Iliana Mogilevskaia

QUANTUM CYPTOGRAPHY AS AN ALTERNATIVE TO MODERN CRYPTOGRAPHY

Thesis

CENTRIA UNIVERSITY OF APPLIED SCIENCES

Information Technologies

November 2018

Centria
UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

Centria University of Applied Sciences	**Date** November 2018	**Author** Iliana Mogilevskaia
Degree programme Information Technologies		
Name of thesis Quantum Cryptography as an alternative to Modern Cryptography		
Instructor Dr Grzegorz Szewczyk		**Pages** 43
Supervisor Dr Grzegorz Szewczyk		

Several big companies already developed working prototypes of quantum computers, however they are not powerful enough to perform complicated calculations and are very massive, just like the first models of conventional computers in the twentieth century. However, the process of improvement is progressing fast. The growth of quantum computers might take another five or ten years, maybe less, and those machines will be able to help scientists to solve difficult problems. On the other hand, they will endanger some popular cryptographic protocols.

Cryptologists around the world are working on an encryption system that will allow people to stay confidential, even when very fast quantum computers will appear. This new type of encryption is differing from every known type of cyphering. It may give people absolute information security. In theory, this new method does not have any weaknesses. Unlike other encryption methods which are based on mathematical functions, the new encryption system is based on a Quantum Physics laws, the same laws which are the foundation of quantum computers. The name of this system is quantum cryptography.

The main purpose of this work was to research different types of the conventional cryptographic algorithms and the quantum cryptographic algorithms, and a possible future of cryptography.

Centria
UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

Key words
BB84, B92, Cryptography, E91, photon, QKD, qubit.

CONCEPT DEFINITIONS

AES	Advanced Encryption Algorithm.
Alice	One of two party communication process, usually she is a sender.
Block	A portion of text with a fixed number of bits.
Bob	A receiver of Alice's messages.
Cipher	An algorithm of hiding text with unreadable sequence of characters or bits.
Ciphertext	Plain text that was encoded.
Coherent source	Two sources of light are called coherent if they have the same frequency and a constant phase difference.
Cryptography	It is s a science of converting plaintext into cipher text, unreadable for an un-authorized user.
Eve	An all-powerful eavesdropper, she has highly advanced equipment.
Homodyne detection	A method of extracting information encoded as a modulation of the phase or frequency of an oscillating signal.
Key	A key is a sequence of bits used by a cryptographic algorithm to transform text into cipher text.
MAC	Message authentication code
Plaintext	A message sent between legitimate users.
PNS	Photon number splitting attack.
Polarization	Orientation of electro-magnetic fields of a photon.
QBER	Quantum Bit Error Rate.
QKD	Quantum key distribution.
Quadrature	A phase difference of 90° between two waves of the same frequency, as in the colour difference signals of a television screen.
WCS	Weak coherent source.

ABSTRACT

CONCEPT DEFINITIONS

CONTENTS

1 INTRODUCTION

Cryptography was introduced at ancient times and has continued to evolve through times. The ability to think gave birth to secrets. Secrets are an essential part of society, everyone has information they do not want to share with others or to share only with close people. The moment ancient people learned how to communicate, it became clear that secrets can be read or heard by unwanted parties.

During the course of human history cryptography was not open for common public. Politicians and military, priests and traders, writers and scientists have been developing the craft of secret communication for centuries. Without secret messages people cannot win a battle or make profit, overcome their political opponents in a fierce struggle for power or retain the primacy in technology. Secrets form the basis of science, technology and politics of any human formation, are a foundation of statehood.

Cryptography was used in the past, primarily for military purposes. However, now, as the information society is formed, cryptography becomes one of the main tools providing confidentiality, trust, authorization, corporate security and countless other important things. Practical application of cryptography has become an integral part of the life of modern society - it is used in such industries as electronic commerce, electronic document management (including digital signatures), telecommunications and others.

Historically, the first task of cryptography was to protect the transmitted text messages from unauthorized acquaintance with their content, which was reflected in the very title of this discipline, this protection is based on the use of a "secret language" known only to the sender and recipient, all methods of encryption are just the development of this philosophical idea. With the increasing complexity of information interactions, new tasks have emerged and continue to arise in human society, some of them have been solved within the framework of cryptography, which required the development of fundamentally new approaches and methods.

Very quickly, after the proliferation of computers in the business sphere, practical cryptography has made a huge leap in its development, and in several directions. Firstly, strong block ciphers with a secret key were designed to solve the classical problem of securing transmitted or stored data, they remain the "workhorse" of cryptography, the most commonly used means of cryptographic protection. Secondly

methods have been created for solving new ones, the most important of which are the task of signing a digital document and an open distribution of keys.

All throughout history, the main reason for evolution of the cryptography was cryptanalysis, cryptographers and cryptanalysts would challenge each other using new cipher and decipher algorithms. In the twentieth century an idea of a new type of computers was introduced. A computer which theoretically will be thousands of times faster than any modern super computer. Quantum computers and related technologies have recently become more relevant. Research in this area has not ceased for decades, and several revolutionary achievements are evident. Cryptography is now facing a new challenge of laws of universe. The quantum computer will be able to break any modern cipher. Any kind of communication will be readable. Additionally, any information that needs to be stored for a long time and already encrypted, like, medical records, military or government documents, will not be safe. Quantum cryptography is a new step of an evolution of cryptography. The purpose of this thesis is to get a better understanding of modern cryptographic protocols and quantum cryptographic protocols.

2 DEVELOPMENT OF CRYPTOGRAPHY

Cryptography has an undeniable impact on people's everyday life. Most of the time people do not even know that so many operations involve encryption process. Through thousands of years cryptography evolved from being the art of hiding messages to becoming a science. (Stalling, 2006)

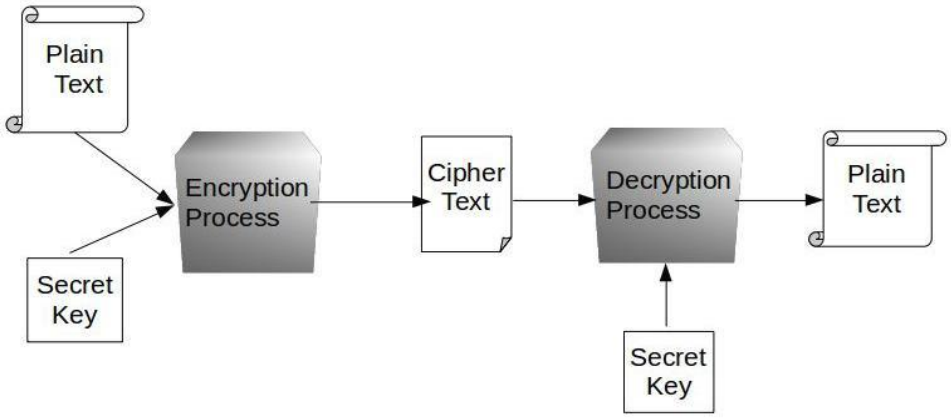


FIGURE 1. General scheme of encryption process (adapted from Stalling 2006)

Cryptography uses special terms. Original messages are called plaintext, after some transformations it become coded and called ciphertext. The process of modifying the plaintext into the cipher text is called enciphering or encryption. To recover the plaintext from the ciphertext, deciphering or decryption is performed as shown in FIGURE 1. Cryptography studies many different schemes used for the encryption. Such a scheme mostly consists of two parts: a key and an algorithm and known as a cryptographic system or a cipher. Cryptanalysis is the area of studying technics of retrieving plaintext or a key from the ciphertext. (Stalling, 2006)

Cryptography had only one task, it was to make text unreadable using different approaches. The only way to communicate was by using letters of the alphabet. The encryption methods were to simply manipulate the position of the symbols, cryptography operated using linguistic approach. (Stalling, 2006)

During the 20th century humans started to rely on machines for communication, this introduced new requirements for cryptography. It was not enough to make the message not readable for the third-party providing privacy for the sender. Communication using machinery allows two parties to be on different continents without seeing each other, each party wants to be confident in the identity of another. Both

users want to be sure that a third party cannot make any malicious changes to the information during communication or to be able to detect it. Cryptography offers different solutions applying mathematical methods. (Konheim, 2007).

