Practical Test of a Quantum Key Distribution System

Teemu Manninen

School of Electrical Engineering

Thesis submitted for examination for the degree of Master of Science in Technology.

Espoo 13.3.2017

Thesis supervisor:

Prof. Ilkka Tittonen

Aalto University
School of Electrical
Engineering

AALTO UNIVERSITY
SCHOOL OF ELECTRICAL ENGINEERING

ABSTRACT OF THE
MASTER'S THESIS

Author: Teemu Manninen

Title: Practical Test of a Quantum Key Distribution System

Date: 13.3.2017 Language: English Number of pages: 8+57

Department of Electronics and Nanoengineering

Professorship: Electrophysics

Supervisor and advisor: Prof. Ilkka Tittonen

The development of quantum computers presents a threat to the security of modern communication systems; with Shor's algorithm, all currently used asymmetric cryptography schemes can be broken. Fortunately, secure communication is still possible in the post-quantum era using symmetric encryption algorithms, such as the Advanced Encryption Standard (AES) or the provably secure one-time pad (OTP). However, the main problem of symmetric cryptography, the key distribution, has to be solved.

Quantum key distribution (QKD) uses the fundamental properties of quantum mechanics to distribute encryption keys in a provably secure manner. In this thesis, the practical applicability of QKD is examined. This is achieved by testing the performance, stability, and usability of one of the few commercially available QKD platforms, ID Quantique's Clavis 2.

The tested system was stable for multiple months in normal operation and did not require any intervention from the user. The maximum distance with the test platform was 54 km. However, at these distances, the secret key rate was only tens of bits per second. For distances below 25 km, secret key rates in the kilobits per second range were achieved. Thus, if high data rates or communication distances close to 50 km are desired, ciphers less secure than OTP have to be used. Additionally, two flaws were discovered in the tested system, one making the system unstable, and the other preventing the key distribution process from starting. Fortunately, neither issue reduces the security of the system, and both could be fixed by modifying the software. Our results show that QKD can be considered as a mature technology that is ready for practical applications and even for commercial use.

Keywords: Quantum key distribution, QKD, Cryptography, Quantum information

AALTO-YLIOPISTO
SÄHKÖTEKNIIKAN KORKEAKOULU

DIPLOMITYÖN
TIIVISTELMÄ

Tekijä: Teemu Manninen

Työn nimi: Kvanttiavainjakelujärjestelmän käytännön testaus

Päivämäärä: 13.3.2017 Kieli: Englanti Sivumäärä: 8+57

Mikro- ja nanotekniikan laitos

Professuuri: Sähköfysiikka

Työn valvoja ja ohjaaja: Prof. Ilkka Tittonen

Kvanttitietokoneiden tuleva kehitys muodostaa uhan nykyaikaisten viestintäjärjestelmien ja tallennetun digitaalisen tiedon turvallisuudelle; kaikki nykyisin käytettävät epäsymmetriset salausjärjestelmät pystytään murtamaan Shorin algoritmilla. Turvallinen viestintä on kuitenkin edelleen mahdollista käyttämällä symmetrisiä salausalgoritmeja, joita ovat esimerkiksi Advanced Encryption Standard (AES) ja todistettavasti turvallinen one-time pad (OTP). Symmetrisen salauksen pääongelma, avaimien jakaminen, vaatii kuitenkin uuden teknisen ratkaisun.
Kvanttiavainjakelu (QKD) käyttää kvanttimekaniikan perusominaisuuksia salausavaimien todistettavasti turvalliseen jakamiseen. Tässä diplomityössä arvioidaan QKD:n käytännön soveltuvuutta sen nykyisessä tilassa. Tämä saavutetaan testaamalla kaupallisen QKD-alustan, ID Quantiquen Clavis^2:n, suorituskykyä, vakautta ja käytettävyyttä.
Tuloksien perusteella voidaan todeta, että QKD on toimiva teknologia ja valmis käytännön sovelluksiin. Testattu järjestelmä oli stabiili pitkiä aikoja normaalissa käytössä eikä vaatinut toimenpiteitä käyttäjältä. Vaikka pisin saavutettu etäisyys testatulla alustalla oli 54 km, oli avainnopeus näillä etäisyyksillä kymmeniä bittejä sekunnissa. Alle 25 km:n etäisyyksille saavutettiin kilobittien avainnopeuksia. Jos halutaan korkeita tiedonsiirtonopeuksia tai pitkiä viestintäetäisyyksiä, täytyy käyttää OTP:tä vähemmän turvallisia salausjärjestelmiä. Testatusta järjestelmästä löydettiin lisäksi kaksi vikaa, joista ensimmäinen teki järjestelmästä epävakaan ja toinen esti avainjakoprosessin aloittamisen. Kumpikaan ongelma ei kuitenkaan vähennä järjestelmän turvallisuutta, ja molemmat voidaan korjata tekemällä pieniä muutoksia systeemin ohjelmistoon.

Avainsanat: Kvanttiavainjakelu, QKD, Kryptografia, Kvantti-informaatio

Preface

Ei oo käyttist, toimii ku PNS.
– Iikka Elonsalo

First, I would like to thank Professor Tittonen for the opportunity to work in the Micro and Quantum Systems group and for the extensive feedback on this thesis. I would like to also thank Jari Lietzén for his help with measurements and for providing essential equipment for the experiments. Finally, thanks also to the LaTeX, Bash, and Linux wizard Iikka Elonsalo for his expertise and input on how nothing actually works.

Otaniemi, 13.3.2017

Teemu Manninen

Contents

Symbols and abbreviations

Symbols

$\hat{a}$	Annihilation operator
$\hat{a}^\dagger$	Creation operator
$\hat{A}, \hat{B}, \hat{O}$	Hermitian operators of observables A, B, and O
$A_{\omega,\omega'}$	SARG04 sifting pair
B	Bandwidth limit
f	Universal$_2$ hash function
H_{bin}	Binary entropy
I_{Bob}	Bob's information
I_{Eve}	Eve's information
I_1, I_2	Intensities at detectors 1 and 2
l	Fiber length
l_d	Delay line length
l_m	Authentication message length
l_t	Authentication tag length
N	Block size
N_d	Number of bits disclose during error correction
N_f	Final key size
N_s	Sifted key size
n	Number of photons; Number of bits
p	Probability of choosing the X basis
p_c	Probability of a conclusive measurement result
p_{dark}	Probability of a dark count in Bob's detector
p_{det}	Probability of detection
$p_n(\mu)$	Poissonian distribution
$\hat{P}_x$	Projection operator onto subspace orthogonal to $\|-z\rangle$
$\hat{P}_z$	Projection operator onto subspace orthogonal to $\|-x\rangle$
Q	Quantum bit error rate
Q_{det}	Quantum bit error rate caused by dark counts
Q_{opt}	Quantum bit error rate caused by optical misalignment
Q'	$\sqrt{Q(1-Q)}$
t	Transmittance; Authentication tag
t_c	Crash time
t_{ed}	Number of bits disclosed through eavesdropping
t_{ec}	Number of bits disclosed during error correction
$\hat{U}$	Unitary operator
r	Final key size
V	Visibility
$\hat{X}_1$, $\hat{X}_2$	Quadratures of coherent light
Y_s, Y_d	Signal and decoy state yields
β	Fiber attenuation per kilometer

$\delta_{n,m}$	Kronecker delta
η_d	Detection efficiency
μ	Mean photon number
ν	Duty cycle
$\hat{\rho}$	Density matrix
ϕ_A	Alice's phase shift
ϕ_B	Bob's phase shift
$\|n\rangle$	Fock state
$\|t\rangle$	Target state
$\|\pm x\rangle$	Basis vectors of the X basis
$\|\pm z\rangle$	Basis vectors of the Z basis
$\|\alpha\rangle$	Coherent state
$\|\varphi\rangle, \|\psi\rangle$	Arbitrary state vectors
$\|\uparrow\rangle, \|\downarrow\rangle$	Spin up and down states
$\|\updownarrow\rangle, \|\leftrightarrow\rangle$	Rectilinear polarization basis states
$\|\nearrow\rangle, \|\nwarrow\rangle$	Diagonal polarization basis states
$\oplus$	Bitwise exclusive or

Abbreviations

APD	Avalanche photo diode
COW	Coherent one way
DPS	Differential phase shift
FWHM	Full width at half maximum
LDPC	Low-density parity-check
OPT	One-time-pad
PNS	Photon number splitting
QBER	Quantum bit error rate
QKD	Quantum key distribution
WDM	Wavelength-division multiplexing

1 Introduction

Until recently, the applications of cryptography, the science of secure transmission of messages, has mostly been limited to military and state level applications. However, with the rise of the internet, cryptography has attained a significant role in the every day life of ordinary people securing, for example, private messaging, personal information, and online banking.

The general setting of cryptography, using the established place holder names, is the following; Alice and Bob wish to communicate securely with each other, and an eavesdropper, Eve, attempts to intercept this communication in order to obtain information or to manipulate the contents of their messages. To prevent Eve's intentions, Alice combines her message with a secret key through some mathematical manipulation, producing an encrypted message. After receiving the encrypted message, Bob decrypts it using his key and the appropriate mathematical manipulation. In an ideal case, Eve can only access the encrypted message and cannot obtain any information about the contents of the original message, since she does not possess the secret key.

Cryptography can be divided roughly into two subsets, which are called symmetric and asymmetric, based on the relation between Alice's and Bob's keys. In symmetric cryptography, the same key is used for both encrypting and decrypting the message. An example of a symmetric cryptography scheme is the one-time-pad (OTP), where each bit of the message is combined with the key using bitwise exclusive-or operation. This produces an absolutely secure encrypted message [1] as long as the length of the key is equal or greater than the length of the original message and each key is used only once. The security is guaranteed by the fact that any message can produce any encrypted message when combined with the appropriate key. Due to the aforementioned limitations of OTP, more practical, the so-called block ciphers, such as AES-256 [2], the current *de facto* symmetric encryption standard, are used. Although more than one message can be encrypted using the same key with these more complex ciphers, the frequent changing of the encryption key is still recommended to maximize security. The fundamental problem with symmetric cryptography is the distribution of keys; when there is no secure connection between Alice and Bob, there is no way for them to efficiently share secret keys using classical communication. In critical applications, this can be, and has been circumvented by using physical means, such as couriers, for distributing the keys. However, this is inefficient and cumbersome.

Until now, the problem of key distribution has been solved by using asymmetric cryptography. In asymmetric cryptography, Bob generates a pair of keys, a public and a private key. The public key can be distributed freely, while Bob keeps the private key to himself. When Alice wishes to send a message to Bob, she encrypts her message using Bob's public key, after which the message can only be decrypted using Bob's private key. The security of asymmetric cryptography clearly relies on the process by which the key pair is produced to be difficult to reverse; even if someone knows the public key, they can not produce the private key and decrypt the message. Usually this property is achieved by using large prime numbers and the factorization of their product, discrete logarithms, or the properties of elliptic curves. All of

these problems are computationally difficult to reverse using classical computers. However, encrypting and decrypting messages using asymmetric cryptography is also computationally intensive and not usually viable with modern data rates. Therefore, the so-called session keys are frequently used, where a secret key is distributed between the parties using asymmetric cryptography, and the actual data is encrypted using symmetric cryptography and the shared secret key.

Although asymmetric cryptography algorithms are secure against attacks using classical computers, quantum computers present a new threat to all of these schemes. Using Shor's algorithm, a quantum computer can break all current asymmetric cryptography algorithms in polynomial time [3]. However, it should be noted that a quantum computer with enough qubits to break any actual cryptography algorithm has not yet been built. To counter this threat, new post-quantum cryptography schemes that are immune to Shor's algorithm have been proposed. However, these new algorithms still rely on computational complexity to ensure their security and are, therefore, vulnerable to unexpected advances in computational science or mathematics [4].

Since symmetric encryption algorithms are immune to Shor's algorithm, another solution for secure communication in the post-quantum era is to move to purely symmetric cryptography. Although a proposed search algorithm for quantum computers, Grover's algorithm [5], can significantly speed up the cracking of block ciphers, this can be efficiently countered with the use of longer keys [4]. Nevertheless, when maximum security is required, OTP should be used as the encryption algorithm. However, as stated above, the use of symmetric cryptography requires an efficient method of distributing encryption keys between Alice and Bob. This problem can be solved with quantum key distribution (QKD), which uses the fundamental properties of quantum mechanics to offer an information theoretically secure way of distributing secret keys between two parties.

The main objective of this thesis is to assess the practical applicability of QKD at its current state. For the testing, one of the few commercially available QKD platforms, ID Quantique's Clavis^2, is used. In addition to security, the most significant criteria for any practical QKD system are performance, stability, and usability; the platform should be able to continuously and without user intervention provide secret keys at a rate that is sufficient for encryption using either AES or, more ideally, OTP.

The structure of this thesis is the following. In the first section, the fundamental properties of quantum mechanics are introduced on the level that is relevant to quantum key distribution and this thesis. Next, the basic idea and required steps of QKD are described, which is complemented with ways of realizing QKD in practice and the most relevant protocols in the following two sections. In the experimental part of the thesis, the testing methodology and the results are described and discussed. Lastly, the thesis is concluded with the most significant findings.

2 Some Aspects of Quantum Mechanics

This section is a brief introduction to the fundamental properties and notation of quantum mechanics on the level that is needed for understanding quantum key distribution in the scope of this thesis.

2.1 States, Superposition and Measurement

According to the postulates of quantum mechanics, a closed system, which can be a single particle or a collection of particles, can be represented as a state vector $|\psi\rangle$ in an N dimensional Hilbert space, and this state vector contains all the information that can be known about the system. Furthermore, every observable, i.e. measurable physical quantity, is represented by a Hermitian operator, and the only possible results of the measurement are the eigenvalues o_k of this operator:

$$\hat{O}\,|\phi_k\rangle = o_k\,|\phi_k\rangle\,. \tag{1}$$

Here $\hat{O}$ is a Hermitian operator of an observable O, $|\phi_k\rangle$ is its eigenstate, and o_k is an eigenvalue that corresponds to this eigenstate. Additionally, since the operator $\hat{O}$ is Hermitian, the eigenvalues $\{o_k\}_{k=1}^N$ are always real. Furthermore, the eigenstates $\{|\phi_k\rangle\}_{k=1}^N$ of a Hermitian operator form a complete orthonormal basis, i.e. their inner product follows

$$\langle\phi_k|\phi_l\rangle = \delta_{k,l}, \tag{2}$$

assuming that the state vectors $|\phi_k\rangle$ are normalized to unity:

$$\langle\phi_k|\phi_k\rangle = 1. \tag{3}$$

Thus, any state $|\psi\rangle$ can be represented as a superposition of the eigenstates of an observable:

$$|\psi\rangle = \sum_k |\phi_k\rangle\,\langle\phi_k|\psi\rangle = \sum_k c_k\,|\phi_k\rangle\,. \tag{4}$$

Here $c_k = \langle\phi_k|\psi\rangle$ are constants that project the state $|\psi\rangle$ onto the eigenstates $|\phi_k\rangle$. The squares of the absolute values of these constants, $|c_k|^2$, are the probabilities of a measurement of O yielding the result o_k.

After a measurement, that yields the result o_k, the system is left in the eigenstate $|\phi_k\rangle$. This is usually referred to as the collapse of the state. Thus, if the same observable is measured again, the result is the same value o_k. This follows directly from Equations (3) and (4). However, the eigenstate $|\phi_k\rangle$ can also be represented as a superposition of the eigenstates $\{|\alpha_i\rangle\}_{i=1}^N$ of some other observable A:

$$|\phi_k\rangle = \sum_i |\alpha_i\rangle\,\langle\alpha_i|\phi_k\rangle = \sum_i b_i\,|\alpha_i\rangle\,. \tag{5}$$

Thus, if A is measured after the first measurement of O, the state collapses again, this time into an eigenstate $|\alpha_i\rangle$ of the operator $\hat{A}$. This state is in turn a superposition of the eigenstates $\{|\phi_k\rangle\}_{k=1}^N$ of the observable O, and a new measurement of O can

yield any of the eigenvalues o_k as a result. In other words, the pure act of measuring A added uncertainty to the value of O.

This collapsing of states into an eigenstate of the observable being measured, described above, is the source for the Heisenberg uncertainty principle, which states in its most general form that the uncertainties ΔA and ΔB of observables A and B follow the equation

$$\Delta A \Delta B \geq \frac{1}{2}\langle[\hat{A}, \hat{B}]\rangle. \tag{6}$$

Here $[\hat{A}, \hat{B}]$ is the commutator of the operators $\hat{A}$ and $\hat{B}$:

$$[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}, \tag{7}$$

and $\langle[\hat{A}, \hat{B}]\rangle$ is the expectation value of the operator $[\hat{A}, \hat{B}]$, which for state $|\psi\rangle$, is

$$\langle[\hat{A}, \hat{B}]\rangle = \langle\psi|[\hat{A}, \hat{B}]|\psi\rangle\,. \tag{8}$$

It can also be seen from Equation (6) that if operators $\hat{A}$ and $\hat{B}$ commute, i.e. $[\hat{A}, \hat{B}] = 0$, the uncertainty of both observables A and B can be zero at the same time, or in other words, both quantities can be known accurately at the same time. This is due to the fact that if two operators commute, they have a complete set of common eigenstates. Therefore, if A is measured and the state of the system collapses into an eigenstate of $\hat{A}$, it is possible that this state is also an eigenstate of $\hat{B}$. Therefore, when B is measured, the state does not collapse further, since it already is an eigenstate of $\hat{B}$. This way, the value of both A and B can be known accurately by using successive measurements.

2.2 No Cloning

For cloning of a state to be possible in quantum mechanics, there should exist a unitary operator $\hat{U}$ that can copy any state to the target state $|t\rangle$. Therefore, when applied to states $|\psi\rangle$ and $|\varphi\rangle$, the result must be

$$\hat{U}\,|\psi\rangle\,|t\rangle = |\psi\rangle\,|\psi\rangle\,, \tag{9}$$

$$\hat{U}\,|\varphi\rangle\,|t\rangle = |\varphi\rangle\,|\varphi\rangle\,. \tag{10}$$

Since $\hat{U}$ is unitary, $\hat{U}^\dagger\hat{U} = \hat{\mathbb{1}}$, where $\hat{\mathbb{1}}$ is the identity operator. Taking the inner product of the states after cloning, equations (9) and (10) imply that

$$\langle\varphi|\,\langle\varphi|\psi\rangle\,|\psi\rangle = \langle\varphi|\,\langle t|\,\hat{U}^\dagger\hat{U}\,|\psi\rangle\,|t\rangle \tag{11}$$

$$\left(\langle\varphi|\psi\rangle\right)^2 = \langle\varphi|\,\langle t|\;\;|\psi\rangle\,|t\rangle \tag{12}$$

$$\left(\langle\varphi|\psi\rangle\right)^2 = \langle\varphi|\psi\rangle\,\langle t|t\rangle \tag{13}$$

$$\left(\langle\varphi|\psi\rangle\right)^2 = \langle\varphi|\psi\rangle\,. \tag{14}$$

This is only possible if $\langle\varphi|\psi\rangle = 0$ or $\langle\varphi|\psi\rangle = 1$. Thus, cloning is possible only if $|\psi\rangle$ and $|\varphi\rangle$ are the same state or orthogonal states, and cloning of any arbitrary state is not possible.

