Industrial Engineering Journal
ISSN: 0970-2555
Volume : 50, Issue 5, No. 1, May 2021

A Novel Quantum Key Distribution Protocol for E Governance

Y.HARINATH
Assistant Professor
harinath5404@gmail.com

SOMARLA LOKESH KUMAR
Assistant professor
smkumaraltss@gmail.com

VAJRAKARUR KEERTHANA
Assistant Professor
vkeerthanaalts@gmail.com

Abstract*—In recent years, most emerging nations, including India, have placed a greater emphasis on the use of electronic governance. E-Governance will result in faster and more accurate information, greater transparency in governance, increased administrative efficiency, and improved public services in a variety of domains, including education, water, transportation, health, power, security, municipal services, and the administration of the state. It is essential to guarantee security when the information is being sent between the parties in this situation. Cryptography is used to ensure citizens' safety in today's electronic governments. The distribution of the key across the various cryptographic key exchange methods is accomplished through the usage of the traditional route. In this regard, there can be certain restrictions. Quantum cryptography was developed specifically with the goal of overcoming the constraints of traditional encryption. Quantum cryptography relies on the use of quantum channels in order to carry out key distribution. A secure transmission may be achieved by the use of quantum key distribution. It lets two people to construct a shared random bit string that is only known to them. This string may be used as a key to encrypt and decrypt communications, and it is only known to the two parties involved. The capability of the two users speaking with one another to identify the existence of any third party attempting to get knowledge of the key is one of the distinctive characteristics of quantum cryptography. This kind of quantum cryptography facilitates the transfer of data using qubits, which have the unique ability of changing their states if they are copied. This trait allows for the secure transmission of data. In order to ensure the safety of the e-governance applications, this research makes use of quantum key distribution. In today's world of e-governance, a great number of transactions may be completed in only one hour. Through the use of OTP, electronic transactions may be completed. One-time passwords, often known as OTPs, are an integral part of the authentication process that helps to make it more secure. A significant challenge is getting OTPs to the appropriate users. At the moment, this OTP may be given to users via traditional channels, which may result in the user being trapped. Quantum Key Distribution is used here as a means of overcoming this challenge so that the OTP may be shared. In this context, the QKD Simulator may be used to carry out simulations and analyses of the BB84 protocol, which displays probabilistic behavior.

***Index Terms*—E-Governance, Cryptography, Quantum Cryptography, Quantum key distributions.**

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 50, Issue 5, No. 1, May 2021

I. INTRODUCTION

A. Cryptography

The study of cryptography is the process of deciphering secretly written material. It is the skill of converting a communication that can be understood into one that cannot be understood, and then reverting that message back into its original format when the transformation has been completed. Plaintext refers to the message that has been organized in a straightforward manner. By executing the encryption calculation, the plaintext is transformed into figure material that is in an undecipherable shape. The process of converting figurative material into plaintext is referred as as decoding. The method of cryptography allows for the message's setting to be concealed from everyone, with the exception of the person who sent the message and the person who received it.

B. Quantum ciphering technology

Quantum cryptography is entirely safe against being sold off without the sender or the collector of the communication gaining knowledge of the other party. In contrast to more traditional approaches of cryptography, quantum cryptography is distinguished by the fact that it places a greater emphasis on the use of material science, rather than mathematics, as an essential component of its security show. The creation of a secure cryptosystem via the use of quantum cryptography relies on the exploitation of individual particles of bar and the specific quantum features that each particle has. Quantifying the quantum condition of any framework without making that framework more complicated is a very challenging task.

C. Quantum key distribution

The concept of quantum key distribution is a method for providing limitless security. This approach may make use of the rules of quantum physics to guarantee that two different groups have the same key (sender: Alice, beneficiary: Bob). It is made possible by using single photon technology, and it is able to see potential listening in via the quantum bit blunder rates of the quantum channel. The exchange of data that has been carelessly stored on single photons results in a common enigma, which is an arbitrary string, and the probabilistic method of determining the state of the photon provides the premise upon which its security is based.

