IRSTI 47.35.01

N. Abdinurova[1], Y. Mukhamed[2], D. Demeuov[3]
[1,2,3]Suleyman Demirel University, Kaskelen, Kazakhstan

COMPARATIVE ANALYSIS OF CLASSICAL MESSAGE FLOW AND INTEGRATION OF QUANTUM TECHNOLOGIES INTO MESSAGE TRANSMISSION USING QISKIT LIBRARY

Abstract. The issue of secure connectivity is becoming increasingly common these days. Practically all encryption methods can be hacked, prompting the development of a data transport that is impenetrable. This scientific paper discussed the way of classic transmission of information and integration of quantum technologies into this network in order to increase the safety of the channel. This paper includes information about work done on research, such as learning principles of quantum cryptography technologies, basic logical gates and key terms such as superposition, entanglement and teleportation. Qubits are formed and exchanged between 2 parts of the Local Area Network (LAN) using Qiskit library. 2 protocols of data transmission: classic and quantum have been analyzed and compared.

Keywords: Quantum technologies, Qubit, Quantum gates, Qiskit, Data Transmission.

***

Аңдатпа. Қазіргі уақытта қауіпсіз қосылу мәселесі күнделікті өмірде жиі кездеседі. Шифрлаудың барлық дерлік әдістерін бұзуға болады, бұл деректердің берілмеуіне әкеледі. Бұл ғылыми мақалада арнаның қауіпсіздігін арттыру мақсатында ақпаратты классикалық түрде беру әдісі және кванттық технологияны осы желіге біріктіру талқыланды. Бұл мақалада кванттық криптография технологиясының принциптері, негізгі логикалық элементтері мен терминдері: суперпозиция, түйісу және телепортация сияқты негізгі ұғымдарын зерттеу жұмыстары туралы ақпарат қамтылған. Qiskit кітапханасын қолдана отырып, кубиттер жергілікті желінің (LAN) 2 бөлігі арасында қалыптасады және алмасады. Деректерді берудің 2 протоколы талданды және салыстырылды: классикалық және кванттық.

Түйін сөздер: Кванттықтехнологиялар, Кубит, кванттыққақпа, Qiskit, деректасымалдау.

***

Аннотация. В наши дни проблема безопасного подключения становится все более распространенной. Практически все методы

шифрования могут быть взломаны, что приводит к разработке непроницаемой передачи данных. В этой научной статье обсуждался способ классической передачи информации и интеграция квантовых технологий в эту сеть с целью повышения безопасности канала. Эта статья включает информацию о проделанной работе по исследованиям, таким как изучение принципов технологий квантовой криптографии, основных логических элементов и ключевых терминов, таких как суперпозиция, запутанность и телепортация. Кубиты формируются и обмениваются между 2 частями локальной сети (LAN) с использованием библиотеки Qiskit. Были проанализированы и сравнены 2 протокола передачи данных: классический и квантовый.

Ключевые слова: Квантовые технологии, Кубит, Квантовые ворота, Qiskit, Передача данных

I. Introduction

The main task of information security is to ensure that the transmitted data, including message or login/password pairs are not able to be decrypted even in case of eavesdropping attack. To solve this problem, scientists have created many algorithms for cryptography. Since the creation of the first encryption algorithm has passed about a century, today, due to the evolution of the latest technology, they are not secure enough. Our world is not made up from zeros and ones, it is composed of quanta. Scientists in the early twentieth century realized that physical interactions cannot be divided into arbitrarily small units; rather, they have a physical "minimum size" – the quantum [1].

The 1935 paper by Einstein, Podolsky and Rosen on the completeness of quantum mechanics [2], flourished in the 1980 s with the theoretical proposals on quantum computation (Feynman [3] and Deutsch [4]) and on quantum cryptography (Bennett and Brassard [5]). Quantum Image Processing (QIP) has great potential for practical applications with recent breakthroughs in physical concepts, material sciences, and in electrical and photonic engineering techniques.

The question is if our world is a quantum world we must be able to use quantum systems and understand our world and organize it better. Now, this is what quantum technologies are about. If we can discover tools that work based on quantum rules we might discover relations that are hidden from us.

