Institutionen för systemteknik
Department of Electrical Engineering

Examensarbete

Quantum Key Distribution - current state of the technology and prospects in the near future.

Examensarbete utfört i Datateknik
vid Tekniska högskolan i Linköping
av

Karl Vestgöte

LiTH-ISY-EX-ET--09/0358--SE

Linköping 2009

Linköpings universitet
TEKNISKA HÖGSKOLAN

Department of Electrical Engineering
Linköpings universitet
SE-581 83 Linköping, Sweden

Linköpings tekniska högskola
Linköpings universitet
581 83 Linköping

Quantum Key Distribution - current state of the technology and prospects in the near future.

Examensarbete utfört i Datateknik
vid Tekniska högskolan i Linköping
av

Karl Vestgöte

LiTH-ISY-EX-ET--09/0358--SE

Handledare: **Jan-Åke Larsson**
ISY, Linköpings universitet

Examinator: **Viiveke Fåk**
ISY, Linköpings universitet

Linköping, 30 March, 2009

Avdelning, Institution
Division, Department

Division of Information Coding
Department of Electrical Engineering
Linköpings universitet
SE-581 83 Linköping, Sweden

Datum
Date

2009-03-30

Språk
Language

☐ Svenska/Swedish
☒ Engelska/English
☐ ________________

Rapporttyp
Report category

☐ Licentiatavhandling
☒ Examensarbete
☐ C-uppsats
☐ D-uppsats
☐ Övrig rapport
☐ ________________

ISBN
—

ISRN
LiTH-ISY-EX-ET--09/0358--SE

Serietitel och serienummer
Title of series, numbering

ISSN
—

URL för elektronisk version

`http://www.icg.isy.liu.se`
`http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-17579`

Titel
Title Quantum Key Distribution - current state of the technology and prospects in the near future.

Författare
Author Karl Vestgöte

Sammanfattning
Abstract

The thesis presents the basics of Quantum Key Distribution, a survey of the present techniques, a look at the possible future, and finally a comparison to the alternative technique of using public key or manual distribution of keys.

Techniques to integrate QKD with the existing telecom fiber infrastructure have been studied, and so has the EU-funded project SECOQC.

Last the security and efficiency of QKD have been examined, with focus on what level of security that is required, existing security solutions have been used as a comparison.

Nyckelord
Keywords Quantum Key Distribution, Quantum Network, Quantum Cryptography

Abstract

The thesis presents the basics of Quantum Key Distribution, a survey of the present techniques, a look at the possible future, and finally a comparison to the alternative technique of using public key or manual distribution of keys.

Techniques to integrate QKD with the existing telecom fiber infrastructure have been studied, and so has the EU-funded project SECOQC.

Last the security and efficiency of QKD have been examined, with focus on what level of security that is required, existing security solutions have been used as a comparison.

Acknowledgments

I would like to thank my supervisor Jan-Åke Larsson for his patience and guidence in this area which was completely new to me. I would also like to thank Robert Forchhiemer for giving me the opportunity to do this thesis, Viiveke Fåk for being my examiner and also for introducing me to the fascinating world of computer security, Gregg Yeager for the inspiring chat we had over a lunch at Växjö University and last but not least Åsa Lundberg for proofreading this thesis.

Contents

Chapter 1

Introduction

1.1 Background

Quantum Key Distribution is a technology to distribute, or rather generate, secure random keys between two communicating parties using optical fiber or freespace as a channel. The idea was first proposed by Stephen Wiesner in an unpublished manuscript around 1970[1] and later in 1984 by Bennett and Brassard who presented the first protocol based on Wiesners ideas. Much research have been done and the area is constantly progressing, both in the theoretical part and in the laboratories. We are now at a very interesting stage where large scale QKD networks are researched outside the laboratory and there are even a few QKD products available on the market.

1.2 Purpose

The aim for this thesis is to investigate the possibilities with quantum key distribution, also called quantum cryptography or quantum key generation, in an optical overlay network, what is possible today and in the near future, and compare it with other solutions for encryption. The method of choice is to study the area and read as much as possible and then draw conclusions based on gained knowledge.

The focus in this thesis is on the technology and the usefulness of QKD and not on the theoretical background of quantum key distribution, the theoretical background has been thoroughly studied before. I will try to draw conclusions on what needs to be improved to take QKD one step further and what is currently limiting the usefulness and performance of QKD.

There are a few specific questions that I will try to answer, one of the most important is if it is possible to use the existing telecom network for quantum key distribution. Another is if it is cost effective to use QKD today or in the near future. If the answer is no, which parts need to improve to make it cost effective?

1.3 Outline

Chapter 2 will give the reader a brief introduction to classical cryptography mainly public-key cryptography but also some information about symmetrical ciphers, the AES algorithm will be briefly presented. This background is essential to the later discussion of the performance and attributes of quantum key distribution.

The 3rd chapter will introduce the concept of quantum key distribution. The basics for QKD will be explained and a few examples will be given to further clarify the idea. We will also see what happens when someone tries to eavesdrop on the key agreement process and show how this can be detected.

Chapter 4 will deal with the technical aspects and difficulties with QKD, a number of different solutions for photons sources, detectors and physical medium will be presented. A number of different techniques to code the information in the photons and several protocols for QKD will be explained.

Chapter 5 will describe how to incorporate QKD in existing telecom networks with wavelength division multiplexing. A large part of the chapter is used to discuss different designs for multi-user QKD networks.

Quantum repeaters based on entanglement swapping are presented in chapter 6. This is a technique that isn't possible today but might contribute greatly to the usefulness of QKD in the future.

In chapter 7 I write about a project called SECOQC which is a secret distribution network in Vienna. Based on QKD links and trusted nodes this project is the first out of the laboratory large scale QKD experiment with multi-users and devices from many different manufacturers.

The last chapter, number 8, contains the discussion part of this thesis and my conclusions.

Chapter 2

Classical Cryptography

In this section a brief description of the security of the technology used today to exchange cryptographic keys over public channels will follow. This is important so we can understand what competition quantum key distribution are up against. I will also comment on the security of AES which is a symmetrical cipher often used when the secret key have been distributed by public key exchange. AES is also often combined with QKD systems, due to the low key generation rate of QKD it is not possible to use one-time-pad to encrypt the secret data so instead AES is used with frequent key exchange. In these cases, when the whole system is considered, the theoretical security of QKD is degraded to that of AES.

2.1 Public-key exchange

Public-key cryptography or asymmetric cryptography is a form of cryptography which uses one key for encryption and another for decryption. It is not possible to derive one key from the other and this makes it possible to encrypt and send secrets to a person which we never meet.

In a simple example Alice has her public key, the one used to encrypt, available on her web page. The key she uses to decrypt messages is kept secret. If Bob wants to send Alice a secret he visits Alice's homepage and collects her public key. After that he uses the key to encrypt his secret message and sends it over the public communication channel to Alice. When Alice gets the cryptogram from Bob she uses her private key to decrypt the message.

This is basically how it works but in reality someone needs to guarantee that Alice's public key is really Alice's and not Eve's public key. Otherwise Eve can mount a man-in-the-middle attack. This means that Eve positions herself between Alice and Bob and intercepts all messages between the two, she then alters the messages to suit her needs and forwards them. The communication between Alice and Bob is now controlled by Eve, Alice believes she is communicating directly with Bob and Bob believes he is communicating directly with Alice.

The public-key algorithms are rather slow, so often they are used to exchange a secret key to a symmetrical cipher like the AES algorithm. After the key exchange the encryption and decryption is performed by using the transferred key and a symmetrical cipher.

2.1.1 Security of Public-key algorithms

Public-key algorithms like RSA have been around for 30 years or so and no devastating weakness in the algorithm has yet been found. Although it is not proven to be secure, it is considered classically hard to solve the underlying mathematical problem.

The key length used for RSA is much longer than the key length for a symmetrical cipher. This is due to the fact that the RSA algorithm works with very large primes, so the key size must be very large. Otherwise the key-space doesn't contain enough primes and the key would be easy to guess. The RSA Laboratories currently recommends a 1024 bit key length for corporate use and 2048 bit for extremely sensitive information[2].

If the public key can be factorized, it is possible to calculate the secret private key. In 2004 RSA-200, a 663 bit, number was factorized, which took the equivalence of 75 years using one 2,2 GHz Opteron computer[3]. Even if today's computers are much faster, it would take more than 10 years to factor this with one desktop computer. Considering that RSA is recommending at least 1024 bit keys or more, the risk for the key to be broken is small as long as the adversary does not have access to supercomputers, and then it would still be difficult if not impossible to do it in reasonable time. For example if RSA is used for a money transaction and a new RSA key pair is used for every new transaction, it would be enough if it would take more than 10 minutes to break the secret key. When the information reaches the bank, it is to late too change the information and the attacker has missed the opportunity.

