Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 65 (2015) 701 – 710

Procedia Computer Science

International Conference on Communication, Management and Information Technology (ICCMIT 2015)

Quantum Key Distribution: Simulation and Characterizations

Omer K. Jasim[a]*, Safia Abbas[b], El-Sayed M. El-Horbaty[b] and Abdel-Badeeh M. Salem[b]

[a]*Ph.D. student, Al-Ma'arif University College, Anabr, +964, Iraq*

[b] *Faculty of Computer and Information Sciences, Ain Shams University*

Abstract

All traditional cryptographic algorithms used in the network communication environments, relied on mathematical models and computational assumptions, are actually unsafe and apt by many attackers (quantum and man-in-the-middle attacks). Therefore, nowadays Quantum Key Distribution (QKD) promises a secure key agreement by using quantum mechanical systems. QKD becomes a significant trend of new cryptographic revolution. This paper explains how cryptography exploits the quantum mechanics in order to achieve an encryption/decryption process. Additionally, this paper provides a standard simulation for QKD-BB84 protocol and describes improvement key generation and key distribution mechanisms. Then, validation, results and efficiency of BB84 protocol are presented using different security configurations. Finally, our results indicated that the QKD is susceptible to corporate with different security applications and achieve the key availability for such applications. However, it suffers from the higher rate of authentication cost.

Peer-review under responsibility of Universal Society for Applied Research

Keywords: QKD, BB84, Key distribution, qubit, secure communication, encryption/decryption algorithms.

1. Introduction

The term of secure communication is an abstract concept that can cause serious problems during the measurement, transmission and computation processes [1]. In this era, secure communication environments are required by the masses and huge companies in order to guarantee a secure exchange of their data through open environment [2]. Thus, most of them are relied on Public Key algorithms (PK) thinking of them; it is reliable and secure.

* Corresponding author. Tel.: +2-01154567015;
E-mail address: omer.k.jasim@ieee.org

Peer-review under responsibility of Universal Society for Applied Research
doi:10.1016/j.procs.2015.09.014

Although PCKs', especially with large and randomly generated keys, are safe and trust within the context of current technology. However, they can well become invalid when extremely high-performance quantum computers come into actual existence and adopt [3, 4]. A quantum algorithm with polynomial time for factorization has already been discovered and applied [5]. Therefore, if quantum computers become a reality, PCKs would become obsolete.

In order to such adversity, will be coming from the quantum computer, QKD is an excellent solution for that. Theoretically, QKD provides an unconditional security (achievable only when the key length is same as message length [4] which are missing from computational security (cryptosystem based on a mathematical model). Furthermore, QKD depending on quantum mechanics in order to make sure that any measurement modifies the state of the transmitted quantum bits (qubit). This modification can be detected by the sender (Master) and the receiver (Slave) of the quantum bits.

Currently, key distribution and management algorithms can establish a shared secret key over an insecure classical communication channels [5]. The security of these algorithms based on the fact that successful eavesdropping requires excessive computational effort (computational security). QKD brings an entirely new way of solving the key distribution problem. It provides secure key distribution via the laws of quantum mechanics [6]. In addition, several protocols support the QKD system to be viable such as Bennett and Brassard-1984 (BB84), Eckert -1991 (E91) and Bennett-01992 (B92) [4, 5, 6].

This paper presents a holistic simulation that simulates a QKD by utilizes the BB84 protocol with different configurations (noise level, length of initial qubits and attack influence). Many features led to based BB84 protocol, such as a higher bit rate (up to 6 Mbps), secure up to 140 KM and resistance against Photon Number Splitting (PNS) and Man-in-the-middle (MITM)attacks[7]. Also, this paper presents an analytical analysis for the obtained results and discusses the QKD usage and integration susceptibility with other security applications (algorithms).

The rest of the paper is organized as follows: Section 2 surveys the recent studies that focused on QKD simulation and improvement. QKD concept and protocol are given in Section 3. Section 4 illustrates the experimental setup for the QKD-BB84 protocol. Experimental results are resolved from the experimental environment, and discussions are presented in Section 5. Section 6 presents the conclusion and future works.