2.1 Basic theory of data security

Information is an idea or anything one person would like to communicate to another. There a lot of different ways to deliver information, the most common method is language. Speaking, writing or sending information digitally, these are methods to get through to receiver. Information security includes different parts of a communication process, not only the method of transferring information, but also means to deliver it. In other words, information security is a state of an information security system that combines the information itself and the infrastructure supporting it. The information system is protected if its confidentiality, availability and integrity are ensured. (Shannon, 1948)

Confidentiality ensures that secret information will be accessible to legal and authorized parties of communication. (Shannon, 1948)Availability ensures that authorized users can always have access to information. (Shannon, 1948)Integrity ensures that during transmission unauthorized party was not able trample, modify, destroy or add new information. (Shannon, 1948)

2.1.1 Dole and Yao theory

In the twentieth century several ideas of cryptographic protocols were proposed, this raised the need for a method to analyse protocols for their security. In 1983 Danny Dolev and Andrew C. Yao proposed a formal threat model for interactive protocols. The Dolev and Yao model cannot be applied to the more sophisticated protocols, but it is general enough to use for p (Dolev & Yao, 1983)

The main idea is the following: two parties (Alice, Bob) run a ‘perfectly secure’ protocol to exchange messages. The cryptographic algorithms used for encoding message are considered unbreakable and the public network used for transmitting messages is secured. (Dolev & Yao, 1983)

Adversary (Eve) has a complete control over the entire network. Eve is a legitimate user and can obtain any message passing through the network. She can initiate conversation with any other users and be a receiver for their messages, she also can impersonate other parties. (Dolev & Yao, 1983)

According to the model the adversary has unlimited power, the only constrains are cryptographic. The p today, mainly because it is easy to use model and general enough. (Dolev & Yao, 1983)

2.1.2 Kerckhoffs law

Auguste Kerckhoffs stated in the ninetieth century, the security of a cryptosystem should depend only on the secrecy of the key. When a cryptographer wishes to create a secure cryptosystem, he should take in consideration that the adversary knows the crypto system used for transferring information between sender and receiver, including encoding scheme, the algorithm, the protocol. The only part unknown for the eavesdropper is the key used for encoding the plain text into cipher text. Eve even knows how exactly the key is used in the algorithm, still without the said key she cannot break the (Konheim, 2007)

2.2 History of cryptography

The history of the human civilization has become a history of the creation of safe ways to transfer information between sender and receiver thus the formation of cryptography as science. Ways of secret writing were used by the ancient civilizations of India, Mesopotamia and Egypt. The writings of Ancient India mention ways to change the text, which was used not only by the rulers, but also by artisans, who wanted to hide the secret of their skill. The source of cryptography is the use of special hieroglyphs in the ancient Egyptian script about four thousand years ago. (Davies, 1997)

The finite number of characters in European language families allowed people to perform different kinds of operations like permutation or substitution of characters which basically is an origin of Cryptography. The first known cryptographic tools were used in ancient Greece and Rome. A devise called ‘skytale’ was used in Sparta in 400 BC. Skytale was implementing permutation. As shown in FIGURE 2, it consists of a narrow strip of parchment which is wrapped around a wooden cylinder of a certain diameter. The message is written on the parchment and the strip is unwrapped from the cylinder and delivered to the receiver which has a baton of the same diameter. (Davies, 1997).

FIGURE 2. Skytale (commons.wikimedia 2007)

The most famous cipher, originated in ancient times is a shift cipher which used substitution of characters, also called mono alphabetic cipher. Mono alphabetic means that substitution happens one on one. Algorithm is quite simple, replacing each letter of the original message with the another, which is separated from the original one by a given number of positions in the alphabet. This number of positions is called a key. With a key equal to three, this method is called Caesar's cipher. The emperor used it for secret correspondence. In order to encrypt a message, you need to build a lookup table. (Blakley, 1999)

TABLE 1. Caesar's cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

In TABLE 1 it is seen cleanly, in the second row the symbols of the alphabet are shifted three positions back. To encrypt a message, for each character of the source text, sender needs to take the corresponding symbol from the lookup table. The way to break shift ciphers was introduced by Al-Kindi, an Arab Muslim philosopher and scientist. He came up with the idea that each letter in the alphabet has a specific frequency of use in the language, even if it substituted by another character. This type of frequency analyses attack is very effective on mono-alphabetic ciphers. (Menezes, Katz, Oorschot, & Vanstone, 2001)

In the 15th century Leon Battista Alberti developed a polyalphabetic cipher which revolutionized encryption. The process of encryption was helped by Alberti's disk consisted of two metal circles, one movable, and one immovable, attached in the centre so the inner disk can be rotated as seen in FIGURE 3. (Davies, 1997)

FIGURE 3. Alberti cipher disk (commons.wikimedia 2008)

One letter on the inner disk was marked to adjust with a character on the otter disk. Unlike the mono alphabetic cipher where only one key was used to shift letters this disk allowed to perform a sequence of shifts. The sender and the receiver agree on how many times to turn the disk. It means that even if a letter appears in a word several times it will be substituted with a different character Alberti cipher offered secure communication for three centuries. Charles Babbage came up with the systematic way how to break polyalphabetic ciphers in the 18th century. (Davies, 1997)

Until the 19th and early 20th centuries cipher algorithms had to be simple to use with a pen and paper. The invention of the telegraph opened a new path of development for cryptography. Messages could be sent almost instantaneously across big distances. In the early 1900s several types of electronic cipher machines with rotors were patented. Vernam's cipher is also known as the "One-time pad" was invented in 1917 by Gilbert Vernam of AT&T (American telephone operating company) and Major Joseph O. Mauborgne. In 1949, the work of Claude Shannon was published, where Shannon proved the absolute resilience of Vernam's cipher. In this paper Shannon showed that there are no other ciphers with similar properties and its conclusion is the following statement: Vernam's cipher is the safest cryptosystem of all available. However, it should be noted that in order for the cipher to be truly persistent, it is necessary to fulfil the following three rules. Firstly, the key for encryption is selected randomly. Secondly, the length of the key should be equal to the length of the plaintext. Thirdly, the key must be used ONLY once. (Konheim, 2007)

In the classical sense, a one-time notepad is a large non-repeating sequence of key symbols randomly distributed. Originally it was a one-time tape for teletypes. The sender used each key symbol to encrypt only one plain text character. Encryption is an addition modulo n (power of the alphabet) of a plain text symbol and a key symbol from a one-time notepad. Each key symbol is used only once and for a single message, otherwise even if you use a notebook a few gigabytes in size, when the cryptanalyst receives several texts with overlapping keys, he can restore the source text. He will move each pair of cipher texts relative to each other and calculate the number of matches in each position. If the cipher texts are shifted correctly, the ratio of coincidences will increase sharply. From this point of view, cryptanalysis is not difficult. If the key is not repeated and random, the cryptanalyst, whether he intercepts the texts or not, always has the same knowledge. A random key sequence, combined with non-random plain text, gives a completely random cryptographic text, and no computing power can change it. (Blakley, 1999).

The main disadvantage of this system is that for each bit of transmitted information, a bit of key information must be prepared in advance, and these bits must be random. When encrypting a large amount of data, this is a serious limitation. Therefore, this system is used only for the transmission of messages of the highest secrecy. (Menezes, Katz, Oorschot, & Vanstone, 2001)

Arthur Scherbius invented the rotor-based polyalphabetic cipher machine Enigma which was a way to automate the one-time pad algorithm. Originally Enigma consisted of a combination of rotors and wires latter a plug board has been added as shown in FIGURE 4. In 1933 the German Army acquired the rights for the device, through years they tried to improve the design which will allow more combinations. The pre-war version of Enigma was broken in 1932 by Polish mathematician and cryptographer Marian Rejewski with two other colleagues. Rejewski was able to realise the mathematical relationships between ciphering letters in different positions, and he reconstructed the internal wiring of Enigma without seeing the original one what led to the development of electro-mechanical bombes. The Bomb was a contraption which consisted of six replicas of Enigma. This information was provided to the French and British in 1939. At Bletchley park in Buckinghamshire a top-secret group of mathematicians started to decipher military codes used by Germany. At the outbreak of war codes security was improved by changing the cipher system daily which made deciphering more complex. Alan Turing a mathematician improved The Bomb allowing to break the code much faster using ‘cribs’ common words and short phrases from the code which might be the plain text. Tuning automated the process of deciphering encrypted messages. (Blakley, 1999).

