International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 09 | Sep 2020 www.irjet.net p-ISSN: 2395-0072

Simulation of BB84 Protocol over Classical Cryptography Channel for File Transfer

Rimitha Shajahan[1], Suchithra.S.Nair[2]

[1]Student, Information Technology, LBS Institute of Technology for Women, Poojappura, Kerala, India
[2]Assistant Professor, Dept. of Computer Science and Engineering, LBS Institute of Technology For Women, Poojappura, Kerala, India

---

Abstract - *All cryptographic algorithms used in classical network communications stems on the pure mathematical foundation, since it depends on calculating computational variance like factors of prime numbers, GCD etc. It is highly prone to vicious attacks. This paper explains how a networking scenario can exploit pure laws in physics that can be simulated inside a classical communication channel. So that we can ensure a secure and flawless exchange of information. Nowadays, the perplexing properties of quantum computing is widely used in different applications, so adapting the key concepts in QKD can promise a much more efficient, authentication, transfer of information. Apart from implementing the most celebrated BB84 protocol in QKD, we also investigating a different level of application aspect which efficiently utilises, its very own essence over a classical network. Additionally, the paper provides a hybrid approach incorporating various traditional key generation, encryption-decryption and BB84. Then, the validation and efficiency of the system is analysed by implementing an auditing phase which uses quantum circuits based on the principle of Qbit commitment.*

Key Words: *QKD, BB84, RSA, AES, SHA, QISKIT, QASM*

1. INTRODUCTION

Classical cryptography is the technique that is used for the conversion of plain text into cipher text through insecure communication channels. Due to the lack of security, it may lead to the possibility of attacks and thus efficiency diminishes [1][13]. Quantum Key Distribution (QKD) is a reliable communication method that associated with the cryptographic protocol like BB84 and properties of quantum mechanics namely Heisenberg's Uncertainty Principle and Quantum no cloning theory [1] [14].

Heisenberg's Uncertainty Principle [2] [15] states that the position and momentum of a particle cannot be simultaneously measured with arbitrarily high precision. There is a minimum for the product of the uncertainties of these two measurements:

$$\Delta x \Delta p > \hbar/2. \quad (1)$$

Photon Polarization Principle refers that an eavesdropper cannot copy the unique quantum bits that is unknown quantum state, due to the no cloning principle. If an attempt is made for measuring any properties, it will disturb the other information [3][15].

No-Cloning Theorem states that "it is impossible to make a copy of an unknown quantum state" [4] [16]. **Quantum Entanglement** is a type of quantum mechanical phenomenon in which the quantum states of two or more quantum particles have to be related to each other, even individual particles may be spatially separated [5] [19]. **Principle of Causality** states that "the same cause or set of causes always produces the same effects (other things being equal) and the causes temporally precedes, or is simultaneous with, its effects". In this paper, use the third postulate of principle of causality, that is Quantum measurements are described by a set {Mm} of measurement operators. These operators are acting on the state space of the system being measured. The index m indicates to the measurement outcomes that may occur in the experiment [6] [11].

A qubit [7][11] (short for quantum bit) is physical object, such as a photon or an electron, which is the basic unit for quantum computation and quantum information.

In general, the state of a qubit can described by

$$|\psi\rangle = |\alpha\rangle + |\beta\rangle. \quad (2)$$

The basis is defined as

$$|+\rangle = |0\rangle + |1\rangle/\sqrt{2} \text{ and } |-\rangle = |0\rangle - |1\rangle/\sqrt{2}. \quad (3)$$

Re-expressed the basis to the state of a qubit as

$$|\psi\rangle = (\alpha + \beta/\sqrt{2})\,|+\rangle + (\alpha - \beta/\sqrt{2})\,|-\rangle. \quad (4)$$

A quantum observable is a measurable quantity, expressed as an operator, such that the property of the system state can be determined by means of an operational definition [8] [11]. A bit commitment scheme defines a two-party method such that a party can commit to a chosen value, keeping it secret to everyone else, with the capacity to reveal its commitment later, while forcing the commitment to remain unchanged from the commitment moment until it is revealed [9].

