Quantum Cryptography and Security of Information Systems

Dalibor Hrg
University of Zagreb,
Faculty of Electrical Engineering and Computing, Zagreb
dalix@fly.srk.fer.hr

Leo Budin
University of Zagreb,
Faculty of Electrical Engineering and Computing, Zagreb
leo.budin@fer.hr

Marin Golub
University of Zagreb,
Faculty of Electrical Engineering and Computing, Zagreb
marin.golub@fer.hr

Abstract: *We show concept of BB84 quantum key distribution (QKD) protocol and analyze its use as an information system. The difference between classical and quantum cryptography is presented in a way of understanding the main advantage of quantum information processing over classical information processing. At the end of the article, we present today and future use of quantum cryptography and possible impact on security of information systems.*

Keywords: *BB84, QKD, information, information system, quantum cryptography*

1. INTRODUCTION

Classical schemes for key distribution rely on the unproven computational assumptions. Since the RSA public-key cryptosystem is widely used, we shall consider a problem of prime factorization. If someone finds a fast procedure for factoring large integers, the RSA system will not exist anymore, and discretion of public-key cryptosystems could vanish overnight. We believe that a polynomial algorithm for prime factorization does not exist, because the problem of prime factorization is in the NP complexity class. But, this is just a belief.

The theory of quantum computation and quantum information gave us some new results related to hierarchy of complexity classes and information processing [3,5,7]. P. Shor found a polynomial quantum algorithm for prime factorization in 1994. To be used, the Shor's algorithm for fast factorization needs to be implemented on a quantum computer, but with the present technology this is not possible. Experiments and theory will perheps be at the same level in a few years, maybe decades. It is only a matter of time when new, quantum key distribution systems will be needed to overcome that threat.

Quantum cryptography – quantum key distribution (QKD) – allows two parties to communicate in absolute privacy during the presence of an eavesdropper, i.e. passive listener. The Heisenberg uncertainty principle of quantum mechanics assures a detection of the presence of an eavesdropper located somewhere on a quantum channel. In addition, an eavesdropper can't copy unknown qubits, i.e. unknown quantum states, due to no-cloning theorem which was first shown by Wooters and Zurek in 1984 [9].

The paper has two main objectives. Primarily, we want to explain main problems in classical cryptography and give a review on the first QKD protocol which secrecy is guaranteed by physics of quantum mechanics. Secondly, we shall present, in short, experimental achievements and future development of QKD.

2. PROBLEMS IN CRYPTOGRAPHY

In the language of cryptography, two persons known as Alice and Bob communicate in order to share a secret message, i.e. a plaintext. Alice will use a symmetrical cryptosystem – the system which requires the use of a secret key for both encryption and decryption – to encrypt the plaintext with a secret key, obtaining so a cryptogram. After that, Alice sends the cryptogram to Bob over a public communication channel. Bob then decrypts the cryptogram with the same system and secret key used by Alice, and obtains the original message – Alice's plaintext. To achieve that, first, Alice needs to give a secret key to Bob. This problem is known as key distribution, and it is a major problem in cryptography. For example, one simple solution could be face-to-face meeting between Alice and Bob. The third person is known as Eve who eavesdrops the public channel used by Alice and Bob. Eve can intercept all the data through the public channel during Alice's and Bob's communication, receiving so the cryptogram. In this general position, Alice and Bob can only rely on good security of today symmetrical cryptosystems, i.e. cryptograms. The systems like DES, AES, IDEA, etc., all use a secret key which length is shorter that the length of the plaintext. There exist a specific symmetrical cryptosystem, known as one-time-pad, in which the secret key has the same length as the message. Also, the system require a new key for each new message. Hence, the name "one-time-pad". The one-time-pad is perfectly secure cryptosystem, according to a proof by Shannon in 1949 [8]. The first one-time-pad was proposed by Gilbert Vernam of AT&T in 1926. Due to perfect secrecy, it is impractical to use, since Alice and Bob need to share a secret key every time they want to send a message.

