Quantum Key Distribution Protocols: A Survey♠

Mohamed Elboukhari*, Mostafa Azizi, Abdelmalek Azizi*,*****

**dept. Mathematics & Computer Science, FSO, University Mohamed I[st], Morocco*
elboukharimohamed@gmail.com
***dept. Applied Engineering, ESTO, University Mohamed I[st], Oujda, Morocco*
azizi.mos@gmail.com
****Academy Hassan II of Sciences & Technology, Rabat, Morocco*
abdelmalekazizi@yahoo.fr

Submitted: 22/02/2010
Accepted: 23/03/2010
Appeared: 30/03/2010

Abstract—Most cryptographic mechanisms, such as symmetric and asymmetric cryptography, often involve the use of cryptographic keys. However, all cryptographic techniques will be ineffective if the key distribution mechanism is weak. The security of most modern cryptographic systems of key distribution mechanism is based on computational complexity and the extraordinary time needed to break the code. Quantum Key Distribution (QKD) or Quantum Cryptography is attracting much attention as a solution of the problem of key distribution; QKD offers unconditionally secure communication based on quantum mechanics. In this article we survey the most popular QKD protocols. Also, we give a short state of the art of Quantum Cryptography.

Keywords: Quantum Cryptography, ey distribution, Quantum Key Distribution protocols.

1. INTRODUCTION

The security has become a big concern in wired and wireless networks. The characteristics of networks pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and no repudiation. Cryptographic techniques are widely used for secure communications.

Cryptography is composed schematically by two systems: symmetric encryption and asymmetric encryption.

The cryptosystems of symmetric encryption use the same key for cipher and decipher messages. The key must be preserved secret by the parties of a communication. So in a network of n people wanting to communicate in a confidential way with a cryptosystems of symmetric encryption, it is necessary that the keys are distinct. Precisely, it is necessary to create and distribute $n(n-1)/2$ keys which are distinct and secret. As we can remark, the cryptosystems of symmetric encryption suffers from the problem of creation and distribution the keys. This problem is mainly solved by the installation of the cryptosystems of asymmetric encryption (A. J. Menezes, 1996).

A cryptosystem of asymmetric encryption operates by handling two keys: secret and public. Each participant diffuses a public key with his name. If one wishes to communicate with a participant, it is necessary to recover his public key and cipher with it the message, and send the ciphered message to this participant which is the only person who knows the secret key which makes possible to decipher the received messages. The secret key is of course related to the public key, in practice by a mathematical relation. The power of the security of these cryptosystems is based on algorithmic complexity; it is difficult in practice to deduce the secret key from the public key in a reasonable delay. Nothing proves however that this security is not compromised in a near future because there is an accelerated evolution of the software and the specific hardware. So, many cryptographic schemes in use today would be broken with either unanticipated advances in hardware and algorithm or the advent of quantum computers.

Another solution to the delicate problem of distribution of keys met in cryptography consists at using the laws of the quantum physics. It is precisely to place at the disposal of security of computing systems a Quantum Cryptography protocols in order to carry out a task of exchanged keys with a great security. Quantum Cryptography has been proven secure even against the most general attack allowed by the laws of physics and is a promising technology for adoption in realistic cryptographic applications. Quantum Cryptography

♠ This work is partially supported by the Academy Hassan II of Sciences and Technology (Morocco).

allows two parties to expand on a secret key that they have previously shared. Various quantum cryptographic protocols have been proposed in order to achieve unconditional security.

In this article, we give in details the descriptions of the famous Quantum Cryptography protocols: BB84, B92 and E91. Also, we provide a short presentation of some others recent protocols.

The organization of the remainder of our paper is as follows. In section II, we introduce the state-of-the-art of Quantum Cryptography. The description of the protocols BB84, B92, E91 and others protocols is given in section III. Finally, we conclude the paper in section IV.

2. STATE OF THE 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"(S. Wiesner, 1983), 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. (E. Biham, 1996). 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.(S.J.D. Phoenix, 1995) 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 (B. Hutter and A. Peres, 1994), and Huttner et al. also applied a weak correlation to reduce significantly the level of tapped information (B. Hutter, 1995). Wiesner used bright light to construct a quantum cryptosystem (S. Wiesner, 1993).

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 (N. Lutkenhaus, 1996). In (E. Biham and T. Mor, 1997a, b) Biham and Mor presented a method of resolving collective attack. Mayers and Salvail (D. Mayers and L. Salvail, 1994), Yao (A.C.-C. Yao, 1995) and Mayers (D. Mayers, 1996) based their research on BB84 Protocol (C.H. Bennett and G. Brassard, 1984), believing that this method could provide unconditional security and resist various attacks. In the article (C.H. Bennett, 1996) Bennett et al. examined the security of even–odd bits of Quantum Cryptography.

