SEMINAR

QUANTUM CRYPTOGRAPHY

Author: Luka Debenjak
Adviser: prof. dr. Anton Ramšak

University of Ljubljana
Faculty of Mathematics and Physics.

February 22, 2006

Abstract

Quantum cryptography could well be the first application of quantum mechanics at the individual quanta level. In this paper I shall describe the theory of quantum cryptography and how to perform quantum cryptography over an optical fiber communications link. This seminar reviews how quantum physics allows information coding in classically unexpected ways. Quantum logic gates and key distribution are also discussed.

Contents

1 Introduction

Human desire to communicate secretly is at least as old as writing itself and goes back to the beginnings of our civilisation. Methods of secret communication were developed by many ancient societies, including those of Mesopotamia, Egypt, India, and China, but details regarding the origins of cryptology remain unknown.

Until some years ago, cryptography was restricted primarily to the military world. Only the military had sufficient resources to produce mechanical devices, such as the famous enigma which was widely used by Germans during World War II or its American counterpart the M-209. Enigma ciphers were broken before at Bletchley Park in England. The Bletchley Park team had to develop the electro-mechanical tools to break these ciphers, which resulted in building the first digital computer called *Colossus*. Thus modern cryptology was born together with computer science. [1]

2 Classical cryptography

Originally the security of a cryptosystem or a cipher depended on the secrecy of the entire encrypting and decrypting procedures. In such ciphers a set of specific parameters, called a *key*, is supplied together with the *plaintext* as an input to the encrypting algorithm, and together with the cryptogram as an input to the decrypting algorithm. This can be written as

$$\widehat{E}_k(P) = C, \text{ and conversely, } \widehat{D}_k(C) = P, \tag{1}$$

where P stands for plaintext, C for cryptotext or cryptogram, k for cryptographic key, and $\widehat{E}$ and $\widehat{D}$ denote an encryption and a decryption operation respectively.

It was shown, that as long as the key is truly random, has the same length as the message, and is never reused then the one-time pad is perfectly secure. So, if we have a truly unbreakable system, what is wrong with classical cryptography?

There is a snag. It is called *key distribution*. Once the key is established, subsequent communication involves sending cryptograms over a channel. However in order to establish the key, two users, who share no secret information initially, must at a certain stage of communication use a reliable and very secure channel. Since the interception is a set of measurements performed by an eavesdopper on this channel, however difficult this might be from a technological point of view, in principle any classical key distribution can always be passively monitored, without the legitimate users being aware that any eavesdropping has taken place.

In the late 1970s Whitfield Diffie and Martin Hellman proposed an interesting solution to the key distribution problem. It involved two keys, one public key π for encryption and one private key κ for decryption:

$$\widehat{E}_\pi(P) = C, \text{ and, } \widehat{D}_\kappa(C) = P. \tag{2}$$

In these systems users do not need to share any private key before they start sending messages to each other. Every user has his own two keys; the public key is publicly announced and the private key is kept secret. Several public-key cryptosystems have been proposed since 1976; here we concentrate our attention on the most popular one namely the RSA.

Suppose that Alice wants to send an RSA encrypted message to Bob (Alice and Bob are two individuals who want to communicate secretly). The RSA encryption scheme works as follows:

Key generation: Bob picks randomly two distinct and large prime numbers p and q. We denote $n = pq$ and $\phi = (p-1)(q-1)$. Bob then picks a random integer $1 < e < \phi$ and computes the inverse d of e modulo ϕ ($\gcd(e, \phi) = 1$). This inversion can be achieved efficiently using for instance the extended Euclidean algorithm for the greatest common divisor. Bob's private key is $\kappa = d$ and his public key is $\pi = (e, n)$.

Encryption: Alice obtains Bob's public key $\pi = (e, n)$ from some sort of yellow pages or an RSA public key directory. Alice then writes her message as a sequence of numbers. For example she can replace each letter with a number, which represents the location of that letter in the alphabet (in this case 1 means "A", 2 means "B"...). This string of numbers is subsequently divided into blocks such that each block when viewd as a number P satisfies $P \leq n$. Alice encrypts each P as

$$C = \widehat{E}_\pi(P) = P^e \bmod n \tag{3}$$

and sends the resulting cryptogram to Bob.