The key distribution is the main problem in cryptography. If Alice and Bob want to communicate securely, they need to share a secret key before any encryption process can be started. Except, not so practical solution like the face-to-face meeting, there exist two main solutions: asymmetrical (public-key) cryptosystems and quantum cryptography. In public-key cryptosystems, each person has a private and a public key. The public key is released into public use, while the private key is secret. If Alice wants to send a plaintext (a secret key) to Bob, she will encrypt the plaintext with Bob's public key. Bob will then decrypt the cryptogram with his private key. Public-key cryptosystem was first proposed in 1976 by Whitfield Diffie and Martin Hellman. The first implementation was then developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1978. It is known as RSA and it is widely used. The problem is that public-key cryptosystems rely on unproven computational assumptions. Security and future use of these systems depends on further theoretical and mathematical progress. Some mathematical problems, like prime factorization and discrete logarithm calculation, are foundations of the most widely used public-key cryptosystems today. Theoretical results from last decade showed that quantum mechanical principles can be used to extract more computational power than any classical information processing can do. For example, some problems which are NP hard in classical computation are efficiently solvable on a quantum computer, i.e. on a new model of computation. The progress of present technology can't follow fast progress of theory, but some parts of quantum information processing were experimentally shown. Mainly, that experimental progress is related to the quantum cryptography – quantum key distribution (QKD). For more information on quantum information and computation see [3,5,7].

As we have mentioned, the second solution on the key distribution problem is QKD. QKD is the way of generating a secret key to both parties in a process of repetitive communication. During the QKD, Alice and Bob use two channels: a classical public channel and a quantum channel. First, Alice sends quantum bits, i.e. qubits or photons to Bob over the quantum channel which could be an optical fiber or a free-space optical link. Bob is measuring those qubits obtaining so a sequence of bits. The sequence depends on a coding system between two parties and chosen measurements which have random characteristic. Then Alice and Bob communicate over the public channel, in order to agree or disagree with Bob's received bits. This procedure must be repeated few times in order to make some error corrections and to gather enough bits to form a secret key. In next section, we shall describe how specific QKD protocol known as BB84 work and automatically detect Eve's presence. In QKD protocols, the public channel can be freely monitored by Eve. But, we need to put a limitation: Eve can't change the data on the public channel! This limitation is due to the problem known as man-in-the-middle (MitM) attack, i.e. when some intruder, like Eve, impersonates two other parties during the communication. It can be shown that Eve is a severe threat, and the integrity of data is broken. That's why, in classical cryptography, we use authentication to prevent MitM attacks. Efficient authentication methods exist, but only if two parties already share a secret key. However, so far there is now particular way to authenticate a public key [3]. The only reliable way to check a key's authenticity is to meet other person face-to-face or rely on some third side, i.e. a trusted third partie. Today, trusted parties are known as key distribution centers (KDCs) and public key managers (PKMs). But, we are currently not interested in protocols which consider all three sides, only two sides: Alice and Bob. Unfortunately, QKD does not provide any more convenient ways to counter a MitM attack. In real life, Alice and Bob should initially possess a secret key of definite length which is used for authentication of public channel messages. Then, using the QKD protocol, Alice and Bob can generate a much larger number of key bits (a secret key) for future use.

3. THE FIRST QKD PROTOCOL – BB84

The first quantum key distribution protocol was proposed by Charles Bennett and Gilles Brassard in 1984 [1]. It is also known as BB84. The system is based on the distribution of single particles or photons. The value of a classical bit will be encoded by the polarization of a photon. Before we give a description of the BB84 system, we would like to present some facts about photons and the quantum mechanical description used in the protocol.

