DOI 10.52209/1609-1825_2023_1_423 UDC 004.056.5

Quantum Key Distribution Protocols Based on Heisenberg's Uncertainty

[1]***BEGIMBAYEVA Yenlik,** PhD, Associate Professor, enlik_89@mail.ru,*
*[2]**ZHAXALYKOV Temirlan,** Senior Lecturer, zhaxalykov8@gmail.com,*
[1]NCJSC «Kazakh National Research Technical University named after K.I. Satpayev», Kazakhstan, Almaty, Satpayev Street, 22a,
[2]Kazakh-British Technical University, Kazakhstan, Almaty, Tole Bi Street, 59,
**corresponding author.*

***Abstract.** The proposed article is devoted to the analysis of quantum key distribution protocols based on the Heisenberg uncertainty. The peculiarity of this topic lies in the fact that modern methods of key distribution, which use classical calculations at their core, have significant drawbacks, in contrast to quantum key distribution. This problem concerns all types of algorithms and systems for encrypting secret information, both symmetric encryption with a private key and asymmetric encryption with a public key. An example is that in a communication channel protected by quantum key distributions, it is possible to detect an interceptor between two legal network entities using the principles laid down in quantum physics at the beginning of the last century. Principles and theorems such as the Heisenberg principle, quantum entanglement, superposition, quantum teleportation, and the no-cloning theorem. The field of study of this topic is a promising and rapidly developing area in the field of information security and information protection. There are already created commercial products with the implementation of some of the quantum key distribution protocols. Many of the created products are used in various spheres of human activity. The relevance of applying quantum key distribution protocols under ideal conditions without taking into account errors in the form of quantum noise is analyzed. The implementation of two quantum key distribution protocols based on the Heisenberg uncertainty principle is demonstrated, as well as the results of the appearance of keys and the probability of occurrence of each of them. The purpose of the article is aimed at analyzing and researching quantum key distribution protocols based on Heisenberg uncertainty. The article discusses the advantages and disadvantages of the BB84, B92 quantum key distribution protocols.*

***Keywords:** quantum cryptography, quantum key distribution, Heisenberg's uncertainty principle, superposition, quantum gate, photon, polarization, quantum computing, measurement, quantum circuit.*

Introduction

The fundamental errand of cryptography is to cover up information, as a rule by altering it numerically. Over time, cryptography started to illuminate other issues that are near to encryption in terms of arrangement strategies, for illustration, such as the issues of producing and distributing keys, the issue of confirming parties. At the same time, the facilitated activities of clients, the result of which is the arrangement of such issues, are called cryptographic protocols [1].

At the starting of the twentieth century a near association was found between information theory and material science. Victory in tackling numerous issues that at to begin with look are related as it were to the theory of information and, in like manner, its security, can be accomplished by applying the material science of quantum particles. That's, with the utilize of photons and their polarization, electrons and the direction of their spin. Application has found itself in different regions of information theory and computer science. A striking case is the Grover algorithm, the Bernstein-Vazirani algorithm, and the Deutscha-Jozsa algorithm. Two fundamental questions emerged some time recently researchers [2]: how extraordinary are the conceivable outcomes of quantum algorithms? Is it conceivable to make gadgets that actualize these calculations?

Within the 60s of the twentieth century, when information technologies and computer innovation started to create at a fast pace, a unused science was born – quantum information theory. Quantum theory may be a numerical show of the advanced thought of the physical properties of the encompassing world and the physical frameworks of which it consists [3].

Judging by the comes about of inquire about carried out within the field of quantum information theory and the investigation of quantum systems that are as of now being built in hone, quantum information theory has brilliant prospects in cryptography, covering a really wide extend of issues in this region. One such issue is quantum key distribution.

Quantum cryptography, a way of applying the laws of quantum physics to nullify all the efforts of an eavesdropping agent, has grown over the past decade from the level of a fundamental idea into a whole multidisciplinary scientific direction [4-6]. In the modern world, the spectrum of quantum cryptography is very wide. It includes such areas as: quantum key distribution, quantum secure direct communication protocols, quantum digital signature. Among the aforementioned areas, the main focus is quantum key distribution, which already has applications in the industry. Therefore, a thorough analysis of the quantum key distribution protocols is one of the priority tasks.