FIGURE 4. Enigma (commons.wikimedia 2009)

Creation of the Enigma and the Bomb has become a turning point for the cryptology as a science. Linguistic methods were insufficient for ciphering and deciphering texts, mathematical algorithms run by machinery have mad cryptography a science. Beginning with the post-war period and to this day, the emergence of computing tools has accelerated the development and improvement of cryptographic methods. In the seventies there were two events that seriously affected the further development of cryptography. Firstly, the data encryption standard (DES) was adopted. Secondly, after the work of American mathematicians W. Diffie and M. Hellman, a "new cryptography" was born - public key cryptography. Both of these events were born of the needs of rapidly developing communications media, including local and global computer networks, which required easily accessible and reasonably reliable cryptographic tools. Cryptography are widely in demand not only in military, diplomatic, state spheres, but also in commercial, banking and other spheres. (Blakley, 1999).

Following the idea of Diffie and Hellman associated with the hypothetical concept of a unidirectional (or one-way) function with a secret, a "candidate" for this function and a real-time RSA public key cipher system appeared. Such a system was proposed in 1978 by Ron Riverst, Adi Shamir and Leonard Adleman. RSA used different keys for encryption and decryption, and the encryption key can be open, that is, known for everyone. Following RSA, a number of other systems have appeared. In connection with the asymmetric use of keys, the term asymmetric cipher system began to be used, while traditional cipher systems became known as symmetric cipher systems. (Davies, 1997)

In 1970 Stephen Wiesener submitted an article “Conjugate Coding” to IEEE Information Theory Society, but it was not published, because the assumptions it contained were described in scientific language, using specific terminology. He came up with an idea of using quantum states to protect banknotes. Wiesener offered to produce bills with light traps and put in each one photon, polarized in strictly certain condition. Each note is marked with a special serial number, which concluded the position of the polarization photon filter. As a result of this when applying other than pre-set filter combination of polarized photons, polarization of the trapped photon is erased, meaning someone tried to forge banknote. Unfortunately, his proposal was impossible to realize technically. (Singh, Gupta , & Singh, 2014)

In 1983 Charles Bennet and Gilles Brassard found a way to apply Wiesener’s idea to a field of cryptography. They developed the first quantum key distribution scheme that was called BB84. (Bennett, Bessette, Brassard, Salvail, & Smolin, 1992)

Arthur Eckert worked on a quantum cryptography protocol based on tangled states. The publication of the results of his work took place in 1991. It is based on the principles of the Einstein–Podolsky–Rosen paradox, in particular, the non-locality principle of entangled quantum objects. This protocol will be explained in a later chapter. (Ekert, 1991).

The first experimental demonstration of the installation of quantum key distribution carried out in 1989 in the laboratory, the transfer was carried out through an open space at thirty-two centimetres. (Bennett, Bessette, Brassard, Salvail, & Smolin, 1992)

After the first experiments of Muller et al. in Geneva, using fiber 1.1 km long, in 1995 the distance transmission has been increased to 23 km through optical fiber laid underwater and later to 30 km. (Mueller, Breguet & Gisin, 1993).

The record for transmission distance information belongs to the association of scientists of Los Alamos and the National Institute of Standards and Technology and is 184km. It used single photon receivers cooled to temperatures close to zero Kelvin. **(**Hiskett, Rosenberg, Peterson, Hughes, Nam, Lita, Miller & Nordholt 2006**).**

The first commercial quantum cryptography system was presented at the CeBIT-2002 exhibition. Swiss company GAP-Optique presented the first compact QKD system. It consisted of two boxes connected by an optical fiber, they could be plugged in two computers via USB. Later more companies like (IBM, Tochiba) became interested in the development of commercial QKD systems. Improvement of these systems is an engineering challenge. (Stucki, Gisin, Guinnard, Ribordy & Zbinden, 2002)

Quantum cryptography has gone from theories to realization into a commercial system of quantum key distribution in less than 50 years. The operating equipment allows you to distribute the key and through a quantum channel at a distance greater than 100 km (a record of 184 km), with speeds enough to transmit encryption keys, but not sufficient for encryption streams of information using the Vernam cipher. High cost of QKD apparatus limits their massive use for organizing confidential communication between small and medium firms and individuals. (Bennett, Bessette, Brassard, Salvail, & Smolin, 1992)

3 MODERN CRPTOGRAPHY

From the beginning, the main and only task for cryptography was confidentiality, but with the development of technology, more areas of human life became automated. Interest in information security grew even bigger. New ways of transferring information created new problems for the cryptography, simply to encrypt the text was not enough. In many applied areas, the problem of the integrity of information arises, which is understood as the guarantee that the information came from a reliable source and was not altered by a third party. When sending important letters, the sender and the receiver should be able to authenticate themselves and information before starting communication. (Menezes, Katz, Oorschot, & Vanstone, 2001)

3.1 Requirements for cryptography

Ensuring confidentiality of a cipher text while it is being transferred through an open channel, where a third party can eavesdrop, is a main task of cryptography. The sender of the initial information, known as plain text, uses one of many ciphers to encode the text, so that only the receiver would be able to decipher it. The sender assumes that the third party (eavesdropper) will try to catch the encoded message and using cryptanalysis to read the content of it. The eavesdropper can use passive or active attacks. Passive attacks include to listen, to analyse traffic, to intercept and to write encrypted messages, trying to decipher it. When an enemy uses active attacks, he can intercept communication or create a false message, also he can alter data inside. The safety of ciphered text is defined by the key and the cryptographic algorithm. (Konheim, 2007).

$$E_k(M) = C \quad [1]$$

$$D_k(C) = M \quad [2]$$

M means plain text and C cipher text, k stands for the key, the processes of ciphering and deciphering can be written mathematically. (Menezes, Katz, Oorschot, & Vanstone, 2001)

Both algorithms must satisfy the following formula:

$$D_k\big(E_k(M)\big) = M \qquad [3]$$

There are two types of cipher systems; symmetric and asymmetric. Symmetric algorithms are algorithms in which the encryption key can be calculated by the decryption key and vice versa. In most symmetric algorithms, the encryption and decryption keys are the same. These algorithms, also called secret key algorithms or single-key algorithms, require that the sender and the recipient agree on the key used before the safe transmission of messages begins. The security of a symmetric algorithm is determined by the key, the disclosure of the key means that anyone can encrypt and decrypt messages. While the transmitted messages must be secret, the key should be kept secret. (Konheim, 2007).

Symmetric algorithms fall into two categories. Some algorithms process the plaintext bitwise (sometimes byte-byte), they are called streaming algorithms or stream ciphers. Others work with groups of plaintext bits. Groups of bits are called blocks, and algorithms are called block algorithms or block ciphers. For algorithms used in computer modems, the typical block size is 64 bits - quite large enough to interfere with the analysis, and small enough and convenient for work. (Konheim, 2007)

Public key algorithms (called asymmetric algorithms) are designed in such a way that the key used for encryption is different from the decryption key. Moreover, the decryption key cannot be (at least for a reasonable interval of time) calculated by the encryption key. Algorithms are called "public key" because the encryption key can be opened: anyone can use the encryption key to encrypt the message, but only a particular person with the corresponding decryption key can decrypt the message. In these systems, the encryption key is often called a public key, and the decryption key is closed. A private key is sometimes called a secret key, but so that there is no confusion with symmetric algorithms. Public key encryption K is denoted as:

$$E_k(M) = C \qquad [4]$$

Although the public and private keys are different, the decryption with the corresponding private key is designated as:

$$D_k(C) = M \qquad [5]$$

Sometimes messages are encrypted with a private key, and are decrypted open, which is used for digital signatures. (Konheim, 2007)

3.1.1 Integrity

Ensuring the integrity of information, meaning to ensure immutability in the transfer process is the second important task of cryptography. This problem requires the cipher algorithm not only to check the message for changes, but to not let the third-party force false information. For this purpose, a one-way harsh function is used to calculate a hash code of a fixed size which will be added to a plain text. Hush code or a message digest plays the role of a fingerprint of a message, if any bit of a message was changed it will cause a change in the hash code. (Konheim, 2007).

