Quantum Computation of Perfect Time-Eavesdropping in Position-Based Quantum Cryptography

Quantum Computing and Eavesdropping over Perfect Key Distribution

Sayantan Gupta[1]
Computer Science Department
University of Engineering and Management, Kolkata
Kolkata, India
Sayantangupta999@gmail.com

Kartik Sau[2]
Computer Science Department
University of Engineering and Management, Kolkata
Kolkata, India
Kartik_sau2001@yahoo.co.in

Jyotirmoy Pramanick[3]
Electronics and Communication Department
University of Engineering and Management, Kolkata
Kolkata, India
Jomanick97@gmail.com

Swarnava Pyne[4]
Electronics and Communication Department
University of Engineering and Management, Kolkata
Kolkata, India
Pyneswarnava@gmail.com

Rizwan Ahamed[5]
Computer Science Department
University of Engineering and Management, Kolkata
Kolkata, India
Ahamedrizwan94@gmail.com

Rahul Biswas[6]
Electronics and Communication Department
University of Engineering and Management, Kolkata
Kolkata, India
Rahul98457@gmail.com

***Abstract*—**In this paper, we proposed the Implementation of Perfect Time Eavesdropping in Position Based Quantum Cryptography. The Security of Quantum Key Distribution lies in the Laws of Quantum Mechanics and is recognized to be one of the most secure cryptography ever known. The major advantage of Position-Based Key Distribution is that an authenticated server or device will be able to use its Inter-Space Positions while authenticating in an environment while exchanging a secure key for communication over the network. In Position Cryptography the Authentication is done by verifying that a particular Device holds a definite and fixed position in Space-Time. In this paper, we proposed the experimental Time-Based Attack which evolved as modern day Decoy-Fake Shift Attack. The key idea is: an Attacker Eve can change the Shift of the Key randomly to T1 or T2 with the probability of shift, F and G = 1−F respectively. Also, the attacker can Authenticate and Randomize the Probability F in such a way so that it ensures the Receiver's Detection Ratio is constant i.e. 1:1. So, as a result, the two parties communicating via a secure Quantum channel will not be able to detect the Eavesdropping caused by the attacker and therefore the attacker can have an Authentication over the shared key and can, therefore, the parties will not be able to conceal its information. Thus the secure Position Quantum Cryptography can be broken by this proposed Architecture model. In this paper, we represented the Architecture Model experimentally and the Security Analysis for such an attack has been proposed.

Keywords— Quantum Computing; Quantum Cryptography; Quantum Key Distribution; Perfect Eavesdropping; Time-Shift Attack; Quantum Position Cryptography.

I. INTRODUCTION

Safe and Secure Communication network provided by Quantum Key Distribution is needed by humans in various fields like defense, development, science, telecommunication etc. New Technologies in Cryptography was invented and broken and further new technologies are invented for the cause. Quantum Key Distribution is based on the laws of

978-1-5386-2215-5/17/$31.00 ©2017 IEEE

Quantum Mechanics and is the most significant technology in Cryptography [2][3]. Today Quantum Cryptography is commercial available across 300 km and is also available for Domestic purposes and is considered to be most secure. The security of Quantum Cryptography has been proved, but the physical implementation of it has been a problem for many scientists across the globe. Different kinds of eavesdropping methods have been introduced till date each having their own characteristics and limitations [4][5][6]. We implemented an attack in the QKD assuming that the software credentials and the hardware are known to the Attacker. In this paper, we proposed the Perfect Eavesdropping Attack under normal conditions where the Secret key is shared between the Source "Alice" and the Destination "Bob"[1] over a 30m long connected cable. The communication was started from the source end and after some time the Eavesdropper was able to obtain the same Secret Key as received by "Bob" the receiver. This key was achieved as Eve was able to change the probability of Bob receiving the signal so the Quantum Laws were not disturbed and thus the Attacker was undetected.

In the previous Quantum Cryptographic experiments, many people tried using Coherent-Photon Key Transfer as a medium to share the Key and this proved to be very accurate and immune to vulnerability. These models are commercially available to use, but there are still ways in which an intelligent attacker can get into the system as the Coherent Pulse used sometimes may contain more than one inherited Pulse and the attacker can use such pulse to change the probabilities of receiving the Key and ultimately gaining access to the system without getting detected [10]. We prove that in the Position based Quantum Cryptography the overall security of the system can be broken by the attackers by introduction Non-Local Computing over the Secret key in Time-shared basis [8].

II. Position Based Quantum Cryptography

A. Experimental Setup of the Model

The Quantum Cryptographic Model has Four Detectors namely α_1, α_2, α_3, α_4 and uses the Coherent-Polarization Algorithm to share the Key (Fig. 1). Now in this setup, the attacker can disable all the 4 possible devices by using a high polarized Laser-Shift Diode. Let the Event of selecting or activation a device be known as "Clicking" [1]. Now we make 3 devices inactive for the Attacker to Eavesdrop and we keep only one device active. Later in the attacker setup, we will see that Eve does this by transmitting a high-frequency Phase-Polarized Photon Pulse to the devices to make them Inactive, the Power required in such case let be $2P_{th}$. As the diodes are arranged in order of 45 degrees Phase-Shift the attacker can intentionally deactivate any of the Receiver's Device and then implement the Fake-Shift Attack in the QKD. We compromised the setup and inserted the attacker in the transmission section by matching the shift of the attacker Eve with the Receiving Devices. Now the Shift caused by the Eve can be represented as:

$$\Delta = \sum_{i,j} \mu_i * \mu_j - \gamma_{i,j} \qquad (1)$$

Where μ_i, μ_j are Phase-Shift of the Devices active and $\gamma_{i,j}$ be the Phase-shift of Device currently made inactive by Eve.
During the authentication of this algorithm, only 3 devices will be regarded as "Clicks" the attacker can easily verify the Fake-shift caused in the Receiving End of Bob. Hence the attacker has an authenticated over the network and will have the same amount of information as the Receiver. The Fake-Shift Generator (FSG) used by the attacker has the probability to deactivate more than 1 device but such high-level FSG is not used in this experiment. The FSG used by the attacker will help Eve to change the Probabilities of the shift in the device "Clicks".

