Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 10, JUNE 2022

DOI: 10.37943/QRKJ7456

Y. Begimbayeva
PhD, Assistant Professor of the Department of Intelligent Systems and Cybersecurity
Astana IT University, Kazakhstan
enlik_89@mail.ru, orcid.org/0000-0002-4907-3345
Associate Professor of the Department of Cybersecurity, data processing and storage
Satbayev University, Kazakhstan

T. Zhaxalykov
Master student of Cybersecurity, Faculty of Information Technology
zhaxalykov8@gmail.com, orcid.org/0000-0002-6994-6377
Kazakh-British Technical University, Kazakhstan

RESEARCH OF QUANTUM KEY DISTRIBUTION PROTOCOLS: BB84, B92, E91

Abstract. The proposed article is devoted to the investigation of quantum key distribution protocols. The idiosyncrasy of this theme lies within the truth that present day strategies of key distribution, which utilize classical computing at their center, have critical downsides, in contrast to quantum key distribution. This issue concerns all sorts of calculations and frameworks for scrambling mystery data, both symmetric encryption with a private key and deviated encryption with an open key. A case is that in a communication channel ensured by quantum key distribution, it is conceivable to distinguish an interceptor between two legitimate organize substances utilizing the standards laid down in quantum material science at the starting of the final century. Standards and hypotheses such as the Heisenberg guideline, quantum trap, superposition, quantum teleportation, and the no-cloning hypothesis. The field of ponder of this theme may be a promising and quickly creating zone within the field of data security and data security. There are as of now made commercial items with the usage of a few of the quantum key dispersion conventions. Numerous of the made items are utilized in different circles of human movement. The significance of applying quantum key distribution conventions beneath perfect conditions without taking into consideration blunders within the frame of quantum clamor is analyzed. The usage of three quantum key distribution conventions is illustrated, as well as the comes about of the appearance of keys and the likelihood of event of each of them. The purpose of the article is pointed at analyzing and investigating quantum key distribution conventions. The article examines the points of interest and impediments of the BB84, B92, and E91 quantum key distribution conventions.

Key words: quantum cryptography, quantum key distribution, Heisenberg's uncertainty principle, superposition, quantum gate, quantum entanglement.

Introduction

The basic errand of cryptography is to cover up data, as a run the show by modifying it numerically. Over time, cryptography began to clarify other issues that are close to encryption in terms of the course of action methodologies, for the outline, such as the issues of creating and conveying keys, the issue of affirming parties. At the same time, the encouraged exercises

DOI: 10.37943/QRKJ7456

of clients, the result of which is the course of action of such issues, are called cryptographic conventions [1].

At the beginning of the twentieth century, a close affiliation was found between data hypotheses and fabric science. Triumph in handling various issues that, to start with, look related because they were to the hypothesis of data and, in a like way, its security can be achieved by applying the fabric science of quantum particles. That's, with the utilize of photons and their polarization, electrons and the direction of their turn. Application has found itself in several districts of data hypothesis and computer science. A striking case is the Grover algorithm, the Bernstein-Vazirani algorithm, and the Deutscha-Jozsa algorithm. Two crucial questions have been raised a few times as of late analysts [2]: how exceptional are the conceivable results of quantum algorithms? Is it conceivable to form contraptions that actualize these algorithms?

In the 60s of the twentieth century, when data advances and computer development began to form at a quick pace, a new science was born - quantum data hypothesis. Quantum hypothesis may be a numerical appear of the progressed thought of the physical properties of the including world and the physical systems of which it comprises [3].

Judging by the results of the experiments almost entirely carried out in the field of quantum data hypothesis and the examination of quantum frameworks that are presently being built in sharpen, quantum data hypothesis has brilliant prospects in cryptography, covering an extremely wide range of issues in this locale. One such issue is quantum key distribution [4].

Quantum cryptography, a way of applying the laws of quantum material science to invalidate all the endeavors of a listening in specialist, has developed over the past decade from the level of a principal thought into a multidisciplinary logical course [5]-[6]. Within the advanced world, the range of quantum cryptography is exceptionally wide. It incorporates such zones as quantum key conveyance, quantum secure coordinate communication conventions, and quantum advanced signature. Among the previously mentioned ranges, the most center is quantum key dispersion, which as of now has applications within the industry. In this manner, an intensive examination of the quantum key conveyance conventions is one of the necessary errands.

