Quantum Cryptography on IBM QX

Dhoha AL-Mubayedh[1], Mashael AL-Khalis[2], Ghadeer AL-Azman[3], Manal AL-Abdali[4], Malak AlFosail[5], Naya Nagy[6]
College of Computer Science and Information Technology
Cyber Security and Digital Forensics
Imam Abdulrahman bin Faisal University
Dammam, Saudi Arabia
2150001651@iau.edu.sa[1], 2150001151@iau.edu.sa[2], 2150006115@iau.edu.sa[3], 2150003246@iau.edu.sa[4], mkaalfosail@iau.edu.sa[5]
nmnagy@iau.edu.sa[6]

***Abstract*— Due to the importance of securing electronic transactions, many cryptographic protocols have been employed, that mainly depend on distributed keys between the intended parties. In classical computers, the security of these protocols depends on the mathematical complexity of the encoding functions and on the length of the key. However, the existing classical algorithms 100% breakable with enough computational power, which can be provided by quantum machines. Moving to quantum computation, the field of security shifts into a new area of cryptographic solutions which is now the field of quantum cryptography. The era of quantum computers is at its beginning. There are few practical implementations and evaluations of quantum protocols. Therefore, the paper defines a well-known quantum key distribution protocol which is BB84 then provides a practical implementation of it on IBM QX software. The practical implementations showed that there were differences between BB84 theoretical expected results and the practical implementation results. Due to this, the paper provides a statistical analysis of the experiments by comparing the standard deviation of the results. Using the BB84 protocol the existence of a third-party eavesdropper can be detected. Thus, calculations of the probability of detecting/not detecting a third-party eavesdropping have been provided. These values are again compared to the theoretical expectation. The calculations showed that with the greater number of qubits, the percentage of detecting eavesdropper will be higher.**

Keywords—quantum, cryptography, quantum key distribution, BB84, quantum bit commitment.

I. INTRODUCTION

Recently, the development of information technologies has influenced the importance to have stronger security measures. In the present, security measures mainly rely on the complex mathematical algorithms to make the encryption key hard for eavesdroppers to break in a short time [1]. While looking to the quantum paradigm with its proprieties, it opens a door for a new world of security since it helps to formulate more securable techniques with less dependency on mathematical complexity [2]. Basically, quantum cryptography is an approach of cryptography that depends on the laws of quantum physics and exploits its properties. Also, quantum cryptography improves security over classical approaches, making it impossible for a classical computer to break the security of a quantum computer. Two basic quantum cryptography primitives are quantum key distribution and quantum bit commitment [3]. For that purpose, various protocols for quantum key distribution and quantum bit commitment have been proposed with some theoretical analysis. The main purpose of this paper is to show practical implementations of some major quantum key distribution protocols and to statistically evaluate their behavior in comparison to the theoretical expectation. Additionally, the probability of detecting/not detecting a third-party trial to sniff the key is calculated.

In the end, the primary objective is to provide outstanding security work that differs from traditional security works by using quantum machines instead of classical computers.

II. PROPLEM STATEMENT

Despite the variety of used encryption techniques, all the existing classical encryption algorithms still pose a concern on how to distribute a secret key. The concern refers to the following actions: the key may be copied or sniffed by another unauthorized party during key generation. This problem shows precisely the importance and the need for a quantum key distribution system, where copying of an unknown quantum state is impossible and reading an unknown state leaves an unmistakable mark on the state of the system where this trial can be detected.

III. METHODOLOGY

In this paper, all the practical implementations have been done using IBM quantum experience (IBM QX). Which is an online based platform that let public users have access to interact with IBM's real quantum processors housed in an IBM research lab using the cloud [4]. IBM QX contains quantum composer which is a tool with a graphical user interface let the user drag and drop quantum gates to operate the qubits. The main purpose of the quantum composer is to allow the development of quantum algorithms or run other experiments [4].

IV. BACKGROUND

A) The Quantum Bit

The quantum bit (qubit), is the basic unit of quantum information. It has a similar concept of the bit in the classical computer, but besides the ability to hold states 0 or 1, it can hold both states at once [5].

B) Quantum bit Principles:

The qubits take advantage of using three principles, which are superposition, entanglement, and non-clonability.

