BULETINUL Universităţii Petrol – Gaze din Ploieşti	Vol. LXVI No. 3/2014	15 - 22	Seria Tehnică

Quantum Encryption BB84 Protocol Application

Otilia Cangea

Universitatea Petrol-Gaze din Ploieşti, Bd. Bucureşti 39, Ploieşti
e-mail: ocangea@upg-ploiesti.ro

Abstract

In the present, technology is in a continuous development process and, with the spread of the Internet, the need for more secure data communications has grown in order to protect information. The security of the common methods of cryptography is measured by the computing power needed to break the key. With quantum cryptography, every intervention upon the encrypted message by measuring the physical properties of the signal is interpreted as a cryptanalysis attack. The paper presents a quantum encryption BB84 protocol application, simulated by means of a specially designed graphical interface.

Key words: *quantum cryptography, qubit, BB84 protocol, information security.*

Introduction

Information is power, that is a very well-known fact since the very ancient times of humanity. Information transmission, therefore, had to be performed in a very secure manner so that it can be protected in order not to reveal important secrets to intruders. This is the main reason why one has always tried to design encryption algorithms that allow data transmission in a very secret way, offering unconditioned security, so that a cryptanalyst cannot obtain the plaintext message. The best example is the *Vernam cipher*, or the *one-time pad* method; nevertheless, it has some disadvantages, referring to the fact that the encryption key has to be completely random, secure and not reused, having the same length as the text. In addition, the security of the channel is essential.

Quantum cryptography, based upon phenomena that take place at subatomic level, solves the problem of the channel security, being able to detect intruders, and even interrupt the transmission, so that, combining quantum cryptography with the Vernam cipher, one can obtain a completely secure data transmission system.

Can a cipher be truly indestructible?

Despite its long history, cryptography became part of mathematics and information theory in the late 1940's, mainly due to the remarkable results of Claude Shannon from Bell Laboratories in New Jersey. Shannon proved that there are indestructible ciphers, designed in 1918 by engineer Gilbert Vernam from American Telephone and Telegraph, and Major Joseph Mauborgne from U.S. Army Signal Corps, named *Vernam ciphers* [4].

Both the original design of the Vernam cipher, and the modern version of it, are based upon the binary alphabet. The plaintext message is converted into a bit sequence, of 0 and 1; the cryptographic key is another bit sequence, having the same length. Using mod 2 addition rules,

one obtains the respective cryptogram. As the key is a random bit sequence, the resulted cryptogram will always be random, too, and cannot be decrypted unless the cryptographic key is known. The original plaintext may be revealed by mod 2 addition between the cryptogram and the cryptographic key, as seen in Figure 1.

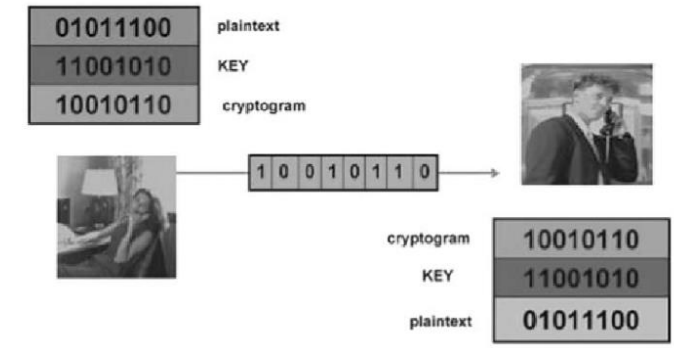

Fig. 1. Vernam cipher example [4]

If the message is intercepted, it cannot be decrypted unless someone has the original cryptographic key. Shannon has, thus, demonstrated that, in the case of a secret key, having the same length as the plaintext, completely random and never reused, the Vernam cipher is indestructible [4].

