IRSTI 49.03.05

Sh. Habiburahman[1], O. Baimuratov[2], N. Abdinurova[3]
[1,2,3]Suleyman Demirel University, Kaskelen, Kazakhstan

ANALYSIS OF QUANTUM CRYPTOGRAPHY AND TECHNOLOGIES IN INDUSTRIES

Abstract. In today's connected world it's crucial to make sure telecommunication is not a risk. Eavesdroppers will always find a way to attack and harm big companies systems or governmental databases. It's very important to find the best possible way to keep our services safe. Quantum cryptography is one the best way since it's based on rules of quantum physics. In this paper we are going to analyse the best solutions, protocols and different aspects of encryption. Real life implementations by different IT companies and investors will also be included in this paper. Weakness and pros always exist in every system and it's impossible to indicate the system we are proposing is not breakable but it's going to be the best possible solution for now. Why? It's going to be discussed in later sections.

Keywords: Index Terms—Quantum technologies, Qubit, Quantum gates, Transmission, Quantum cryptography.

***

Аңдатпа. Қазіргі заманауи әлемде телекоммуникацияның қауіпті емес екендігіне көз жеткізу керек. Қателер әрдайым компанияның ірі жүйелеріне немесе мемлекеттік дерекқорларға шабуыл жасаудың және бүлдірудің жолын табады. Біздің қызметтеріміздің қауіпсіздігін қамтамасыз етудің жақсы әдісін табу өте маңызды. Кванттық криптография - бұл жақсы әдістердің бірі, өйткені ол кванттық физика ережелеріне негізделген. Бұл мақалада біз ең тиімді шешімдерді, хаттамаларды және шифрлаудың әртүрлі аспектілерін талдаймыз. Бұл мақалада әр түрлі IT компаниялары мен инвесторлардың нақты енгізулері қосылады. Кемшіліктер мен атрықшылықтары әр жүйеде әрқашан бар және біз ұсынып отырған жүйенің бұзылмайтындығын көрсету емес, бірақ қазіргі уақытта бұл ең жақсы шешім болып табылады. Неге? Бұл келесі бөлімдерде талқыланады.

Түйін сөздер: кванттық технологиялар, кубит, кванттық қақпалар, беріліс, кванттық криптография.

***

Аннотация. В современном соединенном мире важно убедиться, что телекоммуникации не представляют опасности. Подслушивающие всегда найдут способ атаковать и наносить вред системам больших компаний или правительственным базам данных. Очень важно найти наилучший способ обеспечить безопасность наших услуг. Квантовая криптография - один из лучших способов, поскольку она основана на правилах квантовой физики. В этой статье мы собираемся проанализировать лучшие решения, протоколы и различные аспекты шифрования. Реальные реализации различных ИТ-компаний и инвесторов также будут включены в эту статью. Слабость и плюсы всегда существуют в каждой системе, и невозможно указать, что предлагаемая нами система не поддается разрушению, но на данный момент это будет наилучшее возможное решение. Почему? Это будет обсуждаться в следующих разделах.

Ключевые слова: квантовые технологии, кубит, квантовые врата, передача, квантовая криптография.

Introduction

Keeping the data and information safe is the most important thing and with the development of technology breaking any security systems or accessing any secure systems were becoming easier. Everyone was looking for something new in order to stop hackers or eavesdroppers. Quantum physics was the only hope and researchers thought of using quantum physics which seems they have made the right decision by applying the quantum rules on quantum cryptography. European union and big companies like IBM [1], Ali Baba [2] and Microsoft [3] announced their interest and that they are willing to invest and build a secure communication system based on this technology which is known as SECOQC [4] or secure communication based on quantum cryptography. Of course, Quantum computers and quantum algorithms also received a lot of interest in the past. Quantum mechanics [5] is the reason behind the technology that we are using today. It's mainly because it has the ability to do some tasks better and faster than classical cryptography.

