



LUND UNIVERSITY
Faculty of Science

The Implementation of the Frequency-Time Encoded Decoy-State Protocol with the Slow-Light Effect for Quantum Memories

Koray Dinçer

Thesis submitted for the degree of Master of Science
Project duration: 9 months

Supervised by Andreas Walther

Department of Physics
Division of Atomic Physics
May 2017

Abstract

Quantum key distribution (QKD) is a secure encryption key generation process to be used by two users in the presence of an eavesdropper. The no-cloning theorem allows the sender "Alice" to securely send qubits with single photons to the receiver "Bob". However, due to real-life imperfections, it is not always possible to have a single-photon source with its properties matching to the quantum memories based on the rare-earth ions. Besides, it might be resource demanding to build and use such a source on our quantum memories. In order to overcome this problem, one can use a special protocol called the decoy state protocol. In the decoy state protocol, it is possible to have a secure communication channel while having a multi-photon source that can send two different states with different photon number distributions.

In this project, the decoy state protocol has been implemented on our current setup to be used in the determination of the efficiencies of the quantum memories. The performance of the quantum memories developed in this group is polarization dependent. Besides, maintaining and detecting the polarization of the qubits is another challenge. Thus, the encoding type of the protocol has been selected to be Frequency-Time (FT), in which the security of the protocol is maintained by the time-frequency uncertainty. Moreover, in this project, a new technique has been introduced, which allows Bob to detect the frequencies of few-photon pulses in the single photon regime. This new technique is based on the slow-light effect, which can be achieved by using special materials, where the speed of light is reduced by 4 to 5 orders of magnitude compared to its speed in vacuum. The speed of light in this special material is frequency dependent, thus, photons with different frequencies will be distinguishable, since they will be separated in time domain. It has been determined that this method gives promising results for the measurements in the field of the QKD. Additionally, this thesis contains some discussions about possible developmental steps which can be used to improve the implemented protocol.

Popular Science Summary

Since the dawn of the first civilizations, the security of information has proven vital to the success of any given community. History records the first attempts at using cryptography techniques in a 1900 BC to 600 BC time frame. In ancient times, the working mechanism of this technique involved the use of letters in the alphabet. To secure the information, these techniques shifted the letters' number in the alphabet, in a way that all letters would be changed to the position determined by the amount of that number. This way, if the shift variable is equal to nine, then the word 'quantum' will be 'zdwcdv'. In ancient times, this was considered to be quite a feat for information security. However, due to the advancement of our computation power, these ancient ciphers would now most certainly be instantly solved. This explains that current encryption techniques, such as RSA, present more complex algorithms in order to secure data flows in digital communication networks. An RSA encryption secures the key by a mathematical process that uses prime factorization. Even though there is no practical way of factoring in two prime numbers using conventional computation techniques, it is not proven that it can not be practical. This notion would explain why the RSA cryptosystem is both an unproven and secure technique. In any case, it is clear that an unconventional quantum computer can easily reduce the processing time of any decryption without the knowledge of any secret variable. We could foresee, therefore, a scenario in which if someone collected all the data encrypted with RSA today, he would be able to brute force it to gain the information whenever quantum computers become available. However, there are some other ways to protect the information. For instance, when using a one-time pad encryption technique, the information has been proven to be secure if the encryption key is securely shared between users. However, the main issue remains, which is that the key should still be shared and securely distributed.

Quantum key distribution (QKD) is an encryption key generation method in which the key is secured by the fundamental laws of physics. In this project, a QKD protocol has been implemented to be used in order to determine the efficiencies of quantum memories. The reason is that the quantum memories can also be used as quantum repeaters, which are necessary to increase the distance between users to metropolitan distances while allowing users to communicate securely.

Additionally, this project proposes a new frequency measurement technique for the sources that send few-photons in each pulse. This technique uses the slow-light effect where the speed of light is reduced by 4 to 5 orders of magnitude compared to its speed in the vacuum. The frequency measurements with this technique gives promising results for the usage of the slow-light effect in the key distribution process.

Acronyms and Abbreviations

QKD - Quantum Key Distribution
FT - Frequency-Time Encoding
PNS - Photon Number Splitting
MDI - Measurement-Device-Independent
CNOT - Controlled-NOT Gate
QBER - Quantum Bit Error Rate
APN - Average Photon Number
EDM - Entanglement Distillation Method
E91 - Ekert91
EPR - Einstein-Podolsky-Rosen
HOM - Hong-Ou-Mandel
FWHM - Full Width Half Maximum
AOM - Acousto-Optic-Modulator
AWG - Arbitrary Waveform Generator
CW - Continuous-Wave
RF - Radio Frequency
Pr⁺³ - Praseodymium Ion
Y₂SiO₅ - Yttrium Silicate

Contents

1	Introduction	1
2	Quantum Key Distribution	4
2.1	Quantum Key Distribution Protocols	4
2.1.1	BB84	4
2.1.2	Decoy-State	8
2.2	Encoding Types	11
2.2.1	Polarization	11
2.2.2	Phase	12
2.2.3	Time-Bin	13
2.2.4	Frequency-Time	14
3	Frequency Measurement in the Single Photon Regime	18
3.1	Spectral Hole Burning	18
3.2	Slow-Light Effect	19
4	Experimental Setup	22
4.1	Alice	22
4.1.1	Dye Laser	23
4.1.2	Acousto-Optic Modulators	23
4.1.3	Implementation of the FT-QKD	24
4.2	Bob	25
4.2.1	Single Photon Detector	26
4.2.2	Cryostat	27
4.2.3	Rare-Earth-Ion Doped Crystal	27
4.2.4	Frequency Measurement	28
4.2.5	Detection Algorithm	29
5	Results	32
5.1	Numerical Simulation of the Decoy-State Protocol	32
5.2	Reducing Intensity to the Single Photon Regime	34
5.3	Time Base Measurements	37
5.4	Frequency Base Measurements	38
6	Discussion	43
7	Conclusion	45
8	Appendix	46
8.1	Ekert91	46
8.2	Measurement-Device-Independent	47

1 Introduction

From the beginning of the first civilizations, security of information was a crucial thing. So far it is known that the very first attempts of cryptography techniques has been used in ancient times since around 1900 BC - 600 BC. However, the first ones that directly aimed to protect the information were the Atbash cipher and the Caesar cipher techniques. Usually, the ancient ciphers were used to protect messages about diplomatic and military matters. Their working mechanism is all about the order of letters in the alphabet. Such as, if one introduces a shift number, the letters in the alphabet will be shifted by the amount of that number. Thus, if the shift is determined as nine, the word "quantum" will be "zdwjcdv". Those ciphers would be solved almost instantly with our current computation power but that was not the case when they were in use. Those ancient techniques were developed to increase the processing time of enemies trying to gather intelligence. Therefore, the communication was not secured for a long time since the size of the encryption key was not long enough.

The need of information security has dramatically increased, since our personal and private information is stored, analyzed and processed via digital communication networks. One can think about this example of a Roman ambassador carrying a letter from Rome to Constantinople. It would take roughly 9 months for him to deliver a page which corresponds to approximately a two kilobytes of digital data. Now we are able to do the same operation in less than a few milliseconds. Conventional encryption techniques such as RSA has more complex algorithms to secure data flows through digital communication networks. RSA [1], which is named after Ron Rivest, Adi Shamir, and Leonard Adleman, is a cryptosystem that allows two users to form a secret common key without announcing it directly. RSA secures the key by a mathematical process which involves prime factorization. There is no practical way of factoring two prime numbers in conventional computation techniques. However, it is not proven that it can not be practical. This leaves the RSA cryptosystem as an unproven but secure technique. RSA usually uses 2048 bits encryption. Increasing the size of the key demands more computation power and, thus, the key size is limited by the computation power of the users. However, an unconventional quantum computer can easily reduce the processing time of decryption without the knowledge of any secret variable using Shor's algorithm [2] [3]. This means that if someone collects all the data which is encrypted with RSA today, he can use brute force to gain the information with quantum computers when they become available. The reason is that for a fixed length of n bit key, one can generate 2^n different keys. However, brute forcing such key with Grover's algorithm [4] will be done in $2^{\frac{n}{2}}$ iterations.

The aim of non-theoretic information security generally depends on the processing time of the eavesdropper. However, in information theoretic security, the encryption is secured even if the eavesdropper has limitless computation power. One-time pad encryption technique is one of them [5]. It has been proven by the information theory that the one-

time pad method is unbeatable¹. In this method, the key size is equal to the size of the message and the key is only used once per message. The problem here is that the key should be shared secretly. Therefore, the key distribution should be done in a secure way.

A practical solution for the key distribution problem is to have a protocol that can warn users about the presence of an eavesdropper while sharing an encryption key. In the presence of an eavesdropper, the shared key will be discarded and the transmission of information will not be initiated. In the absence of an eavesdropper, the generated encryption key will be used and the information will be sent to the receiver to decrypt. The only possible way to access the information, when it is encrypted with an information-theoretic security, is to guess the key. Building up a secure channel is not an easy task since the security of the channel should be unconditional. In other words, it should be invulnerable to every possible attack at any time. This is not possible in classical communications since any data flow can be obtained from the channel.

Quantum key distribution (QKD) is an encryption key generation method in which the key is secured by the fundamental laws of physics. This encryption key is generated by qubits (quantum bit) which are sent by "*Alice*" (*sender*) and received by "*Bob*" (*receiver*) via a quantum channel. The properties of the quantum channel are well-known by the users. In the presence of an eavesdropper ("*Eve*") the error rate of the key will be disturbed. This fluctuation will warn the users whether they are being listened to or not. There are several quantum key distribution protocols with different encoding types that satisfy the unconditional security conditions. However, most of them are not secure due to real-life imperfections of the devices used in the transmission and the detection of the qubits.

In the very first QKD protocols, Alice has a single-photon source which only sends a single photon per pulse. Thus, due to no-cloning theorem [6], Eve will not be able to receive a qubit and send the exact copy of it to Bob. The distance between two users is also a crucial parameter in a QKD system. In this sense, multi-photon sources are open to photon number splitting (PNS) attacks where Eve can have one photon from a multi-photon pulse and let other photons in the same pulse to reach Bob. The decoy-state protocol [7] is specially designed for QKD systems with multi-photon sources. It is also increasing the operation length ² of the channel since the probability of detecting multi-photon signals is higher than the probability of detecting single-photon pulses due to the attenuation of the channel.

The decoy-state is a commonly used QKD protocol/method. Currently, there are many ongoing projects aiming to develop new methods for QKD systems. These projects mostly aim to increase the operation length and the transmission rate of the key distribution. In order to do that one should improve the current state of single-photon detectors and the low-intensity laser sources. Nowadays, it has been shown that the QKD systems can be used for up to 311 kilometers [8]. However, increasing it to ~ 2000 km (metropolitan distance) with fibers seems challenging due to the attenuation of optical fibers. QKD systems are

¹Unbeatable means that an eavesdropper has no chance to obtain the key or the information that has been encrypted.

²Maximum distance between Alice and Bob allows secure key generation.

now also commercially available (e.g. ID Quantique and Toshiba Corp.). They have also been used in various places, for instance, Toshiba's secure genome data transfer lines [9] in Japan.

In this project, a decoy state protocol has been implemented to be used in order to determine the efficiencies of quantum memories. The reason being is that quantum memories can also be used as quantum repeaters. Quantum repeaters are necessary to increase the operation length. The loss of the signal in an optical fiber follows an exponential relation ($\frac{I_o}{I_i} = \exp(-\alpha l)$). It is not possible to amplify the signal due to no-cloning theorem. As a solution to this problem, a quantum network built with quantum repeaters can be used to transmit entangled pairs. In this case, the operational distance will be equal to the maximum distance where the quantum entanglement is possible. In this instance, the maximum distance has no theoretical limit.

Currently, the retrieval efficiency of a quantum repeater developed in our group is 58% [10]. Thus, any quantum repeater developed by this group can now be tested by an actual QKD protocol (frequency-time encoded QKD with decoy-state protocol). Frequency-time (FT) encoding has been chosen for various reasons. One of the reasons is that the performance of a quantum repeater built in a rare-earth-ion-doped crystal depends on the orientation of polarization. Thus, polarization encoding is not a practical type of encoding to be used. Another reason is that phase, time-bin and frequency-bin encoding requires stabilization systems. This project aims at implementing a QKD protocol avoiding any stabilization system, since it would require to design, build and test an entire new setup, and would thereby increase unnecessarily the complexity of the work. Instead I focus on a protocol and an encoding type that allow us to place two detectors in order to find out the retrieval efficiency of the quantum repeaters.

This being said, this thesis report gives brief information about the QKD and some bit encoding types (Chapter 2). In Chapter 3, the thesis proposes a new frequency measurement technique for the sources in the single-photon regime [11]. This technique uses the slow-light effect where the speed of light is reduced by 4 to 5 orders of magnitude compared to its speed in the vacuum. In Chapter 4, the equipment used in the experiments are stated together with the implementation process of the FT-QKD protocol. In Chapter 5 and Chapter 6, one can find the results and the discussions about the experiments conducted in this project. Finally, in order to determine the retrieval efficiency of the quantum repeaters, I propose (as a next step) possible developments and adjustments of the setup.

2 Quantum Key Distribution

Quantum key distribution is a crucial part of information-theoretic cryptography. The very first protocol was introduced by Charles H. Bennett and Gilles Brassard in 1984 [12]. This protocol is frequently used in many QKD systems as well as in this project. The "BB84" protocol requires a single-photon source. The single-photon sources are highly cost demanding and it is challenging to modify its parameters. It also has a short operational distance compared to the other QKD protocols. Thus, after some certain distance, it will be impossible for two users to track the presence of an eavesdropper or even distributing the key itself. Similarly to the BB84 protocol, the "E91" is another protocol that uses single-photon sources. It has been introduced by A. K. Ekert in 1991 [13]. This protocol uses the famous Bell's theorem to distribute the key securely. The E91 and the BB84 give almost the same results experimentally. In this sense, the "decoy-state" protocol has proven to be a giant step in the development of the field. The decoy-state protocol [7] is the first protocol that allows Alice to use multi-photon pulses which are close to the single-photon regime. Decoy-state is not just a standalone protocol. It can also be used with any other protocol since it is currently like a method that allows users to get rid of single-photon sources.

In this project, the BB84 and the decoy-state protocols are used. Therefore, this section of the thesis will mostly focus on these two subjects. However, it is also relevant to keep track of recent developments in the field. Thus, brief information about "Measurement-Device-Independent" (MDI) protocol will also be given (Appendix 8.2). The weakest point of the QKD systems is their detectors. As a consequence, most of the attacks on QKD systems target the detectors. MDI made QKD systems invulnerable to such attacks by moving detectors of Bob to the mid-point and giving Bob a source.

2.1 Quantum Key Distribution Protocols

In this section, one can find brief information about various QKD protocols. Additionally, E91 and MDI is given in the Appendix (Section 8).

2.1.1 BB84

Even though it has been thirty-three years since the publication of the BB84 protocol, it is still the most commonly used protocol. Since, it is simple to implement and easily modifiable. The crucial point of QKD systems is that the signal cannot be copied due to no-cloning theory [6]. One can prove the no-cloning theory by trying to copy a qubit using CNOT (Controlled-NOT Gate) operation [14]. This operation is one part of a universal set of quantum gates. The same operation can be made by a classical computer with two inverters and one OR gate. The input of the CNOT contains two qubits: the control qubit and the target qubit. If the control qubit is $|0\rangle$, target qubit stays the same. In the other case where the control qubit is $|1\rangle$, the bit value of the target qubit will be flipped. (see Table 2.1).

Table 2.1: Input/Output values of Controlled-NOT operation

Input	Output
$ 0\rangle 0\rangle$	$ 0\rangle 0\rangle$
$ 0\rangle 1\rangle$	$ 0\rangle 1\rangle$
$ 1\rangle 0\rangle$	$ 1\rangle 1\rangle$
$ 1\rangle 1\rangle$	$ 1\rangle 0\rangle$

Let's assume that the input is given as the two following states: $|\psi_{unk}\rangle = (a|0\rangle + b|1\rangle)$ and $|0\rangle$. At this point, when CNOT operation is used, it is expected that the unknown input state will be duplicated. Consequently, the input state can be written as follows:

$$|\psi_i\rangle = [a|0\rangle + b|1\rangle] |0\rangle = a|00\rangle + b|10\rangle \quad (2.1)$$

The output state after the CNOT operation is stated below.

$$|\psi_o\rangle = a|00\rangle + b|11\rangle \quad (2.2)$$

Since this operation is aiming to copy the unknown state, one should do a comparison of the output with the duplicated state.

$$|\psi_{unk}\rangle |\psi_{unk}\rangle = a^2|00\rangle + ab|01\rangle + ba|10\rangle + b^2|11\rangle \quad (2.3)$$

In theory, $|\psi_{unk}\rangle |\psi_{unk}\rangle$ should be equal to $|\psi_o\rangle$. However, the only case where they are equal to each other is when $ab = 0$ (situations where $(a=1, b=0)$ and $(a=0, b=1)$ are not taken into account since it makes the state to be a known state). This proves that cloning an unknown state is impossible. Since it is impossible to copy an unknown state, Eve will not be able to interrupt the signal and copy it.