D. E-Governance

E-governance is the process of streamlining public administration with the objective of enhancing effectiveness, straightforwardness, accessibility, and responsiveness to inhabitants. This is accomplished by making intensive and significant use of information and communication technologies. E-Governance has become more important in a variety of spheres, including education, water and transit systems, health and wellness, regulation and safety, civil administrations, and state organization. The many forms of media are capable of transmitting information. During the process of transferring the information, security is ensured with the help of key.LITERATURE

Modern cryptography without quantum is vulnerable to attacks due to the dramatic increase in technological innovations and evolution of mathematics. This has led to the research in quantum cryptography to safeguard IT systems in the real world [1]. Mink, Frankel and Perlner [2] proposed an integration of QKD and commodity protocols such as TLS and IPSec. Thus they could provide a layer for QKD services for security applications in the real world. Walton et al. [3] proposed explored the performance of photon-pair QKD and proved that their implementation could provide several orders of

magnitude in securing bit rate. Stuki et al. [4] experimented on photon counting as part of QKD research. In the process they could record the dynamics of three types of photodiodes. The detection efficiency and probability were encouraging. However an error rate of 5% and 10% were recorded 40 km and 54 km empirical study.

Fung et al. [5] proposed phase-remapping attack on a QKD system made up of BB84 with single photon sources. At Quantum Bit Error Rate (QBER) between 14.6% and 20%, the system was compromised as the attacker could render the final key insecure in spite of the usage of quantum mechanics. However, when the attack is not known to users explicitly, the protocol was problem secure. Therefore it is essential to have an understanding on phase-remapping attack. Tamaki et al. [6] explored Bennett 1992 QKD scheme with strong reference pulse. The research on the security of the scheme proved that the protocol is unconditionally secure. Lutkenhaus [7] explored BB84 under the standard detection scheme and proved unconditional security bestowed by BB84.

Elboukhari, Azizi, and AbdelmalekAzizi [8] employed quantum cryptography [9] to Local Area Networks (LANs). Moreover they tried to integrate QKD with Transport Layer Security (TLS) protocol. Their work towards this has indicated the possibility and feasibility of integrated QKD with TLS kind of protocol for fool proof security. Poppe et al. [10] explored QKD with polarization entangled photons. Towards this end, they proposed an entangled-state QKD that was empirically tested among hardware devices that were connected in a distributed network. The distance between nodes was 1.5 km and the application was proved to be highly secure. Hwang, Lee, and Li [11] explored multi-party QKD authentication with explicit and implicit user authentication. They also employed Unbiased-Chosen Basic (UCS) assumption to prove the security and robustness of their proposed schemes. Pattaranantakul et al. [12] explored an enterprise application model with secure quantum cryptography.

Lin and Tzeng [13] proposed a threshold proxy re-encryption scheme that secures outsourced data. Their security architecture is facilitated by number of storage servers and key servers. The storage servers store data while the key servers act as access nodes. The scheme supports encoding, encryption and forwarding. Each storage server and key server independently performs encoding and re-encryption and partial decryption respectively.

Lim et al. [14] proposed a new device independent quantum key distribution mechanism that is compatible with Bell's theory with respect to inequalities between two parties. Thus they could overcome the problem of detection loophole attack.

Cotler and Shor [15] proposed a new QKDP that works faster than the existing such protocols. The protocol increases key generation rate by using a single photon's spatio-temporal modes effectively. Fiber optic and line of sight channels were used to demonstrate the proof of concept.

Mosca, Stebila and Ustaoglu [16] described BB84 QKD protocol which is then integrated with traditional AKE models. Their experiments proved that QKD can withstand future advances in computing arena. They used both classical cryptography and QKD and tested long-term and short-term security of BB84.

II. Related Work

In this study, quantum entry dispersal is employed as a component of E-Governance applications in order to overcome the limitations of existing key dissemination. In this section, the findings of the QKD test system are dissected in order to transfer the key via quantum key circulation. The depiction of stages in QKD Simulator is as follows, according to the rules:

A. The First Phase: BB84 Quantum Transmission

Alice organizes a collection of five hundred qubits, and then she sends it to Bob across the quantum channel. She chooses at random a cause for each qubit, either rectilinear polarization (level 0 degrees and vertical 90 degrees) or a corner to corner polarization (plus 45 degrees and minus 45 degrees moved). After that, she maps horizontal and vertical with the qubit states |0> and |1>, and she maps +45 degrees and -45 degrees moved with the states |+> and |->, individually. Alice communicated her premise choice predilection of 0.1 to Bob when she transmitted him 500 qubits. Eve is listening in on the quantum channel with a rate of 0.1 and with a predisposition toward the option of 0.1 for the premise. Eve, a snoop, is now monitoring the transmissions on the channel. She begins by obstructing the qubits, then randomly measures them in either of the two previously mentioned bases, decimating the initial qubits in the process, and finally she sends Bob another cluster of qubits that she has compared to her estimates and premise judgments. Because Eve is only able to choose the proper premise around half of the time, approximately one quarter of her bits are different from those Alice chose.