Quantum key distribution is a method by which a secret key can be distributed between two subscribers (Alice and Bob) if they have access to a quantum communication channel, i.e. a channel for transmitting individual quantum particles, for example, photons, and an open conventional channel with the ability to authenticate the sender of a message [6]. The qubits that have been transmitted via quantum communication are exploited in order to form a secret key. The generated key is used by encryption algorithms to create a secret message in the implementation of receiving and transmitting secret information between subscribers. Secret key generation using quantum key distribution protocols can be used in both symmetric and asymmetric encryption systems.

The main advantage of quantum key distribution over conventional classical schemes is the fundamental possibility of detecting an eavesdropping agent, which, due to the laws of quantum physics, is forced to disturb the states of transmitted quantum particles during eavesdropping [5, 6].

In this case, the party standing between two legal communication subscribers makes changes to the sent stream of qubits and a certain percentage of errors are made when measuring the state of the qubit. In the case of a high percentage of errors when sending the sequence, this will serve as a notification for two legal entities to stop the key generation process and start generating a new key.

It should be taken into account that inaccuracies in poisoning qubits can appear not only due to the presence of an eavesdropper in the quantum network, but also due to physical interference and attenuation in quantum communication. With quantum key distribution, due to the inability to distinguish physical interference from the presence of the fact of listening by a third party, all inaccuracies fall into the rank of inaccuracies created by the eavesdropper. Currently, in experiments on the transmission of qubits via fiber optic channels, as well as over the air, the level of natural interference is achieved no more than a few percent [7].

The current quantum key distribution protocols use quantum bits, or as they can be called qubits in another way. These systems can be divided into two classes. The first is protocols that provide the secrecy of key distribution and are based on the Heisenberg uncertainty principle. The second class is protocols based on the principle of quantum entanglement.

Nowadays, it is still a difficult task to confirm the security of the entire scheme of the quantum key distribution protocol, since it has not yet been solved for a single protocol. But it can be noted that in the literature there are analyzes of some aspects of resistance to attacks of certain protocols. In this paper, not only one specific protocol is considered, but a subclass of protocols operating on the same principle.

Method & Materials

BB84 Protocol Principle

This protocol works as follows: at each step, the transmitting side sends one of the states from the non-orthogonal set, and the receiving side measures that, after additional exchange of classical information between the parties, they should have bit strings that completely match in the case of an ideal channel and no interceptor. Errors in these lines can indicate both the imperfection of the channel and the actions of the eavesdropper. If the error exceeds a certain limit, the operation of the protocol is interrupted, otherwise legitimate users can extract the fully secret key from their bit strings.

The BB84 protocol uses two bases:

$$+ : |V\rangle = |0\rangle,\ |P\rangle = |1\rangle,$$

$$\times : |a\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\ |b\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

At the state preparation stage, Alice randomly chooses one of the specified bases, and then randomly chooses a bit value: 0 or 1, and in accordance with this choice sends one of four signals (Table).

On each of these signals, Alice remembers her choice of basis and choice of bit, resulting in two random bit strings on her side.

Bob, receiving each of the signals sent by Alice, randomly performs one of two measurements on him, each of which is able to give a reliable result due to the orthogonality of the states within each Alice's basis.

As a result, he has two lines: with which of the bases were chosen for the measurement, and with the outcomes of these measurements.

So, after transferring all the states and taking

Alice's sending signals according to basis and bit value

Signal	Basis	Bit value
v	+	0
p	+	1
a	×	0
b	×	1

measurements, Alice and Bob have two rows each. Here the bases are matched: through an open channel, Alice and Bob announce to each other their lines with the choice of bases, and they throw out messages in which their bases do not match. It should be noted that if the basis used to send the state by Alice coincided with the basis of Bob's measurement, then in the absence of interference in the communication channel, the results in their bit strings at the corresponding position will match, therefore, after the stage of matching the bases in the case of an ideal channel and no Interceptor actions Alice and Bob must have the same bit strings.