To overcome the attacks and efficiency issue in classical cryptography, combine the concepts of QKD and classical aspects. QKD uses BB84 protocol, which is secure for the exchange of information. Qbit commitment is used for checking the bits altered or not.

This paper gives an idea about the hybrid system which deploys principles in theoretical physics and concepts in computer science and to analyze its efficiency compared to classical methods and evaluate the application proposed in solving the security issues during the file transfer.

2. LITERATURE REVIEW

The list of Quantum Key Distribution Protocols are:

2.1. BB84 Protocol

This protocol is proposed by Charles Bennet and Gilles Brassard in 1984. It is based upon conventional cryptographic techniques like photon polarization and extends the communications through the quantum and public channel. The first quantum key distribution protocol which is provenly secure [10][17].

2.2. B92 Protocol

This protocol uses two polarization states- 0 degrees for rectangular basis and 45 degrees for diagonal basis. If the sender transmits to receiver a string of photons encoded with randomly selected bits but this time the bits sender chooses dictates which bases receiver must use. Sender will not measure if receiver opt the same basis. Thus arise the problem of erasure [10][16].

2.3. COW Protocol

Coherent One-Way protocol is a new protocol for Quantum cryptography enhanced by Nicolas Gisin et al in 2004. Setup is easy and resist to lowered interference visibility and more efficiency in terms of distilled secret bits per qubit [17] [18].

2.4. SSP Protocol

Six State Protocol is a type of quantum key distribution protocol and like a version of bb84. It uses six state polarization based on three orthogonal bases. So there occur high error rate of eve [18] [19].

2.5. EPR Protocol

The EPR quantum protocol is a 3-state protocol and define in terms of the polarization states of an EPR photon pair. This protocol uses Bell's inequality to note the presence or absence of Eve as a hidden variable [18] [19].

2.6. DPS Protocol

Differential Phase Shifting Protocol is a novel quantum cryptography scheme proposed by the authors Inoue K, Woks E and Yamamoto, which explains a single photon is prepared in a linear superposition state of three basis. This protocol is acceptable for fiber transmission systems and provides a key creation efficiency [18] [19].

2.7. KMB09 protocol

KMB09 protocol is a substitute quantum key distribution protocol, where sender and receiver use two mutually unbiased bases- '0' and '1'. The security of the scheme is due to a least possible index transmission error rate (ITER) and quantum bit error rate (QBER) established by an eavesdropper [18] [19].

2.8. SARG04 PROTOCOL

This protocol was proposed in 2004 by Scarani et.al. When sender and receiver determine for which bits their bases matched, sender announces a pair of non-orthogonal states one of which she used to encode her bit. If Bob used the correct basis, then she will measure the correct state, otherwise not. The length of the key remaining after the sifting stage is ¼ of the raw key (no errors) [18] [19].

2.9. S09 PROTOCOL

S09 protocol is based on public private key cryptography for secure transmission of data over a public channel. The security of the protocol derives from the fact that sender and receiver, each use secret keys in multiple exchange of the qubit [18] [19]. Briefly, each protocol has its own advantages and performance aspects. Here try to implement the physics of quantum mechanics into a classical channel. BB84 is found suitable very much adaptable in classical channel. We opt the BB84 rather than other protocols go for the simulation process.

Protocol Name	Characteristics
BB84 Protocol	The advantage that there is no need of public announcement of bases and increased efficiency.
B92 Protocol	When one of the qubits travels through the channel having collective noise, it gets affected by the noise and as a consequence singlet state also gets affected by the noise.
COW Protocol	Does not use symbol-per-symbol type of coding and the standard security proofs do not apply in any straight way.

SSP Protocol	Due to the presence of more possible states than in bb84, it increases the error rate.
EPR Protocol	Asymptotically secure, but the process that stores the qubits has little limitations on the operability.
KMB09 Protocol	Claims the long distance quantum communication with high error rate.
SARG04 Protocol	After the sifting process, receiver is left with one-fourth of the raw bits which when compared to bb84 is very less.
SO9 Protocol	secure transmission of data over a public channel

Table -1: Comparison of BB84 and Other Protocols

3. PROPOSED SYSTEM

The proposed system mainly focuses on exploring the aspect of classical cryptography over QKD. After quantum communication is simulated using a python module in **PyCharm**. Since quantum channel inherently able to defend classical attacks. The challenges arise while trying to perform a full proof secure communication over the classical channel using the keys obtained from QKD protocol. Since BB84 protocol seems to be more accurate while incorporating with discrete algorithms like RSA and Digital Signature (**Fig-1**).

