NTNU

Norwegian University of
Science and Technology

# Security of quantum key distribution source

**Eivind Sjøtun Simonsen**

Master of Science in Electronics
Submission date: June 2010
Supervisor: Johannes Skaar, IET
Co-supervisor: Lars Lydersen, IET

Norwegian University of Science and Technology
Department of Electronics and Telecommunications

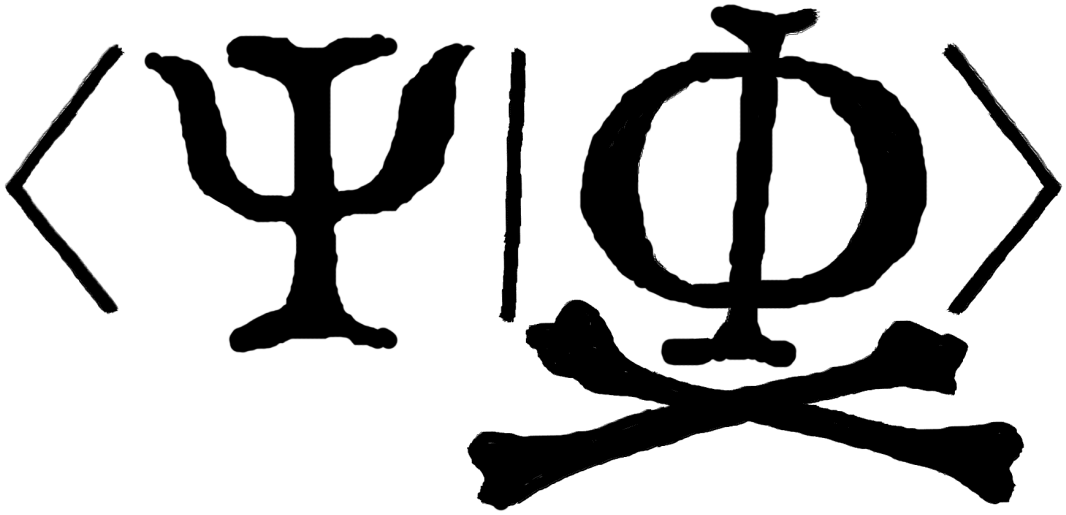
# Problem Description

Quantum key distribution (QKD) allows to securely exchange a secret key over an open optical channel. The key can subsequently be used to encrypt information, allowing for unconditionally secure communication. It can be proven using quantum theory and information theory that QKD is perfectly secure if there are no imperfections in the system. When the imperfections are small, QKD remains secure. However, this bound needs to be analyzed and quantified in detail.

The student will participate in the development of such a security proof, emphasizing on the source side of the system. In particular, a certain source security parameter needs to be quantified or bounded for a realistic system such as the one at NTNU. This involves calculating the source parameter in the presence of phase and amplitude fluctuations. In addition the student will participate in the ongoing development of an uncrackable QKD system.

Assignment given: 15. January 2010
Supervisor: Johannes Skaar, IET

# Security of quantum key distribution source



Master thesis

Eivind Sjøtun Simonsen

June 11, 2010

Supervisors:
Prof. Johannes Skaar
Post.doc. Vadim Makarov

Norwegian University of Science and Technology
Department of Electronics and Telecommunications

# Abstract

Cryptography has begun its journey into the field of quantum information theory. Classical cryptography has shown weaknesses, which may be exploited in the future, either by development in mathematics, or by quantum computers. *Quantum key distribution* (QKD) is a promising path for cryptography to enable secure communication in the future. Although the theory of QKD promises absolute security, the reality is that current quantum crypto systems have flaws in them, as perfect devices have proven impossible to build. However, this can be taken into account in security proofs to ensure security, even with flaws.

Security loopholes in QKD systems are being discovered as development progresses. Nevertheless, the system being built at NTNU is intended to address them all, creating a totally secure system. During this thesis, work was continued assembling the interferometer which is the basis for encoding qubits. It was fully connected on an optical table, and interference was obtained.

Concerning theoretical work, calculations for a photon source specific parameter was carried out. It consisted of expanding previous framework and applying the results in both an established security proof, and a recent generalization of this proof. Two source effects were in focus, the lasers random phase and its fluctuating pulse intensity. Where analytical derivation was no longer possible, Matlab was used for numerical calculations. Under the conditions of the framework and proofs this thesis lies on, randomized phase turned out to have a negligible improvement over the case of non-random phase. Fluctuating amplitude showed a larger effect, reducing system performance. The input parameters were extreme, thus in a realistic situation it should not affect system performance significantly. However, these fluctuations must be taken into account when proving system security.

# Acknowledgement

This project was carried out for the *Quantum Hacking group*. The group's main research focus is security of quantum key distribution. The people in this group were a pleasure to get to know. (To those who consider working with them: You won't regret it!)

I want to thank my supervisors Johannes Skaar and Vadim Makarov for having orthogonal working hours. Johannes answering my emails before my day started. Vadim was still available in the lab when hours became late. And thank you Line for being patient as my working hours gradually phase shifted towards Vadim's.

# Contents

# List of figures

# 1 Introduction

Alice and Bob[1] have the need to speak with each other secretly without Eve[2] picking up the message. This calls for the message to be encrypted so that only Bob and Alice know what the message is, while Eve, unable to decrypt it, is left in the dark.

## 1.1 State of cryptography today[3]

There are two ways of encrypting messages sent between Alice and Bob. The most secure way is by using *symmetric ciphers*. Here both Alice and Bob share the same key and can encrypt and decrypt messages with it. The problem with this method is sending this key between them. This is why *asymmetric ciphers* are used. When Alice wants to share something with Bob securely without having a secure key or a way to distribute it, Alice asks Bob to give her a *public key*. This key is made in such a way that it can only encrypt messages, while Bob keeps a *private key* secretly which he can use to decrypt the message. To generate the public key Bob uses ideally a one-way function to calculate it from the private key. This way one can make a public key based on the private key, but not obtain the private key from the public key. And this is the core: All current functions are possible to reverse. The security is based on the time it takes to reverse it, which is exponential using known algorithms on a classical computer. It is said to be *computationally secure*. This means that if you have a long enough key it could take the lifetime of the universe to crack it. Of course, at the end of existence, cracking a key is probably not our main concern. So unless there is a faster way to do this, current asymmetric ciphers are secure.

There *is* a faster way. Using the laws of quantum physics there are suggested algorithms which could crack at least the common asymmetric encryptions (such as RSA[4] [2]) using only polynomial time [3], i.e. within reasonable time. This however requires the construction of a *quantum computer*. Currently there are only suggested ways of doing quantum computation, but nobody knows how to make a large scale computer, or if it is possible at all. In addition, there exists asymmetric encryption (e.g. McEliece cryptosystem [4]) which even a quantum computer may use exponential time to crack [5]. This is still to be

[1] Alice and Bob are the standard names for sender and receiver for secure communication in cryptography.

[2] Eve is the standard name for eavesdropper.

[3] For a broader discussion see [1], which my discussion is partially based on.

[4] RSA is a public-key encryption based on the exponential time it takes for classical computers to factorize large prime numbers. It is named after its inventors Rivest, Shamir, and Adleman [2].

proven. On the other hand, the non-existence of *classical* algorithms which would crack asymmetric encryption in less than exponential time, is not proven either.

## 1.2 Motivation

The obvious reason for studying quantum cryptography is that if today's cryptography is cracked, either by mathematicians or by quantum computers, *quantum cryptography* already in place has that problem sorted out. According to the theory of quantum cryptography it is possible to make uncrackable key distribution. This is also what quantum cryptography in reality is; key sharing. The cryptography is still classical, using symmetric ciphers, but the problem of distributing the key is solved using quantum physics. Hence the term *quantum key distribution* (QKD), which is more accurate.

Why is secure communication important? For the military the reasons are obvious; Alice and Bob being allies, while Eve being the enemy. Other reasons may be commercial or governmental secrets. However, the most obvious reasons for us are money and privacy. Privacy because certain things we think or do, can be abused if such information falls into the wrong hands. When it comes to economy, if the banks are cracked, it could lead to malicious persons not only stealing money, but creating them from nothing. Stealing money would be a huge problem itself, but if one produces more money, the value of them decreases. This could lead to a tremendous inflation, and the world economy could collapse. Hence, QKD could potentially save the world!

As the other extreme, it could turn out that current encryption is proven computationally secure and building quantum computers proves to be impossible. This would not mean that the research was all a waste. Since quantum physics is not completely explored, one can still learn much about Nature and techniques which may be usable for other purposes. And, if current cryptography is cracked, dare we wait until then to develop a secure system? If we wait all previously recorded communication could be cracked retroactively and secret information leaked. Therefore we need to be prepared in advance, in case of this event.

## 1.3 Previous project

My autumn semester project report *Decoy state generator for quantum key distribution system* [6] consisted of the assembly of the signal source of the QKD system. The laser in the light source allows an attack called the *photon number splitting* attack. Countermeasures for this loophole will be done by using a *decoy state* method. This is dependent on the pulses being of varying intensity and is realized by using an intensity modulator.

Experiments were done with the laser and intensity modulator in order to characterize their properties, and create the electronic circuits required for them to work. The intensity modulator needed to be biased permanently with a battery powered circuit. The laser driver needed to be tuned for the laser to output the required 100 ps pulses. The laser operation was characterized in the time and spectral domains.

The light source and electronics were mounted into the Alice's rack case. Together with her counterpart Bob, they will form a complete QKD system, hopefully leaving the evil

Eve unable to hack it.

## 1.4 This thesis

This project partially is a continuation of building the QKD system. It involves setting up the interferometers in both Alice and Bob (see chapter 5). The major part is of more theoretical nature, analyzing the security of the source. As mentioned in the previous section, the laser is not an ideal source for QKD. However, it is the best off-the-shelf device available, which is why it is used in practical setups. Its non-ideal property could threaten security. However, taking these properties into account, security can still be proven.

In this thesis, calculations concerning random phase and fluctuating amplitude will be carried out. This is motivated by the properties of the laser. It is designed to have random phase, but also showed unwanted intensity fluctuations. The results will be plotted and their impact on the QKD system being built will be discussed.

The work from the autumn semester project, and parts from this thesis, were presented as a poster (appendix A) at the Norwegian electro-optics meeting in Ålesund, April 2010.

# 2 Theory

## 2.1 How quantum key distribution works

Quantum cryptography promises unconditional[1] security. This security is dependent on the key and the key distribution system. In 1917, Gilbert Vernam invented the *One-time pad* [7]. It encrypts the message using XOR operation[2] on the message and a random symmetric key. If the key is at least as long as the message, and only used once, it is impossible to crack. This is true, as long as Eve does not have a copy of the key. With a *classical* communication channel it is possible for Eve to obtain a copy of the key without Alice and Bob knowing about it. This is where QKD comes in to play. Based on the *no cloning theorem*[3] of physics, Eve is unable to copy a key, sent between Alice and Bob, without them noticing. There are different ways of realizing this. The following explanation is based on the *Bennett-Brassard 1984* (BB84) protocol.

### 2.1.1 The BB84 protocol

In 1984, Charles Bennett and Gilles Brassard proposed a protocol for distributing a key securely through a quantum channel [9]. Information sent through a quantum channel is encoded as *quantum bits* or *qubits* which is the quantum version of the classical bits (explained in section 2.2.1). When measuring, the only possible outcome is one of the orthogonal states in the basis of the measuring operator.[4] After the measurement the qubit is left in that state. In the case of photons, they are usually destroyed.

Qubits can be represented in many ways. The BB84 protocol [9] uses polarized light as qubits. The photons are sent with one of four different polarizations (states); 0°, 45°, 90° and 135°. The two first polarizations correspond to the 0 bit and the latter two to 1 bit. 0° and 90° is called the + basis, while 45° and 135° is called the × basis. Now each basis consists of two orthogonal polarizations; $|0_+\rangle$ and $|1_+\rangle$, and $|0_\times\rangle$ and $|1_\times\rangle$. If Alice sends a qubit, say $|0_+\rangle$ (0 in + basis), and Bob measures the qubit in the same basis, he measures 0. Now if he instead tries to measure it in the × basis, the incoming photon, which is 0°

[1] Unbreakable even with no limit on computational power.
[2] XOR - eXlcusive OR: adds the message and key modulo 2. $(0+0=1+1=0, 0+1=1+0=1)$.
[3] It is impossible to copy an arbitrary unknown quantum state [8].
[4] A measuring operator is a matrix describing the physical measuring operation.

polarized, is a superposition of the two polarizations of this basis.

$$|0_+\rangle = \frac{1}{\sqrt{2}}|0_\times\rangle - \frac{1}{\sqrt{2}}|1_\times\rangle \tag{2.1}$$

This gives a 50/50 percent chance for the photon to be measured as 0 or 1. Eve must not know in advance which basis Alice and Bob chooses, because then she could always choose the right basis, measure the photon and resend it in the same state to Bob. For this reason Alice and Bob do not know which basis the other has chosen. The basis choice should not be possible to predict by Eve, hence it is randomly selected. Both Alice and Bob choose basis at complete random, so there is only 50% chance of them choosing the same basis. After the key is sent, Alice and Bob anounce on a public channel which basis they chose without sharing which bit values were sent or recieved. They keep the bits where they have the same basis, and discard the rest. They now share the same secret key (see figure 2.1).

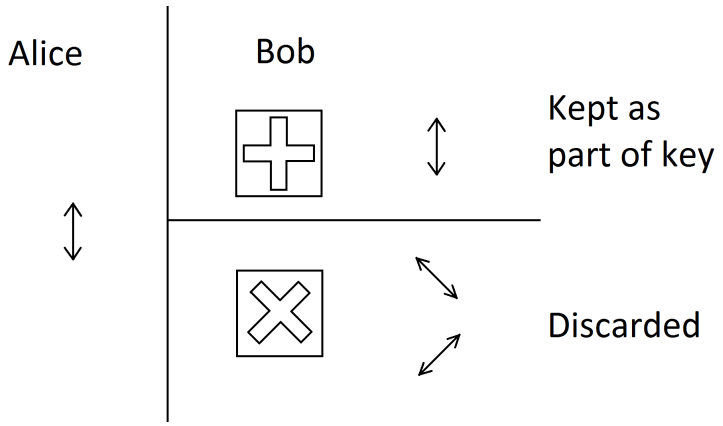



Figure 2.1: Alice has randomly selected $|1_+\rangle$ and sends it to Bob. If he choose in the same basis, he will measure the correct bit value.

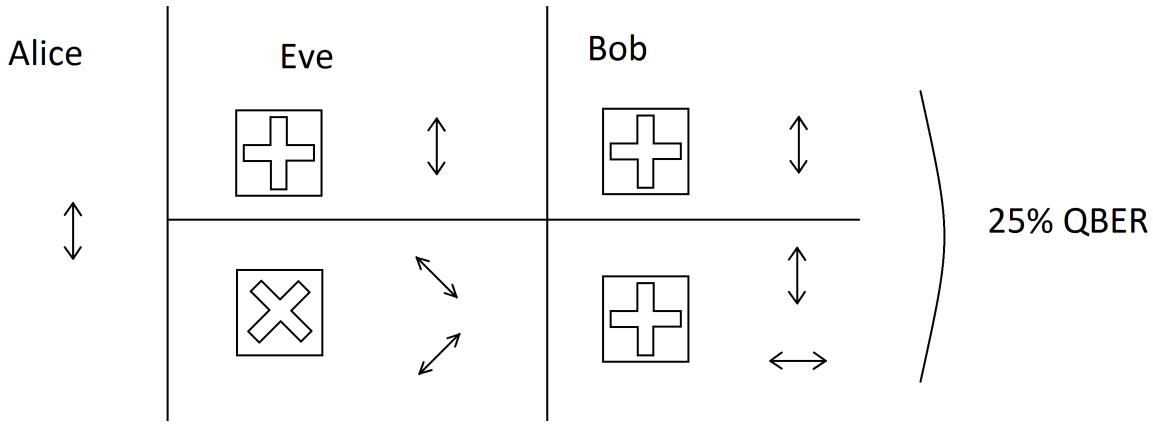



Figure 2.2: If Eve intercepts communication, for the bits which Alice and Bob use the same basis, she will introduce 25% QBER.

### 2.1.2 Eve attacks

Now, if Eve puts herself in between Alice and Bob, there are numerous things she can do to try and gain information about the key.[5] One way is to intercept the photons, and resend them. Choosing to measure in the same two bases as Alice and Bob, she also has 50% chance of choosing the right basis. Since the measurement destroys the photons, she has to resend all photons recieved. These bits are sent with a basis which has a 50% chance of being the same as Alice's. If we look only at the photons which are not discarded by Alice and Bob, 50% of these photons will be in the wrong basis. This causes Bob to measure the wrong bit value, with 50% chance. 25% of the bits Alice and Bob choose to keep will then have different values. Hence, Eve introduces a *quantum bit error rate* (QBER) of 25%. So, if Alice and Bob measure too much QBER, they know Eve is eavesdropping, and will abort communication (see figure 2.2).

## 2.2 Quantum mechanics

In the section a few basic principle in quantum mechanics will be explained.

### 2.2.1 Quantum bits

From classical information theory we have bits which can be either 0 or 1. In quantum information theory the equivalent is *quantum bits* or *qubits* [11, p. 80]. These are two dimensional quantum mechanical states. We can encode the bits as qubits using orthogonal states, with notation $|0\rangle$ and $|1\rangle$.[6] The advantage qubits give is that they can be in a superposition

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \tag{2.2}$$

where $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$. Trying to measure on this state gives 0 with probability $|\,\langle 0|\psi\rangle\,|^2 = |a|^2$ and 1 with probability $|\,\langle 1|\psi\rangle\,|^2 = |b|^2$.

Examples of qubits are photon polarization and photon phase.

### 2.2.2 Photon number states

Another important quantum state is the *photon number states*. The basic concept of QKD (section 2.1) is understood by the use of single photons. Unfortunately, true single photon sources have not exceeded experimental stage, and are not used in QKD systems today. Therefore we need to describe state which contain a number of photons. It is denoted $|n\rangle$ where $n$ refers to the number of photons in that state. The states are orthogonal; $\langle m|n\rangle = \delta_{mn}$.

[5] A review of different attacks can be found in [10].

[6] This is known as the bra-ket notation. $\langle c|$ (*bra c*, bra with label c) represents the vector $[c_0^*\ c_1^*\ ...]$. $|c\rangle$ (*ket c*, ket with label c) represents the vector $[c_0\ c_1\ ...]^T$.

### 2.2.3 Coherent states

In practical QKD attenuated pulsed lasers, which are coherent sources, are used. They are described using *coherent states*. The laser output follows the Poisson distribution [12, p. 463-464] which is expressed using infinite dimensional state vectors [13, p. 190]

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{2.3}$$

where $|\alpha| = \sqrt{\mu/2}$. $\mu$ is the expected photon number of a pulse. The probability for a pulse to contain exactly $n$ photons is given as

$$p(n) = |\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!} \tag{2.4}$$

The reason why coherent states are important is that they model the laser with the unwanted property of emitting multi photon pulses. If a pulse contains two or more photons in the same qubit state, there exists redundant information, which can be exploited by Eve as explained in section 2.3.1.

### 2.2.4 A few definitions

#### Pure state

A *pure state* is a state which can be expressed as a superposition of eigenstates [11, p. 100]

$$|\psi\rangle = \sum_i \lambda_i |i\rangle \tag{2.5}$$

where $\sum_i |\lambda_i|^2 = 1$.

#### Mixed state

A *mixed state* is a state which cannot be expressed in terms of a vector, but is expressed as a density matrix [11, p. 100]

$$\rho = \sum_i p_i \rho_i \tag{2.6}$$

where $\sum_i p_i = 1$, $p_i < 1$. $\rho_i$ is a pure state and can be expressed as $|\psi_i\rangle \langle\psi_i|$.[7] The mixed states describe states which are not completely known.

#### Entangled state

An *entangled state* is a state which cannot be expressed as a product state[8] [11, p. 95].

$$|\Psi_{ent}\rangle = \frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}} \neq |a\rangle|b\rangle \tag{2.7}$$

[7] $|\Psi\rangle\langle\Phi|$ is known as the outer product. It follows the same multiplication rules as the inner product $\langle\Psi|\Phi\rangle$, but instead of a scalar, it produces a matrix.

[8] A product state $|a\rangle|b\rangle$ is also written as $|ab\rangle$.

Entangles state pairs are also known as Bell states or EPR[9] pairs, explained in [11, p. 111-117], and are central in QKD. It arose from the EPR paradox, and the solution is that measuring half the pair instantaneously collapses the other half to the corresponding state. We can see this from (2.7), if we use a measuring operator $M_0 = |0\rangle\langle 0|$ on one of the halves, the state after is $|0\rangle|0\rangle$ (see [11, p. 84]):

$$\begin{aligned} |\Psi_0\rangle &= \frac{M_{0,A}|\Psi_{ent}\rangle}{\sqrt{\langle\Psi_{ent}| M_{0,A}^\dagger M_{0,A}|\Psi_{ent}\rangle}} = \frac{M_{0,A}}{1/\sqrt{2}}\frac{|0_A0_B\rangle + |1_A1_B\rangle}{\sqrt{2}} \\ &= |0_A\rangle\langle 0_A|0_A\rangle|0_B\rangle + |0_A\rangle\langle 0_A|1_A\rangle|1_B\rangle = |0_A0_B\rangle \end{aligned} \tag{2.8}$$

### Fidelity

The *fidelity* is a distance measure between two states [14]. If equal to one, the states are equal, if equal to zero they are orthogonal. It is defined as

$$F(\rho,\sigma) = \left(\mathrm{tr}\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right)^2 \tag{2.9}$$

where tr refers to the trace defined as $\mathrm{tr}(A) = \sum_i A_{ii}$, and $0 \leq F(\rho,\sigma) \leq 1$. Fidelity is central in proving security, as we will see in the next sections. It gives a measure for how easy Eve can tell the difference between bases and gain information about the key.

### Purification

A purification $|\psi_A\rangle$ of $\rho_A$ constructed by introducing a reference system $\rho_R$ of the same dimension [11, p. 110]. We have

$$|\psi_A\rangle = \sum_i \sqrt{p_i}|i_A\rangle|i_R\rangle \tag{2.10}$$

where $\rho_A = \sum_i p_i|i_A\rangle\langle i_A|$ and $\rho_R = \sum_i p_i|i_R\rangle\langle i_R|$. Moving from mixed states to pure states, we move from a subsystem for which we have little knowledge of, to a larger system for which we can know everything about.

## 2.2.5 Distinguishing between states

Having two pure quantum states $|\psi_A\rangle$ and $|\psi_B\rangle$ the difference between them can be measured by the inner product of the states $\langle\psi_B|\psi_A\rangle$. If this is equal to one, the states are identical. Mixed states cannot be expressed as vectors, but as density matrices, eg. $\rho_A$ and $\rho_B$. In general, letting $|\psi_A\rangle$ and $|\psi_B\rangle$ be any purifications of these, we have

$$|\langle\psi_B|\psi_A\rangle|^2 \leq F(\rho_A,\rho_B) \tag{2.11}$$

By Ulhmann's theorem[10] there exists an optimal purification for each, $|\psi_{A,O}\rangle$ and $|\psi_{B,O}\rangle$, such that

$$|\langle\psi_{B,O}|\psi_{A,O}\rangle|^2 = F(\rho_A,\rho_B) \tag{2.12}$$

Similar to the case of pure states, if $F(\rho_A,\rho_B) = 1$ then $\rho_A = \rho_B$.