The key distribution problem

All the Vernam ciphers have a major disadvantage, known as the *key distribution problem*, referring to the fact that all the potential key users have to agree about the distribution of the used key, and everything has to be done in secret. The cryptographic key is a long random bit sequence that, after it is generated, may be used for encryption/decryption and the obtained cryptogram may be publicly transmitted (posted on Internet or printed in a paper), without compromising the security of the content. But the encryption key has to be agreed between the emitter (Alice) and the receiver (Bob) and distributed through a secure channel (fig. 2).

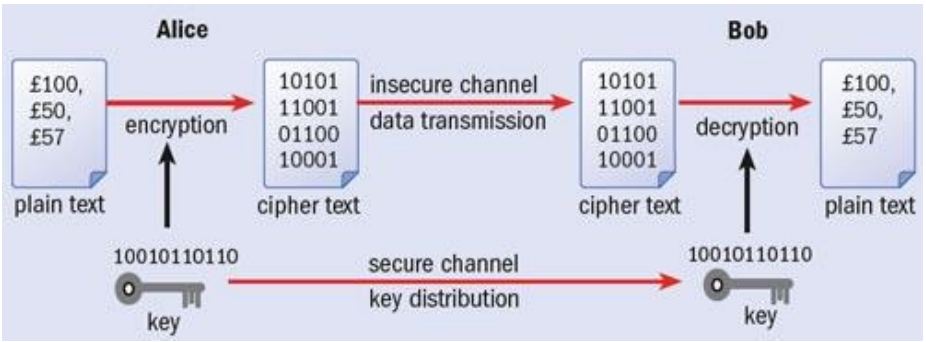

Fig. 2.Example of a key distribution system [4]

In addition, even if a secure channel is available, the security of data transmission cannot truly be ensured, this being a fundamental major problem because, in principle, every classic private channel may be passively monitored, even if the emitter and receiver are not aware of the fact that an interception is actually taking place. This is a consequence of the fact that classic physics allows the measurement of all physical properties of an object without influencing these properties. In this respect, because all the information, including the encryption keys, are coded in measurable physical properties of an object or of a signal, classic theory allows passive interception because, in principle, it allows the intruder to measure the properties without

influencing them. *In the case of the quantum theory, that is the basis of quantum cryptography, things are different: measuring the physical properties of the signal is interpreted as a cryptanalysis attack* [4].

Quantum Encryption

Long time ago before the discovery of the public key encryption, a very interesting research project took place: a union between cryptography and quantum mechanics. Around 1970, Stephen J. Wiesner, from Columbia University, wrote a paper, "Conjugate Coding" (that, unfortunately, was unpublished at the time, despite its highly innovative ideas), explaining how quantum physics can be used for combining two classical messages in a single quantum transmission, so that the receiver can extract only one message, never both. In 1984, Bennett and Brassard, that were familiar with Wiesner's ideas, studied the possibility of combining these ideas with public encryption. The former quantum encryption systems, developed between 1982 and 1984, were not very practical but, in 1989, at IBM Thomas J. Watson Research Center, important researches led to a significant prototype [4].

Quantum theory represents the basis of quantum encryption, measuring being a part of it, so that it is possible to built a quantum channel for transmitting signals based on quantum phenomena, through which every attempt of monitoring will alter signals in a detectable manner. This effect is due to the fact that, in quantum theory, some pairs of physical properties are complementary, so that measuring one of them is disturbing the other. This statement, known as the *Heisenberg uncertainty principle*, can be applied in order to build a completely secured channel based on the quantum properties of light, considering the fact that the smallest quantum of light, the photon, can be polarized in order to send the information through a secured channel. At the receiver, these photons have to be measured, building thus the greatest part of the transmitted information [3, 5].

Just as the bit represents the elementary unit of classic information, *qubit is the elementary unit of quantum information*. Qubit is not a binary unit, it is a quaternary unit, it exists in states corresponding to a mix of the classic states that is a *qubit may be zero, one, or simultaneously zero and one, with a numerical coefficient representing the probability for each state.* A qubit is a quantum system in a Hilbert bidimensional space, dim$H$ = 2. The basis of H is {|0⟩,|1⟩}, a computational basis. A qubit state is described as $c_0|0\rangle + c_1|1\rangle$, with $|c_0|^2 + |c_1|^2 = 1$ [5].

