ECAI 2017 - International Conference – 9th Edition
Electronics, Computers and Artificial Intelligence
29 June -01 July, 2017, Targoviste, ROMÂNIA

Hybrid Scheme for Secure Communications Using Quantum and Classical Mechanisms

Mihail-Iulian Pleşa
Computer Science Dept.
Military Technical Academy
Bucharest, Romania
Email: yulyus.m@gmail.com

***Abstract* – The paper proposes a new scheme for secure data transmission based on a hybrid technology quantum and classical. Our scheme addresses two important problems: the confidentiality and integrity of data. The scheme is based on quantum teleportation circuit but the data transmission is accomplished through classical channels. Several experiments were conducted using the new IBM Q platform.**

Keywords – quantum-based security; quantum teleportation; data confidentiality; data integrity;

I. INTRODUCTION

In 1982 the physicist Richard Feynman has proposed for the first time the idea of a computer based on quantum mechanics [3]. Although at the beginning the idea was considered pure theoretical, in 1994 Peter Shor propose a factorization algorithm for such a device [4]. Without any doubt the classical computers have revolutionized the world but certain problems remains too much complicated for them. A simple caffeine molecule cannot be comprehended of all the computers in the world.

Nowadays, 35 years later, the original idea of quantum computers begins to be a reality. Today IBM is trying to build universal quantum computers for business, but also for science. For instance, researchers are trying to build molecules for new materials using quantum processors [5]. Even with a small numbers of 8 qubits it is possible to efficiently simulate chemistry on a quantum computer. The most efficient IBM universal quantum computer has 17 qubits and 16 of them are available to the public through IBM cloud [6].

In May 2016, IBM has released a new cloud based platform through which the entire Internet community gained access to a real quantum processor [16]. The goal of IBM Q is to produce a commercially available universal quantum computer. Although, at this point there are technologies for searching and interpreting massive data such as IBM Watson AI, the increasing amount of data will soon overcome the current technologies. In this case, searching for new ways of approaching the problem becomes necessary. IBM Q is a community that tries to find out new algorithms and techniques for programming quantum computers. The huge effort of IBM demonstrates that quantum computers are a real and available technology. Google has also invested in quantum technologies. The researchers from D-Wave claim they will build a quantum computer which dispose by a lattice of 2000 qubits used for solving optimization problems [17].

Cloud computing is a technology that is used more and more in nowadays. The model based on cloud computing provides considerable advantages of cost-quality regarding the access to a range of IT services. It can be used to backup data, create new applications, hosting websites etc. There are many benefits among those the most important are reducing costs by eliminating the necessity of buying hardware, speed and global scale. Outsourcing data processing in the cloud in good security conditions offers the use of cloud services a major advantage. Cloud services can be accessed anywhere where a network connection exists [12]. Anyway, the cloud services involve data transmission at distance. The transmitted data can be personal, financial, or any other data type but all the transmissions must be protected. Our scheme proposes a new way of ensuring data confidentiality and integrity using OTP and key distribution through quantum teleportation and can be used in a cloud computing model. By addressing those two important problems of data transmission, the cloud services may become an obvious application of our scheme.

The paper contribution is twofold. Firstly, we propose a new quantum-based hybrid scheme for data secure communication. The scheme addresses two important cryptographic problems regarding the data confidentiality and data integrity. In our scheme the quantum teleportation circuit determines a perfect security in the transmission of data while ensuring also their integrity. Although the scheme could be fully implemented using quantum mechanisms, it is known that for current technological level the conservation of the qubits is a problem, thus we consider also the integration of classical technologies for effective data transmission. Secondly, we prove the theoretical assumptions by conducting several experiments on the very new IBM Q quantum platform.

The rest of the paper is organized as follows. Section 2 contains an introduction part regarding the quantum topic with focus on its usage in cryptography. In Section 3 is presented the main workflow of the proposed scheme. There is also detailed the quantum teleportation circuit that has been used in our scheme to transfer the key and data between the communicating parties. Section 4 includes the details of our scheme

978-1-5090-6458-8/17/$31.00 ©2017 IEEE

with key generation and data transfer using quantum circuits. Finally, the section 5 outlines our conclusions.