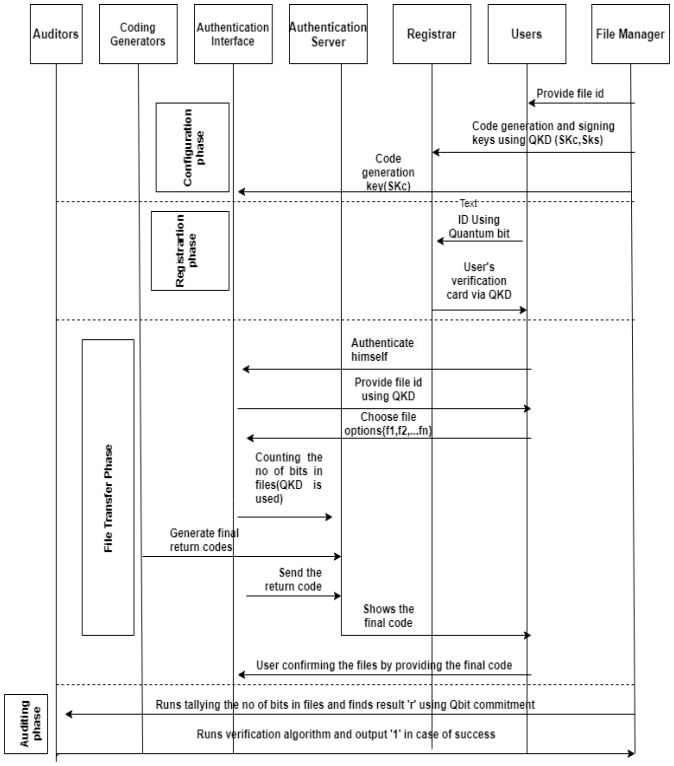

Fig -1: Sequence Diagram

In configuration phase, the file manager will provide file id to user (sender). For the simulation of QKD protocol using BB84 protocol, give the inputs like key-amount and key-size. After entering the values, generate key-pairs (sender's key and receiver's key).

For the authentication of key-pairs, use the RSA algorithm to encrypt the keypairs. That encrypted keypairs generated are send to Sender and Registrar by file manager. Sender also send the encrypted key-pairs to Registrar and file manager.

In the registration phase, registrar will check or verify the encrypted key-pairs send by file manager and Sender are same or not. If both are same, then registrar will send confirmation message to Sender that both encrypted keypairs are same. Sender can use the shared encrypted keypairs for the file transfer process.

In file transfer phase, use AES and SHA algorithm for the encryption and decryption process for the files. Here Sender selects a file (that must be text file, image file, video file) and enter the value of encrypted key-pairs. Sender encrypt the file. On the other side, receiver decrypt the encrypted file of Sender. QKD is important because key-pairs are generated randomly and also eaves cannot be identified due to its randomly changing nature.

In auditing phase, focus on the Qubits that are generated from the QKD protocol. Qubit commitment is used for checking the probability of possibilities of no of 00 and 11.

QISKIT is used for proving the Qbit commitment process. First of all, build a quantum circuit (holds all quantum operation) that represents the case as key distributed from QKD. Then, Aer use QASM simulator backends for running purpose.

Create a Quantum Circuit acting on the q register and add a Hadamard gate on qubit0.Add a CNOT gate on control qubit 0 and target qubit 1. Map the quantum measurement of qubits from QKD module to the classical bits. Execute the circuit on the QASM simulator and counts the probability of 00 and 11 with eaves presence and absence.

