Date of Publication: August 30, 2019 | Volume 7, Issue 3| Pages: 15-19

Quantum Security Using Enhanced BB84 Protocol

Kushalpreet Kaur , Student at Department of Computer Science, Doaba Institute of Engineering and Technology - [DIET], Mohali Affiliated from IKG-PTU, Jalandhar, India, kushalpreetkaur7@gmail.com

ABSTRACT: With the advancement of technology especially electronic communication industry, there is a need generated to keep data secure and confidential during online transactions. This makes cryptography a crucial part of IT industry. Our classical network systems are using symmetric and asymmetric cryptographic methods which are based on mathematical calculations such as large prime factorization these methods are impossible to be solved by present computer systems, due to the computational limitations or absence of efficient algorithms for solving a factorization problem. [12]

Quantum Computers are the super-fast computers that work on the principle of polarization of light photons. The quantum computer threat against public key cryptography is very serious due to its speed. The new key distribution called Quantum Key Distribution is introduced by researchers which will bring very high security during transferring data at communication channel. [2][14]

Quantum Key Distribution (QKD) provides a way for distributing secure key from sender to receiver. There are many QKD protocols [6] i.e. BB84, E91, SARG04, KMB09, S13, S09, AK15 protocol etc. BB84 protocol is much easier for practical implementation in Quantum Computing. [5, 15]

In this paper, existing BB84 protocol is enhanced by giving two side securities. How to eliminate the problems of existing BB84 protocol [6] is described in proposed work. In this paper there is a two qubit BB84 algorithm implementation by using local Qasm simulator of IBM quantum computers and results are given in tabular form.

General Terms: Security, Algorithms.

Keywords: Quantum Cryptography using BB84 protocol, Security by Photon Polarization, Quantum Mechanics, IBM Q BB84 protocol implementation.

1. INTRODUCTION

With the expansion of technology, there is inflation in security demands. The cryptography transfers data in a secure and confidential manner. Cryptography is a part of broad field cryptology. It has the cryptanalysis which is the art of code breaking. The present cryptography can be divided into two types – Asymmetric and Symmetric cryptography. The PKI (Public Key Infrastructure) cryptography system makes it possible to make emails and files secure with digital signature. These techniques boost safety to the data for internet transactions. But now with entry of Quantum Computing, these methods will not remain so much integrated as they are now.
Quantum computing work was first used by Richard Feynman [9] in 1982, who is also called the “destructor of the present Asymmetric cryptography"

1.1 Comparison of Classical and Quantum Computing

ETSI (European Telecommunication Standards Institute) has given a tabular representation of the comparison of security level of classical cryptography algorithms over classical Quantum Computing.

Table 1. ETSI- Post Quantum Security analyzation [3]

Algorithms	Key Length	Effective Key Strength / Security Level	
		Conventional Computing	Quantum Computing
RSA -1024	1024 bits	80 bits	0 bits
RSA - 2048	2048 bits	112 bits	0 bits
ECC - 25	256 bits	128 bits	0 bits
ECC - 3846	384 bits	256 bits	0 bits
AES - 128	128 bits	128 bits	64 bits
AES - 256	256 bits	256 bits	128 bits

The security of asymmetric cryptography is based on computational complexity using one way function. But by quantum computing, the one way function can be reversed which make it not secure anymore. It can break the classical cryptography just by cracking on searching secret keys in between the communication channel.

1.2 Quantum Computing

Quantum Physics leads towards the nano scope level. This computing can be used to solve certain mathematical problems like large factorization and searching at a very fast speed as compared to classical computing. For example **Grover's Algorithm** is very fast searching algorithm in quantum computers.

"*The implementation of Quantum computing practically will break all the public key cryptography algorithms*", written in August 2016 by NIST publication [11]. The era before the implementation of Quantum is **pre-quantum cryptography** and after its implementation is called **post-quantum cryptography.**

1.3 Quantum Cryptography

Quantum Cryptography is the first commercial use of Quantum physics which is based on the concept of Quantum mechanics as below [1];

1.3.1 Heisenberg Uncertainty principle

In this, the states of quantum or polarization of light particle can only be measured by perturbing it. It also signify no-cloning theorem.

1.3.2 Photon Polarization principle

This principle states that photon can be polarized in a particular direction and the photon filter with similar polarization can catch it else it will be lost.

This principle makes the Quantum Cryptography secure and safe from attacker.

1.4 Quantum Key Distribution

A new key Distribution named Quantum Key Distribution (QKD) protocol is analyzed which provides highly secure way for exchanging key. Ekert has introduced the QKD protocol by using Bell's Theorem [8] in 1994. After that Bennett and Brassard had proposed practical implementation of QKD protocol [7] in 1984.

