorrect basis. The state after the measurement is $|+\rangle$ with probability 0.5. Eve sends the state

$$\sqrt{1-\gamma}|+\rangle + \sqrt{\gamma}|-\rangle$$

to Bob. The probability that Bob measures bit value 1 in the RL-basis is

$$\frac{|\sqrt{1-\gamma} - \sqrt{\gamma}|^2}{2} = \frac{1}{2} - \sqrt{(1-\gamma)\gamma}.$$

The state after Eve's measurement can also be $|-\rangle$ with probability 0.5. Eve sends the state

$$\sqrt{\gamma}|+\rangle + \sqrt{1-\gamma}|-\rangle$$

to Bob and the probability that Bob measures the correct bit value 1 in the RL-basis is $\frac{1}{2} - \sqrt{(1-\gamma)\gamma}$ as well.

We see that if Alice sent state $|1\rangle$ then on average the probability that Bob finds bit value 1 by measuring in the correct basis is

$$\frac{1}{2}(1-\gamma) + \frac{1}{2}\left(\frac{1}{2} - \sqrt{(1-\gamma)\gamma}\right).$$

On average the probability that Alice and Bob find the same bit value is

$$\frac{1}{2}(1-\gamma) + \frac{1}{4} = \frac{3}{4} - \frac{1}{2}\gamma < \frac{3}{4}$$

while the probability that Eve finds the correct bit value is $\frac{3}{4}$. With this strategy the probability that Alice and Bob find the same bit value is in the interval $[\frac{1}{2}, \frac{3}{4})$ because $0 < \gamma \leq 1/2$. We see that Bob is always worse off than in the first scenario. We find the first scenario for Eve by substituting $\gamma = 0$.

We may conclude that if Eve applies the strategy of measuring the qubit received from Alice in the rectilinear or the diagonal basis then the best thing she can do after the measurement is to send the state produced by the measurement to Bob. The probability that Alice and Bob find the same bit value is $\frac{3}{4}$. The probability that Eve finds the same bit value as Alice is $frac34$ as well.

Eve measures in the Breidbart basis

In the previous scenario, Eve measured in the same bases as Alice encoded bits in and Bob measured in. The risk here was that Eve could measure in the incorrect basis. She could also make a new basis in which she would measure all qubits received from Alice. The best

measurement basis for extracting as much information as possible about the qubits received from Alice is the Breidbart basis [19]. This basis is given by

$$\{|a\rangle, |b\rangle\} = \{\cos\left(\frac{\pi}{8}\right)|0\rangle + \sin\left(\frac{\pi}{8}\right)|1\rangle, -\sin\left(\frac{\pi}{8}\right)|0\rangle + \cos\left(\frac{\pi}{8}\right)|1\rangle\}.$$

It is an orthonormal basis so measurement in this basis is a projective measurement. We assume that Eve lets the state $|a\rangle$ correspond to bit value 0 and the state $|b\rangle$ to bit value 1. We show that if Eve does all the measurements in the Breidbart basis then the probability that she finds the same bit as Alice is around 0.85 whereas the probability that Bob finds the same bit as Alice is $\frac{3}{4}$.

First we calculate the probability that Eve finds the same bit value as Alice. We calculate this for the case that Alice sends bit value 0. The case where Alice sends bit value 1 goes in a similar way and the resulting probability is the same.

- With probability $\frac{1}{2}$ Alice sent the state $|0\rangle$. Eve measures the state $|a\rangle$ and finds bit value 0 with probability
$$|\langle 0|a\rangle|^2 = \left|\cos\left(\frac{\pi}{8}\right)\right|^2.$$
- With probability $\frac{1}{2}$ Alice sent the state $|+\rangle$. Eve measures the state $|a\rangle$ and finds bit value 0 with probability
$$|\langle +|a\rangle|^2 = \left|\frac{1}{\sqrt{2}}\left(\cos\left(\frac{\pi}{8}\right) + \sin\left(\frac{\pi}{8}\right)\right)\right|^2 = \left|\cos\left(\frac{\pi}{8}\right)\right|^2.$$

We find that the probability that Eve finds the same bit as Bob is equal to

$$\left|\cos\left(\frac{\pi}{8}\right)\right|^2 \approx 0.85.$$

The probability that Alice and Bob find the same qubit is calculated in the following. Suppose Alice encodes a bit value 0. The case where Alice encodes bit value 1 gives the same result.

- With probability $\frac{1}{2}$ Alice sends the state $|0\rangle$. The probability that Bob finds bit value 0 is
$$\begin{aligned} P(B:0) &= P(B:0|E:0)P(E:0) + P(B:0|E:1)P(E:1) \\ &= |\langle 0|a\rangle|^2|\langle a|0\rangle|^2 + |\langle 0|b\rangle|^2|\langle b|0\rangle|^2 \\ &= |\langle 0|a\rangle|^4 + |\langle 0|b\rangle|^4 \\ &= \left|\cos\left(\frac{\pi}{8}\right)\right|^4 + \left|\sin\left(\frac{\pi}{8}\right)\right|^4 \end{aligned}$$
- With probability $\frac{1}{2}$ Alice sends the state $|+\rangle$. The probability that Bob finds bit value 0 is
$$\begin{aligned} P(B:0) &= P(B:0|E:0)P(E:0) + P(B:0|E:1)P(E:1) \\ &= |\langle +|a\rangle|^2|\langle a|+\rangle|^2 + |\langle +|b\rangle|^2|\langle b|+\rangle|^2 \\ &= |\langle +|a\rangle|^4 + |\langle +|b\rangle|^4 \\ &= \left|\frac{1}{\sqrt{2}}\left(\cos\left(\frac{\pi}{8}\right) + \sin\left(\frac{\pi}{8}\right)\right)\right|^4 + \left|\frac{1}{\sqrt{2}}\left(\cos\left(\frac{\pi}{8}\right) - \sin\left(\frac{\pi}{8}\right)\right)\right|^4 \\ &= \left|\cos\left(\frac{\pi}{8}\right)\right|^4 + \left|\sin\left(\frac{\pi}{8}\right)\right|^4. \end{aligned}$$

The probability that Alice and Bob find the same bit value is given by

$$\begin{aligned} P(BitID) &= \left|\cos\left(\frac{\pi}{8}\right)\right|^4 + \left|\sin\left(\frac{\pi}{8}\right)\right|^4 \\ &= \frac{3}{4}. \end{aligned}$$

The case where Eve for example measures the state $|a\rangle$ and sends the state $\sqrt{1-\epsilon}|a\rangle + \sqrt{\epsilon}|b\rangle$ is no issue in this scenario. This is because Eve does not have to choose between two bases and therefore does not have to compensate for a possible mistake in the choice of basis.

We can conclude that with the presented scenarios in order to maximize the probability that Eve finds the correct bit value and the probability that Bob finds the correct bit value the best thing Eve can do is to measure all qubits received by Alice in the Breidbart basis and send the state produced by the measurement to Bob.

5.2.4 Capacity BB84

A quantum channel cannot be modelled directly as a classical channel. In the quantum protocols we deal with however, we are interested in whether bit transmission succeeded or not. In these protocols there are two different probability distributions for the bit transmission corresponding to two different situations within each protocol. With this we can model the corresponding bit transmission of the quantum channel into two classical channels and compute the capacities of these classical channels separately. We use Theorem D.0.9 presented in Appendix D.

To compute the capacity of BB84 with help of classical channels, we need the probability distribution of the bit Bob deduces from the measurement. Before Bob's measurement this probability distribution is in a superposition of two probability distributions;

1. With probability $\frac{1}{2}$ Bob measures in the correct basis (the basis Alice sent the state in). With probability 1, Bob wil find the correct bit value. The classical channel that corresponds to this probability distribution is visualized in Figure 5.1. This is a binary symmetric channel and so the capacity is $1 - h(1) = 1$.

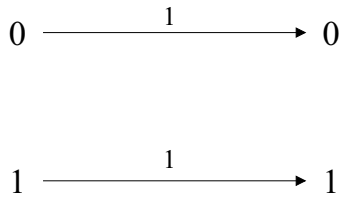


Figure 5.1: Correct basis

2. With probability $\frac{1}{2}$ Bob measures in the incorrect basis. Bob will find a random bit value. The classical channel that corresponds to this probability distribution is visualized in Figure 5.2. The capacity of this channel is $1 - h(0.5) = 0$.

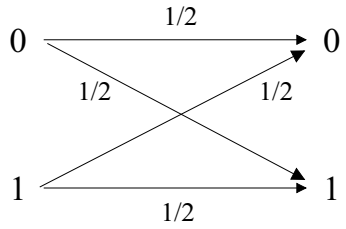


Figure 5.2: Incorrect basis

This gives us that the capacity of the $BB84$ quantum channel is given by

$$C_{BB84} = \frac{1}{2} \cdot 0 + \frac{1}{2} \cdot 1 = \frac{1}{2}.$$

This states that the maximum rate of the protocol is $\frac{1}{2}$. Indeed, Alice and Bob use the same basis with probability 1/2. On these positions, if there is no eavesdropper, they will find the same bit value, which is on half of the total positions.

5.3 Squeezed state protocol by Gottesman & Preskill (GP00)

In GP00 squeezed states are used as non-orthogonal quantum states. Alice prepares squeezed states $|r, \alpha\rangle$ squeezed in x (position) or in p (momentum) at random. If Alice squeezes in x, she chooses $r = -\hat{r}$ and if she squeezes in p, she chooses $r = \hat{r}$ for some fixed $\hat{r}$ (see Section 4.5). The value of α determines the expectations of x and p of the squeezed states. She then sends the squeezed states to Bob over a quantum communication channel.

Alice extracts bit values from the squeezed states she sends to Bob. Bob extracts bit values from measurements he made on the squeezed states he receives. They extract bits according to some bit extraction strategy they agreed on beforehand. In Section 5.3.1 we will explain and study the bit extraction strategy used by Alice and Bob. We calculate the probability that Alice and Bob find the same bit value for different scenarios.

In Section 5.3.2 we describe the protocol GP00 and in Section 5.3.3 we list some possible attacks for Eve. In Section 5.3.4 we calculate the capacity of GP00 to find the maximal key rate.

5.3.1 Bit extraction: strategy and probabilities

Measuring in both bases gives no extra information

If a squeezed state $|r, \alpha\rangle$ is measured in the x or the p-basis, then a subsequent measurement in the other basis does not give extra information. The commutator $[x, p] = i\hbar$ and therefore the Heisenberg uncertainty relation tells us that it is impossible to have exact knowledge of both the position and the momentum of a quantum state. Suppose namely that a squeezed state is measured in the x-basis and that the position value $x_n \in \mathbb{R}$ is measured. The state after this measurement is

$$\beta|x_n\rangle = \beta\delta(x - x_n)$$

for some $\beta \in \mathbb{C}$ with $|\beta|^2 = 1$. If at this moment the momentum of this state would be measured then every possible outcome for the momentum is equally likely. This is because for every p_m it holds that

$$\begin{aligned} P_P^{\beta|x_n\rangle}(p_m) &= \langle x_n|p_m\rangle\langle p_m|x_n\rangle \\ &= \left|\int_{-\infty}^{\infty} e^{-ip_m x}\delta(x-x_n)dx\right|^2 \\ &= \left|e^{-ip_m x_n}\right|^2 \\ &= 1 \end{aligned}$$

Every $p_m \in \mathbb{R}$ has probability 1 to be measured and that means that every value $p_m \in \mathbb{R}$ is equally likely to be measured.

Bit extraction strategy

From now on we assume that states are squeezed with a fixed squeezing parameter. We already saw in Section 4.5 that if a squeezed state is squeezed in x then $r < 0$ and if a squeezed state is squeezed in p then $r > 0$. We fix this squeezing parameter at the value $\hat{r} > 0$ if we squeeze in p and at $-\hat{r}$ if we squeeze in x.

We define the following intervals that divide $\mathbb{R}$ in two intervals of equal size.

$$\begin{aligned} \mathcal{L}_0 &= \{\ldots, \left[-2\sqrt{\pi\hbar}, -\sqrt{\pi\hbar}\right), \left[|0, \sqrt{\pi\hbar}\right), \left[2\sqrt{\pi\hbar}, 3\sqrt{\pi\hbar}\right), \ldots\} \\ \mathcal{L}_1 &= \{\ldots, \left[-\sqrt{\pi\hbar}, 0\right), \left[\sqrt{\pi\hbar}, 2\sqrt{\pi\hbar}\right), \left[3\sqrt{\pi\hbar}, 4\sqrt{\pi\hbar}\right), \ldots\}. \end{aligned}$$

The intervals $\mathcal{L}_0$ and $\mathcal{L}_1$ are visualized in Figure 5.3.

Encoding scheme

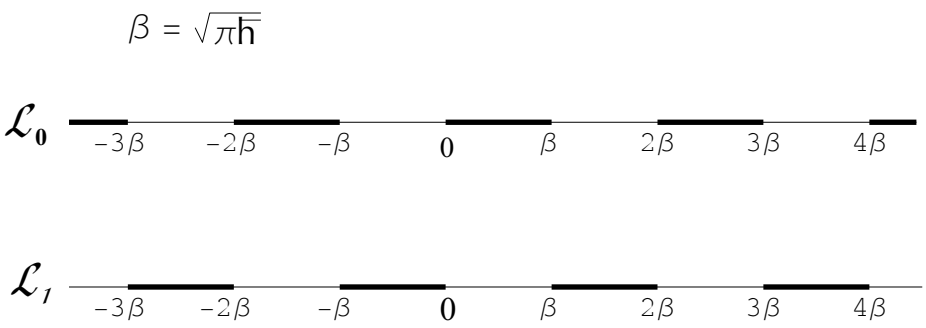


Figure 5.3: Visualization of the encoding intervals $\mathcal{L}_0$ and $\mathcal{L}_1$.

Alice uses the following bit encoding scheme. Define $b \in \{0, 1\}$ to be the bit to be encoded.

Define $\mathcal{K} = \{-n_k, -n_k+1, \ldots, n_k-1\}$ for some $n_k \in \mathbb{N}$.

b	squeezing in x
0	$\lvert -\hat{r}, \alpha\rangle$ with $\langle x\rangle \in \mathcal{L}_0$ and $\langle p\rangle = \langle x\rangle + (k+\frac{1}{2})\sqrt{\pi\hbar}$ for random $k \in \mathcal{K}$
1	$\lvert -\hat{r}, \alpha\rangle$ with $\langle x\rangle \in \mathcal{L}_1$ and $\langle p\rangle = \langle x\rangle + (k+\frac{1}{2})\sqrt{\pi\hbar}$ for random $k \in \mathcal{K}$

b	squeezing in p
0	$\lvert \hat{r}, \alpha\rangle$ with $\langle p\rangle \in \mathcal{L}_0$ and $\langle x\rangle = \langle p\rangle + (k+\frac{1}{2})\sqrt{\pi\hbar}$ for random $k \in \mathcal{K}$
1	$\lvert \hat{r}, \alpha\rangle$ with $\langle p\rangle \in \mathcal{L}_1$ and $\langle x\rangle = \langle p\rangle + (k+\frac{1}{2})\sqrt{\pi\hbar}$ for random $k \in \mathcal{K}$

We will see later, that with this encoding scheme, if Bob measures in the correct basis, then he finds the correct bit with high probability. If Bob measures in the incorrect basis, then he finds a random bit.

To obtain certain values of $\langle x\rangle$ and $\langle p\rangle$ for a squeezed state, Alice chooses a proper $\alpha \in \mathbb{C}$. We note that if Alice squeezes in x, then the value $\langle x\rangle$ has to be secret and if Alice squeezes in p, then the value $\langle p\rangle$ has to be secret. This means that the parameter $\alpha = se^{i\theta}$ is secret. Whether Alice squeezes in x or p is secret too.

We define

$$\phi_x = \langle x\rangle \bmod \sqrt{\pi\hbar}$$

and

$$\phi_p = \langle p\rangle \bmod \sqrt{\pi\hbar}$$

so $0 \leq \phi_x, \phi_p < \sqrt{\pi\hbar}$. Alice calculates ϕ_x if she squeezed in x and she calculates ϕ_p if she squeezed in p. The values $\langle x\rangle$ (if Alice squeezed in x) and $\langle p\rangle$ (if Alice squeezed in p) can then be written as

$$\begin{aligned} \langle x\rangle &= n_x\sqrt{\pi\hbar} + \phi_x \\ \langle p\rangle &= n_p\sqrt{\pi\hbar} + \phi_p \end{aligned}$$

with $n_x, n_p \in \mathbb{N}$. The main bit encoding scheme properties become

$$\begin{aligned} &\langle x\rangle \in \mathcal{L}_0 \Leftrightarrow n_x \text{ is even} \\ &\langle x\rangle \in \mathcal{L}_1 \Leftrightarrow n_x \text{ is odd} \end{aligned}$$

$$\begin{aligned} &\langle p\rangle \in \mathcal{L}_0 \Leftrightarrow n_p \text{ is even} \\ &\langle p\rangle \in \mathcal{L}_1 \Leftrightarrow n_p \text{ is odd.} \end{aligned}$$

The values $\langle x\rangle$ (if Alice squeezes in x) and $\langle p\rangle$ (if Alice squeezes in p) should be chosen from the intervals $\mathcal{L}_0$ and $\mathcal{L}_1$ according to some normalized probability distribution. If we use a probability distribution for $\langle x\rangle$ or $\langle p\rangle$ that gives us a value in $\mathcal{L}_0$ with probability $\frac{1}{2}$ and a value in $\mathcal{L}_1$ with probability $\frac{1}{2}$, then we do not have to choose a random bit by ourselves. This is because the probability distribution determines a random bit by sampling a mean value for the squeezed state. A proper distribution that satisfies this condition is a Gaussian distribution centered at the origin and with some variance σ^2;

$$P_{\text{pos}}(\langle x\rangle) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(\frac{\langle x\rangle^2}{2\sigma^2}\right)$$

$$P_{\text{mom}}(\langle p\rangle) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(\frac{\langle p\rangle^2}{2\sigma^2}\right)$$

If we wanted to encode a random bit by squeezing in x, we now sample $\langle x\rangle$ from $P_{pos}(\langle x\rangle)$ and choose α such that $\angle p\rangle = \langle x\rangle + (k + \frac{1}{2}\sqrt{\pi\hbar})$ for some $k \in \mathbb{Z}$. We find $\langle x\rangle \in \mathcal{L}_0$ with probability $\frac{1}{2}$ and $\langle x\rangle \in \mathcal{L}_1$ with probability $\frac{1}{2}$. If $\langle x\rangle \in \mathcal{L}_0$ we deduce bit 0 otherwise we deduce bit 1.

