UNIVERSITY OF KWAZULU-NATAL

Experimental Realization of Quantum Key Distribution

by

Mpinda Kabeya

Submitted in partial fulfilment of the academic
requirements for the degree of
Master of Science in the
School of Physics,
University of KwaZulu-Natal
Durban

August 2009

As the candidate's supervisor I have/have not approved this thesis for submission.

Signed: —————————— Name: —————————— Date: ——————

ABSTRACT

Nowadays, the information society that presides the everyday life is dependent on the communication industry to facilitate unintelligible data transfers between authenticated parties. Human desire to communicate secretly since the beginnings of the civilisation. Methods of secret communication were developed by many ancient societies, including those of Mesopotamia, Egypt, India, China and Japan, but details regarding the origins of cryptology, i.e. the science and art of secure communication, remain unknown. Secure communication as well as the protection of sensitive data against unauthorised eavesdropping are inevitably important. For example, the device, used for communication between military commanders, consisted of a tapered baton around which was wrapped a spiral strip of parchment or leather containing the message.

The key is a random sequence of 0's and 1's, and therefore the resulting cryptogram, i.e. the plaintext plus the key, is also random and completely scrambled unless one knows the key. Indeed, Shannon proved that if the key is secret, the same length as the message, truly random, and never reused, then the one-time pad is unbreakable. All one-time pads suffer from serious practical drawback, known as the key distribution problem. The key itself must be established between the sender and the receiver by means of a very secure channel for example a very secure telephone line, a private meeting or hand-delivery by a trusted courrier.

Even if a secure channel is available, this security can never be truly guaranteed, a fondamental problem remains because any classical private channel can be monitored passively without the sender or receiver knowing that the eavesdropping has taken place. Since all information, including cryptographic keys, is encoded in measurable physical properties of some object or signal, classical theory leaves open the possibility of passive eavesdropping, because in principle it allows the eavesdropper to measure physical properties without disturbing them. This is not the case in quantum theory, which forms the basis for quantum cryptography.

Modern cryptographic practice rests on the use of one-way functions which are easy to evaluate in the forward direction but infeasible to compute in the reverse direction without additional information. For example, multiplying large prime numbers can be done in a time that is a polynomial function of their size, but finding the prime factors of the product is believed to require exponential time. Factoring the product of two large prime numbers can be accomplished in polynomial time on a quantum computer. However, the advancement of computing power and the advent of the quantum computer together with the vulnerability of this scheme to mathematical progress have prompted the introduction of quantum cryptography which process through the laws of quantum mechanics, ensures provably secure data transfers.

The use of physical mechanisms for cryptography is well known in quantum cryptography, based on the combinations of concept from quantum mechanics and information theory, i.e. the impossibility of cloning quantum information. The Heisenberg's uncertainty principle is exploited to designe an unconditionally secure quantum communications schemes. Quantum cryptography mades enormous progress in the technology of quantum optics, optical fibers and free space optical communication. It can be used over a classical communications channel providing a physical protection to individual bits of information as well as a hardware implemented solution. The implementation of this theoretical concept requires much practical innovation for transparent deployment into current cryptographic solutions.

The theory of quantum cryptography as well as its potential relevance and the application of prototype system at the University of KwaZulu-Natal are described and the phenomenon of single-photon interference is used to perform quantum cryptography over an optical communications link. The method of BB84 (a quantum key distribution protocol that works with qubits which are two-dimensional) is presented to solve the problem of key distribution between two parties. Theoretically, BB84 is secured under certain conditions.

The practical of id 3000 Clavis (quantum key distribution system) over installed terrestrial cables of distances 13,08 km at Cato Manor in Durban between Central Application Office and Minicipal original Office buildings and 15.6 km in Pinetown between Pinetown Civic Center and Pinetown Clinic buildings is the proof that the solution to the key distribution problem is given by quantum cryptography. The experiments in this work are the practical real quantum key distribution that produces the key which can be shared between two parties at the distances enunciated above.

PREFACE

The experimental work described in this Masters thesis was carried out in the School of Physics, University of KwaZulu-Natal, Westville Campus, from June 2006 to August 2009, under the supervision of Professor Francesco Petruccione.

These studies represent original work by the author and have not otherwise been submitted in any form for any degree or diploma to any Tertiary Institution. Where use has been made of the work of others it is duly acknowledged in the text.

DECLARATION 1 - PLAGIARISM

I, Mpinda Kabeya, declare that

1. The research reported in this thesis, except where otherwise indicated, is my original research.

2. This thesis has not benn submited for any degree or examination at any other university.

3. This thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

4. This thesis does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

   a. Their words have been re-written but the general information attributed to them has been referenced

   b. Where their exact words have been used, then their writing has been placed in italics and inside quotation marks, and referenced.

5. This thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specfically acknowledged, and the source being detailed in the thesis and in the References sections.

Signed: ....

Contents

ACKNOWLEDGEMENTS

I would sincerely like to thank my project supervisor Prof. Francesco Petruccione for his full support, inspiring ideas and encouragement. I would like to thank him for giving me the opportunity to work in the Quantum Research Group. I appreciate his valuable advice, patiente, understanding, discussions and expert guidance given to me while doing this master thesis.

Francesco Petruccione, thank you for your positive approach and enthusiasm. It was excellent having you as my supervisor, as you have many ideas and the ability to know the best way to proceed. I would like to thank you for my scholarship and organizing that I could do my Masters at the University of KwaZulu-Natal. Thank you for coming up with the original idea that forms the basis of this thesis.

A big part of my gratitude is reserved to the Head of School of Physics Prof. Sadha Pillay for allowing me to do my Master program at the University of KwaZulu-Natal.

I would like also to extend my thanks to my colleagues and friends for their encouragement and spirit support.

Thanks to everyone else in the Quantum Research Group, for never failing to answer questions, and helping me with any difficulties I had.

To me the biggest sacrifice made for this Master studies is the time I did not get to spend with my family. I thank my Mother, Mother-in-law, Uncles, Brothers and Sisters for their understanding of, and encouragement on, my aim to become a scientist.

Finally, I would like to thank my wife, Anna Kanku Ntambue, for her loving company and for sharing the stress and hardship faced by an overworked Masters student.

List of Figures

List of Tables

Chapter 1

Introduction and History

1.1 Introduction

Quantum cryptography or simply quantum key distribution (QKD) [1] is a technology that exploits a fundamental principle of quantum mechanics (observation causes perturbation) to exchange cryptographic keys between two remote parties over optical fiber networks with absolute security [2]. It is a relatively novel discipline in the fields of optical communication and security assurance of the inviolability of a law of Nature [3]. It involves subjects like quantum mechanics, optics, mathematics and computer science.

The goal of quantum key distribution is to allow two distant participants, traditionally Alice and Bob, to share a long random string of secret (commonly called the key) in the presence of an eavesdropper [4]. In principle, quantum cryptography is limited to distances of 100 km, because of losses and noise of optical fiber and detector technology. In the other context, a free-space quantum key distribution experiment over a distance of 144 km was performed and this between La Palma and Tenerife on the Canary Islands [5].

The main reason of choosing the topic Experimental Realization of Quantum Key Distribution is that, cryptography is currently not any more only the domain of military or diplomatic communications, but it is also becoming more and more important in everyday life [6]. Transfer of knowledge or sensitive information is an example of important role played by communications in, once again, everyday life. Information, often need to be secured when transferred through an insecure environment such as the internet or telephone lines.

Cryptology is defined as the mathematical science of secret communications, it has a long and distinguished history of military and diplomatic used dating back to the ancient Greeks [7]. In World War II, Allied successes in breaking the ciphers of Germany and Japan played an important part in the outcome of the conflict and the development of the modern computer [3].

One of the principal problems of cryptography is the so-called key distribution problem [5]. How do the sender and intended recipient come into possession of secret key material while being sure that third parties (eavesdroppers) cannot acquire even partial information about it? It is provably impossible to establish a secret key with conventional communications, and so key distribution has relied on the establishment of a physically secure channel (trusted carriers) or the conditional security of difficult mathematical problems in public key cryptography.

With the growth of computer networks for business transactions and communication of confidential information there is an ever increasing need for encryption to ensure that this information cannot be acquired by third parties. Remarkably, the seemingly unrelated philosophical foundations of quantum mechanics are now being brought to bear directly on the problem of communications security in the potentially practical emerging technology of quantum cryptography [8].

The aim of the presented experiment was focused on the test of a fibre optical quantum key distribution system working at 1550 nm and based on the id 3000 Clavis Quantum Key Distribution System (also known to as plug and play) setup. The stability of id 3000 QKDS over installed terrestrial cables of a distance 13,08 km was our preoccupation at Cato Manor in Durban between Central Application Office and Municipal Original Office buildings. Another test was done over a distance of 15.6 km in Pinetown between Pinetown Civic Center and Pinetown Clinic buildings. The results to these tests are presented in this thesis.

1.2 History

The story of quantum cryptography begins in the early 1960's, when Stephen Wiesner and Charles Bennett were undergraduate students together at Brandeis University [9]. Indeed, Wiesner went to graduate school at Columbia and Bennett at Harvard, they kept in touch. But during a visit in the late 60's or early 70's Wiesner [10] shared with Bennett his ideas for using quantum mechanics to make banknotes that would be impossible to counterfeit according to the laws of nature, as well as of a "quantum multiplexing" channel, which would allow one party to send two messages to another in a way that the receiving party could decide which message to read but only at the cost of destroying the other message irreversibly [11].

Wiesner in 1970, submitted his paper "Conjugate Coding" to the IEEE Transactions on Information Theory. Unfortunately, it was rejected, probably deemed incomprehensible by the editors and referees because it was written in the technical language of physicist (which must have seemed normal for a physicist!). Wiesner had expounded his ideas to Bennett, for they might otherwise have been lost forever. Instead, Bennett mentioned them occasionally to various people in the subsequent years.

On October 1979, Charles Bennet of IBM Research met Gilles Brassard of the University of Montreal at the beach of a posh hotel in San Juan, Puerto Rico. Together they have found the ways to mesh Wiesner's coding scheme with some of the new concepts of public-key cryptography [9]. Thus, was born a wonderful collaboration that was to spin out quantum teleportation, entanglement distillation [12], the first lower bound on the power of quantum computers [13], privacy amplification [14], and, of course, quantum cryptography [15, 16].

The ideas that Charles Bennet and Gilles Brassard tossed around on the beach that day resulted in the first paper ever published on quantum cryptography [17]. Indeed this was the paper in which the term "Quantum Cryptography" was coined [18, 19]. It was presented at Crypto '82 paper [17], an annual conference that had started one year earlier. Their paper triggered the belated publication of Wiesner's original paper in a special issue of the ACM Newsletter Sigact News [15, 20] that was otherwise devoted to a selection of papers from the earlier Crypto '81 conference.

The heart of quantum cryptography is a protocol for establishing a symmetric secret key between two distant parties [6]. In 1984, Charles Bennet of IBM Research and Gilles Brassard of the University of Montreal proposed a Quantum Key Distribution protocol known as BB84 [17]. BB84 took another five years to be the first convincingly successful quantum key distribution protocol (meaning that it was the first quantum key distribution scheme by which a secret common key between Alice and Bob could be established) and experimentally demonstrated by C. H. Bennett and his group in 1989 [21, 22]. They carried out this protocol in 1991 by lightwave transmission from a distance of 32 centimeters [23]. It is essential that Alice and Bob acquire the key material with a high level of confidence. This is to ensure that any third party (Eve) does not have even partial information about the random bit sequence. If Alice and Bob communicate solely through classical messages it is impossible for them to generate a certifiably secret key owing to the possibility of passive eavesdropping [24, 25]. BB84 was proved, in 1994, to be secure against eavesdropping by Dominic Mayers, Eli Biham, and Michael Ben-Or [26, 27]. It is a non-deterministic protocol, which means that it is useful only for the distribution of a random sequence.

However, secure key distribution becomes possible if they use the single-photon communication technique of quantum cryptography, or more accurately, quantum key distribution [28]. After a short historical review of quantum cryptography, we report on the quantum key distribution apparatus of UKZN and latest results obtained with it [29].

Initially, quantum cryptography was thought of by everyone mostly as a work of science fiction because the technology required to implement it was out of reach (for instance, quantum bank notes [20] require the ability to store a single polarized photon or spin-1/2 particle for days without significant absorption or loss of polarization). Unfortunately, the impact of the Crypto '82 conference had left most people under the impression that everything having to do with quantum cryptography was doomed from the start to being unrealistic.

The main breakthrough came when Bennett and Brassard realized that photons were never meant to store information, but rather transmit it (although it should be said half of Wiesner's original paper dealt precisely with the use of quantum physics for the transmission of information). This lead initially to the self-winding reusable one-time pad [30] which was still not very practical. Later, Bennett thought of the quantum key distribution channel (whose implementation is the important role played in this thesis) and Brassard designed the somewhat less realistic quantum coin-tossing protocol (which can be used to implement bit commitment) [23, 31].

Quantum cryptography was also picked up by other researchers. For instance, Crepeau and Kilian showed how the quantum channel could be used in principle (although not in practice) to implement oblivious transfer [32] in a strong way (Wiesner's original multipexing channel could leak information on both channels), zero-knowledge protocols, and secure two-party computation [33, 34].

In 1991, Ekert proposed an alternative approach to implement quantum key distribution [35] making use of EPR (Einstein-Podolsky-Rosen) and Bell's theorem. A simplified version of his scheme is shown in [36] to be equivalent to the idealized quantum key distribution protocol originally put forward by Bennett and Brassard in 1984 [23]. Let us also mention that Bennett, Brassard, and Crepeau have developed a practical quantum protocol to achieve oblivious transfer, bit commitment and coin-tossing [32, 37].

We shall evaluate in Chapter 2, the encryption of messages to render them unintelligible to third parties and their authentification to certify that they have not been modified. Encryption and authentification are two main goals of cryptography that can be accomplished with provable security if the sender (Alice) and the recipient (Bob) are in possession of a shared key (secret random bit sequence) that they use as a parameter in a cryptographic algorithm.

Chapter 3 shows that the key distribution problem cannot be solved classically since the unconditionally secure cryptographic algorithm requires a random key, which has to be as long as the message itself. Quantum mechanics with its property of hiding some information shows the way how to solve this problem using Heisenberg's uncertainty principle.

However, provably secure key distribution becomes possible with quantum communications, as will be shown in Chapter 4. It is only the procedure to build key distribution that is accomplished by quantum cryptography, and not the transmission of an encrypted message itself. Hence, a more accurate name is quantum key distribution (QKD).

The Chapter 5 of this Thesis reviews the theory of quantum key distribution, its potential applications and the development of an experimental prototype system at the University of KwaZulu-Natal, which utilises the phenomenon of single-photon interference to perform quantum cryptography over an optical fiber communications link. We shall answer the questions such as: What is quantum about quantum cryptography? What are the limitations imposed by practical issues? At the end, some results from the tests done at Cato Manor close to Howard College and at Pinetown are given in this Chapter.

Chapter 2

Classical Cryptography

This chapter introduces the concept of classical cryptography and its now famous protagonists, in terms of communication technology, the sender of a message is often referred to as Alice and the receiver called Bob, along with its leading antagonist, the eavesdropper typically referred to as Eve. It also goes over a brief history of classical cryptography and its various forms. The concept of key distribution - private and public - is then introduced.

2.1 Introduction

Cryptography is the study of reading and writing messages in code or secret ciphers [38]. It is considered as the art and science of data protection. Cryptography can be subdivided in two main parts: classical and quantum. Classical cryptography is based on mathematical complex problems which can be solved in principle. On the other hand Quantum Cryptography relies on laws of physics [6]. It is necessary to describe some of the important features of cryptography before explaining the significance of quantum cryptography.

Historically, Cryptography arose as a means to enable parties to maintain privacy of the information they send to each other, even in the presence of an adversary with access to the communication channel [39]. While providing privacy remains a central goal, the field has expanded to encompass many others, including not just other goals of communication security, such as guaranteeing integrity and authenticity of communications, but many more sophisticated and fascinating goals.

Once largely the domain of the military, cryptography is now in widespread use, and everyone is likely to have used it even if he doesn't know it. When you shop on the Internet, for example to buy a book at www.amazon.com, cryptography is used to ensure privacy of your credit card number as it travels from you to the shop's server. In electronic banking, cryptography is used to ensure that your transaction cannot be forged [40].

Cryptography has been used almost since writing was invented. For the larger part of its history, cryptography remained an art, a game of ad hoc designs and attacks. Although the field retains some of this flavor, the last twenty-five years have brought in something new. To give an overview over classical cryptography and the motivation for the need of quantum cryptography, we shall introduce in this chapter some basic cryptographic algorithms.

2.2 Terminology

Briefly, Cryptography is about constructing and analyzing protocols which overcome the influence of adversaries. Suppose that you are trying to solve some cryptographic problem. The problem will usually involve some number of parties [41].

2.2.1 Parties

The cryptographers often like to anthropomorphize the parties, giving them names like "Alice" and "Bob" and referring to them as though they are actual people. They do this because it's convenient and fun. But one shouldn't think that it means that the parties are really human beings. They might be, but they could be lots of other things, too. Like a cell phone, a computer, a process running in a computer, an institution, or maybe a little gadget sitting on the top of your television set. We usually think of the parties as the "good guys," and we want to help them accomplish their goal. We do this by making a protocol for the parties to use.

2.2.2 Protocols

A cryptographic protocol is essentially a program, but it is a distributed program which tells each party how to behave. A protocol instructs the parties what to do, but it doesn't tell the adversary what to do. That is up to her.

A protocol can be probabilistic: This means it can make random choices. To formalize this we usually assume that the model of computation that allows a party to specify a number $n \geq 2$ and then obtain a random value $i \longleftarrow \{0, 1, ..., n-1\}$. This notation means that i is a random value from the indicated set, all values being equally likely.

A protocol can also be stateful: This means that when a party finishes what he is doing he can retain some information for next time that he is active. When that party runs again he will remember the state that he was last in. So, for example, one could have a party that knows "this is the first time I have been run," "this is the second time I have been run," and so on. When we formalize protocols, they are usually tuples of algorithms. The actual formalization will vary from problem to problem.

For example, a protocol for symmetric encryption is not the same "type" of thing for a protocol for a telephone coin flip. How can we devise and analyze protocols? The first step is to try to understand the threats and the goals for our particular problem. Once we have a good idea about these, we can try to find a protocol solution.

2.2.3 Adversaries

The adversary is the agent that embodies the "source" of the threat. Adversaries aim to defeat the protocol's goals. Protocols, in turn, are designed to surmount the behavior of adversaries. It is a game; a question of who is clever, protocol designer or adversary. The adversary is usually what we focus on. In rigorous formalizations of cryptographic problems, the parties may actually vanish, being "absorbed" into the formalization. But the adversary will never vanish, she will be at center stage. That is why cryptography is largely about thinking about adversary. What can one do, and what can't he do? What is he trying to accomplish? We have to answer these questions before we can get very far.

The adversary might represent an actual person, but it might just as well be an automated attack program, a competitor's company, a criminal organization, a government institution, one or more of the protocol's legitimate parties, a group of friendly hackers, or merely some unlucky circumstances conspiring together, not controled by any intelligence at all. By imagining a powerful adversary we take a pessimistic view about might go wrong. In that case, we should at least be achieving high reliability. After all, if a powerful adversary can't succeed disrupting our endeavors, then neither will noisy lines, transmission errors due to software bugs, unlucky message delivery times, careless programmers sending improperly formatted messages, and so forth [40].

The usual situation is the following one (see Fig. 2.1): Party A (Alice) wants to send a message to party B (Bob) in a secure way. An eavesdropper (Eve) or Adversary who gets hold of the message should not be able to gain any information about its contents [42].

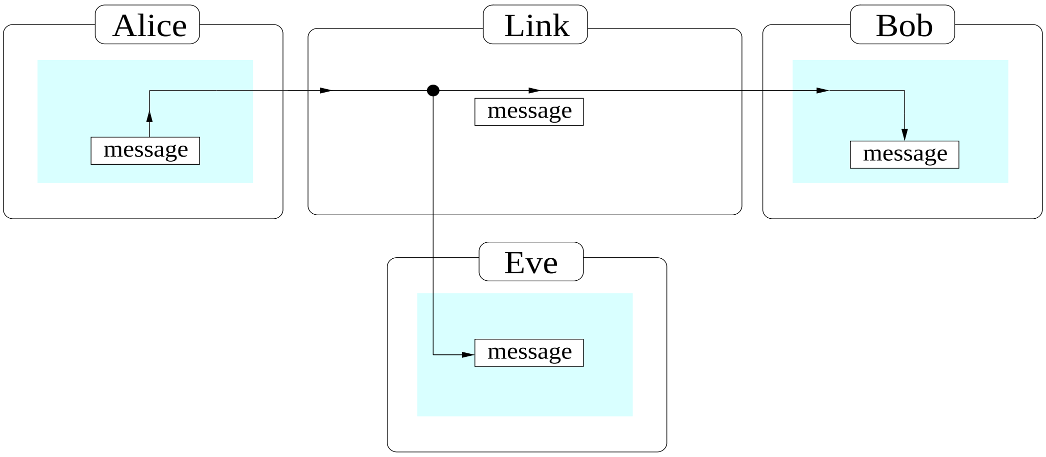

FIG. 2.1: Alice sends a plaintext message to Bob with an Eavesdropper (Eve) present.

2.3 Classical Encryption Techniques

2.3.1 Rudiments of Encryption Vocabulary

Encryption or enciphering is the process by which plaintext is converted into ciphertext. That means the process of disguising the message that Alice writes in plaintext or clear text, such that the information is hidden. Encryption is used with a secret key that is known only by the sender and receiver of the sensitive information. The method of scrambling information to secure it against onlookers is called encryption. The encrypted message is the so-called ciphertext [43].

An Encryption algorithm is the sequence of data processing steps that go into transforming plaintext into ciphertext. Various parameters used by an encryption algorithm are derived from a secret key.

Decryption or deciphering is the reversal of the encryption process performed by Bob. Decryption requires the knowledge of a secret key. It is recovering plaintext from ciphertext. The method of descrambling information from a previous encryption is called decryption. The terms encipher and decipher are synonymously used for encryption and decryption.

A Decryption algorithm is the sequence of data processing steps that go into transforming ciphertext back into plaintext. Various parameters used by a decryption algorithm are derived from the same secret key that was used in the encryption algorithm. In classical cryptography for commercial and other civilian applications, the encryption and decryption algorithms are made in public. The encryption vocabulary is depicted in Fig. 2.2.

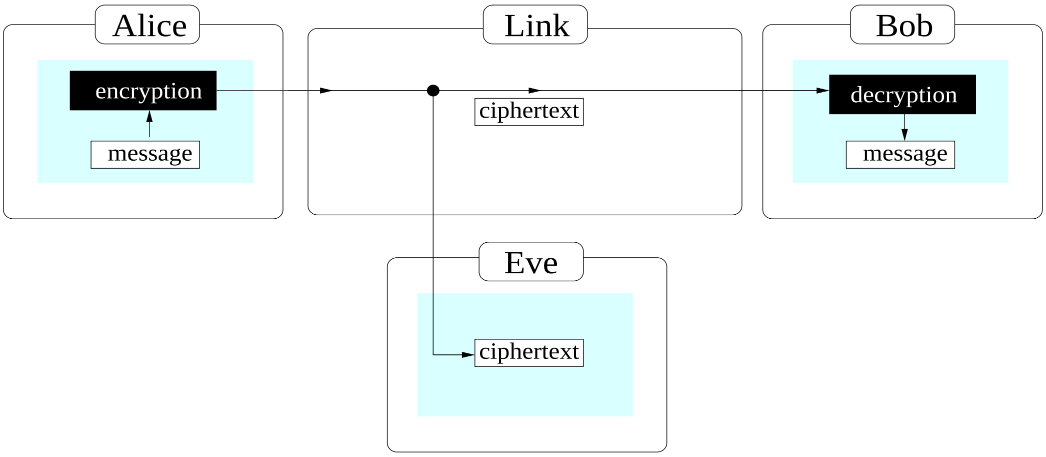

FIG. 2.2: Alice encrypts her message and sends the ciphertext to Bob. The message can be decrypted and read by Bob, the eavesdropper should not be able to do so.

Plaintext is the information to be secured.

Ciphertext is the encrypted output, meaning the scrambled information after an encryption process using a cryptographic algorithm and a secret key.

Good cryptographic methods assure us that we can keep our secrets from others. That is, Alice and Bob's encrypted files remain private between them as long their secret key stays secret. Modern-day cryptographers use the term confidentiality to mean that encrypted secrets aren't available to unauthorized users.

A block cipher processes a block of input data at a time and produces a ciphertext block of the same size.

Cryptanalysis means "breaking the code". It relies on a knowledge of the encryption algorithm and some knowledge of the possible structure of the plaintext (such as the structure of a typical inter-bank financial transaction) for a partial or full reconstruction of the plaintext from ciphertext. The goal is to infer the key for decryption of future messages. The precise methods used for cryptanalysis depend on whether the "attacker" has just a piece of ciphertext, or pairs of plaintext and ciphertext, how much structure is possessed by the plaintext, and how much of that structure is known to the attacker. All forms of cryptanalysis for classical encryption exploit the fact that some aspect of the structure of plaintext may survive in the ciphertext.

A brute-force attack is when encryption and decryption algorithms are publicly available, this means trying every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

Key space is the total number of all possible keys that can be used in a cryptographic system. For example, Data Encryption Standard (DES) is a widely used method of data encryption using a private (secret) key that was judged so difficult to break by the U.S. government that it was restricted for exportation to other countries. In general, DES takes as input a 64 bit key (binary digits "0"s or "1"s), of which only 56 bits are randomly generated and used directly by the algorithm. So the key space is of size 2^{56}, which is approximately the same as 7.2×10^{16} [25, 24].

Cryptology: Cryptography and Cryptanalysis together constitute the area of cryptology.

2.3.2 The Human Communication Channels

Humans can communicate in different ways, i.e. using different human communication channels, depending on the requirements. For example, if one being needs to reach another being for urgent matters, he must choose a channel with high availability and low latency such as a telephone link. But, if he would transfer an amount of money, he must establish a reliable authentication by going to the desk to encounter the clerk of the bank [44]. (Currently, he can use the Internet with prior established security association.)

The security of communication channels can be characterized by some security attributes which are defined below. Assume a communication channel between a sender, called Alice, and a receiver, called Bob. A message m is sent on the input and a message $\widehat{m}$ can be read on the output. We define the following security properties:

Confidentiality means that only owners of a shared key can decrypt a computer file that has been encrypted with the shared key; in another word only the legitimate receiver, i.e. Bob, can read the message $\widehat{m}$.

Authenticity is that only the legitimate sender, i.e. Alice, can input a message m into the channel. This is often combined with integrity, i.e. $m = \widehat{m}$ can only be issued by Alice. Authentication stops masquerading imposters.

Integrity assumes that the received message $\widehat{m}$ is the same as the input message m meaning that a file was not changed during transit and is also called message authentication.

Nonrepudiation assurance that the sender cannot deny a file was sent, this cannot be done with the secret key alone.

Freshness means that the received message $\widehat{m}$ was not received before.

Liveliness assumes that a message m which has been sent by Alice will eventually be delivered to Bob.

Timeliness assumes that a message m which has been sent by Alice will be delivered immediately to Bob.