Hush function is independent from the key. It has such properties as uniqueness and being difficult to invert. The hash function processes every bit of a message. (Stalling, 2006)

$$h = H(M) \qquad [6]$$

The hush function takes a message of any size and shrinks it to a fixed size message digest. Then the sender adds a fingerprint to the message, encrypts the message and the hash code and transmits a pair over the network. The process of the hash function is shown in FIGURE 5. (Stalling, 2006)

$$C = (h, M) \qquad [7]$$

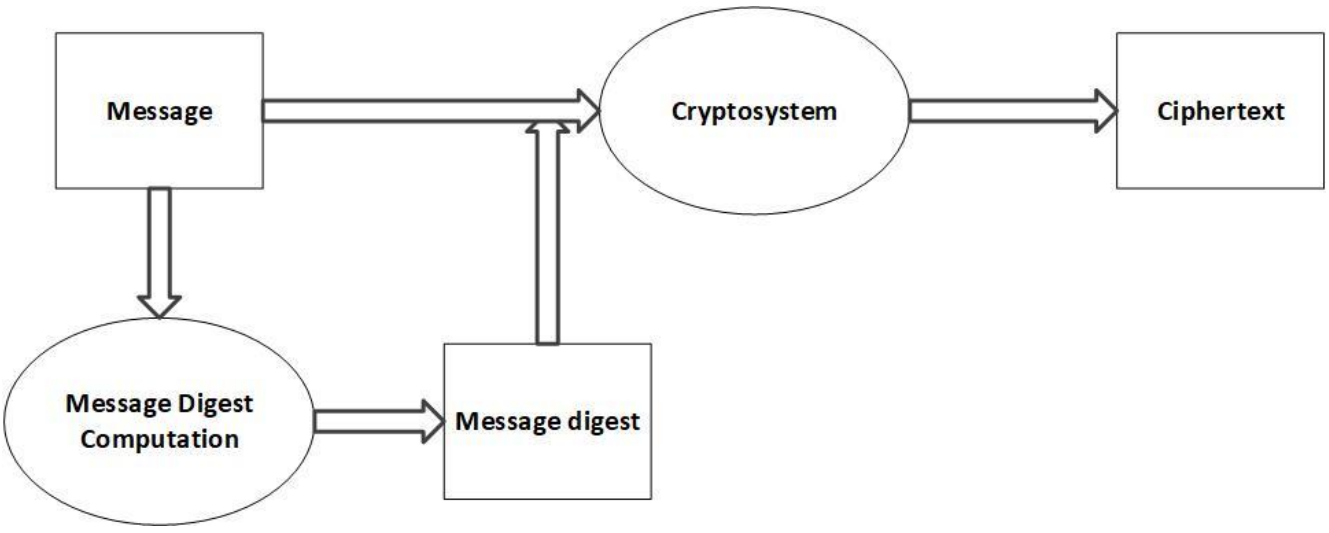


FIGURE 5. Hash Function (adapted from Stalling 2006)

The receiver computes initial value of the hash function. If the value differs it means someone altered the information. (Stalling, 2006)

3.1.2 Authentication

Establishing the authenticity of all aspects of information interaction is an important part of the problem of ensuring the reliability of the information received. This is especially important if both sides are not trusting each other. (Konheim, 2007).

A message authentication code (MAC) also called as a tag is calculated and added to the message. The presence of the tag prevents one of the sides to prevent attempts to retransmit, reorder or reverse the sending of a part of the transmitted messages. Authentication of the parties of interaction means checking one of the parties that the party interacting with it is the one for which it issues itself. (Konheim, 2007).

3.2 DES

The DES (Data Encryption Standard) algorithm, developed by IBM and since 1977 the federal standard of US data encryption, was used for encryption not only by the US government, but also widely distributed around the world among private users. With the increasing computing power of computers, questions about the cryptographic strength of DES before the opening by the "brute force" method began to arise, but the standard successfully passed the re-certification conducted in 1983, 1988 and 1993. Although by the mid-1990s there was a discrepancy between the generally accepted encryption standard DES (Data Encryption Standard) to modern requirements. This was due to the insufficient key length of only 56 bits. In 1998 Electronic Frontier Foundation build a special-purpose DES hardware cracker called “Deep Crack”. The machine used a brute-force attack on DES key-space, using every possible combination to decrypt the encoded messages. DES was broken. (Konheim, 2007)

3.3 AES

The process of developing a new federal information standard (FIPS) for encryption of Advanced Encryption Standard (AES) data was initiated by the National Institute of Standards and Technology

(NIST). In early January 1997, NIST announced the beginning of the development of AES by issuing the document "Announcing the development of a federal information processing standard for advanced encryption standard", containing the primary requirements for the algorithm. Firstly, the AES encryption algorithm must be publicly published. Secondly, the algorithm must be a symmetric block cipher. Thirdly, AES should provide for the possibility of increasing the length of the key and AES should be easily implemented both hardware and software. Finally, AES should be distributed free of charge or publicly available under ANSI patents. (Dworkin, et al., 2001)

In September 1997, the clarifying document "Call for AES Candidate Algorithms" came out, announcing the holding of a competition for AES and containing official requirements for candidates. In particular, the algorithm should support the following combinations of block lengths and keys 128-128, 128-192 and 128-256 bits. By June 15, 1998, 21 cryptographic algorithms were claimed, but only 15 of them met the original requirements. In 1999 5 finalists were chosen, among them was the algorithm Rijndael designed by Vincent Rijmen and Joan Daemen. (Dworkin, et al., 2001)

AES is the standard based on the Rijndael algorithm. For AES, the length of the block is constant and equal to 128 bits, the process of encryption has 10,12 or 14 rounds, depending on the length of the encryption key which is 128, 192, or 256 bits. Each round uses sub-keys generated from the original key. The algorithm operates with bytes not bits like DES. 128 bit plain text or encrypted text is treated as sixteen bytes by 8 bits. (Dworkin, et al., 2001)

Encryption process is shown in FIGURE 6.

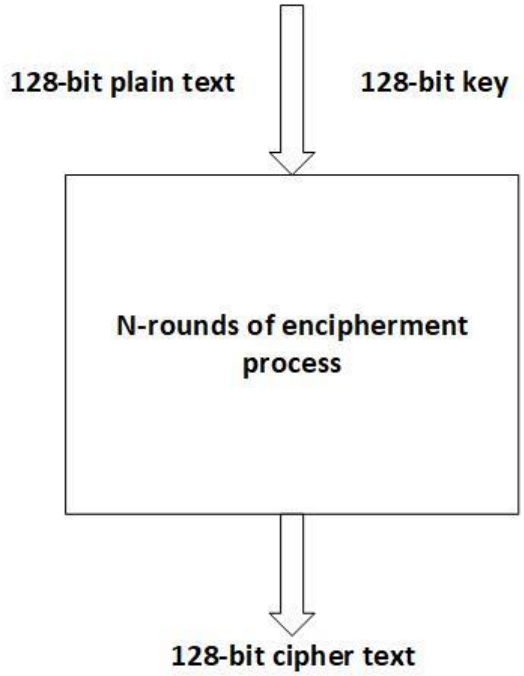


FIGURE 6. AES structure (adapted from Dworkin 2001)

For the mathematical operations AES uses two-dimensional arrays of bytes called the State. To strengthen the security of the algorithm, each round consists of four sub-processes: SubBytes, ShiftRows, MixColumns and AddRoundKey. Every round, except for the last one, performs all four transformations. (Dworkin, et al., 2001)