There is one more thing to consider: if we use RSA to agree on a symmetrical cipher key, the level of security is determined by the length of the RSA key, not the length of the symmetrical key. If the RSA key is 2048 bits long, it is no use to exchange a 256 bit AES key, because breaking the much less secure RSA key will compromise the AES key. An RSA key that equals the 128 bit AES in security would need to be 3200 bit long, and to match the AES-256 we need a RSA key that is over 13000 bit long[4].

An interesting problem with public key exchange algorithms like RSA and Diffie-Hellman is that although it is hard to solve the underlying problem with classical mathematics, this is not the case with quantum computers where efficient algorithms are available[5]. If we had access to quantum computers, we would be able to break RSA keys in a blink of an eye with existing algorithms. However, according to many experts in the area it is highly unlikely that quantum computers will be available for many years if not decades.

2.2 Symmetrical Cipher

Symmetrical ciphers are using the same key to encrypt and decrypt the information, they are often very fast, and with long key length some of them are very secure. One of the most used algorithms is AES, Advanced Encryption Standard, which can be used with at most 256 bit key length.

2.2.1 Security of AES

Much research for weaknesses has been done in the decade since AES was first introduced, then named Rijndael. So far no attack better than the brute-force attack, try all possible keys until you find the right one, have been found. If we try to attack the weakest AES with a 128 bit key length by a brute-force attack the time needed to find the key is mind-boggling, a device that can try a billion keys per second need 10^{21} years to try all keys[6].

The interesting part here is how often we need to change the key if we are using AES with a 128 or 256 bit key. It is sometimes argued by the QKD researchers that high-end AES equipment today does not change the key frequently enough, only once a minute or in the worst case once every day. Is this insecure? There exists known cryptographic problems with block ciphers, as the AES, such as known plain-text attacks based on the birthday paradox, when the number of blocks encrypted with the same key reaches $2^{key-length/2}$. Recently dedicated research hardware for AES-128 was able to encrypt at a rate of 21.54 Gbit/s and in this case birthday paradox collisions becomes very likely after 2^{64} blocks have been encrypted with the same key. This occurs after 2^{37} seconds which is roughly 4000 years, which means that in practice this is not a problem[7]. So the answer is no, since no attack faster than the brute-force attack exists for the AES, it is secure as long as the key is handled in a safe manner. If the key is compromised, the adversary will get more information if the key is changed seldom.

Chapter 3

Introduction to Quantum Key Distribution

3.1 History

Stephen Wiesner first introduced the idea of quantum cryptography in the early 1970s and in 1984 the first protocol for quantum key distribution, called BB84, was presented by Charles H. Bennett and Gilles Brassard. In 1991 Artur Ekert presented another QKD protocol based on entangled states. The first demonstration of QKD was performed in 1991 by a group consisting of Charles H. Bennett, Francois Bessette, Gilles Brassard, Louis Salvail and John Smolin over a distance of 32 cm free-space[8].

Since this first experiment there have been numerous new protocols and experiments, the range for QKD has increased to more than 100 km in optical fiber and the record distance for free-space QKD is more than 140 km.

3.2 The Basic Idea

In this section a description of the fundamentals behind QKD will be provided. The foundation lies in quantum physics so we have to start there. Quantum physics establishes a set of rules stating that certain things cannot be done:

1. One cannot perform a measurement without perturbing the system.

2. One cannot simultaneously measure the polarization of a photon in the vertical-horizontal basis and the diagonal basis.

3. One cannot duplicate an unknown quantum state.

If information is coded in a quantum system, like an individual photon, these rules apply. Alice codes her information in photons and sends them to Bob. If he receives the photons unperturbed, no measurement was carried out on them according to rule number one. No measurements means that Eve did not eavesdrop, and therefore has no information. So after exchanging photons Alice and Bob can check if someone was listening, measuring. This is done by comparing a subset of the photons over a public channel. Now Alice and Bob knows if someone was eavesdropping, but this doesn't prevent the eavesdropper from gaining information. So all Alice and Bob achieved is that they know that their secret isn't secret anymore. But if Alice and Bob exchange a secret key instead of secrets, they can use the key to encrypt the secret information and send it over a public channel, because they will know if the key is secure.

Let us make this a little more precise; the individual quanta used by Alice and Bob, often called qubits for quantum bits, are encoded in individual photons. Number 2 in our list of rules gives that if we encode the information, 0 or 1, in one of two non-orthogonal bases in the photon, the vertical-horizontal and the diagonal, an eavesdropper that wants to know which information a photon is carrying must choose one of the basis in which to measure. If she chooses correctly she will get the information, and the system, the photon, will be unperturbed. If she chooses wrong she will get a random value, either 0 or 1, and the photon will be polarized in the basis she measured in, and the information it carried will be lost.

When Bob receives a photon he doesn't know in which of the two bases Alice encoded it. So he has to randomly choose a basis to measure in. He will get the basis right half the time, so out of 200 photons he has on the average 100 photons measured in the right basis. Then Alice announces over an authenticated public channel which basis she encoded the different photons in and Bob announces which basis he measured in. Now both Alice and Bob throw away the photons were Bob measured in the wrong basis.

Table 3.1. BB84

A basis	X	X	+	X	+	X	X	+	+	X	X	+
A qbits	1	1	0	0	0	1	1	0	0	0	1	1
B basis	+	X	+	+	+	X	+	X	+	X	+	+
B qbits	0	1	0	0	0	1	0	1	0	0	1	1
Basis A=B	N	Y	Y	N	Y	Y	N	N	Y	Y	N	Y
Sifted Key		1	0		0	1			0	0		1

3.3 Detecting the Eavesdropper

The next step is to check if someone was listening on the key. If Eve was eavesdropping, measuring, she has to guess the basis like Bob, but Eve has to encode the information she gets in a photon and send it to Bob or she will just execute a denial of service attack. The problem for Eve is that she has no way of telling if she measured in the right basis. When a photon is coming from Alice, Eve randomly picks a basis and measures the photon, she then records the outcome and sends a photon with the same value that she recorded in the same basis as she measured in to Bob. This will introduce detectable noise at Bob's end of the quantum channel because statistically Eve will only get the basis right in half of the attempts.

3.3.1 An Illustrative Example

In the following example all the numbers, except the 200 photons Alice starts with, are average numbers.

200 photons leave Alice, Eve measures them all and polarizes 100 of them in the wrong basis. The photons arrive to Bob and out of the 100 right ones he measures 50 in the right basis. These will be kept after the announcement of the basis and they will all have the right value. Out of the 100 that Eve polarized in the wrong basis 50 will have the wrong value compared to Alice's bits. Bob measures 50 in the basis Alice chose and 50 in the wrong basis. The 50 that are measured in the wrong basis are thrown away. The rest are measured in the same basis as Alice encoded, but since Eve measured in the wrong basis the value Bob gets when he measures is completely random. So 25 of these 50 photons have the right value by coincidence and 25 have the wrong value. So out of the 100 bits that Alice and Bob keep, 25 bits have the wrong value. Now Alice and Bob compares a subset of the bits, and when they notice that around 25 % have the wrong value they know that Eve was listening. If there are no errors, Alice and Bob knows that no one was listening.

Table 3.2. Illustrative Example

A basis	X	+	+	X	X	+	X	X	+	X	+	+
A bits	1	0	0	1	1	0	1	0	0	1	1	0
E basis	X	X	+	X	+	X	+	+	X	X	+	+
E bits	1	1	0	1	0	0	0	0	1	1	1	0
B basis	X	+	X	X	+	X	+	X	+	X	X	X
B bits	1	0	1	1	0	0	0	1	1	1	0	1
Basis A=B	Y	Y	N	Y	N	N	N	Y	Y	Y	N	N
Bits A=B	Y	Y		Y				N	N	Y		
Errors								X	X			

3.3.2 Real World Complications and Solutions

Of course there are more complications. Due to the attenuation in the fiber and other imperfections in the hardware, there will always be a small percentage of errors in the key. There is no way of telling if the errors are due to technical imperfections or an eavesdropper, so Alice and Bob must consider the worst case scenario and attribute all errors to an eavesdropper. In the case when Eve only eavesdrops on a fraction of the photons, the error rate would be lower and Alice and Bob wouldn't notice Eve's presence. When the error rate is below a certain threshold, 14.6 %, the key is proven to be secure[9].

When Alice and Bob have agreed on a sifted key that has lower error rate than the threshold, they use error correction to eliminate the errors in the key so it can be used for encryption and decryption. Often privacy amplification is also used to reduce Eve's knowledge of the key.

