ON QUANTUM CRYPTOGRAPHY

Review Paper

DOI 10.7251/ZBKEN1901041J	COBISS.RS-ID 8274456	UDK 003.26:004.056.55

Stevo Jacimovski[1]
University of Criminal Investigation and Police Studies, Belgrade, Serbia

Jovan Setrajcic
Faculty of Sport, Union University, Belgrade

Jelena Lamovec
Institute of Chemistry, Technology and Metallurgy, Belgrade

Abstract: In the late twentieth century, human race entered the era of information technology (IT). The IT industry, which deals with the production, processing, storage and transmission of information, has become an integral part of the global economic system, a completely independent and significant sector of the economy. The dependence of the modern society on information technologies is so great that omissions in information systems may lead to significant incidents. Telecommunications are the key information technology industry. However, information is very susceptible to various types of abuse during transmission. The units for data storage and processing can be physically protected from anyone wishing harm, but this does not hold true for the communication lines that span hundreds or thousands of kilometers and are virtually impossible to protect. Therefore, the problem of information protection in the field of telecommunications is highly significant. Cryptology, particularly cryptography, deals with this issue. Quantum cryptography is a relatively new field ensuring safe communication between the sender and the recipient using the laws of quantum physics. This paper seeks to address the principles of the quantum distribution of a key for information encryption and the fundamental problems arising from the execution.

Keywords: cryptography, algorithms, encryption, key, quantum physics, protocols

INTRODUCTION

According to Anglo-Saxon tradition, the participants in the process of encryption and decryption are called Alice and Bob. An enemy, who wishes to disclose unauthorized information shared by Alice and Bob, is called Eva

[1] Stevo Jaćimovski: Full Professor, University of Criminal Investigation and Police Studies, Belgrade, Serbia, Belgrade. E-mail: stevo.jacimovski@kpu.edu.rs

which is derived from *eavesdropper* (Bennett, 1992). The enemy, it is assumed, has unlimited computer resources and is familiar with the use of cryptographic methods, algorithms[2], protocols[3], and so on (Dugić, 2009).

The primary task of cryptography is to transform an initial text (plaintext) into an arbitrary string of characters called a cryptogram. The number of characters in the plaintext and the cryptogram may differ. The secrecy of the encryption algorithm itself cannot, in principle, ensure the unconditional security of the cryptograms, as it is assumed that Eva (the enemy) has infinitely large computer resources. Therefore, public key algorithms are used nowadays. The security of modern cryptosystems is based on the secrecy of a small item of information called a key, rather than on the secrecy of an algorithm. The key is used to manage the encryption process and should be easily changeable at any time. At the end of the nineteenth century, the Dutch scientist Kirchhoff formulated a rule by which the security of a key is ensured if the entire encryption system, other than the secret key, that is, the information that manages the process of cryptographic transformation, becomes known to the enemy, (Kilin, Horosko & Nizovcev, 2007).

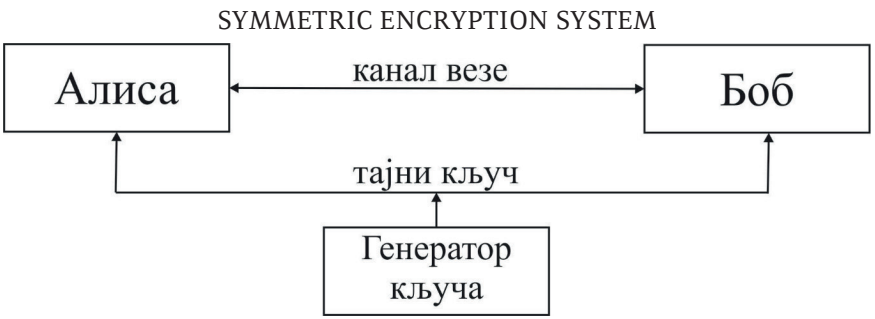


Figure 1. Structure of symmetric cryptosystems[4]

In symmetric cryptosystems, the sender and the recipient use the same secret key (Figure 1). An item of information is also encrypted and decrypted with this secret key. The key must be periodically updated and distributed at the same time to both the sender and the recipient. The process of distributing secret keys among the regular participants in the information exchange is a very complex process. If an illegitimate user (Eve) had the secret key, it would

[2] An algorithm is a set of commands, instructions, actions, calculations executed in order to achieve a result of initial data.