Decryption: Receiving the cryptogram C, Bob decrypts it by calculating

$$\widehat{D}_\kappa(C) = C^d \bmod n = P. \tag{4}$$

For example, let us suppose that Bob's public key is $\pi = (e, n) = (179, 571247)$. He genearated it following the prescription above choosing $p = 773, q = 739$ and $e = 179$. The private key d was obtained by solving $179d = 1 \bmod 772 \times 738$ using the extended Euclidean algorithm which yields $d = 515627$. Now if we want to send Bob encrypted "SHAKEN NOT STIRRED" we replace each letter with a number in divide whole plaintext into blocks:

$$180700 \quad 100413 \quad 261314 \quad 192618 \quad 170403.$$

Then we encipher each block P_i by computing $C_i = P_i^e \bmod n$. The first block $P_1 = 180700$ will be enciphered as

$$P_1^e \bmod n = 180700^{179} \bmod 571247 = 141072 = C_1,$$

and the whole message is enciphered as:

$$141072 \quad 253510 \quad 459477 \quad 266170 \quad 286377 \quad 087175.$$

The cryptogram C composed of blocks C_i can be send over to Bob. He can then decrypt each block using his private key $d = 515627$. The first block is decrypted as

$$141072^{515627} \bmod 571247 = 180700 = P_1.$$

In order to recover plaintext P from cryptogram C, an outsider, who knows C, n and e, would have to solve the congruence

$$P^e \bmod n = C,$$

for example, in our case,

$$P_1^{179} \bmod 571247 = 141072.$$

Solving such equation is believed to be hard computational task for classical computers. So far, no classical algorithm has been found that computes the solution efficiently when n is large integer (say 200 decimal digits long or more). However, if we know the prime decomposotion of n it is a piece of cake to figure out our private key: we simply follow the key generation procedure and solve the congruence $ed = 1 \bmod (p-1)(q-1)$. This can be done efficiently even when p and q are very large. Thus, in principle, anybody who knows n can find d by factoring n. The security of RSA therefore relies among others on the assumption that factoring large numbers is computationally difficult. In the context of classical computation, such difficulty has never been proved. Worse still there is a quantum algorithm that factors large numbers efficiently. This means that the security of the RSA cryptosystem will be completly compromised if large-scale quantum computation becomes one day practical. [2]

The best known factorization algorithm can factor a number n in time t: $t \approx e^{1.9(\ln n)^{\frac{1}{3}}} (\ln \ln n)^{\frac{2}{3}}$. Shor's (quantum) algorithm, on the other hand, can factor numbers in time: $t \approx (\ln n)^2 (\ln \ln n) (\ln \ln \ln n)$. This is polynomial time algorithm, which is in practice [6]:

number of digits of the argument	Classical computer	Quantum computer
130	one week	one week
400	10^9 years	1 year

On the other hand, quantum computation provides novel techniques to generate a shared private key wih perfect confidentiality, regardless the computational power (classical or quantum) of the adversaries. Such techniques are referred to as *quantum key distribution* protocols. [2]

3 Quantum cryptpgraphy

It is impossible to establish a secret key with conventional communications, and so key distribution has relied on the establishment of a physically secure channel ("trusted couriers") or the conditional security of "difficult" mathematical problems in public key cryptography. However, provably secure key distribution becomes possible with quantum communications. In this procedure the key is distributed over the quantum channel and not the encrypted message. That is why we need two channels between Alice and Bob. One public channel for transmission of encrypted messeage or cryptogram and another channel which, is called quantum channel, and used for key distribution. Hence, a more accurate name is quantum key distribution (QKD). The most obvious security feature of QKD is that it is impossible to "tap" single quantum signals in the conventional sense. The eavesdropper's activities produce an irreversible change in the quantum states ("collapse of the wavefunction") before they are retransmitted to the intended recipient. These changes will introduce an anomalously high error rate in the transmissions between the sender and intended recipient, allowing them to detect the attempted eavesdropper. [1]

3.1 Basic concepts in quantum computation

Consider the two binary strings: $011, 111$. The first one can represent, for example, the number 3 (in binary) and the second one the number 7.

A qubit is a *quantum* system in which the Boolean states 0 and 1 are represented by a prescribed pair of normalised and mutually orthogonal quantum states labeled as $\{|0\rangle, |1\rangle\}$. The two states form a "computional basis" and any other state of the qubit can be written as a superposition $\alpha|0\rangle + \beta|1\rangle$ for some α and β such that $|\alpha|^2 + |\beta|^2 = 1$. A qubit is typically a microscopic system, such as an atom, a nuclear spin, or a polarised photon. A collection of n qubits is called a quantum register of size n.