A quantum key distribution could be a strategy by which a mystery key can be dispersed between two endorsers (Alice and Bob) in case they have to get to a quantum communication channel, i.e. a channel for transmitting person quantum particles, for illustration, photons, and an open customary channel with the capacity to confirm the sender of a message [6]. The qubits that have been transmitted via quantum communication are abused in arrange to make a mystery key. The generated key is utilized by encryption calculations to make a mystery message within the execution of accepting and transmitting mystery data between endorsers. The mystery key era utilizing quantum key dispersion conventions can be utilized in both symmetric and hilter kilter encryption frameworks.

The biggest advantage of quantum key dispersion over conventional classical plans is the elemental plausibility of recognizing a listening in operator, which, due to the laws of quantum material science, is constrained to aggravate the states of transmitted quantum particles amid spying [5, 6].

In this case, the party standing between two legitimate communication endorsers makes changes to the sent stream of qubits and a certain rate of blunders are made when measuring the state of the qubit. In the case of a high rate of blunders when sending the arrangement, this will serve as a notice for two lawful substances to halt the key era handle and begin creating a modern key.

It ought to be taken into consideration that mistakes in harming qubits can show up not only due to the presence of a spy within the quantum arrangement, but also due to physical impedances and weakening in quantum communication. With quantum key dispersion, due

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 10, JUNE 2022

to the failure to recognize physical impedances from the nearness of the truth of tuning in by a third party, all mistakes drop into the rank of mistakes made by the busybody. As of now, in tests on the transmission of qubits by means of fiber optic channels, as well as over the discuss, the level of normal impedances is accomplished no more than some percent [7].

The current quantum key dispersion protocol utilizes quantum bits, or as they can be called qubits in another way. These frameworks can be isolated into two classes. The primary is conventions that give the mystery of key dispersion. The present course is conventions based on the rule of quantum ensnarement.

These days, it is still a troublesome errand to affirm the security of the whole plot of the quantum key conveyance convention since it has not yet been illuminated for a single convention. But it can be famous that within the writing there are analyzes of a few angles of resistance to assaults of certain conventions. In this paper, not only one particular convention is considered, but a subclass of conventions working on the same rule.

Literature review and problem statement

Various ponders by researchers Warke A., Behera B.K., Panigrahi P.K. and others [8] are committed to the issues of test execution of quantum key distribution protocols. Kronberg D., Ozhigov Y., Chernyavskyi A. consider strategies for deciding the security of quantum key distribution protocols [1]. Baumeyster D. bargains with the utilization of physical models in clarifying the development of protocol security [6]. Despite the ever-growing intrigue in this region, a number of issues stay pertinent and got to be addressed. In addition, the works are separated into two categories: the primary investigate and consider the security of protocols against different spying assaults, the moment investigate a productive execution demonstrate on diverse quantum computers, the third attempt to combine diverse quantum properties to move forward the security of quantum key distribution protocols, the fourth investigate the combination of classical cryptography protocols with quantum. So, most of the of the inquiries about concerns are the last mentioned, since classical cryptography is right now solid, and quantum cryptography has not however demonstrated viable from a commonsense point of see. There are considers in which different quantum key dissemination conventions are utilized to create a key in symmetric and hilter kilter encryption frameworks. This region is very complex, the environment around it is continually changing, in this manner, present-day data innovations are required for the foremost successful arrangement of rising issues.

Method & Materials

BB84 Protocol Principle

This protocol works as takes after: at each step, the transmitting side sends one of the states from the non-orthogonal set, and the accepting side measures that, after extra trade of classical data between the parties, they ought to have bit strings that totally coordinate within the case of a perfect channel and no interceptor [11]. Blunders in these lines can show both the defect of the channel and the activities of the spy. If the mistake surpasses a certain constrain, the operation of the protocol is hindered, something else authentic clients can extricate the completely mystery key from their bit strings.

The BB84 protocol uses two bases:

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

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

DOI: 10.37943/QRKJ7456

At the state planning organize, Alice haphazardly chooses one of the required bases, and after that arbitrarily chooses a bit esteem: or 1, and in agreement with this choice sends one of four signals (Table 1):

Table 1. Alice's sending signals according to basis and bit value

Signal	Basis	Bit value
V	+	0
P	+	1
A	x	0
B	x	1

On each of these signals, Alice recollects her choice of premise and choice of bit, coming about in two irregular bit strings on her side.

Bob, accepting each of the signals sent by Alice, arbitrarily performs one of two estimations on him, each of which is able to allow a solid result due to the orthogonality of the states inside each Alice's premise.