[3] A protocol is a set of actions (instructions, commands, calculations, algorithms) executed in a particular order by two or more actors with the aim of achieving a result.

[4] Translator's note: Alice – link channel– Bob; secret key; key generator.

enable the knowledge of the information exchanged between Alice and Bob (Румянцев, Голубчиков 2009).

Symmetric cryptographic algorithms provide a high level of protection, as long as the key is only known to the sender and the recipient of the message. Therefore, the basic measure of the security of symmetric algorithms is the method of key distribution. The well-known and most widespread symmetric algorithm is DES and an improved version of 3 DES (Čisar, 2015).

This problem has previously been solved by a non-cryptographic method – by transferring the key to the physically protected eavesdropping channels. However, the creation of such a channel and its maintenance in operational readiness in case of an urgent need for a key transfer is very long and costly. Therefore, in the conditions of a constant increase in the intensity of information flows, this key distribution method has become less acceptable and satisfactory.

The problem has been successfully solved within modern cryptography. There are two ways to solve the key distribution: mathematically and physically. The mathematical method is realized by using a two-key based protocol or public-key cryptography. The physical way is realized by means of quantum cryptography.

ASYMMETRIC ENCRYPTION METHOD

Figure 2. Structure of asymmetric cryptosystems[5]

Asymmetric cryptosystems use two keys – Figure 2. The first key is public and is available to all users of the information exchange. Information is encrypted with this key. Only the recipient (Bob) has the second secret key. Decrypting information with the public key is impossible. Also, the decryption key cannot be determined by using public key encryption (Румянцев & Голубчиков, 2009).

[5] Translator's note: Alice – link channel – Bob; public key – key exchange center – secret key.

In 1976, the scheme of asymmetric cryptography was proposed by Diffie and Hellman, Stanford University. If Alice and Bob want to establish a secret key, it is enough to follow this protocol (Jakus, 2016):

- Alice generates a random number A, computes $P=e^A$ and sends P to Bob
- Bob generates a random number B, computes $Q=e^B$ and sends Q to Alice.

Then Alice and Bob compute the secret key, K, as shown in Figure 3.

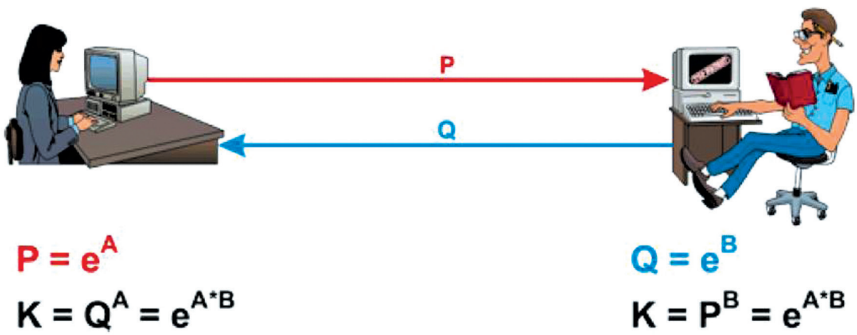


Figure 3. Diffie–Hellman protocol

Suppose Eva has P and Q. Can she compute K? To compute K, Eva must compute A or B because she can then repeat the computation of the key in the same way as Alice or Bob can. The idea is that the calculation A or B requires computing the discrete logarithm:

$$A=\ln P,\ B=\ln Q$$

for which there is no effective way (Stipčević, 2007). The security of the Diffie–Hellman method is based on the complexity of the discrete logarithm. The most famous algorithm within the group of asymmetric cryptographic methods is the RSA.

In the first case, different keys are encrypted and decrypted in the two-key based protocol, so there is no need to keep the secret key secure. However, due to the extremely low performance characteristics and exposure to the special types of attacks, such ciphers have proved inappropriate to close direct user information. Instead, asymmetric ciphers are used as part of combined schemes, when a string of data is encrypted with a symmetric cipher on a one-time key, which is encrypted with a two-key cipher and is transmitted in this form along with the data.

