Modified Novel Quantum Key Exchange using BB84 Algorithm

N.Vivek Chetty[1], Bikumalla Abhijith [2], Goli Nihar[3],P.M.Durai Raj Vincent [4]
[1,2,3]IIIrd B.Tech(IT),SITE, VIT University, Vellore.
[4] Assistant Professor(Senior), SITE, VIT University, Vellore.
abhijith_bikumalla@live.com, vivekchetty@yahoo.com, golinihar@live.com

Abstract

With the increasing number of eavesdroppers on communication channels, securing the reliability of digital communication has become a herculean task. For any communication and information exchange the most important step of securing the data is encryption and decryption (cryptography). The primary step involved in any efficient cryptographic system is Key Distribution. The paper deals with an efficient Key Distribution Technique based on Quantum Mechanics. The concept of Heisenberg's Uncertainty Principle and quantum indeterminacy property are used to detect the presence of eavesdropper and secure the process of Key Distribution.

Keywords-Quantum Mechanics, Heisenberg's uncertainty principle, eavesdropper, quantum indeterminacy.

Introduction

With the advent of internet, the digitalization of data has reached to great extents. The digitalised data includes highly secure and confidential information related to varied branches. The maintenance of this data is a major task of Information Systems. The confidentiality, integrity and availability features of the data need to be maintained for further extending the usage of digitalized data for many more purposes.

In the process of protecting data from unauthorised access, many access control mechanisms have come up. The securing of data exchange between 2 parties has been a major concern in the recent years. The communication security process involves the authentication (access control), secure data exchange and termination of the channel of communication.

Cryptography involves encryption and decryption of data to be exchanged between the 2 ends. The sender takes the information to be transmitted and uses an encryption algorithm and encrypts the message using a key. Encryption is the process of encoding or converting the message into a form so that the eaves dropper cannot understand the message even if he acquires the message during the communication process. The sender then sendsthis encrypted information to the receiver using the channel of communication. The receiver then decrypts the message using the algorithm for decryption and a key .Decryption is the process of decoding or converting the message into human readable form using an algorithm and a key if needed. There are many cryptographic algorithms now that are used for encryption and decryption.

The most efficient algorithms use a 'Key' in their encryption process (1). The algorithms which use key in their processes are of 2 types- symmetric and asymmetric. In the Symmetric key cryptography the key used during the encryption and decryption is the same. While, in the asymmetric key cryptography the key used during encryption is different from the key used during decryption. For either of the above 2 there is a need for Key distribution.

Key distribution (2) is the process of exchanging a secret key between the parties before the data exchange process. For the public key cryptography public key servers, public announcement, public key authority and public certificates are used for the key distribution process.

Quantum Key Exchange

The main goal of Quantum key exchange is the secure exchange of secret key. It uses the basic principles of Quantum i.e. if the value of one property of a quantum particle is determined accurately then the value of another particle cannot be determined as accurately as the former. When the properties of quantum particle are measured then the other properties of the quantum particle change drastically.

The above quantum principle can be used determine the presence of an eavesdropper. If the eavesdropper tries to determine the key, the quantum states would be altered when received by the receiver and then the presence can be determined based on the algorithm.

Related Work

BB84 Algorithm

This algorithm makes use of 2 channels for communication. The channels are as follows-

1. Quantum channel- This channel is used to exchange the qbits in this algorithm. It can be any optical communication fiber.
2. Public Classical Channel-This channel is the common channel used in every communication mechanism.

In this algorithm, the sender selects some bases randomly. The states are generated based on the key bits and the chosen states, these generated states are then forwarded to the receiver, and the receiver again randomly generates some bases and passes the states through the bases. Based on the resultant states and the bases used the receiver determines the key bits. The receiver then sends his bases to the sender in public classical channel. The sender based the states available with him and the received bases, determines the key generated at receivers end. Then for verification of eavesdropper, the send a subset of their keys to check if they match, if it matches then the channel is secure else it is insecure. This algorithm needs high level of synchronization

Literature Review

In the paper "Analysis statistical Fluctuation for quantum key distribution system" by Jiao Rong-zhen, Han Qing-yao, Tang Shao-jie states that The limited number of resources utilized in consideration with statistical ups and downs for rate of error and yield that decides the performance of quantum key distribution. The number of working quantum states distributed decides the security level of quantum key distribution. The concept of performance of quantum key distribution with limited resources and its calculations and considerations are focused.