- Superposition

A Superposition principle means that each qubit can be represented by $|0\rangle$, $|1\rangle$ or combination of these two states at the same time. Which means that the state of the qubit is 0 with a probability p, and 1 with probability (1-p).

978-1-7281-0108-8/19/$31.00 ©2019 IEEE

The superposition can be represented by a linear combination, by adding coefficient α and β beside |0⟩ and |1⟩ states like the following equation (1) [5]:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad (1)$$

The state has to be normalized, such that $\alpha^2 + \beta^2 = 1$. The equation illustrates that the proportion of |0⟩ and |1⟩ states, depends on both coefficients α and β. The state |0⟩, |1⟩ and the linear combination α |0⟩+ β |1⟩ is considered as a single qubit state. The coefficients α and β can be real numbers or complex numbers. Thus, to visualize the state of this single qubit, a Bloch Sphere concept with three-dimensional vectors (x, y, z axis) can be used, as shown in Fig (1). This Sphere can represent any qubit state, including states with complex coefficients [6].

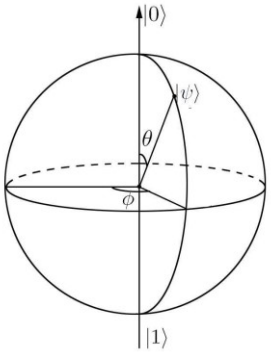

Figure 1: Bloch Sphere

Measuring a qubit can result |0⟩ or |1⟩, with the probability $|\alpha|^2$ and $|\beta|^2$ respectively, which can be represented by $|\alpha|^2 + |\beta|^2 = 1$. Implementing superposition state gives 50% |0⟩ half the time and half the time 50% for |1⟩, this state denoted by |+⟩ which can be represented with a gate called Hadamard [5][7].

- Entanglement

Quantum entanglement happens when multiple superposition quanta linked together where the measurement of one quantum state will determine the possible states of the other quantum. This connection does not depend on the quantum location because even if the entangled quantum separated by large distance, any change in one quantum will influence the other quantum [8].

- Non-clonability:

One of the most incredible characteristics that have a significant impact on cybersecurity is the non-clonability feature. No cloning means that the quantum state cannot be duplicated [9]. Unlike the classical computer where eavesdropping attacks can be performed on the classical bits (0 and 1). When a hacker tries to eavesdrop, a quantum bit a measurement process must be performed. In quantum machine, it is impossible to not affect the quantum state during the measurement [10]. There is no defined operation that has the ability to clone an unknown quantum state [9].

C) Quantum Gates:

- (X) gate:

X gate is a single qubit, changes the state of the qubit to the opposite. X gate will change the qubit |0⟩ to |1⟩ and from |1⟩ to |0⟩ [5].

- Hadamard (H) gate:

H gate operate on a single qubit and turns it to be in the superposition state. Which means the implementation of H gate will result in equal probabilities to become 1 and 0. The Hadamard equation is shown below

$$H = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad (2)$$

The use of two H gates is similar to the square root of X gate, simply it does nothing to the initial value [5].

- (Z) gate:

Z gate it is a single qubit gate, takes π rotation around Z axis of the Bloch Sphere. When the state is |0⟩ it will remain unchangeable, while if the state is |1⟩, it will flip to -|1⟩ state (but on the measurement the outcomes will be equal) [5][7].
For example, in case of implementing superposition state |+⟩ with H gate following with z gate, the measurement outcome will change [7] [11].

- Controlled-NOT(CNOT) gate:

CNOT gate is a type of the controlled gate. The controlled gates work on no less than two qubits, so that one or more of the qubits will control the operation. For CNOT gate, it will have two qubits input one act as a control, and the other is the target qubit that wants to manipulate, CNOT ($Control_n$, $Target_n$) [12]. CNOT will not operate the NOT operation on the targeted qubit unless the control qubit equal one [13].

D) Physical realization of qubits

In order to build a quantum computer, there are many physical systems might be good candidates. Below a brief discussion of one of them.

- Spin and quantum computing:

Spin is a fundamental angular momentum that carried by elementary particles and composite particles. The spin can be represented either up | ↑⟩ or down | ↓⟩. So, the spin state for the electron or proton is "|ψ ⟩= α| ↑⟩ +β| ↓⟩", which means the spin can be represented as qubit "with |0⟩= | ↑⟩ and |1 ⟩= | ↓⟩" [5].
The spin is helpful in visualizing the superposition. It can be found by rotating the spin partially from down to up [14]. In case the spin is vertically is 0, it becomes in superposition state when the spin rotated horizontally and resulted $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ state.