In the second case, in public-key cryptography, the schemes for the distribution of the key over open communications channels solve the same problem in a slightly different way: during an interaction, two participants

exchanging information generate a shared secret key, which is then used to encrypt the data being transferred using a symmetric cipher. Furthermore, intercepting information in a channel during a generating session of such a key does not allow the enemy to obtain the key by himself or herself.

The security of two-key cryptosystems is based on a slow technical progress. Their security is based on the problem of factorizing large numbers and computing discrete logarithms in certain final groups. These problems are believed to be "tough" in the sense that they might be solved by guessing all possible solutions (keys), with a number of steps increasing exponentially with the key length.

Secrecy in the modern world is based on the idea that something is computer-secure, in other words, it is secure in the sense that it would take too much computer time and power to break the cipher (Vedral, 2014). Finding a factor for large numbers is a difficult problem. Let us imagine the number 100. What are its factors? Two times 50 equals 100. But this is also true for 4 times 25, or 5 times 20 or 10 times 10. The number of factors grows rapidly and finding all of them poses a significant difficulty to every modern classical computer.

Nevertheless, with the expected emergence of quantum computers for which rapid factoring algorithms have been developed, the cryptographic systems based on the mathematical cryptographic methods can be compromised.

The procedure for this was developed by Peter Shore (Shor, 1994) who created an algorithm according to which a quantum computer can exist simultaneously in many different states, as it uses the quantum superposition principle. Let us imagine a single computer in a superposition, which is simultaneously at different locations. In each of these locations, we can configure a computer to share our number with another number to search for factors. In this way, we get an extremely rapid acceleration of the solution to the factorization problem, given that one quantum computer now simultaneously performs all these divisions, one at each spatial location. According to experts, a quantum computer that can break the RSA crypto system will be designed in about 15-25 years.

It is precisely for this reason that the idea of protecting information must be sought in, colloquially speaking, "hardware", that is, by using the laws of quantum mechanics for protection.

Therefore, the need to protect cryptosystems has arisen for other reasons. The solution of key distribution is realized in quantum cryptography based on the laws of physics (Jaćimovski & Šetrajčić, 2016).

The basic arguments for this are twofold:

- It is impossible to copy an unknown quantum state
- Without perturbation, it is impossible to have information about non-orthogonal quantum states (in other words, when accessing an information channel, Eva changes the status of the information holders)

Quantum cryptography uses the uncertainty of the quantum world during the measuring process, the so-called Heisenberg's uncertainty principle (Heisenberg, 1974). With quantum physics, a communication channel which cannot be eavesdropped without interfering with the transmission can be established. Two users who communicate with each other can always detect the presence of the third party trying to discover the key.

Also, an eavesdropper cannot copy unknown quantum bits, the so-called qubits, that is, unknown quantum states, because of the no-cloning theorem. Quantum cryptography is only used to generate and distribute a key, rather than to transmit messages. The generated key can thus be used in a cryptosystem for encryption and decryption.

In this way, quantum cryptography allows for relatively fast key exchange and the detection of Eve's attempts to enter the link channel. Note that the occurrence of errors during the transmission and reception of quantum states does not necessarily lead to the loss of secrecy. A critical error is defined for each protocol of quantum cryptography, above which secrecy is not ensured. If the error level (usually expressed in terms of percentages) is below the critical level, then the error correction protocols and the subsequent compression of the remaining bits are used to create the key. Following these procedures, Eva has as much information about the key as Alice and Bob want her to have (Picek & Golub, 2009).

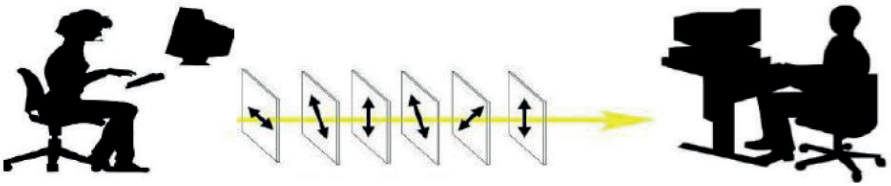
Presently, three forms of quantum state encryption are used in quantum cryptography: polarization encoding, phase enciphering and encoding using time shifts. This paper demonstrates the procedure for the polarization encoding of quantum states, the so-called BB84 protocol, and elaborates the E91protocol. Other protocols of quantum cryptography are also used.