However, if there were errors in the channel or an interceptor attempted to eavesdrop, Alice's and Bob's bitstrings might not match, so they would need to consistently reveal about half of their bitstrings to verify. According to the central limit theorem, the error in the disclosed bit sequence gives a fairly accurate estimate of the error in the entire sequence, and it can be used to accurately estimate the error probability in the remaining positions. If the error value is greater than a certain value, the data transfer stops: this means that the interceptor has too much information about the key.

Realization of BB84

This area portrays the execution of the BB84 quantum key distribution protocol on the IBM Quantum Experience stage. In this try, we are going utilize the 8-qubit adaptation of this protocol.

At the starting, the sender will produce two sequences of zeros and ones. The primary arrangement is for encoding bases and the moment arrangement is utilized for encoding states. Then, having produced two arrangements, the sender employments quantum gates to encode the data. In the event that the sender decides to encode 1 into a qubit, at that point he will got to utilize an X gate on that qubit. When deciding to encode 0, no gates are required to apply watts to this qubit, since qubits in a qiskit are within the state by default. After performing these operations, the sender sends qubits to the beneficiary. The recipient continues to the activity of perusing the sender's qubits with regard to its created bit arrangement. When measuring qubits within the Hadamard basis, the recipient applies the suitable Hadamard gate to perform the perusing. Realization of quantum key distribution protocol BB84 with eight qubits are presented in the Figure 1 [8].

B92 Protocol Principle

This protocol uses the idea of a non-orthogonal pair of states. It should be noted that in the BB84 protocol, in the absence of interceptor actions and interference in the channel, the error on the receiving side is 25%. This is caused by the use of a «hard» configuration of two pairs of basis vectors. The purpose of the B92 protocol is to be able to flexibly change this parameter depending on additional conditions – such as the length of the channel or its quality. This can in some cases help to achieve a higher data transfer rate.

At each step of the B92 protocol, Alice sends Bob one of two non-orthogonal states $|\varphi_0\rangle$ and $|\varphi_1\rangle$, where $\langle\varphi_0|\varphi_1\rangle = \cos(n)$ is the main parameter of the protocol. Bob on his side performs the «measurement» already described above with three outcomes (1):

$$M_0 = \frac{\left|\varphi_1^{\perp}\right\rangle\left|\varphi_1^{\perp}\right\rangle}{1+\cos(n)} = \frac{I-|\varphi_1\rangle\langle\varphi_1|}{1+\cos(n)},$$
$$M_1 = \frac{\left|\varphi_0^{\perp}\right\rangle\left|\varphi_0^{\perp}\right\rangle}{1+\cos(n)} = \frac{I-|\varphi_0\rangle\langle\varphi_0|}{1+\cos(n)}, M_? = I - M_0 - M_1. \quad (1)$$

Recall that when such a measurement is applied to the indicated states, the first two outcomes will, in the absence of errors, give exact results, while the

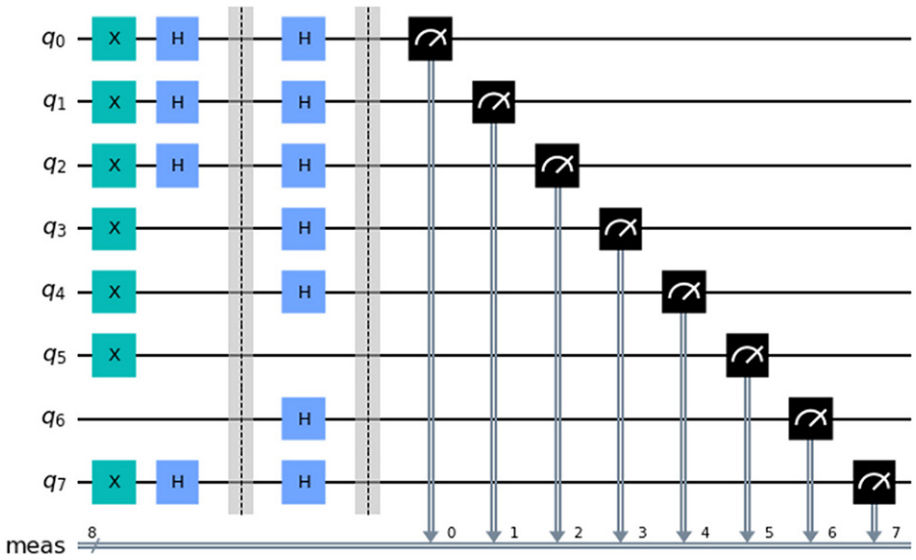

Figure 1 – Realization of quantum key distribution protocol BB84 with eight qubits

inconsistent outcome does not provide useful information about the transmitted state. Messages with such outcomes are discarded.

