ISSN:0975-9646

Survey on Various Quantum Key Distribution Algorithms

Vivek Singh
Computer Science & Engineering
B.S Anangpuria Institute of Technology and Management
Faridabad, India

Bhawna Chauhan
Computer Science & Engineering
B.S Anangpuria Institute of Technology and Management
Faridabad, India

***ABSTRACT*-Key distribution is the process of sharing the key between the parties who intend to communicate with each other such that any unintended party would not intercept the key. The classical approach is less secure as the key can be intercepted within fixed interval. Therefor more secure approach is devised called as Quantum Key Distribution which can detect the intrusion while communication is going on. This paper aims at surveying some of these quantum key distribution algorithms**

Keywords—Quantum computing Quantum Key Distribution, Three party authentication

INRODUCTION

The most important aspect of any encryption technique is the key used for the ciphering the plain text. Security of whole cryptosystem depends on the key used in encryption. Every algorithm devised for encryption is worthless, if the key used is not strong and secure. A strong, unique and untraceable key strengthen the cryptosystem, whereas a weak key destroy its integrity and make it vulnerable. Therefore key distribution is the inextricable part in any encryption algorithm. Since key distribution must be secure enough to prevent any attempts to compromise the system. So this paper aims at studying various quantum key distribution algorithms.

As in classical computers, electrical signals such as voltages represent the 0 and 1 states as one-bit information. Similarly in the quantum computer, a quantum bit called a "qubit," represents the one-bit information. Qubit is a two-state system. Unlike an electrical signal in classical computers, an electron can be used as a qubit. The spin-up represents state 0 and spin-down represent state 1, respectively. A photon can also be used to represent a qubit, and its horizontal and vertical polarization can be used to represent both states. Using these qubits, quantum computers can perform its basic operations like arithmetic and logical operations. These qubits are the basic building blocks of the quantum computing. The basic difference between the classical bit and quantum bit is that one qubit can also represent the superposition of both states where as classical bit cannot.

Quantum computing is the field of computing which, heavily relies on various quantum-mechanical phenomena, such as uncertainty principle, superposition, entanglement etc. Quantum cryptography secure the communication between two parities in quantum communication. It allows two parities to generate a key with special properties and use it for secure data transfer between them.

In order to make Quantum key distribution safer Quantum computing uses two principles from quantum mechanics. First, the Heisenberg uncertainty principle and second, the no-cloning theorem. This approach can detect the presence of eavesdropper as measuring the quantum state destroy that state.

LITERATURE SURVEY

QKD mainly revolves around three algorithms; BB84, B92, and EPR. These protocols interchange qubits using quantum channel and then apply probabilistic measures to regulate the sequence of the key bits. Bases used to transfer data in BB84 are rectilinear and diagonal.

Alice sends random train of photons polarized according to the random bases(rectilinear or diagonal) to Bob over a quantum channel. Bob receives the photons and guesses the bases used by Alice independently and stores the result as 0 or 1. Now subsequent steps takes place over classical channel where both interchanges the information about the bases used by them and compute the final key. No cloning principle ensures that the photon state cannot be copied and hence eavesdropping can be detected. Whole process is repeated again in case eavesdropping is detected.

B92 is essentially a simplified version of BB84.In this protocol quantum cryptography is applied using any two non-orthogonal states. The key difference in B92 is that it only needs two states rather than the four polarization states required in BB84. Like the BB84, Alice transmits a string of photons to Bob which she encoded with randomly chosen bits. Now the bits chosen by Alice determine the base she have to use. Bob still randomly chooses a basis by which to measure the bits but wrong basis selection completely remove the information and he will not measure any readings because of a condition in quantum mechanics called as an erasure. Bob simply informs Alice after receiving each bit, if he measured the bit correctly or not. In this way they both determine the key to be used in secretly encoding the messages.

EPR protocol is another quantum key distribution protocol proposed by Einstein, Podolsky, and Rosen (EPR). In this protocol they discovered a paradox to take advantage of EPR correlations which states that all particles are produced in a way that they are "entangled" which means that despite very large distances between them, they depends on each other. They are associated with each other