Example of the BB84 protocol without noise

The BB84 protocol (Bennett & Brassard, 1984) is the historical first protocol for quantum key distribution (Kilin, Khoroshko & Nizovtsev, 2007), whose security is based on the principles of quantum mechanics, making it absolutely safe if there is no noise in the quantum channel. The absence of noise in a given situation assumes that the quantum state of particles does not change along the quantum channel.

The BB84 protocol is formulated in the language of individual photons, (Figure 4), although it can be applied to other realizations of a qubit. To encode information, four polarization states forming two interconnected non-orthogonal bases are used in the protocol: rectangular $|\leftrightarrow\rangle$ and diagonal $|\updownarrow\rangle$

$$\left|\swarrow\right\rangle = (\left|\leftrightarrow\right\rangle + \left|\updownarrow\right\rangle)/\sqrt{2} \qquad \left|\nwarrow\right\rangle = (\left|\leftrightarrow\right\rangle - \left|\updownarrow\right\rangle)/\sqrt{2}$$



Quantum channel – sending polarized photons

Figure 4. The BB48 protocol demonstration

The essence of the BB84 protocol is that one of the users (Alice) randomly selects a series of bits (stage 1) and a series of bases (stage 2) and then sends a user (Bob) a string of photons (stage 3) each of which encodes one bit from the selected string in the base corresponding to the prime number of that bit, where the states$|\leftrightarrow\rangle$ $|\nearrow\rangle$ are encoded into (0) zero, and the states $|\uparrow\rangle$ $|\searrow\rangle$ into one (1). In obtaining a photon, Bob randomly selects the measurement base (rectangular or diagonal) for each photon and independently of Alice, (stage 4), analogously interprets the result of his measurement for each photon in two ways, as a zero or one (stage 5). In accordance with the laws of quantum mechanics and following the measuring of the diagonal photon in a rectangular base, its polarization turns into the horizontal or vertical line and vice versa, with random results. In this way, Bob obtains the results coinciding with the state of the photons sent in about half the cases (50%), that is, when he correctly hits the base.

The next stage of the protocol is realized via a public channel, through which Alice and Bob can openly convey classical information to each other. At this stage, we assume that Eva can listen to the announcements by both parties, but she cannot change them or send notifications instead of them. To begin with, Alice and Bob determine (via a public channel) which photons were successfully obtained by Bob and which of them were measured in the correct base (stages 6 and 7). After that, Alice and Bob have the same bit values encoded in these photons, regardless of the fact that this information has never been established in the open communication channel (stage 8). In other words, each of these photons carries a bit of random information, which is known only to Alice and Bob and no one else. Information about the photons measured in the wrong base is rejected, so Alice and Bob get the so-called sieved key, which, in the event that Eva did not intercept the information, should be the same for both parties.

Table 1. Example of the realization of the BB84 protocol. States $|\nearrow\rangle$ $|\nearrow\rangle$ encrypt (0) zero, while states $|\updownarrow\rangle$ $|\nwarrow\rangle$ encrypt one (1). Rectangular and diagonal bases are indicated by ⊗ and by ⊕.

Stage 1	Random bit transmission (Alice)	0	1	1	0	1	1	0	0
Stage 2	Random bit transmission (Alice)	⊗	⊗	⊗	⊕	⊕	⊗	⊗	⊕
Stage 3	Polarization of photons distributed along the quantum channel	⤡	⤡	⤢	↔	↕	⤢	⤢	↔
Stage 4	Randomly received bases (Bob)	⊕	⊕	⊗	⊕	⊕	⊕	⊕	⊕
Stage 5	Bits received by Bob	0	0	1	1	1	0	0	0
Stage 6	Bob informs Alice about the bases of reception	⊕	⊗	⊗	⊗	⊕	⊕	⊕	⊕
Stage 7	Alice tells Bob which of their bases are harmonized								
Stage 8	Sieved key			1		1			0
Stage 9	Bob discovers a portion of bits					1			
Stage 10	Alice confirms it								
Stage 11	Sieved key after error assessment			1					0