In the beginning, the input text is copied into the State array and added with the Round Key. After that, the State array is going through transformation by performing 10, 12 or 14 rounds. (Dworkin, et al., 2001) During the SubBytes step, bytes of the plain text are substituted independently by using a substitution table S-box. S-box is reversible, it is constructed by using mathematical calculations in the finite field GF(2). (Dworkin, et al., 2001) In the ShiftRows step, the bytes of the rows of the State, except for the first one, are shifted cyclically by various number of bytes. (Dworkin, et al., 2001)

The MixColumns step shuffles bytes column-by-column of the State using multiplication of polynomials. Four bytes of each column are transformed into completely new bytes, which replace the input bytes. (Dworkin, et al., 2001)In the AddRoundKey step, the algorithm adds the bytes of the RoundKay and the bytes of the State the bitwise XOR operation. (Dworkin, et al., 2001)

AES is not vulnerable to known attacks because two rounds provide complete dispersion and mixing of information. This is achieved by using the functions of ShiftRows and MixColumns . SubBothes operation gives encryption strength against differential cryptanalysis, and operation AddRockKey provides the necessary randomness. (Dworkin, et al., 2001) To decrypt a ciphertext, all used cipher transformations can be inverted and applied in the reverse order. (Dworkin, et al., 2001)

3.4 RSA

The RSA algorithm was developed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977. It is one of the first practical public-key cryptosystems, which is widely used for secure data transmission. RSA is based on the difficulty of factorizing very large prime numbers. (Brown, et al., 2011)

The RSA algorithm consists of four stages: key generation, key distribution, encryption, and decryption. Rivest–Shamir–Adleman encryption includes the public key and the private key. Open key can be known to everyone and is used to encrypt messages. Its essence is that messages encrypted with a public key can only be decrypted (Brown, et al., 2011)

The algorithm consists of the following steps:

1. Two large primes P and Q are chosen randomly.

2. Compute N=P*Q. N is a product of prime numbers. Calculate the Euler's totient of N

$$\varphi(N) = (P-1) * (Q-1) \quad [8]$$

3. Find number E which is relatively prime to φ (N) and calculate D

$$D = \left(1 mod \varphi(N)\right)/E \quad [9]$$

4. Numbers N and E are published as a private key, numbers D and N are kept secret as a private key.

5. For encryption process a message M should be represented by an integer between 0 and N-1, then encrypt by raising it to the power of D modulo N. The result will be the ciphertext C.

$$C = M^e (mod N) \quad [10]$$

6. Decryption process uses C number to get M

$$C = M^d (mod N) \quad [11]$$

For security purposes, integers should be randomly chosen and be the same in size but differ in length by several numbers to make factoring more difficult. The same numbers can be effectively found using the test for their simplicity, so the encryption of information must necessarily be complicated. (Brown, et al., 2011)

RSA is a relatively slow algorithm, which is why it is not so widely used to directly encrypt user data. Most often, this method is used combined with some symmetric algorithm to transmit shared keys in encrypted form for a symmetric encryption key, which, in turn, can perform mass encryption and decryption operations at a much higher speed. (Brown, et al., 2011)

3.5 Idea of quantum computers

At the beginning of the century it became clear that the use of electrical circuits to create computing devices has its limits, and all of them were practically achieved. Now, mankind faces more and more new tasks, for which classical computers will not be enough to solve. The simplest example of such a problem is the factorization of large numbers and the discrete logarithms problem. Most cryptographic systems like RSA and the Digital Signature Algorithm were built based on these dilemmas. This will seem trivial, but if someone could quickly decompose a large number into simple factors, then transactions in all banks of the world would become available to him. (Nielsen & Chuang, 2010)

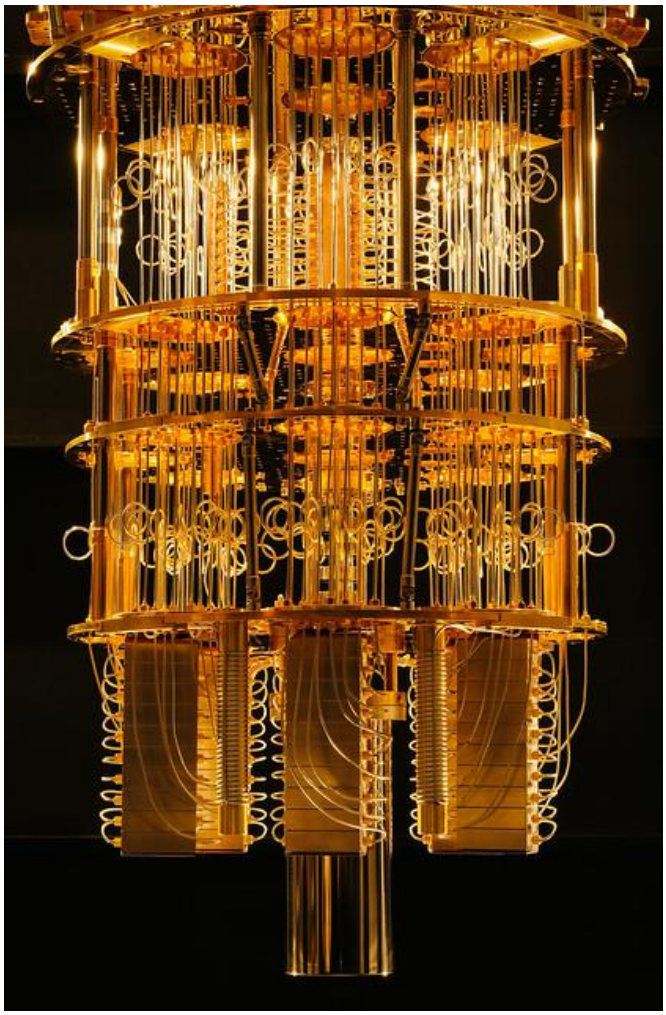
A conventional machine performs operations using classical bits, which can take values of 0 or 1. A quantum computer, unlike a classical computer, is built on the use of effects of quantum entanglement and quantum superposition. Since the elementary object of the quantum theory of information basically exists in nature, one must be able to choose a system in which the quantum properties of a qubit are embodied, their dynamics are controlled, and also need to be able to prepare a certain set of initial states and measure the final result. They can take the values 1 and 0 at the same time. That is what gives such computing technology their superior computing power. Qubit can be represented by a spin or a photon itself. (Nielsen & Chuang, 2010)

All electrons have a magnetic field, as a rule, they look like small magnets and this property of them is called a spin. If they are placed in a magnetic field, they adjust to it in the same way as a compass arrow

does. This is the lowest energy position, so we can call it 0 or lower spin. But you can redirect the electron to the state of 1 or in the upper spin. But this requires energy. If you take the glass out of the compass, you can redirect the arrow in a different direction, but for this you need to apply force. There are two accessories: the lower and upper spin, which correspond to the classical 1 and 0, respectively. But the fact is that photon objects can be in two positions simultaneously. When the spin is measured, it will be either upper or lower. But before the measurement, the electron will exist in the so-called quantum superposition, in which these coefficients indicate the relative probability of finding the electron in a particular state. Superposition will collapse after being measured. (Nielsen & Chuang, 2010)

Four classical bits can be in one of the 16 different configurations at a time from which only one can be used. Four qubits in superposition can be in all 16 states at once. This number grows exponentially with every added qubit. This allows quantum computers to perform large computations in a short time. (Nielsen & Chuang, 2010)

Quantum computers (PICTURE 1) are not meant to take the place of a desktop computers. For browsing or writing and sending emails, quantum computers are not better at performing these tasks than classical computers, additionally installations of currently developed quantum computers are too big. Quantum computers will help to advance areas where classical computers can not help researchers such as chemistry and medicine, sorting large databases. However, quantum algorithms can also break some popular cryptographic protocols, this possibility encouraged several research institutions in different countries to start to look for measures to secure the transmission and the storage of important information. Efforts of many professionals led to a development of Quantum cryptography. (Nielsen & Chuang, 2010)



PICTURE 1. An IBM Q cryostat (flickr 2018)