In addition, to compare the different human communication channels, it is necessary to define other properties which characterize the usability of these channels. These communication properties are defined below.

The cost represents the required amount of money spent to establish the communication channel and to transmit a message from Alice to Bob.

The availability expresses the fact that the channel can easily be established at any time.

The speed rate is the amount of data that can be transfered from Alice to Bob for a fixed time duration.

The latency is the amount of time between the moment when Alice sends the message and the moment when Bob receives it.

Using the above denitions, it is possible to compare the common human communication channels in a cryptographic way.

Face to face conversation allows perfect authentication, perfect integrity and in certain cases, confidentiality. In addition, freshness, liveliness, and timeliness are trivially ensured. However, this channel can have a very high cost if, for example, the two persons are far from each other. For the same reasons, the availability is also bad. Note that the communication has no latency but a low speed rate. In conclusion, this human channel achieves high security but low throughput.

Telephone is like a face to face conversation but allows a third party to spy the communication. Thus, this channel does not guarantee confidentiality. On the other hand, it has a much lower cost and a higher availability. In short, it guarantees authentification assuming that both users can recognize the remote voice.

Mail, like a postcard or a parcel, is not confidential either. It can be easily lost and thus this channel does not guarantee liveliness. We can consider that a handwritten mail achieves authentification by assuming that the recipient can identify the writing. As for telephone, this channel guarantees availability but has a long latency.

Electronic mail is the worst communication channel in terms of security, it protects nothing by itself. However, it is the easiest communication channel and its costs is very small (too small if we consider the spam phenomenon), the availability and the speed rate are very high.

2.4 Early Approaches to Cryptography

2.4.1 Blocks of Classical Encryption Techniques

There are two building blocks of all classical encryption techniques, substitution and transposition.

- Substitution means replacing an element of the plaintext with an element of ciphertext.
- Transposition means rearranging the order of appearance of the elements of the plaintext. Transposition is also referred to as permutation.

2.4.2 Caesar Cipher

Caesar cipher is the earliest known example of a substitution cipher. See the Table 2.1 in which each character of a message is replaced by a character three position down in the alphabet.

plaintext:	are	you	ready
ciphertext:	DUH	BRX	UHDGB

TABLE. 2.1: Change of plaintext in ciphertext.

If we represent each letter of the alphabet by an integer that corresponds to its position in the alphabet, the formula for replacing each character p of the plaintext with a character C of the ciphertext, in the example above, can be expressed as

$$C = E(3, p) = (p + 3) \bmod 26. \tag{2.1}$$

A more general version of this cipher that allows for any degree of shift would be expressed by

$$C = E(k, p) = (p + k) \bmod 26. \tag{2.2}$$

The formula for decryption would be

$$p = D(k, C) = (C - k) \bmod 26. \tag{2.3}$$

In these formulas, "k'' would be the secret key. The symbols "E'' and "D'' represent encryption and decryption.

2.4.3 Vernam Cipher

Classical cryptography can provide an unbreakable cipher, which resists adversaries with unlimited computational and technological power-the Vernam cipher. The Vernam cipher was invented in 1917 by an engineer Gilbert S. Vernam [24], who thought it would become widely used for automatic encryption and decryption of telegraph messages.

The Vernam cipher belongs to the symmetric secret-key ciphers, i.e., the same key is used for both, encryption and decryption. The principle of the cipher is that if a random key is added to a message, the bits of the resulting string are also random and carry no information about the message. If we use the binary logic, unlike Vernam who worked with a 26-letters alphabet, the encryption algorithm E can be written as

$$E_K(M) = (M_1 + K_1, M_2 + K_2, ..., M_n + K_n)\, mod\, 2\,, \tag{2.4}$$

where $M = (M_1, M_2, ..., M_n)$ is the message to be encrypted, and $K = (K_1, K_2, ..., K_n)$ is the key consisting of random bits. The message and the key are added bitwise modulo 2, or exclusive OR without carries. The decryption D of ciphertext $C = E_K(M)$ is identical to encryption, because double modulo-2 addition is identity, therefore

$$M = D_K(C) = (C_1 + K_1, C_2 + K_2, ..., C_n + K_n)\, mod\, 2\,. \tag{2.5}$$

For this system to be unconditionally secure, three requirements are imposed on the key:

1. the key must be as long as the message;
2. it must be purely random;
3. it may be used once and only once.

This was shown by Claude E. Shannon [45], who laid the foundations of communication theory from the cryptographic point of view and compared various cryptosystems with respect to their secrecy. Until 1949 when his paper was published, the Vernam cipher was considered unbreakable, but it was not mathematically proved. If any of these requirements is not fulfilled, the security of the system is jeopardized. A good example is the revelation of the World War II atomic spies because of repetitive use of the key incorrectly prepared by the KGB.

The main drawback of the Vernam cipher is the necessity to distribute a secret key as long as the message, which prevented it from wider use. The cipher has so far found applications mostly in the military and diplomatic services. As will be shown in the next Section, the difficulty of secure key distribution can be removed by virtue of quantum key distribution. The Vernam cipher then turns invaluable because of its capability to provide unconditional security and ease of use.

2.4.4 Cryptographic Algorithm and Secret Key

In this section we describe the classical cryptographic communication systems, as illustrated in Figure 2.3

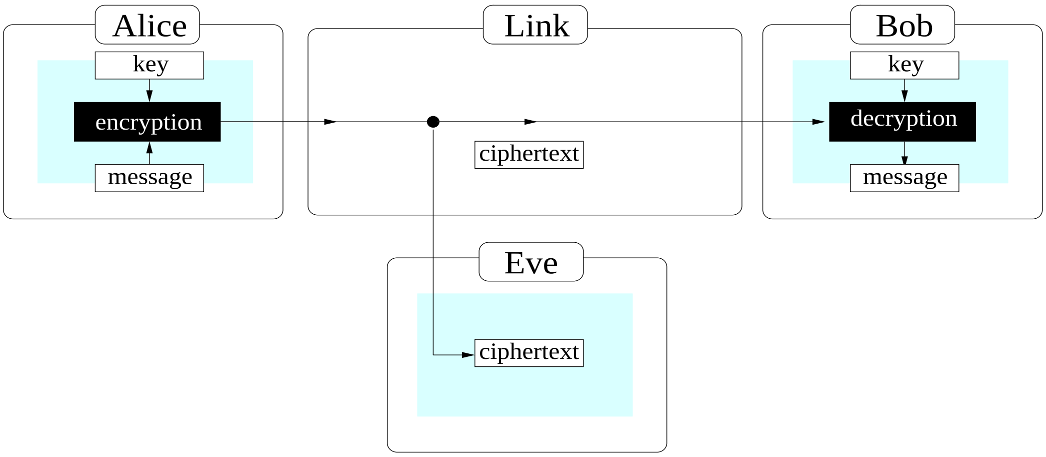

FIG. 2.3: The encryption algorithm and the decryption algorithm have two inputs: Message or ciphertext and a key, which both parties share. The employed algorithm may be publicly known, only the key has to be kept secret.

Alice, the sender, encrypts her plaintext P into ciphertext C using a secret key K which she shares only with Bob, and sends the ciphertext C over an insecure channel on which the evil Eve is ever vigilantly eavesdropping. Bob, the receiver, receives the ciphertext C, and uses the secret key K, shared by him and Alice only, to decrypt the ciphertext C into plaintext P.

In the classical cryptographic communication system Alice and Bob must first communicate over a secure channel to establish a secret key K shared only by Alice and Bob before they can communicate in secret over the insecure channel.

Cryptographic Algorithm or cipher is the procedure that Alice uses to encrypt the message. In general, there are two algorithms, one for the encryption and one for decryption. The restricted algorithm is in security if the algorithm itself is kept secret. This is why in 1883, Kerckhoffs Auguste van Nieuwenhof proposed in his book (*La cryptographie militaire*) that cryptographic methods should be divided into algorithms and keys (see the description in the Section 2.6). This is, only the key has to be kept secret.

Secret Key is a secret piece of information which is shared by two parties and used when securely exchanging information takes place. To be effective, the secret key is smaller than the information to be shared. The important thing is that it is used in conjunction with a cryptographic algorithm to encrypt or decrypt sensitive data in classical cryptography, to make the ciphertext depend strongly on the key itself. It is for this reason that classical cryptography is also referred to as symmetric key cryptography.

Kerckhoffs' principle: The algorithm may be publicly known when a keyed algorithm is used, but the security of the cipher depends on the key.

Practical Secrecy

A cryptographic communication system is practically secure if the encryption scheme can be broken after X years, where X is determined by one's security needs and by existing technology. Practically secure cryptographic systems have existed since antiquity [46]. One example would be the Caesar cipher used by Julius Caesar during Grallic wars, a cipher that was difficult for his opponents to break at that time, but easily breakable by today's standards. A modern day example of a practically secure classical cryptographic system is the Digital Encryption Standard (DES) which has just recently been broken [47]. For this and many reasons, DES is to be replaced by a more practically secure classical encryption system, the Advanced Encryption Standard (AES), which will be replaced by an even more secure cryptographic system.

Perfect Secrecy

A cryptographic communication is said to be perfectly secure if the ciphertext C gives no information what so ever about the plaintext P, even when the design of the cryptographic system is known. In mathematical terms, this can be stated succintly with the equation:

$$Prob(P|C) = Prob(P) \tag{2.6}$$

In other words, the probability of plaintext P given ciphertext C, written $Prob(P|C)$, is equal to the probability of the plaintext P. An example of a perfectly secure classical cryptographic system is the Vernam Cipher, better known as the One-Time-Pad. The plaintext P is a binary sequence of zeroes and ones, i.e.,

$$P = P_1, P_2, P_3, \dots, P_n, \dots$$

The secret key K consists of a totally random binary sequence of the same length, i.e.,

$$K = K_1, K_2, K_3, \dots, K_n, \dots$$

The ciphertext C is the binary sequence

$$C = C_1, C_2, C_3, \dots, C_n, \dots$$

obtained by adding the sequences P and K bitwise modulo 2, i.e.,

$$C_i = P_i + K_i \; mod \; 2 \tag{2.7}$$

for $i = 1, 2, 3, \dots$

P	0110	0101	1101
K	1010	1110	0100
$P \oplus K = C$	1100	1011	1001

TABLE. 2.2: Ciphertext obtained by adding plaintext (P) and the secret key (K).

For example,

This cipher is perfectly secure if the key K is totally random and shared only by Alice and Bob. The only problem with the one-time-pad is that long bit sequences must be sent over a secure channel before it can be used.

2.5 Secure Communication

2.5.1 Introduction

Secure communication has become such a common thing that people are barely aware of it when dealing with electronic shopping, bank account management or e-mail transmission. Examples of secret codes range back to the times of the ancient Egyptians who used modified hieroglyphs to conceal their messages [48]. Since then, cryptography become the art of transmitting a ciphered message from a sender to a receiver, allowing no one else to eavesdrop [45].

2.5.2 Cryptosystems

A cryptosystem [49, 50] is a mechanism or convention that allows two or more legitimate users to exchange messages secretly, but these users must be able to learn the content of the messages.

The classical Shannon's cryptosystem is only secure if the eavesdropper does not have access to the secret channel as it is shown into the diagram (Figure 2.4) below.

The only protocol proven to be unconditionally secure is the One Time Pad (OTP). Other known protocols, including Public Key protocols, are at best computationally secure. Eve is supposed to be able to copy perfectly and without interference [6].

Every message, m, is subjected to an encrypting operation, E, to produce a so-called ciphertext or cryptogram. To recover the message corresponding to a given ciphertext, a decrypting operation D must be performed.

Formally, we have

$$c = E(m), \tag{2.8}$$

and

$$m = D(c). \tag{2.9}$$

In a symmetric cryptosystem, these two operations require one more argument: the common key k. The key is a unique sequence of bits known only to the legitimate users of the system. Usually, the procedures E and D are publicly known, and the key is the only piece of information needed by an enemy to recover the contents of a transmitted message. The basic scenario that arises in most cryptographic applications is the following:

1. The legitimate sender of a message m uses the key k to produce a ciphertext

$$c = E(m, k)\,. \tag{2.10}$$

2. An enemy tries to recover the value of m by guessing the value of k, and performing

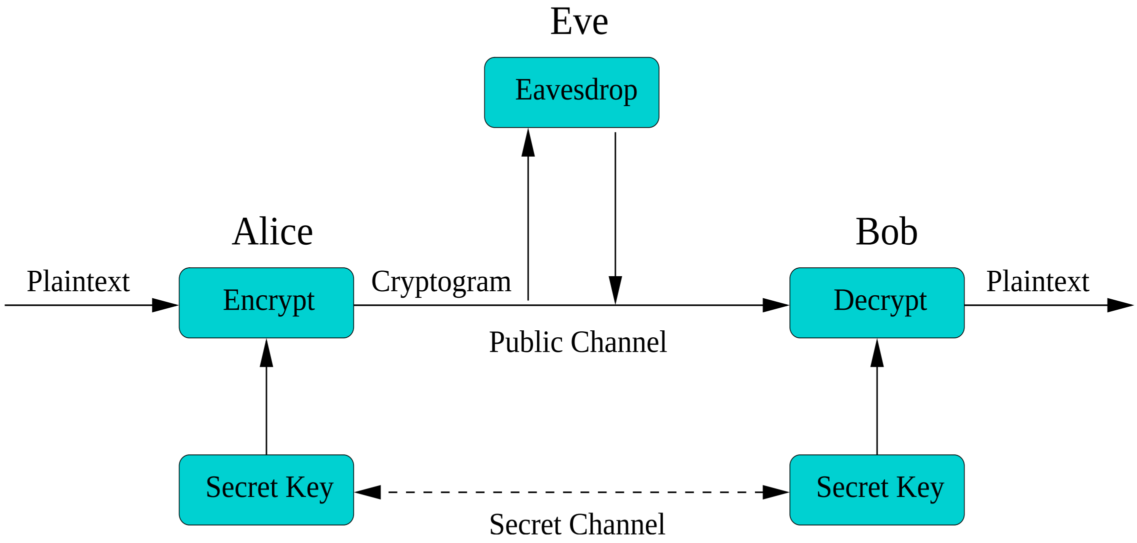

FIG. 2.4: Classical Shannon's Cryptosystem

$$D(c, k)\,.$$

3. The legitimate receiver of the message uses the key k to recover the message

$$m = D(c, k)\,. \tag{2.11}$$

Classical cryptography is concerned to a great extent with developing operations E and D that are practically impossible to compute unless k is known. The enemy is assumed to have limited computational power, and limited time on his hands.

A perfect, or unconditionally secure cryptosystem, cannot be broken even in the face of unlimited time and computational power. The standard example of a perfect cryptosystem is the Vernam cipher, or one-time pad.

As an illustration of the one-time pad, consider the message, key and ciphertext as binary strings, such as 010 or 110111. To encrypt a message m with a key k, we need to perform a bitwise XOR operation on these two values. For example,

if $m = 010$ and $k = 110$, then

$$c = m \text{ XOR } k = 100\,. \tag{2.12}$$

In other words, the encrypting operation for the one-time pad is $E(m, k) = m$ XOR k. To recover the original message from c, the XOR operation is applied again, this time on c and k: if $c = 100$ and $k = 110$, then

$$m = c \text{ XOR } k = 010\,. \tag{2.13}$$

So, the decrypting operation is again, an application of exclusive-or:

$$D(c, k) \;=\; c \text{ XOR } k\,. \tag{2.14}$$

The one-time pad is difficult to use in practice because a new secret key must be issued prior to every communication, and the key becomes too long for larger messages. Assuming that the problem of key length does not matter much, the major problem is the random key which must be truly secret at all the time. This aspect of (symmetric) cryptography is referred to as the key distribution problem.

2.5.3 Key Distribution Problem

The One-Time Pad is a generalization of the substitution cipher that advances each letter by a random number of positions in the alphabet. These random numbers then form a cryptographic key (as long as the message) that must be shared between the sender and recipient. The Vernam cipher offers unconditional security against adversaries, it faces the problem of how to securely distribute the key itself.

Since the security of the one-time pad is only dependent on the secrecy of the key, one has to be absolutely sure, that a potential eavesdropper has no information at all about the key. So the key distribution method has to be of least as secure as the one-time pad itself. There is no efficient classical method to fulfil this requirement.

At this point, a new surge of interest in cryptography was triggered by the upswing in electronic communications in the late 70s of the 20th centry. It became essential to enable secure communication between users who have met never before and share no secret key. The question was how to distribute the key in a secure way. A solution was found by Whitfield Diffie and Martin E. Hellman who invented the concept of public-key distribution in 1976 [41]

2.6 Modern Cryptography

Cryptography is traditionally associeted only with keeping data secret. However, modern cryptography can be used to provide many security services, such as electronic signatures and ensuring that data has not been modified.

This section describes cryptography as a tool for satisfying a wide spectrum of computer security needs and requirements. It also describes fundamental aspects of the basic cryptographic technologies and some specific ways cryptography can be applied to improve security [51].

2.6.1 Basic Cryptographic Technologies

Cryptography relies upon two basic components: an algorithm (or cryptographic methodology) and a key [52]. In modern cryptographic systems, algorithms are complex mathematical formulae and keys are strings of bits. For two parties to communicate, they must use the same algorithm (or algorithms that are designed to work together). In some cases, they must also use the same key. Many cryptographic keys must be kept secret; sometimes algorithms are also kept secret.

There are two basic types of cryptography: "secret key" and "public key cryptography".

- In secret key systems (also referred to as symmetric cryptography), the same key is used for both encryption and decryption.
- In public key systems (also referred to as asymetric cryptography), each party gets a pair of keys, one called the public key and other called the private key [41].

Table 2.2 compares some of the distinct features of secret and public key systems. Both types of systems offer advantages and disadvantages, and often, are combined to form a hybrid system to exploit the strengths of each type [51].

DISTINCT FEATURES	**SECRET KEY CRYPTOGRAPHY**	**PUBLIC KEY CRYPTOGRAPHY**
NUMBER OF KEYS	Single key.	Pair of keys.
TYPES OF KEYS	Key is secret.	One key is private, and one key is public.
PROTECTION OF KEYS	Disclosure and modification	Disclosure and modification for private keys and modification for public keys.
RELATIVE SPEEDS	Faster.	Slower.

TABLE. 2.3: Distinct features of secret and public key systems.

To determine which type of cryptography best meets its needs, an organization first has to identify its security requirements and operating environment.

Secret key systems are often used for bulk data encryption and public key systems for automated key distribution. Although public key cryptography does not require users to share a common key, secret key cryptography is much faster: equivalent implementations of secret key cryptography can run 1,000 to 10,000 times faster than public key cryptography.

To maximize the advantages and minimize the disadvantages of both secret and public key cryptography, a computer system can use both types in a complementary manner, with each performing different functions. Typically, the speed advantage of secret key cryptography means that it is used for encrypting data. Public key cryptography is used for applications that are less demanding to a computer system's resources, such as encrypting the keys used by secret key cryptography (for distribution) or to sign messages.

2.6.2 Public-Key Cryptography

Public key cryptography is a modern invention and requires the use of advanced mathematics, it uses a pair of keys for each party. One of the keys of the pair is "public" and the other is "private". Therefore, encryption and decryption is carried out using these two different keys. The public key can be made known to other parties; the private key must be kept confidential and must be known only to its owner. Both keys, however, need to be protected against modification. Public key cryptography is particularly useful when the parties wishing to communicate cannot rely upon each other or do not share a common key [53].

There are several public key cryptographic systems. One of the first public key systems get the names of Rivest, Shamir, and Adleman (RSA), which can provide many different security services. The Digital Signature Standard (DSS) is another example of a public key system.

The ease of use of public-key cryptography, in turn, stimulated the boom of electronic commerce during the 1990s. As we shall see, this solves one of the most vexing problems associated with symmetric-key cryptography - the problem of key distribution. With public key cryptography, all parties interested in secure communications can publish their public keys.

Party A, if wanting to communicate confidentially with party B, can encrypt a message using $B's$ publicly available key. Such a communication would only be decipherable by B as only B would have access to the corresponding private key. This is illustrated by the communication link in Figure 2.5:

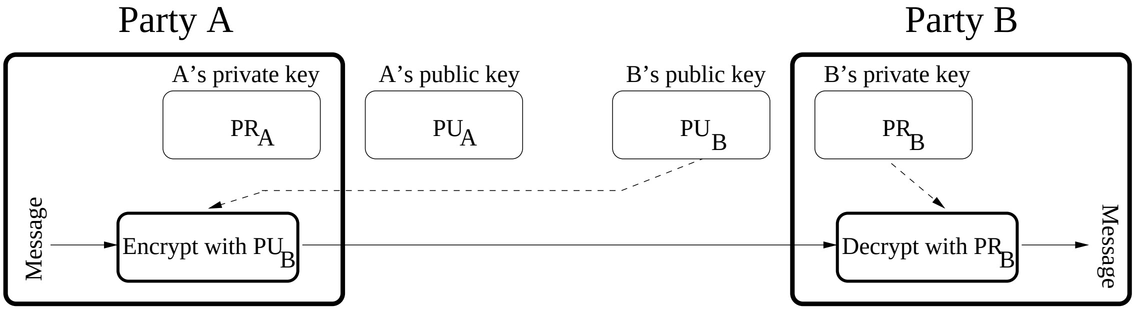

FIG. 2.5: When only confidentiality is needed to send the message, party A use the party $B's$ public key to emcrypt the message, and B use his own private key to decrypt it.

Party A, if wanting to send an authenticated message to party B, would encrypt the message with $A's$ own private key. Since this message would only be decipherable with $A's$ public key, that would establish the authenticity of the message - meaning that A was indeed the source of the message. This is illustrated by the communication link in Figure 2.6.

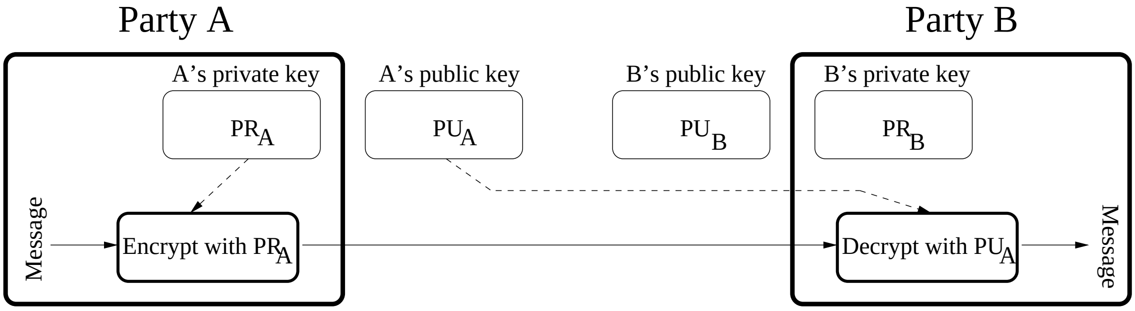

FIG. 2.6: When only authentication is needed to send the message, party A his own private key to encrypt the message and party B use the party $A's$ public key to decrypt it.

The communication link of Figure 2.7 shows how public-key encryption can be used to provide both condentiality and authentication at the same time. Note again that confidentiality means that we want to protect a message from eavesdroppers and authentication means that the recipient needs a guarantee as to the identity of the sender.

As shown in Figure 2.7, let us say that A wants to send a message M to B with both authentication and confidentiality. The processing steps undertaken by A to convert M into its encrypted form C that can be placed on the wire are:

$$C = E(PU_B, E(PR_A, M)), \tag{2.15}$$

where $E(.,.)$ stands for encryption. The processing steps undertaken by B to recover M from C are

$$M = D(PU_A, D(PR_B, C)). \tag{2.16}$$

where $D(.,.)$ stands for decryption.

The sender A encrypting his/her message with its own private key PR_A provides authentication. This step constitutes A putting his/her digital signature on the message. (Instead of applying the private key to the entire message, a sender may also "sign" a message by applying his/her private key to just a small block of data that is derived from the message to be sent).

The sender A further encrypting his/her message with the receiver's public key PU_B provides confidentiality. Of course, the price paid for achieving confidentiality and authentication at the same time is that now the message must be processed four times in all for encryption/decryption. The message goes through two encryptions at the sender's place and two decryptions at the receiver's place. Each of these four steps involves separately the computationally complex public-key algorithm.

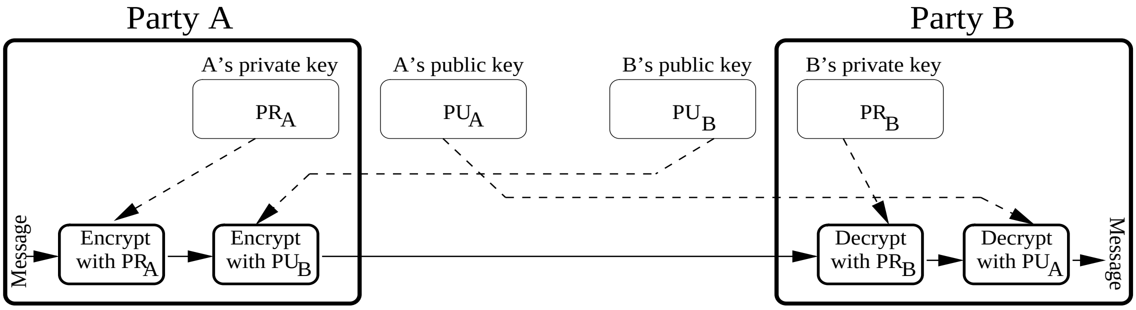

FIG. 2.7: When both confidentiality and authentication are needed, party A use his own private key for authentication and $B's$ public key for confidentiality to encrypt the message, mean while party B use his own private key and $A's$ public key to decrypt the message.

In these figures, $A's$ public and private keys are designated PU_A and PR_A while $B's$ public and private keys are designated PU_B and PR_B.

Note that public-key cryptography does not make obsolete the more traditional symmetric-key cryptography. Because of the greater computational overhead associated with public-key cryptosystems, symmetric-key systems will continue to be used for the foreseeable future. However, it is generally agreed that public-key encryption is indispensable for key management and digital signature applications.

In public-key cryptography, the need for sender and receiver to share a secret key is eliminated. All communications involve only public keys, and no private key is ever transmitted or shared. Anyone can send a confidential message by using public information, but the message can only be decrypted with a private key which is in the sole possession of the intended recipient.

2.6.3 Public-Key Cryptography Weakness

The security of public-key cryptography rests on various computational problems, which are believed to be intractable. The weakness of this system is based on the fact that the private key is always linked mathematically to the public key. Therefore, it is always possible to attack a public-key system if the eavesdropping includes sufficiently large computational resources.

The encryption and decryption algorithms utilize the so-called one-way functions. One-way functions are mathematical functions that are easy to compute in one direction, but their inversion is very difficult. It is, e.g., very easy to multiply two prime numbers, but to factor the product of two large primes is already a difficult task [38].

Other public-key cryptosystems are based, e.g., on the difficulty of the discrete logarithm problem in Abelian groups on elliptic curves or other finite groups. However, it is important to point out that no “one-way function” has been proved to be one-way; they are merely believed to be. Public-key cryptography cannot provide unconditional security. We speak about computational security [54].