3.4 The Importance of Authentication

It is very important that the public channel that Alice and Bob use to communicate is authenticated. If it isn't Eve can mount a man-in-the-middle attack. Even when authentication is performed, one broken round will provide Eve with the authentication key for the next round, and then that one is broken and so on for all future rounds.

Recently a security flaw in the standard authentication scheme was found by Jan-Åke Larsson and Jörgen Cederlöf from Linköping university, which made it possible for an attacker to break the QKD system, without any risk for detection. This is done by tapping the quantum channel in such a way that the disturbance is below the threshold for the error rate. Eve then intercepts the message-tag pairs sent from Alice to Bob over the public channel and uses this information to determine the authentication tag for her forged message. The attack gains Eve a factor 10 000 in the expected time to break the system. Fortunately Jörgen Cederlöf and Jan-Åke Larsson also proposed a solution to fix the problem and restore the security of QKD[10].

3.4.1 The Number of Authentication Keys needed

When the QKD system is first set up, a small pre-distributed key is needed for the authentication process for the first rounds. This is quite important for later discussions, since it requires that Alice and Bob exchange this key in a secure manner.

This authentication key complicates the procedure of starting up or adding a new user to a many-to-many QKD network. Since users must exchange authentication keys with all other users, the number of authentication keys needed grows exponentially with the number of users. When a 10 user network first is started up 45 authentication keys needs to be distributed. This exponential growth of the number of authentication keys with the number of users is a severe problem for large many-to-many QKD networks.

Chapter 4

Quantum Channel

This chapter will describe the different hardware which makes up the quantum channel. Different technologies to solve the problems will be presented briefly to give the reader an idea of the different possibilities and difficulties. We will begin with the photon sources and then the physical medium, the fiber. After that different techniques to encode the information will follow. I will end this chapter outlining the limiting factor for QKD, the photon detectors.

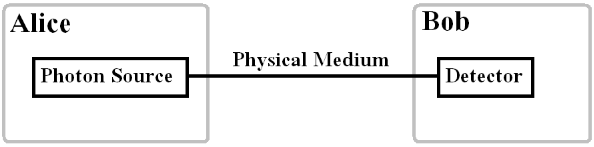

Figure 4.1. Quantum Channel

4.1 Photon sources

In QKD systems only one photon at a time carries information from Alice to Bob. The reason for this is that if there are more than one photon and Eve is eavesdropping, she can easily split off one photon and perform a measurement. This is bad, because Bob or Alice would not notice that Eve is listening. The principle of quantum cryptography is based on that only one photon carries information at a time. Today it is very difficult to build a perfect single photon source. Much effort has been put into the matter, but no practical perfect single photon light source exists.

4.1.1 Attenuated Laser Sources

The most commonly used photon sources in today's QKD systems are attenuated lasers sources. They are essentially the same as the laser sources used in classical optical communication with the addition that heavy attenuation is applied on them so that only one photon is transmitted. The reasons for their popularity are that they are simple, reliable and can reach GHz rates without any effort[1]. The problem with attenuated laser sources is that they have a small probability to emit multi-photon pulses and thereby make it possible for Eve to split off one photon and measure it. If the probability for a pulse to contain only one photon is 0.09 then the probability for an empty pulse is 0.905 and for a pulse with multi-photons is 0.005. Another problem that has more impact on the performance of QKD systems is that the detectors must be active for all pulses, even the empty ones, and the dead-time of the detector after a detection is rather long, so this restrains how frequently the laser can fire[11].

4.1.2 Parametric Down-conversion Sources

Spontaneous parametric down-conversion which generates photon-pairs is another way to generate quasi-single-photon states. The crucial point is the tight time correlation between photons in the pair. If we place a detector in the way of one of the photons in the pair and let the other pass through a quantum channel to Bob, we can predict when a photon is traveling to Bob by detecting its twin. But due to losses and dark counts there may not be a photon in the signal beam to Bob. The risk for this is 30 % which is considered fairly low.

4.1.3 Colour centers

Impurities and vacancies form defects in crystal lattices and result in colour centers. Crystals with colour centers can be easily prepared to be used in photon sources. They are stable and work at room temperature, which are their key advantages. The biggest problem with colour centers is that it is difficult to find crystals with the right defects. Recently a new colour center consisting of a nickel ion surrounded by four nitrogen atoms in a genuine diamond was found. When excited by a focused laser beam, the colour center emits photons at 802 nm which makes it suitable for free-space QKD. Colour centers suitable for telecom wavelengths have so far not been observed.

4.1.4 Quantum Dots

Quantum dots are nanocrystals made by semiconductor nanostructures. These quantum dots emit photons when excited by a laser or an electric current. The photon emissions come from recombination of an electron-hole pair. The wavelength of the emitted photon is determined by the size of the band-gap which is dependent on the size of the quantum dot. Therefore the colour of the emitted photon is tunable with extreme precision by changing the size of the quantum dot. Common materials used in quantum dots are gallium arsenide, gallium aluminum arsenide or indium phosphide. Sources operating at telecom wavelengths are possible. The biggest drawback with quantum-dot photon sources is the need for cooling to liquid-helium temperature, just a few K. More recent research promises working temperatures of 100 K but the photon-number distribution of such high temperature sources are not so good. Another big drawback is very low collection efficiency, which means that the probability of an empty pulse is high. By placing the quantum dot in an integrated solid-state micro-cavity the efficiency can be increased up to 10 %.

There have been a demonstration of QKD using a quantum-dot single-photon source operating in free space over a symbolic distance of one meter[11].

4.1.5 Single atoms and molecules

The radiative transitions between electronic levels of a single molecule, ion or atom can be used to generate single-photon sources. Single ions placed in an optical cavity where they interact with the vacuum field and an excitation laser beam could represent single-photon sources with narrow spectrum and low probability for empty pulses. But the technological complexity, for example high vacuum is required, lowers the practical feasibility for these photon sources.

It is simpler to use single organic-dye molecules because they are usually trapped in a polymer matrix or put in a solvent. A great advantage is that these sources can be operated at room temperature. A large spectrum of wavelengths can be generated and the photon statistics of generated states is good. The limited stability of the molecules due to photo-bleaching is the main problem. Even the most stable dyes survive only a few hours of continuous excitation[11].

4.2 Physical medium

The medium in which the photon travels from Alice to Bob can be either free-space or optical fiber. In this thesis the focus will be on the optical fiber. One of the main benefits of quantum key distribution is the possibility to use the existing telecom network as a channel. There are two transmission windows in standard optical single-mode fiber, one at 1310 nm and one at 1550 nm. The attenuation at these wave-lengths are very low 0,35 dB/km at 1310 nm and 0,21 dB/km at 1550 nm[1] which makes it suitable as a quantum channel. There are a few problems with long fibers. One is chromatic dispersion: different wavelengths travel at slightly different velocities and that leads to problems as soon as subsequent pulses start to overlap. One solution for this problem is to use a narrow bandwidth, 0,5 nm, which eliminates the problem[12]. There are also problems with polarization mode dispersion, a birefringent effect, which is defined as a slow and a fast polarization mode orthogonal to each other so that the pulse tends to split into two components, and that results in a depolarization of the pulse. The direction of the birefringence may vary with time due to environmental factors, so it cannot be statically compensated for. This may be a problem for all implementations that require that the polarization is stable.

Many QKD systems that use dedicated fiber use multi-mode fiber, a fiber with a larger core that is suitable for wavelengths around 850 nm. The reason for this is that cheaper and more effective detectors are available for these wavelengths. The main problem with multi-mode fiber is that the attenuation is much higher than for single-mode fiber, 2 dB/km instead for 0,2-0,35 dB/km. Notice that 0,20 dB/km attenuation means 99 % loss after 100 km[11].

4.3 Physical Coding

There are different ways to encode the information in the quantum system. The system described in the introduction is basically polarization encoded BB84. In the following subsections I will describe some of the different methods to encode the information in the physical layer.

4.3.1 Polarization Encoding

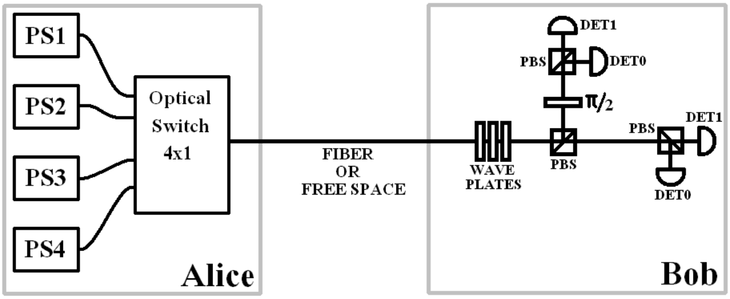

Figure 4.2. Polarization Encoding

The above figure shows a typical QKD system with the BB84 four-state protocol using polarization coding. In the ideal case Alice's system consists of four photon sources which fire single photons polarized at $-\pi/4$, $\pi/4$, 0 or $\pi/2$. For a given qubit, 0 or 1 in either the vertical-horizontal basis or the diagonal basis, a single photon source is triggered and the photon travels in the quantum medium to Bob.