BB84 is stated as the first Quantum Key Distribution protocol. This section shows a brief introduction of Classical and Quantum cryptography. The next section shows the existing BB84 protocol with an implementation example in IBM QISKIT Qasm-simulator. It depicts its algorithm in flowchart.

The third section provides the problems or breaches in this existing algorithm as stated in paper [5]. The fourth section states the proposed protocol with its implementation. In the last section it shows the conclusion of the research analyses.

2. EXISTING BB84 PROTOCOL

2.1 Implementation of BB84 protocol

BB84 protocol is used to generate one-time-pad encryption key. It applies non-orthogonal states by the polarization of photon. QKD creates symmetric key by using quantum properties of light in such a way that no one attacks in the communication network.

For implementing it, the two channels are used for communication- one is Quantum channel and another is classical channel.

The keys are produced randomly which can only be shared by sender and receiver. Stream of a single photon can create one secret key which is encoded with a bit value of 0 or 1. The photons are emitted by a conventional laser as pulses of dim light so that most pulses do not emit a photon. So, if using fiber optic cable some pulses contains more than one photon. Hence, only a small portion of pulses has photon at receiver side. The key can be encoded either by polarization or by the relative phases of photon. Polarization can be done either by rectilinear (+) or diagonal (x) polarization basis [3]. Sender can produce photons with 4 different polarizations, and (using a trusted random number generator) it chooses the basis for each photon at random and sends a stream of randomly polarized photons to receiver for measurement. This protocol is also termed as Prepare and Measure (P & M). The Key Sifting stage is done over a public classical channel, where Sender and receiver each broadcast their choice of basis for each photon. Only the basis is shred publicly, the attacker cannot access the data regarding keys. The bases are measured and matched, and any photon which shows non-matching bases is dropped from the key. The sifting process should, on average, leave half of the exchanged qubits still available for use in the final secret key.

Table 2. Polarization Basis

Bits	Angle	Basis	Photon
0	0°	+ (Rectilinear)	⇔
1	90°	+ (Rectilinear)	⇕
0	45°	X (Diagonal)	⤢
1	135°	X (Diagonal)	⤡

2.2 Steps of communication over Quantum channel using BB84 protocol

There is a sender who wants to send a secret message to receiver but the problem is the attacker who wants to steal that message without notifying the sender and receiver.

Date of Publication: August 30, 2019 | Volume 7, Issue 3| Pages: 15-19

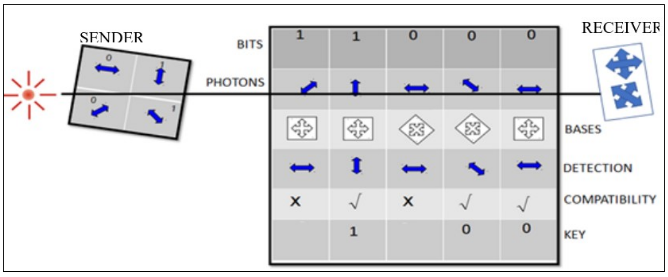

Figure 1: Sender and Receiver Using BB84 Protocol for Key Exchange [15]

1. Sender generates a random string of 0 and 1 to send that to receiver after converting those strings into related qubits by polarization method.
2. Sender sends those qubit keys by rotating some of them into a superposition and stores the polarized basis of every photon set (this rotation will represent keys as a non-understandable noise to attacker).
3. Receiver receives those qubits and randomly rotates some qubits in the opposite direction before measuring them (the measurement of the photon bits just by guessing its polarized basis and concluding the resultant key bits).
4. After measurement each photon is concluded as a string of bits of 0 and 1.
5. Sender and Receiver both shared the basis of information about which qubits they have rotated. Either both rotated or did not rotated on same basis, they will conclude some matched and some mismatched key bits by comparing basis.
6. The mismatched bits will be ignored.

If the attacker was present in the communication channel and trying to get the secret key then both sender and receiver would not get any matched keys. This will result them to start this complete process again. If there was no attacker then both concluded the matched keys to send the secret encrypted message.

2.3 Exemplary representation

The experimental algorithm is performed on QISKIT, an open-source quantum computing framework for quantum processors in research, education, and business. Qiskit Aer is a high performance simulator framework for quantum circuits. It provides several back-ends to achieve different simulation goals. Open QASM Simulator is used because it provides information about the state output by the ideal circuit and the matrix representation of the circuit. However, a real experiment terminates by measuring each qubit (usually in the computational |0>, |1> basis). Without measurement, information cannot be achieved about the state. Measurements cause the quantum system to collapse into classical bits.