After the transmission of all messages, Alice and Bob, just as it happened in the BB84 protocol, unanimously reveal part of their bit sequences and estimate the number of errors. If they turned out to be more than a certain threshold value, the protocol execution is interrupted, otherwise the fully secret key is extracted from the rest of the bit strings. The most important property of the B92 protocol is the presence of a parameter – the angle n between the signal states. The closer this angle is to n/2, the closer the protocol is to simply sending signals using non-orthogonal states. In this case, the data transfer rate increases, but their resistance to interception decreases. When using small values of n, the probability of obtaining inconsistent outcomes is high, which reduces the data transfer rate, but significantly complicates the situation for the hooker [9-10].

Realization of B92

This segment portrays the execution of the B92 quantum key distribution protocol on the IBM Quantum Experience platform. In this explore, we are going utilize the 8-qubit adaptation of this protocol.

The implementation of the B92 (Figure 2) protocol could be a more disentangled form of the usage of the BB84 protocol, in guideline, as is the association between these protocols. At the starting, the sender and collector haphazardly create an arrangement of bits to send and examined, individually. The execution of the protocol is carried out utilizing the Hadamard gate. The protocol is outlined so that in case the sender encodes at that point the beneficiary will study it in a computational basis and get the same when measured. In case the beneficiary considers the given qubit in |+⟩, |–⟩ bases, at that point the result will be smaller |–⟩. It is additionally worth considering if the sender will utilize |+⟩. In case, when sending a given qubit, the recipient will degree it within the same premise, at that point the result of the estimation will be 1.

Results

The paper analyzes the quantum key distribution protocols working on the Heisenberg uncertainty rule. The standards of operation of two protocols B92 and BB84 are portrayed. The realization of quantum key distribution protocols BB84 and B92 was moreover performed on the IBM Quantum Experience platform. Able to see the comes about of the realization of these protocols within the taking after histograms.

Figure 3 appears us the disseminated likelihood between keys that a sender and recipient can create inside a arrange utilizing the BB84 quantum key distribution protocol.

Figure 4 appears us the disseminated likelihood between the keys that a sender and collector can produce inside a arrange utilizing the B92 quantum key distribution protocol.

It ought to be famous that the number of keys created within the B92 protocol varies from the created keys in BB84. Which shows the fruitful adjustment of the BB84 protocol to B92. Since with a large number of keys it'll be troublesome for an interceptor to choose up a key, and due to such an expansive changeability within the state of qubits amid key arrangement, it'll be troublesome to spy and captured the values of a qubit without ruining its state.

Conclusion

In conclusion, we are able say that cryptography has been experiencing a period of alter over the past 30 a long time. In the event that prior cryptography