As a result, he has two lines: with which of the bases were chosen for the estimation, and with the results of these estimations.

So, after exchanging all the states and taking estimations, Alice and Bob have two lines each. Here the bases are coordinated: through an open channel, Alice and Bob declare to each other their lines with the choice of bases, and they toss out messages in which their bases don't coordinate. It ought to be known that on the off chance that the premise utilized to send the state by Alice coincided with the premise of Bob's measurement, at that point within the nonattendance of impedances within the communication channel, the comes about in their bit strings at the comparing position will coordinate, hence, after the arrange of coordinating the bases within the case of a perfect channel and no Interceptor activities Alice and Bob must have the same bit strings.

In any case, in the event that there were mistakes within the channel or an interceptor endeavored to listen in, Alice's and Bob's bitstrings might not match, so they would have to reliably uncover around half of their bitstrings to confirm [11]. According to the central restrain hypothesis, the mistake within the unveiled bit grouping gives a reasonably precise gauge of the error within the whole grouping, and it can be utilized to precisely appraise the blunder likelihood within the remaining positions. On the off chance that the blunder esteem is more prominent than a certain esteem, the information exchange stops: this implies that the interceptor has as well much data around the key [11].

Realization of BB84

This range depicts the execution of the BB84 quantum key dispersion protocol on the IBM Quantum Composer and the IBM Quantum Lab (previously known collectively as the IBM Quantum Experience) [12] organize. In this attempt, we are going to utilize the 8-qubit adjustment of this protocol.

In the beginning, the sender will deliver two arrangements of zeros and ones. The essential course of action is for encoding bases and the minute course of action is utilized for encoding states. At that point, having delivered two courses of action, the sender livelihoods quantum entryways to encode the information. Within the occasion that the sender chooses to encode 1 into a qubit, at that point he will need to utilize an X entryway on that qubit [8-10]. When choosing to encode 0, no doors are required to apply watts to this qubit, since qubits in a qiskit are inside the state by default [8-10]. After performing these operations, the sender sends qubits to the recipient. The beneficiary proceeds to the movement of examining the

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 10, JUNE 2022

sender's qubits with respect to its made bit course of action. When measuring qubits inside the Hadamard premise, the beneficiary applies the reasonable Hadamard entryway to perform the perusing. The realization of quantum key distribution protocol BB84 with eight qubits is displayed in Fig.1.

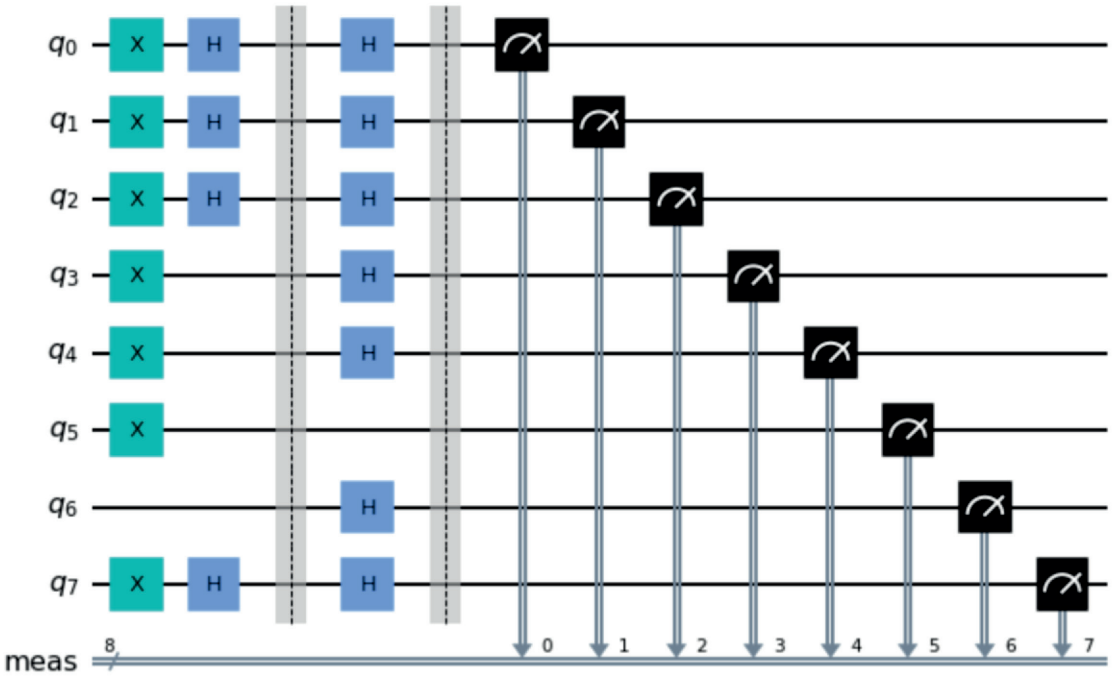

Figure. 1. Realization of quantum key distribution protocol BB84 with eight qubits