When it comes to qubits one can encode them in different ways. The first BB84 protocols are using the polarization encoding. In this protocol one should have two bases. For instance, the diagonal and the rectilinear polarization orientations can be used as two bases. For instance, if the polarization angle is 0-degrees then it will be representing the state $|0\rangle$. On the other hand, if it is 90-degrees then it will correspond to $|1\rangle$. The same encoding should also be done for the diagonal base. This time the orientation angle 45-degrees represents the state $|0\rangle$ and angle of 135-degrees stands for the state $|1\rangle$. It is clear that one cannot form qubits from any properties of the light. Two qubits formed by two different bases should be indistinguishable. In other words, those bases should be non-orthogonal. An indistinguishable base will also cause a randomness when Bob chooses the wrong base. This gives a significant security tool for the users, since Eve will not be able to tell if she has chosen the wrong or the correct base when she tries to measure encoded qubits.

Now that the encoding of qubits is finalized, the users can follow the procedure of the protocol (see Table 2.2). It all starts with Alice. (a) She chooses random bases and (b) random polarization degrees which have been specified before. (c) Then she sends them one by one to Bob via the quantum channel. (d) Bob chooses random measurement bases and (e) measures the incoming qubits. Then the public discussion starts. Bob reports the arrival of qubits and then (f) he reports the bases that he has chosen. (g) Alice announces the correct base selections of Bob. (h) Then, they reveal a portion of the key for the estimation of the QBER (Quantum Bit Error Rate). QBER is the ratio of non-matching bits in the shared-key to the shared-key size. In Table 2.2, the QBER has been determined as 0%, since there are no errors found in the key. For instance, if one changes the first bit of Bob to "0" then QBER value will be increased to 50% since they reveal two bits and find one unmatched bit. (i) If the QBER is lower than the upper limit of its expected value then they share the remaining qubits as a secret key. After this step, Alice encrypts the information with the shared-key and sends it via the classical channel.

Table 2.2: The BB84 protocol procedure. (R/D: Rectilinear/Diagonal polarization base)

a. Alice chooses random bits	1	0	1	0	0	1	1	1	0	0
b. Alice chooses random sending bases	R	R	D	D	R	D	R	R	R	D
c. Alice sends photons										
d. Bob chooses random receiving bases	R	D	D	R	D	R	D	R	D	R
e. Bob receives and measures qubits	1	-	1	-	0	-	-	1	0	0
f. Bob reports his bases	R	-	D	-	D	-	-	R	D	R
g. Alice announces matching base choices (Shared-Key at this point)	R	-	D	-	-	-	-	R	-	-
	1	-	1	-	-	-	-	1	-	-
h. QBER Check	1	-	1	-	-	-	-	-	-	-
i. Confirmation	-	-	-	-	-	-	-	1	-	-

A basic schematic can be seen in the Figure 2.1. In here, Alice has a single-photon source that can send photons with four different polarization angles via the quantum channel. Then an optical switch directs light into different paths depending on the base selection of Bob. A half-wave plate is placed to let polarization beam-splitter to work properly for the diagonal base measurement. Four single-photon detectors are placed to "click" for every qubit that reaches to the detectors.

A crucial task that should to be taken into account is that Alice and Bob should synchronize their operations. Otherwise, there will be a shift in the generated key and every qubit that has been shifted will introduce error by 50% probability.

The security proof of the BB84 protocol comes from the no-cloning theorem. Additionally, one should prove that the key is secured while the exchange operation is taking place. Entanglement distillation method (EDM) is one way of proving that the BB84 protocol is a secure way of distributing the key [15]. EDM's approach states that entanglement is enough to distribute a secure key. Therefore, it is possible to implement the theory of the BB84 as it is using quantum entanglement. As a proof of security, the von Neumann

entropy will not allow Eve to extract any knowledge from the key. The Von Neumann entropy is shown in Equation 2.4.

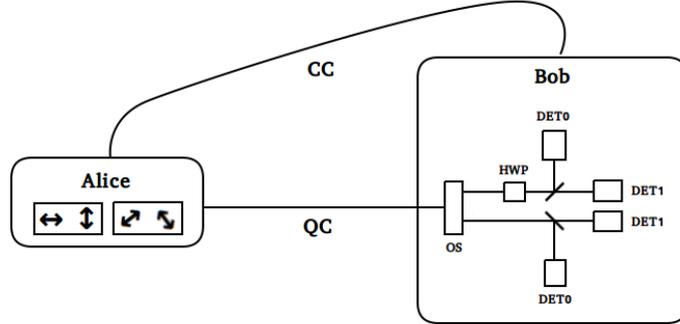


Figure 2.1: A typical schematic of the BB84 protocol. CC: Classical Channel, QC: Quantum Channel, OS: Optical Switch, HWP: Half-Wave Plate, DET0 and DET1: Detectors for $|0\rangle$ and $|1\rangle$ respectively.

$$S = -\text{tr}(\rho \ln \rho) \quad (2.4)$$

where ρ is the density matrix. In the EDM's approach, a state $|\psi\rangle_{ABE}$ represents a system where Alice's, Bob's and Eve's information is kept within. The Von Neumann entropy gives us a clue about the amount of information that has been shared between the users. In this relation, the von Neumann entropy of Eve and Alice+Bob ¹ is zero ($S(\rho_E) = S(\rho_{AB}) = 0$). Thus, it shows that Eve has no idea about the information that Alice and Bob shares. This relation is a result of Holevo's theorem [16] (Equation 2.5):

$$I(X : Y) \leq S(\rho) - \sum_i \rho_i S(\rho_i) \quad (2.5)$$

where $\{\rho_1, \rho_2, \dots, \rho_i\}$ represents a set of mix states and the density matrix is $\rho = \sum_i \rho_i \rho_i$.

This also means that Alice and Bob have no clue about Eve's information. However, this does not mean that the presence of Eve cannot be known by Alice and Bob. It is also possible to determine the amount of information that Alice can share with Bob.

This project focuses on the experimental stage of a QKD system. Therefore, the security proofs of QKDs are not provided in detail. One can find more about this security proofs on the stated references [14][15][16].

Another method of proving the security of the BB84 is called GLLP which is named after D. Gottesman, H. K. Lo, N. Lütkenhaus and J. Preskill [17]. It is used to estimate the key generation rate and the operational distance. The key generation rate is given for several cases where the detector or the source have been targeted by a third party. It is also

¹ ρ_{AB} is the density matrix for the joint system Alice and Bob.

practically useful to use GLLP method since the method also assumes that the source and detector have imperfections. In general, it has been shown that the secure key generation can be written as: [7]:

$$S \geq Q_\mu \{-H_2(E_\mu) + \Omega[1 - H_2(e_1)]\} \quad (2.6)$$

where Q_μ is the gain - which is the ratio of Bob's detection events to the signals sent by Alice (when Alice and Bob choose the same base) - and E_μ is the QBER (when Alice and Bob choose the same base). Ω is the ratio between the gain of the signal state and the gain of a single-photon signal. The $H_2(x)$ is the binary Shannon entropy which equals to $H_2(x) = -\log_2(x) - (1-x)\log_2(1-x)$.

GLLP is modified and used in the decoy-state protocol [7]. Thus, the use of GLLP in the decoy-state protocol will be discussed in the decoy-state section (Section 2.1.2).

2.1.2 Decoy-State

Decoy-state protocol allows users to use a multi-photon source close to the single-photon regime. In other words, users can use a weak coherent source. It has been stated in the BB84 protocol that multi-photon signals are not secured. However, this does not limit the users to track the presence of an eavesdropper. There are at least two types of pulses in the decoy-state protocol. One of them is the signal pulse and the other one is the decoy pulse. The signal state is used for the key exchange and decoy state is only used to track the presence of Eve. In this project, the decoy-state protocol has been used together with the BB84. Instead of using polarization encoding, frequency-time encoding has been used for various reasons, discussed in the section of frequency-time encoding (Section 2.2.4).

It is known that the total photon count in a pulse coming out from a weak coherent source follows the Poisson distribution (Figure 2.2, Equation 2.7).

$$\text{Probability : } p_n = e^{-\mu} \mu^n / n! \quad (2.7)$$

Two different states with different average photon-numbers are necessary for the security of the decoy-state protocol. The main idea is to have the same characteristics for decoy state and the signal state so that they can be indistinguishable. Therefore, the only different parameter should be the average photon number (intensity). This way, Eve can only statistically approach the decision of whether a particular pulse is a decoy pulse or a signal pulse. In this case, one should consider the parameters which depend on the photon number. One of them is the yield Y_n , the probability that Bob detects a signal which contains n-photons. The other one is e_n which is the QBER of an n-photon signal. Obviously, since Y_n and e_n depends only on the photon-number, the following two equations can be written (Equation 2.8 and 2.9).

$$Y_n(\text{signal}) = Y_n(\text{decoy}) = Y_n \quad (2.8)$$

$$e_n(\text{signal}) = e_n(\text{decoy}) = e_n \quad (2.9)$$

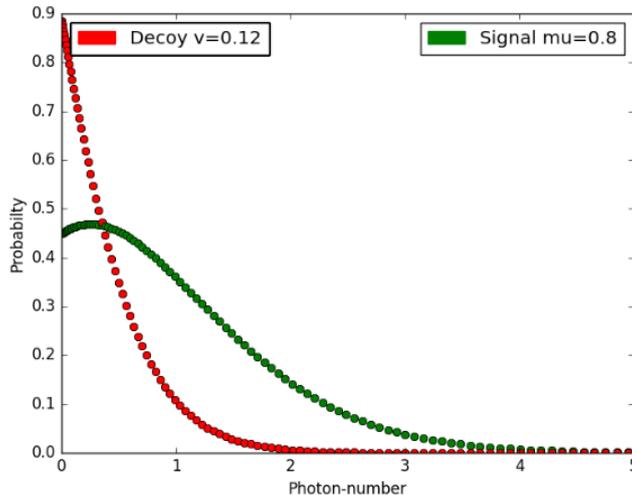


Figure 2.2: A Poisson distribution of the signal state and the decoy state pulses. The red curve represents the decoy state pulses with an average photon number $v = 0.12$ and the green curve represents the signal state pulses with an average photon number $\mu = 0.8$.

The phase of the pulses is also an important parameter. They should be randomized to increase the security of the key since using a non-randomized phase can give Eve a chance to gather some portion of the key [20].

Table 2.3: Some of the crucial parameters in the Decoy-State protocol.

Y_n :	Yield, the probability that Bob detects a signal which contains n -photons.
e_n :	QBER of an n -photon signal.
Q_μ :	Gain, the ratio of Bob's detection events to the signals sent by Alice (when Alice and Bob choose the same base).
E_μ :	Quantum Bit Error Rate (when Alice and Bob choose the same base).

Once the above conditions are satisfied, the relation between the Q_μ and the Y_n , and between E_μ and e_n will be linear (see Table 2.3). Then users can measure Q_μ and E_μ to track the fluctuations of Y_n and e_n . Alice and Bob should specify a reasonable range for the values of the gain and the QBER where the secure key exchange is possible. If Eve interrupts the channel and re-directs a photon in a multi-photon pulse to herself, then her actions will affect the gain and the QBER.

In order to find a suitable range, one should consider the worst case, where every single-photon pulse is absorbed in the channel (due to attenuation) and every multi-photon pulse reaches to Bob. In this case, Eve can obtain every single-photon pulse that will be lost due to the attenuation in the channel. In accordance to this case, the lower bound of Y_1 (or Q_1 see Equation 2.10) and the upper bound of e_1 should be estimated [18] [19]. The key generation rate (per pulse) can be found by the lower and upper bounds. Thus,

the optimum parameters of μ , v and the percentage of the signal pulses (N_μ) and the percentage of decoy pulses (N_v) can be found.

$$Q_i = Y_i \frac{\mu^i}{i!} e^{-\mu} \quad (2.10)$$

It is possible that one can put infinitely many different decoy states to the protocol. Frequently used types are the one-decoy and the weak+vacuum protocols. In the one-decoy protocol, there is only one decoy state that is being used. On the other hand, in the weak+vacuum protocol there are two decoy states, where one of them is a vacuum state that is used to track the noise in the channel.

In the one-decoy state, Alice should send a decoy state with an average photon number v which should be less than the signal's average photon number μ . For the one-decoy state protocol the lower bound of Q_1 and the upper bound of e_1 is given as [20]:

$$Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu v - v^2} (Q_v^L e^v - Q_\mu e^\mu \frac{v^2}{\mu^2} - E_\mu Q_\mu e^\mu \frac{\mu^2 - v^2}{e_0 \mu^2}) \quad (2.11)$$

where $Q_v^L = Q_v (1 - \frac{u_\alpha}{\sqrt{N_v Q_v}})$ and u_α represents the statistical deviation value which has been taken as 10.

$$e_1^U = \frac{E_\mu Q_\mu}{Q_1^L} \quad (2.12)$$

N_v is the total decoy state pulse count and e_0 is the QBER of a vacuum signal which is equal to 1/2. After determining the bounds of the protocol, one can also estimate the lower bound of the key generation rate;

$$R^L = q \{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1^L [1 - H_2(e_1^U)]\} \quad (2.13)$$

where q is 1/2 for the BB84 protocol (since the probability of Bob choosing the right base is 1/2) and $f(E_\mu)$ is the error correction efficiency value which is usually taken as 1.22.

In the weak+vacuum protocol, the method for estimating the upper and the lower bounds is similar to the one-decoy protocol's method. The lower bound of Q_1 is given as [20]:

$$Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu v - v^2} (Q_v^L e^v - Q_\mu e^\mu \frac{v^2}{\mu^2} - Y_0^U \frac{\mu^2 - v^2}{\mu^2}) \quad (2.14)$$

where $Y_0^U = Y_0 (1 + \frac{u_\alpha}{\sqrt{N_0 Y_0}})$ and the upper e_1 is given as:

$$e_1^U = \frac{E_\mu Q_\mu - e_0 Y_0^L e^{-\mu}}{Q_1^L} \quad (2.15)$$

where $Y_0^L = Y_0 (1 - \frac{u_\alpha}{\sqrt{N_0 Y_0}})$. The secure key generation rate of both protocols is the same (Equation 2.13).

2.2 Encoding Types

In this section, brief information about some of the encoding² types is provided. There are many encoding types one can use. However, this project aims to work with the quantum memories developed in *Lund University Quantum Information* group. The quantum memories developed in this group are based on rare-earth-ions [10]. Thus, the encoding type chosen is frequency-time since it has been determined that frequency-time encoding is the most practical one for our setup. In every subsection, a discussion about the usability of the corresponding encoding type can be found.

2.2.1 Polarization

Polarization encoding is a commonly used encoding technique in the quantum key distribution field. As it is the most used technique, nearly all of the protocols that have been proposed use polarization encoding. For instance, BB84, E91, decoy-state, and MDI use polarization encoding. However, it is possible to change their encoding type. One reason for polarization encoding to be this popular is that it is easier to modify the polarization of a photon compared to any other its properties. Basically, Alice can set up a polarization modulator to modulate polarization in four different orientations (Figure 2.3).

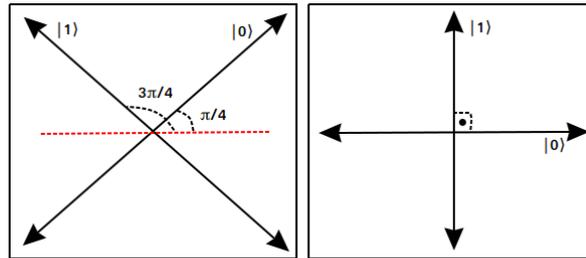


Figure 2.3: Polarization encoding scheme that is introduced in the BB84 protocol.

It is also possible to generate Bell states with the polarization bases. A key figure in quantum key distribution is to have a stable channel. However, polarization encoding is not the best option to use when it comes to the stabilization. In many cases, it has been reported that the channel properties, such as QBER, starts fluctuating after some time of transmission. This fluctuations are coming from the change in the polarization angle of photons when they have been sent through a fiber. It is possible to remove this effect by using polarization maintaining fibers. However, it should be stated that the telecommunication network does not have polarization stabilization. The most useful application of using the polarization encoding is a free-space transmission. The latter is being developed to securely share a key between users while one of them is on a satellite [24], since maintaining polarization through the air is easier.

²Encoding is a technique to convert the information into qubits.

Because the quantum memories developed in this group are polarization dependent, the polarization encoding is not a suitable type for this project. The main reason behind this is that the techniques used for generating a quantum memory contain the spectral hole burning method and other operations that excite ions to higher energy levels. Those operations are maintained by light-matter interactions which contain absorption. Another reason is that the fibers in our laboratory do not have polarization stabilization. Absorption of light by those ions is polarization dependent. Hence, a photon encoded with polarization will be affected differently depending on the encoded information. For instance, the crystal which is used to form a quantum repeater has the principle axes of b , D_1 and D_2 [10]. Depending on the correlation between the polarization angle and the principal axes, the absorption coefficient changes. Therefore, the efficiency of the quantum repeater will change dramatically depending on the information sent. Considering the current methods and reasons stated, using the polarization encoding on our rare-earth-ion based quantum repeater setup needs some modifications such as using two quantum memories together as it has been proposed in the following articles [41] [42] [43].