Limitations of modern cryptography

As we know cryptography is the process of exchanging information in the presence of a third party called adversaries). Or in simple words it's about constructing and analyzing protocols that block adversaries. Since World War I, the methods used to carry out cryptology[6] have become an interest for many big IT companies because everyone noticed that using computers are very helpful but not secure if there's no way to keep the data secured. It protects your

identity, transactions, and prevents your competition from accessing and reading your confidential documents. Although it's very important now but in the future it will become more and more vital. Eavesdroppers will always find a way to harm a system and they don't need many vulnerabilities, one is enough for them to turn down the whole system. Today's security systems might be safe but not forever. Once your application is being used widely it will become a target for criminals. No matter how great your application or a system is, it measures by its security system in the market. It's impossible to guarantee 100 percent security. But it's possible to work toward 100 percent. Since calculations are relatively slow in public key cryptography, they exchange keys instead of encrypting the data. RSA and Diffie Hellman [7] are used widely to distribute symmetric keys between users. However, as we already know that asymmetric encryption is a lot slower than symmetric, that's why the best possible way is to use the advantage of the speed of a public key system in order to exchange symmetric key. RSA and Diffie-Hellman are not based on concrete mathematical proofs that's why encryption algorithms could be defeated soon or later. It's true that the current Cryptosystems may be good but in future it might not provide enough confidentiality with advancements in technology and computer systems. In the past DES [8] with 56 bit keys was secure enough but nowadays it's not considered to be secure enough since the advancement in technology has proven it wrong. Or also we could say quantum computing could break the RSA with the matter of time. It's impossible to say that today's cryptosystem [9] is not hackable but we can say for sure that it's possible to break any cryptosystem with the manner of time. Or a theory could be developed in the future that proves that cryptosystems are vulnerable. If it became true that means that large organizations, governments and other affected institutions should spend a lot of money to create and deploy a new cryptography system as fast as possible.

Quantum cryptography in theory

Quantum encryption [10] has two pillars, one is the Heisenberg Uncertainty principle [11] and the second one is principle of photon polarization [12]. Heisenberg claims that it's impossible to measure the quantum state of any system without distributing it. On the other hand photon polarization of light particles can only be known when it's measured. It plays an important role to stop the eavesdroppers from attacking. Secondly, principles of polarization explain how light photons can be oriented in specific directions. In other words a photon filter can detect only a polarized photon with a correct polarization or it will be destroyed. This is the reason why quantum cryptography is a better option for ensuring the privacy of our data and stopping attackers. In 1984 Charles Bennet and Gilles Brassard [13] developed the concept of quantum cryptography. Depending on the amount of photons reaching to a receiver it's

possible to create an encryption key which corresponds to the fact that light can behave with the characteristics of particles in addition to light waves photons can be polarized at various orientations and Zeros and ones represent the bits that can be used by orientations. The foundation of quantum cryptography is polarized photons that serve as the important principles of quantum key distribution. Although the strength of the modern (digital) cryptography depends on factoring large numbers but quantum cryptography completely depends on physics rules and is also not dependent on the processing power of current computing system That's quantum cryptography has the answer to the problems that current cryptography suffers from. And being worried about the computing power of eavesdroppers or a theory that has the ability to quickly solve the large integer factorization problem is no longer required.

Quantum key distribution example

In this section we are going to provide an example of how Quantum cryptography distributes keys [14] securely. It includes a sender, receiver and a malicious eavesdropper which is called in order Alice, Bob and Eve. Alice sends a message to Bob using a photon gun . This gun will send a stream of photons in an opposing direction which is randomly chosen in one of four polarization that could be vertical, horizontal or diagonal. Bob will randomly choose a filter for each photon and use a photon receiver to measure the polarization which is either diagonal (45 or 135) and rectilinear (0 or 90) and keeps a log of correct measurement that has been selected by Alice and the incorrectly measured will be discarded while the correct ones are translated into bits on their polarization. They will be used to send encrypted information. The important thing about this key is that both parties neither sender or receiver can't determine in advance what the key will be. The reason behind that is because it is the product of their random choices. Let's suppose even if an attacker defeats the quantum key distribution she must also randomly select either a diagonal or a rectilinear filter to measure Alice's photon correctly. It's true that Eve will have an equal chance of selecting the right or wrong filter but he won't be able to confirm with Alice the type of filter he used. Which means that Eve can't interpret the final key or the photon that forms the final key and can't do anything. First of all, according to the Heisenberg Uncertainty principle photons will be destroyed once they are measured and will no longer exist. That's why they can not be duplicated. Secondly, in order to know the length of the one time path since it corresponds to the length of the message, sender and receiver must calculate the amount of photons which is required to form the encryption key.