Let us start with pulses of polarized light. Each pulse contains a single photon. A photon is either vertically (90°) or horizontally (0°) polarized, what is in the quantum mechanical Dirac notation denoted by $|\uparrow\rangle$ and $|\rightarrow\rangle$ respectively. The polarizations $|\uparrow\rangle$ and $|\rightarrow\rangle$ are also known as quantum states (vectors), and they form a basis in two dimensional Hilbert space which is associated with each photon. In order to communicate, a coding systems is necessary. State $|\uparrow\rangle$ codes 1, while $|\rightarrow\rangle$ codes 0. If Alice is sending only $|\uparrow\rangle$ and $|\rightarrow\rangle$ to Bob, we shall say that Alice is using the base $\oplus$. For example, if Alice sends sequence of photons: $|\uparrow\rangle$, $|\uparrow\rangle$, $|\rightarrow\rangle$, $|\rightarrow\rangle$; the binary number represented with these states is 1100. Now, if Bob wants to obtain a binary number sent by Alice, he needs to receive each photon in the same basis. In our case, this is $\oplus$ basis. A system which uses only one base, like $\oplus$, is vulnerable on eavesdropping. Eve can easily obtain states transmitted by Alice, since Alice can use only one base to send all photons in the sequence. Additional basis must be introduced. We shall say that except in the states $|\uparrow\rangle$ and $|\rightarrow\rangle$, a photon can also be in states $|\nearrow\rangle$ and $|\nwarrow\rangle$. These states denote linear diagonal polarization by 45° and 135° respectively. We also say that states $|\nearrow\rangle$ and $|\nwarrow\rangle$ form the basis $\otimes$. The state $|\nwarrow\rangle$ codes 1 while $|\nearrow\rangle$ codes 0. We have introduced a new basis in order to obtain four possible states in which a photon could be prepared. During the reception of a photon, Bob has two possibilities: either to measure the photon in the basis $\oplus$ or in the $\otimes$. For example, if Alice sends a photon in the state $|\rightarrow\rangle$ (0, basis $\oplus$), and Bob decides to measure the photon in the state $\oplus$, then he will obtain same state $|\rightarrow\rangle$, thus, the same bit 0. But, if he chooses the wrong (not-correlated) base $\otimes$, then the physics of quantum mechanics says that there exist equal probability of obtaining 0 or 1, i.e. states $|\nearrow\rangle$ or $|\nwarrow\rangle$. Easy calculation shows, that Bob's probability of obtaining the correct bit is 0.75 and the rest is probability of obtaining wrong bit (error). Hence, in 75% of time, Bob will receive correct bits from Alice, while in 25% of time, he will receive wrong bits [4]. This is the foundation of the BB84 protocol. If there is a presence of Eve, she will intercept the photon in order to measure it, and then she will resend it to Bob. Eve will obtain 75% Alice's bits correctly, but other photons will be corrupted, at least 25% of them. It can be shown, that Bob's probability of reception of the correct bit is decreased on 0.625. The probability of error is then 0.375 [6]. As a result, Eve's presence can be detected due to the increasing number of the error rate on Bob's side.

The BB84 protocol can be described in few stages of communication between Alice and Bob. Each stage will be described and figuratively shown. Following is a description of the BB84 protocol with perfect public channel, the one with no eavesdropper or any noise due to equipment. That is not a realistic situation, but latter, we shall show how protocol stages are arranged if there could be an eavesdropper on both channels, the quantum and the public one, and if there are some errors in bits due to noise in the environment.

Stage 1: Alice chooses at random both the basis and the polarization of her photons, and sends them to Bob. For example, she wants to send a string of bits 110101101001. For each bit, she will choose randomly a basis (either the ⊕ or the ⊗) as it is shown in Fig. 3.1. The photons are then polarized according to the coding system we have already described.

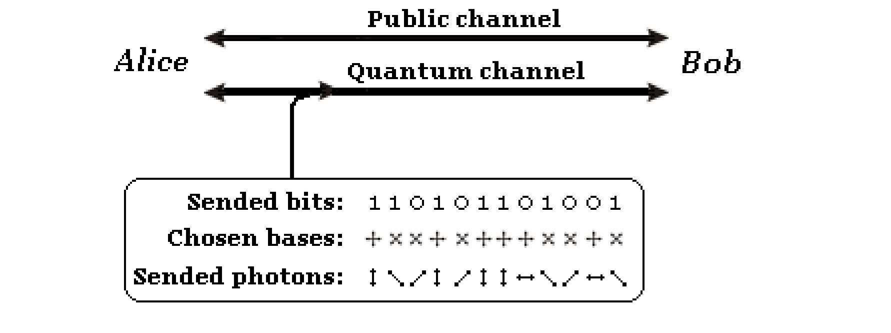
Public channel
Alice
Quantum channel
Bob
Sended bits: 1 1 0 1 0 1 1 0 1 0 0 1
Chosen bases: + × × + × + + + × × + ×
Sended photons: ↕ ⟍ ⟋ ↕ ⟋ ↕ ↕ ↔ ⟍ ⟋ ↔ ⟍