2.6.4 Secret-Key Cryptography

Secret-key cryptography can provide an unbreakable cipher which resists adversaries with unlimited computational and technological power. As an example, coding will be explained for the Vernam cipher. The Vernam cipher adds a random key to every message, the bits of the resulting string are also random and carry no information about the message.

Thereby, the message and the key are added bitwise modulo 2 (equivalent to a XOR logic gate $\oplus$). Then, decryption is identical to encryption, since double modulo-2 addition yields identity. See the Table 2.4, where M is the message to encrypt, K is the secret key allowing the encryption of the message, C the cipher and D the deciphered message. Hence, $C = M \oplus K$, $D = C \oplus K$ and $M = D$.

M	0000	1100	1111
K	0011	0110	0101
C	0011	1010	1010
K	0011	0110	0101
D	0000	1100	1111

TABLE. 2.4: Secret key used to encrypt and decrypt the message.

For this system to be unconditionally secure, three requirements are imposed on the key:

1. the key must be at least as long as the message,
2. it must be purely random and unpredictable,
3. and may be used once and only once (hence the term “One-Time”).

If any of these requirements is not fulfilled, the security of the system is jeopardized. For example, if the key randomness is generated by some known algorithm, one can easily find the key matching the cipher. If the key is used several times, statistical studying can help to uncover information about the key. However, the main drawback of the Vernam cipher is the necessity to securely distribute a secret key as long as the message. Anyone who intercepts the key in transit can read, modify, and forge all messages encrypted with this key.

So the built of quantum computers is possible to perform calculations in massively parallel ways, leading to the known possibility of factoring prime numbers efficiently (using shor's algorithm, [55, 56]). A quantum computer is a computational device that uses the phenomena of quantum physics to perform extremely efficient computations.

2.6.5 Hybrid Cryptographic Systems

The public and secret key cryptography have relative advantages and disadvantages. Although, the public key cryptography does not require users to share a common key meanwhile the secret key cryptography is much faster. The equivalent implementations of secret key cryptography can run 1,000 to 10,000 times faster than public key cryptography [51].

Secret key systems are often used for bulk data encryption and public key systems for automated key distribution. To maximize the advantages and minimize the disadvantages of both secret and public key cryptography, a computer system can use both types in a complementary manner, with each performing different functions.

Typically, the speed advantage of secret key cryptography means that it is used for encrypting data. Public key cryptography is used for applications that are less demanding to a computer system's resources, such as encrypting the keys used by secret key cryptography (for distribution) or to sign messages.

2.7 RSA Algorithm for Public-Key Cryptography

Based on the property of positive integers, the RSA algorithm was invented in 1977 by Rivest, Shamir and Adleman [57]. Since then, it has become the most popular form of public-key cryptography [58, 59].

Suppose we decide to use a number n as the modulus for modular arithmetic, and suppose we choose an integer e just on the basis that it be coprime to $\phi(n)$, and then suppose we derive from e its multiplicative inverse d as stated below:

- Find two large integers p and q that are prime.

- $n = p.q$ which is called the modulus for modular arithmetic.
- Choose an integer e that is relatively prime to the quotient of n [This guarantees that e will possess a multiplicative inverse modulo the quotient of n], such that e is less than $p.q$ and that e and $(p-1)(q-1)$ are coprime.
- Compute d that is the multiplicative inverse of e modulo the quotient of n, and such that $(d\,e-1)$ is divisible by $(p-1)(q-1)$.
- Choose (n, e) as the public key and (n, d) as the private key.

Let $C = T^e \bmod n$ be the ciphered message and $T = C^d \bmod n$ the deciphered message. Suppose that we are given an integer M, such that $M < n$ representing the message, then we can transform M into another integer C that will represent the ciphertext by the following modular operation

$$C = M^e \bmod n \tag{2.17}$$

and recover M back from C by the following modular operation

$$M = C^d \bmod n. \tag{2.18}$$

A simple worked example of RSA algorithm using two prime numbers can be found in [60], to illustrate how it works.

2.7.1 Using the Basic Idea for RSA Algorithm

The basic idea described on the previous section can be used in the following manner for confidential communication:

- An individual who wishes to receive messages confidentially will use the pair of integers $\{e, n\}$ as his/her public key. At the same time, this individual can use the pair of integers $\{d, n\}$ as the private key.
- Another party wishing to send a message to such an individual will encrypt the message using the public key $\{e, n\}$. Only the individual with access to the private key $\{d, n\}$ will be able to decrypt the message.

- The important theoretical question here is as to what conditions if any must be satisfied by the modulus n for this $M \longrightarrow C \longrightarrow M$ transformation to work?

2.7.2 Modulus for the RSA Algorithm

The modulus n must be selected in such a manner that the following is guaranteed:

$$(M^e)^d \equiv M^{ed} \equiv M(\bmod n). \tag{2.19}$$

We want this guarantee because $C = M^e \bmod n$ is the encrypted form of the message integer M and decryption is carried out by $C^d \bmod n$.

It was shown by Rivest, Shamir and Adleman that we have this guarantee when n is a product of two prime numbers:

$$n = p \otimes q\,, \tag{2.20}$$

for some prime p and prime q.

The above factorization is needed because the proof of the algorithm depends on the following two properties of primes and coprimes:

- If two integers p and q are coprimes (meaning, relatively prime to each other), the following equivalence holds for any two integers a and b:

  $$\{a \equiv b \bmod p \quad \text{and} \quad a \equiv b \bmod q\} \Leftrightarrow \{a \equiv b \bmod p \otimes q\}. \tag{2.21}$$

  This equivalence follows from the fact $a \equiv b \bmod p$ implies $a - b = k_1 \otimes p$ for some integer k_1. But since we also have $a \equiv b \bmod q$ implying $a - b = k_2 \otimes q$, it must be the case that $k_1 = k_3 \otimes q$ for some k_3. Therefore, we can write $a - b = k_3 \otimes p \otimes q$, which establishes the equivalence. (This argument breaks down if p and q have common factors other than 1. Here the question is why?)

- In addition to needing p and q to be coprimes, we also want p and q to be individually primes. It is only when p and q are individually prime that we can decompose the quotient of n into the product of the quotients of p and q. That is

  $$\phi(n) = \phi(p) \otimes \phi(q) = (p-1) \otimes (q-1). \tag{2.22}$$

  The step plays a crucial role in the proof of the RSA algorithm.

So that the cipher cannot be broken by an exhaustive search for the prime factors of the modulus n, it is important that both p and q are very large primes. Finding the prime factors of a large integer is computationally harder than determining its primality. We also need to ensure that n is not factorizable by one of the modern integer factorization algorithms.

2.7.3 Proof of the RSA Algorithm

Since the integer d is the multiplicative inverse of the integer e modulo $\phi(n)$, we obviously have

$$e \otimes d \bmod \phi(n) \;=\; 1. \tag{2.23}$$

This implies that there must exist an integer k so that

$$e \otimes d - 1 \;=\; k \otimes \phi(n). \tag{2.24}$$

It must then obviously be the case that $\phi(n)$ is a divisor of the expression $e \otimes d - 1$. But since $\phi(n) \;=\; \phi(p) \otimes \phi(q)$, the quotients $\phi(p)$ and $\phi(q)$ must also individually be divisors of $e \otimes d - 1$.

That is

$$\phi(p) \;\div\; (e \otimes d - 1) \quad \text{and} \quad \phi(q) \;\div\; (e \otimes d - 1). \tag{2.25}$$

Focusing on the first of these assertions, since $\phi(p)$ is a divisor of $e \otimes d - 1$, we can write

$$e \otimes d - 1 \;=\; k_1 \, \phi(p) \;=\; k_1 \, (p - 1)\,, \tag{2.26}$$

for some integer k_1.

Therefore, we can write for any integer M :

$$M^{e \otimes d} \bmod p \;=\; M^{e \otimes d - 1 + 1} \bmod p \;=\; M^{k_1 \, (p-1)} \otimes M \bmod p. \tag{2.27}$$

Now we have two possibilities to consider: Since p is a prime, it must be the case that either M and p are coprimes or that M is a multiple of p.

- Let us first consider the case when M and p are coprimes. By Fermat's Little Theorem, since p is a prime, we have

$$M^{p-1} \;\equiv\; 1 \pmod{p}. \tag{2.28}$$

Since this conclusion obviously extends to any power of the left hand side, we can write

$$M^{k_1(p-1)} \equiv 1 \pmod p. \tag{2.29}$$

Substituting this result in Equation (2.27), we have

$$M^{e\otimes d} \bmod p = M \bmod p. \tag{2.30}$$

- Now let us consider the case when the integer M is a multiple of the prime p. Now obviously, $M \bmod p = 0$. This will also be true for M raised to any power. That is, $M_k \bmod p = 0$ for any integer k. Therefore, Eq. (2.30) will continue to be true even in this case.

From the second assertion in Equation (2.25), we can draw an identical conclusion regarding the other factor q of the modulus n:

$$M^{e\otimes d} \bmod q = M \bmod q. \tag{2.31}$$

We established that, since p and q are coprimes, for any integers a and b if we have $a = b \bmod p$ and $a = b \bmod q$, then it must also be the case that $a = b \bmod p \otimes q$. Applying this conclusion to the partial results shown in Eqs. (2.30) and (2.31), we obtained

$$M^{e\otimes d} \bmod n = M \bmod n. \tag{2.32}$$

2.7.4 Key Distribution Centers

Suppose that we have a large number of people, processes, or systems that want to communicate with one another in a secure fashion. This group of people/processes/systems is not static, meaning that the individual entities may join or leave the group at any time.

A simple-minded solution to this problem would consist of each party physically exchanging an encryption key with every one of the other parties. Subsequently, any two parties would be able to establish a secure communication link using the encryption key they possess for each other. This approach is obviously not feasible for large groups of people/processes/systems, especially when group membership is ever changing.

A more efficient alternative consists of providing every group member with a single key for securely communicate with a key distribution center (KDC). This key would be called a master key. When A wants to establish a secure communication link with B, A requests a session key from KDC for communicating with B.

In implementation, this approach must address the following issues:

- Assuming that A is the initiator of a session-key request to KDC, when A receives a response from KDC, how can A be sure that the sending party for the response is indeed the KDC?
- Assuming that A is the initiator of a communication link with B, how does B know that some other party is not masquerading as A?
- How does A know that the response received from B is indeed from B and not from someone else masquerading as B?
- What should be the lifetime of the session key acquired by A for communicating with B?

2.7.5 Key Distribution Protocol

Assumptions: A party named A wants to establish a secure communication link with another party B. Both the parties A and B, respectively, possess master keys K_A and K_B, for communicating privately with a key distribution center (KDC). The exchange of message is shown graphically in the Figure 2.8, followed by details of the key distribution protocol.

Now A engages in the following protocol:

- Using K_A, A sends a request to KDC for a session key intended specically for communicating with B.
- The message sent by A to KDC includes A's network address (ID_A), B's network address (ID_B), and a unique session identifier N_1. The message sent by A to KDC

can be expressed in shorthand by

$$E(K_A,\,[ID_A,\,ID_B,\,N_1]). \tag{2.33}$$

where $E(.,.)$ stands for encryption of the second-argument data block with a key that is in the first argument.

- KDC responds to A with a message encrypted using the key K_A. The various components of this message are:

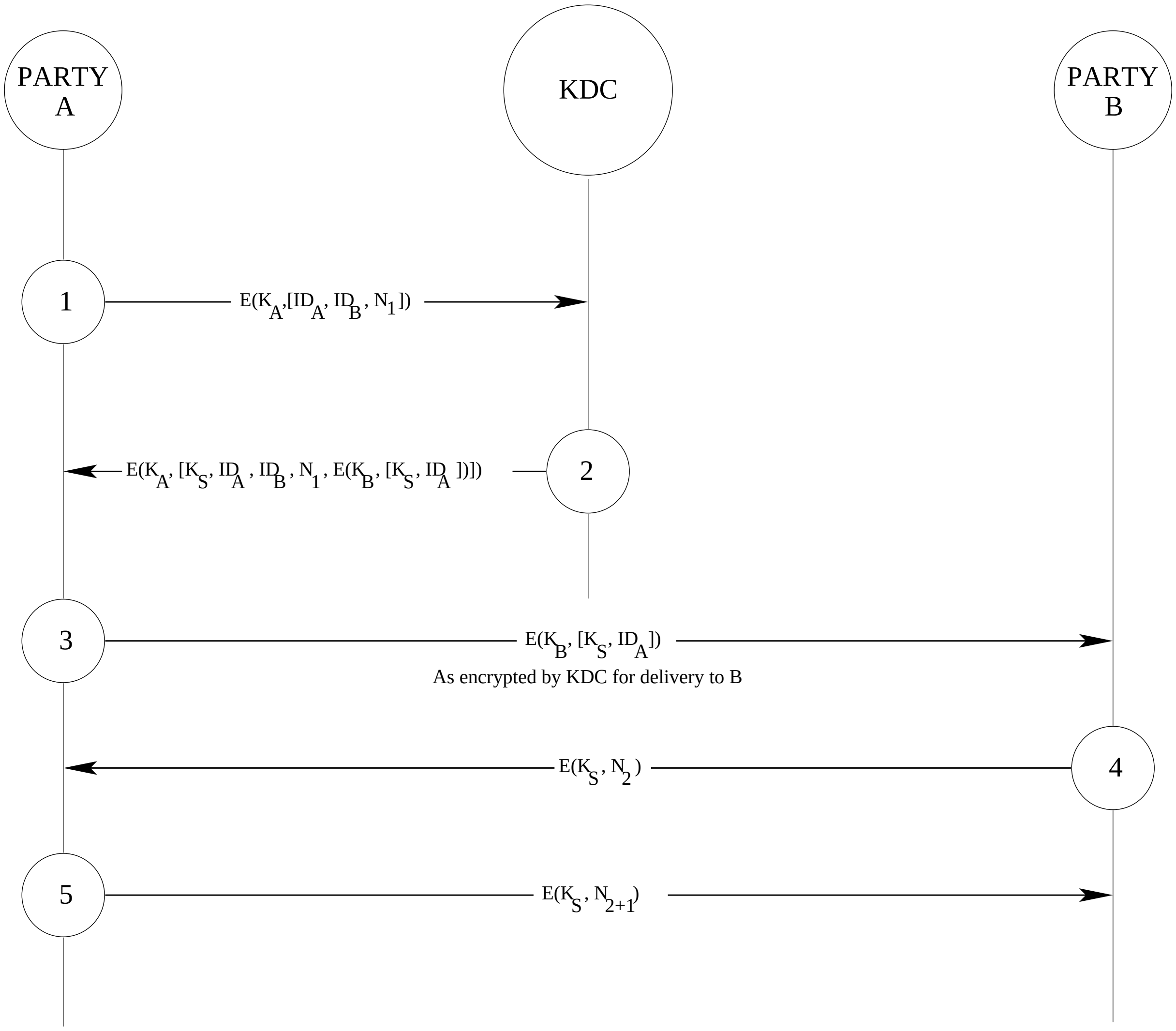
PARTY A
KDC
PARTY B
1
E(K_A,[ID_A, ID_B, N_1])
2
E(K_A, [K_S, ID_A, ID_B, N_1, E(K_B, [K_S, ID_A])])
3
E(K_B, [K_S, ID_A])
As encrypted by KDC for delivery to B
4
E(K_S, N_2)
5
E(K_S, N_2+1)

FIG. 2.8: A most important element of this exchange is that the message (information) that party A receives back from the Key Distribution Center can only be read by party B.

1. The session-key K_S that A can use for communicating with B.
2. The original message received from A, including the unique session identifier N_1 used by A. This is to allow A to match the response received from KDC with the request sent. Note that A may be trying to establish multiple simultaneous sessions with B.
3. A "packet" of information meant for A to be sent to B. This packet of information, encrypted using B's master key K_B includes, again, the session key K_S , and A's identier ID_A. (Note that A cannot look inside this packet because A does not have access to B's master key K_B .

- The message that KDC sends back to A can be expressed as

$$E(K_A, [K_S, ID_A, ID_B, N_1, E(K_B, [K_S, ID_A])]). \tag{2.34}$$

- Using the master key K_A, A decrypts the message received from KDC. Because only A and KDC have access to the master key K_A, A is certain that the message received is indeed from KDC.

- A keeps the session key K_S and sends the packet intended for B to B. This message is sent to B unencrypted by A. But note that it was previously encrypted by KDC using B's master key K_B. Therefore, this first contact from A to B is protected from eavesdropping.

- B decrypts the message received from A using the master key K_B. B compares the ID_A in the decrypted message with the sender identier associated with the message received from A. By matching the two, B makes certain that no one is masquerading as A.

- B now has the session key for communicating securely with A.

- Using the session key K_S , B sends back to A an unique session identifier N_2. A responds back with N_{2+1}, using, of course, the same session key K_S. This way B knows that it did not receive a first contact from A that A is no longer interested in. This is also a protection against a "replay" attack.

- A replay attack is a form of network attack in which a third party E eavesdrops on the communications between A and B. Let us say that E intercepts the first-contact message that B received from A. Now the question is: Would E be able to pose as B during a subsequent attempt by A to initiate a session with B? Let us assume that E has somehow gotten hold of B's master key K_B.

- The message sent by B back to A can be expressed as

$$E(K_S,\, N_2), \tag{2.35}$$

and A's response back to B as

$$E(K_S,\, N_{2+1}). \tag{2.36}$$

2.8 Shor's Algorithm

A quantum computer is a device that uses properties of quantum mechanics to do a number of calculations simultaneously. In 1994 Peter Shor theoretically showed that a quantum computer would be able to factorize a large number exponentially faster than a classical computer - this became known as Shor's algorithm [61].

The possible advent of quantum computers would result in current encryption programs like RSA to be broken almost immediately. The RSA code can be broken in principle [62], but it takes a classical computer, say long time to break; but a quantum computer has the potential to break it in a matter of seconds or minutes.

The mathematical problem to derive the private from the public key must be as difficult as possible. For instance, the idea behind the RSA public-key protocol [63] relies on the factorizing of large number. By now, no classical algorithm is known whose computational requirement scale less than exponentially with the size of the number to factorize.

The most damaging would be for an eavesdropper to discover the private key corresponding to a given public key. The obvious way is to factorize the public modulus n into its two prime factors P and Q which easily leads to the private key d.

It is currently difficult to factorize the product N of two large primes, even the best available classical algorithm scales exponentially in computational resources with the size of N (which is called a non-efficient algorithm). Therefore, security relies on the fact that factorizing will take years with current algorithms and computational capabilities [49].

However, even with the introduction of quantum computers, the one-time pad is still completely secure, 100%. This is an important fact, because the one-time pad is used in the final stage of quantum cryptographic protocols. It uses a randomly generated key. So a quantum computer would generate a number of possible random keys but it would not know which of them is the correct one.

2.9 Conclusion

We have discussed aspects of cryptography and how it is used today in the protection of important information. We finished off with mentioning how quantum theory will enable us, via quantum computers, to break current public key distribution protocols such as RSA, thus giving the code-makers an edge. However, as we will soon see, quantum theory not only weakens current ciphers but gives us a more exciting way of encrypting information through quantum key distribution.

Chapter 3

Quantum Mechanical Background

3.1 Introduction

Let us start this section with a question about what is wrong with classical cryptography? Well, as we have seen from the end of the second chapter, the security of classical cryptography is compromised with the possible advent of a quantum computer. A variety of encryption algorithms have been introduced, providing different levels of security. The RSA cryptosystem, one of the widely used algorithms, relies on the fact that it is difficult to find the factors of large integers [61]. There are two threats to this method:

1. The first is that more computational power will help to make time-consuming attacks (like brute-force attacks) more convenient.
2. The second problem is, that quantum computers are in fact already capable of executing the factorization efficiently [64, 65].

   Up until now, it cannot be done with large integers and it will probably take some time for it to become practical, but for crucial applications probably secure is not enough.

There exists a classical, unconditionally secure cryptographic algorithm, but it has a big problem: It requires a random key, which has to be as long as the message itself and this has to be transported securely from one party to the other [66]. This cannot be done classically. Here, an amazing idea comes into play: Quantum Mechanics has the property of hiding some information, as expressed in Heisenberg's uncertainty relation. Could this inherent ignorance be used as an advantage over a potential eavesdropper? The answer will come after discussing the essential quantum mechanical properties.

Quantum mechanics is viewed as the most remarkable development in 20th century physics. Its point of view is completely different from classical, and its predictions are often probabilistic. The basic principles of quantum mechanics are presented that are needed in this thesis. We gathered this information from [67] and [68].

We shall introduce a method of establishing a secret key between two parties, which is provably secure. This security is a direct consequence of the fundamental axioms of quantum mechanics. Really interesting about this method is that a usually unfavourable property of quantum mechanics is actually employed to achieve something that cannot be done outside the quantum world. The fact that two non-commuting observables can only be measured with limited precision allows uncoditionally secure key distribution. The whole idea has been named quantum cryptography or quantum key distribution (QKD).

3.2 Uncertainty Principles

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

$$\sigma_A^2 \sigma_B^2 \geq \left(\frac{1}{2i} \langle [\hat{A}, \hat{B}] \rangle \right)^2 . \tag{3.1}$$

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

$$\sigma_x \sigma_p \geq \frac{\hbar}{2} . \tag{3.2}$$

This inequality is better known as the Heisenberg Uncertainty Principle.

One of the fundamentals of quantum mechanics is that it is not possible to measure a quantum state without perturbing it [69]. Consider for example a superposition of the eigenstates $|1\rangle$ and $|2\rangle$, writen as $\Psi = \alpha|1\rangle + \beta|2\rangle$.

For this case, the measurement is that the system is projected on an eigenstate. Meaning that there is no information given by measurement on the coefficients α and β of the original superposition, because the original state is distroyed. Then, the original state cannot be constructed again. But, if the system is exclusively in one of the eigenstates e.g. $\Psi = |1\rangle$ or $\Psi = |2\rangle$, a single measurement would allow the reconstruction of the original state. So, we can identify the exclusive states of the system with bits, i.e. $|1\rangle$ = Bit 1 and $|2\rangle$ = Bit 0. Then we say that quantum state can be considered as a carrier of digital information, called a qubit (quantum bit).

3.3 The Quantum Bit

The bit is a fundemental concept of classical computation and classical information. In the classical world of information, the classical bit is like a very decisive individual. It is either 0 or 1, but by no means both at the same time. The classical bit has become so much a part of every day lives that people take many of its properties for granted. They take for granted, for example, that classical bit can be copied.

In quantum computation and quantum information there is an analogous concept called the quantum bit or qubit. Most people may not be familiar with the quantum bit of information. Unlike its sibling rival, the classical bit, the qubit can be both 0 and 1 at the same time. Also, in contrast to the decisive classical bit, the qubit is a very indecisive individual. Moreover, unlike the classical bit, the qubit cannot be duplicated, meaning copied because of the no cloning theorem of Dieks [70, 71], Wootters, and Zurek [72, 71].

The classical bits 0 and 1 correspond in the quantum world to respectively the quantum state $|0\rangle$ and $|1\rangle$, where $|0\rangle$ and $|1\rangle$ are orthonormal wave functions. Whereas a bit can only be in two different states, a qubit can also be in a superposition of the basis states. If the basis states are $|0\rangle$ and $|1\rangle$ then, in general, a qubit is in the state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{3.3}$$

where $|\alpha|^2 + |\beta|^2 = 1$.

In this view, the state of a qubit is a vector in a 2-dimensional vector space basis $|0\rangle, |1\rangle$ also known as the rectilinear or computational basis.

Another possible basis is the diagonal basis consisting of

$$\{|+\rangle, |-\rangle\} = \left\{ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right\}, \tag{3.4}$$

where $|+\rangle$ correspond with a classical bit 0 and $|-\rangle$ with a classical bit 1.

In this basis a qubit is in the general state

$$|\psi\rangle = \alpha|+\rangle + \beta|-\rangle \tag{3.5}$$

obviously there are many more possible bases.

Example 1

One example of a qubit is a spin $\frac{1}{2}$ particle which can be in a spin-up state $|1\rangle$ which we label as 1, in a spin-down state $|0\rangle$ which we label as 0, or in a superposition of these states, which we interpret as being both 0 and 1 at the same time.

Example 2

Another example of a qubit is the polarization state of a photon. A photon can be, either in a vertically polarized state $|\updownarrow\rangle$ (we assign a label of 1 to this state), in a horizontal polarized state $|\leftrightarrow\rangle$ (we assign a label 0 to this state), or in a superposition of these states. In this case, we interpret its state as representing both 0 and 1 at the same time.

Where do qubits live?

They live in a Hilbert space $\mathcal{H}$. By a Hilbert space, we mean:

3.3.1 Definition 1

A Hilbert space is a vector space over complex numbers $\mathbb{C}$ together with an inner product

$$< . , . >: \mathcal{H} \times \mathcal{H} \longrightarrow \mathbb{C}, \tag{3.6}$$

which is complete with respect to the norm

$$\|u\| = \sqrt{(u,u)} \tag{3.7}$$

induced by the inner product $\mathcal{H} \times \mathcal{H}$.

By a complex valued inner product, we mean a map

$$(.\,,.) : \mathcal{H} \times \mathcal{H} \longrightarrow \mathbb{C} \tag{3.8}$$

from $\mathcal{H} \times \mathcal{H}$ into the complex numbers $\mathbb{C}$ such that:

1. $(u,u) = 0$ if and only if $u = 0$
2. $< u, \lambda v > = < \lambda u, v >$ for all $u, v \in \mathcal{H}$ and $\lambda \in \mathbb{C}$
3. $< u_1 + u_2, v > = < u_1, v > + < u_2, v >$ for all $u_1, u_2, v \in \mathcal{H}$
4. $< u, v >^* = < v, u >$ for $u, v \in \mathcal{H}$, where the superscript "$*''$ denotes complex conjugation.
5. For every Cauchy sequence $u_1, u_2, u_3, ...$ in $\mathcal{H}$,

   $$\lim_{n \to \infty} u_n$$

   exists and lies in $\mathcal{H}$.

3.3.2 Some Dirac notation

The elements of $\mathcal{H}$ are called kets, and will be denoted by $|label\rangle$ where $'|'$ and $'\rangle'$ are left and right delimiters, and $'label'$ denotes any label, i.e, name, we wish to assign to the ket.

Given a Hilbert space $\mathcal{H}$, let

$$\mathcal{H}^* = Hom(\mathcal{H}, \mathbb{C})$$

denote the all of linear maps from $\mathcal{H}$ to $\mathbb{C}$. Then $\mathcal{H}^*$ is actually a Hilbert space, called the dual Hilbert space of $\mathcal{H}$, with scalar product and vector sum defined by:

$$\begin{cases} (\lambda.f)(|\Psi\rangle) = \lambda(f(|\Psi\rangle)), \\ (f_1 + f_2)(|\Psi\rangle) = f_1(|\Psi\rangle) + f_2(|\Psi\rangle), \end{cases} \tag{3.9}$$

for all $\lambda \in \mathbb{C}$ and for all $f, f_1, f_2 \in \mathcal{H}^*$.

We call the elements of $\mathcal{H}^*$ bra's, and denote them as: $\langle label|$. We can now define a bilinear map

$$\mathcal{H}^* \times \mathcal{H} \longrightarrow \mathbb{C} \tag{3.10}$$

by

$$(\langle\Psi_1|)(|\Psi_2\rangle) \in \mathbb{C}. \tag{3.11}$$

Since bra $\langle\Psi_1|$ is a complex valued function of kets, we denote the product (3.11) more simply as

$$\langle\Psi_1|\Psi_2\rangle \tag{3.12}$$

and call it the Bra-c-Ket (or bracket) or bra $\langle\Psi_1|$ and ket $|\Psi_2\rangle$.