II. QUATUM IN CRYPTOGRAPHY

With the development of technology appears the need of data confidentiality and integrity thus the cryptography knew a strong advance. Since the RSA appearance in 1977 until the establishment of the new AES standard in 1998 was discovered a large series of cryptographic algorithms. Nowadays, whether we talk about the cryptography with symmetric or asymmetric keys, a common problem of those two schemes is their vulnerability to the brute force attacks powered by the new quantum computers. Currently there are two major ways by which quantum computing can be involved in the cryptography field. First of all, the quantum cryptography is a new direction in the field by using physical properties of quantum systems. For example the quantum systems have the property of being in superposition of ground states. This can be used to hide information. Quantum Key Distribution (QKD) protocols use this property to hide the bits of the key that is going to be distributed [7].

One example of QKD is the following. Let's suppose Alice that wants to establish a secure communication with Bob using OTP. Alice begins sending to Bob photons polarized in a random direction (90 or 45 degrees). Bob will randomly choose a polarization cube to measure Alice's photons. If the cube is oriented in the same direction as the photon then the measurement will be successful, but if the cube is in the wrong direction then the original photon will be destroyed. If the photon has a 90 degrees polarization and the cube is orientated on 45 degrees, then the photon which comes out from the cube will have a polarization of +45 with a 50% probability and a polarization of -45 with 50% probability. Bob transmits to Alice what photons have been measured successfully without transmitting to her the photons polarization. Alice will choose the polarization of the photons as the key for OTP. If the photon has a polarization of +90 then this case will be decoded as 0 or if the photon has polarization of -90 then it will be decoded as 1. An attacker Eve will have 50% chances to choose the same polarization cube as Bob did, and even if she does so then the message sent by Bob to Alice has no meaning to Eve because Bob transmits only what photons were measured successfully and not their explicit values [13][14].

Once a system is in a superposition of its ground states any measurement made on that system will put the system in one of the ground states with a certain probability. Another interesting theorem in quantum field is "no-cloning theorem" [8]. This proves that quantum information (such a qubit) cannot be copied without knowledge about its state. This result is with certainty most useful for cryptography, because it can be used at least in theory to guarantee data integrity [9]. Although there are many ways in which quantum properties provide cryptographic services [7][9], quantum algorithms can be used in brute force attacks on current quantum primitives. For instance, RSA which is one of the most used cryptographic schemes is based on the hard problem of big numbers factorization. The complexity of numbers factorization is sub-exponential [10] on classical computers but on a quantum computer this become polynomial by applying Shor algorithm [4]. The symmetric key algorithms (like AES) become also vulnerable against of quantum computers. The algorithm proposed by Grover in [11] offers an optimal way of searching through an unsorted database in square root complexity time. Using this, the security for breaking the 128 variant of AES is reduced to 2^{64} which give a security complexity not acceptable even for our ordinary computers.

III. THE GENERAL OVERVIEW

In this section we present a general overview of the proposed scheme. Let's illustrate the scheme for Alice and Bob that want to transmit data to each other using a mechanism that must guarantee the confidentiality and integrity of data. The overview of the proposed scheme is illustrated in Fig. 1. Let's take the case when Alice wants to send an n-bit message to Bob, then the scheme involves the following steps:

1) Alice generates the encryption key using Hadamard gate applied to a qubit initialized on 0.
2) Alice transmits the encryption key through the teleportation circuit that will involve the transmission of auxiliary bits through classic channels. These bits are essential to the teleportation process.
3) Alice calculates the hash of the auxiliary bits and teleports this through another teleportation circuit, "Hash Teleportation 1".
4) Alice encrypts the data using OTP scheme and transmit them through classical channels.
5) Alice calculates the hash of the encrypted message and sends it through the teleportation circuit "Hash Teleportation 2".
6) Bob receives the auxiliary bits whose hash will compute it and compare it with the hash received through the "Hash Teleportation 1" circuit, thus checking the integrity of auxiliary data.
7) Bob calculates the hash of the encrypted message and verifies that this is the hash received through the teleportation circuit "Hash Teleportation 2", thus verifying the encrypted data integrity.
8) Bob receives the encryption key and decrypts the data.

A. The teleportation circuit

The teleportation circuit requires that both sides to share a pair of EPR qubits. These qubits are in entanglement state. The scheme of the circuit is shown in Fig. 3.

The information stored in the first qubit that is going to be teleported is not instantly transferred to the destination, thus violating the second postulate of relativity. The system state is a superposition given by the states of those three qubits. Initially that is given by the equation (1).