Fig. 3.1. Alice sends the photons, each one coded in randomly chosen basis.

Stage 2: Bob for each received photon chooses randomly a basis, in which he will measure that photon. If he chooses the same basis as Alice does, he will receive a correct state, i.e. interpreted bit will be correct. But, if he chooses the different basis, he will obtain with equal probability either 0 or 1. So, this is totally random process, and some bits will be interpreted correctly while others will be the errors. Bob's measurement process and his randomly chosen bases are shown in Fig. 3.2. Bob's sequence of interpreted bits in Fig. 3.2. is also known as a raw key. Hence, Alice's raw key is initial sequence of bits she has sent to Bob (Fig. 3.1).

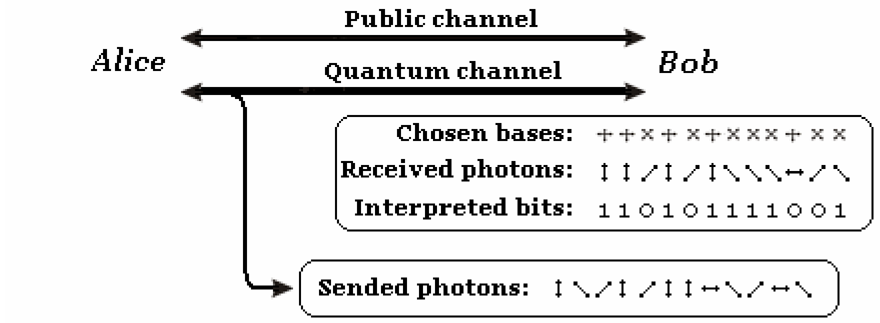
Public channel
Alice
Quantum channel
Bob
Chosen bases: + + × + × + × × × + × ×
Received photons: ↕ ↕ ⟋ ↕ ⟋ ↕ ⟍ ⟍ ⟍ ↔ ⟋ ⟍
Interpreted bits: 1 1 0 1 0 1 1 1 1 0 0 1
Sended photons: ↕ ⟍ ⟋ ↕ ⟋ ↕ ↕ ↔ ⟍ ⟋ ↔ ⟍

Fig. 3.2. Bob receives each photon with a randomly chosen basis.

Stage 3: Bob uses the public channel to discuss with Alice in order to find out what bits he received correctly. He does not tell the results of the measurement, i.e. the raw key, rather he announces the basis used to receive each Alice's photon. If Alice used a same basis for each photon, she will answer to Bob by an agreement. If Alice's basis is not the same as Bob's, she announces a disagreement. This is shown in Fig. 3.3. Alice and Bob then both remove bits, related to disagreeable bases, from their raw keys and obtain a shorter sequence of bits – a sifted key (Fig 3.4).

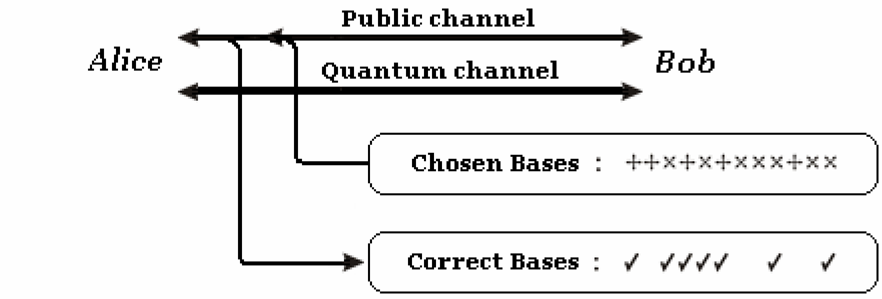

Fig. 3.3. Alice's and Bob's discussion over a public channel.