[9] EPR - Einstein–Podolsky–Rosen

[10] Ulhmann's theorem is explained in [11, p. 410]

## 2.3 Security

*Unconditional security* is the essential property QKD supplies to cryptography. What is meant by unconditional, is that Eve is assumed to only be limited by the laws of physics. Having access to both the quantum and classical communication channels, she may preform any measurement and send any signal suitable to crack the system. In addition she is allowed to have unlimited computational power, including quantum computers. This, of course, is a very strict regime for QKD to work under, especially since all man-made devices are subjects to flaws.

For a perfect system the security of QKD is intuitive, accepting that any Eve will disturb the system. However, proving the security is not straight forward. We will first look at entangled based QKD. We can write an entangled state as

$$|\psi_+\rangle = \frac{|0_{+,A}0_{+,B}\rangle + |1_{+,A}1_{+,B}\rangle}{\sqrt{2}} = \frac{|0_{\times,A}0_{\times,B}\rangle + |1_{\times,A}1_{\times,B}\rangle}{\sqrt{2}} = |\psi_\times\rangle \tag{2.13}$$

Alice creates these states, keeps the first half of the pair (labeled A), and sends the second half (labeled B) to Bob. The middle equality follows by the definition of the states in section 2.1.1. Because of this equality, if neither Alice nor Bob measures the state, they are indistinguishable. Hence, Eve cannot gain any information about whether + of × basis is used; it has not been decided yet. The basis, and bit value, is decided by the first measurement done by either Alice or Bob.

Shor and Preskill proved security for entangled based QKD by utilizing quantum error correcting codes (QECC) [15]. In QECC, redundant information is sent as multiple entangled qubits. If only a few of them is changed, the others contain enough information to correct it. Transmitting redundant qubits in QKD is not a good idea as this would give Eve the ability of gaining information. In an entangled based QKD system, however, Alice keeps the first half of an entangled pair, while the other is sent to Bob and can be affected by Eve.[11] The redundant information is kept by Alice, prohibiting Eve access. Alice and Bob use a part of the key to estimate the error. If the error introduced by Eve is small enough, they can correct it for the rest of the bits creating a shorter key for which Eve has no information. Hence, secure key generation is obtained. However, if the error is too large, secure key sharing can not be guaranteed, and communication is aborted.[12]

This proof however, applies only to true single photon sources,[13] and does not take into account any other error sources than those introduced by Eve. Unfortunately, flawless systems are impossible to build, and we have to assume pessimistically that any flaw may help Eve to apply an attack. Fortunately, security can still be proven, taking the imperfections into account, as shown by Koashi who uses the *Heisenberg's uncertainty principle* to prove security [16]. The interesting result for this thesis is that it proves security for the case where the source leaks information about basis choice. This leakage is quantified by a source parameter $\Delta$. Having two basis states, $\rho_0$ and $\rho_1$,[14] created by Alice, this relates to the fidelity by

$$1 - 2\Delta \leq \sqrt{F(\rho_0, \rho_1)} \tag{2.14}$$

[11] Here, Eve may also be the environment.

[12] Obstructing communication is also a possible attack. But there is a much simpler way of doing that than introducing errors during communication. It involves the fiber between Alice and Bob, and scissors.

[13] The entangled pair is produced by parametric conversion of a single photon into two.

[14] The labeling 0 and 1 for basis is used to clarify that we may use any (ideally) orthogonal basis.

Koashi uses the parameter $\Delta$ when he continues to find the key generation rate. However in this thesis, as we will see in section 2.5, it is more convenient to use the fidelity directly.

True single photon sources, which have no basis choice leakage, are still in the experimental stage. Therefore, in practical QKD, attenuated lasers are used. They are coherent sources which follows the Poisson distribution emitting photon number states (see section 2.2.3). This causes the source to have a basis choice leakage. It appears because the source will have a finite probability of sending redundant photons through the channel. As a consequence of the this, a possible attack is the *photon number splitting* attack.

### 2.3.1 Photon number splitting attack

The Poisson distribution of the laser leaks information about basis choice. This is due to the multi photon pulses such a source emit. The *photon number splitting* (PNS) attack is given as an example of an attack which utilizes this [17, 18].

In figure 2.3 we see a scheme over the attack. If Eve intercepts communication, she could steal one photon from each pulse, and store it until Alice and Bob announce which bases they used. Then Eve can measure her photon in the correct basis and obtain the correct key value. The pulses containing only one photon she simply blocks so they are counted as loss by Alice and Bob. This high loss could reveal an attack. To compensate, Eve is considered to use a lossless channel for the photons she sends to Bob. This way Eve can obtain full key information, without Alice and Bob knowing. Fortunately, there is a method for detecting this attack, namely by using *decoy states*.

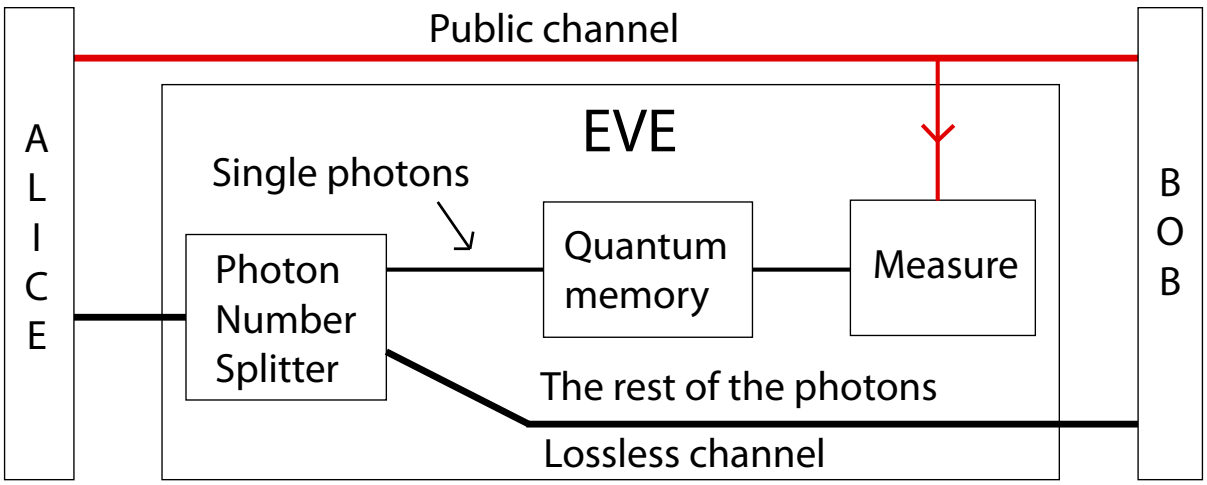



Figure 2.3: Photon number splitting attack

### 2.3.2 Decoy states

This explanation is included as decoy states are mentioned a few times, and since fluctuating pulse intensity will be treated, although not with decoy states in mind. However, this gives a hint for possible expanded uses of the methods concerning fluctuating pulse intensity in section 3.2.

A proper way of handling the PNS attack is by using *decoy states* [19]. It is based on the fact that Eve will always keep/block one photon as long as at least one is present. Alice and Bob do QKD with BB84 using $\mu < 1$. Randomly and intentionally, Alice sends decoy states with $\mu' \geq 1$ with a certain probability. These pulses will then often have multiple photons. As they are random, Eve has no way of knowing which pulses are signal, and which are decoy. However, the weaker signal pulse is more likely to contain only one photon, and is therefore more likely to be blocked. This gives different yield (or transmittance) for the decoy and signal pulses. After a sequence, Alice announces publicly which pulses were decoy states. By public discussion with Bob, they estimate the yield for both the BB84 signal and the decoy. If Eve is not interfering, they should be equal. If however, the decoy pulses have a much higher yield than the signal, they know Eve is snapping up photons and they abort communication. To simplify; by measuring the photon number statistics, a PNS attack can be discovered.

This idea was modified and optimized by [20, 21]. They suggest a *two decoy state* with two weak decoy states (weak+vacuum) $v_1$ and $v_2$. This method is very close to the performance of an asymptotic decoy method using infinite number of decoy states, which gives maximum key generation rate but is more difficult to implement. The photon numbers of the decoy states and the signal state are bounded by

$$\begin{aligned} 0 \leq v_2 \leq v_1, \\ v_1 + v_2 < \mu, \\ \mu \in (0, 1]. \end{aligned} \tag{2.15}$$

The optimum values of these parameters are dependent on implementation, and vary with line loss and thus transmission distance.

## 2.4 Starting point for calculations

To calculate security and QKD system performance, we need to find the basis leakage which quantifies the the information leaked to Eve. To this we need to find the fidelity of the output states. But first we need to model the source.

The starting point for the calculations in chapter 3 is the article *Security of quantum key distribution using weak coherent states with nonrandom phases* by Lo and Preskill [22]. The article provides a proof for coherent sources sending signals of non-random phase, with the BB84 protocol. Following this article, we choose X basis and Y basis, and use this as labels instead of 0 and 1. The eigenvectors of their operators (equation (2.17)) can be expressed in a common Z basis

$$|0_X\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle + |1_Z\rangle) \qquad |1_X\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle - |1_Z\rangle) \tag{2.16a}$$

$$|0_Y\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle - i\,|1_Z\rangle) \qquad |1_Y\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle + i\,|1_Z\rangle) \tag{2.16b}$$

The X, Y and Z vectors are eigenvectors with eigenvalues $\pm 1$ of the Pauli matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ Y = \begin{pmatrix} 0 & \text{-i} \\ \text{i} & 0 \end{pmatrix},\ Z = \begin{pmatrix} 1 & 0 \\ 0 & \text{-1} \end{pmatrix} \tag{2.17}$$

The state Alice creates is expressed as an entangled state. If we had a true single photon source we would have the Bell pair

$$|\psi_X\rangle = \frac{|0_{X,A}0_{X,B}\rangle + |1_{X,A}1_{X,B}\rangle}{\sqrt{2}} = \frac{|0_{Y,A}0_{Y,B}\rangle + |1_{Y,A}1_{Y,B}\rangle}{\sqrt{2}} = |\psi_Y\rangle \tag{2.18}$$

in other words, identical states. The first half of the pair (labeled $A$) is kept at Alice, the second half (labeled $B$) is sent to Bob. After this state is received by Bob, they measure their respective states in randomly selected bases and compare their results. Since Eve only is able to intercept Bob's qubit, she has no way of knowing whether Alice has measured her qubit or not. Let us assume that Alice measures her qubit before sending Bob's qubit, destroying the entanglement. Then Bob's qubit is determined. This is equivalent to Alice just sending the qubit to Bob without creating a qubit for herself. Hence, we do not actually have to create entangled states. However, for security proofs, calculations with Bell pairs are more convenient.

We now turn to the case of a coherent source. It is modeled as an entangled state consisting of a true single photon state which Alice keeps and measures, and a photon number state which is sent to Bob [22, eq. (16) & (17)]

$$|\Psi_X\rangle = \frac{1}{\sqrt{2}}|0_X\rangle|\alpha\rangle + |1_X\rangle|-\alpha\rangle \tag{2.19a}$$

$$|\Psi_Y\rangle = \frac{1}{\sqrt{2}}|0_Y\rangle|-i\alpha\rangle + |1_Y\rangle|i\alpha\rangle \tag{2.19b}$$

As we see, the basis choices and bit values are encoded as phase of values $\pm 1, \pm i$. Since these are pure states, the fidelity is calculated by their inner product. To do this, we express equations (2.19) in Z-basis (equations (2.16)). Using the relations in appendix B.1, we get

$$\begin{aligned}\langle\Psi_Y|\Psi_X\rangle &= \frac{1}{2}\Big((1+i)e^{-|\alpha|^2}e^{i|\alpha|^2} + (1-i)e^{-|\alpha|^2}e^{-i|\alpha|^2}\Big) \\ &= \frac{1}{2}e^{-|\alpha|^2}\Big(e^{i|\alpha|^2} + e^{-i|\alpha|^2} + ie^{i|\alpha|^2} - ie^{-i|\alpha|^2}\Big) \\ &= e^{-|\alpha|^2}(\cos|\alpha|^2 + \sin|\alpha|^2)\end{aligned} \tag{2.20}$$

which is less than 1 for $|\alpha| > 0$. Hence, these are states not identical. Of course, for $\alpha = 0$ they are identical; they are both vacuum states. This gives us the basis choice leakage as it is related to the fidelity, which we will need for the key generation rate in section 2.5.1. In fact, since these are pure states, the fidelity is the same as the inner product squared.

## 2.5 Key generation rate

The purpose of calculating the distinguishability of the states are to find the *secure key generation rate*. We want as strong pulses as possible to overcome line loss and detector inefficiency. Pulling in the other direction is the information leaked to Eve by strong pulses.

The normalized key generation rate is defined as the number of bits in the final key divided by the number of bits Bob receive, thus it is independent on pulse repetition frequency. We also have the empirical detection rate which is the number of bits Bob receive divided by the number of pulses Alice sends. So, when looking at overall key generation in terms of key bits per pulse, we multiply these two to get the transmission key generation rate.

### 2.5.1 Normalized key generation rate

First we look at the normalized key generation rate, which is what is provided in security proofs. It is defined as the fraction of secure key bits Bob can extract for the bits he receives. We label Alice's basis choice as $a$ and Bob's as $b$, where $a, b \in \{0, 1\}$. We emphasis that 0 and 1 are only labels for orthogonal bases, and may be any such bases. Furthermore, we label the event $a = b = 0$ as 0, $a = b = 1$ as 1 and $a = 1, b = 0$ as $ph$. $\delta_{event}$ is the QBER in the case of the labeled event. Koashi's article provides an equation to calculate the secure key generation rate [16].[15]

$$R_0 \geq 1 - h(\delta_0) - h(\delta_{ph}) \tag{2.21}$$

where $h$ is the binary entropy

$$h(\delta) = -\delta \log_2(\delta) - (1 - \delta) \log_2(1 - \delta) \tag{2.22}$$

$R_0$ is the key generation rate for the bits measured in 0-basis. Correspondingly, $R_1$ is the key generation rate for the bits measured in 1-basis. Secure communication is possible for $R > 0$. Setting $\delta_0 = \delta_{ph}$ and solving for $R = 0$ we get a maximum allowed QBER of 11% in the channel between Alice and Bob.

In the calculations done in this thesis, it is not needed to go through the parameter $\Delta$ from equation (2.14) to calculate the key generation rate, as fidelity is both in the equation below, and is what is to be calculated in the next chapter. $\delta_{ph}$ is given implicit (from [16, eq. (3) & (9)]) as

$$\sqrt{F} = \sqrt{(1 - \delta_1)(1 - \delta_{ph})} + \sqrt{\delta_1 \delta_{ph}} \tag{2.23}$$

which is valid if Eve only emit single photons. However, by using what is called a squash operator, the proof still applies if the detectors are perfect [23, 24]. We see that for $F = 1$ for $\delta_1 = \delta_{ph}$. For $\delta_1 > 0$, there are two value of $\delta_{ph}$ which give the same $F < 1$ (see figure 2.4). While being pessimistic, we of course select the largest $\delta_{ph}$. The equation (2.23) is solved numerically, handling the problem of two solutions by requiring that $\delta_{ph} \geq \delta_1$; the larger solution.

Marøy et al. [25] generalized Koashi's estimate of $\delta_{ph}$ to include arbitrary individual imperfections simultaneously in the source and detectors. Equation (2.23) is expanded to (from [25, eq. (11)])

$$\sqrt{F} = \sqrt{q_1(1 - \delta_1)q_{ph}(1 - \delta_{ph})} + \sqrt{q_1 \delta_1 q_{ph} \delta_{ph}} + \sqrt{(1 - q_1)(1 - q_{ph})} \tag{2.24}$$

This equation has also two solutions, for which we must select the larger (see figure 2.4). From [25, eq. (13)] we have an expression for the key generation rate[16]

$$R_0 \geq \eta_0 q_{ph}/q_0[1 - h(\tilde{\delta}_{ph}))] - h(\delta_0) \tag{2.25}$$

where [25, eq. (12)]

$$\tilde{\delta}_{ph} = \delta_{ph} + \frac{q_0 \epsilon_0}{q_{ph} \eta_0} \tag{2.26}$$

Here $q_0$, $q_1$ and $q_{ph}$ are the probabilities of non-vacuum events. $\delta_0$ and $\delta_1$ are QBER in each basis, $\eta_0$ is the detector blinding parameter.[17] $\epsilon_0$ is a measure of quantum leakage

[15] The labels *bit* and *phase* in the article is replaced with *0* and *ph*, respectively.

[16] [25] uses $X$ and $Z$ for labeling. To avoid confusion, it is relabeled 1 and 0, respectively.

[17] *Detector blinding* is a non-linear property of single photon detectors. Shining a bright light on the detectors cause them loose single photon detection ability [26].

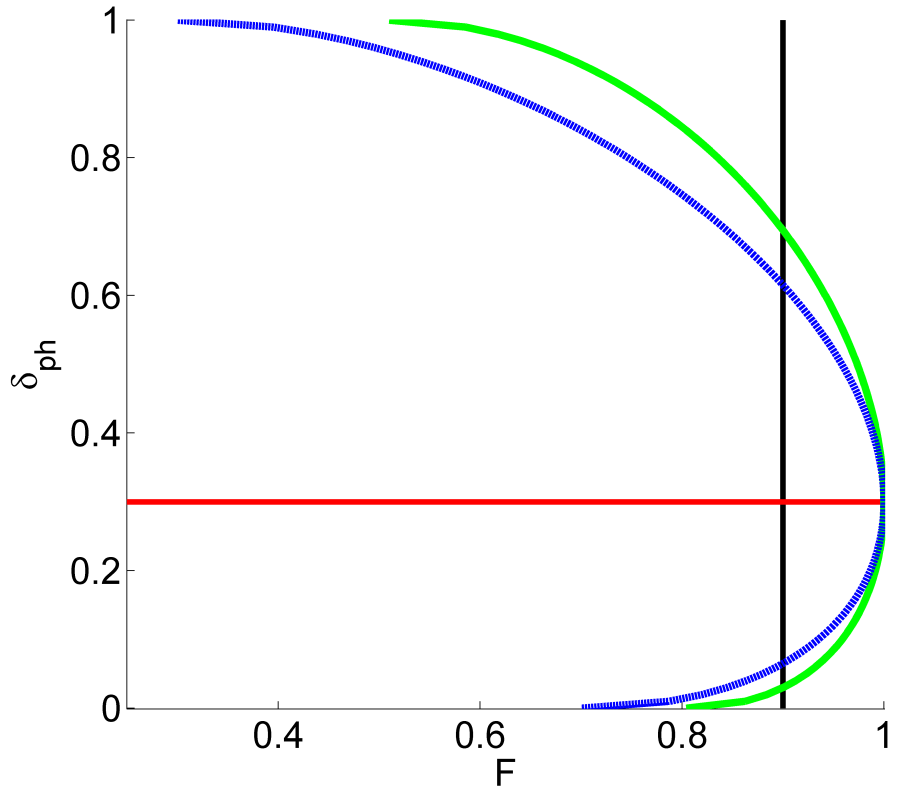



Figure 2.4: $\delta_{ph}$ (curved) for equation (2.23) (blue dashed) and equation (2.24) (green solid) as a function of fidelity with $\delta_1 = 0.3$ (red vertical). Two solutions of $\delta_{ph}$ (black vertical) are possible.

from the detectors. Assuming no line loss and flawless detectors ($\eta_0 = 1$ and $\epsilon_0 = 0$), the probability of a non-vacuum event is the same as the probability of non-vacuum emission, which follows the Poisson distribution. Using equation (2.4) we have that the probabilities of non-vacuum events are

$$q_0 = q_1 = q_{ph} = p(n > 0) = 1 - p(0) = 1 - e^{-|\alpha|^2} \tag{2.27}$$

Thus we reduce equation (2.25) for key generation rate to

$$R_0 \geq 1 - h(\delta_{ph}) - h(\delta_0) \tag{2.28}$$

and the equation (2.24) for finding $\delta_{ph}$ to

$$\sqrt{F} = q_{ph}\sqrt{(1-\delta_1)(1-\delta_{ph})} + q_{ph}\sqrt{\delta_1\delta_{ph}} + (1 - q_{ph}) \tag{2.29}$$

We assume flawless detectors, since we will treat only the source.

### 2.5.2 Transmission distance

The normalized key generation rate gives us the fraction of the signals Bob detects which contributes to the key. However, we want to find the overall key generation rate as a

function of distance. In other words, the fraction of pulses which during transmission, contribute to the key. With a line loss of $\xi$, still assuming flawless detectors, we have the probability of a non-vacuum event to be

$$q_0 = q_1 = q_{ph} = \eta_{Bob}(1 - e^{-|\alpha|^2 10^{-\xi L}}) = \eta_{Bob} q_L \tag{2.30}$$

where $\eta_{Bob}$ is the detector efficiency and L is the transmission distance. This is also the fraction of pulses which reach Bob, thus *transmission* key generation rate is[18]

$$TR_0 = \eta_{Bob} q_L R_0 \tag{2.31}$$

The fidelity is still calculated for the value of $\alpha$ before entering the line. We must assume that Eve has full access to the entire line. Another way of seeing this is that Eve is the line. She receives a high intensity input with high basis choice leakage, and sends a low intensity output with low detection rate. Both gives Eve advantages for gaining key information. Alice and Bob must be able to send qubits though Eve, which she can treat in any way she like, and still extract a secure key of which Eve has no knowledge of.

[18] $TR_0$ is the label, and not the product between $T$ and $R_0$, although in most cases, this would also work.

# 3 Modeling the source: Derivations and calculations

In this section, calculations for the distinguishability between state of different bases will be done. First we will treat the case of random reference phase, then we will combine this with the case where the source has amplitude fluctuations.

## 3.1 Random phase

In an attempt to increase the secure key generation rate, the laser is phase-randomized. Lo and Preskill carried out analytical calculations for non-random phase [22]. Here this basic framework will be expanded to random phase.

### 3.1.1 Analytical derivation

Keeping to the notation of Lo and Preskill, we expand (2.19) to include a reference state $|\beta\rangle$.

$$|\Psi_X\rangle = \frac{1}{\sqrt{2}}\Big( |0_X\rangle\,|\alpha\rangle + |1_X\rangle\,|-\alpha\rangle \Big)\,|\beta\rangle \tag{3.1a}$$

$$|\Psi_Y\rangle = \frac{1}{\sqrt{2}}\Big( |0_Y\rangle\,|-i\alpha\rangle + |1_Y\rangle\,|i\alpha\rangle \Big)\,|\beta\rangle \tag{3.1b}$$

here both $|c\alpha\rangle$ ($c \in \{\pm 1, \pm i\}$) and $|\beta\rangle$ are coherent states. The information is coded as the relative phase $c$ between these two states. The first part ($|b_a\rangle$, $b$ is the bit value 0 or 1, $a$ is the basis X or Y) is the state which Alice keeps. For a source with non-random phase, these state are pure. Since $\langle\beta|\beta\rangle = 1$, this part disappears when taking the inner product, it gives the same result as [22].

$$\langle\Psi_Y|\Psi_X\rangle = e^{-|\alpha|^2}(\cos|\alpha|^2 + \sin|\alpha|^2) \tag{3.2}$$

From this we see that in this case, the strength of the reference pulse does not matter; its phase is predetermined and thereby also known to Eve. Hence, it carries no additional information.