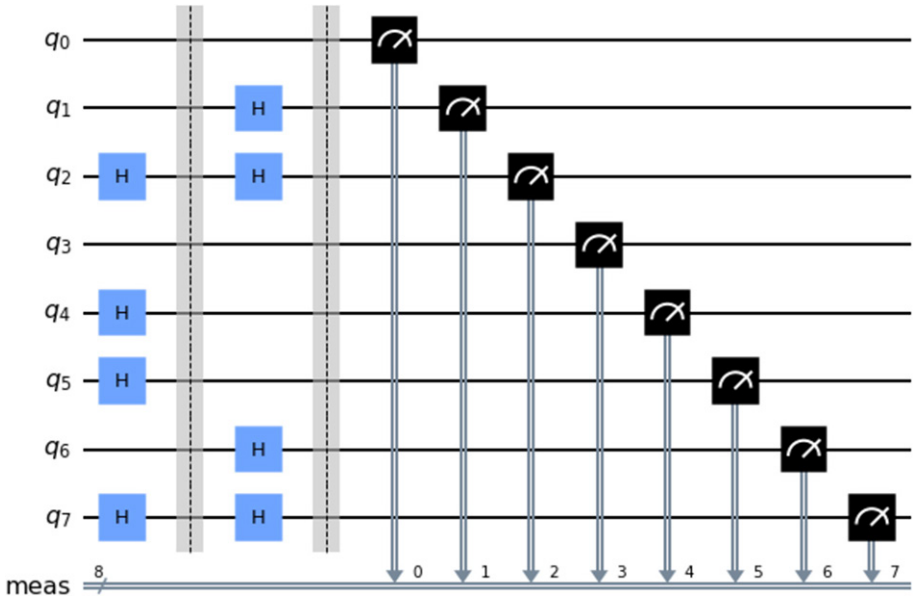

Figure 2 – Realization of quantum key distribution protocol B92 with eight qubits