B. Sifting, which is the 2.1st phase

Bob broadcasts over an open conventional channel the qubits that he is now able to effectively assess and announces the opening of the channel. After that, Alice and Bob unearth and negotiate the bases that they used. They vouch for the validity of these three communication exchanges. When the bases chance to coordinate with one another, which happens around half the time on average, both bases add their comparing bit to the key that they have for themselves. The two keys ought to be distinct from one another in the absence of channel commotion, unless there has been an eavesdropper.

The C. Phase 2.2: Sifting Procedures Linear Feedback Shift Register (LFSR) Universal Hashing Authentication

Alice and Bob use a generally preshared mystery key in conjunction with the LFSR widespread hashing strategy to verify the authenticity of the premise exchange messages that they send and receive. During the filtering step, three messages are examined for accuracy. In addition, more understated components

• Bob sends Alice a message in which he notifies her of the qubits that he was able to measure accurately and in which he also includes an authentication tag. The amount of key material required for authentication is 64.

• Bob includes an authentication tag in his message and notifies Alice of the bases he has selected for measuring the qubits. Additionally, Bob appends the tag to the message. The amount of key material required for authentication is 64.

• Alice sends Bob a message that includes an authentication tag and details the bases she will use in the preparation of the qubits. In addition, she shares the message with Bob. The amount of key material required for authentication is 64.

D. Reconciliation at the Phase 3.1 level, using Biased Error Estimation

Alice and Bob are using an error estimate plot with just one side. They choose two different irregular test subsets, the first of which includes all of the estimates in which Alice and Bob have both used the rectilinear premise, and the second of which includes just those guesses in which they have used the corner to corner premise. This strategy provides emphasis points with reference to a certain attack, such as the one-sided listening covertly method. They finally utilize the estimated error rate to decide whether or not they should continue to blunder amend or whether or not they should prematurely end the convention based on a predefined error resilience limit, which is generally somewhere around 11%. This limit is utilized to decide whether or not they should continue to blunder amend. In addition, some sites of interest are as follows:

• Alice and Bob must first permute their filtered keys before attempting to flatten the mistakes that are present throughout the whole bit string. After that, they estimate the amount of error by comparing a subset of their error-flattened filtered keys.

• Based on the sampling ratio of 0.1, it was determined that the error rate was 0.0.

E.

Phase 3.2: Error Correction and Cascade in the Reconciliation Process

Alice and Bob carry out a plan known as Cascade, which is an intelligent error amendment plot, on individuals in general direct with the express intention of locating and correcting any incorrect bits in the filtered bit strings of these people. Additional items worth noting are as follows: • The Cascade algorithm was executed for a total of four rounds in order to fix the mistakes.

• The investigation uncovered and fixed two incorrect bits.

• In order to fix the problems, 33 bits were lost throughout the process.

• The Shannon limit for the number of leaked bits is 39.0, which is based on an error probability of 0.0133. This is in comparison to the actual number of lost bits, which is 1. 51. \sF. Error Correction, Confirmation, and Authentication Make Up the Fourth Phase

Alice and Bob authenticate and validate the error correction stage by registering the hash of their error-corrected keys using their commonly preshared mystery key and by looking at their individual summaries. Other noteworthy points include the following: • 64 bits of key material (the preshared secret key) were used to authenticate.

• The authentication process was carried out by using the Linear Feedback Shift Register (LFSR) global hashing algorithm.

G. Phase 5: Enhanced Protection of Personal Information

Alice and Bob analyze the general data spillage and execute a protection improvement convention with the intention of reducing the amount of information that Eve has obtained about the key as a result of her eavesdropping on the channel. They do this by locally using a hashing strategy that encompasses

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 50, Issue 5, No. 1, May 2021

everything in consideration of Toeplitz lattices. The hashing capability will be listed with the help of yet another component of their preshared secret keys. They may also define a safety parameter in order to restrict Eve's learning to a level that is sufficient for her to function independently. Additional nuances include the following:

- As at this moment, 83 bits have been lost due to a leak.
- The length of the key, in bits, before executing the privacy amplification process was 376.
- The total number of bits in the final key is 286.
- The value 20 has been selected for the security parameter.