2. Related Works

Newly, QKD is a new emerging technology for protecting sensitive data during transmission process in a new communications environment. So, many researchers have focused on the simulation of QKD to achieve a secure communication for files depending on different simulator environments.

Mohsen S.and Hooshang A.[6] reviewed a modification to the BB84 protocol that is logically claimed to increase its efficiency. They are presented the simulation of BB84 and discussed the results. Moreover, the authors improved such protocol and showed that the efficiency of the improved version without undermining the security level of BB84 protocol.

Amrin M. et al. [7] proposed an algorithm that gives a solution to MITM attack in BB84. It uses computational security algorithms and chooses another algorithm for generation key from image algorithm. By using these two keys, computational key and Information theoretic key, both will constitute hybrid key and use it for further communication. This proposed system doesn't offer offline key establishment and scalability.

Sufyan T. and Omer K. [8] presented the integration of the techniques of unconditionally secure authentication from classical cryptography with QKD. The output of such integration is a two-party authenticated quantum key distribution protocols (based on BB84) that takes care of the problem are associated with above studies and reducing the authentication cost. As far as the phases constituting each QKD session are concerned, two modes of authentication have been considered: "partial" authentication and "full" authentication modes. The proposed authentication modes, especially the full mode, are effected on the efficiency of such QKD system.

Hui Q. and Xiao Ch. [9] employed the BB84 protocol as the basic model of QKD in depolarization channel. Also, they are presented the simulation of QKD protocol using MATLAB simulator. The simulation results are consistent with the theoretical results. A sufficient analysis for the obtained results in this study is weak.

Marcin N. and Andrzej R. [11] described a new concept of security measurement in QKD and proposed a new concept of entropy of security in QKD and a unique measure of security be defined. Authors presented two different security levels, the basic security level and the advanced security level. This differentiation of security helps to choose the appropriate security level for specific end-users' requirements and needs. However, the authors did not test the strength of the developed system against intrusion attacks.

Finally, Table 1. summarizes all above surveys paper and explains the objective, scope of study and pros and cons for each one.

Table 1. Existing studies for QKD simulation and development

Authors, ref. and Year	Proposed Tech.	Advantage	Disadvantages
Mohsen S. Hooshang A. [6, 2007]	a new version of BB84	Increase the length of quantum key	Long time of key generation
Amrin M. et al. [7, 2013]	Hybrid key (security image and BB84)	Avoid the MITM attack	doesn't offer offline key establishment and scalability
Sufyan T. and Omer K. [8,2010]	A standard simulator for QKD environment	Reducing the authentication cost(key availability	Decrease the efficiency of proposed system.
Hui Q. and Xiao Ch. [9, 2009]	BB84 through depolarizing channel	It nears to real environment	Weak in result analysis
Marcin N. and Andrzej R. [11, 2012]	A new security measurement in QKD	appropriate security level for specific end-users'	ambiguity resistance against attacker

3. QKD: Concept and Protocol

QKD is used to distribute an encryption key for symmetric and asymmetric ciphers, and it is not to transmit any plain data between communication parties (usually called master and slave). In this era, a lot of QKD protocols have been created, nevertheless, few are used in practice [8]. The QKD is merely used to negotiate secret quantum keys among parties through two communication channels, classical and quantum channels, like Unshielded Twisted Pair (UTP) and fiber optic channels. In a sense, QKD comes as an alternative to the existing "public/secret key distribution system.

The first invented protocol was BB84 [9]. This protocol, based on photon polarization (states aided to transmit classical information over a quantum channel), is the most reputable solution in practice quantum cryptographic environment. Others protocol, such as B92 or E91 are modified versions of the BB84 protocol. Both communication parties must have devices or simulators that can generate and detect pulses of light in different polarization. As shown in figure1, secure privacy of the BB84 protocol stemmed from encoding the classical information in non-orthogonal states (vertical-V, horizontal-H, left diagonal-LD and right diagonal-RD, for more details about photon polarization computing see [9, 10]). The characteristic of quantum physics, the state cannot be measured without discarding or disturbing it, is a central feature that bolstered the strength of quantum cryptographic key [11].