E) Quantum Cryptography: Bennett-Brassard (BB84)

One of the encryption algorithms that have been proved to be secure is one-time pad. It uses a random encryption key longer than the message itself and each bit of the message will be XORed with one bit of the random key and that will result in hard to break ciphertext. The problem of this algorithm is the key should be distributed in a secure way. For that, BB84 exists [15]. BB84 is the first quantum cryptography protocol developed in 1984 by Charles Bennett and Gilles Brassard.

The protocol utilizes the non-clonability property of the quantum. Also, the qubit will be sent as photon in the BB84 and it utilizes the polarization basis of that photons that have a rectilinear (+) and diagonal (x) basis. Mainly, BB84 uses two channels, the first channel is a one-way quantum channel that used by the first user to send qubits that will help to create a random key and the second channel is a two-way authenticated public classical channel used to communicate the result between the users and to exchange the encrypted message [16].

The protocol will follow some steps in order to generate and distribute the key as follow, first, if there are two user wants to communicate e.g. Alice and Bob, Alice will choose a random bit value and a random polarization basis and send that qubits to Bob. Then Bob will do measurements on that qubits based on the polarization basis that Bob chooses and determine the bit values. After that, Bob will use the public channel to send the used polarization basis to Alice. Then Alice will determine which of these bases were right and identical with Alice bases and share the result with Bob by the public channel. At the end, Alice and Bob will combine the bit values associated with the right polarization basis and use it as the key that encrypts the messages. In the case of a third part e.g. Eves, Alice and Bob will detect that because the Eves will do measurement on the sent qubit by Alice itself since the qubit cannot be copied due to the non-clonability property, and then send it to Bob, these changes will be noticed if Bob uses the same as Alice polarization basis but with getting different bit values, then this key won't be used and another BB84 key distribution process will start again. The advantage of this method, the communication in the public channel will not give any idea about the key value because only the polarization state will be sent throw it [16].

F) Quantum Bit Commitment (QBC)

QBC considered as an essential primitive schema to supply the communications between two distrustful parties (ex: Alice and Bob), with a cryptographic protocol for secure computation. It can be done usually through two phases, commit phase and unveil phase. In commit phase, Alice (the commitment sender) select the value of bit b (0 or 1) that she wants to commit to the receiver Bob and place it in safe before delivering it to Bob. Thus, she will send some evidence about b to Bob. Bob cannot know the committed bit b until Alice unveils it. On the other hand, Bob ensures that Alice would not be able to change the value of b. In the unveiling phase, Alice discloses some information about bit b, so that Bob can reconstruct it, using the evidence and the unveiled information by Alice [26].

V. LITERATURE REVIEW

In a paper about quantum cryptography done by S. Mitra, et al, [2] had done a comparison between the classical computers and the quantum computers. The comparison proved that major classical algorithms that use public key encryption and digital signature such as RSA are vulnerable and can be broken by utilizing quantum computational power [2]. Another paper that provided a review of quantum key distribution (QKD) by S. Krithika. [17], claims that the presence of a third party in the network may not be detected using the classical cryptography. Therefore, the paper demonstrated that such limitations could be solved by using quantum cryptography and the QKD. The most common QKD which is BB84 protocol was discussed in another paper [18]. The paper mentions that BB84 helps in having several shared key and error probabilities of the eavesdropper based on the quantum phase [18]. Also, a paper tested the BB84 protocol by implementing it with a simulator using Matlab. The test found that in a BB84 protocol single quantum channel the efficiencies of the Quantum Bit Error Rate (QBER) and the key qualification are 25% and 50% [19]. While the concept of QBC was discussed in another paper by N. Nagy et al. [20], proposed a new concept in the protocol and proved the security of the protocol by using algebraic properties that describe the quantum state used in this protocol, which is the equivalence class.

The previously reviewed papers have discussed theoretically the concept of quantum protocols or implement it with simulators using Matlab that simulates the quantum protocol in a classical computer. While this paper discusses the concept of the QKD BB84 protocol theoretically, and practically by implementing the protocol on IBM QX. Which is a software that can run its implementations on the real quantum processor or on a simulator. Then comparing and analyzing the results statistically, to prove its merit and effectiveness.

