ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

Emulation of BB84 Quantum Key Distribution Algorithm

Nihal Kaul[1], Hatim Chathiwala[2], Rishabh Shukla[3], Abbasali Antelawala[4]

U.G. Student, Department of Computer Engineering, KJ College of Engineering and Management Research, Pune, Maharashtra, India[1234]

ABSTRACT: Quantum computing is the branch of science that studies theoretical computation systems (Quantum computers) that make direct use of mechanical phenomena, such as superposition to perform operations on data. Quantum key distribution (QKD) uses Quantum mechanics to guarantee secure communication. It enables two parties (Alice and Bob) to produce a shared random secure secret key known only to them, which can then be used to encrypt and decrypt messages. QKD system makes use of the No-Cloning theorem which states that no identical copies of the quantum states can be cloned. This system uses two communication channels to share the secret key. The first channel is the Quantum channel on which the photons are transmitted and the second channel is the Conventional channel through which the superposition states of the qubits are transmitted. This paper projects the emulation of QKD algorithm, BB84 which determines the presence of eavesdropper in the communication channel.

KEYWORDS: Quantum Computing, QKD, Quantum mechanics

I. Introduction

A. *Quantum Computing:*

Quantum Computing is the branch of science which deals with the design and development of computers based on the principles of Quantum Mechanics. The subject of physics studies elementary objects and simple systems & the study becomes more interesting when things are larger & more complicated. Quantum Computation & information based on the principles of Quantum Mechanics will provide tools to put up the gulf between the small & the relatively complex systems in Physics.

B. *Qubit:*

Qubit structure, the x-axis denotes horizontal polarization and y – axis denotes the vertical polarization. Spin up is the phenomena of spinning the position of the qubit upwards. Spin down is the phenomena of spinning the position of a qubit downwards. The spin up and Spin down is required to change the value if the qubit from 0 to 1 or 1 to 0.Therefore the qubits can be represented mathematically as:

$\alpha|0> + \beta|1> \rightarrow$ Amount of energy required to spin the atom. 2 Qubits will represent 4 states. Therefore to spin the atom to any of four states, we will require four coefficients determining the magnitude to change the state of the qubit. Therefore, the qubit can be represented as:

$\alpha|00> + \beta|01> + \gamma|10> + \sigma|11> \rightarrow$ Amount of energy required to spin the atom

Similarly, we can imagine for 3-qubits, 4-qubits, ..., n-qubits, which will have2n states.

DOI: 10.15680/IJIRCCE.2018.0604074

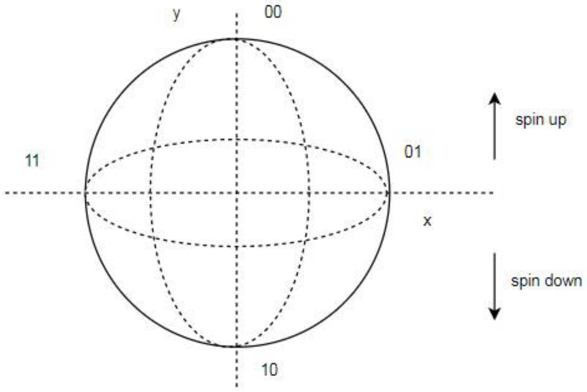


Fig.1. 2-Qubit

C. *Superposition Principle:*

Superposition is the principle of Quantum mechanics and its states that a particular atom can exist in multiple states in space simultaneously. This property of quantum mechanics is widely used in Quantum Key Distribution algorithms.

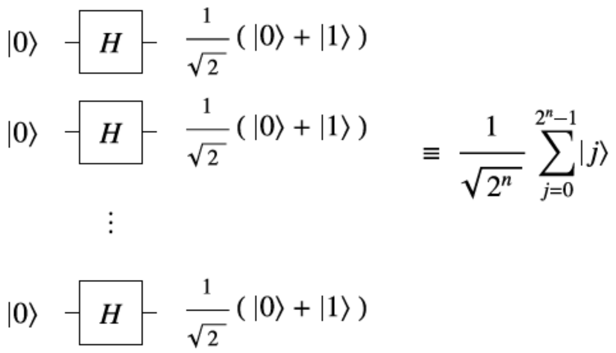
D. *No-Cloning Theorem:*

The no-cloning theorem states that no identical copies of the qubits can be formed.