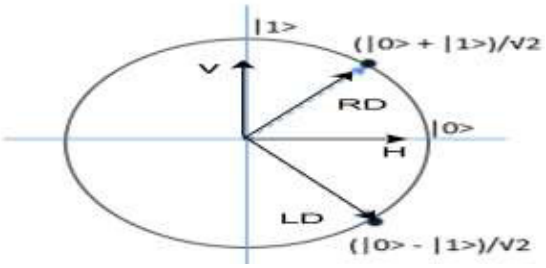

Fig. 1. Photon states (P_s) – orthogonal sate

In order to generate a secret quantum cryptographic key depending on BB84 protocol, two primary phases must be implemented.

- Transmission: a qubit randomly selected and sent based on photon polarization (Master side).
- Negotiation: two communication parties check the degree of compatibility between their key obtained. In order to produce a final secret key in this phase, four primary stages must be achieved. These stages are:

3.1. Raw Key Extraction (RK)

The central purpose of RK is to eliminate all possible errors which occurred through qubits discussion over a quantum channel. Negotiated communication parties compare their photon polarizations are selected, then, non-valent qubits will be eliminated, otherwise, the qubit will be considered [4,8].

3.2. Error Estimation (EE)

The negotiation process is to resolve a quantum key might occur over a noisy-unsecured classical channel. Such channel can cause a partial key damage or unmet conditions due to physical noise of transmission medium.Therefore, in order to avoid this dilemma, both master and slave determine an error threshold value "E_{max}" when they are sure that there is no attacks on transmission medium. Then, after each QKD round, they compare some qubits of their RK in order to compute a transmission error rate "E". In a nutshell, if $E > E_{max}$ they can be sure about existence of an attack [9].

3.3. Key Reconciliation (KR)

In case of $E \leq E_{max}$, errors might/can be found within the non-valent parts of the raw key. KR is provided to minimize those errors within the key as possible. This stage consists of a number of sub-stages. Such dividing the raw key into blocks of length K bits, computing the parity bits for each block and parity comparison [12]. Finally, those sup-stage are repeatedly executed by communication parties for N number of rounds.

3.4. Privacy Amplification (PA)

PA is the final stage of quantum key extraction protocol (BB84) which applied to minimize the number of bits that an attack might know the raw resolved key from KR [10, 11]. Communication parties apply a shrinking method to their qubits sequences in a way that reduces the authentication cost and reduces an attacker presence [12].

4. Experimental Environment

In order to create an innovative system capable to simulate the processes of QKD system and quantum computation, the illustration and description of physical processes must be achieved. Any process of quantum mechanics can be depicted as an operator (operator is formalized as multiplication by a matrix). Consequently, the logic gates (circuits), embrace the operator as a square matrix, are given in matrices of vectors. Drastically, matrices illustration is a delightful topic in scientific quantum computing. Furthermore, many tools and random algorithms are considered in the simulation of QKD.

Generally, Master and Slave must be guaranteed an acceptance secure communication without the presence of the attack. Consequently, in order to obtain the quantum cryptographic key, two communication parties going to be executed the stages of the QKD-BB84 (RK, EE, KR and PA).

As shown in figure 2, the main hardware requirements for the deployment of BB84 simulation are at least two computers machines connected by switches. Each machine has a static IP (computer join to domain) to communicate over the switch and on each machine will implement assigned software (Master, Slave). The simulation is performed using a Core i5 (4.8 GHz) processor associated with 8GB of RAM as a Master hardware and a Core i3 (2.4 GHz) processor associated with 4GB of RAM as a Slave hardware.

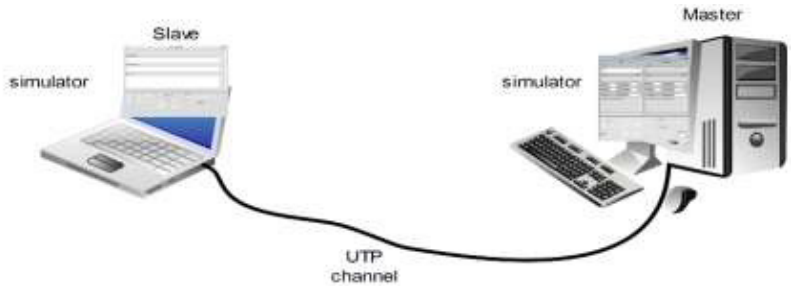

Fig. 2. Experimental environment for QKD –BB84

In addition, Figure 3 shows the main parameter for system development (simulation environment) such as states, mathematics operations, randomness algorithms, etc.