As we already know conventional or classical computers are built from billions of transistors which can be turned on and off to represent a value of one or zero. Thus, traditional computers can now store and analyze data using binary numbers or bits. Quantum computers (QC), on the other hand, work on quantum bits, also known as qubits, which may be represented by superconducting electric circuits. At the same moment, qubits can reside in more than one state or superposition. This permits a qubit to take on the value of one, zero, or both of these numbers at the same point on schedule. As well as expecting

superpositionscan become ensnared which is a crucial quantum mechanical feature in which the condition of one qubits relies upon the condition of another. Making and controlling qubits is exceptionally hard without a doubt. A large number of the present trial quantum processors exploit quantum phenomena that happen in superconducting materials and thus should be cooled, more precisely, around 272 degrees celsius below zero. Figure 1 shows the application areas of QC [2].

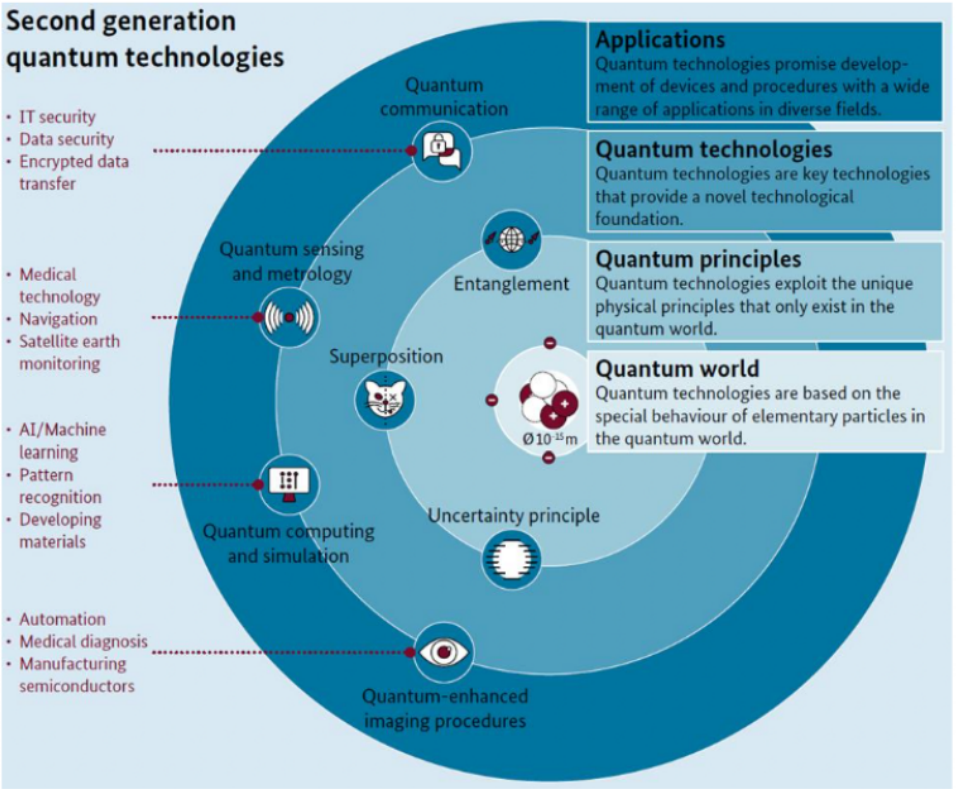

Fig. 1. Quantum applications.

II. Aim and objectives of research

Aim of this research is to develop the system known as Secure Communication based on Quantum Cryptography (SECOQC), discover quantum technologies field for information security and scrutinize several ways of using quantum technologies in order to enhance secure communication. Main objective is to determine methods and models for quantum cryptography usage in telecommunication [6].

III. Theoretical framework. (Background knowledge)

A. Photon Polarization and Quantum Key Distribution

In the early 1980s, research into cryptography algorithms and their power became grounded and well known, and the attention shifted to developing methods to break algorithms - crypt analysis. All techniques may be classified