When the photon travels through the fiber it can be depolarized due to polarization mode dispersion which is caused by small imperfections in the fiber, this can be devastating for QKD based on polarization encoding. Fortunately this depolarization can be compensated with a set of wave-plates when the fiber is short. With a long fiber the problem is more severe due to that the polarization transformation induced by the long fiber is unstable over time. Polarization encoding over long fibers therefore requires some kind of active alignment[13].

When the pulses arrive at Bob, they travel through a set of wave-plates to compensate for the transformation induced by the optical fiber. The photons then reach a symmetrical beam-splitter, implementing the basis choice. Transmitted photons are analyzed in the vertical-horizontal basis with a polarizing beam-splitter and two photon-counting detectors. The polarization state of the reflected photons is rotated with $\pi/4$ by a wave-plate, $-\pi/4$ becomes 0. The photons are then analyzed with a second set of polarizing beam-splitters and photon-counting detectors. There are several other ways to implement polarization coding but the scheme above describes the general idea very well.

Encoding the qubits in the polarization of the photon is a very natural choice, but due to the polarization mode dispersion it is not the optimal choice for fiber based QKD. For free-space QKD it works very well as air has essentially no birefringence at all.

4.3.2 Phase Encoding

The different polarizations in the polarization encoding is here replaced by different phase shifts between two arms in the Mach-Zehnder interferometer. Alice has the photon source, a coupler and the first phase modulator. Bob's setup consists of the detectors, a coupler and the second phase modulator.

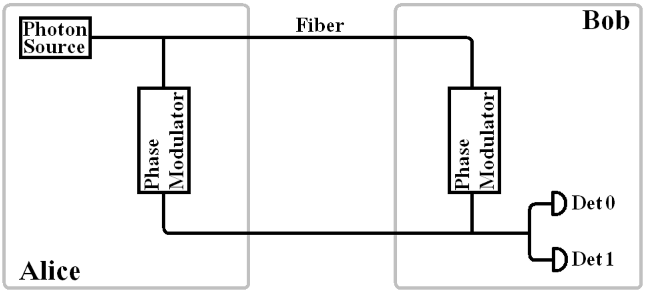

Figure 4.3. Phase Encoding

Due to destructive or constructive interference Alice can alter the probability that the photon reaches a certain detector by altering the phase shift in one arm of the interferometer. Bob controls the phase shift in the other arm.

Alice associates different phase shifts with different bit values, 0 and $\pi/2$ with 0 and π and $3\pi/2$ with 1. Bob randomly applies a phase shift of 0 or $\pi/2$. He then associates the detector at port 0 with bit value 0 and the detector at port 1 with bit value 1.

Alice and Bob use compatible bases when the phase difference is 0 or π, that means that the outcome at the ports are deterministic. Alice can then infer from the phase shift she and Bob applied which port the photon chose and Bob records which detector that clicked. When the phase difference is $\pi/2$ or $3\pi/2$ the bases are incompatible and the photon randomly chooses output port. Alice publicly announces in which basis she encoded her photon, either horizontal basis which is either a phase shift of 0 or π or the vertical basis which is when she used $\pi/2$ or $3\pi/2$ as phase shift.

Bob checks the phase difference between his and Alice's phase and if the bases are compatible he tells Alice to keep the bit, if they are incompatible he tells Alice to throw away the bit.

Table 4.1. Phase Coding

Alices bit value	Alices phase shift	Bobs phase shift	Difference in phase shift	Bobs bit value
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$	?
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$	?
0	$\pi/2$	0	$\pi/2$	?
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$	?
1	$3\pi/2$	$\pi/2$	π	1

For this scheme to work it is extremely important that the difference in length between the two paths in the interferometer is stable during a key exchange session. It should not be changed by more than a fraction of a wavelength of the photon or the phase relation between Alice and Bob would change and induce errors in their bit sequence. Unfortunately it is impossible to keep the path difference that small when Alice and Bob are separated by more than a few meters[13].

Double Mach-Zehnder Interferometer Scheme

To avoid the problem with path difference changing the two communicating parties can use a time multiplex and two unbalanced Mach-Zehnder interferometers, one for Alice and one for Bob, connected in series by a single optical fiber. The photons travel through Alice's interferometer then along the fiber to Bob and into his interferometer. When monitoring photon detections as a function of time since emission of the photon, Bob gets a graph with three peaks, the first peak represents photons which take the short path in both interferometers and the last peak photons that chose the long path in both interferometers. The central peak corresponds to photons that chose the long path in Alice's interferometer and the short path in Bob's interferometer or the short path in Alice's interferometer and the long path in Bob's interferometer. If there is no difference in length in the last two paths, the photon in these events produce interference. If a timing window now is used to discriminate between interfering and non-interfering events, the latter are disregarded. Alice and Bob can exchange a key.

Because the photon travels in only one fiber between Alice and Bob, the problem with different path lengths is now only local in the interferometers. By keeping the interferometers in containers with stabilized temperature the imbalance of the interferometers can be kept constant. For long key exchanges an active system is necessary to compensate for drift, and in order to ensure the indistinguisability of both interfering processes one must make sure that in each interferometer the polarization transformation is the same in both the long and the short arm. A polarization controller must be used for this. Fortunately in short optical fiber which is kept at a constant temperature the polarization transformation is quite stable, so this adjustment does not need to be repeated often.

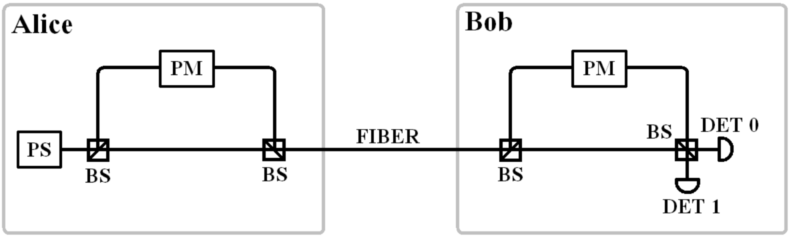

Figure 4.4. Double Mach-Zehnder Interferometer Scheme

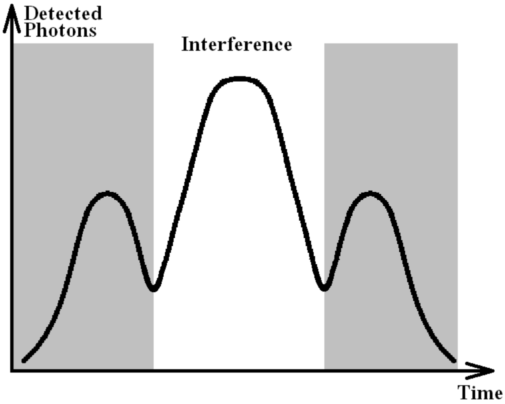

Figure 4.5. Interference

Plug & Play Scheme

An improved version of the double Mach-Zehnder interferometer scheme is the Plug & Play scheme. It has only one Mach-Zehnder interferometer and the light propagates through the same channel and interferometer twice due to the Faraday mirror on Alice's side.

A short laser pulse sent by Bob is split into two at coupler C_2. The first part, P_1, goes straight to Alice while the second one, P_2, is delayed by the M_2-M_1 delay line. Both pulses are reflected back towards Bob at M_3. Alice measures the intensity of the incoming pulses and attenuates them to single-photon levels. The phase modulators, PM, modulate the path length between the two pulses. On arrival to Bob's side, P_1 is delayed by M_1-M_2 and interferes with P_2. The interference pattern at D_0 gives the relative phase settings of Alice and Bob. The Faraday rotators in front of the mirrors cancel out all birefringence effects in

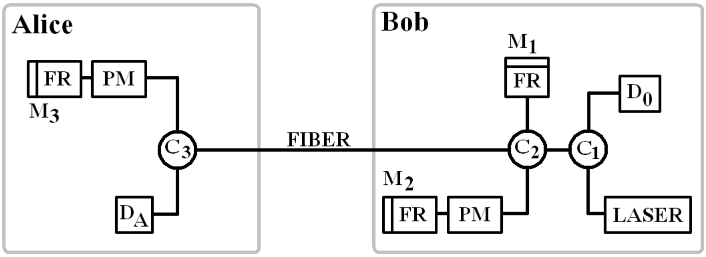

Figure 4.6. Plug & Play Scheme

the fiber[14]. This scheme automatically compensates for all birefringence effects and polarization dependent loss in the fiber. Shortly after this scheme had been introduced there were concerns that the security of the protocol was weak as Eve can make sophisticated operations on the bright pulses sent from Bob. Recently the security of the Plug & Play scheme was proven[1].