VI. STATISTICAL AND PRACTICAL IMPLEMENTATION OF BB84 QKD

This section shows the practical implementation of BB84 (QKD) using IBM QX. As well, discusses several implementations of distributing the cryptography key between Alice and Bob without existing of Eves and in case that Eves exists. Also, calculate the statistical results from the practical implementation and compare it with the theoretical results.

A) Practical implementation of Alice and Bob in BB84 protocol with 8-qubit and 16-qubit:

In the first example, the 8-qubits implemented. Table (1) below shows the values that will be implemented.

Table 1: 8-Qubits Random Values by Alice and Bob

Qubit Number	Q0 $\|0\rangle$	Q1 $\|0\rangle$	Q2 $\|0\rangle$	Q3 $\|0\rangle$	Q4 $\|0\rangle$	Q5 $\|0\rangle$	Q6 $\|0\rangle$	Q7 $\|0\rangle$
Alice bit Values	0	1	0	1	1	1	0	0
Alice basis	1	1	1	0	0	0	1	0
Bob basis	0	1	0	0	0	0	1	1
Accepted identical values	X	√	X	√	√	√	√	X
The Final key	11110							

Table (2) below shows the gates used to implement the table (1) above. The chose gates depends on the values selected by Alice and Bob. When Alice random bit value is zero no gate will be used but when it is one X-Not gate will be used. As for

the polarization basis, if the value is one then Hadamard gate will be used, but if it is zero, then the measurement gate will be used to provide the value as it is, without changes.

Table 2: Quantum Gates for the 8-Qubits example

Qubit Number	Q0 |0⟩	Q1 |0⟩	Q2 |0⟩	Q3 |0⟩	Q4 |0⟩	Q5 |0⟩	Q6 |0⟩	Q7 |0⟩
Alice Bit Value and Used Gates	-	X	-	X	X	X	-	-
	H	H	H	-	-	-	H	-
Bob Used Gates	M	H and M	M	M	M	M	H and M	H and M

Hadamard gate (H), Measurement gate (M), and Not gate (X).

Table (3) below shows the theoretical statistical results of the example provided in table (1) above. The qubits with the probability 100% will generate the key.

Table 3: The Theory Expected Result for 8-Qubits example

Qubit Number	Theory Expected Result	Qubit Number	Theory Expected Result
Q0	50% probability of each1 and 0	Q4	100% probability of 1
Q1	100% probability of 1	Q5	100% probability of 1
Q2	50% probability of 1 and 0	Q6	100% probability of 0
Q3	100% probability of 1	Q7	50% probability of 1 and 0

Fig (2) below is the implementation of the 8-qubit example listed above in IBM QX [21]:

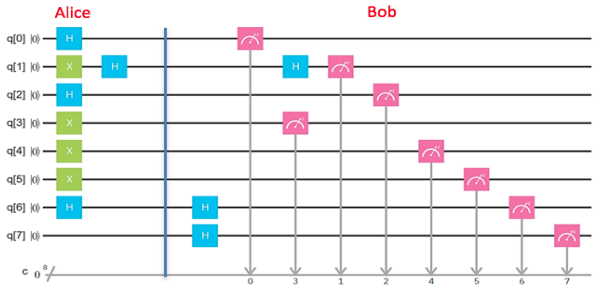

Figure 2: 8-Qubits example on IBM QX

This example executed on the processor with 300 runs; to make the results more specific. Fig (3) below is the results of the runs:

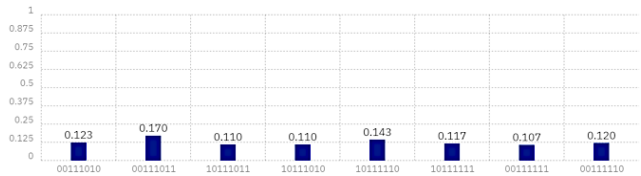

Figure 3: 8-Qubits Example Results of IBM QX Implementation

Fig (4) shows an example of calculating the probability of having zero in Q0 from the practical implementation. First, select the zero values. Second, sum the probabilities 0.123 + 0.110 + 0.143 + 0.120 = 0.496 (49.6%). All the rest probabilities calculated in the same way.