3 Fundamentals of Quantum Key Distribution

This section introduces the basic steps of quantum key distribution. First, the BB84 protocol is presented to describe the general idea behind QKD and show how quantum mechanics ensures its security. In the following sections, the required classical data processing steps, error correction, privacy amplification, and authentication, are introduced. Lastly, different attack strategies against the BB84 protocol and their effects are discussed.

As is customary in cryptography, place holder names are used in the following sections in the following fashion; Alice and Bob are trying to communicate securely with each other, while Eve is trying to eavesdrop on their communication. Additionally, Alice and Bob have two communication channels, one channel for transmitting photons, which is usually referred to as the quantum channel, and one for classical communications, called classical channel. The quantum channel is usually implemented using either an optical fiber or a free space link, while any means of classical communication can be used for the classical channel. Furthermore, it is assumed that Eve can freely eavesdrop on all communication in both channels as long as she follows the laws of physics.

3.1 Steps

This section introduces the steps that Alice and Bob have to take in order to obtain a shared sequence of secret bits using quantum key distribution. These steps and their order are presented in Figure 1. BB84 is used as an example of a QKD protocol due to its historical importance and simplicity.

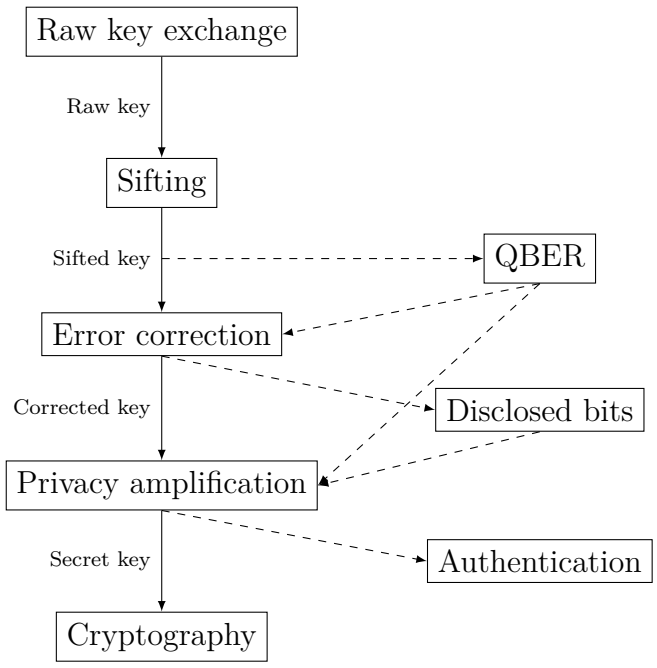


Figure 1: Steps of quantum key distribution.

3.1.1 Raw Key Exchange Using BB84

Originally introduced by Bennett and Brassard in 1984 [6], BB84 is the oldest quantum key distribution protocol, and it was first experimentally demonstrated by Bennett and Bessette et al. in 1992 [7]. The protocol uses two complementary bases in a two-dimensional Hilbert space to ensure secure key distribution [6]. If the orthonormal basis vectors of the first basis, called X basis, are $|-x\rangle$ and $|+x\rangle$, the basis vectors of the second basis, called Z basis, are

$$|\pm z\rangle = \frac{1}{\sqrt{2}} \left(|+x\rangle \pm |-x\rangle \right). \tag{15}$$

Naturally, the same applies vice versa

$$|\pm x\rangle = \frac{1}{\sqrt{2}} \left(|+z\rangle \pm |-z\rangle \right). \tag{16}$$

These relations are visualized in Figure 2. Additionally, for practical implementation to be possible, there must exist a measurement for both bases that can unambiguously discriminate between the two basis states.

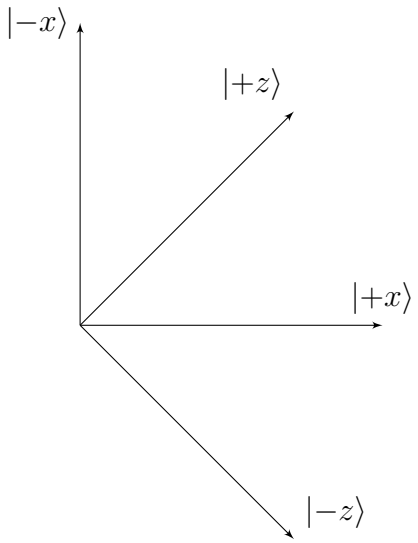


Figure 2: Visualization of the BB84 basis vectors.

Alice starts the protocol by preparing n photons and measuring an observable of each photon. Alice and Bob have agreed before hand what observable they use for their measurements. For each measurement, she chooses randomly either the X or Z basis, and both bases must have equal probability of being chosen. If the measurement result is $-x$ or $-z$, Alice assigns the photon a classical bit value 0, and if the result is $+x$ or $+z$, the bit value is 1. After each measurement, Alice sends the photon to Bob, who also measures the observable in a random basis and assigns each photon a bit value using the same rules as Alice. This phase is usually referred to as

the raw key exchange, and the obtained key is the raw key. In cases where Bob's random basis choice is the same as Alice's, their measurement results, and therefore their bit values, must match. This is guaranteed by the laws of quantum mechanics. However, when Bob measures the observable in different basis from Alice, there is only a 50 % chance that they obtain the same bit value, because the basis vectors of the basis X are equal superposition states in the basis Z and vice versa. Therefore, after Bob has received and measured all photons, Alice and Bob compare publicly their basis choices using the classical channel and discard any results where they used different bases for their measurements, because in these cases there is no correlation between their bit values. [6] This is usually referred to as the sifting phase, and the key that is obtained after this step is the sifted key. In the absence of eavesdropping or any other error sources, Alice and Bob have now a shared sequence of bits that they can use as an encryption key. An example of this process is presented in Table 1 for 8 photons.

Table 1: An example of the key distribution using the BB84 protocol.

Alice's state	$\|+x\rangle$	$\|-z\rangle$	$\|+x\rangle$	$\|-x\rangle$	$\|+x\rangle$	$\|-z\rangle$	$\|-z\rangle$	$\|-z\rangle$
Alice's bit	1	0	1	0	1	0	0	0
Bob's state	$\|+x\rangle$	$\|+x\rangle$	$\|-z\rangle$	$\|-x\rangle$	$\|+x\rangle$	$\|+x\rangle$	$\|-x\rangle$	$\|-z\rangle$
Bob's bit	1	1	0	0	1	1	0	0
Compatibility	✓	×	×	✓	✓	×	×	✓
Sifted key	1			0	1			0

3.1.2 Eavesdropping

The security of the BB84 protocol relies on the fact that Eve does not know the bases that Alice used while detecting her photons, and the only thing Eve can do is just to make a guess. If her guess is incorrect, and she measures the observable in different basis from Alice, she obtains the correct bit value with a 50 % probability. Additionally, she alters the state of the photon, because her measurement causes the state to collapse to the eigenstate corresponding to her measurement result. On the other hand, if her measurement destroys the photon, the best Eve can do is to prepare a new photon in the same state as the one she measured and send the new photon to Bob. This most basic type of attack is usually referred to as intercept-resend. Now, due to the eavesdropping, the photon is in an eigenstate of the complementary basis of the basis chosen by Alice. Thus, there is a 50 % probability that Bob's bit value is different from Alice's, when their basis choices match, as visualized in Figure 3. Here, only the case where Alice's and Bob's basis choices match is considered, because otherwise the bit value is discarded in the sifting phase. On the other hand, if Eve's guess about the measurement basis is correct, she obtains the correct bit value without altering the state of the photon. [6] It should be noted that after her measurement, Eve can not know whether her basis choice was correct or not. This she can determine only in the sifting phase, when Alice and

Bob compare their basis choices publicly.

Overall, there is a 75 % probability that Eve can obtain a single bit value without it being detected by Alice and Bob. However, when using n bits, the probability of Alice and Bob detecting the eavesdropping is $1 - \left(\frac{3}{4}\right)^n$, if Eve eavesdrops on every photon.

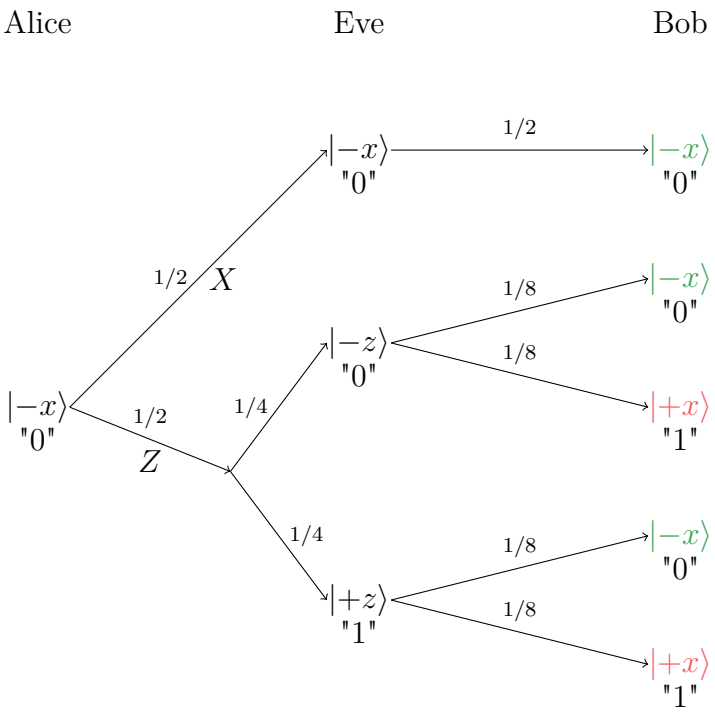


Figure 3: An example of eavesdropping in BB84. In cases mark with red, eavesdropping causes an error and can be detected.

To detect the errors caused by Eve's eavesdropping, Alice and Bob have to compare some fraction of their sifted keys. Because there is no encrypted connection yet, this comparison has to be done publicly using the classical channel. Therefore, the bits used for the comparison must be discarded to minimize Eve's information about the key. If the percentage of bits with errors, i.e. the quantum bit error rate (QBER), is below a certain threshold, which is discussed in detail in Section 3.2, Alice and Bob can be sure that the amount of information Eve has about the bit sequence is low enough that they can continue with the protocol. Otherwise, the bit sequence has to be discarded and the key distribution started again from the beginning. [6]

3.1.3 Error Correction

Regardless of the exact protocols used for QKD, there are bound to be errors in the sifted key shared between Alice and Bob. These errors can be caused by eavesdropping or physical error sources. Therefore, some error correction scheme has to be used

in order to guarantee that Alice's and Bob's keys are identical and can be used for encryption.

Because there is no secure connection between Alice and Bob, the error correction has to be done publicly in the classical channel, and Eve can use this communication to obtain additional information about the key. Therefore, the error correction used has to be as efficient as possible, i.e. the amount of information Alice must send to Bob per bit should be as close as possible to the so-called Shannon limit. This limit is given by $H_{bin}(Q)$, where Q is the QBER and H_{bin} is the binary entropy:

$$H_{bin}(Q) = -Q\log_2(Q) - (1-Q)\log_2(1-Q). \tag{17}$$

Because of this, an error correction algorithm, called Cascade, was developed to be used with QKD.

In Cascade, Alice and Bob first agree on a permutation that they apply on their sifted keys. Next, the key is divided into blocks, where the block size is chosen by Alice and Bob, and the optimal size depends of the QBER. Alice computes the bit parity of each block and sends the parities to Bob. Bob checks whether the parities of his blocks match the ones sent by Alice, and for each block with parity mismatch Alice and Bob perform an interactive binary search to find and correct the error. [8]

In interactive binary search, the block is split into two halves. Alice computes the parity of the first half, and and Bob checks if the parity of his corresponding half matches. If the parity does not match, the error is in the first half. Otherwise, the error is in the second half. This splitting and parity checking is repeated until the error is found and corrected. [8]

After the first pass, Alice and Bob have the same parity for each block, and therefore each block has an even number of, or zero, errors. Now, they reverse their previous permutation, apply a new one, double the blocks size, and repeat the parity check and interactive binary search for the new blocks. This process is repeated over multiple passes. Additionally, when an error is corrected during a pass, this changes the parity of the blocks that the corrected bit was part of in the previous passes. Alice and Bob can use this to correct errors in these blocks using interactive binary search, which again changes parities of other blocks in other passes. This iterative process is repeated until the parities of all of the blocks in all of the passes match. [8]

If the parity of a block matches between Alice and Bob, the amount of disclosed bits is 1. However, if the parity does not match and binary search has to be used, a block of size N has to be split into halves $\log_2(N)$ times before the error is found, and each time the parity of one half in disclosed. Therefore, the amount of disclosed bits is $\log_2(N) + 1$ for blocks with parity mismatch.

While Cascade is easy to implement and rather efficient, it is highly interactive, i.e. it requires large amounts of messages between Alice and Bob. This can reduce the secret key rate of the system significantly when the latency of the classical channel is high. This interactivity can be reduced to a single message by using low-density parity-check (LDPC) codes. Furthermore, these codes can even be made more efficient than Cascade [9]. However, different LDPC codes have to be used for different QBER values.

3.1.4 Privacy Amplification

As was described in the previous sections, Eve can obtain some information about the secret bit sequence by eavesdropping on the quantum channel during the key distribution phase or by listening to the classical channel during the error correction phase. Therefore, after they have corrected any discrepancies in their sequences, Alice and Bob have to use some scheme to minimize Eve's information about the key. This step is usually referred to as privacy amplification.

Eve's information about the key in bits, t, consists of the bits she obtained by eavesdropping on the quantum channel t_{ed} and the bits Alice and Bob disclosed during error correction t_{ec}. The former can be estimated from the QBER, while the latter can be calculated during the error correction phase as described in the previous section.

If Alice and Bob knew of which physical bits of the key Eve has full information about, they could simply discard these bits from the secret key, and the final key length would be $n-t$. However, because Eve's eavesdropping on the quantum channel produces an error with probability 1/4, Alice and Bob can identify only a fraction of the bits that were leaked. Furthermore, the information that Eve can obtain by listening to the public channel during error correction is spread over multiple bits as parity information. Therefore, Alice and Bob must use universal$_2$ hash functions in order to generate a shorter key and minimize Eve's information. If Alice and Bob discard $s < n-t$ additional bits and use a random function from a class of universal$_2$ hash functions, which map the length n bit sequence into a length $r = n - t - s$ bit sequence, Eve's expected information about the new shorter key is [10]

$$I_{Eve} \leq \frac{2^{-s}}{\ln 2}. \tag{18}$$

This process is visualized in Figure 4.

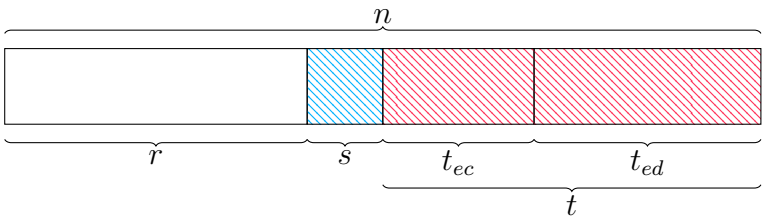


Figure 4: Key usage in privacy amplification.

3.1.5 Authentication

After all of the aforementioned steps, Alice and Bob finally share an identical key, and Eve's information about this key has been minimized. The final step is to authenticate that the parties that have shared the key are actually Alice and Bob. Without any authentication, Eve could impersonate Bob to Alice and vice versa, sharing one secret key with Alice and another one with Bob, as depicted in Figure 5.

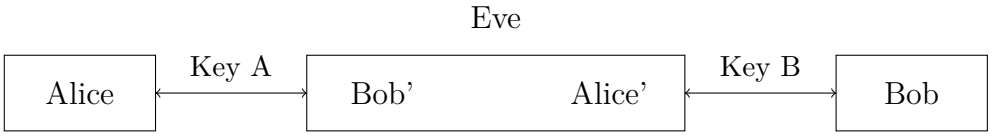


Figure 5: Visualization of the man-in-the-middle attack.

In this scheme, usually called man-in-the-middle attack, Eve can access, and even modify, all of the information that is exchanged between Alice and Bob while they are under the impression that their communication is secured.

To authenticate their key exchange, Alice creates a message m of length l_m and a so-called authentication tag t of length l_t and sends them to Bob. The generation of this tag requires Alice and Bob to share a sequence of secret bits. The first part of the secret is used to specify a function f in a class of universal$_2$ functions that maps the message m from length l_m to length l_t, and the result is combined with the remaining part of the secret, b, using bitwise exclusive or: [11]

$$t = f(m) \oplus b \tag{19}$$

To authenticate that the message was sent by Alice, Bob needs to conduct the same process on the message m received from Alice and verify that the result is the same as the tag t sent by Alice, as visualized in Figure 6. Additionally, Bob has to create a new message and authentication tag and send them to Alice in order to let her authenticate their key exchange.

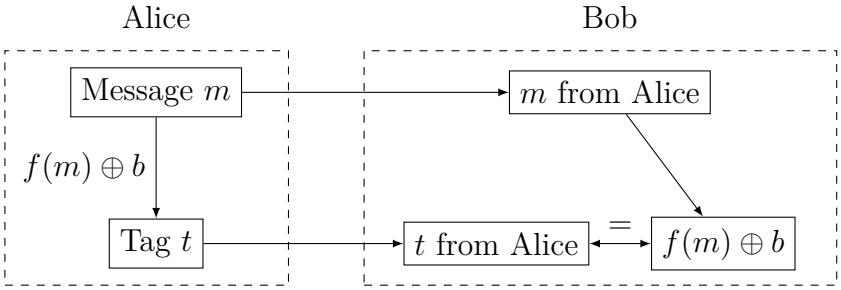


Figure 6: The authentication process.

If Alice and Bob have already shared secret keys during previous rounds of QKD, parts of these keys can be used as the secret needed for authentication. However, after the first key exchange, Alice and Bob have no shared secret keys to use for the authentication of their communication. Therefore, they must share an initial secret even before the key exchange begins. Furthermore, Eve could conduct the man-in-the-middle attack during the key exchange phase and forward the authentication messages between Alice and Bob during the authentication phase. To counter this, Alice and Bob have to use some data from their communication during the key distribution in the authentication message in order to ensure that the secret key is actually shared between them.

3.2 Attacks

As was discussed in Section 3.1.2, the security of QKD relies on the fact that any eavesdropping can be detected as errors in the bit sequence shared between Alice and Bob, and these errors can be quantified using the quantum bit error rate. Furthermore, efficient use of privacy amplification requires that Alice and Bob can reliably estimate the amount of information Eve has obtained about the sifted key. In order to estimate the maximum amount of information Eve can obtain while causing a certain QBER value, different eavesdropping strategies have to be analyzed.