Bit decoding scheme
Alice sends the squeezed states to Bob who measures them in the x or p-basis at random. Suppose that the outcome of a measurement is z with $z \in \mathbb{R}$. A bit b' is extracted from the value z according to a bit decoding scheme that maximizes the probability that the correct bit is extracted. The value ϕ_x (ϕ_p) is independent of whether $\langle x\rangle$ ($\langle p\rangle$) is in $\mathcal{L}_0$ or $\mathcal{L}_1$. This means that Alice can announce ϕ_x or ϕ_p without giving information about $\langle x\rangle$ or $\langle p\rangle$ and therefore about the secret bit value b. It holds that

$$P(b' = b|\phi_x \text{ or } \phi_p) \geq P(b' = b)$$

and therefore Bob uses ϕ_x or ϕ_p to maximize the probability that he finds the correct bit b. Suppose that the squeezed state was squeezed in x. The state is measured by Bob in the x or the p-basis at random. Suppose that the outcome of this measurement is $z \in \mathbb{R}$. Alice will announce ϕ_x because she squeezed in x. We have that

$$\begin{aligned} z - \phi_x &= z - (\langle x\rangle - n_x\sqrt{\pi\hbar}) \\ &= \left(\frac{z - \langle x\rangle}{\sqrt{\pi\hbar}} + n_x\right)\sqrt{\pi\hbar}. \end{aligned}$$

To extract a bit value from z we rescale z to $z' = n'_x\sqrt{\pi\hbar} + \phi_x$ where n'_x is equal to $\left(\frac{z-\langle x\rangle}{\sqrt{\pi\hbar}} + n_x\right)$ rounded to the nearest integer. If n'_x is even then Bob extracts bit value 0 ($z' \in \mathcal{L}_0$). If n'_x is odd Bob extracts bit value 1 ($z' \in \mathcal{L}_1$). We define the interval $\mathcal{C}$ to be

$$\mathcal{C} = \{\ldots, \left[-\frac{1}{2}\sqrt{\pi\hbar}, \frac{1}{2}\sqrt{\pi\hbar}\right), \left[1\frac{1}{2}\sqrt{\pi\hbar}, 2\frac{1}{2}\sqrt{\pi\hbar}\right), \ldots\}.$$

If n_x is even (odd) then n'_x is even (odd) as well if

$$z - \langle x\rangle \in \mathcal{C}$$

and Alice and Bob extract the same bit value. If the state was squeezed in p we find similar results; if n_p is even (odd) then n'_p is even (odd) as well if

$$z - \langle p\rangle \in \mathcal{C}$$

and Alice and Bob find the same bit value.

Bit extraction probabilities

In this section we find out why $\langle p\rangle = \langle x\rangle + (k + \frac{1}{2})\sqrt{\pi\hbar}$ if Alice squeezes in x and $\langle x\rangle = \langle p\rangle + (k + \frac{1}{2})\sqrt{\pi\hbar}$ if Alice squeezes in p. We will also see why the bit decoding scheme, given the encoding scheme, maximizes the probability that Alice and Bob find the same bit value.

In the theorem we present the probability that Alice and Bob find the same bit value in the case where they use the same basis or different bases, given that there is no eavesdropper.

Theorem 5.3.1 *Let $\hat{r} > 0$ and $\alpha = se^{i\theta} \in \mathbb{C}$. Alice prepares squeezed states squeezed in x or p at random. If Alice squeezes in x, then she samples $\langle x \rangle$ from the probability distribution $P_{pos}(\langle x \rangle)$ and chooses $\langle p \rangle = \langle x \rangle + (k + \frac{1}{2})\sqrt{\pi\hbar}$, for some $k \in \mathbb{Z}$. If Alice squeezes in p, then she samples $\langle p \rangle$ from the probability distribution $P_{mom}(\langle p \rangle)$ and chooses $\langle x \rangle = \langle p \rangle + (k + \frac{1}{2})\sqrt{\pi\hbar}$, for some $k \in \mathbb{Z}$.*

Suppose Alice extracted bit value b. Bob measures the squeezed state in the x-basis or in the p-basis at random. Let z be the outcome of this measurement. Whether Bob will extract the correct bit b from the value z, given that Alice squeezed in a certain basis is indicated below.

	b	$1-b$
Alice squeezed in x $(r = -\hat{r})$	$z - \langle x \rangle \in \mathcal{C}$	$z - \langle x \rangle \in \mathbb{R} \backslash \mathcal{C}$
Alice squeezed in p $(r = \hat{r})$	$z - \langle p \rangle \in \mathcal{C}$	$z - \langle p \rangle \in \mathbb{R} \backslash \mathcal{C}$

The probability of finding the correct bit value b for a measurement in x or p is then

$$P_X(b) = \begin{cases} 1 - \epsilon_s & \text{if } r = -\hat{r} \text{ (original state was squeezed in } x\text{)} \\ \frac{1}{2} & \text{if } r = \hat{r} \text{ (original state was squeezed in } p\text{)} \end{cases}$$

and

$$P_P(b) = \begin{cases} 1 - \epsilon_s & \text{if } r = \hat{r} \text{ (original state was squeezed in } p\text{)} \\ \frac{1}{2} & \text{if } r = -\hat{r} \text{ (original state was squeezed in } x\text{)} \end{cases}$$

for some $0 < \epsilon_s < \frac{1}{2}$.

Proof. Suppose that a squeezed state squeezed in x is measured in the x-basis. The probability that the value $z = x$ is measured is $P_X^{|-\hat{r},\alpha\rangle}(x)$ (see Theorem 4.2.5). We have that

$$\begin{aligned} P_x(b) &= P\left(x - \langle x \rangle \in \mathcal{C}\right) \\ &= \int_{x - \langle x \rangle \in \mathcal{C}} P_X^{|-\hat{r},\alpha\rangle}(x) dx \\ &= 1 - \epsilon_s \end{aligned}$$

for some $0 < \epsilon_s < \frac{1}{2}$. If the squeezing parameter $\hat{r}$ is fixed then $P_x(b)$ is fixed as well. This means that ϵ_s is a function of $\hat{r}$. In the first graph of Figure 5.4 the area is marked that represents the probability $1 - \epsilon_s$. This probability is the same for every $\langle x \rangle \in \mathbb{R}$.

Suppose that a squeezed state squeezed in p is measured in the p-basis. The probability that the value $z = p$ is measured is $P_P^{|\hat{r},\alpha\rangle}(p)$ (see Theorem 4.2.5). From this theorem we see that $P_P^{|\hat{r},\alpha\rangle}(p - \langle p \rangle) = P_X^{|-\hat{r},\alpha\rangle}(x - \langle x \rangle)$. We have that

$$\begin{aligned} P_p(b) &= P\left(p - \langle p \rangle \in \mathcal{C}\right) \\ &= \int_{p - \langle p \rangle \in \mathcal{C}} P_P^{|\hat{r},\alpha\rangle}(p) dp \\ &= \int_{x - \langle x \rangle \in \mathcal{C}} P_X^{|-\hat{r},\alpha\rangle}(x) dx \\ &= 1 - \epsilon_s. \end{aligned}$$

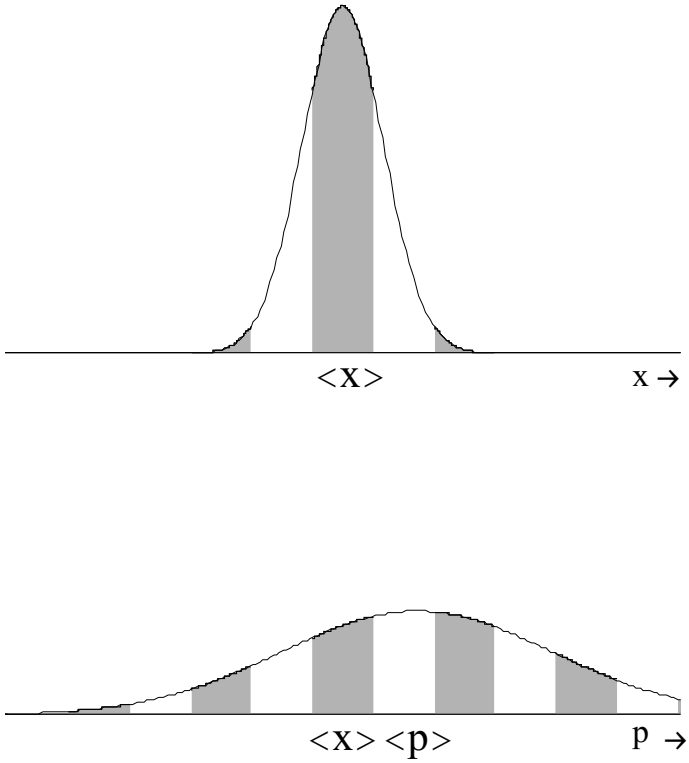


Figure 5.4: Probability to find the correct bit value when the measurement is taken in the x- and the p-basis when the state was squeezed in x.

Suppose on the other hand that a squeezed state squeezed in x is measured in the p-basis. The probability of measuring the correct bit value is

$$\begin{aligned} P_p(b) &= P\left(p - \langle x \rangle \in \mathcal{C}\right) \\ &= \int_{p-\langle x \rangle \in \mathcal{C}} P_P^{|-\hat{r},\alpha\rangle}(p)dp \end{aligned}$$

Suppose that $\langle p \rangle$ was not fixed at $\langle x \rangle + (k+\frac{1}{2})\sqrt{\pi\hbar}$ but was likely to have any value in $\mathbb{R}$. This would mean that the positions of p where $p - \langle x \rangle \in \mathcal{C}$ are placed randomly on the probability distribution for measuring p. This is because these positions of p depend on $\langle x \rangle$ and $\langle x \rangle$ would be independent of $\langle p \rangle$. This means that on average the probability of finding the correct bit b is $1/2$. An instance of the area that leads to the correct bit value is shown in the second graph of Figure 5.4. From the graph we see that the probability to measure the correct bit is maximized if $\langle p \rangle$ is in the middle of an interval of $\mathcal{C}$, so $\langle p \rangle = \langle x \rangle + 2k\sqrt{\pi\hbar}$. It is minimized when $\langle p \rangle = \langle x \rangle + (2k+1)\sqrt{\pi\hbar}$ and equal to $\frac{1}{2}$ when $\langle p \rangle = \langle x \rangle + (k+\frac{1}{2})\sqrt{\pi\hbar}$. The probability distribution for finding the correct bit as a function of $\langle p \rangle$ can be seen in Figure 5.5. It is clear that if we take $\langle p \rangle = \langle x \rangle + (k+\frac{1}{2})\sqrt{\pi\hbar}$ for some $k \in \mathbb{Z}$, then the probability that Bob finds the correct bit is always $\frac{1}{2}$.

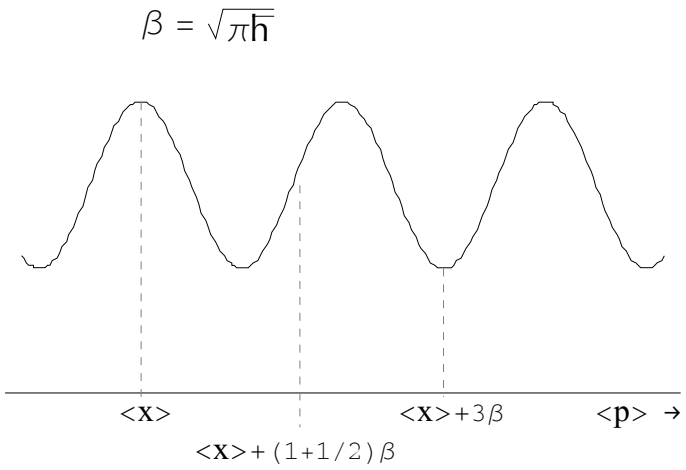


Figure 5.5: Probability of finding the correct bit value when a measurement is taken in the incorrect basis as a function of $\langle p \rangle$. We use $\gamma = \sqrt{\pi\hbar}$.

Suppose that a squeezed state squeezed in p is measured in the x-basis. We have that

$$\begin{aligned} P_x(b) &= P\left(x - \langle p \rangle \in \mathcal{C}\right) \\ &= \int_{x-\langle p \rangle \in \mathcal{C}} P_P^{|\hat{r},\alpha\rangle}(x)dx. \end{aligned}$$

For the same reasons as described in the previous case it holds that the probability of finding the correct bit value is $\frac{1}{2}$. □

In BB84, if Alice and Bob used the same basis, the probability that they would find the same bit was 1 (given that Eve did not interfere). We see here that if squeezed states are used that are not infinitely squeezed, then there is still some probability (noise) that Alice and Bob will not find the same bit. As an illustration, suppose that $|r| = 0.2$. For this choice of the squeezing parameter the probability that the correct bit is found by measuring in the correct basis is (given that there is no eavesdropper)

$$|r| = 0.2 \Rightarrow P(b) = 1 - \epsilon_s = 0.874$$

and when $|r| = 1$ this probability is

$$|r| = 1 \Rightarrow P(b) = 1 - \epsilon_s = 0.999.$$

We see that the probability that Alice and Bob find the same bit, given that they used the same basis, is always equal to $1 - \epsilon_s$. This probability is dependent of $\hat{r}$, and goes to 1 if $r \to \infty$. From now on we assume that ϵ_s is that error probability corresponding to the squeezing parameter $\hat{r}$.
Because $1 - \epsilon_s$ is independent of which mean value Alice encoded ($\langle x \rangle$ if she squeezed in x, $\langle p \rangle$ if she squeezed in p), we see that the bit decoding scheme, given the encoding scheme, maximizes the probability that Alice and Bob find the same bit value.

5.3.2 Protocol

Now we explained which non-orthogonal quantum states are used in GP00 and the bit extraction strategy is studied, we can describe the protocol. Before we describe the complete protocol we give a brief description of the protocol in which we explain some important steps.

Alice prepares $(4+\delta)n$ squeezed states, where $\delta > 0$ and $n \in \mathbb{N}$, and chooses to squeeze in x or in p at random. She samples $\langle x \rangle$ or $\langle p \rangle$ from a Gaussian distribution centered at the origin. If the expectation is an element of $\mathcal{L}_0$ then she extracts bit value 0, otherwise, she extract bit value 1. Alice finds bit string X''. Alice then sends the squeezed states to Bob who measures them in the x- or the p-basis at random.
In Corollary 4.4.3 we saw that the expectations and the variances of x and p of a squeezed state at time $t = 2k\pi$ where $k \in \mathbb{N}$ are equal to these properties at time $t = 0$. From now on we assume that Alice and Bob have a mutual clock and that Alice sends a state at time $t = 0$ and Bob measures the state at time $t = 2k\pi$ where $k \in \mathbb{N}$.

Eve cannot clone the squeezed states sent by Alice (see Theorem 4.3.3) and therefore, after Bob received the squeezed states, Alice and Bob are perfectly safe to announce which bases they used. Theorem 5.3.1 tells us that if Alice and Bob used the same basis then, given that there is no eavesdropper, the extracted bit values from Alice and Bob have high probability to be the same. On the positions where they used a different basis, then the bit value Bob extracts is random. This means that Alice and Bob can discard the bits where they used a different basis.
Alice announces the values ϕ_x or ϕ_p of the squeezed states she sent such that Bob can extract bit values from the measurements he made. Alice can announce these values because they do not give any information about $\langle x \rangle$ or $\langle p \rangle$ with respect to the extracted bit values.

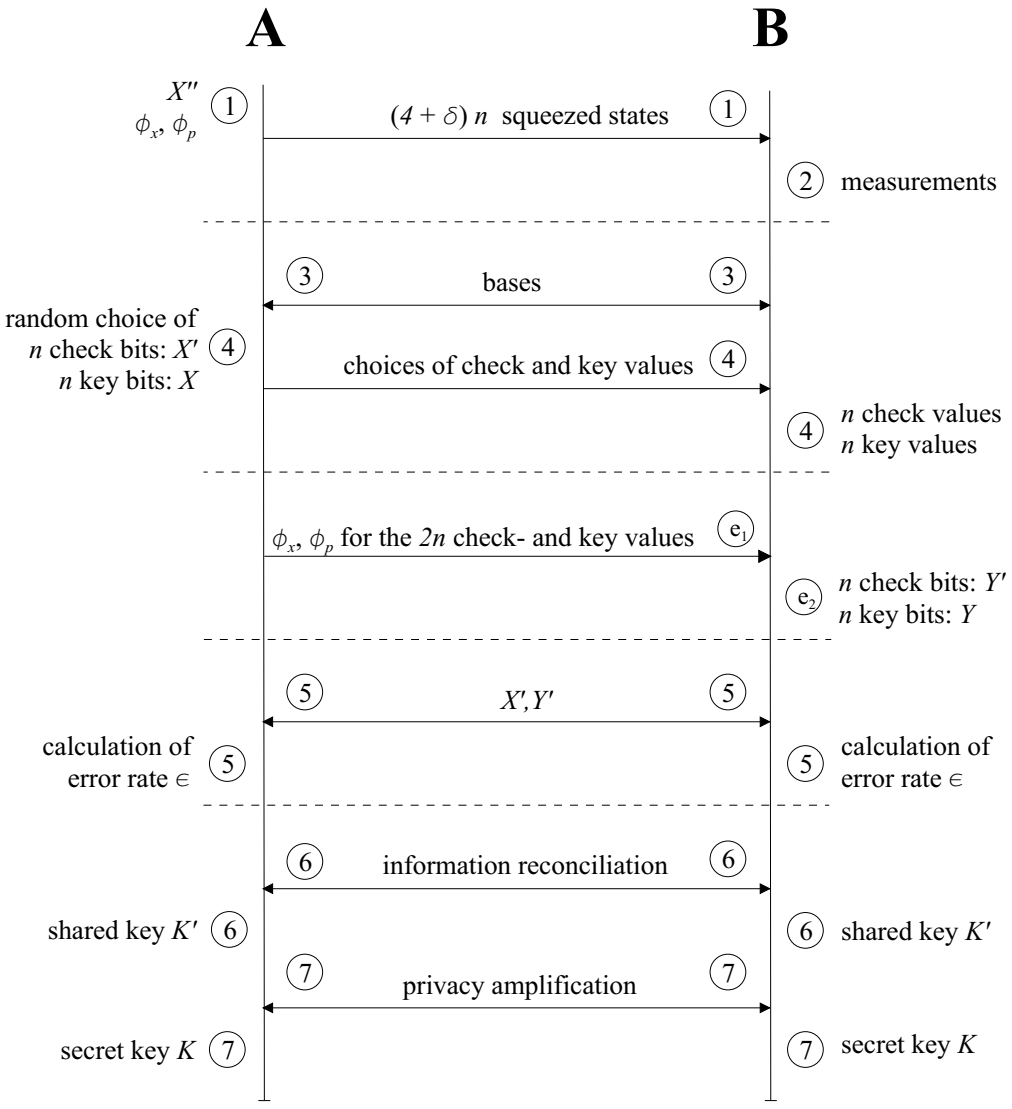
Next, if the number of positions where Alice and Bob used the same basis is at least $2n$, then Alice chooses from the corresponding bits n check bits (X') and n key bits (X). Alice announces the choice of these bits so that Bob can determine his check bit string (Y') and his key bit string (Y). Then Alice and Bob announce their check bits X', Y' such that they can estimate the bit error rate ϵ. Bit errors are introduced by the channel and by Eve who introduces disturbance in the system by trying to distinguish between the non-orthogonal states. Bit errors are also introduced by the squeezed states themselves because the states are not infinitely squeezed. For example, if there is no eavesdropper, then the bit error probability is equal to $0 < \epsilon_s < \frac{1}{2}$, as defined in the previous section.
There are methods to find a threshold for the error rate ϵ. In [23] it is proved that if $\epsilon < 0.11$ and $\hat{r} > 0.289$ then GP00 is secure (as an illustration; if $\hat{r} = 0.289$ then $1 - \epsilon_s = 0.906$). In Chapter 7 we will study thresholds on the error rate for different squeezing parameters $\hat{r}$.