B92 Protocol Principle

This protocol employments the thought of a non-orthogonal combine of states [13]. It ought to be famous that within the BB84 protocol, within the nonappearance of interceptor activities and impedances within the channel, the blunder on the getting side is 25%. Typically caused by the utilize of a "difficult" setup of two sets of premise vectors. The reason 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 [13]. This could in a few cases offer assistance to attain a better information exchange 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 $\langle\varphi_0|\varphi_1\rangle = \cos(n)$ s the most parameter of the protocol [14]. Bob on his side performs the "measurement" as of now depicted over with three results (1):

$$M_0 = \frac{|\varphi_1^{\perp}\rangle\langle\varphi_1^{\perp}|}{1+cosn} = \frac{I - |\varphi_1\rangle\langle\varphi_1|}{1+cosn}, \quad M_1 = \frac{|\varphi_0^{\perp}\rangle\langle\varphi_0^{\perp}|}{1+cosn} = \frac{I - |\varphi_0\rangle\langle\varphi_0|}{1+cosn}, \quad M_? = I - M_0 - M_1. \tag{1}$$

Review that when such an estimation is connected to the demonstrated states, the primary two results will, within the nonattendance of mistakes, deliver correct comes about, whereas the conflicting result does not give valuable data approximately the transmitted state [14]. Messages with such results are disposed of.

After the transmission of all messages, Alice and Bob, fair because it happened within the BB84 protocol, consistently uncover portion of their bit groupings and assess the number of blunders. On the off chance that they turned out to be more than a certain edge esteem, the protocol execution is hindered, something else the completely mystery key is extracted from

DOI: 10.37943/QRKJ7456

the rest of the bit strings. The foremost vital property of the B92 protocol is the nearness of a parameter – the point n between the flag states. The closer this point is to n/2, the closer the protocol is to basically send signals utilizing non-orthogonal states. In this case, the information exchange rate increments, but their resistance to interferences diminishes. When utilizing little values of n, the likelihood of getting conflicting results is tall, which decreases the information exchange rate, but essentially complicates the circumstance for the hooker.

Realization of B92

This fragment depicts the execution of the B92 quantum key conveyance protocol on the IBM Quantum Composer and the IBM Quantum Lab (previously known collectively as the IBM Quantum Experience) [12]. In this investigation, we are going to utilize the 8-qubit adjustment of this protocol [15].

The usage of the B92 (Fig.2) protocol may be a more unraveled frame of the utilization of the BB84 protocol, in rule, as is the affiliation between these protocols. In the beginning, the sender and collector erratically make a course of action of bits to send and inspect separately. The execution of the protocol is carried out utilizing the Hadamard door. The protocol is laid out so that in case the sender encodes at that point the recipient will think about it in a computational premise and get the same when measured [15]. In case the recipient considers the given qubit in $|+\rangle, |-\rangle$ bases, at that point the result will be littler $|-\rangle$. It in addition worth considering in case the sender will utilize $|+\rangle$. In case, when sending a given qubit, the beneficiary will degree it inside the same introduce, at that point the result of the estimation will be 1.