Faraday-Michelson Scheme

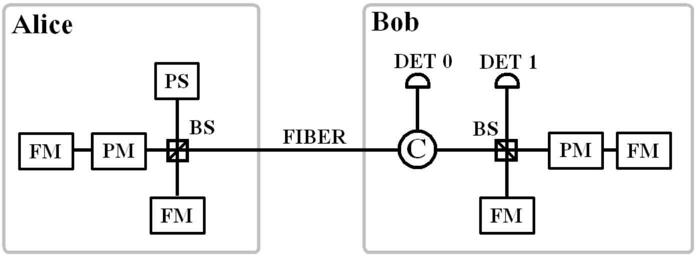

Figure 4.7. Faraday-Michelson Scheme

This is also an improved version of the double Mach-Zehnder interferometer scheme. The difference is that each interferometer has only one beam-splitter. Due to a Faraday mirror the light travels through the same fiber twice, so the polarization drift is self-compensating. The phase drift of the local interferometers still needs compensation. This compensation should be done in real-time since a drift of π takes a few seconds[1].

Sagnac Loop Scheme

Another bi-directional optical layer design is to use a Sagnac loop where the quantum signal is encoded in the relative phase between the clockwise and counter-clockwise pulses that go around the loop. The Sagnac interferometer has the advantage of being free from birefringence effects and polarization dispersion since

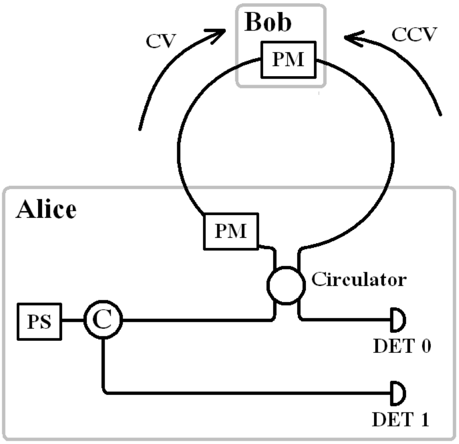

Figure 4.8. Sagnac Loop Scheme

the counter-propagating pulses pass through the exact same fiber paths inside the loop. Sagnac loop QKD is simple to set up and can be used in a network setting with a loop layout. However it is very difficult to do security analysis of this scheme. In the section about QKD networks there will be an example on how to use the Sagnac loop scheme for a multi-user QKD network.

4.3.3 Frequency Coding

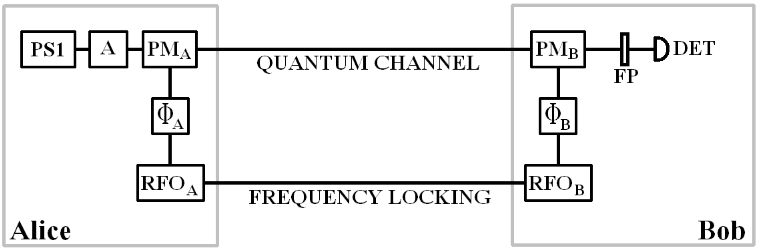

Figure 4.9. Frequency Coding

The name of this section is somewhat inaccurate since the value of the qubits is not coded in the frequency of the light but in the relative phase between sidebands of a central optical frequency. A source emits short classical pulses of monochromatic light with angular frequency ω. Phase modulator PM$_A$ modulates the phase of this beam with a frequency $\Omega \ll \omega_S$ and a small modulation depth. Two sidebands are generated at frequencies $\omega_s \pm \Omega$. The phase modulator is driven by a radio-frequency oscillator RFO$_A$ whose phase Φ_A can be varied. Finally the beam is attenuated so that the sidebands contain much less than one photon per pulse, while the central peak remains classical. After traveling to Bob's side the beam is again modulated by PM_B. This phase modulator is driven by a second radio-frequency oscillator RFO_B, synchronized with RFO_A, with the same frequency Ω and phase Φ_B. Now the beam contains the original central frequencies ω_S, the sidebands created by Alice and the sidebands created by Bob. The sidebands at frequencies $\omega_S \pm \Omega$ are mutually coherent and yield interference. After removal of the central frequency and high-order sidebands with a spectral filter Bob can record the interference pattern in these sidebands[13].

4.4 Detectors

The major limiting factor for long distant fiber-based QKD at telecom wavelengths is the lack of efficient detectors with low dark counts. There are a number of different technologies but they all have some major disadvantage that makes them less than ideal.

4.4.1 InGaAs-APD Single Photon Detectors

These are the most common type of single-photon detectors in fiber based QKD. They are commercially available, the reliability is relatively high and they are easy to calibrate and operate. InGaAs-APD Single Photon Detectors utilize the avalanche effect of semiconductor diodes. A strong biased voltage is applied on the InGaAs diode. The incoming photon will trigger the avalanche effect and a detectable voltage pulse will be generated. The narrow band gap of these detectors makes it possible for them to work at the telecom wavelengths, 1310 and 1550 nm. The working temperature is normally -50 degrees C to -110 degrees C which is easily achieved by thermal-electric coolers. The detection efficiency of InGaAs-APD Single Photon Detectors is about 10 %. Another important parameter in single photon diodes is the dark count rate, which is the event when the detector is triggered without any photon hitting it. The dark count rate of an InGaAs single photon diode is relatively high even if it is cooled. To make matters worse there is an after-pulse effect when the detector has been triggered by a photon where the dark count rate is increased. Therefore the detector is set to be deactivated for a period of time after a successful detection. This is called the dead-time and severely limits the detection frequency of the InGaAs-APD single photon diode. A method to decrease the dark count rate is to only activate the detectors when a photon is expected to hit them. This is called gating mode and this reduces the dark count by several orders of magnitude. Recently a QKD system has been operated at 500 MHz by using an InGaAs-APD single photon diode gated in a sinusoidal manner which make these detectors competitive with newer single photon detector technologies[1].

4.4.2 Si-APD Single Photon Detectors

These detectors can operate at room temperatures. They have a very low dark count rate, they are very compact in size and most important they have high detection efficiency, more than 60 %, and they can work at gigahertz frequency. The problem is that the band gap of silicon is too large to detect photons at telecom wavelengths, but it works very well at visible photons around 800 nm. This makes the Si-APD single photon detectors ideal for free-space QKD systems, but the high attenuation of telecom fiber on visible wavelengths makes it impractical to use them in long distance fiber based QKD systems [1].

4.4.3 Parametric Up-conversion Single Photon Detectors

This is a method to try to use Si-APD single photon detectors to detect photons at telecom wavelengths. Periodically poled lithium niobate waveguide and a pumping light is used to up-convert incoming photons from telecom wavelengths to visible wavelengths so they can be detected using a Si-APD single photon detector. The efficiency of up-conversion detectors is similar to that of InGaAs-APD single photon detectors. It is possible to reach GHz rates in fiber-based QKD systems using this method[1].

4.4.4 Transiting-edge Sensor

These detectors are based on critical state superconductors. It uses squared superconductor thin film to measure the electron temperature. To keep the thin film in critical state a biased voltage is applied. When one or more photons are absorbed by the sensor the electron temperature will change and this leads to a change of the current. The electron temperature is proportional to the number of photons that have been absorbed, so the TES detector can resolve photon numbers. The bandwidth of the TES detector is very wide which makes the sensor sensitive to all wavelengths, even the black body radiation of the fiber or environment can trigger the detection event. Therefore a spectral filter must be used to decrease the dark count. Unfortunately this also decreases the detection efficiency which otherwise would be up to 89 %. The thermal nature of the TES detectors limits their counting rate. Once a photon has been absorbed it takes a few microseconds before the heat has dissipated to the substrate. This limits the counting rate to a few megahertz. One of the greatest disadvantages with TES detectors is that they have a working temperature of 100 mK[1].

4.4.5 Superconductive Single Photon Detectors

Like the TES detector SSPDs use superconductive film to detect incoming photons, but instead of using a piece of plain thin film a zigzag pattern of superconductor wire is used. A current is applied to the wire to set it in critical state, and when a photon hits a spot on the wire it makes the spot over-critical, non-superconductive. As the current is the same as before, the current density in the areas around this hot-spot increases and makes these areas non-conductive. This results in a voltage spike that can be observed. Only half of the detector area is covered by the wire, so the detection efficiency is lower than that of the TES detector. The superconductor wire can dissipate the heat in a few tens of picoseconds, so the counting rate that can be achieved is very high, up to 10 GHz, and the detector also has very low dark count rate around 10 Hz. The working temperature of the SSPDs is higher than that of the TES detector, 3 K, which makes it possible to cool the SSPD detector with a closed cycle refrigerator. However, the fabrication of the complicated zigzag superconductor wire with smooth edges is very complicated[1].