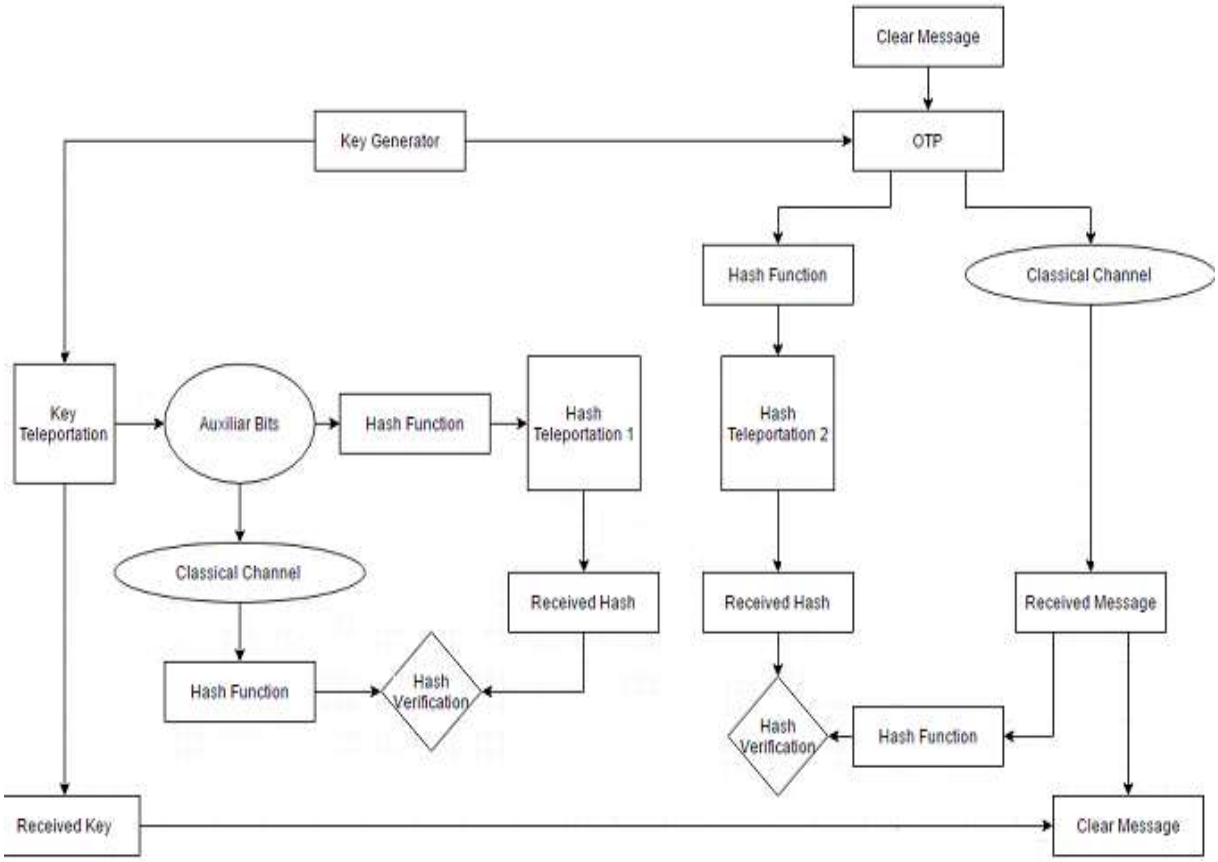

Fig. 1 The general overview of the proposed scheme

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)] \quad (1)$$

Note the EPR pair of qubits. The next state is that described in (2) after the CNOT gate changes the qubit 2.

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)] \quad (2)$$

The CNOT gate prepares the transfer of the amplitudes of probability from the first qubit to the third qubit. After the Hadamard gate is applied it can be observed the transfer of the amplitudes of probability as it is shown in the equation (3). Now, the complex numbers α and β, the amplitudes of the first qubit (the one which is going to be teleported) are the amplitudes for the third qubit.

$$|\psi_2\rangle = \frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)] \quad (3)$$

As can be seen, the system superposition state includes the third qubit as being in several superposition states, all having the probability amplitudes α and β but different signs. By measuring the first two qubits, the system will collapse and the state of the third qubits will be one of the states shown in Fig. 2. The values of the first two qubits after the measurement will determine the state of the third qubit. Depending on the result of the previous measurement it could require to apply some transformations on the teleported qubit to recover the original qubit according to Fig. 2.