We turn to the case where the source emits states of random phase. Now we cannot see these states as pure states, but rather a mixed state of all the possible phases. First we

define the density matrices for the pure state of one phase.

$$|\Psi_X\rangle\langle\Psi_X| = \rho'_{X00} + \rho'_{X01} + \rho'_{X10} + \rho'_{X11} \tag{3.3a}$$
$$|\Psi_Y\rangle\langle\Psi_Y| = \rho'_{Y00} + \rho'_{Y01} + \rho'_{Y10} + \rho'_{Y11} \tag{3.3b}$$

where $\rho'_{ab_1b_2} = \frac{1}{2}|b_{1,a}\rangle\langle b_{2,a}| \otimes |c_1\alpha\rangle\langle c_2\alpha| \otimes |\beta\rangle\langle\beta|$. $b_i$ refers to the bit value 0 or 1, while $a$ refers to the basis $X$ or $Y$. $c_i$ refers to the modulation phase correlated with $b_{i,a}$. Furthermore we need to write coherent states in terms of amplitude and phase.

$$|c\alpha\rangle = \left|c|\alpha|e^{i\phi}\right\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{c^n|\alpha|^n}{\sqrt{n!}} e^{i\varphi n}|n\rangle \tag{3.4}$$

This gives

$$|c_1\alpha\rangle\langle c_2\alpha| = e^{-|\alpha|^2} \sum_{m,n=0}^{\infty} \frac{c_1^m c_2^{*n}|\alpha|^{m+n}}{\sqrt{m!n!}} e^{i\varphi(m-n)}|m\rangle\langle n| \tag{3.5}$$

This is also done for $|\beta\rangle$, exchanging $\alpha$ with $\beta$ and setting $c_1 = c_2 = 1$. For the general case we assume that the phase varies over $[0, 2\pi]$ with a probability distribution $p(\varphi)$ fulfilling

$$\int_0^{2\pi} p(\varphi)d\varphi = 1 \tag{3.6}$$

with Fourier coefficients

$$P(n) = \int_0^{2\pi} p(\varphi)e^{i\varphi n}d\varphi \tag{3.7}$$

Then we calculate each mixed state components of the total state

$$\begin{aligned}
\rho_{ab_1b_2} &= \int_0^{2\pi} \rho'_{ab_1b_2}p(\varphi)d\varphi = \int_0^{2\pi} \frac{1}{2}|b_{1,a}\rangle\langle b_{2,a}| \otimes |c_1\alpha\rangle\langle c_2\alpha| \otimes |\beta\rangle\langle\beta|\, p(\varphi)d\varphi \\
&= e^{-|\alpha|^2-|\beta|^2} \sum_{klmn} \frac{c_1^k c_2^{*l}|\alpha|^{k+l}|\beta|^{m+n}}{2\sqrt{k!l!m!n!}} \int_0^{2\pi} p(\varphi)e^{i\varphi(k-l+m-n)}d\varphi \\
&\quad |b_{1,a}\rangle\langle b_{2,a}| \otimes |k\rangle\langle l| \otimes |m\rangle\langle n| \\
&= e^{-|\alpha|^2-|\beta|^2} \sum_{klmn} \frac{c_1^k c_2^{*l}|\alpha|^{k+l}|\beta|^{m+n}}{2\sqrt{k!l!m!n!}} P(k-l+m-n) \\
&\quad |b_{1,a}\rangle\langle b_{2,a}| \otimes |k\rangle\langle l| \otimes |m\rangle\langle n|
\end{aligned} \tag{3.8}$$

to arrive at the mixed states for X basis and Y basis

$$\rho_X = \rho_{X00} + \rho_{X01} + \rho_{X10} + \rho_{X11} \tag{3.9a}$$
$$\rho_Y = \rho_{Y00} + \rho_{Y01} + \rho_{Y10} + \rho_{Y11} \tag{3.9b}$$

Since the important parameters for further calculations are $b_i$, $a$ and $c_i$, it is convenient to put the rest behind a single symbol

$$\rho_{kl} = \frac{1}{2}e^{-|\alpha|^2-|\beta|^2} \sum_{mn} \frac{|\alpha|^{k+l}|\beta|^{m+n}}{2\sqrt{k!l!m!n!}} P(k-l+m-n)\,|k\rangle\langle l| \otimes |m\rangle\langle n| \tag{3.10}$$

which gives

$$\rho_{ab_1b_2} = \sum_{kl} c_1^k c_2^{*l}\,|b_{1,a}\rangle\langle b_{2,a}| \otimes 2\rho_{kl} \tag{3.11}$$

Through some tedious calculations in appendix B.2, we can write the density states to

$$\rho_X = \sum_{kl} \{(I+X) + (Z-iY)(\text{-}1)^l + (Z+iY)(\text{-}1)^k + (I-X)(\text{-}1)^{k+l}\} \otimes \rho_{kl} \tag{3.12a}$$

$$\rho_Y = \sum_{kl} i^{k+l}\{(I+Y)(\text{-}1)^k + (Z+iX)(\text{-}1)^{k+l} + (Z-iX) + (I-Y)(\text{-}1)^l\} \otimes \rho_{kl} \tag{3.12b}$$

where I, X, Y and Z are the identity matrix and the Pauli matrices expressed in the Z basis (see B.2). Once $\rho_X$ and $\rho_Y$ have been obtained, we can calculate the fidelity by equation (2.9).

To model the phase variation of the source it is interesting to look a the two extreme special cases. The first is when the phase is completely determined or non-random. The second is when the phase is completely random, having a uniform distribution. In addition it is interesting to look at an in-between case where the probability distribution has the two extremes as special cases. These cases have the probability functions

$$p_{det}(\varphi) = \delta(\varphi) \tag{3.13a}$$

$$p_{unif}(\varphi) = \frac{1}{2\pi} \tag{3.13b}$$

$$p_{cos}(\varphi) = \frac{q}{2\pi(q-qd+d)} \begin{cases} 1 - d\cos q\varphi & ,\varphi \in [0, \frac{2\pi}{q}] \\ 1-d & ,\varphi \in (\frac{2\pi}{q}, 2\pi] \end{cases} \tag{3.13c}$$

were $d \in [0,1]$ and $q \in [1,\infty)$.[1] For $p_{cos}$ we can see that $p_{unif}$ and $p_{det}$ are limits when $(d=0)$ and $(d=1, q=\infty)$, respectively. These distributions gives the Fourier coefficients

$$P_{det}(n) = 1 \tag{3.14a}$$

$$P_{unif}(n) = \begin{cases} 1 & ,n=0 \\ 0 & ,n \neq 0 \end{cases} \tag{3.14b}$$

$$P_{cos}(n) = \begin{cases} 1 & ,n=0 \\ -\frac{d}{2(q-qd+d)} & ,n=\pm q \\ i\frac{qd}{2\pi(q-qd+d)}\left(1-e^{i2\pi n/q}\right)\left(\frac{1}{n} - \frac{1}{2(n+q)} - \frac{1}{2(n-q)}\right) & ,\text{otherwise} \end{cases} \tag{3.14c}$$

This is as far as the analytical calculations go. The fidelity is calculated numerically using Matlab in next section.

### 3.1.2 Numerical calculations

To calculate the fidelity numerically we have to limit the size of our density matrices.

$$\sum_{k,l,m,n=0}^{\infty} \rightarrow \sum_{k,l,m,n=0}^{N-1} \tag{3.15}$$

This give matrices of size $2 \times N^4$. Fortunately the expected photon numbers for the states we are considering are small, so high photon numbers are improbable. Hence, leaving these out should not cause a security issue, as long as their probabilities are small enough. We see that for small $\alpha$ it is sufficient to calculate with small $N$. But when we increase $\alpha$, we must also increase $N$.

[1] In general, there should be a phase constant $\varphi_0$ (exchanging $\varphi$ with $\varphi - \varphi_0$) in the expressions. But, since this is just an arbitrary phase constant, it may as well be zero, simplifying calculations.

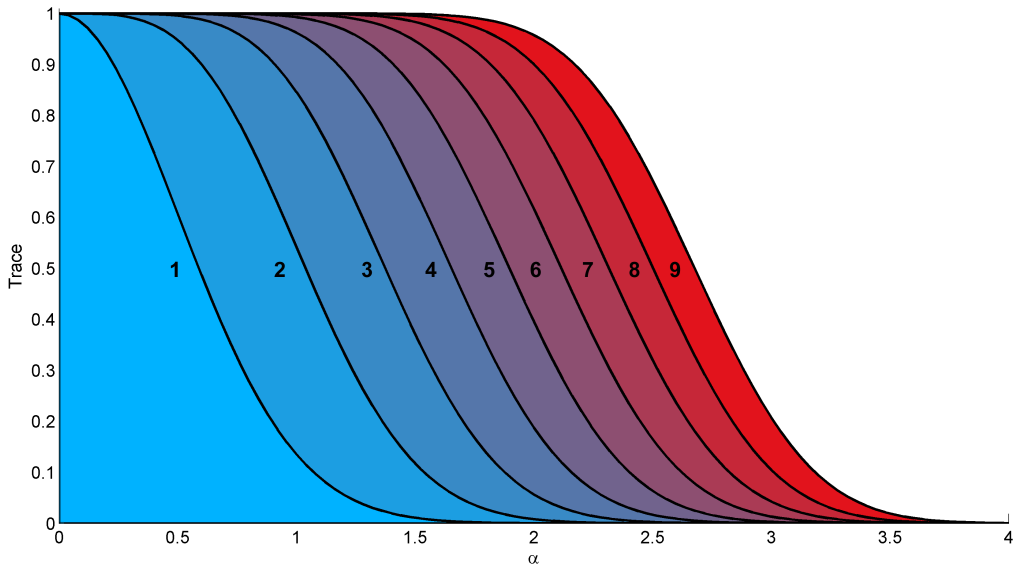



Figure 3.1: Trace dependence of $N$ form 1 to 9.

Realizing this, we can speed up calculations for small $\alpha$ by using small $N$ and increase $N$ as required for large $N$. When do we need an increased $N$? A property of a valid density matrix is that its trace is equal to one (shown in [11, p. 101]). The trace is the sum of the diagonal elements. As explained above, we have to cut the high photon number elements, thus making the trace smaller than one. Hence, the trace is dependent on the size parameter $N$ as seen in figure 3.1. We can exploit this to determine $N$ by saying that for a given $\alpha$ (and $\beta$), if the trace is below a certain threshold, we have to increase $N$. This is also done in figures 4.1 and 4.2 where the fidelity is plotted, which the the other figures in chapter 4 is based on. Here the threshold trace value is set to 0.999999, and $N$ is increased by 2 for the next $\alpha$ in the iteration when the trace has reached it (see code in C.2.1).

## 3.2 Fluctuating intensity

The laser may also be unstable in terms of pulse intensity. This was the case for the laser in QKD system being buit at NTNU [6]. This should, of course, also be accounted for when analyzing the security.

### 3.2.1 Analytical derivation

Since both signal and reference pulse originates for the same laser they will be proportional. By putting $\beta = B\alpha$ we can rewrite eq. (3.10) as

$$\rho_{kl} = e^{-(1+B^2)|\alpha|^2} \sum_{mn} \frac{|\alpha|^{k+l+m+n} B^{m+n}}{2\sqrt{k!l!m!n!}} P(k-l+m-n) \left|k\right\rangle \left\langle l\right| \otimes \left|m\right\rangle \left\langle n\right| \tag{3.16}$$

Now, we turn to the case the photon number varies; $|\alpha|$ varies with distribution $r(|\alpha|)$. Assuming independence of phase and no correlation between pulses, this gives the integral

(extracting the $\alpha$ dependent factors)

$$\int_0^\infty e^{-(1+B^2)|\alpha|^2}|\alpha|^{k+l+m+n}r(|\alpha|)d|\alpha| \tag{3.17}$$

This integral is hard to solve. We may approximate this by dividing $|\alpha|$ into a discrete set set of possible values; $|\alpha| = \{|\alpha|_j\}$. Since strong pulses leaks more information than weak pulses, we can round any $|\alpha|$ in the interval $(|\alpha|_{j-1}, |\alpha|_j]$ up to $|\alpha|_j$. With $r(|\alpha|_j) = r_j$ we can exchange the integral for a sum.

$$\sum_j e^{-(1+B^2)|\alpha_j|^2}|\alpha_j|^{k+l+m+n}r_j \tag{3.18}$$

To find $r$ we have to measure the statistics of the actual system.

This is the best case scenario. However, the intensity of each pulse may be correlated so that Eve can know in advance the intensity of the pulses. In the worst case scenario, she knows the expected photon number of all pulses. This will be the same as Alice announcing the expected photon number she uses. Then we must treat each case separately, calculating the secure key generation rate for each $|\alpha|_j$, and then take the probability weighted average.

### 3.2.2 Numerical calculations

When comparing the fluctuating intensity case with the stable case we do this with the same average intensity. This is the same as taking the probability weighed RMS[2] over amplitudes. Having a set $\{|\alpha|_j\}$ $(j = [0, ..., J])$ of amplitudes for the instable source, this gives

$$|\alpha|_{wrms} = \left(\sum_{j=0}^{J}|\alpha|_j^2 r_j\right)^{\frac{1}{2}} \tag{3.19}$$

Instead of having a several values of $\alpha$, for calculations it is convenient to have a scaling factor and a single $\alpha$, writing $\alpha_j = K_j\alpha_S$. We can then write the corresponding sum

$$1 = \frac{1}{K_{wrms}}\left(\sum_{j=0}^{J}K_j^2 r_j\right)^{\frac{1}{2}} \tag{3.20}$$

Using equation (3.20), we can easily compare fidelity for fluctuating and stable $\alpha$ for the same average mean photon number $\mu$.

There are two extreme cases. The best case scenario is when the fluctuations are truly random. We then create states with equation (3.16) and (3.18), calculate the fidelity and compare it with the fidelity of states with $\alpha_{wrms}$. Using these two fidelities we can compare the key generation rates.

The worst case scenario is when the pulses are not random at all. This would be the same as Alice announcing to Eve which amplitudes she uses. The key generation rate would then be the weighted average over the rates for each amplitude.

[2]RMS - Root Mean Square

## 3.3 Key generation rate

For all cases, the main result is the key generation rate. It is calculated using equation (2.28) where $\delta_{ph}$ is found by the use of Newton's method on equation (2.23) (Koashi) or (2.29) (Marøy). Since there are two solutions to this equation (as seen in figure 2.4) a method for selecting the higher solution was implemented. The Matlab code is found in appendix C.3.3.

To calculate the normalized key generation rate for the non-random fluctuating amplitude case, we have to go through the transmission key generation rate.

$$TR_0 = \sum_j r_j q_{L,j} R_{0,j} \tag{3.21}$$

We then divide by the fraction of pulses which reach Bob

$$R_0 = \frac{TR_0}{\sum_j r_j q_{L,j}} \tag{3.22}$$

### 3.3.1 Finding $\delta_{ph}$

Newton's method may cause a problem if it does not converge sufficiently fast, i.e. the required accuracy is not reach within a reasonable number of iterations. However, we can find conditions where we do not have any solutions, or any usable solutions. We can check these conditions to skip calculations where no useful output will be produced. This will not only speed up calculations, but also guaranties that for useful values of $\delta_{ph}$, the calculations are stopped only when the required accuracy is reached.

One condition for positive key generation rate is that QBER $< 11\%$. We have that $\delta_{ph} \geq \delta_0$. Still assuming $\delta_0 = \delta_1$, we see that if $\delta_1 > 0.1101$ we will not get positive rate.[3] Hence, as long as we know that value $\delta_{ph}$ will cause zero rate, it does not matter what it is, so we can skip the calculations for finding $\delta_{ph}$ and set $\delta_{ph}$ to any value above 0.1101, e.g. 0.5.

Assuming optimum values for all parameters except for the fidelity, we can find the absolute minimum fidelity which allow positive key generation rate. Optimum values are zero QBER ($\delta_0 = \delta_1 = 0$), and a probability of non-vacuum event of 1. From equation (2.21) we see that the maximum $\delta_{ph} = 0.5$. In both equation (2.23) and (2.24) the minimum usable fidelity is

$$F_{min} = 1 - \delta_{ph} = 0.5 \tag{3.23}$$

Hence, if the fidelity is too low, positive key generation rate is impossible. When calculating $\delta_{ph}$ we can use this knowledge to simply skip the calculation in these cases, and set $\delta_{ph} = 0.5$.

Another limit we can extract is dependent on the probability of a non-vacuum event in equation (2.29). Still setting $\delta_1 = 0$ and assuming $q_1 = q_{ph}$, we see from the requirement $\delta_{ph} < 0.5$ that

$$\sqrt{F} = q_{ph}\sqrt{1 - \delta_{ph}} + 1 - q_{ph} > 1 + q_{ph}(\sqrt{0.5} - 1) \tag{3.24}$$

for positive key generation rate. Hence, if the opposite is the case, we can skip calculation and set $\delta_{ph} = 0.5$.

[3] The exact value of the QBER limit is just above 11%, hence 0.1101 since $h(0.1101) = 0.5002 > 0.5$.

Furthermore, as we can see in figure 2.4, equation (2.29) reaches its maximum when $\delta_{ph} = \delta_1$, and reaches its minimum at $\delta_{ph} = 0 \wedge \delta_{ph} = 1$. Putting these two values into the equation we get

$$\sqrt{F} = q_{ph}\sqrt{1-\delta_1} + 1 - q_{ph} \tag{3.25a}$$

$$\sqrt{F} = q_{ph}\sqrt{\delta_1} + 1 - q_{ph} \tag{3.25b}$$

respectively. In the function for finding $\delta_{ph}$ in appendix C.3.3 we have $F$ as an input parameter. We can use (3.25) to say that if it is larger than the input F, no solution for $\delta_{ph}$ will be found, and abort calculation, returning $\delta_{ph} = 0.5$.

### 3.3.2 Transmission distance

To give a realistic plot, experimental data is fetched from [27]. Here we have a function describing the QBER as a function of the detectors probability $P_e$ of dark count[4], and detector efficiency $\eta_{Bob}$, in addition to the line loss $\xi$. [27, eq. (2)]

$$\delta_0 = \delta_1 = \frac{0.5P_e}{0.5\mu 10^{-\xi L/10}\eta_{Bob} + P_e} \tag{3.26}$$

where $P_e = 8.5 \cdot 10^{-7}$, $\eta_{Bob} = 0.045$ and $\xi = 0.2$ dB/km. $L$ is the transmission distance.

## 3.4 Problems and sources of error

When moving from analytical to numerical calculations, accuracy is lost. In this case, where we have coherent states, we move from matrices of infinite size to finite size. The most obvious effect of this is that contributions of photon number states above a certain value are left out. Fortunately, since we are dealing with number states of low average photon number, high number states have low probability. Hence, we can leave the highest number states out. However, the density matrices has many non-diagonal elements which may be important during calculations.

### 3.4.1 Not a number

During calculations a few problems occurred. The most profound was that for a some values of input $A$, $B$ and $N$ in the function `rhoxyU` in C.1.1, the `sqrtm` in line 5 in the `fidelity`-function (C.2.3) gave an output where all elements were NaN[5]. This caused an error on line 7 because the subroutine `schur` of `sqrtm` cannot take NaN as input. An example of values for which this occurred is $A = B = 0.005$ and $N = 8$. The error did not occur when $B$ was change to 0.006 or $N$ to 10. It was tracked down to line 49 in `sqrtm` (Revision: 5.15.4.4). This line, `R(i,j)=(T(i,j)-s)/(R(i,i)+R(j,j));`, produces a 0/0-expression and causes a NaN. Of course, once a NaN is produced, whenever it is multiplied

[4] A *dark count* appears when a detector clicks without receiving a photon. Usually caused by thermal excitations.

[5] NaN - Not a Number

with anything it gives NaN. This causes the error to spread throughout the matrices, and in the end entire matrix in line 5 of `fidelity` consists of NaNs.

This problem disappeared when removing lines 3 and 4 (in C.2.3). These two lines are there to ensure the matrices are Hermitian.[6] Because of their finite size the matrices are not 100% valid. Hence, it is reasonable to assume that they may become less valid for every calculation done. This could have lead to the major error of NaN. Since there is a finite precision in numerics, the values may have become to small for floating-point numbers to handle, and are stored as zero.

### 3.4.2 Newton's method

To find $\delta_{ph}$ Newton's method was used (code in appendix C.3.3). This caused a problem when limiting the number of iterations allowed. Early testing indicated that few iterations was required even for high accuracy. This however was not the case for the non-random/announced fluctuating amplitude. Here, at least 2000 iterations were required to get decent results. When the number of iterations was less, discontinuities appeared for low values of $\alpha$ (see figure 3.2).

Having an iteration maximum sufficiently large, and by using the optimalizations in section 3.3.1, errors where eliminated, guaranteeing the validity of $\delta_{ph}$ within the required accuracy.

Newton's method includes using the derivative of function. For $\delta_{ph} \approx \delta_1$, the derivatives with respect to $\delta_{ph}$ of equations (2.23) and (2.24) are close to zero. Since Newton's method uses one divided by the derivative, if this is too close to zero for floating point numbers to be accurate, it may cause the method to never reach the required accuracy. This was solved by saying that if $F$ was sufficiently close to 1, then $\delta_{ph} = \delta_1$.

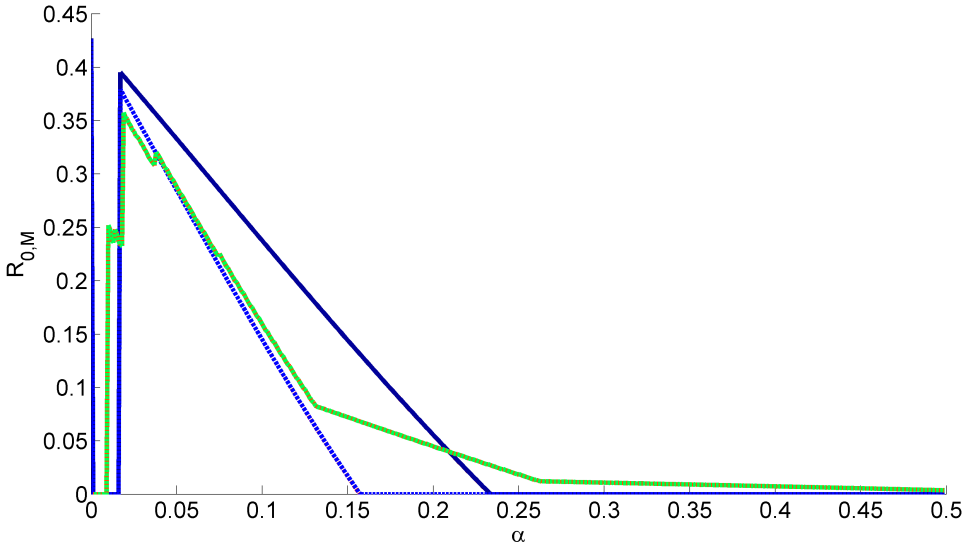



Figure 3.2: Key generation rate plot with erroneous estimate of $\delta_{ph}$. Maximum allowed iteration is 100. For plot guide see caption of figure 4.6.

[6] A matrix $A$ with the property $A^\dagger = A$ is said to be Hermitian [11, p. 70]. Having a matrix $B$ which is not Hermitian then $\sqrt{BB^\dagger}$ is Hermitian since $(BB^\dagger)^\dagger = BB^\dagger$.

# 4 Results and discussion

This chapter is organized so that we see both plot of the results and discussion on the same double page. We will look at the results step by step, starting with the fidelity, continuing with key generation rate, and finally key transmission key generation rate as a function of distance. The optimum value of $\mu$ as function of distance is also plotted. In the end, a discussion of how the results affect a practical QKD system.