Quantum cryptography, or key quantum distribution, made its debut with the **BB84 protocol**, presented in Figure 3, proposed by C.H. Bennett and G. Brassard in 1984 [1].

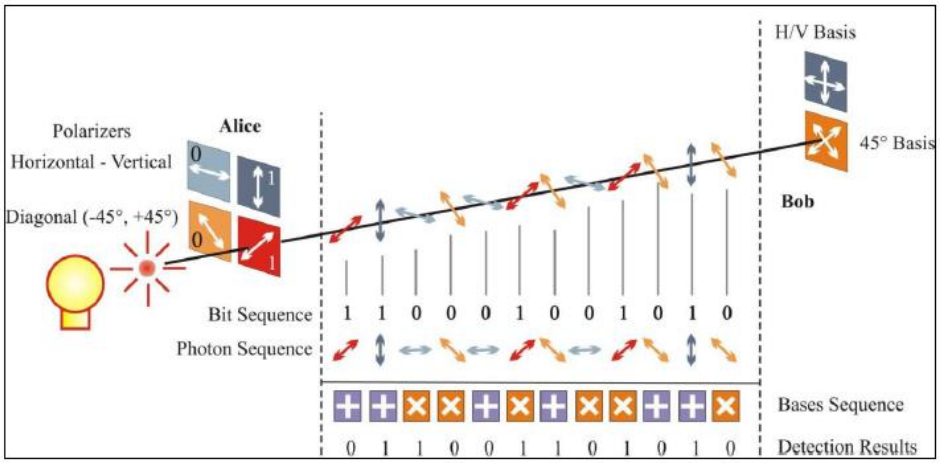

Fig. 3. BB89 Protocol diagram [2]

BB84 protocol defines the manner of distributing a secret random key between two entities, Alice and Bob, using singular qubits, along a quantum channel. The security of quantum distribution is given by the random measurements upon the qubits in one of the two non-orthogonal bases, and also by the fact that quantum mechanics restricts a cryptanalist to obtain any information about an unknown qubit without disturbing it [1].

Quantum Encryption BB89 Protocol Implementation

The implemented application is referring to data transmission between the two entities, Alice and Bob. The message is encrypted using a symmetric key sent from Alice to Bob.

The initial key is a completely random bit sequence, named *raw key*. The first stage of the application assumes forming the random raw key that has to be sent on a secure channel. Figure 4 presents the screen shot of the application graphical interface corresponding to this phase: one has to push the *Generate the key* button on Alice form. Consequently, a 32 bit random key is obtained.

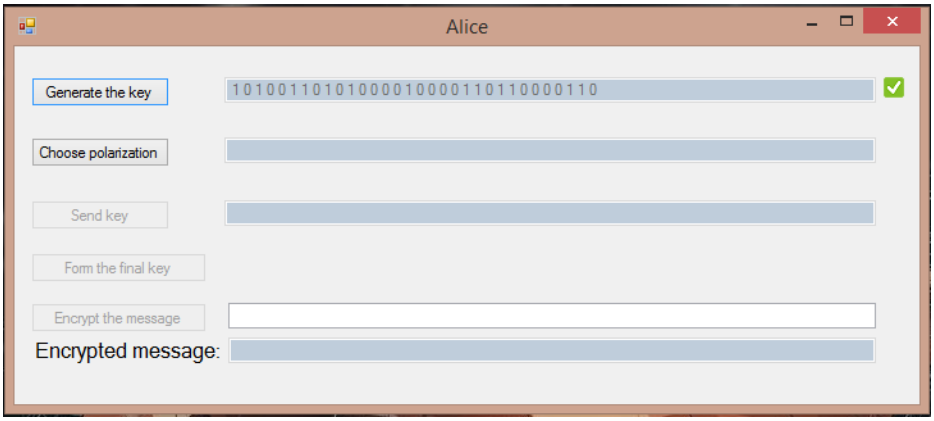

Fig.4. Raw key obtaining phase

The security of the channel is conferred by the laws of quantum physics. In this respect, the key bits will be transmitted using polarized photons, thus performing a quantum encryption of the key. The photons polarization is obtained by using two databases of polarization: horizontal – vertical and diagonal – antidiagonal.