So, whenever Alice and Bob used the same basis, either ⊕ or ⊗ for a photon, they should share a same sifted keys. In the theory, the sifted key will be the secret key. But, this is only when we are dealing with perfect experiment. In real case, environment will change the photon's polarization in optical fiber, or Eve will corrupt some photons due to a wrong chosen basis during an eavesdropping. As a result, Alice's and Bob's sifted key will not match what means that Eve is eavesdropping.

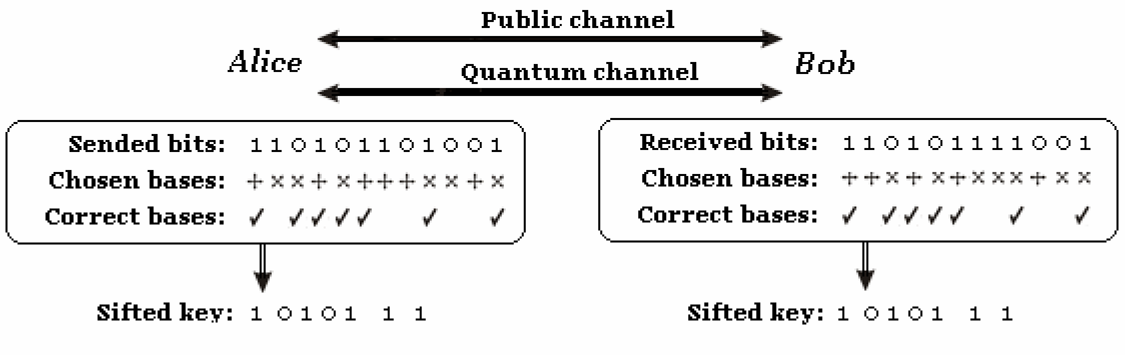
Public channel
Alice
Quantum channel
Bob
Sended bits: 1 1 0 1 0 1 1 0 1 0 0 1
Chosen bases: + × × + × + + + × × + ×
Correct bases: ✓ ✓ ✓ ✓ ✓ ✓ ✓
Received bits: 1 1 0 1 0 1 1 1 1 0 0 1
Chosen bases: + + × + × + × × × + × ×
Correct bases: ✓ ✓ ✓ ✓ ✓ ✓ ✓
Sifted key: 1 0 1 0 1 1 1
Sifted key: 1 0 1 0 1 1 1

Fig. 3.4. Alice and Bob extract the sifted key separately.

After the three main stages of the BB84 protocol, Alice and Bob poses the sifted keys which are, in practice, not equal. In that case, few other steps must be done: estimation of the error rate of the transmission based on random sample from the raw keys on both sides (random bits are then discarded from the raw keys); extraction of reconciled key, i.e. error free common key, using some error correction methods; and the end, privacy amplification, i.e. extraction of final secret key by randomly choosing a subset of bits from the reconciled key. This is done by using the information on error rate and the upper bound of the number of the bits that Eve could poses, since the reconciled key is partially secure [6].

The steps we have mentioned here are also common to other QKD protocols. For information purpose only, there also exist EPR and B92 QKD protocols. B92 protocol can be reduced to BB84, while EPR protocol uses quantum-correlated particles which are pairs of photons generated by certain particle reactions. Various QKD protocols and descriptions of specific error correction methods are described in [3,4,6].