We shall assume that information is stored in the registers in binary form. For example, the number 6 is represented by a register in state $|1\rangle \otimes |1\rangle \otimes |0\rangle$. A quantum register of any size can also store individual numbers simultaneously. If we take the first qubit and instead of setting it to $|0\rangle$ or $|1\rangle$ we prepare a superposition $1/\sqrt{2}\,(|0\rangle + |1\rangle)$ then we obtain

$$\frac{1}{\sqrt{2}}\,(|0\rangle + |1\rangle) \otimes |1\rangle \otimes |1\rangle \equiv \frac{1}{\sqrt{2}}\,(|011\rangle + |111\rangle) \equiv \frac{1}{\sqrt{2}}\,(|3\rangle + |7\rangle)\,.$$

This means that this quantum register, when measured, can store number 3 or 7, each with the probability of 50%.

These preparations, and any other manipulations on qubits, have to be performed by unitary operations. A *quantum logic gate* is a device which performs a fixed unitary operation on selected qubits in a fixed period of time and a *quantum network* is a device consisting of quantum logic gates whose computational steps are synchronised in time. The outputs of some of the gates are connected by wires to the inputs of others. The *size* of the network is the number of gates it contains.

The most common quantum gate is the *Hadamard gate*, a single qubit gate H performing the unitary transformation known as the Hadamard transformation. It is defined as

$$\widehat{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \widehat{H}|x >= (-1)^x\,|x\rangle + |1-x\rangle. \tag{5}$$

The matrix is written in the computational basis $\{|0\rangle, |1\rangle\}$ and the diagram, on the right side of the matrix representation (previous page), provides a schematic representation of the gate H acting on a qubit in state $|x\rangle$, with $x = 0, 1$.

We will need another single qubit gate- the phase shift gate ϕ defined as $|0\rangle \to |0\rangle$ and $|1\rangle \to e^{i\phi}|1\rangle$, or in matrix notation:

$$\widehat{\phi} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \qquad \widehat{\phi}|x\rangle = e^{ix\phi}|x\rangle. \tag{6}$$

The Hadamard gate and the phase gate can be combined to construct the following network (of size four), which generates the most general pure state of a single qubit:

$$\left(\widehat{\frac{\pi}{2}+\phi}\right)\widehat{H}\widehat{(2\theta)}\widehat{H}|0\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle. \tag{7}$$

Consequently, the Hadamard and phase gates are sufficient to construct any unitary operation on a single qubit. [2]

3.2 Quantum key distribution

To understand QKD we must first move away from the traditional key distribution, we should have in mind a more symmetrical starting point, in wich Alice and Bob initially generate their own, independent random number sets, containing more numbers than they need for key material that will ultimately share. Next, they compare these sets of numbers to get a shared subset, which will become the key material. Alice prepares a sequence of tokens, one kind of a "0" and a diffrent kind for a "1", and sends a token to Bob for each bit in her set. Bob proceeds through his set bit-by-bit in synchronisation with Alice, and compares Alice's token with his bit, and replies to Alice telling her whether the token is the same as his number (but not the value of his bit). With Bob's information Alice and Bob can identify the bits they have in common. They keep these bits, forming the key, and discard the others. If one of Alice‘s tokens fails to reach Bob this does not spoil the procedure, because it is only tokens that arrive which are used in the process.

The obvious problem with this procedure is that if the tokens are classical objects they carry the bit values before they are observed by Bob, and so they could be passively monitored by Eve (an eavesdropper). However, we shall now see that it is possible to generate a secure key if the tokens are quantum objects. We shall describe the B92 QKD protocol in terms of the preparation and measurement of states in a two-dimensional Hilbert space such as that of a particle with spin 1/2. The spin operators $\sigma_1, \sigma_2, \sigma_3$, obey the algebra