In the second stage, one randomly chooses the polarization databases for each photon and these are encrypted, thus resulting a quantum encrypting key as an equivalent of the former raw key. The main difference is that this key is not represented by means of bits, but of qubits. Consequently, Alice sends the quantum key on a secure channel, usually an optical fibre.

In this respect, Alice will have to send the key by means of quantum encryption, using photons. As seen in figure 5, Alice has to choose between two polarization databases, denoted by „1”and„2”, „1”meaning a horizontal –vertical database and „2” a diagonal–antidiagonal database. For this, one has to click the button *Choose polarization* displayed on the interface. The polarized photons are created as follows:

- Is Alice has to send a bit 1, and the polarization database is also 1, then the photon will be vertically polarized (V);
- Is Alice has to send a bit 0, and the polarization database is 1, then the photon will be diagonally polarized (D);

- Is Alice has to send a bit 1, and the polarization database is 2, then the photon will be horizontally polarized (H);
- Is Alice has to send a bit 0, and the polarization database is 2, then the photon will be anti diagonally polarized (A).

When the polarization is complete, Alice will send the key to Bob, with a click on *Send key* button. The key will be represented as A, D, V, H symbols, signifying the polarization of each photon (fig. 5).

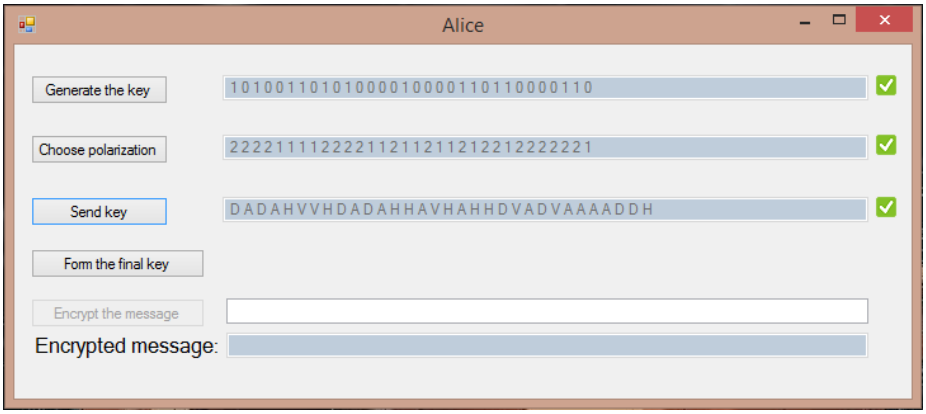

Fig. 5. Quantum encrypted key obtaining phase
D-diagonal polarization; A- antidiagonal polarization; V- vertical polarization;
H- horizontal polarization.

Bob receives the quantum key and measures it, using for each photon a randomly chosen polarization database (click on *Choose polarization* button, figure 6), thus obtaining a key. This key is different from the raw key, having only the same size, given the fact that the filters Bob and Alice have chosen do not always match.

The next stage assumes the comparison of the polarization databases (*Exchange information* button, fig. 6), only the qubits obtained by using the same polarization database being retained and used in order to form the final symmetric key, identical for both entities.