In so-called individual attacks, Eve can only measure the state of each photon Alice sends to Bob independently, and this measurement has to be done before the classical data processing steps, i.e. error correction and privacy amplification. An example of such an attack is the aforementioned intercept-resend. [12] The maximum amount of information Eve can obtain per bit by using this type of attack is [13]

$$I_{Eve} = 1 - H_{bin}\left(\frac{1}{2} + Q'\right). \tag{20}$$

Here, $H_{bin}(Q)$ is the binary entropy, defined in Equation (17), and $Q' = \sqrt{Q(1-Q)}$, where Q is the QBER. This can be expressed in the form

$$I_{Eve} = \frac{1}{\ln 4}\left[4Q' \tanh^{-1}(2Q') + \ln\left(1 - 4Q'^2\right)\right], \tag{21}$$

and for a small QBER this simplifies to

$$I_{Eve} \approx \frac{2}{\ln 2} Q \approx 2.89Q. \tag{22}$$

Therefore, the amount of bits Eve has obtained by eavesdropping, t_{ed}, when Alice has sent n photons, is approximately

$$t_{ed} = I_{Eve} n \approx 2.89Qn. \tag{23}$$

On the other hand, Bob's information per bit is given by

$$I_{Bob} = 1 - H_{bin}(Q). \tag{24}$$

These two curves are depicted in Figure 7. In order to correct the errors in Bob's key using an ideal error correction algorithm, $1 - I_{Bob} = H_{bin}(Q)$ bits of information has to be disclosed per bit, as discussed in Section 3.1.3. This is the area above the I_{Bob} curve in the figure. Additionally, Eve has obtained I_{Eve} bits of information about the raw key per bit. Therefore, the maximum fraction of the raw key that Alice and Bob can use for the secret key is $I_{Bob} - I_{Eve}$, i.e. the area between the two curves. Thus, the generation of a secret key becomes impossible after the point at which these two curves cross, i.e. $Q \approx 0.147$.

With collective attacks, Eve is still restricted to measuring each photon independently. However, now she is allowed to measure her probes that have interacted with the photons after the classical data processing steps. This way she can use any

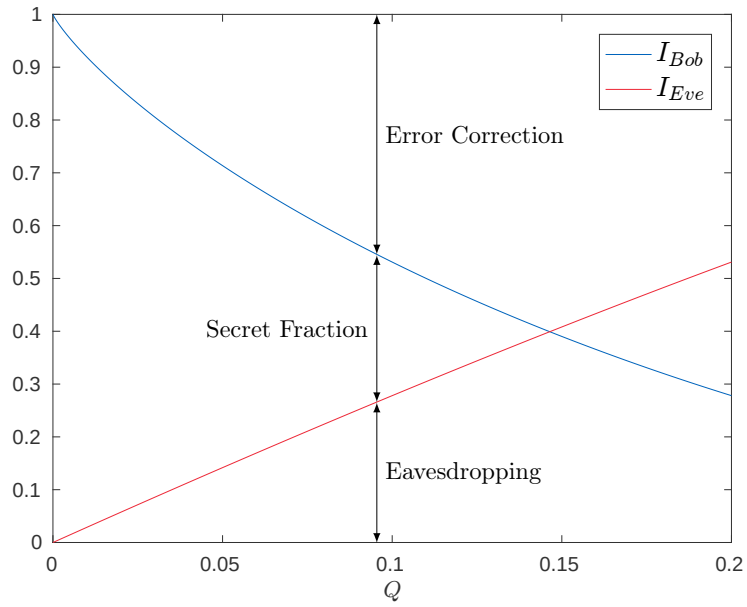


Figure 7: Information of Bob and Eve as functions of the QBER for an individual attack.

information she may obtain from, for example, the messages encrypted with the key to choose the best possible measurement. [12]

The most general class of attacks Eve can use are called coherent attacks, where in addition to the methods stated above, she is also allowed to use coherent measurements of multiple photons. This may give an advantage to Eve, because when the key is shortened during the privacy amplification phase, the final key is actually determined by the relations between different bits. [12] If Eve's arsenal of attacks is extended to include coherent attacks, it can be shown that Eve's maximum information per bit is given by [12, 14]

$$I_{Eve} = H_{bin}(Q). \tag{25}$$

Therefore, the generation of a secure key is possible when Bob's information is larger than Eve's

$$1 - H_{bin}(Q) > H_{bin}(Q). \tag{26}$$

This gives the bound $Q \lesssim 0.11$ for the unconditional security of BB84.

4 Practical Implementation

In the previous section, quantum key distribution was introduced in the ideal case. However, when QKD is implemented in practical scenarios, non-ideal components have to be used, and the properties of these components must be taken into account. In this section, we discuss the effects of these factors on the performance and security of practical QKD systems.

4.1 Single Photon Sources

The ideal implementation of BB84 requires Alice to be able to prepare and measure states that consist of single photons. A practical single photon source should have a low probability of emitting pulses with more than one photon and high efficiency, i.e. triggering should lead to photon emission with a high probability. Furthermore, the spectral width of the emitted photons should be narrow and the wavelength should be either in the O-band (1310 nm) or more preferably in the C-band (1550 nm) to ensure low losses with modern telecommunication optical fibers. Lastly, all of these requirements should be fulfilled close to room temperature in order for the source to be usable in practical QKD systems.

Although single photon sources have been implemented using quantum dots [15], diamond color centers [16], and single atoms [17], none of these techniques have fulfilled all of the aforementioned requirements. Because of these difficulties, highly attenuated lasers are the most common photon sources used for practical QKD. A pulse of light emitted by a laser is best described by a coherent state

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,. \tag{27}$$

Here $\alpha = \sqrt{\mu} e^{i\theta}$, where μ is the mean photon number of a pulse and θ defines the phase. Furthermore, $|n\rangle$ is a Fock state, also referred to as number state, which contains n photons. Since with QKD there is no reference phase for the laser outside of Alice's device, the state is actually a mixed state with a random phase, represented by a density matrix $\hat{\rho}$

$$\hat{\rho} = \frac{1}{2\pi} \int_0^{2\pi} |\alpha\rangle \langle\alpha| \, d\theta. \tag{28}$$

In other words, with mean photon number $\mu = |\alpha|^2$, the probability $p_n(\mu)$ of a pulse containing n photons is given by the Poissonian distribution

$$p_n(\mu) = e^{-\mu} \frac{\mu^n}{n!}. \tag{29}$$

This distribution is presented in Figure 8 for mean photon numbers $\mu = 0.1, 0.5, 1$. To best mimic pure single photon pulses and minimize the probability of a pulse containing multiple photons, coherent states must be attenuated so that $\mu \ll 1$. This has the significant drawback that most pulses actually contain zero photons and are not usable for key distribution, which significantly reduces the secret key rate.

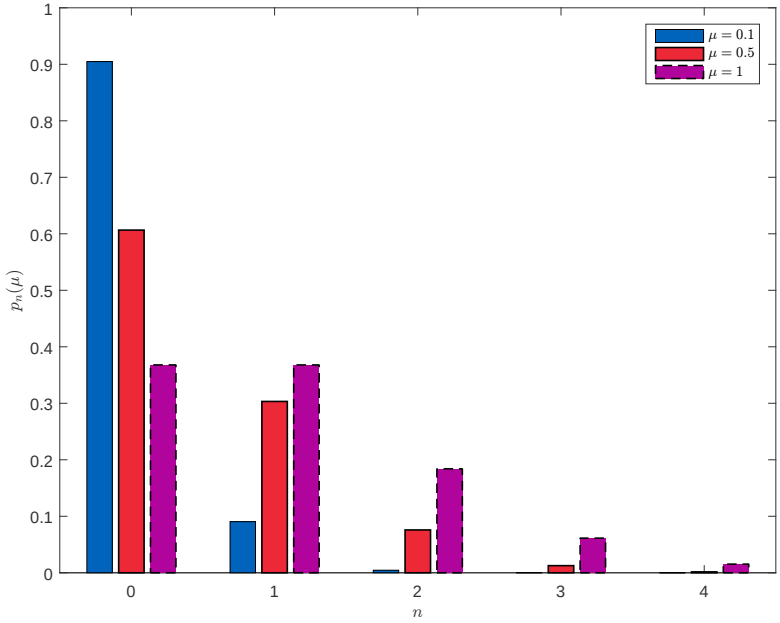


Figure 8: Probabilities of a coherent pulse containing n photons for three different mean photon numbers.

4.2 Single Photon Detectors

The most important figures of merit of a single photon detector in QKD are the quantum efficiency, the probability that when a photon hits the detector, the detector is triggered, the dark count rate, the amount of false detections per unit time, dead time, the minimum amount of time between two detections [12], and jitter, the time between the absorption of a photon and a detection signal [13]. Additionally, like a the single photon source, the detector should operate near to room temperature to be usable in practical QKD systems.

Avalanche photo diodes (APDs) are the most practical option for single photon detection in QKD. Usually, APDs are operated in the so-called Geiger mode, where a voltage exceeding the breakdown voltage is applied to the diode. In this regime, absorption of a photon causes an avalanche of charge carriers, which can be detected as a macroscopic current. To make the detection of a new photon possible, the voltage must be reduced below breakdown in order to stop the avalanche effect. This can be achieved with a passive- or active-quenching circuit, where the avalanche itself causes the quenching process, or by using the APD in gated mode, where the voltage is applied only in certain time windows. [18] Gated mode is typically used with QKD, when timing information of the incident light pulses is available to Bob. In order to maximize the possible key rate when using APDs in gated mode, it is desirable to have as many gates per unit time as possible. However, because the charge carriers decay exponentially with time when the voltage is reduced below breakdown, reducing the dead time between gates causes so-called afterpulses, false detections due to avalanches in previous gates. [13] This fundamentally limits the

maximum raw key rate that can be achieved with QKD when using APDs.

When detecting photons at wavelengths below 1100 nm, Si APDs can be used. Such detectors are commercially available and feature quantum efficiencies up to 70 % at 700 nm with maximum count rates of 50 MHz and dark count rates of 50 Hz while operating at −20 °C. However, because of the large band gap of Si, it can not be used to detect lower energy photons at 1310 nm and 1550 nm typically used with optical fibers. For the first of the aforementioned wavelengths, germanium APDs can be used, although InGaAs/InP APDs have replaced germanium, because these can be used at both wavelengths. [13] However, the quantum efficiencies of these types of APDs are much lower than that of the Si counterparts, around 10 % in −50 °C [12], and due to significant afterpulsing, InGaAs/InP APDs can not be used with passive quenching [13]. At telecom wavelengths, passive quenching and quantum efficiency up to 56 % can be achieved using parametric frequency up conversion and Si APDs [19]. On the other hand, this solution has high dark count rates [19, 20].

4.3 Coding

When the BB84 protocol was introduced in Section 3.1.1, the states of the photons used for transmitting the bit sequence from Alice to Bob were denoted by $|\pm x\rangle$ and $|\pm z\rangle$ with the only limitation being that there must exist a measurement that can unambiguously discriminate between the basis states of each basis, and the states must follow Equations (15) and (16). The most intuitive example of such states is the polarization of a single photon; the polarization can be measured in one of two complementary bases, rectilinear $\{|\updownarrow\rangle, |\leftrightarrow\rangle\}$ or diagonal $\{|\nearrow\rangle, |\nwarrow\rangle\}$ [13]. Alice can have four sources of linearly polarized light, each rotated by 45° relative to the previous one, Bob can separate the two orthogonal polarization states using a polarization beam splitter, and the basis choice is simply done by rotating the beam splitter. However, polarization encoding is difficult to implement in optical fibers due to birefringence; telecommunication fibers do not conserve the polarization of photons.

When using optical fibers, a more practical option than polarization coding is to code the bit value into the phase difference of two consecutive pulses of light. The simplest possible QKD phase coding system is visualized in Figure 9. Here, Alice splits the light pulse into two branches and applies a phase shift ϕ_A to one of them from one of the two bases, $\{0, \pi\}$ or $\{\pi/2, 3\pi/2\}$. The basis states are, therefore,

$$|-x\rangle = \left|\sqrt{\mu/2}\right\rangle \left|\sqrt{\mu/2}\right\rangle, \tag{30}$$

$$|+x\rangle = \left|\sqrt{\mu/2}e^{i\pi}\right\rangle \left|\sqrt{\mu/2}\right\rangle, \tag{31}$$

$$|-z\rangle = \left|\sqrt{\mu/2}e^{i\pi/2}\right\rangle \left|\sqrt{\mu/2}\right\rangle, \tag{32}$$

$$|+z\rangle = \left|\sqrt{\mu/2}e^{i3\pi/2}\right\rangle \left|\sqrt{\mu/2}\right\rangle. \tag{33}$$

According to the previously introduced notation, the states with a negative sign represent the bit value 0 and states with a positive sign represent the bit value 1.

After receiving the pulses, Bob applies a phase shift ϕ_B of either 0 or $\pi/2$ to the other branch. This serves as his basis choice. Finally, Bob combines the branches using either a beam splitter or a coupler. If Alice and Bob applied the same phase shift, $\phi_A - \phi_B = 0$, a constructive interference takes place in one of the branches of the coupler and a destructive interference in the other branch, and a photon is detected at detector D_1 corresponding to the bit value 0. On the other hand, if they applied the opposite phase shifts from the same basis, $\phi_A - \phi_B = \pi$, a photon is detected at D_2 corresponding to the bit value 1. Thus, the detector at which a photon was detected corresponds to the bit value encoded by Alice. On the other hand, if they applied their phase shifts from different bases, i.e. their basis choices were incompatible, the photon is detected randomly in one of the detectors, and these results are discarded in the sifting phase, when Alice and Bob compare their basis choices, as discussed in Section 3.1.1. [13]

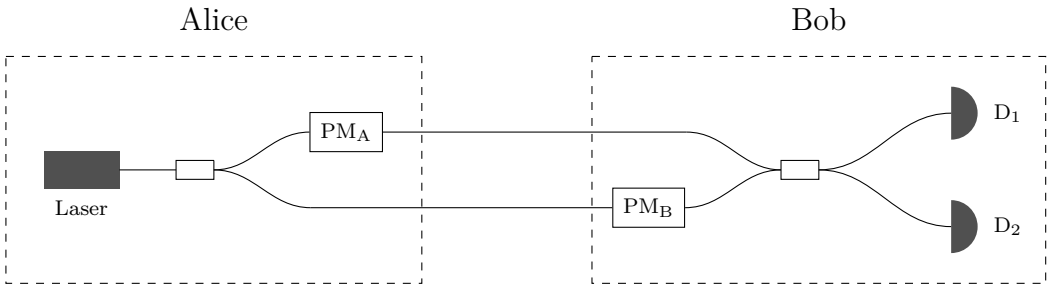


Figure 9: Simple phase coding QKD system.

The implementation of phase coding described above functions well when the distance between Alice and Bob is short. However, there must exist two optical paths, and the length difference between these paths has to be extremely stable in order to maintain the interference at Bob's end. Since the distance is usually tens of kilometers, this can be considered practically impossible. This problem can be circumvented by using one path between Alice and Bob and unbalanced Mach-Zehnder interferometers at both ends, as depicted in Figure 10. In this implementation, the pulse can arrive to Bob at three different times depending on the path it takes; the first times slot corresponds to the photon taking the short path at both ends, the last slot corresponds to the long paths, and the middle slot corresponds to the short and the long path or vice versa. Alice and Bob apply phase shifts according to the rules described above, and these phase shifts determine whether the interference in the center time slot is destructive or constructive. Although this implementation removes the need for stability between two paths, the problem still exists in Alice's and Bob's interferometers, and the length difference between the two arms must be adjusted during long key exchange sessions to compensate for any drift. Furthermore, the two possible paths corresponding to the middle time slot, short-long and long-short, must be indistinguishable for interference to take place. Therefore, polarization effects in the two paths of the interferometers must be identical. [13]

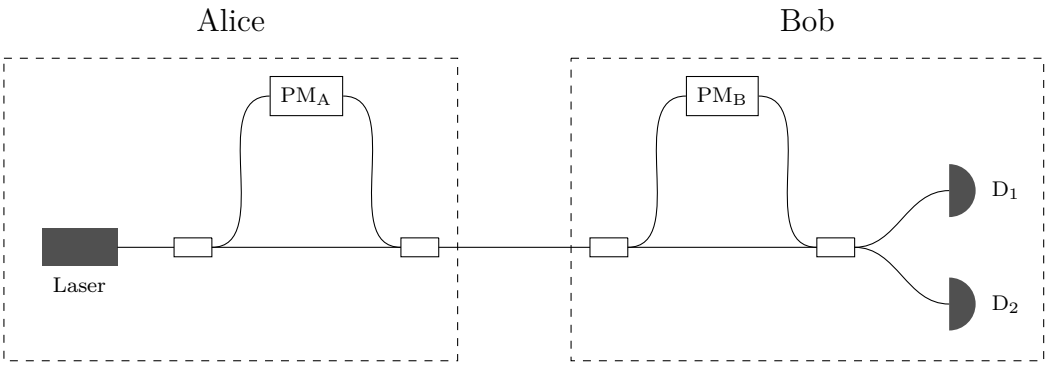


Figure 10: Phase coding using two Mach-Zehnder interferometers.

4.4 Plug & Play Implementation

The drawbacks related to using Mach-Zehnder interferometer implementation for phase coding can be circumvented by using the so-called Plug & Play implementation, which is depicted in Figure 11. Unlike with the previous implementations, now Bob starts the protocol by emitting a macroscopic coherent pulse from his laser. This pulse is split in the coupler C_1 into two pulses, one going to the long and one to the short arm. In these arms, the polarization of the pulses evolves in such a way that the pulse in the short arm goes through the polarization beam splitter (PBS) into the fiber connecting Alice and Bob, while the pulse in the long arm is reflected and goes also into the same fiber. Therefore, both pulses are in the fiber propagating towards Alice with some time difference caused by the length difference between the two arms. Additionally, the polarizations of the two pulses are orthogonal. [21]

Both pulses are split again into two parts in the coupler C_2. The fractions of the pulses that propagate to the detector D_A are used for the synchronisation of Alice with Bob and to detect a possible Trojan horse attack, which is described in Section 4.10.2. After propagating through the delay line (DL), the remaining fraction of the pulses is reflected back from a Faraday mirror (FM), which changes the polarization states of both pulses to orthogonal ones. After the reflection, Alice's phase modulator (PM_A) applies a phase shift to the second pulse encoding the bit value using the aforementioned rules. Before the pulses propagate out of Alice's device, they are attenuated to mean photon number that is much less than one. [21]

Due to the possible birefringence of the optical fiber connecting Alice and Bob, the polarizations of both pulses change as they propagate from Bob to Alice. However, because the Faraday mirror changes the polarization states to orthogonal states, exactly the opposite transformation is applied to the polarizations on the way back. Therefore, the polarization of each returning pulse is orthogonal to the polarization of the corresponding original pulse that Bob emitted to the fiber. Hence, the system compensates for any birefringence effects in the fiber automatically, as long as there are no significant changes in the birefringence of the fiber during the time that the pulses travel from Bob to Alice and back.

