Bachelor Thesis

Quantum Cryptography

Petra Pajic

28.09.2013

Bachelor Thesis
for the degree of
Bachelor of Science
at the
University of Vienna

universität
wien

assisted by

ao. Univ.-Prof. i.R. Dr. Reinhold A. Bertlmann

Contents

1 Introduction

Since the beginning of the twentieth century, physicists have followed with great interest the developments in quantum physics. Even people who never had the pleasure of attending a quantum mechanics course are fascinated by the often bizarre behaviour which differs from classical observations. For example, almost everyone has heard at least of one of the famous quotes concerning quantum mechanics. These include Niels Bohr's quote "Those who are not shocked when they first come across quantum theory cannot possibly have understood it" and Albert Einstein's claim that "God does not play dice".
Another reason for the great attraction of this theory is that one has to give up the classical way of thinking, in order to get an idea of the concept of quantum physics. Otherwise, it would not be possible to explain, for instance, quantum entanglement.
There is a set of rules that belongs to quantum physics which cannot be fully understood by everyday physics. For example:

- The no-cloning theorem states that one cannot create a copy of an unknown quantum state.
- One cannot measure a system without perturbing it.
- The uncertainty principle states that one cannot simultaneously measure complementary variables (such as position and momentum of a particle) with arbitrarily high precision.

The given examples have one thing in common: They conclude what cannot be done [1]. This leads to a negative viewpoint of quantum mechanics. But on closer inspection, it turns out that these properties have their positive sides.
Quantum cryptography is the best example that these "drawbacks" can be turned into useful applications. But what exactly is quantum cryptography?

2 History of Cryptography

Cryptography (from Greek *kryptós* "hidden" and *gráphein* "writing")[2] is the art of creating secure codes, whereas cryptanalysis deals with breaking these codes. These two fields belong to cryptology, the science of secure communication [3].
Ancient civilisations, including Mesopotamians and ancient Egyptians, early realised the importance of communicating securely. They have been aware of the threat of revealing precious secrets to enemies. Throughout the years, many techniques of cryptography were developed to avoid that confidential information falls into the wrong hands [4].
Cryptography can be divided into two methods of encryption, known as transposition and substitution.
In transposition, the order of letters in a plaintext, which is the technical term for the message before being encrypted into a ciphertext, is rearranged by a certain permutation. A famous example for this method is called scytale, which represents the first ever military cryptographic device. It was used by Spartans military commanders around the fifth century BC. The scytale consists of a cylinder with a strip of leather or parchment wound around it. On this strip a message is written, which can only be read correctly if one uses a cylinder with the same diameter. Otherwise, it appears to be a list of random letters.

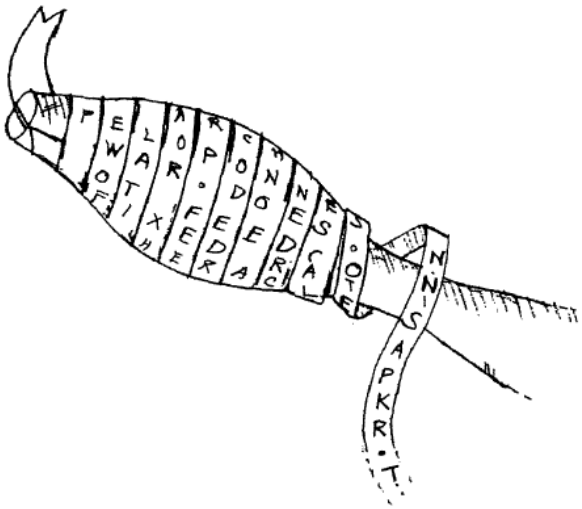

Figure 1: The scytale is the first military cryptographic device used by Spartans. [3]

In transposition each letter is rearranged in a different order, but its identity is left unchanged. In contrast to that, in substitution each letter changes its identity, but keeps its position.
A simple letter substitution was used by Julius Caesar for military purposes. In his message, each letter was replaced by the letter that followed three places further down the alphabet. Therefore, the letter A is substituted by D, B by E, and so on. Using the Caesar substitution, for example the word "folk" transforms into "iron". Note that this process, where the alphabet is shifted a certain number of places (not just three), is called Caesar cipher.

3 Classical Cryptography

Nowadays, the security of a cryptogram is not dependent on the secrecy of the encryption and decryption process, but rather on the secrecy of the key. The key must contain randomly chosen and sufficiently long string of bits in order to guarantee that it is impossible to unlock the cryptogram without the key. This demand is softened in practice. The idea is that the valuable information must remain secret at least as long as the time required to break the code [1].
In order to explain the following cryptosystems, it is convenient to introduce Alice and Bob, two parties who want to communicate secretly, as well as Eve, the unauthorized eavesdropper.
One distinguishes between two cryptosystems: the symmetrical and the asymmetrical cryptosystem.

3.1 Symmetrical (Secret-Key) Cryptosystem

The symmetrical cryptosystem shares the key in secret, therefore it is also known as secret-key cryptosystem. It uses a single key for both encryption and decryption. The "one-time pad" belongs to this category and was invented by the American engineer Gilbert Vernam in 1917. In this cryptosystem, Alice adds a randomly generated key to the plaintext and receives a ciphertext. This scrambled message is sent to Bob, who decrypts the ciphertext by subtracting the same key. The best way to illustrate the Vernam's one-time pad scheme is by the following example.

Using a simple digital alphabet with capital letters

A	B	C	...	...	X	Y	Z
01	02	03	...	...	24	25	26

Alice sends the message "Bertlmann" to Bob and obtains during the encryption process the ciphertext:

Alice	Encryption								
Message	**B**	**E**	**R**	**T**	**L**	**M**	**A**	**N**	**N**
Plaintext	02	05	18	20	12	13	01	14	14
Key	26	07	13	05	02	11	03	21	10
Ciphertext (mod 26)	02	12	05	25	14	24	04	09	24

Note that the ciphertext is as random as the key. Consequently, they both do not contain any information.