Although Koashi's proof has limitations when it comes to the line loss and detectors it will be considered as we are only looking at the source. Also this is more established, as the Marøy et al. article [25] has only recently been published.

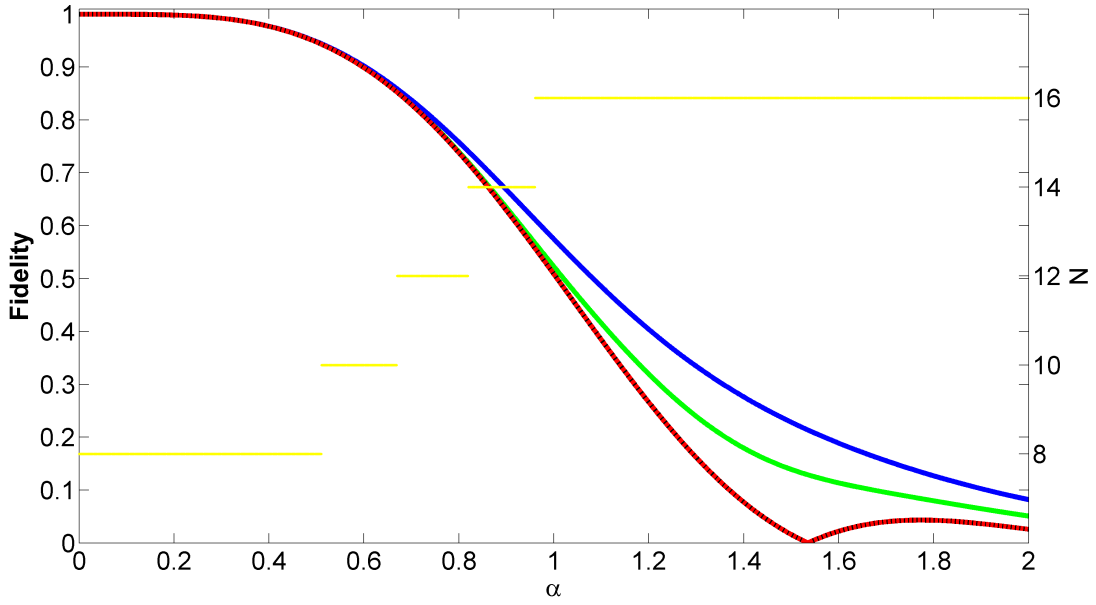



Figure 4.1: Square root fidelity of non-random (analytical (black solid) and numerical (red dashed)), cosine (green solid) and uniform (blue solid) distributed phase. The yellow dotted line is the matrix size parameter N used to calculate fidelities for the different $\alpha$.

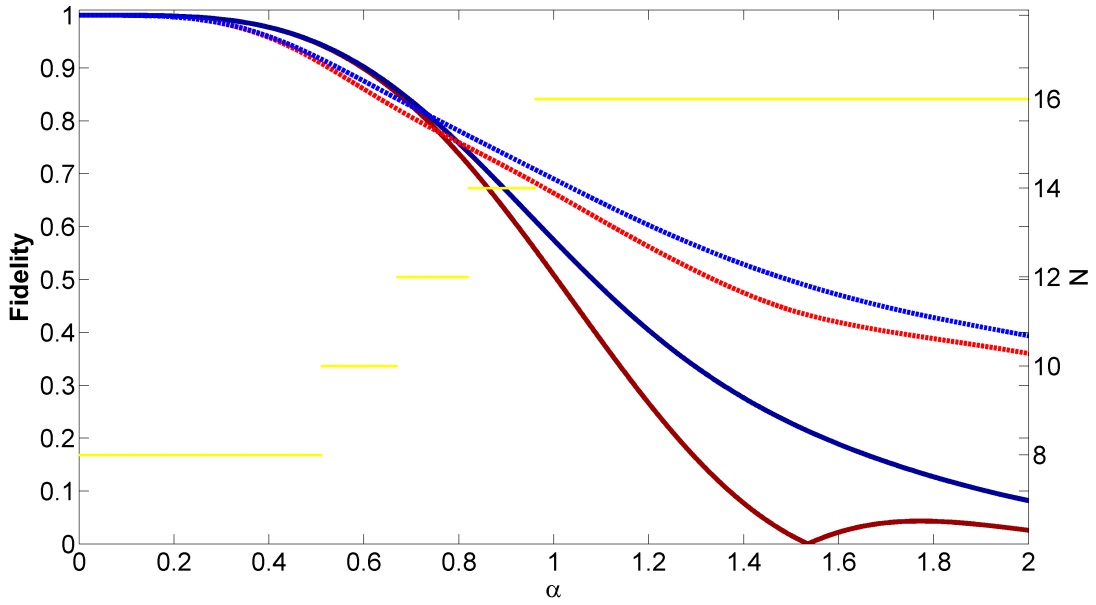



Figure 4.2: Numerical square root fidelity of fluctuating $\alpha$ (light colored dashed) vs. stable $\alpha_{vrms}$ (dark solid). For both cases, uniform random phase (blue) and non-random phase (red) are plotted. $K = \{0.25, 0.5, 1, 2\}$ with probabilities $r = \{0.2, 0.2, 0.4, 0.2\}$. The yellow dotted line is the matrix size parameter N used to calculate fidelities for the different $\alpha$.

## 4.1 Fidelity

In figure 4.1 the numeric solution (red dashed) is plotted with the analytical (black solid) solution of the fidelity. These two overlap; numerical calculations are very accurate. For cosine distributed phase, with $d = 5$ and $q = 1$ in equation (3.14c), and for uniform random phase (blue dashed line), we see an improvement in the fidelity over the non random case. However, this improvement does not start to show until $\alpha \simeq 0.6$ which a high value in QKD systems.

In figure 4.2 we see the fidelity of the fluctuating vs. stable $\alpha$ case. Both uniform random and non-random cases are plotted. For $\alpha$ larger than $\sim$0.75 we see that we have an improvement in fidelity. However, for smaller $\alpha$, we have a deterioration. Since these are the values relevant for key generation rate, fluctuating $\alpha$ should give a lower rate.

To give a measure for the accuracy the difference between numerical and analytical fidelity for the non-random case is plotted in figure 4.3. We see that for $\alpha < 1.8$ the difference between the is maximum $10^{-6}$, which is the same as the maximum allowed fall in trace value for the density matrices. When we move closer to $\alpha = 2$, the difference increases above this value, as the maximum allowed $N$ is reached.

Valid fidelity is real. However, the fidelities in figure 4.2 are complex, with the absolute real value plotted.[1] In figure 4.4, their absolute imaginary parts are plotted, showing their maximums for each value of $\alpha$. We see that the values are below $10^{-8}$, thus it is not significant. Also, the values seems to be fairly random, suggesting they are artifacts caused by the numerical approximation, and that in the analytical case, they would be zero. Thus the matrices are approximately valid.

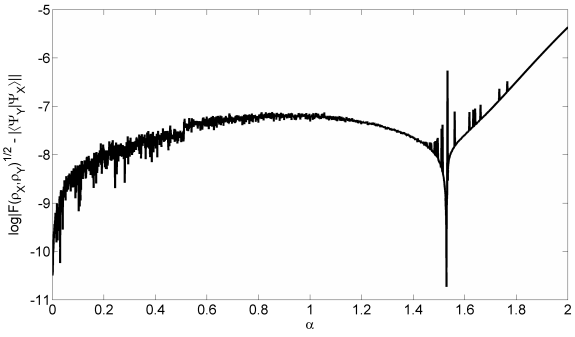



Figure 4.3: Difference between non-random numerical and analytical fidelity. The y-axis is base 10 logarithmic.

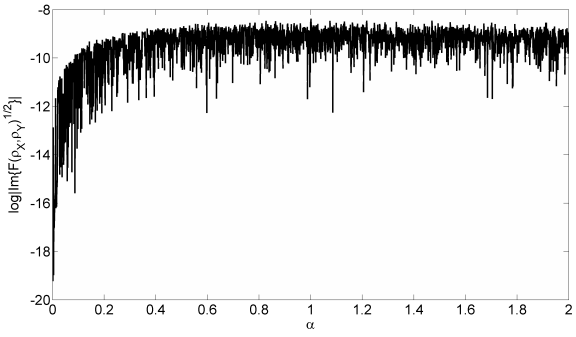



Figure 4.4: Imaginary part of numerical fidelity for all cases. The y-axis is base 10 logarithmic.

[1] Absolute real values were chosen instead of only absolute values, as this is more pessimistic.

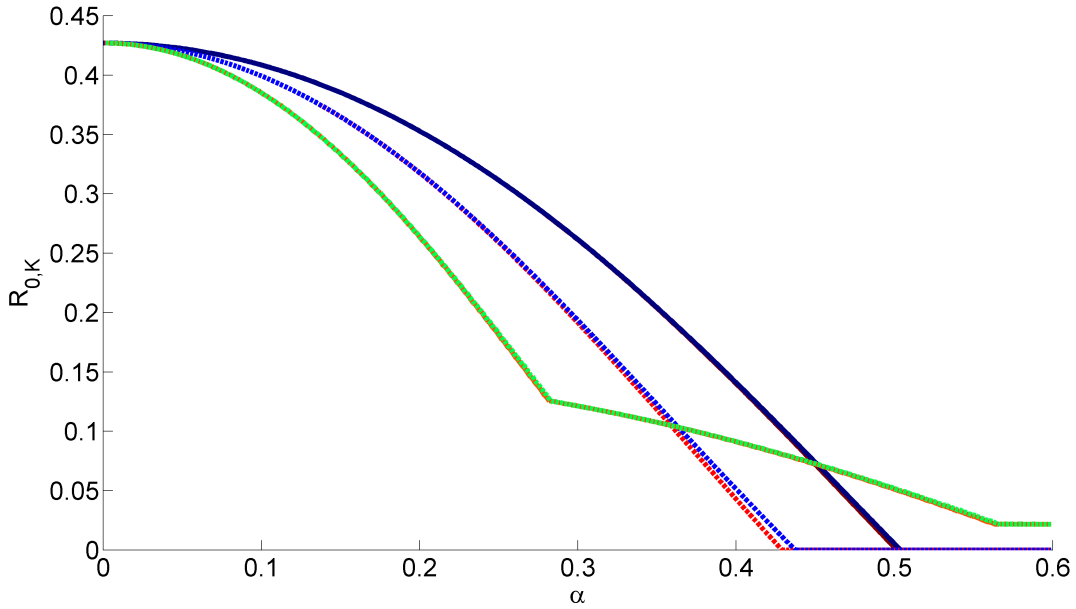



Figure 4.5: Key generation rate based on the Koashi [16] estimate of $\delta_{ph}$ with 5% QBER. The plot shows every combination of non-random (red) and uniform (blue) phase, and random fluctuating (light dashed) and stable (dark solid) amplitudes. In addition, non-random fluctuating amplitudes for non-random (orange solid) and uniform (green dashed) phase. $K = \{0.25, 0.5, 1, 2\}$ with probabilities $r = \{0.2, 0.2, 0.4, 0.2\}$. The non-random plots are overlapped by the uniform random plots.

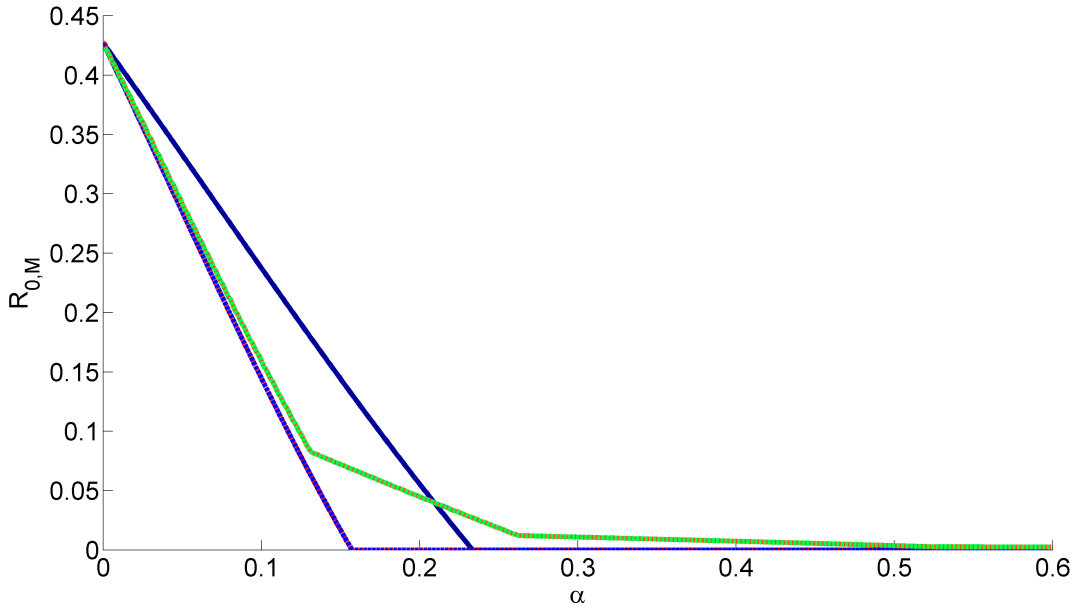



Figure 4.6: Key generation rate based on the Marøy et al. [25] estimate of $\delta_{ph}$ with 5% QBER. See figure 4.5 for plot description.

## 4.2 Key generation rate

In figures 4.5 and 4.6 we see the key generation rate for lossless line and perfect detection with a QBER of 5%, plotted against $\alpha$, with Koashi and Marøy et al.'s $\delta_{ph}$ estimate from equations (2.23) and (2.24), respectively. The non-random case plots are overlapped by the uniform random case plots. This shows that there is almost no difference between when uniform and non-random phase. The place where the difference is most visible is in figure 4.5 where the lines for random fluctuating $\alpha$ seperates just before reaching $R_0 = 0$. The difference appeared to be dependent on the QBER. Low QBER led to a larger difference between the cases uniform and non-random phase, while high QBER led to a small difference. This can be seen when comparing figures 4.7 and 4.8, with 4.5 and 4.6, respectivly. The cosine distributed phase is left out, as this would not be visible between its two extremes.

An interesting feature in the non-random/announced fluctuation case are the bends. These appear because the total key generation rate is calculated by the probability weighted average of key generation rate of each of the possible values of $\alpha$. The bends corresponds to the places where one curve for a large $\alpha$ stops contributing to key generation rate, but a lower $\alpha$ still does.

We see in both figures that random fluctuating amplitudes causes a lower key generation rate. Hence, this should also give a lower transmission rate. However, for non-random fluctuating amplitudes we see that for high intensities (high $\alpha_{wrms}$), there is a positive key generation rate while the other cases are not. This suggest that non-random fluctuating amplitudes could have a better transmission rate. For Marøy's estimate, this is the case for non-random vs. random fluctuating amplitudes, as we see in figure 4.6.

Comparing the two figures, we see how much we loose when we take into account line loss and detector imperfections. Perfect detectors and no line loss is assumed for both plots, which required for Koashi's proof to be valid. However, the Marøy plot takes into account the effect the probability of non-vacuum ($q_{\{0,1,ph\}}$) events have on $\delta_{ph}$. If these are set to one the plots will be identical, as is also apparent from equation (2.24). Matlab functions for these plots is found in appendix C.3.1.

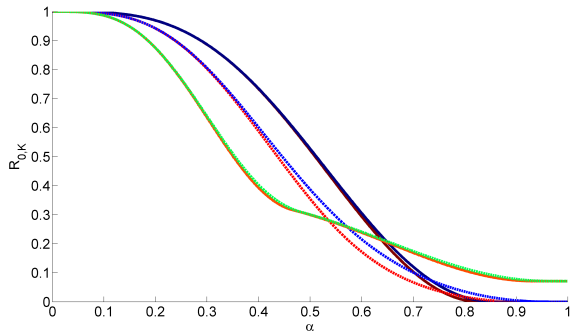



Figure 4.7: Key generation rate based on the Koashi [16] estimate of $\delta_{ph}$ with 0% QBER. See figure 4.5 for plot description.

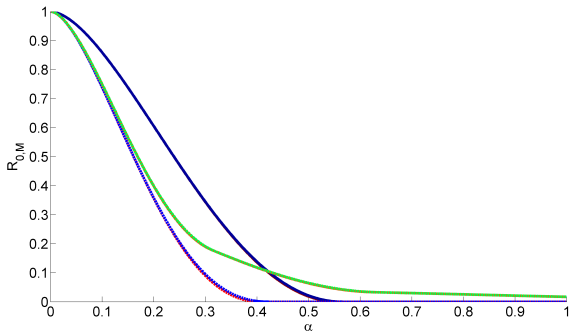



Figure 4.8: Key generation rate based on the Marøy et al. [25] estimate of $\delta_{ph}$ with 0% QBER. See figure 4.5 for plot description.

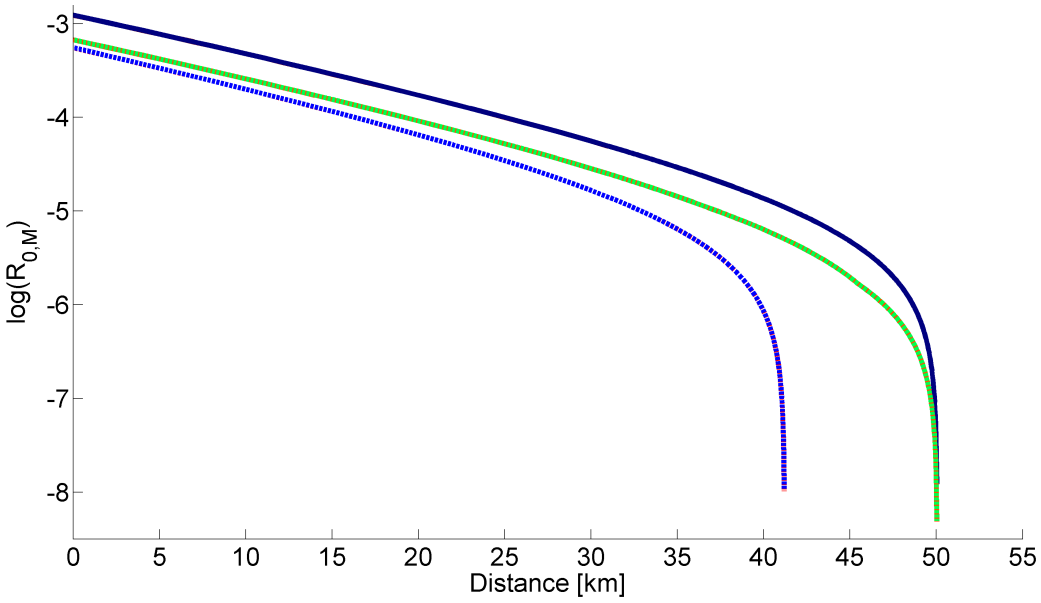



Figure 4.9: Transmission rate vs. distance: Marøy estimate of $\delta_{ph}$ with experimental data. The plots are for stable $|\alpha|$ (upper dark sold blue), random fluctuating $|\alpha|$ (middle dashed blue) and non-random fluctuating $|\alpha|$ (lower dashed green). Both uniform random and non-random phase are plotted (reddish); the latter is overlapped by the first. The y-axis is base 10 logarithmic.

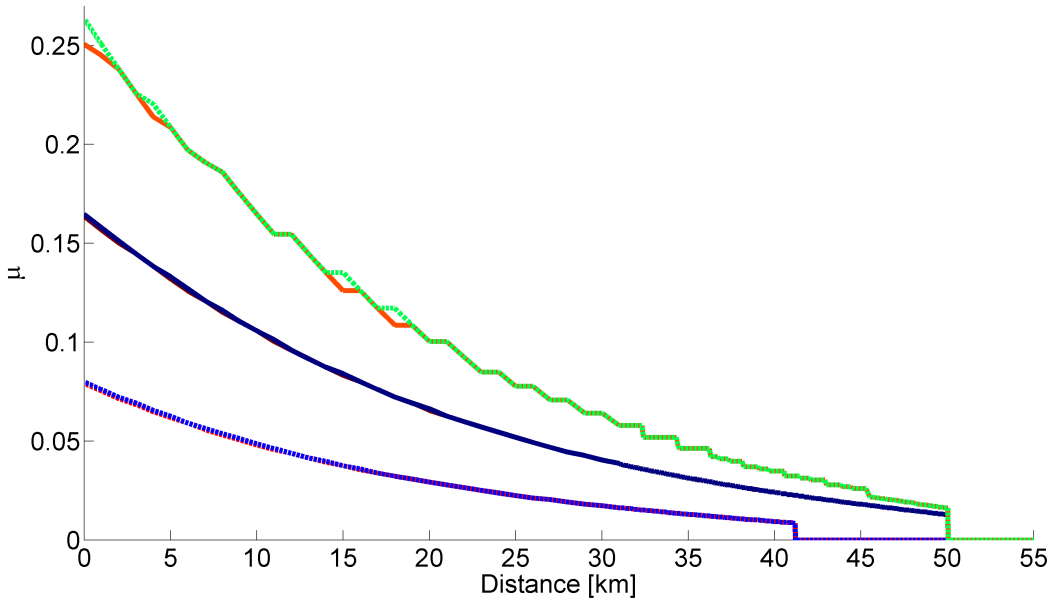



Figure 4.10: Optimum mean photon number with Marøy estimate. See figure 4.9 for plot guide.

## 4.3 Transmission distance

In figure 4.9 we see the plot of key generation rate as a function of distance, with the Marøy estimate of $\delta_{ph}$. Experimental data is fetched from [27]. Maximum transmission rate is obtained for stable amplitude, while minimum is obtained for non-random fluctuating phase. The difference between non-random and uniform random phase is negligible, hence although both are plotted, only uniform random phase is visible. It seems that the maximum transmission distance is reached at a rate around $10^{-7}$.

To find the maximum transmission key generation rate, we need to find the optimum mean photon number $\mu = 2|\alpha|^2$. In figure 4.9, for each distance the rate was calculated for all values of $\alpha$, and the the maximum found. The optimum values of $\mu$ we can see in figure 4.10. Matlab functions for these plots are found in appendix C.3.4.

We see that stable amplitude gives the best key generation rate. For varying amplitude, non-random fluctuations appear to be best. It actually gives about the same maximum transmission distance, only with a lower rate. The reason for this may be that at most one of the values of $\alpha$ (or $\mu$) is the optimal value. Hence, many pulses will be of non-optimal amplitudes, which have lower rate.

The random fluctuation gives a lower rate for all distances, and a shorter maximum distance. When having random fluctuations, Eve has no prior knowledge of the amplitude. Thus, having announced fluctuations giving Eve this prior knowledge should give Eve an advantage, and lower the key generation rate. However, we must remember that for these two situations, Alice and Bob shares the same knowledge about the amplitude as Eve does. Hence, we can interpret from this plot that it is better that all of them know the amplitude than none.

## 4.4 Optimum mean photon number

In figure 4.10 we see the optimum values of $\mu$ as a function of transmission distance, based on the Marøy estimate of $\delta_{ph}$. The optimum $\mu$ is decreasing as a function of transmission distance. At maximum transmission distance, the optimum value is as low as $\mu = 0.0085$. At maximum transmission distance we see that $\mu$ goes to zero; when secure key generation rate can no longer be guaranteed, transmission is aborted.