3.3.3 Definition

Finally, a qubit is a ket (state) in a two dimensional Hilbert space $\mathcal{H}$. Thus, if we let $|0\rangle$ and $|1\rangle$ denote an arbitrary orthonormal basis of a two dimensional Hilbert space $\mathcal{H}$, then each qubit in $\mathcal{H}$ can be written in the form

$$|\text{qubit}\rangle = \alpha|0\rangle + \beta|1\rangle \tag{3.13}$$

where $\alpha, \beta \in \mathbb{C}$.

Since any scalar multiple of a ket represents the same state of an isolated quantum system, we can assume that $|\text{qubit}\rangle$ is a ket of unit length, i.e, that

$$|\alpha|^2 + |\beta|^2 = 1 \tag{3.14}$$

The above qubit is said to be in a superposition of the states $|0\rangle$ and $|1\rangle$. This is what we mean when we say that a qubit can be simultaneously both 0 and 1.

However, if the qubit is observed it immediately makes a decision. It decides to be 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$. Some physists call this the collapse of the wave function. For more information about this being called collapse of the wave function, which engenders a war cry in most physists, we refer to [71].

3.4 The Polarization of Photons

A photon is an elementary particle of light, carrying a fixed amount of energy. Light may be polarized, and polarization is a physical property that emerges when light is regarded as an electromagnetic wave [71].

Firstly we consider the polarized light in the classical perspective. The polarization of light is the direction of oscillation of the electromagnetic field associated with its wave [73]. Light waves in the vacuum are transverse electromagnetic (EM) waves with both electric and magnetic field vectors perpendicular to the direction of propagation and also to each other. (See Figure 3.1)

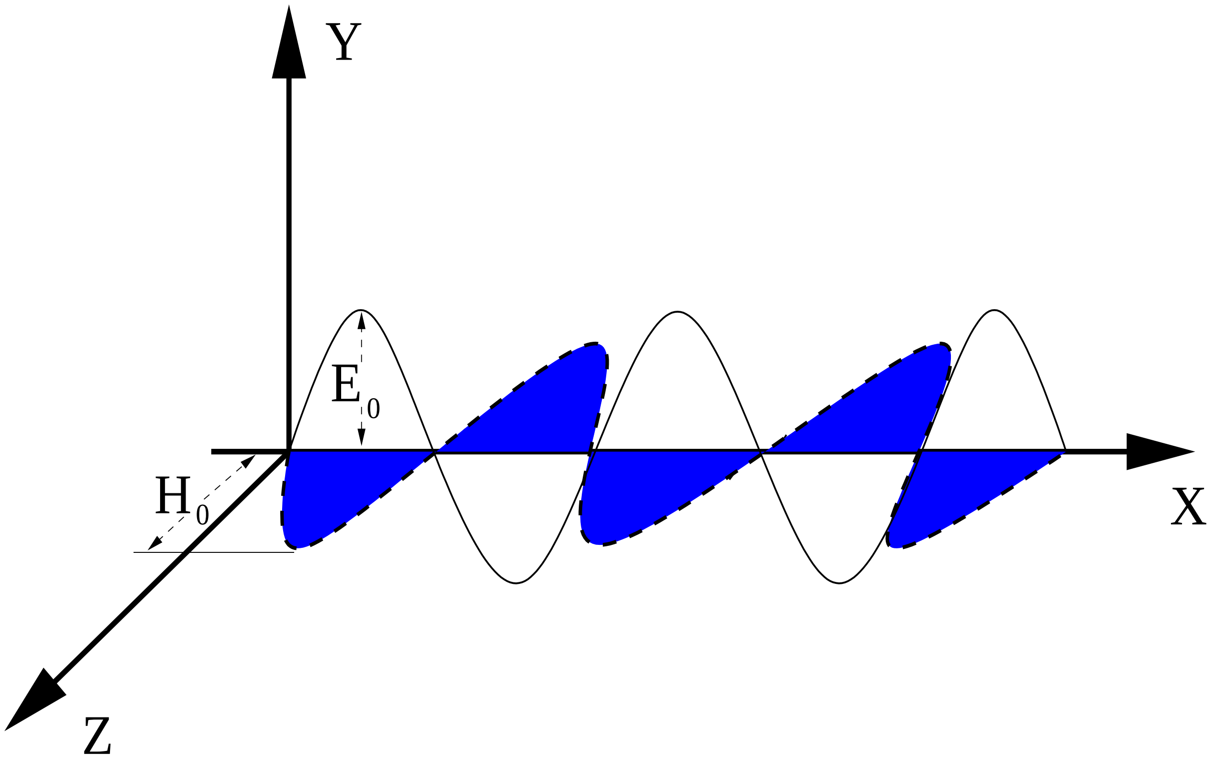

FIG. 3.1: A linearly polarized electromagnetic wave.

If the electric field vector is always parallel to a fixed line, then, the EM wave is said to be **rectilinearly polarized**. If the electric field vector rotates about the direction of propagation forming a right-(left-) handed scew, it is said to be right (left) elliptically polarized. If the rotating electric field vector inscribes a circle, the EM wave is said to be right- or left- circularly polarized.

As an illustration of the previous concepts, let us now consider the polarization states of a photon. Linear polarization states can be defined by the direction of oscillation of the field. Horizontal and vertical orientations are examples of linear polarization states. Diagonal states (+ and $-45°$) are also linear polarization states. Linear states can point in any direction. The polarization of photon can be prepared in any of these states.

Filters exist to distinguish horizontal states from vertical ones. It is constituted of two crosswise bases and is used to read last polarization of a polarized photon. In the Figure 3.2 there exists two form of filters: Diagonal Filter and Rectilinear Filter.

FIG. 3.2: Rectilinear Filter (left) and Diagonal filter (right).

When passing through such a filter, the course of a vertically polarized photon is deflected to the right, while that of a horizontally polarized photon is deflected to the left [73].

The polarization states of a photon are represented as state kets in a two dimensional Hilbert space $\mathcal{H}$. One orthonormal basis of $\mathcal{H}$ consists of the kets $|\circlearrowleft\rangle$ and $|\circlearrowright\rangle$ which represent respectively the quantum mechanical states of left- and right-circularly polarized photons [74].

Another orthonormal basis consists of the kets $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$ representing respectively vertically and horizontally linearly polarized photons. And yet another orthonormal basis consists of the kets $|\nearrow\rangle$ and $|\nwarrow\rangle$ for linearly polarized photons at the angles $\theta = \frac{\pi}{4}$ and $\theta = -\frac{\pi}{4}$ off the vertical, respectively.

These orthonormal bases are related as follows:

$$\begin{cases} |\nearrow\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle + |\leftrightarrow\rangle) \\ |\nwarrow\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle - |\leftrightarrow\rangle)\,. \end{cases} \tag{3.15}$$

In order to distinguish between diagonally polarized photons, one must rotate the filter by

45°. If a photon is sent through a filter with the incorrect orientation - diagonally polarized photon through the non-rotated filter for example - it will be randomly projected in one of the two directions. In this process, the photon also undergoes a transformation of its polarization state, so that it is impossible to know its orientation before the filter [73].

Chapter 4

Quantum Cryptography

Quantum Cryptography is the research discipline that applies the principles of quantum mechanics for cryptographic purposes [75]. The following are some of the main principles used in Quantum Cryptography:

1. It is not possible to copy quantum states (no-cloning-theorem) [76].
2. No one can measure the polarization of a photon in the vertical-horizontal basis and simultaneousily in the diagonal basis.
3. It is impossible to determine simultaneousily the position and momentum of a particle with arbitrary high accuracy (Heisenberg's uncertainty principle).
4. Each measurement of quantum state modifies the quantum state.

In other words, quantum cryptography is the combination of quantum key distribution with a one-time pad cipher and an information theoretically secure messsage authentication scheme.

One can solve the problem of key distribution using quantum effects. Messages can be encrypted and decrypted using perfect cryptosystems (E_k, D_k) [53], if a secret key k is exchanged in perfect secrecy meaning that

$$D_k\{E_k\{m\}\} = m\,, \tag{4.1}$$

where E_k is the encrypted key, D_k is the decrypted key and m is the message.

It might be instructive to sketch very briefly how a quantum cryptography system can be used to transmit binary data from Alice to Bob, and this, before reviewing general properties of quantum particles (See Figure 4.1 where Alice can send qubits into a quantum channel, at which Bob listens. Both have bidirectional access to an authentic classical channel).

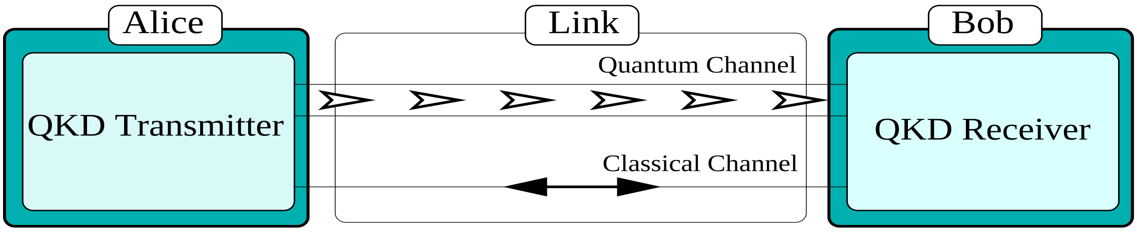

FIG. 4.1: The basic quantum cryptography system.

First, Alice and Bob need to establish a secret key between them, using quantum key distribution. This requires a quantum channel, into which Alice can send and Bob can listen to. They will need an authentic classical communications channel. They still cannot be forged by an eavesdropper, while their messages are not secure against eavesdroping. But soon, they both share the secret key, which allows them to encrypt a message with classical algorithm.

Quantum Cryptography solves the key distribution problem by allowing the exchange of a cryptographic key between two remote parties with absolute security, guaranteed by the laws of physics. This key can then be used with conventional cryptographic algorithms [73].

The aim of Quantum Cryptography is to exploit the laws of quantum mechanics in order to carry out cryptographic tasks, but the use of quantum mechanics for cryptographic ends is limited, mainly to the distribution of secret keys, therefore, there is not really cryptography involved. That is why we very often use the more precise term of Quantum Key Distribution (QKD) [77].

Contrary to what one could expect, the basic principle of QKD is quite straightforward. It exploits the fact that according to quantum mechanics, the mere fact of observing a quantum object perturbs it in an irreparable way. When you read this paper for example, the sheet of paper must be lighted. The impact of the light particles will slightly heat it up and hence change it. This effect is very small on a piece of paper, which is a macroscopic object.

However, the situation is slightly different with a microscopic object. If one encodes the value of a digital bit on a single quantum object, its interception will necessarilly translate into a perturbation, because the eavesdropper is forced to observe it. This perturbation causes errors in the sequence of bits exchanged by the sender and recipient. By checking the presence of such errors, the two parties can verify whether their key was intercepted or not.

It is important to stress that since this verification takes place after the exchange of bits, one finds out a posteriori whether the communication was eavesdropped or not. That is why this technology is used to exchange a key and not valuable information. Once the key is validated, it can be used to encrypt data. Quantum mechanics allows to prove that interception of the key without perturbation is impossible [73]. While conventional encryption relies on keys that are computationally hard to crack, quantum key distribution transmits the key with single photons [77].

In telecommunication networks, light is routinely used to exchange information. For each bit of information, a pulse is emitted and sent down an optical fiber (a thin fiber of glass used to carry light signals) to the receiver, where it is registered and transformed back into an electronic signal. These pulses typically contain millions of particles of light, called photons.

In quantum cryptography, one can follow the same approach, with the only difference that the pulses contain only a single photon. A single photon represents a very tiny amount of light (when reading the paper your eyes register billions of photons every second) and follows the laws of quantum mechanics. In particular, the photon cannot be split into halves meaning that an eavesdropper cannot take half of a photon to measure the value of the bit it carries, while letting the other half continues its course. If one wants to obtain the value of the bit, he must observe the photon and will thus interrupt the communication and reveal his presence.

A more clever strategy is for the eavesdropper to detect the photon, register the value of the bit and prepare a new photon according to the result obtained which is sent to the receiver. In quantum cryptography, the two legitmate parties cooperate to prevent the eavesdropper from doing so, by forcing him to introduce errors. Protocols have been devised to achieve this goal [73].

4.1 Quantum Key Distribution

4.1.1 Introduction

Quantum key distribution (QKD) is a methodology for generating and distributing random encryption keys using the principles of quantum mechanics [75]. In quantum key distribution systems, the phase of single photons (called polarization) carries the information and sends it over an optical fiber or free-space. At the receiver's site the photons are detected and measured to build the so-called raw key, and this, only if the randomly chosen quantum state preparation is identical for the sender and the receiver. Publicly, the basis of the measurements is announced in the procedure called sifting. The sifted key bits will be perfectly correlated if no eavesdropping has happened. Practically, the sifted key contains errors (which can be attributed to a potential eavesdropper) due to background photons, detector noise and polarization imperfections.

The basis of quantum key distribution is explained as follow:

- Take a sequence of bits $\{b_i\}$.
- Map each bit to a state $|\Psi_i\rangle$ using the basis $\boxplus$ or $\boxtimes$ (see on pages 56 and 57 for definition). For each bit these basis are chosen randomly.
- The only way to recover each b_i is by using the same basis for decoding:
    1. if the correct basis is used, correct result
    2. if the wrong basis is used, result is random.

4.1.2 Quantum Key Distribution Protocols

In the last decade, many quantum key distribution protocols were proposed, experimented and proven for secure communications. Among these quantum key distribution protocols, there are mainly two types of quantum key distribution schemes:

- The first type is the prepare-and-measure scheme: In a "prepare and measure" protocol, Alice encodes bits by preparing non-orthogonal quantum states. She sends the prepared states to Bob who extracts bits values by measuring every received state in one of the non-orthogonal bases. Example one, BB84 [78, 23], in which Alice sends each qubit in one of four states of two complementary bases. Another example is the B92 [79] in which Alice sends each qubit in one of two non-orthogonal states. A further example is the Six-state protocol [80] in which Alice sends each qubit in one of six states of three complementary bases.
- The other type is the entanglement based QKD scheme: In an "entanglement based" protocol, Alice and Bob each receive a part of an entangled state from the dealer, which could be Alice herself. Alice and Bob extract bits by measuring every received state in one of non-orthogonal bases agreed on beforehand [81]. For example in the Ekert 91 protocol [35], entangled pairs of qubits are distributed to Alice and Bob, who then extract key bits by measuring their qubits in non-orthogonal bases [82].

All of these protocols' main aim is to form an encryption key and distribute it to both sides in such a secure way that a possible eavesdropping attempt can be detected. Today, BB84 protocol is the widely used one in commercial models of Quantum Key Distribution. Common working principle of BB84 and B92 protocols for Alice's/Bob's process is:

- Alice's Side:

  - In each time slot, generate one bit of encryption key randomly.
  - In order to represent the same qubit value with the generated bit, polarize a photon with one of four bases suitable polarization angle.
  - Send polarized photon to Bob over an optical line.

- Write down the qubit values sent and the type of bases used in polarization process.

- Bob's Side:

  - In order to read the polarization of the photon coming over an optical line, choose either a diagonal or a rectilinear filter randomly and read incoming photon's polarization.

  - Write down the type of filter used and the qubit values after reading the process.

4.2 BB84 Protocol

In BB84, Alice's side can use two of four different polarization angles in order to send a 0 or 1 valued qubit [21]. In Figure 4.2, the Qubit-polarization matching of BB84 protocol is shown.

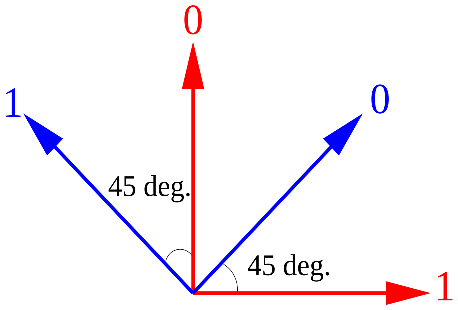

FIG. 4.2: Qubit-polarization matching of BB84 protocol for sending/receiving process.

Each qubit is represented by one of two non-perpendicular polarization angles. For the matching rule of Figure 4.2, polarization angles of 0 and 135 degrees represents a qubit with value of 1 and polarization angles of 45 and 90 degrees represents a qubit value of 0. Both sides must choose the same matching rule for a flawless transmission process.

If an eavesdropper tries to read the polarization of a photon with a filter which contains a base with the same polarization angle of this photon then the photon's polarization cannot change. But if the eavesdropper uses the wrong type of filter for reading process, photon's original polarization angle changes by ±45 degrees. When the sending and receiving sides compare their chosen base/filter types for each photon and together with a small amount of revealed (sacrified) qubit values using public channel, they can realize if the photon's polarization is changed or not. They can compute an error rate and compare it with a threshold value in order to determine eavesdropping.

4.2.1 Principle

The Figure 4.3 shows that Alice would like to communicate with Bob without the ever vigilant Eve eavesdropping on their conversation. Alice has connected a BB84 transmitter to her end of the quantum channel, Bob needs a BB84 receiver that can also be connected to the same quantum channel. Both have access to an authentic classical channel, which can later be used to transmit the encoded message [83].

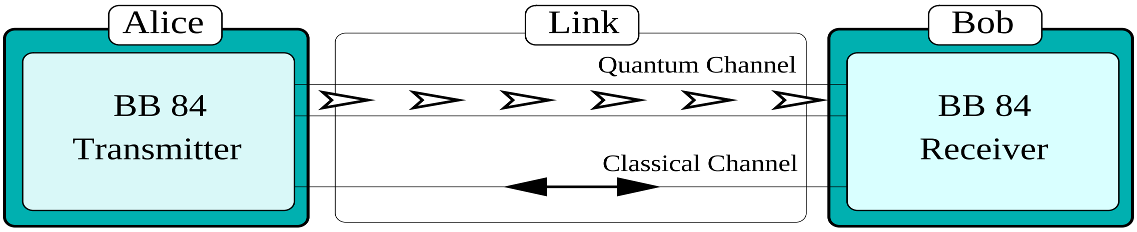

FIG. 4.3: A BB84 quantum cryptography system.

The operating mode of BB84 as published in 1984 [23], consists of two main steps : Quantum Transmission and Public Discussion.

In the phase of quantum transmission, the information is encoded in non-orthogonal quantum states which can be a single photon with polarization direction of $0(\leftrightarrow)$, $\frac{\pi}{4}(\nearrow)$, $\frac{\pi}{2}(\updownarrow)$ or $\frac{3\pi}{4}(\nwarrow)$. Alice, the sender and Bob, the receiver must agree first on the meaning of the photon polarizations for instance 0 or $\frac{\pi}{4}$ for a binary 0, and $\frac{\pi}{2}$ or $\frac{3\pi}{4}$ for a binary 1.

The qubits are randomly chosen by Alice from two non-orthogonal qubits bases such as $RL = \{|0\rangle, |1\rangle\}$ the rectilinear basis and $DG = \{|+\rangle, |-\rangle\} = \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ the diagonal one.

Alice prepares a polarized photon in some direction, so the qubits $|0\rangle$ and $|1\rangle$ correspond to a photon with a horizontal polarization and a vertical polarization while the qubits $|+\rangle$ and $|-\rangle$ correspond to a photon with a diagonal polarization, respectively a plus 45 degree orientation and a minus 45 degree orientation [82].

Alice generates a random sequence of polarization bases then sends photon by photon to Bob. Each photon represents a bit of the generated string polarized by the random basis for this bit position. When receiving photons, Bob selects the polarization filters (rectilinear or diagonal) to measure the polarization of the received photon.

In the phase of public discussion, after finishing the quantum transmission Bob reports the bases that he picked for each received photon and then Alice checks Bob bases and says which ones were corrects. Alice extracts bit values from the qubit states she sent to Bob. Bob, also extracts bit values from the measurement he made on the received quantum states.

4.2.2 The BB84 Protocol Without Noise

Suppose that Alice would like to transmit a secret key K to Bob, and Eve plans to make every effort to eavesdrop on the transmission and learn the secret key [84]. The aim in this Section is to show how the principles of quantum mechanics can be used to build a cryptographic communication system in such a way that the system dectects if Eve is eavesdropping, and which also gives a guarantee of no intrusion if Eve is not eavesdropping. As it is shown in Figure 4.3, the system consists of two communication channels:

- One is non-classical one-way quantum communication channel.
- The other is an ordinary classical two-way public channel, such as a two-way radio communication system.

This classical two-way channel is public, open to whomsoever would like to listen in, and is noise free.

Let us now describe how polarization states of the photon can be used to construct a quantum one-way communication channel. In the Section 3.4, we saw that the polarization states of a photon lie in a two dimensional Hilbert space $\mathcal{H}$. For this space, there are many orthonormal bases, but we will use only two for our quantum channel.

- The first is the basis consisting of the vertical and horizontal polarization states, i.e., the kets $|\updownarrow\rangle$ and $|\leftrightarrow\rangle$, respectively. We will refer to this orthonormal basis as the vertical/horizontal (V/H) basis, and denote this basis with the symbol $\boxplus$.
- The second orthonormal basis consists of the polarization states $|\nearrow\rangle$ and $|\nwarrow\rangle$, which correspond to polarizations directions formed respectively by 45^o clokwise and 135^o clokwise. We call this oblique basis, and denote it with the symbol $\boxtimes$.

If Alice decides to use the (V/H) basis $\boxplus$ on the quantum channel, then she shall use the following quantum alphabet:

$$\begin{cases} 1 = |\updownarrow\rangle \\ 0 = |\leftrightarrow\rangle\,. \end{cases}$$

In other words, if Alice use this quantum alphabet on the quantum channel, she shall transmit a 1 to Bob simply by sending a photon in the polarization state $|\updownarrow\rangle$, and she shall transmit a 0 by sending a photon in the polarization state $|\leftrightarrow\rangle$.

On the other hand, if Alice decides to use the oblique basis $\boxtimes$, then she shall use the following quantum alphabet:

$$\begin{cases} 1 &= &|\nearrow\rangle \\ 0 &= &|\nwarrow\rangle\,. \end{cases}$$

sending a 1 as a photon in the polarization state $|\nearrow\rangle$, and sending a 0 as a photon in the polarization state $|\nwarrow\rangle$.

She has chosen these two bases because the Heisenberg Uncertainty Principle implies that observations with respect to the $\boxplus$ basis are incompatible with observations with respect to the $\boxtimes$ basis [85]. The Table 4.1 shows the summary of the BB84 protocol without the presence of Eve.

Let us now show how Alice and Bob communicate with one another using a two stage protocol, called BB84 protocol.

Stage 1 protocol: Communication over a quantum channel

QUANTUM TRANSMISSION										
Alice's random bits	1	0	0	1	1	0	0	1	0	1
Alice's random sending basis	⊞	⊠	⊠	⊠	⊞	⊠	⊞	⊠	⊞	⊠
Photons polarization Alice sends	↕	↖	↖	↗	↕	↖	↔	↗	↔	↗
Bob's random receiving basis	⊠	⊠	⊞	⊠	⊞	⊠	⊞	⊞	⊞	⊞
Photons polarization Bob measures	↗	↖	↕	↗	↕	↖	↔	↔	↔	↔
Bits as received by Bob	1	0		1	1	0	0		0	0
PUBLIC DISCUSSION OF BASIS										
Bob reports basis of received bits	⊠	⊠		⊠	⊞	⊠	⊞		⊞	⊞
Alice says which basis were correct		ok		ok	ok	ok	ok		ok	
Presumably shared information		0		1	1	0	0		0	
Bob reveals some key bits at random				1		0				
Alice confirm them				ok		ok				
OUTCOME										
Shared secret Key ⇒		0			1		0		0	

TABLE. 4.1: The BB84 protocol without Eve present (No noise).

In this stage, Alice creates a random sequence of bits, which she sends to Bob over quantum channel as it is shown in Figure 4.4.. With this sequence, they will build a secret key that can be shared by themselves.

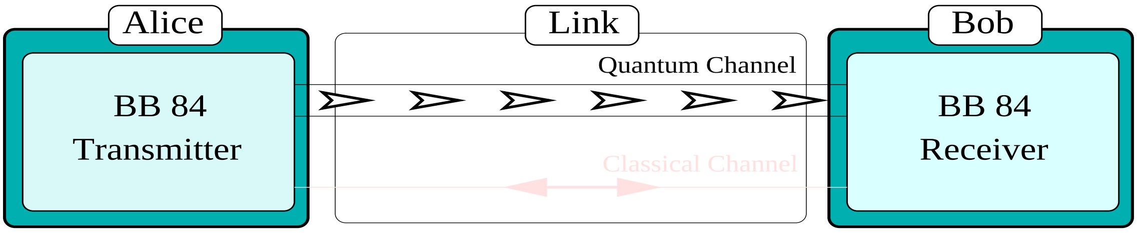

FIG. 4.4: Communication over a quantum channel.

- First, Alice flips a fair coin to generate a random sequence S_{Alice} of zeroes and ones. This sequence will be used to construct a secret key shared only by Alice and Bob.

- Second, for each bit of the random sequence, Alice flips a fair coin again to choose at random one of the two quantum alphabets. She transmits the bit as a polarized photon according to the chosen alphabet.

- Third, each time Bob receives a photon sent by Alice, he has no way of knowing which quantum alphabet was chosen by Alice. So he simply uses the flip of a fair coin to select one of the two alphabets and makes his measurement accordingly. Half of the time he will be lucky and choose the same quantum alphabet as Alice. In this case, the bit resulting from his measurement will agree with the bit sent by Alice. However, the other half of the time he will be unlucky and choose the alphabet not used by Alice. In this case, the bit resulting from his measurement will agree with the bit sent by Alice only 50% of the time. After all these measurements, Bob now has in hand a binary sequence S_{Bob} [37].

Stage 2 protocol: Communication over a public channel

Alice and Bob now proceed to communicate over the public two-way channel to compare the portion of their raw keys estimate know if Eve has eavedropped their resulting raw keys or not. Figure 4.5 shows this communication, and the process is subdivised in two phases below:

Phase 1. *Raw key extraction*

- Over the public channel, Bob communicates to Alice which quantum alphabet he used for each of his measurements.
- In response, Alice communicates to Bob over the public channel which of his measurements were made with the correct alphabet.
- Alice and Bob then delete all bits for which they used incompatible quantum alphabets to produce their resulting raw keys. If Eve has not eavesdropped, then their resulting keys will be the same. If Eve has eavesdropped, their resulting raw keys will not be in total agreement [85].

Phase 2. *Error estimation*

- Over the public channel, Alice and Bob compare small portions of their raw keys to estimate the error-rate R, and delete the disclosed bits from their raw keys to

> produce their tentative final keys. If through their public disclosures, Alice and Bob find no errors (meaning $R = 0$), then they know that Eve was not eavesdropping and that their tentative keys must be the same final key. If they discover at least one error during their public disclosures (which means $R > 0$), then they know that Eve has been eavesdropping. In this case, they discard their tentative final keys and start all over again.

