

ACHIEVING UNCONDITIONAL SECURITY BY QUANTUM CRYPTOGRAPHY

Mohamed Elboukhar¹, Mostafa Azizi², Abdelmalek Azizi^{1,3}

¹dept. Mathematics & Computer Science, FSO, University Mohamed Ist, Morocco

²dept. Applied Engineering, ESTO, University Mohamed Ist, Oujda, Morocco

³Academy Hassan II of Sciences & Technology, Rabat, Morocco

elboukharimohamed@gmail.com, azizi.mos@gmail.com, abdelmalekazizi@yahoo.fr

ABSTRACT

Classical cryptography algorithms are based on mathematical functions. The robustness of a given cryptosystem is based essentially on the secrecy of its (private) key and the difficulty with which the inverse of its one-way function(s) can be calculated. Unfortunately, there is no mathematical proof that will establish whether it is not possible to find the inverse of a given one-way function. Since few years ago, the progress of quantum physics allowed mastering photons which can be used for informational ends and these technological progresses can also be applied to cryptography (quantum cryptography). Quantum cryptography or Quantum Key Distribution (QKD) is a method for sharing secret keys, whose security can be formally demonstrated. It aims at exploiting the laws of quantum physics in order to carry out a cryptographic task. Its legitimate users can detect eavesdropping, regardless of the technology which the spy may have. In this study, we present quantum cryptosystems as a tool to attain the unconditional security. We also describe the well known protocols used in the field of quantum cryptography.

Keywords: quantum cryptography, quantum key distribution, unconditional security.

1 INTRODUCTION

1.1 The Origin of the Concept of Quantum Computer

In his article [1] Richard Feynman presented an interesting idea illustrating how a quantum system can be used for computation reasons. Also the article described how effects of quantum physics could be simulated by such quantum computer. Every experience investigating the effects and laws of quantum physics is expensive and complicated. The idea of Richard Feynman was very interesting because it can be used for future research of quantum effects.

A quantum computer is a machine for computation that uses quantum mechanical phenomena, such as superposition and entanglement, to perform operations on data. The principle behind quantum computation is that quantum properties can be exploited to represent data and perform operations on these data [2]. Later in 1985, it was proved that a quantum computer would be much more powerful than a classical one [3].

A technology of quantum computers is also very different. For operation, quantum computer uses quantum bits (qubits). Quantum mechanic's laws are completely different from the laws of a classical physics. A qubit can exist not only in the states

corresponding to the logical values 0 or 1 as in the case of a classical bit, but also in a superposition state.

The major difference between quantum and classical computers is related to the memory. While the memory of a classical computer is a string of state 0 (0's) and state 1 (1's) and it can perform calculations on only one set of numbers simultaneously, the memory of a quantum computer is a quantum state that can be a superposition of different numbers. A quantum computer can do an arbitrary reversible classical computation on all the numbers simultaneously and performing a computation on many different numbers at the same time interferes all the results to get a single answer.

For example as in Fig. 1.1 a quantum computer with 4 qubits gives 24 superposition states. Each state would be classically equivalent to a single list of 4 1's and 0's. Such computer could operate on 24 states simultaneously. Eventually, observing the system would cause it to collapse into a single quantum state corresponding to a single answer, a single list of 4 1's and 0's.

Some problems occur in production of quantum computers. Any kind of measurement of quantum state parameters considers interaction process with environment (with other particles as particles of light for example), which changes some parameters of this

quantum state. Also, measurement of superposition quantum state will collapse it into a classical state, this is called decoherence. The decoherence problem is the major obstacle in a process of producing of a quantum computer. If this problem cannot be solved, a quantum computer will be no better than a silicon one [4].

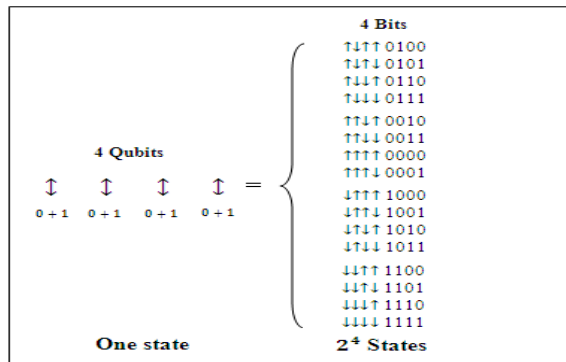


Figure 1: Effect of four qubits

To make quantum computers powerful, many operations must be performed before quantum coherence is lost. It can be impossible to construct a quantum computer that will make calculations before the problem of decoherence. But if one makes a quantum computer, where the number of errors is low enough, than it is possible to use an error-correcting code for preventing data losses even in the case when qubits in the computer decohere.

A hardware problem is another one problem in building quantum computers. Because of some successful experiments Nuclear Magnetic Resonance (NMR) technology is the most popular today. Also, some other designs are based on ion trap and quantum electrodynamics (QED). All of these methods have significant limitations and nobody knows what the architecture of future quantum computers hardware will be [3].

The quantum computing is still in its infancy and although the concept of quantum computers has remained purely theoretical for a long time, recent developments in quantum computers have aroused interest. Experiments have been carried out in which quantum computational operations were executed on a very small number of qubits (quantum bit). Both practical and theoretical research continues with interest, and many national government and military funding agencies support quantum computing research to develop quantum computers for both civilian and national security purposes, such as cryptanalysis.