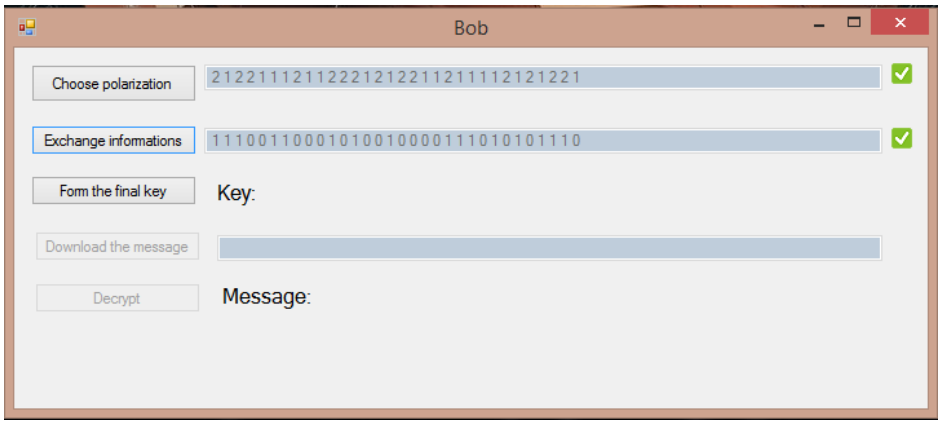

Fig. 6. Choice and comparison of the polarization databases at the receiver

The *Exchange information* process assumes measuring the received photons, using the chosen polarization databases, obtained as a result of the comparison. The filtered raw encryption key thus formed is presented in Figure 7.

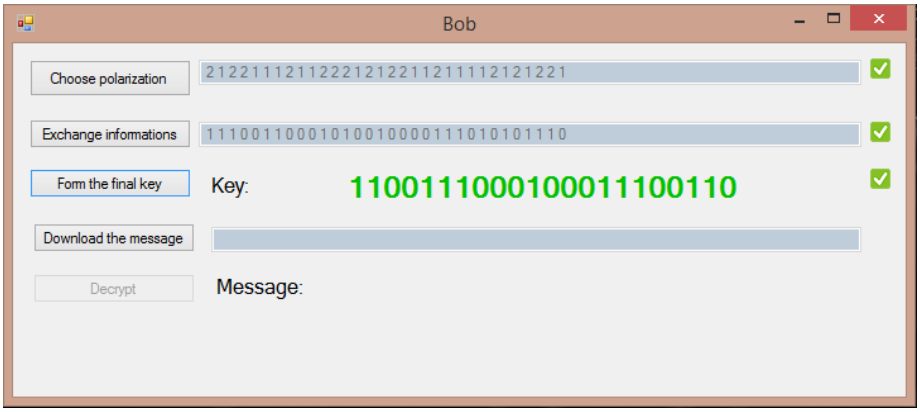

Fig. 7. Raw encryption key obtained by Bob as a result of the information exchange

Alice, pushing the *Form the final key* button, downloads Bob's polarization databases and compares them with hers. Finally, the program delivers two identical keys (presented in figure 8), that Alice and Bob will be using in order to encrypt/decrypt the transmitted messages.