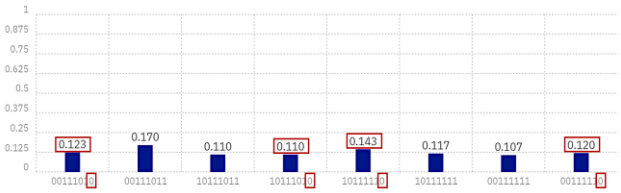

Figure 4: Calculating Q0 probability of getting zero value

Table (4) shows the probabilities of all qubits from the practical implementation:

Table 4: 8-Qubits example resulted probabilities of IBM QX Implementation

	Q0 |0⟩	Q1 |0⟩	Q2 |0⟩	Q3, Q4, Q5 |0⟩	Q6 |0⟩	Q7 |0⟩
Probability of 0	49.6%	0%	51.3%	0%	100%	52%
Probability of 1	50.4%	100%	48.7%	100%	0%	48%

It's observable that there are minor differences between the probabilities of the theory and the implementation results. Fig (5) below demonstrates the qubits that have different result probabilities which are Q0, Q2, and Q7. As well shows the probabilities of the theory and implementation of each of them.

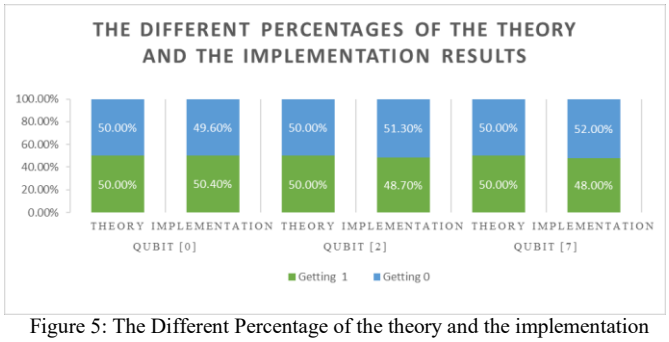

Figure 5: The Different Percentage of the theory and the implementation results

The same steps done for an example with 16 qubits with 300 runs. Table (5) shows the implemented values with 16 qubits.

Table 5: 16-Qubits Random Values by Alice and Bob

Qubit Number	Q0 |0>	Q1 |0>	Q2 |0>	Q3 |0>	Q4 |0>	Q5 |0>	Q6 |0>	Q7 |0>	Q8 |0>	Q9 |0>	Q10 |0>	Q11 |0>	Q12 |0>	Q13 |0>	Q14 |0>	Q15 |0>
Alice bit Values	1	0	0	0	0	0	1	1	1	0	1	1	0	0	1	1
Alice basis	1	1	0	0	1	1	1	1	1	1	1	0	1	1	1	1
Bob basis	1	0	1	1	1	0	0	0	1	1	0	1	0	0	0	1
Accepted identical values	√	X	X	X	√	X	X	X	√	√	X	X	X	X	X	√
The Final key	1 0 1 0 1															

Fig (6) below shows the implementation on IBM QX [23]:

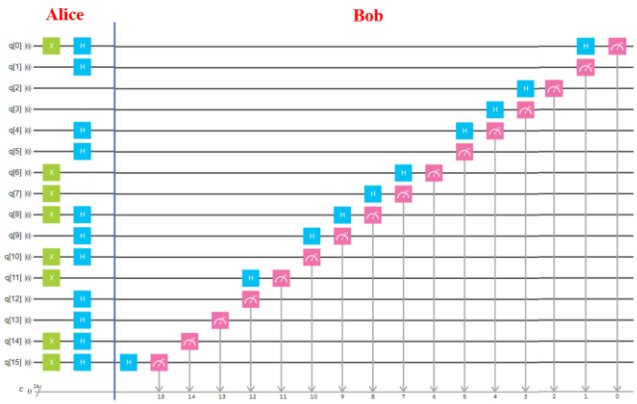

Figure 6: 16-Qubits example on IBM QX

Table (6) shows the probabilities of all qubits from the practical implementation:

Table 6: 16-Qubits example resulted probabilities of IBM QX Implementation

The probability of 0	**Q0|0>**	**Q1 |0>**	**Q2 |0>**	**Q3 |0>**	**Q4|0>**	**Q5 |0>**	**Q6|0>**	**Q7|0>**
	0%	52.33%	51.67%	53.33%	100%	50.67%	51%	46%
	Q8|0>	**Q9|0>**	**Q10|0>**	**Q11|0>**	**Q12|0>**	**Q13|0>**	**Q14|0>**	**Q15|0>**
	0%	100%	48.7%	52%	46.4%	46%	46.6%	0%
The probability of 1	**Q0|0>**	**Q1 |0>**	**Q2 |0>**	**Q3 |0>**	**Q4|0>**	**Q5 |0>**	**Q6|0>**	**Q7|0>**
	100%	47.66%	48.33%	46.67%	0%	49.33%	49 %	54%
	Q8|0>	**Q9|0>**	**Q10|0>**	**Q11|0>**	**Q12|0>**	**Q13|0>**	**Q14|0>**	**Q15|0>**
	100%	0%	51.3	48%	53.6%	54%	53.3%	100%

It appears that there are differences between the theoretical and implementation probabilities the highest one around 4%.

B) Practical implementation of the existence of Eve between Alice and Bob in BB84 protocol with 8-qubit example:

This example is based on the first example of 8-qubits but here with the existing of Eve during the key distribution. Eve sniffs the qubits and cannot copy the qubits according to non-cloning property. Therefore, Eve will randomly choose a different basis and perform the measurements in the actual transmitted qubits. So, there are two cases of Eve either lucky or unlucky. Lucky when Eve guess the basis correctly as it chose by Alice and Bob or when Eve chose the basis that do not affect the measurement results in Bob side. So that, both sides cannot detect the existing of Eve since the values did not change. While unlucky when Eve guesses the basis wrongly. So, the values will change, and Alice and Bob can detect that. Since, it will have 50% of getting $|0\rangle$, 50% for $|1\rangle$. So, it will discard by both communication parties. Fig (7) below shows The implementation of the Existing of Eve in both cases lucky at qubits q[1], q[4] and unlucky at qubits q[3], q[5] and q[6] using the same values at the table(1) above [24].

In a single qubit, when Eve is unlucky then she can be detected with the probability 50 % $(\frac{1}{2})$ for $|0\rangle$ qubit and 50% $(\frac{1}{2})$ for the $|1\rangle$ qubit, which means $(\frac{1}{2})$ $(\frac{1}{2})$ = $(\frac{1}{4})$ ≈25% to be caught, and the chance to escape on this single qubit is $(\frac{3}{4})$ ≈75%. In the mentioned 8-qubit example, the qubits that generated the keys is 5 qubits, thus Eve chance to escape is power to the number of key qubits, $(\frac{3}{4})^5$≈0.24 (24%). From these calculations, it can be observed that with a greater number of qubits that sniffed by Eve, the chance of escape become less with higher detection.

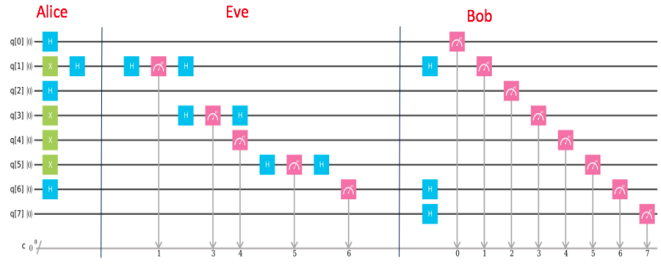

Figure 7: Eve exsitense between Alice an Bob

Table (7) shows the implementation probabilities of the qubits:

Table 7: the resulted probabilites after Eve basis

	Q1 $\|0\rangle$	Q3 $\|0\rangle$	Q4 $\|0\rangle$	Q5 $\|0\rangle$	Q6 $\|0\rangle$
The cryptography key between Alice and bob	1	1	1	1	0
Probability of Eve to get 0	0%	46%	0%	46%	54%
Probability of Eve to get 1	100%	54%	100%	54%	46%

It is noticeable that there are differences between the theoretical and implementation probabilities around 4% at the unlucky qubits. Fig (8) below demonstrates the differences.