4.4.6 Homodyne Detectors

These detectors are used to count the number of photons in a very weak pulse, 100 or so photons. A very strong pulse is used to interfere with the weak pulse. Then two photo diodes are used to convert the two resulting optical pulses into electrical signals, and make a subtraction between the two electrical signals. Although the efficiency of the homodyne detector is very high, the noise of the detector and the electronics is also very high and the two photo diodes must be identical which is hard to achieve[1]. The homodyne detector is used in Gaussian-modulated Coherent State Protocol.

Chapter 5

Networks, multiplexing and the impossibility of amplification

This chapter will discuss different technologies to improve the range for QKD and investigate the possibilities to use the telecom infrastructure for QKD. Finally different schemes for QKD networks with multiuser techniques will be presented.

5.1 Amplifying the quantum signal

I will start this chapter with stating that it is impossible to amplify the quantum signal without introducing noise in the quantum system. The effect would be the same as when Eve is trying to eavesdrop on the quantum channel. If there is a need to increase the range, the only possibility today is to have an intermediate node that is trusted. In chapter 7 the SECOQC secret sharing network based on trusted nodes will be presented. In chapter 8 the idea of entanglement swapping will be introduced and the technology for quantum repeaters based on entanglement swapping will be discussed.

5.2 Wavelength Division Multiplexing

WDM technology is used to divide the transmission windows in the fiber into different channels. Thus being able to send different data streams at different wavelengths and thereby increase the total transmission rate. It seems that the number of channels in dense WDM could reach 500 and beyond[15]. A report from 2007 shows that it is possible to have channels with a bandwidth of 0,5 nm at 1555 nm and photons can then be transmitted over a 150 km single mode fiber without having to compensate for chromatic dispersion. The same report shows that a spacing of 0,8 nm will achieve an isolation of 100 dB between adjacent channels[12].

In an article from 1997 WDM is used to add a quantum channel to a classical 1,2 Gbit/s data channel operating over 28 km of optical fiber. They also find that the crosstalk between the different channels differs depending on what wavelengths that are used. The error rate of the quantum channel is as low as 4 % and increases to 22 % in the worst case. The classical data channel is essentially unaffected by the quantum channel[16]. Depending on the crosstalk between the different channels it might not be possible to use the whole transmission window, but with carefully chosen wavelengths it should be possible to have several quantum channels along with classical channels in the same fiber without lowering the amount of classical data transmitted in the cable.

There are other advantages with WDM as we will see in the section about quantum network.

5.3 Quantum Network

Lately there have been a lot of research going on in this area. If quantum key distribution is going to be widespread it is necessary to develop large quantum networks with high key generation rate and many nodes. There are several benefits with a QKD network; In the case where Alice serves several Bobs with keys one can connect a new node to the network and communicate with Alice. Once a secure key has been negotiated with Alice, the new node can communicate with any Bob through Alice without having to agree on a key with any other end-user. Because the main bottleneck in QKD systems is the photon detector, one lightsource should be able to serve several detectors with photons without any severe degradation of the key rate between the sender and the receiver. A very interesting project has recently been presented in Vienna, the SECOQC QKD network which will be described in a later chapter. In the following subsections different schemes for addressing different users will be described.

5.3.1 Passive-Star Network

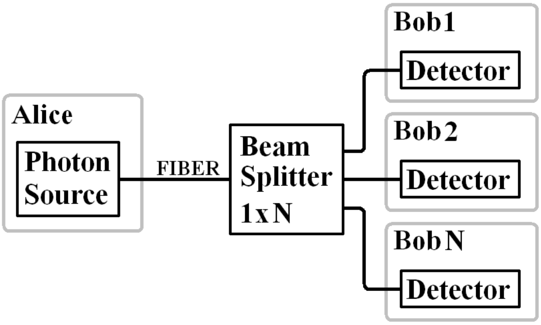

Figure 5.1. Passive-Star Network

A passive star network was first demonstrated by Townsend to send photons to connect four users[17]. The network was an extension of the point-to-point QKD link with a 1xN beamsplitter, which randomly routed the photon to one of the N Bobs. It can be easily implemented but suffers from high attenuation induced by the splitter, for example a three user network with 1x2 beamsplitter halves the probability that the photon reaches the desired receiver. Because the routing to different users is non-deterministic, the different users might also have different key rates[18].

5.3.2 Wavelength-Routed Network

This network topology is similar to the star network. The main difference is that Alice can control which user which will receive the photon by tuning her pulsed laser source to a specific wavelength. The photon travels from Alice to a Bob via an arrayed waveguide grating. The advantage of this topology is that the insertion loss of the arrayed waveguide grating is uniform regardless of the number of channels. The number of users allowed is limited by the channel spacing of the arrayed waveguide grating and the bandwidth of the fiber [18].

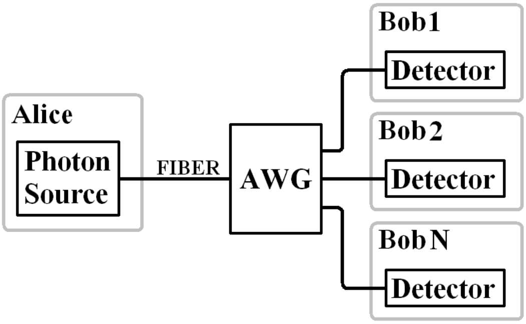

Figure 5.2. Wavelength-Routed Network

5.3.3 Wavelength-Addressed Bus Network

In this scheme Alice has a tuneable photon-source and each Bob is assigned a specific wavelength. The Bobs are connected to the bus fiber through a Bragg grating which allows them to retrieve only the photons intended for them. These gratings are designed to reflect photons of a specific wavelength to a specific user and transmit all others. This topology allows the network to be easily expanded by tapping the bus and inserting a suitable grating. It should be possible to have as many as 50 users on this kind of network without raising the attenuation to levels where it has a severe impact on the key generation rate[18].

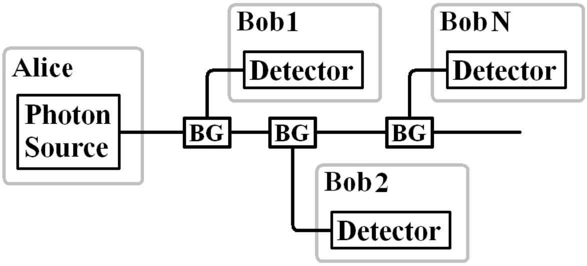

Figure 5.3. Wavelength-Addressed Bus Network

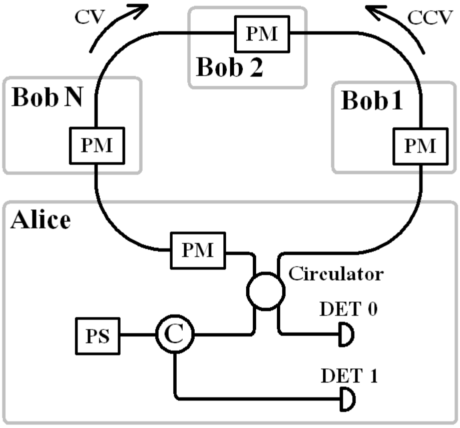

Figure 5.4. Optical-Ring Network

5.3.4 Optical-Ring Network

This topology uses a Sagnac loop and the protocol used is based on phase encoding. This topology is significantly different from the ones based on the Mach-Zehnder interferometer. The single-photon pulse enters the Sagnac interferometer through an optical circulator, the pulse splits into two in the coupler and one pulse travels around the loop in clockwise and the other in the counter-clockwise direction. Any user who is communicating with Alice modulates the pulse traveling in clockwise direction and Alice modulates the pulse traveling in the counter-clockwise direction. The position of Alice's phase modulator is important since the pulse that it modulates must be returning from its trip around the loop in order to prevent information about Alice's modulation choice from traveling through the loop. A timing and control mechanism must be established so that only one Bob modulates the photon traveling through the loop at a time. When the pulses have traveled through the loop, they interfere in the coupler and enters one of the two detectors. If the phase difference between the pulses is π the photon enters detector 1 and if the phase difference is 2π it enters detector 2. Because this topology is based on a Sagnac loop it has the advantage that it is free from thermal fluctuations. Another potential advantage is that all users on the network contain only one phase modulator except for Alice. This can simplify the process of connecting new users to the network, since Alice is the only one that requires single-photon detectors. The attenuation added when adding a new user to the network also seems to be very low which is a big advantage compared to the passive-star network[18].