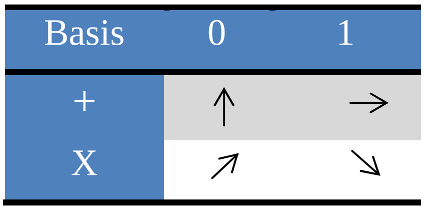
The paper "A New Secure Model for Quantum Key Distribution Protocol" by Rishi Dutt Sharma and Ashok De [1] states that the numbers of classical distribution methods are unsafe for key distribution but the quantum key distribution solves this problem by reducing the risk in distributing the key using the latter method. It provides a great extent of safety and several improvements to basic defects such as error detection etc. The concepts of improvements to basic defects of Quantum key distribution such as identity authentication, estimating attacker's information, secrecy enhancement are focused.

The paper "Quantum Key Distribution In Practice : The State of Art by Mohamed Elboukari and Abdelmalek Azizi [2] states that anyone could break public key methods based on number theory techniques and many new algorithms. So a great study has done on Quantum Key Distribution to make the things secure. In this paper the cryptography techniques used are explained as very promising and also enhanced technology to improve performance of implemented technologies. The quantum cryptography by exposing popular works and projects of Quantum Key Distribution are used. The concept of enhanced technology to improve performance and reliability of implemented technologies and popular works discussed in the paper are focused.

The paper "Reconciliation for Practical Quantum Key Distribution with BB84 Protocol" by N.Benletaief, H.Rezig [3] states that when two parties exchange information in presence of a third party reconciliation may occur. The reconciliation is watched as a new case of coding. This paper described the new method for reconciliation based on codes. The concept of an explicit new method for reconciliation based on codes when a new third party or eaves dropper is in between communication is focused.

Modified Algorithm

Here we use 2 pairs of orthogonal basis which are conjugate to each other. A pair of states that are orthogonal to each other and another pair of states that are also orthogonal to each other but are conjugate to the later pair.



Basis	0	1
+	↑	→
X	↗	↘

Figure:1

Similar to the BB84 algorithm we use 2 channels for communication(quantum channel and public classical channel).

The following are the steps of the modified algorithm-

1. The sender chooses a key (K).
2. The sender chooses random basis (B_0).
3. Based on the basis and the bits the states (S_0) are resulted.
4. The states S_0 are the sent to the receiver in the quantum channel.
5. The receiver randomly chooses basis (B_1).

6. The receiver then gets the states (S_1) based on the basis chosen.
7. Based on the basis B_0 and the states S_1, the receiver determines the secret key (S).
8. Then Receiver sends the States S_1 to the sender in the quantum channel.
9. The sender uses the basis B_0 on the received states S_1.
10. Based on the resultant states and the basis used the secret is determined
11. The sender and receiver are idle till the time of communication.
12. When a message is sent from the sender, a nonce (random number) is appended to the message and sent.
13. The receiver does the required operation on the nonce and sends it back to the sender.
14. If the sender verifies the nonce then the channels are secure and secret key can be used.

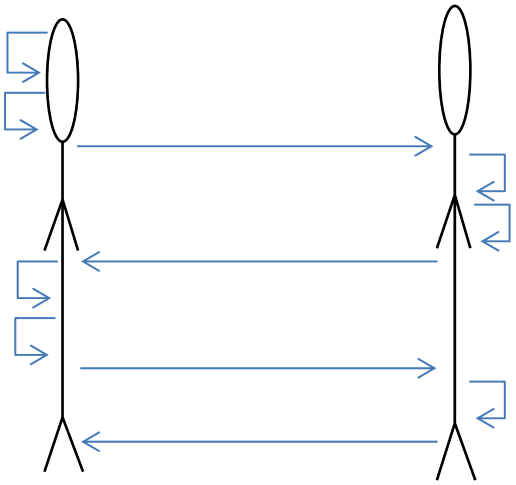


Figure:2

Example

Let the sender be Alice and the receiver be Bob. Let the eavesdropper be eave.