The ciphertext is now sent to Bob, who decrypts the message by subtracting the same key:

Bob	Decryption								
Ciphertext	02	12	05	25	14	24	04	09	24
Key	26	07	13	05	02	11	03	21	10
Plaintext (mod 26)	02	05	18	20	12	13	01	14	14
Message	**B**	**E**	**R**	**T**	**L**	**M**	**A**	**N**	**N**

Years later it was shown that this cryptosystem provides perfect secrecy as long as the key is truly random and has the same length as the message. Furthermore, the key can be used only for a single encryption - hence the name "one-time pad" [5]. Although this classical cryptosystem is truly unbreakable, there are still drawbacks. The main problem is the key distribution. Alice and Bob have to use a very secure and reliable channel in order to share the key.
As already mentioned, the key has to be renewed for every single message. Otherwise, Eve could gain too much information after a certain amount of time. Repeating this whole procedure for every single key would become far too expensive.

3.2 Asymmetrical (Public-Key) Cryptosystem

The alternative method to symmetrical cryptosystem is the asymmetrical cryptosystem, which is often referred to as public-key cryptosystem. In contrast to the first method, the public-key cipher uses different keys for the encryption and decryption.
In 1978, the RSA encryption system was developed, the first implementation of the public-key cryptography technique. It was named after its inventors Ronald Rivest, Adi Shamir and Leonard Adleman [6] and is still widely used.

RSA works as follows:
Alice chooses a private key that she uses to compute a public key. Any interested party has access to this public key. If for instance Bob wants to securely communicate with Alice, he will use the public key to encrypt his message. He sends the encrypted message to Alice who decrypts it with the private key. Without knowing the private key, Eve cannot gain any valuable information, because knowledge of the public key will not help in decryption. Only the person with the private key, in this case Alice, can unlock the message.
Using the following padlock analogy, makes the method of asymmetric cryptography even clearer. Anybody can lock a padlock. However, only the person who has the key can open it.

Imagine that Alice can produce many copies of open padlocks. These open padlocks can be interpreted as the public key. Bob who wants to send Alice a private message receives such an open padlock. Once the padlock is locked only Alice can access the data, because only she has the correct key. Obviously, Alice's key can be viewed as the private key [4].
A big advantage of public-key cryptosystems is that the key distribution problem does not appear. Over the last decades, these cryptosystems have become very popular. For example, parts of the Internet security are based on these systems. In theory, the process of the public-key cryptography technique seems simple. Nevertheless, it took some years to find a mathematical function that fulfils the needed criteria. The idea is to use one-way functions. For example, it is easy to compute the function $f(x)$ knowing the variable x. But the opposite direction, computing x from $f(x)$, is more difficult. In this context, the word "difficult" is interpreted as follows: the time needed to do a task grows exponentially with the number of bits in the input. It is intuitively clear that calculating 61×89 is much faster than finding the prime factors of 5429. However, the problem can be easily solved, if some additional information is given, for instance, knowing that 61 is one of the prime factors of 5429.
The major disadvantage of this system is that the security of RSA depends on unproven mathematical assumptions, namely on the difficulty of factorising large integers. Until now, it has not been possible to prove that an algorithm, which could factorise numbers fast enough, does not exist. Finding such an algorithm would cause that the whole security system collapses. For example, electronic money could become worthless overnight [1]. Indeed, recent developments in quantum computation have shown that it will be eventually possible to build quantum computers. In principle, these machines factorise much faster than classical computers [7]. Consequently, the security of RSA systems is dependent on the slowness of technological progress. There is no other way than turning to secret-key cryptosystems. As mentioned above, secret-key cryptosystems suffer from a major flaw: key distribution. However, quantum cryptography brings a new way of solving this problem.

4 Quantum Key Distribution

Because of the progress in quantum physics, cryptographers have to think of new methods to ensure security in communication, in particular when quantum computers become reality. It turns out that exactly the theory, that caused the need of a new cryptosystem, is the answer to the problem.
As already discussed, secret-key cryptosystems transmit a message with proven and absolute security. The only problem is distributing the key securely. But quantum cryptography enables that secret-key cryptosystems, as the Vernam one-time pad scheme, work.
Quantum cryptography makes it possible that two parties, in this case Alice and Bob, share a random key in a secure way. Therefore, the notion "quantum key distribution" is more accurate than "quantum cryptography".

In quantum key distribution, a single or entangled quantum is transmitted between Alice and Bob. Both have access to two channels: the quantum channel for the exchange of quanta and the classical public channel to verify that no eavesdropping has taken place. If Eve performs measurements on the transmitted quanta, Alice and Bob will discover the eavesdropping in the public communication. According to the rules of quantum mechanics, any measurement performed by Eve modifies the quantum state [3]. Furthermore, Eve cannot clone an arbitrary quantum state.

4.1 No-Cloning Theorem

In 1982, W.K. Wootters and W.H. Zurek published a paper with the title "A single quantum cannot be cloned" [8].
Suppose that there exists a unitary operator U_{cl} that can indeed clone an unknown quantum state of a photon or electron. This perfect cloning machine would have the following effect on an incoming photon with vertical polarisation $|\updownarrow\rangle$ and horizontal polarisation $|\leftrightarrow\rangle$:

$$U_{cl}|\updownarrow\rangle \rightarrow |\updownarrow\rangle|\updownarrow\rangle \tag{1}$$

$$U_{cl}|\leftrightarrow\rangle \rightarrow |\leftrightarrow\rangle|\leftrightarrow\rangle. \tag{2}$$

But a problem occurs when the cloning machine tries to copy a linear combination, such as $\alpha|\updownarrow\rangle + \beta|\leftrightarrow\rangle$.