$$[\sigma_i, \sigma_j] = 2i\varepsilon_{ijk}\sigma_k, \tag{8}$$

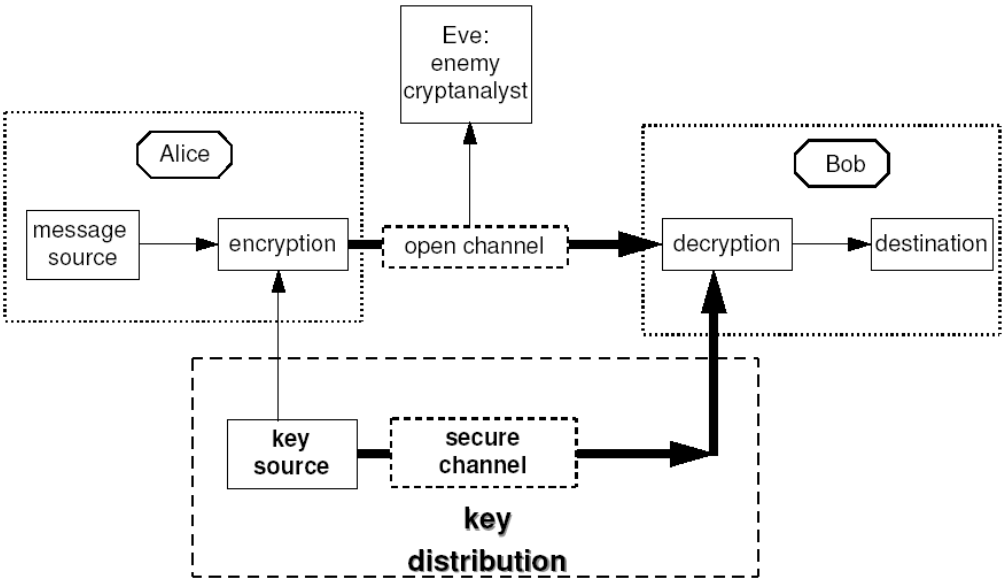


Figure 1: Key distribution in quantum cryptography. The key is transmited over the secure or quantum channel. [3]

and we may introduce a basis of states with spin-up ($|\uparrow\rangle$) or spin-down ($|\downarrow\rangle$) along the z-axis:

$$\begin{aligned} \sigma_3 \left|\uparrow\right\rangle &= \left|\uparrow\right\rangle \\ \sigma_3 \left|\downarrow\right\rangle &= -\left|\downarrow\right\rangle \end{aligned} \tag{9}$$

satisfying the orthonormality relations. From these states we can also make eigenstates with spin-up or spin-down along the x-axis:

$$\begin{aligned} \sigma_1 \left|\rightarrow\right\rangle &= \left|\rightarrow\right\rangle \\ \sigma_1 \left|\leftarrow\right\rangle &= \left|\leftarrow\right\rangle, \end{aligned} \tag{10}$$

where $|\rightarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right)$ and $|\leftarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle - |\downarrow\rangle\right)$.

A measurement in quantum theory is a projection operator in Hilbert space. A measurement for spin-down along the z-axis is represented by projection operator P. The result of a measurement P on a state $|\Psi\rangle$ is given by the "collapse of the wavefunction". Thus, the outcome of a measurement in quantum mechanics is, in general, only predictable with some probability.

For the B92 protocol Alice has two non-orthogonal state preparations: $|\uparrow\rangle$ or $|\rightarrow\rangle$; and Bob can make two non-orthogonal measurements: $P_{|\downarrow\rangle}$ or $P_{|\leftarrow\rangle}$. The "pass" probabilities of the various preparation-measurement combinations are given in this table:

	$\lvert\uparrow\rangle$	$\lvert\rightarrow\rangle$
$P_{\lvert\downarrow\rangle}$	0	0.5
$P_{\lvert\leftarrow\rangle}$	0.5	0

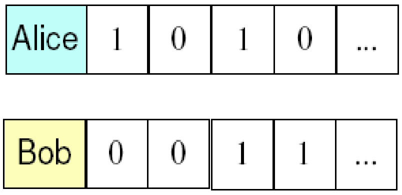
In the first step of the B92 protocol (see Figure 2) Alice and Bob generate their own independent sets of random numbers. In step 2 they proceed through their sets bit-by-bit in sychronisation, with Alice preparing a state for each of her bits:

bit	state
0	$\lvert\uparrow\rangle$
1	$\lvert\rightarrow\rangle$

Alice sends each state over a quantum channel to Bob. The quantum channel is a transmission medium that isolates the quantum state from interactions with the environment. Bob takes a measurement of each state he recieves, according to the value of his bit:

bit	measurement
0	$P_{\lvert\leftarrow\rangle}$
1	$P_{\lvert\downarrow\rangle}$

and records the result ("pass"= Y, "fail"=N).



Alice	1	0	1	0	...
Bob	0	0	1	1	...

Figure 2: First step of the B92 protocol, where Alice and Bob generate their sets of random numbers. [3]

Note that Bob will never record a "pass" if his bit is different from Alice's, and that he records a "pass" on 50% of the bits that they have in common. In Figure 2 we see that for the first and fourth bits Alice and Bob had different bit values, so that Bob's result is definite "fail" in each case. However, for bits two and three, Alice and Bob have the same bit values and the protocol is such that there is a probability of 0.5 that Bob's result is a "pass" in each case. Of course, we cannot predict which one will be a "pass", but the chances are that one will pass and the other fail. In step 4 Bob sends a copy of his results to Alice (but not the measurement that he made on each bit). He may send this information over a public channel which may be subject to eavesdropping. But this information is meaningless for Eve, becasue she still does not know the values of the bits. Now Alice and Bob retain only those bits for which Bob's result was "Y" and these bits become the shared key material.