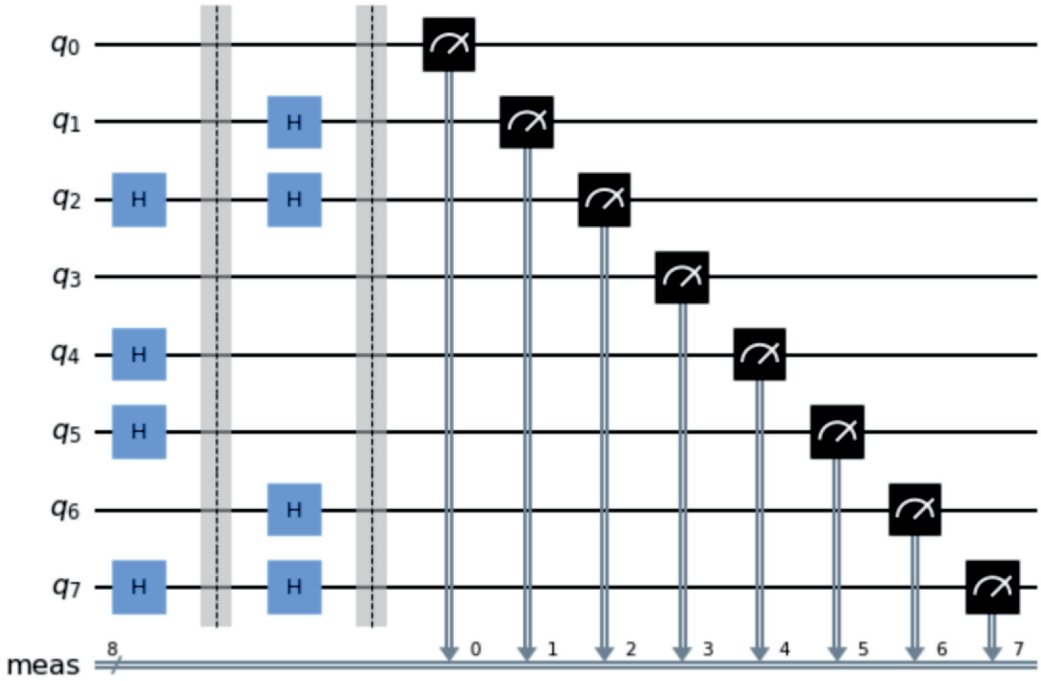

Figure 2. Realization of quantum key distribution protocol B92 with eight qubits

E91 Protocol Principle

This tradition was started by Arthur Eckert in 1991. It is called EPR (Einstein-Podolsky-Rosen) since it is based on the Einstein-Podolsky-Rosen problem [2].

The protocol proposes to utilize, for case, sets of photons made in antisymmetric polarization states. The capture endeavors of one of the photons of the coordinate does not bring Eve any information but may be a hail to Alice and Bob that their talk is being tapped.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 10, JUNE 2022

The EPR affect happens when a circularly symmetric atom exudes two photons in converse headings towards two onlookers [15]. Photons are emanated with a questionable polarization, but due to symmetry, their polarizations are ceaselessly reverse [15]. A crucial highlight of this affect is that the polarization of photons gets to be known because it was after estimation. Based on the EPR, Eckert proposed a tradition that guarantees the security of sending and putting absent the key. The sender makes some EPR photon sets. He keeps one photon from each combine for himself and sends the minute to his assistant. In this case, on the off chance that the selection adequacy is close to one, when the sender gets a polarization regard of 1, his accomplice will enroll a regard of and awful propensity versa. It is obvious that in this way the assistants can get vague pseudo-random code courses of action at anything point required.

Let N maximally trapped EPR-pairs of photons be to start with made, at that point one photon from each combine is sent to Alice, and the other to Bob. The three conceivable quantum states for these EPR sets are

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|\frac{3\pi}{6}\rangle_B - |\frac{3\pi}{6}\rangle_A|0\rangle_B\right), \tag{2}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|\frac{\pi}{6}\rangle_A|\frac{4\pi}{6}\rangle_B - |\frac{4\pi}{6}\rangle_A|\frac{\pi}{6}\rangle_B\right), \tag{3}$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}\left(|\frac{2\pi}{6}\rangle_A|\frac{5\pi}{6}\rangle_B - |\frac{5\pi}{6}\rangle_A|\frac{2\pi}{6}\rangle_B\right), \tag{4}$$

This may be composed in common as

$$|\psi_i\rangle = \frac{1}{\sqrt{2}}(|0_i\rangle_A|1_i\rangle_B - |1_i\rangle_A|0_i\rangle_B). \tag{5}$$

The ultimate condition unequivocally shows up that each of these three states encodes bits “0” and “1” in a uncommon preface. Alice and Bob at that point take estimations on their parts of the disconnected EPR sets utilizing the reasonable projectors.

$$P_1 = |0\rangle\langle 0|, \; P_2 = |\frac{\pi}{6}\rangle\langle\frac{\pi}{6}|, \qquad P_3 = |\frac{3\pi}{6}\rangle\langle\frac{3\pi}{6}|. \tag{6}$$

For each bit, Alice and Bob subjectively select a introduce for particle estimation, as inside the case of BB84 they conversation almost which procedures they utilized to degree particles in an open channel.

