International Journal of Engineering Science Invention Research & Development; Vol. I Issue XI May 2015
www.ijesird.com e-ISSN: 2349-6185

STUDY OF BB84 PROTOCOL USING QKD SIMULATOR

K.Elampari[1], B.Ramakrishnan[2]
[1]*Department of Physics,* [2]*Department of Computer Science, S.T. Hindu College, Nagercoil, India-629002.*
[1]elampari@gmail.com,[2] ramsthc@gmail.com

Abstract- **The field of cryptography provides the tools to protect sensitive information from unauthorised parties. The next level is the development of quantum cryptography which provides a very high security through the incredibly successful laws of quantum mechanics. In this paper, a popular quantum key distribution protocol BB84 is studied using a web based QKD simulator.**

Keywords: **Quantum Cryptography, QKD simulator, BB84 Protocol**

1. INTRODUCTION

The rules of quantum physics play a major role in the field of cryptography. Quantum cryptography or quantum key distribution (QKD) applies fundamental laws of quantum physics to guarantee secure communication between two legitimate users, commonly named Alice and Bob. It is used to produce a shared secret random bit string, which can be used as a key in cryptographic applications, such as message encryption and authentication. Unlike conventional cryptography, whose security often relies on unproven computational assumptions, QKD promises unconditional security based on the fundamental laws of quantum mechanics [1]. The key problem which is solved by using quantum techniques is that of eavesdropping detection. Thus the unique contribution of quantum cryptography for secure communication is it provides a new mechanism enabling the parties communicating with one another to automatically detect eavesdropping. Consequently, it provides a means for determining when an encrypted communication has been compromised [2].

There are basically two types of quantum key distribution schemes elaborately discussed in the literature. The first is the prepare-and-measure scheme. The BB84 [3], in which Alice sends each qubit in one of four states of two complementary bases, B92 [4] in which Alice sends each qubit in one of two non-orthogonal states, six-state [5] in which Alice sends each qubit in one of six states of three complementary bases fall under the first category. The second is the entanglement based QKD, such as Ekert91 [6] in which entangled pairs of qubits are distributed to Alice and Bob, who then extract key bits by measuring their qubits, BBM92 [7] where each party measures half of the EPR pair in one of two complementary bases.

2. QKD SIMULATION PROCESS

A fundamental truth about QKD technology is that, because of the limitations of technology, it is impossible to build the ideal system described in theory [8]. Therefore, A practical way to testing the actual hardware is to develop a simulation capability that can accurately model a wide variety of existing and proposed QKD implementations and generate the analysis needed. In this paper, the (BB84) first scheme is taken for simulation studies. Two channels, quantum channel and classical channel are used for the QKD procedure (Fig.1). A series of polarized photons representing the key bits are sent to the receiver with designed QBER (Quantum Bit Error Rate) using the quantum channel. The classical channel is used to recover the final key by removing errors introduced during key transmission which includes eaves dropping. The final key recovery stage using classical channel consists of four important processes namely i. Sifting ii. Error Estimation, iii. Reconciliation, and iv. Privacy Amplification. In this work simulation analysis has been conducted to estimate error rate of the BB84 protocol for various input configurations using a QKD simulator developed by Arash Atashpendar [9].

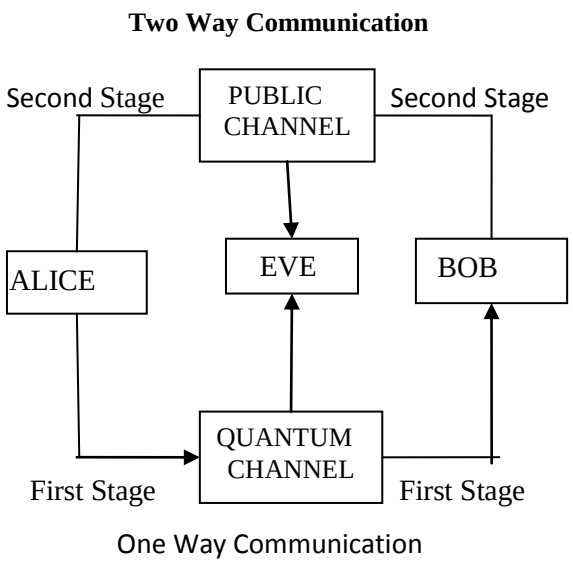

Fig.1. A quantum Cryptographic Communication System

3. RESULTS OF QKD SIMULATOR RUNS

Detailed run information for a particular case with the initial configuration shown in Table 1. is described in section 3.1. The results of the simulation runs are presented in Table 2.

3.1 PHASE 1: BB84 QUANTUM TRANSMISSION

The BB84 protocol uses two sets of non-orthogonal coordinate systems, which are the usual *x–y* (rectilinear) basis and the diagonal basis which is the rectilinear basis rotated by 45 degree. In the rectilinear basis, the qubit can be either in the horizontal *(0 degree)* or in the vertical *(90 degree)* polarization state. In the diagonal linear basis, the qubit can be either in the diagonal (45 degree) or in the anti-diagonal (-45 degree) polarization state.

