Quantum Key Distribution Simulation

Suhail Akhtar
Department of CS&IT
Maulana Azad National Urdu University, Hyderabad

Pradeep Kumar
Department of CS&IT
Maulana Azad National Urdu University, Hyderabad

Abdul Wahid
Head, Department of CS&IT
Maulana Azad National Urdu University, Hyderabad

***Abstract*— Quantum cryptography is a new type of cryptographic system. In the traditional system we use mathematic properties in the algorithm to make them strong but these type of algorithms are vulnerable by high computation power computers such as Quantum computer because the security of these algorithms are based on unproven mathematical formula which is thought to be secure and it is thought that currently available computers will take a very long time to break these types of security. So the Quantum cryptography uses the solid concept of Quantum mechanics to secure the data and theoretically it is impossible to crack it. In this technique, data is sent as Quanta which is polarized light.**

***Index Terms*—Cryptography, Quantum Cryptography, Highly Secure cryptography, Light based cryptography, Quantum mechanics**

I. Introduction

Quantum Cryptography is a new type of cryptography in which polarized light is used to generate the secret key for the encryption/decryption algorithm. This technique helps both parties in the generation of the secret key and it also tells them if someone is trying to snoop the communication and they can take the required measures to protect the communication from the attack.

This study is to understand the alternative of classic cryptography algorithms to generate the cryptographic secret keys for the encryption-decryption algorithm.

This study explores the BB84 algorithm for generation of cryptographic keys on two cases: with and without the attack by an attacker Eve.

II. Implementation (Simulation)

Phase 1: BB84 Quantum Transmission

The first step in the algorithm is to prepare a sequence of qubits so Alice create a sequence of 500 qubits by randomly choosing a basis for each qubit,rectilinear polarization (horizontal/0 degrees and vertical/90 degrees) or a diagonal polarization (+45 degrees and -45 degrees shifted) and then by using a quantum channel she sends it to Bob. Then she does the mapping of basis to qubit states. Horizontal and vertical are mapped to qubit states |0> and |1>, and +45 degrees and -45 degrees shifted with the states |+> and |->, respectively.

- Alice selects basis randomly with a basis selection bias of 0.5 which means 50% probability for choosing the basis.
- An eavesdropper Eve is also in between the communication, trying to steal the key. Eve is eavesdropping at a rate of 0.1 and its basis selection bias is 0.5, means its probability to choose a basis will be same for all choices and it will not be biased. She intercepts the qubits, randomly measures them in one of the two mentioned bases either rectilinear or diagonal and thus destroys the originals because a photon will be lost once it is measured, 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.

Phase 2.1: Sifting

When Bob receives the qubits, he measures them by randomly choosing the basis for the qubits and announces on a public classical channel. 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. If there is no channel noise then 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 257 bits.
- 0.514 of Alice's and Bob'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.

Phase 2.2: Sifting Authentication - Linear Feedback Shift Register (LFSR) Universal Hashing

Alice and Bob authenticate their basis exchange messages using the LFSR [11] 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

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 0.0784 was estimated using a sample size of 51 given a sampling ratio of 0.2

Phase 3.2: Reconciliation - Error Correction, Cascade

Alice and Bob perform an interactive error correction scheme called Cascade [11] 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.
- 18 erroneous bits were detected and corrected.
- 114 bits were leaked in order to correct the errors.
- With an error probability of 0.0874, the Shannon bound for the number of leaked bits is 89.0, compared to the actual number of leaked bits: 114.

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 pre-shared secret key and by comparing their respective digests. Further details:

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

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 [12]. The hashing function will be indexed using yet another chunk of their pre-shared secret keys. They can also define a security parameter to minimize Eve's knowledge to an arbitrary amount. Further details:

- 146 bits were leaked up to this point.
- The key length before running privacy amplification: 206 bits.
- The final key length is 40 bits.
- The chosen security parameter is 20.

All these steps are repeated for different no of qubits.

Table 1: Simulation results with attack

Initial number of qubits	Final key length	Estimated error
500	40	0.0784
510	30	0.0588
520	73	0.06
530	63	0.0962
540	64	0.0545
550	59	0.0877
Average		0.0726

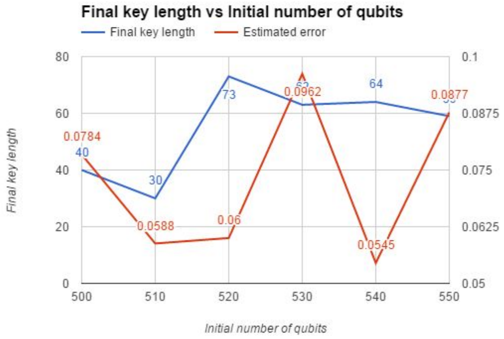

Fig 1: Graph between Final key length vs Initial number of qubits and Estimated error for simulation with attack

Table 2: Simulation results without attack

Initial number of qubits	Final key length	Estimated error
500	68	0. 0408
510	67	0.08
520	68	0.0638
530	82	0.0769
540	102	0
550	89	0.0741
Average		0.05593

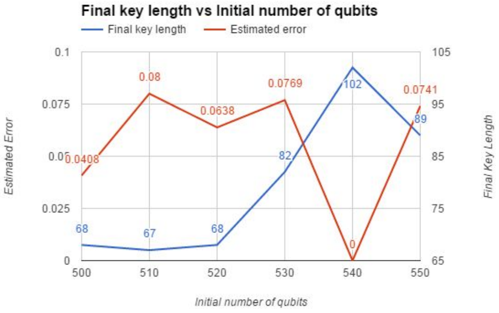

Fig2: Graph between Final key length vs. Initial number of qubits and estimated error for simulation without attack

III. Conclusion

QKD is a technique to generate the secret key for an encryption algorithm that takes the data in the form of a light photon. It makes use of Quantum physics and hence theoretically impossible to crack.