This is because eavesdropping on the quantum channel adds noise to it which disturbs the quantum state. The quantum state is determined by the polarization of the qubit.

E. *Hadamard Gate:*

Hadamard is a Quantum gate. Hadamard helps in establishing superposition of the qubits. It also determines the probabilistic distribution of the qubits.


$|0\rangle$
H
$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
$|0\rangle$
H
$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
$\equiv \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}|j\rangle$
$\vdots$
$|0\rangle$
H
$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

F. *Heisenberg's Uncertainty Principle:*

In quantum mechanics, the uncertainty principle, also known as Heisenberg's uncertainty principle or Heisenberg's indeterminacy principle, is any of a variety of mathematical inequalities asserting a fundamental limit to the precision with which certain pairs of physical properties of a particle, known as complementary variables, such as position x and momentum p, can be known, it states that the more precisely the position of some particle is determined, the less precisely its momentum can be known, and vice versa.

G. *QKD:*

Quantum key distribution (QKD) uses quantum mechanics to guarantee secure communication. QKD is used to generate a shared secret key and not to transfer data. The key is known only to the sender and receiver which is then used to encrypt and decrypt messages. The ability of QKD is that the presence of any eavesdropper trying to intercept the channel can be detected. By using the principles of superposition and entanglement the system to detect eavesdroppers can be implemented. The network consists of a certain threshold. If the eavesdropping level is below a certain threshold, a key can be produced otherwise key will not be produced and communication will be aborted. The efficiency of the QKD system relies on the foundations of Quantum Mechanics. It depends on the mathematical functions. Once the key is produced it can be wrapped around with algorithms to encrypt or decrypt a message, which can be transmitted over a standard communication channel. Most commonly used algorithm associated with the QKD is the one-time pad. It can also be used with encryption using symmetric key algorithms like the Advanced Encryption Standard (AES).

H. *BB84:*

The first ever cryptographic protocol in Quantum computation is BB84. This protocol was invented and developed by Charles Bennett and Gills Brassard in 1984. The protocol is secure and provably relying on the Quantum property that information gain is only possible if the 2 states, one is trying to distinguish are not orthogonal. The concept behind this point is no cloning theorem.BB84 protocol is used for secure communication from source to destination in Quantum computers. BB84 scheme, suppose that the source 'A' wishes to send a private key to 'B'. 'A' begins with a 2 string of bits 'a' and 'b', each of n bits long. Then these strings are encoded of n qubits.

$$|\psi> = \otimes n_i = 1\ |\psi a_i b_i>$$

I. *Bloch Sphere:*

Quantum mechanics is mathematically formulated in Hilbert space or projective Hilbert space. The space of pure states of a quantum system is given by the one-dimensional sub spaces of the corresponding Hilbert space (or the “points" of the projective Hilbert space). For a two-dimensional Hilbert space, this is simply the complex projective line. This is the Bloch sphere.

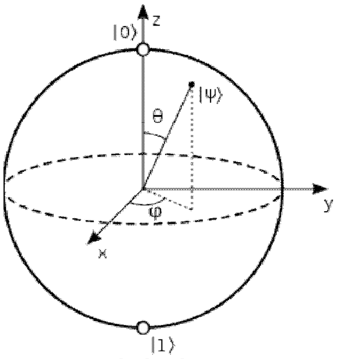


Fig.2. Bloch sphere

II. Literature Survey

A. *Model Checking Quantum Key Distribution Protocols:*

In this paper, a new group quantum key distribution protocol is designed based on BB84 protocol, which is a possible solution to handle the security issue in communication between multiusers. Discrete time Markov chain and probabilistic computation tree logic are used to model the protocol procedure and verify its security properties in PRISM. [1]

B. *Security of Entanglement Based Version of BB84 protocol for Quantum Cryptography:*

In this paper, author describes the ultimate way for key distribution. Unlike many of the classical cryptosystems in use today, whose security often draws on unproven assumptions about the computational complexity of mathematical problems, the security of quantum cryptography is based on the laws of physics. The Quantum Key Distribution follows some protocols for key distribution.