2.2.2 Phase

Phase encoding is another commonly used encoding type. It has been first introduced by C. Bennett (also known by his work in the BB84 protocol [25]). A phase encoding requires an interferometer. Usually, an interferometer is built with fibers for practical reasons. Simply by adding a phase modulator to one arm of the interferometer, one can encode the information in phase. In the BB84 protocol, Alice modulates the phase in one arm of her interferometer. Then Bob also modulates the phase of the light which Alice sent (Bob's measurement base selection).

Table 2.4: Scheme of the phase encoded BB84 protocol [26].

Alice's Bit	ϕ_A	ϕ_B	$\phi_A - \phi_B$	Bob's Bit
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$?
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$?
0	$\pi/2$	0	$\pi/2$?
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$?
1	$3\pi/2$	$\pi/2$	π	1

Depending on the outcome, Bob determines the value of the bit. Alice can modulate her light by applying following phase shifts: $\phi_{A1} = 0$, $\phi_{A2} = \pi/2$, $\phi_{A3} = \pi$ or $\phi_{A4} = 3\pi/2$. Here, ϕ_{A1} and ϕ_{A2} represent the bit value of "0", and ϕ_{A3} and ϕ_{A4} represents the bit value of "1". Bob also varies the phase of incoming light, by $\phi_{B1} = 0$ or $\phi_{B2} = \pi/2$. After applying his own phase shift value, Bob splits the light into two detectors. Depending on

the phase difference applied by Alice and Bob, the probability of light taking one specific output changes. Hence, depending on the encoded bit, a click in the detector "0" or "1" occurs (Table 2.4).

This thesis project does not involve any stationary setup, hence the installation of the setup in the laboratory should be simple. However, phase encoding requires at least one interferometer. This interferometer should be very stable with a path length difference that should not change more than the wavelength of the photons [26]. Otherwise, it will affect the phase of the light and it will introduce an additional error rate. In our case, setting up an interferometer which is stable less than 606 nm (wavelength of the source) will require stabilization systems. Additionally, it will not be practical to install such system in the laboratory for this project.

2.2.3 Time-Bin

Time-bin encoding type is another common method to share information. In this part, a time-bin encoding with an entanglement will be discussed. There are many ways to create an entanglement, such as using parametric down-conversion or two-photon interference (Hong-Ou-Mandel effect). Entanglement is also used in the security proof of the BB84 even though it is not necessary to have entangled photons. The bit value is determined by a pulse which arrives early or late. One can form up an interferometer with a short and a long arm. If the photon passes from the short one it will be in state $|0\rangle$. On the other hand, if it passes from the long arm, it will represent the state $|1\rangle$. For instance, entanglement created by a parametric down-conversion through a non-linear crystal can be used[27]. Since the interferometer has two arms with different lengths, it will introduce a delay (phase). Thus, it will represent the state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B - e^{i\phi} |1\rangle_A |1\rangle_B) \quad (2.16)$$

The entangled photons are sent to Alice and Bob separately for the measurement of the generated states. Depending on the phase difference introduced by the first interferometer (Pump interferometer in Figure 2.4), Alice and Bob should balance the phase difference in their measurement setups with interferometers.

The measured states are given in the lower insets of the Figure 2.4. The detectors are tracking three different time intervals, where the satellite peaks¹ correspond to the paths taken by a photon until it reaches to the detectors of Alice and Bob. In Alice's case, the first satellite peak represents a photon which passed through the short arm of both interferometers ($|0\rangle$). Similarly, the second satellite peak represents a photon that passes from the long arms of both interferometers ($|1\rangle$). A click in the central peak can be any photon that passes through one short and one long arm. In this case, since the photons hitting to both detectors are entangled, they can record the counts in the central peak and decide together if the outcome is the state $|0\rangle$ or $|1\rangle$. For instance, if Alice detects the

¹The satellite peaks corresponds to temporally distinguishable states.

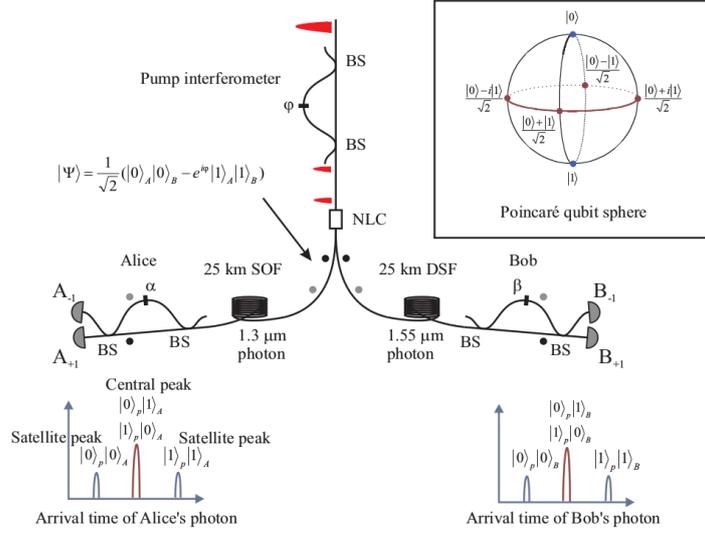


Figure 2.4: A time-bin configuration with entanglement used with telecommunication wavelengths. (Figure taken from [27] with permission, copyrighted by the American Physical Society)

photon in the first satellite peak, she will be sure that the detected photon has passed from one short and one long arm. Thus, Bob can use Alice's central peak counts to determine the state encoded depending on his detections for the same entangled photon. In other words, to be able to decide, they should arrange the path-length differences in each interferometer accurately. Therefore, the interferometers should be stabilized which makes this encoding type hard to maintain for our project.

Frequency-bin encoding is also a similar encoding type. Instead of encoding information based on the arrival times of photons, the shifts in frequencies is used. However, it also has a similar setup scheme to Time-bin encoding which is again not practical to use in this project.

2.2.4 Frequency-Time

So far several types of encoding of information have been discussed. None of them managed to fulfill the criteria of having a compact easy-to-install setup. Frequency-time (FT) encoding is fulfilling this criteria by using arrival time of photons and their frequencies. It has been stated that the FT-QKD setup does not need any stabilization or any interferometers [28]. It is also reasonable to use this encoding type since the stationary equipment in our laboratory is able to modify many properties of light, such as intensity, frequency, arrival-time, phase etc.

The frequency-time encoding relies on the BB84 protocol in which users need to create four different states to encode the information. Let us assume that Alice has two different coherent light sources with different central frequencies where f_0 represents the state $|0\rangle$

and f_1 represents the state $|1\rangle$. She sends the pulses within some time frame which is known by Bob. When she chooses the frequency base, she sends the signal at time t_c . In the case where Alice chooses the time-base, she sends the pulses at time t_0 which corresponds to state $|0\rangle$. On the other hand, if she sends it at time t_1 , it represents the state $|1\rangle$. The photons that she sends encoded in time base should have the same frequency which is centered at $f_c = (f_0 + f_1)/2$. Similarly, the photons that she sends encoded in frequency base should have the arrival time $t_c = (t_0 + t_1)/2$. The security of frequency-time encoding comes from the frequency-time uncertainty. Therefore, if Eve or Bob measure an incoming pulse using the wrong base, they will not be able to tell that they have chosen the correct or the incorrect base (until Alice declares her base choices). It is important to note that, when a state is measured in the wrong base, there should be 1/2 probability for the measurer to get one specific bit value. This is maintained by specifying the values of t_0 - t_1 and f_0 - f_1 such that the pulses will overlap. (Figure 2.5). Thus, the measurement at the point t_c or f_c will not give any information about the base choice of Alice to the measurer.

There are several parameters that one should consider. Those are obviously the t_0 , t_1 , f_0 and f_1 . It is also crucial to know the full width half maximum (FWHM) of the pulses in both time and frequency domains (δt , $\delta \tau$, δf and $\delta \nu$ (ref. to Figure 2.5)). The pulses assured to be Fourier-limited. Hence, the following relations can be given:

$$\delta \nu = 0.44/\delta t \quad (2.17)$$

$$\delta \tau = 0.44/\delta f \quad (2.18)$$

In order to fulfill the frequency-time uncertainty, the following relations should be satisfied:

$$\delta f < \Delta f \quad (2.19)$$

$$\delta t < \Delta t \quad (2.20)$$

where $\Delta f = (f_0 - f_1)$ and $\Delta t = (t_0 - t_1)$.

The FT-QKD protocol procedure starts with the transmission of qubits sent by Alice. Then Bob confirms the arrival of qubits and declares his choices of measurement bases. Then Alice announces her base choices and pulse types (if the decoy-state has been used). They estimate the error rate and, in the absence of Eve, they use the key for encrypting and decrypting the information. QBER of the protocol is a crucial parameter for the security of the shared-key. It should be less than 11% as it is stated in the BB84 security proof (In Equation 2.6, if it is assumed that a single-photon source has been used then Ω and μ will be equal to one. Thus, the equation becomes $1 - H_2(e_1) = 0$ and e_1 has an upper limit of 11%.) This limit is only defined for single-photon sources. If a weak-coherent source has been used then the calculation becomes much more complex. The security proof of FT-QKD with a weak coherent source has been given by the following articles [29] [30] [31]. However, in this project a fair assumption has been done by stating that the error

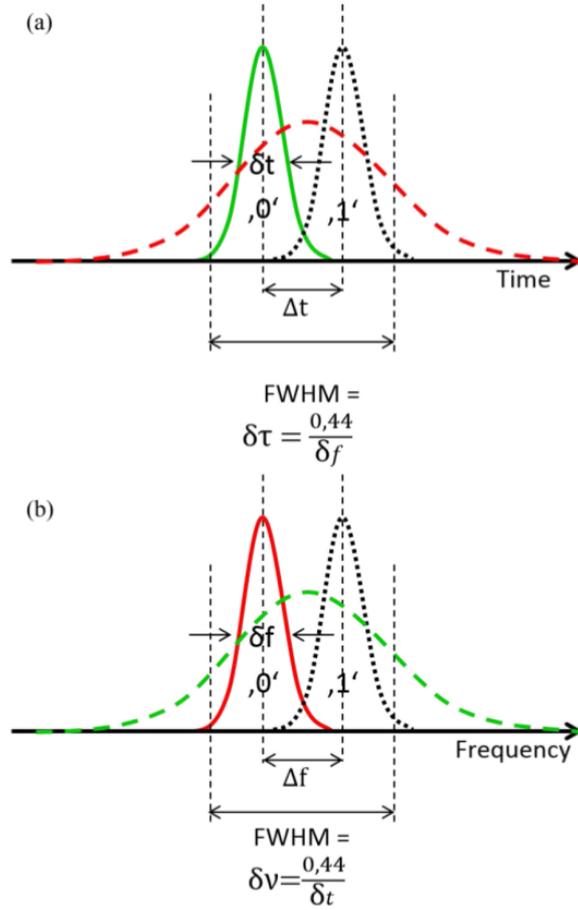


Figure 2.5: FT protocol scheme with Gaussian pulses. **a.** Pulses in time domain where the dashed line corresponds to the arrival time of pulses encoded in frequency base. **b.** Pulses in frequency domain where the dashed line corresponds to the frequency of pulses encoded in time base. (Figure taken from [28] with permission, copyrighted by the American Physical Society)

should be less than 11%. A weakness of the FT-QKD comes from the uncorrelated pulses. Thus, Eve can limit herself to measuring narrow intervals in time (or frequency) which are close to the peaks of each pulse. Thus, she can obtain some portion of the key without being noticed. However, this is also the case in the BB84 protocol. Since Eve can always perform a one-stage attack and obtain a small portion of the key. Compared to the BB84 protocol, the FT-QKD protocol allows Eve to access more information than the BB84 with one-stage attacks.

FT-QKD also allows users to use a larger alphabet to encode information. In the polarization encoded BB84, there are four bins that are being used. From the following relation, it is possible to determine the value of information bits that a pulse can carry.

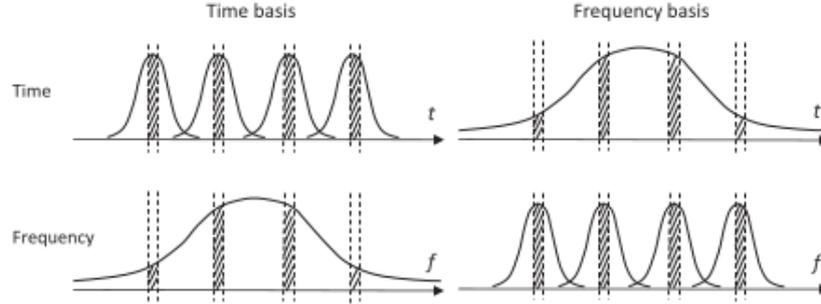


Figure 2.6: FT protocol scheme with a larger alphabet-size. Dashed areas indicates possible attacks of Eve to obtain some bit information from the key. (Figure taken from [31], copyrighted by the Taylor & Francis)

$$N = \log_2(M) \quad (2.21)$$

where M is the encoding bin count. In FT-QKD it is possible to extend M to infinity, which allows users to use more than two information bits (alphabet-size)(Figure 2.6) [31] [34].

Let us now discuss the usability of FT-QKD in this project. The frequency of our source is 606 nm and the optimum δt is 500 ns. Thus, the upper limit of δv is around 0.8 MHz (Equation 2.17). It is not an easy task to measure such frequency difference in the single-photon regime. A similar problem has been stated in a frequency-bin QKD, where acousto-optic-modulators (AOMs) have been used to shift the frequencies of the pulses [32] (as AOMs have also been used in this project to shift frequencies). It has been stated by the authors that an ultra-narrow dual-transmission-band fiber Bragg grating might be used to detect frequency shifts in the order of few megahertz. However, this type of fiber Bragg grating is developed only for optical telecommunication wavelengths ($\sim 1.5\mu m$). As a result, measuring the frequency in the single-photon regime is the most challenging part of this project and has been discussed in the next chapter (Chapter 3).

3 Frequency Measurement in the Single Photon Regime

The FT-QKD protocol consists of two domains, time and frequency, where the information is encoded in. Measuring the arrival time of photons is an easy task since a single-photon detector will click whenever a photon hits to the detector. In this thesis, for the first time, the frequency measurement that uses the slow-light effect for single-photon pulses is proposed (to be used in QKD systems) [11]. This new method allows users to determine the frequency of a photon by measuring their arrival times.

3.1 Spectral Hole Burning

The spectral hole burning has been used to generate the slow-light effect. In this section, the usage of rare-earth-ion-doped crystals in QKD measurements will be discussed. In a rare-earth-ion-doped crystal, due to different positions of the ions placed in the crystal, an inhomogeneous broadening exists. This means that every ion has a different frequency in the absorption spectrum. Thus, one can interact with those ions one-by-one and excite them to higher electronic energy levels with a laser.

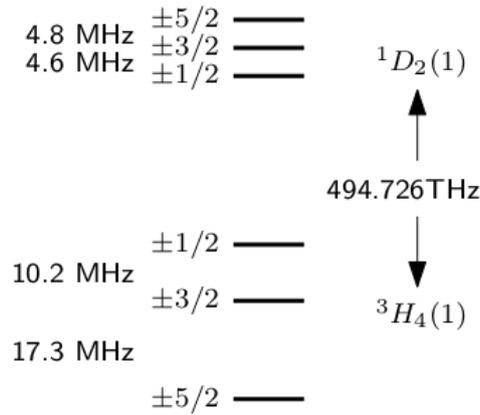


Figure 3.1: The hyperfine energy level structure of Pr^{3+} (Figure taken from [35] with permission).

The excited ions might return to the same energy level after a short time. Thus, one should excite them for several times. Since all the ions in the laser's frequency will be excited at some point there will be no ions left in the targeted frequency and it will create an spectral pit. This is a crucial thing to have in a detection setup, especially in the single-photon regime since any photon loss will cause a reduction of detection efficiency. In an experimental approach, a focused laser beam passing through the crystal will excite the ions to upper energy levels. If one continuously modulates the frequency of the laser (frequency scan) then all the ions in the frequency scan interval will be excited to higher energy levels. As a result, there will be an spectral pit with the width equal to the frequency scan interval. The crystal used in this project is $Pr^{3+} : Y_2SiO_5$ and its hyperfine energy

level structure is shown in Figure 3.1. Overall, the entire splitting of ground states is 27 MHz. However, due to relative positions of the excited states (~ 9 MHz total splitting), the maximum achievable pit width has been reduced to ~ 18 MHz [35].

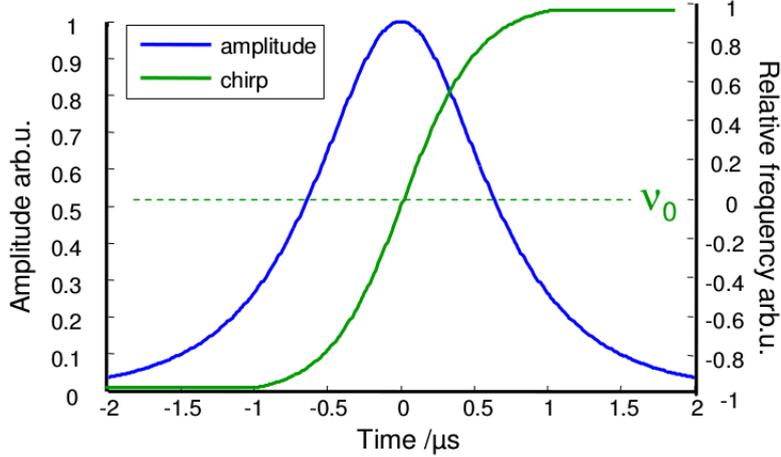


Figure 3.2: A hyperbolic secant pulse with the its amplitude and its relative frequency vs. time. (Figure taken from [35] with permission.)