as symmetric or asymmetric [7] depending on the number of keys utilized for encryption. In symmetric codes the plain message is encoded and decoded utilizing a similar key, but in asymmetric ciphers, a public key is used to encrypt the message and a private key known only to the recipient is used to decode the message. The most extensively utilized and researched aspect of quantum technology is quantum key distribution. The technique for exchanging keys based on qubits was first presented in 1984. It is beyond the realm of possibilities to expect to make an ideal duplicate of an obscure quantum state [8], in light of the fact that all things considered will be obliterated by snoop. Maybe the user would recollect the Heisenberg vulnerability standard: which states that when a particle's precise position is measured, all data about its energy is lost, as well as the other way around. Wiesner's thought was created by Charles Bennett and Gilles Brassard in 1984 in a more reasonable structure: photon quantum states travelling across an optical channel have presently encrypted a key [9]. We should perceive how the BB84 [10] convention can send a secret key across an open channel. Alice and Bob are names commonly used as conventions for interacting agents or archetypal symbols in fields such as cryptography, computer security, and physics [17]. According to Alice's work description, it appears to be like this, each photon is prepared in one of four linear polarizations: horizontal, vertical that having a place with the horizontal-vertical basis, or one of the two 45° diagonal ones that having a place with the diagonal basis [16].

It's accepted that every basis has one polarization that addresses bit 0 and the other polarization that addresses bit 1. Therefore, Alice picks the basis and bit value for each photon at random. While, Bob attempts to gauge the polarization of every photon by picking a measurement basis at random from horizontal-vertical and diagonal. A birefringent prism isolating the approaching photons into orthogonal polarization, trailed by a couple of single photon detectors, might represent Bob's estimation device for each basis. In this process we are able to measure polarization once since the photon is obliterated during the measurement procedure. Consequently, Bob has just one effort to gauge polarization. After the results obtained,

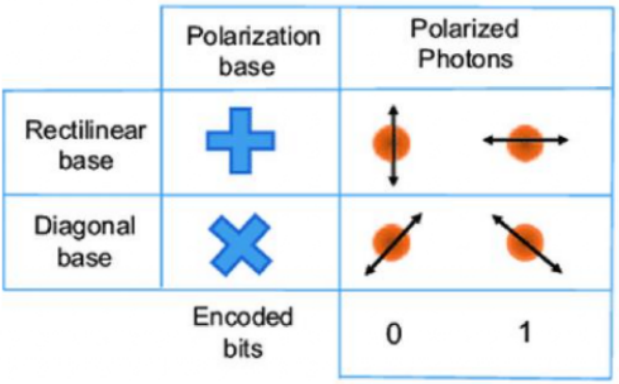

Fig. 2. Photon Polarization

where a specific number of photons has been sent, Alice and Bob inform each other. They do it through a regular correspondence channel, as by means of a web association, and freely look at the transmission and location bases for every photon (except not the bit values). In around a large portion of the cases Bob has ended up identifying the photon not in the basis in which it was transmitted. These bits are removed from the key since his detection result is irregular and uncorrelated to Alice in these circumstances. Bob has recognized the photon on the identical basis in which it was transmitted by Alice in the leftover portion of the occurrences. In these circumstances, Bob receives the similar bit value as Alice, and the bits combine to produce a secret key that Alice and Bob now share.

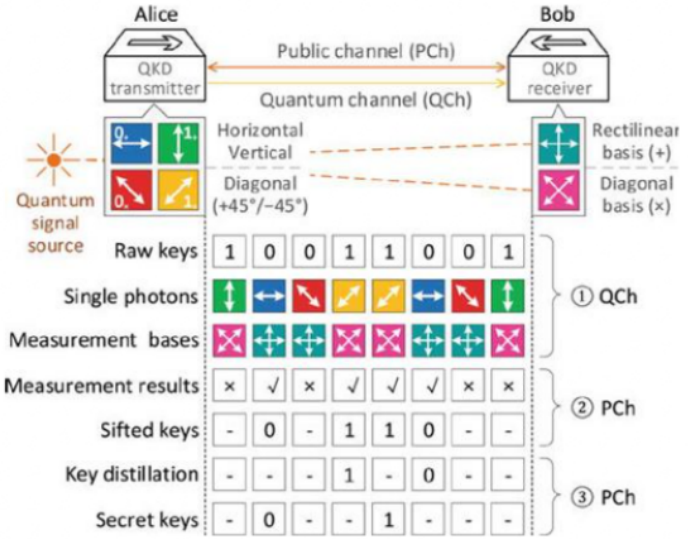

Fig. 3. Quantum Key Distribution

B. Quantum gates

Like in traditional frameworks, there are additionally a few kinds of entryways in quantum frameworks moreover. However, in contrast to conventional gates, such as (NOT), which are reversible and irreversible gates like (OR, AND), quantum entryways cannot be irreversible on the grounds that the association of subatomic particles should be even on schedule.