After propagating back to Bob, the pulses take opposite paths from before at the

polarization beam splitter due to the orthogonal polarization states. This is how the Plug & Play system circumvents the need for compensation between the two arms. If a pulse goes through the long (short) path when propagating from Bob to Alice, it must take the short (long) path on the way back. [21] However, the path difference must remain constant during the time the pulse propagates from Bob to Alice and back.

After Bob has applied a phase shift, i.e. his basis choice, to the pulse in the long arm, the pulses arrive to the coupler C_1 at the same time. Finally, the pulses interfere and a photon is detected either in detector D_{B1} or D_{B2} depending on Alice's and Bob's phase shifts. [21]

Because in the Plug & Play system Bob sends macroscopic pulses to Alice, unlike in other implementations, where Alice has the photon source, backscattering from these pulses can cause significant amounts of errors. To prevent this, Bob sends a "train" of pulses to Alice, and a delay line (DL) is added to her device. The length of this delay line is such that the whole pulse train can be stored in it. By knowing the distance between him and Alice, Bob can emit the pulse train, ignore any detection that occur during the time the pulses propagate to Alice, and detect the pulses once they propagate back. [21]

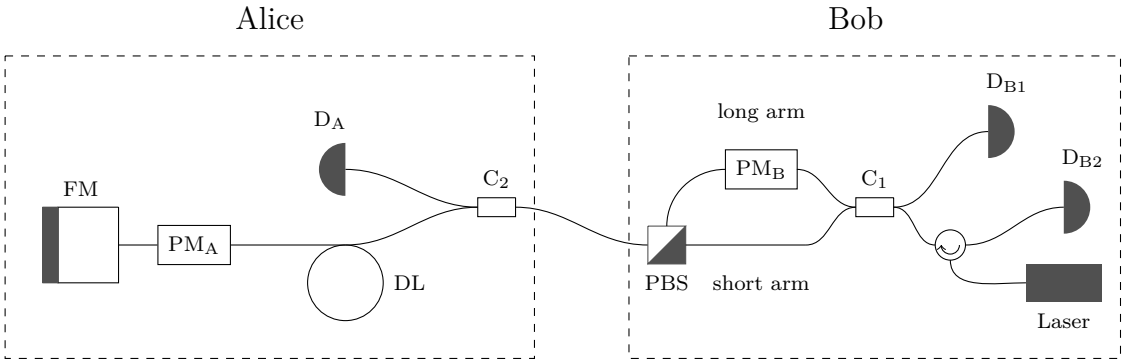


Figure 11: Phase coding using the Plug & Play scheme.

4.5 Error Sources

As was discussed in Section 4.2, the dark counts and afterpulses of the single photon detectors cause false photon detections and, therefore, increase the QBER of a QKD system even without eavesdropping. When using two detectors and the BB84 protocol, the QBER caused by the dark counts, Q_{det}, is

$$Q_{det} = \frac{p_{dark}}{t\eta_d\mu}. \tag{34}$$

Where p_{dark} is the probability of a dark count per gate, t is the transmittance of the quantum channel, η_d is the probability of detection of the detectors, and μ is the mean photon number of a pulse. [13] For example, with typical values $p_{dark} = 10^{-5}$ and $t = \eta_d = \mu = 0.1$, the QBER due to the dark counts is 1 %.

In addition to Q_{det}, the second most important term in the total QBER of fiber based QKD implementations is the error rate caused by the optical system,

$$Q_{opt} = \frac{1 - V}{2}. \tag{35}$$

Here, V is the visibility of the optical system, which measures the distinguishability of two orthogonal states. [13] For phase coding, this is simply the fringe visibility,

$$V = \frac{I_1 - I_2}{I_1 + I_2}, \tag{36}$$

where I_1 and I_2 are the intensities at detectors 1 and 2, respectively, when all intensity should be at detector 1 due to interference. Unlike Q_{det}, Q_{opt} is clearly independent of the losses in the quantum channel.

4.6 Random Number Generation

Before Alice and Bob can share a secret encryption key using QKD, they must be able to generate random bit values for their basis choices and for Alice's raw key. These bit values should be as random as possible, i.e. all bit sequences should have the same probability of being generated, because this minimizes Eve's information. The so-called pseudorandom number generators can be implemented using classical computers. However, the processes used in these types of generators are fundamentally deterministic, and knowing the state of the generator at some point may give Eve information about previously generated keys. Therefore, some physical process should be used for random number generation.

Like in QKD, the fundamental randomness of quantum mechanics can also be used to generate truly random bits for the key distribution process. The simplest way of implementing such a quantum random number generator is a single photon source, a 50:50 beam splitter, and two single photon detectors [22, 23]. When a single photon interacts with such a beam splitter, which path the photon takes after the beam splitter is purely random each path having equal probability, and the path that the photon took can be determined using the single photon detectors. When one detector is assigned the bit value 1 and the other one bit value 0, a random bit sequence of any length can be generated using consecutive measurements. However, since an exactly 50:50 beam splitter is impossible to implement, mathematical operations must be used to remove any bias caused by this imbalance [22].

4.7 Maximum Distance

As with any signal in an optical fiber, the quantum signals used in QKD decay exponentially with distance. In modern telecommunication fibers, a typical value for this attenuation is 0.20 dB/km at 1550 nm wavelength. Therefore, efficient ways of amplifying optical signals without converting them into electrical ones have been developed. However, these amplifiers do not conserve the quantum state of the

signal photons, since this would contradict the no-cloning theorem. Therefore, these methods are not applicable to QKD.

When Alice sends a coherent pulse with a mean photon number $\mu < 1$, over a fiber of length l with attenuation of β, and the detection efficiency of Bob's detector is η_d, the probability of detection is

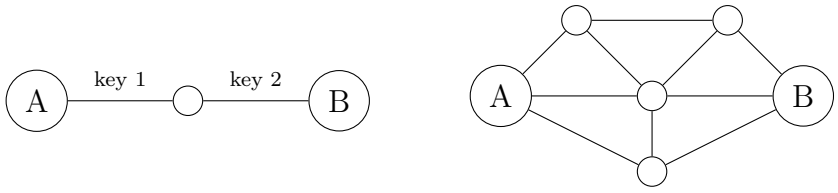
$$p_{det} = \eta_d \mu \times 10^{-\beta l/10}. \tag{37}$$

Naturally, Alice's and Bob's optical systems introduce additional losses that are neglected here. Thus, as the probability of detection decreases exponentially as a function of distance, after some point it becomes of the same order of magnitude with the probability of a dark count in Bob's detector. In this regime, the QBER increases rapidly, as can be seen from Equation (34), which causes the secret key rate to drop to zero. Thus, the dark counts of Bob's detectors fundamentally limit the maximum distance at which QKD can function.

Theoretically, the so-called quantum repeaters can extend the range of QKD by using entanglement swapping. However, these types of repeaters require quantum memories [24] and the ability to do entanglement swapping between these memories [25]. Thus, these kinds of repeaters have not been realized in practice.

A more practical solution for increasing the range of QKD with current technology is to use the so-called trusted nodes, where each node shares a secret key with the next and previous node using QKD. When a message is sent through the nodes, it is decrypted and then encrypted again with a new key in each node. Alternatively, the secret keys between nodes can be used with OTP to securely transfer a new secret key from Alice to Bob so that the message does not need to be decrypted and encrypted in each node [26]. Thus, nodes need to be physically secure so that messages or keys can not be compromised in the them. An example of a QKD system with a single trusted node between Alice and Bob is depicted in Figure 12 (a).

The idea of trusted nodes can be extended to construct QKD networks, where each node can be connected to multiple other nodes in the network, and each connected node pair shares a secret key using QKD. An example of such network is presented in Figure 12 (b). Clearly, this kind of system increases the robustness of QKD, because as long as there are enough connection in the network, there are multiple paths a message can take between two nodes, which makes any type of denial of service attack more difficult. Furthermore, different links do not have to use the same protocol and some can even be free space QKD links, while others are implemented using optical fibers [26, 27].



(a) (b)

Figure 12: (a) A QKD system with a trusted node, (b) a QKD network.

4.8 Free Space

In addition to using an optical fiber as the quantum channel of QKD, research effort has also been directed to the implementation of QKD in free space. As was discussed above, the maximum distance of QKD is fundamentally limited by the absorption of silica when using optical fibers. On the other hand, for wavelengths 780 – 850 nm, absorption caused by the atmosphere can be less than 0.1 dB/km [12]. Furthermore, silicon APDs can be used as the single photon detectors at these wavelengths, which results in significantly higher detection efficiencies, as was discussed in Section 4.2. Lastly, decoherence caused by the atmosphere is practically negligible, and therefore, polarization coding can be used for free-space QKD [12], which simplifies the design of Bob's device, since interference does not need to be used.

Although in the ideal situation, the implementation of free-space QKD is possible with lower losses than with fiber based systems, also new sources for losses are introduced. Most significantly, beam spreading and alignment introduce geometric losses, which can be reduced with optics and additional systems that align the beam correctly. Additionally, stray light from other light sources increases the error rate of free-space QKD compared to optical fiber implementations, and losses are significantly affected by weather conditions. Despite these challenges, free space QKD has been demonstrated over a 144 km link with an average secret key rate of 12.8 bits/s [28].

Maybe the most interesting application for free space QKD is satellite communication. For satellite to satellite communication, there are basically no absorption losses due to the close-to-vacuum environment. Furthermore, even for communication between a ground station and a satellite in low earth orbit, the losses are approximately 30 – 50 dB, and free space QKD links have been demonstrated with even higher losses [29]. With ground to satellite communication, the satellite could act as a trusted node between Alice and Bob due to its physical isolation, possibly enabling QKD for much larger distances than what is possible using optical fibers.

4.9 Wavelength-Division Multiplexing

Wavelength-division multiplexing (WDM) is an important technology in modern optical communication systems. By using multiple channels at different wavelengths in a single optical fiber, data rates can be increased by orders of magnitude compared

to using a single wavelength in each fiber. Fortunately, this technology can also be applied to QKD in multiple ways.

In many QKD systems, a macroscopic timing signal for synchronization between Alice and Bob has been used in the same fiber with the quantum channel using WDM [30]. Other experiments have demonstrated that even the classical channel can be implemented in the same fiber with the quantum channel [31], which simplifies the deployment of QKD in practical scenarios, since only a single optical fiber is needed between Alice and Bob. Even implementations of multiple classical channels and with a quantum channel in a single fiber using dense wavelength-division multiplexing (DWDM) have been demonstrated [32, 33, 34]. Lastly, WDM can also be used to implement multiple quantum channel in a single fiber [35], which significantly increases the secret key rate.

4.10 Side Channel Attacks

As was discussed in Section 3.1.2, Eve can obtain information about the raw key by eavesdropping on the quantum channel in various ways. Fortunately, due to the properties of quantum mechanics, this always causes errors to the raw key. Thus, Eve's information about the key can be minimized by proper analysis to find the correct bounds for the allowed QBER and with the use of privacy amplification. However, when a QKD system is implemented using practical components described in the previous sections, side channels for obtaining secret information are opened to Eve. Furthermore, many of these attacks can be implemented in ways that are not detectable to Alice and Bob without new ways of monitoring the quantum channel.

4.10.1 Photon Number Splitting Attack

The most practical compromise for the single photon source needed for QKD is a highly attenuated laser, as was discussed in Section 4.1. Since a laser is a coherent light source, the amount of photons in a single pulse follows a Poissonian distribution according to Equation (29). Therefore, even when the mean number of photons in a pulse, μ, is less than one, there are cases where Alice's pulse contains multiple photons. Because the same information is encoded into every photon in a pulse, Eve can use this to her advantage by measuring the photon count in each pulse using a quantum nondemolition measurement. If the pulse contains only one photon, Eve blocks it, because she cannot obtain any information about the bit value without perturbing the state. However, if the pulse contains more than one photon, Eve can store one of the photons into a quantum memory while letting rest of the photons in the pulse go through to Bob unaltered. When Alice publicly discloses the correct basis in the sifting phase, Eve can measure the state in her quantum memory in the correct basis and get all information about the correct bit value. This way Eve can obtain the whole raw key without introducing any errors that Alice and Bob could detect. This scheme is called the photon number splitting (PNS) attack. [36, 37]

Because the PNS attack requires Eve to block all of the pulses that contain only one photon, the attack introduces extremely high losses. For this not to be detectable,

the fiber that Alice and Bob use as the quantum channel must have high losses without the PNS attack, and Eve needs a channel with lower losses to transfer the remaining photons to Bob. In the worst case scenario, Eve can be located physically close to Alice so that the losses before her measurement are negligible, and she can transmit the remaining photons to Bob without losses. If the attenuation per kilometer of the fiber used by Alice and Bob is β, length of the fiber is l, and the mean photon number per pulse is μ, Bob detects on average $\mu \times 10^{-\beta l/10}$ photons per each pulse sent by Alice. This must be equal or greater than the probability that a pulse contains more than one photon, $p_{n>1}(\mu)$, for the PNS attack to be undetectable, if Eve uses a lossless channel to transmit the remaining photons to Bob:

$$\mu \times 10^{-\beta l/10} \geq p_{n>1}(\mu). \tag{38}$$

Thus, the maximum distance beyond which the PNS attack becomes undetectable is

$$l_{max} = -\frac{10 \log_{10}\left(\frac{p_{n>1}(\mu)}{\mu}\right)}{\beta}. \tag{39}$$

This means that for typical values of $\beta = 0.2\,\mathrm{dB/km}$ and $\mu = 0.1$, BB84 becomes unsecure with fibers longer than $l = 66\,\mathrm{km}$.

In its most basic form, Bob can detect the PNS attack by measuring the photon statistics of the detected photons. Because Eve blocks all pulses that contain less than two photons, she alters the Poissonian distribution. However, this requires that Bob has a detector that can measure the number of photons in a pulse, which is often not the case with single photon detectors. Furthermore, Eve can alter the photon statistics of the states she forwards to Bob by blocking additional photons, making the distribution Poissonian [38].

To counter the PNS attack, Alice must decrease the mean photon number of her pulses linearly with the transmittance $t = 10^{-\beta l/10}$ of the quantum channel. When this is combined with the fact that the secret key rate with a pure single photon source is proportional to the transmittance, the secret key rate of BB84 with a Poissonian photon source becomes proportional to t^2. [39, 40]

In addition to a way of transmitting the remaining photons with low losses to Bob, Eve must also be able to measure the number of photons in a pulse without disturbing the state of the pulse, which is not possible with current technology [13]. It could also be argued that if such a measurement becomes feasible, Alice could use it to produce pure single photon states by removing any additional photons from her pulses. Furthermore, the PNS attack requires Eve to have a quantum memory in which to store the state of the photon until the correct measurement basis is revealed during the sifting phase. However, a quantum memory with a long enough lifetime has not been realized in practice [41, 42]. Even if such a memory were possible to manufacture in the future, Alice and Bob could add a delay longer than the coherence time of the memory between the raw key exchange and the sifting phases making the memory ineffective.

In cases where the number of photons in a pulse is larger or equal to three, Eve can use an even more powerful attack than the PNS attack by conducting a

measurement, where she obtains a conclusive results about the state of the photons with probability

$$p_c = 1 - \left(\frac{1}{2}\right)^{\left\lfloor \frac{n-1}{2} \right\rfloor}. \tag{40}$$

If the measurement is conclusive, she can prepare a new photon in the correct state and send it to Bob, if not, she can discard the photons. In this attack, no quantum memory is needed, and because Eve can send the information classically to a friend located physically close to Bob, she does not need a low loss channel. [37]

4.10.2 Trojan Horse Attack

Eve does not necessarily need to obtain information about the secret key from the photons used for the key distribution, but she can also use a photon source of her own in the so-called Trojan horse attack. By injecting her photons into Alice's or Bob's device and analyzing the backscattered light, Eve can obtain information about the structure of their devices and even deduce the correct bit values if Alice codes the secret bit values into Eve's photons. [43] How realistic this type of attack is, depends highly on the physical realization of the protocol.

The simplest way to counter the Trojan horse attack is for Alice to use an isolator at her output, so that any light sent by Eve is blocked. However, Eve is not limited by technology and could send more intense light, which would get through due to the finite attenuation of the isolator. Furthermore, for realizations like Plug & Play, described in Section 4.4, where Bob sends pulses of light to Alice, this solution is not applicable. Therefore, additional counter measures must be used to detect unusually high light intensities, and components that encode the bit information, i.e. phase modulators, should be active only when used. Additionally, filters should be used to prevent Eve from using light at different wavelength for the probing. Eve's information can also be reduced by randomizing the global phase of the states when using phase coding. Since the secret bit value is encoded to the phase difference of two pulses, this does not affect the performance of the system. [43]

4.10.3 Blinding Attack

Since most single photon detectors in QKD are based on avalanche photo diodes operating in Geiger mode, as discussed in Section 4.2, Eve can also use these components to obtain additional information about the raw key. By sending bright continuous-wave light to Bob's detectors, Eve can force the APDs to linear mode, where they function as classical light detectors with some optical power threshold. By superimposing pulses of light over the continuous light, Eve can gain full control over Bob's detectors. [44]

To use the control of Bob's detectors to her advantage, Eve can conduct an intercept-resend attack, where she measures the phase of Alice's photons in random bases and resends her results to Bob in the superimposed classical pulses, the power of each pulse being just above Bob's detectors threshold. If Eve's and Bob's basis

choices match, Bob detects the same bit value as Eve. On the other hand, if their basis choices are different, the pulse, and therefore the power, is split between Bob's detectors, and they do not click, because the power is below the threshold in both detectors. After the raw key exchange, Eve can eavesdrop on the sifting in the public channel and obtain the whole secret key without causing any errors. [44] However, Eve causes additional losses, because the basis choice of Alice, Bob, and Eve must match for a bit value to be accepted to the secret key.

Like the Trojan horse attack, this basic form of the blinding attack can be prevented by using an additional optical power meter at Bob's input to detect Eve's continuous light source. However, the detecting of the control pulses may be much more difficult due to possibly low threshold power in the transition between Geiger and linear mode [44].

5 Protocols

After the invention of BB84, there have been numerous other QKD protocols, some of these modifying BB84 to increase the robustness against the PNS attack, some introducing altogether new ways of encoding the bits value, while most have no practical significance. This section introduces the most important QKD protocols beyond BB84.

5.1 BB84 Related

This section introduces three protocols, SARG04, decoy state, and T12, which can be considered as modifications of BB84 to make it significantly more robust against the photon number splitting attack.