In our implementation of BB84, Alice uses half of the positions where they used the same basis as check bits. There are alternative methods, studied for example in [16], where Alice uses less bits for check bits. This might lead to a better rate but we will not explore that case, we will focuss on the case presented.

The reason that Alice starts with a bit string of length $(4+\delta)n$ is the same as in BB84. How to choose δ such that the probability that Alice and Bob have at least $2n$ values where

they used the same basis is discussed in Appendix C.

The scheme below displays the actions in the protocol of Alice and Bob. We see that $X'', X, \langle x \rangle, \langle p \rangle$ and the squeezed states Alice sends are secret and only known by Alice. The bit string Y is secret and only known by Bob. The strings K, K' are secret and known by Alice and Bob. The check bit strings X', Y' are public and after Bob has measured all squeezed states, the bases Alice and Bob used for all squeezed states are public as well. The values ϕ_x, ϕ_p are public as well.



The protocol described step by step.

Distribution & Measurements

1. Alice prepares $(4 + \delta)n$ minimum uncertainty squeezed states, where $\delta > 0$. For each squeezed state Alice decides at random to squeeze in either x or in p. If Alice squeezes

in x, then she samples $\langle x \rangle$ from the probability distribution $P_{\text{pos}}(\langle x \rangle)$ and chooses $\langle p \rangle = \langle x \rangle + (k + \frac{1}{2})\sqrt{\pi\hbar}$, for some $k \in \mathbb{Z}$. If Alice squeezes in p, then she samples $\langle p \rangle$ from the probability distribution $P_{\text{mom}}(\langle p \rangle)$ and chooses $\langle x \rangle = \langle p \rangle + (k + \frac{1}{2})\sqrt{\pi\hbar}$, for some $k \in \mathbb{Z}$. If $\langle x \rangle$ or $\langle p \rangle \in \mathcal{L}_0$ Alice extracts bit value 0, if $\langle x \rangle$ or $\langle p \rangle \in \mathcal{L}_1$ Alice extracts bit value 1. This results in a bit string X'' of length $(4 + \delta)n$.

2. Bob receives the $(4 + \delta)n$ squeezed states and measures each of them in the x or p-basis at random.

Bases Comparison & Determination of Check- and Key Values

3. Bob confirms having received the squeezed states. Alice announces whether each squeezed state was squeezed in x or p. Also Bob announces whether he measured each squeezed state in the x or in the p-basis.

4. Alice and Bob discard the results in the cases where Alice squeezed and Bob measured the squeezed states in a different basis. If there are less than $2n$ values left, they abort the protocol. Alice decides randomly on a set of $2n$ values to use for the protocol and chooses at random n of these to be check values to check the interference of Eve. The other n values are key values. Alice announces these choices. Alice now has check bit string X' and a key bit string X both of length n.

Key Extraction

e1. For all $2n$ values left, Alice announces the value ϕ_x if she squeezed the corresponding squeezed state in the x-basis. She announces ϕ_p if she squeezed the squeezed state in the pa basis.

e2. Bob subtracts the corresponding value announced by Alice from each of his measured values, and then corrects the result to the nearest integer multiple of $\sqrt{\pi\hbar}$. If this nearest multiple is even, then Bob extract bit value 0, otherwise he extracts bit value 1. Bob now has a check bit string Y' and a key bit string Y both of length n.

Determination of error rate

5. Alice and Bob announce X' and Y' and determine the error rate ϵ by comparing the values of their check bits. If ϵ is greater than a certain threshold, the Alice and Bob abort the protocol. If this is not the case, they know that Eve's interference is negligible.

Information Reconciliation & Privacy Amplification

6. Alice and Bob now have highly correlated key bit strings X and Y that can be made identical with high probability by a procedure called information reconciliation. For this Alice sends $H(X|Y) = nh(\epsilon)$ bits to Bob. With error correction Alice and Bob retrieve an equal bit string K' with high probability. We will not give further details about how the information reconciliation works because this is outside the scope of this thesis. For more information we refer to [15, 16].

7. Alice and Bob now have the same bit string but it is still possible that Eve has partial information about these bits. To eliminate this partial information Alice and Bob apply privacy amplification to their bit strings K'. The resulting $m < n$-bit string K is used as the secret key. We will not give further details about how the privacy amplification works because this is outside the scope of this thesis. For more information we refer to [17, 18].

5.3.3 Possible attacks by Eve

We assume that Alice and Bob both encoded and measured in the same basis, because they discard the bits for which this is not the case.

In Section 4.4 we found that at time $t = 2k\pi$ where $k \in \mathbb{N}$ the statistical properties of a squeezed state are equal to the initial state. This means that Alice and Bob always measure squeezed states at these moments. Is it for Eve beneficial to measure the squeezed state at other moments? In Corollary 4.4.3 we found that if Alice squeezes in the x-basis then

$$\sigma_{x,t}^2 \geq \sigma_{x,0}^2$$

and if Alice squeezes in the p-basis then

$$\sigma_{p,t}^2 \geq \sigma_{p,0}^2$$

with equality for $t = 2k\pi$. This, together with the fact that the expectation of the squeezed state changes during time, gives us that the probability that Eve finds the correct bit value is maximized when she measures at time instances $t = 2k\pi$. From now on we assume that Eve measures at time instances $t = 2k\pi$.

Just like in Section 5.2.3 Eve's goal in GP00 is to act in such a way that the probability that Alice and Bob find the same bit is maximized whereas Eve also maximizes the probability that she herself finds the correct bit. Eve cannot copy the squeezed state and therefore the only thing she can do is to intercept the state, measure it in some basis and send a state to Bob. Eve also intercepts the values ϕ_x, ϕ_p to be able to extract the bit values. We discuss some strategies.

Eve measures in the x- or p-basis

In this scenario Eve measures the squeezed state received from Alice in the x or p-basis and sends a state to Bob. We will see that the probability that Alice and Bob find the same bit is maximized when Eve sends the state produced by the measurement to Bob. This maximum probability is $\frac{3}{4} - \frac{\epsilon_s}{2}$ and equals the probability that Eve finds the correct bit value (in the BB84 case this was $\frac{3}{4}$).

Let $|\psi\rangle$ be the state sent by Alice. This is a squeezed state squeezed in x or p, squeezed with a fixed squeezing parameter $\hat{r} > 0$ or $-\hat{r}$. Let $\langle x \rangle_A$ and $\langle p \rangle_A$ be the expectation of respectively x an p of the squeezed state sent by Alice. The squeezed state sent by Alice has the variance $\sigma_A^2 = \frac{\hbar}{2} e^{-2\hat{r}}$ in the variable where the state is squeezed in. Let x_E, p_E and x_B, p_B be the respective x or p value measured by respectively Eve and Bob.

Eve sends the state produced by her measurement to Bob
First, we assume that Eve sends the state produced by her measurement to Bob. There are two possibilities;

- With probability $\frac{1}{2}$ Eve measures $|\psi\rangle$ in the correct basis. Suppose that this is the x-basis. As we saw in Theorem 5.3.1, Eve finds the correct bit value with probability $1-\epsilon_s$. The state produced by the measurement in the x-basis is the x eigenstate $|x_E\rangle$. Eve sends $|x_E\rangle$ to Bob who measures it in the x-basis as well. With probability 1, Bob will measure position value x_E. This is because

$$|\langle x_E|x_E\rangle|^2 = 1.$$

  This gives us that the probability that Bob will find the correct bit value is $1-\epsilon_s$. If the correct basis is the p- basis the calculations and the results are the same.

- With probability $\frac{1}{2}$ Eve measures $|\psi\rangle$ in the incorrect basis. Suppose that this is the p-basis. As we saw in Theorem 5.3.1, Eve finds the correct bit value with probability $\frac{1}{2}$. The state produced by the measurement in the p-basis is the p eigenstate $|p_E\rangle$. Eve sends $|p_E\rangle$ to Bob who measures it in the correct basis, the x-basis. In Section 5.3.1 we saw that if an p-eigenstate is measured in the x-basis then each possible position value is equally likely to be measured. Bob measures the correct bit value when $x_B - \langle x\rangle_A \in \mathcal{C}$. Because every x-value is equally likely to be measured this probability becomes $\frac{1}{2}$. If the incorrect basis is the x- basis the calculations and the results are the same.

The average probability that Alice and Bob extract the same bit value in this scenario is $\frac{1}{2}\cdot(1-\epsilon_s)+\frac{1}{2}\cdot\frac{1}{2} = \frac{3}{4}-\frac{\epsilon_s}{2}$. Eve finds the correct bit value with the same probability.

Eve sends a different state than the one produced by her measurement to Bob
Suppose now that Eve measures the squeezed state received from Alice and sends a squeezed state to Bob. Suppose she fixes her squeezing parameter at the value $\hat{r}_E > 0$ for squeezing in p and $-\hat{r}_E$ for squeezing in x. Eve uses the following strategy;

- If she measures in the x-basis she sends to Bob the squeezed state $|-\hat{r}_E, \alpha\rangle$ with $\langle x\rangle_E = x_E$ and $\sigma_E^2 = \frac{\hbar}{2}e^{-2\hat{r}_E}$.

- If she measures in the p-basis she sends to Bob the squeezed state $|\hat{r}_E, \alpha\rangle$ with $\langle p\rangle_E = p_E$ and $\sigma_E^2 = \frac{\hbar}{2}e^{-2\hat{r}_E}$.

Suppose that Alice and Bob used the same basis. If Eve applies the just described strategy then we have the following two scenarios.

- With probability $\frac{1}{2}$ Eve measures $|\psi\rangle$ in the correct basis. Suppose that this is the x-basis. Eve finds the correct bit value with probability $1-\epsilon_s$. Eve sends $|-\hat{r}_E, \alpha\rangle$ with $\langle x\rangle_E = x_E$ to Bob who measures it in the x-basis. We will show why the probability that Bob measures the correct bit value is less than $1-\epsilon_s$.

  The position value x_B measured by Bob has a Gaussian distribution with mean x_E and standard deviation σ_E^2. Here x_E has a Gaussian distribution with mean $\langle x\rangle_A$ and

standard deviation σ_A^2. In Appendix E it is proved that then the probability distribution for x_B is a Gaussian distribution with mean $\langle x \rangle_A$ and variance $\sigma_A^2 + \sigma_E^2 > \sigma_A^2$. This means that the probability distribution for x_B is less peaked (less squeezed) and therefore the probability that Alice and Bob find the same bit is $P(x_B - \langle x \rangle_A \in \mathcal{C}) < 1 - \epsilon_s$.

The calculations for when the correct basis is the p-basis are the same.

- With probability $\frac{1}{2}$ Eve measures $|\psi\rangle$ in the incorrect basis. Suppose that this is the p-basis and Eve measures momentum value p_E. Eve finds the correct bit value with probability $\frac{1}{2}$. Eve sends $|\hat{r}_E, \alpha\rangle$ with $\langle p \rangle_E = p_E$ to Bob who measures it in the correct basis, the x-basis. Eve has no knowledge about the value $\langle x \rangle_A$ and therefore, the expectation $\langle x \rangle_E$ of Eve's squeezed state has no relation with $\langle x \rangle_A$. Therefore, the positions where $x_B - \langle x \rangle_A \in \mathcal{C}$ are placed randomly on the probability distribution for x_B. This means that, on average, the probability that Bob finds the correct bit value is $\frac{1}{2}$.

  If the correct basis was the x-basis, the calculations are similar.

The average probability that Alice and Bob extract the same bit value in this scenario is smaller than $P < \frac{1}{2} \cdot (1 - \epsilon_s) + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4} - \frac{\epsilon_s}{2}$. Eve finds the correct bit value with probability $\frac{3}{4} - \frac{\epsilon_s}{2}$.

We see that, given that Eve measures in the x or p-basis, the probability that Alice and Bob find the same bit is maximized in the first scenario; Eve sends the state produced by her measurement to Bob.

In BB84, we studied the case where Eve measured in a different basis. In the squeezed state case there is no similar scenario known that maximizes the probability that Eve finds the correct bit value. Because the number of basis states of the x-basis and the p-basis is infinite, it is much harder to find a basis where the bit error rate is minimized than in the BB84 protocol where there are only 4 basis states.

5.3.4 Capacity of GP00

Just like in the $BB84$ case we can model the bit transmission of the quantum channel as a superposition of two classical channels. In this way the bit probability distribution is a superposition of two bit probability distributions;

1. With probability $\frac{1}{2}$ Bob measures in the correct basis (the basis Alice squeezed the state in). With probability $\frac{1}{2} < 1 - \epsilon_s < 1$ he will extract the correct bit. The classical channel that corresponds to this probability distribution is visualized in Figure 5.6. We see that because of the properties of squeezed states noise is introduced. The channel is a binary symmetric channel and thus the capacity is $1 - h(\epsilon_s)$.

2. With probability $\frac{1}{2}$ Bob measures in the incorrect basis and then the extracted bit will be random. The classical channel that corresponds to this probability distribution is visualized in Figure 5.7. This is a binary symmetric channel and thus the capacity is $1 - h(\frac{1}{2}) = 0$.

We see that even if Alice and Bob squeezed and measured in the same basis, there is noise in the channel because of the properties of a squeezed state. The magnitude of the noise, for a

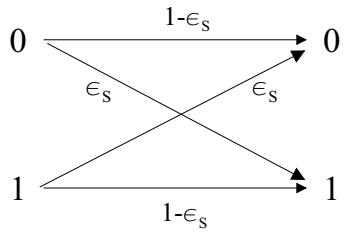


Figure 5.6: Correct basis

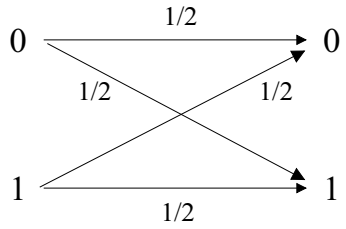


Figure 5.7: Correct basis

given squeezing parameter r depends on the chosen bit extraction strategy.

For a fixed squeezing parameter r and therefore a fixed probability $1 - \epsilon_s$ the capacity of the squeezed state distribution protocol is

$$C_{SS} = \frac{1}{2} \cdot (1 - h(\epsilon_s)) + \frac{1}{2} \cdot 0 = \frac{1}{2} - \frac{h(\epsilon_s)}{2}.$$

We see that

$$\lim_{1-\epsilon_{s1} \uparrow 1} \frac{1 - h(\epsilon_s)}{2} = \frac{1}{2}$$

so that the maximum rate of GP00 can approach the maximum rate of BB84.

Chapter 6

Bit Extraction Strategies and Further Ideas with respect to GP00

The bit extraction strategy used in a protocol is determined by the bit encoding and decoding scheme. The bit extraction strategy that is chosen for a protocol influences the bit error probability of a protocol and therefore also the capacity.

In Section 6.1 we will study the bit extraction strategy used in GP00. In Section 6.2 we note a different bit extraction strategy of which we did not analyse the security aspects. However, it results in a smaller bit error probability than the bit error probability corresponding to the bit extraction strategy used in GP00.

In GP00, Bob's measurement gives a continuous outcome. It is possible to use this continuous spectrum in such a way that more than one bit can be extracted from each squeezed state. In Section 6.3 we will study a possible m-bit extraction strategy, which, if it is secure, will be much more beneficial for Alice and Bob because the capacity will be much higher i.e. there are less squeezed states needed to make a secret key of the same length.

In the following sections we suppose that Alice and Bob use the x-basis. The case where they both used the p-basis follows the same line of reasoning.

6.1 Bit extraction strategy GP00

In Section 5.3.1 the bit extraction strategy of GP00 is explained; the value $\phi_x = \langle x \rangle \bmod \sqrt{\pi\hbar}$ plays a crucial role. Whether Alice encodes bit value 0 or 1 depends on whether $\langle x \rangle - \phi_x$ is an even or odd integer multiple of $\sqrt{\pi\hbar}$, or, equivalently, whether $\langle x \rangle$ is in $\mathcal{L}_0$ or $\mathcal{L}_1$. Bob decodes to bit value 0 or 1 when $x_B - \phi_x$ rounded to the nearest integer multiple is even or odd, or, equivalently, whether $x_B - \langle x \rangle \in \mathcal{C}$. We found that the (bit transmission) capacity of GP00 is given by

$$C_{SS} = \frac{1}{2} - \frac{h(\epsilon_s)}{2}$$

where ϵ_s is a function of $\hat{r}$ and is the bit error probability of GP00 defined by

$$\epsilon_s = 1 - \int_{x-\langle x \rangle \in \mathcal{C}} P_X^{|-\hat{r},\alpha\rangle}(x)dx = 1 - \int_{p-\langle p \rangle \in \mathcal{C}} P_P^{|\hat{r},\alpha\rangle}(p)dp.$$

An important question is why Gottesman and Preskill choose for the particular value $\sqrt{\pi\hbar}$? Before we get into detail about this question we will note about something that relates to this question.

In [23], the protocol works with the number $\sqrt{\pi}$ instead of $\sqrt{\pi\hbar}$. In physics it often happens that constants are set to 1 to make calculations easier. Also in the protocol described by Gottesman and Preskill they do this and they set $\hbar = 1$. I did not do this because first, I wanted to make my calculations as general as possible and second, it gave me an extra opportunity to verify the correctness of some of my calculations by substituting $\hbar = 1$ and checking if they were equal to calculations made by others.
The variances of a minimum uncertainty squeezed state are $\sigma_x^2 = \frac{\hbar}{2}e^{2r}$ and $\sigma_p^2 = \frac{\hbar}{2}e^{-2r}$. Gottesman and Preskill however assumed that the variances were $\sigma_{x,GP}^2 = \frac{1}{2}e^{2r}$ and $\sigma_{p,GP}^2 = \frac{1}{2}e^{-2r}$. We have that $\sigma_{x,GP}^2 = \frac{\sigma_x^2}{\hbar}$ and $\sigma_{p,GP}^2 = \frac{\sigma_p^2}{\hbar}$. For the exponent in the Gaussian distribution for measuring x it holds that

$$\exp\left(\frac{-(x-\mu)^2}{2\sigma_{x,GP}^2}\right) = \exp\left(\frac{-\hbar(x-\mu)^2}{2\sigma_x^2}\right) = \exp\left(\frac{-(\sqrt{\hbar}x - \sqrt{\hbar}\mu)^2}{2\sigma_x^2}\right).$$

This gives us that in the Gottesman and Preskill protocol ($\hbar = 1$) the probability to measure a certain x value, given a certain mean value $\langle x\rangle$, is equal to the probability to measure the value $x\sqrt{\hbar}$, given the mean value $\langle x\rangle\sqrt{\hbar}$, if we do not set $\hbar = 1$ in the calculations with squeezed states. The two implementations of the squeezed state protocol ($\hbar = 1$ and $\hbar = \hbar$) are equivalent if all the values of the bit encoding intervals and the bit decoding interval are multiplied by $\sqrt{\hbar}$. This gives us our bit encoding intervals $\mathcal{L}_0$ and $\mathcal{L}_1$ and the bit decoding interval $\mathcal{C}$. It means that $\phi_x = \langle x\rangle \bmod \sqrt{\pi\hbar}$ instead of $\phi_x = \langle x\rangle \bmod \sqrt{\pi}$. By doing this, in both implementations the bit error probability is equal to ϵ_s given that Alice and Bob measured in the same basis.