In this paper author describes the BB84 protocol which is used in Quantum Cryptography and the security aspect of entanglement based version of BB84. [2]

C. *An Efficient Parallel Algorithm for Secured Data Communications using RSA Public Key Cryptography Method:*

In this paper, author describes the Public-key cryptography and RSA based cryptography. To compute very large integers, typically 1024 bits, very large sequential computation in RSA becomes compute-intensive.the paper describes the modular calculations based on parallel computing. [3]

D. *New Protocol for Quantum Public Key Cryptography:*

In this paper author presents a quantum public key cryptographic protocol that allow Bob to send any arbitrary qubit state to Alice, securely. The paper proposes quantum pad-lock protocol that uses quantum entanglement and does not discard any qubits during the transfer process. This protocol allows for more number of bits to be transferred securely compared to BB84 and other protocols based on random measurements. [4]

E. *Secure Deployment of Quantum Key Distribution in Optical Communication Systems:*

Quantum Key Distribution (QKD) is a secure key agreement technique based on the theory of quantum mechanics. QKD has been widely studied for secure communication since it allows two distant parties to share a secret key even in the presence of an eavesdropper who has unlimited computational power and memory capabilities. In this paper, there is discussion of three security properties: data confidentiality, data integrity and user authenticity. This paper proposes a realistic system model and security solutions to protect the data from adversary attacks. [5]

F. *Robust Quantum key distribution based on two levels QRNA technique to generate encrypted key:*

The Quantum Key Distribution agrees for the secure transmission of unbreakable encryption keys and it provides a flawless secure coding to solve the problem of key distribution. The entanglement distillation approach of BB84 is widely used because the act of reading a quantum bit (Qubits) changes the bit; it is difficult for hackers to interfere without being detected sufficient number of bits. But this technique uses only four directions of electron movements so it is possible to guess the key. To overcome these drawbacks here two level QRNA technique is proposed for security. [6]

G. *Single-photon Synchronization Mode of Quantum Key Distribution System:*

The synchronization a two pass self-compensation quantum key distribution system (QKDS) with phase-encoded photon states. The most important component of QKDS efficient operation is the synchronization process which involves logging of the photon impulse receipt moment by single photon photo detectors. The purpose of the study is to improve the security of the synchronization algorithm QKDS by eliminating false solutions in case of equal number of accumulated impulses in adjacent signal time windows, with the photon impulse energy distributed between them. [7]

H. *Encryption Techniques: A Theoretical Overview and Future Proposals:*

In this paper, we provide a theoretical overview of various encryption techniques, namely those that range from changes in the position of a letter or word, to word transformations and transposition. This paper encapsulates the latest advances in science, which are used to obtain the maximum objective of an encrypted message, i.e. the secret coded message. In addition, there is a comparative study of them, and provided a summary of the main scientific contributions to this field. Lastly, conclusions of this work are provided in which we reflect on the proposal of having various levels of disseminated security, which can be applied for improving the performance and speed of encryption algorithms. [8]

I. *Security of Quantum Key Distribution:*

In this paper, the security issues facing quantum key distribution (QKD) are explained, herein focusing on those issues that are cryptographic and information theoretic in nature and not those based on physics. The problem of security criteria is addressed. It is demonstrated that an attackers success probabilities are the fundamental criteria of security that any theoretic security criterion must relate to in order to have operational significance. [9]