The following is a graphical depiction of the results obtained by the QKD simulator, as well as the results themselves.:

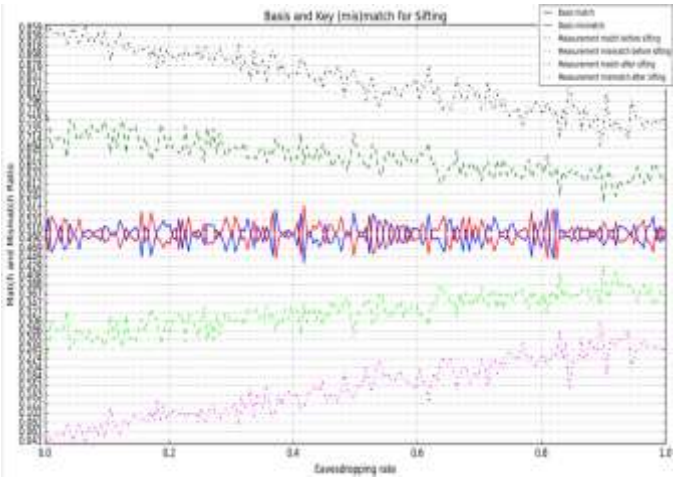

Fig. 1. QKD Sifting Plot

The Fig. 1 shows QKD Sifting Plot generated by QKD simulator. Here matching and mismatching of basis and key, before and after sifting are presented.

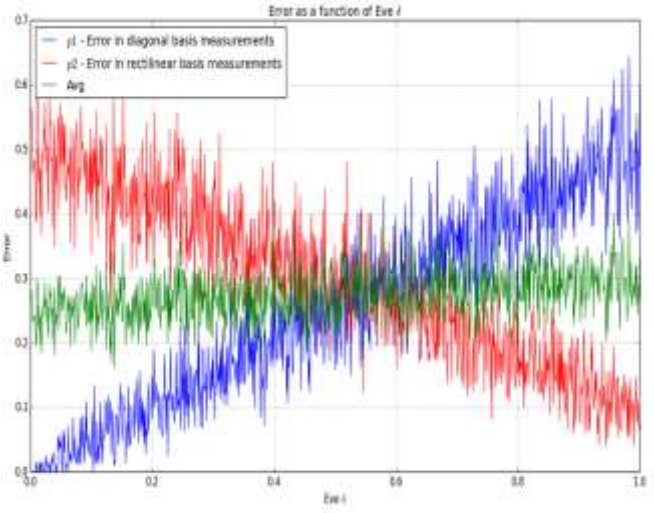

Fig. 2. QKD Biased Error Estimation Plot

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 50, Issue 5, No. 1, May 2021

The Fig. 2 shows QKD Biased Error Estimation Plot generated by QKD simulator. Here probability of error measurement in diagonal, rectilinear basis and average are presented

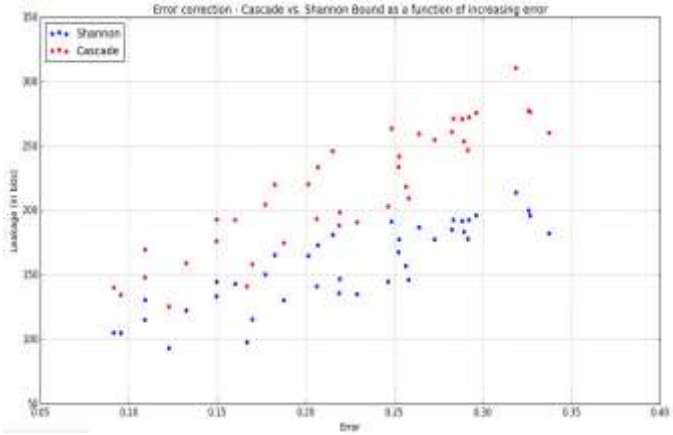

Fig. 3. QKD Shannon Bound vs. Error Correction Plot

The Fig. 3 shows QKD Shannon Bound vs. Error Correction Plot. Here Shannon bound and error correction-cascade as a function changes when leakage changes.