Due to the benchmarks of quantum trap, when utilizing the same introduce, Alice and Bob need to expect the reverse comes approximately, for the most part, this suggests that in organize to encourage the key, one of them must adjust its result. For the rest of the comes approximately, Alice and Bob test Bell’s dissimilarity as a test for the closeness of Eve.

Realization of E91 Protocol

To actualize the E91 quantum key distribution convention (Fig.3), there must be a source of qubits organized inside the singlet state. It does not matter to whom this source includes a place: to Alice, to Bob, to a number of trusted third-party Charlie or undoubtedly to Eve.

The steps of the E91 protocol:

1) Charlie, the proprietor of the singlet state arranging contraption, makes N entangled states and sends qubits A to Alice and qubits B to Bob by implies of the quantum channel.
2) Members Alice and Bob make strings. Depending on the components of these strings,

DOI: 10.37943/QRKJ7456

Alice and Bob degree the turn projections of their qubits along the taking after headings. We'll depict this handle as an estimation of the observables for each singlet state made by Charlie.

3) Alice and Bob record the come around of their estimations as components of strings exclusively.
4) Utilizing the classical channel, individuals compare their strings. In other words, Alice and Bob tell each other which estimations they have performed in the midst of the step 2. On the off chance that Alice and Bob have measured the turn projections of the m-th trapped combine of qubits onto the same course, at that point, they are past any question that they gotten reverse comes approximately.
5) Using the comes approximately gotten after measuring the turn projections Alice and Bob calculate the CHSH relationship regard, at that point Alice and Bob can be past any question that the states they had been getting from Charlie were captured in reality. This truth tells the individuals that there were no impedances inside the quantum channel.

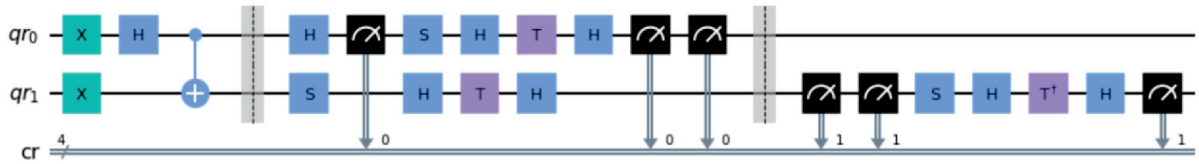

Figure 3. Realization of quantum key distribution protocol E91 with two qubits

Results

The paper analyzes the quantum key dispersion conventions working on the Heisenberg vulnerability run the show and quantum trap. The benchmarks of operation of two conventions B92, BB84, and E91 are depicted. The realization of quantum key distribution conventions BB84, B92 and E91 was in addition performed on the IBM Quantum Encounter stage. Able to see the comes around of the realization of these conventions inside the taking after histograms.

Fig. 4 shows us the spread probability between keys that a sender and beneficiary can make interior a organize utilizing the BB84 quantum key distribution convention.

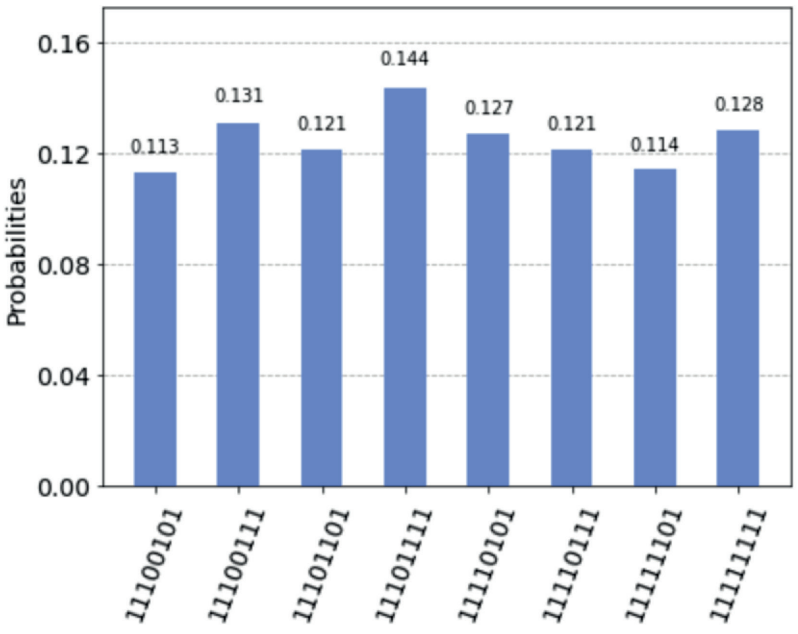

Figure 4. Realization result of BB84

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 10, JUNE 2022

Fig. 5 shows us the dispersed probability between the keys that a sender and collector can deliver interior a orchestrate utilizing the B92 quantum key distribution convention.