$$\mathbf{00} \longmapsto |\psi_3(00)\rangle \equiv \left[\alpha|0\rangle + \beta|1\rangle\right]$$
$$\mathbf{01} \longmapsto |\psi_3(01)\rangle \equiv \left[\alpha|1\rangle + \beta|0\rangle\right]$$
$$\mathbf{10} \longmapsto |\psi_3(10)\rangle \equiv \left[\alpha|0\rangle - \beta|1\rangle\right]$$
$$\mathbf{11} \longmapsto |\psi_3(11)\rangle \equiv \left[\alpha|1\rangle - \beta|0\rangle\right]$$

Fig. 2 States of the third qubit after the system collapse

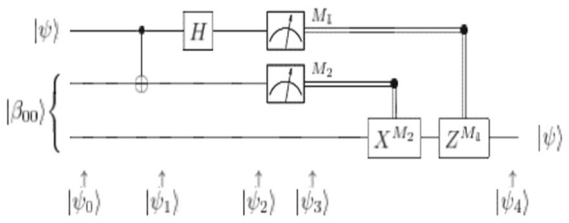

Fig. 3 The theoretical scheme of the quantum teleportation circuit

If the first two qubits have both the value 0 after the measurement, then the third qubit has the information

stored by the first qubit thus the teleportation process was succeed. If the values of the first two qubit are 0 and 1 then the third qubit will be put through an X gate that will change the amplitudes of probability, so the state of the third qubit will be change from $\alpha|1\rangle + \beta|0\rangle$ to $\alpha|0\rangle + \beta|1\rangle$, which is the state of the first qubit. If the first two qubits are 1 and 0 then the third qubit will be put through a Z gate that will change the state of the qubit from $\alpha|0\rangle - \beta|1\rangle$ in the original qubit. In the last case, if the first two qubits are both 1 then the third qubit will be successively put through a Z gate, that will change the state to $\alpha|1\rangle + \beta|0\rangle$, followed by an X gate that recovers the original qubit.

As it was exemplified above, the information in the first qubit is not immediately transferred to the third qubit, but depending on the result of the measurement of the first two qubits, a series of auxiliary transformations applied to the third qubit are needed to recover the information from the first qubit. The transfer of the measurement result of the first two qubits is necessary for the information to be recovered, thus ensuring the integrity of the second principle of relativity.

The correctness of the above equations was demonstrated through an practical implementation of the teleportation circuit using the IBM Q platform [2]. In Fig. 5 is presented the circuit that we implemented.

The square box marks the components that creates an entanglement pair of qubits (the last two qubits) and the oval box marks a series of gates that are going to change the state of the first qubit from $|0\rangle$ to $\sqrt{0.85}|0\rangle + \sqrt{0.15}|1\rangle$ (in order to show that the teleportation circuit is working the state of the qubit that is to be teleported is change to a state different from $|0\rangle$, in this case the state is a rotation around Z axis with 45 degrees as it is exemplified in Fig. 6). This state being chosen for demonstration purposes because the amplitudes α and β are different thus highlighting the process of teleportation. Following the gate sequence shown in Fig. 5, we obtain the results from Fig. 4. As we can see, the practical results are consistent with the theoretical ones from equation (3). For example, according to the equation (3) the amplitude of the ground state$|000\rangle$ is $\frac{\alpha}{2}$. As it can been seen in Fig. 6, α=$\sqrt{0,85}$ so α=0,92 thus the amplitude of the state $|000\rangle$ is 0,46 so the probability that all three qubits are 0 is $0{,}46^2 = 0{,}21$ (theoretical result). In the first column from Fig.4 it can be observed that the probability of the system to be |000> is 0,22.