With this argumentation, the choice of the original value $\sqrt{\pi\hbar}$ becomes rather random; an implementation of a squeezed state protocol is equivalent to the original ($\sqrt{\pi\hbar}$) if the bit error probability in the case that Alice and Bob use the same basis is equal to ϵ_s. To reach that the bit error probability stays the same for different values than $\sqrt{\pi\hbar}$ the squeezing parameter should be adapted. The adapted squeezing parameter can be written as a function of $\hat{r}$. Then, if $\hat{r}$ is chosen in such a way that the original implementation of the protocol is secure, then also the alternative implementations are secure. We show how to this in the following example.

Example 6.1.1 *Suppose we choose $\phi_x = \langle x\rangle \bmod y$ with $y > 0$. The encoding intervals change into*

$$\mathcal{L}_0 = \{\ldots, [-2y, -y), [0, y), [2y, 3y), \ldots\}$$

and

$$\mathcal{L}_1 = \{\ldots, [-y, 0), [y, 2y), [3y, 4y), \ldots\}.$$

The decoding interval changes into

$$\mathcal{C} = \{\ldots, \left[-\frac{5}{2}y, -\frac{3}{2}y\right), \left[-\frac{1}{2}y, \frac{1}{2}y\right), \left[\frac{3}{2}y, \frac{5}{2}y\right), \ldots\}.$$

We want the bit error probability of this implementation of the squeezed state protocol be the same as the original. Let $y = c^2\sqrt{\pi\hbar}$ with $c > 0$. Let $\sigma_x^2 = \frac{\hbar}{2}e^{2r} = \frac{\hbar}{2}e^{-2\hat{r}}$ be the variance of a squeezed state in the original protocol. We find

$$\begin{aligned}\exp\left(\frac{-(x-\mu)^2}{2\sigma_x^2}\right) &= \exp\left(\frac{-c^2(x-\mu)^2}{2c^2\sigma_x^2}\right)\\ &= \exp\left(\frac{-(cx-c\mu)^2}{2(c\sigma_x)^2}\right).\end{aligned}$$

We see that if we choose $\phi_x = \langle x\rangle \bmod y$ and change the encoding and decoding intervals then the protocol is equivalent if the variance is equal to $(c\sigma_x)^2 = \frac{c^2\hbar}{2}e^{2r}$. We have

$$\begin{aligned}\frac{c^2\hbar}{2}e^{2r} &= \frac{\hbar}{2}e^{2r}e^{\ln c^2}\\ &= \frac{\hbar}{2}e^{2(r+\ln c)}.\end{aligned}$$

This means that in order that this implementation is equivalent to the original we have to choose squeezing parameter $r + \ln c$. If Alice squeezes in x so $r = -\hat{r}$ in the original protocol then the squeezing parameter in this alternative protocol becomes $-\hat{r}+\ln c$. Similar calculations in the p-basis show that for squeezing in p the squeezing parameter becomes $\hat{r} - \ln c$.

From the example we may conclude that if $y > \sqrt{\pi\hbar}$ then less squeezing is needed and if $y < \sqrt{\pi\hbar}$ more squeezing is needed. It has to hold however that the squeezing parameter $\hat{r} - \ln c > 0$.

The choice for the value $\sqrt{\pi\hbar}$ was not completely random however. In [23] Gottesman and Preskill derive the (security of the) squeezed state protocol from a so-called stabilizer code where the allowed values of x and p are integer multiples of $\sqrt{\pi}$. In the squeezed state protocol they did not change this value.

6.2 Proposal alternative bit extraction strategy

There might be other bit extraction strategies than the one used in GP00 that, for the same choice $\hat{r}$ of the squeezing parameter result in a lower bit error probability ϵ_s'. A bit extraction strategy that has a different approach is the following. We set $\delta > 0$.

Bit encoding
Alice decides at random to squeeze a state in either x or in p. The mean value $\langle x\rangle$ or $\langle p\rangle$ of the squeezed state is determined by sampling $P_{\text{pos}}(\langle x\rangle)$ or $P_{\text{mom}}(\langle p\rangle)$. If $\langle x\rangle > \delta$ or $\langle p\rangle > \delta$ Alice extracts bit value 0, if $\langle x\rangle < -\delta$ or $\langle p\rangle < -\delta$ Alice extracts bit value 1. She discards the samples where $|\langle x\rangle| \leq \delta$ or $|\langle p\rangle| \leq \delta$.

Recall that a squeezed state is represented as $|r, \alpha\rangle$ with $\alpha = se^{i\theta}$. For every squeezed state, Alice chooses θ random. Then, if the squeezed state is measured in the incorrect basis, a random bit will be extracted.

This means we split $\mathbb{R}$ into two intervals; the positive numbers and the negative numbers. We

take $\delta > 0$ because it gives us a security marge. Suppose namely that $\delta = 0$. Alice can then send the squeezed state with $\langle x \rangle = 0$. If Bob receives this state and measures in the x-basis he will find a random bit value.

Bit decoding
The decoding scheme is much simpler than in the Gottesman and Preskill version. If Bob measures a value x or p smaller than 0 he extracts bit value 0 otherwise bit value 1.

Bit probability distribution
Suppose that $\delta > \frac{1}{2}\sqrt{\pi\hbar}$. We choose the same squeezing parameter $\hat{r}$ as in the Gottesman and Preskill protocol. Let the bit error probability of this alternative bit extraction method be ϵ_s'. It then holds that

$$\epsilon_s' << \epsilon_s$$

and thus the capacity is better. Suppose namely that Alice sends a squeezed state with $|\langle x \rangle| = \delta$. The probability that Bob finds the incorrect bit value is smaller than ϵ_s because $\delta > \frac{1}{2}\sqrt{\pi\hbar}$ and therefore

$$\begin{aligned} P_{error}(|\langle x \rangle| = \delta) &= \int_{-\infty}^{0} P_X^{|-\hat{r},\alpha\rangle}(x)dx \\ &< \int_{x-\langle x \rangle \in \mathbb{C}} P_X^{|-\hat{r},\alpha\rangle}(x)dx = \epsilon_s. \end{aligned}$$

If Alice sends a squeezed state with absolute mean value even further from the origin then the bit error probability becomes even smaller. This means that the average bit error probability ϵ_s' is much smaller than ϵ_s.

We see that with this bit extraction strategy less squeezing is needed to reach the same capacity. It seems that Eve is not better off than in the original bit extraction strategy, but we did not do a full security analysis so perhaps we overlook something. With the original strategy there are more possibilities to use the beneficial properties of the continuous x and p spectrum of the squeezed states. We will see this in the next section.

6.3 Proposal for sending m bits per squeezed state

We propose a bit extraction strategy for which m bits per sent squeezed state can be extracted. It is only a proposal, we do not analyze the security. Presumably, if we can prove the security of GP00 with the method described in Chapter 7, then we can also prove the security of the protocol proposed with the method.

We continue with Gottesman and Preskill's strategy and instead of dividing the real numbers into 2^1 subsets, we divide it into 2^m subsets. The notation stays the same. Let $\phi_x = \langle x \rangle \bmod \sqrt{\pi\hbar}$, $\phi_p = \langle p \rangle \bmod \sqrt{\pi\hbar}$. Then the mean values can be written as $\langle x \rangle = \phi_x + n_x\sqrt{\pi\hbar}$ and $\langle p \rangle = \phi_p + n_p\sqrt{\pi\hbar}$ where $n_x, n_p \in \mathbb{N}$.

Bit encoding scheme

Suppose Alice wants to encode a bit string $\underline{b}_i$ of length m. A bit encoding strategy is.

$\underline{b}$	squeezing in x	squeezing in p
$0\ldots0$	$\lvert-\hat{r},\alpha\rangle$ with $n_x = 0 \bmod 2^m$	$\lvert\hat{r},\alpha\rangle$ with $n_p = 0 \bmod 2^m$
$0\ldots1$	$\lvert-\hat{r},\alpha\rangle$ with $n_x = 1 \bmod 2^m$	$\lvert\hat{r},\alpha\rangle$ with $n_p = 1 \bmod 2^m$
$\vdots$	$\vdots$	$\vdots$
$1\ldots1$	$\lvert-\hat{r},\alpha\rangle$ with $n_x = (2^m-1) \bmod 2^m$	$\lvert\hat{r},\alpha\rangle$ with $n_p = (2^m-1) \bmod 2^m$

If $n_x = i \bmod \sqrt{\pi\hbar}$ this corresponds with a value $\langle x\rangle$ that is in the interval $\mathcal{L}_i$ where $\mathcal{L}_i$ is defined as

$$\mathcal{L}_i = \{\ldots, \left[i\sqrt{\pi\hbar}, (i+1)\sqrt{\pi\hbar}\right), \left[(2^m+i)\sqrt{\pi\hbar}, (2^m+i+1)\sqrt{\pi\hbar}\right), \ldots\}.$$

The values $\langle x\rangle$ and $\langle p\rangle$ and therefore also the bit strings $\underline{b}_i$ are determined by Alice by sampling a certain probability distribution. This probability distribution gives a value in $\mathcal{L}_i$ with probability $\frac{1}{2^m}$ so that the extracted bit string is random.

Bit decoding scheme
Suppose that the squeezed state was squeezed in x. The state is measured in x or p with outcome z. We have that

$$z - \phi_x \quad = \quad \left(\frac{z-\langle x\rangle}{\sqrt{\pi\hbar}} + n_x\right)\sqrt{\pi\hbar}.$$

Depending on the value of $\left(\frac{z-\langle x\rangle}{\sqrt{\pi\hbar}} + n_x\right)$ rounded to the nearest integer multiple, Bob extracts a certain m-bit string. If $\left(\frac{z-\langle x\rangle}{\sqrt{\pi\hbar}} + n_x\right)$ rounded to the nearest integer and then modulo 2^m is the same as $n_x \bmod 2^m$ then the correct bit string is extracted. This is when

$$z - \langle x\rangle \in \mathcal{C} = \{\ldots, \left[-\frac{1}{2}\sqrt{\pi\hbar}, \frac{1}{2}\sqrt{\pi\hbar}\right), \left[\left(2^m - \frac{1}{2}\right)\sqrt{\pi\hbar}, \left(2^m - \frac{1}{2}\right)\sqrt{\pi\hbar}\right), \ldots\}.$$

If the state was squeezed in p then Bob finds the correct bit string when $z - \langle p\rangle \in \mathcal{C}$.

Bit string probabilities
Suppose that Alice encoded bit string $\underline{b}_i$ as a squeezed state squeezed in x. If Bob measures in the correct basis then the probability distribution is peaked at the position value $\langle x\rangle$ that corresponds to bit string $\underline{b}_i$. Bob will find the correct bit string with high probability, but Bob can also measure a value that corresponds to other bit strings. These probabilities are

$$\epsilon_{(j-i) \bmod 2^m} = P(\underline{b}_j) \quad = \quad P(\left(x_B - \langle x\rangle - ((j-i) \bmod 2^m)\sqrt{\pi\hbar}\right) \in \mathcal{C})$$

for $j \in \{0, 1, \ldots, 2^m - 1\}$. We see that the greater the value $(j-i) \bmod 2^m$ the smaller the probability that bit string $\underline{b}_j$ is measured. In general, ϵ_0 is the probability that the correct bit string $\underline{b}_i$ is found, ϵ_1 the probability that bit string $\underline{b}_{i+1}$ is found, ϵ_{-1} the probability that bit string $\underline{b}_{i-1}$ is found etcetera.

Suppose on the other hand that Bob measures in the incorrect basis. If the values $\langle x\rangle$ and

$\langle p \rangle$ are independent then the area where $\left(x_B - \langle x \rangle - ((j-i) \bmod 2^m)\sqrt{\pi\hbar}\right) \in \mathcal{C}$ is placed randomly on the probability distribution for measuring p. This means that on average the probability that Bob extracts a certain bit string is equal to $\frac{1}{2^m}$.

Capacity
Just like in the calculation of the capacity of BB84 and GP00 we can calculate the capacity of this m-bit squeezed state protocol by modelling the bit transition channel of the quantum channel as a superposition of two classical channels. Once Bob has chosen which basis to use, the channel is determined. In Appendix D we found that the capacity of an m-bit symmetric channel is given by

$$C_{mSC} = m + \sum_{y \in Y} p(y|x_0) \log p(y|x_0).$$

- With probability $\frac{1}{2}$ Bob measures in the correct basis. The possible bit strings are extracted with probabilities $\epsilon_0, \ldots, \epsilon_{2^m-1}$. The capacity of this channel is

$$m + \sum_{i=0}^{2^m-1} \epsilon_i \log \epsilon_i.$$

- With probability $\frac{1}{2}$ Bob measures in the incorrect basis. All possibly extracted bit strings are equally likely and thus the capacity of this channel is

$$m + \log\left(\frac{1}{2^m}\right) = 0.$$

This gives us that the total capacity is

$$C_{mGP00} = \frac{m}{2} + \frac{1}{2} \sum_{i=0}^{2^m-1} \epsilon_i \log \epsilon_i < \frac{m}{2}.$$

We see that if $\hat{r} \uparrow \infty$ then $\epsilon_0 \uparrow 1$ and $C_{mGP00} \uparrow \frac{m}{2}$.

Chapter 7

Generic Security Proof for Quantum Key Exchange

7.1 Introduction to generic security proof protocol

As we mentioned in Chapter 2 and Chapter 5, quantum key exchange protocols can be proven to be perfectly secure because the security of the protocols relies on the fundamental principles of quantum mechanics rather than lack of computational power.

However, known security proofs of quantum key exchange protocols are non trivial and are usually restricted in their applicability to specific protocols. In [24], a general method is given to prove the security of a quantum key exchange protocol. This method can be applied to a number of different protocols. The presented method relies on a fact discussed in the following paragraph. Let X and Y denote the key bit string belonging to respectively Alice and Bob before information reconciliation such that they both have a shared key bit string K' after information reconciliation.

Every quantum key exchange protocol uses either classical or quantum privacy amplification to guarantee the security of the secret key distilled from the protocol. To be able to apply privacy amplification to the shared key bit string K', an upper bound on Eve's knowledge about this key string has to be determined. In Chapter 5 we supposed that Eve's upper bound for the amount of information about X is $H(Y|X)$ bits (sent during information reconciliation) plus t quantum bits of information. Information gained from classical information is never more than the information gained from quantum information and therefore we can say that Eve has no more than $H(Y|X) + t$ qubits of information about X.
From the results presented in [25] it can be deduced that classical privacy amplification can be extended to the case where Eve's information about the secret key is quantum rather than classical. No matter which observable Eve measures after the classical privacy amplification, she is no better off than she would be if she had $H(Y|X) + t$ classical bits of information before the privacy amplification. The method presented in [24] is based on this fact and helps them to find an upper bound for t.

In this chapter, our goal is to give a direct proof of security of GP00 using the method presented in [24]. In [24], a generic key exchange protocol is presented that represents all

protocols for which the method of the proof of security can be applied. We simplify this generic protocol into a reduced generic protocol such that both BB84 and GP00 are instances of this protocol. The method presented in [24] however does not immediately apply to the infinite case (GP00).

In Section 7.2 we give the reduced generic key distribution protocol and summarize the method presented in [24]. In Section 7.3 we show how to apply the method to BB84 and in Section 7.4 we apply the method to GP00.

7.2 Description of generic security proof protocol

We make the following assumptions about the players of the protocol.

Eve

- Eve can distribute quantum states to Alice and Bob and entangle the states with an ancilla that she controls. This ancilla is an "assistent" quantum state that can reveal information to Eve about Alice's and Bob's information.
- Eve has access to unlimited quantum computational power.
- Eve can monitor all the public communication between Alice and Bob.

Alice and Bob

- Alice and Bob can only perform measurements on individual quantum states.
- They can communicate classically over a authenticated public channel.

In key exchange protocols Alice distributes the quantum states over a quantum channel. For the security analysis of key exchange protocols however, we assume that it is rather Eve than Alice who distributes the quantum states to Alice and Bob. Eve starts with an entangled composite system describing the states sent to Alice, to Bob and the ancilla which is kept by Eve.

First we characterize some quantum key exchange protocols for which the method holds by giving a reduced generic key exchange protocol.

7.2.1 A reduced generic key exchange protocol

Eve distributes k quantum states to Alice and Bob where $k \in \mathbb{N}$.

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be Hilbert spaces. Let ρ be a density operator on $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes k}$. That means that each of the k quantum states received by Alice is in the Hilbert space $\mathcal{H}_A$ and each of the k quantum states received by Bob is in the Hilbert space $\mathcal{H}_B$. The density operator ρ describes the mutual quantum state of Alice and Bob.

Let $\mathcal{F}$ and $\mathcal{G}$ be two POVM's on $\mathcal{H}_A$ and let $\mathcal{F}'$ and $\mathcal{G}'$ be two POVM's on $\mathcal{H}_B$ (see Section 2.4). For example, these POVM's could be measurements in the x-basis or the p-basis or

measurements in the RL-basis or the DG-basis.

Let T be a p-random selection on $\{1, 2, \ldots, k\}$ made by Alice. This means that the set $\{1, 2, \ldots, k\}$ is divided into two subsets: T and $\{1, 2, \ldots, k\}\backslash T$. An element of $\{1, 2, \ldots, k\}$ is assigned to T with probability p and to $\{1, 2, \ldots, k\}\backslash T$ with probability $1 - p$. Let T' be a p-random selection made by Bob.

For every $i \in \{1, 2, \ldots, k\}$, if $i \in T$ then Alice measures her i'th quantum state with respect to $\mathcal{F}$. If $i \neq T$ then she measures her i'th quantum state with respect to $\mathcal{G}$. Let X_i denote the result of the i'th measurement such that $X' = X_1 X_2 \ldots X_k$ is the bit string extracted by Alice after the measurements.
For every $i \in \{1, 2, \ldots, k\}$, if $i \in T'$ then Bob measures his i'th quantum state with respect to $\mathcal{F}'$. If $i \neq T'$ then he measures his i'th quantum state with respect to $\mathcal{G}'$. Let Y_i denote the result of the i'th measurement such that $Y' = Y_1 Y_2 \ldots Y_k$ is the bit string extracted by Bob after the measurements.

Alice and Bob communicate T and T' over the authenticated public channel. On average there are $\left(p^2 + (1-p)^2\right) k$ positions where Alice and Bob measured with respect to respectively $\mathcal{F}$ and $\mathcal{F}'$ or $\mathcal{G}$ an $\mathcal{G}$. They discard the other cases. The remaining bits are in the sets $T \cap T'$ and $(\{1, 2, \ldots, k\}\backslash T) \cap (\{1, 2, \ldots, k\}\backslash T')$. Alice then makes a random selection S on $T \cap T'$ and a random selection S' on $(\{1, 2, \ldots, k\}\backslash T) \cap (\{1, 2, \ldots, k\}\backslash T')$. The bits from S and S' will be used as check bits to verify if the error rate is below a certain threshold. The remaining bits will be used to construct a secret shared key.

Alice announces the selections S and S'. Alice and Bob announce the bit values X'_S, Y'_S corresponding to S and the bit values $X'_{S'}, Y'_{S'}$ corresponding to S' such that Alice and Bob can estimate the bit error rate ϵ. We assume that the bit error rate deduced from X'_S, Y'_S equals that from $X'_{S'}, Y'_{S'}$. If not, Alice and Bob can always randomly flip some of the bits of the set with the lower error rate to make the error rates equal. The remaining bit values are used as key bit values. Let X and Y be the resulting key bit strings belonging to respectively Alice and Bob. If we take $k = (2\left(p^2 + (1-p)^2\right)^{-1} + \delta)n$ for some $\delta > 0$ and $n \in \mathbb{N}$, then with high probability, X and Y are bit strings of length at least n.