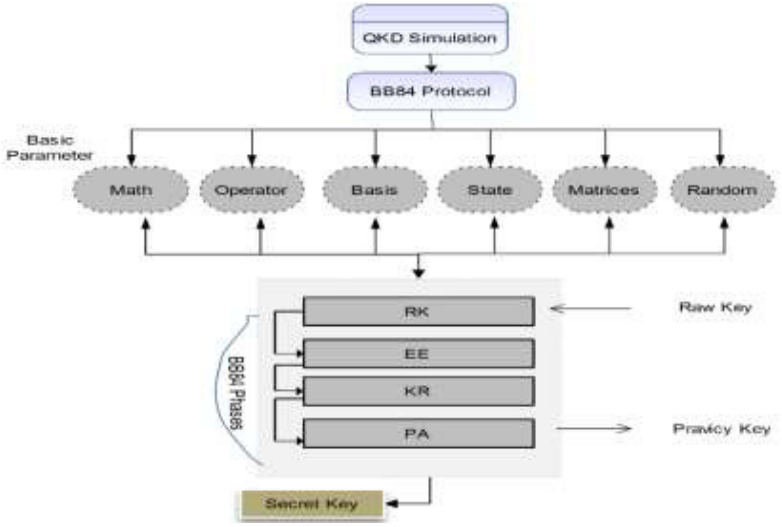

Fig. 3. Main diagram for QKD simulator: basic parameters and key distillation phases

The availability of these parameters in our simulator gives the tester an insight look and experience of BB84 protocol work. The procedure of the BB84 protocol simulation is illustrated as follows:

- Master sends to slave a sequence of random photon states (independently chosen),
$$P_s = \{p_0, p_1, p_2, \dots, p_n\}, where\ P_s \in \uparrow, \rightarrow, \nearrow\ and\ \nwarrow.$$
- For each photon deployed bases (P_b), Slave randomly selected one of two measure of $P_b = (\times, +)$.
- Master and Slave eliminate all non-valent bases.
- Master and Slave compute the error percentage (E_r), and compare with threshold (E_t)
$if\ E_r \leq E_t$, go to the next step, otherwise, aborting negotiation.
- Master and Slave obtained a series of an initial qubit, according to photon measurement and coding [].
$$S_n = \{inqubit_0, inqubit_1, inqubit_2, \dots, inqubit_n\}$$
- Master and Slave perform (KR) phase, through
  - Divide the intimal series into number of blocks (b)
  $$B_n = \{b_0, b_1, b_2, \dots, b_n\}$$
  - Compute the parity bit for each two block which has even location or odd location
  $$P_{i=0}^{i=n} = b[i]$$
- Master and Slave perform PA, in order to generate a series of final secret key (Sk).
$$S_k = \{sk_0, sk_1, sk_2, \dots, sk_n\}$$

Finally, this proposed simulator is programmed using Visual Studio Ultimate 2012 (VC#) based on Windows Server 2012 Data Center as an operating system. As shown in figure 4, the main system GUI has many configurations options that strive to make our simulator nears in real environment.