Using the superposition principle and the linearity of quantum mechanics, one obtains as an output of the quantum cloner

$$\alpha|\updownarrow\rangle|\updownarrow\rangle + \beta|\leftrightarrow\rangle|\leftrightarrow\rangle. \tag{3}$$

But concentrating on the definition of cloning, one should get the following result: the original and the copy of the linear combination

$$(\alpha\,|\updownarrow\rangle + \beta\,|\leftrightarrow\rangle)(\alpha\,|\updownarrow\rangle + \beta\,|\leftrightarrow\rangle). \tag{4}$$

Obviously, the cloning machine does not give the correct result. This problem occurs due to the definition of cloning which requests that "two of the same" are equal to the square of the original state. This leads to a contradiction of the linearity of quantum mechanics.
Since quantum mechanical states are normalised, it follows:

$$\langle\updownarrow\,|\leftrightarrow\rangle = \langle\updownarrow\,|\leftrightarrow\rangle^2. \tag{5}$$

This equation is only fulfilled for $\langle\updownarrow\,|\leftrightarrow\rangle = 1$ and $\langle\updownarrow\,|\leftrightarrow\rangle = 0$. This implies that either both states must be the same or the states are orthogonal to each other. Consequently, this result does not hold for more general quantum states.
One could build a quantum cloner that copies two orthogonal states. However, this cloner would only work for this special set of states. For instance, a quantum cloner which is able to copy the states $\{|\updownarrow\rangle, |\leftrightarrow\rangle\}$ will fail for different orthogonal states, such as $\{|\nearrow\rangle, |\searrow\rangle\}$. But without further knowledge, one does not know which cloner fits the requirement.
One can conclude that it is impossible to clone an unknown state [9].

4.2 The BB84 Protocol

In 1984, the first protocol for quantum cryptography was proposed by Charles H. Bennett and Gilles Brassard, therefore the name "BB84" [10]. In the protocol, they introduced a different foundation for cryptography - not relying on mathematical complexity but rather on quantum mechanics.
The BB84 protocol uses pulses of polarised light, where each pulse contains a single photon. Alice and Bob are connected by a quantum channel, for example an optical fibre, and a classical public channel, such as a phone line or an Internet connection. In practice, it is common to use the same link for both channels. In the case of polarised photons, this would be an optical fibre, differing only in the intensity of light pulses: for the quantum channel one photon per bit and for the classical channel hundreds of photons per bit [5].
In order to provide a secure communication, Alice can choose between four non-orthogonal states. She has two bases with polarised photons:

The **horizontal-vertical basis** $\oplus$

- Horizontally polarised $|\leftrightarrow\rangle$
- Vertically polarised $|\updownarrow\rangle$

and the **diagonal basis** $\otimes$

- +45° polarised $|\nearrow\rangle$
- −45° polarised $|\nwarrow\rangle$

To transmit information, a coding system is needed. In this case, $|\updownarrow\rangle$ and $|\nwarrow\rangle$ code for 0, while $|\leftrightarrow\rangle$ and $|\nearrow\rangle$ code for 1 . Alice chooses at random one of the polarisation states for each photon and sends the corresponding state to Bob. Note that "choosing a random" is a tricky problem in practice [1]. Now, Bob measures the incoming state in one of the two bases. If Alice and Bob use the same basis, they will get perfectly correlated results. However, every time when Bob chooses a different basis than Alice, he will not get any information about the state of the photon. For instance, if Alice sends a horizontally polarised photon $|\leftrightarrow\rangle$ and Bob measures in the diagonal basis $\otimes$, he will get with a probability of 50 % either the +45° or the −45° polarised photon. Even if he finds out afterwards that he has chosen the wrong basis, he will not be able to determine which polarisation state Alice has sent.

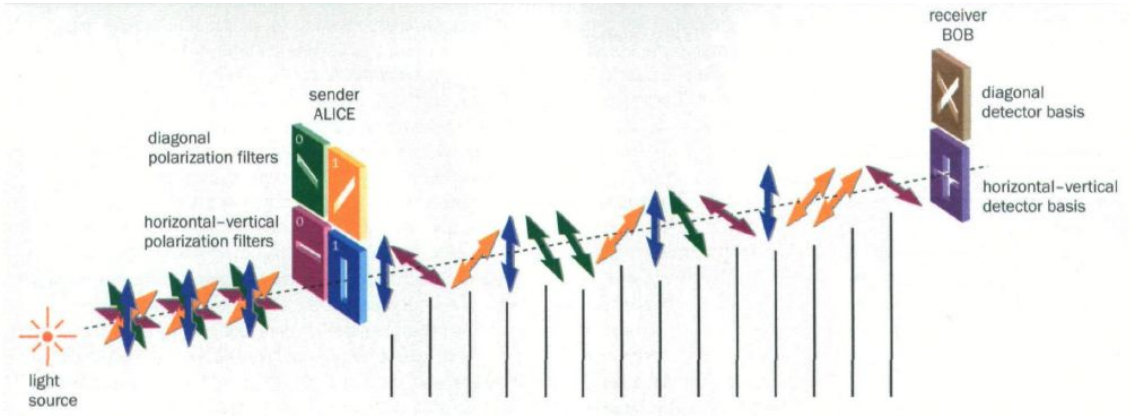

Figure 2: BB84 protocol [5]

The following steps describe the process of the BB84 protocol:

1. Alice chooses randomly both the basis and polarisation of each photon and sends the corresponding polarisation state to Bob.

2. Independently and randomly for each photon, Bob chooses one of the two bases. He either measures in the same basis as Alice and gets a perfectly correlated result or the exact opposite, he measures in the different basis than Alice and gets an uncorrelated result. Sometimes, it also happens that Bob does not register anything because of errors in the detection or in the transmission.

3. Bob obtains a string of all received bits, also called "raw key".

4. For each bit, Bob announces via the public channel which bases was used and which photons were registered. Of course, he does not reveal which result he obtained.

5. After comparing the selected bases, Alice and Bob keep only the bits corresponding to the same basis. Because both have randomly chosen the basis, they get correlated and uncorrelated results with equal probability. Therefore, about 50 % of the raw key is discarded. This shorter key is called sifted key.

6. Alice and Bob choose at random some of the remaining bits which they discard later to check the error rate. There are two main reasons why the error rate can differ from the expected value: technical imperfections in the set-up and a potential eavesdropper. To ensure a secret key, Alice and Bob must correct the errors. With the help of this procedure, they reduce Eve's knowledge of the key. The remaining string of bits is the secret key.

7. Eventually, the actual process of securely encrypting a message can begin.

Note that the secret key is truly random and neither Alice nor Bob can decide which key results, because they choose randomly between the bases.

4.2.1 Example

The following example is given to illustrate the process of the BB84 protocol. In this case $|\updownarrow\rangle$ and $|\nwarrow\!\!\searrow\rangle$ code for 0, while $|\leftrightarrow\rangle$ and $|\nearrow\!\!\swarrow\rangle$ code for 1. Note that in practice Alice and Bob will choose in half of the cases the same basis.