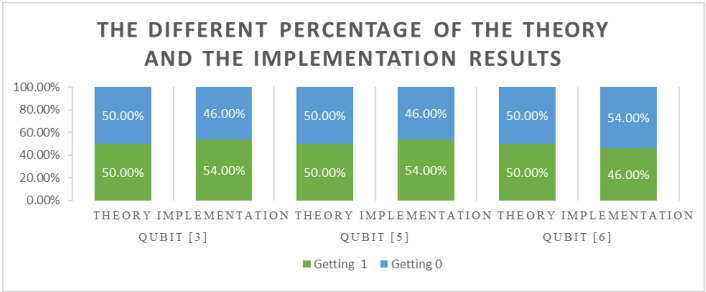

Figure 8: the differences between the theoretical and practical implementation probabilities

C) *Statistical Analysis*

While noting the results out of the implementation, there were observable differences between the theory and the practical implementation. Basically, the range of differences in the probabilities from 0.6 % to 4%. In this section, these differences were tested and analysed.

To show the differences between the result values, the standard deviation (SD) has been calculated for the probabilities of both the theory and the implementation results. Using the following equation (3) [22]:

$$SD = \sqrt{\frac{\Sigma|x-\mu|^2}{N}} \qquad (3)$$

Also, the comparison was based on F-test tool which is a tool that used to compare the standard deviation by computing the significant level value. If the significant level was below < 0.05 then there is a significant difference, otherwise not significant difference [25].

Table (8) below has the calculated standard deviation values of the theory and the IBM QX implementation results of BB84

Table 8: Standard Deviation Comparision of BB84

	The SD of the theory	The SD of the implementation	Significant Level
8-Qubits Implementation	24.21	23.61	0.95
16-Qubits Implementation	23.18	22.05	0.85

The significant level was computed using F-test tool for both implementations. As it appears in the table the significant level values was near to 1 which is more than the value 0.05. This means that although there are differences on the values, but these differences are not significant, and the implementations showed BB84 protocol function since the results were approximately near to the theorem expectations.

CONCLUSION

Quantum Cryptography is expected to cause a very considerable leap in the cybersecurity world. But the fact is, quantum cryptography is still a developing field that needs to go through several tests and analyses in order to prove its merit and efficiency. In this spirit, this paper provides a brief literature review that covers QKD and QBC protocols, then the paper focused to practically implement one of the most common quantum key distribution protocols which is "BB84" with and without the existence of the eavesdropper Eve. Moreover, this paper compared the theoretical and practical results of this protocol and provides a statistical analysis of it. The result of the statistical analysis showed that between BB84 implementations and the theorem expectations, the differences are minors and not significant. Moreover, the papers observed that with greater number of qubits that sniffed by eavesdropper, the detection will be higher.

REFERENCES

[1] H. Li, L. Zhu, K. Wang and K. Wang, "The improvement of QKD scheme based on bb84 protocol,", 2016 International Conference on Information System and Artificial Intelligence (ISAI), Hong Kong, 2016, pp. 314-317. Available: http://ieeexplore.ieee.org/document/7816726

[2] S. Mitra, B. Jana, S. Bhattacharya, P. Pal, and J. Poray, "Quantum cryptography: overview, security issues and future challenges," 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix), Kolkata, 2017, pp. 1-7. Available: https://ieeexplore.ieee.org/document/8350006

[3] P. Kilor, P. Soni, "Quantum cryptography: realizing next generation information security," International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2014. Available: http://ijaiem.org/volume3issue2/IJAIEM-2014-02-28-090.pdf

[4] IBM Research and the IBM QX team, "User guide / frequently asked questions," 2017. Available: https://quantumexperience.ng.bluemix.net/proxy/tutorial/full-user-guide/000-FAQ/000-Frequently_Asked_Questions.html

[5] M. Nielsen, I. Chuang, "Quantum computation and quantum information," 2000. Available: http://csis.pace.edu/ctappert/cs837-18spring/QC-textbook.pdf

[6] IBM Research and the IBM QX team, "The weird and wonderful world of the qubit," 2017. Available: https://quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=beginners-guide&page=004-The_Weird_and_Wonderful_World_of_the_Qubit~2F001-The_Weird_and_Wonderful_World_of_the_Qubit

[7] IBM Research and the IBM QX team, "Creating superposition," 2017. Available: https://quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=beginners-guide&page=005-Single-Qubit_Gates~2F002-Creating_superposition