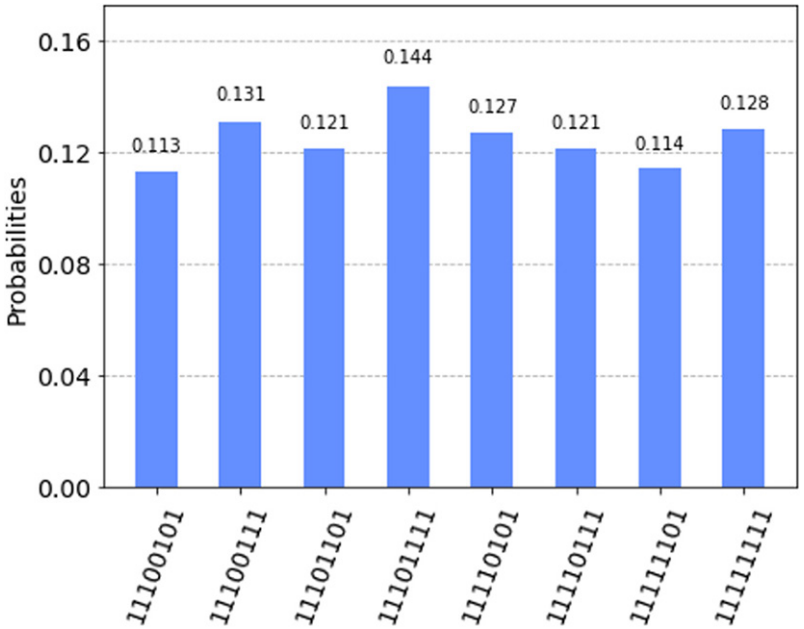

Figure 3 – Realization result of BB84

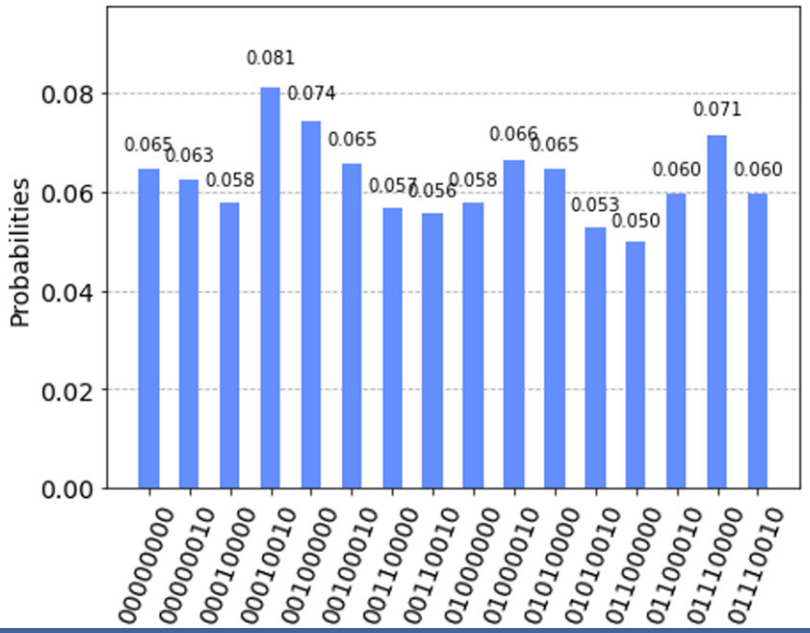

Figure 4 – Realization result of B92

depended on the soundness of the laws of arithmetic, at that point with the appearance of a modern sort of calculation, such as quantum computing, everything started to alter significantly. Presently the standards, hypotheses and laws laid down by the founders of quantum mechanics are utilized to essentially actualize the most columns of cryptography, such as privacy, astuteness, accessibility. This work was committed to the use of one of these standards in cryptography. The Heisenberg Uncertainty Rule could be a habitually utilized rule in quantum key dissemination that's still in utilize nowadays. The foremost well-known protocols working on this guideline are BB84 and B92, which were sanctified in this work. In this work, the usage and depiction of these protocols was illustrated, where the comes about appeared us the probabilities of creating a certain key in both protocols. These implementations appear in detail and clearly the utilize of the Heisenberg uncertainty rule by both quantum key distribution protocols, utilizing the Hadamard gate, which drives the qubits into a superposition, in this manner guaranteeing an alter within the polarization of the qubit amid its reading. The usage specified within the work could be a great illustration for studying the forms of these protocols. Besides, these

usages don't utilize a expansive number of qubits and operations on them to get a range of produced key comes about, which diminishes the working time and the number of operations performed by a quantum computer.

The foremost prevalent protocols working on this rule are BB84 and B92, which were sanctified in this work. In this work, the execution and portrayal of these protocols was illustrated, where the comes about appeared us the probabilities of producing a certain key in both protocols. It ought to be famous that the B92 protocol may be an alteration of the BB84 protocol. The victory of the alteration can be considered a broader department of key era.

REFERENCES

1. Кронберг Д., Ожигов Ю., Чернявский А. Квантовая криптография / МГУ имени М.В. Ломоносова. Москва, 2006, С. 23-40.
2. Вялый М. (2011). Квантовые алгоритмы: возможности и ограничения. Санкт-Петербург. URL: https://storage.yandexcloud.net/lms-vault/private/2/courses/2011-spring/spb-quantumalgorithms/materials/20110403_quantum_algorithms_vyali_lecture_notes.pdf (дата обращения 05.05.2022).
3. Постулаты квантовой теории. ВГУ,2012. URL: http://www.rec.vsu.ru/rus/ecourse/quantcomp/sem2.pdf (дата обращения 05.05.2022).
4. Shicheng Zhao, Wendong Li, Yuan Shen, YongHe Yu, XinHong Han, Hao Zeng, Maoqi Cai, Tian Qian, Shuo Wang, Zhaoming Wang, Ya Xiao, and Yongjian Gu, «Experimental investigation of quantum key distribution over a water channel», Appl. Opt. 58, 3902-3907 (2019). https://opg.optica.org/ao/abstract.cfm?URI=ao-58-14-3902 (дата обращения 05.05.2022).
5. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145-195.
6. Баумейстер Д., Экерт А., Цайлингер А. Физика квантовой информации. – Москва: «Постмаркет», 2002. – 376 с.
7. Bechmann-Pasquinucci, H. (2006). Eavesdropping without quantum memory. Physical Review A, 73, 44-305. Retrieved from The Heat Is Online website: https://doi.org/10.1103/PhysRevA.73.044305.
8. Bloom, Y.; Fields, I.; Maslennikov, A.; Rozenman, G.G. Quantum Cryptography – A Simplified Undergraduate Experiment and Simulation. Physics 2022, 4, 104-123. https://doi.org/10.3390/physics4010009.
9. Diffie W. Hellman M.E. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory, 22, 644. DOI: 10.1109/TIT.1976.1055638
10. Chi Zhang, Xiao-Long Hu, Cong Jiang, Jiu-Peng Chen, Yang Liu, Weijun Zhang, Zong-Wen Yu, Hao Li, Lixing You, Zhen Wang, Xiang-Bin Wang, Qiang Zhang, and Jian-Wei Pan Experimental Side-Channel-Secure Quantum Key Distribution // Phys. Rev. Lett. 128, 190503 – Published 13 May 2022.