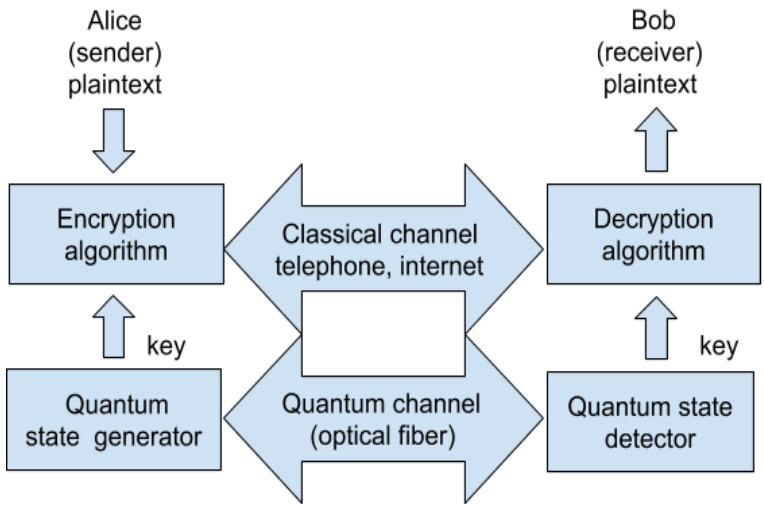

Fig. 1. Quantum key distribution example

Bob should receive about 25 percent of transmitted photons if not he can be certain that there's something wrong. The fact is that a photon will no longer exist to be detected by Bob. Even if an eavesdropper tries to create a photon and pass it to Bob, she must be lucky to randomly choose its orientation correctly too since the chances of not being correct is 50 percent is enough to reveal her presence.

1 - Alice sends a random sequence of photons polarized horizontal, vertical, right circular And left circular;

2 - Bob measures the photons polarization in a random sequence of bases, rectilinear (+) and circular;

3 - result of Bob's measurement (some photons may not be received at all);

4 - Bob tells Alice which bases he used for each photon he received;

5 - Alice tells him which bases were correct;

6 - Alice and Bob keep data only from these correctly measured photons discarding all the rest;

7 - This data is interpreted as a binary sequence according to the coding scheme = = 0 and = = 1.

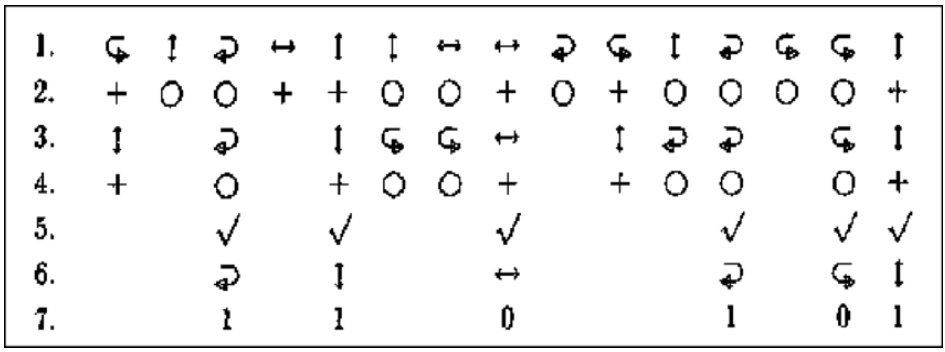

Fig. 2. Basic quantum key distribution protocols signs.