Information reconciliation is applied to X and Y such that after this phase Alice and Bob both have the same bit string K'. Then privacy amplification is applied such that Alice and Bob both have a secure bit string K of length m.

7.2.2 Secret key rate of reduced generic key exchange protocol

The security of the protocol is guaranteed as long as the rate of the protocol as given in [24] is positive. The rate R of the protocol [24] is defined by

$$R \;=\; H(X) - H(X|Y) - S(\rho) \tag{7.1}$$

where $H(.)$ is the classical, Shannon entropy function and $S(.)$ is the quantum, von Neumann entropy function. Let λ_i with $1 \leq i \leq g$ be the eigenvalues of the density operator ρ. The

von Neumann entropy is defined by

$$S(\rho) = -tr(\rho \log \rho) = -\sum_{i=1}^{g} \lambda_i \log \lambda_i.$$

Because the density operator ρ is not known to Alice and Bob, they have to assume that ρ is that density operator that maximizes the von Neumann entropy and still agrees with the results of the measurements Alice and Bob made. This means that Alice and Bob choose ρ such that

$$S(\rho) = \max_{\hat{\rho} \in \mathcal{R}} S(\hat{\rho}).$$

Here $\mathcal{R}$ is the set of density operators on $\mathcal{H}_A \otimes \mathcal{H}_B$ for which it holds that if they are measured with respect to $\mathcal{F} \otimes \mathcal{F}'$ or $\mathcal{G} \otimes \mathcal{G}'$ then the extracted bit error rate is equal to ϵ. This is the bit error rate determined by Alice and Bob from their measurements. With this choice of ρ Alice and Bob create a worst-case scenario with which they find the rate R.

A similar relation is given in [24] if we condition on additional information W of Alice and Bob obtained during privacy amplification. The relation is

$$R = H(X|W) - H(X|Y) - S(\rho|W) = H(X|W) - H(X|Y) - \max_{\hat{\rho} \in \mathcal{R}} S(\hat{\rho}|W).$$

With a clever choice of W the rate R can be improved. The conditional von Neumann entropy $S(\rho|W)$ is defined as

$$S(\rho|W) = \sum_{w} P_W(w) S(\rho_w)$$

where P_W is the probability distribution of W and ρ_w is the "worst case scenario" density operator conditioned on $W = w$. The density operator ρ_w describes the possible states of the quantum system given that $W = w$.

We now explain how to calculate $S(\rho)$ and $S(\rho|W)$.

7.2.3 Calculation of $S(\rho)$ and $S(\rho|W)$

Calculation of $S(\rho)$

For every projective measurement $\mathcal{Z}$ on a density operator ρ with outcome given by a random variable Z it holds that ([20])

$$H(Z) \quad \geq \quad S(\rho). \tag{7.2}$$

Let ρ be the density operator such that $S(\rho) = \max_{\hat{\rho} \in \mathcal{R}} S(\hat{\rho})$. Our goal is to calculate $S(\rho)$. Let $\mathcal{Z}$ be a projective measurement on a density operator $\hat{\rho} \in \mathcal{R}$. If we maximize $H(Z)$ over $\hat{\rho} \in \mathcal{R}$ then we have that $\arg_{\hat{\rho} \in \mathcal{R}} \max H(Z) \geq \max_{\hat{\rho} \in \mathcal{R}} S(\hat{\rho})$. Let $\mathcal{Z}$ be defined as

$$\mathcal{Z} \quad = \quad \sum_{i=1}^{g} m_i |\psi_i\rangle\langle\psi_i| \tag{7.3}$$

where for $1 \leq i \leq g$, $|\psi_i\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and m_i denotes a possible measurement outcome. Suppose that l_i is the probability to measure m_i, for $1 \leq i \leq g$, such that $H(Z) = -\sum_{i=1}^{g} l_i \log l_i$.

Let $\lambda_i, 1 \leq i \leq g$ be the measurement probabilities that maximize $H(Z)$. For the density operator ρ with

$$\rho = \sum_{i=1}^{g} \lambda_i |\psi_i\rangle\langle\psi_i|$$

it holds that $S(\rho) = -\sum_{i=1}^{g} \lambda_i \log \lambda_i = \arg_{\hat{\rho}\in\mathcal{R}} \max H(Z)$ and therefore

$$\arg_{\hat{\rho}\in\mathcal{R}} \max H(Z) \quad = \quad \max_{\hat{\rho}\in\mathcal{R}} S(\hat{\rho}) = S(\rho). \tag{7.4}$$

This means that ρ is the "worst case" density operator.

Calculation of $S(\rho|W)$

We use similar reasoning to calculate $S(\rho|W)$. With Eq. 7.2 we find that for every projective measurement $\mathcal{Z}$ on a density operator $\hat{\rho} \in \mathcal{R}$ with outcome given by a random variable Z it holds that

$$H(Z|W) = \sum_{w} P_W(w) H(Z|W=w) \geq \sum_{w} P_W(w) S(\hat{\rho}_w) = S(\hat{\rho}|W)$$

such that

$$\arg_{\hat{\rho}\in\mathcal{R}} \max H(Z|W) \geq \max_{\hat{\rho}\in\mathcal{R}} S(\hat{\rho}|W) = S(\rho|W).$$

Suppose that for $1 \leq i \leq g$ and every $w \in W$, $l_{i|w}$ is the probability to measure m_i given that $W = w$, such that $H(Z|W=w) = -\sum_{i=1}^{g} l_{i|w} \log l_{i|w}$. Let for $1 \leq i \leq g$ and every $w \in W$, $\lambda_{i|w}$ be the measurement probabilities such that $H(Z|W)$ is maximized. Let the projective measurement $\mathcal{Z}$ be as in Eq. 7.3. For the density operator ρ with

$$\rho_w \quad = \quad \sum_{i=1}^{g} \lambda_{i|w} |\psi_i\rangle\langle\psi_i| \tag{7.5}$$

for every $w \in W$, it holds that $S(\rho_w) = -\sum_{i=1}^{g} \lambda_{i|w} \log \lambda_{i|w} = H(Z|W=w)$ such that

$$\arg_{\hat{\rho}\in\mathcal{R}} \max H(Z|W) \quad = \quad \arg_{\hat{\rho}\in\mathcal{R}} \max \sum_{w} P_W(w) H(Z|W=w) = \sum_{w} P_W(w) S(\rho_w) = S(\rho|W). \tag{7.6}$$

Note that for the density operator ρ with ρ_w as described in Eq. 7.5 it holds that

$$\begin{aligned} \rho &= \sum_{w} P_W(w) \rho_w \\ &= \sum_{i=1}^{g} \left(\sum_{w} P_W(w) \lambda_{i|g} \right) |\psi_i\rangle\langle\psi| \\ &= \sum_{i=1}^{g} \lambda_i |\psi_i\rangle\langle\psi|. \end{aligned}$$

It holds that ρ is the "worst case" density operator.

7.3 Security bound for BB84

In [24], the generic security proof method is applied to BB84. In this section we give an extended version of this derivation.

7.3.1 BB84 as an entanglement based protocol

BB84 can be seen as an entanglement based protocol in which Alice prepares $(4+\delta)n$ entangled two qubit states $|\psi^+\rangle \in L^2 \otimes L^2$ with

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle).$$

She randomly measures these states in the RL- or the DG-basis. The measurement gives her a random element of the corresponding basis and thus a random bit value. This can be seen in the following way. Suppose Alice measures in the RL-basis. The probability that Alice measures qubit state $|0\rangle$ is

$$\begin{aligned}
\langle\psi^+| \left(|0\rangle\langle 0| \otimes I\right) |\psi^+\rangle &= \frac{1}{2} \left(\langle 00| + \langle 11|\right) \left(|0\rangle\langle 0|0\rangle \otimes |0\rangle + |0\rangle\langle 0|1\rangle \otimes |1\rangle\right) \\
&= \frac{1}{2} \left(\langle 00| + \langle 11|\right) \left(|00\rangle\right) \\
&= \frac{1}{2}\langle 00|00\rangle \\
&= \frac{1}{2}.
\end{aligned}$$

The state after the measurement is

$$\left(|0\rangle\langle 0| \otimes I\right) |\psi^+\rangle = |00\rangle. \tag{7.7}$$

It is straightforward that the probability that she measures qubit state $|1\rangle$ is $\frac{1}{2}$. In the same way we find that if Alice measures in the DG-basis then she measures basis state $|+\rangle$ or $|-\rangle$ at random.

After Alice's measurement, she sends the second part of the entangled state to Bob. As we saw in the above calculations, if there is no eavesdropper then the state Bob receives is the same as the state Alice measured. This means that if there is no Eve and Alice and Bob measure in the same basis, then they find the same bit value with probability 1.

Alice and Bob continue with $2n$ bit values for which they used the same basis. Alice chooses n of these bits to serve as check bits, the other n bits will serve as key bits. Alice announces these choices such that Alice and Bob can determine their check bit strings (X' and Y') and their key bit strings (X and Y). Alice and Bob compare their check bits X' and Y' to estimate the bit error rate ϵ.

Information reconciliation and privacy amplification are applied to X and Y to obtain a secret key K of length m.

This version of BB84 is similar to the one described in Section 5.2. Instead of choosing a random $(4+\delta)n$ bit string, Alice chooses to measure $|\psi^+\rangle$ in the RL- or the DG-basis at random. This will give her a random bit string as well.

7.3.2 Secret key rate of BB84

For the proof of security we assume that Eve distributes quantum states to Alice and Bob.

The BB84 protocol is retrieved from the reduced generic key exchange protocol presented in Section 7.2.1 in the following way. We choose $p = \frac{1}{2}$ and $\mathcal{H}_A = \mathcal{H}_B = L^2$. Further, the following POVM's are used

$$\mathcal{F} = \mathcal{F}' = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$$
$$\mathcal{G} = \mathcal{G}' = \{|+\rangle\langle +|, |-\rangle\langle -|\}$$

which correspond to measurements in the RL- and the DG-basis. Every key bit in X is random and therefore the entropy of X is $H(X) = h(\frac{1}{2}) = 1$. With probability ϵ a bit in Y differs from the corresponding bit in X and therefore the conditional entropy of X given Y is $H(X|Y) = h(\epsilon)$. With this we see that the rate of the protocol is given by

$$R = 1 - h(\epsilon) - S(\rho) = 1 - h(\epsilon) - \max_{\hat{\rho}\in\mathcal{R}} S(\hat{\rho})$$

where ρ over $L^2 \otimes L^2$ is the "worst-case scenario" density operator that Alice and Bob choose such that $S(\rho) = \max_{\hat{\rho}\in\mathcal{R}} S(\hat{\rho})$.

7.3.3 Calculation of $S(\rho)$

Let $\hat{\rho} \in \mathcal{R}$. The single knowledge Alice and Bob have about $\hat{\rho}$ is that if both quantum states of $\hat{\rho}$ are measured in the RL- or the DG-basis, then the extracted bit error probability equals ϵ. This is formulated as

$$\begin{array}{lcll}
tr\left((|00\rangle\langle 00| + |11\rangle\langle 11|)\,\hat{\rho}\right) & = & \langle 00|\hat{\rho}|00\rangle + \langle 11|\hat{\rho}|11\rangle & = & 1-\epsilon \\
tr\left((|++\rangle\langle ++| + |--\rangle\langle --|)\,\hat{\rho}\right) & = & \langle ++|\hat{\rho}|++\rangle + \langle --|\hat{\rho}|--\rangle & = & 1-\epsilon \\
tr\left((|01\rangle\langle 01| + |10\rangle\langle 10|)\,\hat{\rho}\right) & = & \langle 01|\hat{\rho}|01\rangle + \langle 10|\hat{\rho}|10\rangle & = & \epsilon \\
tr\left((|+-\rangle\langle +-| + |-+\rangle\langle -+|)\,\hat{\rho}\right) & = & \langle +-|\hat{\rho}|+-\rangle + \langle -+|\hat{\rho}|-+\rangle & = & \epsilon.
\end{array}$$

Let $\mathcal{Z}$ be a projective measurement on $\hat{\rho}$ given by the projectors

$$\{|\psi^+\rangle\langle\psi^+|, |\psi^-\rangle\langle\psi^-|, |\phi^+\rangle\langle\phi^+|, |\phi^-\rangle\langle\phi^-|\}$$

where

$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right) \quad \text{and} \quad |\phi^\pm\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right)$$

are the so called Bell states. A convenient property of these states is that

$$\begin{array}{ll}
|\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|++\rangle + |--\rangle\right) & |\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|++\rangle - |--\rangle\right) \\
|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|-+\rangle + |+-\rangle\right) & |\phi^-\rangle = \frac{1}{\sqrt{2}}\left(|-+\rangle - |+-\rangle\right).
\end{array}$$

The Bell states express whether Alice and Bob measure the same qubit state and therefore extract the same bit value, rather than which qubit state they measure. This comes in very useful because therefore the properties of $\hat{\rho}$ expressing the bit error probabilities can be used in an easy way to calculate and maximize $H(Z)$. It turns out that $\mathcal{Z}$ is a very useful measurement to maximize $H(Z)$ because $H(Z)$ will have only one free variable.

The entropy of $\mathcal{Z}$ is given by

$$H(Z) = -\sum_{i=1}^{4} \lambda_i \log \lambda_i$$

where λ_1 is the probability that $|\psi^+\rangle$ is measured, λ_2 is the probability that $|\psi^-\rangle$ is measured, λ_3 is the probability that $|\phi^+\rangle$ is measured and λ_4 is the probability that $|\phi^-\rangle$ is measured. We express these probabilities in terms of λ_4.

$$\begin{aligned}
\lambda_1 &= \langle\psi^+|\hat{\rho}|\psi^+\rangle \\
&= \frac{1}{2}\left(\langle++| + \langle--|\right)\hat{\rho}\left(|++\rangle + |--\rangle\right) \\
&= \langle++|\hat{\rho}|++\rangle + \langle--|\hat{\rho}|--\rangle - \frac{1}{2}\left(\langle++| - \langle--|\right)\hat{\rho}\left(|++\rangle - |--\rangle\right) \\
&= 1 - \epsilon - \langle\phi^+|\hat{\rho}|\phi^+\rangle
\end{aligned}$$

$$\begin{aligned}
\lambda_2 &= \langle\psi^-|\hat{\rho}|\psi^-\rangle \\
&= \frac{1}{2}\left(\langle-+| + \langle+-|\right)\hat{\rho}\left(|-+\rangle + |+-\rangle\right) \\
&= \langle-+|\hat{\rho}|-+\rangle + \langle+-|\hat{\rho}|+-\rangle - \frac{1}{2}\left(\langle-+| - \langle+-|\right)\hat{\rho}\left(|-+\rangle - |+-\rangle\right) \\
&= \epsilon - \langle\phi^-|\hat{\rho}|\phi^-\rangle
\end{aligned}$$

$$\begin{aligned}
\lambda_3 &= \langle\phi^+|\hat{\rho}|\phi^+\rangle \\
&= \frac{1}{2}\left(\langle01| + \langle10|\right)\hat{\rho}\left(|01\rangle + |10\rangle\right) \\
&= \langle01|\hat{\rho}|01\rangle + \langle10|\hat{\rho}|10\rangle - \frac{1}{2}\left(\langle01| - \langle10|\right)\hat{\rho}\left(|01\rangle - |10\rangle\right) \\
&= \epsilon - \langle\phi^-|\hat{\rho}|\phi^-\rangle
\end{aligned}$$

$$\lambda_4 = \langle\phi^-|\hat{\rho}|\phi^-\rangle$$

Such that $\lambda_1 = 1 - \epsilon - \lambda_3 = 1 - 2\epsilon + \lambda_4$. We saw that to express λ_1 and λ_2 in terms of λ_4, we first had to convert $|\psi^+\rangle$ and $|\psi^-\rangle$ to the diagonal basis. If we would calculate λ_1 in the RL-basis, then the relation $\lambda_1 = 1 - \epsilon - \lambda_2$ would be found, which is trivial.

We note that the probabilities $\lambda_1, \lambda_2, \lambda_3$ can be expressed in terms of λ_4 in a more easy way. The probability $\lambda_1 + \lambda_2$ is the probability that if Alice and Bob both measure in the rectilinear basis, then Alice and Bob find the same bit. Therefore it holds that

$$\lambda_1 + \lambda_2 = 1 - \epsilon.$$

The probability $\lambda_3 + \lambda_4$ is the probability that if Alice and Bob both measure in the rectilinear basis, then Alice and Bob find different bits. Therefore it holds that

$$\lambda_1 + \lambda_2 = 1 - \epsilon.$$

The Bell state $|\psi^-\rangle$ expresses in the rectilinear basis the same situation as the Bell state $|\phi^+\rangle$ in the diagonal basis. Therefore

$$\lambda_2 = \lambda_3.$$

With these three relations, the probabilities $\lambda_1, \lambda_2, \lambda_3$ can be written easily in terms of λ_4;

$$\begin{aligned} \lambda_1 &= 1 - 2\epsilon + \lambda_4 && (7.8) \\ \lambda_2 &= \epsilon - \lambda_4 && (7.9) \\ \lambda_3 &= \epsilon - \lambda_4. && (7.10) \end{aligned}$$

We find that the entropy $H(Z)$ is given by

$$\begin{aligned} H(Z) &= -\sum_{i=1}^{4} \lambda_i \log \lambda_i \\ &= -(1 - 2\epsilon + \lambda_4) \log (1 - 2\epsilon + \lambda_4) - 2(\epsilon - \lambda_4) \log (\epsilon - \lambda_4) - \lambda_4 \log \lambda_4 \end{aligned}$$

The derivative of $H(Z)$ with respect to the free variable λ_4 is given by

$$\frac{dH(Z)}{d\lambda_4} = \log \left(\frac{(\epsilon - \lambda_4)^2}{(1 - 2\epsilon + \lambda_4)\lambda_4} \right)$$

such that $H(Z)$ is maximized for $\lambda_4 = \epsilon^2$. With this choice of the parameter λ_4 we have $H(Z) = 2h(\epsilon)$. We can conclude that the "worst case scenario" density operator ρ for which it holds that $S(\rho) = \max_{\hat{\rho} \in \mathcal{R}} S(\hat{\rho})$ is given by

$$\rho = \lambda_1 |\psi^+\rangle\langle\psi^+| + \lambda_2 |\psi^-\rangle\langle\psi^-| + \lambda_3 |\phi^+\rangle\langle\phi^+| + \lambda_4 |\phi^-\rangle\langle\phi^-| \tag{7.11}$$

where $\lambda_4 = \epsilon^2$ and it holds that (see Eq. 7.4)

$$S(\rho) = \arg_{\hat{\rho} \in \mathcal{R}} H(Z) = 2h(\epsilon).$$

We find that the rate is given by

$$R = 1 - h(\epsilon) - S(\rho) = 1 - 3h(\epsilon).$$

The security threshold is the highest value of ϵ for which the rate is positive. In this case we find $\epsilon < 0.061$.

7.3.4 Using additional information to improve the secret key rate

We use the additional information $W = X \oplus Y$ obtained by Alice and Bob during privacy amplification. The random variable W has value $w = 0$ with probability $P_W(0) = 1 - \epsilon$ and then no error occurred. It has value $w = 1$ with probability $P_W(1) = \epsilon$ and then an error occurred.