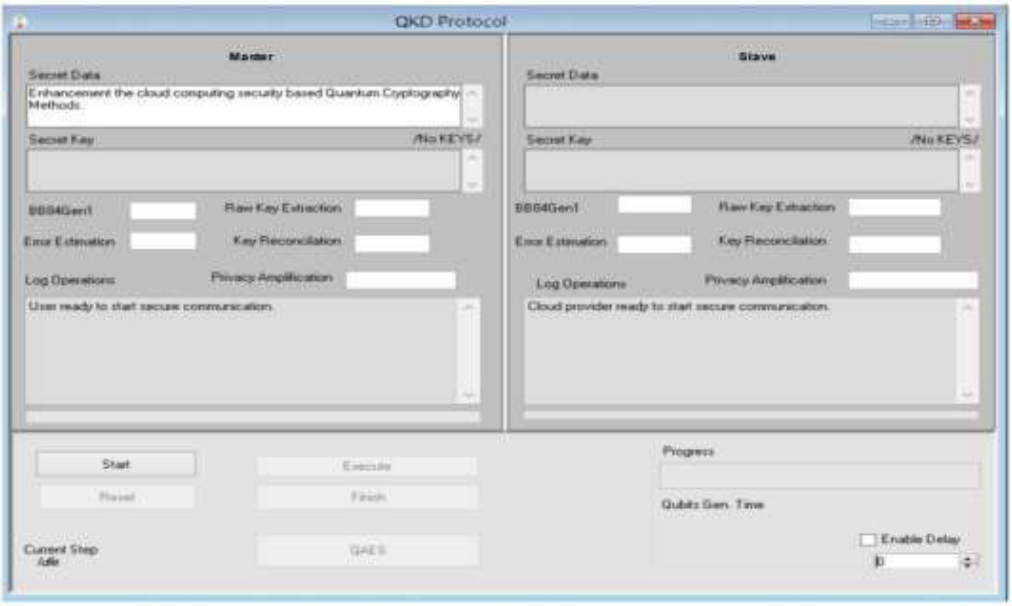

Fig. 4. Main screen of proposed QKD system

5. Results and Discussion

This section demonstrates the experimental results of the developed simulator based on the precise hardware specification with different configurations (such as length of initial qubits are pumped, noise level and attack influences). Moreover, analytical analysis and QKD usage are discussed in the following sections.

5.1. Analytical analysis

This subsection discusses the experimental results are obtained in our simulator environment. Figure 5 illustrates that the simulator reflects the number of qubits resolved at each phase of the QKD phases, in qubits, gained by two communication parties where the noise level assigned to 0.5 GHZ without attacking. This figure reveals the simulator is starting from 5000 (an initial qubit) up-to 20000 qubits and it shows the variance of the obtained results when different numbers of qubits are deployed.

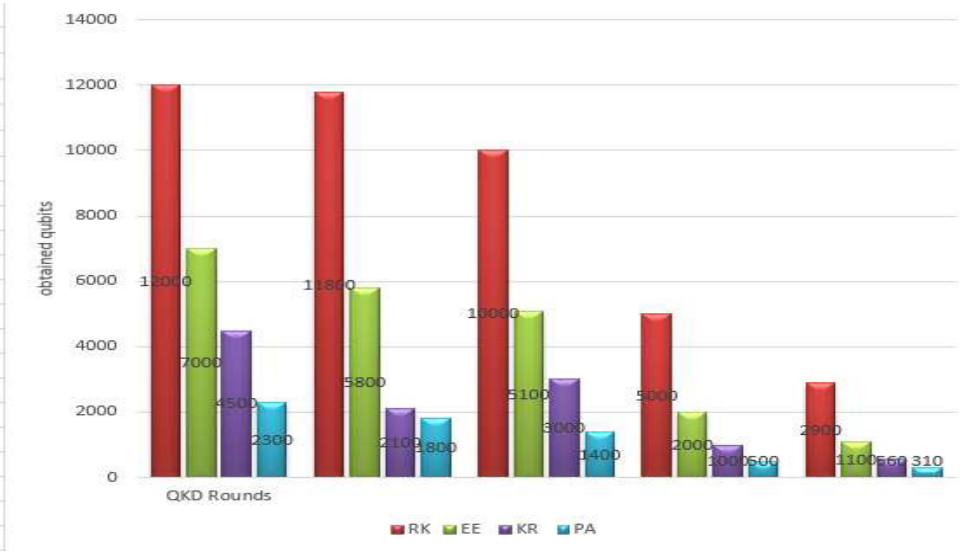

Fig. 5. Resolved qubits - configuration level: Nr= 0.5 GHZ and attack effect=0.0 GHZ

Regarding figure 5, at round 1(5000 qubits are pumped), the RK holds 2900 qubits, which in turn are processed till the PA phase to succeed 310 qubits. The obtained qubits reduction has occurred during the key distillation phases (EE, KR and PA), and the lost qubits are usually known as the authentication cost [8].