5.1.1 SARG04

The transmission and measurement scheme of photons in SARG04 is identical to that of BB84. Instead, the differences are in how Alice and Bob encode the information into the measurement results and what information they disclose during sifting. In SARG04, the basis contains the bit value that Alice wishes to send to Bob; the X basis corresponds to bit value 0, and the Z basis corresponds to bit value 1. The relation between the bases is presented in Equations (15) and (16). In the sifting phase, instead of disclosing the basis, since this would disclose the secret bit, Alice discloses one of four possible sifting pairs $A_{\omega,\omega'} = \{|\omega x\rangle, |\omega' z\rangle\}$, where $\omega, \omega' \in \{+, -\}$, so that one of the two states in the pair is the state she sent. If the state that corresponds to Bob's measurement result is not in the sifting pair, he can deduce which state and bit value Alice sent. [36]

For example, if Alice sends the state $|-x\rangle$, then discloses the pair $A_{-,-} = \{|-x\rangle, |-z\rangle\}$, and Bob measures in the X basis and obtains the result $-x$ or measures in the Z basis and obtains the result $-z$, Bob can not know the state Alice sent.

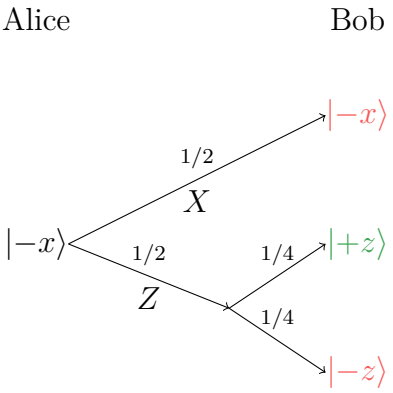


Figure 13: An example of SARG04. Alice sends state $|-x\rangle$ and discloses the pair $A_{-,-}$. In the case marked with green, Bob knows which state Alice sent.

However, if Bob measures in the Z basis and obtains the result $+z$, since this state is not in the sifting pair, he knows that Alice must have measured in different basis from him and the original state must have been $|-x\rangle$. Therefore, the bit value is 0. This process is visualised in Figure 13. While with BB84, Alice and Bob must discard on average 1/2 of the photons during sifting due to basis incompatibility, with SARG04, 3/4 of the photons have to be discarded due to Bob's measurement being inconclusive [36].

Interestingly, unlike with BB84, with SARG04, Eve's eavesdropping actually decreases the fraction of the photons that have to be discarded, as can be seen by comparing Figure 14, where the eavesdropping is visualized, with Figure 13; without eavesdropping 3/4 of photons are discarded, while with eavesdropping the fraction is 5/8. Figure 14 also shows that eavesdropping in SARG04 causes $\frac{1/8}{3/8} = 1/3$ of accepted bits to be incorrect compared to BB84's 1/4.

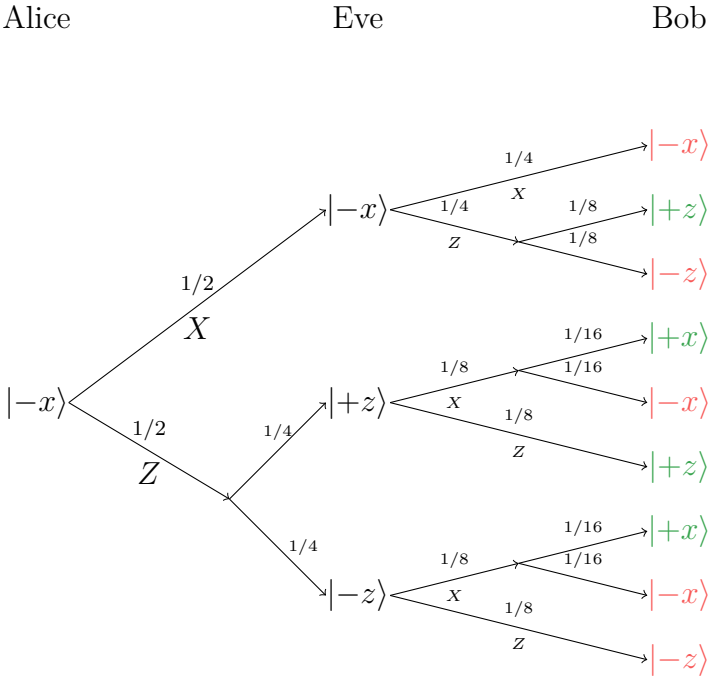


Figure 14: An example of eavesdropping in SARG04. Alice sends state $|-x\rangle$ and discloses the pair $A_{-,-}$. In the cases marked with green, Bob thinks he knows which state Alice sent.

The main advantage of SARG04, its robustness against the photon number splitting attack, is based on the fact that Alice does not disclose her measurement basis. Therefore, even though Eve can wait for the sifting phase before she measures the state of her photon that she has stored in a quantum memory, she does not know which basis she should use for the measurement. Thus, her measurement is conclusive only in 1/4 of the cases, while with BB84 she obtains a conclusive results every time. [36]

In practical terms, the robustness of SARG04 against the PNS attack leads to Alice being able to use higher mean photon numbers in her pulses. As a function of the transmittance of the quantum channel t, the optimal mean photon number scales as $\mu \propto t^{1/2}$ [37, 40]. Therefore, the secret key rate is proportional to $t^{3/2}$, while with BB84 optimal $\mu \propto t$, which caused the secret key rate to be proportional to t^2. This clearly increases the secret key rates and maximum operating distance of QKD. Considering that this is achieved without any hardware changes, the result is quite significant.

Interestingly, when considering single photon implementations, the maximum QBER value for which SARG04 is secure against coherent attacks is $Q \lesssim 11\,\%$, [37]. This is the same bound that was mentioned for BB84 in Section 3.2.

5.1.2 Decoy State

Like SARG04, decoy states are a modification of BB84, that are used to make the protocol more robust against the PNS attack. This modification, however, actually changes the photons exchange part of the protocol, unlike SARG04. [45]

The key distribution procedure with decoy states is identical to that of BB84 without decoy states, but now Alice replaces some fraction of the signal states with decoy states. These decoy states are otherwise identical to the signal states, expect that they have a larger mean photon number. The signal states are still used for key distribution, while the decoy states are used only for the detection of a PNS attack. Because Eve blocks all single photon pulses in the PNS attack, and she cannot distinguish signal states from the decoy states, the attack causes abnormal differences in the yields of decoy and signal states, which can be detected by Alice and Bob. [45]

More precisely, μ and μ' are the mean photon numbers of Alice's signal and decoy state, respectively, and η_n and η'_n are the probabilities that Bob's imperfect detector detects the respective pulse type with n photons after the losses caused by the quantum channel. Then, the yields of the signal and decoy sources are

$$Y_s = \sum_n p_n(\mu)\eta_n, \tag{41}$$

$$Y_d = \sum_n p_n(\mu')\eta'_n. \tag{42}$$

Here, $p_n(\mu)$ is the probability that a pulse with a mean photon number μ contains n photons, determined by the Poissonian distribution in Equation (29). Because the signal and decoy states have identical properties apart from the mean photon number, $\eta'_n = \eta_n$. After Bob has received all of the photons from Alice, she declares which states were decoy states and they can compute the yields Y_s and Y_d. If Y_d is much larger than Y_s, they abort the protocol, because this can be caused by Eve's PNS attack. [45]

Although the original idea of decoy states was to use a single type of strong decoy states with weaker signal states, better results can actually be achieved by using decoy states with varying mean photon numbers. The varying of μ' allows Alice and Bob to estimate the values of η_n and detect any abnormal variations. Furthermore,

this analysis can be applied to the QBER as well. If the QBER of a n photon pulse is q_n, the total QBER Q_μ of a coherent signal with mean photon number μ is

$$Q_\mu = \frac{\sum_n p_n(\mu)\eta_n q_n}{\sum_n p_n(\mu)\eta_n}. \tag{43}$$

Again, because signal and decoy states can not be distinguished, q_n are independent of the pulse type. [46]

The most notable improvement achieved by the decoy state QKD compared to BB84 is that the mean photon number of the signal states does not need to be adjusted according to the losses in the quantum channel. Therefore, the secret key rate of the system is proportional to the transmittance t of the quantum channel [46]. Thus, with the use of decoy states, the same scaling over distance can be achieved as with an ideal implementation of BB84 using a pure single photon source, while with BB84 using coherent pulses without decoy states the possibility of an PNS attack limits the scaling of the secret key rate to t^2 and with SARG04 to $t^{3/2}$.

5.1.3 BB84 With Basis Bias and T12

As was discussed in Section 3.1.1, the security of BB84 is based on the usage of two complementary measurement bases, and Alice chooses either basis with probability of 1/2. However, Alice and Bob can also add bias to their basis choices by choosing one of the bases with the probability p and the other one with probability $1 - p$ [47]. Since the probability of Alice's and Bob's bases being incompatible is $2p(1 - p)$, this clearly improves the efficiency of the protocol, because smaller fraction of the raw key is discarded in sifting. However, this also enables Eve to obtain more information while causing a smaller amount of errors, if she always uses the basis of higher probability for her measurement. To prevent this, Alice and Bob have to compute separate QBER values for each basis, which can be used to effectively detect this new eavesdropping strategy [47]. In fact, the security of this scheme can be guaranteed for any arbitrary small non-zero value of p [47].

The decoy state and basis bias ideas have been combined in the so-called T12 QKD protocol. In T12, $p = 1/16$, which causes only 11.7 % of the raw key to be discarded in sifting. Using a laser source pulsed at 1 GHz, this protocol has been experimentally demonstrated to provide a secret key rate of 1.09 Mbits/s, while with an equivalent unbiased decoy state BB84 secret key rate of 0.63 Mbits/s was achieved in the same experiment. [48]

5.2 Distributed-Phase-Reference

Distributed-phase-reference quantum key distribution protocols represent a more practical approach to QKD. Unlike many theoretical QKD protocols, like BB84, that require an ideal single photon source to provide unconditional security, these protocols have been designed to use coherent pulses for the transmission of secret bits. Additionally, the protocols themselves include how the key distribution is accomplished in practice using physical components.

5.2.1 Differential Phase Shift

Alice's and Bob's devices for the Differential Phase Shift (DPS) protocol are depicted in Figure 15. Alice starts the protocol by generating a sequence of coherent pulses with a time interval T between each consecutive pulse, shifts the phase of each pulse randomly by either 0 or π, and attenuates the sequence so that the mean photon number $\mu < 1$ for each pulse. Thus, the state of every pulse in the sequence is either $\left|\sqrt{\mu}\right\rangle$ or $\left|\sqrt{\mu}e^{j\pi}\right\rangle$. As Bob receives the pulses, he splits the sequence into two branches using a coupler. He then recombines the two branches using another coupler so that the length difference between the two branches is set to be equal to the time interval T. Due to this time difference, the pulse sequence from the longer path is delayed by one pulse compared to the sequence in the shorter path, as depicted in Figure 16. When the paths are combined, if the phase difference between consecutive pulses is 0, the pulses interfere constructively in the output of the coupler connected to detector D_1 and destructively in the other output and vice versa, if the phase shift is π. Detection in detectors D_1 and D_2 represents bit values 0 and 1, respectively. However, because the mean photon number of each pulse is less than one, Bob does not detect a photon in all time slots. Therefore, to generate a secret key, Bob needs to tell Alice at which time slot he detected a photon. Since Alice knows the phase of each pulse, she can deduce in which detector the photon was detected, i.e. the correct bit value. [49]

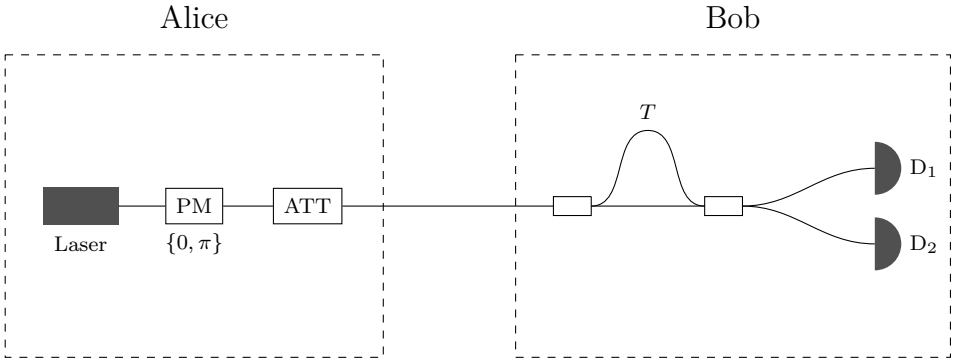


Figure 15: Implementation of the Differential Phase Shift protocol.

Eve can try to conduct an intercept-resend attack using the same measurement scheme as Bob. If she measures the phase between two consecutive pulses, labelled i and $i+1$, she has two possible strategies for the resend part. First, she can resend two new pulses with a mean photon number of 0.5 per pulse and the correct phase difference. Because she did not measure the phase difference between pulses $i-1$ and i or $i+1$ and $i+2$, she sends empty pulses to the slots $i-1$ and $i+2$. However, if Bob now measures the phase difference between pulses $i-1$ and i or $i+1$ and $i+2$, the result is going to be random and can introduce errors when Alice and Bob compute the QBER. On the other hand, Eve can also use the same mean photon number as Alice for all of the pulses and use a random phase for the pulses $i-1$

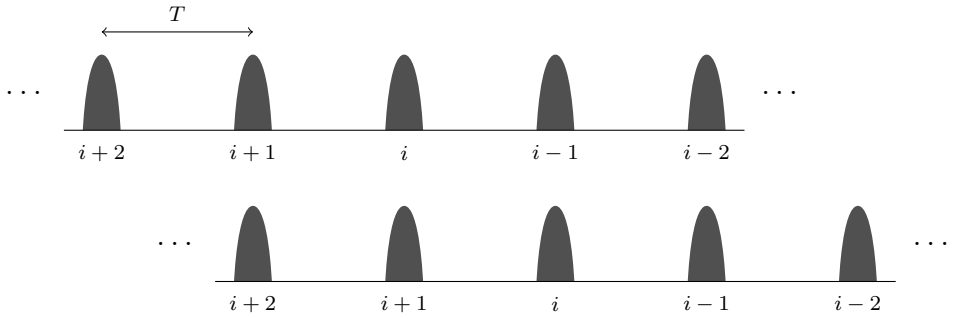


Figure 16: Interference of pulses in the Differential Phase Shift protocol.

and $i + 2$. However, like the previous strategy, this also introduces errors when Bob measures the phase difference between different pulses from Eve. [49]

The fact that in the DPS protocol the bit values are encoded into the differential phase of two consecutive pulses also makes it robust against the photon number splitting attack. In order to obtain any information, Eve must find a photon that is in a superposition state of being in two consecutive pulses. Furthermore, to conduct a PNS attack, there must be two such photons so that Eve can store one of them. Additionally, Eve must block all other pulses, because she can not obtain any information from them. Like with the intercept-resend strategies described above, this blocking can be detected by Bob, because he can measure the phase difference between a blocked pulse and a pulse that Eve has let go through. In these cases, a photon is detected randomly in one of the detectors causing errors to the final key. [50]

5.2.2 Coherent One Way

Like with the Differential Phase Shift protocol, in the Coherent One Way (COW) protocol, Alice produces a sequence of coherent pulses of a mean photon number μ equally spaced in time. However, she does not modulate the phase of the pulses, but lets the phase difference remain constant. Naturally, the coherence time of the laser used must be longer than the time difference between the pulses. Alice uses an intensity modulator to block off some of the pulses generating three possible pulse pairs:

$$|0_i\rangle = |\sqrt{\mu}\rangle_{2i-1} |0\rangle_{2i}\,, \tag{44}$$

$$|1_i\rangle = |0\rangle_{2i-1} |\sqrt{\mu}\rangle_{2i}\,, \tag{45}$$

$$|d_i\rangle = |\sqrt{\mu}\rangle_{2i-1} |\sqrt{\mu}\rangle_{2i}\,. \tag{46}$$

A pulse followed by an empty pulse corresponds to a bit value 0, an empty pulse followed by an pulse corresponds to a bit value 1 and two consecutive pulses is used as a decoy state. [51] These possibilities are visualized in Figure 17.

To obtain the correct bit value, Bob needs to measure the time of arrival of the non-empty pulse. For this, he needs only one single photon detector $\mathrm{D_B}$, as depicted

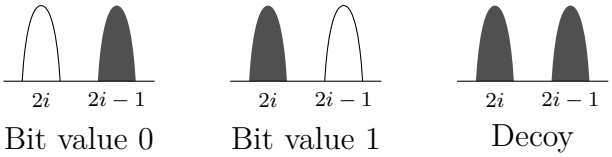


Figure 17: Pulse pairs in the Coherent One Way protocol.

in Figure 18. However, this scheme alone cannot provide any security. Therefore, Bob splits the pulse sequence into two branches using the coupler c_B. Fraction t_B of the pulses go to the detector D_B, while the rest go to an interferometer, which is used to check the coherence of two consecutive pulses in the same fashion as with the differential phase shift protocol. Because Alice does not modulate the phase of the pulses, the same detector clicks for every pair of non-empty pulses. In addition to using the decoy states to check the coherence of the sequence, coherence checks can be done also between different bits. [51] For example, if Alice sends the bit sequence 10, coherence can be tested between the second pulse of the first bit and the first pulse of the second bit, which are both non-empty.

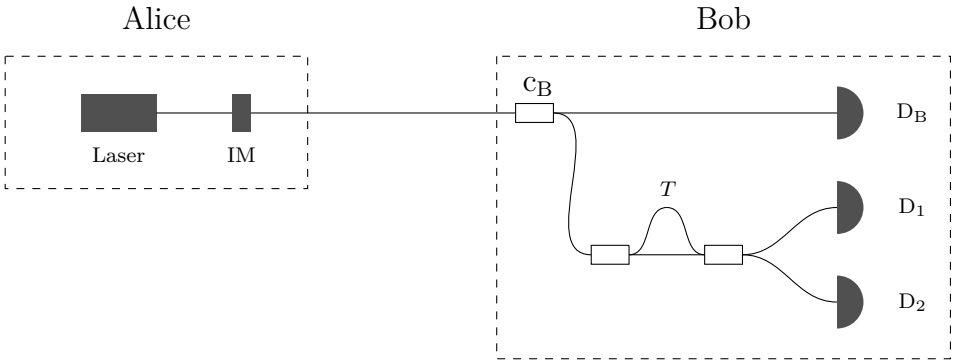


Figure 18: Implementation of the Coherent One Way protocol.

After Bob has receiver all of the pulses, he informs Alice in which time slots he had a detection and when detector D_2 clicked. Alice tells Bob which bit detections were due to decoy states, and must be discarded. She also analyzes from the detector D_2 data whether the coherence was broken by an eavesdropper. [51]

Both of the aforementioned distributed-phase-reference protocols, DPS and COW, differ from the previously discussed QKD schemes in the sense that Bob does not make any choice about his basis of measurement. Therefore, there is no need for any sifting and no fraction of the raw key is lost in the sifting phase, which clearly improves efficiency of the protocols.