The process of these two stages (communication over a quantum channel and communication over a classical channel) is summarized in Table 4.2 to show how Alice and Bob share their secret key with Eve present.

4.2.3 The BB84 protocol with noise

Since Bob can not distinguish between errors caused by noise and those caused by Eve's intrusion, we must assume that Bob's raw key is noisy. The only practical working assumption he can adopt is that all errors are caused by Eve's eavesdropping. Under this working assumption, Eve is always assumed to have some information about bits transmitted from Alice to Bob. Thus, the raw key is always only partially secret.

What is needed is a method to distil a smaller secret key from a larger partially secret key, this is called privacy amplification. Therefore, from the old protocol a new is created that allows for the presence of noise, a protocol that includes privacy amplication. The stages in the procedure are listed below:

Stage 1: Communication over a quantum channel

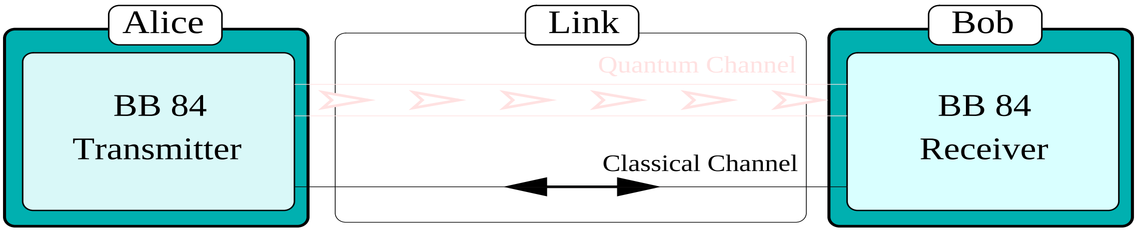

FIG. 4.5: Communication over a public channel.

QUANTUM TRANSMISSION													
Alice's random bits	1	0	0	1	1	0	0	1	0	1	0	0	0
Alice's random sending bases	⊞	⊠	⊠	⊠	⊞	⊠	⊞	⊠	⊞	⊠	⊠	⊠	⊞
Polarizations Alice sends	↕	↖	↖	↗	↕	↖	↔	↗	↔	↗	↖	↖	↔
Eve's random measuring bases	⊠	⊞	⊞	⊠	⊞	⊞	⊠	⊠	⊞	⊞	⊞	⊞	⊞
Eve measures and sent	↗	↔	↕	↗	↕	↕	↗	↗	↔	↔	↕	↔	↔
Eve's random bits	1	0	1	1	1	1	1	1	0	0	1	0	0
Bob's random receiving bases	⊠	⊠	⊞	⊠	⊞	⊠	⊞	⊞	⊞	⊞	⊠	⊠	⊞
Polarizations Bob measures	↗	↖	↕	↗	↕	↖	↕	↔	↔	↔	↗	↖	↔
Bits as received by Bob	1	0	1	1	1	0	1	0	0	0	1	0	0
PUBLIC DISCUSSION													
Bob reports bases of bits	⊠	⊠	⊞	⊠	⊞	⊠	⊞	⊞	⊞	⊞	⊠	⊠	⊞
Alice says bases were correct		ok		ok	ok	ok	ok		ok		ok	ok	ok
Presumably shared info	$*$	0	$*$	1	1	0	1	$*$	0	$*$	1	0	0
Bob reveals bits at random						0						0	
Alice confirm them						ok						ok	
OUTCOME													
Shared secret key ⇒		0		1	1		1		0		1		0
Errors in key and values kept		$\surd$		$\surd$	$\surd$		E		$\surd$		E		$\surd$

TABLE. 4.2: The BB84 protocol with Eve present (No noise). The symbols ($*$) indicate disregarded bits due to base incompatibility between Alice and Bob. The letter (E) shows the errors in the key (or the communication has been eavesdropped, because Alice's and Bob's bit values do not although having choses the same base). And the symbols ($\surd$) indicate the values kept afterwards.

This stage is exactly the same as before, except that errors are now also induced by noise.

Stage 2: Communication over public channel

Phase 1: Raw key extraction

This phase is exactly the same as in the noise-free protocol, except that Alice and Bob also delete those bit locations at which Bob should have received but did not receive a bit. These non-receptions could be caused by Eve's intrusion or by dark counts in Bob's detection device. The location of dark counts are communicated by Bob to Alice over the public channel.

Phase 2: Error estimation

Over the public channel, Alice and Bob compare small portions of their raw keys to estimate the error rate R, and delete the disclosed bits from their raw key to produce their tentative final keys. If R exceeds a certain threshold R_{Max}, then privacy amplification is not possible. So, Alice and Bob return to stage 1 to start over. On the other hand, if $R \leq R_{Max}$, then Alice and Bob proceed to phase 3.

Phase 3*: Extraction of Reconciled Key*

In this phase, Alice and Bob remove all errors from what remains of raw key to produce a common error-free key, called reconciled key.

- Alice and Bob now have highly correlated bit strings that can be made identical with high probability by information reconciliation. For this Alice sends $H(X|Y) = nh(\epsilon)$ bits to Bob. With error correction Alice and Bob retrieve an equal bit string K' with high probability. We will not give further details about how the information reconciliation works because this is outside the scope of this thesis. For more information we refer to [82].

Suppose X is the bit string of Alice and Y is the bit string of Bob just before the information reconciliation. Both bit strings contain n bits. Information reconciliation reconciles errors between X and Y to obtain a shared bit string K' while giving away as less information as possible to Eve. The uncertainty Bob has about the bit string X is equal to $H(X|Y)$. This means that information reconciliation implies that Alice communicates in public to Bob approximately $H(X|Y)$ of her n bits. Then, with the information reconciliation, Alice and Bob find the same bit string K' with high probability [42, 86].

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

- Alice and Bob publicly select randomly chosen subsets of remnant key, publicly compare parities, each time discarding an agreed upon bit from their chosen key sample.

If a parity should not agree, they employ the binary search strategy of step 1 to locate and delete error.

The strings shared by Alice and Bob after the steps of the BB84 protocol will be highly correlated but not completely identical, if there is noise in the quantum channel due whether to an eavesdropper or not. These have to be broken up into corresponding blocks which are short enough if the number of errors is not too large [87].

Phase 4: Privacy Amplification

Privacy Amplification is about Alice and Bob who want to remove any residual information Eve may have about the key. They apply some algorithm to compress their partially secure key into a shorter one that is almost perfectly secure [4, 14]. It is proved by König, Maure and Renner in [88] that no matter which observable on her quantum states Eve measures after the classical privacy amplification, she is no better off than she would be if she had $H(X|Y) + t$ classical bits of information about X before the privacy amplification. This means that (classical) privacy amplification can be applied to eliminate Eve's partial (quantum) information about the key string Alice and Bob possess. The protocol creates a shorter string K of which Eve has negligible knowledge. Because the key bit string K is secret, it can subsquently be used for secure encryption [89, 90].

Alice and Bob now have a common reconciled key which they know is only partially secret from Eve. They now begin the process of privacy amplification, which is the extraction of a secret key from a partially secret one [81].

- Alice and Bob compute from the error-rate R obtained an upper bound k of the number of bits of reconciled key known by Eve. Let n denote the number of bits in recociled key, and s be a security parameter to be adjusted as required.
- Alice and Bob publicly select $n - k - s$ random subsets of reconciled key, without revealing their contents. The undisclosed parties of these subsets become the final secret key. It can be shown that Eve's average information about the final secret key is less than $2^{-s}/\ln 2$ bits [82].

4.2.4 Eavesdropping Attacks

The novelty of BB84 protocol and hence its huge advantage over classical ones is, that quantum mechanical principles allow sender and receiver to find out whether an eavesdropper was present or not. They can even calculate an upper bound of the amount of information an eavesdropper could have gained. The reasons for this are the principles of the no-cloning theorem forbids to create a perfect copy of the photon [72].

Eve cannot measure the polarisation of the photon precisely, since the used states are non-orthogonal. Moreover, Alice and Bob will be able to spot Eve trying to do that, because she will cause errors. Lo and Chau [91] presented a security proof for the principle of quantum key distribution, considering ideal systems.

In order to ensure unconditional security for a QKD protocol, a security proof needs to take into account all possible classes of attacks Eve might conduct. From the theoretical point of view of quantum mechanical measurements, any eavesdropping attack can be thought of as an interaction between a probe and the quantum signals. Eve then performs measurements on the probe to obtain information about the signal states. In this framework, three main classes of attacks are possible:

- Individual attacks: The adversary is supposed to apply some fixed measurement operations to each of the quantum signals, that is, Eve lets each of the signals interact with a separate probe (unentangled to the other probes) and measures the probes separately afterwards.
- Collective attacks: As in the individual attack, each signal interacts with its own independent probe. In the measurement stage of an collective attack, however, the restriction for Eve to measure the probes individually is dropped: Eve is allowed to perform measurements on all probes coherently.
- Coherent attacks: In the most general (also called joint attacks), Eve can apply the most general unitary transformation to all the qubits simultaneously. Effectively, this means that Eve has access to all signals at the same time.

  A further differentiation of these attacks can be made by determining whether Eve may delay the measurement of the probes till receiving all classical data, that Alice and Bob exchange for error correction and privacy amplification.

Individual attacks are generally weaker than collective attacks [91]. Hence, the security against individual attacks does not imply full security. Meanwhile, methods have been developed to prove unconditional security, that is, security against coherent attacks. However, it turns out that it is often sufficient to consider only collective attacks, since for typical protocols coherent attacks are not stronger than collective attacks [92].

4.2.5 Some Specific Attacks

In this Section, we study some possible scenarios for Eve and see what the best strategy is for Eve. Because she wants Bob to think that he received the state directly from Alice, Eve has to send such a state to Bob that the average probability that Alice and Bob find the same bit given that they both encode and measure in the same basis is as high as possible.

The spectrum of attacks ranges from the simple intercept-resend attack to more advanced methods like photon number splitting (PNS) attacks [93].

4.2.5.1 Intercept - Resend Strategy

Alice and Bob need to have some criteria to determine whether the key transmission was secure or not. The one way to find this is to imagine eavesdropping strategies on the BB84 protocol in order to reveal security limits of the system. The easiest eavesdropping strategy one can think of is the so-called intercept-resend attack (or direct attack) shown in Figure 4.6. Eve tries to measure every qubit and sends out the state which corresponds to the outcome of her measurement.

The idea with this kind of attack is to measure all or a proportion, ϵ, of the states Alice sends to Bob. If she chooses to measure only a fraction, ϵ, of the states, how she chooses which states to measure is dependent on how much information she wishes to obtain on the final message while making her presence as inconspicuous as possible. We will not consider how she chooses this fraction.

In this attack Eve simply interrupts the quantum channel, measures each incoming photon from Alice in a fixed or random basis. A photon is prepared in the state corresponding to that which was measured. This prepared photon is then sent to Bob, without that Eve reveal herself [82]. This leads to an average error rate of 25% in the sifted key, composed of events with 0% error whenever Eve uses the same basis as Alice and Bob, and events with 50% when her basis differs from theirs. In this way, Eve learns 50% of the sifted key.

4.2.5.2 Quantum Cloning Attack

Another attack that Eve could do against a continuous variable quantum key distribution is a quantum cloning attack (or a passive attack). In this attack, Eve obtains the data, stores it in quantum memory, and then sends it onto Bob. However in this case, unlike a direct attack, she is unable to manipulate the data once Bob has measured it.

This method was proposed for eavesdropping purposes by Gisin and Huttner [76]. They suggested that Eve can use either a machine that they named "Pretty Good Quantum Copying Machine" (PGQCM) or the Universal Quantum Cloning Machine (UQCM) to

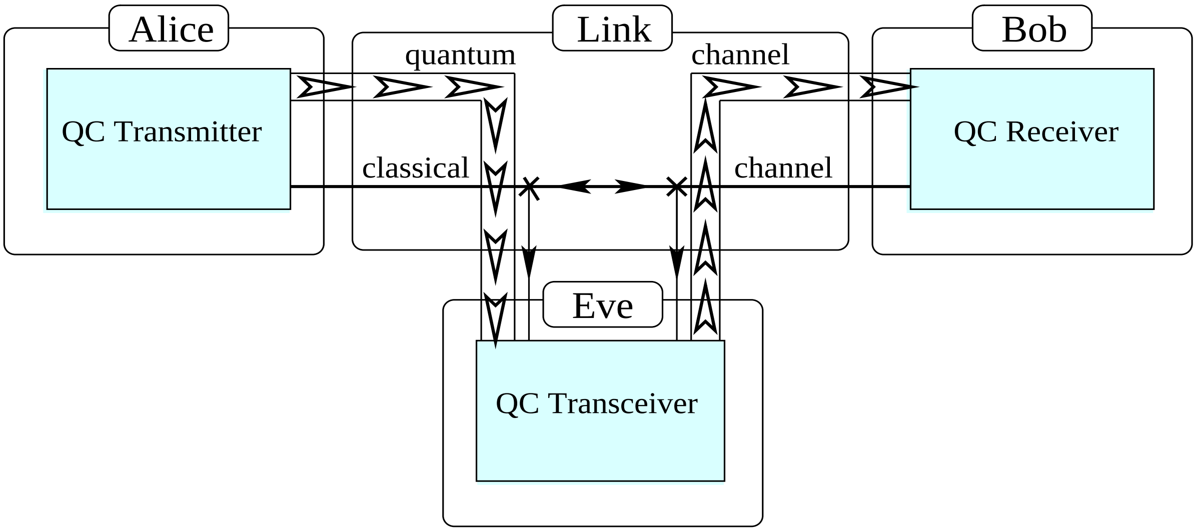

FIG. 4.6: The intercept-resend attack where Eve intercepts the pulses from Alice and read them in her chosen bases. She performs a measurement of each pulse as qubits in one of the two bases and then she will pretend as Alice and resend to Bob another qubits in the state corresponding to her measurement result.

copy Alice's qubit. Figure 4.7 shows how this attack can be done by Eve.

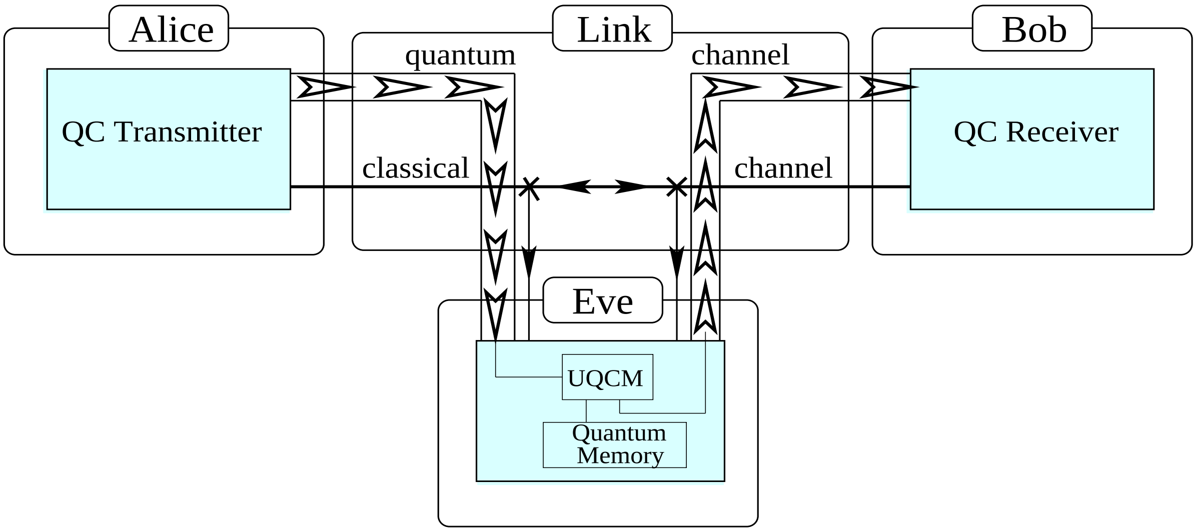

FIG. 4.7: A quantum cloning attack: Eve uses a universal quantum cloning machine to copy Alice's qubit. She keeps one of the copies in her quantum memory and sends the other one to Bob. When Alice and Bob discuss their choice of the bases, she can measure her qubit in the correct basis.

Quantum Cloning Machine (QCM) [94] is the trace preserving completely positive map, or equivalently the pair

$$QCM = \{U, |M\rangle\}, \tag{4.2}$$

where QCM can be seen as a quantum processor U that processes the input data according to some program $|M\rangle$.

The identity $|\psi\rangle_A|R\rangle_B \longrightarrow |\psi\rangle_A|R\rangle_B$ that transfers no information from qubit A to qubit B and the swap $|\psi\rangle_A|R\rangle_B \longrightarrow |R\rangle_A|\psi\rangle_B$ that swaps information between A and B are examples of $QCMs$.

The attack would look like this: Eve intercepts every photon, that Alice sends out and uses a cloning machine to end up with two photons which have a certain fidelity F_j defined for each of the outputs $j = 1, ..., M$ of the cloning machine as the overlap between ρ_j and the initial state $|\psi\rangle$:

$$F_j = \langle\psi|\rho_j|\psi\rangle, \tag{4.3}$$

where ρ_j is the partial state of clone j.

Eve keeps one of the photons in a so-called quantum memory and sends the other one to Bob. When the bases are announced during the sifting procedure, Eve can take her photons from the quantum memory and measure in the correct basis [76]. A QCM is called universal if it copies equally well all the states and if F_j is independent of $|\psi\rangle$.

4.2.5.3 Optimal Individual Attack

There are also specific attacks for particular protocols. For example, the reverse reconciliation protocol, an entangling cloner attack has shown to be the optimal attack [61]. This particular attack can be thought of as Eve creating two quantum correlated states, one that she keeps and the other she sends to Bob. In the direct reconciliation (and postselection) protocol, a direct attack using a beam splitter is used as Eve's attack.

A more advanced form of measuring for the adversary involves positive operator-valued measures (POVMs) which allow to increase the ratio of gathered information per induced disturbance. Lütkenhaus investigated the use of POVMs under the restriction that Eve performs her measurements before Alice reveals the basis [95].

A good indicator for the possibility to recover a safe cryptographic key is the comparison of the mutual information I_{AB} between Alice and Bob (after eavesdropping) to the mutual informations I_{AE} and I_{BE} between Alice and Eve, and between Bob and Eve, respectively. If (whether due to eavesdropping or channel noise) $I_{AB} \leqslant min\{I_{AE}, I_{BE}\}$, Alice and Bob cannot establish a secret key any more, using only one-way classical post-processing [5, 95]. For more details about how the mutual information I_{AB}, I_{AE}, and I_{EB} are calculated we refer to [96, 97].

4.2.6 Other Protocols

Several QKD protocols have been proposed since the birth of the BB84 protocol also called a four-state protocol. Other protocols can be developped such as two-state protocol (e.g. the B92 [5]), three-state protocol [98] or six-state protocol [99, 100]. Some of them are optimised to be efficient with respect the secret key rate (the number of key bits generated per transmitted quantum state), while others are designed to be efficient with higher noise levels, which makes them more suitable for practical implementations.

4.2.6.1 Two-state Protocol: B92

In 1992, Charles Bennett one of the BB84 developers published the simplified BB84 protocol named B92 protocol which uses only two states, although non-orthogonal, on Alice's side to represent a 0 or 1. The BB84 and B92 protocols are nowadays widely used, they are securely proven and largely experimented. In this protocol Alice's side uses two non-perpendicular polarization angles and the other two polarization angles are used on Bob's side for reading process [101]. Qubit-Polarization matching for B92 protocol for Alice's side is shown at Figure 4.8.

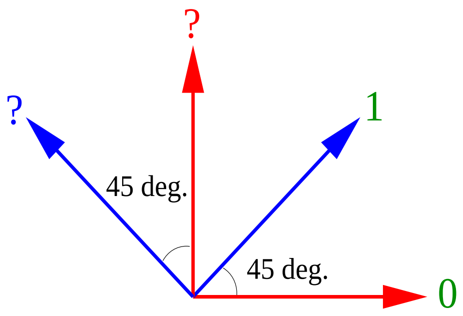

FIG. 4.8: Qubit-Polarization matching for B92 protocol on Alice's side.

In the case of the qubits being realised as polarization encoded single photons, Alice polarizes the photon with 0 degree in order to send a qubit with value of 0 and with 45 degree in order to send a qubit with value of 1.

On Bob's side we must read polarization of the photon with a filter that does not contain a base having the same polarization as the photon because reading of photon and its qubit value is considered as invalid. Similar to the BB84 protocol, in the B92 protocol eavesdropping can be detected after comparing a small amount of revealed (sacrified) qubit values but chosen base types for sending process are not revealed. This means that in the sifting step, Bob announces only the signals (photons) on which he obtained the final results, but not the measurement basis, since this would effectively reveal the bit value itself. On Bob's side, Qubit-Polarization matching for B92 protocol is shown in Figure 4.9 [29].

4.2.6.2 The EPR Protocol

In 1991, Eckert published the EPR protocol (EPR refers to the Einstein-Podolsky-Rosen paper of 1935) which is closely related to BB84, but the difference is in proofs of security against an eavesdropper [6]. The idea is that Alice and Bob initially share a large number of qubit pairs in one of the Bell states, for example $|B_0\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.

A pair of correlated states $(|\Psi_1\rangle, |\Psi_2\rangle)$ such that measuring one of the two collapses the state of the other. To do key distribution, an EPR source generates N pairs $(|\Psi_1\rangle, |\Psi_2\rangle)$ and sends $|\Psi_1\rangle$ to Alice and $|\Psi_2\rangle$ to Bob. When the polarization of $|\Psi_1\rangle$ is measured, measuring $|\Psi_2\rangle$ will give a known result (and vice versa).

An eavesdropper's only hope is to attack the EPR source and try to get $|\Psi_1\rangle$ or $|\Psi_2\rangle$. In this case, the pair will be disturbed and Alice and Bob's qubits will not match. So Alice and Bob make measurements and compare their results. If their results are different when the same measurement basis was used, they know that they have detected an eavesdropper. So they start again, some other day.

4.2.7 Security of Quantum Key Distribution

Quantum Key Distribution (QKD) protocols can be provably secure because the security, first, relies on fundamental laws of quantum mechanics instead of intractability assumptions. Furthermore, for every attempt to distinguish between two no-orthogonal quantum

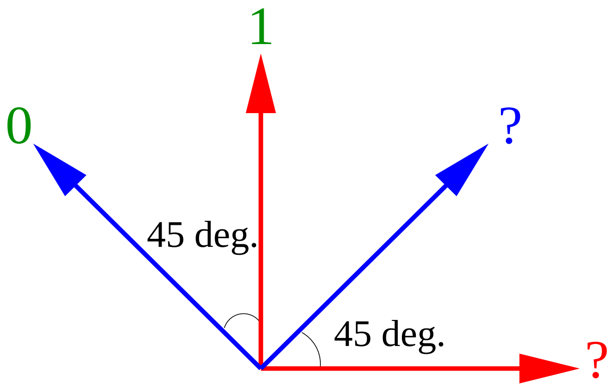

FIG. 4.9: Qubit-polarization matching for B92 protocol on Bob's side.

states, information gain is only possible at the expense of introducing disturbance in the system.

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

Information reconciliation and privacy amplification are described in the section 4.2.3. The threshold for the bit error rate is thus determined by the properties of the particular protocol and efficiency of the information reconciliation and privacy amplification protocols. In this way a private classical key can be created between two parties. The key can then be used to implement a (classical) private key cryptosystem to enable the parties to communicate securely.

4.2.8 Bit Extraction: Strategies and Probabilities

Bit Extraction Strategy

The bit encoding scheme used by Alice is the following. Let $b \in \{0, 1\}$ be the bit to be encoded. Suppose that a bit value is encoded using photons polalarizations states in the rectilinear RL or the diagonal DG basis, chosen at random. The encoded bit is then sent to Bob. Suppose Bob receives the qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. He measures the state $|\psi\rangle$ in the RL basis or the DG basis at random. Bob decodes measurement of state $|0\rangle$ or $|+\rangle$ to bit value 0 and a measurement of state $|1\rangle$ or $|-\rangle$ to bit value 1.

Bit Extraction Probabilities

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

Theorem 1

Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ be the general qubit state that Bob can measure in the RL or the DG basis [82] with $|\alpha|^2 + |\beta|^2 = 1$. Let $RL = \{|0\rangle, |1\rangle\}$ be the rectilinear basis and $DG = \{|+\rangle, |-\rangle\}$ be the diagonal basis. Let a measurement of $|0\rangle$ or $|+\rangle$ correspond to a measurement of bit value 0 and let a measurement of $|1\rangle$ or $|-\rangle$ correspond to a measurement of bit value 1. The probability to extract bit value $b \in \{0, 1\}$ from $|\psi\rangle$ when one measures in basis RL is denoted by $P_{RL}^{|\psi\rangle}(b)$. The probabilities corresponding to the state after the measurement are given by

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

Proof

If a measurement is done in an orthonormal basis RL then the operator describing the measurement is Hermitian and thus the measurement itself is a projective measurement. We can proof this by doing the following calculation.

The probability to extract bit value 0 is

$$P_{RL}^{|\psi\rangle}(0) = \langle\psi|P_0|\psi\rangle = |\langle\psi|0\rangle|^2 = |\alpha|^2. \tag{4.4}$$

The state after this measurement is

$$\frac{P_i|\psi\rangle}{\sqrt{P_{|\psi\rangle}(0)}} = \frac{\alpha}{\sqrt{|\alpha|^2}}|0\rangle = \frac{\alpha}{|\alpha|}|0\rangle. \tag{4.5}$$

In the same way we find

$$P_{RL}^{|\psi\rangle}(1) = |\beta|^2, \tag{4.6}$$

and the state after measurement is

$$\frac{\beta}{|\beta|}|1\rangle. \tag{4.7}$$

Another theorem says that if Alice and Bob used the same basis with probability 1 then the extracted bit values from them are same, which means that there is no eavesdropper. But if the basis used are different then the extracted bit value by the receiver is random.

Theorem 2

Let the bit to be encoded be $b \in \{0, 1\}$. Suppose the bit is encoded into $|\psi\rangle$ according to the bit encoding strategy. Suppose a measurement of $|0\rangle$ or $|+\rangle$ corresponds to bit value 0, a measurement of $|1\rangle$ or $|-\rangle$ corresponds to bit value 1. If there is no eavesdropper, then

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

and

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

If $|\psi\rangle$ is measured in correct basis then the state after the measurement is equal to $|\psi\rangle$.

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

Proof

If $|\psi\rangle \in RL$, then $\alpha = 1$ and $\beta = 0$ or $\alpha = 0$ and $\beta = 1$.

If $|\psi\rangle \in DG$, then $\alpha = \frac{1}{\sqrt{2}}$ and $\beta = \frac{1}{\sqrt{2}}$ or $\alpha = \frac{1}{\sqrt{2}}$ and $\beta = -\frac{1}{\sqrt{2}}$.

The results are obtained from Theorem 1.

Measuring in both bases gives no extra information.

After a measurement of a qubit state $|\psi\rangle$ in the $RL-$ or the $DG-$ basis, a following measurement in the other basis does not give an extra information about $|\psi\rangle$. This is because the outcome of the second measurement would be random.