2.3.1 Without Attacker's presence

Table 3. Sending data in Qubits without attacker

Sender Keys(S)	0	0	0	1	1	0	1	0	0	1	0	0	1	1	0	0
Receiver Keys(R)	0	0	0	0	1	1	1	1	0	1	0	0	0	1	0	0
Sender's Basis	Z	X	Z	Z	X	Z	Z	Z	Z	Z	Z	X	Z	X	X	Z
Receiver's Basis	X	X	Z	X	X	X	Z	X	Z	Z	X	Z	X	X	X	X
Matched Keys (S and R)		0	0		1		1		0	1				1	0	

Receiver keys= 0000111101000100
Percentage to discard the choice 0.5
Sender Keys= 0001101001001100
Receiver keys in histogram graph is {'0010001011110000': 1}

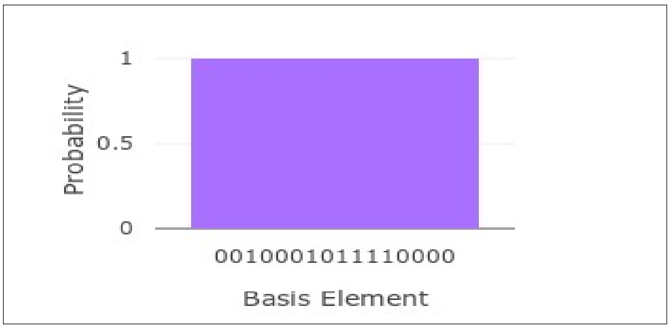

Figure 2: Plot Histogram View of Probability

This histogram shows the visualized form of data run on a quantum circuit.

The view of states of quantum system is approximately 100 times the output bit string is 1.

2.3.2 In Attacker's presence

Table 4. Sending data in Qubits in attacker's presence

Sender Keys(S)	0	0	0	1	1	0	1	0	0	1	0	0	1	1	0	0
Attacker's Keys(A)	1	0	0	1	1	0	1	0	1	1	0	0	0	1	0	0
Sender's Basis	Z	X	Z	Z	X	Z	Z	Z	Z	Z	Z	X	Z	X	X	Z
Attacker's Basis	X	Z	X	X	Z	Z	Z	Z	X	X	Z	Z	X	Z	X	X
Matched Keys(S and A)						0	1	0			0				0	
Receiver Keys (R)	1	0	0	1	0	1	0	0	0	0	1	1	0	0	0	0
Receiver's Basis	X	Z	X	Z	X	Z	Z	Z	Z	Z	Z	Z	X	X	X	X
Receiver's Keys based on Basis				1	0	1	0	0	0	0	1			0	0	
Sender's Keys based on Basis (S and R)				1	1	0	1	0	0	1	0			1	0	
Matched Keys (S and R)				1	_	_	_	0	0	_	_			_	0	

Date of Publication: August 30, 2019 | Volume 7, Issue 3| Pages: 15-19

Percentage to discard the choice 0.625% out of 1%
Measurement by chance 0.4375
Percentage of similarity: 0.4
Receiver Keys= 1001010000110000
Receiver keys in histogram graph is {'0000110000101001': 1}

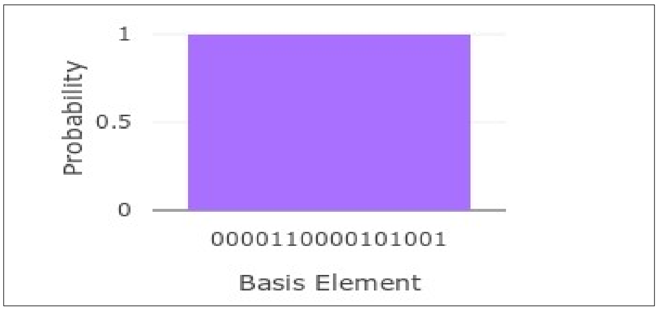

Figure 3: Plot Histogram View of Probability

2.4 Problems in Existing Protocol

In this algorithm, the attacker is not detected if the number of comparing bits size is small than the message. The probability to catch the attacker present in between the communication channel is not possible. The various problems are:

1. When the key size is less than the tendency to detect the attacker.
2. When both sender and receiver shared large number of key bits over the channel then the attacker could detect the keys data by taking assumptions from some attacked keys portion.

3. ENHANCED BB84 PROTOCOL

In the enhanced algorithm various limitations are removed by increasing security at the last step.