If a quantum computer becomes a reality then the artificial intelligence is one of its benefits. It has been proved that quantum computers will be much faster and consequently will perform a large amount of operations in a very short period of time. So, increasing the speed of operation will help computers

to learn faster even using the one of the simplest methods. Also, high performance will allow us in development of complex compression algorithms, voice and image recognition, molecular simulations, true randomness and quantum communication. Randomness is very interesting in simulations. Molecular simulations are important for developing simulation applications for biology and chemistry.

Also, the quantum communication has great benefits in the field of security because both receiver and sender are alerted when an eavesdropper tries to catch the signal and thus quantum computers make communication more secure. Actually there a lot of research concerning a new type of cryptography called quantum cryptography. Quantum cryptography, or also quantum key distribution (QKD), uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages [5].

1.2 New Field of Cryptography: Quantum Cryptography

The current cryptographic technologies, such as RSA and others are based on factorization. Integer factorization problem is believed to be computationally infeasible with an ordinary computer for large integers that are the product of only a few prime numbers (e.g., products of two 300-digit primes) [6]. A quantum computer by comparison could efficiently solve this problem using Shor's algorithm [7] to find its factors. This ability would allow a quantum computer to "break" many of the cryptographic systems in use today, in the sense that there would be a polynomial time (in the number of digits of the integer) algorithm for solving the problem of factorisation. In particular, most of the popular public key ciphers are based on the difficulty of factoring integers (or the related discrete logarithm problem which can also be solved by Shor's algorithm), including forms of RSA. These are used to protect secure Web pages, encrypted email, and many other types of data. Breaking these would have significant ramifications for electronic privacy and security. The only way to increase the security of an algorithm like RSA would be to increase the key size and hope that an adversary does not have the resources to build and use a powerful enough quantum computer.

A way out of this dilemma would be to use some kind of quantum cryptography. Wiesner [8] proposed the one-time pad method for key distributions, exploiting the laws of physics to scan for system intrusion or wiretap in the 1970s. Quantum mechanics does not regard measurement as an external and passive process, but instead as one that changes the internal states of the system. Detection, wiretaps, and intrusion are measurement behaviors, any wiretap and intrusion during key distribution can

be detected. Hence, a quantum cryptosystem attains unconditional security.

Quantum cryptography is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel (classical channel).

The security of quantum cryptography relies on the foundations of quantum mechanics, in contrast to traditional public key cryptography which relies on the computational difficulty of certain mathematical functions. Also traditional public key cryptography cannot provide any indication of eavesdropping or guarantee of key security. Quantum key distribution has an important and unique property; it is the ability of the two communicating users (traditionally referred to as Alice and Bob) to detect the presence of any third party (referred to as Eve) trying to gain knowledge of the key. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum superpositions or quantum entanglement and transmitting information in quantum states over a quantum channel (such as an optical fiber or free air), a communication system can be implemented which detects eavesdropping.

2 STATE OF ART OF QUANTUM CRYPTOGRAPHY

Mathematicians have searched for ages, for a system that would allow two people to exchange messages in perfect privacy. Quantum Cryptography was born in the early seventies when Stephen Wiesner wrote the article "Conjugate Coding"[8], was rejected by IEEE Information Theory but was eventually published in 1983 in SIGACT News (15:1 pp. 78-88, 1983). Stephen Wiesner showed in his paper how to store or transmit two messages by encoding them in two "conjugate observables", such as linear and circular polarization of light, so that either, but not both, of which may be received and decoded. His idea is illustrated with a design of unforgeable bank notes.

The ongoing development of quantum cryptosystems thereafter was primarily the result of the efforts of Charles Bennett and Gilles Brassard. Most quantum cryptographic key distribution protocols developed during that time were based on Heisenberg's Uncertainty Principle and Bell's Inequality. Others employed the quantum non-localization, such as the cryptosystem developed by Biham et al. [9]. Users store a particle in the quantum memory of the sending center, such that the users of the same center are assured secure communication. Phoenix et al. [10] introduced a method of developing a quantum cryptographic network rather than adopting quantum non-

localization. Huttner and Peres employed non-coupled photons to exchange keys [11], and Huttner et al. also applied a weak correlation to reduce significantly the level of tapped information [12]. Wiesner used bright light to construct a quantum cryptosystem [13].

The early quantum cryptosystems developed in the 1980s and 1990s however lacked complete facilities of research on the security of key distribution protocols. An eavesdropper in these systems was assumed to be able to adopt only simple wiretap methods but quantum mechanics can in practice support more complex methods. Applying a separate method to manage each possible attack is quite difficult and numerous research scholars devote themselves in enhancing the system security by applying specific methods for key distribution under various attacks.

The first one who examined the security of quantum cryptosystems was Lutkenhaus [14]. In [15,16] Biham and Mor presented a method of resolving collective attack. Mayers and Salvail [17], Yao [18] and Mayers [19] based their research on BB84 Protocol [20], believing that this method could provide unconditional security and resist various attacks. In the article [21] Bennett et al. examined the security of even-odd bits of quantum cryptography.

Despite the development of Quantum Key Distribution protocols, after 20 years, a group of scholars asserted that although quantum cryptosystem based on the QKDP can achieve unconditional security, its key generation is not efficient in practice because the qubits transmitted in the quantum channel cannot be completely employed. For example, out of 10 qubits, only 5 qubits are used for key generation. Also, its key distribution applies one-time pad method, and the length of the key must be the same as that of the plaintext, so the number of qubits required far exceeds the length of plaintext. So, the cost of frequent transmission of bulk messages is much too high. Consequently, the new idea of Quantum Secure Direct Communication (QSDC) is proposed. A QSDC protocol transforms plaintext to qubits to replace the key, and transmits the messages via the quantum channel. This reduces the number of qubits used, thus enables automatic detection of eavesdroppers.