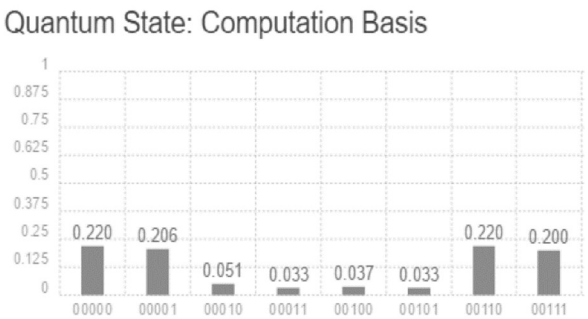

Fig. 4 Results obtained from teleportation experiment

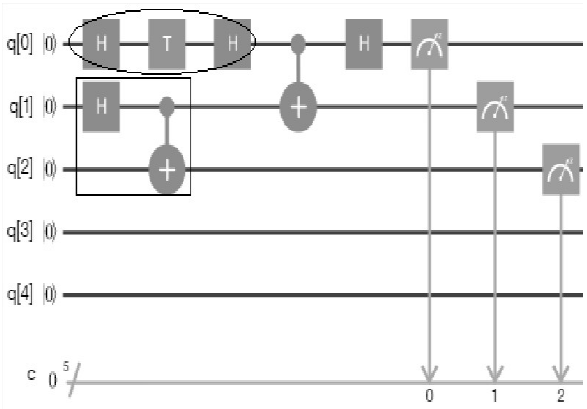

Fig. 5 Real teleportation circuit implemented in IBM Q platform

Gate sequence	Rotation around Z	Probability of 0	Probability of 1
H H	0	1.0	0
H T H	π/4	0.85	0.15
H S H	π/2	0.50	0.50
H S T H	3π/4	0.15	0.85
H Z H	π	0	1

Fig. 6 States obtained applying different sequences of gates

The teleportation circuit was run 1024 by the quantum processor and the three qubits were measured every time thus obtaining the statistical results shown in Fig.4.

IV. KEY TRANSFER AND DATA ENCRYPTION

A. OTP key generation

The key generation process is done using a quantum circuit that guarantees a perfect randomization. The design of the used circuit is presented in Fig. 7. As can be seen the circuit involves putting qubits initially on $|0\rangle$ through the Hadamard gate. According to the definition of the gate, the output will be a superposition of $|1\rangle$ and $|0\rangle$ which means that measuring the qubit after it passed through the gate it will give the value 1 with probability of 50% and 0 with probability of 50%. By applying this procedure repeatedly we can generate perfectly random bits for the key used by OTP. Once generated *n* random bits for key, the data will be encrypted using the OTP. The circuit figured out in Fig. 7 is able to generate random bits using only one qubit. After one single running of this circuit, a truly random bit of the encryption key will be generated. To complete the statistics, we run the circuit for 1024 times in IBM Q, obtaining 0 in 49.6% and 1 in 50.4% of the cases.

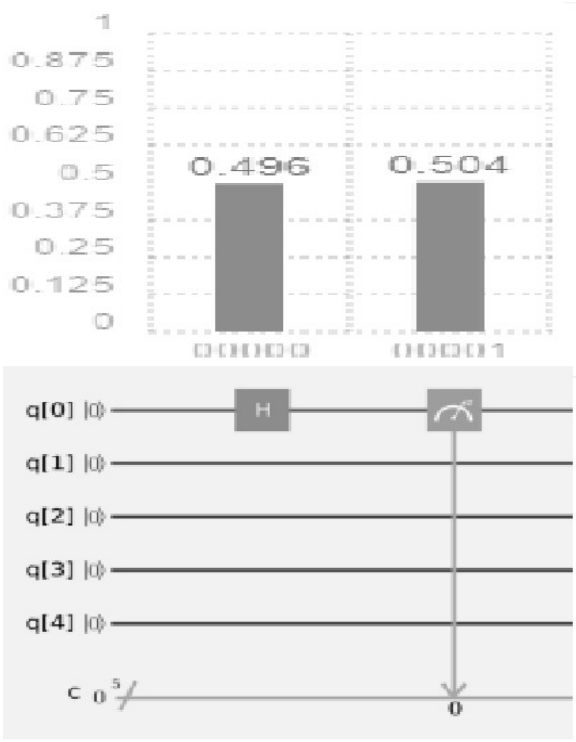

Fig. 7 Quantum-based circuit for randomization. The statistical result on 1024 measurements of the circuit is represented in the top figure and the circuit itself in the bottom figure.