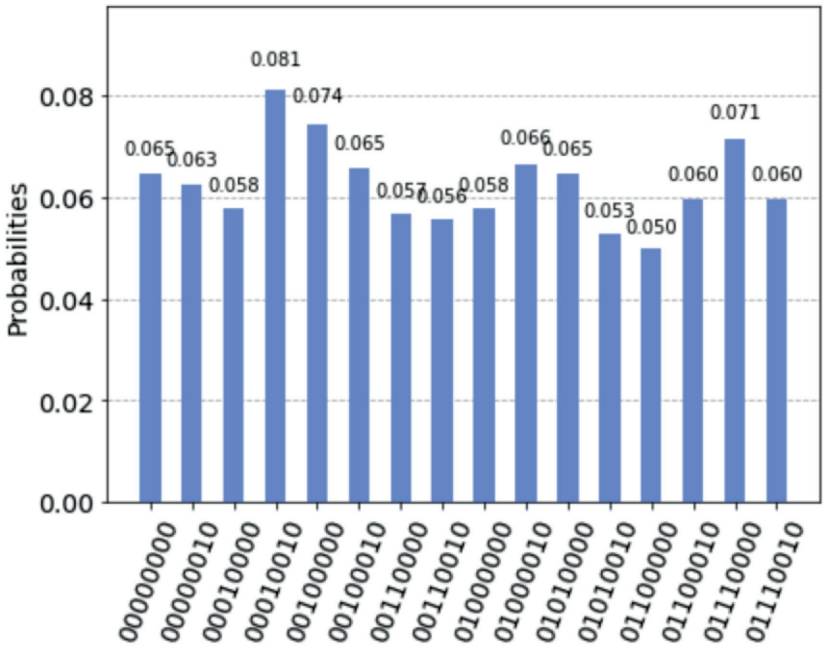

Figure 5. Realization result of B92

Fig. 6 shows us the dispersed probability between the keys that a sender and collector can create interior a organize utilizing the E91 quantum key distribution convention.

.

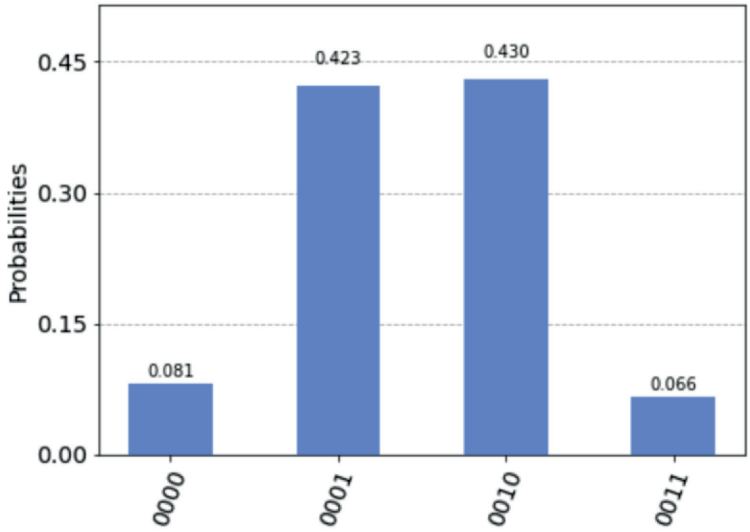

Figure 6. Realization result of E91

It needs to be known that the number of keys made in the B92 convention changes from the number of keys made in BB84. Which appears to be the productive alteration of the BB84 convention to B92. Since with a huge number of keys it'll be troublesome for an interceptor to select up a key, and due to such a sweeping changeability inside the state of qubits in the midst of key course of action, it'll be troublesome to spy and captured the values of a qubit without destroying its state.