Alice prepares a sequence of 500 qubits and send them to Bob over the quantum channel. She randomly chooses a basis for each qubit, rectilinear polarization (horizontal -0 degree and vertical -90 degrees) or a diagonal polarization (+45 degrees and -45 degrees shifted). She then maps horizontal and vertical with the qubit states |0> and |1>, and +45 degrees and -45 degrees shifted with the states |+> and |->, respectively.

Further details:

- Alice sent 500 qubits to Bob with a basis selection bias of 0.5.
- Eve is eavesdropping on the quantum channel at a rate of 0.1 and with a basis selection bias of 0.5. There is an eavesdropper, Eve, listening in on the channel. She intercepts the qubits, randomly measures them in one of the two mentioned bases and thus destroys the originals, and then sends a new batch of qubits corresponding to her measurements and basis choices to Bob. Since Eve can choose the right basis only 50% of the time on average, about 1/4 of her bits differ from those of Alice.

3.2 PHASE 2.1: SIFTING

Bob announces on a public classical channel the qubits that he has managed to successfully measure. Alice and Bob 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.

Further details:

- The sifting phase started with 500 transmitted qubits and the resulting bit string was reduced to 242 bits.
- 0.484 of Alice's and Bob's chosen measurement bases match. 0.516 of their chosen bases do not match.
- 0.734 of the two parties measured qubits match before sifting and 0.266 of them do not.
- 0.9298 of the two parties measured qubits match after sifting and 0.0702 of them do not.

3.3 PHASE 2.2: SIFTING AUTHENTICATION - LINEAR FEEDBACK SHIFT REGISTER (LFSR) UNIVERSAL HASHING

Alice and Bob authenticate their basis exchange messages using the LFSR universal hashing scheme and a mutually preshared secret key for authentication. 3 messages are authenticated in the sifting phase.

Further details:

- Bob informs Alice of the qubits he managed to successfully measure and he appends an authentication tag to his message. Authentication cost in terms of key material: 64
- Bob informs Alice of the bases he has chosen for measuring the qubits and he appends an authentication tag to his message. Authentication cost in terms of key material: 64
- Alice informs Bob of the bases she has chosen for preparing the qubits and she appends an authentication tag to her message. Authentication cost in terms of key material: 64

3.4 PHASE 3.1: RECONCILIATION - ERROR ESTIMATION

Alice and Bob 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%.

Further details:

- Alice and Bob permute their sifted keys in order to flatten the errors across the entire bit string. They then perform the error estimation by comparing a subset of their error-flattened sifted keys.
- An error rate of 0.0833 was estimated using a sample size of 24 given a sampling ratio of 0.1

3.5 PHASE 3.2: RECONCILIATION - ERROR CORRECTION, CASCADE

Alice and Bob perform an interactive error correction scheme called Cascade on the public channel in order to locate and correct the erroneous bits in their sifted bit strings.

Further details:

- Cascade was run 6 rounds in order to correct the errors.
- 15 erroneous bits were detected and corrected.
- 104 bits were leaked in order to correct the errors.
- With an error probability of 0.0688, the Shannon bound for the number of leaked bits is: 79.0, compared to the actual number of leaked bits: 104.

3.6 PHASE 4: ERROR CORRECTION CONFIRMATION AND AUTHENTICATION

Alice and Bob confirm and authenticate the error correction phase by computing the hash of their error corrected keys using their mutually preshared secret key and by comparing their respective digests.

Further details:

- 64 bits of key material (preshared secret key) were used to authenticate.
- The Linear Feedback Shift Register (LFSR) universal hashing scheme was used for authentication.

3.7 PHASE 5: PRIVACY AMPLIFICATION

Alice and Bob compute the overall information leakage and run a privacy amplification protocol in order to reduce/minimize Eve's knowledge gained on the key by having eavesdropped on the channel. They do so by locally applying a universal hashing scheme based on Toeplitz matrices. The hashing function will be indexed using yet another chunk of their preshared secret keys. They can also define a security paramter to minimize Eve's knowledge to an arbitrary amount.

Further details:

- 136 bits were leaked up to this point.
- The key length before running privacy amplification: 218 bits.
- The final key length is: 62 bits.
- The chosen security parameter is: 20

Similar runs have been conducted for different input configurations and the consolidated result is depicted in the Table 2.

4. ERROR ESTIMATION

If the quantum cryptography protocol is designed properly, the presence of the eavesdropper is revealed by an increase of the error rate in the bits that are being transmitted from sender to receiver [10]. The simulation study show that the increase in the eavesdropper rate from 0.1 to 0.25 increase the error rate from 0.036 to 0.0963 for 2750 qubits and from 0.0479 to 0.106 for 3000 qubits respectively Quantum Bit Error Rate – QBER method involves

calculating the percentage of errors in the final key [11] , obtained at the end of quantum transmission, after Bases reconciliation stage.