Confidentiality of keys

It is possible that Diffie-Hellman may perhaps be broken in the future by eavesdropping. Beside this classic secret system has suffered from different problems due to the insider threats or some other problems. Also public key suffers from ongoing uncertainty and mathematically its intractable and its widely used as internet security architecture nowadays. Since QKD [15] is capable of providing automatic distribution of keys that may offer more security, we can assume it as properly embedded techniques and overall secure system.

QKD protocols implementation

Many aspects of QKD protocols [16] are unusual both in motivation and implementation and it might be an interest in communication protocols for specialists. Because quantum cryptography contains specialized protocols which are called as QKD protocols.

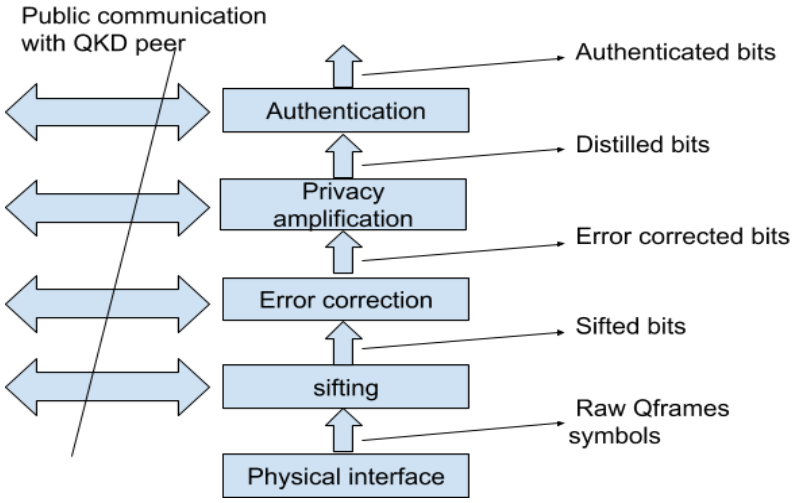

Fig. 3. QKD protocol implementation.

The protocols that we are talking about here are running in C language which is designed by DARPA that makes plugging new protocols easier and it's also possible that they invent and practice new QKD protocols in coming years. These protocols are more like pipeline stages and could be examples as sub layers.

Quantum solution and tools in industries

Nowadays , it's almost impossible to imagine a company or a big organization without using IT facilities. Banking systems, nuclear power plants, aircrafts, satellites and space crafts, all of them are being controlled and measured by their security level. Availability, integrity and confidentiality are the main factors in development secure telecommunication systems. Cryptographic systems are the best way to ensure they are working effectively. This is a great system but there's a problem which is Key distribution, but it can be solved with the help of SECOQC. After analysing different papers it seems that QKD could be an alternative solution for key distribution problems. Quantum key distribution protocols are used to generate keys and distribute them between two parties using quantum and classical channels. The first protocol was proposed by Bennett and Brassard from IBM and Montreal university in 1984 using single qubit with polarization states. (0, 45, 90, 135) are the four polarization states of photons.

Authentication

Authentication job is to guard Alice and Bob against attacks like "man in the middle attacks". It helps to make sure that Alice is communicating with Bob not eavesdroppers and vice versa. Since eavesdroppers may get into the conversation between Bob and Alice at any stage that's why it's recommended to perform authentication on an ongoing basis for all key management traffic.

Types of cryptography	*Description*	*Advantages*	*Limitations*
Modern cryptography (DES (Tuchman, 1997), IDES (Dang and Chau, 2000), AES (Zeghid et al., 1996), RSA (Cormen et al., 2001).	Algorithms operate on strong mathematical concepts that make them computationally efficient for protection and secrecy of highly sensitive.	Non-dependency on the medium colossal communication range multiple platforms for implementation. very high security.	Absolutely impractical because of the inherent properties of image such as bulk data capacity, strong correlation among adjacent pixels and high redundancy.
Quantum cryptography or quantum key distribution (QKD)	Makes use of the secret key whose randomness and secrecy are assured based on the Heisenberg uncertainty principle of physics.	The QKD would be unconditionally secure even with the endurance of quantum computer and with the users can perform QKD without quantum	Weak properties of coherent pulses and the detectors used ir the implementation of QKD (Valerio ar Christian, 2014).