4. RESULTS AND DISCUSSIONS

4.1 Configuration phase

File id provided by file manager:

def file id( ): for i in range (0 , 1): a = random.randint (0, 5000)

Fig -2: Key encryption using RSA

def rsa_encrypt(): pt = entry.get(keypairs) ct = rsa.encrypt (pt,'random') entry.insert (0 , ct)

Here key-amount gives as 10 and key-size as 12 and thus generate keypairs. Choose the key-pair randomly. For ensuring additional authentication of keypairs, use RSA encryption algorithm.

4.2 Registration phase

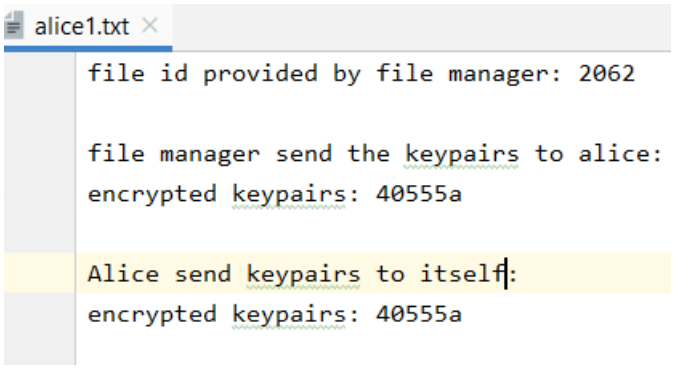

Fig -3: Encrypted key-pairs provided to sender by file manager

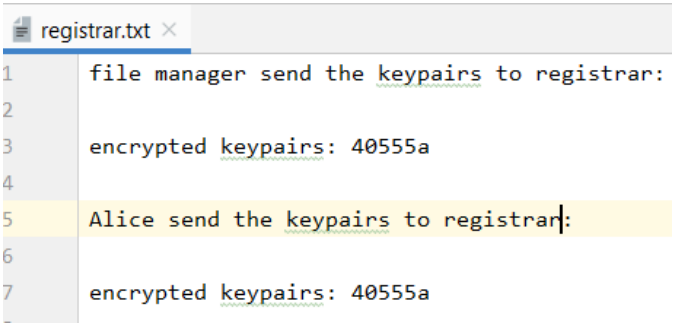

Fig -4: Encrypted keypairs provided by sender and file manager for checking the similarity

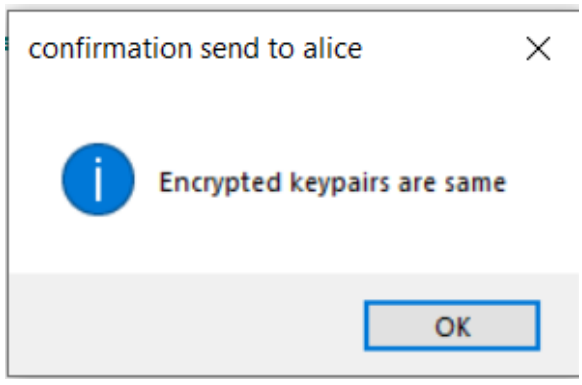

Fig -5: Registrar confirmation

Registrar confirms that both encrypted keypairs send by Sender and file manager are same. So the sender can use the encrypted keypairs for file transfer process.