Despite the development of Quantum Key Distribution protocols (QKDP), 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. (A. Beige, 1999) 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 Felbingeer developed a Ping-Pong QSDC Protocol (K. Bostro, 2002) that adopts the Einstein–Podolsky–Rosen (EPR) pairs (A. Einstein, 1935) 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 acts as a one-time pad (F.-G. Deng and G.L. Long, 2004) is proposed by Deng et al. in 2004 and in 2005 Lucamarini and Mancini presented a protocol (M. Lucamarini and S. Mancini, 2005) 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 (J. Wang, 2006).

3. PROTOCOLS OF QUANTUM CRYPTOGRAPHY

3.1 BB84 Protocol

This protocol (C.H. Bennett and G. Brassard, 1984) 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 (D. Mayers, 2001), and a simple proof was later shown by Shor and Preskill (P. W. Shor and J. Preskill, 2000).

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 (R.Hughes, 2002). Recent research are experimenting the use of atoms and electrons as a quantum particle (Knight, 2005)-(Tonomura, 2005) and perhaps a novel kind of quantum channel will appear. The quantum channel may be tampered with by an enemy. By its 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 need 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°), 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 (M. Nielsen and I. Chuang, 2000)).

-base $\otimes$ of the diagonal polarizations (+45°) and (+135°). 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 (M. Elboukhari, 2009a, b):

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.

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	⊕	⊕	⊗	⊕	⊗	⊗	⊗	⊕
Photon polarization Alice sends	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$
Eve's random measuring basis	⊕	⊗	⊕	⊕	⊗	⊕	⊗	⊕
Polarization Eve measures and sends	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$
Bob's random measuring basis	⊕	⊗	⊗	⊗	⊕	⊗	⊕	⊕
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	✓	-	✘	-	-	✓	-	✓

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: $1-(3/4)^n$.

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

3.2 B92 Protocol

In 1992, Bennett proposes a protocol for QKD based on two nonorthogonal states and known under the name of B92 or protocol of two states (C.H. Bennett, 1992). 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 (Tamaki, 2003). That is mean 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 (Tamaki.K and Lütkenhaus.N, 2003)-(Tamaki, 2006).

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 polarised 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.

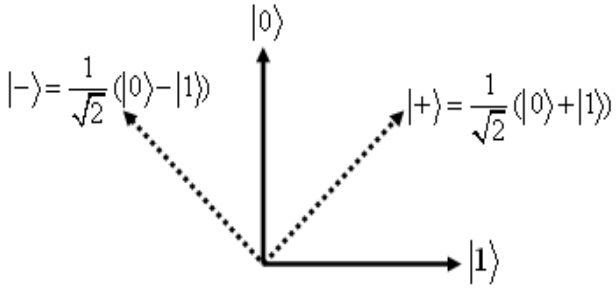

Fig. 1. Different states of photons used in B92 protocol

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

In B92 protocol, several setups must be done (Elboukhari, 2008)-(Elboukhari, 2010):

1) First phase (Quantum Transmissions)

a) Alice chooses 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 $i \in \{0,1,\ldots,n\}$.

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 $i \in \{0,1,\ldots,n\}$.

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 $i \in \{0,1,\ldots,n\}$.

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**	-

3.3 The EPR Protocol

Preliminary:

In (Ekert, 1991), 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 (A. Einstein, 1935). 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 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:

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

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 (J.S. Bell, 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.

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:

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

$$|S_1\rangle = \tfrac{1}{\sqrt{2}}(\left|\frac{\pi}{6}\right\rangle_1 \left|\frac{4\pi}{6}\right\rangle_2 + \left|\frac{4\pi}{6}\right\rangle_1 \left|\frac{\pi}{6}\right\rangle_2) \quad (3)$$

$$|S_2\rangle = \tfrac{1}{\sqrt{2}}(\left|\frac{2\pi}{6}\right\rangle_1 \left|\frac{5\pi}{6}\right\rangle_2 + \left|\frac{5\pi}{6}\right\rangle_1 \left|\frac{2\pi}{6}\right\rangle_2) \quad (4)$$

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 (M. Nielsen and I. Chuang, 2000) corresponding to this encoding are respectively:

$$M_0 = |0\rangle\langle 0|, \qquad M_1 = \left|\frac{\pi}{6}\right\rangle\left\langle\frac{\pi}{6}\right|, \quad M_2 = \left|\frac{2\pi}{6}\right\rangle\left\langle\frac{2\pi}{6}\right|$$

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 be described as follows (S. J. Lomonaco Jr, 1999):

1) Quantum Transmissions (First phase)

Firstly, a state $|S_i\rangle$ is randomly selected from the set of states $\{|S_j\rangle, 0 \le j \le 2\}$ 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 remaining bit.