DOI: 10.15680/IJIRCCE.2018.0604074

J. *Security Proof of Improved-SARG04 Protocol Using the Same Four Qubit States:*

This paper proposes a security proof for a new class of quantum key distribution protocol namely Improved SARG04. This protocol differs from BB84 and SARG04 protocol in the sifting process and provably outperforms those protocols against Photon Number Splitting attack at zero error, with secure transmission distance of 125 km of SSMF. [10]

III. Proposed System

Our proposed system is based on Quantum Key Distribution mechanism. The QKD system is useful in sharing a secret key between two parties (namely Alice and Bob) securely. Quantum key distribution requires a transmission medium on which quantum carriers are transmitted from Alice to Bob. In theory, any particle obeying the laws of quantum mechanics can be used. The quantum carriers are photons, the elementary particle of light; while the channel may be an optical fibre.

In the quantum carriers, Alice encodes random pieces of information that will make up the key. These pieces of information may be, for instance, random bits or Gaussian-distributed random numbers. During the transmission between Alice and Bob, Eve might listen to the quantum channel and therefore spy on potential secret key bits. This does not pose a fundamental problem to the legitimate parties, as the eavesdropping is detectable by way of transmission errors. Also, the secret key distillation techniques allow Alice and Bob to recover from such errors and create a secret key out of the bits that are unknown to Eve. After the transmission, Alice and Bob can compare a fraction of the exchanged key to see if there are any transmission errors caused by eavesdropping.

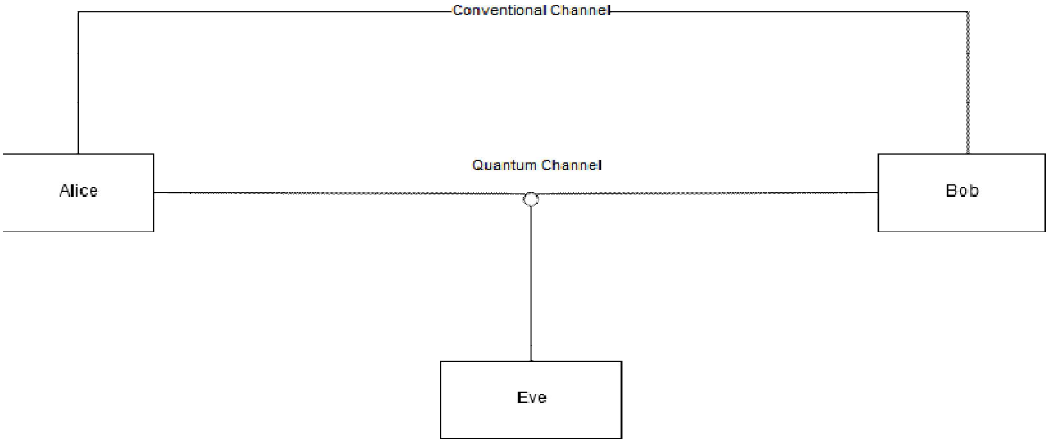


Fig.3. Proposed System

Methodology:

Participants:

1) Alice: Sender (Initiator of QKD).
2) Bob: Receiver
3) Eve: Eavesdropper
4) Quantum Channel: Secure channel made up of Fiber Optic through which photons are transmitted.
5) Conventional Channel: Channel through which Qubits are transmitted for comparing the Qubit-states of Alice and Bob.

1) Alice :

a) Generate random Qubits.
b) Apply Hadamard gate to establish superposition.

c) Generate random sending basis (rectilinear or horizontal).
d) Generate photon polarization.
e) Send polarized photons to Bob over Quantum Channel.