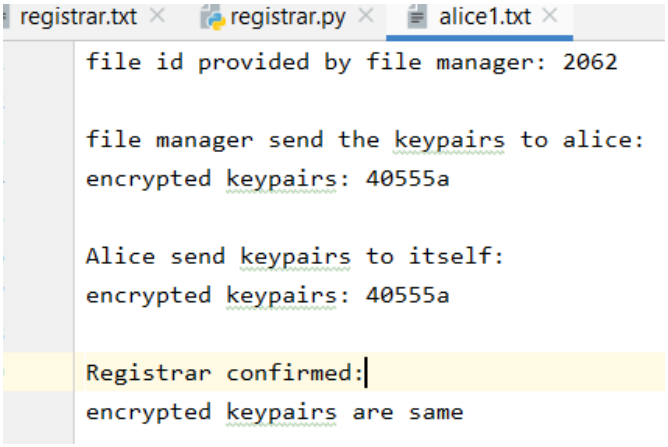

Fig -6: Sender can use the encrypted key-pairs for file transfer

4.3 File Transfer phase

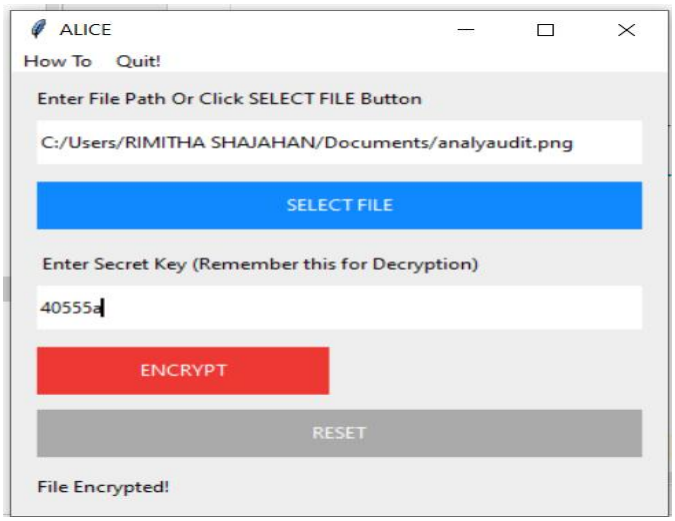

Fig -7: Sender encrypt the file using encrypted key-pairs

Sender selects a file and insert the encrypted key-pair value for encryption process. AES and SHA algorithm are used for the encryption and decryption process. Thus get the encrypted file.

Receiver uses the encrypted file for decryption. Atlast, get the original file that are undergone file transfer process. It is secure file transfer because uses the encrypted key-pairs. So attackers cannot detect the key-pairs.

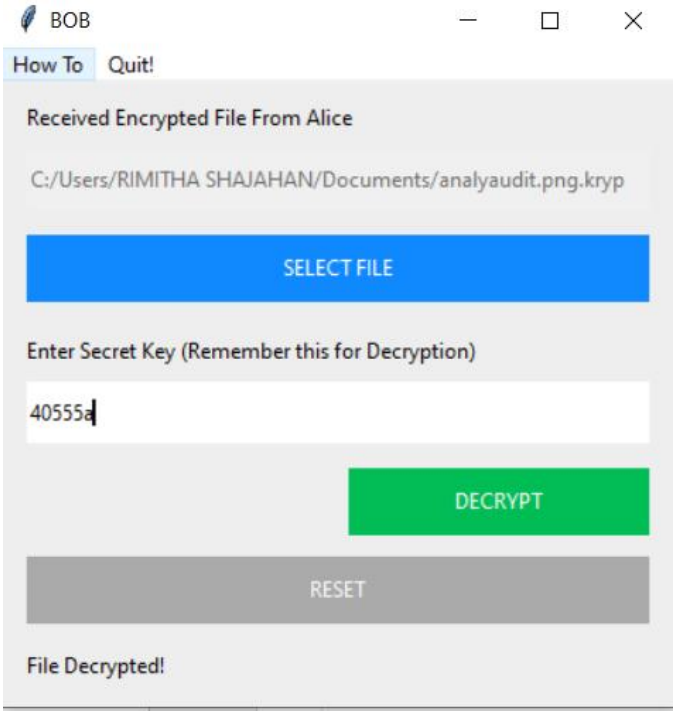

Fig -8: Receiver decrypt the encrypted file of sender

4.4 Auditing phase

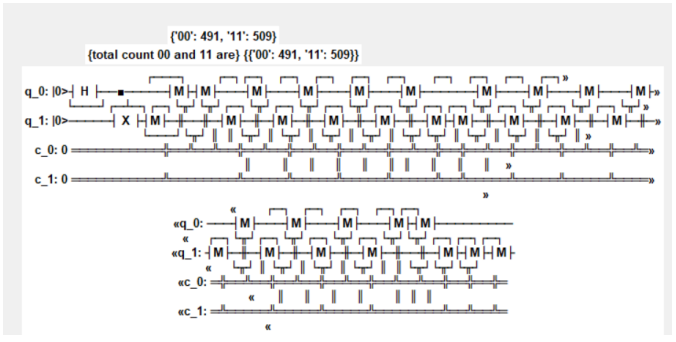

Fig -9: Perform Qbit commitment based on the key-size and key-amount

Qbit Commitment:

Consider a two party (sender and receiver) bit commitment. sender chooses a bit $b \in \{0, 1\}$, locks it and sends it to receiver (commitment phase). When it is the time to reveal b (opening phase), receiver locks the bit with his own lock (i.e., he locks the bit locked by sender), and sends it back to sender. Sender then opens her lock and sends the bit back to receiver and announces b. Receiver then opens his lock and checks whether the locked bit b is the same as the one which was announced [12]

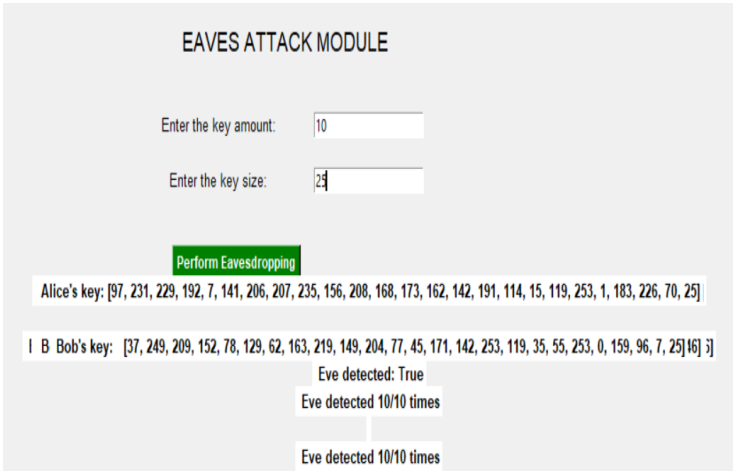

Fig -10: Perform eavesdropping

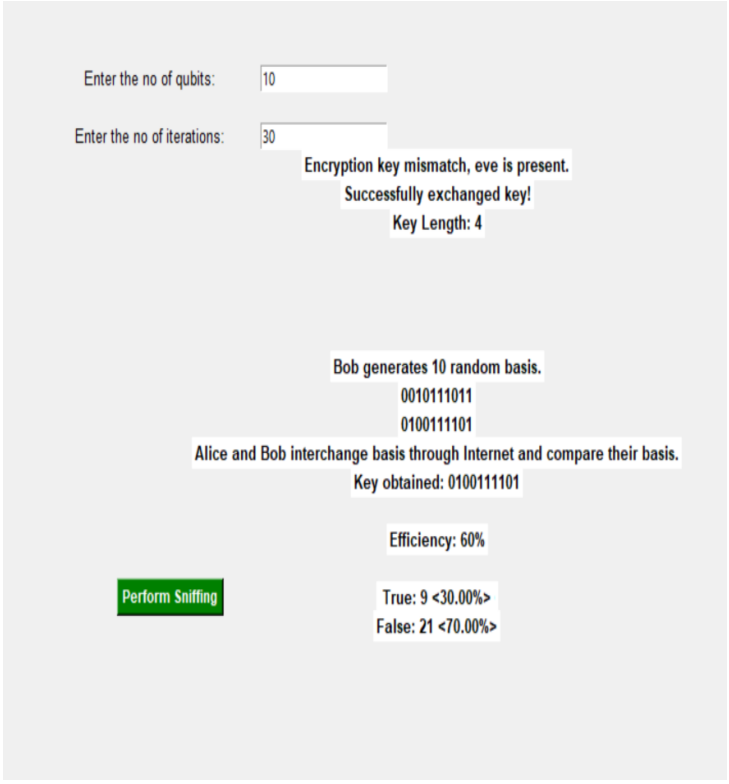

Fig -11: Perform sniffing attack

	Quantum Key Distribution using Quantum Channel			Normal Key Distribution using Classical Channel	
	With Eavesdropping	Without Eavesdropping		With Eavesdropping	Without Eavesdropping
Initial number of qubits	500	500	Initial no of bits	500	500
Final Key Length	106	128	Final Key Length	98	120
Estimated Error	0.0769	0.0	Estimated Error	1.25	0.5
Eavesdropping Rate	1	0	Eavesdropping Rate	1	0
Alice/Bob basis selection bias	0.5	0.5	Alice/Bob basis selection bias	0	0
Eve basis selection bias	0.5	0.5	Eve basis selection bias	0	0
Information Leakage	83	48	Information Leakage	85	53
Overall key cost for authentication	256	256	Overall key cost for authentication	324	324
Bit error Probability	0.0144	0.0	Bit error Probability	0.5	0.2
Security Parameter	20	20	Security Parameter	18	18