Because the coherence between different bit values is crucial for distributed-phase-reference protocols, the states coding separate bit values can not be considered as separate signals, as can be done with BB84 or SARG04. Instead, all of the coherent states encoding the bit sequence have to be analyzed as a whole. Therefore, methods

that can be used to prove the security of other protocols cannot be used for DPS or COW. [12]

Currently, the longest distance on record for QKD, 307 km with an average secret key rate of 3.18 bits/s was achieved using the COW protocol. Furthermore, in the same experiment, the highest secret key rate for distances over 100 km was also demonstrated with 12.7 kbits/s. [52]

5.3 Other Schemes

BB84 and all of the aforementioned protocols derived from it use two complementary bases of measurement to ensure the security of QKD. Furthermore, all of the protocols mentioned so far are so-called prepare and measure and also discrete variable protocols. This section briefly introduces other interesting approaches to QKD.

5.3.1 B92

Secure key distribution can also be achieved with only two non-orthogonal states as is done with the B92 protocol. Alice begins the protocol by preparing each photon either in state $|-x\rangle$ or in state $|-z\rangle$. Here, the same notation is used as with BB84 in Section 3.1.1 for consistency. However, the states $|-x\rangle$ and $|-z\rangle$ do not have to follow the definitions used in BB84, but they must be non-orthogonal. After receiving the photons, Bob conducts one of two measurements described by the projection operators $\hat{P}_x = 1 - |-z\rangle\langle -z|$ and $\hat{P}_z = 1 - |-x\rangle\langle -x|$. These operators project states onto subspaces orthogonal to $|-z\rangle$ and $|-x\rangle$, respectively.

$$\hat{P}_x |-z\rangle = (1 - |-z\rangle\langle -z|)\,|-z\rangle = 0 \tag{47}$$

$$\hat{P}_x |-x\rangle = (1 - |-z\rangle\langle -z|)\,|-x\rangle = |-x\rangle - \langle -z|-x\rangle\,|-z\rangle \tag{48}$$

Therefore, the measurements $\hat{P}_x$ and $\hat{P}_z$ yield zero when applied on $|-z\rangle$ and $|-x\rangle$, respectively. On the other hand, if $\hat{P}_x$ is applied on $|-x\rangle$ or $\hat{P}_z$ on $|-z\rangle$, the measurement yields a positive result with probability $1 - |\langle -x|-z\rangle|^2$ and zero otherwise. [53]

After the measurements, Alice and Bob discard any cases where the measurement result was zero. Without eavesdropping or errors, Alice and Bob have now a shared key, because in the remaining cases either Alice sent the state $|-x\rangle$ and Bob measured $\hat{P}_x$ or Alice sent $|-z\rangle$ and Bob measured $\hat{P}_z$. Like in other QKD schemes, Alice and Bob use some fraction of the shared key to compute the QBER to ensure that there has been no eavesdropping. [53]

5.3.2 Entanglement Based

In all of the QKD protocols discussed above, Alice initiates the key distribution by preparing a photon in some state and sending the photon to Bob, and the security is provided by the non-distinguishability of non-orthogonal states. This approach is usually referred to as prepare and measure. However, another fundamental property of

quantum mechanics, entanglement, can also be used to achieve secure key distribution between Alice and Bob.

In the first entanglement base QKD protocol, E91, a source produces a pair of entangled spin-$\frac{1}{2}$ particles in a so-called singlet state

$$|\text{singlet}\rangle = \frac{1}{\sqrt{2}} \left(|\uparrow\rangle |\downarrow\rangle - |\downarrow\rangle |\uparrow\rangle \right). \tag{49}$$

As can be seen from this definition, due to the entanglement, when the spin of one of the particles in a singlet state is measured, the spin of the other particle is also known, regardless of the physical distance between the particles at the time of the measurement. In order to use this state for key distribution, the first particle is sent to Alice and the second one to Bob. Alice measures the spin in one of three angles $\{0, \pi/4, \pi/2\}$ randomly, while Bob chooses one of the angles $\{\pi/4, \pi/2, 3\pi/4\}$. In cases, where Alice and Bob measure the spin using the same angle, their results are perfectly anti-correlated, and these results can be used to generate a secret key. In cases where the spin was measured in different angles, Alice and Bob can test Bell's theorem to detect any eavesdropping. [54]

Bell's theorem is actually not necessary for the security of entanglement based QKD, as was demonstrated by the entanglement based version of BB84, BBM92. This protocol also uses a source of singlet states, like E91, but now Alice and Bob simply measure the states of their particles in random bases, producing a secret key in an identical manner as with BB84. [55]

An interesting aspect of entanglement based QKD protocols compared to prepare and measure schemes is the fact that the bit value is not actually encoded to the particles that travel between Alice and Bob. Instead, the entanglement simply ensures the correlation between Alice's and Bob's measurement results in the cases where their basis choices match.

5.3.3 Continuous Variable

All of the QKD protocols discussed so far are discrete variable protocols, where single photons, or in most practical scenarios, attenuated laser pulses, are used to encode single bit values and the detection is done using single photon detectors. Another demonstrated scheme is continuous variable quantum key distribution, where the properties of much stronger coherent light pulses are used with homodyne detection.

The quantum states of coherent light can be split into two quadratures

$$\hat{X_1} = \frac{1}{2} \left(\hat{a}^\dagger + \hat{a} \right), \tag{50}$$

$$\hat{X_2} = \frac{i}{2} \left(\hat{a}^\dagger - \hat{a} \right). \tag{51}$$

Here, $\hat{a}^\dagger$ and $\hat{a}$ are the creation and annihilation operators of the number states $|n\rangle$, respectively. Since the operators $\hat{X_1}$ and $\hat{X_2}$ do not commute, the observables X_1 and X_2 obey the uncertainty relation of Equation (6). For a coherent state, as defined in Equation (27), the uncertainty is split equally between the two quadratures,

$\Delta X_1 = \Delta X_2$. However, the uncertainty of one quadrature can be decreased as long as the uncertainty of the other one is increased so that Equation (6) applies. This produces the so-called squeezed states of light.

The properties of squeezed light described above can be directly applied to QKD. In the simplest case, BB84 can be implemented if Alice displaces the expectation value and squeezes one of the two quadratures randomly and Bob measures one of the quadratures randomly as well. If Bob measures the quadrature that Alice has squeezed, his measurement result correlates with the expectation value set by Alice. If he measures the wrong quadrature, the result is random due to the large uncertainty of the other quadrature. [56]

The aforementioned QKD scheme can be seen a hybrid between discrete and continuous variable QKD protocols, since Alice sends a discrete value and Bob measures a continuous value. However, squeezed states can be also used to share purely continuous variables between Alice and Bob by applying Gaussian modulation to either one of the quadratures [57] or both [58]. To obtain a secret key from these continuous variables, specialized error correction protocols have to be used and the performance of the whole system is highly dependent on the performance of the error correction [12].

6 Setup

For all of the measurements presented here, ID Quantique's ID3110 Clavis^2 commercial QKD platform was used. The platform implements phase coding using the Plug & Play scheme, described in Section 4.4, with a 24 km delay line and BB84 and SARG04 protocols. The photon source of the platform is an attenuated laser operating at 1550 nm wavelength, and it emits coherent pulses at 5 MHz repetition rate. Photon detection is done using InGaAs avalanche photo diodes cooled to −35 °C in gated operation. In both Alice's and Bob's end of the system, the platform is connected to a PC using a USB connection, and the PCs manage all of the classical communication, i.e. error correction, privacy amplification, and authentication, using an ethernet connection. The distributed secret keys are stored in the RAM of both PCs, and they can be requested using the IDQ3P protocol. The initial secret, used for authentication after the first round of key distribution, is stored on the hard drive of both PCs and can be changed by the user.

On the software side, the platform is managed by two programs, called *QKDMenu* and *QKDSequence*. The former offers greater amount of control over the key distribution process and is intended for demonstrational and troubleshooting purposes, while the latter automatically manages all of the required steps of QKD, and the only required user input is the loss of the quantum channel as the software is started. Even the used protocol is chosen automatically, based on these losses; BB84 is used for 3 dB and below and SARG04 otherwise. The different steps, raw key exchange, sifting, error correction, privacy amplification, and authentication are managed by different threads of *QKDSequence*, which allows the platform to distribute raw key material even during the classical data processing steps.

The lengths and measured attenuations at 1310 nm and 1550 nm wavelengths of the single mode optical fibers used for the measurements are presented in Table 2. For connecting the fibers to each other and to the QKD platform, SC/PC connectors with approximately 0.3 dB loss per connector were used. Furthermore, short SC/PC – LC/APC fibers were made using fusion splicing for compatibility with the platforms LC/APC ports. The losses caused by the splices were negligible. Additionally, a variable optical air gap attenuator was used to obtain additional data for loss values that were not achievable using the available optical fibers. A 2 m-fiber with LC/APC

Table 2: Used fiber lengths and losses

Length [km]	Loss [dB]	
	1.31 µm	1.55 µm
2	1.5	0.5
4	1.7	0.8
8	2.5	1.8
25(1)	8.3	4.5
25(2)	8.6	4.8

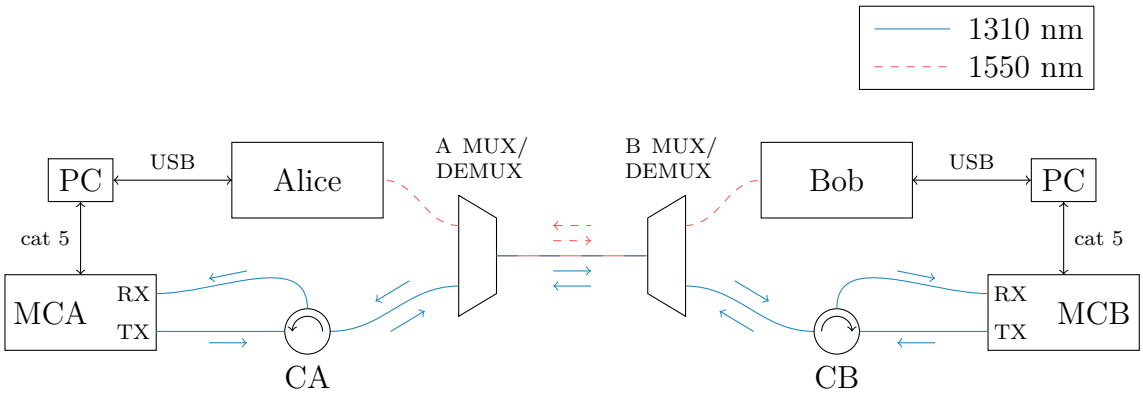


Figure 19: System for combining the quantum and classical channels into the same fiber using WDM.

Table 3: Properties of the used circulators.

Property	Ports	Value [dB]	
		CA	CB
Insertion	$1 \rightarrow 2$	0.7	0.6
Insertion	$2 \rightarrow 3$	0.6	0.4
Isolation	$2 \rightarrow 1$	55	59
Isolation	$3 \rightarrow 2$	58	61
Return		51	53

connectors was used as a reference of the best possible performance, because the loss of the fiber was considered negligible. Insertion losses of either platforms were not taken into consideration, because these are inevitable and cannot be affected by the user in most cases. To make the results reflect the use of the QKD system in a practical scenario and continuous operation, the system was run for at least 12 hours in each configuration, and the average value of each measured quantity was used for the results.

As was discussed in Section 4.9, it has been demonstrated that the quantum and classical channels required for QKD can be combined into the same optical fiber using wavelength-division multiplexing. However, these experiments have been done using costly, commercial grade components. Therefore, the feasibility of this technique in a simple and cost-effective manner using consumer grade components is also tested in this thesis. This should also simulate a worst-case scenario where the quantum channel shares the same fiber with multiple photon sources, the spectral properties of which are not known.

The WDM system is depicted in Figure 19. The classical communication between Alice and Bob was converted to optical signals at 1310 nm wavelength using off-the-shelf media converters (AOA Technology AOM-3100L-S20-EA) MCA and MCB, while

Table 4: Losses of the used WDM-modules.

Multiplexer	Loss [dB]
A MUX	0.8
A DEMUX	0.3
B MUX	0.2
B DEMUX	0.8

the quantum channel was at 1550 nm, as stated above. The 1310 nm wavelength for the classical channel was chosen in order to maximize the spectral distance between the two channels while taking advantage of the relatively low losses of the O-band. Furthermore, this type of configuration is quite typical in older telecommunication WDM systems, which should ensure good compatibility. The properties of the circulators (Thorlabs CIR1310) CA and CB, used for separating the transmitted and received classical signals, are presented in Table 3. The combination of the classical and quantum channels into a single fiber was done using 2-channel WDM modules, and the losses of these modules are presented in Table 4.

7 Results

7.1 Performance of Clavis^2

The most important figure of merit for any QKD system, the secret key rate, R_s, is presented in Figure 20 as a function of fiber length for Clavis^2. For distances below 40 km, the secret key rate decreases exponentially from the maximum value of 4370 bits/s, achieved with a 2 m-fiber, as the losses in the fiber reduce the amount of pulses that reach Bob. However, when the distance is increased beyond 50 km, the probability of Alice's pulse being detected by Bob becomes comparable to the probability of a dark count in Bob's detectors, and the secret key rate drops rapidly to zero. Due to this, 54 km was the longest fiber length for which key distribution was possible with an average secret key rate of 18.7 bits/s. It should be noted that for the first four data points, which correspond to fiber lengths 2 m, 2 km, 4 km, and 8 km, BB84 was used, while SARG04 was used for the rest of the fiber lengths due to the automatic choice done by the software controlling the key distribution.

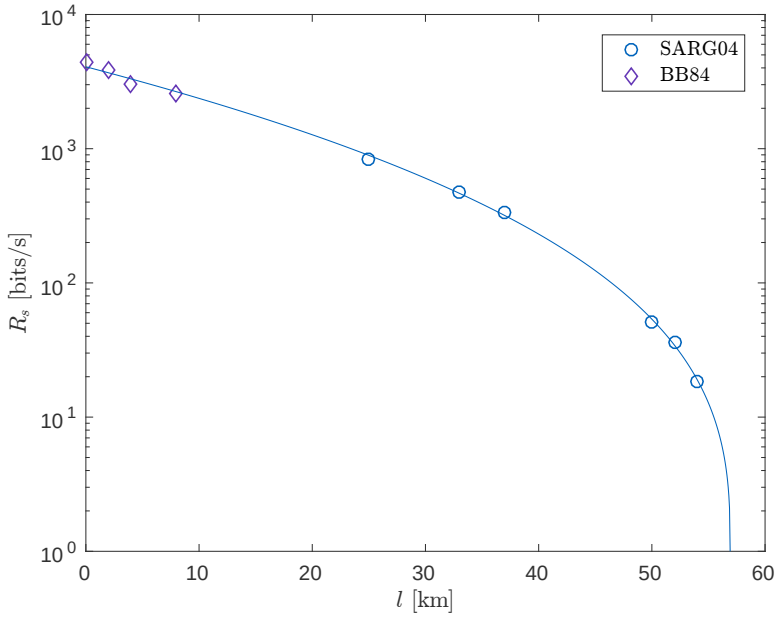


Figure 20: Secret key rate of Clavis^2 as a function of distance.

As can be seen in Figure 21, the quantum bit error rate of the system reflects the same behaviour described above; it increases exponentially with the length of the fiber as the dark counts of the detectors become more and more significant with higher losses in the quantum channel. The minimum QBER, reached with the 2 m-fiber, was 1.74 %. However, the most interesting point is the boundary after which key distribution is no more possible. For Clavis^2, this point was reached between fiber lengths 54 km and 58 km, where the QBER values were 6.54 % and 8.23 %, respectively. Due to the Plug & Play implementation, the visibility of the

system was always in the 99.0 – 99.4 % range. Thus, the most significant error source was the detector dark counts.

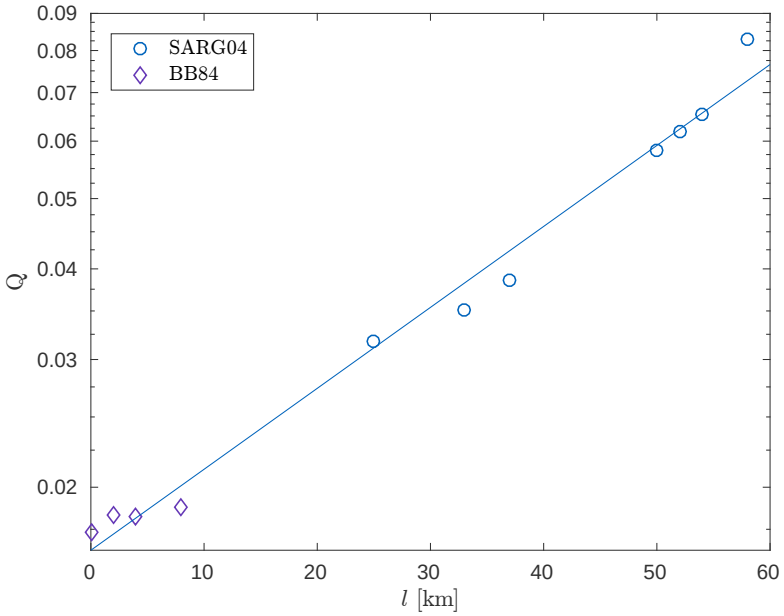


Figure 21: QBER of Clavis[2] as a function of distance.

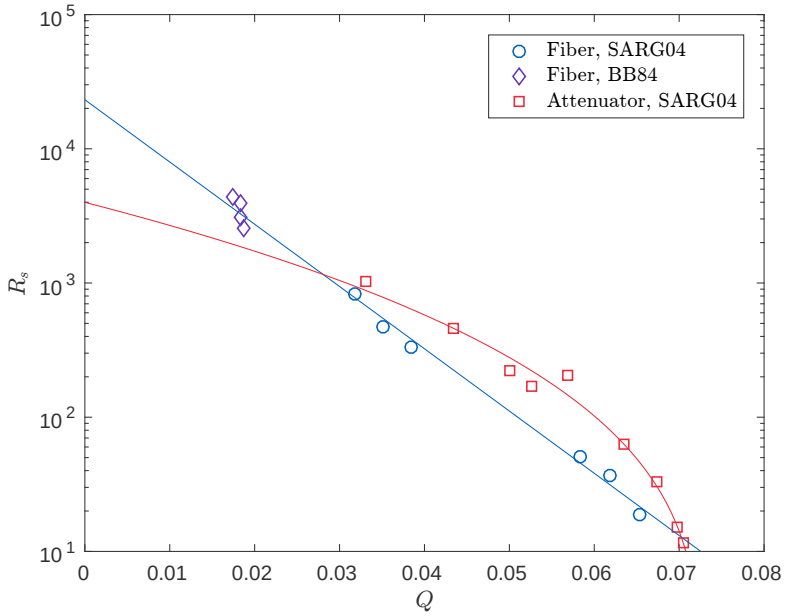


Figure 22: Secret key rate as a function of QBER for fiber and attenuator.