(For example in Figure 2 the third bit can become the first bit of the shared key). They continue with this procedure untill they share enought bits, which compose the shared key. [3]

3.3 Eavesdropping on B92

We shall now approach the B92 protocol from Eve's perspective to see why it is secure. So, we should set out in detail what it is that Eve wants to accomplish, what knowledge she may supposed to have, and what she can do to the quantum and public channels. Eve could simply stop any communications between Alice and Bob by disrupting the quantum channel. But the scenario that we should have in mind is that it is much more rewarding for Eve to acquire information about Alice's and Bob's communications without being detected. We shall assume that Eve knows the possible state preparations and measurements available to Alice and Bob, but of course no knowledge of their initial random number sets.

We should consider what happens if Eve makes her own measurements (projections) on Alice's states and sends the results to Bob. Eve faces an immediate difficulty because the projection operators corresponding to Alice's two state preparations do not commute; $\left[P_{|\uparrow\rangle}, P_{|\rightarrow\rangle}\right] \neq 0$.

We shall restrict ourselves to an illustrative example, in which Eve makes the same projection , $P_{|\uparrow\rangle}$, on every state that Alice transmits, recording the result as "0" if the result is a "pass" and as a "1" if the result is a "fail". Eve then sends the resulting state on to Bob. This tactic allows all of Alice's "0" bits to pass this test, but it also erroneously passes 50% of Alice's "1" bits, giving Eve only a 66.6% probability of correctly identifying a "0". On the other hand, Eve can with certainty identify the 25% of Alice's initial sequence which are the "1" states that fail her test. But the nature of quantum measurements is such, that Eve irreversibly alters all of Alice's "1" states so that 50% of them are $|\uparrow\rangle$-states and the other 50% are $|\downarrow\rangle$-states when they reach Bob. Now, if Bob tests either of these states with his "0"-measurement there will be a 50% probability that the state will pass, which is in conflict with 0% probability of this happening for Alice's $|\rightarrow\rangle$ state, in the absence of eavesdropping. There is a bias introduced into Bob's results: more than 50% of his results are "0"s.

The result of Eve's activities is that she has only reliably identified Alice's "1"s, at the expense of introducing an error between Alice's and Bob's key material. Thus, Alice and Bob can sacrifice a portion of their key to test the error rate. If the rate is found to be high, they will know that Eve has been listnening and they would not use the key material.

Perhaps the most obvious way to implement the QKD quantum channel is with single-photon polarisation states, such as the preparation of vertical and linear-diagonal or right-handed-circular polarisations, and the measurement of horizontal linear and linear-diagonal or left-handed-circular polarisations. [3]

3.4 Phase encoded systems

However, another set of single-photon states, which we shall call "phase" states, have the algebraic properties required for quantum cryptography. If Alice and Bob use the phase angles $(\phi_A, \phi_B) = (0, 3\pi/2)$ for their "0" bits (respectively) and $(\phi_A, \phi_B) = (\pi/2, \pi)$ for their "1" bits they have an exact representation of B92. They both have identical interferometers with a short path and a long path with one output port of Alice's interferometer optically coupled to one of the input ports of Bob's. In this interferometers we have two beamspliters, and two mirrors. Between the mirrors in each interferometer we have phase modulators.

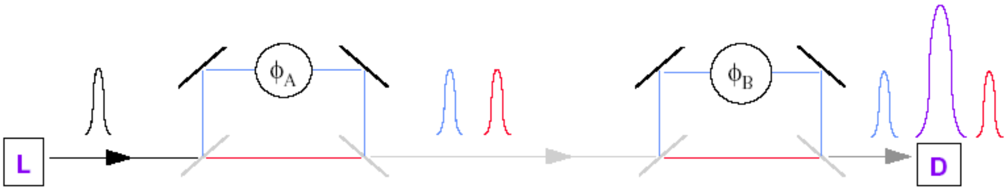


Figure 3: A time-multiplexed version of the interferometer constructed from two smaller interferometers. [3]