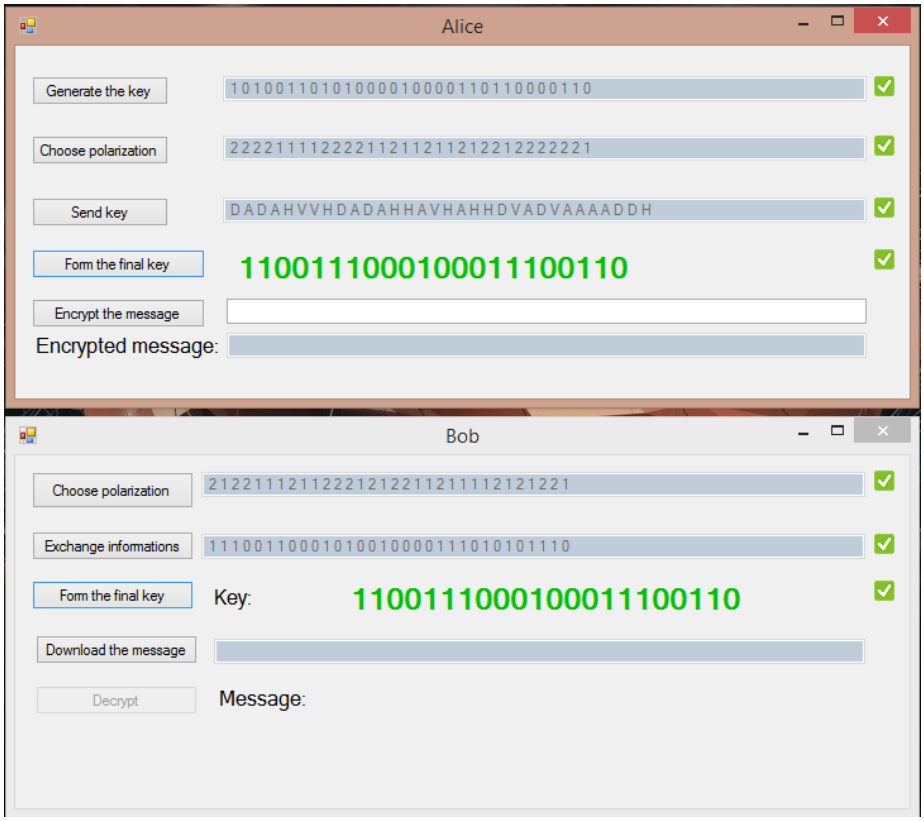

Fig. 8. Identical encryption keys obtained by Alice and Bob

The next stage refers to Alice's encryption of a message using the obtained key and sending it to Bob, on a possible unsecure channel. Receiving the message, Bob will decrypt it using his own cryptographic key.

In this respect, using the *Encrypt the message* button, Alice introduces the message "Hello, world!" she wishes to send to Bob. As a result, the message will be encrypted, displayed in the corresponding textbox, *Encrypted message*, as seen in Figure 9.

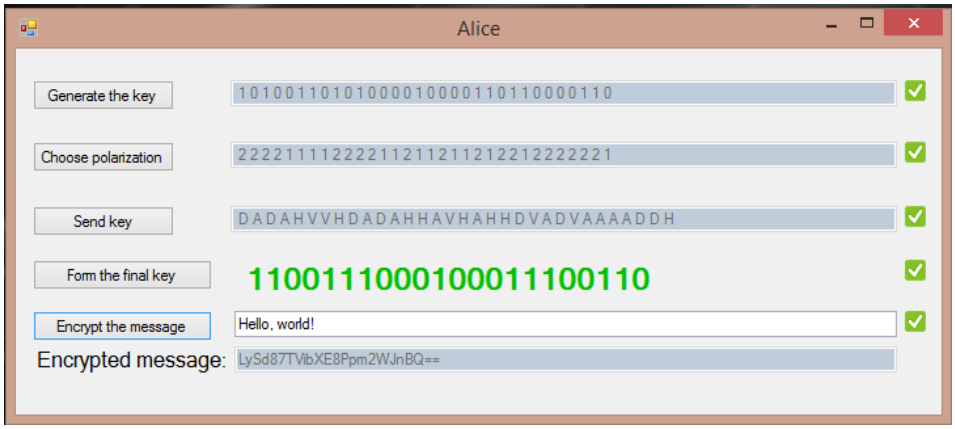

Fig. 9. Encrypted message sent from Alice to Bob

Next, the encrypted message is downloaded (Bob pushes the *Download the message* button, figure 10) and the decryption of the received message is performed. Figure 10 displays the decrypted message, identical to that transmitted by Alice.