Let the key chosen by Alice be-

Step1: K=10101

Step2: B_0=+++xx

Step3: Based on the figure 1-

S_0= → ↑ → ↗ ↘

Step4: Send the states to Bob.

Step5: B_1=+++++

Step6: S_1= → ↑ → → →

Step 7: S=101

Step 8: Send S_1 to Alice.

Step 9: States are formed using S_1 and B_0.

Step10: The new States are used to determine the S.

B_0=+++xx

S_1= → ↑ → → →

S=101.

Step11: Idle

Step12: Alice appends nonce to message.

Step13: Bod replies the modified nonce.

Step14: Alice checks the nonce and determines if the channel is safe.

When eave interrupts in between the communication, then the states would be altered and then the secret key Bob’s end would differ from that at Alice’s end. Then the nonce in the message cannot be extracted accurately and Alice would get a wrong reply and she would declare the channel insecure.

Comparison:

In the BB84 algorithm the security of the system would be of the order of 2^n if the number of bits in the key is ‘n’. The above mentioned security can is the best security that can be achieved by the BB84 algorithm, i.e. the Eave gets the entire basis exactly as Alice chooses. If eave is in a position to get the basis sent by Bob to Alice then he would get the secret key.

We have overcome the above limitation by not using the classical channel, the security provided by optical fiber if reasonably better than that by classical channel. And, Eave must also get the basis of Alice and Bob both right otherwise the states would alter and so does the key. Even if Eave manages to get the basis right, he would not be able to return the right nonce back to Alice as he does not have the algorithm to modify the nonce and reply.

Result:

The order of security provided by the above algorithm is 2^nx2^n.As seen the complexity of the algorithm is high enough to resist a brute force attack.The usage of only quantum channel or optic fiber for exchange if key ensures safety as it has been observed that unauthorized extraction of data through hardware insertion leads to loss of data and collapse of communication. The communication between the sender and receiver is minimum in order to reduce the time required for key exchange.

Conclusion:

The above suggested algorithm for key distribution will help in the key distribution process between the sender and receiver for safe and reliable communication.

References:

[1] Rishi Dutt Sharma, Asok “A New Secure Model for Quantum Key Distribution Protocol” 6th International Conference on Industrial and Information Systems, ICIIS 2011, Aug. 16-19, 2011, Sri Lanka.

[2] Mohamed Elboukhari1, Abdelmalek Azizi,Mostafa Azizi “Quantum Key Distribution in Practice: The State Of Art” **Published in:** I/V Communications and Mobile Network (ISVC), 2010 5th International Symposium Sept. 30 2010-Oct. 2 2010.

[3] N. Benletaief, H. Rezig, A. Bouallegue “Reconciliation for Practical Quantum Key Distribution with BB84 protocol” Mediterranean Microwave Symposium (MMS), 2011 Sept. 2011 219 - 222.

[4] Jiao Rong-zhen, Han Qing-yao, Tang Shao-jie “Analysis statistical fluctuation for quantum key distribution system”, 2010 International Conference on Information, Networking and Automation (ICINA), Oct. 2010, V2-296 - V2-298.

[5] Di Jin, Pramode Verma, Stamatios Kartalopoulous “Key Distribution using Dual Quantum Channels” Information Assurance and Security, 2008. ISIAS '08 Sept. 2008, 327 – 332.

[6] Sun baili, Hao Shangfu, Zhang Xiao, Wang Zhihui “An Improved Method of Quantum Key Distribution”, Computer Science-Technology and Applications, 2009. IFCSTA '09, Dec. 2009, 115 - 117

[7] Mei Zhao, Fei Li, and Bao Yu Zheng “A Proof of security of Quantum Key Distribution in Probabilistic Clone Scheme” Communication Technology Proceedings, 2003. ICCT 2003, April 2003, 1507 - 1509

[8] Lee Oesterling, Don Hayford andGeorgeanne “Comparison of Commercial and next Generation Quantum Key Distribution” , Homeland Security (HST), 2012 IEEE Conference, Nov. 2012, 156 - 161