A photon injected into one of the input ports of Alice's interferometer from the pulsed laser source ("L" in Figure 3) therefore has a 50% probability of entering Bob's interferometer, in a wave packet that is a superposition of two pieces that are seperated in time by ΔT. One component corresponds to taking the short path, and delayed component is the one which took the long path. On entering Bob's interferometer each component of the wave packet is again split into a short component and a long component, so that at each output port there are three "time windows" in which the photon may arrive. The first of these corresponds to the short-short propagation, which is followed after a delay of ΔT by the central component comprising the short-long and long-short propagation, and finally, after a further time ΔT, the delayed time window corresponds to the long-long- propagation. There is no interference in short-short or long-long propagations, so the probability that the photon arrives in either of these time windovs is 1/16 (we assume 50/50 beamsplites and lossless mirrrors). Because Alice and Bob can control their long paths with their adjustable phases ϕ_A or ϕ_B, respectively, the probability that the photon emerges in the central time window at the detector ("D" in figure 3) in the output port is

$$P = \frac{1}{16}\left(1 + \cos\left(\phi_A - \phi_B\right)\right). \tag{11}$$

Note that within a factor of four (only a quarter of all photons reach the detector, other are lost in second beamspliter in each interferometer) this expression is almost identical with photon arrival probability for the version of B92. The "pass" probabilities are smaller here, but ratios of the probabilities are the same. Thus, by sacrificing a factor of four in data rate, this interferometers can be used to implement the QKD based on single-photon interference.

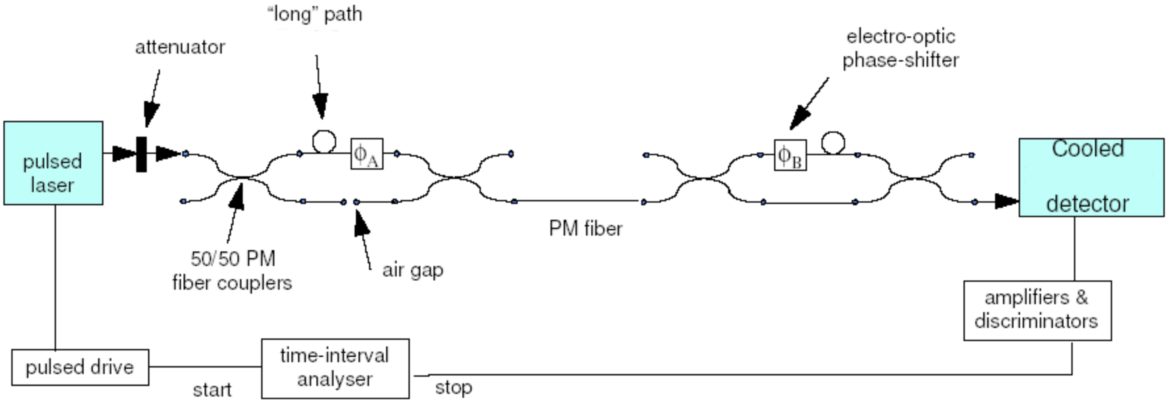


Figure 4: Shematic representation of the optical system. [3]

Instead of beamspliters it is more convenient to use 50/50 fiber couplers (figure 4). Each coupler has two input and two output legs: a photon entering on one leg has 50% to emerge from either of the output legs. No mirrors are required because the output fiber legs from the first coupler convey the photons to the input legs of the second coupler via a long fiber path or a short path. One of the output legs of Alice's interferometer is connected by a long optical fiber path to one of the input legs of Bob's interferometer. Finally photons emerge from one of the output legs of Bob's interferometer into a fiber that is connected to the cooled detector. We also included an air-gap in Alice's short path so as to adjust the lengths of the two interfering paths to be equal.

A lineary polarised singel–photon is generated by electrical pulse. The electrical pulse is also the start signal for the time-interval analyzer. The detector acts as the stop signal. The detector send electrical pulse to the time-interval analyzer when the photon is detected. This is how we can get arrival times for photons. Figure 5 shows a time spectrum of photons arrival times. The seperation of the different paths is clearly visible, as the width of the laser pulse. The unequal height of the short-short and long-long peaks is due to the attenuation in the phase modulators. The photons "lost" in the prompt or the delayed time windows are useful to test for highly invasive Eve [7].

To turn this optical system into a QKD device we place it under the control of two