4. EXPERIMENTS AND PRACTICALITY

The appropriate question at this point will be whether it is possible to build the BB84 protocol in practice. Bennet and Brasard, the authors of [2], implemented the first BB84 protocol using a simple light emitting diode (LED). The photons were transmitted through free-space, and the distance between two parties were only 32 cm long. There is a severe problem with the implementations of the BB84 over the long distances. Optical fibers, which are used as quantum channels, ruin the polarization of photon over a long distance transmission. It looks like, one should use an optical free-space transmission in order to avoid the problems with polarization. But, in that case, new problems crop up. Free-space distribution faces with problem of transmission photons through turbulent media and receiving single photons due to high background noise [3]. Another, very severe problem is that a single photon gun, currently, does not exist. In theory, we want to transmit a single photon for a single bit of information. But, this requirement is not fulfilled in experiments. Puls of light contains more than one photon. So, the photons in the puls carry the same information (polarization), and Eve could use some photons to gather the information – the encoded bit. She can do that if she "shave off" some photons. During the measurement, if Eve gets the same result for all photons she gathered, then she has picked a right basis, but, if she obtains a different result, a few 0 and a few 1, then she knows that she picked a wrong basis. Technically, this eavesdropping strategy is possible, but the act of shaving off the photons, like beamsplitting, will in most usages with the present instruments corrupt the data for both parties. High precision instruments will be a severe threat in the lack of the single photon guns.

During the last decade, few experiments were developed with new coding systems and technological improvements. A group in Los Alamos achieved in the distribution over a 950 m free-space path. Further improvements with transmission over fiber optic channels were achieved also by the Los Alamos group. The distance was 48 km. Another group at Geneva achieved to transfer a key over a 23 km long optical fiber in 1996. Additionally, the EPR protocol, theoretically proposed by Ekert in 1992, was also implemented in 2000 by two independent groups: The group of Anton Zeilinger, then at the University of Innsbruck, and a group at the Los Alamos National Laboratory. For more information on experimental achievement, the reader is directed to [4].

So, although QKD is not yet so practical, it's principle is very important for future study and research on security of information systems. Unlike public-key cryptosystems, the security of QKD is provable [4] and it does not depend on computational power of attacker or eavesdropper. Hence, if someone give a proof that P=NP, what is not so likely, classical cryptosystems will not be useful, since they rely on hard mathematical problems. In the other hand, the security of QKD is guaranteed by the fundamental principles of quantum physics, and it can not be overcome.

5. CONCLUSION

Future development of many research groups is oriented toward long distance QKD and the physical improvement of equipment needed to implement QKD protocols. Lots of effort is also given to space programs involved in the realization of QKD protocols between base stations and satellites. Also, a commercial QKD setup exist, and it can be bought on a market. Recently (2004), the group of Anton Zeilinger at University of Vienna has shown how can a QKD protocol be used for a safe bank transfer. Over all, the theoretical and experimental results will have a main impact, in near future, on the process of commercialization of the QKD systems.

ACKNOWLEDGMENT

The contents of this paper is in a close relation with the research interest and the diploma thesis of the first author. Diploma thesis can be described as mathematical foundations of classical and quantum computation, and it was supervised by Prof.dr.sc. Leo Budin at the Department of Electronics, Microelectronics, Computer and Intelligent Systems, Faculty of Electrical Engineering and Computing, University of Zagreb.

REFERENCES

[1] Bennett, C.H.; Brassard, G. (1984): *Quantum cryptography: public key distribution and coin tossing*, Procedings of IEEE International Conference on Computers, Systems, and Signal Processing, IEEE press

[2] Bennett, C. H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J. (1992): "*Experimental Quantum Cryptography*", Journal of Cryptology, Vol. 5

[3] Bouwmeester, D.; Ekert, A.; Zeilinger, A. (2000): *The Physics of Quantum Information,* Springer-Verlag, Berlin

[4] Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. (2001): *Quantum cryptography*, arXive e-print quant-ph/0101098

[5] Kitaev, A.Y.; Shen, A.H.; Vyalyi, M.N. (2002): *Classical and Quantum Computation*, AMS

[6] Lomonaco, S.J. (1998): *A Quick Glance at Quantum Cryptography*, arXive e-print quant-ph/9811056

[7] Nielsen, M.A.; Chuang, I.L.(2002): *Quantum Computation and Quantum Information*, Cambridge University Press

[8] Shannon, C.E. (1949): *Communication theory of secrecy systems*, Bell Systems Technical Journal

[9] Wootters, W.K.; Zurek, W.H. (1982): *A single quantum cannot be cloned*, Nature, Vol. 299