Гейзенберг белгіліктігіне негізделген кілтті бөлу кванттық хаттамалары

[1]***БЕГИМБАЕВА Енлик Ериковна,*** *PhD, қауымдастырылған профессор, enlik_89@mail.ru,*
[2]***ЖАКСАЛЫКОВ Темирлан Мирамбекович,*** *аға оқытушы, zhaxalykov8@gmail.com,*
[1]*«Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті» КеАҚ, Қазақстан, Алматы, Сәтбаев көшесі, 22а,*
[2]*Қазақстан-Британ техникалық университеті, Қазақстан, Алматы, Төле би көшесі, 59,*
**автор-корреспондент.*

Аңдатпа. *Ұсынылған мақала Гейзенбергтің белгісіздігіне негізделген кванттық кілтті тарату хаттамаларын талдауға арналған. Бұл тақырыптың ерекшелігі – классикалық есептеулерге негізделген кілттерді таратудың қазіргі әдістерінің кванттық кілтті бөлуден айырмашылығы айтарлықтай кемшіліктері бар. Бұл мәселе құпия ақпаратты шифрлауға арналған алгоритмдер мен жүйелердің барлық түрлеріне қатысты, яғни симметриялық жеке кілт шифрлауы және асимметриялық ашық кілт шифрлауы. Мысал ретінде кванттық кілтті тарату арқылы қорғалған байланыс арнасында өткен ғасырдың басында кванттық физикада белгіленген қағидаларды пайдалана отырып, екі заңды желі субъектілері арасындағы интерцепторды анықтауға болады. Гейзенберг принципі, кванттық түйісу, суперпозиция, кванттық телепортация және клондаудың жоқтығы теоремасы сияқты принциптер мен теоремалар. Бұл тақырыптың зерттеу саласы ақпараттық қауіпсіздік және ақпаратты қорғау саласындағы перспективті және қарқынды дамып келе жатқан бағыт болып табылады. Коммерциялық өнімдер қазірдің өзінде кейбір кванттық кілттерді тарату хаттамаларын енгізу арқылы жасалған. Жасалған өнімдердің көпшілігі адам қызметінің әртүрлі салаларында қолданылады. Кванттық шу түріндегі қателерді есепке алмай, идеалды жағдайларда кванттық кілтті тарату хаттамаларын қолдану өзектілігі талданады. Гейзенбергтің белгісіздік принципіне негізделген екі кванттық кілтті тарату хаттамасының орындалуы, сонымен қатар кілттердің пайда болу нәтижелері және олардың әрқайсысының пайда болу ықтималдығы көрсетілген. Мақаланың мақсаты Гейзенбергтің белгісіздігіне негізделген кванттық кілтті тарату хаттамаларын талдауға және зерттеуге бағытталған. Мақалада BB84, B92 кванттық кілттерді тарату хаттамаларының артықшылықтары мен кемшіліктері талқыланады.*

Кілт сөздер: *квантық криптография, кванттық кілттердің таралуы, Гейзенбергтің белгісіздік принципі, суперпозиция, кванттық қақпа, фотон, поляризация, кванттық есептеу, өлшеу, кванттық схема.*

Квантовые протоколы распределения ключей, основанные на неопределенности Гейзенберга

[1]***БЕГИМБАЕВА Енлик Ериковна,** PhD, ассоциированный профессор, enlik_89@mail.ru,*
[2]***ЖАКСАЛЫКОВ Темирлан Мирамбекович,** старший преподаватель, zhaxalykov8@gmail.com,*
[1]НАО «Казахский национальный исследовательский технический университет имени К.И. Сатпаева», Казахстан, Алматы, ул. Сатпаева, 22а,
[2]Казахстанско-Британский технический университет, Казахстан, Алматы, ул. Толе би, 59,
**автор-корреспондент.*