In the plot for non-random fluctuating amplitude, we see that it is not as smooth as the others. This may occur because this is the average of multiple key generation rates. It could be that the relative amplitude contributing the most to the key generation rate is changing between the possible values, and thus creates the steps we see. Also there is a larger rounding error as the values of $\alpha$ was picked from the set with $10^{-3}$ step size. Thus the relative step between the four values $\alpha$ could vary between was not constant, but was rounded to the closest $10^{-3}$ step.

We see that for non-random fluctuations $\mu$ is larger. In general, $\mu$ is small, so for non-random fluctuations it could be that the highest values of $\mu$ causes to much QBER, and simply does not contribute to key generation rate, leaving only the lower values of $\mu$ contributing. This is consistent with this case having a lower transmission rate, but the same maximum transmission distance as for the stable amplitude.

## 4.5 Impact on a practical system

The first calculations were done in order to treat random phase vs. non-random phase for a laser source. As it turned out, random phase had minimal impact on this system, using the proofs of Koashi and Marøy. Hence, for the QKD system being built, whether the phase is random or not, has minimal effect on system performance.

A positive consequence of this is that a strong reference pulse will have negligible impact on system performance. This is because a strong reference pulse will only make the the fidelity go closer to the non-random case. On the other hand, if we flip the argument, a weaker reference pulse could give better system performance, since the fidelity becomes better. However, for detection, the pulses need to be of equal strength to interfere. This means that the stronger pulse must be attenuated and thus decrease detection rate. In a practical setup, as we will see in the next chapter (figure 5.1), we have a phase modulator in one arm which introduces loss. Hence, the pulses must be of different strength through the transmission channel. When calculating the performance of a practical system, these considerations must be included. There is nothing speaking against letting Bob modulate the reference pulse in stead of the signal pulse. Thus it is possible to select which configuration of strong/weak reference pulse that gives the best performance.

The second calculations treated fluctuating laser intensity. These plots gave a notable difference from the stable amplitude case. However, the plot were done for extreme cases of fluctuation. Although extreme, the system performance was still acceptable. As sources can be made very stable, this should not cause a security issue. We can measure the statistics of the system, and calculate the parameters required for secure communication. If the fluctuations are rare, and we measure pulse intensity continuously, we can simplify by just skipping abnormal pulses.

At last we have the optimum value of $\mu$ as a function of distance. This is a very applicable result as this gives the value for the intensity Alice must output for best performance. Of course, for a specific system, the experimental data from [27] must be replaced with corresponding data for that system. All parameters in equations (2.24) to (2.26) should be found for the specific system, to guarantee secure key generation.

# 5 Experimental work

Building the QKD system was started in [6] with the assembly of Alice's rack case with electronics and the decoy state generator. For this thesis, the building process was continued by setting up the interferometer. As this required more fine tuning, it was set up on an optical table for adjustments. When everything works on the optical table, it will be put inside the rack cases of Alice and Bob.

## 5.1 System overview

The system setup (Figure 5.1) was designed by *The Quantum Hacking group*, and is based on previous systems and advances in theory. This system is an updated version of that which Vadim Makarov used in his PhD thesis [28]. The goal is to build a working system which is unhackable by all current methods.

### 5.1.1 Tour of the system from photon's point of view

We begin at the upper right corner of figure 5.1. A short laser pulse is created by the 1.55 $\mu$m[1] laser, and is polarized by a linear polarizer. Its intensity is adjusted by a Mach-Zehnder intensity modulator. The pulse then goes through the interferometer, starting with a 50/50 beam splitter. Half the pulse is sent through the left arm where it is modulated by the phase modulator. This modulator decides the basis and bit value of the output photon. (A variable time delay ensures that the two pulses reach the last beam splitter down at Bob at the same time, interfering fully when Alice and Bob select matching bases.) The other half of the pulse goes through the right arm. (It is attenuated to match losses in the other arm.) Before leaving Alice, they are attenuated to sub single photon level.

If a photon survives transmission, Bob now receives it. It goes through a polarization controller which counteracts the polarization change by the line. Bob has an interferometer, equal to Alice's, which chooses a basis to measure in. At the end two single photon detectors (SPDs), corresponding to values '0' and '1', do the final measurement.

[1] 1.55 $\mu$m is chosen as it has the lowest fiber loss [12, p. 350], making it the best choice for long distance transmission.

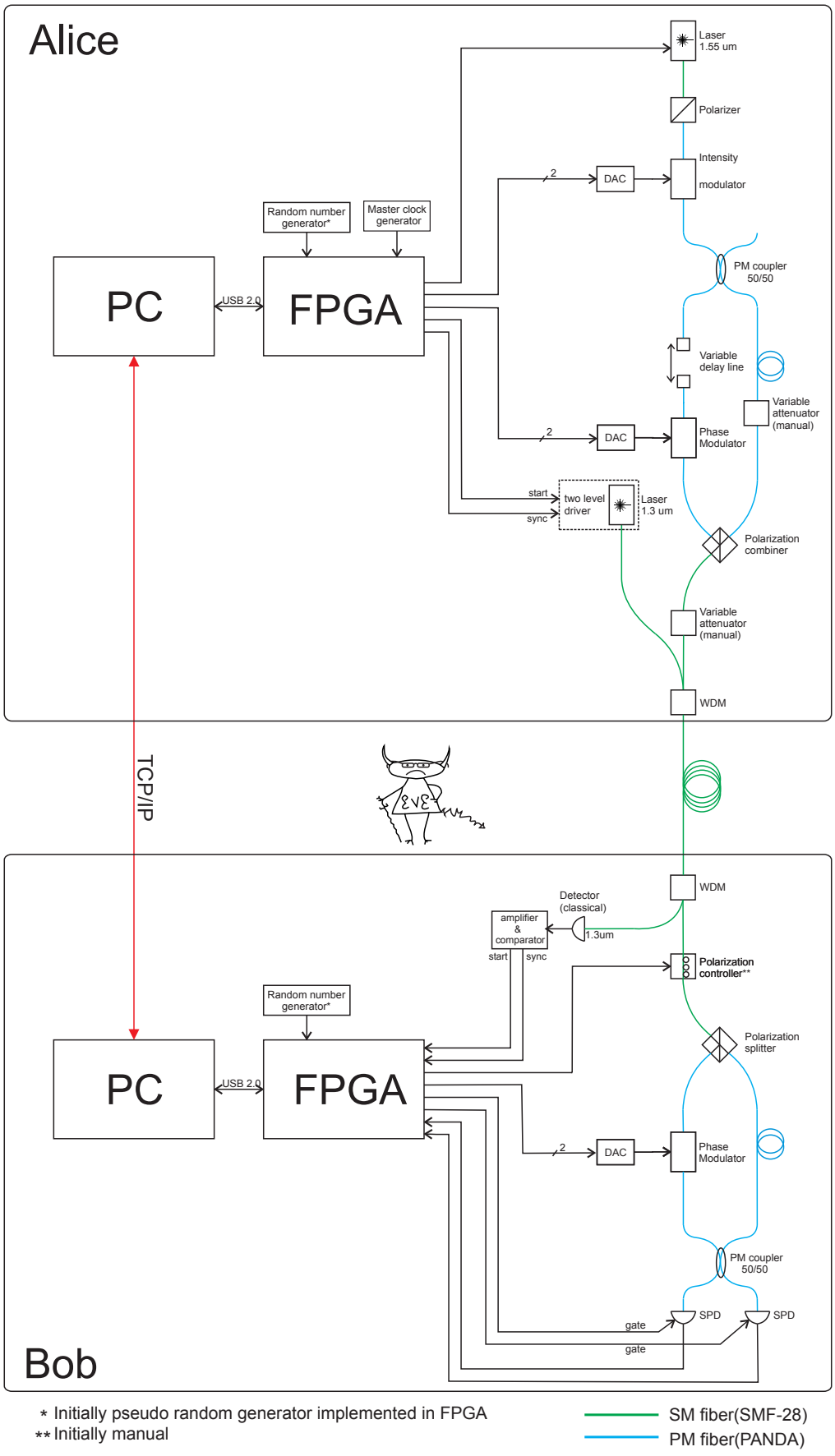



Figure 5.1: Planned structure of the QKD system. This is an updated version of the one drawn by [29].

The 1.3 $\mu$m laser is used to send a clock signal from Alice to Bob for them to be in sync. It is multiplexed into the same fiber as the signal by the WDM.[2] This is mainly for long distance QKD, as the clock can be sent directly if Alice and Bob are in the same room during initial experiments. The FPGAs[3] control the hardware while the PCs do all public communication needed to settle on a key, encrypt, send and decrypt messages.

### 5.1.2 Unbalanced Mach-Zehnder interferometer

The most important parts of a QKD system are its encoding and decoding units. In this system this is realized by an *unbalanced Mach-Zehnder interferometer* [30]. In figure 5.2 we see a scheme of this part of the system, which was mounted on an optical table. Half the interferometer, where the beam is split in two, is placed in Alice. The other half, where the interference happens, is placed in Bob. That it is *unbalanced* means that the optical path lengths in Alice are different. For interference to occur in Bob, the pulses must arrive the coupler at the detectors at the same time. Thus, Bob's difference in optical paths must match Alice's. The different components also introduce unbalance in loss. The intensities of the two arms must also equal when reaching Bob's coupler. This is why an attenuator is placed in the non-modulated part of Alice's arm, which we will call the reference arm. Whereas the modulated arm will be called the signal arm or modulation arm.

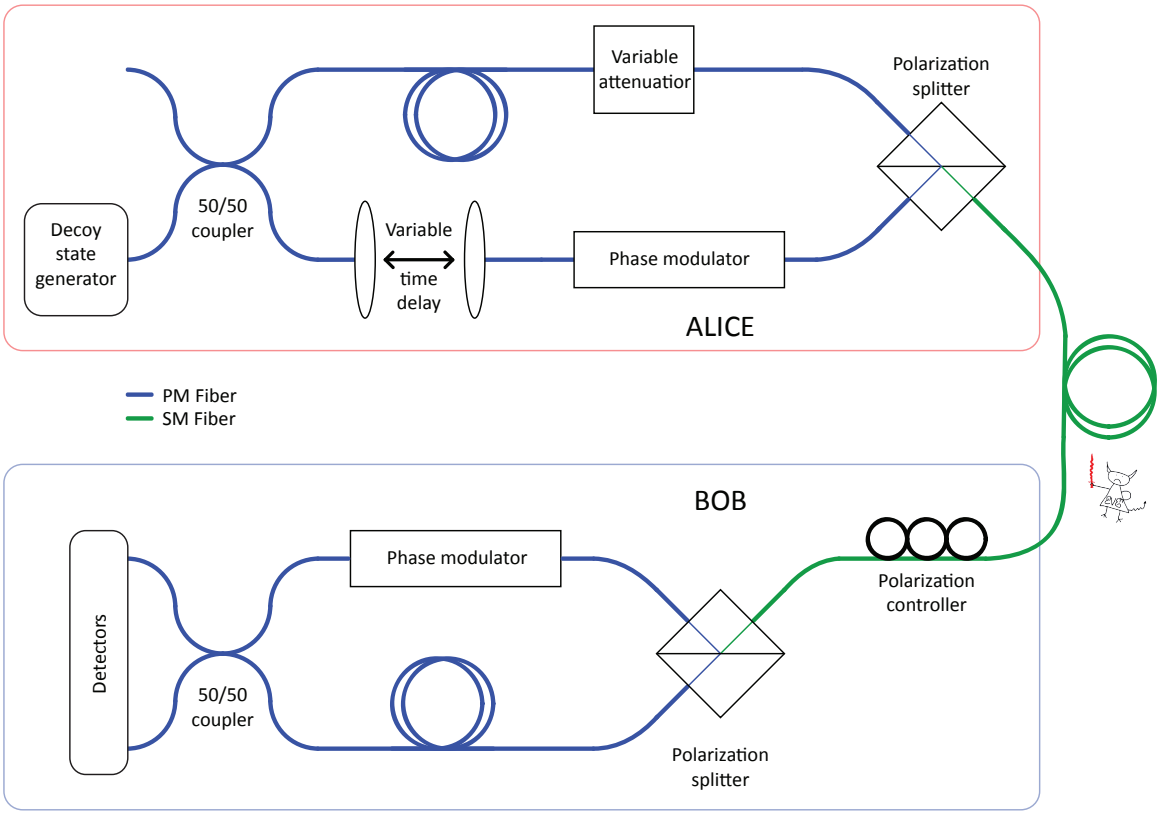



Figure 5.2: Unbalanced Mach-Zehnder interferometer

[2]WDM - Wavelength-Division Multiplexing.
[3]FPGA - Field Programmable Gate Array

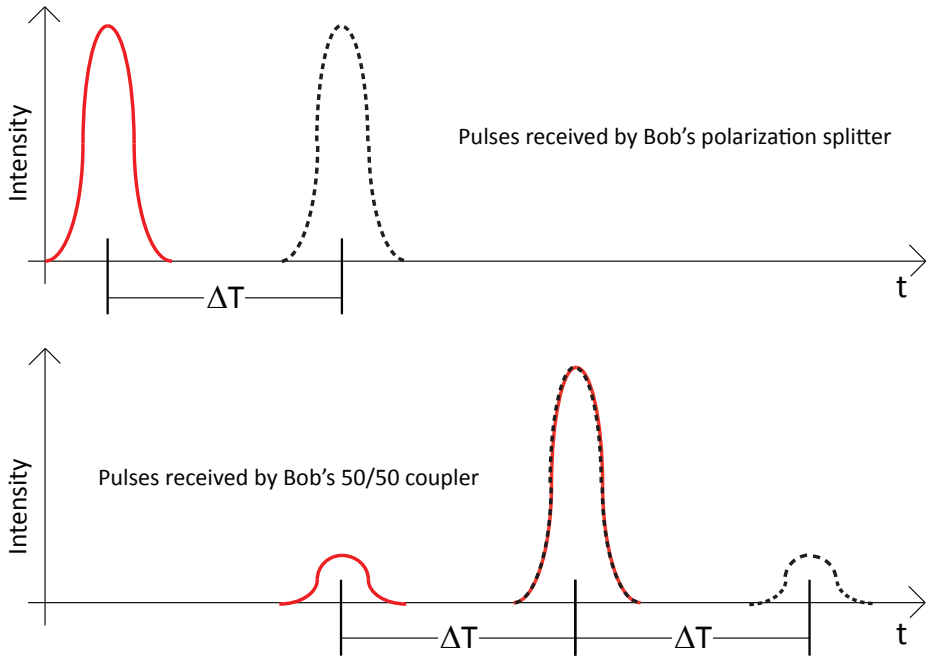



Figure 5.3: Two pulses leaving Alice at different times. When going through Bob's polarization combiner the cross-talk's smaller pulses arrives to his coupler at different times than the main pulse.

## 5.2 Timing of pulses

To maximize system performance, the pulsed should be timed properly. The polarization combiner combines the two pulses of orthogonal polarization in Alice so the splitter in Bob can direct them to the correct arm. However, the combiner and splitter can only differ the polarizations by a finite value, introducing cross-talk. This means that a small part of pulse addressed to Bob's left arm is leaked to his right arm, and vice versa. In a balanced interferometer, this would affect interference, since then a small part would be modulated which should not have been, and vice versa.

In this setup where the interference is unbalanced, the difference in optical path lengths makes the pulses leave Alice and arrive to Bob with a time delay. This directs the cross-talk to arrive at different times in Bob's coupler, as seen in figure 5.3. Still, the cross-talk pulses, although weak, will create extra clicks[4] in the detectors. But these clicks will only give extra hits for which Alice has no counterpart. Thus, it should in principle not affect QKD. However, in practical devices, perfect time discrimination is not possible, as we will be explained in the next section.

In the end the two pulses must arrive at the same time in Bob's 50/50 coupler to interfere and output the bit value they carry.

### 5.2.1 Timing with gated detectors

To lower the dark count rate, the detectors will be gated. When no signal is expected, the detectors are off. When a signal is expected, they are turned on. So, if we control

[4]When a single photon detector receives a photon it *clicks*.

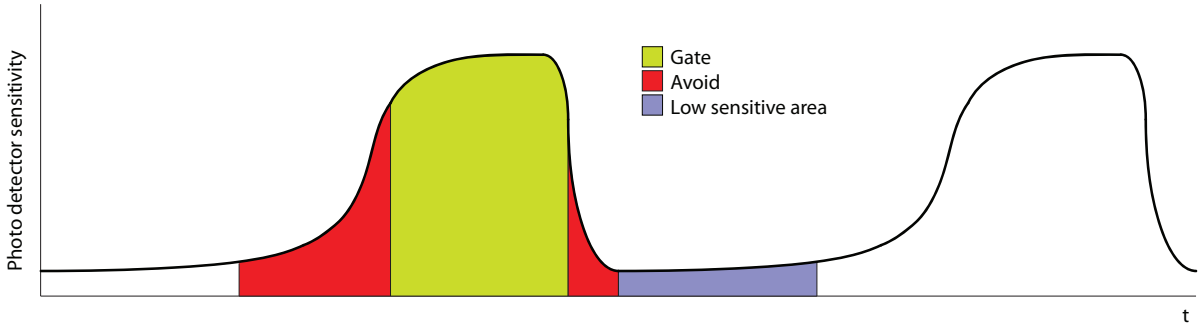



Figure 5.4: Gated detectors

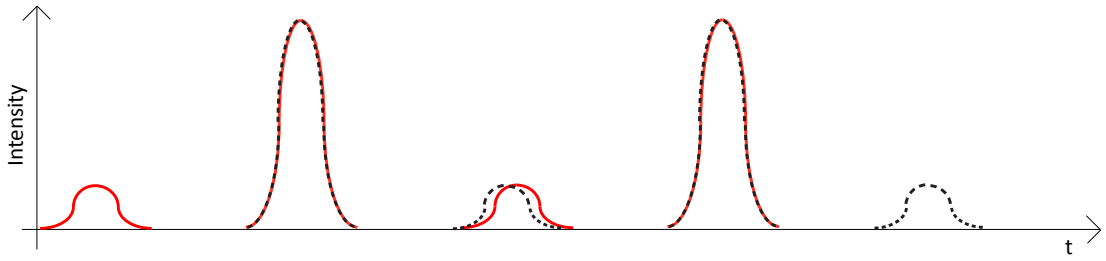



Figure 5.5: Subsequent pulses with proper time delay

the time delay between the pulses, we can send cross-talk to times outside the gate, when the detectors are off. This way we can avoid that a cross-talk click is misinterpreted as a signal, as the time resolution of the detectors may be limited. Unfortunately the gating is not ideal, but typically looks like figure 5.4 [31, 32, 33]. A photon arriving before the gate may still be registered as a click. This is because this photon may linger before causing a click inside the gate. The cross-talk should be timed to arrive at the least sensitive point in the gating cycle.

As we can see in figure 5.4, the lowest sensitivity is just after the gate. This would be the best point to send the cross-talk. However, in figure 5.3 we can see that the cross-talk appears with the same time distance before and after the pulse. Just before the gate is not a good place to send cross-talk. Hence, it is best to time the delay to about half the pulse repetition period as seen in figure 5.5.

### 5.2.2 Fiber lengths

To get the optimal time delay we need to calculate length difference needed in the arms. In optical fiber this corresponds a fiber length difference of

$$\Delta L = \Delta t \frac{c_0}{n_{fiber}} \tag{5.1}$$

where $\Delta t$ is the time delay, $c_0$ is the vacuum speed of light and $n_{fiber}$ is the effective refractive index of the fiber. The system is planned to be working at 200 MHz, which is a period of 5 ns. Hence, the pulse time delay should be $\Delta t = 2.5$ ns. In silica fiber $n_{fiber} \approx 1.5$. This gives a path difference of 50 cm.

The accuracy of the fiber length must be within the range of time delay, which is ±17 mm. This translates to a time range of ±85 ps; close to the operation pulse length of 100 ps.

### 5.2.3 Interference

QKD is dependent on good interference. The phase coding, having chosen the right basis, determine which detector the photon arrives at, and thus its bit value. Any inaccuracies contribute to QBER.

The laser is a coherent source, thus interference will appear as long as there is overlap between the pulses. A measure for the quality of the interference obtained is *visibility*. It is defined as [12, p. 73]

$$\mathcal{V} = \frac{I_{max} - I_{min}}{I_{max} + I_{min}} \tag{5.2}$$

where $I_{max}$ and $I_{min}$ is the intensities of maximum constructive and destructive interference. The operating pulse will be 100 ps long which corresponds to 2 cm of fiber, or 20k wavelengths. We should come as close to zero wavelengths difference as possible. This can be adjusted with a variable time delay. The pulses should also be of the same strength. The difference in line loss between the interferometer arms can be compensated using a variable attenuator. This will produce maximum visibility as wave fronts many wavelengths apart will have lower constructive interference then those close to each other. Also, if there is a large mismatch in optical path length, the first and the last part of the pulse will not interfere. If the photon sent does not interfere, it will be detected randomly, contributing to QBER. This is also the case for mismatch in attenuation, since the pulses will only partially interfere.

### 5.2.4 Obtaining zero path length difference

The lasers wavelength may also vary throughout the pulse. We can take advantage of this non-ideal effect to obtain zero path length difference.

In the interferometer the pulse is split in two, before they meet to interfere. We can model the two pulses as

$$A(t) = f_t e^{i\omega_t t} \tag{5.3a}$$

$$A_{\Delta t}(t) = f_{t-\Delta t} e^{i\omega_{t-\Delta t} t} \tag{5.3b}$$

where $f_t$ is the pulse shape and $\omega_t$ is the frequency, as a function of time. $\Delta t$ is the time delay. This gives the interference pattern

$$I(t) = |A(t) + A_{\Delta t}(t)|^2 \tag{5.4}$$

where $I$ is the intensity. If a laser pulse goes through the interferometer, but meets to interfere with a slight time delay, they have slightly different frequency, as seen in figure 5.6, and make the light beat [12, p. 70]. We see that the frequency difference varies as a function of time delay. This will cause fringes to appear as seen in figure 5.7, which is an example of how this may look.[5] This serves as a tool for adjusting the time delay to obtain zero path length difference. By minimizing $\Delta\omega$, we minimize $\Delta t$ and $\Delta L$.

[5]Figures 5.6 and 5.7 are not based on any experimental data, but are simply illustrations of the effect.

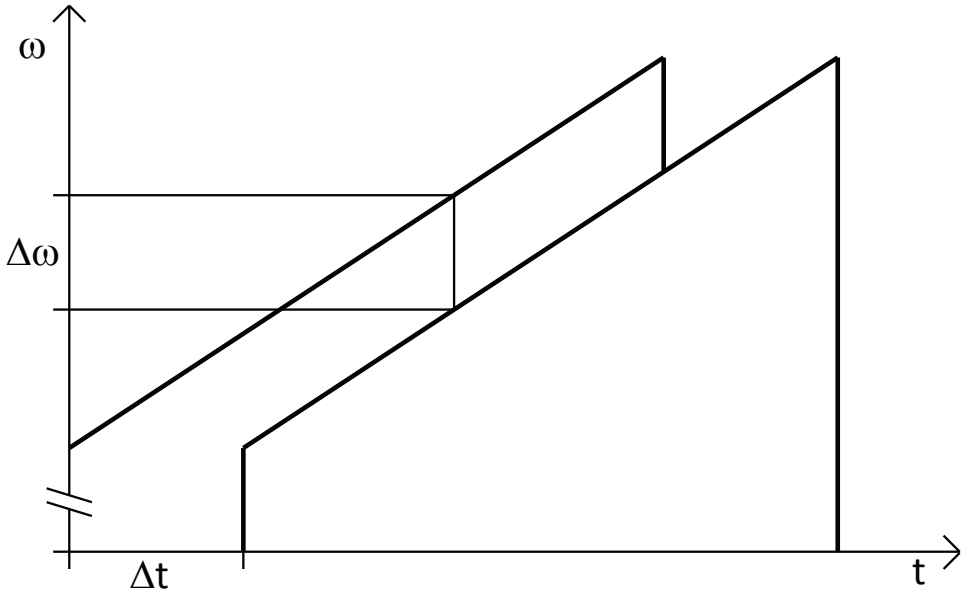



Figure 5.6: Pulses of varying wavelength with time delay.