B. Data transfer using the teleportation circuit

As outlined above, in order for the teleportation circuit to work, it is necessary to transmit the result obtained by measuring the first two qubits through some classical channels (referred to as auxiliary bits or auxiliary information) so implicitly it is necessary to transmit the measurement of the first qubit that is to be teleported. If this qubit is in a ground state, the teleportation circuit becomes useless because the information transmitted through classical channels is the only information that characterizes the qubit. If, however, the first qubit would be in a state of superposition $\alpha|0\rangle + \beta|1\rangle$ then what would be transmitted by classical channels would be 0 with the probability of $|\alpha|^2$ or 1 with the probability of $|\beta|^2$ but what is being teleported is the entire state of the qubit, $\alpha|0\rangle + \beta|1\rangle$. From another point of view, it can be said that the information transmitted through classical channels is not correlated with the teleported information. This immediately leads to the idea of using the teleportation mechanism to "hide" information in the form of qubits, thus ensuring confidentiality.

The scheme we propose uses the property of a quantum system to be in a superposition. To transmit the encryption key, a string of *n* qubits is going to be initialized with the values of the bits from the key. Immediately after this stage, each qubit will be put through the Hadamard gate thus becoming a superposition. For example, if a bit from the key has a value of 0, a qubit will be initialized to $|0\rangle$, which after passing through the Hadamard gate will have the state $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. Each of these qubits made from bits of the key will be teleported by Alice to Bob. At destination, after Bob receives the auxiliary information and the teleportation process will be completed, Bob will apply the Hadamard gate to each qubit thus recovering the original bit from the key. For example, if Alice teleports to Bob to the state $|+\rangle$, after Bob applies the Hadamard gate to the qubit, the qubit will change to state 0, recovering the value of the original bit. As mentioned above, the auxiliary information is not correlated with the teleported information. If the qubit that Alice wishes to teleport is in the state $|+\rangle$, when Alice will measure the qubit value, it will find 0 with the probability of $\frac{1}{2}$ and 1 with the same probability (so the value of the qubit after the measurement, that of 0 or 1 is not correlated with the state of the qubit, that of $|+\rangle$) but after transmitting the auxiliary information to Bob, he is able to recover the original bit from the key. This ensures the confidentiality of the transmitted data.

The issue of data integrity is not so obvious. Data integrity must be guaranteed twice. Firstly, it must be guaranteed the integrity of the encrypted message, and, secondly, the integrity of the auxiliary information.

In the first case, if an attacker intercepts and modifies a bit of auxiliary information, its presence may not be detected if Alice continues to use Hadamard gates to create superposition. Let us presume that, for example, Alice sends to Bob the values 00 (the values of the first two qubits after measuring them) and that the state of the teleported qubit is $|+\rangle$. This information, transmitted through classical channels, is intercepted by an attacker who will send Bob the values of 01. When this information reaches Bob, he decides to apply the X gate to the qubit he owns (the third qubit in Fig. 3) in order to reverse the amplitudes of probability of the two ground states as exemplified in section 3.1. The state of the qubit that has been teleported is $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ therefore the amplitudes of the two ground states are equal, $\alpha=\beta=\frac{1}{\sqrt{2}}$. Since Bob received the information 01 from the attacker through classical channels, he will conclude that the state of the qubit is not the original one, $\alpha|0\rangle + \beta|1\rangle$, $\alpha = \beta = \frac{1}{\sqrt{2}}$ but that it is $\alpha|1\rangle + \beta|0\rangle$, $\alpha = \beta = \frac{1}{\sqrt{2}}$ therefore he will apply the X gate but without effect because the amplitudes are equal and in this case $\alpha|0\rangle + \beta|1\rangle = \alpha|1\rangle + \beta|0\rangle$. After he will apply the Hadamard he will obtained the same bit even if the auxiliary information were modified. Thus, the teleportation circuit applied in this way does not ensure integrity of the data.

In the second case, if an attacker intercepts and modifies a bit of encrypted information, the teleportation mechanism cannot ensure the integrity of the data because the information itself is transmitted through classical channels. In order for the teleportation circuit to ensure the integrity of the encrypted information, a hash of those data will be

calculated and it will be teleported. Thus, the data incorruptibility analysis can be restricted to the auxiliary information only.

To ensure data integrity through the teleportation mechanism, the probability amplitudes α and β should not be equal. In this way, each of the states presented in Fig. 2 will be different from the others, and there is no possibility to be obtained from two pair of auxiliary bits the same state of superposition of the teleported qubit. For the probability amplitudes α and β to be different, the application of a single gate (such as the application of the Hadamard gate) to create the superposition state is not sufficient, thus it is required to apply a sequence of gates such as the ones described in Fig. 6. Applying a series of gates is obviously more costly than the application of a single gate, therefore ensuring data integrity through this mechanism is also costly. For example, if a three-gate sequence is chosen to create the superposition, each of these three gates will have to be applied by both Alice and Bob to each of the key qubits. To ensure perfect security, the length of the encryption key is equal to the length of the encrypted text. In this case the data integrity mechanism can become costly if it is applied directly to the message (especially when the message has large dimensions).