It is possible to have different types of frequency scans. It has been stated that hyperbolic secant pulses (Figure 3.2) are much more convenient while being used in inhomogeneously broadened structures [35] [36] [37]. The reason is that a hyperbolic secant pulse has a very high transfer efficiency, which affects all the ions in the same way. Additionally, it gives a low transfer efficiency to the ions outside of the frequency scan which allows us to form better (steeper edged) absorption pits.

Reading-out this absorption profile is fairly simple. A broader frequency scan can be done to detect the transmitted light that passes through the crystal. Therefore, the spectral pit will be visible, since only the unabsorbed light will be able to pass through the crystal.

3.2 Slow-Light Effect

The slow-light effect reduces the group velocity of light while passing through a medium. This effect is frequency-dependent when the slow-light effect is generated by a spectral pit. The reason is that in the spectral pit, the dispersion has a positive value. Thus, it slows down the velocity of light. It has been reported that it is possible to reduce the velocity of light down to 17 meters per second [38].

In a theoretical approach, one can use Kramers-Kronig relations to determine the frequency-dependent refractive index (Equation 3.22).

$$n(\omega) = 1 + \frac{X'(\omega)}{2} + i\frac{X''(\omega)}{2} \quad (3.22)$$

where $X(\omega)$ is the susceptibility:

$$X(\omega) = \frac{i}{\pi} \int \frac{X(\omega')}{(\omega - \omega')} d\omega' \quad (3.23)$$

$$X'(\omega) = -\frac{1}{\pi} \int \frac{X''(\omega')}{(\omega - \omega')} d\omega' \quad (3.24)$$

$$X''(\omega) = \frac{1}{\pi} \int \frac{X'(\omega')}{(\omega - \omega')} d\omega' \quad (3.25)$$

Absorption can be also given as:

$$\alpha = \frac{\omega}{c} X''(\omega) \quad (3.26)$$

Equation 3.22 can be written as follows by using Equations 3.23-3.25:

$$n(\omega) = 1 + \frac{c}{\pi} \int_0^\infty \frac{\alpha(\omega')}{(\omega'^2 - \omega^2)} d\omega' \quad (3.27)$$

By using this relation one can actually numerically simulate the group velocity of the light in a spectral absorption pit (Figure 3.3) and also the refractive index. Here, the x-axis shows the relative frequency in reference to a 606nm laser's frequency. (Figure 3.4).

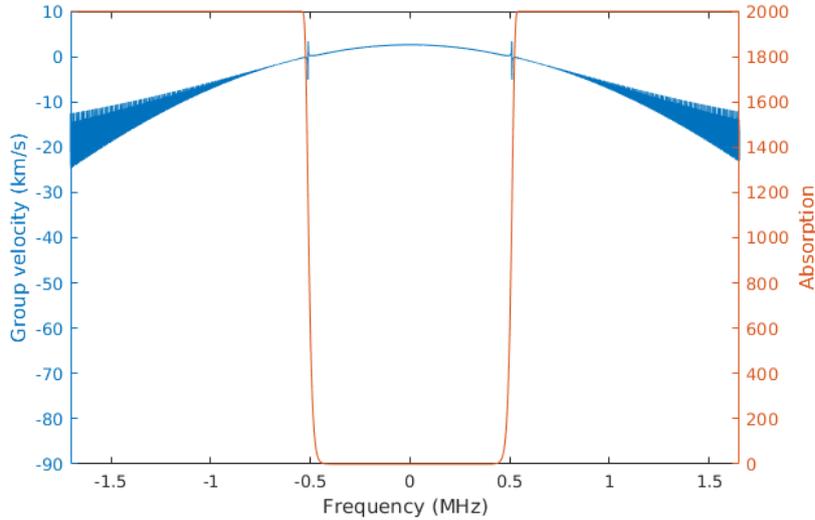


Figure 3.3: Numerical simulation of slow-light effect in a spectral absorption pit with 1MHz width. Figure shows the relation between phase velocity and frequency. [39]

In the Figure 3.3 and Figure 3.4, the results of the numerical simulation of a spectral pit are given. As it can be seen from the refractive index profile the dispersion is positive in the pit. Thus, the velocity of the light is slowed down. Depending on the frequency of the incoming light, the group velocity changes. This difference delays the light in different

durations depending on their frequency. In other words, depending on the arrival time of a photon, one can determine its frequency. The separation in time can be expressed as:

$$t_{sep} = \frac{L}{v_g(f_0)} - \frac{L}{v_g(f_1)} \quad (3.28)$$

Here, L is the length of the crystal and f_0 and f_1 is the frequency of pulses sent by Alice which are encoded in the frequency base (Section 2.2.4).

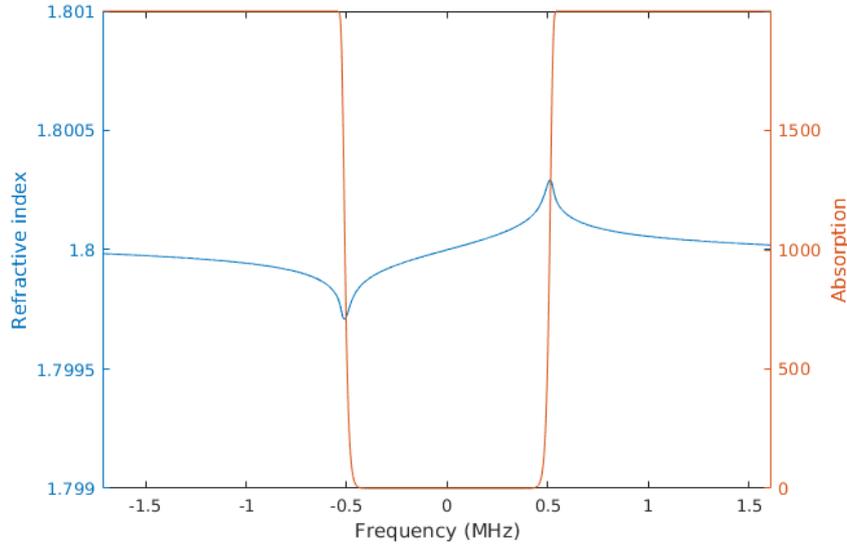


Figure 3.4: Numerical simulation of slow-light effect in a spectral absorption pit with 1 MHz width. Figure shows the relation between refractive index and frequency. Here, x-axis shows the relative frequency in reference to a 606nm laser's frequency. [39]

In our case, we expect to have a separation between two pulses in different frequencies (for FT-QKD). Thus, a relatively large group velocity difference is needed. This can be done by forming the spectral hole in a specific interval which will position the central frequency of one pulse to the center of the pit and the other pulse to the edge of the pit. Considering this fact, the edges of the pit should be as steep as possible to increase the transmission of the pulse. Every absorbed photon will reduce the gain (Q_μ) of the protocol. As a result, it will reduce the key generation rate. Another consequence of steeper edges is that it will make the group velocity difference (between the center and the edge) larger.

In conclusion, one should determine the frequencies of pulses accurately so that it will position them in the pit to get the optimum group velocity difference. The spectral hole burning operation should be also precisely performed to get the steepest pit edges.

4 Experimental Setup

In this chapter, one can find the description of the equipment that has been used to implement the FT-QKD protocol together with the information about the experiments that have been conducted. This section has been divided into two: Alice and Bob. In Alice's section, a brief information about the dye laser and AOMs have been given together with their usage in the implementation process. In Bob's section, the detection process of the time bins and the frequency bins have been given. Also, the detection algorithm and the synchronization of Alice and Bob have been given in the Sections (4.1.3) - (4.2.5). One should note that the setup has been changed for various different tests. Therefore, one can find the corresponding schemes of the test setups in this chapter.

4.1 Alice

Alice is the key generator and the transmitter. The key should be generated with perfect random bits (i.e. Quantum Random Number Generators). Then, the key should be encoded to form qubits with random base selections. This process has been maintained by an Arbitrary Waveform Generator (AWG) which controls two AOMs. Both of the AOMs have been used to control the intensities of the pulses. The setup of Alice is shown in Figure 4.1.

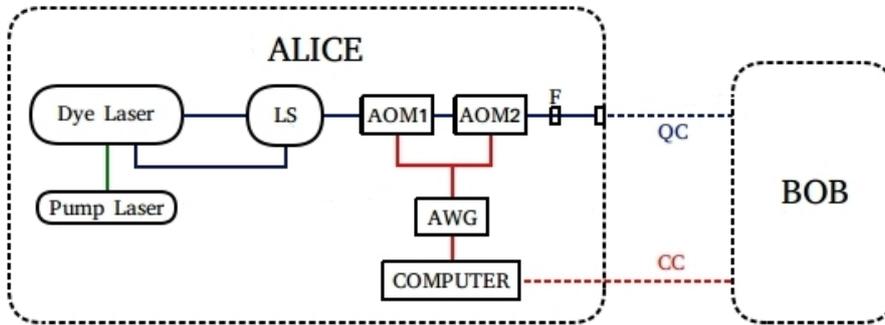


Figure 4.1: Schematic of Alice for the implementation of FT-QKD protocol. LS: Locking System, AOM1/AOM2: Acousto-Optic-Modulator, AWG: Arbitrary-Waveform-Generator, F: Filter/Attenuator, QC: Quantum Channel, CC: Classical Channel.

There have been several developmental steps taken in Alice's device. The first step was to control both AOMs to reduce the intensity of the laser to the single-photon-regime. After successfully reducing the intensity to the single-photon-regime, the pulse sequence, which consists of the qubits, has been generated.

Our laser source is also responsible for creating the spectral absorption pits for the frequency measurements. Since creating the spectral pits requires relatively high intensity, the filter in the setup has been removed during the frequency measurement tests (Section 4.2.4). Additionally, the locking system has been used to lock the frequency of the laser.

4.1.1 Dye Laser

The dye laser is one of the main optical elements of Alice. In this project, a continuous-wave (CW) dye laser has been used. The wavelength of the laser is 606 nm, which has been determined by the dye (Rhodamine 6G) and several intra-cavity stages. The temperature of the dye has been fixed to 10°C by a temperature controller. The pump of the laser is a neodymium laser with 532 nm wavelength and its power has been fixed to 6 W, while the output power of the dye laser is around 400 mW.

The frequency stabilization of the dye laser has two components. The dye laser contains an internal and an external stabilization systems. The internal stabilization system is able to stabilize the frequency of the laser within ~ 1 MHz. On the other hand, the external locking system is able to lock the frequency within ~ 10 Hz [40]. Hence, the external locking system has been used to generate spectral pits and the qubits for the frequency base.

A stable output from the laser is also a crucial property of Alice. It has been observed that the intensity of the laser has fluctuations. Thus, one can see some disturbances in the average photon number values of the pulses in the single-photon-regime. The stabilization of the intensity can be achieved if needed. However, it has not been used in this project since the intensity fluctuations of the laser does not change the Poisson distribution in the single photon regime. The intensity stabilization might be used in future for a developmental work to this project.

4.1.2 Acousto-Optic Modulators

It has been stated before that the AOMs are the main optical elements of Alice. They have been used to reduce the intensity to the single-photon-regime and encode the information in time and frequency bases. The first AOM has a center frequency of 210 MHz and the second AOM has a center frequency of 360 MHz. The first AOM is a double-pass AOM (Figure 4.2) in which the light passes two times through it.

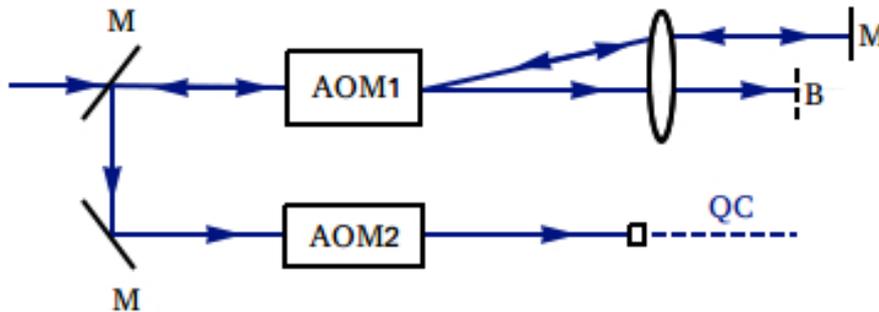


Figure 4.2: Schematic of the double-pass AOM and the single-pass AOM. M: Mirror, B: Beam block and QC: Quantum channel.

The double-pass AOM has been used to shape the pulses, where the generation of the

Gaussian pulses takes place. The second AOM is a single-pass one, which controls both the frequency and the intensity. The output intensities of the AOMs have been calibrated with the Rabi frequency values of specific transitions. Thus, the intensity of Alice has been determined with the Rabi frequency given by the user. The AOMs have been controlled by an arbitrary-waveform-generator. AWG is a device that sends radio frequency (RF) signals to the AOMs, which are then transformed to sound waves by the drivers within the AOMs. The AWG has been controlled by a computer using a "LabView" software. This software reads an output of a MATLAB code and then sends the created pulse sequences to the AWG. Therefore, the pulses are pre-determined by the output of the MATLAB code.

4.1.3 Implementation of the FT-QKD

In this thesis, the laser source has two tasks. The first task is to generate a key and then transmit it to Bob (Alice). The second task is to create a spectral pit for frequency measurements of Bob. In this section, the implementation of the FT-QKD has been given. Therefore, this section contains only the information about the first task of Alice. The setup and the procedure of the second task has been given in the frequency measurement section (Section 4.2.4).

The most crucial part of the decoy-state protocol is to have a weak coherent source. Thus, Alice should reduce the intensity of the dye laser to the single-photon-regime. Hence, both of the AOMs have been used to reduce the intensity to the lowest possible value. A photodiode detector is placed to measure the intensity of Alice. The voltage output of the detector has been used to estimate the total photon count in a pulse. If the calibration of the AOMs is accurate then the relation between the Rabi frequency and intensity should follow the relation below:

$$I_o \propto \Omega^2 \quad (4.29)$$

where, I_o is the output intensity of an AOM and Ω is the Rabi frequency. In our case, this relation can be written as:

$$I_o \propto \Omega_1^2 \Omega_2^2 \quad (4.30)$$

where, Ω_1 and Ω_2 are the input Rabi frequencies¹ of the AOMs. The photodiode is unable to detect few-photon pulses even with 10^7 gain option. Thus, one should use a single-photon detector to detect few-photon pulses. The single-photon detectors have a damage threshold value, which is close to the few-photon level. This means that any bright pulse that hits the detector will damage the detector. Therefore, it is crucial to measure the intensities for different Rabi frequencies to compare it with the relation stated in the Equation 4.29 and in the Equation 4.30. The measured intensity values should follow the calibration relation for the estimation of a secure intensity interval. After obtaining satisfactory results, the single-photon detector has been placed in our setup to determine

¹Here, the Rabi frequency is only an input parameter that has been determined by a calibration process. This input parameter has been used to control the intensity and does not state the actual Rabi frequency.

the average photon numbers for corresponding Rabi frequencies of the AOMs. This measurement is also necessary since the decoy-state protocol assumes the output of Alice to follow the Poisson distribution.

After the calibration and the estimation processes, one can now encode the key in qubits. As the FT-QKD protocol uses the Gaussian pulses, those pulses have been generated in both frequency and time base. It should be stated that the generated Gaussian pulses should follow the relations of the FT-QKD protocol for the security proof (see Section 2.2.4). The random key has been generated in a MATLAB code, which also has been used to control the AOMs. This procedure starts with generating the random key. After the generation of the random key, Alice randomly¹ determines the pulse type which can be the signal state, the decoy state or the vacuum state (weak+vacuum decoy-state protocol). Afterwards, Alice randomly selects the base (frequency or time). Depending on the outcomes of the random choices, Alice prepares the pulses. Those prepared pulses are saved in a file that the AWG can access and read. All base choices of Alice have been saved into a file that has been stored in a network for the public discussion (Table 4.1).

Table 4.1: An example of the procedure of Alice in the implemented FT-QKD protocol.

Alice generates the random key	1	1	1	0	1	1	0	1	0	0
Alice randomly chooses the pulse types	S	S	S	S	D	S	D	V	S	D
Alice randomly chooses the base types	F	T	T	F	T	F	F	F	T	T
Alice stores the shared key	1	1	1	0	-	1	-	-	0	-

The implemented protocol has been tested in time-base, where Alice always chooses the time-base to encode the key. A numerical simulation has been used to estimate the optimum parameters of the pulses which can be used in the implemented protocol. For the frequency base measurements, the bright pulses have been used.