PAULI Gates/Matrices

Pauli matrices, which are 2x2 matrices, are used to define three normal single-qubit gates analytically. A single quantum bit can be passed through these gates (a 2x1 column vector). The Pauli matrices are written as follows: Pauli-X is a traditional NOT gate.

Pauli-Z $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Pauli-Y $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

Hadamard gate

Because of its capacity to deposit qubits in a superposition, the Hadamard gate [3] is a significant quantum gate in quantum circuits. The Hadamard transformation, also known as the Hadamard gate, is a one-qubit operation that turns any basis state into an equal superposition of both basis states in quantum information processing. In other words, assessing each base state has an equal chance of happening. A Hadamard gate can be stated numerically as follows:

$$\begin{bmatrix} \frac{1}{\sqrt{(2)}} & \frac{1}{\sqrt{(2)}} \\ \frac{1}{\sqrt{(2)}} & -\frac{1}{\sqrt{(2)}} \end{bmatrix}$$

CNOT Gate

The controlled NOT gate, abbreviated as CNOT, is a reversible gate. With two inputs, this gate produces two outputs. The control bit and the target bit are the two sections of a CNOT gate that must be understood. The control bit (top) is represented by a solid dot, while the target bit (bottom) is represented by the exclusive-or operator symbol (XOR). The target bit will remain intact if the control bit input is a $|0\rangle$. The target bit, on the other hand, will flip if the control bit is a $|1\rangle$. Matrix of CNOT gates:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

IV. Literature review

The authors in [5] presented an encryption schema using third part for decryption and matching messages from both sides and avoided using one time

pad techniques explaining that it was impossible to resist eavesdropping attack. Pauli-Y gate, Fredkin gate and Hadamard gates have been implemented in order to enhance the security of the encryption algorithm. The primary objective of this scheme is generating a digital signature using quantum technologies. A digital signature [12] is considered an authentication mechanism that allows the sender of the message to add a code that serves as a signature. Quack - quantum MATLAB [13] simulator, have been used for simulation of this work. Authors could encrypt, decrypt, match, and send the Quantum data among all parties of communication. The third party also was able to check and match the messages received from Bob and Alice.

Quantum technologies are playing an important role in our daily life and work. We are all using quantum technologies. Computers, cameras, sensors, data networks and the majority of medical imaging techniques could not have been achieved without using principles of quantum physics [14]. The laser is an excellent example of this. Starting from a purely scientific phenomenon, institutes and enterprises have developed a device that is used today in research, for manufacturing machinery and vehicles, 3D printing, measurement technology, in communications and all kinds of everyday devices. We used to work with quantum indirectly but now we are moving forward and working with them directly and controlling them. We can simply claim that we are on the second generation of quantum technologies that we could improve different areas of quantum technologies with higher precision. Building higher-performance satellites, computers measuring devices, data communication security increase the possibilities of a higher growth on the economy and society, as well as being extremely relevant to security policy. Big companies have already started to work harder and invest more. For example: in China, quantum technologies are very well financed and have strong political support. The world's first satellite using quantum key distribution (QKD) in 2016 is drawn a lot of attention. USA, quantum technology research and space applications in the USA, Japan, Singapore and Canada and UK are strongly supporting institutes and enterprises into the development of quantum computers and applications. Its been 35 years that IBM is working on quantum computers and in 2016 they launched a website called "IBM Q Experience" [15] that made a 5 qubit quantum computer publicly available over the Internet. IBM offers an open source quantum computing software framework called Qiskit [15]. Google and Microsoft, ALibaba, and Intel are also working hard to make quantum computing a reality. A logic gate, whether quantum or classical, is any physical system or structure that takes a set of binary inputs (whether 0s and 1s,) and returns a single binary output by using the Boolean function. And then they are combined into circuits, and the circuits into Central Processing Units (CPUs) or other computational components. As we know Classical gates operate on classical bits and quantum gates are based on quantum bits (qubits).