Fig. 4. QKD comparison.

Based on hash functions introduced by Wegman and Carter [17] the solution to the authentication problem and discussed a solution. To solve the authentication problem Alice and Bob should already share a secret key in order to use a hash function from the family and generate an authentication between them. With the use of hashing the chances of accessing or eavesdropping between two parties is really low no matter how high the system computational power is. There are many more details including symmetric authentication which limits the opportunities for attackers and the main point is that the bits of a secret key can not be used on a different data once it's used. We also need to mention that authenticating QKD protocols is not the only thing we should care about. Authenticating VPN traffic is also as important as QKD protocols and we must apply the techniques to control the traffic of data. After drawing the circuit shown in figure and applying CNOT and Hadamard gate we got two results. The figure 5 shows the result of running our model on a simulator and the figure 4 shows the result on a real quantum device.

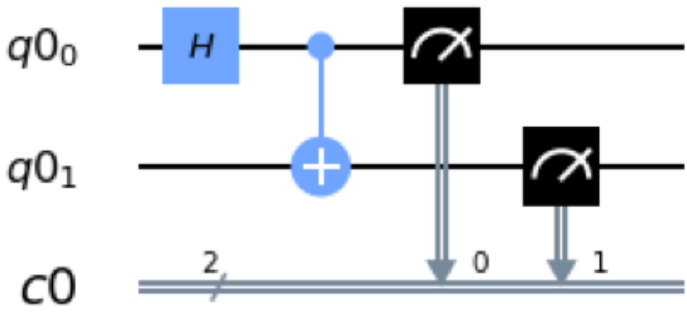

Fig. 5. Result of running a model on a simulator.

Below is the result of Aer's Qasm simulation on a classical device and on a real quantum device on IBM Q Experience. The full source code is on my GitHub's [18] account.

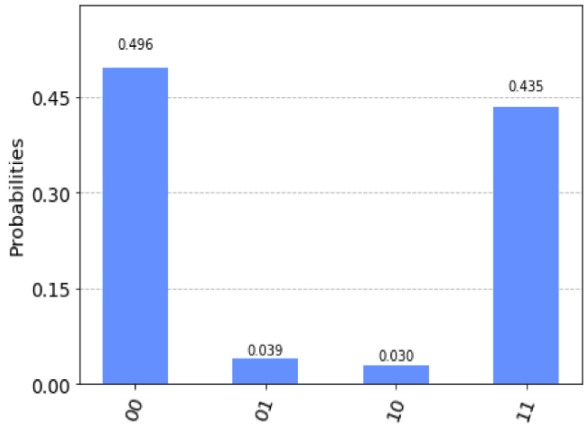

Fig. 6. Result of running a model on a real quantum device.

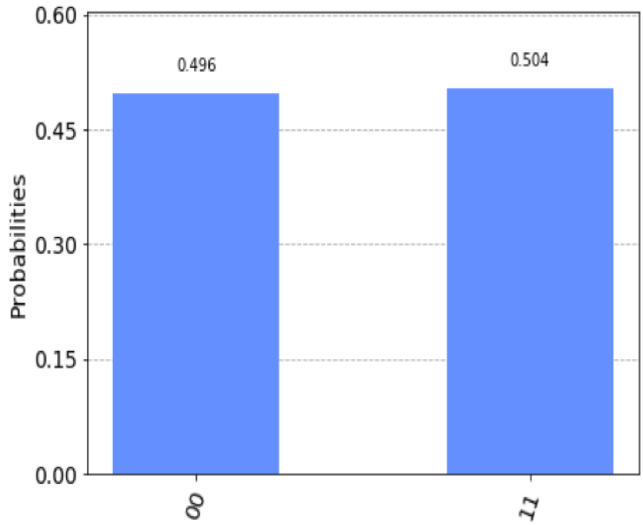

Fig. 7. Result of running a model on a simulator.