Our scheme proposes applying of the hash functions mechanism. In order to reduce the cost of the data integrity mechanism, a hash of the auxiliary bit string and a hash of the encrypted message will be created. The bits from the key will be transmitted through a Hadamard-based teleportation circuit to create the superposition states (mechanism that does not guarantee data integrity). The previously created hashes which will be smaller than the original message (for hashing can be used a function such a SHA2) will be transmitted through a teleportation circuit based on a sequence of gates to create the superposition. The sequence of gates can be any sequence in the table shown in Fig. 6 that creates a superposition with different amplitudes of probability. Assuming an attacker would intercept a pair of auxiliary bits necessary for the teleportation process in which the superposition states have been created by the Hadamard gate, the attacker would be able to modify the pair without being noticed. However, if the attacker intercepts and modifies the auxiliary bits in the teleportation process which is based on the application of a sequence of gates, this can be detected because there is no pair of auxiliary bits leading to the same state superposition of the third qubit in the teleportation process. Thus, any modification of the auxiliary bits transmitted to the hash will not allow the restoration of the initial state of the teleported qubit. In this way, if Bob receives previously modified bits, he will also receive a hash that is different from the original one, which obviously results in a discrepancy between the value of the teleported hash and the initial hash value calculated either from the auxiliary bit values resulted from the teleportation of the key or from the bits of encrypted message. By this mechanism, the costs are reduced because the sequence of gates is only applied in the process of hashes teleportation that obviously have shorter lengths than the original message and ensures the integrity of the auxiliary information required in the teleportation of the key and the integrity of encrypted information.

V. Conclusions

As it has been shown in the previous sections, the proposed hybrid scheme ensures both the confidentiality and the integrity of the data. In terms of disadvantages, one of them is represented by the special conditions for maintaining and transporting a pair of EPR qubits. The experiments were performed on a real quantum processor provided by IBM through the cloud. The current technological conditions do not make it possible to get immediate results with the schema presented because for a 2048 bits message are needed 2048 qubits. Current quantum computers do not have more than 17 quits at the time this paper is written, but the growth rate of quantum processor capacity is impressive, IBM announcing the availability of universal quantum computer with 50 qubits this year [15].

References

[1] Quantum Computation and Quantum Information 10th Anniversary Edition - Isaac Chuang and Michael Nielsen Editura Cambridge University Press.

[2] IBM Q experience, https://quantumexperience.ng.bluemix.net/qx/community.

[3] Simulating Physics with Computers - Richard P. Feynman International Journal of Theoretical Physics, VoL 21, Nos. 6/7, 1982.

[4] Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer – Peter Shor SIAM J.Sci.Statist.Comput. 26 (1997) 1484

[5] https://www.aps.org/publications/apsnews/201705/quantum.cfm

[6] http://www-03.ibm.com/press/us/en/pressrelease/52403.wss

[7] Quantum Cryptography - Richard J. Hughes LA-UR-95-806

[8] Quantum copying: Beyond the no-cloning theorem - V. Buzek, M. Hillery RevTex, 26 pages, to appear in Physical Review A.

[9] http://www.physics.umd.edu/studinfo/courses/Phys402/AnlageSpring09/TheNoCloningTheoremWoottersPhysicsTodayFeb2009p76.pdf.

[10] The Number Field Sieve - Carl Pomerance – Proceedings of Symposia in Applied Mathematics Volume 48 1994.

[11] A fast quantum mechanical algorithm for database search - Lov K. Grover - https://arxiv.org/pdf/quant-ph/9605043.pdf.

[12] https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/.

[13] https://www.sans.org/reading-room/whitepapers/vpns/securing-key-distribution-quantum-cryptography-1448.

[14] Using quantum key distribution for cryptographic purposes: a survey - Romain Alléaume - Theoretical Computer Science, 560 (2014), pp. 62-81.

[15] https://www-03.ibm.com/press/us/en/pressrelease/51740.wss

[16] https://www.wired.com/2016/05/ibm-letting-anyone-play-quantum-computer/

[17] https://www.dwavesys.com/d-wave-two-system