Fig 12-: Comparison of QKD using quantum channel and Normal key distribution using classical channel

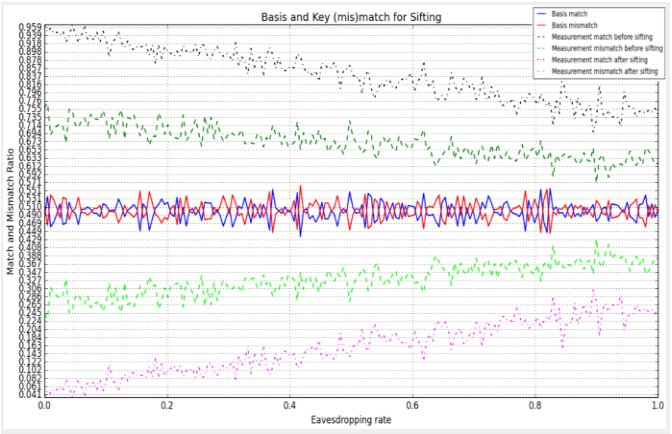

Fig 13 -: QKD sifting plot

Receiver announces on a public classical channel the qubits that he has managed to successfully measure. Sender and Receiver then reveal and exchange the bases they used. They authenticate these three message exchanges. Whenever the bases happen to match- about 50% of the time on average- they both add their corresponding bit to their personal key. In the absence of channel noise, the two keys should be identical unless there has been an eavesdropper:

- The sifting phase started with 500 transmitted qubits and the resulting bit string was reduced to 257 bits.
- 0.514 of sender's and receiver's chosen measurement bases match. 0.486 of their chosen bases do not match.
- 0.716 of the two parties measured qubits match before sifting and 0.284 of them do not.
- 0.9144 of the two parties measured qubits match after sifting and 0.0856 of them do not.

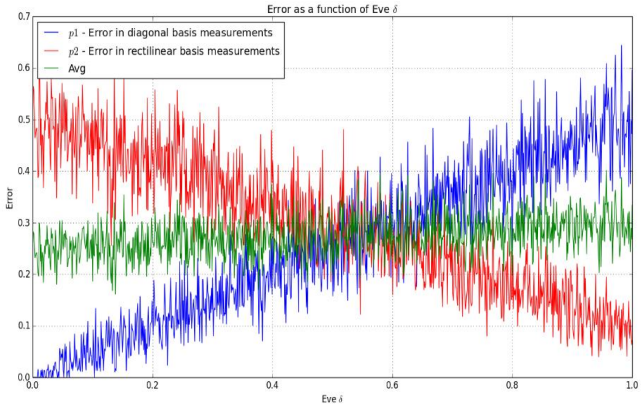

Fig 14-: QKD biased error estimation plot

Sender and Receiver estimate the error rate in their sifted keys to determine whether they should proceed to error correction or whether they should abort the protocol based on a predefined error tolerance threshold, usually around 11%.

- Sender and Receiver permute their sifted keys in order to flatten the errors across the entire bit string. Then they perform the error estimation by comparing a subset of their error-flattened sifted keys.
- An error rate of 0.0784 was estimated using a sample size of 51 given a sampling ratio of 0.2.