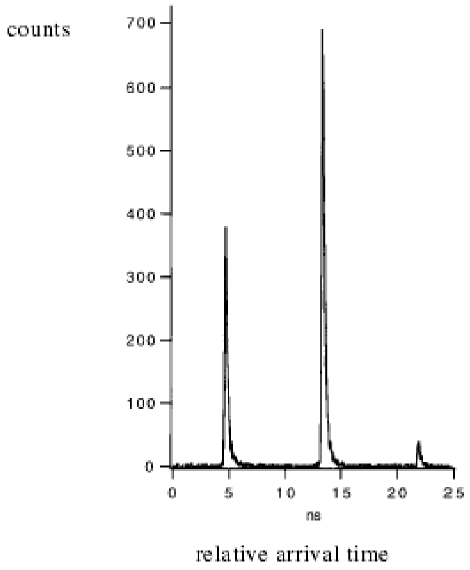


Figure 5: Time-of-arrival spectrum of single photons propagating through the fiber interferometer of Figure 4. The leftmost peak corresponds to photons that travelled by both short paths. The number of the photons in the central peak varies with the difference of the phases in each interferometer because of interference between the short-long and long-short paths. [3]

personal computers: one to control the overall timing and to set Alice's phases, and the other to set Bob's phases and record his results (see Figure 6). The computers are linked together, forming the public channel, in order to initialize their activities and to perform the results-transfer step of the QKD. A key sending procedure starts with Alice's and Bob's computers first generating independent sets of random bits. Key sending starts under the control of Alice's master timer. During this time the voltage on each phase modulator is set. When the laser is pulsed the detector gate is opened and the output of the detector in the central time window records the result. The procedure is then repeated with the next bit, and so on. At the end of this procedure, Bob's computer has a file recording the bit number, the bit value and whether the detector fired or not ("hit" or "miss"). Then Alice's computer receives over the public channel a file from Bob of the "hit" or "miss" status for each bit number. The probability for "hit" is denoted by the equation (11).With this information Alice and Bob retain only the bits corresponding to "hits" which become the key material. More sets of bits are generated and sent until a long enough key is built up to encrypt the message that is to be sent. [3]

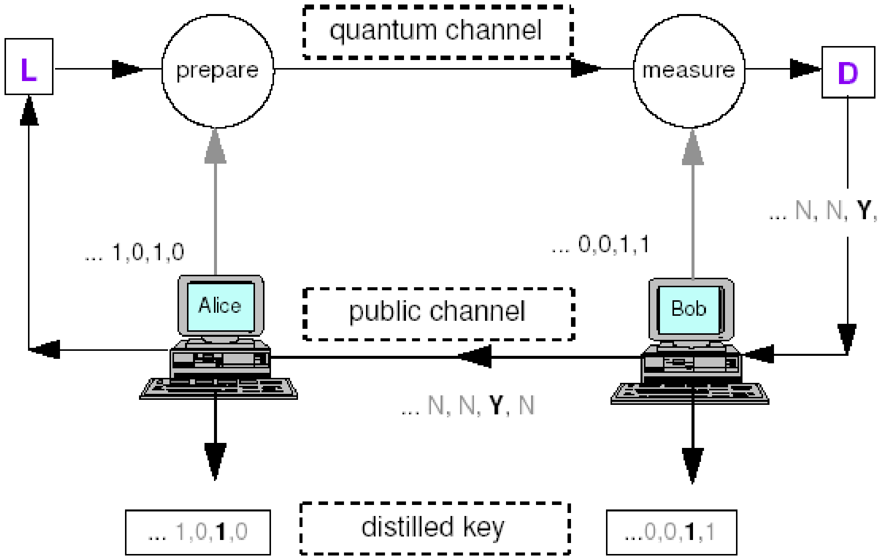


Figure 6: Shematic representation of the complete QKD system. Computer control systems prepare and measure single photons, produced at the laser "L" and detected at the detector "D", using the optical system of Figure 5. The reconcilation of the results occours over public channel between the two computers. [3]

4 Practical implementations of QKD

For photons the quantum communication channel can either be free space or optical fibers-special fibers or the ones used in standard telecommunication. The communication channel is thus not really quantum. What is quantum are the information carriers. Perhaps the most obvious way to implement the QKD quantum channel is with single-photon polarization states. Light is guided in optical fibers thanks to the refraction index profile $n(x, y)$ across the section of the fibers. Over the last 25 years, a lot of effort has been made to reduce transmission losses- initially several dB per km, and nowadays the attenuation is as low as 2 dB/km at 800 nm wavelength, 0.35 dB/km at 1320 nm, and 0.2 dB/km at 1550 nm (see Figure 7). Unit dB actually means: $dB = 20 \log_{10} \left(\frac{A}{A_0} \right)$. Here A denotes the amplitude of the signal and A_0 the amplitude of the reference signal. For example $6dB$ means that the ratio between the amplitudes of the signal and the reference signal is approximately $\frac{1}{2}$. So the unit dB/km tells us the reduction of the signal over the distance of one kilometer.