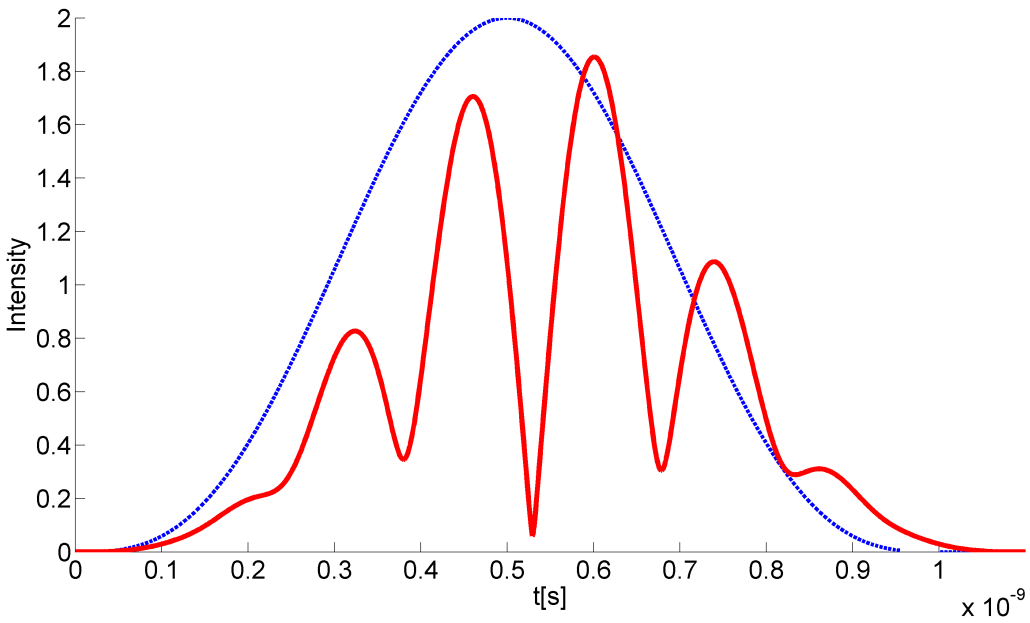



Figure 5.7: Fringes caused by time delay and varying wavelength. The frequency starts at 200 THz (1.5 $\mu$m) and increases as a function of time. The blue dashed curve corresponds to zero time delay. The red solid curve, where fringes appear, correspond to a 0.1 ns time delay. The fringes are 700 MHz, which is the same as the delay induced frequency difference.

### 5.2.5 Dependencies for laser wavelength

This section is a short overview over various effect which cause the laser wavelength to vary. When the laser's drive current is switched on, there is a delay before the laser start to lase. This is due the capacitive effect [34, p. 212] which causes the current to have a transient response. The delay appears because the laser needs a threshold current to lase [34, p. 425]. In addition, this change in carrier density gives a varying space charge, which in turn gives an electro-optic effect [12, p. 863-866]. This varying refractive index in the cavity makes the wavelength fluctuate. In addition, the energy band gap is dependent on temperature [35], which also has an effect on the wavelength. The laser heats and cools because of its internal resistance as the current is switched on and off. All these effect are especially apparent in a high power laser.

## 5.3 Assembly on the optical table

The interferometer (figure 5.2) was assembled on an optical table. This involved mounting components, splicing and connectorization of fibers.

### 5.3.1 Equipment

- Digital Oscilloscope (DO) - Tektronix TDS 7104 (SN: B020503)
- Communications Signal Analyzer (CSA) - Tektronix CSA 803A
- Digital Delay Generator (DDG) - Highland Technology Model P400
- Amplified Lightwave Converter (ALC) - Hewlett-Packard 1198A (SN: 5022A00113)

### 5.3.2 Orienting connectors

Some fibers had to be fitted with connectors manually. The interferometer relies on polarization maintaining (PM) fiber. In contrast to normal single mode (SM) fiber, the axial orientation of connecting fiber is essential. To allow the connectors to be aligned, the ferrule was left rotatable. If properly aligned, the intensity throughput should be at its maximum. However, small deviations of a high intensity are difficult to see. Hence, it is difficult to find the precise maximum. On the contrary, these deviations are relatively large at minimum intensity, which should ideally be zero. Thus to align the ferrule with the connector key, it is better use an orthogonal polarization. This was realize by using a polarization crossing fiber which rotates the polarization by 90°.

The setup used is shown in figure 5.8. Polarized light[6], rotated 90°, was sent through the connector, and then through the polarization combiner which transmits the slow axis[7] polarization, and block the other. Proper alignment was attained at minimum intensity throughput, and the ferrule was locked with glue. Then the polarization crossing fiber was removed to allow maximum throughput.

[6] Laser with linear polarizer (LP).

[7] *Slow axis* is the axis of a PM fiber with the highest effective refractive index.

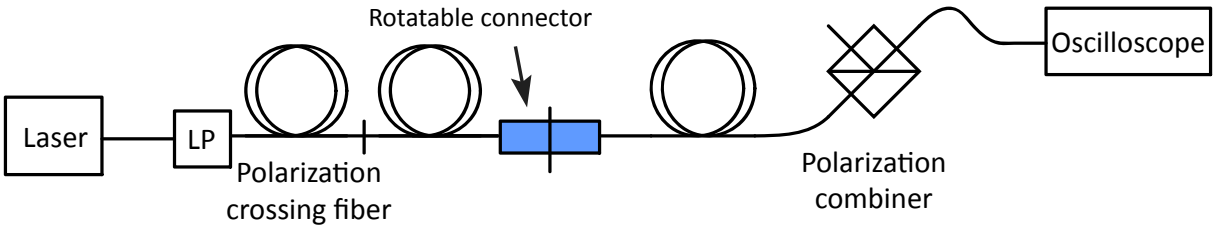



Figure 5.8: Scheme for orienting connector keys

### 5.3.3 Measuring fiber length

The length of the fibers where measured using a ruler. This gave a good starting point for more precise measurements. To do this, the difference in actual optical path length was determined by measuring the travel time of the pulses. As mentioned in section 5.2.2, the margin of error is ±17 mm or ±85 ps. To attain this level of accuracy, the pulse was measured at the rising edge, with the DO. See figure 5.9 for explanation. The difference was then measured to be 1.24 ns, which gives a fiber length of 24.8 cm which can either be subtracted from the arm which is too long, or added to the arm which is too short. When testing for inference with a more powerful laser, and an oscilloscope with higher resolution (CSA), it turned out that this path cord was ∼200 ps too long. Thus, it was shortened by 4 cm.

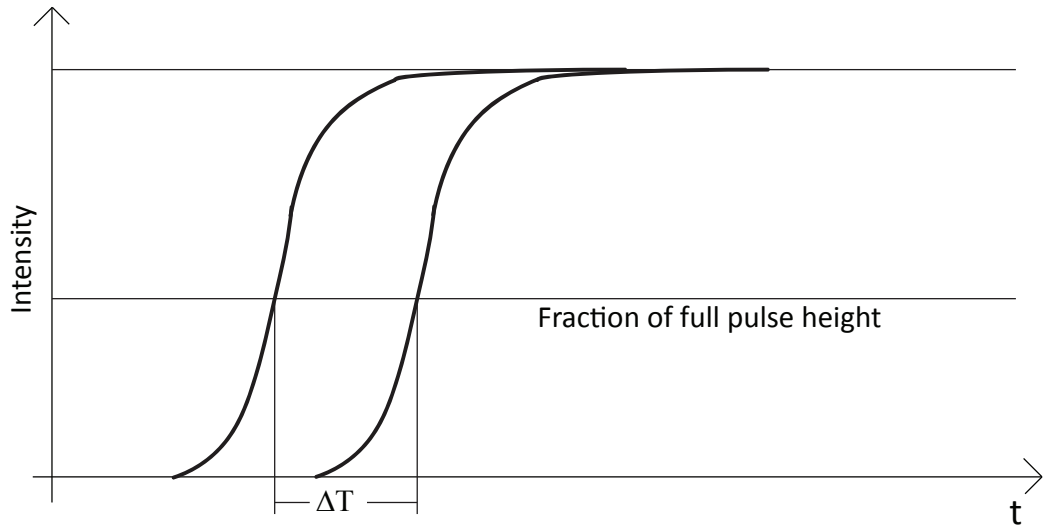



Figure 5.9: Measurement of optical time delay. The oscilloscope is triggered by a signal of equal timing and shape as the laser driving signal. The pulses are measured one at a time, noting the time position of each pulse. Then the time difference is found by comparing the positions.

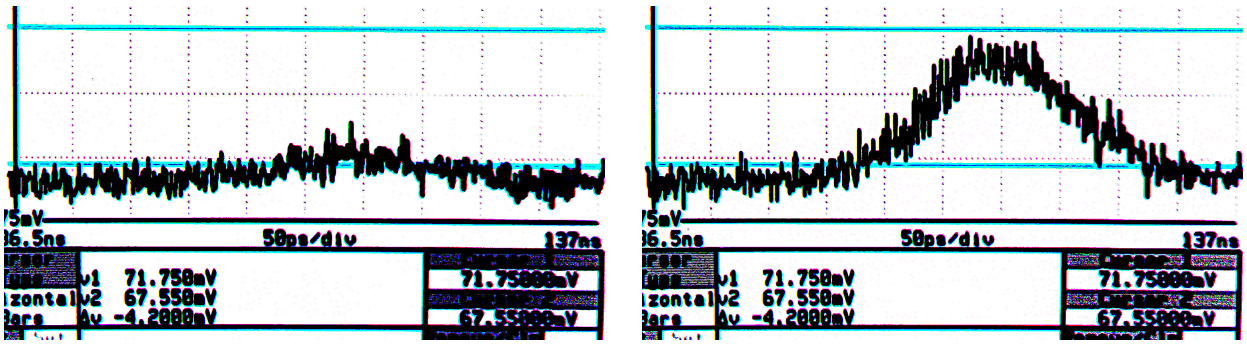



Figure 5.10: Destructive and constructive interference of output one.

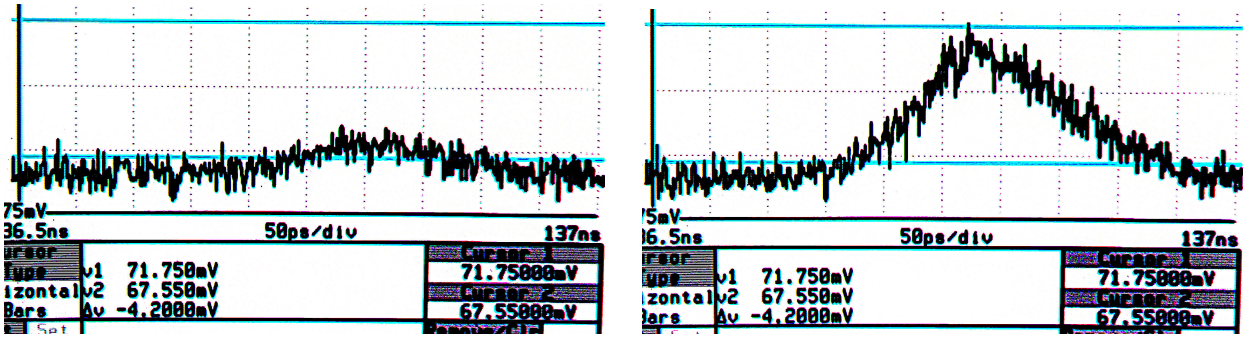



Figure 5.11: Destructive and constructive interference of output two.

Figures 5.10 and 5.11: Vertical axis has 2 mV/div. There is a DC-offset which originates from the ALC. The horizontal axis has 50 ps/div. The pulse is 150-200 ps wide.

### 5.3.4 Interference

The laser being used for the QKD system is low power as it is supposed to emit pulses with average power below single photon level, as we can see from section 4.4. When testing for interference, although it was not attenuated to single photon level, the throughput was too low to get any accurate measurements. Thus a more powerful laser, capable of 100 mW, was used.

When the laser pulses overlapped, interference appeared. The test pulse was in order of nanoseconds, or decimeters long, thus interference was visible over the whole adjustment range of the optical time delay. As the interferometer was assembled on an optical table without insulation, the inference observed was unstable. The fibers are sensitive to temperature variations, and slight fluctuations causes the length to change by a number of wavelength. Just letting your hand hover above the fibers caused them to heat enough for their lengths to run through a multiple of wavelengths rapidly. This was apparent when measuring pulse output as the fringes ran across the oscilloscope screen.

When tuning the setup to obtain interference both time delay and variable attenuator (see figure 5.2) needs to be adjusted. The attenuation of the time delay line varied as a function of delay, thus it had to be compensated by tuning the variable attenuator. The laser used was pulsed with a 1.3 ns square signal from the DDG. When the pulses overlapped, wobbling interference fringes appeared. Adjusting the two variables, a single pulse was obtained, with intensity going up and down as the path length difference varied about zero.

By measuring the peak of the pulse at constructive and destructive interference, a visibility (equation (5.2)) of 95% was obtained. This is a promising result as the measurement was not done under optimal conditions. Both a large path length drift was present, and the test laser did not output a stable spectrum during the pulse. During normal operation, where the interferometer will be insulated and maintain a very stable temperature, and a laser with more stable wavelength will be used, higher visibility should be possible to obtain. Also this visibility should be measured for both outputs, as this directly affects the corresponding QBERs $\delta_0$ and $\delta_1$ from section 2.5.1. A 95% visibiliy alone adds 2.5% QBER.[8]

In figures 5.10 and 5.11 we see photographs[9] of the oscilloscope screen for constructive and destructive interference for both output channels. The path length fluctuations were too severe to allow averaging for smooth curves. Also these do not show the maximum visibility obtained. However, this shows how visibility was found. Letting the interference jump up an down, the marker lines were adjusted, and their position used to find the visibility. These images were taken without adjusting any parameters in between, and the two outputs appear to be symmetrical.

### 5.3.5 Pictures of the setup

This section is dedicated to pictures of the interferometer. In figure 5.12 we see an overview of the whole setup. Tn the background we see the red box of Alice, where her part of the interferometer will be fit into. This box already has mounted electronics and the decoy state generator from [6]. Just in front of the box we see the 100 mW laser used for interference testing. In figures 5.13 and 5.14 we see the a detailed picture of the scheme in figure 5.2. The red lines separate the two interferometer arms.

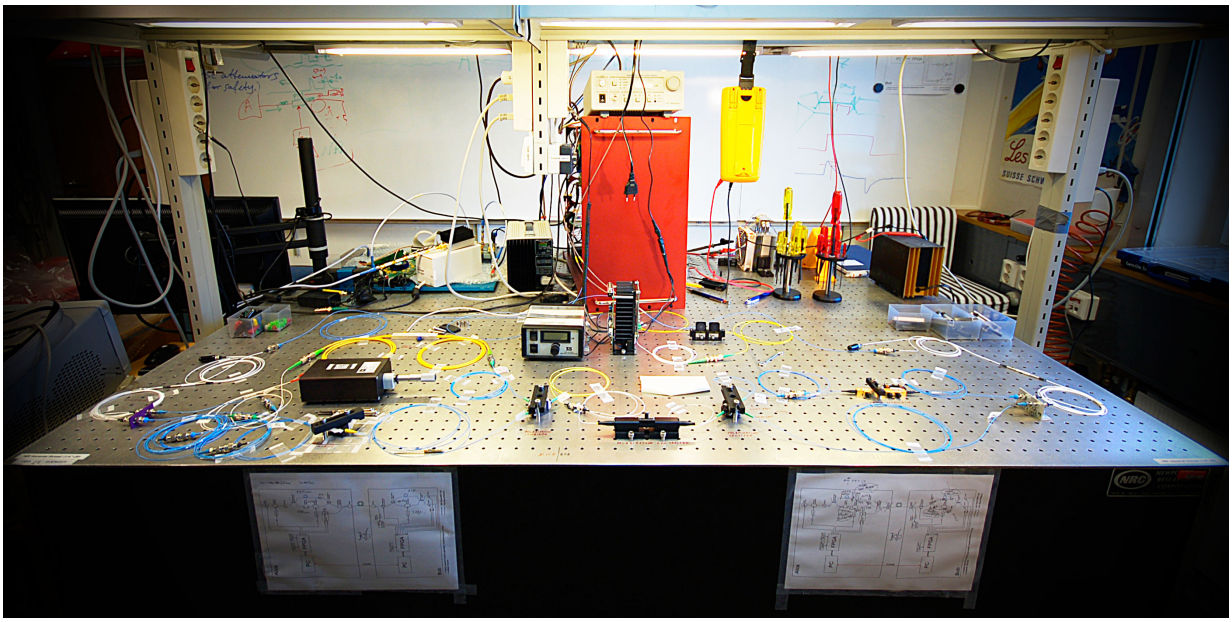


Figure 5.12: Overview of the setup

[8] QBER for caused by interference visibility is $\frac{1-\mathcal{V}}{2}$ [1, eq. (34)].
[9] The age of the oscilloscope made it difficult to extract data directly.

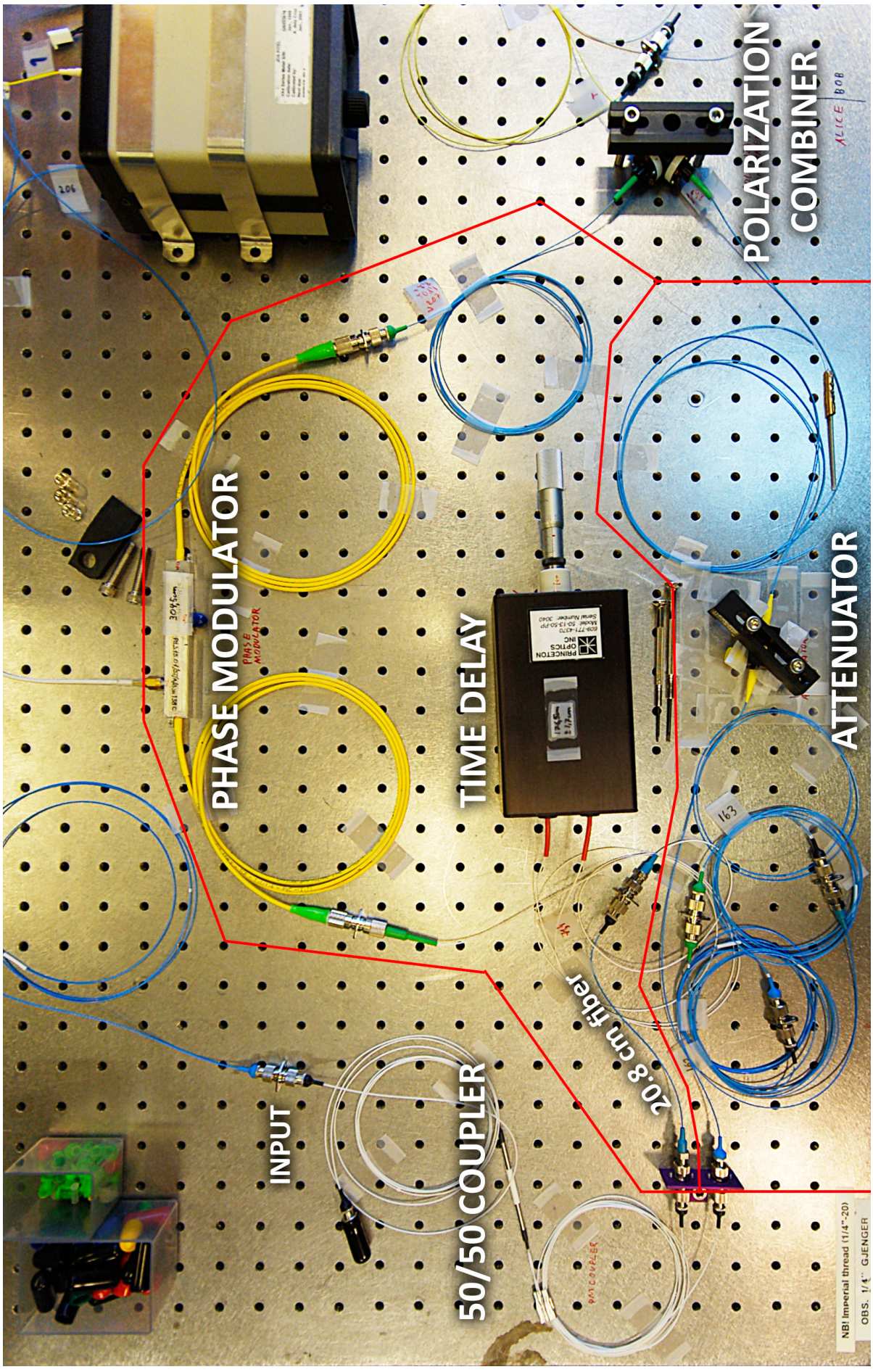



Figure 5.13: Alice's part of the interferometer

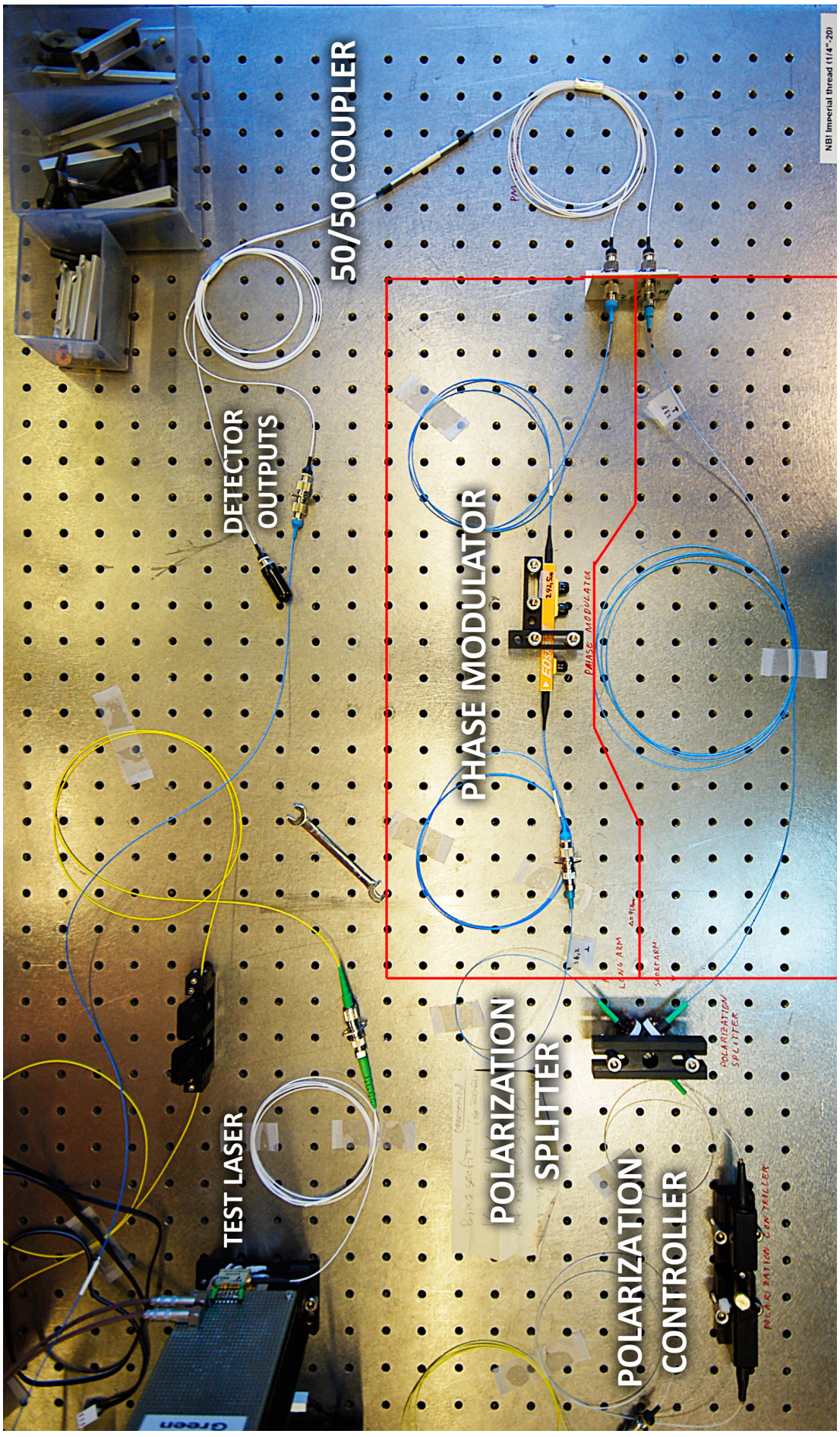



Figure 5.14: Bob's part of the interferometer

# 6 Conclusion and further work

Based on the framework of Lo and Preskill [22], and the security proofs of both Koashi [16] and Marøy et al. [25], QKD system performance has been treated. More specifically, the source has been analyzed concerning its effect on security. In addition, the ongoing project of building a complete secure QKD system has been continued, setting up the interferometer at an optical table.