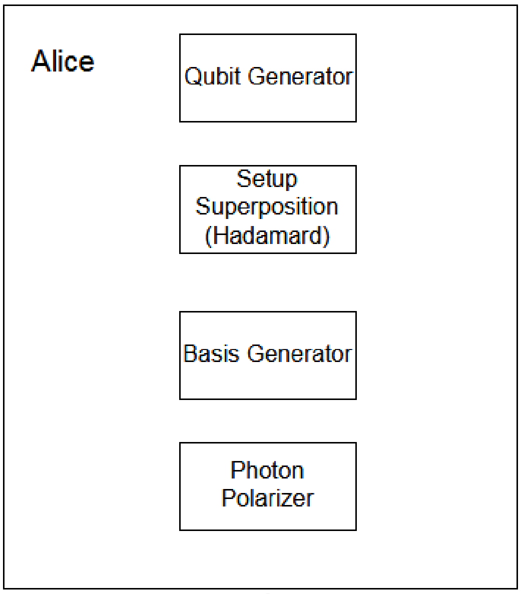


Fig.4. Alice

Diagram Components in detail:

A) *Qubit Generator*: This block generates Qubits. Qubits can be manipulated by spin-up and spin-down mechanisms. The Quantum particles are sandwiched between two semi-conductors. The Quantum particles can be spun up by applying a specific magnitude of force from the lower semi-conductor and the particles can be spun down by applying a specific magnitude of force from the upper semi-conductor. Our system though does not comprise of a Quantum Computer. Therefore we have emulated the generation of Qubits programmatically using the following matrices.

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

B) *Setup Superposition:*

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

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

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

C) *Basis Generator*: Basis is of two types i.e. Rectilinear Basis and Diagonal Basis. The rectilinear and diagonal basis is the orthogonal position in the Bloch Sphere.

DOI: 10.15680/IJIRCCE.2018.0604074

Basis	0	1
+	↑	→
x	↗	↘

Table 1. Basis Generation

Alice Basis Generation								
Alice's random bits	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	x	+	x	x	x	+

Table 2. Alice Basis

D) *Photon Polarizer*: Alice prepares a photon polarization state depending both on the bit value and basis.

Alice Photon Polarization								
Alice's random bits	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	x	+	x	x	x	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→

Table 3. Photon Polarizer

2) Bob

a) Receive the photons sent by Alice over Quantum Channel and measure the photons.
b) Generate measured random basis from the received photons.
c) Generate Qubits from the random basis.
d) Alice will now send the Qubits over conventional channel to Bob.
e) Bob will now compare its measured Qubits with that of Alice.
f) The two parties decide on a particular threshold. While comparing, they simply discard the bits which did not match**.** Receive the photons sent by Alice over Quantum Channel and measure the photons.

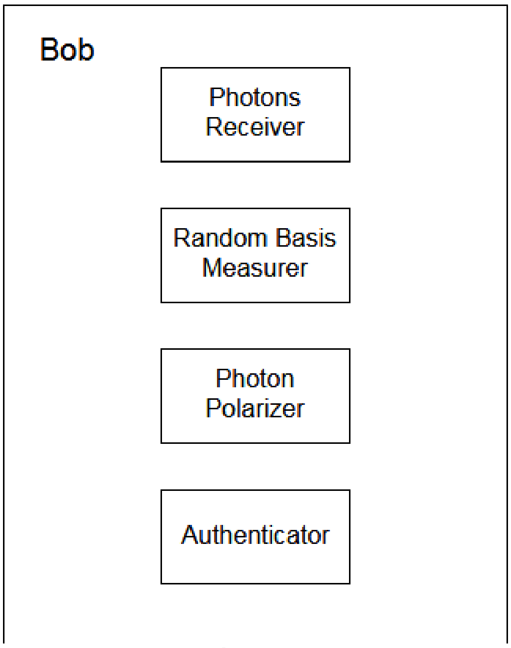


Fig.5. Bob

Diagram Components in detail:

A) *Photon Polarizer*: This block receives the photons transmitted by Alice sent over Quantum Channel.

Bob's Photon Measure								
Photon polarization Bob measures	↑	↗	↘	↑	↘	↗	↗	→

Table 4. Photon Polarizer

B) *Bob's Random Basis Measurer*: This block generates random measuring basis.