Like the above graphs mentioned in Fig. 1, Fig. 2 and Fig. 3 for each parameter changes simulator generates three graphs like as above. By analyzing all the graphs the following are the statistics of the results.

TABLE I

ALICE/BOB BASIS SELECTION CHANGES AND EVE BASIS SELECTION, EAVESDROPPING RATE KEPT IDLE

Initial number of qubits	Alice/Bob basis selection bias	Information leakage (Total number of disclosed bits)	Key length before error correction	Bit error probability	Bits leaked during error correction	Shannon bound for leakage	Final key length	Estimated error
500	0.1	83	376	0.0133	51	39	273	0
500	0.2	65	315	0.0063	33	18	230	0
500	0.3	125	266	0.0451	93	71	121	0
500	0.4	147	236	0.072	115	89	69	0
500	0.5	126	208	0.0625	94	71	62	0
500	0.6	175	233	0.1073	143	115	38	0.0388
500	0.7	222	264	0.1212	190	141	22	0.04
500	0.8	249	296	0.1318	217	167	27	0.0645
500	0.9	276	375	0.1173	244	196	79	0.1

The above table shows the how information leakage, key length before error correction, bit error probability, bits leaked during error correction, Shannon bound for leakage, final key length and estimated error varies when Alice/Bob basis selection changes from 0.1 to 0.9 and remaining parameters kept constant (Eve basis choice bias delta=0.1, Eavesdropping=1, Eavesdropping rate=0.1, Error estimation sampling rate=0.1, Biased error estimation=1, Error tolerance=0.1). The below figure show the graphical representation of the above table.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 50, Issue 5, No. 1, May 2021

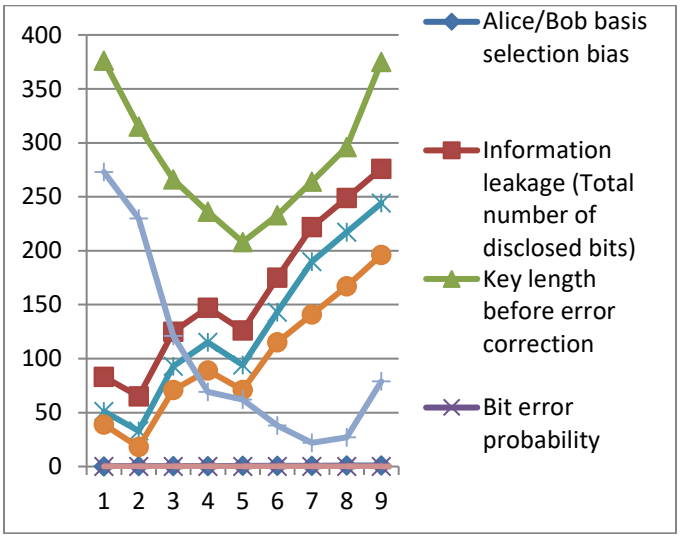

Fig. 4. Alice/Bob basis selection changes and Eve basis selection, Eavesdropping rate kept idle

TABLE II

EVE BASIS SELECTION CHANGES AND ALICE/BOB BASIS SELECTION, EAVESDROPPING RATE KEPT IDLE

Initial number of qubits	Eve basis selection bias	Information leakage (Total number of disclosed bits)	Key length before error correction	Bit error probability	Bits leaked during error correction	Shannon bound for leakage	Final key length	Estimated error
500	0.1	83	376	0.0133	51	39	273	0
500	0.2	78	359	0.0056	46	18	261	0.0256
500	0.3	123	374	0.0294	91	72	231	0
500	0.4	95	364	0.0192	63	50	249	0
500	0.5	106	368	0.0245	74	62	242	0
500	0.6	160	376	0.0452	128	100	196	0.0244
500	0.7	127	365	0.0301	95	72	218	0
500	0.8	168	369	0.0488	136	104	181	0
500	0.9	175	363	0.0523	143	108	168	0

The above table shows the how information leakage, key length before error correction, bit error probability, bits leaked during error correction, Shannon bound for leakage, final key length and estimated error varies when Eve basis selection changes from 0.1 to 0.9 and remaining parameters kept constant (Alice/Bob basis selection=0.1, Eavesdropping=1, Eavesdropping rate=0.1, Error estimation sampling rate=0.1, Biased error estimation=1, Error tolerance=0.1). The below figure show the graphical representation of the above table.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 50, Issue 5, No. 1, May 2021