4.2 Bob

In our experimental setup for the FT-QKD protocol, Bob is the receiver. Thus, the detection is made in his side. There are two different types of measurements that Bob should do. One of them is the detection of the arrival times of the photons that can be done with the single-photon detector directly. The other one is the measurement of the frequency. This has been done with the slow-light effect, which allows Bob to determine the frequencies of the photons by their arrival times.

The frequency base measurements and the time base measurements have not been conducted at the same time. However, an ideal setup of Bob can be formed by building the setup in the Figure 4.3. In this setup, Bob directs the incoming light from Alice to the cryostat, if he chooses the frequency base. In the other case, he directs the light to a

¹It has been randomly selected by the given probability of each pulse type. In this case, the following properties are given. 60%: Signal, 30%: Decoy and 10%: Vacuum.

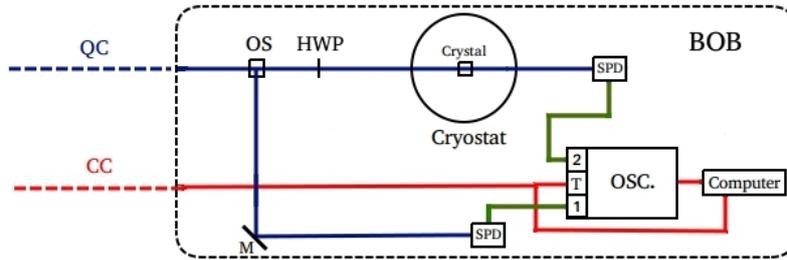


Figure 4.3: An ideal schematic of Bob for the implementation of FT-QKD protocol. M: Mirror OSC.: Oscilloscope (1: Channel 1, 2: Channel 2, T: Trigger), SPD: Single-Photon-Detector, HWP: Half-wave plate OS: Optical Switch, QC: Quantum Channel, CC: Classical Channel

single-photon detector directly. The oscilloscope reads the data whenever a trigger signal is present. The data has been processed to determine the bit values of the qubits sent by Alice. Afterwards, the public discussion starts upon Bob's confirmation for receiving the last trigger signal.

4.2.1 Single Photon Detector

The single-photon detector is the main optical element of Bob. The detector gives a specific signal whenever a photon hits to the detector. This signal gives a square-like signal for every photon that reaches to the detector.

The resolution of the detector is 35 ns. Thus, two photons hitting the detector within 35 ns will only send a single signal. One should note that if the width of the pulses is close to this value, then it would be impossible to distinguish the bit value of the qubits encoded in time base.

Table 4.2: Specifications of the single photon detector: Hamamatsu H8259-01

Dark Count	80 s^{-1}
Amplitude	2 V
Pulse Width	30 ns
Pulse-Pair Resolution	35 ns
Count Sensitivity at 600 nm	$2.3 \times 10^5 \text{ s}^{-1} \cdot \text{pW}^{-1}$

The detector has been used to determine the average photon number values of the pulses. This can be done by tracking every pulse that has been sent by the detector and then counting them. The detector gives a specific signal with parameters given in Table 4.2 and the shape of the pulse is given in Figure 4.4.

Therefore, one can increase the count whenever the amplitude exceeds 1 V (half of the amplitude of the signal). It has been observed that the regions around the peak point (1.9V - 2.1V) of the detector's output signal contains some fluctuations.

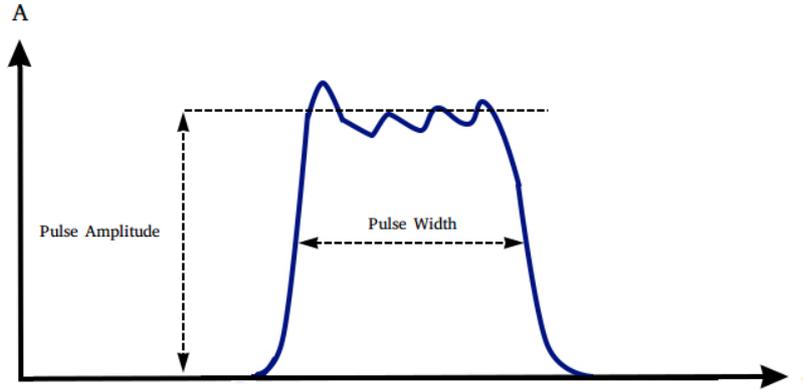


Figure 4.4: A typical output signal from the single-photon detector (Hamamatsu H8259-01)

The average photon number of the pulses are determined with the help of a trigger pulse. For every pulse that has been sent by Alice, the AWG sends a trigger pulse to the oscilloscope. Thus, the arrival time of the photons will be known by Bob. Basically, every signal that is been sent by the detector (within the duration of the trigger pulse) has been counted. At the end, one can divide the total count of the detector pulses by the total count of the trigger pulses, which, as a result, gives the average photon number. It is also possible to count the number of photons that a particular pulse contains. Therefore, it is possible to plot the histogram of the pulses' photon counts, which should follow a Poisson distribution as expected (Section 5.3).

4.2.2 Cryostat

The cryostat is a cylindrical tank that has been used to reduce the temperature of the crystal down to 2 K. There are several chambers in the cryostat (vacuum chamber, nitrogen chamber, helium chamber and the sample chamber). The inner side of the outer shell has a liquid nitrogen chamber that cools down the cryostat to the level in which helium can preserve its liquid form without being boiled by large amounts. The crystal is placed in the sample chamber where a needle valve has been used to transfer liquid helium to the sample chamber. The sample chamber has a low pressure (reduced with pump) which allows liquid helium to be cooled down to 2 K. At temperatures higher than this value, the liquid helium boils while producing bubbles. The bubbles generated disturbs the laser beam and reduces the measurement sensitivity. The bubbles are removed by reducing the pressure to less than 50 mbar where liquid helium becomes a superfluid and does not produce bubbles while boiling [35].

4.2.3 Rare-Earth-Ion Doped Crystal

The crystal used in the frequency measurements is a $\text{Pr}^{+3}\text{Y}_2\text{SiO}_5$ crystal in which the praseodymium (Pr^{+3}) ions are doped into a host crystal yttrium silicate (Y_2SiO_5). The

praseodymium ion doping concentration is 0.05%. The crystal is 12 mm long with the length of 10 mm along D1 and D2 axes. The rare-earth-ion-doped crystals have long lifetimes and long coherence times, which allows us to create the spectral pits. It is also important to have the crystal in the cryostat since the phonons generated by the temperature disturbs the ions. Thus, it introduces decoherence which makes the generation of spectral pits impossible.

The crystal has been placed into a crystal holder and then placed into the sample chamber of the cryostat. It is also possible to apply a magnetic field to the crystal inside the cryostat. A magnetic field increases the relaxation time of the hyperfine levels, which helps us to create precise spectral pits.

The absorption in the crystal is polarization dependent. If the orientation of the polarization is along the D1 axis, the absorption is fairly low. If it is along the D2 axis, then the absorption is high. Thus, one should orient the polarization angle to be the same as D2 axis, since it will be easier to create a spectral pit. Additionally, the slow-light effect is also absorption dependent (Equation 3.27). This means that the depth of the spectral pit has a linear relation with the group velocity of the photons passing through the crystal.

4.2.4 Frequency Measurement

The theory of the frequency measurements has been given in Chapter 3. In this section, information about the experimental setup and the procedure is given. The frequency measurement has been done with a similar setup to the one shown in the Figure 4.3. The only difference with the actual setup is that the single-photon detector has not been used. Instead, it has been replaced by a photodiode since the bright pulses have been employed to determine the slow-light effect. This effect has been observed by measuring the arrival time of the pulses that passes through the crystal. A lens with 30 mm focal length has been placed before the cryostat to focus the laser beam into the crystal for the spectral hole burning operation.

The most crucial operation for our frequency measurement is the spectral hole burning. The spectral pit should have steep edges to increase the group velocity difference between the pulses positioned (in frequency domain) at center and at the edges of the pit. It has been discussed in the Section 3.1 that the hyperbolic secant pulses are much more convenient while creating a narrow pit (< 2 MHz). Thus, the hyperbolic secant pulses have been generated for the spectral hole burning operation (Table 4.3). It is crucial to determine the optimum hole burning parameters such as the number of cycles, frequency scan interval, pulse duration and the number of erasing pulses to increase the resolution of the measurements.

The crystal which has been placed in the cryostat is relatively long, thus, the photons sent to the crystal might not reach to the ions at the back of the crystal. The reason is that the ions to the front of the crystal might absorb all the incoming photons before they reach the other end of the crystal. This might also broaden the spectral hole formed in the front of the crystal compared to the back of it. In order to eliminate all these disadvantageous events, one can reduce the intensity of the laser beam and increase the number of burn-

Table 4.3: Pulses used in the experiments for spectral hole burning operation

Target Width	Scan Range	Pulse Type	Rabi Freq.	FWHM	Duration	Repetition
a. 0.1 MHz	0.1 MHz	Hyp. Secant	14.6 kHz	8.4 μ s	100 μ s	120000
b. 0.5 MHz	0.1 MHz	Hyp. Secant	22 kHz	8.4 μ s	100 μ s	60000
	0.5 MHz	Hyp. Secant	22 kHz	8.4 μ s	300 μ s	60000
c. 1.0 MHz	1.0 MHz	Hyp. Secant	5.5 kHz	8.4 μ s	300 μ s	120000
d. 2.0 MHz	2.0 MHz	Hyp. Secant	5.5 kHz	8.4 μ s	300 μ s	120000

pulse cycles. It is also effective to do a narrow frequency scan before the main frequency scan (Table 4.3/b), to increase the efficiency of the hole burning operation.

The symmetry of the spectral hole is also critical, since the asymmetry will affect the group velocity of the photon differently due to the slow-light effect. The direction of the frequency scan should be taken into account while creating symmetrical spectral pits. Thus, in every second hole burning pulse, the frequency scan intervals has been reversed. In other words, half of the burning pulses had a scan interval from $(f_0 - f_w/2)$ to $(f_0 + f_w/2)$ and the other half of the burning pulses had an interval from $(f_0 + f_w/2)$ to $(f_0 - f_w/2)$. Here, f_w is the scan range.

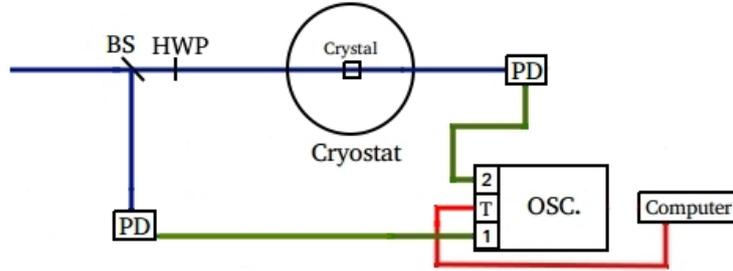


Figure 4.5: The experimental setup of the spectral hole burning operation. BS: 10/90 Beamsplitter, PD: Photo-diode, OSC.: Oscilloscope (1: Channel 1, 2: Channel 2, T: Trigger)

Two different reading techniques have been used to determine the created spectral pit and the slow-light effect. The first one is used to scan a frequency interval broader than the pit, thus, one can compare the intensity of the sent pulse to the intensity of the pulse that passed through the crystal (Figure 4.5). The other one is to send several Gaussian pulses with different center frequencies. Hence, one can measure the slow-light effect exerted on the pulses by measuring the arrival time of the photons.

4.2.5 Detection Algorithm

In this section, the detection algorithm is described, to determine the average photon number of the pulses and the detection of the qubits. The signal sent by the single-photon

detector has been given in the Figure 4.4. Measuring the average photon number of the pulses is fairly easy. It has been done by counting the total trigger pulses sent to the oscilloscope and the signal that has been sent by the single-photon-detector. Reading-out the qubits have been done in a similar way. However, in this part one needs to work with a more complex detection algorithm.

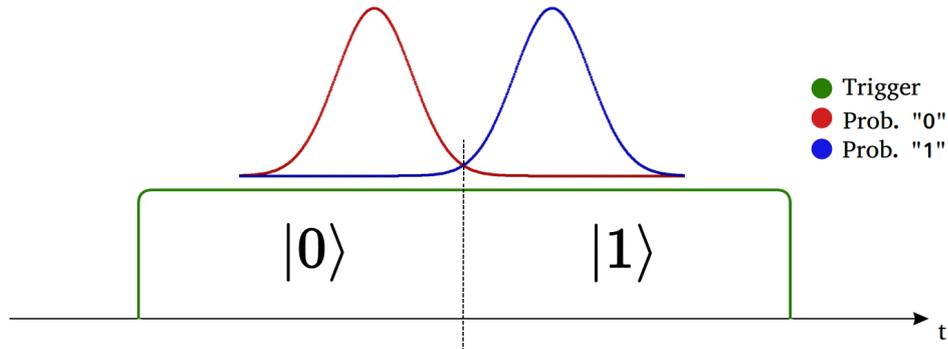


Figure 4.6: The detection frame for each trigger signal. The time interval of the state $|0\rangle$ and the $|1\rangle$ with their correspondence to the probability distribution of the Gaussian pulses.

The detection algorithm (see Table 4.4) is based on the probabilities of the arrival time of the photons. This algorithm has been used in the time-bin detection. It is also possible to use them in the frequency-bin detection, since our frequency-bin measurements are also converted to the time-domain with the help of the slow-light effect. The detection algorithm has been written in MATLAB programming language, which reads the data and processes it within the oscilloscope. The detection starts with the trigger pulses sent by the AWG to reach the oscilloscope. The oscilloscope has been programmed to only read the data when the trigger pulse is present. Thus, the arrival time intervals of the photons are determined. After saving all the data points for all of the qubits sent by Alice, the data-processing starts. The first thing that should be done is to identify the signals that have been sent by the single-photon-detector. This procedure has been done by tracking the amplitude of the signal (see Section 4.2.1). At this point, it is possible for us to know the arrival time of the photons when they arrive at the detector. Additionally, it is also possible to know the total number of photons in a pulse. Therefore, one can calculate the average photon number of the pulses that has reached to Bob.

After the read-out process of the oscilloscope, the decisions of the bit values have been done. In the time-bin measurement of the FT-QKD protocol, the qubits are encoded by their time of arrival (Figure 2.5). Thus, the time-frame has been divided into two for every trigger pulse (Figure 4.6). If the photon arrives before the mid-point of the trigger pulse then it will be known by Bob that Alice sent the state $|0\rangle$. On the other case, if it arrives after the mid-point, it will be known that Alice sent the state $|1\rangle$. However, pulses in the FT-QKD are overlapping and there might be more than one photon in each pulse. If only a single photon reaches Bob, then, there is not much one can do. The decision will be made

Table 4.4: The detection algorithm and the protocol procedure that is maintained by Bob. N_0 (N_1) is the photon count in the $|0\rangle$ ($|1\rangle$) interval. t_m is the mid-point of the trigger signal. t_e and t_l is the arrival times of the earliest and the latest photons.

Bob saves the signal from the detector whenever a trigger signal is present.		
Bob waits until the last trigger signal to arrive.		
Bob processes the saved data to obtain arrival times of photons.		
Bob divides the time-frame of every trigger signal into two.		
Bob makes the decision of the bit value for every qubit sent by Alice.		
Condition	State: $ 0\rangle$	State: $ 1\rangle$
$(N_0 \neq N_1)$	$(N_0 > N_1)$	$(N_0 < N_1)$
$(N_0 = N_1)$	$[(t_m - t_e) > (t_l - t_m)]$	$[(t_m - t_e) < (t_l - t_m)]$
Bob reads the pulse types and the base choices of Alice.		
Bob saves the shared-key.		
Bob calculates the QBER and the gain. ¹		

depending on the arrival time of this single photon. In the cases where a multi-photon signal hits the single photon detector, the detection algorithm follows this procedure: First, the comparison of the total number photons in both intervals takes place. For instance, there are two photons in the interval of state $|0\rangle$ and only one in the interval of $|1\rangle$. Since the probability of having two photons in the interval of the state $|0\rangle$ is much larger than having only one in the interval of the state $|1\rangle$, the bit value will be determined as "0". It is also possible to have an equal number of photons in both intervals. In this case, the decision will be made by checking the arrival times of the "earliest" and the "latest" photons. The photon with the longest time difference to the mid-point will be taken into account for the decision of the bit value. After determining the bit values, Bob calculates the QBER¹ and gain for both signal and decoy states (Table 5.3).

¹Here, Bob should reveal a portion of the key for the calculation of the QBER, however, in this part, the key has been directly used to increase the precision of the calculation.

5 Results

In this chapter, one can find brief information about the experiments and their results. Additionally, the discussions of the results is provided in this chapter, where a general discussion will be given in the Chapter 6.

5.1 Numerical Simulation of the Decoy-State Protocol

In the decoy-state protocol, one can optimize the secure-key-generation rate by modifying the average photon numbers (APN) of the signal and the decoy pulses (Figure 5.1). The test the numerical simulation the experimental parameters are taken from [19] and the results are compared. The input parameters are the detector error ($e_{detector}$), the transmittance of Bob (η_{Bob}) and the dark count of the detector (Y_0) (see Table 5.1).

Table 5.1: Values of experimental input parameters (taken from [19]).