Alice's polar. states	$\|\nearrow\!\!\swarrow\rangle$	$\|\updownarrow\rangle$	$\|\updownarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nwarrow\!\!\searrow\rangle$	$\|\nwarrow\!\!\searrow\rangle$	$\|\updownarrow\rangle$	$\|\nearrow\!\!\swarrow\rangle$	$\|\leftrightarrow\rangle$
Alice's bit value	1	0	0	1	0	0	0	1	1
Bob's basis	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$
Bob's measured states	$\|\nearrow\!\!\swarrow\rangle$	$\|\nearrow\!\!\swarrow\rangle$	$\|\updownarrow\rangle$	$\|\nearrow\!\!\swarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nwarrow\!\!\searrow\rangle$	/	$\|\updownarrow\rangle$	$\|\leftrightarrow\rangle$
Bob's bit value	1	1	0	1	1	0	/	0	1
Same basis?	Y	N	Y	N	N	Y	/	N	Y
Bit sequence	1	/	0	/	/	0	/	/	1
Test Eve?	N	/	N	/	/	Y	/	/	N
Secret key	1		0						1

Figure 3: Alice chooses at random a polarisation state and sends it to Bob who chooses also at random a basis. After comparing their bases over a public channel, they discard bits that do not correspond to the same basis. Some of the remaining bits are used to test for Eve and are discarded as well. The retained bits form the secret key.

4.2.2 Eavesdropping

Eve's goal is to obtain as much valuable information as possible. The easiest way is to intercept a qubit (= quantum bit) which is transmitted from Alice to Bob. But Eve must send a qubit to Bob. Otherwise, he will tell Alice to disregard this measurement, because he did not receive the expected qubit. Consequently, Eve would not gain any useful information.
In the ideal case, Eve would send a qubit in its original state. But because of the no-cloning theorem which states that creating a copy of an unknown quantum state is impossible, Eve must find another eavesdropping strategy.
One of them is the intercept-resend strategy.

In this case, Eve uses the same equipment as Bob and just like him, she cannot know in which basis Alice has measured the qubit. She has no other choice but to choose the bases randomly. In 50 % of the cases, Eve will guess the correct basis and resend a qubit in the correct state to Bob. Consequently, Eve's intervention will not be noticed by the legitimate users. However, in the remaining cases, Eve will use the wrong basis as she has no information about Alice's choice. This intervention will be discovered, in half of the cases, by Alice and Bob as they get uncorrelated results.
With the help of the intercept-resend strategy, Eve will get 50 % information. But Alice and Bob will obtain a 25 % error rate in their sifted key, which reveals the presence of Eve. A more serious problem appears, if Eve applies this strategy to only a fraction of the measurements. For example, this fraction amounts to 10%, then the error rate will be approximately 2.5 %, while Eve's information will be around 5 %.
In order to appeal against such an attack, Alice and Bob use classical algorithms, first to correct the errors, and then to reduce Eve's knowledge of the final key. This process is called privacy amplification [1].

4.3 The Ekert Protocol

In 1991, Artur K. Ekert suggested a different approach for quantum key distribution [11]. His idea is based on entangled particles. With the help of Bell's theorem, it can be tested if eavesdropping has taken place. The connection between cryptography and Bell's theorem is not obvious at the first moment. Therefore, it is helpful to take a closer look at the EPR protocol.
Albert Einstein, Boris Podolsky and Nathan Rosen, known collectively as EPR, published a paper in 1935 that challenged the completeness of quantum mechanics [13]. Einstein, Podolsky and Rosen stated the following requirement for a complete theory:

Every element of a physical reality must have a counter part in the physical theory [13] .

In the EPR paper, they started from two assumptions, namely

- **Reality:** A measured quantity exists even before the quantum mechanical measurement.
- **Locality:** The measurement of a particle does not influence the reality of another particle at a distant location.

It took almost 30 years to prove that the theory of local realism is not consistent. In 1964, John Stewart Bell published his famous paper "On the Einstein-Podolsky-Rosen Paradox" [12] , where he derived an important result from the same key assumptions as in the EPR paper: Bell's theorem.

Bell's theorem represents an important comparison between quantum mechanics and classical physics. Bell showed that the principle of locality was not consistent with the local hidden variable theory as initially proposed by EPR.
He proved his theorem by creating Bell's inequalities. These inequalities are valid for correlations that can be produced by any theory obeying local realism. However, quantum mechanics predicts the violation of Bell's inequalities for certain entangled states.
Bell's inequalities have been tested in numerous experiments, including the work of Freedman and Clauser in 1972 [15] and Aspect in 1982 [16]. Furthermore, it is worth mentioning the experiment by the Zeilinger group in 1998 [17] and the latest work in 2013 [18]. All experiments have confirmed the principle of quantum mechanics rather than the theory of local realism [1, 3, 14].

The Ekert protocol, often also Einstein-Podolsky-Rosen protocol due to its direct connection to the EPR paradox, works as follows:

1. A source emits pairs of qubits in a maximally entangled state like:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|\updownarrow\rangle |\leftrightarrow\rangle + |\leftrightarrow\rangle |\updownarrow\rangle \right). \tag{6}$$

2. Alice and Bob choose randomly between three bases, obtained by rotating the horizontal-vertical basis $\oplus$ around the z-axis by angles :

$$\begin{array}{lll} \phi_1^a = 0 & & \phi_1^b = 0 \\ \phi_2^a = \frac{1}{8}\pi & \text{for Alice and} & \phi_2^b = \frac{1}{8}\pi \quad \text{for Bob.} \\ \phi_3^a = \frac{1}{4}\pi & & \phi_4^b = -\frac{1}{8}\pi \end{array}$$

3. After the transmission has taken place, Alice and Bob release publicly which basis they have chosen for each measurement. They separate the measurements into three groups:

   - **First group:** Consisting of measurements using *different* orientation of the analysers.
   - **Second group:** Consisting of measurements using the *same* orientation of the analysers.
   - **Third group:** Consisting of measurements in which at least one of them failed to register a particle.

   Note that the first group is used to test Bell's inequalities and the second group to establish a secure key, while the third group is discarded.