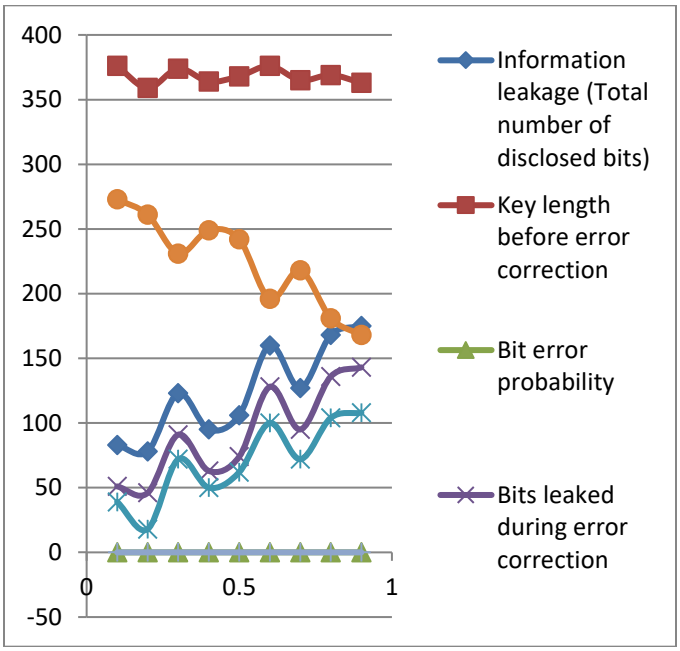

Fig. 5. Eve basis selection changes and Alice/Bob basis selection, Eavesdropping rate kept idle

TABLE III

EAVESDROPPING RATE CHANGES AND ALICE/BOB BASIS SELECTION, EVE BASIS SELECTION KEPT IDLE

Initial number of qubits	Eavesdropping rate	Information leakage (Total number of disclosed bits)	Key length before error correction	Bit error probability	Bits leaked during error correction	Shannon bound for leakage	Final key length	Estimated error
500	0.1	83	376	0.0133	51	39	273	0
500	0.2	85	369	0.0136	53	39	264	0
500	0.3	104	378	0.0212	72	56	254	0
500	0.4	80	370	0.0108	48	32	270	0
500	0.5	169	358	0.0531	137	108	169	0.0256
500	0.6	169	363	0.0523	137	108	174	0.0256
500	0.7	119	373	0.0295	87	72	234	0
500	0.8	159	369	0.0434	127	96	190	0
500	0.9	183	382	0.0602	151	126	179	0.0488

The above table shows the how information leakage, key length before error correction, bit error probability, bits leaked during error correction, Shannon bound for leakage, final key length and estimated error varies when Eavesdropping rate changes from 0.1 to 0.9 and remaining parameters kept constant (Alice/Bob basis selection=0.1, Eve basis selection=0.1, Eavesdropping=1, Error estimation sampling rate=0.1, Biased error estimation=1, Error tolerance=0.1). The below figure show the graphical representation of the above table.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 50, Issue 5, No. 1, May 2021

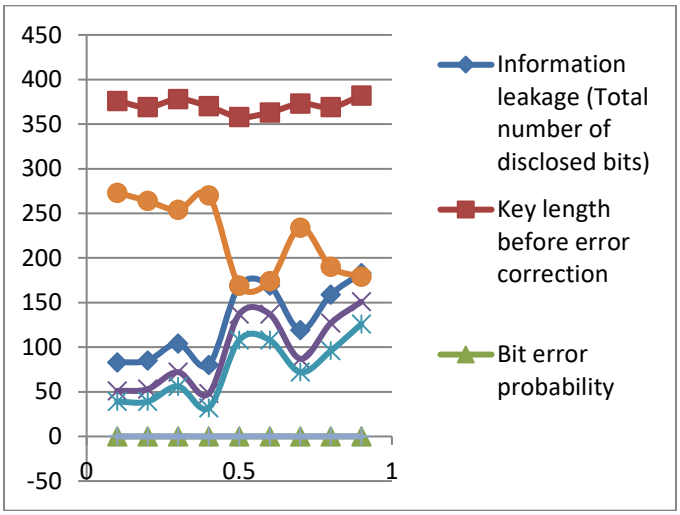

Fig. 6. Eavesdropping rate changes and Alice/Bob basis selection, Eve basis selection kept idle

CONCLUSION

QKD stands for "quantum key distribution," and it is a relatively recent method for the production and distribution of cryptographic keys. As a result, the QKD is presented in this study as an alternative to the conventional key distribution algorithms. It does so by basing its implementation of the QKD simulator on the QKD–BB84 protocol. The approach of quantum key distribution was used in this study for the distribution of the key in e-governance applications. Due to the fact that it needs prior authentication, the findings presented here indicate that the quantum key distribution approach is more secure than the classical key distribution method..