Beige et al. in 2002 [22] was initialized the elaboration of QSDC Protocol. In their scheme, the secure message comprises a single photon with two qubit states; it becomes read-only after a transmission of an extra classical message via a public channel for each qubit. Later Boström and Felbinger developed a Ping-Pong QSDC Protocol [23] that adopts the Einstein-Podolsky-Rosen (EPR) pairs [24] as the quantum information carriers. In this protocol, the secure messages are decoded during transmission, and no additional information needs to be transmitted. A QSDC scheme using batches of

single photons that act as a one-time pad [25] is proposed by Deng et al. in 2004 and in 2005 Lucamarini and Mancini presented a protocol [26] for deterministic communication without applying entanglement. Wang et al. proposed a QSDC approach that uses single photons, of which the concepts were resulted from the order rearrangement and the block transmission of the photons [27].

3 PRINCIPLES USED IN ELABORATION OF QUANTUM KEY DISTRIBUTION PROTOCOLS

3.1 Photon and Polarization

A photon in physics is an elementary particle, the quantum of the electromagnetic field and the basic "unit" of light and all other forms of electromagnetic radiation. It is also the force carrier for the electromagnetic force. Like all elementary particles, photons are governed by quantum mechanics and will exhibit wave-particle duality – they exhibit properties of both waves and particles. For example, a single photon may be refracted by a lens or exhibit wave interference, but also act as a particle giving a definite result when quantitative mass is measured.

Polarization is a physical property; it emerges when a light is considered as an electromagnetic wave. The polarization direction of a photon can be fixed to any desired angle with a polarizing filter.

3.2 Heisenberg's Uncertainty Principle

The Heisenberg's Uncertainty Principle shows that two complementary quantum states cannot be simultaneously measured. When Heisenberg was performing a light diffraction experiment he discovered this principle. He remarked the decoherence of wave function of the system while measuring the position of photons. A shorter wavelength corresponds to a more precise position of the photons; as the wavelength rises, disturbances increase, and the position of the photons becomes imprecise and uncertain. So, the simultaneous measurements of two complementary quantum states are imprecise, and they alter the system. Therefore, the new state differs from that before the measurement.

Heisenberg's Uncertainty Principle is the main principle to assure the security of early Quantum Key Distribution protocols. For an eavesdropper who attempt to tap into a system to hack secret information needs to measure the quantum state but Heisenberg's Uncertainty Principle states that the measurement of a quantum system affects the entire system. Thus, the legitimate users can monitor any change to determine the presence of an eavesdropper or a wiretap.

The application of the Heisenberg's Uncertainty Principle and two types of orthogonal quantum state have lead Bennett and Brassard [20] to build a key

distribution protocol, named the BB84 Protocol. Also, Bennett [28] presented a similar protocol but simpler using a non-orthogonal quantum states; it was called the B92 Protocol.

3.3 Bell's Inequality

In 1935, Einstein et al. argued for the completeness of quantum mechanics [24]. They projected that a strong non-classical mechanical connection exists between two particles A and B that are separated, and they form an entangled photon pair. Restated, very strong connection is observed when two quantum bits are in an entangled state. Modifying or measuring the state of one of the quantum bits determines the relative change in the rest of the quantum bit states within the entangled state. Also, even if they are later widely separated, their behavior remains that of a single unit or a single entity, exhibiting a form of locality; space has no impact on the quantum behavior of the entity. The measurement result of B depends on that of A and vice versa.

A beautiful result discovered in 1964; Bell [29] applied the restrictive classical probability correlation function to prove and explain that a connection exists between the correlation functions satisfying Bell's Inequality when a classical probability is employed to illustrate the quantum status of a system. However, in the 1970s many experiments [30] revealed that the inequality cannot be satisfied if different bases are employed to measure the separated photons of the entangled pair mentioned in EPR paradox. So, entangled quantum states exist whose correlation function cannot be expressed using classical probability. These quantum states are non-local. To the researchers who attempt to contradict that quantum states have locality, these findings were an important victory.

4 PROTOCOLS OF QUANTUM CRYPTOGRAPHY

4.1 BB84 Protocol

This protocol [20] was elaborated by Charles Bennett and Gilles Brassard in 1984. It is based in its design on Heisenberg's Uncertainty Principle. It is known as BB84 after its inventors and year of publication, was originally described using photon polarization states to transmit the information. Any two pairs of conjugate states can be used for the protocol, and many optical fiber based implementations described as BB84 use phase encoded states. This protocol is surely the most famous and most realized quantum cryptography protocol. The security proof of this protocol against arbitrary eavesdropping strategies was first proved by Mayers [31], and a simple proof was later shown by Shor and Preskill [32].

The sender and the receiver (Alice and Bob) are connected by a quantum communication channel

which allows quantum states to be transmitted. Actually, there are two means to transport photons: the optical fiber or free space [33]. Recent research are experimenting the use of atoms and electrons as a quantum particle [34]-[35] and perhaps a novel kind of quantum channel will appear. The quantum channel may be tampered with by an enemy. By its very nature, this channel prevents passive monitoring.