4. Finally, Alice and Bob announce publicly only their results of the first group. Thus, they can check if eavesdropping has taken place.
   If no eavesdropper has perturbed the system, Alice and Bob can use the measurements of the second group to obtain a secret string of bits, also known as the key.

Assuming a source that emits pairs of photons, each measurement can yield two results:

- +1 for photons that are measured in the first polarisation state of the chosen basis
- -1 for photons that are measured in the second polarisation state of the chosen basis

Revealing the basis, Alice and Bob can obtain a bit of information.
In order to test for an eavesdropper, Eve, Alice and Bob need the quantity

$$E(\phi_i^a, \phi_j^b) = P_{++}(\phi_i^a, \phi_j^b) + P_{--}(\phi_i^a, \phi_j^b) - P_{+-}(\phi_i^a, \phi_j^b) - P_{-+}(\phi_i^a, \phi_j^b), \tag{7}$$

which is the correlation coefficient of the measurements performed by Alice and Bob in the independently and randomly chosen basis. Note that for example $P_{+-}(\phi_i^a, \phi_j^b)$ denotes the probability that +1 has been obtained by Alice in the basis rotated by the angle ϕ_i^a and -1 by Bob in the basis roated by the angle ϕ_i^b.
According to the quantum rules

$$E(\phi_i^a, \phi_j^b) = -\cos\left[2(\phi_i^a - \phi_i^b)\right]. \tag{8}$$

For bases with the same orientation, in this case ϕ_1^a, ϕ_1^b and ϕ_2^a, ϕ_2^b, quantum mechanics predicts total anticorrelation. So Alice and Bob obtain $E(\phi_1^a, \phi_1^b) = E(\phi_2^a, \phi_2^b) = -1$.
The correlation coefficients for which Alice and Bob used bases with different orientation can be composed to define the quantity S

$$S = E(\phi_1^a, \phi_2^b) + E(\phi_1^a, \phi_4^b) + E(\phi_3^a, \phi_2^b) - E(\phi_3^a, \phi_4^b). \tag{9}$$

This quantity is the same S as in the generalised Bell's theorem proposed by Clauser, Horn, Shimony and Holt, better known as CHSH inequality [19]. Quantum mechanics requires

$$S = -2\sqrt{2}. \tag{10}$$

Note that the CHSH inequality is only violated if the correlation cannot be reproduced by a local hidden variable theory [20]. Consequently, it is the strongest possible inequality for two qubits. This inequality can be used to guarantee a secure key distribution.

Recalling that the legitimate users Alice and Bob have divided their measurements into three groups, they can now use their results of the first group (measurements with different orientation) to establish the value of S. If the particles were not directly or indirectly disturbed, for example by Eve, they should reproduce the result of equation (10).
This assures that the results of the second group (measurements with the same orientation) are anticorrelated and can be used to establish a secure key [3, 14].

4.3.1 Eavesdropping

In order to emphasise that Bell's theorem can indeed expose eavesdropping, one should take a closer look at an eavesdropper, Eve.
Eve gets no useful information, if she intervenes during the transmission, because at this time no information is encoded in the particles. The requested information is "formed" only after the measurements by the legitimate users and the public announcement have taken place.
One strategy may be that Eve substitutes her own prepared data for Alice's and Bob's data to misguide them. But because she does not know which orientation of the analysers the two will choose, Eve's tampering will eventually be detected. In this case, Eve's intervention will be the same as introducing elements of *physical reality* to the polarisation directions and will lower S below its quantum value [3].
Let us take a closer look at the most favourable method for eavesdropping. In this case, Eve herself prepares each particle separately giving her total control over the state of individual particles. The well defined polarisation directions may vary from pair to pair. Therefore, it is convenient to introduce the probability $p(\theta_a, \theta_b)$ with which Eve prepares Alice's particle in state $|\theta_a\rangle$ and Bob's particle in state $|\theta_b\rangle$. However, Alice and Bob will detect Eve by estimating the value of S. To verify this one writes the density operator for each operator down

$$\rho = \int_{-\pi/2}^{\pi/2} p(\theta_a, \theta_b)\, |\theta_a\rangle\langle\theta_a| \otimes |\theta_b\rangle\langle\theta_b|\, d\theta_a d\theta_b. \tag{11}$$

Rewriting Equation (9) with modified correlation coefficients, one obtains

$$\begin{aligned}\rho = \int_{-\pi/2}^{\pi/2} p(\theta_a, \theta_b)\, d\theta_a d\theta_b \, \Big(& \cos\left[2(\phi_1^a - \theta_a)\right] \cos\left[2(\phi_2^b - \theta_b)\right] \\ & + \cos\left[2(\phi_1^a - \theta_a)\right] \cos\left[2(\phi_4^b - \theta_b)\right] \\ & + \cos\left[2(\phi_3^a - \theta_a)\right] \cos\left[2(\phi_2^b - \theta_b)\right] \\ & - \cos\left[2(\phi_3^a - \theta_a)\right] \cos\left[2(\phi_4^b - \theta_b)\right] \Big) . \end{aligned} \tag{12}$$

This leads to

$$S = \int_{-\pi/2}^{\pi/2} p(\theta_a, \theta_b)\, d\theta_a d\theta_b \, \sqrt{2} \cos\left[2(\theta_a - \theta_b)\right] , \tag{13}$$

which implies

$$-\sqrt{2} \leq S \leq \sqrt{2} \tag{14}$$

for any state preparation described by the probability distribution $p(\theta_a, \theta_b)$.
The obtained result confirms the assumption that Alice and Bob will notice Eve's tampering, because the result (14) will always be smaller than the requested $|S| = 2\sqrt{2}$ [3].