While, figure 6 shows the length of secret keys are obtained with a new optional configurations, noisy rate (N_r) and influence of attacks set to 0.5 GHZ. In a sense, when the 5000-qubits are deployed as initial qubits, 2100-qubits are provided.

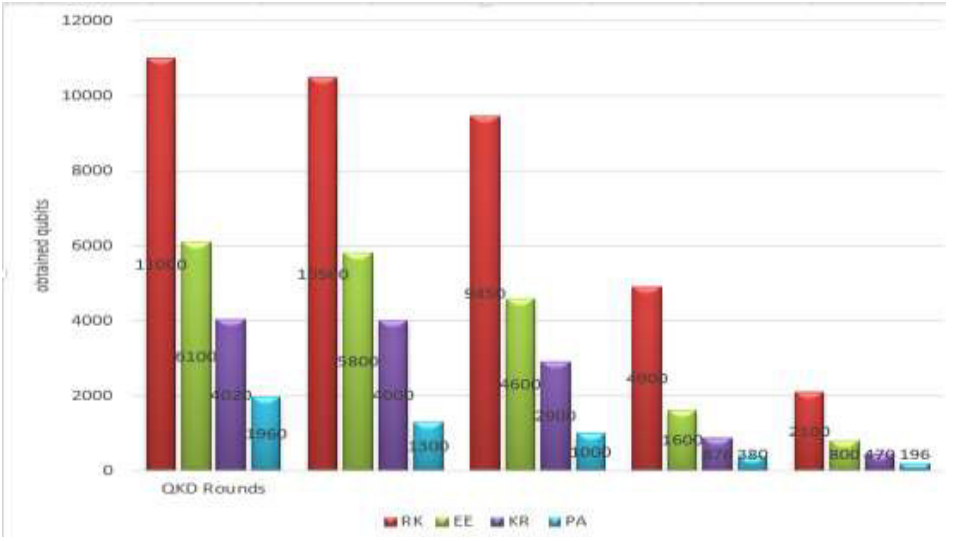

Fig. 6. Resolved qubits –configuration level: Nr=0.5 and attack effect=-0.5

Generally, the quantum bit error rate (QBER) between the initial qubits are pumped and the RK extraction is 26.1% when the Nr set to 0,5 GHZ without the presence of eavesdroppers. That's mean, just 7% is the ratio of the final secret key has been obtained (relation between initial qubit and PA). On the other side (Nr=0.5, attack influence =0.5), the QBER between initial qubits and the RK extraction is 54%. This ratio indicates just 3% is the ratio of the final secret key has been obtained. Now, we can conclude from above:

- The influences such as unexpected noise, attack intrusion, and key distillation phases are considered as the main reason beyond the authentication cost issue.
- Any change in the value of configuration levels (increasing or decreasing) direct impact on the length of the secret key and the time of generation it.

5.*2 QKD Usage*

As noted above, the process of quantum key generation mainly depends on deploying photons' between two communication parties over limited distances (314-kilometer) [2, 3]. Such distance limitation considered as a big problem for authors and organizations, also, it effects on the technology adopted in the real world of network communications. Accordingly, to overcome this obstacle, NIST and DIEHARD suites have been implemented in order to examine and to evaluate the randomness rates for final resolved qubits based on the p-values. Regarding [1], the P-value indicates the true randomness of the qubits generation and periodically changed with the rounds' contents. The randomness characteristic helps to adopt the QKD as a source to generate a random number that used with various encryption algorithms (key session). So, this feature helps to adopt the quantum technology, as an excellent source of generating random numbers see figure 7.