For example, suppose the qubit $|\psi\rangle = \gamma|0\rangle + \delta|1\rangle$, with $|\gamma|^2 + |\delta|^2 = 1$, is measured in the $RL-$ basis. Suppose bit value 1 is measured. We know according Theorem 1 that the state after the measurement is equal to $\frac{\delta}{|\delta|})|1\rangle$. Suppose that this state is subsequently measured in the $DG-$ basis. The probability that bit value 0 is (substitute $\alpha = 0$ and $\beta = \frac{\delta}{|\delta|}$ in the Theorem 1)

$$P_{DG}(0) \;=\; \frac{|\alpha+\beta|^2}{2} = \frac{|\delta|^2}{2|\delta|^2} = \frac{1}{2} \tag{4.8}$$

and

$$P_{DG}(1) \;=\; \frac{|\alpha-\beta|^2}{2} = \frac{|\delta|^2}{2|\delta|^2} = \frac{1}{2}\,. \tag{4.9}$$

Chapter 5

Practical Real Quantum Key Distribution

5.1 Introduction

As well as focussing on possible applications, the first experimental demonstration of quantum cryptography was performed by Bennett and Brassard in 1989, a key was exchanged over 30 cm of air [82, 102]. This experiment motivated other research groups to enter the field. The first demonstration over optical fiber took place in 1993 by researchers at the University of Geneva. The 90s saw a host of experiments, with key distribution distance spans reaching up to several dozens of kilometers. The performance of a quantum cryptography system is described by the rate at which a key is exchanged over a certain distance. For more information, refer to [73].

When a photon propagates in an optical fiber, it can have a certain probability to get absorbed, because of transparency limitations of the glass used. When the distance between the two quantum key distribution stations increases, two effects reinforce each other to reduce the effective key exchange rate. First, the probability that a given photon reaches the receiver decreases. This effect causes a reduction of the raw exchange rate. Second, the signal-to-noise ratio decreases. A higher error rate implies a more costly key distillation, in terms of the number of bits consumed, and in turn a lower effective key creation rate.

The main cause of reduction of the number of photons detected by the receiver is the imperfection of single-photon source and detectors. The fact that only a fraction of the photons reaches the detectors does not constitute a vulnerability, as these do not contribute to the final key. It only amounts to a reduction of the key exchange rate.

Typical key exchange rates for existing quantum cryptography systems range from hundreds of kilobits per second for short distances to hundreds of bits per second for distances of several dozens of kilometers. These rates are low compared to typical bit rates encountered in conventional communication systems. In a sense, this low rate is the consequence of the absolute secrecy of the key exchange process. One must remember though that the bits exchanged using quantum cryptography are only used to produce relatively short keys (128 or 256-bits). Nothing prevents transmitting data encrypted with these keys at high bit rates.

The span of current quantum cryptography systems is limited by the transparency of optical fibers and typically reaches 100 kilometers. In conventional telecommunications, optical repeaters located approximately every 80 kilometers are used to amplify and regenerate the optical signal. In quantum cryptography, it is not possible to do so. Repeaters would indeed have the same effect as an eavesdropper. The laws of quantum physics forbid this. It is obviously possible to increase this span by chaining links.

In 2002, id Quantique launched the first commercial quantum cryptography system called Clavis (plug-and-play) Quantum Key Distribution System, designed for research and development applications [103]. Figure 5.1 shows the picture of this Clavis.

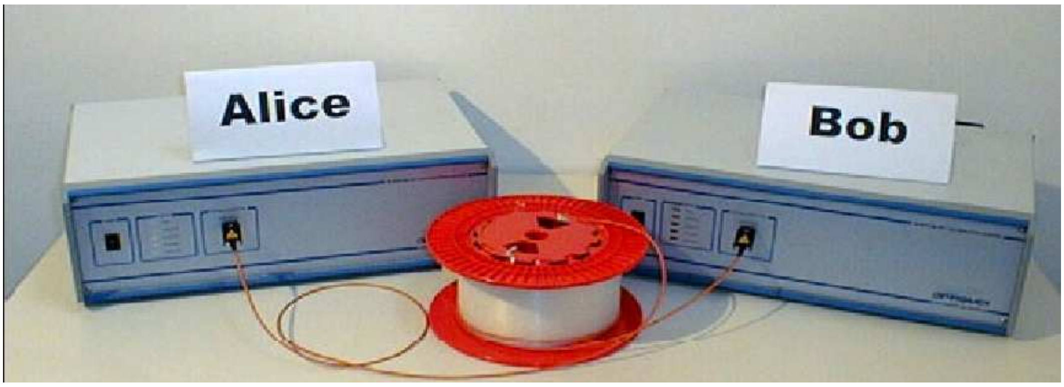

FIG. 5.1: Picture of the first commercial quantum key distribution system.

The roll of optical fibre on the table is the optical fibre link representing the quantum channel. This roll contains 13 km of uncladded optical fibre for bench testing of the system.

In 2004, this system was used in one of the first commercial applications of quantum cryptography. Data transmissions between two data centers of a data hosting company in Geneva were encrypted using keys exchanged by a Clavis system. The primary data center hosted mission critical information, which were replicated in the secondary data center, located 11 kilometers away, to guarantee business continuity of the company.

In early 2005, id Quantique has released a new version of its quantum cryptography system. It is called Vectis and consists of a link encryptor [2]. It features automated key exchange by quantum cryptography over an optical fiber up to a distance of 100 kilometers, as well as high-bit rate full duplex Ethernet traffic encryption and authentication. It can be easily deployed in an existing network and is used by private and public organizations to secure critical optical links.

The experiment in this work was focused on the test of a fibre optical quantum key distribution system working at 1550 nm and based on the id 3000 Clavis System. Figure 5.2 shows the Quantum Key Distribution System Alice and Quantum Key Distribution System Bob connected to the computers and quantum channel.

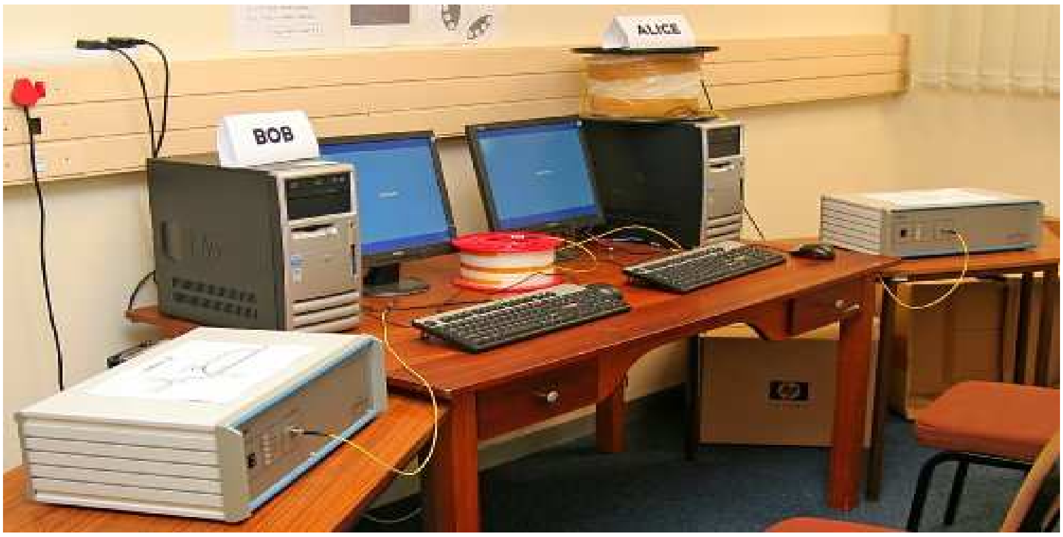

FIG. 5.2: Picture of the id 3000 Clavis Quantum Key Distribution System.

The stability of id 3000 QKDS over installed terrestrial cables of a distance 13,08 km was our preoccupation at Cato Manor in Durban between the Central Application Office and Municipal Original Office buildings. Another test was done over a distance of 15.6 km in Pinetown between the Pinetown Civic Centre and Pinetown Clinic buildings. The results to these tests are presented in this thesis.

5.2 Experimental Setup

5.2.1 id 3000 Clavis Quantum Key Distribution System

The experimental setup for id 3000 Clavis Quantum Key Distribution System (QKDS) as shown in Figure 5.3 is usually divided into three building components, two stations named Alice (QKDS-A) and Bob (QKDS-B) controlled by one or two external computers and one quantum channel.

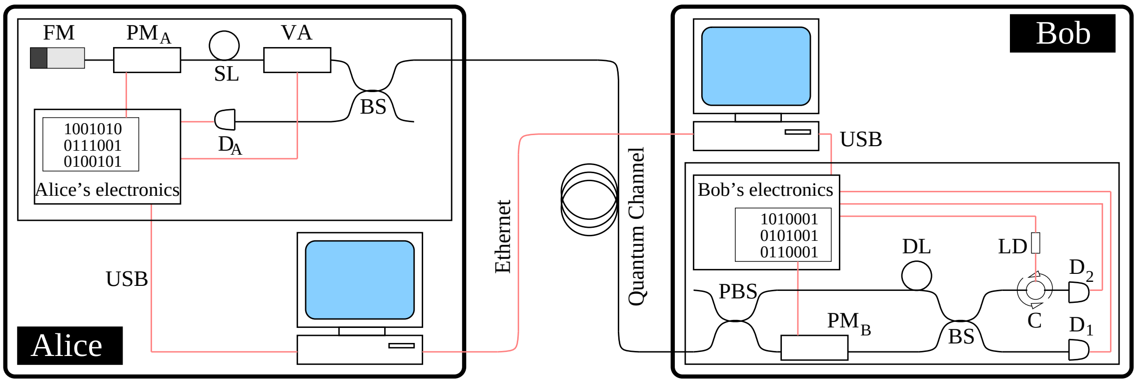

FIG. 5.3: Schematic of the Plug and Play system for Quantum Key Distribution.

The first component, (QKDS-A) the transmitter consists of the phase modulation used to encode bit values on the pulses. The second component, quantum channel or optical link for transfering the phase encoding between (QKDS-A) and (QKDS-B) stations, it may be either an optical fiber or just the free-space (atmosphere). The third component, (QKDS-B) the receiver detects the phase encoding using a single photon detectors.

A comprehensive software suite developed by id Quantique implements automated hardware operation and complete key distillation. Two quantum cryptography protocols are implemented. The exchanged keys can be used in an encrypted file transfer application, which allows secure communications between two stations [104].

5.2.2 Transmitter (QKDS-A Station)

5.2.2.1 Optical System of Transmitter

The optical system of the transmitter is used to modulate the phase between the two components of the optical pulses P_1 and P_2 sent by the Bob's setup (refer to Figure 5.3). The intense incoming pulses are split at the input by a beam splitter (BS). The beam splitter (BS) with its detector D_A is used only to trigger Alice's phase modulator (PM_A) from which a phase shift φ_A is added to the first pulse P_1 only. The pulses P_1 and P_2 are reflected on a Faraday mirror and their polarization turned by 90^o which means that they come back orthogonally polarized.

When leaving Alice's setup, the pulses contain not more than a single photon because of the role (task) played by the variable attenuator (VA) to attenuate them. The attenuation in this part must be set to guarantee that the intensity of reflected pulses is approprietely low. The attenuator is preceded by a long delay line or storage line SL which serves to prevent the problem of increasing of Quantum Bit Error Rates (QBER) which can be caused by the high intensity ratio between forward and backward propagating light, and the single photon sensitivity of the detectors.

In turn, Alice randomly phase modulates a pulse train of weak coherent states by $(0, \pi)$ for each pulse and sends it to Bob via quantum channel, with an average photon number of less than one per pulse. To understand how detection of photon states is done by Bob, we refer to Subsection 5.2.4.1, first paragraph on page 83.

5.2.2.2 Electronic System

The electronic system of the transmitter is subdivided into two parts: The high-level and low-level electronics. The high-level elctronics is connected into an external computer (which is used to control this high-level) through the optical system. The low-level electronics is used to interface the high-level with the optical system. The five main tasks below are performed by the high-level:

- status monitoring: consists of power supplies and temperature.
- variable optical attenuator control: used to control the attenuation applied by the two channels of the variable optical attenuator.
- classical detector control: it can be set to check the voltage and security level of the two discriminators connected to its output.
- application of phase modulation by phase modulator: this function allows setting the voltage corresponding to the four phase values (one for each state). Delaying the timing of a pulse (signal) coming from the classical detector obtains the precise timing of the application of the phase modulation.
- transfer of bit values for key exchange: the bit values sent by the computer are used for next key exchange session.

According to the principle of the so-called *p&p* (plug and play) auto-compensating set-up as shown in Figure 5.3, the key is encoded in the phase between two pulses travelling from Bob to Alice and back.

5.2.3 Quantum Channel

A quantum channel is a communication channel which can transmit quantum information, as well as classical information. The state of a qubit is an example of quantum information while a text document transmitted over the internet is an example of classical information. Quantum information cannot be transmitted by classical channels themselves, but it is done in combination with quantum channels [105].

5.2.3.1 Optical Fiber

The optical link for transfering the photons in Quantum Key Distribution Systems may be either an optical fiber or just the atmosphere. Non-telecom-standard single-mode fibers with wavelength around 800 nm are used in experiments, because efficient detectors are commercially available for visible light detection. The drawback is the high attenuation, so that these systems can only be used for short distances (below 5 km). The ability of telecommunication optical fibers with wavelength near 1300 or 1550 nm for long transmission distances is also perfect for quantum signals, but only poor single photon detectors are avalable for those wavelengths [75].

Nowadays, the most popular choice channel is Standard Optical Single-Mode Fiber (SMF) [21]. It connects two arbitrary points, and can be easily extended to networks. SMF has two window wavelengths: one is 1310 nm, and the other is 1550 nm. At these two wavelengths the absorptions are very low ($\sim$ 0.35 dB/km at 1310 nm, and $\sim$ 0.21 dB/km at 1550 nm).

Today most fiber-based Quantum Key Distribution implementations use 1550 nm photons as information carriers. The main disadvantage of optical fiber is its birefringence. The two dispersions for optical fiber are the strong polarization dispersion, which made it hard to implement polarization-coding system, and the strong spatial dispersion, which affects the high speed ($10 + GHz$) QKD systems heavily [106] as the pulses are broadened and overlap with each other. This is the reason why the loss in fibers (0,21 dB/km at 1550 nm) puts a limit on the longest distance that a fiber-based Quantum Key Distribution System can reach.

5.2.3.2 Free Space

Recently, many researchers are interested with Free Space channel than optical fiber channel because of the negligible dispersion on the polarization and the frequency. But the big problem with free space is the alignment of optical beams for long distances, particularly due to the atmospheric turbulence. Mountains and buildings are serious obstacles for free space QKD systems which requires a direct line of sight between Alice and Bob. The greatest motivation free space QKD scheme is the hope for ground-to-satellite [107, 21] and satellite-to-satellite quantum communication.

In reference [108], researchers discuss the feasibility of building a completely secure channel for global communication, via satellites in space. That is why, in 2008, photons have been fired directly at the Japanese Ajisai Satellite and received back at the Matera ground-based station in southern Italy. The research team, led by Paolo Villoresi and Cesare Barbieri from Padova University, Italy, proves that the photons on the ground-based station were the same as the originally emitted.

This innovation can maybe solve the problem of quantum-encrypted communication which has only, until now, been proven possible at distances up to about 150 kilometers, either down optical fibres or via telescopes. Let us remind that photons sent down optical fibres are dissipated due to scattering and absorption and those sent through free space are subject to interfering atmospheric conditions.

5.2.4 Receiver (QKDS-B Station)

5.2.4.1 Optical System of Receiver

The laser diode (LD) in Bob's setup that is shown in Figure 5.3 emits at 1550 nm a strong pulse which is separated at a first 50/50 beamsplitter (BS). The pulse P_1 is taking the short arm through the phase modulator (PM_B) which is inactive, while the pulse P_2 is taking the long arm through a 50 ns delay line (DL).

Both pulses converge on the input ports of a polarizing beam splitter (PBS) where the polarization of the pulse P_1 is adjusted so that P_1 is being transmitted by the polarizing beam splitter. Meanwhile, the pulse P_2 is being delayed whereas polarization evolution is ajusted so that it is being reflected by the polarizing beam splitter. So P_2 exits Bob's setup (by the same port of the PBS) with some 100 ns delay and a phase shift of π resulting from the coupler and the reflection at the PBS. The pulses travel down through the fibre and enter Alice's setup.

P_1 will now be reflected at the PBS, since its polarization has been changed at the Faraday mirror of Alice's setup. While P_2 will be transmitted by PBS, and will pick up the phase shift φ_B at Bob's phase modulator. In its arm, P_1 is delayed at the slope so that they arrive at the same time at the BS, where they interfere. Then, they are detected either in D_1, or after passing through the circular (C) in D_2.

When a pulse train of weak coherent states sent by Alice arrives on Bob's site, Bob measures the phase difference between two sequential pulses using a 1-bit delay Mach-Zehnder interferometer and photon detectors, and records the photon arrival time and which detector clicked [97]. After raw level transmission, Bob tells Alice the time instances at which a photon was counted. From this time information and her modulation data, Alice knows which detector clicked at Bob's site. Under an agreement that a click by detectors 1 denotes "0" and a click by detector 2 denotes "1", for example, Alice and Bob obtain an identical bit string.

5.2.4.2 Electronic System

The electronic system of the QKDS-B station consists of high-level electronics which is interfaced to an external computer through the USB bus and low-level electronics which is used to interface the hifh-level electronics with the optical system. The high-level electronics is controled by the external computer. As for the transmitter, QKDS-B Station also has five functions which are performed by the high-level electronics:

- The first function "status monotoring“, consists of the monitoring of the status (power supplies, temperature, Avalanche Photo Detector cooler current temperature, etc.) of the station.
- The second function "laser diode control“, consists in controlling the laser. The setting duration of the pulses, their amplitude, as well as their timing is done by the electronics, which also allows to read the laser power using the internal photodiode.
- The third function "phase modulator“, consists in controlling the phase modulator. The setting duration of the phase modulation pulses, as well as their amplitude is done by the electronics. It controls also the timing of the phase modulation pulses.
- The fourth function "photon counting detectors control“, consists in controlling the photon counting detectors. The electronics allows to set the bias voltage of each detector independently.
- The last function of the high-level electronics is the transfer and storage in a buffer

of the bit values sent by the computer and which are to be used in the next key exchange session.

The interferometer inside Bob's setup is auto-compensated since the two pulses take the same path in the reversed order. To the application of BB84, Alice applies a phase shift of 0 or π and $\pi/2$ or $3\pi/2$ on the second pulse with phase modulator (PM_A). Meanwhile Bob chooses the measurement basis by appling a 0 or $\pi/2$ shift on the first pulse on its way back.

In this section, we described the hardware of the two stations of id-3000 Quantum Key Distribution System. The optical system and the electronic system were presented for each station. The goal of thesis is novel protocol investigation, quantum network implementation or cryptographic study. The id 3000 Clavis system allows quick experimental preparation and validation [103].

5.3 Clavis Application

The Clavis software package consists of a single program. It performs key distribution, key distillation, as well as file encryption and transfer. The Clavis program running the QKDS-B station acts as the master taking control on the Clavis program running the QKDS-A station, which acts as the slave. There are two processes running in parallel in the Clavis: One is in charge of key buffer replenishment using quantum key distribution and other allows to transfer the encrypted files. The key buffer performs sequentially four main tasks, which are run repeatedly.

- The first task is a hardware check-up that allows to verify that the different subsystems are operating correctely. Among these subsystems we set out the status of the stations (temperature, power supplies for both QKDS stations); the laser (QKDS-B: measurement of the emitted power); the noise probability of the photon counting detectors (QKDS-B).
- The second task is a line length measurement which consists in measuring the length of the optical link in order to synchronize the emission of the laser pulses with their

detection. The delay between the emission and the detection of the pulses is scanned by the QKDS-B in order to maximize signal detection.

- The third task is a raw key production; once the optical link length has been measured, the Clavis can move to the production of the raw key by exchange of quantum pulses.
- The fourth task is a key distillation that allows to take the raw key bits, stored in a key distillation buffer, and distillate them in order to produce the cryptographic key. It includes four steps: Sifting, Error correction, Privacy amplification and Authentication.

5.3.1 Using the id-3000 QKDS

In order to use the id-3000 QKDS, the QKDS-A station and QKDS-B station have to be connected together via an optical fiber link serving to as a quantum channel. The optical link can be installed after the id 3000 QKDS has been connected to computers. The connector of one of the optical links (optical fiber spool, installed optical fiber, etc.) must be cleaned and compatible with that of the id-3000 QKDS. This optical link is connected to the first station. The connector of the second end must also be cleaned and compatible with that of the id 3000 QKDS. The optical link also is connected to the second station [104].

It is recommended to keep clean at all times the patch cord fiber ends connected to a id-3000 QKDS station opical input port, this is done, in order to ensure minimum insertion losses and to reduce reflection. In case of inappropriate insertion losses, the connector of the patch cord can be easily cleaned or repolished by the user.

The QKDS stations are exclusively driven by two computers via the USB port and these two computers communicate via an ethernet or internet link. The link can take the following form:

- Ethernet local area network (this solution requires that the computers have Ethernet cards).

- Direct Ethernet connection (using a crossed Ethernet cable).
- Internet: any internet connection (local area network, modem) is suitable.
- Second optical fiber link with media connectors.

5.3.2 Configuration

The software package consists of two applications, CryptoMenu and Clavis software programs allowed by the cofiguration to run the system.

The CryptoMenu application allows to access all the hardware parameters of the id 3000 QKDS stations and to perform simple tasks, such as line length measurement and key exchange. It includes two programs (CryptoMenuAlice and CryptoMenuBob), which allows to run on two computers connected to the QKDS-A and QKDS-B stations.

The Clavis application constitutes a complete Quantum Key Distribution software suite allowing key exchange, key distillation, as well as file encryption/decryption and transfer. It includes a single program, which allows to run on two computers connected to the QKDS-A and QKDS-B stations.

5.4 Experimental Results

In this section the results from one of the experiments done are described and performed with the CryptoMenu programs. In this experiment, we played the role of Bob by using the CryptoMenuBob program and the results obtained are summarized in different Tables by the end of this chapter, meanwhile the figures of different graphs are described in the subsections. Of particular interest is the temperature of the detectors which must be approximately $-49°C$ and the error is the obtained value which is different to $-49°C$ (called set temperature) when the program start working. If this error becomes too large, the station will generate another error which can be corrected only by id Quantique support. Therefore, in the case of large error the users have to switch off the system and start it again.

5.4.1 Status Verification

The CryptoMenuBob program displays in the first step the status information about internal parameters of the station. The information displayed with this program is different from that displayed with CryptoMenuAlice program. Table 5.1 shows this displaying of temperature and voltage, and Figure 5.4 shows the graph of the system temperature time whisch is the combination of two temperatures one for the Central Processing Unit (CPU) and other for the system being shown during a period of time. The labeled Readings on the graphs meant the number of time the program read the temperatures during a period of time from 10:32 to 14:03, time the machines start and stop to work.

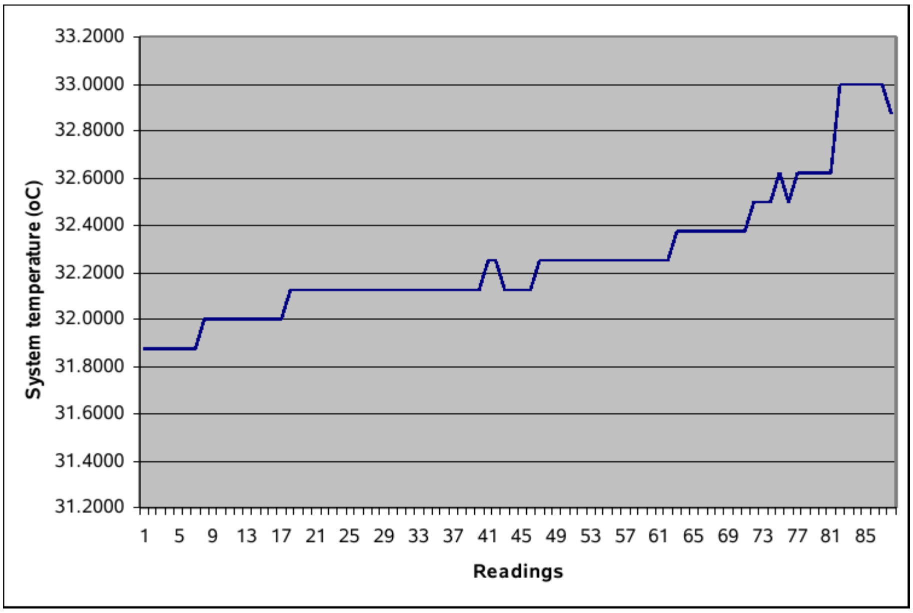

FIG. 5.4: System temperature time on QKDS-B station.

In order to abtain correct results, some internal parameters are described and the results are shown in Table 5.2 where the bias voltage of the photon counting avalanche photodiode (APD Bias 1) and avalanche photodiode (APD Bias 2) was set in order to avoid damages. It is essential that the number of pulses used in the QKDS-B station matches that used in QKDS-A station when performing a key exchange. The product of the number of pulses and spacing between two pulses (40 [m] corresponding to 200 [ns] = 1/5 [MHz]) was not exceed twice the length of the delay line of the QKDS-A (normally 12,500 [m]).

When performing a key exchange, the value number of detection pulses (gates) is normally equal to the number of the laser pulses and the duration of laser pulse emitted is set to 500 [ps] for this key exchange. The coarse delay line is used to set the timing of the photon counting avalanche photodiodes (common to both detectors). The fine delay line 1 and fine delay line 2 respectivelly are used to set the timing of the photon counting avalanche photodiodes 1 and avalanche photodiodes 2. Figure 5.5 shows the internal parameter read temperature detector of QKDS-B station.

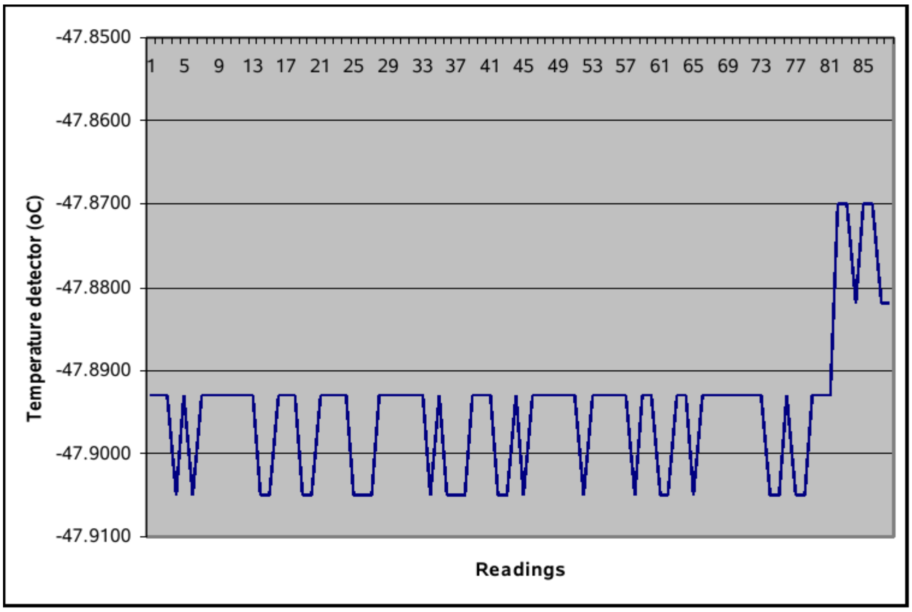

FIG. 5.5: Temperature detector of QKDS-B station.