5 Real-World Implementation

Although published in 1992, the first quantum key distribution experiment was demonstrated in 1989 by the IBM-Montreal group [21]. Since then, the experimental realisations have made an enormous progress. In practice, photons are the best candidates for carrying the different quantum states. The reason is that they are easy to produce and their interaction with the environment, e.g. decoherence, can be controlled. Moreover, researchers can benefit from the developments in the last three decades in optical telecommunications.
In general, there are two possibilities: the first is to use optical fibres to guide the light between two points. The other one is to establish quantum communication from a satellite down to earth or to another satellite.
As it is often the case with experimental realisations, there is a gap between theory and reality. In theory, all errors are only caused by an eavesdropper, but the situation is rather different in practice. Many factors define how well a quantum cryptography system works. These include transmission length, key generation rate and quantum bit error rate (QBER) which is the ratio of the error rate to the key rate.
Experimental imperfections may lead to uncorrelated bits. If, for example, Bob's polariser cannot distinguish perfectly between two orthogonal states, he will occasionally detect photons in the wrong channel. Another problem is to ensure that the encoded bits are maintained during transmission. For instance, a horizontally polarised photon should still be horizontally polarised by the time it reaches Bob. However, most errors are not because of photons that have been incorrectly detected, but rather due to the noise of the detectors. These errors arise when a detector registers a count, although no photon has reached the detector. These false detections are mostly of thermal origin which can produce fluctuations within seconds or minutes. To overcome this problem, a classical error correction procedure is applied which leads to a reduction of the key rate. But the real problem is to estimate the amount of information obtained by Eve. Therefore, Alice and Bob use privacy amplification which reduces Eve's knowledge to an arbitrary low level. In this procedure, several bits are combined into one in such a way that they only correlate if Alice's and Bob's initial bits are the same. The drawback of privacy amplification is that it shortens the key length and it is only possible to a certain error rate [5].

5.1 Polarisation Encoding

The first demonstration of quantum key distribution in 1989 [21] used polarised photons and free space propagation over a distance of 30 cm. Despite the small scale of the experiment, it had a strong impact. Since then, the progress in this

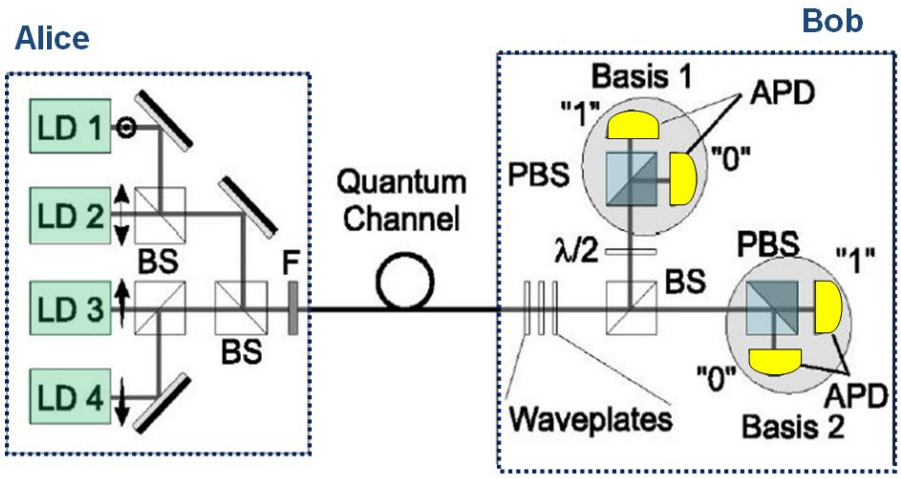

Figure 4: Set-up for a typical QC system using the polarisation of photons. Abbr.: LD = laser diode, BS = beam splitter, F = neutral density filter, $\lambda/2$ = half waveplate, PBS = polarising beam splitter, APD = avalanche photodiode [1].

new field was enormous and several groups have shown that quantum cryptography works also outside of a physics laboratory.

A typical system for quantum cryptography following the BB84 four-state protocol with polarised photons is shown in Figure 4. Alice's system consists of four laser diodes which emit photon pulses polarised at $-45°$, $0°$, $+45°$ and $90°$. The faint laser pulses are attenuated by a set of filters to reduce the average number of photons below one.

In order to illustrate how the experiment works, consider a photon which is, for example, polarised at $+45°$. It is essential that the pulses remain polarised for Bob. But the state of polarisation is arbitrarily changed when transported along an optical fibre cable. Due to the birefringence in the fibre, fluctuations in the resulting polarisation are caused and the polarisation mode dispersion leads to a reduction of the polarisation. At Bob's end, the polarisation controller must recover the initial polarisation, in this case $+45°$. If Bob chooses the horizontal-vertical basis, he will get a random outcome, because there is an equal probability of reflection and transmission at the polarising beam splitter. But if he chooses the diagonal basis, he will get a deterministic outcome.

Further experiments have shown that polarisation encoding by using optical fibres is not the best choice for quantum cryptography, because the polarisation transformation in a long optical fibre becomes unstable after a while.

This problem can be reduced by using free space systems, since air has essentially no birefringence [1, 3].

5.2 Polarisation Entanglement

An elegant alternative to the previously discussed method is quantum cryptography based on entangled photon pairs. An advantage of using photon pairs is that false detection can be easily revealed, since a detected photon implies the presence of another photon of the pair. This is beneficial because currently available single photon detectors have a high dark count rate, which is the average rate of falsely registered photons.
The set-up which is illustrated in Figure 5 resembles the already discussed system for polarisation encoding which is based on faint laser pulses.

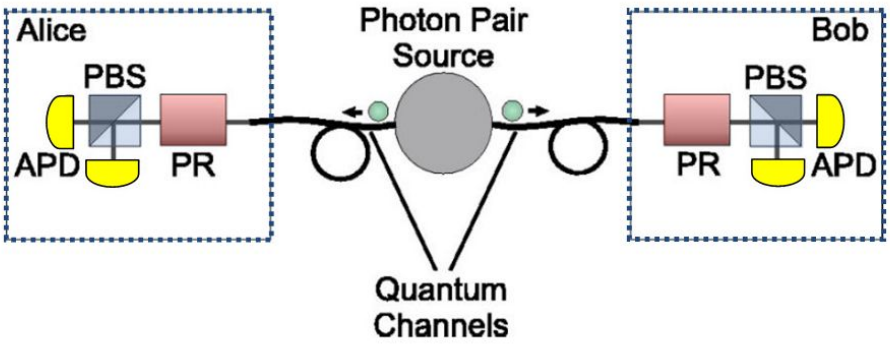

Figure 5: Set-up for a typical QC system using entangled photon pairs.
Abbr.: PR = active polarisation, PBS = polarising beam splitter,
APD = avalanche photodiode. [1]

In this quantum cryptography system a two photon source emits pairs of entangled photons towards Alice and Bob. Each photon is analysed with a polarisation beam splitter. The orientation of the beam splitter can be changed rapidly with respect to a common reference.
A significant advantage of polarisation entanglement is that analysers are simple and efficient. Nevertheless, the difficulty to keep the polarisation stable over distances of a few kilometres in optical fibres remains. However, these experiments play an interesting role in free space quantum cryptography [1] .