In addition Alice and Bob communicate via a public classical channel, for example using broadcast radio or the internet. Neither of these channels needs to be secure; the protocol is designed with the assumption that an eavesdropper (Eve) can interfere in any way with both. So, this classical channel may be passively monitored but not tampered with by Eve.

BB84 uses the transmission of single polarized photons (as the quantum states). The polarizations of the photons are four, and are grouped together in two different non orthogonal basis.

Generally the two non-orthogonal basis are:

-base \oplus of the horizontal (0°) and vertical polarization ($+90^\circ$), and we represent the base states with the intuitive notation: $|0\rangle$ and $|1\rangle$. We have $\oplus = \{|0\rangle, |1\rangle\}$ (for details about quantum computation please see [36]).

-base \otimes of the diagonal polarizations ($+45^\circ$) and ($+135^\circ$). The two different base states are $|+\rangle$ and

$|-\rangle$ with $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and

$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. We have $\otimes = \{|+\rangle, |-\rangle\}$.

In this protocol, the association between the information bit (taken from a random number generator) and the basis are described in Table 1.

Table 1: Coding scheme for the BB84 protocol.

Bit	\oplus	\otimes
0	$ 0\rangle = a_{00}$	$ +\rangle = a_{10}$
1	$ 1\rangle = a_{01}$	$ -\rangle = a_{11}$

The BB84 can be described as follows [37]:

1) Quantum Transmissions (First Phase)

- a) Alice chooses a random string of bits $d \in \{0,1\}^n$, and a random string of bases $b \in \{\oplus, \otimes\}^n$, where $n > N$ (N is the length of the final key).

- b) Alice prepares a photon in quantum state a_{ij} for each bit d_i in d and b_j in b as in Table 1, and sends it to Bob over the quantum channel.

- c) With respect to either \oplus or \otimes , chosen at random, Bob measures each a_{ij} received. Bob's measurements produce a string $d' \in \{0,1\}^n$, while his choices of bases form $b' \in \{0,1\}^n$.

2) Public Discussion (Second Phase)

- a) For each bit d_i in d :

- i) Alice over the classical channel sends the value of b_i to Bob.

- ii) Bob responds to Alice by stating whether he used the same basis for measurement.

Both d_i and d'_i are discarded if $b_i \neq b'_i$.

- b) Alice chooses a random subset of the remaining bits in d and discloses their values to Bob over the classical channel (over internet for example). If the result of Bob's measurements for any of these bits do not match the values disclosed, eavesdropping is detected and communication is aborted.

- c) The string of bits remaining in d , once the bits disclosed in step 2b) are removed is the common secret key, $K = \{0,1\}^N$ (the final key).

To understand BB84 protocol it is very important to describe how we measure a qubit in the field of quantum physics; if we have a qubit as $|qubit\rangle = e|c\rangle + f|g\rangle$ so the measure of this state in the basis $\{|c\rangle, |g\rangle\}$ produces the state $|c\rangle$ with the probability of $|e|^2$ and the state of $|g\rangle$ with the probability of $|f|^2$ and of course $|e|^2 + |f|^2 = 1$ ($|e|^2$ is the absolute square of the amplitude of e). So, measuring with the incorrect basis yields a random result, as predicted by quantum theory. Thus, if Bob chooses the \otimes basis to measure a photon in state $|1\rangle$, the classical outcome will be either 0 or 1 with equal probability because $|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$; if the \oplus basis was chosen instead, the classical outcome would be 1 with certainty because $|1\rangle = 1|1\rangle + 0|0\rangle$.

To detect Eve, Alice and Bob perform a test for eavesdropping in step 2b) of the protocol. The idea is that, wherever Alice and Bob's bases are identical (i.e. $b_i = b'_i$), the corresponding bits should match

(i.e. $d_i = d'_i$). If not, an external disturbance is produced or there is noise in the quantum channel, we suppose all that is caused by Eve.

Eve can perform several attacks. One type of possible attack is the intercept-resend attack, where Eve measures photons sent by Alice and then sends replacement photons to Bob, prepared in the state she measures. This produces errors in the key shared between Alice and Bob. As Eve has no knowledge of the polarization of photons sent by Alice, she can only guess which basis to measure photons, in the same way as Bob. In the case where she chooses correctly the basis, she measures the correct photon polarization state as sent by Alice, and resends the correct state to Bob. But if its choice is incorrect, the state she measures is random, and the state sent to Bob is sometimes not the same as the state sent by Alice. If Bob then measures this state in the same basis Alice sent, he gets a random result instead of

the correct result he would get without the presence of Eve. An illustration of this type of attack is shown in the Table 2.

Eve chooses the incorrect basis with the probability 0.5, and if Bob measures this intercepted photon in the basis Alice sent he gets a random result, i.e., an incorrect result with probability of 0.5. The probability an intercepted photon generates an error in the key string is then $0.5 \times 0.5 = 0.25$. If Alice and Bob publicly compare n of their key bits the probability they find disagreement and identify the presence of Eve is:

$$P_d = 1 - \left(\frac{3}{4}\right)^n \quad (1)$$

So to detect an eavesdropper with probability $P_d = 0.9999999\dots$ Alice and Bob need to compare $n = 72$ key bits.

Table 2: An example of the intercept-resend attack.