4 QUANTUM CRYPTOGRAPHIC ALGORITHMS

Quantum physics is a basic theory that underpins all the matter systems and light. It describes states. Quantum cryptography has two main paths of development based on different quantum physics laws. The first area of research is encoding quantum state of a single particle based on a principle of impossibility to distinguish between two non-orthogonal quantum states. (Hill, 2008)

It is impossible to create an identical copy of an unknown quantum state without altering the original one. A sender, called Alice, and a receiver, called Bob, use two-state quantum systems, also called qubits, encoding stats of it. If the its state. The presence of a third party in the quantum channel will lead to higher error rates in exchange. BB84 and B92 protocols utilize properties of this theorem. (Chizhov, 2004)

The second direction of development is based on quantum entanglement as a physical phenomenon. Two particles are in a state of correlation in a way that measurement of a spin of one particle will determine the result of measurement of the same property on the other particle. E91 protocol is based on quantum entanglement. (Chizhov, 2004)

4.1 Single photon protocols

Quantum cryptography is based on properties of photons. Photons are particles of light which have no mass. While particles are moving, they oscillate. Oscillation can be horizontal, vertical or diagonal. The different angle of oscillation is called polarization. LEDs can emit particle of every polarization, which means that the light in this state is unpolarized. Per laws of physics, photons can exist in several states at the same time. This means that whatever oscillation the photon has it does all of them at once. (Hjelme& Lydersen& Makarov 2011)

To make photon polarized, a filter should be placed on the path of a photon's movement. Filters have some holes, but these holes can be vertical, horizontal or diagonal. It is possible to produce a beam of light that will consist of equally polarized photons. These filters are called polarized (polarizer). Because of the principle of photon polarization, any photon with the same polarization as the polarizer will go

through it without delay as shown in FIGURE 7. Photons which have an opposite oscillation direction than a polarizer will be delayed. (Hjelme et al. 2011)

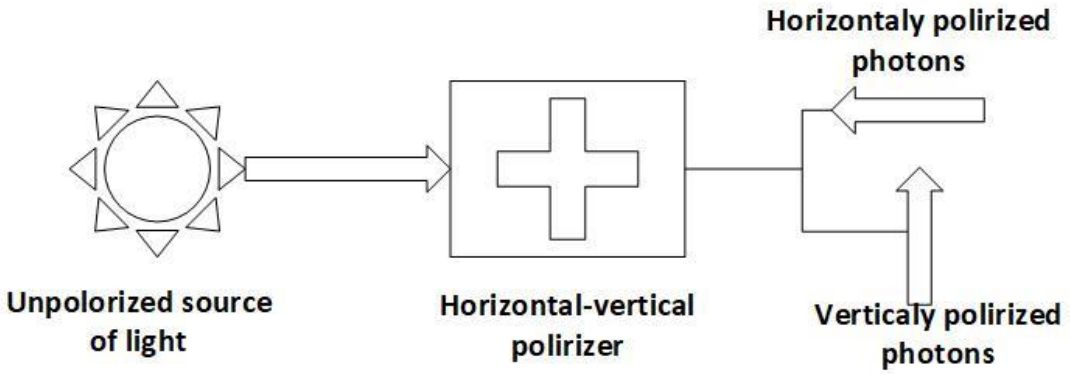


FIGURE 7. Polarization of photons (adapted from Hjelme 2011)

Unfortunately, percentage of correct guesses is not so easy with diagonally polarized photons. When a polarized stream of photons has reached a horizontal filter, vertically polarized photons will be stopped by the filter, but diagonally polarized photons will pass through the polarizer and will change their own polarization. Actually, only half of the diagonally polarized photons will go through, some of them will be stopped. (Hjelme et al. 2011)

4.1.1 BB84

Protocol BB84 is the first protocol for quantum key distribution, it was suggested in 1984 by Charles Bennet and Gilles Brassard. BB84 is based on the principles of quantum mechanics, which makes it secure under conditions of no disturbances in a quantum channel and using states of particles that cannot be cloned. Those conditions would be ideal conditions for quantum key distribution. (Bennett & Brassard, 1984)

A condition of no disturbances means that during a travel of particles through the optical channel particle state will not change. In classical cryptography it is common to think that the third party can copy or eavesdrop the message without altering bits. However, if information is encrypted in non-orthogonal quantum states, like for photons with polarization 0°, 45°, 90° or 135°, then it is impossible for the

eavesdropper to read or copy that information. An attempt to do so will change states uncontrollably and legitimate users of the channel will notice. (Bennett & Brassard, 1984)

Original BB84 was written for single photons sequence. For encoding information BB84 proposes four states of photon polarization, which form non-orthogonal bases: horizontal-vertical and diagonal. (Bennett & Brassard, 1984)

The sender generates a sequence of bits and randomly picks polarization filters. Before the transmission, each bit is encoded by photons according the chosen bases as shown in TABLE 2These photons are sent to the receiver. (Bennett & Brassard, 1984)

TABLE 2. Bases of polarization

		Bits	
		0	1
Horizontal-vertical basis	+	–	|
Diagonal basis	×	/	\

Bob chooses measurement bases randomly between horizontal-vertical and diagonal. According to laws of quantum mechanics, if a photon with diagonal polarization measured with horizontal-vertical base, the photon polarization will change to either vertical or horizontal. Results of measurements will be truly random. Bob does not know what bases Alice used, his results will coincide with Alice's only in 50% cases when he selects the right base. (Bennett & Brassard, 1984)

The next step of the protocol is to connect, using an open communication channel like an Internet connection, to have a discussion. The open channel means that anyone can eavesdrop on the conversation. Alice tells Bob which polarizers she used (orthogonal or diagonal) for every photon. Alice does not tell him how she polarized each photon. In other words, the sender tells that she used orthogonal for the first photon, but she will not say that the particle is polarised vertically. Then, Bob says in which cases he chose correct polarization filter. In these cases, he got correctly 1 and 0. Now both of them have similar values. All particles that were measured wrongly are discarded. In the end Alice and Bob have a secure

secret key of correctly measured photons that they can use to cypher messages. (Bennett & Brassard, 1984)

In case an eavesdropper has to pick bases randomly, she can get only half of them right. She also needs to generate a new photon, using the value she got and base of her choice, to transmit it to Bob. It means that polarization of some of the photons will be different from the original. When Alice and Bob discuss their choices of bases, they will notice that even if Bob used a correct base for measurement, but the value is wrong. It means that a third party is trying to eavesdrop. In this case Alice and Bob discard this sequence of bits and do the steps above again. (Bennett & Brassard, 1984)

4.1.2 B92 protocol

Protocol B92 was proposed by Charles Bennett in 1992, it uses the same preparations and measurements as BB84, except B92 uses only two non-orthogonal polarizations, for example: bit ‘0’ can be encoded using 0° orthogonal base and photons polarized by 45° diagonal base carry information about ‘1’. (Bennett, Bessette, Brassard, Salvail, & Smolin, 1992)

Alice sends photons randomly polarized by 0° and 45°, which represent ‘0’ and ‘1’. When Bob receives qubits, he uses 90° and 135° filters. Because of the quantum physics phenomenon, send photons will pass through a filter with a probability of 0.5 if polarization of the filter will be different from photon's polarization by 45°. If the angle of difference is 90° photon will be blocked. (Bennett, Bessette, Brassard, Salvail, & Smolin, 1992)

Bob can try to use bases with orthogonal axes, but he will not be able to determine which value was sent: ‘1’ corresponding to a photon which was blocked or ‘0’ encoded as a photon which is blocked with probability 0.5. However, if axes of polarized photon and filter are non-orthogonal, then the receiver can determine that photon encoded ‘0’. (Bennett, Bessette, Brassard, Salvail, & Smolin, 1992)

4.2 Entanglement-based QKD

In 1935 Albert Einstein together with Boris Podolsky and Nathan Rosen published an article entitled "Can Quantum Mechanical Description of Physical Reality Be Considered Complete?". Also referred to as "EPR", this paper questions the notion of locality and reality, principles of classical physics. EPR features a phenomenon of two quantum systems correlate in a way that measuring a property of one of the particles will instantaneously determine the same property of the other. This case applies even if particles are separated by a large distance. (Ekert, 1991).