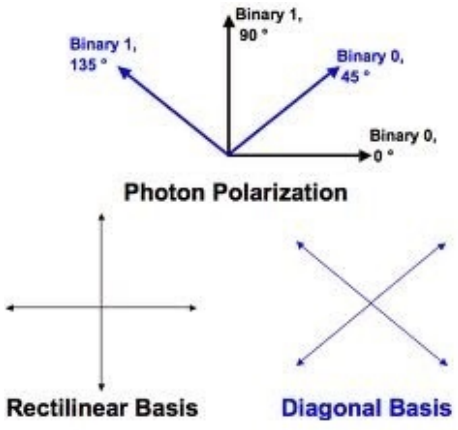
in such a way that the measurement of one automatically measure other. For example if one of the particles of photon is measured according to the diagonal basis and have a left-circular polarization, then the other particle must have a left-circular polarization if it is measured according to diagonal basis. Alice generates a sequence of random bits and then generates EPR pairs of polarized photons for each bit. She sends one particle of each pair to Bob keeping other particle for herself. She then randomly measures the polarization of all the kept particles according to the rectilinear or diagonal basis and then records each measurement type and the polarization measured.

On the other hand Bob also randomly measures each received particle according to the rectilinear or diagonal basis. He also documents each measurement type and the polarization measured. Alice and Bob communicates with each other telling each other which measurement types they used, and they stores the data where same measurement type was used. They changes the equivalent data to a string of bits using an agreed upon convention.

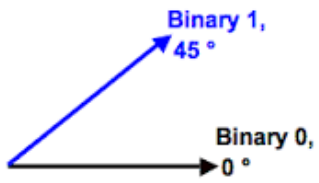
All the above discussed protocols have both advantage and disadvantage over each other. These protocols suffers from the problem of user's authentication.

Another algorithm was introduced which is based on Third Party authentication and establish the trust between different parties. The trusted third party aims at bringing the communicating parties to an agreement over the basis to be used. This protocol works in two steps.

1. User Authentication & Quantum Bases distribution
2. Data Transfer over the Quantum channel



Photon Polarization
BB84 4 State Encoding



Photon Polarization
B92 2 State Encoding

In first step, a public key cryptography algorithm (RSA) is used to authenticate the communicating parties by the trusted third party. After successful authentication this trusted third party generate the random bases and distribute them to the communicating parties to encode the data in state.

In second step Alice encode the data in qubits and send the data over quantum channel to Bob. Bob select his bases to measure received qubits. Then both Alice and Bob transfer the data to trusted third party after encrypting it. Then this third party decrypts the message and check if both the data are same. If both data from Alice and Bob are found to be same then the communication goes on otherwise trusted third party notify all the communicating parties that eavesdropping is detected and data transfer is stopped

CONCLUSION

All the above algorithms are secure to eavesdropping and hence provide the secure way of key distribution. But these algorithm stops after eavesdropping detection. And whole process is to be started from the scratch after some time. Moreover there is no guarantee that eavesdropper is not present later. So these algorithms don't specify any action plan to execute after the eavesdropping is detected, which makes these algorithms less usable and more complex.

ACKNOWLEDGMENT

I would like to thank my guide Dr. A.K. Sharma, Mrs Bhawna Chauhan and staff members for their generous help. Without their help, guidance and support, this paper would not have been possible

REFERENCES

[1] Y. Kanamori, S.M. Yoo, W.D. Pan, and F.T. Sheldon, -A Short Survey On Quantum Computers, International Journal of Computers and Applications, Vol. 28, No. 3, 2006.

[2] Charles H. Bennett, Gilles Brassard, ―Quantum Cryptography:Public Key Distribution and Coin Tossing, International Conference on Computers, Systems and Signal Processing Bangalore, India, December 10-12, 1984.

[3] Ammar Odeh, Khaled Elleithy, Muneer Alshowkan, Eman Abdelfattah, ―Quantum Key Distribution by Using Public Key Algorithm (RSA), London, United Kingdom: third International Conference on Innovative Computing Technology (INTECH),IEEE, August 2013.

[4] Sneha Charjan, D. H. Kulkarni, -Quantum Key Distribution using Different Techniques and Algorithms, International Journal of Engineering Research & Technology (IJERT).

[5] Ching-Nung Yang and Chen-Chin Kuo ―Enhanced Quantum Key Distribution Protocols Using BB84 and B92.

[6] Rambabu Saini and Shavita Shiwani -Quantum Cryptography Enhancement of QKD EPR Protocol & Identity Verification,International Journal Of Engineering Sciences & Research Technology(IJESRT), Oct 2012.

[7] Abdulrahman Aldhaheri, Khaled Elleithy, Majid Alshammari, Hussam ―A Novel Secure Quantum Key Distribution Algorithm‖, University of Bridgeport.

[8] Xiaoyu Li and Dexi Zhang, -Quantum authentication protocol using entangled states , Proceedings of the 5th 78 WSEAS International Conference on Applied Computer Science, Hangzhou, China, April 16-18, 2006