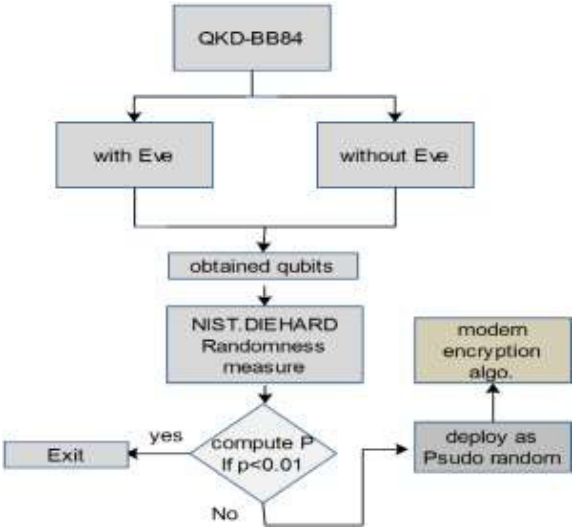

Fig.7. QKD integration capability (randomness property)

In order to assure the strength of such keys, Omer et al [4] developed a new version of the symmetric AES integrated between cryptographic quantum key and traditional AES. Such developed algorithm guarantees an unconditional security level [8] for any cipher system built on symmetric encryption algorithms [for more details see [4]].

6. Conclusion and Future Works

QKD is a new emerging technology for cryptographic key generation and distribution. Accordingly, this paper presents the QKD as an alternative for the traditional key distribution protocols. It implements the QKD –BB84 protocol using two different modes, with/without attack influences, based on a holistic simulation (experimental and real simulator).

After then, the obtained results associated with various configurations, such as length of an initial qubit, noise level and attack influences, are discussed. Such configurations show direct effects on the length of the obtained key and the time needed for the key generation. Finally, the paper reveals that the QKD has the capability to integrate with different security applications or modern encryption algorithms.

In the future, a new version of BB84 protocol will be developed and implemented with two different communications modes, offline and online modes.

Acknowledgements

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions that improved the presentation of this paper.

References

1. Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem, "Statistical Analysis for Random Bits Generation on Quantum Key Distribution", 3rd IEEE- Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec2014), ISBN: 978-1-4799-3905-3 ©2014 IEEE, Faculty of Engineering - Lebanese University, April 2014,pp. 45-52.
2. http://www.queenslandrail.com.au/NetworkServices/DownloadsandRailSystemMaps/Freight/Pages/WestMoretonSystem.aspx
3. G., An Experimental Implementation of Oblivious Transfer in the Noisy Storage Model, Nature Communications Journal Vol. 5, No. 3418,2014.
4. Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem, "Advanced Encryption Standard Development Based Quantum Key Distribution", the 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), UK, Dec.,2013, pp.536-541.
5. Matthew P., Caleb H., Lamas L., Christian K., Daylight operation of a free space, entanglement-based quantum key distribution system, Centre for Quantum Technologies, National University of Singapore, 2008.
6. Mohsen Sharifi1 and Hooshang Azizi, A Simulative Comparison of BB84 Protocol with its Improved Version, JCS&T Vol. 7 No. 3, 2007.
7. AmrinBanu M. Shaikh, Parth D. Shah, BB84 and Identity Based Encryption (IBE) Based A Novel Symmetric Key Distribution Algorithm, Fifth International Conference on Advances in Recent Technologies in Communication and Computing, ARTCom, 2013
8. Sufyan T. Faraj Al-Janabi, Omar Kareem Jasim," Reducing the Authentication Cost in QuantumCryptography",http://www.cms.livjm.ac.uk/pgnet2011/Proceedings/Papers/m1569449 157-al-janabi.
9. Hui Qiao, Xiao-yu Chen, Simulation of BB84 Quantum Key Distribution in depolarizing channel, Proceedings of 14th Youth Conference on Communication, 2009.
10. Rishi Dutt Sharma , Asok De, A New Secure Model for Quantum KeyDistribution Protocol, 6th International Conference on Industrial and Information Systems, ICIIS 2011, Aug. 16-19, 2011, Sri Lanka
11. Marcin Niemiec and Andrzej R. Pach, The measure of security in quantum cryptography, IEEE Global Communications Conference (GLOBECOM), 967 - 972,2012.
12. Omer Abd Al Kareem Jasim, Anas Ayad Abdulrazzaq, The Goals of Parity Bits in Quantum Key Distribution System, International Journal of Computer Applications (0975 – 8887) Volume 56– No.18, 2012.