The results above clearly demonstrate the effect that the increasing QBER has

on the secret key rate as the length of the quantum channel increases. However, this is not the only significant effect that determines the secret key rate in a practical system, as can be seen from Figure 22. Here, the secret key rate of the system is plotted as a function of the QBER separately for the cases where optical fibers and where a variable optical air gap attenuator was used. If the secret key rate depended only on the QBER, these two curves should be identical. However, this is clearly not the case; for the measured QBER values, the secret key rate was significantly higher when using an attenuator than with a fiber with the same QBER. Therefore, the physical length of the fiber has a clear effect on the secret key rate in addition to the losses caused by the length. This is partially caused by the Plug & Play system, since Bob has to wait after each sequence of pulses he emits for all of the pulses to return in order to reduce errors caused by backscattering.

The maximum length of Bob's pulse sequence in time is l_d/c, where l_d is the length of Alice's delay line and c the speed of the pulses in the quantum channel. Since the pulses must propagate twice through the delay line and the quantum channel, from Bob to Alice and back, the delay between Bob emitting the last pulse of a sequence and detecting the same pulse is $(2l_d + 2l)/c$. Thus, the total length of a raw key exchange round is $(3l_d + 2l)/c$, and out of this Bob spends $2l_d/c$ either emitting or detecting photons. Therefore, the duty cycle ν of the system can be defined as $\nu = 2l_d/(3l_d + 2l)$. From this, one can see that, for fiber lengths close to 50 km, the system spends approximately 73 % of the time waiting for the pulse sequence to return, while with an attenuator this is constant 33 %. This is a clear drawback of the Plug & Play system compared to other phase coding implementations. It should be noted, however, that in other implementations, Alice's and Bob's interferometers must be adjusted between rounds of raw key exchange, which also introduces additional delay. This type of adjustments are not needed with Plug & Play, as was discussed in Section 4.4.

In Figure 23, the secret key rate has been normalized with respect to the duty cycle defined above. Now there is no distinguishable difference between the secret key rates when using optical fibers and an attenuator. Thus, the difference is dominantly caused by the duty cycle of the system.

Another phenomenon cause by high losses is that Clavis^2 has to remeasure the length of the quantum channel occasionally in order to maintain proper synchronization between emitting of pulses and gating of the detectors. For example, for a 50 km-fiber, the length has to be measured on average once for every 20 rounds of the raw key exchange. Furthermore, the software controlling the platform waits until there is approximately 9×10^5 bits of raw key available before error correction is initiated. When the losses in the quantum channel are high, this accumulation of the raw key material takes a significant amount of time. The effect of these delays and the aforementioned duty cycle can be clearly seen in Figure 24, where the average delay between sets of secret keys is presented as a function of the QBER. For short optical fibers, the delay is fairly constant at approximately 2 min. However, when $Q > 3\,\%$, the delay increases linearly reaching a maximum of 32 min with the 54 km-fiber. For the attenuator, the behaviour is radically different; for $3\,\% < Q < 6\,\%$, the delay increases linearly, but at a significantly lower rate than with optical fibers. For

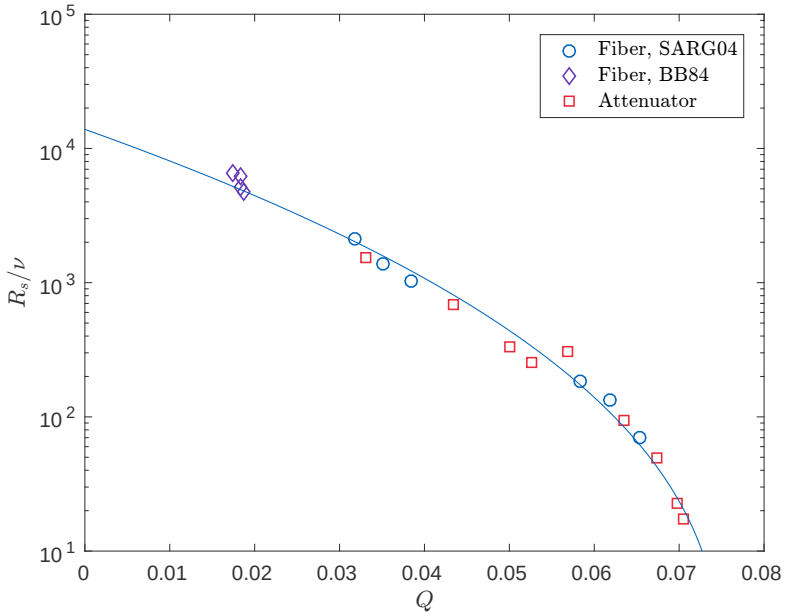


Figure 23: Normalized secret key rate as a function of QBER for fiber and attenuator.

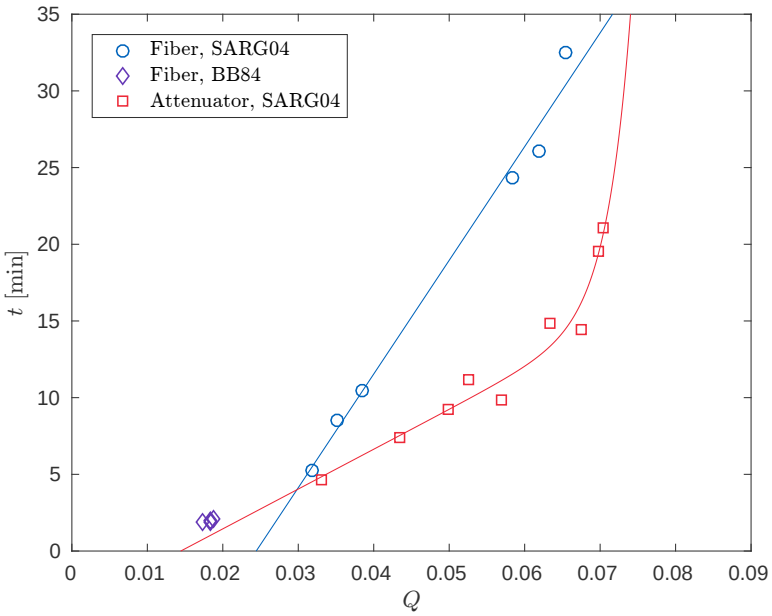


Figure 24: Average delay between sets of secret keys as a function of the QBER.

example, at $Q = 6\,\%$, the average delay is approximately 10 min for the attenuator and 26 min for the fibers. Beyond this point, the delay with the attenuator starts to increase exponentially reaching maximum value of 21 min when $Q = 7.0\,\%$.

The long delay between sets of secret keys discussed above can significantly affect the usability of the system in some practical applications. This is especially true when the system is first started up, since there can be up to a 30 min delay before any secret keys are available for use, if the losses in the quantum channel are high. In the worst case, if privacy amplification fails to produce any secret bits after the first round of key distribution, which occurs occasionally with high QBER values, this time can double. Furthermore, an additional 9 min start up delay is added by the fact that Bob's detectors must be cooled to $-35\,^{\circ}\mathrm{C}$ before key distribution can begin. However, if the system is used in continuous operation and some type of key management that takes into account the infrequency of the key sets is put in place, these factors should not affect the performance of the system in most cases.

For the hardware of the system, the longest tested time of continuous operation was approximately 2 months. Additionally, the longest tested continuous key exchange run was approximately four days. During these tests or any other time of normal operation, no issues were detected with the stability of the platform. Additionally, no user intervention was needed after starting the key distribution process.

7.2 Classical Processing

As can be seen from Figure 25, the fraction of the sifted key that is disclosed during error correction with ID Quantique's Cascade implementation increases linearly as

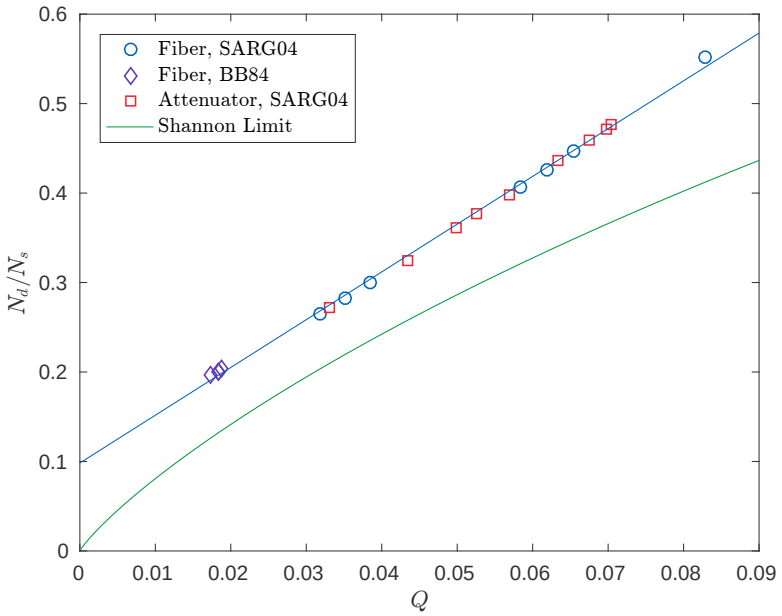


Figure 25: Fraction of disclosed bits as a function of QBER.

a function of the QBER. In the same figure, the so-called Shannon limit is also presented, which defines the minimum amount of information Alice must send to Bob per bit, and therefore disclose to Eve, for Bob to be able to correct the errors in his key. The minimum relative difference between the disclosed bits and the Shannon limit is reached around $Q = 5.2\,\%$, where Cascade discloses 28 % more bits than an ideal error correction algorithm. On the other hand, at the last data point, where $Q = 8.3\,\%$ and Cascade discloses 55 % of the key, the difference has grown to 34 %. It should also be noted that, since the QBER increases exponentially as the length of the fiber increases, the fraction of disclosed bits also increases exponentially with the fiber length.

In Figure 26 the number of communications between Alice and Bob during error correction, N_{com}, is presented as a function of the QBER. Here, one can clearly see the major drawback of Cascade; even when the QBER is as low as 1.7 %, Cascade still requires approximately 1600 communications to correct the errors in Bob's sifted key. Furthermore, for QBER values between 3.2 % and 8.3 %, which represent a range of more realistic values in a practical scenario, the number of communications grows linearly from 2300 to 6700. When this high number of communications is combined with the amount of disclosed bits presented above, Cascade can be considered obsolete, especially since LDPC codes can achieve better results with a single communication, as was discussed in Section 3.1.3.

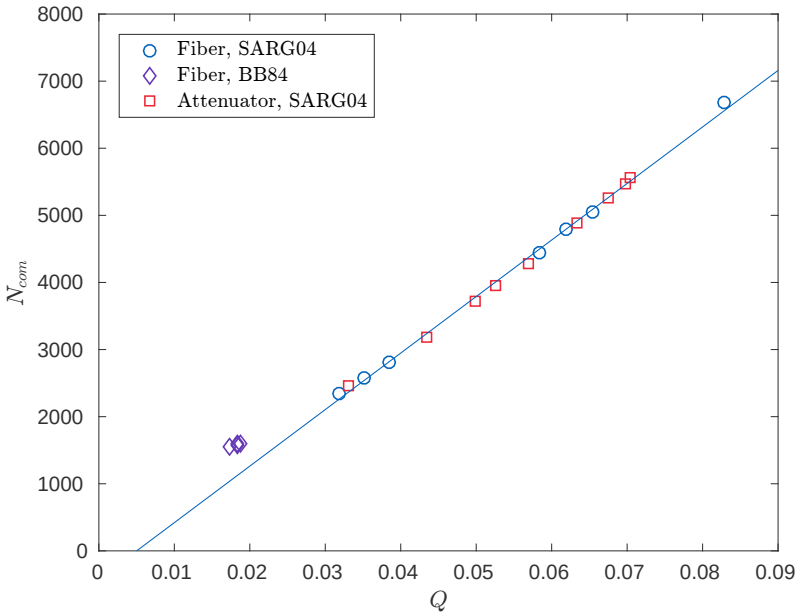


Figure 26: Number of communications during error correction as a function of the QBER.

In Figure 27, the fraction of bits left to the secret key after privacy amplification is depicted as a function of the QBER. In order to eliminate the effect of the bits disclosed during error correction, here the final key size N_f is compared to $N_s - N_d$,

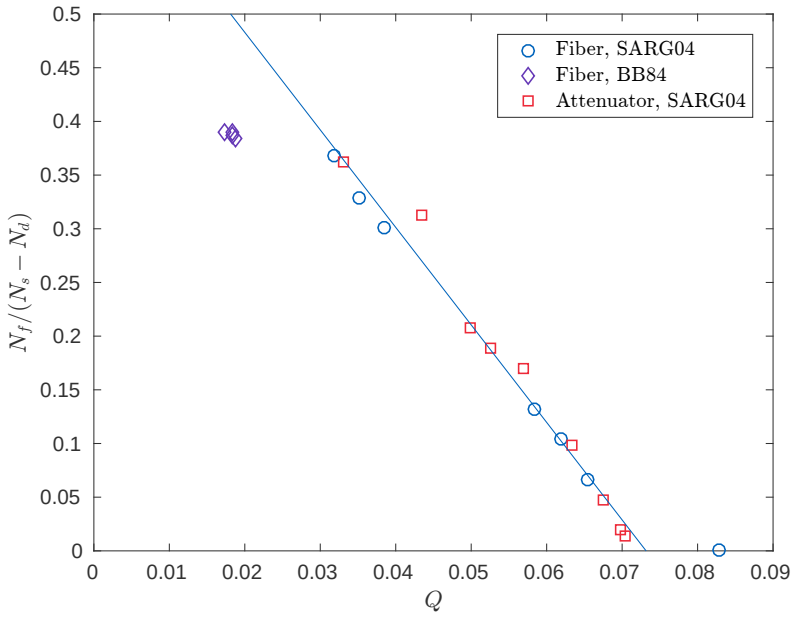


Figure 27: Fraction of bits left after privacy amplification as a function of QBER.

where N_s and N_d are the sifted key size and amount of bits disclosed by Cascade, respectively. For fiber lengths of 8 km and below, where the QBER was 1.7 – 2.0 % and the used protocol was BB84, there is only a small change from 0.39 to 0.38 in the fraction of bits left after privacy amplification. However, for $Q > 3.7\,\%$, the fraction starts to decreases linearly from 0.32 as the QBER increases. Furthermore, privacy amplification produced zero secret bits in 1.7 % and 6.0 % of cases for fiber lengths 52 km and 54 km, respectively. Interestingly, when studying the raw data of these runs as a function of time, no correlation was found between the cases where privacy amplification produced zero secret bits and any other relevant quantity that could have caused this.

The average bandwidth used in the classical channel by Bob during the key distribution is depicted in Figure 28 as a function of the fiber length. The bandwidth clearly decreases exponentially with the fiber length from 890 kbits/s transmitted and 70 kbits/s received measured with the 2 m-fiber. Interestingly, the amount of data Bob receives is over an order of magnitude smaller than how much he transmits for all fiber lengths. This indicates that majority of the bandwidth is used in the sifting phase, where Bob sends information to Alice about which photons he detected and what were his basis choices.

Although the need for error correction increases with longer fibers and higher QBER values, which require more bandwidth in the classical channel, this is not reflected by the measurement results. Instead, the used bandwidth correlates rather well with the raw key rate and the losses in the fiber; with higher losses, the raw key rate is reduced, which in turn reduces the amount of classical processing and the used bandwidth.

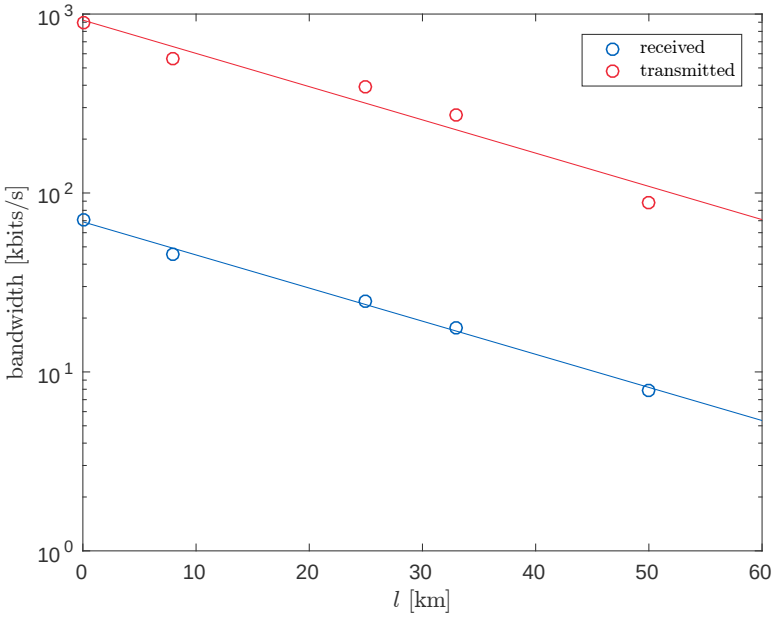


Figure 28: Use of the classical channel at Bob's end.

7.3 Issues in Operation

Some interesting behaviour was detected, when a 2 m-fiber was used to maximize the raw key rate of the system, and both receiving and sending bandwidths of the classical channel were limited in both Alice's and Bob's ends to 50 kbits/s. The software managing the key distribution in Bob's PC crashed in 98 min. The bandwidth limitation prevented the sifting of the raw keys at a higher rate than the raw key rate, which caused the key management software to fill all of the available memory with raw key material, run out of usable RAM, and crash due to improper error handling of `std::bad_alloc`. In Figure 29, the average time period for how long the system took to crash, the crash time, t_c, is presented as a function of the bandwidth limitation B. For $B \geq 50$ kbits/s, the crash time increases exponentially as the bandwidth limitation is increased, because with the larger bandwidth the system is able to sift some of the key raw key material and even do error correction, which increases the time the system takes to fill the RAM. Interestingly, the crash time also increases when the bandwidth limitation approaches zero. For example, for $B = 2$ kbits/s, the crash time was 144 min, which is significantly longer than for the aforementioned $B = 50$ kbits/s. This is caused by the fact that such a low bandwidth started to limit even the speed of the raw key exchange, which naturally increased the time the system took to fill the RAM with the raw key material. Due to these effects, the shortest crash time was reached with the aforementioned $B = 50$ kbits/s.