Quantum bit error rate is defined as

QBER = (Qi- Qf) /Qi *100

where Qi represent the number of qbits from primary key and Qf represent the number of qbits from final key.QBER method relies on the fact that the eavesdropper will create an increase in the QBER value. In this study, for Qi= 2750 with Eavesdropping rate =0.1 the QBER is = 0.7930 and the QBER is increased to 0.855 with eavesdropping rate of 0.25.

6. CONCLUSION

In the process of communication, the challenge is preventing unauthorised parties from spying on the communication. In QKD the exchange of information is showed secure in very physically powerful sense using the laws quantum mechanics. In this study, the BB84 protocol is studied using a QKD simulator and the results obtained were in coherence with the theoretical concepts.

ACKNOWLEDGEMENT

The authors greatly acknowledge Arash Atashpendar and Peter Y. A. Ryan , University of Luxembourg, for allowing to use the QKD toolkit for this study.

REFERENCES

[1] Xiongfeng Ma, "*Quantum Cryptography:from theory to Practice*", arXiv:0808.1385, University of Toronto,2008.

[2] Lomonaco, Samuel J., "*A quick glance at quantum cryptography*", Crypologia, Vol.23, No.1, January, 1999, pp1-41.

[3] Bennett C.H, and G. Brassard. "*Quantum cryptography: Public key distribution and coin tossing*" in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, pages 175–179, Bangalore, India, 1984. IEEE, New York.

[4] Bennett.C.H., "*Quantum cryptography using any two nonorthogonal states*", *Phys. Rev. Lett.* , 68:3121, 1992.

[5] Bruss.D, "*Optimal eavesdropping in quantum cryptography with six states*", *Phys. Rev. Lett.* , 81:3018, 1998.

[6] Ekert.A.K., "*Quantum cryptography based on bell's theorem*", *Phys. Rev. Lett.* ,67:661, 1991.

[7] Bennett, C.H G. Brassard, and N. D. Mermin. "*Quantum cryptography without bells theorem*", *Phys. Rev. Lett.*, 68:557, 1992.

[8] Jeffrey D. Morris, Douglas D. Hodson, Michael R. Grimaila, David R. Jacques, Gerald Baumgartner, "*Towards the Modeling and Simulation of Quantum Key Distribution Systems*", International Journal of Emerging Technology and Advanced Engineering, Vol.4, Issue 2, 2014.

[9] Arash Atashpendar , "*A Software Simulation Toolkit for Quantum Key Distribution and Information Leakage*", Masters thesis,University of Luxembourg, 2014.

[10] Shuang Zhao and Hans De Raedt, "*Event-by-Event Simulation of Quantum Cryptography Protocols*", Journal of Computational and Theoretical Nanoscience Vol.5, 490–504, 2008

[11] Anghel.C, "*Research, Development and Simulation of Quantum Cryptographic Protocols*", Elektronika Ir Elektrotechnika,Vol. 19, No. 4, 2013.

Table 1. Initial Configuration

Property Qubit Count	Basic choice bias delta	Eave Basic choice delta	Eavesdropping	Eavesdropping rate	Error estimation Sampling rate	Biased Error estimation	Error tolerance
500	0.5	0.5	1 (enabled)	0.1	0.1	0	0.13

Table 2. Test Runs

Property	Value											
Initial number of qubits	500	750	1000	1250	1500	1750	2000	2500	2750	2750	3000	3000
Final key length	62	149	185	256	306	345	427	496	569	399	626	549
Estimated error	0.0833	0.0277	0.0962	0.0317	0.0548	0.092	0.0526	0.0574	0.036	0.0963	0.0479	0.106
Eavesdropping enabled	1	1	1	1	1	1	1	1	1	1	1	1
Eavesdropping rate	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.25	0.1	0.25
Alice/Bob basis selection bias	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
Eve basis selection bias	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
Raw key mismatch before error correction	0.0702	0.0538	0.08	0.0665	0.0726	0.0823	0.071	0.0808	0.0761	0.1114	0.0765	0.0958
Raw key mismatch after error correction	0	0	0	0	0	0	0	0	0	0	0	0
Information leakage (Total number of disclosed bits)	136	166	268	293	331	423	416	587	664	801	672	794
Overall key cost for authentication	256	256	256	256	256	256	256	256	256	256	256	256
Key length before error correction	218	335	473	569	657	788	863	1103	1253	1220	1318	1363
Bit error probability	0.0688	0.0567	0.0782	0.0703	0.0746	0.0812	0.073	0.0834	0.0806	0.1131	0.0797	0.0946
Bits leaked during error correction	104	134	236	261	299	391	384	555	632	769	640	762
Shannon bound for leakage	79	106	188	209	252	321	326	457	507	622	529	616
Security parameter	20	20	20	20	20	20	20	20	20	20	20	20
QBER	0.876	0.801	0.815	0.7952	0.796	0.802	0.7865	0.8292	0.7930	0.855	0.7913	0.817