[8] IBM Research and the IBM QX team, "Entanglement," 2017. Available: https://quantumexperience.ng.bluemix.net/proxy/tutorial/beginners-guide/007-Entanglement/001-Entanglement.html

[9] E. Rieffel, W. Polak, "An introduction to quantum computing for non-physicists," 2000. Available: https://arxiv.org/pdf/quant-ph/9809016.pdf

[10] S. Rao, D. Mahto, D. Yadav and D. Khan, "The AES-256 cryptosystem resists quantum attacks," International Journal of Advanced Computer Research, 2017. Available: https://www.researchgate.net/profile/Sandeep_Rao10/publication/316284124_The_AES-256_Cryptosystem_Resists_Quantum_Attacks/links/58f999200f7e9ba3ba4d22b1/The-AES-256-Cryptosystem-Resists-Quantum-Attacks.pdf

[11] IBM Research and the IBM QX team, "Introducing qubit phase," 2017. Available: https://quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=beginners-guide&page=005-Single-Qubit_Gates~2F005-Introducing_qubit_phase

[12] A. Aruna, K. Vani, C. Sathya and R. Meena, "A study on reversible logic gates of quantum computing," (IJCSIT) International Journal of Computer Science and Information Technologies, 2016. Available: http://ijcsit.com/docs/Volume%207/vol7issue1/ijcsit2016070194.pdf

[13] IBM Research and the IBM QX team, "Beginners Guide / Multi-Qubit Gates" 2017. Available: https://quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=beginners-guide&page=006-Multi-Qubit_Gates~2F001-Multi-Qubit_Gates

[14] G. Benenti, G. Casati, and G. Strini, "Principles of quantum computation and information," 2004. Available: http://www-reynal.ensea.fr/docs/iq/PrinciplesOfQuantumComputation1.pdf

[15] G. Gilbert, Y. Weinstein, "Introduction to Special Issue on quantum cryptography," 2014. Available: https://link.springer.com/content/pdf/10.1007%2Fs11128-013-0719-1.pdf

[16] Ch. Bennett, G. Brassard, "Quantum cryptography: public key distribution and coin tossing," 2014. Available: https://core.ac.uk/download/pdf/82447194.pdf

[17] S. Krithika, "Quantum key distribution (QKD): a review on technology, recent developments and future prospects," Research J. Engineering and Tech, 2017. Available: http://ijersonline.org/AbstractView.aspx?PID=2017-8-3-24

[18] A. Chen, W. Peng, and T. Gui, "A variant of bb84 protocol based on quantum phase," 2013 International Conference on Information and Network Security (ICINS 2013), Beijing, 2013, pp. 1-5. Available: https://ieeexplore.ieee.org/document/6826014

[19] O. Foong, T. Low, and K. Hong, "simulation study of single quantum channel bb84 quantum key distribution," 2017. Available: https://link.springer.com/chapter/10.1007/978-981-10-6454-8_21

[20] N. NAGY and M. NAGY, "Quantum Bit Commitment -Within an Equivalence Class," Unconventional Computing, 2016.

[21] IBM Q, "Take a look at this ibm q experience experiment!" 2018. Available: https://quantumexperience.ng.bluemix.net/qx/display/code?id=5be80b143017dc00512f34f3&idExecution=5be80ba13017dc00512f34f5

[22] Calculator.net, "Standard deviation calculator," 2008-2018. Available: https://www.calculator.net/standard-deviation-calculator.html

[23] IBM Q, "Take a look at this ibm q experience experiment!" 2018. Available: https://quantumexperience.ng.bluemix.net/share/code/5bddc4f894ab2f0052ed200e

[24] IBM Q, "Take a look at this ibm q experience experiment!" 2018. Available: https://quantumexperience.ng.bluemix.net/share/code/5be8433cd4d36f005459602c/execution/5be8433cd4d36f005459602d

[25] MedCalc, "Comparison of standard deviations (f-test)," 2018. Available: https://www.medcalc.org/manual/comparison_of_standard_deviations_f-test.php

[26] G. He, "Security bound of cheat sensitive quantum bit commitment," 2015. Available: https://pdfs.semanticscholar.org/5f7d/102a8ac12a6f0905c55b4919d86263ce6d37.pdf