V. Methods and Materials

After learning ways of combining quantum technologies with classical ciphering systems, it was decided to create simple topology, try to send some piece of information first via classic channel, then using quantum methods, more precisely, using Qiskit library methods. Qiskit supports python 3.5 or later. Installing anaconda (Jupyter) is recommended. Windows 7, macOS 10 and Ubuntu 16.04 or later versions of them are tested and supported by Qiskit. Simplest way to use Qiskit in anaconda is to use the conda command and create our environment. Next we need to install Qiskit packages which include Terra, Aer, Ignis, and Aqua.

With Qiskit 0.13.0 we need pip 19 or newer to install Qiskit from a precompiled binary on linux. If you don't have pip 19 you can run pip install -U pip to upgrade it. Without pip 19 or newer this command will install Qiskitaer from source distribution. After installing the package correctly we should be able to see the active packages using the conda list command. There are some visualization functions available in Qiskit that we can use by installing optional dependencies by the following command pip install Qiskit-terra[visualization]. After verifying the package that we want to use we should import them into our environment. Note that IBM offers real quantum computers that we can use on IBM Q Experience by creating an account. After that we will have access to a token that we can use to enter the Qiskit environment.

VI. Tools and Platforms of Quantum Engineering (QE)

1) QISKIT - Qiskit is an open-source quantum computing software development framework for leveraging today's quantum processors in research, education, and business.

Note: If you are not comfortable with Qiskit you required the following;

2) Python (Anaconda is recommended), Jupyter notebook, Matlab, Pandas, Matplot;

VII. Data and Results

After comparative analysis the researchers made a conclusion with these results:

1) Programming skills are not considered as one of the obstacles anymore, Qiskit creates the source code automatically. It means that anyone can write regular python code and Qiskit will generate quantum circuits depending on this code.

2) Compared with Matlab it doesn't need or required high level of understanding of principles of quantum systems or predictions of the results. As it was stated above we create quantum circuits by just calling the functions from Qiskit Python library.

3) It doesn't need any specific hardware properties for running and checking quantum systems. Because we can send our circuits to remote IBM real quantum computers and get results from them.

As it is shown below in the Figure 4 we can see that the researchers used gates such Hadamart, CNOT and Z. These gates are located in the circuits. These circuits convert classical bits to qubits and vice versa. For better understanding,

we have qubit 1 (q[1]) and using gates we convert it to classical bits. Then, we receive those classical bits and apply gates to qubit 2 (q[2]) depending on state on classical bits. That is how we get the simple teleportation. The Figures 5 and 6 show the results of this experiment. This teleportation is the transfer of the quantum state of a particle from one place to another.

Fig. 4. Quantum Circuit

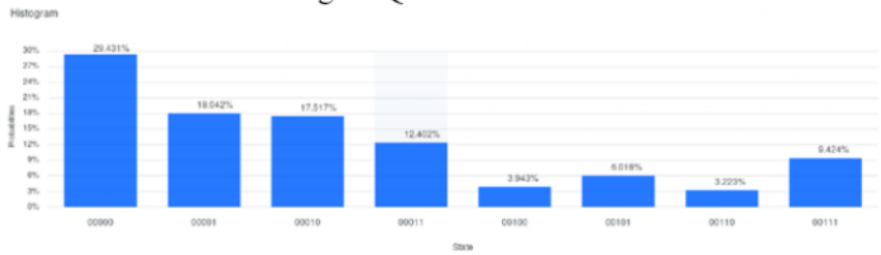

Fig. 5. Result 2.03.2019

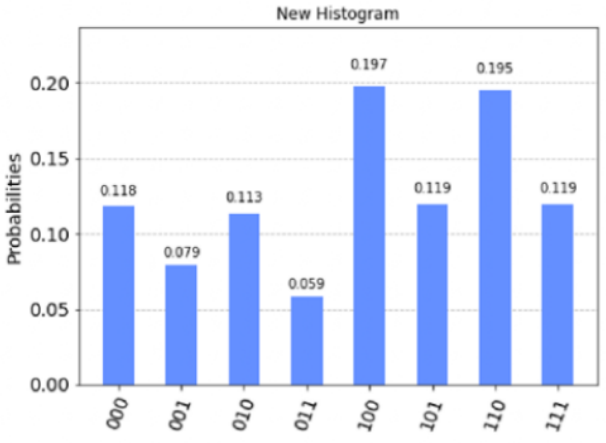

Fig. 6. Result 2.03.2019

VIII. Discussion

As it was already described above, the results showed that teleportation of qubits is possible on practical basis. It means that in the future we can develop this technology to send and receive more data using quantum computers. After comparative analysis the researchers have noticed and pointed out given limitations:

1. The main limitation of this work/experiment is that there are only few numbers of IBM quantum computers all over the world and the results cannot be received fast. Because lots of people try to execute the circuits and got their

results from quantum computers there are queues. While waiting the results from IBM quantum computers because of these queues the loss of the relevance and validity is possible.