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	\oplus	\oplus	\otimes	\oplus	\otimes	\otimes	\otimes	\oplus
Photon polarization Alice sends	$ 0\rangle$	$ 1\rangle$	$ -\rangle$	$ 0\rangle$	$ -\rangle$	$ +\rangle$	$ +\rangle$	$ 1\rangle$
Eve's random measuring basis	\oplus	\otimes	\oplus	\oplus	\otimes	\oplus	\otimes	\oplus
Polarization Eve measures and sends	$ 0\rangle$	$ +\rangle$	$ 1\rangle$	$ 0\rangle$	$ -\rangle$	$ 1\rangle$	$ +\rangle$	$ 1\rangle$
Bob's random measuring basis	\oplus	\otimes	\otimes	\otimes	\oplus	\otimes	\oplus	\oplus
Photon polarization Bob measures	$ 0\rangle$	$ +\rangle$	$ +\rangle$	$ -\rangle$	$ 1\rangle$	$ +\rangle$	$ 0\rangle$	$ 1\rangle$
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0	-	0	-	-	0	-	1
Errors in key	✓	-	✗	-	-	✓	-	✓

4.2 B92 Protocol

In 1992, Bennett proposes a protocol for Quantum Key Distribution based on two nonorthogonal states and known under the name of B92 or protocol of two states[28]. The quantum protocol B92 is similar to the BB84 protocol but it uses only two states instead of four states. B92 protocol is also based on the on Heisenberg's Uncertainty Principle.

B92 protocol is proven to be unconditional secure. A remarkable proof of the unconditional security of B92 is the proof of Tamaki [38]. That is meant that this proof guaranteed the security of B92 in the presence of any enemy who can perform any operation permitted by the quantum physics; consequently the security of the protocol cannot be compromised by a future development in quantum calculation. Others results related to unconditional secure of B92 are discussed in [39]-[40].

The use of a quantum channel that Eve (enemy) cannot monitor without being detected makes possible to create a secret key with an unconditional security based on the laws of the quantum physics. The presence of Eve is made manifest to the users of such channels through an unusually high error rate. B92 is a protocol of quantum key distribution (QKD) which uses polarized photons as information carriers. B92 supposes that the two legitimate users, Alice and Bob, communicate through two specific channels, which the enemy also has access to:

- A classical channel, which can be public; Eve can listen passively (without being detected);
- A quantum channel that (by its nature) Eve cannot listen passively.

The first phase of B92 involves transmissions over the quantum channel, while the second phase takes place over the classical channel.

To describe B92 we use the same notations as those used for the description of BB84 protocol. For simplicity we give the Fig. 4.2 to show different states of photons (polarizations) which we use in this protocol. Encoding data on photons is shown in Table 1.

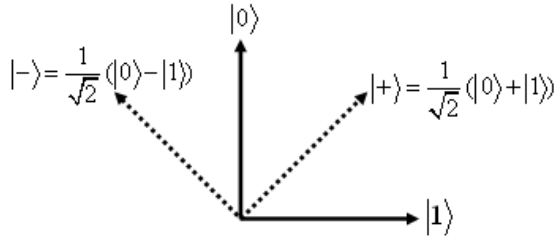


Figure 2: Different states of photons used in B92 protocol.

In B92 protocol, several setups must be done [41]:

1) First phase (Quantum Transmissions)

- a) Alice choose randomly a vector of bits $A \in \{0,1\}^n, n > N$ (N is the length of the final key). If $A_i = 0$ Alice sends to Bob the state of $|0\rangle$ over the quantum channel and if $A_i = 1$, she sends to him the state of $|+\rangle$, for all $i \in \{0,1,\dots,n\}$.
- b) Bob creates in its turn a random vector of bits $B \in \{0,1\}^n, n > N$. If $B_i = 0$, Bob chooses the basis \oplus and if $B_i = 1$ Bob chooses the basis \otimes , for all $i \in \{0,1,\dots,n\}$.
- c) Bob measures respectively each quantum state sent by Alice ($|0\rangle$ or $|+\rangle$) in the selected basis (\oplus or \otimes).
- d) Bob builds the vector test $T \in \{0,1\}^n, n > N$ by complying the following rule: if the measurement of Bob produces $|0\rangle$ or $|+\rangle$ then,

$T_i = 0$ and if it produces $|1\rangle$ or $|-\rangle$, $T_i = 1$, for all $i \in \{0,1,\dots,n\}$.

2) Second phase (Public Discussion)

- a) Over the classical channel, Bob sends T to Alice.
- b) Alice and Bob preserve only the bits of the vectors A and B for which $T_i = 1$. In such case and in absence of Eve, we have: $A_i = 1 - B_i$ and the shared raw key is formed by A_i (or $1 - B_i$).
- c) Alice chooses a sample of the bits of the raw key and reveals them to Bob over the classical channel. If it exists i such as $A_i \neq 1 - B_i$, then Eve is detected and the communication is aborted.
- d) The shared secret key $K \in \{0,1\}^N$ is formed by the raw key after elimination of the samples of the step 2c).

The Table 3 illustrates how the B92 protocol operates. There are three points to understand the protocol B92 perfectly. Firstly, if the test of Bob is equal to 0 for a measure, then Bob does not know what Alice sent to him. Thus if Bob chooses the basis \oplus (resp. \otimes), he can obtain as result of his measure $|0\rangle$ (resp. $|+\rangle$) for any quantum state sent by Alice ($|0\rangle$ or $|+\rangle$). Secondly, if the test of Bob is equal to 1 then Bob knows with exactitude what Alice sent to him, for example if Bob chooses the basis \otimes (resp. \oplus), he will obtain after measure the state $|-\rangle$ (resp. $|1\rangle$) and Alice surely sent to him $|0\rangle$ (resp. $|+\rangle$). Thirdly, in the step 2b), Alice and Bob test the presence of Eve; the idea is that if it exists i such as $T_i = 1$ then $A_i = 1 - B_i$, if not an external disturbance is produced or there is noise in the quantum channel, we suppose all that is caused by Eve.