Suppose Eva is eavesdropping on a quantum channel. Due to the random selection of a rectangular or diagonal base, Eva influences the information in such a way that it changes the bits of the sieved key, which would have to be the same for Alice and Bob if there was no Eve. No measurement of the photons performed by Eve gives more than one half of the bit information encrypted by this photon; any such measurement gives b bits of information (b <1/2) and is not in compliance with the probability which is ultimately equal to $b/2$ if the measured photon or its replacement is measured in the initial base by Bob. Alice and Bob can check if someone is eavesdropping on them by openly comparing a portion of bits (stages 9 and 10) for which they must have the same information, although these bits cannot, any longer, be used for the secret key. The position of the bits being compared should be a random subset of the properly measured bits so that the presence of Eve must be noticed. If all the bits compared match, it is clear that there was no eavesdropping, and the remaining bits properly measured can be used for the secret key encryption (stage 11) and transmission over the open channel.

Once this key is used, Alice and Bob repeat the procedure to create a new secret key.

The security of the BB84 protocol

The BB84 protocol would be threatened if Eve is able to perform the following interventions on the quantum channel (Markagić, 2012):

1. To measure the polarization of the photon sent by Alice, reproduce the same one and send it to Bob
2. To reproduce the photons sent by Alice

In the first case, Eva would have the same information that Alice and Bob had, so at the end of the procedure they would have the same key. However, Alice uses photons from the conjugated bases, in other words, there is no orientation of a polarizer with which Eva could with certainty distinguish the polarization of photons. In the second case, Eva wants to assure the polarization of the photons with a number of differently oriented polarizers. However, the reproduction of an unknown quantum state is not possible due to the no-cloning theorem.

In the communication process between Alice and Bob, a portion of the photons accurately measured is likely to be detected incorrectly. Also, if Eva attempts to measure the photons sent by Alice before they reach Bob, errors are likely to occur due to the fact that Eva is attempting to measure the data pertaining to the polarization of photons. These two situations cannot be distinguished: natural or artificial sounds look the same. As a result, Alice and Bob agree on a smaller cryptographic key in three phases viz. error assessment, information leverage and privacy enhancement.

The E91 protocol (Ekert, 1991)

Further, the improvement of cryptosystem reliability can be achieved using the Einstein-Podolsky-Rosen (EPR) effect (Einstein, Podolsky & Rosen, 1935). The EPR effect occurs when a spherical symmetric atom radiates two photons in opposite directions to two observers. The photons are emitted with an unspecified polarization, but due to the symmetry of their polarization, they are always opposite (the quantum interference effect). An important feature of this effect is that the polarization of photons becomes known only after having been measured. Based on the EPR, Ekert proposed a crypto-scheme guaranteeing the security of the key transfer and storage. The sender generates a number of the APR photon pairs and leaves one photon from each pair for himself or herself, and sends the other one to his or her partner. At the same time, if the registration efficiency is close to the unity, when the sender receives the value of polarization 1, his or her partner will register the value 0 and vice versa. Clearly, in this way, partners, whenever necessary, can get identical pseudo-random code sequences. Practically, the implementation of this scheme is problematic due to the low efficiency of recording and measuring the polarization of one photon.

CONCLUSION

The task of cryptography is the exchange of secret messages. There are traditional methods that practically guarantee a secure communication (between Alice and Bob) if the secret decryption key is known to both parties, and at the same time, the key is not known to anyone else, even the potential enemy Eve.