Bob's Random Basis Measurer								
Photon polarization Bob measures	↑	↗	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	x	x	x	+	x	+	+

Table 5. Bob's Random Basis Measurer

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

C) *Authenticator*: At last, this block matches the Qubits sent by Alice and the Qubits which Bob measured.

Preparation of Manuscript								
Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	x	+	x	x	x	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	x	x	x	+	x	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

Table 6. Photon Polarizer

3) Eve

a) Eve eavesdrop/intercept the channel while Alice and Bob are communicating over Quantum Channel.
b) While intercepting the channel, Eve adds noise to the Quantum Channel which distorts the photons being transmitted.
c) This way Bob measures incorrect basis which results in generating incorrect Qubits.
d) Therefore, when Alice and Bob compare their Qubits over Conventional Channel, their Qubits don't match.
e) If the percentage of distortion is greater than the threshold, then the Qubits are discarded and the process is started all over again.
f) If the percentage of distortion is less than the threshold, Bob and Alice both establish connection to transmit data.

IfEve randomly modifies the Qubits which also match the Qubits sent by Alice i.e. with no distortion. Then, Bob will not realize whether eavesdropping has happened.

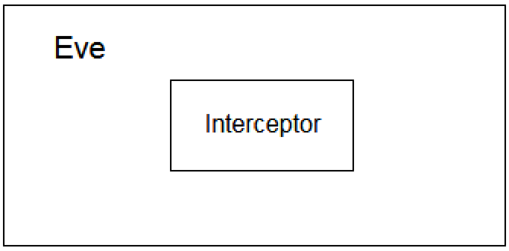


Fig.6. Eve

Diagram Components in detail:

A) *Interceptor*: This block intercepts over Quantum Channel resulting in addition of noise which results in distorting the Qubits.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

Preparation of Manuscript								
Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	x	+	x	x	x	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	x	+	+	x	+	x	+
Polarization Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Bob's random measuring basis	+	x	x	x	+	x	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1
Errors in key	✓		×			✓		✓

Table 7. Photon Polarizer

4. Detailed Diagram

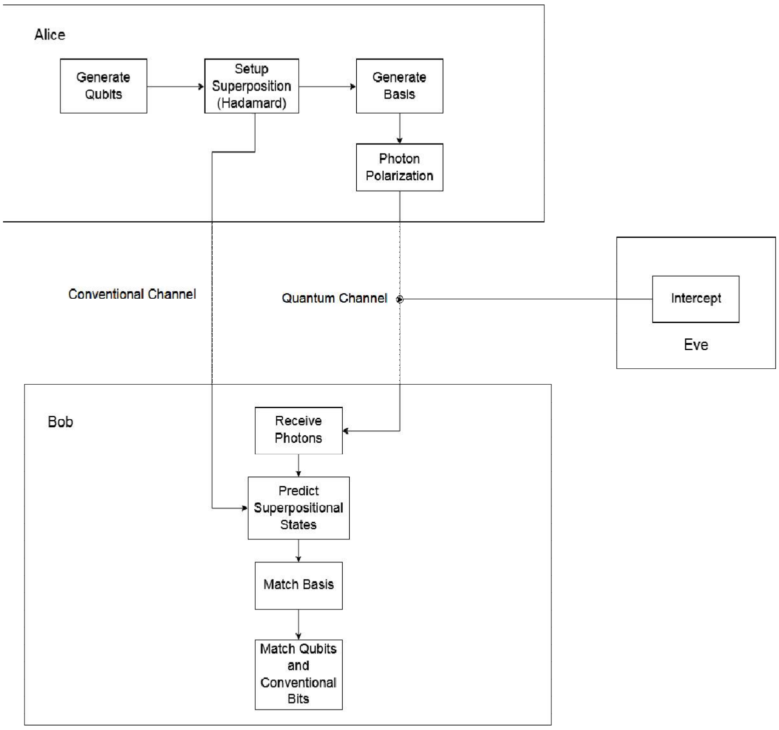


Fig.7. Detailed Diagram

DOI: 10.15680/IJIRCCE.2018.0604074

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 4, April 2018

IV. RESULTS

The eavesdropper in our system disturbs the photons generated by the sender or receiver. The eavesdropping ratio is decided randomly by the method or the eavesdropping system. This chart shows the increasing mismatch ratio at increasing eavesdropping rate.