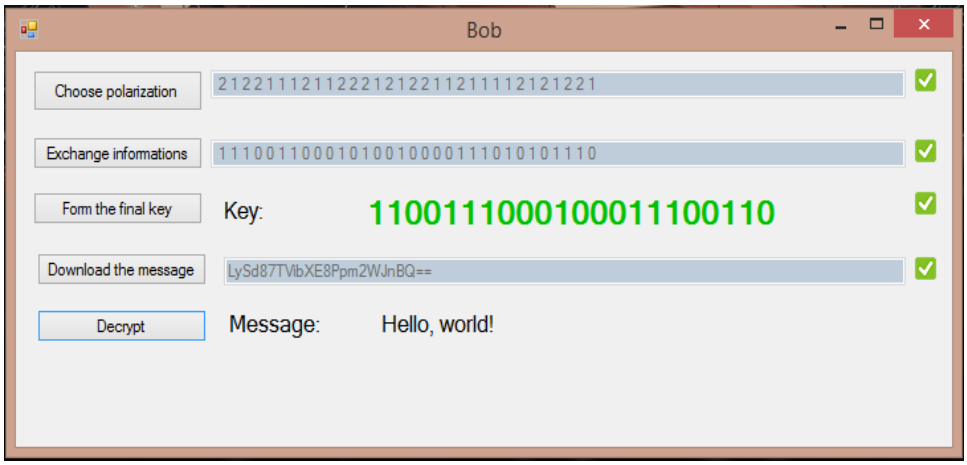

Fig. 10. Decrypted message obtained by Bob by using the same decryption key as Alice

Due to the fact that in the presented application, the simulated transmission environment is an ideal one, without interception, there were not considered the error correction and the estimation calculus of these errors. In practical applications, however, it is necessary to use algorithms of correction for errors, before final key formation

Conclusion

The paper presents the concept of quantum cryptography, emphasizing the Heisenberg uncertainty principle, the concept of qubit – as the unit of quantum representation of the information, and there is analysed the quantum encryption BB84 protocol.

The aim was to build the quantum encryption BB84protocolexperimental application, simulated by means of a graphical interface that presents the quantum key distribution between two legal entities, emphasizing the characteristic stages, from key generating to successful message decryption, with special attention paid to implementing the laws of quantum physics in order to ensure the security of the channel.

Quantum encryption using BB84 protocol can be performed using weak coherent laser pulses. However, this type of system is vulnerable to the attack that divides the number of photons, if there are more than one single photon in a pulse. In this case, a cryptanalist can steal a photon, measure it and, thus, obtain information regarding the key. Quantum distribution key protocols have been, therefore, extended in order to use entangled qubits pairs.

As future directions, one may consider the comparison between BB84 and BBM92 quantum protocols, in order to conclude which is the one with superior performances regarding a greater speed of the encryption key distribution.

References

1. Bennet, C. H., Brassard, G. – Quantum Cryptography: Public key distribution and coin tossing, *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, p. 175, 1984.
2. Cobourne, S. – *Quantum Key Distribution Protocols and Applications*, Technical Report RHUL-MA-2011-05, 8th March 2011.
3. Erven, C. – *On Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source*, PhD thesis, University of Waterloo, Waterloo, Ontario, Canada, 2007.
4. Sergienko, V.A. – *Quantum Communications and Cryptography*, CRC Press, 2006.
5. Van Assche, G. – *Quantum Cryptography and Secret-key Distillation*, Cambridge University Press, 2006.

Aplicaţie protocol BB84 pentru criptare cuantică

Rezumat

În prima parte a lucrării au fost prezentate noţiuni generale referitoare la conceptul de criptare cuantică şi de qubit, ca unitate elementară a informaţiei cuantice, în contextul discuţiei referitoare la securitatea transmisiei informaţiei din punct de vedere al distribuţiei cheii. Lucrarea detaliază protocolul de criptare cuantică BB84, pe baza căruia este construită aplicaţia experimentală simulată prin intermediul unei interfeţe grafice care prezintă etapele caracteristice, de la generarea cheii de criptare până la decriptarea cu succes a mesajului informaţional, subliniind utilizarea legilor fizicii cuantice pentru asigurarea securităţii transmisiei.