As we can see in this chapter there are many different possibilities to extend the QKD scheme from two user links to multi-user networks. The WDM technology makes it possible to use the existing telecom fiber network as a quantum channel without interfering with the classical data streams.

Chapter 6

Quantum Repeaters

In this section I will briefly describe the basics of entanglement in quantum mechanics. This will be done in casual way just to give the reader enough knowledge to understand how entanglement based QKD and entanglement swapping works. This is crucial when we later discuss quantum repeaters.

When two objects are entangled the quantum state of one object cannot be described without full mention of its counterpart. In layman's words it can be described as if some kind of connection exist between two entangled objects and if one objects quantum state is altered the other object is affected. There is no time delay between the alteration of object one and the effect on object two even when they are separated.

6.1 Entanglement based QKD

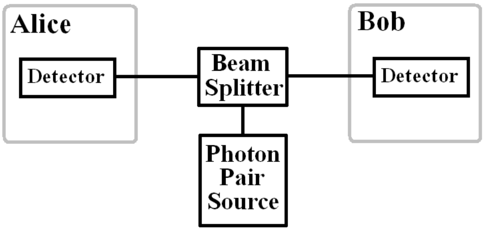

Figure 6.1. Entanglement based QKD

We place an entangled photon pair source between Alice and Bob and one photon travels to Alice through an optical fiber or free-space and the other travels to Bob. Alice and Bob now share an entangled pair of qubits. Now instead of sending a photon to Bob, as in BB84, Alice measures her photon in one of two conjugate bases. She must select the bases randomly. The rest is very similar to BB84, Bob measures his photon in a random chosen basis and then Alice and

Bob communicate over a public channel and discard the photon pairs where they measured in different bases. The qubits are then correlated and form the key. This is one of many entanglement based QKD schemes but it is enough for the following discussion.

6.2 The Bell states

The Bell states, named after John S. Bell, represent the simplest form of entanglement and a Bell pair is a pair of qubits which together form a Bell state. Now say that Alice and Bob share a photon pair which is in a Bell state, Alice has one of the photons and Bob the other. If Alice takes a measurement on her photon the outcome is completely random, either 1 or 0. But if Bob then measures his qubit he will get a result that is correlated to the result Alice got. This is the result of entanglement and this is the foundation for QKD based on entanglement.

6.3 Bell state measurement

This is an important concept in quantum information and it is very interesting for QKD based on entanglement because it makes it possible to forward the entanglement from one photon to another. A Bell state measurement is a quantum-mechanical measurement of two qubits that determines what Bell state the pair is in. When the measurement is performed the qubit-pair gets projected into a Bell state, according to the projection rule of quantum measurement, and as Bell states are entangled a Bell state measurement is an entangling operation.

6.4 Quantum repeater based on entanglement swapping

We add another entangled photon pair source between Bob and the first source and places a gadget that performs a Bell state measurement between the two photon pair sources.

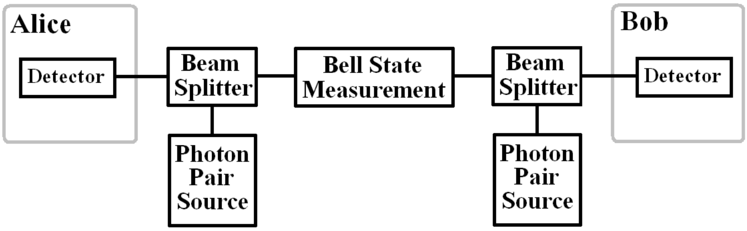

Figure 6.2. Entanglement Swapping

Now when the Bell state measurement is performed, the two photons that are subject to the measurement will be entangled, and destroyed during the measurement. But since they are already entangled with their respective 'twin' the new entanglement will spread to the two photons that never met. Now Alice and Bob can perform the entanglement based QKD scheme described above.

In theory we can insert an infinite number of photon pair sources and Bell state measurement gadgets between Alice and Bob and increase the distance between them as long as we like.

Chapter 7

SECOQC

7.1 Introduction

SECOQC - Development of a Global Network for Secure Communication based on Quantum Cryptography - is an EU funded project the main goal of which is to develop, operate and test an integrated secrets distribution network placed in Vienna. 41 partners from 12 European countries have worked together since April 2004 to realize this network. The network is formed as a Quantum Back Bone network based on trusted nodes to which new users can connect with a QKD link and communicate with all other end users connected to the QBB network.

The goals for this project are to try to overcome several limiting factors for QKD, the point to point paradigm, the exponential growth of the initial authentication key with the number of users, the limited range of a single QKD link, the question of integrability in existing networks but also issues like missing standards.

A test network with six nodes connected by eight QKD links was demonstrated in October 8, 2008.

7.2 The layout of the QBB network

The QBB network consists of building blocks made up by four trusted nodes connected with six QKD links. The reason for this multi-link setup is that even if one QKD link fails, there will be other paths between two trusted nodes.

The meaning of a trusted node is that the trusted node receives the data from Alice and decrypts it. It then encrypts it with the key shared with the next trusted node and sends the data to it etc until it reaches Bob. The secret is forwarded in a hop-by-hop fashion.

All the intermediate trusted nodes will therefore have full access to the information sent between the end-users. These intermediate nodes must be trusted and should be situated in a secure location, for example government building or a bank. The trusted node scheme is currently the only feasible solution to increase the range for QKD.

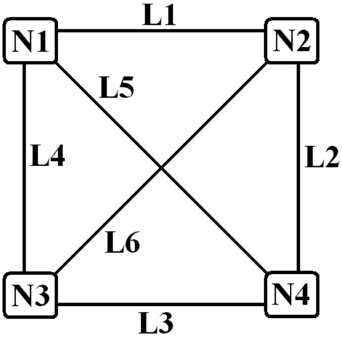

Figure 7.1. Building Block

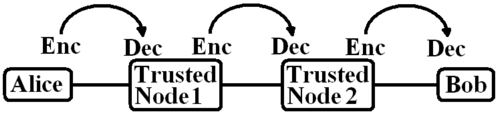

Figure 7.2. Trusted Nodes

7.3 Protocols

A large effort have been put into developing protocols for the secret distribution network. The trusted nodes must handle several QKD devices, provide them with authenticated communication with their counterpart and store and handle generated keys. The nodes also provide services like routing traffic if one QKD-link fails or if the network becomes congested in an area. A common interface for the QKD-devices has been developed, since they come from different manufacturers. Encryption and decryption of the end-users communication is constantly performed in the trusted nodes.

7.4 Benefits of a secrets distribution network

When a new end-user wants to connect to the QBB network she only has to establish a QKD link to the nearest trusted node to be able to communicate with all the other end-users. In a metropolitan area the distance between the new user and the nearest trusted node would be considerable shorter than the average distance to another end user. This makes the cost to include a new user to the secret distribution network lower than it would be to include a user to a QKD network based on a many-to-many setup without trusted nodes. As mentioned earlier the QBB network will be more resistant against failure of a QKD-link since there exists several different paths in the QBB network between two end users.

7.5 The demonstrated QKD network in Vienna

In November 2008 a functioning secret distribution network was demonstrated. A building block with four stations in Vienna was extended with a QKD-link to the near city of St.Poelten. The quantum medium connecting each QKD device pair in the building block is dedicated fiber and the classical channel uses an additional fiber. The circumference of the fiber ring is 63 km and the fiber connecting the node in St.Poelten is 85 km long.

A mix of different manufacturers provided QKD devices that meet the specific criteria required to participate in the project. Only devices that could deliver a secure key rate of 1 kbit/s over a distance of 25 km of fiber were accepted to build up the QBB network. The devices must also be able to generate keys for six months without human interaction, and the latency time for a restart is limited to one minute.

The devices used by the end-user were not required to meet the same standards as the ones which build up the QBB network. Almost any device could be used, as the cost for the end users should be much lower. To extend the network to areas where the penetration of fiber infrastructure is lower, two systems based on free-space QKD have been included[19].

Chapter 8

Discussion

8.1 Commercially available systems today

Today only a few companies offer QKD solutions on the market and they are typically point-to-point QKD using a dedicated fiber. The key generation rate is fairly low, around 1 kbit/s over 25 km for the product offered by IdQuantique. The range in IdQuantique's system is around 50 km and above 50 km on demand. It should be pointed out that the key generation rate falls considerably when the distance increases. Therefore the key generation rate at 50 km is much lower than that at 25 km. Another company, SmartQuantum, offers a point-to-point solution with a range of 80 km without mentioning the bit rate for the key generation.

The key generation rate of 1 kbit/s is not high enough to do one-time-pad encryption for larger amounts of data, but it is possible to use AES with a 256 bit key and change key four times every second, which should be considered extremely secure. The range is enough for inner-city communications.