Although telecommunication based on optical fibers is very advanced nowadays, such channels may not always be available. Hence, there is also some effort in developing free space communication systems-not only for classical data transmission

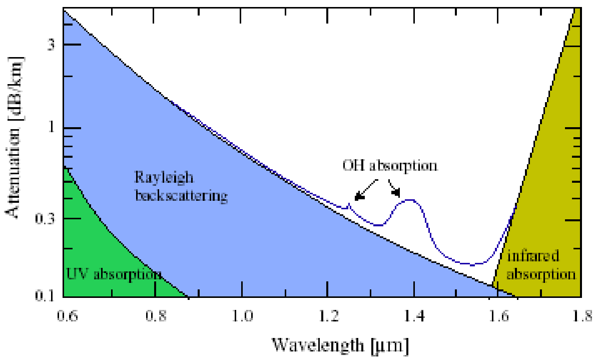


Figure 7: Transmission losses versus wavelength in optical fibers. Electronic transitions in SiO_2 lead to absortion at lower wavelenghts, exitations of vibrational modes to losses at higher wavelenghts. Superposed is the absorption due to Rayleigh backscattering and to transitions in OH groups. [3]

but for quantum cryptography as well. Transmission over free space advantages compared to the use of optical fibers. The athmosphere has a high transmission window at a wavelength of around 770 nm (see Figure 8) where photons can easily be detected using commercial high efficiency photon counting detectors. Furthemore, the athmosphere is only weakly dispersive at these wavelengths. It will thus not alter the polarization state of a photon. [4]

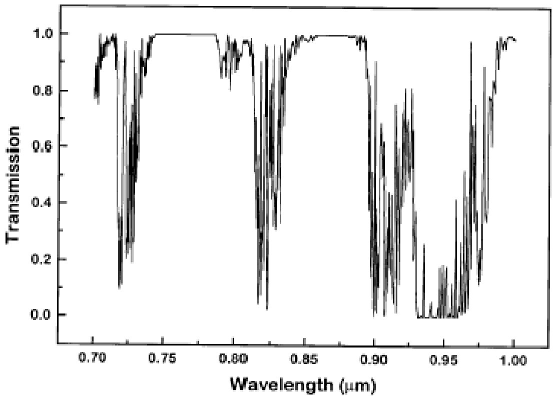


Figure 8: Transmission losses in free space. Note that there is a low loss window at around 770 nm. [3]

5 Conclusion

Quantum cryptography could be the first application of quantum mechanics at the single quanta level. Experiments have demonsrated that keys can be exchanged over distances of a few tens of kilometers (see for example Figure 9) at rates at least of the order of a thousand bits per second. There is no doubt that the technology can be mastered and the question is not whether quantum cryptography will find commercial applications, but when. Present quantum crptography is still very limited in distance. These days public key systems occupy the market and every so often, classical ciphersystems are broken. This would be impossible with properly implemented quantum cryptography. We can look forward to an exciting future for QKD with many possibilities for future theoretical, experimental and applied phisics research.

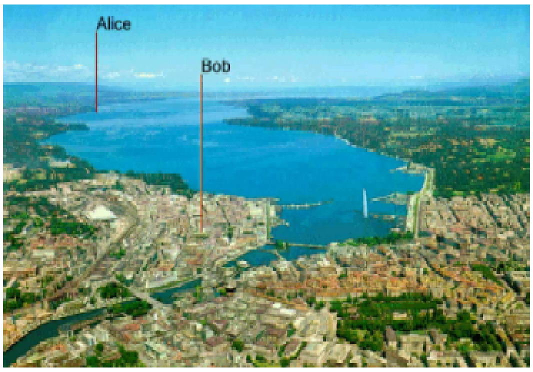


Figure 9: Geneva and lake Geneva. The optical fiber cable used for quantum cryptography experiments runs under the lake, between the town about 23 km north of Geneva, and the centre of the city. [4]

References

[1] D. Boukwmeester, A. Ekert, A. Zeilinger, *The physics of quantum information*, Springer-Verlag Berlin Heidelberg (2000).

[2] A. Ekert, P. Hayden, H. Inamori, *Basic concepts in quantum computation*, quant-ph/0011013 (2001).

[3] R. J. Huges, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, M. Schauer, *Quantum Cryptography*, quant-ph/9504002 (1995)

[4] N. Gisin, G. Ribordy, W. Tittel, Hugo Zbinden, *Quantum Cryptography,* quant-ph/0101098 (2005)

[5] http://www.theory.caltech.edu/people/preskill/ph229/

[6] Seminar: Quantum computing, G. Resman (2001)

[7] C.H. Bennett, *Quantum cryptography using any two nonorthogonal states,* Phys. Rev. Lett. **68,** 3121 (1991)