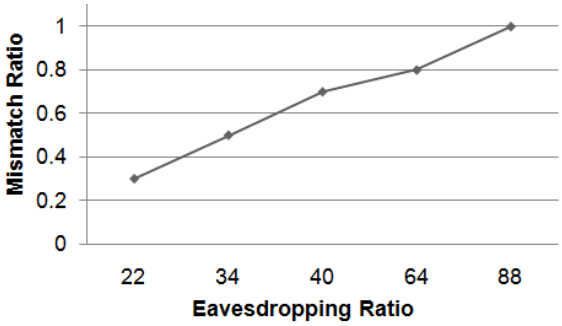


Chart 1. Analysis

Thus, this system figures the increasing mismatch ratio with the quantum algorithm and thus senses the eavesdropper in the system.

V. CONCLUSION

As we know, the QKD relies on quantum mechanics. Highly secure communication is possible with the QKD. With the help of Quantum computer and this communication algorithm, we can set up the possibly the secure system. The classical public key and private key algorithms only work with the classical systems and are quite feasible for the conventional system. But due to advancement in the computing system, the quantum computers can be a better choice for solving large sized problems. Thus, designing the Key distribution system can help in simple QKD in new generation computers.

REFERENCES

1. Baichuan Huang, Yan Huang, Jiaming Kong, Xin Huang: Model Checking Quantum KeyDistribution Protocols, Department of Computer Science, University of Liverpool, 8thInternational Conference on Information Technology in Medicine and Education (2016)
2. Anand Sharma, VibhaOjha, Prof. S.K.Lenka:Security of Entanglement Based Version ofBB84 protocol for Quantum Cryptography, Computer Science and Information Technology(ICCSIT), 2010 3rd IEEE International Conference (2010)
3. SapnaSaxena and Bhanu Kapoor: An Efficient Parallel Algorithm for Secured DataCommunications using RSA Public Key Cryptography Method,Advance Computing Conference(IACC), 2014 IEEE International (2014)
4. Abhishek Parakh: New Protocol for Quantum Public Key Cryptography, University ofNebraska, Omaha Advanced Networks and Telecommuncations Systems (ANTS), 2015IEEE International Conference (2015)
5. JooYeon Cho and Helmut Griesser: Secure Deployment of Quantum Key Distributionin Optical Communication Systems (2017)
6. M. Deepthi and G. Murali: Robust Quantum Key Distribution Based On Two LevelQRNA Technique To Generate Encrypted Key, Applied and Theoretical Computing andCommunication Technology (iCATccT), 2016 2nd International Conference (2016)
7. Anton Pljonkin and Konstantin Rumyantsev: Single-photon Synchronization Mode ofQuantum Key Distribution System, Southern Federal University Taganrog, Russia, ComputationalTechniques in Information and Communication Technologies (ICCTICT), 2016International Conference (2016)
8. Javier Sanchez, Ronny Correa, Hernando Buenano, Susana Arias and Hector Gomez:Encryption Techniques: A Theoretical Overview and FutureProposals, Universidad Tecnicade Ambato, Ecuador, eDemocracyeGovernment (ICEDEG), 2016 Third InternationalConference, (2016)
9. Horace P. Yuen: Security of Quantum Key Distribution, Northwestern University,Evanston, IL 60208, USA, IEEE (2016)
10. LizalIswady Ahmad Ghazali, Ahmad Fauzi Abas: Security Proof of Improved- SARG04Protocol Using the Same Four Qubit States, Photonics (ICP), 2010 International Conference(2010)

DOI: 10.15680/IJIRCCE.2018.0604074