1. If the keys matched is length six which is short for providing security.
2. Suppose the key length should be 15 bits.
3. Adding remaining bits as 0 at the end.
4. Dividing the key string into equal blocks and inverting the last bits of each block as 0 to 1 or 1 to 0.
5. Then the first and second block will be XOR operated and their resultant will be saved in second block.
6. The resultant second block will be XOR operated with the third block and their resultant will be saved into third block.
7. The new key string will be in encrypted form that will not be understood by attacker.

3.1 Reasons for the enhanced algorithm

There are certain reasons for the enhanced BB84 protocol.

1. Increases the security.
2. 2. Increases key size which will create confusion for attacker to realize the keys
3. 3. It also increases security against PNS (photon number splitting) attack.

3.1.1 Exemplary representation

Matched Keys (S and R)	1	0	0	0											
Added 0s at the end	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Divide the string into equal blocks	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Convert last bit of blocks	1	0	0	0	1	0	0	0	0	1	0	0	0	0	1
XOR first and second block	1	0	0	0	1	1	1	1	1	0	0	0	0	0	1
XOR Second and third block(Resultant key)	1	0	0	0	1	1	1	1	1	0	1	1	1	1	1

3.2 Result

Probability analyses of Error estimation to analyze the level of security during communication.
Percentage for not discarding the choice is 0.625 % out of 1%.
The increased size of the keys also increased the security level in the communication channel.

4. CONCLUSION

This result provides more secure way to implement the BB84 protocol. Quantum provide unconditional security method for establishing a secure key [5], [10]. The real difference is the ability of the detection method of keys. For future perspective, there is certain practical challenges in-order to implement the quantum algorithms [13].

5. ACKNOWLEDGEMENT

I acknowledge the use of the IBM Q experience for this work. This work does not reflect the official policy or position of IBM or the IBM Q experience team.

REFERENCES

[1] [1] DelftX, "The Quantum Internet and Quantum Computers: How Will They Change the World", QTM1x Lecture notes, 2018.

[2]
[3] [2] C.H.F. Fung, K. Tamaki,B. Qi, H-K. Lo, "Security proof of quantum key distribution with detection efficiency mismatch", Quantum Information and Computation, Vol - 9, pp.0131 - 0165, 2009.

[4]
[5] [3] Anastasija Trizna, Andris Ozols, "An Overview of Quantum Key Distribution Protocols ", December 2018, vol. 21, pp. 37–44.

[6]
[4] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Josang, "The Impact of Quantum Computing on Present Cryptography", IJACSA, Vol 9, No. 3, 2018.

Date of Publication: August 30, 2019 | Volume 7, Issue 3| Pages: 15-19

[5] Tianqi Zhou, Jian Shen, Xiong Li, Chen Wang and Jun Shen, “Quantum Cryptography for the Future Internet and the Security Analysis”, February 2018, Article ID 8214619, Hindawi Security and Communication Networks.

[6] Hitesh Singh, D.L. Gupta, A.K Singh, “Quantum Key Distribution Protocols: A Review”, ISSN: 2278-8727, Volume 16, Issue 2, Ver. XI,Mar-Apr. 2014,IOSR Journal of Computer Engineering (IOSR-JCE).

[7] Charles. H. Bennetta,Gilles Brassard, “Quantum cryptography: public key distribution and coin tossing,” IBM Research, NY 10598, USA Department IRO, Theoretical Computer Science 560, 2014.

[8] E. Artur “Quantum cryptography based on Bell‟s theorem.” Vol. 67, No, 6,5, Aug-1991, pp 661-663.

[9] Richard Feynman, “On quantum physics and computer simulation” at quantum-dynamic feynman85_qmc_optics letters. 1982.

[10] ETSI, “Quantum Safe Cryptography and Security”, White Paper No. 8, ISBN No. 979 – 10 – 92620 – 03 – 0, June 2015.

[11] Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. NIST: Report on Post-Quantum Cryptography. Technical report, NIST, 2016.

[12] L. Grover, “A fast quantum mechanical algorithm for database search,” ACM Press, New York, 1996, pp. 212–219.

[13] Eleni Diamanti, Hoi-Kwong Lo, Bing Qi and Zhiliang Yuan, “Practical challenges in quantum key distribution”, Rev. Quantum Information, Vol. 2, 16025, Nov 2016.http://doi.org/10.1038/npjqi.2016.25.

[14] Abdulbast Abushgra, Khaled Elleithy, “QKDP’s Comparison Based upon Quantum Cryptography Rules”, April 2016, DOI: 10.1109, LISAT.2016.7494101.

[15] Anindita Banerjee, Anil Prabhakar and Mark R.Mathias, “Quantum Key Distribution–Technology Review”, Journal on Defence Information and Communication Technology, Vol.No.3, 2017.