8.1.1 Alternatives to point-to-point QKD

When we look for alternative solutions, they have to match the security of QKD. Otherwise the comparison is useless since this is the advantage of QKD. This means that we cannot compare it with public key ciphers, since they are not proven to be secure against other attacks than brute-force. The only alternative that is as secure as a QKD-link is to use one or several trusted couriers to deliver the key. At first this seems to be a poor choice since we have to generate the random key before we can send our courier and then he has to travel to deliver the key. But we should also consider the time it takes to manufacture the QKD devices and the time it takes to setup the system. Some might argue that we can buy already manufactured equipment and eliminate the time this would consume. This is true but we could also buy a random key from a company or from two companies and XOR the keys to eliminate the companies knowledge of the key. This means that we could probably set up and start to operate a system based on couriers faster than a QKD system.

The most important factor is how often we have to send the courier to deliver a fresh key. If we want to match the key generation speed of a QKD system we need roughly 1 kbit/s. This is 32 Gbit/year and a modern blu-ray disc with two layers can contain 50 Gbyte which equals 400 Gbits. A single blu-ray disc can contain keys for a little more than 12 years of operation. If we burden the courier with 8 blu-ray discs, he has to make the trip once every century. It would probably be difficult to match the cost for this courier based system with a QKD system, especially if we consider that the courier could use a bicycle to travel the 25 km to his destination.

Another major advantage for the courier based system is that once the key is delivered the communicating parties could use any public channel for communication. Those who use a QKD system are bound to the fiber used as quantum channel if they want to continue to generate keys.

An advantage for the QKD system is that in order to threaten the security of a QKD-link, the authentication of the messages sent over the classical channel must be broken before or during the execution of the quantum key establishment protocol. If the courier sent key is copied, unnoticed, the attacker can record the encrypted messages and later decrypt the data.

This might open up a possibility to use a public-key scheme to distribute an authentication key for the QKD instead of using a courier.The attacker has limited computational power at the specific time, and when the short time the first QKD round takes expires the opportunity is lost for the attacker. This holds until quantum computers are available. They can break a public key cipher instantly.

It should be noted that if the attacker misses the opportunity to break the first authentication round, she could mount a denial-of-service attack until the communicating parties runs out of the generated key and must re-initiate the QKD-session. She then has another opportunity to succeed with the attack. This behavior should of course raise suspicion.

8.2 QKD in the near future

In the last section I argue that today's QKD products are not marketable. If we consider a much longer reach for the QKD link, maybe around the world by satellite based free space QKD, and a key generation rate of 500 kbit/s the picture might change. If we have a key generation rate of 500 kbit/s it will result in almost 2 Tbyte of key every year. This means that the courier needs a small bag to transport the two hard-drives needed to store the key, and he has to make the trip once every year. If we allow the courier a large trunk in which he stores 20 hard-drives, he will need a seat on an airplane once every decade. Those running a QKD-system must then launch a satellite into orbit to be able to compete.

A large secret sharing network based on a quantum back bone system with trusted nodes like the SECOQC project might be what we need to take the QKD one step further. This would increase the range to more useful distances and it would be a great advantage to have access to the whole network once connected to the nearest node. A fundamental problem exists with the trusted nodes, they decrypt and encrypt all information that the end users transmit to each other and can thereby store and read all communications. The question who should be running the secret sharing network is therefore quite delicate. A company that is interested in new technology might not be the best candidate. Even the government might be interested in information that could reveal possible threats against the nation. Can we trust that whoever is running the network won't be tempted to eavesdrop? Even if this is unlikely, it has the power to throw the theoretical security of QKD down the drain. In the future we might be able to use quantum repeaters based on entanglement swapping instead of trusted nodes. Then the theoretical security of QKD would be restored.

The question who needs the QKD technology remains. It should not be aimed at the average person who uses his computer to communicate with the bank or to buy things over the Internet. If anyone wants to steal his money, it is easier to fool him to give us his password or to install spyware on his computer. Even breaking the public encryption system used for communication with the bank today is too difficult. It is also important to consider how much security we need. Everyone doesn't need to send 1 Mbit of extremely sensitive data every second. Then the cost for the extra security is unnecessary.

There is a catch with QKD: if the transmission speed is low we can use a courier with pre-generated keys to solve the problem at a lower cost. If the QKD technology improves so that the transmission speed increases up to 500 kbit/s, we need enormous amounts of secret data to transfer or it would be like using a supertanker to deliver one barrel of oil.

8.3 Conclusion

Several experiments have shown that it is possible to use the existing telecom network with QKD and at the same time send traditional data streams in the same fiber. It should be noted that it most likely will have a small negative effect on the range and transmission speed of the QKD system. But the gains of using the existing telecom network is far greater than the degradation in the performance of QKD.

SECOQC has shown that it is possible to integrate a large secret sharing network with trusted nodes in a city. The question who will be running the secret sharing network is quite important. Another interesting question is if there are enough companies willing to pay for this level of security.

I am inclined to draw the conclusion that the fiber based QKD systems available today are not cost effective, and that QKD in the foreseeable future will be forced into a small niche market because of the expense of running the system and the built in limitation of the technology. In most cases there are cheaper alternatives to QKD which are secure enough. A public key exchange like RSA could be used with a long key, more than 1024 or 2048 bits, for data that is secret but only has to remain secret for a shorter period of time, maybe a few weeks to some years. AES with 128 or 256 bit preshared key could be used for data that has to be secure for a longer period of time and depending on the level of security that is desirable the frequency of the key change can be increased or decreased.

In the end, it is a very interesting technology and the area develops rapidly. Presently, it is the only existing technology that is theoretically secure against eavesdropping.

Bibliography

[1] Hoi-Kwong Lo and Yi Zhao. Quantum crypography. *Optics Express*, 15(11), 2008.

[2] How large a key should be used in the rsa cryptosystem? www.rsa.com/rsalabs/node.asp?id=2218, 2008.

[3] Rsa-200 is factored! www.rsa.com/rsalabs/node.asp?id=2879, 2008.

[4] Arjen K. Lenstra. Unbelievable security. matching aes security using public key systems. *Lecture Notes in Computer Science*, 2248:67–86, 2001.

[5] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dusek, Norbert Lutkenhaus, and Momtchil Peev. A framework for practical quantum cryptography. arxiv.org/pdf/0802.4155v1, 2008.

[6] Svante Seleborg. About aes - advanced encryption standard. www.axantum.com/AxCrypt/etc/About-AES.pdf, 2004.

[7] Romain Alleaume. Secoqc white paper on quantum key distribution and cryptography. arxiv.org/pdf/quant-ph/0701168, 2008.

[8] Charles H. Bennett, Francois Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5:3–28, 1992.

[9] L.P. Lamoureux, E. Brainis, N.J. Cerf, Ph. Emplit, M. Haelterman, and S. Massar. Experimental error filtration for quantum communication over highly noisy channels. *Physical Review Letters*, 94:230501–230504, 2005.

[10] Jörgen Cederlöf and Jan Åke Larsson. Security aspects of the authentication used in quantum cryptography. *IEEE Transactions on Information Theory*, 54:1735–1741, 2008.

[11] Miloslav Dusek, Norbert Luthenkenhaus, and Martin Hendrych. Quantum cryptography. arxiv.org/pdf/quant-ph/0601207, 2008.

[12] S. Sauge, M. Swillo, S. Albert-Seifried, G. B. Xavier, J. Waldebäck, M. Tengner, D. Ljunggren, and A. Karlsson. Narrowband polarization-entangled photon pairs distributed over a wdm link for qubit networks. *Optics Express*, 15:6926–6933, 2007.

[13] Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74:145–195, 2002.

[14] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin. "plug and play" systems for quantum cryptography. *Applied Physics Letters*, 70:793–795, 1997.

[15] Ying Lu and Okan K. Ersoy. Dense wavelength division multiplexingby the method of irregularly sampled zero crossings. docs.lib.purdue.edu/ecetr/154, 2008.

[16] P.D. Townsend. Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fiber using wavelength-division multiplexing. *Electronics Letters*, 33:188–190, 1997.

[17] Paul D. Townsend. Quantum cryptography on multiuser optical fiber networks. *Letters to Nature*, 385:47–49, 1997.

[18] P. D. Kumavor, A. C. Beal, S. Yelin, E. Donkor, and B. C. Wang. Comparison of four multi-user quantum key distribution schemes over passive optical networks. *Journal of lightwave technology*, 23:268–276, 2005.

[19] A. Poppe, M. Peev, and O. Maurhart. Outline of the secoqc quantum-key-distribution network in vienna. *International Journal of Quantum Information*, 6:209–218, 2008.