To encode bits, in quantum cryptography usually used a property of a photon polarization. There are lots of different types of polarization. Measurement of this attribute can give only two results: +1 and -1. (Ekert, 1991)

$$\boldsymbol{A = \pm 1} \qquad \boldsymbol{A' = \pm 1} \qquad \boldsymbol{B = \pm 1} \qquad \boldsymbol{B' = \pm 1}$$

Alice measures states A and A', Bob – B and B'. A new variable S is introduced. It is a sum of all possible combinations. (Ekert, 1991)

$$S = A(B + B') + A'(B - B') \qquad [12]$$

$$S = \pm 2 \qquad -2 \leq S \leq 2$$

Experiments show that, there is violation of Bell's equation. (Ekert, 1991)

$$-2\sqrt{2} \leq S \leq 2\sqrt{2}$$

Photons do not carry predetermined values of polarization, they are in a superposition of all possible states. If the values did not exist prior to measurements, they weren't available to anybody including eavesdropper. (Ekert, 1991).

In 1991 Artur Ekert proposed the idea of using quantum entanglement to securely distribute quantum key. For the purpose of Alice and Bob, having a secure cryptographic key, both of them have a wire connection that can send entangled particles. One of them uses equipment to generate and send a pair of qubits in superpositions. (Ekert, 1991).

A big number of photons are sent and stored on both computers. Alice and Bob measure their qubits along one of the three axes. The sender and the receiver chose bases of three directions randomly and

independently. They do it for all photons. Alice calls Bob and they openly tell which orientation of filters they used for each quantum system. Results are saved and divided in two groups: the first group consists of measurements both parties used the same bases, the second one – with different. Values that weren't properly received are discarded. The second group of observed states is needed to check for the presence of Eve using Bell's equality. If Bell's equality is violated it means that the qubit was not seen by anyone. If there is no violation, it may mean that the particle was measured by Eve, because it acquired an attribute. The remaining photons were measured with the same bases by Alice and Bob are used to generate a secret key. (Ekert, 1991).

4.3 Continuous variables quantum cryptography

In 1999 Timothy Ralph proposed a new type of quantum key distribution scheme. Protocol is based on encoding information as phase and amplitude values of the optical field which are continuous variables, that is, when changing, gives a value continuously varying in a certain range of values. This is the main difference between CV and qubit, which measurement results as discrete variables. Security of this scheme is ensured by no-cloning theorem for continuous variables. An attempt to copy coherent state of optical field will introduce errors at the receiver. (Shukla, Pathak, & Radhakrishna, 2012)

CV protocol has some similar steps with discrete variable protocol, like BB84. The first one is randomness of the key, the second is use of two different measurements and the last one is a communication between Alice and Bob over the open channel. (Shukla, Pathak, & Radhakrishna, 2012)

Alice generates two sequences of numbers and two variables X and Y. One sequence of numbers is encoded on the phase quadrature X and the other on the amplitude quadrature Y of a bright coherent beam. Both X and Y are random numbers normally distributed over the whole numerical line with a mean value of zero and a chosen by Alice variance. Coherent states (X_A , Y_A) are sent X_B or Y_B. Bob informs Alice through an open channel which state he observed for any particular time. The sender discards all irrelevant data. Now both of them share sets of correlated Gaussian variables. (Shukla, Pathak, & Radhakrishna, 2012)

Alice and Bob decide which quadrature to use as the key and which for testing. They may choose phase quadrature for testing out presence of eavesdropper by comparing cases when Alice send X_A with results

when Bob looked at the X_B. This process evaluates the error rate and transmission efficiency of quantum channel. They can consider connection secure within some adequate error rate. The last step is to use the amplitude quadrature variables as a key. (Stucki, Gisin, Guinnard, Ribordy, & Zbinden, 2002)

4.4 Decoy State Quantum Key Distribution

The decoy state QKD protocol was introduced by Won-Young Hwang in his paper "Quantum Key Distribution with High Loss: Toward Global Secure Communication". The idea is to secure the BB84 protocol against photon number splitting (PNS) attack. PNS attack exploits imperfections of single-photon sources. Hardware inadvertently emits pulses which contain multi-photons, the sender cannot know when it happens. In PNS attack, Eve can measure the number of photons, if it is more than one, she catches this pulse, split photons, store one and send the other qubits to Bob. (Hwang, 2003)

The basic algorithm is the following. Alice intentionally blends together the signal pulses with multi-photon pulses (the decoy state). Bob uses an open channel to tell Alice that the transmission ended. Now the sender announces which qubits are decoys. Both legitimate users use photon number statistics to check the presence of an eavesdropper. Eve cannot distinguish between multi-photon pulses of decoy source from those of signal source, this can be seen in frequency of decoy state. (Hwang, 2003)

4.5 AK15

AK15 is a decoy state protocol adopts BB84, but unlike the one proposed by Hwang, it provides authentication using features of EPR protocol. In 2015 Abdulbast Abushgra and Khaled Elleithy presented their paper "Initiated decoy States in Quantum Key Distribution Protocol by 3 ways channel" at IEEE conference. (Abushgra & Elleithy, 2016)

Alice and Bob have a connection over a quantum channel and an EPR channel. Alice want to communicate with Bob. The first step before starting a transmission is to create a string of EPR pairs of photons. The s (Abushgra & Elleithy, 2016)

Bob resends the authentication key and the encoded bases. AK15 is based on matrices (TABLE 3) which divided a diagonal row of parity sells in two triangles. The bits are encoded by polarized photons. Alice randomly fills in the matrix with qubits and decoy state, starting from the lower triangle. In TABLE 3 the grey column shows the order before sending, the last column is reshuffled and will be sent She uses the information from the authentication key to resort the rows then sends the string to Bob. At this stage, even if Eve will be able to catch some particle, she will not be able to understand them, because of the randomness of rows and the presence of decoy state. (Abushgra & Elleithy, 2016)

TABLE 3. Matrix (adapted from Elleithy &Abushgra, 2015)

								1	7
1								2	5
1	1							3	4
0	0	1						4	6
1	1	0	1					5	2
0	1	1	0	1				6	1
0	0	0	1	0	1			7	3
1	1	0	0	1	0	1		8	8

Bob measures incoming qubits, choosing randomly states and bases. He places photons in the matrix, which parameters he knows from the EPR session. Then he sends the upper triangle qubits as a string to Alice. If Alice agrees that it is correct, they can continue secure communication. On the other hand, if Alice does not accept the string of qubits, she sends Bob a sequence of used bases. Bob checks weather the string, sent by Alice, contains differences from his own. It means that someone tried to eavesdrop on their communication. (Abushgra & Elleithy, 2016)

5 SECURITY OF QKD

Real life implementations of QKD protocols and attacks on them present an engineering challenge. There are some continuous variable algorithms that are impossible to test, because the current technology will not allow it. Additionally, most applications of quantum cryptography use optical fiber for communication. Fiber cannot keep photon's state very good, introducing noise, which changes the qubits information. The presence of the noise gives Eve some loopholes for attacks. (Chizhov, 2004)

A man-in-the-middle attack is possible, if Eve can replace the part of the wire between Alice and Bob to a more noiseless one. According to quantum cryptography security proofs, Eve can have any kind of equipment that does not violate the known laws of quantum mechanics. She will be able to take measurements without disturbing the general level of noise. When Alice and Bob will check the noise level, they will not be able to see any abnormalities. (Xu, et al., 2015)

Single photon protocols require a special equipment. Practical quantum cryptography systems use a weak coherent source (WCS), which is inexpensive, unlike the single photon source. WCS is created with a weak laser and has an imperfection, it produces single-photons and multi-photons with a different time interval. (Xu, et al., 2015)

The emission of photons is probabilistic, which give Eve a possibility for a photon number splitting attack (PNS). The eavesdropper choses time intervals in which she catches optical pulses generated by Alice. Then, she determines the number of photons, N. If $N < 2$, qubit is blocked, otherwise the pulse is split. One photon is stored by Eve, the other is sent Simple PNS attacks will introduce more errors in Bob's results. To stay undetectable Eve need more sophisticated schemes, current technologies cannot do that. (Jain, et al., 2015)

The difference between theory and reality is quite big. Imperfections in hardware open doors for a Trojan-horse attack on both sender and receiver's apparatus. Alice is more vulnerable, because she has to generate qubits to initialize the connection using BB84. Eve can make use of Fresnel reflection and scattering, by directing a strong laser at Alice's device. An eavesdropper can catch a stream of reflected pulses and determine which bases Alice used. (Sajeed, Minshull, Jain, & Makarov, 2017)

6 CONCLUSION

The analysis showed that quantum cryptography has already taken a decent place among the systems providing confidential communication. The discussion of the advantages and disadvantages of different key distribution protocols helps scientists around the world to search for the most successful protocols and algorithms design solutions that increase the distance of information transfer, increase the speed of key generation and reducing the influence of destabilizing factors. One of the development trends is to improve the element base quantum systems cryptography to overcome technological difficulties manufacturing components.