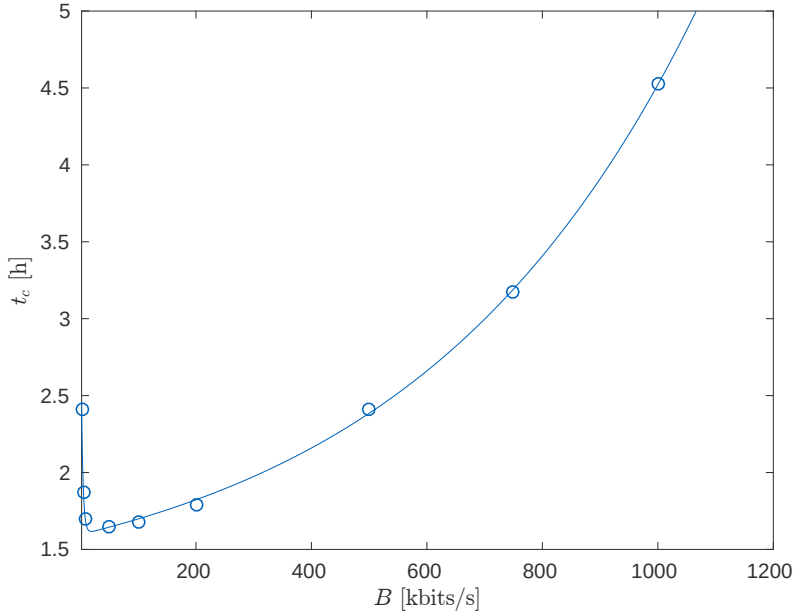


Figure 29: Average crash time of the system as a function of bandwidth of the classical channel.

It could be argued that limiting the bandwidth of the classical channel to such low values does not fairly represent any practical situation. However, since all of the secret keys are lost in the crash and distributing new secret keys can take a significant amount of time, Eve could use this kind of attack to hinder the key distribution between Alice and Bob even in cases where she does not have access to the quantum channel. On the other hand, if she has access to the quantum channel, and she has somehow obtained information about the initial secret used by Alice and Bob, she could use this attack to force Alice and Bob to restart the key distribution process giving her a window of opportunity to conduct a man-in-the-middle attack during the first round of key distribution, when the initial secret is used for authentication. Lastly, even without an eavesdropper, this behaviour makes the system unstable in all situations where the available bandwidth is below the value indicated by Figure 28.

As was mentioned earlier, the Clavis^2 system must measure the physical length of the quantum channel in order to maintain proper synchronization between the emitting of pulses and gating of the detectors. This measurement is done when the controlling software is started and any time the synchronisation is lost. Interestingly, when multiple optical fibers were connected together to form the quantum channel using standard telecommunication SC/PC connectors, the system would occasionally measure the length of the quantum channel incorrectly. In all of these cases, the measurement recognized only some of the fibers. For example, when two 25 km-fibers and one 4 km-fiber were used, the system would occasionally measure the length to be 29 km, 25 km, or even 4 km. This would indicate that the error was caused by reflections from the SC/PC connections. However, the return loss of all of the connections was measured to be greater than 45 dB, which is quite typical for these

types of connectors. This problem could probably be prevented by using only APC connectors, but this is not always possible in practical scenarios. Therefore, giving the user the option to input an approximate quantum channel length when the system starts and using this information during the measurement would be the most practical solution to the problem.

7.4 Wavelength-Division Multiplexing

Spectra of the media converters used for the wavelength-division multiplexing experiments are presented in Figure 30. The main peak of the media converter A at 1308 nm is fairly close to the claimed 1310 nm, while the peak of the media converter B is at 1318 nm. Both spectra consist of peaks with 1 nm spacing and −50 dB spectral widths are 38 nm and 39 nm for media converters A and B, respectively.

Bob's detectors' noise measurements when one classical channel was multiplexed into the same 10 m-fiber with the quantum channel using the media converter B are presented in Table 5. As a result, we get probabilities of detecting a photon in the detector during a single gate when there is no quantum channel, i.e. no photons should be detected. Separate measurements are presented for cases where the light of the classical channel propagated from Alice to Bob, i.e. in the same direction with a hypothetical quantum channel, and from Bob to Alice. Additionally, 10 dB and 15 dB optical attenuators were added to the output of the media converter, and Bob's input was filtered using a 17 nm FWHM optical bandpass filter centered around the wavelength of the quantum channel.

As could be expected, the highest amount of noise was caused by a classical

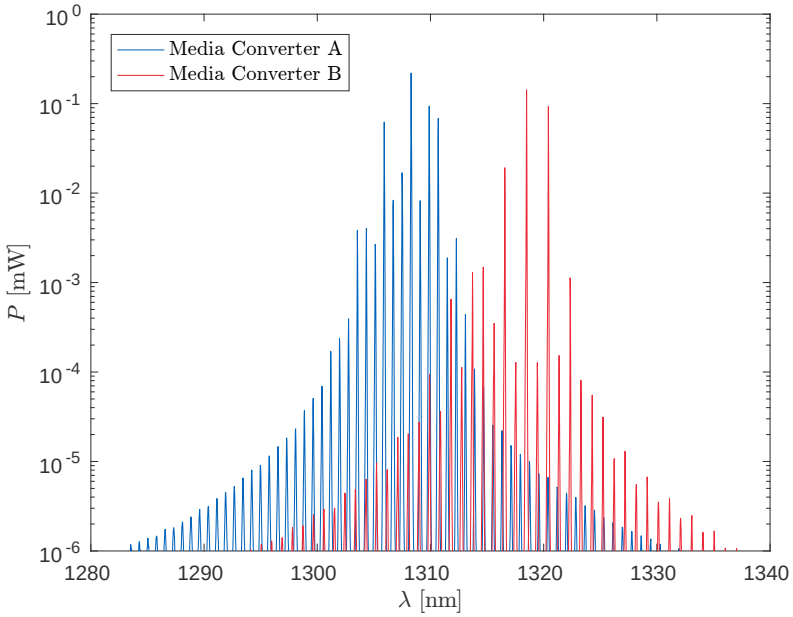


Figure 30: Spectra of the media converters.

Table 5: Bob's detectors' noise measurements.

Classical Channel	Without a filter		With a filter	
	D1	D2	D1	D2
None	8.08×10^{-5}	4.35×10^{-5}		
B → A	1.43×10^{-1}	1.81×10^{-1}	1.15×10^{-3}	6.97×10^{-4}
A → B	7.13×10^{-1}	7.55×10^{-1}	1.49×10^{-2}	7.02×10^{-3}
B → A, 10 dB	7.52×10^{-3}	1.13×10^{-2}	1.40×10^{-4}	6.98×10^{-5}
A → B, 10 dB	6.33×10^{-2}	9.90×10^{-2}	5.87×10^{-4}	4.04×10^{-4}
B → A, 15 dB	4.01×10^{-3}	2.97×10^{-3}	1.08×10^{-4}	5.82×10^{-5}
A → B, 15 dB	3.78×10^{-2}	2.34×10^{-2}	3.52×10^{-4}	2.90×10^{-4}

channel that propagated to the same direction with the quantum channel when no filtering or attenuation was used. In this case, there was a 71 % probability of detecting a photon in detector 1 and 76 % in detector 2. Since the photon detectors are gated at 5 MHz, this corresponds to an optical power of approximately 5×10^{-12} W, if the quantum efficiency of the detectors is assumed to be 10 %. This explains why the power is not detectable in the spectrum of Figure 30, where the noise floor of the spectrum analyzer limited the lowest detectable power to 10^{-6} mW. This noise is approximately four orders of magnitude larger than without multiplexing, where the noise levels were 8.1×10^{-5} and 4.4×10^{-5} for detectors 1 and 2, respectively. Interestingly, if the classical channel is reversed to propagate from Bob to Alice, the noise is reduced by 75–80 %. Furthermore, adding the bandpass filter to Bob's input reduced the noise even more significantly, by two orders of magnitude.

Unsurprisingly, adding a 10 dB attenuator to the output of the media converter further reduced the noise levels by one order of magnitude, and a 15 dB attenuator by additional 47–76 %. Using a 20 dB attenuator was also tested. However, the media converter did not function under such high losses. Thus, the lowest noise levels were achieved by setting the direction of the classical channel to be from Bob to Alice, attenuating the classical channel by 15 dB and using the optical filter at Bob's input. With this configuration, the noise levels were 1.1×10^{-4} and 5.8×10^{-5} for detectors 1 and 2, respectively, which is a 34 % increase for both detectors compared to the noise without multiplexing. However, if the entire classical channel was multiplexed into the same fiber with the quantum channel, the noise would clearly be dominated by the light propagating from Alice to Bob. Therefore, the noise levels 3.5×10^{-4} and 2.9×10^{-4} are a better figure of merit in a practical situation.

Although the filtering and attenuating reduced the amount of noise quite close to the values achieved without multiplexing when the classical channel was set to propagate from Bob to Alice, the key distribution was not possible even with this configuration, because the QBER was approximately 12 %. Since the additional noise in the detectors caused by the classical channel can be considered effectively as additional dark counts, this increase of the QBER cannot be caused by the noise alone, as can be seen from Equation (34). Furthermore, changing the direction of

the classical channel caused the length measurement of the quantum channel to be impossible, which prevented even starting of the key distribution. Therefore, using the system of Figure 19 for combining the classical and quantum channels into a single fiber is not feasible with the chosen components. Additionally, these results clearly demonstrate the challenges in combining quantum and any classical signals into the same fiber; due to the drastically different optical power levels, the isolation between quantum and classical channels has to be orders of magnitude greater than in ordinary WDM applications.

Since the addition of the bandpass filter to Bob's input improved the noise measurements of the detectors by almost two orders of magnitude in all cases in Table 5, the results could be further improved significantly, if a filter with a narrower passband was used either at Bob's input port or at the output of the media converter. Alternatively, a probably more effective solution would be to use media converters with significantly narrower spectra. However, both of these solutions would significantly reduce the cost-effectiveness of the system, which was one of the main objectives.

8 Conclusion

The main objective of this thesis was to assess whether quantum key distribution is applicable to practical applications at its current state. In addition to security, the most important criteria for this were set to be performance, stability, and usability. All of these criteria were tested using one of the few commercially available QKD platforms, ID Quantique's Clavis^2.

The highest achieved key rate with the tested QKD platform was 4370 bits/s with a 2 m optical fiber. The longest fiber length for which the platform was able to provide secret keys was 54 km. At this distance, the average secret key rate was 18.7 bits/s. Whether these rates are sufficient for practical applications, depends highly on the desired level of security, one-time pad representing the best level possible. For distances well below 50 km, the provided secret key rate may be adequate for basic communication using OTP. However, if distances close to 50 km or high data rates are desired, more advanced ciphers remain as the only option; even the 18.7 bits/s secret key rate is sufficient to change a 256-bit AES key every 14 seconds.

Like with most discrete variable QKD systems, the most limiting factor of Clavis^2 are the photon detectors; dark counts limit the maximum distance, and after pulses limit the maximum raw key rate. Furthermore, the implemented protocols, BB84 and SARG04, are not as robust against the PNS attack as many newer protocols, which limits the maximum distance even further. Lastly, the Cascade error correction algorithm can be considered obsolete, since more efficient protocols that require less interactivity have been demonstrated.

The tested QKD platform was stable during normal operation for long periods of time and did not require any intervention from the user during operation. However, it was observed that limiting the bandwidth of the classical channel makes the system unstable. This is caused by the managing software running out of usable memory and improper error handling. Furthermore, when the quantum channel consisted of multiple optical fibers connected with SC/PC connectors, the system was occasionally unable to measure the length of the quantum channel correctly, preventing the key distribution from starting. This effect was especially prominent with long fibers and high losses. Fortunately, both of the observed problems could be fixed by modifying the software.

In its current state, QKD can be considered a mature technology that can provide provably secure communication within the limitations presented above. However, since this provable security is the strength of QKD compared to the alternatives, further development is needed to achieve secret key rates sufficient for encryption using OTP at modern data rates.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[2] J. Daemen and V. Rijmen, *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2013.

[3] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*. IEEE, 1994, pp. 124–134.

[4] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-quantum cryptography*. Springer Science & Business Media, 2009.

[5] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. ACM, 1996, pp. 212–219.

[6] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *International Conference on Computer System and Signal Processing, IEEE*, 1984, pp. 175–179.

[7] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[8] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1993, pp. 410–423.

[9] D. Elkouss, A. Leverrier, R. Alléaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *2009 IEEE International Symposium on Information Theory*. IEEE, 2009, pp. 1879–1883.

[10] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[11] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," *Journal of computer and system sciences*, vol. 22, no. 3, pp. 265–279, 1981.

[12] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of modern physics*, vol. 81, no. 3, p. 1301, 2009.

[13] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.

[14] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Physical review letters*, vol. 85, no. 2, p. 441, 2000.

[15] J. Claudon, J. Bleuse, N. S. Malik, M. Bazin, P. Jaffrennou, N. Gregersen, C. Sauvan, P. Lalanne, and J.-M. Gérard, "A highly efficient single-photon source based on a quantum dot in a photonic nanowire," *Nature Photonics*, vol. 4, no. 3, pp. 174–177, 2010.

[16] I. Aharonovich, C. Zhou, A. Stacey, J. Orwa, S. Castelletto, D. Simpson, A. D. Greentree, F. Treussart, J.-F. Roch, and S. Prawer, "Enhanced single-photon emission in the near infrared from a diamond color center," *Physical Review B*, vol. 79, no. 23, p. 235316, 2009.

[17] J. McKeever, A. Boca, A. Boozer, R. Miller, J. Buck, A. Kuzmich, and H. Kimble, "Deterministic generation of single photons from one atom trapped in a cavity," *Science*, vol. 303, no. 5666, pp. 1992–1994, 2004.

[18] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, "Avalanche photodiodes and quenching circuits for single-photon detection," *Applied optics*, vol. 35, no. 12, pp. 1956–1976, 1996.

[19] M. A. Albota and F. N. Wong, "Efficient single-photon counting at 1.55 μm by means of frequency upconversion," *Optics letters*, vol. 29, no. 13, pp. 1449–1451, 2004.

[20] R. T. Thew, S. Tanzilli, L. Krainer, S. Zeller, A. Rochas, I. Rech, S. Cova, H. Zbinden, and N. Gisin, "Low jitter up-conversion detectors for telecom wavelength GHz QKD," *New Journal of Physics*, vol. 8, no. 3, p. 32, 2006.

[21] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, ""plug and play" systems for quantum cryptography," *Applied Physics Letters*, vol. 70, no. 7, pp. 793–795, 1997.

[22] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," *Journal of Modern Optics*, vol. 47, no. 4, pp. 595–598, 2000.

[23] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Review of Scientific Instruments*, vol. 71, no. 4, pp. 1675–1680, 2000.

[24] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: the role of imperfect local operations in quantum communication," *Physical Review Letters*, vol. 81, no. 26, p. 5932, 1998.

[25] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Reviews of Modern Physics*, vol. 83, no. 1, p. 33, 2011.

[26] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes *et al.*, "The secoqc quantum key distribution network in vienna," *New Journal of Physics*, vol. 11, no. 7, p. 075001, 2009.

[27] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the darpa quantum network," in *Defense and Security*. International Society for Optics and Photonics, 2005, pp. 138–149.

[28] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Physical Review Letters*, vol. 98, no. 1, p. 010504, 2007.

[29] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang *et al.*, "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," *Nature Photonics*, vol. 7, no. 5, pp. 387–393, 2013.

[30] A. Tanaka, M. Fujiwara, S. W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K.-i. Yoshino, S. Miki, B. Baek, Z. Wang *et al.*, "Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization," *Optics express*, vol. 16, no. 15, pp. 11 354–11 360, 2008.

[31] P. D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," *Electronics Letters*, vol. 33, no. 3, pp. 188–190, 1997.

[32] N. Peters, P. Toliver, T. Chapuran, R. Runser, S. McNown, C. Peterson, D. Rosenberg, N. Dallmann, R. Hughes, K. McCabe *et al.*, "Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments," *New Journal of physics*, vol. 11, no. 4, p. 045012, 2009.

[33] P. Eraerds, N. Walenta, M. Legre, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 gbps data encryption over a single fibre," *New Journal of Physics*, vol. 12, no. 6, p. 063027, 2010.

[34] K. Patel, J. Dynes, M. Lucamarini, I. Choi, A. Sharpe, Z. Yuan, R. Penty, and A. Shields, "Quantum key distribution for 10 gb/s dense wavelength division multiplexing networks," *Applied Physics Letters*, vol. 104, no. 5, p. 051123, 2014.

[35] K.-i. Yoshino, M. Fujiwara, A. Tanaka, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki *et al.*, "High-speed wavelength-division multiplexing quantum key distribution system," *Optics letters*, vol. 37, no. 2, pp. 223–225, 2012.

[36] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Physical review letters*, vol. 92, no. 5, p. 057901, 2004.

[37] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, "Security of two quantum cryptography protocols using the same four qubit states," *Physical Review A*, vol. 72, no. 3, p. 032301, 2005.

[38] N. Lütkenhaus and M. Jahma, "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack," *New Journal of Physics*, vol. 4, no. 1, p. 44, 2002.

[39] A. Niederberger, V. Scarani, and N. Gisin, "Photon-number-splitting versus cloning attacks in practical implementations of the bennett-brassard 1984 protocol for quantum cryptography," *Physical Review A*, vol. 71, no. 4, p. 042316, 2005.

[40] B. Kraus, C. Branciard, and R. Renner, "Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses," *Physical Review A*, vol. 75, no. 1, p. 012316, 2007.

[41] B. Julsgaard, J. Sherson, J. I. Cirac, J. Fiurášek, and E. S. Polzik, "Experimental demonstration of quantum memory for light," *Nature*, vol. 432, no. 7016, pp. 482–486, 2004.

[42] A. I. Lvovsky, B. C. Sanders, and W. Tittel, "Optical quantum memory," *Nature photonics*, vol. 3, no. 12, pp. 706–714, 2009.

[43] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Physical Review A*, vol. 73, no. 2, p. 022320, 2006.

[44] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature photonics*, vol. 4, no. 10, pp. 686–689, 2010.

[45] W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Physical Review Letters*, vol. 91, no. 5, p. 057901, 2003.

[46] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical review letters*, vol. 94, no. 23, p. 230504, 2005.

[47] H.-K. Lo, H.-F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *Journal of Cryptology*, vol. 18, no. 2, pp. 133–165, 2005.

[48] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, "Efficient decoy-state quantum key distribution with quantified security," *Optics express*, vol. 21, no. 21, pp. 24 550–24 565, 2013.

[49] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," *Physical Review A*, vol. 68, no. 2, p. 022317, 2003.

[50] K. Inoue and T. Honjo, "Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack," *Physical Review A*, vol. 71, no. 4, p. 042305, 2005.

[51] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Applied Physics Letters*, vol. 87, no. 19, p. 194108, 2005.

[52] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photonics*, vol. 9, no. 3, pp. 163–168, 2015.

[53] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, no. 21, p. 3121, 1992.

[54] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.

[55] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Physical Review Letters*, vol. 68, no. 5, p. 557, 1992.

[56] M. Hillery, "Quantum cryptography with squeezed states," *Physical Review A*, vol. 61, no. 2, p. 022309, 2000.

[57] N. J. Cerf, M. Levy, and G. Van Assche, "Quantum distribution of gaussian keys using squeezed states," *Physical Review A*, vol. 63, no. 5, p. 052311, 2001.

[58] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical review letters*, vol. 88, no. 5, p. 057902, 2002.