***Аннотация.** Предлагаемая статья посвящена анализу протоколов распределения квантовых ключей, основанных на неопределенности Гейзенберга. Особенность данной темы заключается в том, что современные методы распределения ключей, использующие в своей основе классические вычисления, имеют существенные недостатки, в отличие от квантового распределения ключей. Эта проблема касается всех типов алгоритмов и систем шифрования секретной информации, как симметричного шифрования с закрытым ключом, так и асимметричного шифрования с открытым ключом. Примером может служить то, что в канале связи, защищенном квантовыми распределениями ключей, можно обнаружить перехватчик между двумя легальными сетевыми субъектами, используя принципы, заложенные в квантовой физике в начале прошлого века: принципы и теоремы, такие как принцип Гейзенберга, квантовая запутанность, суперпозиция, квантовая телепортация и теорема о запрете клонирования. Область изучения данной темы является перспективным и бурно развивающимся направлением в области информационной безопасности и защиты информации. Уже созданы коммерческие продукты с реализацией некоторых протоколов квантового распределения ключей. Многие из созданных продуктов используются в различных сферах человеческой деятельности. Анализируется актуальность применения протоколов квантового распределения ключей в идеальных условиях без учета ошибок в виде квантового шума. Продемонстрирована реализация двух квантовых протоколов распределения ключей на основе принципа неопределенности Гейзенберга, а также результаты появления ключей и вероятности появления каждого из них. Цель статьи направлена на анализ и исследование протоколов распределения квантовых ключей, основанных на неопределенности Гейзенберга. В статье рассматриваются преимущества и недостатки протоколов распределения квантовых ключей BB84, B92.*

***Ключевые слова:** квантовая криптография, квантовое распределение ключей, принцип неопределенности Гейзенберга, суперпозиция, квантовый вентиль, фотон, поляризация, квантовые вычисления, измерение, квантовая схема.*

REFERENCES

1. Kronberg D., Ozhigov Y., Chernyavskyi A. Kvantovaya kriptographiya [Quantum Cryptography] / MSU named after M.V. Lomonosov. Moscow, 2006, pp. 23-40.
2. Vyalyi M. (2011). Quantum Algorithms: Possibilities and Limitations. St. Petersburg. URL: https://storage.yandexcloud.net/lms-vault/private/2/courses/2011-spring/spb-quantumalgorithms/materials/20110403_quantum_algorithms_vyali_lecture_notes.pdf (accessed 05.05.2022).
3. Postulates of quantum theory. VSU, 2012. URL: http://www.rec.vsu.ru/rus/ecourse/quantcomp/sem2.pdf (accessed 05.05.2022).
4. Shicheng Zhao, Wendong Li, Yuan Shen, YongHe Yu, XinHong Han, Hao Zeng, Maoqi Cai, Tian Qian, Shuo Wang, Zhaoming Wang, Ya Xiao, and Yongjian Gu, «Experimental investigation of quantum key distribution over a water channel», Appl. Opt. 58, 3902-3907 (2019). https://opg.optica.org/ao/abstract.cfm?URI=ao-58-14-3902 (accessed 05.05.2022).
5. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145-195.
6. Baumeyster D. Fizika kvantovoy informatsii [Physics of quantum information]. Postmarket, Moscow. 2002. – 376 p.
7. Bechmann-Pasquinucci, H. (2006). Eavesdropping without quantum memory. Physical Review A, 73, 44-305. Retrieved from The Heat Is Online website: https://doi.org/10.1103/PhysRevA.73.044305.
8. Bloom, Y.; Fields, I.; Maslennikov, A.; Rozenman, G.G. Quantum Cryptography – A Simplified Undergraduate Experiment and Simulation. Physics 2022, 4, 104-123. https://doi.org/10.3390/physics4010009.
9. Diffie W. Hellman M.E. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory, 22, 644. DOI: 10.1109/TIT.1976.1055638
10. Chi Zhang, Xiao-Long Hu, Cong Jiang, Jiu-Peng Chen, Yang Liu, Weijun Zhang, Zong-Wen Yu, Hao Li, Lixing You, Zhen Wang, Xiang-Bin Wang, Qiang Zhang, and Jian-Wei Pan Experimental Side-Channel-Secure Quantum Key Distribution // Phys. Rev. Lett. 128, 190503 – Published 13 May 2022.