We defined the waiting duration 1 as the duration of the pause between the laser pulse train and the delay preceding the detection gates train and the waiting duration 2 as the duration of the pause between the end of the frame and the begining of the next one. The duration of the dead time is used to inhibit detector gates after each detection. Both detectors are inhibited after a detection. The dead time value is calibrated in microseconds [μs].

When the pulser is started, the number of times the frames emission procedure will be executed. For proper operation, the number of frames used in CryptoMenuAlice is identical as that used in CryptoMenuBob. The total numbe of bits in a cycle is equal to the product of the number of pulses and the number of frames. This value must not exceed

$1,048,576 = (2^{20})$. The PM Pulse Width is the duration of the pulse applied by the phase modulator of the QKDS-B station (Should normally be set to 2). The Laser power parameter of the fitting function is used to calculate optical power recorded by the internal photodiode of the laser diode.

5.4.2 Noise Probability Measurement

In the second step the CryptoMenuBob application measures the dark count probability of the photon counting detectors of the id-3000 QKDS-B station. The graph of the noise probability measurement performed on detector 1 is shown in Figure 5.6 while the graph of noise probability measurement performed on detector 2 is shown in Figure 5.7.

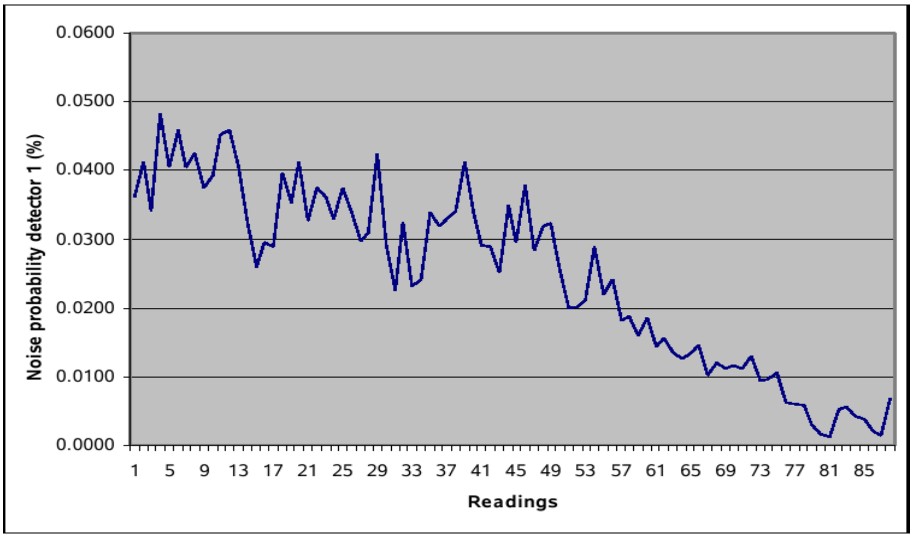

FIG. 5.6: Noise probability measurement performed on detector 1.

The program performs a dark count measurement after asking to enter the target statistical uncertainty in %. During the measurement, the program will wait until $1/\delta^2$ dark counts are accumulated for individual detector before being interrupted, where (δ represents the targeted relative uncertainty or targeted statistical error in which usually is equal to 10).

In order to obtain correct noise values, it is recommended to keep the number of detection pulses larger than 100. To measure the dark count (or noise) probability for each detector, the system the pulser without laser pulses which means the number of laser pulses is equal to zero. During the experiment, the repetition frequency was set to approximately 5 [MHz] and the dead time was set to 12 [μs], and this in order to mitigate the effect of after pulses. The number of laser pulses is set to 1 (minimum). In order to prevent light emission, which could influence the noise measurement, the laser curent is set to 0%.

The decreasing trends in noise probability as observed in figures 5.6 and 5.7 mean that when the system start to work from 10:31 to about 12:00 O'clock, the noise measurement was very high and after 12:00 to 14:00 O'clock time to stop the system, it was less noise measurement due to the temperature. The program displays the number of dark counts as well as the dark count probability and the results of this command are shown in the Table 5.3.

5.4.3 Line length measurement

The line length measurement consists in measuring the length of the optical link in order to synchronize the emission of the laser pulses with their detection. In the QKDS-B station, the optical link length measurement function starts to scans the value of coarse delay, fine delay 1, fine delay 2 and waiting duration 1 between the emission and the detection of the pulses in order to find the maximum of the detected signal for both detectors. During

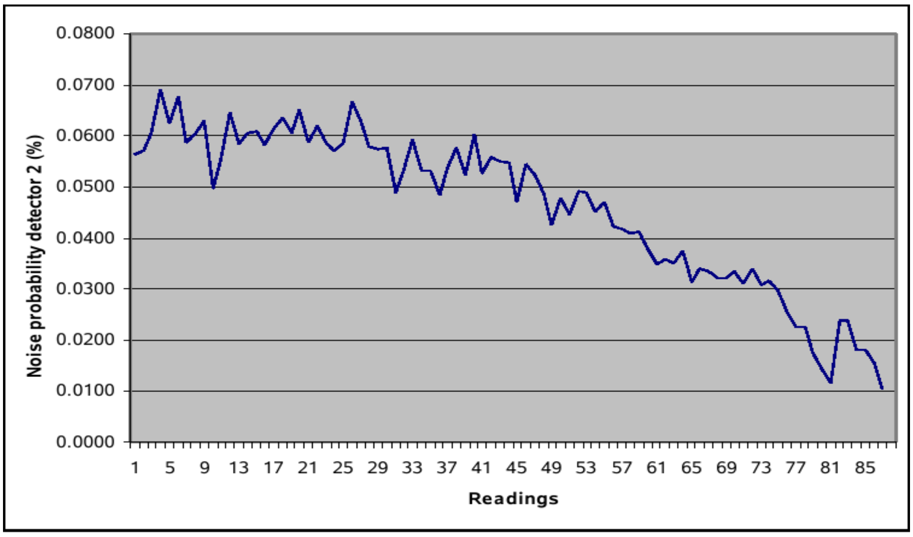

FIG. 5.7: Noise probability measurement performed on detector 2.

the measurement, the phase modulator of the QKDS-B system is turned on to direct the photons to both detectors equally.

The id-3000 QKDS follows a two-way approach to perform an optical link length measurement, this means that in this system, the light pulses are emitted by the QKDS-B station, travel to the QKDS-A station where they are attenuated and reflected back. They are finally detected by the photon counting detectors of the QKDS-B station. This is developed in the section 5.2.4. The timing of the photon counting detectors gates must be precisely set, which is achived by performing a time of flight optical link length measurement. The length of the optical link used for this experiment was approximately 13 km. It is shown in Figure 5.8 and its measurement with time is shown in the graph of Figure 5.9.

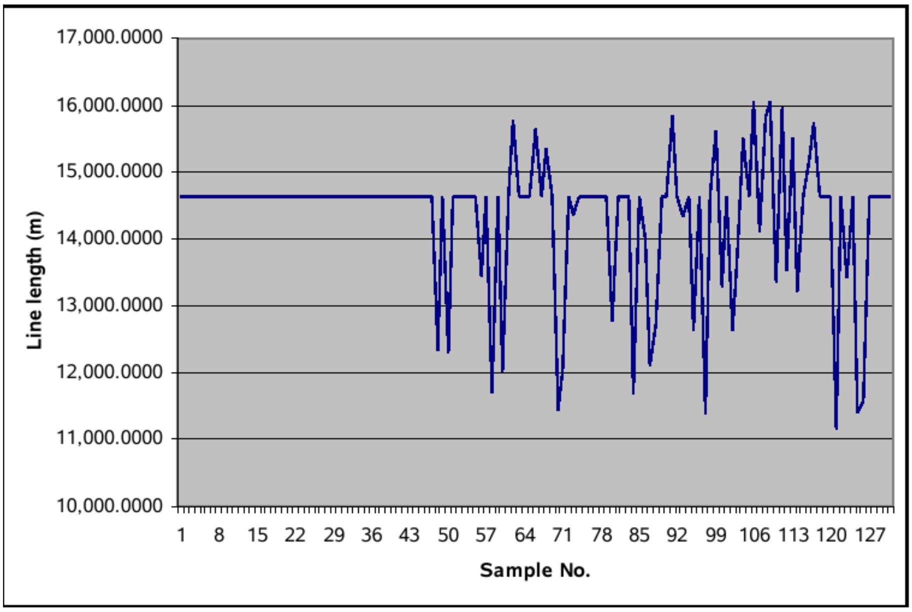

FIG. 5.8: Line length.

The QKDS-B emits a single-laser pulse and opens a large number of detection gates. The scan of the timing of these gates is performed by the internal parameters (waiting duration 1, coarse delay, Fine delay 1 and Fine delay 2) which are stored in the memory. The CryptoMenuBob program indicates whether the length is still approximately the same as that of the last measurement such as it is recommended to repeate the length measurement of the optical link for each different link. Table 5.4 displays the internal parameters (waiting duration, coarsse delay, fine delay 1 and fine delay 2) stored in memory.

5.4.4 Quantum Key Exchange Procedure

Performing a key exchange involves both QKDS stations and both the CryptoMenuAlice and the CryptoMenuBob programs. It is divided in 3 steps below:

1. Preparation of the files:

   The CryptoMenuAlice program alows the user to get the file called alice.dat and containing pseudo-random values. In CryptoMenuBob program produces files called bob.dat and alice.dat which contains pseudo-random values. The alice.dat file is generated by CryptoMenuBob, in order to estimate the error rate and perform simple statistical tests. The graph of Figure 5.10 shows the raw key production. The raw key exchange is shown in Figure 5.11.

2. QKDS-A in emission mode:

   This steps ensures that alice.dat file is downloaded to the QKDS-A station which is waiting to receive light pulses to apply the phase modulation and this, by typing the key 3 and pressing Enter in the CryptoMenuAlice program.

3. QKDS-B initiates key exchange:

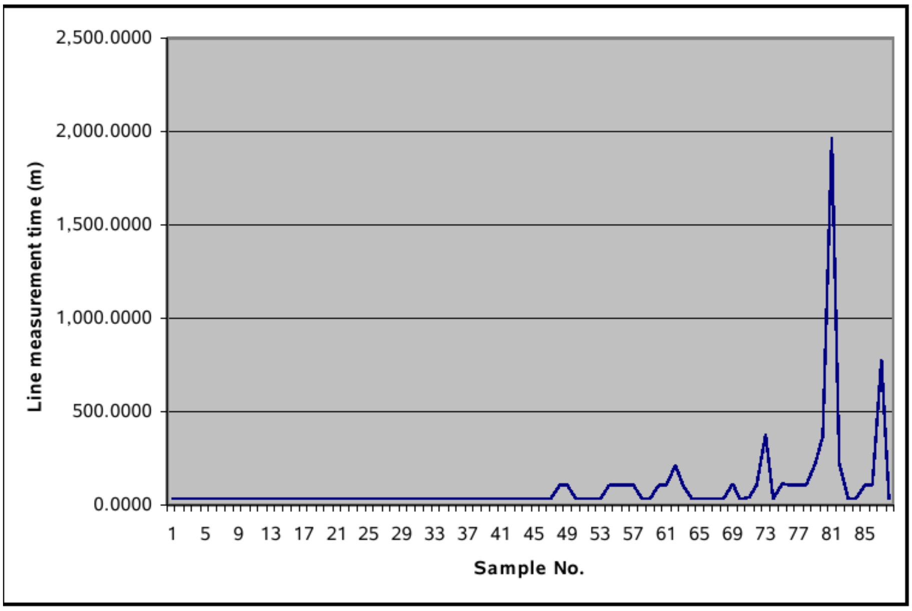

FIG. 5.9: Line measurement time.

The file bob.dat is downloaded to the QKDS-B station and this initiates the key exchange session by emitting and detecting trains of pulses. The detection events are stored in a rawkey dat file. In the computer running CryptoMenubob, three files are stored and are processed to estimate the error rate or other statistical quantities or to distillate a key. These files are alice.dat, bob.dat and rawkey.dat.

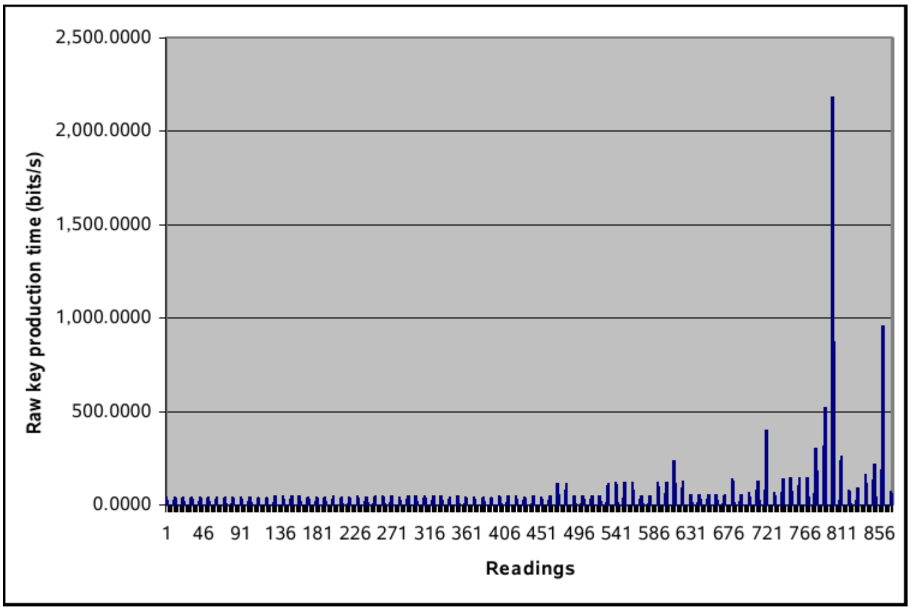

FIG. 5.10: Raw key production.

5.4.5 Sifting

5.4.5.1 Error Rate Acceptable

We explained in the section 4.3.3, phase 2, that Alice and Bob compare portions of their raw keys over the public channel to estimate the error rate R_{error}. They delete the bits tested from their raw keys if $R_{\text{error}} = 0$, so, the remaining bits form their find secret Key. The graphs of error rate acceptable is shown in Figure 5.12 and secret key length is shown in Figure 5.13.

Alice and Bob, also, can apply privacy amplification techniques to minimize Eve's knowledge about their final secret key, and this, if $R_{\text{error}} > 0$ but still sufficiently small [109].

That is why this R_{error} is called error rate acceptable.

Then again, if R_{error} exceds a certain threshold, Alice and Bob discard the whole sequence

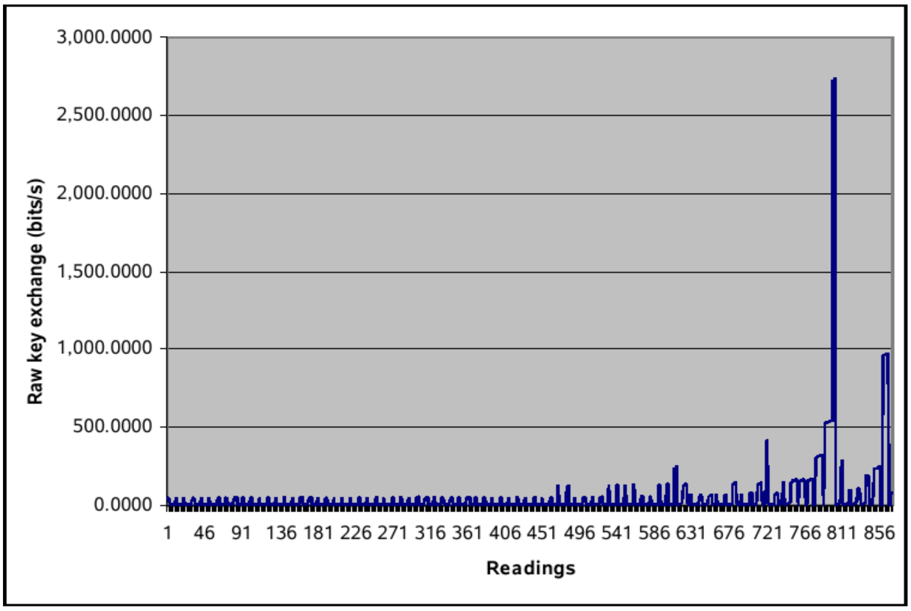

FIG. 5.11: Raw key exchange.

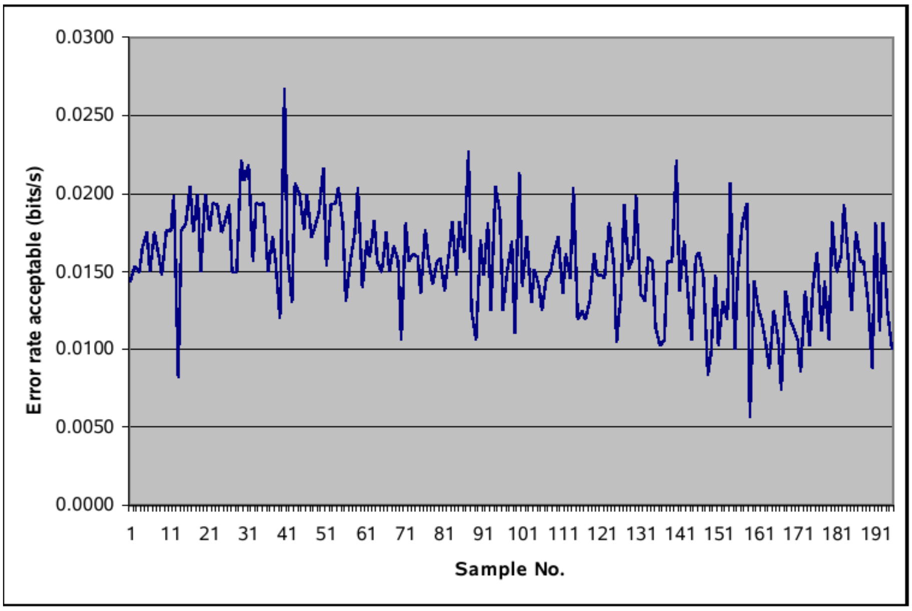

FIG. 5.12: Error acceptable.

and start all over again.

5.4.5.2 Quantum Bit Error Rate

The Quantum Bit Error Rate (QBER) is the number of wrong bits to the total number of received bits (also called key) and contains information on the existence of an eavesdropper. If Eve measures every photon, the QBER is 25% in the case of the BB84 protocol. The CryptoMenuBob program performs sifting and error estimation after rawkey.dat has been created. Figures 5.14 and 5.15 show respectivelly the graphs of sifted bit rate and quantum bit error rate while Table 5.5 shows the output of the sifting/error estimate function.

5.4.5.3 Calculating the Expected QBER Value

The general formula for QBER can be expressed as a function of rates such as

$$QBER = \frac{N_{\text{wrong}}}{N_{\text{right}} + N_{\text{wrong}}} = \frac{R_{\text{error}}}{R_{\text{sift}} + R_{\text{error}}} \approx \frac{R_{\text{error}}}{R_{\text{sift}}} \tag{5.1}$$

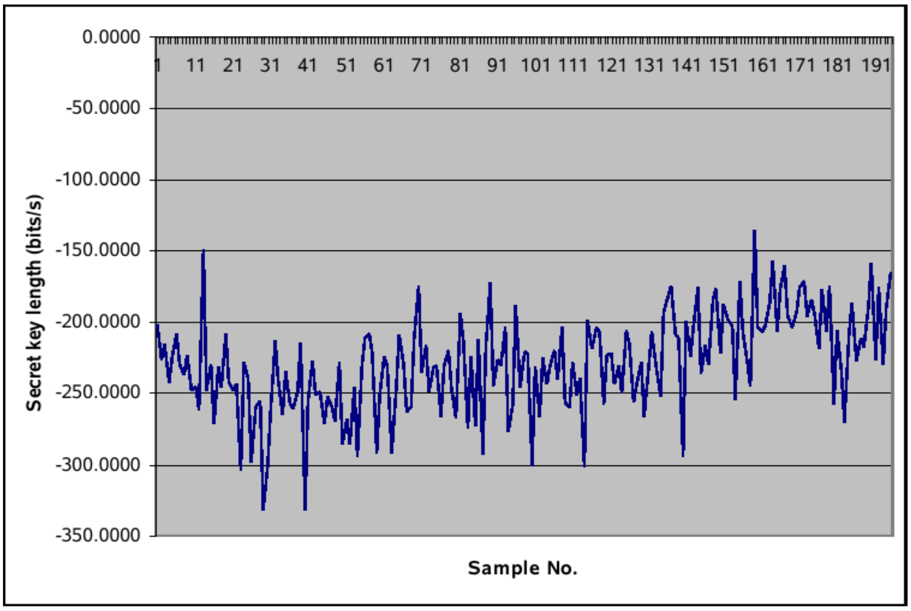

FIG. 5.13: Secret key length.

The sifted key corresponds to the cases in which alice and Bob made compatible choises of bases, hence its rate is half that of the raw key.

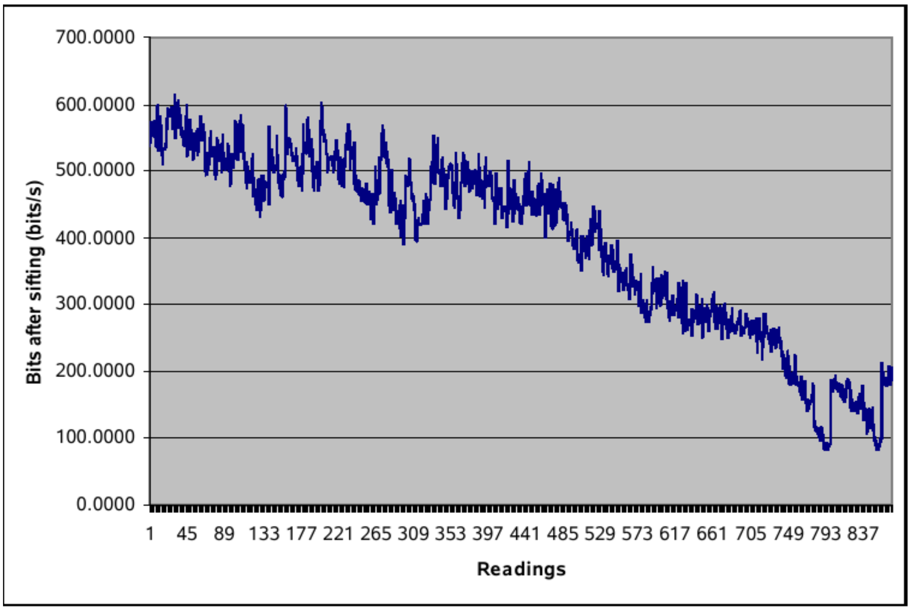

FIG. 5.14: Sifted bit rate.

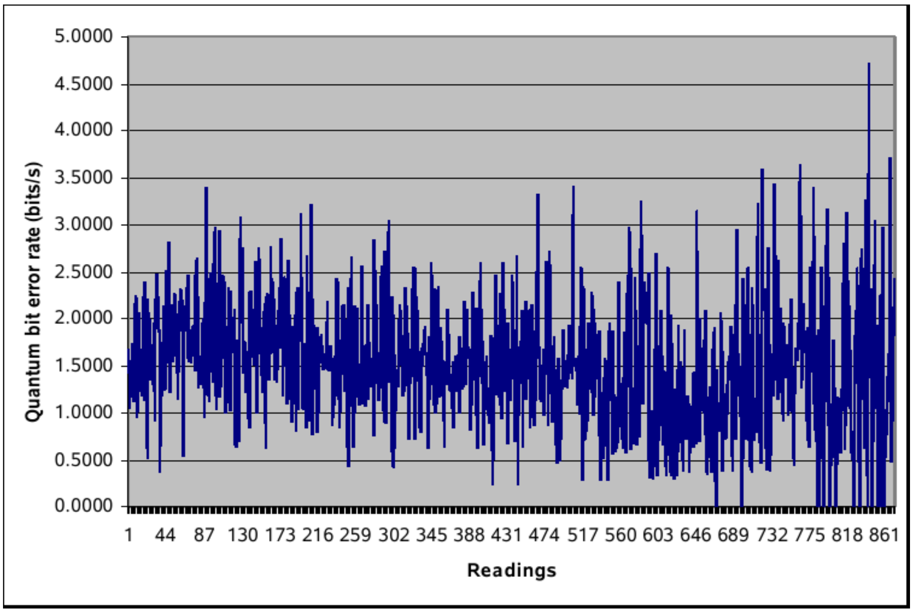

FIG. 5.15: Quantum bit error rate.

$$R_{\text{sift}} = \frac{1}{2}\, R_{\text{raw}}. \tag{5.2}$$

Where the raw rate is the product of the pulse repeat frequency f_{rep}, the attenuation for light pulses (single photons) μ, the probability t_{link} of a photon to arrive at the analyzer and the probability η of the photon being detected:

$$R_{\text{sift}} = \frac{1}{2}\, q\, f_{\text{rep}}\, \mu\, t_{\text{link}}\, \eta\,, \tag{5.3}$$

where q is introduced for phase-coding with $q \leqslant 1$. There are three different contributions to R_{error}:

The first contributin, R_{opt}, arises because of photons ending up in the wrong detector, due to unperfect interference or polarization contrast. It is the product of the sifted key rate R_{sift} and the probability p_{opt} of a photon going in the wrong detector:

$$R_{\text{opt}} = R_{\text{sift}}\, p_{\text{opt}} = \frac{1}{2}\, q\, f_{\text{rep}}\, \mu\, t_{\text{link}}\, p_{\text{opt}}\, \eta\,. \tag{5.4}$$

The second contribution, R_{det}, arises from the detector dark counts which fall in a short time window and give rise to errors when a photon is expected. So,

$$R_{\text{det}} = \frac{1}{2}\frac{1}{2}\, f_{\text{rep}}\, p_{\text{dark}}\, n\,, \tag{5.5}$$

where p_{dark} is the probability of registering a dark count per time-window and per detector, and n is the number of detectors. The two $\frac{1}{2}$ factors are related to the dark count that has either a 50% chance to happen with Alice and Bob having chosen incompatible bases or a 50% chance to arise in the correct detector.

The final contribution, error conuts R_{acc}, can arise from uncorrelated photons, because of inperfect photon sources.

$$R_{\text{acc}} = \frac{1}{2}\frac{1}{2}\, p_{\text{acc}}\, f_{\text{rep}}\, t_{\text{link}}\, n\, \eta\,, \tag{5.6}$$

where the quantity p_{acc} is the probability to find a second pair within the time window, since the first one was created. The factor in this equation appears only in systems based on entangled photons. Therefore, the photons belong to different pairs and different states, arrive in the same time window.