Table 3: Description of the mechanism of B92 protocol.

Bits chosen by Alice	$A_i = 0$				$A_i = 1$			
States sent by Alice	$ 0\rangle$				$ +\rangle$			
Bits chosen by Bob	$B_i = 0$		$B_i = 1$		$B_i = 0$		$B_i = 1$	
Basis chosen by Bob	\oplus		\otimes		\oplus		\otimes	
Results of the measures of Bob	$ 0\rangle$	$ 1\rangle$	$ +\rangle$	$ -\rangle$	$ 0\rangle$	$ 1\rangle$	$ +\rangle$	$ -\rangle$
Probability to measure the state	1	0	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1	0
The value of the test	0	-	0	1	0	1	0	-

4.3 The EPR Protocol

4.3.1 Preliminary

In [42], Artur Ekert has elaborated a quantum protocol based on the properties of quantum-correlated particles. He uses a pair of particles (called pair EPR).

EPR refers to Einstein, Podolsky and Rosen, which presented a famous paradox in 1935 in their article [24]. They challenged the foundations of quantum mechanics by pointing out a “paradox”. The authors state that there exist spatially separated pairs of particles, called EPR pairs, whose states are correlated in such a way that the measurement of a chosen observable A of one automatically determines the result of the measurement of A of the other. Since EPR pairs can be pairs of particles separated at great distances, this strange behavior is due to “action at a distance.”

It is possible for example to create a pair of photons (each of which we label below with the subscripts 1 and 2, respectively) with correlated linear polarizations. An example of such an entangled state is given by:

$$|S\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2)$$

Thus, if one photon is measured to be in the state $|0\rangle$, the other, when measured, will be found to be in the state $|1\rangle$, and vice versa.

To explain the paradox of “action at a distance”, Einstein et al. suppose that there exist “hidden variables”, inaccessible to experiments. They then state that such quantum correlation phenomena could be a strong indication that quantum mechanics is incomplete. Bell [29] in 1964, gave a means for actually testing for locally hidden variable (LHV) theories. He demonstrated that all such LHV theories must satisfy the Bell inequality. On the other hand, quantum mechanics has been shown to violate the inequality.

4.3.2 EPR Protocol

Unlike BB84 and B92 protocols, this protocol uses Bell’s inequality to detect the presence or absence of Eve as a hidden variable. The EPR quantum protocol is a 3-state protocol. We describe this protocol in terms of the polarization states of an EPR photon pair.

We use the notation of $|\theta\rangle$ which denotes the polarization state of a photon linearly polarized at an angle θ . As the three possible polarization states of our EPR pair, we choose:

$$|S_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|3\pi/6\rangle_2 + |3\pi/6\rangle_1|0\rangle_2)$$

$$|S_1\rangle = \frac{1}{\sqrt{2}}(|\pi/6\rangle_1|4\pi/6\rangle_2 + |4\pi/6\rangle_1|\pi/6\rangle_2)$$

$$|S_2\rangle = \frac{1}{\sqrt{2}}(|2\pi/6\rangle_1|5\pi/6\rangle_2 + |5\pi/6\rangle_1|2\pi/6\rangle_2)$$

For each of these states, we choose the following encoding data:

The state	$ 0\rangle$	$ \frac{3\pi}{6}\rangle$	$ \frac{\pi}{6}\rangle$	$ \frac{4\pi}{6}\rangle$	$ \frac{2\pi}{6}\rangle$	$ \frac{5\pi}{6}\rangle$
Bit	0	1	0	1	0	1

The measurement operators [36] corresponding to this encoding are respectively:

$$M_0 = |0\rangle\langle 0|,$$

$$M_1 = \left|\frac{\pi}{6}\right\rangle\left\langle\frac{\pi}{6}\right|,$$

$$M_2 = \left|\frac{2\pi}{6}\right\rangle\left\langle\frac{2\pi}{6}\right|$$

Like BB84 and B92 protocols, there are two phases to the EPR protocol, the first phase over a quantum channel and the second over a public channel. EPR protocol could describe as follows [43]:

1) Quantum Transmissions (First phase)

Firstly, a state $|S_i\rangle$ is randomly selected from the set of states $\{|S_j\rangle, 0 \leq j \leq 2\}$ to create EPR pair in the selected state $|S_i\rangle$. One photon of the established EPR pair is sent to Alice, the other to Bob. With equal probability separately and independently, Alice and Bob at random select one of the three measurement operators M_0 , M_1 and M_2 . They measure their respective photons with the selected measurement operators. Alice records her measured bit. And Bob records the complement of his measured bit. This procedure is repeated for as many times as needed.

2) Public Discussion (Second phase)

Alice and Bob establish a discussion over a public channel to determine those bit at which they used the same measurement operators. Next, they separate their respective bit sequences into two subsequences. The first subsequence, called raw key, consists of those bit at which they used the same measurement operators. The second subsequence, called rejected key, consists of all the remaining bit.