Huge companies like Google, IBM, Microsoft and Intel, are racing with each other to develop chips with more operational qubits. IBM developed IBM Q System that allows to experience quantum computation outside the laboratory via cloud. Development of quantum computers with big enough qubits will take several years. The threat of breaking some cryptographic algorithms is real, all existing information which has been encrypted and is stored will be decrypted. Researchers are looking for different ways to protect people's privacy. However, when an emergency will happen implementing new cryptographic schemes will take years especially in industries. On the other hand, QKD protocols are already working and some of them are tested. Governments, military and banks in different countries are operating quantum cryptography devices.

Theoretical quantum cryptography is advancing every year, unfortunately the development of working hard ware implementations is a real engineering challenge. Despite not being very popular, there are several companies that are working on commercial implementations of quantum cryptography algorithms. ID Quantique is a Swiss company that successfully developed a quantum random number generator, in addition, the company sells single-photon systems and offers systems for QKD. Australian company QuintessenceLabs offers solutions for clouds and the Key and Policy Manager.

In recent years cryptologists came up with a new concept of device independent quantum cryptography. This idea will allow to safely communicate without worrying about hardware weaknesses. Additionally, the user will be able to discover if a device was modified by an untrustworthy seller, by running a test on Bell's equality. Development of quantum computers present much harder challenges to keep qubits

in an operational state. At this stage quantum cryptography solutions are more advanced. There are several working commercial implementations of quantum key distribution.

REFERENCES

Abushgra, A., & Elleithy, K. 2016. QKDP's comparison based upon quantum cryptography rules. *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT).* Farmingdale, NY, USA: IEEE. Available: https://core.ac.uk/download/pdf/52956870.pdf. Accessed: 16/12/2018

Ali, S., Mahmoud , O., & Saeed, R. 2011. Estimation of Decoy State Parameters for Practical QKD. *Australian Journal of Basic and Applied Sciences*, 430-439.

Bennett, C. H., & Brassard, G. 1984. Quantum Cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175-179. Available: https://core.ac.uk/download/pdf/82447194.pdf. Accessed: 19/11/2017

Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J. 1992. Experimental quantum cryptography. *Journal of Cryptology*, 3-28. Available: https://www.academia.edu/3729789/Experimental_Quantum_Cryptography. Accessed: 14/10/2018

Blakley, G. 1999. Twenty years of cryptography in the open literature. *Proceedings of the 1999 IEEE Symposium on Security and Privacy (Cat. No.99CB36344).* Oakland, CA, USA, USA: IEEE.

Brown, P., Finch, S., Gordon, I., Hunt, D., Mathews, D., & Watson, R. 2011. *RSA Encryption.* Melbourne: The University of Melbourne.

Chizhov, M. 2004. *Quantum cryptography systems.* Available: http://www.vad1.com. Accessed: 13/11/2018

Davies, D. 1997. A Brief History of Cryptography. *Information*, 14-17.

Dolev, D., & Yao, A. C. 1983. On the Security of Public Key Protocols. *IEEE TRANSACTIONS ON INFORMATION THEORY Vol. 29,* 198-208.

Dworkin, M. J., Barker, E., Nechvatal, J., Foti, J., Bassham, L., Roback, E., & Dray Jr., J. 2001, November 26. *Advanced Encryption Standard (AES).* Retrieved from www.nist.gov: November

Ekert, A. K. 1991. Quantum Cryptography Based on Bell's Theroem. *Physical Review Letters*.

Goldenberg, L., & Vaidman, L. 1995. Quantum Cryptography Based on Orthogonal States. *Physical Review Letters*, 1239-1243.

Google. Analyzing and Repairing Compilation Errors. Available: https://ai.google/research/pubs/. Accessed: 10/05/2019

Hill, P. C. 2008. Vigenère through Shannon to planck — a short history of electronic cryptographic systems. *2008 IEEE History of Telecommunications Conference.* Paris, France: IEEE.

Hiskett, P. A., Rosenberg, D., Peterson, C., Hughes, R., Nam, S., Lita, A., . . . Nordholt, J. 2006. Long-distance quantum key distribution in optical fibre. *New Journal of Physics*.

Hwang, W.-Y. 2003. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Physical Review Letters*.

IMB. Available: https://www.research.ibm.com/ibm-q/. Accessed: 22/04/2018

IDQuantique. Available: https://www.idquantique.com/about-idq/company-profile/. Accessed on 25/03/2019

Jain, N., Anisimova, E., Khan, I., Makarov, V., Marquardt, C., & Leuchs, G. 2014. Trojan-horse attacks threaten the security of practical quantum cryptography. *New Journal of Physics*.

Jain, N., Stiller, B., Khan, I., Makarov, V., Marquardt, C., & Leuchs, G. 2015. Risk Analysis of Trojan-Horse Attacks on Practical Quantum Key Distribution Systems. *IEEE Journal of Selected Topics in Quantum Electronics*. Available: http://www.vad1.com/lab/publications.html. Accessed: 22/03/2018

Konheim, A. G. 2007. *Computer Security and Cryptography.* New Jersey: John Wiley and Sos, Inc.

Menezes, A. J., Katz, J., Oorschot, P. C., & Vanstone, S. A. 2001. *Handbook of Applied Cryptography.* CRC Press.

Mueller, A., Breguet, J., & Gisin, N. 1993. Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km. *EPL (Europhysics Letters)*, p.383.

Nielsen, M. A., & Chuang, I. L. 2010. *Quantum Computation and Quantum Informayion.* Cambrige: University Press.

QuintessenceLabs. Available: https://www.quintessencelabs.com/. Accessed on 15/12/2018

Sajeed, S., Minshull, C., Jain, N., & Makarov, V. 2017. Invisible Trojan-horse attack. *Scientific Reports*. Available: http://www.vad1.com/lab/publications.html. Accessed: 22/02/2018

Shannon, C. E. 1948. A Mathematical Theory of Communication. *The Bell System Technical Journal*, 379-423.

Shukla, C., Pathak, A., & Radhakrishna, S. 2012. Beyond the Goldenberg-Vaidman protocol: Secure and efficient quantum communication using arbitrary, orthogonal, multi-particle quantum states. *International Journal of Quantum Information*. Available:https://arxiv.org/abs/1210.2583. Accessed: 16/05/2018

Singh, H., Gupta , D., & Singh, A. 2014. Quantum Key Distribution Protocols: A Review. *IOSR Journal of Computer Engineering*, 01-09.

Stalling, W. 2006. *Cryptography and network security : principles and practices.* Upper Saddle River, New Jersey: Pearson Prentice Hall cop.

Stucki, D., Gisin, N., Guinnard, O., Ribordy, G., & Zbinden, H. 2002. Quantum key distribution over 67 km with a plug&play system. *New Journal of Physics*. Available: https://arxiv.org/pdf/quant-ph/0203118.pdf. Accessed: 15/02/2018

Xu, F., Wei, K., Sajeed, S., Kaiser, S., Sun, S., Tang, Z., . . . Lo, H.-K. 2015. Experimental quantum key distribution with source flaws. *Physical Review A*. Available: http://www.vad1.com/lab/publications.html. Accessed: 23/11/2018