The interferometer, consisting of Alice's and Bob's parts, was assembled on an optical table. Calculations were done for timing of pulses, and measurements were done to find the required fiber lengths. The fibers were connectorized and spliced accordingly, and interference was obtained. Optimum settings for the variable time delay and variable attenuator were well within the adjustment range. Hence it should be able to tackle all future adjustments of these. Further work will consist of obtaining single photon interference and make the system able to share a symmetric key with the BB84 protocol. Once QKD is demonstrated, the system will be assembled in the rack cases of Alice and Bob and made ready for real-world demonstration. System performance will be analyzed, and the system adjusted to obtain secure key generation.

The two effects in focus when analyzing the source were random phase and fluctuating amplitude. Calculations on random phase showed minimal improvement over non-random phase. In practice, by the methods used in this thesis, there was no difference in system performance for the two cases.

For fluctuating amplitude, a change in system performance was observed. However, the input data for these plots were extreme. Hence, rare fluctuations should not degrade system performance significantly. Still, this imperfection has to be included when considering the performance. Also, non-random, or announced, fluctuations gave a better performance than random fluctuations. It appears that it is better for Alice and Bob to share their information about amplitude with Eve, than not knowing it themselves. Further work may be to model a case where Alice has this information to share after communication, without revealing it Eve during communication. This is relevant for using decoy states, which will be implemented in the QKD system being built.

The results for transmission key generation rate and optimum values of $\mu$ are based on experimental data from [27]. When the QKD system at NTNU is finished, data from this system should be used to calculate its performance.

The work in this thesis is based on the fidelity, as this what the proofs [16, 25] used as the distance measure. Having pure states, the fidelity is simply the inner product. However,

for mixed states (e.g. $\rho_X$ and $\rho_Y$) we cannot calculate the inner product directly. We can calculate the fidelity directly, or we can calculate it by taking the inner product of the optimal purification of the states. This larger system has these mixed states ($\rho_X$ and $\rho_Y$) and another mixed state, called the reference system (e.g. $\rho_R$), as subsystems. But what is the reference system? In general, the reference system has no physical interpretation, and is only an abstract tool for purification. If we are to put a physical interpretation in the reference system, it may be inside Alice, or anywhere else, except in Eve. However, when calculating the inner product of the purification, we give Eve the reference system. It seems that we give Eve more information than she actually has access to. Thus, an interesting question arises. Is fidelity the best way to measure the difference between states? Giving the reference system to Eve is certainly not disadvantageous for her. Hence, the proofs are valid. On the other hand, if it is advantageous for Eve, then characterizing and limiting her gain could lead to higher key generation rate. Answering this question would be an interesting future task.

Appendix

# A Poster

The poster on the next page was presented at the Norwegian electro-optics meeting in Ålesund, April 2010. Authors: E. S. Simonsen, V. Makarov, L. Lydersen, J. Skaar.

# Quantum Key Distribution Source

NTNU
Department of Electronics and Telecommunications

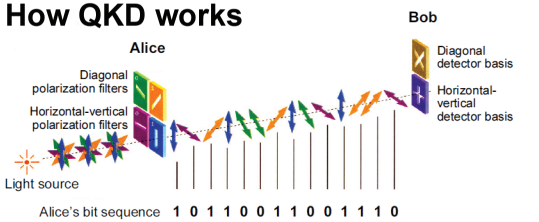
Eivind Sjøtun Simonsen*, Vadim Makarov, Lars Lydersen & Johannes Skaar

Quantum Hacking
Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway.
* E-mail: eivinsi@stud.ntnu.no

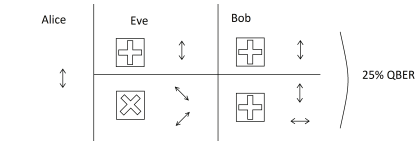
## Introduction

QKD promises unconditional secure symmetric key sharing. Practical implementations have flaws. This system has the goal of adressing all known loopholes.

### How QKD works




*-What happens when Eve attacks?*

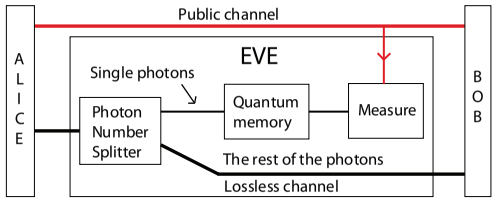




### Laser imperfection

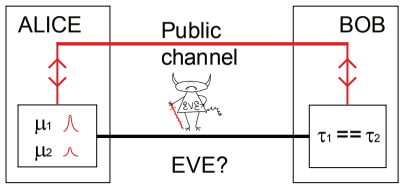
The laser follow the Poisson distribution which creates multi photon pulses that leak information about basis choice. This helps Eve to apply a basis dependent attack.

### PNS attack




### Decoy states

Alice sends pulses of different strengths, $\mu_1$ or $\mu_2$. Then checks with Bob if they measure the same transmittance, $\tau_1 = \tau_2$. If not, they abort.

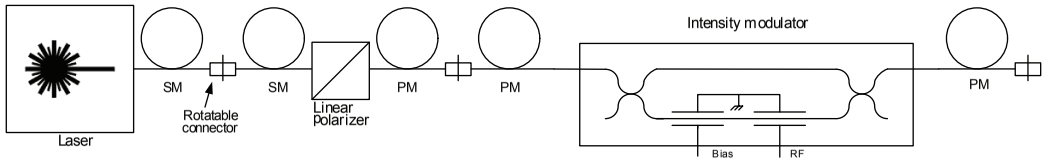


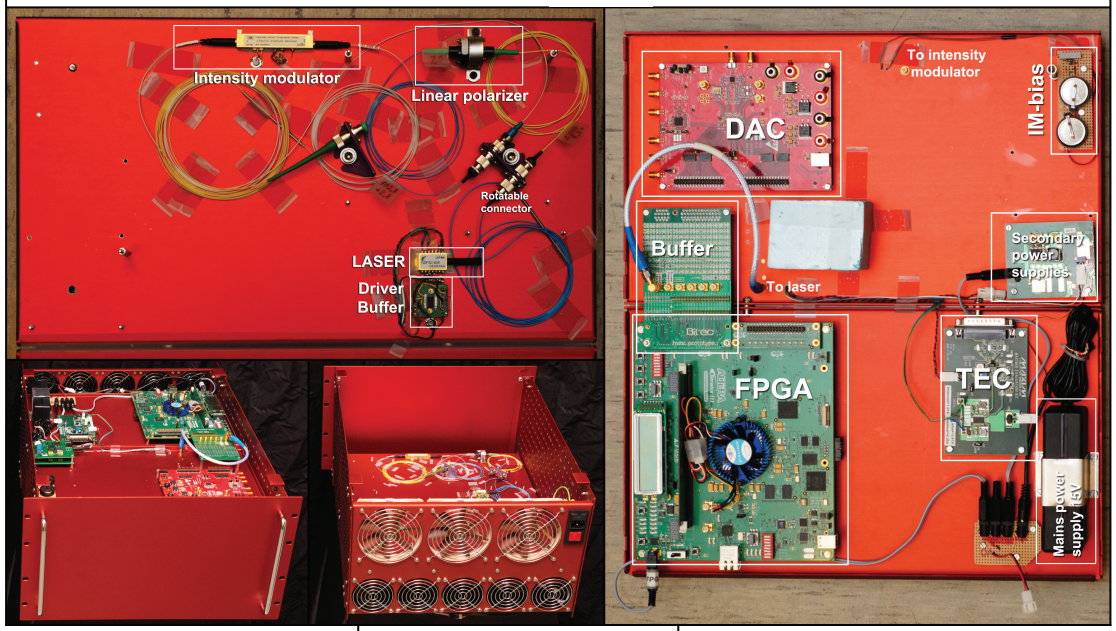

## Decoy state generator

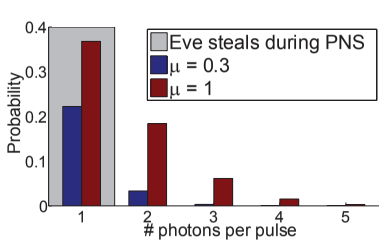
### Practical implementation

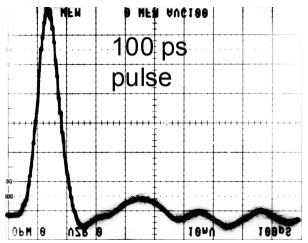
To create decoy pulses, an intensity modulator is used to control expected photon number. FPGA controls the pulse frequency, intensity modulator and the DAC which will control the phase modulator for sending random bits in random bases.

- The laser creates 100 ps phase randomized pulses.
- Produces unstable pulses which has to be accounted for when calculating the secure key generation rate.

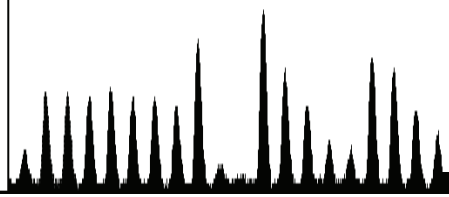



Fluctuating pulses



## Modeling the source

Use BB84 to send phase coded random 0 or 1 in randomly selected X or Y basis.

$$|\Psi_X\rangle = \left(|0_X\rangle|\alpha\rangle + |1_X\rangle|-\alpha\rangle\right)|\beta\rangle$$

$$|\Psi_Y\rangle = \left(|0_Y\rangle|-i\alpha\rangle + |1_Y\rangle|i\alpha\rangle\right)|\beta\rangle$$

Ideally these states are indistinguishable

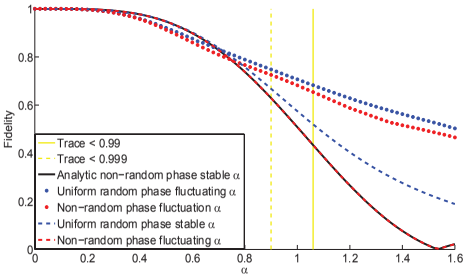
$$\langle\Psi_Y|\Psi_X\rangle = 1$$

But, $\alpha$ (signal) and $\beta$ (ref) follow Poisson distribution. Photon number states

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

Random phase to improve indistinguishability (fidelity)

$$\rho_a = \int_{\varphi=0}^{2\pi} |\Psi_a\rangle\langle\Psi_a| p(\varphi) d\varphi$$




### Fluctuating pulse intensity

Amplitudes $\alpha$ fluctuate on a descrete set of values $\{\alpha_j\}$ with probabilities $\{q_j\}$. Comparing against the weighted average of intensities; weighted RMS over $\alpha$.

#### Random fluctuations

Best case scenario. No correlation between pulses.

$$\rho_a(\alpha) = \sum_j \rho_a(\alpha_j) q_j \quad \text{vs.} \quad \rho_a(\alpha_{RMS})$$

The fidelity plot for fluctuating case uses $\alpha = \{1, 2, 4\}$ and $q = \{0.5, 0.3, 0.2\}$.

#### Non-random fluctuations

Worst case scenario. Eve knows the expected intensity. Weighted sum over key generation rates $G$ for different $\alpha$.

$$G(\alpha) = \sum_j G(\alpha_j) q_j \quad \text{vs.} \quad G(\alpha_{RMS})$$

Presented at Norwegian electro-optics meeting in Ålesund, April 2010

Appendix

# B Calculations

## B.1 Inner product of some states

Having two coherent states $|c_1\alpha\rangle$ and $|c_2\alpha\rangle$ where $c_j \in \{\pm 1, \pm i\}$ the inner product is

$$\langle c_2\alpha|c_1\alpha\rangle = e^{-|\alpha|^2} \sum_{mn} \frac{c_2^{*m}\alpha^{*m}c_1^n\alpha^n}{\sqrt{m!n!}} \langle m|n\rangle = e^{-|\alpha|^2} \sum_n \frac{c_2^{*n}c_1^n|\alpha|^{2n}}{n!} = e^{-|\alpha|^2}e^{c_2^*c_1|\alpha|^2} \tag{B.1}$$

which gives us

$$\begin{aligned} \langle i\alpha|\alpha\rangle &= e^{-|\alpha|^2}e^{-i|\alpha|^2} = \langle -i\alpha|-\alpha\rangle \\ \langle -i\alpha|\alpha\rangle &= e^{-|\alpha|^2}e^{i|\alpha|^2} = \langle i\alpha|-\alpha\rangle \end{aligned} \tag{B.2}$$

All possible inner products of $\langle b_Y|b_X\rangle$, $b \in \{0, 1\}$:

$$\langle 0_Y|0_X\rangle = \frac{1}{2}\Big( \langle 0_Z|0_Z\rangle + \langle 0_Z|1_Z\rangle + i\langle 1_Z|0_Z\rangle + i\langle 1_Z|1_Z\rangle \Big) = \frac{1}{2}(1+i) \tag{B.3a}$$

$$\langle 0_Y|1_X\rangle = \frac{1}{2}\Big( \langle 0_Z|0_Z\rangle - \langle 0_Z|1_Z\rangle + i\langle 1_Z|0_Z\rangle - i\langle 1_Z|1_Z\rangle \Big) = \frac{1}{2}(1-i) \tag{B.3b}$$

$$\langle 1_Y|0_X\rangle = \frac{1}{2}\Big( \langle 0_Z|0_Z\rangle + \langle 0_Z|1_Z\rangle - i\langle 1_Z|0_Z\rangle - i\langle 1_Z|1_Z\rangle \Big) = \frac{1}{2}(1-i) \tag{B.3c}$$

$$\langle 1_Y|1_X\rangle = \frac{1}{2}\Big( \langle 0_Z|0_Z\rangle - \langle 0_Z|1_Z\rangle + i\langle 1_Z|0_Z\rangle - i\langle 1_Z|1_Z\rangle \Big) = \frac{1}{2}(1+i) \tag{B.3d}$$

## B.2 Intermediate calculations for random phase

With equation (3.11) we get the density matrices

$$\left.\begin{matrix}\rho_{X00}\\ \rho_{X01}\\ \rho_{X10}\\ \rho_{X11}\end{matrix}\right\} = \sum_{kl} \left\{\begin{matrix} & |0_X\rangle\langle 0_X| \\ (\text{-}1)^l & |0_X\rangle\langle 1_X| \\ (\text{-}1)^k & |1_X\rangle\langle 0_X| \\ (\text{-}1)^{k+l} & |1_X\rangle\langle 1_X| \end{matrix}\right\} \otimes \rho_{kl} \tag{B.4a}$$

$$\left.\begin{matrix}\rho_{Y00}\\ \rho_{Y01}\\ \rho_{Y10}\\ \rho_{Y11}\end{matrix}\right\} = \sum_{kl} i^{k+l} \left\{\begin{matrix} (\text{-}1)^k & |0_Y\rangle\langle 0_Y| \\ (\text{-}1)^{k+l} & |0_Y\rangle\langle 1_Y| \\ & |1_Y\rangle\langle 0_Y| \\ (\text{-}1)^l & |1_Y\rangle\langle 1_Y| \end{matrix}\right\} \otimes \rho_{kl} \tag{B.4b}$$

The state vectors of X and Y basis expressed in Z basis are

$$\begin{aligned} |0_X\rangle &= \frac{1}{\sqrt{2}}(|0_Z\rangle + |1_Z\rangle) & |0_Y\rangle &= \frac{1}{\sqrt{2}}(|0_Z\rangle + i\,|1_Z\rangle) \\ |1_X\rangle &= \frac{1}{\sqrt{2}}(|0_Z\rangle - |1_Z\rangle) & |1_Y\rangle &= \frac{1}{\sqrt{2}}(|0_Z\rangle - i\,|1_Z\rangle) \end{aligned} \tag{B.5}$$

This gives the density matrices (remembering $\langle\Psi|\,c^* \Leftrightarrow c\,|\Psi\rangle$)

$$\begin{aligned} 2\,|0_X\rangle\langle 0_X| &= |0_Z\rangle\langle 0_Z| + |0_Z\rangle\langle 1_Z| + |1_Z\rangle\langle 0_Z| + |1_Z\rangle\langle 1_Z| \\ 2\,|0_X\rangle\langle 1_X| &= |0_Z\rangle\langle 0_Z| - |0_Z\rangle\langle 1_Z| + |1_Z\rangle\langle 0_Z| - |1_Z\rangle\langle 1_Z| \\ 2\,|1_X\rangle\langle 0_X| &= |0_Z\rangle\langle 0_Z| + |0_Z\rangle\langle 1_Z| - |1_Z\rangle\langle 0_Z| - |1_Z\rangle\langle 1_Z| \\ 2\,|1_X\rangle\langle 1_X| &= |0_Z\rangle\langle 0_Z| - |0_Z\rangle\langle 1_Z| - |1_Z\rangle\langle 0_Z| + |1_Z\rangle\langle 1_Z| \end{aligned} \tag{B.6a}$$

$$\begin{aligned} 2\,|0_Y\rangle\langle 0_Y| &= |0_Z\rangle\langle 0_Z| - i\,|0_Z\rangle\langle 1_Z| + i\,|1_Z\rangle\langle 0_Z| + |1_Z\rangle\langle 1_Z| \\ 2\,|0_Y\rangle\langle 1_Y| &= |0_Z\rangle\langle 0_Z| + i\,|0_Z\rangle\langle 1_Z| + i\,|1_Z\rangle\langle 0_Z| - |1_Z\rangle\langle 1_Z| \\ 2\,|1_Y\rangle\langle 0_Y| &= |0_Z\rangle\langle 0_Z| - i\,|0_Z\rangle\langle 1_Z| - i\,|1_Z\rangle\langle 0_Z| - |1_Z\rangle\langle 1_Z| \\ 2\,|1_Y\rangle\langle 1_Y| &= |0_Z\rangle\langle 0_Z| + i\,|0_Z\rangle\langle 1_Z| - i\,|1_Z\rangle\langle 0_Z| + |1_Z\rangle\langle 1_Z| \end{aligned} \tag{B.6b}$$

The Pauli matrices expressed in Z basis

$$\begin{aligned} I &= \phantom{-i}\,|0_Z\rangle\langle 0_Z| + \phantom{i}\,|1_Z\rangle\langle 1_Z| \\ X &= \phantom{-i}\,|0_Z\rangle\langle 1_Z| + \phantom{i}\,|1_Z\rangle\langle 0_Z| \\ Y &= -i\,|0_Z\rangle\langle 1_Z| + i\,|1_Z\rangle\langle 0_Z| \\ Z &= \phantom{-i}\,|0_Z\rangle\langle 0_Z| - \phantom{i}\,|1_Z\rangle\langle 1_Z| \end{aligned} \tag{B.7}$$

Combining these expressions gives the density matrices for $\rho_X$ and $\rho_Y$ in equation (3.12) expressed in Z basis in section 3.1.1.

Appendix

# C Matlab code

To convert m-files to tex, *m-code to LaTeX converter* (version 2.1) by Uwe Lelke was used.