DOI: 10.37943/QRKJ7456

Conclusion

In conclusion, we are ready to say that cryptography has been encountering a period of change over the past 30 long times. Within the occasion that earlier cryptography depended on the soundness of the laws of number juggling, at that point, with the appearance of an advanced sort of calculation, such as quantum computing, everything began to change essentially. By and by, the guidelines, speculations, and laws laid down by the originators of quantum mechanics are utilized to basically actualize the foremost columns of cryptography, such as protection, insightfulness, and openness. This work was committed to the use of one of these benchmarks in cryptography. The Heisenberg Instability Run the show can be a periodically utilized run the show in quantum key spread that's still in utilize these days. The first well-known conventions working on this rule are BB84, B92, and E91, which were purified in this work. In this work, the utilization and portrayal of these conventions were outlined, where the results showed the probabilities of making a certain key in both conventions. These usages show up in detail and clearly the utilize of the Heisenberg instability run the show by both quantum key dispersion conventions, utilizing the Hadamard door, which drives the qubits into a superposition, in this way ensuring a modification inside the polarization of the qubit in the midst of its perusing. The utilization indicated in the paper may well be an extraordinary outline for examining the shapes of these conventions. Other than that, these utilizations do not utilize an expansive number of qubits and operations on them to induce an extend of created key comes approximately, which decreases the working time and the number of operations performed by a quantum computer. The preeminent predominant conventions working on this run the show are BB84, B92, E91, which were presented in this work. In this work, the execution and depiction of these conventions were outlined, where the comes almost showed up us the probabilities of creating a certain key in both conventions. It got to be celebrated that the B92 convention may be a change of the BB84 convention. The triumph of the change can be considered a broader division of the key period.

References

1. Kronberg D., Ozhigov Y., Chernyavskyi A. (2006) *Kvantovaya kriptographiya [Quantum Cryptography]*. MSU named after M.V.Lomonosov - Moscow, p. 23-40.
2. Vyalyy M. (2011). *Kvantovyye algoritmy: vozmozhnosti i ogranicheniya [Quantum Algorithms: Possibilities and Limitations]*. St. Petersburg. https://storage.yandexcloud.net/lms-vault/private/2/courses/2011-spring/spb-quantumalgorithms/materials/20110403_quantum_algorithms_vyali_lecture_notes.pdf
3. Postulates of quantum theory. VSU, (2012). http://www.rec.vsu.ru/rus/ecourse/quantcomp/sem2.pdf
4. Bennett, C.H., Bessette, F., Brassard, G. et al. (1992). Experimental quantum cryptography. *J. Cryptology*, *5*, 3–28. https://doi.org/10.1007/BF00191318
5. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, *74*(1), 145-195. https://doi.org/10.1103/RevModPhys.74.145
6. Baumeyster D. (2002) Fizika kvantovoy informatsii [Physics of quantum information]. Postmarket Moscow. -376 p.
7. Bechmann-Pasquinucci, H. (2006). Eavesdropping without quantum memory. *Physical Review A*, *73*, 44-305. Retrievedfrom The Heat Is Online website: https://doi.org/10.1103/PhysRevA.73.044305
8. Warke A., Behera B. K., Panigrahi P. K. Experimental realization of three quantum key distribution protocols //Quantum Information Processing. – 2020. – Т. 19. – №. 11. – С. 1-15. https://doi.org/10.1007/s11128-020-02914-z
9. 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. (2019). «Experimental investigation of

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 10, JUNE 2022

quantum key distribution over a water channel,» *Appl. Opt.,* 58, 3902-3907. https://doi.org/10.1364/AO.58.003902
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. (13 May 2022). Experimental Side-Channel-Secure Quantum Key Distribution. *Phys. Rev. Lett.*, 128, 190503
11. Bennet C. (1992) Quantum Cryptography using any Two Nonorthogonal States. *Phys.Rev.Lett.,* 68, 3121. https://doi.org/10.1103/PhysRevLett.68.3121
12. IBM Quantum Composer and the IBM Quantum Lab. https://quantum-computing.ibm.com/
13. Dhoha A. L. M. et al. *Quantum cryptography on IBM QX*. 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS). – IEEE, 2019. – C. 1-6. https://doi.org/10.1109/cais.2019.8769567
14. Helstrom, C.W. (1969). Quantum detection and estimation theory. *J Stat Phys* 1**,** 231–252. https://doi.org/10.1007/BF01007479
15. Nurhadi A. I., Syambas N. R. *Quantum key distribution (QKD) protocols: A survey*. 2018 4th International Conference on Wireless and Telematics (ICWT). – IEEE, 2018. – C. 1-5. https://doi.org/10.1109/icwt.2018.8527822