2. There is lack of research work on this topic. Despite that Qiskit has its own tutorial videos on how to use Qiskit for creating quantum circuits, it is still hard to understand and develop this topic.

IX. Conclusion

In this paper we have analysed the tools and platforms for quantum systems to make and develop quantum systems elements, after analysing recent researches and solutions for quantum systems. During the research, the experiment was performed in different time periods, and as it can be discerned from the result of the histogram - both outcomes have considerable differences in the values of their probabilities.

We have defined some advantages of building quantum circuits into quantum composers. Indeed our recommendation is to use Qiskit to test and make quantum algorithms, systems and elements. The reason for that is because it is a very popular and cloud based platform that includes all the packages and requirements for realizations and demonstrations of principles of quantum.

References

1 Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical review letters, 67(6), 661.

2 BMBF "Quantum technologies – from basic research to market", IEEE International Conference on Network and Information Systems for Computers, pp. 302-305, China, 2016.

3 Pathak, A. (2018). Experimental quantum mechanics in the classroom: Testing basic ideas of quantum mechanics and quantum computing using IBM quantum computer. arXiv preprint arXiv:1805.06275.

4 Salunke, T. P., &Bharkad, S. D. (2017, July). Power point control using hand gesture recognition based on hog feature extraction and K-NN classification. In 2017 International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1151-1155). IEEE.

5 Abhijith, J., Adedoyin, A., Ambrosiano, J., Anisimov, P., Ba¨rtschi, A., Casper, W., ... Lokhov, A. Y. (2018). Quantum algorithm implementations for beginners. arXiv e-prints, arXiv-1804.

6 Hand-Reader-Dataset, GitHub repository. [Online]. Available: https://github.com/tofighi/Hand-Reader-Dataset

7 Bernal-Garc´ıa, D. N., Rodr´ıguez, B. A., Vinck-Posada, H. (2019). Multiple-scale analysis of open quantum systems. Physics Letters A, 383(15), 1698-1710.

8 Singh, R. K., Ratnaparkhi, P., Behera, B. K., Panigrahi, P. K. (2018). Getting Started With Quantum Computation: Experiencing The Quantum Experience. RESONANCE, 1.

9 Guo, Y., Han, S., Li, Y., Zhang, C., Bai, Y. (2018). K-Nearest Neigh- bor combined with guided filter for hyperspectral image classification. Procedia Computer Science, 129, 159-165.
10 Shor, P. W., &Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. Physical review letters, 85(2), 441.Genuer, R., Poggi, J. M., Tuleau-Malot, C., Villa-Vialaneix, N. (2017). Random forests for big data. Big Data Research, 9, 28-46.
11 Xi-Han, L., Chun-Yan, L., Fu-Guo, D., Ping, Z., Yu-Jie, L., Hong-Yu, Z. (2007). Quantum secure direct communication with quantum encryption based on pure entangled states. Chinese Physics, 16(8), 2149.
12 Kuppam, S. (2016). Modelling and Analysis of Quantum Key Distribution Protocols, BB84 and B92, in Communicating Quantum Processes (CQP) language and Analysing in PRISM. arXiv preprint arXiv:1612.03706.
13 Bouwmeester, D., Zeilinger, A. (2000). The physics of quantum information: basic concepts. In The physics of quantum information (pp. 1-14). Springer, Berlin, Heidelberg.
14 Cross, A. (2018). The IBM Q experience and QISKit open-source quantum computing software. In APS March Meeting Abstracts (Vol. 2018, pp. L58-003).
15 Bennett, C. H., Brassard, G. (2020). Quantum cryptography: Public key distribution and coin tossing. arXiv preprint arXiv:2003.06557.
16 Rivest, R. L., Shamir, A., Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.