Let $\mathcal{Z}$ be the Bell measurement as described in the previous section with outcome given by the random variable Z. The conditional entropy $H(Z|W)$ is given by

$$H(Z|W) = (1 - \epsilon) H(Z|W = 0) + \epsilon H(Z|W = 1).$$

We calculate $H(Z|W = 0)$ and $H(Z|W = 0)$.

- Suppose $W = 0$ so no error occurred. Possible states to be measured are $|\psi^+\rangle$ and $|\psi^-\rangle$. The probability that $|\psi^+\rangle$ is measured, given that no error occurred is

$$\begin{aligned} P(|\psi^+\rangle| \text{ no error}) &= \lambda_{1|0} \\ &= \frac{P(|\psi^+\rangle, W=0)}{P_W(0)} \\ &= \frac{\lambda_1}{1-\epsilon}. \end{aligned}$$

The probability that $|\psi^-\rangle$ is measured given that no error occurred is

$$\begin{aligned} P(|\psi^-\rangle| \text{ no error}) &= \lambda_{2|0} \\ &= \frac{P(|\psi^-\rangle, W=0)}{P_W(0)} \\ &= \frac{\lambda_2}{1-\epsilon}. \end{aligned}$$

This gives that

$$\begin{aligned} H(Z|W=0) &= -\left(\frac{\lambda_1}{1-\epsilon}\right)\log\left(\frac{\lambda_1}{1-\epsilon}\right) - \left(\frac{\lambda_2}{1-\epsilon}\right)\log\left(\frac{\lambda_2}{1-\epsilon}\right) \\ &= -\left(\frac{1-2\epsilon+\lambda_4}{1-\epsilon}\right)\log\left(\frac{1-2\epsilon+\lambda_4}{1-\epsilon}\right) - \left(\frac{\epsilon-\lambda_4}{1-\epsilon}\right)\log\left(\frac{\epsilon-\lambda_4}{1-\epsilon}\right) \\ &= h\left(\frac{1-2\epsilon+\lambda_4}{1-\epsilon}\right). \end{aligned}$$

- Suppose $W = 1$ so an error occurred. Possible states to be measured are $|\phi^+\rangle$ and $|\phi^-\rangle$. The probability that $|\phi^+\rangle$ is measured, given that an error occurred is

$$\begin{aligned} P(|\phi^+\rangle| \text{ error}) &= \lambda_{3|1} \\ &= \frac{P(|\phi^+\rangle, W=1)}{P_W(1)} \\ &= \frac{\lambda_3}{\epsilon}. \end{aligned}$$

The probability that $|\phi^-\rangle$ is measured given that an error occurred is

$$\begin{aligned} P(|\phi^-\rangle| \text{ error}) &= \lambda_{4|1} \\ &= \frac{P(|\phi^-\rangle, W=1)}{P_W(1)} \\ &= \frac{\lambda_4}{\epsilon}. \end{aligned}$$

This gives that

$$\begin{aligned} H(Z|W=1) &= -\left(\frac{\lambda_3}{\epsilon}\right)\log\left(\frac{\lambda_3}{\epsilon}\right) - \left(\frac{\lambda_4}{\epsilon}\right)\log\left(\frac{\lambda_4}{\epsilon}\right) \\ &= -\left(\frac{\epsilon-\lambda_4}{\epsilon}\right)\log\left(\frac{\epsilon-\lambda_4}{\epsilon}\right) - \frac{\lambda_4}{\epsilon}\log\frac{\lambda_4}{\epsilon} \\ &= h\left(\frac{\lambda_4}{\epsilon}\right). \end{aligned}$$

We see that the conditional entropy $H(Z|W)$ is given by

$$\begin{aligned} H(Z|W) &= (1-\epsilon)h\left(\frac{1-2\epsilon+\lambda_4}{1-\epsilon}\right) + \epsilon h\left(\frac{\lambda_4}{1-\epsilon}\right) \\ &= -(1-2\epsilon+\lambda_4)\left(\log(1-2\epsilon+\lambda_4) - \log(1-\epsilon)\right) - (\epsilon-\lambda_4)\left(\log(\epsilon-\lambda_4) - \log(1-\epsilon)\right) - \\ &\quad \lambda_4\left(\log\lambda_4 - \log\epsilon\right) - (\epsilon-\lambda_4)\left(\log(\epsilon-\lambda_4) - \log\epsilon\right) \\ &= H(Z) + (1-2\epsilon+\lambda_4)\log(1-\epsilon) + (\epsilon-\lambda_4)\log(1-\epsilon) + \lambda_4\log\epsilon + (\epsilon-\lambda_4)\log\epsilon \\ &= H(Z) + \epsilon\log\epsilon + (1-\epsilon)\log(1-\epsilon) \\ &= H(Z) - h(\epsilon). \end{aligned}$$

We can conclude that $H(Z|W)$ is maximized for $\lambda_4 = \epsilon^2$ because $H(Z)$ is maximized for $\lambda_4 = \epsilon^2$. For this choice of the free variable λ_4 we have that $H(Z|W) = h(\epsilon)$. The worst case scenario density operator ρ is the same as in Eq. 7.11 with $\lambda_4 = \epsilon^2$. For this worst-case density operator ρ it holds that (see Eq. 7.6)

$$S(\rho|W) = \arg_{\hat{\rho}\in\mathcal{R}} H(Z|W) = h(\epsilon).$$

The uncertainty of X given W does not decrease, therefore $H(X|W) = 1$. This means that the rate of the protocol is improved to

$$R = 1 - h(\epsilon) - h(\epsilon) = 1 - 2h(\epsilon).$$

The security threshold is the highest value of ϵ for which the rate is positive. In this case we find $\epsilon < 0.11$. The same bound is found as given in other security proofs.

7.4 Security bound for GP00

In the previous section we calculated the security threshold for BB84. If the error rate ϵ is lower than this threshold then the key exchange protocol is secure; the information Eve gained about the secret key is negligible.

In Chapter 5 we saw that the key exchange protocol GP00 that works with squeezed state resembles BB84. When the squeezing parameter goes to infinity, then squeezed states become eigenstates of the position or momentum operator and thus the bit transition probabilities equal the bit transition probabilities of BB84, given that there is no Eve.

In [23] it was proved that if the squeezing parameter $\hat{r} > 0.289$, then the protocol GP00 is secure when the error rate $\epsilon < 0.11$. In this section our aim is to calculate a threshold for ϵ as a function of the squeezing parameter $\hat{r}$. We do this analogous to the security proof of BB84 given in Section 7.3.

7.4.1 GP00 as an entanglement based protocol

GP00 can be seen as an entanglement based protocol in which Alice prepares $(4+\delta)n$ entangled states $|\psi^0\rangle$ with

$$|\psi^0\rangle = \frac{1}{\sqrt{\pi}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\exp\left[-\frac{\Delta^2}{8}(x_m\left(1-\tilde{\Delta}^4\right)^{-\frac{1}{2}}+x_n)^2-\frac{1}{2\Delta^2}(x_m\left(1-\tilde{\Delta}^4\right)^{-\frac{1}{2}}-x_n)^2\right]\cdot \exp\left[i(x_m+(k+\frac{1}{2})\sqrt{\pi\hbar})x_n\right]|x_m x_n\rangle dx_n dx_m \quad (7.12)$$

$$= \frac{1}{\sqrt{\pi}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\exp\left[-\frac{\Delta^2}{8}(p_m\left(1-\tilde{\Delta}^4\right)^{-\frac{1}{2}}-p_n)^2-\frac{1}{2\Delta^2}(p_m\left(1-\tilde{\Delta}^4\right)^{-\frac{1}{2}}+p_n)^2\right]\cdot \exp\left[i(-p_m+(k+\frac{1}{2})\sqrt{\pi\hbar})p_n\right]|p_m p_n\rangle dp_n dp_m \quad (7.13)$$

where $|x_m x_n\rangle$ and $|p_m p_n\rangle$ are composite x and p eigenstates. The value of k is chosen randomly from $\mathcal{K}=\{-n_k,-n_k+1,\ldots,n_k-1\}$ for some $n_k\in\mathbb{N}$. It holds that Δ^2 is real and positive and $\tilde{\Delta}^2=\Delta^2/(1+\frac{1}{4}\Delta^4)$. The two formulations 7.12 and 7.13 are equal because of the following. It holds that $\langle p_n|x_n\rangle=\int_{-\infty}^{\infty}e^{-ip_n x}\delta(x-x_n)dx=e^{-ip_n x_n}$ and therefore $|x_n\rangle$ and $|p_n\rangle$ can be expressed in the respective bases $\{|p\rangle\}_{p\in\mathbb{R}}$ and $\{|x\rangle\}_{x\in\mathbb{R}}$ as

$$|x_n\rangle=\int_{-\infty}^{\infty}e^{-ip_n x_n}|p_n\rangle dp_n \quad\text{and}\quad |p_n\rangle=\int_{-\infty}^{\infty}e^{ip_n x_n}|x_n\rangle dx_n.$$

If we substitute

$$|x_m x_n\rangle=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}e^{-ip_m x_m-ip_n x_n}|p_m p_n\rangle dp_m dp_n$$

in Eq. 7.12, then we easily that there is only a solution for $x_m=-p_m$ and $x_n=p_n$. With these substitutions we find Eq. 7.13.

In the following theorem we give some properties of measurements of $|\psi^0\rangle$ from which we easily see that the state $|\psi^0\rangle$ can be used to simulate GP00.

Theorem 7.4.1 *Let $|\psi^0\rangle$ be the quantum entangled state defined above. Suppose Alice has one part of this state and Bob the second part. Alice can measure in the x or the p-basis;*

- *If Alice measures in the x-basis, then the probability that she measures position value x_m is given by*

$$P(x_m)=\frac{\tilde{\Delta}}{\sqrt{\pi(1-\tilde{\Delta}^4)}}\exp\left[-\frac{\tilde{\Delta}^2 x_m^2}{1-\tilde{\Delta}^4}\right]$$

and by measuring x_m she prepares for Bob the state

$$|\psi_B\rangle=\frac{1}{\left(\pi\tilde{\Delta}^2\right)^{\frac{1}{4}}}\int_{-\infty}^{\infty}\exp\left[-\frac{1}{2\tilde{\Delta}^2}(x_n-x_m)^2\right]|x_n\rangle dx_n$$

where

$$\tilde{\Delta}^2=\frac{4\Delta^2}{4+\Delta^4}.$$

The state $|\psi_B\rangle$ is a squeezed state with mean position value x_m and mean momentum value $x_m + (k+\frac{1}{2})\sqrt{\pi\hbar}$. For the variance in x it holds that $2\sigma_x^2 = \tilde{\Delta}^2 = \hbar e^{2r}$ and for the variance in p it holds that $2\sigma_p^2 = \frac{1}{\tilde{\Delta}^2}$.

- *If Alice measures in the p-basis, then the probability that she measures momentum value p_m is*

$$P(p_m) = \frac{\tilde{\Delta}}{\sqrt{\pi(1-\tilde{\Delta}^4)}} \exp\left[-\frac{\tilde{\Delta}^2 p_m^2}{1-\Delta^4}\right]$$

and by measuring p_m she prepares for Bob the state

$$|\psi_B\rangle = \frac{1}{\left(\pi\tilde{\Delta}^2\right)^{\frac{1}{4}}} \int_{-\infty}^{\infty} \exp\left[-\frac{1}{2\tilde{\Delta}^2}(p_n+p_m)^2\right]|x_n\rangle dp_n$$

where

$$\tilde{\Delta}^2 = \frac{4\Delta^2}{4+\Delta^4}.$$

The state $|\psi_B\rangle$ is a squeezed state with mean momentum value $-p_m$ and mean position value $-p_m + (k+\frac{1}{2})\sqrt{\pi\hbar}$. For the variance in p it holds that $2\sigma_p^2 = \tilde{\Delta}^2 = \hbar e^{2r}$ and for the variance in x it holds that $2\sigma_x^2 = \frac{1}{\tilde{\Delta}^2}$.

We see that if Alice chooses $r = -\hat{r}$, with $\hat{r} > 0$ is the squeezing parameter, then, if she measures her state in the x-basis Bob will receive the same squeezed state squeezed in x he would otherwise receive in GP00 and if Alice measures in the p-basis Bob will receive the same squeezed state squeezed in p he would receive in GP00.

PROOF. Suppose Alice measures $|\psi^0\rangle$ in the x-basis. The projector that projects Alice's state onto the x-eigenstate $|x_m\rangle$ and leaves alone Bob's state is given by $|x_m\rangle\langle x_m| \otimes I$. This means that the probability that Alice measures position value x_m is given by

$$\begin{aligned}
P(x_m) &= \langle\psi^0|\left(|x_m\rangle\langle x_m| \otimes I\right)|\psi^0\rangle \\
&= \frac{1}{\sqrt{\pi}}\langle\psi^0| \int_{-\infty}^{\infty} \exp\left[-\frac{\Delta^2}{8}\left(x_m(1-\tilde{\Delta}^4)^{-\frac{1}{2}} + x_n\right)^2 - \frac{1}{2\Delta^2}\left(x_m(1-\tilde{\Delta}^4)^{-\frac{1}{2}} - x_n\right)^2\right] \cdot \\
&\qquad\qquad \exp\left[i\left(x_m + (k+\frac{1}{2})\sqrt{\pi\hbar}\right)x_n\right]|x_m x_n\rangle dx_n \\
&= \frac{1}{\pi}\int_{-\infty}^{\infty} \exp\left[-\frac{\Delta^2}{4}(x_m(1-\tilde{\Delta}^4)^{-\frac{1}{2}} + x_n)^2 - \frac{1}{\Delta^2}(x_m(1-\tilde{\Delta}^4)^{-\frac{1}{2}} - x_n)^2\right] dx_n. \quad (7.14)
\end{aligned}$$

By "completing the square" we find that Eq. 7.15 becomes

$$\begin{aligned}
P(x_m) &= \frac{1}{\pi}\exp\left[-\left(\frac{4\Delta^2}{\Delta^4+4}\right)\frac{x_m^2}{1-\tilde{\Delta}^4}\right]\int_{-\infty}^{\infty}\exp\left[-\left(\frac{\Delta^4+4}{4\Delta^2}\right)(x_n-x_m)^2\right]dx_n \\
&= \frac{1}{\pi}\exp\left[-\left(\frac{\tilde{\Delta}^2}{1-\tilde{\Delta}^4}\right)x_m^2\right]\sqrt{\pi\tilde{\Delta}^2} \\
&= \frac{\tilde{\Delta}}{\sqrt{\pi}}\exp\left[-\frac{\tilde{\Delta}^2 x_m^2}{1-\tilde{\Delta}^4}\right].
\end{aligned}$$

With normalization we find the probability distribution presented in the theorem.

The state after the measurement is given by

$$\begin{aligned}
|\psi\rangle &= (|x_m\rangle\langle x_m| \otimes I)\,|\psi^0\rangle \\
&= \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} \exp\left[-\frac{\Delta^2}{8}\left(x_m(1-\tilde{\Delta}^4)^{-\frac{1}{2}} + x_n\right)^2 - \frac{1}{2\Delta^2}\left(x_m(1-\tilde{\Delta}^4)^{-\frac{1}{2}} - x_n\right)^2 + \right. \\
&\qquad \left. i(x_m + (k+\frac{1}{2})\sqrt{\pi\hbar})x_n\right] |x_m x_n\rangle dx_n \\
&= |x_m\rangle \otimes \left(\frac{1}{\sqrt{\pi}} \exp\left[-\frac{\tilde{\Delta}^2 x_m^2}{2(1-\tilde{\Delta}^4)}\right] \int_{-\infty}^{\infty} \exp\left[-\left(\frac{1}{2\tilde{\Delta}^2}\right)(x_n - x_m)^2\right] \cdot \right. \\
&\qquad \left. \exp\left[i(x_m + (k+\frac{1}{2})\sqrt{\pi\hbar})x_n\right] |x_n\rangle dx_n\right)
\end{aligned}$$

Normalization of the state belonging to Bob gives that

$$|\psi_B\rangle = \frac{1}{\left(\pi\tilde{\Delta}^2\right)^{1/4}} \int_{-\infty}^{\infty} \exp\left[-\frac{1}{2\tilde{\Delta}^2}(x_n - x_m)^2 + i(x_m + (k+\frac{1}{2})\sqrt{\pi\hbar})x_n\right] |x_n\rangle dx_n.$$

This simulates a squeezed state $|r, \alpha\rangle$, with $r \in \mathbb{R}$ and $\alpha \in \mathbb{C}$ such that $\langle x\rangle = x_m$. This is because the probability that Bob measures position value x_n is given by

$$|\langle\psi_B|x_n\rangle|^2 = \frac{1}{\left(\pi\tilde{\Delta}^2\right)^{1/2}} \exp\left[-\frac{1}{\tilde{\Delta}^2}(x_n - x_m)^2\right] = P_X^{|r,\alpha\rangle}(x_n)$$

if and only if $\tilde{\Delta}^2 = \hbar e^{-2r}$ (see Theorem 4.2.5).

If Bob measures in the p-basis, then the probability that he measures momentum value p_k is given by $|\langle p_k|\psi_B\rangle|^2$. We calculate $\langle p_k|\psi_B\rangle$.

$$\begin{aligned}
\langle p_k|\psi_B\rangle &= \frac{1}{\left(\pi\tilde{\Delta}^2\right)^{1/4}} \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-ip_k x} \exp\left[-\frac{1}{2\tilde{\Delta}^2}(x_n - x_m)^2 + i(x_m + (k+\frac{1}{2})\sqrt{\pi\hbar})x_n\right] \cdot \\
&\qquad \delta(x - x_n)dx_n dx \\
&= \frac{1}{\left(\pi\tilde{\Delta}^2\right)^{1/4}} \int_{-\infty}^{\infty} \exp\left[-\frac{1}{2\tilde{\Delta}^2}(x_n - x_m)^2 + i(x_m + (k+\frac{1}{2})\sqrt{\pi\hbar})x_n\right] \cdot \\
&\qquad \left(\int_{-\infty}^{\infty} e^{-ip_k x}\delta(x - x_n)dx\right)dx_n \\
&= \frac{1}{\left(\pi\tilde{\Delta}^2\right)^{1/4}} \int_{-\infty}^{\infty} \exp\left[-\frac{1}{2\tilde{\Delta}^2}(x_n - x_m)^2 - i\left(p_k - (x_m + (k+\frac{1}{2})\sqrt{\pi\hbar})\right)x_n\right]dx_n
\end{aligned}$$

This equation is similar to Eq. 4.1 after substituting $\tilde{\Delta}^2 = e^{2r}\hbar, \langle p\rangle = \hbar(x_m + (k+\frac{1}{2})\sqrt{\pi\hbar})$ and $p_n = \hbar p_k$. Following the steps after Eq. 4.1 we find

$$P_P^{|\psi_B\rangle}(p_k) = \frac{\tilde{\Delta}}{\sqrt{\pi}} \exp\left[-\tilde{\Delta}^2\left(p_k - \left(x_m + (k+\frac{1}{2})\sqrt{\pi\hbar}\right)\right)^2\right].$$

This means that the mean momentum value to measure is $x_m + (k + \frac{1}{2})\sqrt{\pi\hbar}$ and the variance is $\frac{1}{2\tilde{\Delta}^2}$.