$e_{detector}$	η_{Bob}	Y_0
1.38×10^{-2}	5.82×10^{-2}	6.14×10^{-5}

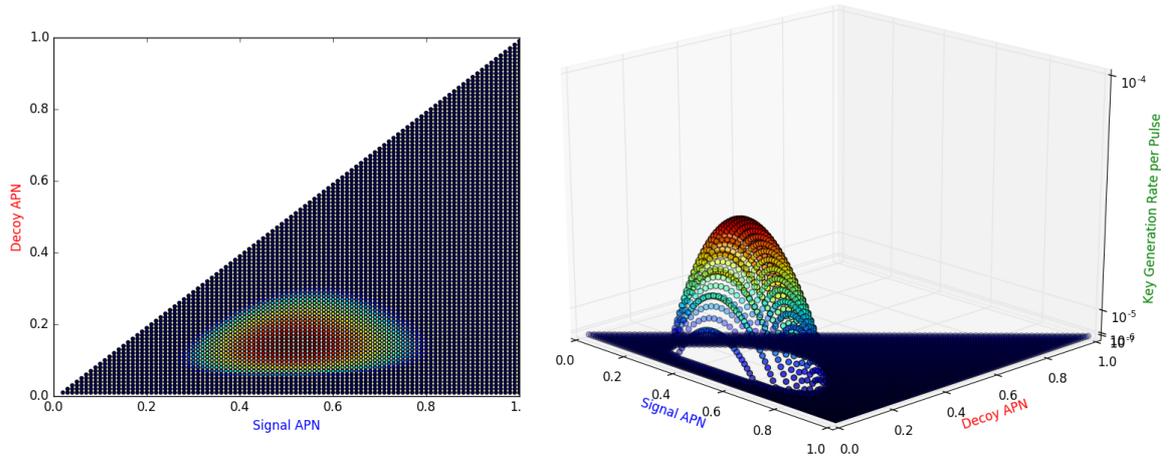


Figure 5.1: The output of the numerical simulation for a given channel length. The experimental parameters are taken from [19].

Additionally, the total number of the signal (N_μ), the decoy (N_v) and the vacuum pulses (N_o) that have been used in the weak+vacuum protocol can be optimized by this numerical simulation. The estimation of the lower bound of Q_1 and the upper bound of e_1 have been calculated for every possible value of μ and v , where μ is greater than v (Equation 2.14 and Equation 2.15). The gains Q_μ and Q_v have been estimated with the following relations [19]:

$$Q_\mu = Y_0 + 1 - e^{-\eta\mu} \quad (5.31)$$

$$Q_\nu = Y_0 + 1 - e^{-\eta\nu} \quad (5.32)$$

where η is the total transmittance of the channel including the transmittance of the detector (η_{Bob}).

The QBERs, E_μ and E_ν have been estimated as [19]:

$$E_\mu = \frac{1}{Q_\mu} [e_0 Y_0 + e_{detector} (1 - e^{-\eta\mu})] \quad (5.33)$$

$$E_\nu = \frac{1}{Q_\nu} [e_0 Y_0 + e_{detector} (1 - e^{-\eta\nu})] \quad (5.34)$$

where, e_0 is the QBER of a vacuum signal which is equal to $1/2$. After calculating the upper and lower bounds, the simulation determines the maximum value of the secure key generation rate (Equation 2.13) for the given input parameters for every possible channel length.

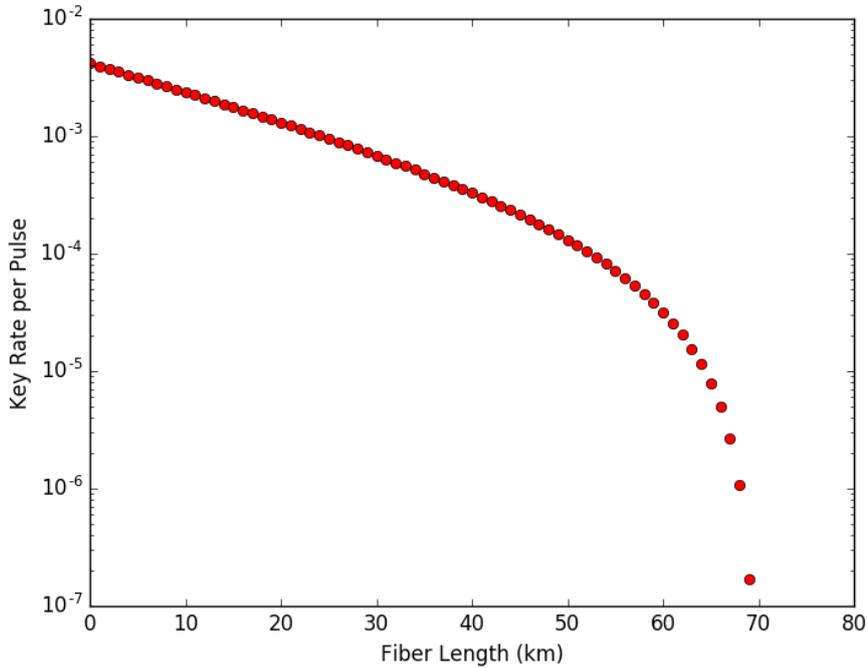


Figure 5.2: The output of the numerical simulation for the secure key generation rate vs. channel distance. The experimental parameters are taken from [19].

It is also possible to calculate the maximum distance that allows the secure key generation (Figure 5.2). In this calculation, the optimum secure key generation rate has been

determined by modifying the following parameters: μ , v , N_μ , N_v and N_0 . The simulation runs until the secure key generation rate goes below zero.

The simulation code has three loops (Table 5.2), where the first loop is increasing the distance by 1 km until the key-generation-rate value goes below zero. The second loop contains three variables: N_μ , N_v and N_0 . Every possible combination of N_μ , N_v and N_0 have been selected in this loop. The last loop contains the variables of μ and v , where μ is greater than v . As a result, largest secure key generation rates for every kilometer have been calculated. Afterwards, it is possible to determine the operational distance of the protocol, which is around 70 km in the Figure 5.2.

Table 5.2: Structure of the numerical simulation.

Declaration of the input parameters: $e_{detector}$, η , Y_0 and N
1 st Loop: $l = [0, l_{end}]$, where $l \in \mathbb{Z}$
2 nd Loop: $\frac{N_\mu}{N}, \frac{N_v}{N}, \frac{N_0}{N} = [0, 1]$, where $\frac{N_\mu}{N} + \frac{N_v}{N} + \frac{N_0}{N} = 1$
3 rd Loop: $\mu, v = [0, 1]$, where $\mu < v$
Calculation of Q_μ, Q_v, E_μ and E_v (Equations 5.31-5.34)
Calculation of Q_1^L and e_1^U (Equations 2.14-2.15)
Calculation of R^L (Equation 2.13)
End of 3 rd Loop (Output: Figure 5.1)
End of 2 nd Loop
End of 1 st Loop
$R_{max}^L(l) < 0$, $l = l_{end}$ (Output: Figure 5.2)

The simulation has not been run with the parameters of our experimental setup. The reason is that the detector error of the frequency measurements has been determined with a photodiode instead of a single photon detector due to the losses of photons passing through the cryostat. Additionally, the transmittance of the channel has not been measured since no quantum channel has been used in any measurements. However, it is possible to use this simulation after some developmental work.

The numerical simulation assumes that the only source of QBER is coming from the imperfections of the devices. However, this is not the case in the FT-QKD protocol due to the overlapping in the time and the frequency bases. The secure key generation rate can still be estimated by adding the theoretical QBER value that has been introduced by the FT-QKD protocol.

5.2 Reducing Intensity to the Single Photon Regime

In this section, brief information about the experiments to reduce the intensity to the single photon regime is given.

The single photon detector has a damage threshold. Thus, one should estimate the intensity output of the AOMs before using the single photon detector. It is also important

that the AOMs follow the calibrated values of the Rabi frequencies which control the output intensity. (Equation 4.30).

A photodiode has been used to determine the intensity output of the setup which consists of two AOMs. Then the voltage output of the photodiode has been used to calculate the total photon count in a Gaussian pulse sent by Alice (Equation 5.35).

$$V_{out} = R(\lambda) * G * \frac{R_{load}}{R_{load} + R_s} * P \quad (5.35)$$

where the detector parameters are: $R(\lambda)$ is the responsivity ($R(606\text{nm})=0.28$), G is the gain and the scale factor is 0.5 ($R_{load} = R_s$).

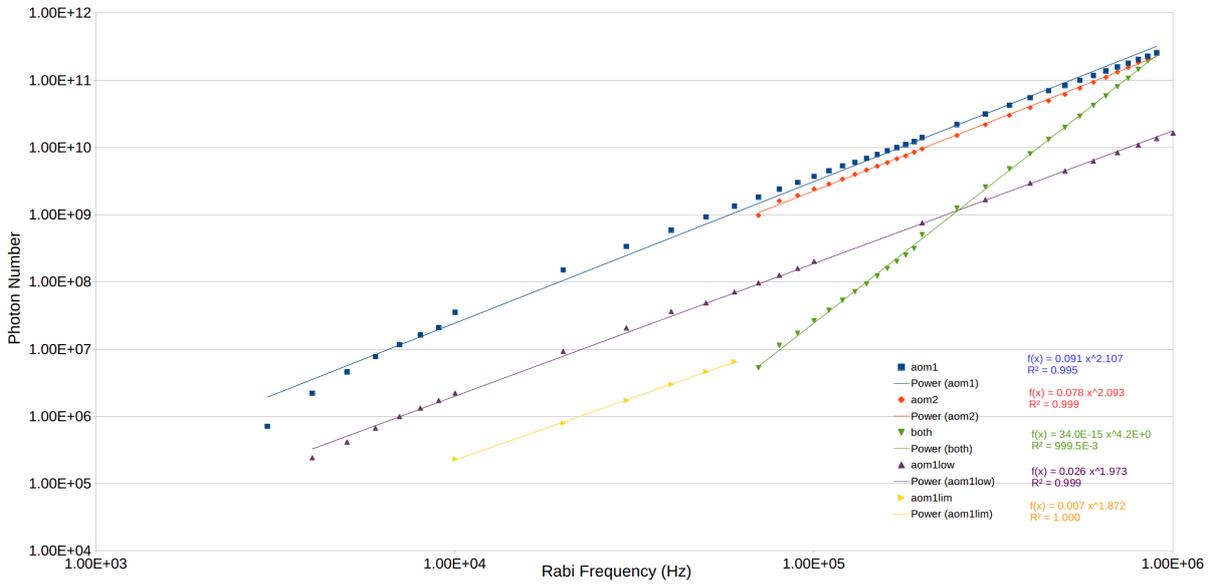


Figure 5.3: The total number of photons sent by Alice depending on the Rabi frequencies of the AOMs.

The gain of the detector goes up to 70db, where it allows us to detect pulses that contains 10^5 photons. In the figure 5.3, one can find the number of photons in a pulse corresponding to the given Rabi frequencies. The blue points represent the case where the second AOM (360 MHz) has a fixed Rabi frequency of 0.9 MHz while the x-axis shows the Rabi frequency of the first AOM (210 MHz). The red points correspond to the case where the first AOM has a fixed Rabi frequency of 0.9 MHz while the Rabi frequency of the second AOM has been modified. The green points show the case where both of the Rabi frequencies of the AOMs have been modified. The purple and yellow points stand for the cases where the second AOM has a fixed Rabi frequency of 70 kHz and 50 kHz respectively.

According to the Equation 4.30, the intensity should follow the relation $I \propto \Omega^2$, when the first AOM or the second AOM has a fixed Rabi frequency. In the case, where they have been modified together, it should follow the relation $I \propto \Omega^4$. In the Figure 5.3, one

can find the equations that correspond to the trend-lines of the data points. It has been determined that the AOMs transmit the expected intensity values depending on the given Rabi frequencies. The second AOM has a lower limit of 50 kHz Rabi frequency and it has been determined that the first AOM has a lower limit of 3 kHz Rabi frequency. The lowest photon count that can be achieved in this setup is around 10^4 photons. Thus, a density filter with the transmittance 10^{-6} has been installed to the setup to reduce the intensity of Alice to the single photon regime. After setting up the density filter, the single photon detector has been installed to measure the average photon number of the pulses.

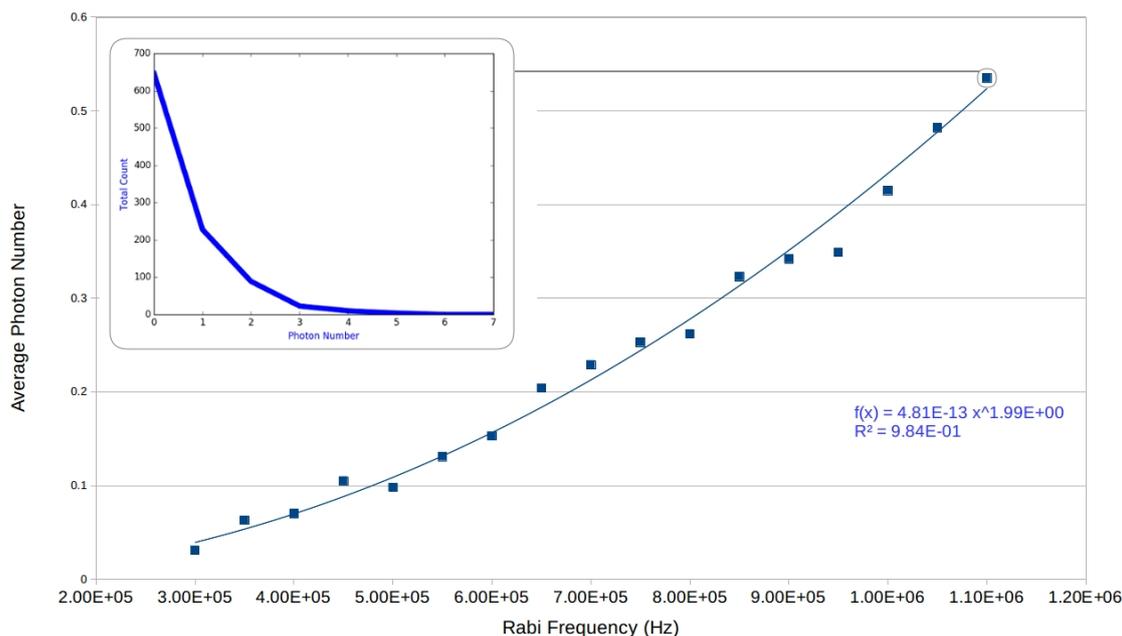


Figure 5.4: The total number of photons sent in a pulse by Alice depending on the Rabi frequency of the first AOM where the Rabi frequency of the second AOM has been fixed to 50 kHz.

In the Figure 5.4, the Rabi frequency of the second AOM has been fixed to 50 kHz. Thus, an APN value greater than 0.5 can be easily achieved by increasing the Rabi frequency of the second AOM. For instance, setting the Rabi frequency of the first AOM to 1.1 MHz and setting the second AOM's Rabi frequency to 90kHz gives the average photon number value of 0.924. Additionally, the Rabi frequency values in Figure 5.4 - 5.3 are not correlated with each other, hence, one should consider the abscissa has being in arbitrary units. In the upper inset of the Figure 5.4, the histogram of the pulses with the corresponding average photon number has been given. As it is expected the histogram follows the Poisson distribution (Equation 2.7). As a result, the weak-coherent source of Alice has been implemented successfully. Additionally, one can use the simulation results (Section 5.1) to determine the optimum parameters of Alice.

5.3 Time Base Measurements

In this section, the time base measurements and their results are given. The pulse parameters in time domain are linked to the pulse parameters in frequency domain. Thus, both of the parameters are described in this section.

The Gaussian pulses for the FT-QKD protocol have been generated by the AOMs. First of all, the bright pulses have been sent to a photodiode to determine the arrival time of photons at the detector which has been discussed in the detection algorithm section (Section 4.2.5). Afterwards, the single photon detector has been placed together with the density filter that has been used in the measurements to reduce the intensity to the single photon regime.

For the first tests of the detection algorithm and the time base detections, Gaussian pulses with 1 μs full-width-half-maximum (FWHM) have been used. In this part, one should note that there has been no quantum channel used during the tests. In other words, the quantum channel was a 10 cm long free-space channel. The first tests have been done with 1 kilobits raw key length (Table 5.3).

Table 5.3: The parameters and the results of the time-base measurements. (R. Size: Raw-key size, S. Size: Shared-key size)

δ_t	Δ_t	μ	v	R. Size	S. Size	E_μ	E_v	Q_μ	Q_v
1 μs	6 μs	0.55	0.06	1000	564	0.035	0	0.564	0.007
1 μs	2 μs	0.57	0.06	1000	577	0.068	0	0.578	0.006
1 μs	1.5 μs	0.55	0.05	1000	547	0.128	0.002	0.548	0.005
1 μs	2 μs	0.736	0.105	1500	633	0.051	0.003	0.422	0.003
1 μs	1.5 μs	0.717	0.116	1500	677	0.062	0	0.451	0.003

In order to measure the detector's error, the pulses in time have been separated by 6 μs which removes the overlapping region between the states $|0\rangle$ and $|1\rangle$. The QBER value of 0.35% has been determined by the public discussion carried between Alice and Bob. Then, the pulse separation has been changed to its optimum value of 2 μs . As it is expected the QBER value has been increased to 6.76%. It is important to meet the requirements of the secure key generation where QBER should be less than 11%. Finally, the separation value has been changed to 1.5 μs and the QBER value has been determined as 12% which can be considered as the limit of the secure key generation operation. The gain values, Q_μ and Q_v have been measured as 0.55 and 0.06 which is equal to the average photon values of signal (μ) and decoy (v) states, since there have been no losses of photons along the quantum channel. The same measurements have been repeated with 1.5 kilobit raw key length (Table 5.3).