The purpose of the rejected key is to detect Eve's presence. Alice and Bob over a 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 expressions:

$$P(=|i,j) = 1 - P(\neq|i,j), \quad (5)$$

$$\Phi(i,j) = P(\neq|i,j) - P(=|i,j), \quad (6)$$

$$\mathrm{I} = 1 + \Phi(1,2) - |\Phi(0,1) - \Phi(0,2)| \quad (7)$$

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

$$\mathrm{I} \ge 0 \quad (8)$$

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

$$\mathrm{I} = -\frac{1}{2} \quad (9)$$

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 (Bennett, 1992)-(D'Espagnat, 1979) for details. Also, the paper (Blow, 1993) treats the various multiple state and rejected data protocols. In the next section we give a short description of some recent protocols of Quantum Cryptography.

3.4 Differential Phase Shift Quantum Key Distribution

The authors Inoue K, Woks E and Yamamoto proposed a novel Quantum Cryptography scheme in which a single photon is prepared in a linear superposition state of three basis kets (Inoue K, 2002). This protocol is suitable for fiber transmission systems and offers a key creation efficiency higher than conventional fiber-based BB84. In this scheme, a photon split to three pulses is sent from Alice to Bob, where

the phase difference between sequential two pulses carries bit information. Bob measures the phase difference by passive differential phase detection.

3.5 COW Protocol

Coherent One-Way protocol (COW protocol) is a new protocol for practical Quantum Cryptography elaborated by Nicolas Gisin and al in 2004 (Gisin N, 2004). It tailored for an implementation with weak coherent pulses. In the description of this protocol, the key is obtained by a very simple time-of-arrival measurement on the data line and also an interferometer is built on an additional monitoring line. The purpose of this line is to allow to monitor the presence of a spy who would break coherence by her attack.

This protocol performs as well as standard protocols with strong reference pulses against zero-error attacks: only as the transmission of the quantum channel the key rate decreases. In their paper, the authors propose possible variations of this protocol. They also present two attacks that introduce errors on the monitoring line: the coherent attack on two subsequent pulses and the intercept-resend.

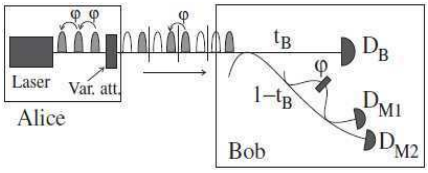

Fig. 2. Scheme of the COW protocol (Gisin N, 2004).

3.5 SARG04 protocol

The SARG04 protocol (V. Scarani, 2004) is built when researchers noticed that by using the four states of BB84 with a different information encoding they could develop a new protocol which would be more robust when attenuated laser pulses are used instead of single-photon sources. SARG04 protocol was defined by Scarani et al. in 2004 in Physical Review Letters as a prepare and measure version; SARG04 is equivalent to BB84 when viewed at the level of quantum processing (Chi-Hang Fred Fung, 2006).

SARG04 is intended to use in situations where the information is originated by a Poissonian source producing weak pulses and received by an imperfect detector (Chi-Hang Fred Fung, 2006).

The authors Tamaki and Lo were successful in proving security for one and two-photon pulses using SARG04. SARG04 protocol in single-photon implementations was theorized to be equal with BB84, but experiments shown that it is inferior (Chi-Hang Fred Fung, 2006).

3.6 Protocol with Private-Public Key

Unlike the BB84 protocol and its many variants, this protocol (Eduin H. Serna, 2009) uses two quantum channels. It is also described with public key cryptography combinations and private key cryptography. Its description does not make reconciliation mechanisms of information to derive the key.

The quantum protocol presented provides a safe sending of information of direct communication between two or more parties. This protocol is suitable for the generalizations of n parties and can allow a network of massive sending information for $n-1$ parties being one of them the key-message distribution center. Because the proposed protocol does not use classical communication, it is immune to the man-in-the-middle attack on the classical communication channel which several cryptography protocols suffer from. But on the other hand, implementation of this protocol may be harder because the qubits get exchanged multiple times.

4. CONCLUSION

QKD protocols are based on 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. Their security relies on deep theorems in classical information theory and on a profound understanding of the Heisenberg's uncertainty principle. Quantum Qryptography protocols have some important contributions to classical cryptography: privacy amplification (Bennett, 1995) and classical bound information are examples of concepts in classical information whose discovery were much inspired by Quantum Cryptography protocols. Also, the fascinating tension between quantum physics and relativity, as illustrated by Bell's inequality, is not far away.

Quantum Cryptography protocols 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 will find commercial applications.

REFERENCES

A. Beige, B.-G. Englert, C. Kurtsiefer, H. Weinfurter, Secure communication with a publicly known key, Acta Physica Polonica A 101 (3) (1999) 357.

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.

A. Einstein, B. Podolsky, N. Rosen, Can quantum-mechanical description of physical reality be considered complete? *Physical Review* 47 (1935) 777–780.