It is this presumption of the secrecy of the "secret key" that is the weakest link in classical cryptography. The only task of quantum cryptography is to ensure a secret key. Thus, in quantum cryptography, not only messages are exchanged via the so-called quantum channel, but also secret keys. Today, there are already commercial devices as well as dozens of implementations of public and corporate secure network communications using the quantum key distribution technologies. The advantage of these technologies is the unconditional security based on the phenomena of quantum mechanics. Today, it is almost possible, with the unconditional security, to generate and distribute a secret key between two parties connected by optical fibers at distances up to 150 kilometers in a few seconds. Eavesdropping on communications by a third party does not lead to the revealing of a secret, but only to the reduction of the speed of key generation, with both parties immediately knowing that the line is being actively eavesdropped. The main disadvantage of these systems is the limited key generation speed, which depends directly on the distance of the participants, the inability to increase the signal or transmission through a type of relay, practical limitations solely on fiber optic communications, as well as the cost of system implementation (Ijačić, 2014).

In ideal systems of quantum communication, the interception of data is impossible, as the participants in the exchange of information immediately identify the interception as errors occurring in the transmission. However, the actual systems are different from the ideal ones.

Unlike the ideal quantum communication system, the actual quantum communication systems are unable to ensure the absolute secrecy of the data transmitted, due to the fact that there is a fond of its own errors in the system, behind which the attempts to intercept information can be hidden, as well as the attenuation of communication channels due to the necessity of using multiphoton pulses. The use of strong photon pulses leads to the dampening of the transmission of information enabling the interception of silent data. This is a factor that cannot practically be removed, as the quality of the channel through which the information is transmitted cannot always be controlled.

However, before the quantum communication systems is applied in practice, a number of technical difficulties need to be solved, such as the development of stable sources of single photons and single-photon detectors that would operate in a normal temperature range and should not be cooled by liquid gases. Different correction codes should be used to fight system errors, while the procedures for increasing security should be used to reduce the

importance of intercepted bits. Additionally, extra security measures of purely technical nature may be undertaken.

Acknowledgements: This paper is part of the project by the Ministry of Education, Science and Technological Development of the Republic of Serbia, number OI 171039, TR34019, and TR32008, the Ministry of Science and Technology, Higher Education and Information Society of the Republika Srpska – the "Funding thermodynamic engineering and the development of software package for researching phonon nanostructures" project.

REFERENCES

Bennett, C. H., Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing* (pp. 175-179). Bangalore, India.

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

Čisar, P (2015). Opšti aspekti kvantne kriptografije. *Info M, 14*(54), 37-44.

Dugić, M. (2009). *Osnove kvantne informatike i kvantnog računanja.* Kragujevac: PMF Kragujevac.

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

Ekart, A. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters*, *67* (6), 661-663.

Hajzenberg, V. (1974). *Fizika i metafizika.* Beograd: Sazvežđa.

Ijačić, S. (2014). Primena kvantne mehanike u kriptografiji, kvantno računarstvo i post-kvantni šifarski sistemi, Master rad. Beograd: Univerzitet Singidunum.

Jaćimovski, S., Šetrajčić, J. (2016). Physical Fundamentals of Quantum Cryptography. *Archibald Reiss Days* (pp. 276-292). Belgrade: Academy of Criminalistic and Police Studies.

Jakuš, M. (2004): Kvantna kriptografija, Faculty of Electrical Engineering and Computation, Zagreb, http://os2.zemris.fer.hr/kvant/2004_jakus/

Килин С.Я., Хорошко Д.Б., Низовцев А.П. (2007). *Квантовая криптография: идеи и практика.* Минск: Беларуская навука.

Markagić, M. (2012). Protokoli i pravci razvoja kvantne kriptografije. *Vojnotehnički glasnik*, *LX* (1), 250-265.

Picek, S., Golub, M. (2009). Kvantna kriptografija: razvoj i protokoli. *Proceedings of the Information Systems Security* (str. 122-127). Opatija: MIPRO.

Румянцев К. Е., Голубчиков Д. М. (2009). *Квантовая связь и квантовая криптография.* Таганрог: ТТИ ЮФУ.

Shor, P. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *35nd Annual Symposium on Foundations of Computer Science* (pp. 124-134). Los Alamos: IEEE Computer Society.

Stipčević M., Kvantna kriptografija, http://www.irb.hr/users/stipcevi/download/fer/171203.pdf (2003)

Vedral, V. (2014). *Dekodiranje stvarnosti.* Beograd: Laguna.

Paper received on: 20. 02. 2019.
Paper accepted for publishing on: 29. 03. 2019.