In QKD, the attack is identified based on the error. If the error rate is up to a threshold value then participating parties are good to go with the communication but if the error is above a threshold value then they conclude that there is a third party that wants to sniff the communication so based on this error based strategy they take measure to stop these attacks by stopping the communication and protecting the data.

As we have seen that the attack is measured in the form of error in the communication so we can see from the data that we have gathered that the average error in the communication when there is no attack is small compared to the communication while eve is attacking.

From the simulation we can see that due to the different errors the length of the final key is small compared to the initial no of quantum bits but they are unique and secret.
Also, it is hard to know the length of the final key because of the different errors that may occur during the key generation.

The presence of attacker is caught as the increase in the error. If the attacker is present then the error is increased.

The keys obtained using the quantum technique can be used together with one-time pad algorithm to create the cryptosystem that is perfectly secure.

IV. Reference

[1]. *QKD Simulator - Analysis and Simulation of Quantum Key Distribution*, www.qkdsimulator.com. Accessed 19 Feb. 2017.

[2]. Bennett, Charles H., et al. "Quantum Cryptography, or Unforgeable Subway Tokens." *Advances in Cryptology*, 1983, pp. 267-275.

[3]. C.A.Fuchs, N.Gisin, R.B.Griffiths, C.S.Niu, and A.Peres, Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy, Physical Review A 56, 1163 (1997).

[4]. Johnson, R. Colin. "MagiQ employs quantum technology for secure encryption." EE Times. 6 Nov. 2002. URL: http://www.eetimes.com/article/showArticle.jhtml?articleId=16506194 (19 February 2017).

[5]. "Quantum Key Distribution QKD." www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/. Accessed 19 Feb. 2017.

[6]. MagiQ Technologies, Inc. – "Any Sufficiently Advanced Technology is Indistinguishable from Magic.", www.magiqtech.com/Products_files/QBox%20Datasheet-2011.pdf.

[7]. Rieffel, Eleanor, and Wolfgang Polak. "An introduction to quantum computing for non-physicists." *ACM Computing Surveys*, vol. 32, no. 3, 2000, pp. 300-335.

[8]. Lomonaco, *Samuel* J. "A QUICK GLANCE AT QUANTUM CRYPTOGRAPHY." *Cryptologia*, vol. 23, no. 1, 1999, pp. 1-41.

[9]. Hjelme, Dag R., et al. "Chapter 5 - Quantum cryptography." *A Multidisciplinary Introduction to Information Security*, CRC P, 2012.

[10]. "Linear Feedback Shift Registers." *Department of Mathematical and Statistical Sciences | Mathematical & Statistical Sciences | University of Colorado Denver*, www-math.ucdenver.edu/~wcherowi/courses/m5410/m5410fsr.html.

[11]. Sugimoto, T., and K. Yamazaki. "Study on secret key reconciliation protocol 'Cascade'IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences." (1987).

[12]. "Toeplitz Matrices, Algorithms and Applications." *ERCIM - the European Research Consortium for Informatics and Mathematics*, www.ercim.eu/publication/Ercim_News/enw22/toeplitz.html.

Suhail Akhtar has received his B.Tech. degree in Computer Science from Uttar Pradesh Technical University, Lucknow, now known as Dr. A.P.J. Abdul Kalam Technical University. Currently, he is pursuing M.Tech. in Maulana Azad National Urdu University in Hyderabad.

Dr. Pradeep Kumar is Associate Professor in the Department of Computer Science & Information technology at Maulana Azad National Urdu University, Hyderabad (Telangana State). He received his Master's degree in Computer Technology and Applications from Delhi Technological University, formerly Delhi College of Engineering, Delhi University. He completed his Ph.D. at the University School of Information & Communication Technology (USICT), Guru Gobind Singh Indraprastha University (GGSIPU), Delhi. His research interests include software reliability engineering, models for software metrics, machine learning, neural network modeling and soft computing. He has more than 25 publications in journals of international repute including national journals, conferences, and proceedings of the international conferences. He is a Member of Association for Computing Machines (ACM), India.

Prof. Abdul Wahid is Dean of School of Computer Science & Information Technology and Head, department of CS&IT at Maulana Azad National Urdu University, Hyderabad (Telangana State), Pin- 500032, India. He is a Member of Association for Computing Machines (ACM), India, Member of Computer Science Teachers Association (CSTA), USA, Senior Member of International Association of Engineers (IAENG), Member of International Association of Computer Science and Information Technology (IACSIT), Singapore and Senior member of Universal Association of Computer and Electronics Engineers. He is a member of editorial board for various national and international journals in the field of Web software engineering.