The purpose of the rejected key is to detect Eve’s presence. Alice and Bob over the public channel compare their respective rejected keys to determine whether or not Bell’s inequality is

satisfied: if it is, Eve's presence is detected and if not, then Eve is absent.

For this specific EPR protocol, Bell's inequality can be formulated as follows. We note $P(\neq i, j)$ the probability that two corresponding bits of Alice's and Bob's rejected keys do not coincide known that the measurement operators chosen by Alice and Bob are respectively either M_i and M_j or M_j and M_i .

We write also the expression:

$$\begin{aligned} P(= i, j) &= 1 - P(\neq i, j), \\ \Phi(i, j) &= P(\neq i, j) - P(= i, j), \\ I &= 1 + \Phi(1, 2) - |\Phi(0, 1) - \Phi(0, 2)|. \end{aligned}$$

So, the Bell's inequality reduces in this case to

$$I \geq 0$$

and for quantum mechanics (i.e., no hidden variables)

$$I = -\frac{1}{2}$$

which is a clear violation of Bell's inequality.

There are others protocols of quantum cryptography. For example, there is the EPR protocol with a single particle and there is also a 2-state EPR implementation of the BB84 protocol. We can consult [44]-[45] for details. Also, the paper [46] treats the various multiple state and rejected data protocols.

5 CONCLUSION

Quantum cryptography is based on a combinations of principles from quantum physics and information theory and made possible thanks to the tremendous progress in quantum optics and in the technology of optical fibers and of free space optical communication. Its security relies on deep theorems in classical information theory and on a profound understanding of the Heisenberg's uncertainty principle. Quantum cryptography has some important contributions to classical cryptography: privacy amplification [47] and classical bound information are examples of concepts in classical information whose discovery were much inspired by quantum cryptography. Also, the fascinating tension between quantum physics and relativity, as illustrated by Bell's inequality, is not far away. Actually, despite the huge progress over the recent years, many technological challenges and open questions remain.

The first technological challenge at present concerns improved detectors compatible with telecom fibers. Also two other issues concern free space and quantum repeaters. The first is presently the only way to realize quantum cryptography over thousands of kilometers using near future technology. The purpose of the idea of quantum

repeaters is to encode the qubits in such a way that if the error rate is low, then errors can be detected and corrected entirely in the quantum domain. So, the hope is that such techniques could extend the range of quantum communication to essentially unlimited distances.

For the open questions side, we emphasize three main concerns. First, complete and realistic analyses of the security issues are still missing. Second, figures of merit to compare quantum cryptography schemes based on different quantum systems (with different dimensions for example) are still awaited. Third, the delicate question of how to test the apparatuses did not yet receive enough attention.

Quantum cryptography could well be the first application of quantum mechanics at the single quanta level. Many experiments have demonstrated that keys can be exchanged over distances of a few tens of kilometers 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!

6 REFERENCES

- [1] R. Feynman, Simulating physics with computers, *International Journal of Theoretical Physics* 21 (6&7) (1982) 467-488.
- [2] http://qist.lanl.gov:80/qcomp_map.shtml
- [3] West, J (2000). *Quantum Computers*. Retrieved December 1, 2002 from California Institute of Technology, educational website: <http://www.cs.caltech.edu/~westside/quantum-intro.html#qc>
- [4] Daniel, G. (1999). *Quantum Error-Correcting Codes*. Retrieved on November 31st, 2002 from: <http://qso.lanl.gov/~gottesma/QECC.html>
- [5] http://en.wikipedia.org/wiki/Quantum_cryptography
- [6] *Integer Factoring By ARJEN K. LENSTRA - Designs, Codes and Cryptography*, 19, 101-128 (2000) Kluwer Academic Publishers. http://modular.fas.harvard.edu/edu/Fall2001/124/misc/arjen_lenstra_factoring.pdf
- [7] P.W. Shor, Algorithms for quantum computation: discrete logarithm and factoring, in: *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, 1994, pp. 124-134.
- [8] S. Wiesner, Conjugate coding, *SIGACT News* 15 (1) (1983) 78-88.
- [9] E. Biham, B. Huttner, T. Mor, Quantum cryptography network based on quantum memories, *Physical Review A* 54 (3) (1996) 2651-2658.
- [10] S.J.D. Phoenix, S.M. Barnett, P.D. Townsend,