There are two types of readout methods that have been used in this part. In the first measurements, a one-by-one readout method has been used. The oscilloscope that has been used in this experiments cannot identify different trigger pulses that are sent within a short time period from each other. Thus, a waiting period has been added to the pulse

sequence. This waiting period is long enough to reduce the raw key distribution speed down to 1 bit per second. In other words, the measurements that have been given in the Table 5.3 took at least 1000/1500 seconds. In the other readout method, a trigger pulse has been sent to locate the pulse train. Thus, the oscilloscope has been programmed to read the pulses that are sent after this main trigger pulse. In this one-time readout method, it is possible to send a pulse train that is 2 seconds long in total which corresponds to 444¹ kilobits. Thus, it is possible to increase the transmission rate of the raw-key up to 222 kilobits per second.

Table 5.4: The optimum pulse parameters for the FT-QKD protocol.

δt	t_{dur}	Δt	$\delta \tau$	δf	Δf	δv
0.5 μs	4.5 μs	1.0 μs	1.5 μs	0.3 MHz	1.0 MHz	0.9 MHz

The parameters in the Table 5.4 have been determined considering the frequency measurements done with the slow-light effect. In the time-bin measurements

5.4 Frequency Base Measurements

In this section, the frequency of the qubits sent by Alice has been measured by creating a spectral pit in the 12 mm long rare-ion-doped crystal. As it has been discussed in the Section 4.2.4, the steepness of the edges of the spectral pit is a crucial parameter. In the simulation of the slow-light effect, the edges have been formed by a super-Gaussian function (Equation 5.36)

$$A = \exp\left[-(f - f_{center})^{(2\alpha)} / (2\sigma^{2\alpha})\right] \quad (5.36)$$

where, $\sigma = \sqrt{(f_{fwhm})^2 / [4 \log(2)]^{1/\alpha}}$ and α is the order of the super-Gaussian function. It represents the steepness of the spectral pit. According to the simulation results (Section 4.2.4), the order of the spectral pit should be at least 10 in order to separate pulses with high efficiency. One should note that the larger values of the order will increase the precision of the frequency measurements. The spectral holes have been created as it has been stated in the Section 4.2.4. The readout of the spectral pit has been done in two different methods. The first one is to scan a frequency interval to measure the transmission of the crystal (Figure 5.5).

The frequency scan readouts have been used to determine the orders of the pits by comparing the readouts with the generated spectral pits. The generated spectral pits have the order which is equal to 2-3. This means that the time delay between two pulses with different frequencies will have less separation than the optimum case. In Figure 5.5, the spectral pit has been measured by a frequency scan with 5 MHz interval with a pulse duration of 200 μs . As a result, the chirp rate of the pulse that has been used is 2.5×10^7 . The

¹The pulse duration is the duration of the pulse in time domain where the peak of the Gaussian pulse is centered at $t_{dur}/2$. Here, the duration of each pulse has been determined as 4.5 μs .

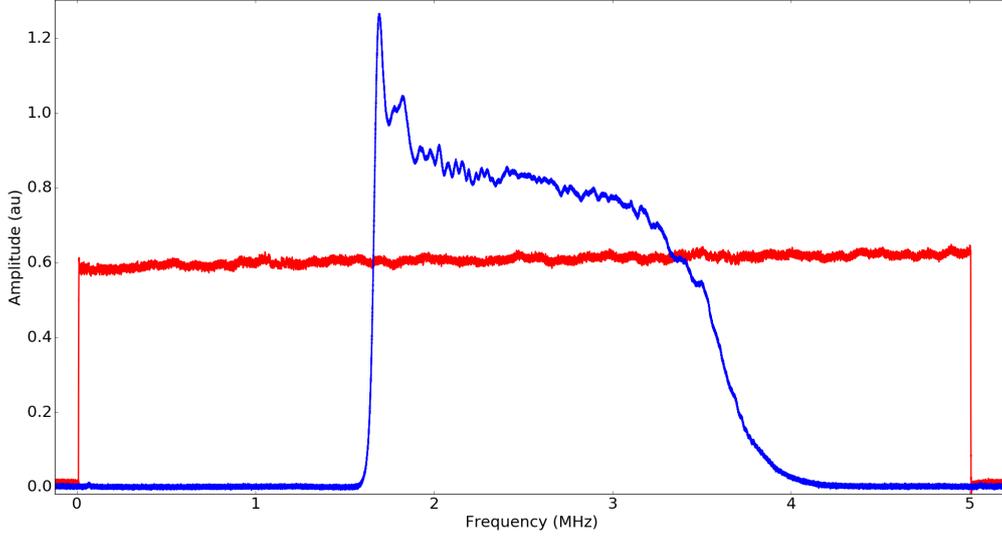


Figure 5.5: The readout scan of a spectral pit that has been created for frequency measurements. The red line represents the output of the reference detector and the blue line represents the transmitted light through the crystal.

transmitted light has a peak to the lower frequency edge due to the ions being excited to the upper energy levels by the frequency scan pulse. Afterwards, the ions return to the ground state while emitting light. Meanwhile, the frequency of the scan pulse increases in time, hence, the light being emitted by the ions and the scan pulse interferes with each other. This interference generates beating depending on the chirp rate. The effect of the interference on our read-out measurements can be eliminated by a deconvolution process. However, in this particular example the peak has very large amplitude which the deconvolution process fails to remove. Additionally due to the direction of the frequency scan, the spectral pit loses its symmetry, which is a crucial aspect for our frequency measurements. Thus, the read-out process of the spectral pit with a train of Gaussian pulses gives better results in this case.

In order to measure the slow-light effect on the Gaussian pulses for the FT-QKD protocol, a sequence of Gaussian pulses has been sent to the crystal and detected with the photodiode. There are in total 31 Gaussian pulses ($\delta t = 1.5 \mu s$) in the sequence where the center frequencies of the pulses can be expressed as:

$$f_n = -1.5 \text{ MHz} + (0.1)n \text{ MHz} \quad (5.37)$$

where n is the number of the pulse in the sequence. Thus, one can compare the delay between pulses that have been detected by the reference and the main detector (Figure 5.6 and Figure 5.7).

Several different spectral holes have been created to be tested with this method where

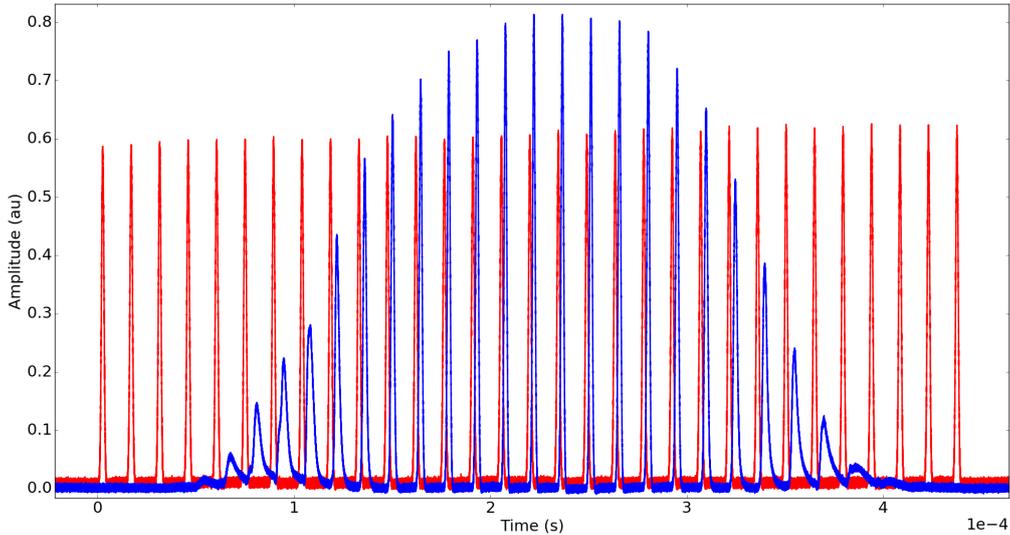


Figure 5.6: The pulse train sent by Alice to determine the slow-light effect. The red line represents the output of the reference detector and the blue line represents the transmitted light through the crystal.

the locking system has been used while creating the spectral pits. It has been explained in the Section 3.2 that the difference between the absorption in the pit and outside of the pit affects the delay introduced by the slow-light effect.

The frequency of the laser has been locked to three different frequencies: 494.7146 THz (low absorption), 494.7176 THz and 494.7209 THz (high absorption). For every different lock frequency, four spectral pits with different hole widths have been created (see Section 4.2.4). The largest time delay difference between two pulses has been measured in the spectral pit with the hole width 2 MHz, which has been created by using the lock frequency with the highest absorption. The separation of the pulses with this configuration gives promising results for the frequency measurements in the single photon regime.

The read-out of the spectral pit with the Gaussian pulse train has been determined to be a symmetrical one. The shape of the same pit was not clear because of the beating in the signal due to the reasons given in the frequency scan part in this section. One can think of this method as the usage of a frequency scan with cutoffs in every $10 \mu\text{s}$. The beating between the ions and the scan pulses has not been observed in this method due to the time duration between the Gaussian pulses. As a result, the shape of the spectral pit has been determined by the intensities of the pulses in the Figure 5.6 (blue signal).

The time delay between the pulses with different center frequencies has been determined by overlapping their reference pulses. Thus, one can compare the time delay within the same time frame (Figure 5.7) which is the case in the FT-QKD protocol. As it can be seen in figure, the Gaussian pulse with -1 MHz center frequency has been attenuated due to the

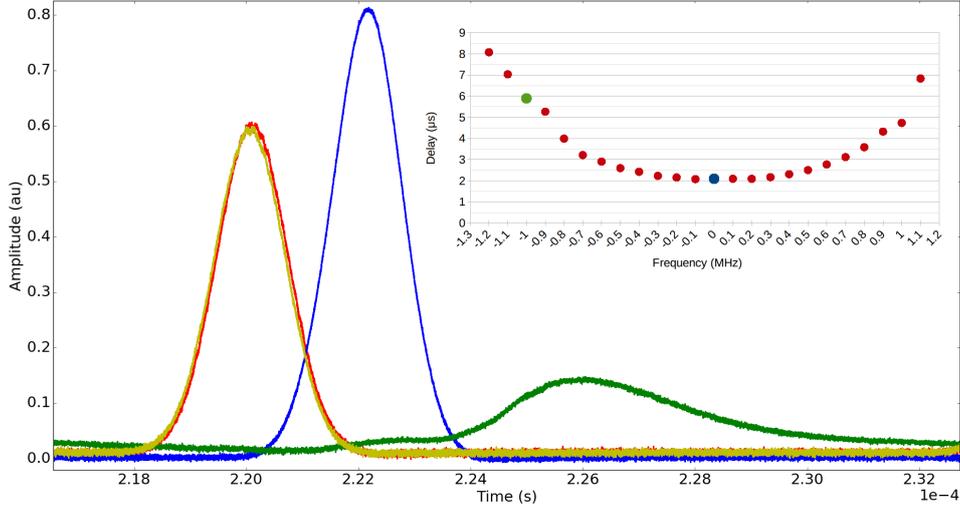


Figure 5.7: The comparison of the Gaussian pulses with 0 MHz and -1 MHz center frequencies (Red/Yellow: Reference Pulse, Blue: 0 MHz , Green: -1 MHz). The upper inset of the figure shows the time delay of the Gaussian pulses with different frequencies to their reference signal.

absorption since the frequency of the pulse is close to the edge of the spectral pit. Thus, the state $|0\rangle$ will have much higher probability to be detected compared to the state $|1\rangle$. As a result, the randomness of the key will be disturbed. As a solution, one can increase the length of the crystal or let the light to pass through the crystal several times to obtain the same delay difference for the frequencies that are closer to the center frequency of the pit. Single photons have been previously used to retrieve the efficiencies of quantum memories which is based on absorption pits [10]. Thus, the only problem in our case is that the central frequency of one Gaussian pulse is close to the edge of the absorption pit which can be shifted to the center if the profile of the absorption pit is improved. The results of the measurements show that the slow-light effect can be used to detect the frequencies of the photons in the single photon regime which can be used in the QKD systems.

The QBER analysis has been carried out after the comparison of the pulses within the same time-frame. The analysis determines the QBER with the probability distribution of the pulses as if they were single photon pulses. However, the detection algorithm that has been implemented for the single photon regime can reduce the QBER depending on the average photon number of the signal state and the decoy state. One should also note that the error of the detector has not been included in the calculation. The pulses that represent the states $|0\rangle$ and $|1\rangle$ does not have the same profile after passing through the crystal. This is due to the attenuation and also the slow-light effect which broadens the pulses. Hence, the QBER values of both states have been given separately (Figure 5.8). As it has been stated before, the QBER of the key should be less than 11%. It has been determined

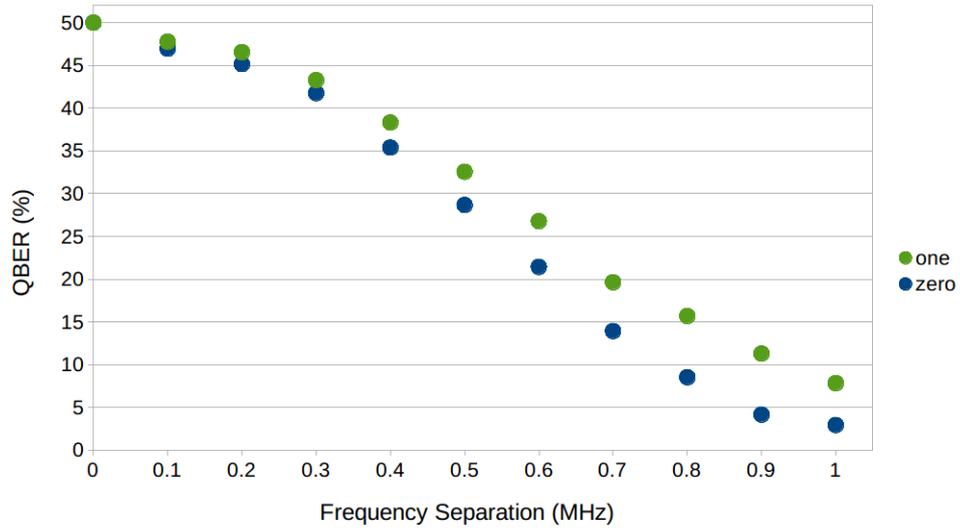


Figure 5.8: The QBER analysis of the frequency measurements.

that the pulses, which have been separated by at least 0.8 MHz (in consideration of the parameters in Table 5.4), can be used in the FT-QKD protocol.

6 Discussion

In this section, discussions about the measurements is provided. First of all, the time-base measurements have given satisfactory results with the low QBER values. However, it is important to state the limits of the experimental setup that has been used in this project.

As it has been stated in the experimental setup chapter (Chapter 4), the AWG has been used to control the AOMs. This AWG loads the pulse sequences from a file and then sends the corresponding pulses to control AOMs with RF signals. However, the sampling rate of the AWG, only allows it to modify the AOMs for every 1 ns (1 giga-samples per second). This means that one can only create pulses that are longer than 1 ns. Additionally, it will be impossible to create a Gaussian pulse with 1 ns width since the generated pulse will be a square pulse. Therefore, in the implemented protocol the shortest pulse that has been used has the width of 500 ns, which corresponds to 500 sample points in total. Another limitation of the AWG is its memory. The pulses in the implemented protocol have been pre-determined by a MATLAB code. Thus, the AWG uses some memory space to read and send the RF signals. The memory of the AWG can be overloaded by a file which contains a very long pulse sequence. This means that the raw key size is limited by the memory of the AWG. Additionally, in this project, Alice has been used to create the spectral pit for the frequency measurements. Thus, the pulse sequence that is responsible for generating the spectral pit will occupy around 80% of the memory of the AWG, which will dramatically limit the raw key size that can be sent by Alice.

While Alice has the limitations due to the AWG, Bob has the limitations due to the oscilloscope. The oscilloscope that has been used in the implemented protocol has the resolution of 2 giga-samples per second. Since the sampling rate of the oscilloscope is larger than the sampling rate of the AWG, one can state that the oscilloscope does not miss any data points which have been sent by Alice. However, the oscilloscope has been controlled by a MATLAB code to run the detection algorithm. Therefore, the oscilloscope should have a memory space which is suitable for both operations. During the tests of the protocol, it has been encountered that the memory of the oscilloscope was not enough to execute both operations while detecting a pulse sequence larger than 7 kilobits. The solution to this problem is to separate the data readouts and the data processes. In other words, one should first save the measurement data to a file manually and then this data can be processed with the written detection algorithm.