The calculations when Alice measured $|\psi^0\rangle$ in the p-basis follow easily from the substitutions $x_m \to -p_m, x_n \to p_n$. □

From Theorem 7.4.1 we see that the key exchange protocol GP00 can be seen as an entanglement based protocol. This entanglement based protocol is as follows.

Entanglement Based version of GP00

Alice prepares $(4 + \delta)n$ states $|\psi^0\rangle$ with $\tilde{\Delta}^2 = \hbar e^{-2\hat{r}}$ with $\hat{r} > 0$ fixed. Alice measures her part of each of these states in the x or p-basis at random and extracts a bit value. After the measurement she sends the other part of each state to Bob, who measures it in the x or the p-basis at random. There are two possible scenarios;

- Suppose Alice measures in the x-basis and measures position value x_m. Because $P(x_m)$ is a Gaussian distribution centered at 0 we have that x_m is an element of $\mathcal{L}_0$ or $\mathcal{L}_1$ with equal probability. Alice extracts a bit value depending on whether x_m is in $\mathcal{L}_0$ or $\mathcal{L}_1$ and therefore the bit extracted by Alice is random. Alice sends the value $\phi_x = x_m \bmod \sqrt{\pi\hbar}$ to Bob.

  Suppose that Bob measures in the x-basis. From Theorem 7.4.1 we see that the probability that Bob measures the value x_n such that $x_n - x_m \in \mathcal{C}$, given that there is no eavesdropper, is equal to the corresponding probability in the original squeezed state protocol GP00. This means that Bob has probability $1 - \epsilon_s$ to extract the correct bit.

  Suppose Bob measures in the p-basis. The mean momentum value to be measured is $x_m + (k + \frac{1}{2})\sqrt{\pi\hbar}$ and therefore the probability that Bob extracts the correct bit is $\frac{1}{2}$.

- Suppose Alice measured in the p-basis and measured momentum value p_m. The value $-p_m$ is an element of $\mathcal{L}_0$ or $\mathcal{L}_1$ with equal probability. Alice extracts a bit from the value $-p_m$ because that is the mean momentum value of the squeezed state received by Bob.

  Alice sends the value $\phi_p = -p_m \bmod \sqrt{\pi\hbar}$ to Bob. Following the same line of reasoning as in the previous scenario, we conclude that if there is no eavesdropper then, with probability $1 - \epsilon_s$, Bob measures $p_n + p_m \in \mathcal{C}$ and thus extract the correct bit. If Bob measures in the x-basis, then the probability that Bob extracts the correct bit is $\frac{1}{2}$.

Alice and Bob announce which bases they used and discard the cases where they did not use the same basis. Alice decides on n bits to use as check bits, the others will serve as key bits. Alice sends the value ϕ_x or ϕ_p (depending on in which basis she measured) to Bob with which Bob can extract bit values. Alice and Bob announce the check bits and estimate the bit error rate ϵ. The key bit strings belonging to Alice and Bob are respectively X and Y.

Information reconciliation and privacy amplification follow. Alice and Bob end with a secret key K of length m if and only if ϵ is smaller than a certain threshold.

We see that this protocol is similar to that described in 5.3.2. Instead of choosing to prepare a squeezed state squeezed in x or in p and sampling the mean value of the squeezed state from a probability distribution, Alice chooses to measure $|\psi^0\rangle$ in the x or p-basis. The measurement automatically samples a mean value and gives Bob a squeezed state squeezed in the correct basis.

7.4.2 Secret key rate of GP00

For the proof of security we assume that Eve distributes quantum states to Alice and Bob.

The key exchange protocol GP00 is retrieved from the reduced generic key exchange protocol presented in Section 7.2.1 in the following way. We choose $p = \frac{1}{2}$ and $\mathcal{H}_A = \mathcal{H}_B = L^2$. Further the following POVM's are used.

$$\mathcal{F} = \mathcal{F}' = \{|x\rangle\langle x|\}_{x\in\mathbb{R}}$$

$$\mathcal{G} = \mathcal{G}' = \{|p\rangle\langle p|\}_{p\in\mathbb{R}}$$

That is, $\mathcal{F}$ and $\mathcal{F}'$ are measurements in the x-basis and $\mathcal{G}$ and $\mathcal{G}'$ are measurements in the p-basis. Alice and Bob use the entanglement based version of GP00, as described in Section 7.4.1.

Every key bit in X is random and therefore the entropy of X is $H(X) = h(\frac{1}{2}) = 1$. With probability ϵ a bit in Y differs from the corresponding bit in X and therefore $H(X|Y) = h(\epsilon)$. With this we see that the rate of GP00 is given by

$$R = 1 - h(\epsilon) - S(\rho) = 1 - h(\epsilon) - \max_{\hat{\rho}\in\mathcal{R}} S(\hat{\rho})$$

where ρ over $L^2 \otimes L^2$ is the "worst-case scenario" density operator that Alice and Bob choose such that $S(\rho) = \max_{\hat{\rho}\in\mathcal{R}} S(\hat{\rho})$. The protocol is secure when the rate R is positive.

7.4.3 Calculation of $S(\rho)$

Let $\hat{\rho} \in \mathcal{R}$. This implies the following. Suppose that both quantum parts of $\hat{\rho}$ are measured in the x-basis or the p-basis. The probability that the bit values extracted from the measured values differ, is equal to ϵ, the estimated bit error rate. In mathematical expressions this becomes

$$\int_{-\infty}^{\infty}\int_{x_n - x_m \in \mathcal{C}} \langle x_m x_n|\hat{\rho}|x_m x_n\rangle dx_n dx_m = 1 - \epsilon \tag{7.15}$$

$$\int_{-\infty}^{\infty}\int_{p_n - p_m \in \mathcal{C}} \langle p_m p_n|\hat{\rho}|p_m p_n\rangle dp_n dp_m = 1 - \epsilon \tag{7.16}$$

$$\int_{-\infty}^{\infty}\int_{x_n - x_m \in \mathbb{R}\setminus\mathcal{C}} \langle x_m x_n|\hat{\rho}|x_m x_n\rangle dx_n dx_m = \epsilon \tag{7.17}$$

$$\int_{-\infty}^{\infty}\int_{p_n - p_m \in \mathbb{R}\setminus\mathcal{C}} \langle p_m p_n|\hat{\rho}|p_m p_n\rangle dp_n dp_m = \epsilon \tag{7.18}$$

Alice and Bob use the entanglement based version of GP00 described in 7.4.1. Therefore, if Alice measures the value x_m, she extracts a bit from the value x_m and sends ϕ_x based on x_m. If Alice measures the value p_m, she extracts a bit from the value $-p_m$ and sends ϕ_p based on $-p_m$.

An important question is which projective measurement to use to calculate $S(\rho)$. Using the similarity with BB84, the projective measurement should have the following properties:

- The measurement operators, in both bases, express whether Alice and Bob extract the same bit value or a different bit value.
- The measurement operators can be converted easily from the rectilinear to the diagonal basis and vice versa.

A projective measurement that satisfies these conditions and is the continuous version of the Bell measurement, is given by the measurement operators $\{|\psi(x,p)\rangle\langle\psi(x,p)| : x,p \in \mathbb{R}\}$ where $|\psi(x,p)\rangle$ is given by

$$\begin{aligned} |\psi(x,p)\rangle &= \int_{-\infty}^{\infty} e^{ipx_n}|x_n, x_n+x\rangle dx_n & (7.19)\\ &\approx \int_{-\infty}^{\infty} e^{ixp_n}|p_n, -p_n+p\rangle dp_n & (7.20)\end{aligned}$$

We see that these operators are easily converted from the x to the p-basis because the state is integrated over all $x_n \in \mathbb{R}$. Further, this is a projective measurement because the measurements states are orthogonal and they form a partition of unity. They are orthogonal because

$$\begin{aligned} \langle\psi(x',p')|\psi(x,p)\rangle &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-ipx_n+ip'x_m}\langle x_n, x_n+x|x_m, x_m+x'\rangle dx_m dx_n \\ &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-ipx_n+ip'x_m}\langle x_n|x_m\rangle\langle x_n+x|x_m+x'\rangle dx_m dx_n \\ &= \int_{-\infty}^{\infty} e^{-ix_n(p-p')}\langle x_n+x|x_n+x'\rangle dx_n \\ &= \delta(p-p')\delta(x-x'). \end{aligned}$$

Further, they form a partition of unity because

$$\begin{aligned} \int\int |\psi(x,p)\rangle\langle\psi(x,p)|dpdx &= \int\int \left(\int e^{ipx_n}|x_n, x_n+x\rangle dx_n\right)\left(\int e^{-ipx_m}\langle x_m, x_m+x|dx_m\right)dpdx \\ &= \int\int\int\int e^{ip(x_n-x_m)}|x_n, x_n+x\rangle\langle x_m, x_m+x|dx_n dx_m dpdx \\ &= \int\int |x_n, x_n+x\rangle\langle x_n, x_n+x|dx_n dx \\ &= \int\int |x_n\rangle\langle x_n|\otimes|x_n+x\rangle\langle x_n+x|dx_n dx \\ &= \int\int |x_n\rangle\langle x_n|\otimes|x_m\rangle\langle x_m|dx_n dx_m \\ &= I\otimes I. \end{aligned}$$

Because $\{|\psi(x,p)\rangle\langle\psi(x,p)| : x,p \in \mathbb{R}\}$ is a projective measurement, we see the following if the state $|\psi(x,p)\rangle$ is measured. If Alice and Bob measure in the x-basis, then if Alice measures position value x_n then Bob measures position value $x_n + x$. If Alice and Bob measure in the p-basis, then if Alice measures position value p_n then Bob measures position value $-p_n + p$. This corresponds to the entanglement based version of GP00.

From this we see that the states $|\psi(x,p)\rangle$ with $x \in \mathcal{C}$ denote the instances where Alice and Bob find the same bit if they both measure in the x-basis and the states $|\psi(x,p)\rangle$ with $x \in \mathcal{C}^c$ denote the instances where Alice and Bob find different bits if they both measure in the x-basis. If $p \in \mathcal{C}$ then Alice and Bob find the same bit if they both measure in the p-basis and if $p \in \mathcal{C}^c$ then Alice and Bob find different bits if they both measure in the p-basis.

With this basis we can calculate $S(\rho)$. Define p_{xp} to be the probability that measurement operator $|\psi(x,p)\rangle$ is measured;

$$p_{xp} = \langle\psi(x,p)|\hat{\rho}|\psi(x,p)\rangle.$$

From Eq. **??** and **??** we see that $p_{xp} = p_{px}$.

We can group these probabilities in such a way that the resulting four probabilities have the same properties as the probabilities $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ in Section 7.3.3. We group in the following way:

$$\lambda_1 = \int_{p\in\mathcal{C}}\int_{x\in\mathcal{C}} p_{xp}dxdp \qquad \lambda_3 = \int_{p\in\mathcal{C}}\int_{x\in\mathcal{C}^c} p_{xp}dxdp$$
$$\lambda_2 = \int_{p\in\mathcal{C}^c}\int_{x\in\mathcal{C}} p_{xp}dxdp \qquad \lambda_4 = \int_{p\in\mathcal{C}^c}\int_{x\in\mathcal{C}^c} p_{xp}dxdp.$$

The probability λ_1 is the probability that if Alice and Bob both measure in the x-basis or the p-basis, then they find the same bit value. The probability λ_2 is the probability that if Alice and Bob measure in the x-basis then they find the same bit value but if they measure in the p-basis, they find different bits. The probability λ_3 is the probability that if Alice and Bob measure in the x-basis then they find different bit values but if they measure in the p-basis, they find the same bit. The probability λ_4 is the probability that if Alice and Bob both measure in the x-basis or the p-basis, then they find different bits. These properties are analogue to the properties of the Bell states of Section 7.3.3 and therefore equal to the properties of the probabilities $\lambda_1, \ldots, \lambda_4$ in Section 7.3.3. We find the same relations;

$$\begin{aligned}
\lambda_1 + \lambda_2 &= \int_{-\infty}^{\infty}\int_{x\in\mathcal{C}} p_{xp}dxdp \\
&= \int_{-\infty}^{\infty}\int_{x\in\mathcal{C}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-ip(x_m-x_n)}\langle x_m, x_m+x|\hat{\rho}|x_n, x_n+x\rangle dx_n dx_m d_x d_p \\
&= \int_{x\in\mathcal{C}}\int_{-\infty}^{\infty}\langle x_n, x_n+x|\hat{\rho}|x_n, x_n+x\rangle dx_n d_x \\
&= \int_{-\infty}^{\infty}\int_{x_n-x_m\in\mathcal{C}}\langle x_m x_n|\hat{\rho}|x_m x_n\rangle dx_n dx_m \\
&= 1-\epsilon.
\end{aligned}$$

In the same way we find

$$\begin{aligned} \lambda_3 + \lambda_4 &= \int_{-\infty}^{\infty} \int_{x \in \mathcal{C}^c} p_{xp} dx dp \\ &= \epsilon. \end{aligned}$$

The third relation becomes

$$\begin{aligned} \lambda_2 &= \int_{p \in \mathcal{C}^c} \int_{x \in \mathcal{C}} p_{xp} dx dp \\ &= \int_{p \in \mathcal{C}^c} \int_{x \in \mathcal{C}} p_{px} dx dp \\ &= \int_{p \in \mathcal{C}} \int_{x \in \mathcal{C}^c} p_{xp} dx dp \\ &= \lambda_3. \end{aligned}$$

With these three relations, $\lambda_1, \lambda_2, \lambda_3$ can be written in terms of λ_4 in the following way

$$\begin{aligned} \lambda_1 &= 1 - 2\epsilon + \lambda_4 \\ \lambda_2 &= \epsilon - \lambda_4 \\ \lambda_3 &= \epsilon - \lambda_4. \end{aligned}$$

These relations equal the relations 7.8,7.9,7.10. Using the additional information $W = X \oplus Y$, further calculations are equal as in Section **??**. We find that

$$\begin{aligned} R &= H(X|W) - H(X|Y) - S(\rho|W) \\ &= 1 - h(\epsilon) - h(\epsilon) \\ &= 1 - 2h(\epsilon). \end{aligned}$$

Therefore, GP00 is secure when $\epsilon < 0.11$. Because the error rate caused by the structure of squeezed states, ϵ_s, is smaller than the total error rate ϵ, we have that $\epsilon_s < 0.11$. This is reached when $\hat{r} > 0.243$. This is an improvement of the lower bound for the squeezing parameter. The lower bound given in [23] was $\hat{r} > 0.289$.

We note that if, for example, $\epsilon_s = 0.09$, then to obtain $\epsilon < 0.11$, Eve can do much less than if $\epsilon_s = 0.04$. This means that if $\epsilon_s = 0.09$, then it will occur more often that $\epsilon > 0.11$ and the protocol is aborted than if $\epsilon_s = 0.04$.

Chapter 8

Conclusion and Suggestions

Quantum Key Exchange (QKE) can solve the problem of Classical Key Exchange in Cryptography. We studied the firstly introduced QKE protocol BB84, which works with qubits, which are two-dimensional. The protocol BB84 has some disadvantages which are partially solved by QKE that works with squeezed states, which are infinite-dimensional. A protocol that works with squeezed states is GP00 [23], it resembles BB84.

We calculated important general properties of squeezed states. With the results of these calculations we were able to fully understand and study SSGP. Together with a study of BB84, the similarity between the protocols BB84 and GP00 was shown.

In [24], a method is presented with which the security of a class of QKE protocols can be proved. We studied the general method and applied it to BB84. If ϵ is the estimated bit error rate then BB84 is secure if $\epsilon < 0.11$ which corresponds to the threshold found by others. In [23], it was proven that if the squeezing parameter $\hat{r} \geq 0.289$, then GP00 is secure when $\epsilon < 0.11$. Using the resemblance of BB84 and GP00 we applied the method to GP00 and found, that if $\hat{r} \geq 0.243$, then GP00 is secure when $\epsilon < 0.11$. This means that we could prove the security of GP00 using the method and that we improved the lower bound of the squeezing parameter.

A suggestion for further research is to apply the security method from [24] to a version of GP00 where more than one bit is extracted from every squeezed state. We proposed a protocol for sending m bits per squeezed state. Now we are able to apply the security method from [24] to GP00, it would be interesting to apply it to a version where m bits are extracted from every squeezed state.

Bibliography

[1] W. Diffie & M. E. Hellman; *"New Directions in Cryptography"*, 1976, IEEE Transactions on Information Theory IT-22, p. 644-654.

[2] A. Einstein; *Über einen der entzeugung und verwandlung des lichtes betreffenden heuristischen gesichtspunkt*, 1905, Ann. Phys. 17 (Berlin).

[3] W. Gerlach & O. Stern; 1922, Z. Phys. 9, 349, 353.

[4] N.A. Kozyrev; *The theory of stars' internal structure and sources of stellar energy.*, 1951, Notices of Crimean Astrophysical Observatory, 6, 54-83 (in Rus- sian).

[5] A.H. MacDonald, Hiroshi Akera & M.R. Norman; *Quantum Mechanics and Superconductivity in a Magnetic Field*, 1992, cond-mat/9211019.

[6] Charles Kittel; *Introduction to solid state physics*,1995, ISBN 0-471-11181-3.

[7] Marc I. Vuletic; *Philosophy and Quantum Mechanics*, 1999.

[8] David Mermin; *What is Quantum Mechanics trying to tell us?*, 1998, quant-ph/9801057.

[9] P. W. Shor; *Algorithms for quantum computation: Discrete logarithms and factoring*, 1994, 35nd Annual Symposium on Foundations of Computer Science, pages 124-134, IEEE Computer Society Press.

[10] C.H. Bennett & G. Brassard; *Quantum Cryptography; Public key distribution and coin tossing*, 1984, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179, IEEE, New York.

[11] K. Fujii; *Introduction to Coherent States and Quantum Information Theory*, 2002, quant-ph/0112090 v2.

[12] E. Schrodinger; 1926, Naturwissenschaften, 14, 664.

[13] W.K. Wootters; *A Single Quantum cannot be Cloned*, 1982, Letters to Nature, 802-803.

[14] A.K. Ekert; *Quantum Cryptography based on Bell's Theorem*, 1991, Phys. Rev. Lett., 67(6): 661-663.

[15] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail & J. Smolin; *Expreimental quantum cryptography*, 1992, Journal of Cryptology, vol. 5, no. 1, 3-28.

[16] G. Brassard & L. Salvail; *Secret-key reconciliation by public discussion*, 1994, Advances in Cryptology-Eurocrypt '93, vol. 765 of Lecture-Notes in Computer Science, 410-423, Springer-Verlag.

[17] C.H. Bennett, G. Brassard, C. Crépeau & U.M. Maurer; *Generalized Privacy Amplification*, 1994, preprint.

[18] C.H. Bennett, G. Brassard & J.M. Robert; *Privacy amplification by public discussion*, 1988, SIAM Journal on Computing, vol. 17, 210-229.

[19] C.H. Bennett, G. Brassard, S. Breidbart & S. Wiesner; *Quantum Cryptology, or unforgeable subway tokens*, 1982, Advances in Cryptology: Proceddings of Crypto '82, Plenum Press, 267-275.

[20] A. Wehrl; *General Properties of Entropy*, 1978, Rev. Mod. Phys., 50, 221-260.

[21] David J. Griffiths; *Introduction to Quantuum Mechanics*, 1995, ISBN 0-13-124405-1.