5.3 The "Venus von Willendorf" Experiment

In 1999, the Zeilinger group demonstrated a quantum cryptography system based on polarisation entangled photon pairs [22]. Two different protocols were implemented:

1. The first scheme is based on the Ekert protocol, but instead of using the CHSH inequality to establish the security, one utilises Wigner's inequality, another special form of Bell's inequalities. The advantage of this implementation is that each user only needs two analyser settings, while the Ekert scheme based on the CHSH inequality requires three settings of Alice's and Bob's analysers.
   The two settings of the analysers are given by $-30°, 0°$ for Alice and $0°, +30°$ for Bob, as shown in Figure 6a. The two parties vary their analysers randomly and independently which leads to four possible combinations. One combination is used to establish the key - in this case, the parallel setting (Alice = $0°$ and Bob = $0°$). The remaining three combinations allow a test of Wigner's inequality. This simplifies significantly the experimental implementations of the quantum key distribution.

2. The second scheme is a variant of the BB84 protocol with entangled photons. In this case, Alice and Bob vary their polarisers between $0°$ and $+45°$, as illustrated in Figure 6b. Whenever they choose the same orientation of their polarisers, they will receive perfectly anticorrelated results which they use for the key. Alice and Bob select at random some of the remaining bits which they discard later to evaluate the error rate.

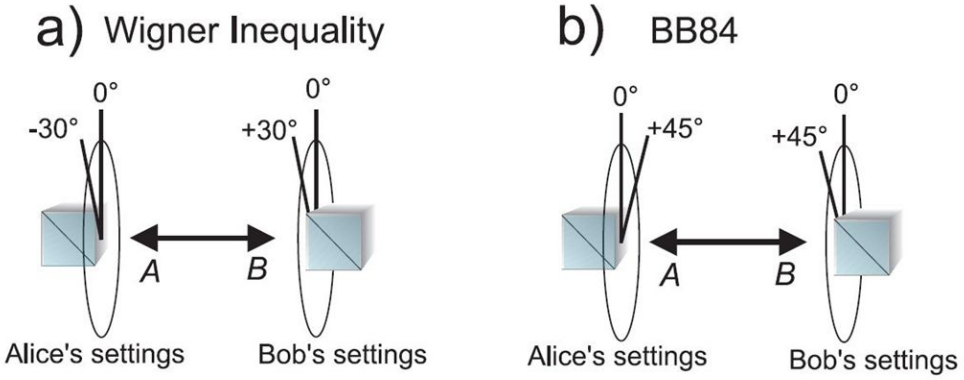

Figure 6: Setting for Alice's and Bob's analysers for a QC system based either on (a) Wigner's inequality or (b) the BB84 protocol [22].

For the experimental realisation entangled photon pairs at a wavelength of 702 nm are produced. They are transmitted, via optical fibres, to Alice and Bob who are apart by a distance of 360 m. In each station, there is an independent Rubidium clock that simply registers the photon arrival times and two channel polarisers with the channels "0" and "1". After the measurement, the coincident detections obtained at parallel settings $(0°, 0°)$, which occur in the quarter of all events, can be used for establishing the key. The other combinations of settings,

including $(-30°, +30°)$, $(-30°, 0°)$ and $(0°, +30°)$, are used to check for a possible eavesdropper by inserting the results in Wigner's inequality. In this experiment, the violation of the inequality is in agreement with the prediction of quantum mechanics and hence ensures a secure key distribution. Alice and Bob established 2161 bits of raw keys at a rate of 420 bits per second and obtained a quantum bit error rate of 3.4 %.
For the BB84 scheme, Alice and Bob have measured, in half of the cases, coincidences with parallel analysers, $(0°, 0°)$ and $(+45°, +45°)$. These results form the raw keys. After the measurement run, the legitimate users collected approximately 80000 bits of key at a rate of 850 bits per second and obtained a quantum bit error rate of 2.5 %. Alice and Bob use 10 % of the key for checking the security and the remaining 90 % of the key to implement a simple error reduction scheme. At last, Alice sends a 43200 bit large image to Bob via the one-time pad protocol. The image illustrates the "Venus von Willendorf" sculpture [1], as shown in Figure 7. This experiment represents the first full implementation of quantum cryptography based on entangled states [14, 22].

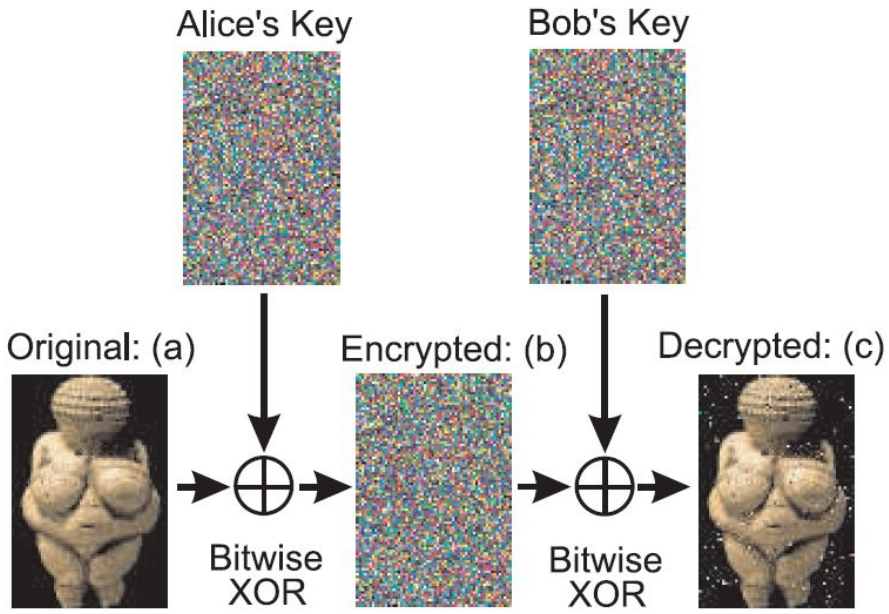

Figure 7: (a) Alice encrypts the "Venus von Willendorf" image, via bitwise XOR operation, with her key. (b) The encrypted image is transmitted to Bob. (c) Bob decrypts the visual information with his key and obtains the "Venus von Willendorf" image with few errors because of the remaining bit errors in the keys [22].