The single-photon detector has the resolution of 35 ns, which means that Bob cannot identify multi-photons arriving within 35 ns. The time-base measurements have been done with the Gaussian pulses which have 1 μ s width. In those cases, it is unlikely that two or more photons would reach to the detector within 35 ns. The resolution of the detector can be improved to reduce the QBER in the time-base measurements. However, the QBER of the time-base measurements has been measured to be around 6% which is a suitable value for the security of the protocol. In the frequency-base measurements, the width of the pulses has been determined as 1.5 μ s. Thus, the error introduced by the single-photon detector (due to its resolution) will be much less compared to the time-base measurements.

The QBER and the gain of the frequency-base measurements are highly dependent on

the created spectral pit. It has been determined that the edges of the created spectral pits are not steep enough to have optimum detection results. As a solution, one can let the qubits pass through the crystal several times, thus, the separation of the pulses with different frequencies will be larger. Therefore, the frequency of the pulses can be selected to be closer to the center of the spectral pit, which will increase the transmission of the pulses. In order to increase the gain, one can also put anti-reflection coatings to the crystal's surfaces.

The spectral pits have been created by Alice where it has been planned that the pulses will be detected by a detector after passing through the crystal. This means that the qubits prepared in the time-base should also travel through the crystal. The qubits in time-base might face an absorption in the crystal since the width of these pulses is wider than the frequency-base qubits. In order to overcome this problem, one can install an optical switch to the system of Bob, where Bob's base selections can be used to control the optical switch to direct the light to the crystal or directly to a single photon detector.

Another possible technique to measure the frequency of the qubits would be to use a quantum repeater instead of a spectral pit [44]. Briefly, in this technique, the state $|0\rangle$ will be directly transmitted through the quantum repeater while the state $|1\rangle$ will be saved in the quantum repeater to be transmitted after few μs . Therefore, the pulses with different frequencies can be again separated in time-domain to be measured by a single-photon-detector. This method is more promising since the single photons have been previously used on quantum memories. However, one will need quantum memory in Bob's setup which which introduces complexity to the setup.

7 Conclusion

The field of quantum key distribution is a brand new topic where currently researches are mostly focused on the operational distance and the quantum repeaters. Projects that focus on the quantum repeaters have been previously done in this group. However, for the first time in this group, an actual QKD protocol has been implemented in this project. Additionally, this project has shown the capabilities of the equipment that is owned by the group since no additional equipment was required for the project. The proposed frequency measurement technique gives propitious results which show that the technique can be used in the QKD protocols. Moreover, the same technique can be used to determine the frequencies of single-photon sources with high precision. As it has been stated in the Chapter 6, the project leaves an open door for a possible developmental work as an extension of this project.

As a possible extension to this project, one can improve the spectral hole burning operation to form steeper pit edges. As it has been stated before, one can also increase the length of the crystal to be able to use Gaussian pulses with less frequency separation. It is also possible to form a larger spectral pit while increasing the length of the crystal or the steepness of the edges. The surfaces of the crystal can be coated to increase the gain of pulses. An optical switch should be used to separate the measurements in time and frequency. Afterwards, it is expected that it will be possible to perform tests with single photon detectors. As a final step, one can test the efficiencies of quantum memories with an actual QKD protocol. It is also possible to increase the raw-key size by modifying the read-out method of the oscilloscope.

8 Appendix

8.1 Ekert91

This section gives brief information about the Ekert91 (E91) protocol, which has not been used in this project. However, the first step of this project was to determine a suitable protocol. Thus, the reader is encouraged to read if he/she is interested on the working mechanism of E91 and the reasons for not selecting this protocol.

The Ekert91 is a QKD protocol which is similar to the BB84 protocol [13]. It is based on the famous Einstein-Podolsky-Rosen (EPR) experiment. In the E91, the source is able to transmit pairs of spin-1/2 particles within a single state. Then, this signal is sent to Alice and Bob separately. Alice has the measurement bases with $\phi_1^a = 0$, $\phi_2^a = \pi/4$, $\phi_3^a = \pi/2$. In other words, if the entanglement is made in polarization, Alice can measure the polarizations with the following angles; 0° , 45° and 90° . On the other hand, Bob can measure the bases with $\phi_1^b = \pi/4$, $\phi_2^b = \pi/2$, $\phi_3^b = 3\pi/4$. Thus, he can measure the polarization with the following angles; 45° , 90° and 135° . Since the source emits half-spin particles, every measurement with $\hbar/2$ will result in spin-up or spin-down state. Thus, it can be used to share information. The main mechanism of this protocol comes from the following expressions:

$$E(a_i, b_j) = -a_i \cdot b_j \quad (8.38)$$

Here E is the correlation coefficient. Using the equation above, if Alice and Bob choose the same measurement orientation, the Equation 8.38 becomes:

$$E(a_2, b_1) = E(a_3, b_2) = -1 \quad (8.39)$$

Thus, it will show that the entangled pairs will give anti-correlated results which can be used to share a bit. The security of the E91 comes from the correlation coefficients of Alice and Bob when they choose different orientations [21]. In this case a quantity S is defined as:

$$S = E(a_1, b_1) - E(a_1, b_3) + E(a_3, b_1) + E(a_3, b_3) \quad (8.40)$$

Also, the following relation should be satisfied:

$$S = -2\sqrt{2} \quad (8.41)$$

Thus, any eavesdropper that tries to steal the shared-key will be introducing a fluctuation to this value ($S = 2\sqrt{2}$). After the transmission of the key, Alice and Bob can determine the value of S . Thus, they can be aware of the presence of any eavesdropper. That being said, the procedure of the E91 protocol starts with the transmission of qubits to Alice and Bob separately. After the transmission both Alice and Bob reveals their measurement orientations for each qubit measurement. In the case where they choose the same base, they use the measured states to form the key. Since, the bit value is anti-correlated

(Equation 8.39), one of the users should do a bit-flip. In the cases where they choose a different base, they use the measurement results to determine the value of S (Equation 8.40). If the value of S is close to $2\sqrt{2}$, they use the key for encrypting and decrypting the information.

The E91 protocol can be used only by generating Bell states. The Bell states are mostly used together with the entanglement which needs stabilization and additional optical elements in the experimental stage. In consideration of having a practical setup, E91 has not been selected as the protocol type.

8.2 Measurement-Device-Independent

Measurement-Device-Independent (MDI) is a recent protocol which has been introduced to deal with attacks that are targeting detectors [22]. Additionally, it has been reported that the secure key generation is possible for long-distances over 200 km. A recent experimental setup of MDI has achieved 404 km while generating the secure shared-key [23]. Similar to the Section 8.1, this protocol has not been used in the project. However, it has been determined that it can be used in a developmental project. Thus, the reader is encouraged to read if interested.

An MDI protocol setup uses phase randomized weak coherent pulses. This means that the MDI protocol uses the decoy-state method. The main idea here is to create two Bell states (Equation 8.42 and Equation 8.43) which can be detected by the measurement device, Charlie. Qubits are sent by Alice and Bob together to a beam-splitter to create Bell states in the measurement device.

$$|\psi\rangle^- = 1/\sqrt{2}(|HV\rangle - |VH\rangle) \quad (8.42)$$

$$|\psi\rangle^+ = 1/\sqrt{2}(|HV\rangle + |VH\rangle) \quad (8.43)$$

As a result of the Hong-Ou-Mandel (HOM) effect, when two identical photons enter to a beam-splitter, photons will exit through the same output (also, when they are both generated in orthogonal polarizations). Thus, with the given basic MDI setup (Figure 8.1), when a click in D_{1H} and D_{2V} , or in D_{1V} and D_{2H} occurs, it will be known that the measured state is $|\psi\rangle^-$. On the other hand, when a click in D_{1H} and D_{1V} , or D_{2H} and D_{2V} occurs, it will mean that the measured state is $|\psi\rangle^+$.

The MDI protocol follows this procedure: Alice and Bob send qubits to Charlie. Charlie announces the arrival of photons and declares the measurement results to users. Then, Alice and Bob share their base selections to each other. They both discard the measurement results, when they have selected different bases (rectilinear/diagonal). According to the results of the measurement, Alice or Bob might need to do a bit flip ¹. In the case they have chosen the rectilinear base; every successful measurement of the state $|\psi\rangle^-$ and the state $|\psi\rangle^+$ will be needing a bit flip. On the other hand, in the case they have both selected

¹Here, bit flip means to change the bit value of a particular element in the key (Zero to one or one to zero).

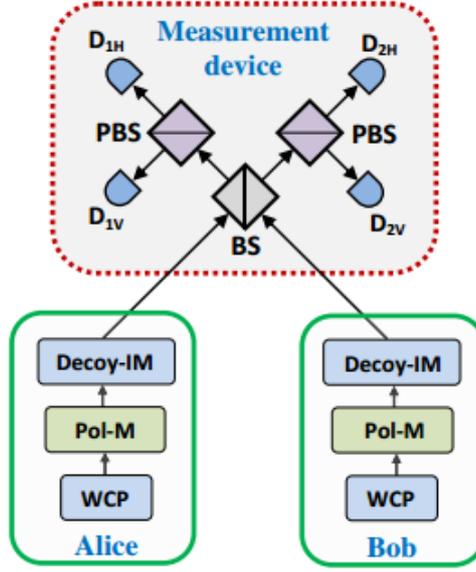


Figure 8.1: A basic MDI setup, which has two polarizing beam splitters (PBS), a beam splitter (BS), two intensity modulators (IM), two polarization modulators (Pol-M) and two phase-randomized weak-coherent-pulses (WCP) (Figure taken from [22] with permission, copyrighted by the American Physical Society)

the diagonal base, a bit flip will be needed for every successful measurement of the state $|\psi\rangle^-$. A flip will not be needed for the state $|\psi\rangle^+$ (a triplet-state) since Alice and Bob sent a correlated bit.

The key generation will be used only when both users use the rectilinear base. The diagonal base is used to track the error rate to know if Eve is present or not. Thus, the key generation is given as:

$$R = Q_{rect}^{n,m} [1 - H(e_{diag}^{n,m})] - Q_{rect} f(E_{rect}) H(E_{rect}) \quad (8.44)$$

where n and m is equal to one ($n = 1$ and $m = 1$), and they represent the number of photons sent by Alice and Bob.

References

- [1] R. L. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM* 21, 120 (1978).
- [2] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill, "Efficient networks for quantum factoring", *Physical Review A*, 54, 1034 (1996)
- [3] P.W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", 26, 1484-1509 (1997)
- [4] L. K. Grover, "A fast quantum mechanical algorithm for database search", *Proceedings, 28th Annual ACM Symposium on the Theory of Computing*, 212 (1996)
- [5] G. S. Vernam, "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications", *Transactions of the American Institute of Electrical Engineers*, 45, 295-301 (1926)
- [6] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned", *Nature*, 299, 802-803 (1982)
- [7] H. K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution", *Physical Review Letters*, 94, 230504 (2005)
- [8] H. L. Yin, T. Y. Chen, Z. W. Yu, H. Liu, L. X. You, Y. H. Zhou, S. J. Chen, Y. Mao, M. Q. Huang, W. J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X. B. Wang, and J. W. Pan, "Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber", *Physical Review Letters*, 117, 190501 (2016)
- [9] Toshiba Corporation, "Press Release: Commencement of Verification Testing of Quantum Cryptographic Communication System that Theoretically Cannot be Tapped", (2015) (visited on 31/03/2017).
- [10] M. Sabooni, Q. Li, S. Kröll, L. Rippe, "Efficient Quantum Memory Using a Weakly Absorbing Sample", *Physical Review Letters*, 110, 133604 (2013)
- [11] Personal communication with Andreas Walther (Assistant Professor in Atomic Physics, Lund University).
- [12] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", *Theoretical Computer Science*, 560, 7-11 (2014)
- [13] A. K. Ekert, "Quantum cryptography based on Bell's theorem", *Physical Review Letters*, 67, 661 (1991)
- [14] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information", Cambridge University Press (2000)

- [15] Y. Zhao, , PhD. Thesis: "Quantum cryptography in real-life applications: assumptions and security", University of Toronto (2009)
- [16] A. Holevo, "Some Estimates for the Amount of Information Transmittable by a Quantum Communications Channel," *Problems of Inf. Transm.* 9, 177 (1973).
- [17] D. Gottesman, H. K. Lo, N. Lütkenhaus and J. Preskill, "Security of Quantum Key Distribution with Imperfect Devices", *Quantum Information and Computation*, 4, 325-360 (2004)
- [18] X. Ma, B. Qi, Y. Zhao and H. K. Lo, "Practical decoy state for quantum key distribution", *Physical Review A*, 72, 012326 (2005)
- [19] Y. Zhao, B. Qi, X. Ma, H. K. Lo, L. Qian, "Simulation and Implementation of Decoy State Quantum Key Distribution over 60km Telecom Fiber", *Proceedings of IEEE International Symposium on Information Theory 2006*, 2094-2098 (2006)
- [20] H. K. Lo and J. Preskill, "Security of Quantum Key Distribution Using Weak Coherent States with Nonrandom Phases", *Quantum Information and Computation*, 7, 431-458 (2007)
- [21] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Physical Review Letters* 23, 880 (1969).
- [22] H. K. Lo, M. Curty and B. Qi, "Measurement-Device-Independent Quantum Key Distribution", *Physical Review Letters*, 108, 130503 (2012)
- [23] H. L. Yin, T. Y. Chen, Z. W. Yu, H. Liu, L. X. You, Y. H. Zhou, S. J. Chen, Y. Mao, M. Q. Huang, W. J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X. B. Wang, and J. W. Pan, "Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber", *Physical Review Letters*, 117, 190501 (2016)
- [24] J. P. Bourgoin, N. Gigo, B. L. Higgins, Z. Yan, E. M. Scott, A. K. Khandani, N. Lütkenhaus, and T. Jennewein, "Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations", *Physical Review A*, 92, 052339 (2015)
- [25] C. H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States", *Physical Review Letters*, 68, 21 (1991)
- [26] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography", *Reviews of Modern Physics*, 74, 145 (2002)
- [27] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, "Distribution of Time-Bin Entangled Qubits over 50 km of Optical Fiber", *Physical Review Letters*, 93, 180502 (2004)

- [28] M. Leifgen, R. Elschner, N. Perlot, C. Weinert, C. Schubert and O. Benson, "Practical implementation and evaluation of a quantum-key-distribution scheme based on the time-frequency uncertainty", *Physical Review A*, 92, 042311 (2015)
- [29] B. Qi, "Quantum key distribution based on frequency-time coding: security and feasibility", arXiv:1101.5995 (2011)
- [30] N. Walk, J. Barrett and J. Nunn, "Composably secure time-frequency quantum key distribution", arXiv:1609.09436 (2016)
- [31] Y. Zhang, I. B. Djordjevic and M. A. Neifeld, "Weak-coherent-state-based time-frequency quantum key distribution", *Journal of Modern Optics*, 62, 1713-1721 (2015)
- [32] T. Zhang, Z. Q. Yin, Z. F. Han and G. C. Guo, "A frequency-coded quantum key distribution scheme", *Optics Communications*, 281, 4800-4802 (2008)
- [33] X. Chen, J. Yao, and Z. Deng, "Ultrannarrow dual-transmission-band fiber Bragg grating filter and its application in a dual-wavelength single-longitudinal-mode fiber ring laser", *Optics Letters*, 30, 2068-2070 (2005)
- [34] S. F. Yelin and B. C. Wang, "Time-frequency bases for BB84 protocol", arXiv:0309105 (2003)
- [35] A. Walther, PhD. Thesis: "Coherent Processes in Rare-Earth-Ion-Doped Solids", Lund University (2009)
- [36] M. S. Silver, R. I. Joseph and D. I. Hoult, "Selective spin inversion in nuclear-magnetic resonance and coherent optics through an exact solution of the Bloch Riccati equation", *Physical Review A* 31, 2753-2755 (1985).
- [37] M. S. Silver, R. I. Joseph, C. N. Chen, V. J. Sank and D. I. Hoult, "Selective-population inversion in NMR", *Nature* 310, 681-683 (1984).
- [38] L. V. Hau, S. E. Harris, Z. Dutton and C. H. Behroozi. "Light speed reduction to 17 metres per second in an ultracold atomic gas", *Nature* 397, 594-598 (1999)
- [39] The numerical simulation of the slow-light effect in a spectral absorption pit by using Kramers-Kronig relations. Matlab code written by Qian Li (PhD Student in Quantum Information group, Lund University)
- [40] B. Julsgaard, A. Walther, S. Kroll and L. Rippe, "Understanding laser stabilization using spectral hole burning", *Optics Express*, 15, 11444-11465 (2007)
- [41] C. Clausen, F. Bussieres, M. Afzelius and N. Gisin, "Quantum storage of heralded polarization qubits in birefringent and anisotropically absorbing materials", *Physical Review Letters*, 108, 190503 (2012)

- [42] M. Gündoğan, P. M. Ledingham, A. Almasi, M. Cristiani, and H. Riedmatten, "Quantum storage of a photonic polarization qubit in a solid", *Physical Review Letters*, 108, 190504 (2012)
- [43] Z. Q. Zhou, W. B. Lin, M. Yang, C. F. Li, and G. C. Guo, "Realization of reliable solid-state quantum memory for photonic polarization qubit", *Physical Review Letters*, 108, 190505 (2012)
- [44] Personal communication with Lars Rippe (Assistant Professor in Atomic Physics, Lund University).