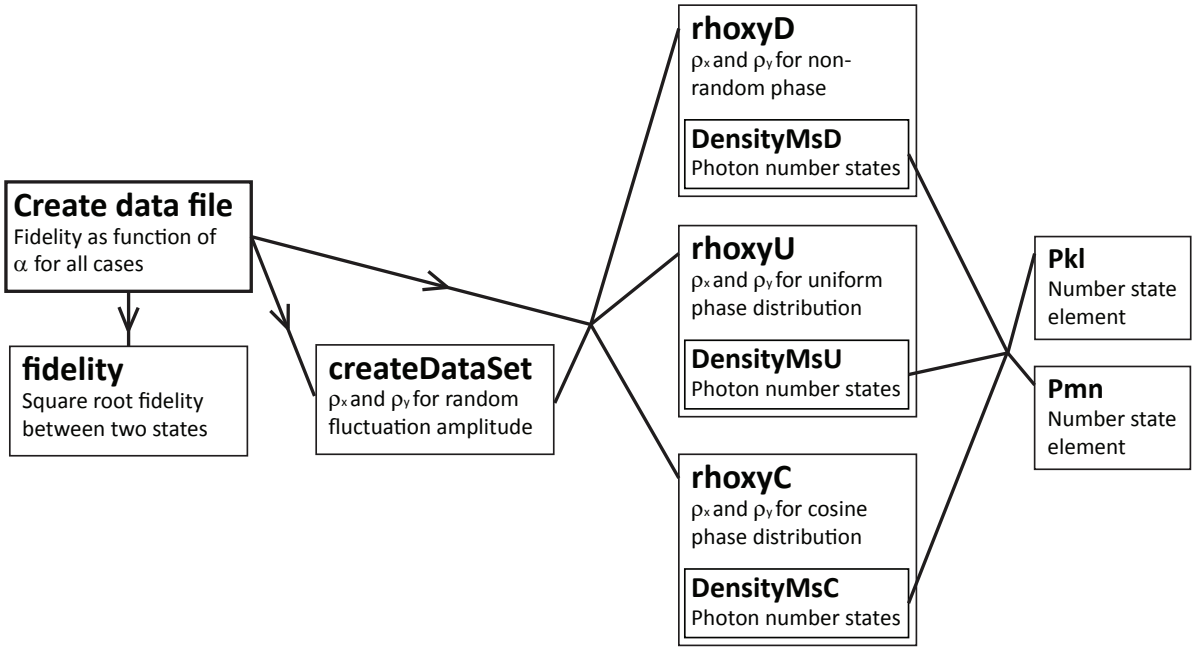



Figure C.1: Scheme over data set creation functions

## C.1 Creating density matrices

### C.1.1 Main functions

#### Non-random phase

```
function [Px,Py] = rhoxyD(A,B,N)
%rhoxyD(A,B,N) produses the X and Y density matrices for
%non-random/determined phase distribution. A and B are
%signal and reference amplitude, N is cacluation size.

I = [1 0; 0 1]; X = [0 1; 1 0];
Y = [0 -1i; 1i 0]; Z = [1 0; 0 -1]; %Pauli matrices

Px = kron(I+X,DensityMsD(1,1,A,B,N)) ...
   + kron(Z-1i*Y,DensityMsD(1,-1,A,B,N)) ...
   + kron(Z+1i*Y,DensityMsD(-1,1,A,B,N)) ...
   + kron(I-X,DensityMsD(-1,-1,A,B,N));

Py = kron(I+Y,DensityMsD(-1i,-1i,A,B,N)) ...
   + kron(Z+1i*X,DensityMsD(-1i,1i,A,B,N)) ...
   + kron(Z-1i*X,DensityMsD(1i,-1i,A,B,N)) ...
   + kron(I-Y,DensityMsD(1i,1i,A,B,N));

%-------------------------
function DMD = DensityMsD(c1,c2,A,B,N)
PklV = zeros(N,N); PmnV = zeros(N,N);
parfor m = 0:N-1 %parallel computing
  for n = 0:N-1
    PklV = PklV + Pkl(c1,c2,A,m,n,N);
    PmnV = PmnV + Pmn(B,m,n,N);
  end
end
DMD = kron(PklV,PmnV);
DMD = 0.25*exp(-(A^2)-(B^2)).*DMD;
```

**Uniform random phase**

```
function [Px,Py] = rhoxyU(A,B,N)
%rhoxyU(A,B,N) produses the X and Y density matrices for uniform
%phase distribution. A and B are signal and reference amplitude,
%N is cacluation size.

I = [1 0; 0 1]; X = [0 1; 1 0];
Y = [0 -1i; 1i 0]; Z = [1 0; 0 -1]; %Pauli matrices

Px = kron(I+X,DensityMsU(1,1,A,B,N)) ...
   + kron(Z-1i*Y,DensityMsU(1,-1,A,B,N)) ...
   + kron(Z+1i*Y,DensityMsU(-1,1,A,B,N)) ...
   + kron(I-X,DensityMsU(-1,-1,A,B,N));

Py = kron(I+Y,DensityMsU(-1i,-1i,A,B,N)) ...
   + kron(Z+1i*X,DensityMsU(-1i,1i,A,B,N)) ...
   + kron(Z-1i*X,DensityMsU(1i,-1i,A,B,N)) ...
   + kron(I-Y,DensityMsU(1i,1i,A,B,N));

%-------------------------
function DMU = DensityMsU(c1,c2,A,B,N)
DMU = zeros(N*N,N*N);
parfor k = 0:N-1 %parallel computing
  for l = 0:N-1
    PmnV = zeros(N,N);
    for m = 0:N-1
      if (k-l+m)>=0 && (k-l+m)<N
        PmnV = PmnV + Pmn(B,m,k-l+m,N);
      end
    end
    DMU = DMU + kron(Pkl(c1,c2,A,k,l,N),PmnV);
  end
end
DMU = 0.25*exp(-(A^2)-(B^2)).*DMU;
```

**Cosine distributed phase**

```
function [Px,Py] = rhoxyC(d,q,A,B,N)
%rhoxyC(A,B,N) produses the X and Y density matrices for cosine
%phase distribution. A and B are signal and reference amplitude,
%N is cacluation size.

I = [1 0; 0 1]; X = [0 1; 1 0];
Y = [0 -1i; 1i 0]; Z = [1 0; 0 -1]; %Pauli matrices

Px = kron(I+X,DensityMsC(d,q,1,1,A,B,N)) ...
   + kron(Z-1i*Y,DensityMsC(d,q,1,-1,A,B,N)) ...
   + kron(Z+1i*Y,DensityMsC(d,q,-1,1,A,B,N)) ...
   + kron(I-X,DensityMsC(d,q,-1,-1,A,B,N));

Py = kron(I+Y,DensityMsC(d,q,-1i,-1i,A,B,N)) ...
   + kron(Z+1i*X,DensityMsC(d,q,-1i,1i,A,B,N)) ...
   + kron(Z-1i*X,DensityMsC(d,q,1i,-1i,A,B,N)) ...
   + kron(I-Y,DensityMsC(d,q,1i,1i,A,B,N));

%-------------------------
function DMC = DensityMsC(d,q,c1,c2,A,B,N)
DMC = zeros(N*N,N*N); W = 0.5*d/(q-q*d+d);
parfor k = 0:N-1 %parallel computing
  for l = 0:N-1
    PmnV = zeros(N,N);
    for m = 0:N-1
      for n = 0:N-1
        if (k-l+m-n) == 0
          PmnV = PmnV + Pmn(B,m,n,N);
        elseif abs(k-l+m-n) == q
          PmnV = PmnV - W*Pmn(B,m,n,N);
        elseif q > 1
          PmnV = PmnV + (1i*q*W*(1-exp(1i*2*pi*(k-l+m-n)/q)) ...
              *((1/(k-l+m-n))-(0.5/((k-l+m-n)+q)) ...
              -(0.5/((k-l+m-n)-q)))*Pmn(B,m,n,N)/pi);
        end
      end
    end
    DMC = DMC + kron(Pkl(c1,c2,A,k,l,N),PmnV);
  end
end
DMC = 0.25*exp(-(A^2)-(B^2))*DMC;
```

### C.1.2 Subfunctions

#### Pkl

```
function f = Pkl(c1,c2,A,k,l,N)
%Creates the element factor which is dependent on k and l.

c1k = c1^k; c2l = (conj(c2))^l;
f = zeros(N,N);
f(k+1,l+1) = c1k*c2l*(A^(k+l))/(sqrt(factorial(k)*factorial(l)));
```

#### Pmn

```
function d = Pmn(B,m,n,N)
%Creates the element factor which is dependent on m and n.

d = zeros(N,N);
d(m+1,n+1) = (B^(m+n))/(sqrt(factorial(m)*factorial(n)));
```

## C.2 Numerical calculations

### C.2.1 Create dataset file

```
%For creating data set and save it to file

N = 8; % Calculation size, proportional to 2*N^4.
A = 0:0.001:2; % Signal pulse photon number mean value u=2A^2
B = A; % Reference pulse photon number mean value u=2B^2
K = [0.25 0.5 1 2]; % Relative amplitudes for fluctating case
q = [0.2 0.2 0.4 0.2]; % Their probabilities
Kavg = sqrt(sum(q.*K.^2)); % to give same average photon number
K = K/Kavg;
qC = 5; dC = 1; % q and d in cosine distribution

L = length(A); Lq = length(q); N2 = 2*N^2;
zerosN2 = zeros(N2,N2); Ns = zeros(1,length(A));

FuR = zeros(L,1); FdR = zeros(L,1);
tuR = ones(L,1); tdR = ones(L,1);
Fu = zeros(L,1); Fd = zeros(L,1); Fc = zeros(L,1);
tu = ones(L,1); td = ones(L,1); tc = ones(L,1);
NonRanPhase = zeros(L,1);

progress = 0 %#ok<NOPTS>
tStart = tic;
for p = 1:L
    % Analytical solution for non-random phase
    NonRanPhase(p) = abs(cos(A(p)^2)+sin(A(p)^2))*exp(-A(p)^2);
    % Numerical solution for non-random phase
    [Pxd,Pyd] = rhoxyd(A(p),B(p),N);
    Fd(p) = fidelity(Pxd,Pyd);
    td(p) = min([trace(Pxd) trace(Pyd)]);
    % Uniform phase distribution
    [Pxu,Pyu] = rhoxyU(A(p),B(p),N);
    Fu(p) = fidelity(Pxu,Pyu); % Fidelity
    tu(p) = min([trace(Pxu) trace(Pyu)]);
    % Cosine distributed phase
    [Pxc,Pyc] = rhoxyC(dC,qC,A(p),B(p),N);
    Fc(p) = fidelity(Pxc,Pyc); % Fidelity
    tc(p) = min([trace(Pxc) trace(Pyc)]);

    % Fluctuating case: u for uniform d for determined
    [PxuS,PyuS,PxdS,PydS] = createDataSet(A(p),B(p),N,K,q);
    % Uniform distributed phase
    FuR(p) = fidelity(PxuS,PyuS); % Fidelity
    tuR(p) = min([trace(PxuS) trace(PyuS)]);
    % Non-random phase
```

```
45      FdR(p) = fidelity(PxdS,PydS); % Fidelity
46      tdR(p) = min([trace(PxdS) trace(PydS)]);
47
48      Ns(p) = N; % Log the Ns used
49      if min([tu(p) td(p) tuR(p) tdR(p) tc(p)]) <= 0.999999 && N<16;
50          N = N+2; end; % Increase calculation size when needed
51  end
52  save('dataUD_A0_0001_2_Nvar_dC1_qC5_K025_05_1_2_q02_02_04_02', ...
53      'A','B','Fu','Fd','Fc','FuR','FdR','NonRanPhase','Ns')
```

### C.2.2 Create dataset for fluctuating case

```
1   function [PxuS,PyuS,PxdS,PydS] = createDataSet(A,B,N,K,q)
2   %createDataSet(A,B,N,K,q) creates data set for fluctuating
3   %fidelity with K as the relative amplitude konstants and q are
4   %the probabilities
5
6   Lq = length(q); N2 = 2*N^2; zerosN2 = zeros(N2,N2);
7   PxuS = zerosN2; PyuS = zerosN2; PxdS = zerosN2; PydS = zerosN2;
8   parfor j = 1:Lq %parallel computing
9       % uniform phase distribution
10      [Pxu,Pyu] = rhoxyU(K(j)*A,K(j)*B,N);
11      PxuS = PxuS + q(j)*Pxu;
12      PyuS = PyuS + q(j)*Pyu;
13      % non-random (determined) phase
14      [Pxd,Pyd] = rhoxyD(K(j)*A,K(j)*B,N);
15      PxdS = PxdS + q(j)*Pxd;
16      PydS = PydS + q(j)*Pyd;
17  end
```

### C.2.3 Fidelity

```
1   function F = fidelity(P,S)
2   % returns the square root fidelity
3   warning off all
4   % P = sqrtm(P*P'); % To ensure they are
5   % S = sqrtm(S*S'); % Hermitian
6   sP = sqrtm(P);
7   Q = sP*S*sP;
8   sQ = sqrtm(Q);
9   F = trace(sQ);
```

## C.3 Key generation rate

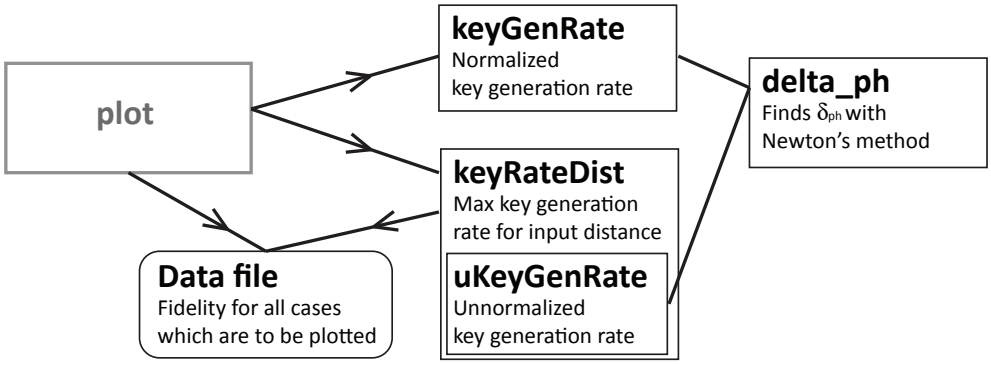



Figure C.2: Scheme over functions for calculating key generate

### C.3.1 keyGenRate

```
function R_Z = keyGenRate2(F,A,QBER,who)
u = A^2;
eta_Z = 1; % Detection efficiency

delta_Z = QBER; % QBER
delta_X = delta_Z;

q_X = 1-exp(-u); % Probability of nonvacuum event
q_ph = q_X; % Or just 1?

if (who == 'M')
% MarÃ¸y
delta_ph = Delta_ph(F,delta_X,q_X,q_ph);
% /MarÃ¸y
else
% Koashi
delta_ph = Delta_ph(F,delta_X);
% /Koashi
end
% R_Z = (eta_Z*q_ph/q_Z)*(1 - H(min(0.5, delta_ph))) - H(delta_Z);
R_Z = eta_Z*(1 - H(min(0.5, delta_ph))) - H(delta_Z);
R_Z = max(real(R_Z),0);
```

### C.3.2 Binary entropy function H

```
function h = H(e)
%Binary entropy
if e == 1 || e == 0
```

```
    h = 0; % log2(0) fails
else
    h = - e.*log2(e) - (1-e).*log2(1-e);
end
```

### C.3.3 Delta ph

```
function Dph = Delta_ph(F,D,Dph0,q,q_ph)
% Newtons method for finding Dph with 'decacc' decimal accuracy
% Here F refers to the square root fidelity
if D>0.1101; Dph = 0.5; return; end
F = real(F);
if F==1; Dph = D; return; end;
if F^2<0.5 || D>=0.5; Dph = 0.5; return; end
if Dph0<1; Dph = Dph0; % Try start at previous Dph
else Dph = 1-F^2 + 2*D; % Starting at the right side of F=1
    if Dph>1; Dph = 1; end % Dph <= 1
end
sD = sqrt(D); s1D = sqrt(1-D);
i = 0; acc = 1; decacc = 9; max = decacc*1000;

if nargin == 3; s1M=0; sM=1; % Koashi
else % MarÃ¸y
    if nargin == 4; q_ph = q; end;
    if F<=1-0.5*q_ph; Dph = 0.5; return; end % F>1-q_ph for +KGR
    s1M = sqrt((1-q)*(1-q_ph)); sM = sqrt(q*q_ph);
end
if (sD*sM+s1M)>=F; Dph = 0.5; return; end % No solution for Dph

while (i<max && acc); i = i+1;
    if Dph < D; Dph = 2*D-Dph; end
    G = s1D*sM*sqrt(1-Dph) + sD*sM*sqrt(Dph) + s1M - F;
    dG = 0.5*sM*(-s1D/sqrt(1-Dph) + sD/sqrt(Dph));
    Dph = Dph - (G/dG);
    if isnan(G/dG); error('Not a number appeared'); end
    % Stop if its accurate to the 'decacc'th decimal
    acc = 0 ~= round(10^decacc*G/dG);
end

Dph = abs(Dph);
% If we cannot guarantie correct solution: abort.
if i==max; error('Loop reached maximum allowed iterations');end
if isnan(Dph); error('Not a number appeared');end
if Dph<D; error('Chose lower solution');end
```

### C.3.4 Transmission key generation rate

Transmission key generation rate with optimum amplitudes

```
function [RnMax RuMax RdRMax RuRMax RdAMax RuAMax, ...
    An Au AdR AuR AdA AuA] = keyRateDist(Pe,nB,dist)

load('dataUD_A0_0001_2_Nvar_dC1_qC5_K025_05_1_2_q02_02_04_02');

Am = A(1:round(length(A)/2));
L = length(Am);
Rn = zeros(L,1); Ru = zeros(L,1);
RdR = zeros(L,1); RuR = zeros(L,1); % Random fluct
RdA = zeros(L,1); RuA = zeros(L,1); % Announced fluct
Dphn = ones(L+1,1); Dphu = ones(L+1,1);
DphdR = ones(L+1,1); DphuR = ones(L+1,1); % Random fluct
DphdA1 = ones(L+1,1); DphuA1 = ones(L+1,1); % Announced fluct
DphdA2 = ones(L+1,1); DphuA2 = ones(L+1,1); % Announced fluct
DphdA3 = ones(L+1,1); DphuA3 = ones(L+1,1); % Announced fluct
DphdA4 = ones(L+1,1); DphuA4 = ones(L+1,1); % Announced fluct

K = [0.25 0.5 1 2]; % Relative amplitudes for fluctating case
q = [0.2 0.2 0.4 0.2]; % Their probabilities
Kavg = sqrt(sum(q.*K.^2)); % to give same average photon number
K = K/Kavg;
K1 = K(1); K2 = K(2); K3 = K(3); K4 = K(4);
q1 = q(1); q2 = q(2); q3 = q(3); q4 = q(4);

for j=1:L
    [Rn(j) Dphn(j+1)] = ...
        uKeyGenRate(NonRanPhase(j),A(j),Pe,nB,dist,Dphn(j));
    [Ru(j) Dphu(j+1)] = ...
        uKeyGenRate(Fu(j),A(j),Pe,nB,dist,Dphu(j));
    [RdR(j) DphdR(j+1)] = ...
        uKeyGenRate(FdR(j),A(j),Pe,nB,dist,DphdR(j));
    [RuR(j) DphuR(j+1)] = ...
        uKeyGenRate(FuR(j),A(j),Pe,nB,dist,DphuR(j));

    j1 = findIndex(K1*A(j)); j2 = findIndex(K2*A(j));
    j3 = findIndex(K3*A(j)); j4 = findIndex(K4*A(j));
    [RdA1 DphdA1(j+1)] = ...
      uKeyGenRate(NonRanPhase(j1),A(j1),Pe,nB,dist,DphdA1(j));
    [RdA2 DphdA2(j+1)] = ...
     uKeyGenRate(NonRanPhase(j2),A(j2),Pe,nB,dist,DphdA2(j));
    [RdA3 DphdA3(j+1)] = ...
     uKeyGenRate(NonRanPhase(j3),A(j3),Pe,nB,dist,DphdA3(j));
    [RdA4 DphdA4(j+1)] = ...
     uKeyGenRate(NonRanPhase(j4),A(j4),Pe,nB,dist,DphdA4(j));
    RdA(j) = q1*RdA1 + q2*RdA2 + q3*RdA3 + q4*RdA4;
```

```
46      [RuA1 DphuA1(j+1)] = ...
47       uKeyGenRate(Fu(j1),A(j1),Pe,nB,dist,DphuA1(j));
48      [RuA2 DphuA2(j+1)] = ...
49       uKeyGenRate(Fu(j2),A(j2),Pe,nB,dist,DphuA2(j));
50      [RuA3 DphuA3(j+1)] = ...
51       uKeyGenRate(Fu(j3),A(j3),Pe,nB,dist,DphuA3(j));
52      [RuA4 DphuA4(j+1)] = ...
53       uKeyGenRate(Fu(j4),A(j4),Pe,nB,dist,DphuA4(j));
54      RuA(j) = q1*RuA1 + q2*RuA2 + q3*RuA3 + q4*RuA4;
55  end
56  [RnMax An] = max(Rn); [RuMax Au] = max(Ru);
57  [RdRMax AdR] = max(RdR); [RuRMax AuR] = max(RuR);
58  [RdAMax AdA] = max(RdA); [RuAMax AuA] = max(RuA);
59
60  %-------------------------
61  function [R_0 delta_ph] = uKeyGenRate(F,A,Pe,nB,dist,Dph0)
62  u = (A^2)*10^(-0.02*dist);
63  QBER = 0.5*Pe/(0.5*u*nB + Pe);
64  delta_0 = QBER;
65  delta_1 = QBER;
66  q_ph = 1-exp(-u); % Probability of nonvacuum event
67
68  delta_ph = Delta_ph(F,delta_1,Dph0,q_ph,q_ph);
69
70  R_0 = 1 - H(min(0.5, delta_ph)) - H(delta_0);
71  R_0 = nB*q_ph*max(real(R_0),0);
72
```

# References


[1] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, Sep 2001.

[2] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[3] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J.Sci.Statist.Comput.*, 26:1484, 1997.

[4] Robert J. McEliece. A public-key cryptosystem based on algebraic coding theory. Technical report, Jet Propulsion Lab Deep Space Network Progress report, 1978.

[5] Daniel J. Bernstein, Sean Hallgren, and Ulrich Vollmer. Introduction to post-quantum cryptography, Quantum computing. In Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, editors, *Post-Quantum Cryptography*. Springer Berlin Heidelberg, 2009.

[6] Eivind Sjøtun Simonsen. Decoy state generator for quantum key distribution source. `http://www.iet.ntnu.no/groups/optics/qcr/publications/simonsen-student-project-report-20091217.pdf`, Norwegian University of Science and Technology, 2009.

[7] Gilbert S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal of the American Institute of Electrical Engineers*, 45:109–115, February 1926.

[8] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, October 1982.

[9] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, 1984.

[10] Lars Vincent van De Wiel Lydersen. Security of QKD-systems with detector efficiency mismatch. Master's thesis, Norwegian University of Science and Technology, 2008.

[11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*, pages 70,80,84,95,100–101,110–117,410. Cambridge University Press, October 2000.

[12] Bahaa E. A. Saleh and Malvin C. Teich. *Fundamentals of Photonics*, pages 70,73,340–341,350,463–464,863–866. Wiley-Interscience, 2nd edition, August 1991.

[13] Rodney Loudon. *The Quantum Theory of Light (Oxford Science Publications)*, page 190. OUP Oxford, 3 edition, September 2000.

[14] Quantiki. Fidelity. `http://www.quantiki.org/wiki/Fidelity`, 16:13, 1 June 2010.

[15] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85:441, 2000.

[16] Masato Koashi. Simple security proof of quantum key distribution via uncertainty principle, 2005.

[17] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *Phys. Rev. A*, 51(3):1863–1869, Mar 1995.

[18] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85(6):1330–1333, Aug 2000.

[19] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91(5):057901, Aug 2003.

[20] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72(1):012326, Jul 2005.

[21] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94(23):230504, Jun 2005.

[22] Hoi-Kwong Lo and John Preskill. Security of quantum key distribution using weak coherent states with nonrandom phases. *Quant.Inf.Comput.*, 8:431, 2007.

[23] Toyohiro Tsurumaru and Kiyoshi Tamaki. Security proof for quantum-key-distribution systems with threshold detectors. *Phys. Rev. A*, 78(3):032302, Sep 2008.

[24] Normand J. Beaudry, Tobias Moroder, and Norbert Lütkenhaus. Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.*, 101(9):093601, Aug 2008.

[25] Øystein Marøy, Lars Lydersen, and Johannes Skaar. Security of quantum key distribution with arbitrary individual imperfections (v3), 2009.

[26] Vadim Makarov. Controlling passively quenched single photon detectors by bright light. *New J. Phys. 11 065003*, 2009.

[27] C. Gobby, Z. L. Yuan, and A. J. Shields. Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters*, 84:3762, 2004.

[28] Vadim Makarov. *Quantum cryptography and quantum cryptanalysis*. PhD thesis, Norwegian University of Science and Technology, 2007.

[29] Mikhail Ulianov. Quantum key distribution system. Master's thesis, St. Petersburg State Polytechnical University, 2009.

[30] J. G. Rarity P. D. Townsend and P. R. Tapster. Single photon interference in 10-km-long optical fibre interferometer. *Electron. Lett. 29, 634–635*, 1993.

[31] Vadim Makarov. Private conversation, 2010.

[32] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A*, 74(2):022313, Aug 2006.

[33] A. Lotito I. Rech S. Cova, M. Ghioni and F. Zappa. Evolution and prospects for single-photon avalanche diodes and quenching circuits. *Journal of Modern Optics, Volume 51, Issue 9 & 10, pages 1267 - 1288*, June 2004.

[34] Ben G. Streetman and Sanjay Banerjee. *Solid state electronic devices*, pages 212,425. Prentice Hall series in solid state physical electronics. Prentice Hall, 6 edition, 2006.

[35] Y. P. Varshni. Temperature dependence of the energy gap in semiconductors. *Physica*, 34(1):149 – 154, 1967.