REFERENCES

[1] Louis Salvail1, Momtchil Peev2, Eleni Diamanti3;4, Romain Alleaume4, Norbert L• utkenhaus5;6, Thomas L• anger2. (2009). Security of Trusted Repeater Quantum Key Distribution Networks. nd. 0 (0), p1-29.

[2] Alan Mink, Sheila Frankel and Ray Perlner. (2009). Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration. IJNSA. 1 (2), p101-112.

[3] Z. Walton,1 A.V. Sergienko,1,2 M. Atat¨ure,2 B.E.A. Saleh,1 and M.C. Teich1,2. (2013). Performance of Photon-Pair Quantum Key Distribution Systems. arxiv. 0 (0), p1-6.

[4] Damien Stucki, Gr´egoireRibordy, Andr´eStefanov, Hugo Zbinden. (2008). Photon counting for quantum key distribution with Peltier cooled InGaAs/InP APD's..arxiv. 0 (0), p1-18.

[5] Chi-Hang Fred Fung,1, ∗ Bing Qi,1, † Kiyoshi Tamaki,2, ‡ and Hoi-Kwong Lo1. (2007). Phase-Remapping Attack in Practical Quantum Key Distribution Systems. arxiv. 0 (0), p1-13.

[6] Kiyoshi Tamaki1,2,∗ Norbert L¨utkenhaus3,4, Masato Koashi2,5, and Jamie Batuwantudawe3 1. (2009). Unconditional security of the Bennett 1992 quantum key-distribution scheme with strong reference pulse. arxiv. 0 (0), p1-10.

[7] Norbert L¨utkenhaus. (2008). Security against individual attacks for realistic quantum key distribution. arxiv. 0 (0), p1-11.

[8] Mohamed Elboukhari1, Mostafa Azizi2, and Abdelmalek Azizi1,3. (2009). Integration of Quantum Key Distribution in the TLS Protocol*. IJCSNS. 9 (12), p21-28.

[9] Mehrdad S. Sharbaf. (2009). Quantum Cryptography: A New Generation of Information Technology Sec urity System. IEEE. 0 (0), p1644-1648.

[10]A. Poppe, A. Fedrizzi, R. Ursin, H. R. B¨ohm,T. Lor¨unser, O. Maurhardt, M. Peev, M. Suda,C. Kurtsiefer, H. Weinfurter,T. Jennewein,A. Zeilinger. (2004). Practical quantum key distribution with polarization entangled photons. . 12 (16), p3865-3871.

[11]Tzonelih Hwang, Kuo-Chang Lee, and Chuan-Ming Li. (2007). Provably Secure Three-Party Authenticated Quantum Key Distribution Protocols. IEEE. 4 (1), p71-80.

[12]MontidaPattaranantakul, AroonJanthong, KittichaiSanguannam,ParaminSangwongngam and KeattisakSripimanwat (2012). Secure and Efficient Key Management Technique in Quantum Cryptography Network. IEEE, ICUFN, p1-6.

[13]Hsiao-Ying Lin and Wen-GueyTzeng. (2012). A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding. IEEE. 23 (6), p995-1003.

[14]Charles Ci Wen Lim, Christopher Portmann, Marco Tomamichel, Renato Renner, and Nicolas Gisin. (2013). Device-Independent Quantum Key Distribution with Local Bell Test. American Physical Society., p1-11.

[15]Jordan S. Cotler and Peter W. Shor. (2013). A New Relativistic Orthogonal States Quantum Key Distribution Protocol. Arxiv. 0 (0), p1-6.

[16]Michele Mosca, Douglas Stebila and BerkantUstaoglu. (2012). Quantum Key Distribution in the Classical Authenticated Key Exchange Framework. IEEE. 0 (0), p1-17.