- K.J. Blow, Multi-user quantum cryptography on optical networks, *Journal of Modern Optics* 42 (1995) 1155–1163.
- [11] B. Hutter, A. Peres, Quantum cryptography with photon pairs, *Journal of Modern Optics* 41 (12) (1994) 2397–2403.
- [12] B. Hutter, N. Imoto, N. Gisin, T. Mor, Quantum cryptography with coherent states, *Physical Review A* 51 (3) (1995) 1863–1869.
- [13] S. Wiesner, Quantum cryptography with bright light, Manuscript, 1993.
- [14] N. Lutkenhaus, Security against eavesdropping in quantum cryptography, *Physical Review A* 54 (1) (1996) 97–111.
- [15] E. Biham, T. Mor, Security of quantum cryptography against collective attacks, *Physical Review Letters* 78 (11) (1997) 2256–2259.
- [16] E. Biham, T. Mor, Bounds on information and the security of quantum cryptography, *Physical Review Letters* 79 (20) (1997) 4034–4037.
- [17] D. Mayers, L. Salvail, Quantum oblivious transfer is secure against all individual measurements, in: *Proceedings of the 3rd Workshop on Physics and Computation—PhysComp’94*, IEEE Computer Society, 1994, pp. 69–77.
- [18] A.C.-C. Yao, Security of quantum protocols against coherent measurements, in: *Proceedings of the 26th Annual ACM Symposium on the Theory of Computing*, 1995, pp. 67–75.
- [19] D. Mayers, Quantum key distribution and string oblivious transfer in noisy channels, in: *Advances in Cryptology—CRYPTO’96*, LNCS 1109, Springer-Verlag, 1996, pp. 343–357.
- [20] C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in: *Proceedings of the International Conference on Computers, Systems & Signal Processing*, Bangalore, India, December 10–12, 1984, pp. 175–179.
- [21] C.H. Bennett, T. Mor, J. Smolin, The parity bit in quantum cryptography, *Physical Review A* 54 (4) (1996) 2675–2684.
- [22] A. Beige, B.-G. Englert, C. Kurtsiefer, H. Weinfurter, Secure communication with a publicly known key, *Acta Physica Polonica A* 101 (3) (1999) 357.
- [23] K. Bostroöm, T. Felbinger, Deterministic secure direct communication using entanglement, *Physics Review Letters* 89 (18) (2002) 187902.
- [24] A. Einstein, B. Podolsky, N. Rosen, Can quantum-mechanical description of physical reality be considered complete? *Physical Review* 47 (1935) 777–780.
- [25] F.-G. Deng, G.L. Long, Secure direct communication with a quantum one-time pad, *Physical Review A* 69 (5) (2004) 052319.
- [26] M. Lucamarini, S. Mancini, Secure deterministic communication without entanglement, *Physics Review Letters* 94 (2005) 140501.
- [27] J. Wang, Q. Zhang, C.-J. Tang, Quantum secure direct communication based on order rearrangement of single photons, *Physics Letters A* 358 (4) (2006) 256–258.
- [28] C.H. Bennett, Quantum cryptography using any two non-orthogonal states, *Physical Review Letters* 68 (21) (1992) 3121–3124.
- [29] J.S. Bell, On the Einstein–Podolsky–Rosen paradox, *Physics* 1 (1964) 195–200.
- [30] J.F. Clauser, Experimental investigation of a polarization correlation anomaly, *Physics Review Letters* 36 (1976) 1223–1226.
- [31] D. Mayers, “Unconditional security in quantum cryptography,” *Journal of the ACM*, vol. 48, no. 3, pp. 351–406, May 2001.
- [32] P. W. Shor and J. Preskill, “Simple proof of security of the BB84 quantum key distribution protocol,” *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, July 2000.
- [33] R. Hughes, J. Nordholt, D. Derkacs, C. Peterson, (2002). “Practical free-space quantum key distribution over 10km in daylight and at night”. *New journal of physics* 4 (2002) 43.1–43.14. URL: <http://www.iop.org/EJ/abstract/1367-2630/4/1/343/>
- [34] Knight, P (2005). “Manipulating cold atoms for quantum information processing”. QUPON conference Vienna 2005.
- [35] Tonomura, A (2005). “Quantum phenomena observed using electrons”. QUPON conference Vienna 2005.
- [36] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [37] M. Elboukhari, M. Azizi, A. Azizi, “Implementation of secure key distribution based on quantum cryptography”, in *Proc. IEEE Int. Conf Multimedia Computing and Systems (ICMCS’09)*, page 361 - 365, 2009.
- [38] Tamaki, K., M. Koashi, and N. Imoto, “Unconditionally secure key distribution based on two non orthogonal states,” *Physical Review Letters* 90, 167904 (2003), [preprint quant-ph/0210162].
- [39] Tamaki.K , Lütkenhaus.N, “Unconditional Security of the Bennett 1992 quantum key-distribution over lossy and noisy channel,“ *Quantum Physics Archive: arXiv:quantph/0308048v2*, 2003.
- [40] Tamaki.K, Lütkenhaus.N, Koashi.M, and Batuwantudawe.J, “Unconditional security of the Bennett 1992 quantum key-distribution scheme with strong reference pulse ,“ *Quantum Physics Archive: arXiv:quant-ph/0607082v1*, 2006.
- [41] M. Elboukhari, M. Azizi, A. Azizi, “Security Oriented Analysis of B92 by Model Checking”,

in Proc. IEEE Int. Conf. new technology, mobility and security (NTMS), page 454-458, 2008.

- [42]Ekert, Artur K., Quantum cryptography based on Bell's theorem, Physical Review Letters, Vol. 67, No. 6, 5 August 1991, pp 661 - 663.
- [43]S. J. Lomonaco Jr: A quick glance at quantum cryptography
<http://www.cs.umbc.edu/~lomonaco/Publications.html>
- [44]Bennett, Charles H., Gilles Brassard, and N. David Mermin, Quantum cryptography without Bell's theorem, Physical Review Letters, Vol. 68, No. 5, 3 February 1992, pp 557 - 559.
- [45]D'Espagnat, B., Scientific American, November 1979, pp 128 - 140.
- [46]Blow, K.J., and Simon J.D. Phoenix, On a fundamental theorem of quantum cryptography, Journal of Modern Optics, 1993, vol. 40, no. 1, 33 - 36.
- [47]Bennett, C. H., Brassard, G., Crepeau, C. and Maurer, U. M., "Generalized Privacy Amplification", IEEE Transactions on Information Theory, 1995.