The QBER, in connection with these three contributions can be expressed as follows:

$$QBER = \frac{R_{\text{opt}} + R_{\text{det}} + R_{\text{acc}}}{R_{\text{sift}}}\,, \tag{5.7}$$

$$QBER = p_{\text{opt}} + \frac{p_{\text{dark}}\,.n}{t_{\text{link}}\,.\eta\,.2\,.q\,.\mu} + \frac{p_{\text{acc}}}{2\,.q\,.\mu}\,, \tag{5.8}$$

$$QBER = QBER_{\text{opt}} + QBER_{\text{det}} + QBER_{\text{acc}}\,. \tag{5.9}$$

In this work, only the first and second terms of the equation 5.8 are considered for all calculation of the QBER value, because the third one is only used in the case of the entangled photons. Therefore,

$$QBER = QBER_{\text{opt}} + QBER_{\text{det}}\,, \tag{5.10}$$

$$QBER_{\text{det}} = \frac{p_{\text{dark}}}{(p_{\text{det}} + 2\,p_{\text{dark}})}\,, \tag{5.11}$$

$$QBER_{\text{opt}} = \frac{(1-V)}{2}\,, \tag{5.12}$$

where

p_{dark}: dark count probability averaged on both detectors.

p_{det}: detection probability averaged on both detectors.

V: interfernce contrast.

Read Temperature and Voltage		
TTL power supply $< 5V >$	=	$4.99V$
ECL power supply $< -5V >$	=	$-4.83V$
Fans power supply $< 12V >$	=	$11.96V$
TEC current $< 0 - 3.5A >$	=	$1.64A$
Device Temperature	=	$25.6°C$
Photodiode Temperature	=	$-49.3°C$
Cooler Temperature	=	$19.1°C$
Error Temperature	=	-0.98%
Read Laser power		
Laser power at $2.5ns$ pulse width	:	$-13.1dBn \pm 0.3dBn$
Laser power at $1.2ns$ pulse width	:	$-18dBn \pm 0.3dBn$

TABLE. 5.1: Output of CryptoMenuBob displaying the temperature and voltage.

Parameters used in CryptoMenuBob.exe and Clavis.exe		
Bias Voltage 1 $< 32V >$	=	$31560mV$
Bias Voltage 2 $< 31V >$	=	$31470mV$
Number of laser pulses	=	624
Number of detection pulses	=	624
Number of frames	=	1680
PM Pulse width	=	2
Laser power parameter A	=	3377
Laser power parameter K	=	773
Dead Time	=	$10^3 ns$
Length of Alice delay line	=	$12,5 \times 10^3 km$
Fine delay 1	=	18
Fine delay 2	=	26
Coarse delay	=	74
Waiting period 1	=	5425
Waiting period 2	=	1990
BobPM1	=	48×10^3

TABLE. 5.2: Output of CryptoMenuBob displaying information status about internal parameters of the station.

Noise Measurement		
Measurement dead time	:	10us
Targeted statistical error in	:	5
Number of detector gate	:	42950003
Detector 1		
Number of detection	:	407
Noise probability	:	947613$e-006$
Statistical error	:	4.96%
Detector 2		
Number of detection	:	594
Noise probability	:	1383$e-005$
Statistical error	:	4.1%
Total iteraction	:	43

TABLE. 5.3: Output of CryptoMenuBob after a noise measurement has been performed.

Pass	Status	Detector 1	Maximum	Deteector 2	Maximum
Pass 1	ok		0.8%		1.3%
Pass 2	ok		0.3%		0.4%
Pass 3	ok		0.3%		0.4%

Statistical error 1	= 2.6%
Statistical error 2	= 2.1%
Line length	= 13202.2m
Waiting period 1	= 5140
Coarse delay	= 44
Fine delay 1	= 22
Fine delay 2	= 22

TABLE. 5.4: Output of CryptoMenuBob displaying the result of a line length measurement. In this case, 13 km was used.

```
Total sent bits           : 104496002
Total detector gates      : 79588640
Double detections         : 427 < 0.001% >
Detections on 1           : 181989 < 0.229% >
Detections on 2           : 344650 < 0.4433% >
Compatibles detections    : 263630
Valid detections          : 261025
QBER                      : 0.988%
P Photon total            : 0.662%
P Photon valid            : 0.328%
P double detections       : 0.001%
Detector 1:
                                                   0       −π/2    −π      −3π/2
                                            0      451     24333   44453   21955
                                            π/2    22514   471     23116   44696
Detector 2:
                                                   0       −π/2    −π      −π/2
                                            0      85959   39037   940     45314
                                            π/2    45142   85936   41560   762
Statistics:
                          Total detection probabi-
                          lity being written to file                       = 0.662
```

TABLE. 5.5: Output of CryptoMenuBob displaying the result of the sifting of a key exchange session.

Chapter 6

Conclusion

In today's world of electronic information, humans desire to use secure communication channels with high availability and low latency such as telephone link to reach another human. The security of communication channels can be characterized by some security properties (i.e. confidentiality, integrity, authenticity) and communication properties (i.e. availability, speed rate, latency). For years, many different cryptographic algorithms have dominated an entire field of research in order to get a solution to the key distribution problem.

The classical shannon's cryptosystem can be secure only if the easdropper does not have an access to the secret channel. The only protocol proven to be unconditionally secure is the One Time Pad, where the key is at least long as the message, purely random and used once and only once. Other protocols, including public key procols are at best computationally secure. Based on the property of positive integers, the RSA algorithm consists of factorization of two large prime numbers, but the problem is that its security relies on the fact that factorizing will take years with current algorithm and computational capabilities. The security of public key cryptography rests on various computational problems, which are believed to be intractable. The weakness of this system is based on the fact that the private key is always linked mathematically to the public key. Therefore, it is always possible to attack a public key system if the eavesdropping includes sufficiently large computational resources.

The approach solution to the key distribution problem is developed in quantum mechanics with the property of hiding an information, as expressed in Heisenberg's uncertainty principle, which is one the fundamental laws showing that it is impossible to measure a quantum state without perturbing it. For this case, the measurement of quantum state shows that the system is projected on an eigenstate which means that there is no information given by measurement on the coefficients α and β of the original superposition state $\Psi = \alpha|1\rangle + \beta|2\rangle$, because it is destroyed, so the original cannot be constructed again. But if the system is exclusively in one the eigenstates, quantum state is considered as a carrier of digital information known as a qubit (quantum bit).

Quantum cryptography indeed, has developed this field around itself merging together quantum mechanics and information theory to form quantum information science. It has made enormous progress in quantum optics, as well as in technology of optical fibers and free space optical communication exploiting the Heisenberg's uncertainty principle to designate an unconditionally secure quantum communication schemes.

Quantum based cryptosystems that rely on physical properties of the communication channel may provide a more assuring solution to key distribution security. By eliminating the need for private and public keys, as well as large computations, quantum cryptosystems, possibly based on the same foundations as the early BB84, B92 and EPR protocols may prove to be faster, simpler and more secure than classical systems of present day.

The goal of this work was to experimentally investigate the stability of id 3000 QKDS over installed terrestrial cables between Westille and Howard College campuses. This test was not done because of cables not found for this distance. The successful generation of a secret quantum key distribution was presented over a distance of 13,08 km at Cato Manor in Durban between the Central Application Office and Municipal Original Office buildings for the first test as well as a distance of 15,6 km in Pinetown between the Pinetown Civic Centre and Pinetown Clinic Buildings for the second one.

Experiments have been demonstrated using id-3000 quantum key distribution system such that the secret keys are able to be exchanged over the distances above at rates at least of the order of thousand bits per second. The quantum key distribution experiment was based on interference of weak coherent states in a time multiplexing interferometer. The attenuating light pulses were generated by semi conductor laser with a main aim to prepare the quantum states which have been detected by silicon avalanche photodiodes.

Two types of optical systems were described such as the QKDS-B station, first optical system, used to produce trains of intense pulses, which were sent to the second optical system QKDS-A station and reflected back. The trains of laser pulses, which are produced using a laser, travel through a circulator and are injected into an interferometer and each of them is split into two halves. One of the half pulses travels through the long arm and the other one through the short arm before being launched the optical link.

The second optical system QKDS-A station was used to modulate the phase between the two components of the optical pulses sent by the QKDS-B station. The bit values are encoded on the pulses by using the phase modulation. The incoming pulses are split at input by a 10/90 coupler. The bright contribution is sent to a classical detector via a variable optical attenuator which is placed in front of the detector. Two purposes are served by the classical detector, timing of the incoming signal and security. The detection of the incoming pulses provide the signal which fed into the electronic system, delayed and serves as a time reference for the application of the phase modulation on the half pulse.

The incoming energy is monitored by classical detector to prevent an eavesdropper, from injecting light in the system. The weak part of the incoming pulses is directed into the quantum emitter, which consists of a variable optical attenuator, delay line (long), phase modulator and Faraday mirror. The delay line serves to prevent spurious detections caused by Rayleigh backscattering. A phase modulation pulse is applied on one of two half pulses, and the pulses are reflected by a Faraday mirror.

The returning half pulses in QKDS-B station travel through the opposite arms of the interferometer and are detected using two single-photon detectors (one of which being connected to the circulator). We analyzed on a global perspective the optical system of QKDS-A and QKDS-B stations. Active pointing mechanisms on both the QKDS-A and QKDS-B stations were employed to perform a quantum key distribution with a total quantum bit error ratio (QBER) of $0,988\%$. The results presented in this thesis show that the key distribution problem can be solved since the key itself is produced and able to be exchanged.

Bibliography

[1] C. H. Bennett and G. Brassard. **The dawn of new era for quantum cryptography: The experimental prototype is working!** *Sigact News*, 20(4):78–82, (1989).

[2] id Quantique. **Vectis**. *Available on http://www.idquantique.com.*

[3] Richard J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer. **Quantum Cryptography**. *Available on arXiv.org:quant-ph/9504002*, vol. 1:36 pages, April (1995).

[4] Hoi-Kwong Lo and Yi Zhao. **Quantum Cryptography**. *arXv:quant-ph./0803.2507*, Vol. 2:pp. 1–50, March 17, (2008).

[5] Tobias Schmitt-Manderbach. **Long distance free-space quantum key distribution**. Phd-thesis, LMU München University, München, December 17 (2007).

[6] Dr. Mario Stipcevic. **New Directions in Quantum Cryptography**. *6th CARNet Users Conference (CUC.2004)*, September 27-29, (2004), Zagreb, Croatia.

[7] David Kahn. ***The Codebreakers***. The Macmillan Company, New York, 1967. xvi + 1164 pages.

[8] Andrew Hodges. ***Alan Turing: The Enigma****, Hutchinson, London.* 1983.

[9] Gilles Brassard. **Brief History of Quantum Cryptography: A Personal Perspective**. *arXiv:quant-ph/0604072*, Vol. 1, April 11, (2006).

[10] Nicolas Gisin, Grgoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. **Quantum cryptography**. *Review Modern Physics*, 74:145–195, 2002.

[11] Charles H. Bennett, Gilles Brassard, Claude Crepeau, Richard Jozsa, Asher Peres, and William K. Wootters. **Teleportating an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels**. *Physical Review Letters*, Vol. 70(No. 13), March 29, (1993).

[12] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and Williams K. Wootters. **Purification of noisy entanglement and faithful teleportation via noisy channels**. *Physical Review Letters*, 76(5):722, January 29, (1996).

[13] C. H. Bennett, E. Bernstein, G. Brassard, and U. V. Vazirani. **Strengths and weaknesses of quantum computing**. *SIAM Journal on Computing*, 26(5):1510–1523, (1997).

[14] Charles H. Bennett, Gilles Brassard, and J.-M. Robert. **Privacy amplification by public discussion**. *SIAM Journal on Computing*, Vol. 17(No. 2), April (1988).

[15] G. Brassard. **Brief history of quantum cryptography: A personal perspective**, awaji island, japan. *Proceedings of IEEE Information Theory Workshop on Theory and Practice in Information Theoretic Security*, pages 19–23, October (2005).

[16] *http://www.iro.umontreal.ca/ crepeau/Biblio-QC.html.*

[17] C.H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner. **Quantum Cryptography, or Unforgeable Subway Tokens** advances in cryptography: Proceedings of crypto 82 plenum (new york). *CRYPTO*, pages 267–275, August (1983), http://dblp.uni-trier.de/db/conf/crypto/crypto82.html.WiesnerBBB82.

[18] Guihua Zeng. **A Simple Attacks Strategy of BB84 Protocol**. *Scientific Commons*, Vol. 1:pp. 01–09, December 22, (1998).

[19] *http://arxiv.org/pdf/quant-ph/9812064.pdf.*

[20] S. Wiesner. **Conjugate Coding**. *Manuscript Written Circa 1970, Unpublished until it appeared in Sigact News*, 15(1):78–88, (1983).

[21] Ergün GÜMÜS, G. Zeynep AYDIN, and M. Ali AYDIN. **Quantum Cryptography and Comparison of Quantum Key Distribution Protocols**. *Journa of Electronical and Electronics Engineering*, Vol. 8(No. 1):pp. 504–508, March 25, (2008).

[22] C. H. Bennett and al. **Experimental Quantum Cryptography**. *Journal of Cryptology*, Vol. 5(No. 1):pp. 3–28, (1992).

[23] C. H. Bennett and G. Brassard. **Quantum Cryptography: Public Key Distribution and Coin Tossing**, bangalore, india, new york. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, December (1984).

[24] Martin Hendrych. ***Experimental Quantum Cryotography***. Doctoral thesis, Department of Optics, Faculty of National Sciences, Palacky University, Olomouc, Czech Republic, September (2002).

[25] *Online http://optics.upol.cz/hendrich/thesis/.*

[26] Dominic Mayers. **Unconditional Security in Quantum Cryptography**. *Journal of the ACM (JACM)*, Vol. 48(No. 3):pp. 351–406, May (2001).

[27] Eli Biham and al. **A Proof of the Security of Quantum Key Distribution**. *arXiv:quant-ph/9912053*, Vol. 1:pp. 12–31, December 11, (1999).

[28] R. J. Hughes and al. **Quantum Cryptography**. *Contemporary Physics*, 36(149), (1995).

[29] C. H. Bennett and al. **Quantum Cryptography**. *Scientific American*, 257(10):50, (1992).

[30] C. H. Bennett, G. Brassard, and S. Breidbart. **Quantum Cryptography II: How to re-use a One-Time Pad safely even if P = NP**. *Unpublished manuscript available from the authors*, November (1982).

[31] C. H. Bennett and G. Brassard. **An update on Quantum Cryptography**, advances in cryptology:. *Proceedings of Crypto '84*, pages 475–480, August (1984), Springer-Verlag.

[32] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélène Skubiszewska. **Practical Quantum Oblivious Transfer**. In *CRYPTO '91: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, pages 351–366, London, UK, 1992. Springer-Verlag.

[33] C. Crepeau. ***Correct and private reductions among oblivious transfers***. Phd thesis, Massachusetts Institute of Technology, Department of Electrical Engineering and Computer Science, February (1990).

[34] C. Crepeau and J. Kilian. **Achieving oblivious transfer using weakened security assumptions**, white plains, new york. *Proceedings of 29th IEEE Symposium on the foundations of Computer Science*, pages 42–52, October (1988).

[35] A. K. Ekert. **Quantum Cryptography based on Bell's Theorem**. *Physical Review Letters*, 67(6):661–663, August 5, (1991).

[36] C. H. Bennett, G. Brassard, and N. D. Mermin. **Quantum cryptography without Bell's theorem**. *Physical Review Letters*, 68(5):557–559, (1992).

[37] Gilles Brassard and Claude Crépeau. **Quantum Bit Commitment and Coin Tossing Protocols**. In *CRYPTO '90: Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology*, pages 49–61, London, UK, 1991. Springer-Verlag.

[38] William A. Maniatty. **Lecture notes on an Introduction to Cryptography and Secret Sharing**. *Available on http://www.cs.albany.edu/.*

[39] Ralph C. Merkle. **Secure Communications Over Insecure Channels**. *Communications of the ACM*, Vol. 21(No. 4):pp 294–299, April (1978).

[40] Mihir Bellare and Philip Rogaway. **Introduction to Modern Cryptography**. *CA 92093, USA, (Online) http://www-cse.ucsd.edu/users/mihir or CA 95616, USA, (Online) http://www.cs.ucdavis.edu/ rogaway*, pages pp. 01–10, September 21, (2005).

[41] Whitfield Diffie and Martin E. Hellman. **New Directions in Cryptography**. *IEEE Transactions on Information Theory*, IT-22(6):644–654, November (1976).

[42] Gilles Brassard and Louis Salvail. **Secret-key reconciliation by public discussion**. In *EUROCRYPT '93: Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, pages 410–423, Secaucus, NJ, USA, 1994. Springer-Verlag New York, Inc.

[43] Avi Kak. **Lecture Notes on Introduction to Computer Security**. January.

[44] Sylvain Pasini. **Secure Communications over Insecure Channels Using an Authenticated Channel**. Master thesis, School of Computer and Communication Sciences, Ecole Polytechnique Federale de Lausanne, September 6, (2005).

[45] G.S. Vernam. **Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications**. *Journal of the American Institute of Electrical Engineering (J. AIEE)*, 45:109–115, (1926).

[46] Biham, Eli, and Adi Shamir. **Differential Crystanalysis of the Data Encryption Standard**. *Springer-Verlag*, (1993).

[47] Mitsuru Matsui. **Linear crystanalysis method for DES cipher**. *Lecture Notes in Computer Science*, 765:386–397, (1994).

[48] Matthias Scholz. **Quantum Key Distribution via BB84 An Advanced Lab Experiment**. *Viewdoc.*, pages 1–13, December 6, (2006), Available on http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.111.8517.

[49] A. Menezes, P. Van Oorschot, and S. Vanstone. **Handbook of Applied Cryptography**. *CRC Press*, (1997).

[50] B. Schneier. **Applied Cryptography**. *Wiley*, (1996).

[51] National Institute of Standards and Technology. **An Introduction to Computer Security: The NIST Handbook**, u.s. department of commerce. *Special Publication.*

[52] James Mechvatal. **Public-key cryptography**; gaithersburg, md: Natinal institute of standards and technology. *Special Publication*, Vol. 800(No. 2), April (1991).

[53] Warren D. Smith. **Cryptography meets voting**. *http://www.math.temple.edu/ wds/homepage/*, 2:64, (2005).

[54] Ueli M. Maurer. **Secret Key Agreement by Public Discussion From Common Information**. *IEEE Transactions on Information Theory*, 39:733–742, (1993).

[55] Peter W. Shor. **Polynomial-Time Algorithms For Prime Factorization And Discrete Logarithms On A Quantum Computer**. *SIAM Journal on Computing*, 26:1484–1509, (1997).

[56] Nick Papanikolaou. **An introduction to quantum cryptography**. *Crossroads*, 11(3):3–3, 2005.

[57] Cetin Kaya Koc. **High-Speed RSA Implementation**, rsa data security, inc., redwood city. *(Online): CA 94065-1031*, Version 2.0:pp. 1–73, November (1994).

[58] *http://world.std.com/ franl/crypto/rsa-guts.html.*

[59] *http://www.sics.se/psm/payments/sld021.htm.*

[60] *http://pajhome.org.uk/crypt/rsa/rsa.html.*

[61] Christian Weedbrook. **Quantum Cryptography Without Basis Switching**. Honours thesis, School of Physics, University of Queensland, October (2004).

[62] R.L. Rivest, A. Shamir, and L.M. Adleman. **A method for Obtening Digital Signatures and Public-Key Cryptosystems**. *Communications of the ACM*, 21(2):120–126, (1978).

[63] *http://www.rsasecurity.com/rsakabs.html.*

[64] M.A. Nielsen and J.L. Chuang. **Quantum Computation and Quantum Information**. *Cambridge University Press*, (2001).

[65] D. Bouwmeester, A. Ekert, and A. Zeilinger (Eds). **The Physics of Quantum Information**. *Springer*, (2000).

[66] Chris Erven. **On Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source**. Master-thesis, Department of Physics and Astronomy, University of Waterloo, May 16 (2007). http://hdl.handle.net/10012/3021.

[67] David J. Griffiths. **Introduction to Quantum Mechanics**. *ISBN 0-13-124405-1*, (1995).

[68] Michael A. Nielsen and Isaac L. Chuang. **Quantum Computation and Quantum Information**. *Cambridge University Press*, pages 1–29, (2000), http://ISBN: 0-521-62503-9.

[69] Stephen Jenkins. **Some Basic Ideas about Quantum Mechanics**. *Available on http://newton.ex.ac.uk/research/qsystems/people/jenkins/mbody/mbody2.html*, November 4, (1996).

[70] D. Dieks. **Communication By EPR Devices**. *Physics Letters*, 92A(6):271–272, November 22, (1982).

[71] Jr. Samuel J. Lomonaco. **A Rosetta stone for Quantum Mechanics with an Introduction to Quantum Computation**. *Lecture notes, Copyright*, (1999), pp 5 - 12.

[72] W.K. Wootters and W.H. Zurek. **A single quantum cannot be cloned**. *Nature*, 299:982–983, October 28, (1982).

[73] id Quantique SA. **Understanding Quantum Cryptography**. *id Quantique White Paper Version 1.0*, page 8, April (2005), Available on http://www.idquantique.com.

[74] J.J. Sakurai. **Modern Quantum Mechanics**. *(Revised edition), addison-Wesley Publishing Company*, Reading, Massachusetts (1994).

[75] Michael Marhoefer, Ilse Wimberger, and Andreas Poppe. **Applicability of Quantum Cryptography for Securing Mobile Communication Network**. *Online: http://www.dzi.tu-darmstadt.de/fileadmin/content/veranstaltungen/20060606-09 etrics/MarhoeferWimbergerPoope.*, (2006).

[76] N. Gisin and B. Huttner. **Quantum Cloning, Eavesdropping and Bell's inequality**, group of applied physics, university of geneva 4, switzerland. *arXiv:quant-ph/9611041*, Vol. 1(No. 25):pp. 2 – 5, November 20, (1996).

[77] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. **Quantum Cryptography**. *Rev. Mod. Phys.*, 74:145–195, (2002).

[78] Xiongfeng Ma. **Quantum Cryptography: From Theory to Practice**. *arXiv: quant-ph/0808.1385*, Vol. 1:pp. 1–157, August 10, (2008).

[79] C.H. Bennett. **Quantum Cryptography Using Any Two Nonorthogonal States**. *Physical Review Letters*, 68(21):3121–3124, May 25, (1992).

[80] D. Bruss. **Optimal Eavesdropping in Quantum Cryptography with Six States**. *Physical Review Letters*, Vol. 81(No. 14):pp. 3018–3021, October 5, (1998).

[81] M. Christandl, R. Renner, and A. Ekert. **A Generic Security Proof for Quantum key exchange**. *http://arxiv.org/abs/quant-ph/0402131*, February (2004), http://citeseer.ist.psu.edu/christandl04generic.html.

[82] Poels Karin JPM. **Quantum Key Exchange using Squeezed States**. Master thesis, Eindhoven University of Technology, (2004).

[83] J. Samuel Lomonaco. **A quick glance at quantum cryptography**. *cryptologia*, 23(1):1–41, January (1999).

[84] Chip Elliott, David Pearson, and Gregory Troxel. **Quantum cryptography in practice**. In *SIGCOMM '03: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 227–238, New York, NY, USA, 2003. ACM.

[85] Jr Samuel J. Lomonaco. **A Talk on Quantum Cryptography or How Alice Outwits Eve**. *Lecture notes, copyright*, (2000), pp 11 - 22.

[86] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. **Experimental Quantum Cryptography**. *Journal of Cryptology*, 5(1):3–28, (1992).

[87] Hoi-Kwong LO and Yi Zhao. **Quantum Cryptography**. *Available on http://www.citebase.org/abstract?id=oai:arXiv.org:0803.2507*, (2008).

[88] R. König, U. Maurer, and R. Renner. **On the power of quantum memory**. *IEEE Transactions*, 51(7):2391 – 2401, July (2005), available on www.arxiv.org, quant-ph/0305154, 2003 or http://citeseer.ist.psu.edu/onig03power.html.

[89] C.H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. **Generalized Privacy Amplification**. *Information Theory, IEEE Transactions on*, 41(6):1915–1923, November (1995).

[90] C. H. Bennett, G. Brassard, and J. M. Robert. **Privacy amplification by public discussion**. *SIAM Journal on Computing*, 17(2):210–229, April (1988), http://dx.doi.org/10.1137/0217014.

[91] Henning Weier. **Experimental Quantum Cryptography**: Diploma thesis. *ScientificCommons - Max Planck Society eDocument Server; http://xqp.physik.uni-muenchen.de*, (2003).

[92] Renato Renner. **Security of Quantum Key Distribution**. Phd-thesis, Swiss Federal Institute of Technology Zurch, January 11 (2006). http://arXiv:quant-ph/0512258v2.

[93] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin. **Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations**. *Phys. Rev. Lett.*, 92(5):057901, Feb (2004).

[94] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antonio Acín. **Quantum cloning**. *Reviews of Modern Physics*, 77(4):1225–1256, November (2005).

[95] Norbert Lütkenhaus. **Security against eavesdropping in quantum cryptography**. *Physical Review A*, Vol. 54(No. 1):pp. 97 – 111, July (1996).

[96] Mark Williamson and Vlatko Vedral. **Eavesdropping on practical quantum cryptography**. *Journal of Modern Optics; (Online): http://www.tandf.co.uk/journals*, Vol. 50(No. 13):1989–2011, (2003).

[97] C.A. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu, and A. Peres. **Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy**. *Phys. Rev. A*, (56):1163, (1997).

[98] J. C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes. **Unconditional Security of Three State Quantum Key Distribution Protocols**. *Physical Review Letters*, 94:040–503, (2005).

[99] D. G. Enzer, P. G. Hadley, R. J. Hughes, C. G. Peterson, and P. G. Kwiat. **Entangled-photon six-state quantum cryptography**. *New Journal of Physics*, 4:45–+, July (2002).

[100] Liu Xiao-Bao, Liao Chang-Jun, Tang Zhi-Lie, Wang Jin-Dong, and Liu Song-Hao. **Quantum Key Distribution System with Six Polarization States Encoded by Phase Modulation**. *Chinese Physics Letters*, 25:3856–3859, (2008).

[101] Chales H. Bennett. **Quantum Cryptography: Uncertainty in the service of privacy**. *Science*, 257:752–753, 1992.

[102] *http://library.tue.nl/catalog/linkToVubis.csp/DataBib=6:583252.*

[103] id Quantique. **Clavis**. *Available on http://www.idquantique.com.*

[104] id Quantique SA. **Quantum Key Distribution System id 3000 User Guide**. *id Quantique, Version 2.35*, June (2005).

[105] Daniel Kalthoff. **Review on Quantum Cryptography**. *Seminar on Quantumoptics SS 2004*, August (2004).

[106] H. Takesue and al. **Quantum Key Distribution over a 40-dB channel loss using superconducting single-photon detectors**. *Nature Photonics 1, Online: doi:10.1038/nphoton.2007.75*, pages pp. 343–348, June 1, (2007).

[107] P. Villoresi and al. **Space-to-ground quantum-communication using an optical ground station: a feasibility study**. *arxiv: quant-ph/0408067*, Vol. 1:pp. 1–8, August 10, (2004).

[108] Science News. **Quantum Channel Between Earth And Space? Firing Photons Makes Advance In Space Communication**. *ScienceDailly*, March 29, (2008).

[109] M. Nagy and S.G. Akl. **Quantum Key Distribution Revised**. Technical report no. 2006-516, School of Computing, Queen's University, Kingston, Ontario, (June) 2006. 21 pages.