Discussion and conclusion

DARPA [19] is one of the biggest leading companies in quantum products and devices and has started to build QKD links woven into an QKD network that connects its endpoints via routers. But in some cases when the given point to point QKD link fails, example fiber cut or too much noise it uses another link instead. This quantum network can be engineered even when it's under the denial of service attack or Dos attack. DARPA quantum network is aiming to reach a great deal of active research to solve the geographic reach problem. And if they achieved these practical devices these problems may not exist anymore and it will be a new step towards a quantum revolution. One of the proposed solutions could be chaining the quantum cryptography links in different stations or it's also possible to transfer through orbiting satellites which here satellite act as bridge or intermediary station. Researchers are still working on this area to send quantum keys to satellites and vice versa to another station securely which is under supervision of giant technology companies and governments like US and European countries. Its true that there's been a huge progress in quantum cryptography in the last decades But still there's a lot of questions remained not answered that's why it's not the correct time to deploy and use quantum cryptography as key distribution system for governments or business Developing new devices with capability of higher qualities and to be able to transfer to longer destinations are part of the not answered questions or challenges. However, advancement of processing powers in computer systems

will remain as a threat for cryptography systems and it could be an influence in development of quantum cryptography. There's been a huge interest in investing big amounts in quantum cryptography technologies. Because it's not because it has the potential to make a valuable contribution in security of businesses and ecommerce but it could open a new door and take us to a new world of science.

References

1 IBM Research Lab, Online IBM Quantum computing. URL: https://www.ibm.com/quantum-computing/.
2 Microsoft, Online Microsoft: Quantum computers. URL: https://www.microsoft.com/en-us/quantum.
3 Ali baba Researchers, Online Ali baba: Quantum computing. URL: https://damo.alibaba.com/labs/quantum.
4 Peev, M. and et.al. The SECOQC quantum key distribution network. URL: https://iopscience.iop.org/article/10.1088/1367-2630/11/7/075001/meta.
5 Gordon L. S. Artical quantum mechanics, Quantum mechanics. URL: https://www.britannica.com/science/quantummechanics-physics.
6 Khan academy, Cryptography. URL: https://www.khanacademy.org/computing/computerscience/cryptography.
7 Exabeam, Information security. URL: https://www.exabeam.com/information-security/rsa-algorithm/.
8 W-pedia, Data encryption standard. URL: https://en.wikipedia.org/wiki/Data-Encryption-Standard.
9 Science direct, Computer science cryptographic science. URL: https://www.sciencedirect.com/topics/computer-science/cryptographicsystem.
10 Wired, Quantum-cryptography and the future of security. URL: https://www.wired.co.uk /article/quantum-cryptography-and-the-futureof-security.
11 Conversation, Heisenberg's Uncertainty-principle, URL: http://theconversation.com/explainerheisenbergs-uncertainty-principle-7512.
12 Wiki, Photon polarization, URL: https://en.wikipedia.org/wiki/Photon-polarization.
13 Gate, R. The Quantagrid project RO-Quantum-security in grid-computing applications. URL: https://www.researchgate.net/publication/234853582-The-

Quantgridproject-RO-Quantum-security-in-grid-computing-applications.
14 Quantum, Quantum Key Distribution, URL: https://qt.eu/understand/underlying-principles/quantum-key-distributionqkd.
15 Kuppam, S. Modelling and Analysis of Quantum Key Distribution Protocols, BB84 and B92, in Communicating Quantum Processes (CQP) language and Analysing in PRISM. URL: https://arxiv.org/pdf/1612.03706.pdf.
16 Intechopen, Advanced technologies of quantum key distribution. URL: https://www.intechopen.com/books/advanced-technologies-of-quantumkey-distribution/security-of-quantum-key-distribution-protocols.
17 Sciencedirect, Hash functions. URL: https://www.sciencedirect.com/science/article/pii/0022000081900337.
18 Darpa, Quantum key distribution in industrie, URL: https://www.darpa.mil.
19 Shirzad, H. Quantum Encryption. URL: https://github.com/habibshirzad/ Quantum-Encryption.