[1]The "Venus von Willendorf" figure was found in 1908 at Willendorf in Austria and is estimated to have been made between 24000 and 22000 BC.

6 Conclusion

Quantum cryptography is the most advanced technology in the area of quantum information. It is the first fundamental quantum concept that is in the process of making the transition from purely scientific research to an industrial application [23]. Thus, it is desirable to make the systems more stable and easier for the use of some potential end-users interested in secure communication, rather than in quantum mechanics. The provided information only scratches the surface of a continued developing topic [2].

This thesis gives a brief overview on quantum cryptography, starting with the history of cryptography. Even ancient civilisations realised the importance of communicating securely to avoid that precious secrets fall into the wrong hands. Two classical cryptograms are introduced which are based on two different types of key. On the one hand, there is the asymmetrical cryptosystem, which is often referred to as public-key cryptosystem. This system still dominates the markets, although the security depends on unproven mathematical assumptions. On the other hand, there is the symmetrical cryptosystem, also known as secret-key cryptosystem, which provides perfect security. But it suffers from a major flaw: the key distribution. The solution for that is quantum cryptography which makes it possible that two parties share a random key securely. Consequently, the notion "quantum key distribution" is more accurate.

The first quantum cryptography protocol was proposed by Charles H. Bennett and Gilles Brassard in 1984, therefore the name "BB84 protocol". Independently of the BB84 paper, Artur K. Ekert published the Ekert protocol which is based on entangled particles and uses Bell's theorem to test if eavesdropping has taken place.

At the moment, quantum cryptography is still limited in distance and suffers from low transmission rates. But in the last decade, lots of experiments have proven to operate outside the laboratory with a high reliability. This confirms the idea that quantum cryptography will find commercial application in the not too distant future .

To sum it up, properly implemented quantum cryptography ensures secure communication, in contrast to classical cryptosystems. But this strength of quantum cryptography might turn out to be its weakness, because this would mean that even security agencies would be unable to break quantum cryptograms [1].

---

[2] For further information on quantum cryptography and related topics, the following websites are recommended:

- http://xxx.lanl.gov/archive/quant-ph
- http://www.qubit.org/
- http://vcq.quantum.at/

References

[1] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden "Quantum Cryptography", Rev. of Mod. Phys. 74, pp. 145 - 195 (March 2002)

[2] H. G. Liddell, R. Scott "A Greek-English Lexicon", Oxford University Press (1995)

[3] D. Bouwmeester, A. Ekert, A. Zeilinger "The Physics of Quantum Information", Springer-Verlag Berlin [et al.] (2000)

[4] S. Singh "The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography", Anchor Books, New York (1999)

[5] W. Tittel, G. Ribordy, N. Gisin "Quantum Cryptography", Phys. World (March 1998)

[6] R. Rivest, A. Shamir, L. Adleman "On Digital Signatures and Public-Key Cryptosystems", MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212 (January 1979)

[7] P. W. Shor "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", (1996) arXiv:quant-ph/9508027

[8] W.K. Wootters, W.H. Zurek "A single quantum cannot be cloned", Letters to Nature, 299 (1982)

[9] W.K. Wootters, W.H. Zurek "The no-cloning theorem", Physics Today (February 2009)

[10] C. H. Bennett, G. Brassard "Quantum Cryptography: Public key distribution and coin tossing", Proc. of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore (1984)

[11] A. K. Ekert "Quantum Cryptography Based on Bell's Theorem", Phys. Rev. Lett. 67, pp. 661 - 663 (1991)

[12] J. S. Bell "On the Einstein-Podolsky-Rosen Paradox", Physics. 1 , pp. 195-200 (1964)

[13] A. Einstein B. Podolsky, N. Rosen "Can Quantum-Mechanical Description of Physical Reality be Considered Complete?", Phys. Rev. 47 (10), pp. 777 - 780 (1935)

[14] R. A. Bertlmann, A. Zeilinger "Quantum [Un]speakables: from Bell to quantum information", Springer-Verlag Berlin [et al.] (2002)

[15] S. J. Freedman, J. F. Clauser "Experimental Test of Local Hidden-Variable Theories", Phys. Rev. Lett. 28 (14), pp. 938 - 941. (1972)

[16] A. Aspect, P. Grangier, G. Roger "Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities", Phys. Rev. Lett. 49 (2), pp. 91 - 94 (1982)

[17] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, A. Zeilinger "Violation of Bell's inequality under strict Einstein locality conditions", Phys. Rev. Lett. 81, pp. 5039 - 5043 (1998)

[18] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, A. Lita, B. Calkins, T. Gerrits, S. Woo Nam, R. Ursin, A. Zeilinger "Bell violation with entangled photons, free of the fair-sampling assumption", Nature, pp. 227 - 230 (2013)

[19] J.F. Clauser, M.A. Horne, A. Shimony, R.A. Holt "Proposed experiment to test local hidden-variable theories", Phys. Rev. Lett. 23 (15), pp. 880 - 884 (1969)

[20] I. Pitowski "Quantum Probability-Quantum Logic", Springer-Verlag Berlin (1989)

[21] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin "Experimental quantum cryptography", Journal of Cryptology (5), pp. 3 - 28 (1992)

[22] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, A. Zeilinger "Quantum cryptography with entangled photons", Phys. Rev. Lett. 84, pp. 4729 - 4732 (2000)

[23] A. Poppe, A. Fedrizzi, T. Lorünser, O. Maurhardt, R. Ursin, H. R. Böhm, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, A. Zeilinger "Practical quantum key distribution with polarization entangled photons", Optics Express 12 (16), pp. 3865-3871 (2004)