A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Oct. 1996.

B. Hutter, A. Peres, Quantum cryptography with photon pairs, *Journal of Modern Optics* 41 (12) (1994) 2397–2403.

B. Hutter, N. Imoto, N. Gisin, T. Mor, Quantum cryptography with coherent states, *Physical Review* A 51 (3) (1995) 1863–1869.

Bennett, C. H., Brassard, G., Crepeau, C. and Maurer, U. M., "Generalized Privacy Amplification", IEEE Transactions on Information Theory, 1995.

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.

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.

Chi-Hang Fred Fung, Kiyoshi Tamaki, Hoi-Kwong Lo, "On the performance of two protocols: SARG04 and BB84", *Phys. Rev.* A 73, 012337 (2006). http://arxiv.org/PS_cache/quant-ph/pdf/0510/0510025v2.pdf

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.

C.H. Bennett, Quantum cryptography using any two non-orthogonal states, *Physical Review Letters* 68 (21) (1992) 3121–3124.

C.H. Bennett, T. Mor, J. Smolin, The parity bit in quantum cryptography, *Physical Review* A 54 (4) (1996) 2675–2684.

D'Espagnat, B., *Scientific American*, November 1979, pp 128 - 140.

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.

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.

E. Biham, B. Huttner, T. Mor, Quantum cryptography network based on quantum memories, *Physical Review* A 54 (3) (1996) 2651– 2658.

E. Biham, T. Mor, Bounds on information and the security of quantum cryptography, *Physical Review Letters* 79 (20) (1997b) 4034– 4037.

E. Biham, T. Mor, Security of quantum cryptography against collective attacks, *Physical Review Letters* 78 (11) (1997a) 2256–2259.

Eduin H. Serna,"Quantum Key Distribution Protocol with Private-Public Key", *Quantum Physics* (quant-ph), 2009. http://arxiv.org/PS_cache/arxiv/pdf/0908/0908.2146v3.pdf

Ekert, Artur K., Quantum cryptography based on Bell's theorem, *Physical Review Letters*, Vol. 67, No. 6, 5 August 1991, pp 661 - 663.

F.-G. Deng, G.L. Long, Secure direct communication with a quantum one-time pad, *Physics Review* A 69 (5) (2004) 052319.

Gisin N, Ribordy G, Zbinden H, Stucki D, Brunner N and Scarani V 2004, "Towards practical and fast quantum cryptography", arXiv:quant-ph/0411022

Inoue K, Woks E and Yamamoto Y 2002, "Differential phase shift quantum key distribution", *Phys. Rev. Lett.* 89 037902.

Knight, P (2005). "Manipulating cold atoms for quantum information processing". QUPON conference Vienna 2005.

K. Bostro¨m, T. Felbinger, Deterministic secure direct communication using entanglement, *Physics Review Letters* 89 (18) (2002) 187902.

M. Lucamarini, S. Mancini, Secure deterministic communication without entanglement, *Physics Review Letters* 94 (2005) 140501.

D. Mayers, "Unconditional security in quantum cryptography," *Journal of the ACM*, vol. 48, no. 3, pp. 351–406, May 2001.

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.

J.S. Bell, On the Einstein–Podolsky–Rosen paradox, Physics 1 (1964) 195–200.

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, 2009a.

M. Elboukhari, Mostafa Azizi, and Abdelmalek Azizi, "Integration of Quantum Key Distribution in the TLS Protocol", *IJCSNS*, Vol. 9 No. 12 pp. 21-28, 2009b. http://paper.ijcsns.org/07_book/200912/20091204.pdf

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.

M. Elboukhari, M. Azizi, A. Azizi, "Analysis of Quantum Cryptography Protocols by Model Checking", *IJUCS*, Vol 1, pp. 34-40, 2010. http://www.hypersciences.org/IJUCS/Iss.1-2010/IJUCS-4-1-2010.pdf

M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

N. Lutkenhaus, Security against eavesdropping in quantum cryptography, *Physical Review* A 54 (1) (1996) 97–111.

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.

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/

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.

S. J. Lomonaco Jr,"A quick glance at quantum cryptography", *Cryptologia*, Vol. 23, No.1, January, 1999,pp1-41.

http://www.cs.umbc.edu/~lomonaco/lecturenotes/9811056.pdf

S. Wiesner, Conjugate coding, *SIGACT News* 15 (1) (1983) 78–88.

S. Wiesner, Quantum cryptography with bright light, Manuscript, 1993.

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].

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.

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.

Tonomura, A (2005). "Quantum phenomena observed using electrons". QUPON conference Vienna 2005.

V. Scarani, A. Ac´ın, G. Ribordy, N. Gisin, *Phys. Rev. Lett*. 92, 057901 (2004)