[22] Michael E. Nielsen & Isaac L. Chuang; *Quantum Computation and Quantum Information*, 2000, ISBN 0-521-63503-9.

[23] D. Gottesman & J. Preskill; *Secure quantum key exchange using squeezed states*, 2000, quant-ph/0008046.

[24] M. Christandl & R. Renner & A. Ekert; *A Generic Security Proof for Quantum key exchange*,2004, quant-ph/0402131.

[25] R. König, U. Maurer & R. Renner; *On the power of quantum memory*,2003, quant-ph/0305154.

Appendix A

Linear Operator formulae

The following lemma's presented will be helpful in calculations that involve linear operators.

The first lemma is known as the Baker-Campbell-Hausdorff formula. The second lemma is a descendent of the Baker-Campbell-Hausdorff formula. For illustration we will prove the first lemma.

Lemma A.0.2 *Let A and B be linear operators. Then*

$$e^A B e^{-A} = B + [A, B] + \frac{1}{2!}[A, [A, B]] + \dots .$$

This is called the Baker-Campbell-Hausdorff formula.

Proof.

$$\begin{aligned} e^A B e^{-A} &= \sum_{n=0}^{\infty} \frac{A^n}{n!} B \sum_{k=0}^{\infty} \frac{(-A)^k}{k!} \\ &= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{(-1)^{n-k} A^k B A^{n-k}}{k!(n-k)!} \\ &= \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) (-1)^{n-k} A^k B A^{n-k} \\ &= \sum_{n=0}^{\infty} \frac{1}{n!} [A_{(1)}, [A_{(2)}, \dots, [A_{(n)}, B]] \dots] \end{aligned}$$

□

Lemma A.0.3 *Let A, B be linear operators. If $[A, [A, B]] = [B, [A, B]] = 0$ then*

$$e^{A+B} = e^{-\frac{1}{2}[A,B]} e^A e^B$$

This is a descendent of the Baker-Campbell-Hausdorff formula.

The next lemma is a very simple one. If gives a trick to calculate the commutator of two operators when they have a certain structure.

Lemma A.0.4 *Let A, B and C be linear operators. Then*

$$[AB, C] = A[B, C] + [A, C]B$$

PROOF.

$$\begin{aligned}
[AB, C] &= ABC - CAB \\
&= ABC - ACB - CAB + ACB \\
&= A(BC - CB) + (AC - CA)B \\
&= A[B, C] + [A, C]B
\end{aligned}$$

□

The following lemma presents formulae for the linear operators $\frac{\partial}{\partial x}$ and $x\frac{\partial}{\partial x}$.

Lemma A.0.5 *Let $c, \tau \in \mathbb{C}$. Let $h(x)$ be a function over $\mathbb{R}$. Then*

$$e^{c\frac{\partial}{\partial x}} h(x) = h(x + c) \text{ and } e^{\tau\left(x\frac{\partial}{\partial x}\right)} h(x) = h(xe^{\tau}).$$

PROOF.

1. In general, the Taylor series of a function $f(x)$ about a point $x = a$ is given by

$$f(x) = \sum_{n=0}^{\infty} \frac{(x-a)^n}{n!} \frac{\partial^n f(a)}{\partial x^n}.$$

In the same manner we can give the Taylor series of $h(x + c)$ about the point x:

$$h(x + c) = \sum_{n=0}^{\infty} \frac{c^n}{n!} \frac{\partial^n h(x)}{\partial x^n} = \left(\sum_{n=0}^{\infty} \frac{(c\frac{\partial}{\partial x})^n}{n!} \right) h(x) = e^{c\frac{\partial}{\partial x}} h(x)$$

2. Following the reasoning of the first proof, the Taylor series of $h(xe^{\tau})$ about the point x is given by

$$h(xe^{\tau}) = h(x + x(e^{\tau} - 1)) = \sum_{k=0}^{\infty} \frac{(x(e^{\tau} - 1))^k}{k!} \frac{\partial^k h(x)}{\partial x^k} = \sum_{k=0}^{\infty} \frac{x^k (e^{\tau} - 1)^k}{k!} \frac{\partial^k h(x)}{\partial x^k}$$

On the other hand,

$$e^{\tau\left(x\frac{\partial}{\partial x}\right)} h(x) = \sum_{n=0}^{\infty} \frac{\tau^n}{n!} \left(x\frac{\partial}{\partial x} \right)^n h(x)$$

In the next definition a direct representation for $\left(x\frac{\partial}{\partial x}\right)^n$ is given.

Definition A.0.6 *For every $n \in \mathbb{N}$ with $n \geq 1$, $(x\partial)^n$ can be written as*

$$(x\frac{\partial}{\partial x})^n = \sum_{k=1}^{n} S_{n,k} x^k \frac{\partial^k}{\partial x^k},$$

where $S(n, k)$ is the stirling number of the second kind and is defined by

$$S(n, k) = \frac{1}{k!} \sum_{i=0}^{k-1} (-1)^i \binom{k}{i} (k - i)^n$$

We want to prove that

$$\sum_{k=0}^{\infty} \frac{x^k(e^\tau - 1)^k}{k!} \frac{\partial^k h(x)}{\partial x^k} = \sum_{n=0}^{\infty} \frac{\tau^n}{n!} \left(x \frac{\partial}{\partial x} \right)^n h(x).$$

For $k = 0$ the left hand side equals $h(x)$. The right hand side equals $h(x)$ for $n = 0$. We can now let the indices on both sides go from 1 to infinity instead of from 0 to infinity and therefore we can substitute the result form Definition A.0.6 into the obtained equation. The equation becomes

$$\begin{aligned}
\sum_{k=1}^{\infty} \frac{x^k(e^\tau - 1)^k}{k!} \frac{\partial^k h(x)}{\partial x^k} &= \sum_{n=1}^{\infty} \sum_{k=1}^{n} \frac{\tau^n}{n!} S_{n,k} x^k \frac{\partial^k h(x)}{\partial x^k} \\
\sum_{k=1}^{\infty} \frac{x^k(e^\tau - 1)^k}{k!} \frac{\partial^k h(x)}{\partial x^k} &= \sum_{k=1}^{\infty} \sum_{n=k}^{\infty} \frac{\tau^n}{n!} S_{n,k} x^k \frac{\partial^k h(x)}{\partial x^k} \\
\frac{(e^\tau - 1)^k}{k!} &= \sum_{n=k}^{\infty} \frac{\tau^n}{n!} S_{n,k}.
\end{aligned}$$

This last equation is one of the stirling identities and holds for $k \in \mathbb{N}, k \geq 1$.

□

Appendix B

Measurement in an orthonormal basis

We prove that if a measurement is done in an orthonormal basis then the operator describing the measurement is Hermitian and thus the measurement itself is a projective measurement. We find this in the following lemma.

Lemma B.0.7 *Let $n \in \mathbb{N}$ and $m_i \in \mathbb{R}$ for every $1 \leq i \leq n$. Suppose $\{|e_1\rangle, |e_2\rangle, \ldots, |e_n\rangle\}$ is an orthonormal basis of the Hilbert space of dimension n. If we define the observable M as*

$$M = \sum_{i=1}^{n} m_i P_{m_i} = \sum_{i=1}^{n} m_i |e_i\rangle\langle e_i|$$

then M is an Hermitian operator with spectral decomposition as above. P_{m_i} is the projector on the eigenspace of M with eigenvalue m_i.

Proof. Because $\{|e_1\rangle, |e_2\rangle, \ldots, |e_n\rangle\}$ is a basis, every state in the Hilbert space can be written as a linear combination of the basis elements. Suppose $|\psi\rangle = \sum_{i=1}^{n} \alpha_i |e_i\rangle$ and $|\phi\rangle = \sum_{i=1}^{n} \beta_i |e_i\rangle$ with $\alpha_i, \beta_i \in \mathbb{C}$ for all $1 \leq i \leq n$. Then

$$\begin{aligned}
\langle\psi|M|\phi\rangle &= \sum_{i=1}^{n} m_i \beta_i \langle\psi|e_i\rangle \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n} m_i \beta_i \overline{\alpha_j} \langle e_j|e_i\rangle \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n} m_i \beta_i \overline{\alpha_j} \delta_{ij} \\
&= \sum_{i=1}^{n} m_i \beta_i \overline{\alpha_i}.
\end{aligned}$$

On the other hand we have

$$\begin{aligned}
\langle M\psi|\phi\rangle &= \sum_{i=1}^{n} \overline{m_i\alpha_i}\langle e_i|\phi\rangle \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n} m_i\overline{\alpha_i}\beta_j\langle e_i|e_j\rangle \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n} m_i\beta_i\overline{\alpha_j}\delta_{ij} \\
&= \sum_{i=1}^{n} m_i\beta_i\overline{\alpha_i}.
\end{aligned}$$

so $\langle\psi|M|\phi\rangle = \langle M\psi|\phi\rangle$ and the operator M is Hermitian. Because $M|e_i\rangle = m_i|e_i\rangle$ the operator M is already described in its spectral decomposition where P_{m_i} is the projector on the eigenspace of M with eigenvalue m_i. □

Appendix C

Choice of δ in step 1 of the protocol

The probability that Alice encodes and Bob measures in the same basis is 1/2. The expected amount of values k where they encoded and measured in the same basis is $\langle k \rangle = \frac{1}{2}(4+\delta)n = (2+\frac{1}{2}\delta)n$. The probability that k is less than $2n$ is given by

$$P(k < 2n) = \frac{1}{2}^{(4+\delta)n} \sum_{k=0}^{2n-1} \left(\begin{array}{c} (4+\delta)n \\ k \end{array} \right).$$

We can say the following about this probability.

Theorem C.0.8 *There are bounds on the probability $P(k < 2n)$. In this theorem we will give two of them.*

$$P(k < 2n) \leq \frac{4+\delta}{8n\delta^2}$$

$$P(k < 2n) \leq \exp\left(-\frac{\frac{1}{4}\delta^2 n}{4+\delta} \right)$$

Proof. If n is very large then the probability distribution of k approximately becomes a normal distribution with mean $\mu = (4+\delta)n \cdot \frac{1}{2} = (2+\frac{1}{2}\delta)n$ and variance $\sigma^2 = (4+\delta)n \cdot \frac{1}{2} \cdot \frac{1}{2} = (1+\frac{1}{4}\delta)n$.

The probability $P(k < 2n)$ can now be expressed as

$$\begin{aligned} P(k < 2n) &= P(k \leq 2n | \mu, \sigma^2) \\ &= \frac{1}{2}\left(P(k \leq 2n | \mu, \sigma^2) + P(k \geq 2n + \delta n | \mu, \sigma^2) \right) \\ &= \frac{1}{2} P(|k - \mu| \geq \frac{1}{2}\delta n | \mu, \sigma^2) \end{aligned}$$

Chebychev says that if X is a random variable with finite mean μ and finite variance σ^2 then it holds for every $m > 0$ that

$$P(|X - \mu| \geq m) \leq \frac{\sigma^2}{m^2}.$$

With this we find that

$$\begin{aligned} P(k < 2n) &= \frac{1}{2}P(|k-\mu| \geq \frac{1}{2}\delta n) \\ &\leq \frac{(1+\frac{1}{4}\delta)n}{\frac{1}{2}(\delta n)^2} \\ &= \frac{4+\delta}{2n\delta^2} \end{aligned}$$

On the other hand, we have Chernoff who says that if $X = \sum_{i=1}^{(4+\delta)n} X_i$ where all X_i are identically and independently distributed with $P(X_i = 0) = P(X_i = 1) = \frac{1}{2}$ then

$$P(X - \frac{1}{2}(4+\delta)n \leq \lambda) \leq \exp\left(-\frac{\lambda^2}{(4+\delta)n}\right).$$

This gives us that

$$P(k - \frac{1}{2}(4+\delta)n \leq -\frac{1}{2}\delta n) \leq \exp\left(-\frac{(\frac{1}{2}\delta n)^2}{(4+\delta)n}\right) = \exp\left(-\frac{\frac{1}{4}\delta^2 n}{4+\delta}\right).$$

□

Only for small n the first bound is better.

Appendix D

The Capacity of an n-ary Symmetric Classical Channel

Suppose we have a classical channel over which Alice sends n bits at once to Bob. Let X represent the bit string of length n sent by Alice and Y represents the bit string of length n received by Bob. The capacity of the channel is given by

$$C = \max_{p(x):x\in X} I(X;Y)$$

where $I(X;Y)$ is the mutual information of X and Y and is defined by

$$I(X;Y) = \sum_{x\in X}\sum_{y\in Y} p(x)p(y|x)\log\left(\frac{p(y|x)}{\sum_{x'\in X} p(x')p(y|x')}\right).$$

Let x_j with $j \in \mathcal{J} = \{0, 1, \ldots, 2^n - 1\}$ be a possible bit string sent by Alice and y_j a possible bit string received by Bob. A channel is a symmetric channel if it has the following properties.

$$\forall_{j\in\mathcal{J}}\left[p(x_j|0), \ldots, p(x_j|y_{2^n-1}) \text{ is a permutation of } p(x_0|y_0), \ldots, p(x_0|y_{2^n-1})\right]$$

$$\forall_{j\in\mathcal{J}}\left[p(x_0|y_j), \ldots, p(x_{2^n-1}|y_j) \text{ is a permutation of } p(x_0|y_0), \ldots, p(x_{2^n-1}|y_0)\right].$$

The following theorem gives the capacity of an n-ary symmetric channel.

Theorem D.0.9 *For a symmetric n-bit channel (n-ary symmetric channel) the capacity is given by*

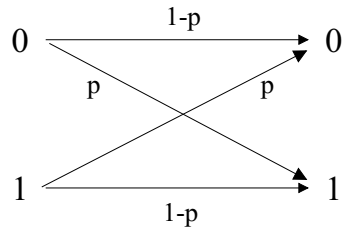
$$C_{nSC} = n + \sum_{y\in Y} p(y|x_0)\log p(y|x_0).$$

The capacity of the binary ($n = 2$) symmetric channel (BSC) is given by

$$C_{BSC} = 1 - h(p)$$

where p is the transition probability $p(1|0) = p(0|1)$ as in the figure below.

Figure D.1: Binary Symmetric Channel



PROOF. For symmetric channels capacity is achieved when the input X has a uniform distribution, so $\forall_{j\in\mathcal{J}} p(x_j) = \frac{1}{2^n}$. This can be seen in the following way

$$\begin{aligned} H(Y|X) &= -\sum_{x\in X}\sum_{y\in Y} p(x)p(y|x)\log p(y|x) \\ &= -\left(\sum_{x\in X} p(x)\right)\sum_{y\in Y} p(y|x_0)\log p(y|x_0) \\ &= -\sum_{y\in Y} p(y|x_0)\log p(y|x_0). \end{aligned} \tag{D.1}$$

Equation D.1 is independent of the input distribution. We further see that

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) \\ &\leq \log 2^n - H(Y|X) \\ &= n - H(Y|X) \end{aligned}$$

so $C_{nSC} \leq n - H(Y|X)$. We substitute $p(x_j) = \frac{1}{2^n}$ in $H(Y)$.

$$\begin{aligned} H(Y) &= -\sum_{y\in Y} p(y)\log p(y) \\ &= -\sum_{y\in Y}\left(\sum_{x\in X} p(x)p(y|x)\right)\log\left(\sum_{x\in X} p(x)p(y|x)\right) \\ &= -\sum_{y\in Y}\left(\sum_{x\in X} \frac{1}{2^n}p(y|x)\right)\log\left(\sum_{x\in X} \frac{1}{2^n}p(y|x)\right) \\ &= -\sum_{y\in Y} \frac{1}{2^n}\log\frac{1}{2^n} \\ &= n \end{aligned}$$

This means that capacity is reached when the input distribution is uniform. If we substitute the uniform input distribution into the formula for the capacity we find that

$$C_{nSC} = n + \sum_{y\in Y} p(y|x_0)\log p(y|x_0).$$

A special case is $n = 1$. The capacity of this binary symmetric channel (BSC) is given by

$$C_{BSC} = 1 + p \log p + (1 - p) \log(1 - p) = 1 - h(p).$$

□

Appendix E

A calculation on Gaussian distributions

The probability distribution of a Gaussian distribution with mean μ and variance σ^2 is given by

$$P(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right).$$

Theorem E.0.10 *Let the variable X be distributed according to a Gaussian distribution with mean Y and variance σ_A^2. Let Y be distributed according to a Gaussian distribution with mean μ and variance σ_B^2. Then X is distributed according to a Gaussian distribution with mean μ and variance $\sigma_A^2 + \sigma_B^2$.*

Proof. The probability that $X = x$ is given by

$$\begin{aligned} P(X=x) &= \int_y P(y)P(X=x|Y=y)dy \\ &= \frac{1}{2\pi\sigma_A\sigma_B}\int_y \exp\left(-\frac{(y-\mu)^2}{2\sigma_B^2}\right)\exp\left(-\frac{(x-y)^2}{2\sigma_A^2}\right)dy \end{aligned} \tag{E.1}$$

where

$$\begin{aligned} \frac{(y-\mu)^2}{2\sigma_B^2} + \frac{(x-y)^2}{2\sigma_A^2} &= \frac{1}{2\sigma_A^2\sigma_B^2}\left((\sigma_A^2+\sigma_B^2)y^2 - 2(\sigma_A^2\mu + \sigma_B^2 x)y + \sigma_A^2\mu^2 + \sigma_B^2x^2\right) \\ &= \frac{1}{2\sigma_A^2\sigma_B^2}\left((\sigma_A^2+\sigma_B^2)\left(y - \frac{\sigma_A^2\mu+\sigma_B^2x}{\sigma_A^2+\sigma_B^2}\right)^2 - \frac{(\sigma_A^2\mu+\sigma_B^2x)^2}{\sigma_A^2+\sigma_B^2} + \sigma_A^2\mu^2 + \sigma_B^2x^2\right) \\ &= \frac{\sigma_A^2+\sigma_B^2}{2\sigma_A^2\sigma_B^2}\left(y - \frac{\sigma_A^2\mu+\sigma_B^2x}{\sigma_A^2+\sigma_B^2}\right)^2 + \frac{(x-\mu)^2}{\sigma_A^2+\sigma_B^2}. \end{aligned}$$

If we substitute this result into Equation E.1 we find

$$\begin{aligned} P(X=x) &= \frac{1}{2\pi\sigma_A\sigma_B}\exp\left(-\frac{(x-\mu)^2}{\sigma_A^2+\sigma_B^2}\right)\int_y \exp\left(-\frac{\sigma_A^2+\sigma_B^2}{2\sigma_A^2\sigma_B^2}\left(y-\frac{\sigma_A^2\mu+\sigma_B^2 x}{\sigma_A^2+\sigma_B^2}\right)^2\right)dy \\ &= \frac{1}{2\pi\sigma_A\sigma_B}\sqrt{\frac{2\pi\sigma_A^2\sigma_B^2}{\sigma_A^2+\sigma_B^2}}\exp\left(-\frac{(x-\mu)^2}{\sigma_A^2+\sigma_B^2}\right) \\ &= \frac{1}{\sqrt{2\pi(\sigma_A^2+\sigma_B^2)}}\exp\left(-\frac{(x-\mu)^2}{\sigma_A^2+\sigma_B^2}\right). \end{aligned}$$

□

We can conclude that X is distributed according to a Gaussian distribution with mean μ and variance $\sigma_A^2+\sigma_B^2$.