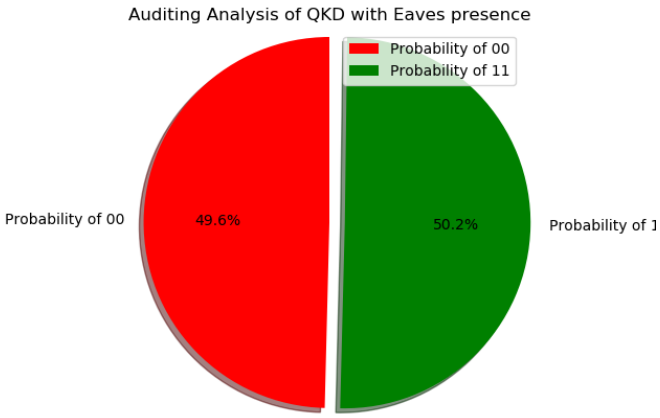

Fig 15-: Analysis of QKD with Eaves presence using Qbit commitment

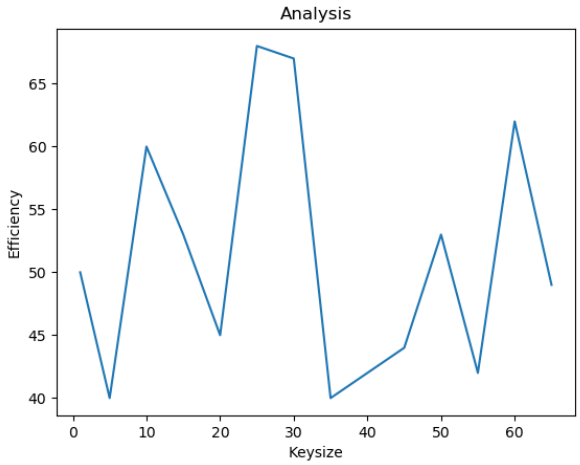

Fig 16-: Analysis of efficiency vs key-size in QKD

REFERENCES

[1] Aakash Goyal, Sapna Aggarwal, Aanchal Jain, Quantum Cryptography & its Comparison with Classical Cryptography: A Review Paper, 5th IEEE International Conference on Advanced Computing & Communication Technologies, CHAPTER-94.pdf

[2] Ian J. R. Aitchison, David A. MacManus, Thomas M. Snyder, Understanding Heisenberg's "magical" paper of July 1925: A new look at the calculational details, 3 June 2004, heisenberg25amer_j_phys.pdf

[3] M. Boca, C.Stoica, A.Dumitriu, V.Florescu, Photon polarization in Compton scattering: pulse shape effects, 2015

[4] Wojciech H. Zurek, William K. Wootters, The no-cloning theorem, January 2008, Physics Today, Volume 62(2)

[5] Fiona MacDonald, Scientists Just Unveiled The First-Ever Photo of Quantum Entanglement, 13 July 2019

[6] L.J. Russell, The Principle of Causality, Volume 46(1945-1946)

[7] Steven J. Weber, Kater W. Murch, Mollie E. Kimchi-Schwartz, Nicolas Roch, Irfan Siddiqi, Quantum trajectories of superconducting qubits, 2016

[8] Wafa Mohamed Elmannai, Varun Pande, Ajay Shreshta, Khaled Elleithy, Quantum observable, June 2013

[9] Hristo Lulev, Overview of Bit commitment schemes, 2007

[10] Mart Haitjema, A survey of Prominent Quantum Key Distribution Protocols

[11] Quantum Cryptography applied to Electronic-Voting Protocols-sabino.pdf

[12] S.A Sheiholesham, A practical quantum bit commitment protocol, 2012

[13] https://www.geeksforgeeks.org/classical-cryptography-and-quantum-cryptography/

[14] https://en.wikipedia.org/wiki/Quantum_key_distribution

[15] http://hyperphysics.phy-astr.gsu.edu/hbase/uncer.html

[16] https://en.wikipedia.org/wiki/No-cloning_theorem

[17] http://reports.ias.ac.in/report/18088/study-of-bb84-qkd-protocol-modifications-and-attacks

[18] https://www.irjet.net/archives/V3/i5/IRJET-V3I5273.pdf

[19] https://fdocuments.in/document/quantum-key-distribution-protocols-a-there-are-many-protocols-for-providing-a-secure.html

BIOGRAPHIES

Rimitha Shajahan,
Student, Information Technology, LBS Institute of Technology For Women, Poojappura

Suchithra.S.Nair,
Assistant Professor,
Dept. of Computer Science and Engineering,LBS Institute of Technology For Women, Poojappura