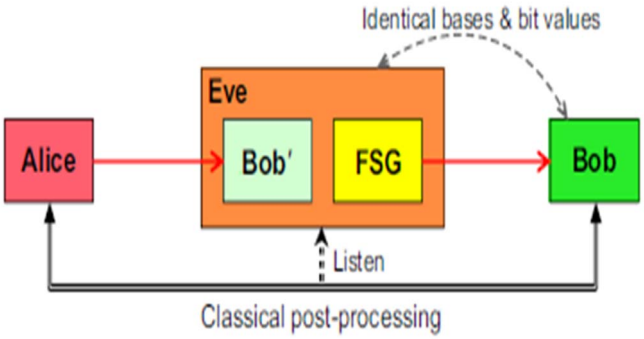


Figure 1: (Quantum Communication Model)

B. The Attacker Setup Model

The main Aim of the attacker FSG setup is to make the target device inactive thus gaining an access in the process. Now in the experiment, if we engulf a Pulse shift of Optimal Power (P_{th}) any of the required devices will be inactivated in the case with high success rate. Also if we engulf an Optimal Power of (P_{th})/2 we can ensure that two consecutive devices which are Conjugate of each other are not being Inactive i.e. they will never cause a Click. During the execution phase, we saw that the conjugate of the Inactive device had much greater threshold value then it other counterparts (Fig 2.). The minimum power required for a device to be made inactive was about 1 μW and during this minimum value all the threshold values were seen a uniform, so our condition failed during this initial value. So, our necessary condition for any device to be made inactive was (P_{th}). Also, changing the Optical Polarization of the devices didn't help as we assumed it will

receive much greater power than the peak value. The FSG made the Perfect Eavesdropping condition for the attacker to gain control of the information received by Bob with an efficiency of about 94%. This means that the attacker has almost all the information which is transmitted by the Source and the other half can be obtained by just repeating the shift again or by using high-performance FSG.

Now we made a change in the Pulse-Shift by introducing an Optical Polarized Pulse with a different orientation which randomly helped to improve the performance. But this setup required much more hardware thus the cost increased but this method never deactivated the wrong device. In this method, we tried to measure the efficiency of the attacker pulse and we saw that the probability of receiving the information was about 99%. Thus, almost the same information is received by the attacker which ultimately compromised the QKD mechanism and error rate was also less as compared to its counterpart. Also in the previous mechanism, the attack was able to regain access to the leftover transmission by implementing a good recovery Algorithm after the initial processing was done. Thus by both this method, Eve the attacker can successfully implement the Perfect- Eavesdropping condition which we wanted to achieve in this case.

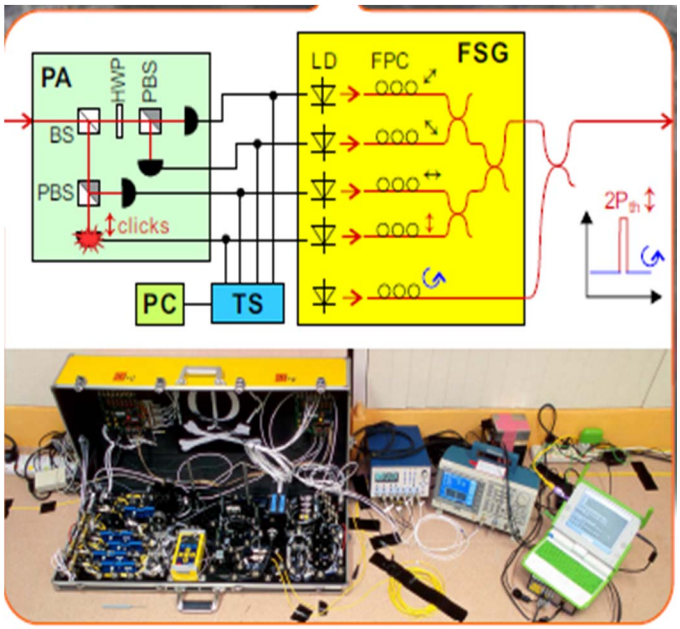


Figure 2: (Experimental Setup of the Proposed Model)

III. Analysis of Perfect Eavesdropping

Here the attacker uses a duplicate copy of the authenticated Receiver device to eavesdrop the receiver device by using Time-Shift Attack which can hamper the transmission between Alice and Bob. As in the Eve setup, we have used an FSG to replicate the key by deactivating a particular device and we saw that the entire transmission has compromised in such case. In the case of Perfect Eavesdropping condition, the attacker keeps a track of the Quantum bits transferred and implements several algorithms to guess the next quantum key to be shared between Alice and Bob[19][20]. The conventional algorithms used for replicating the key introduce several errors in the execution phase which ultimately reduces the efficiency of the method and is overruled by the Time-Shift Attack and thus it becomes very effective in such cases.

The attacker's control over the transmission is essential for the success of the Time-Shift Attack. In the experiment, we used the Optical Polarized Pulse to get such hold in the receiver's end. The Quantum Key Distribution Model being eavesdropped has been assumed to behave positively under Perfect Eavesdropped condition [12] [13].

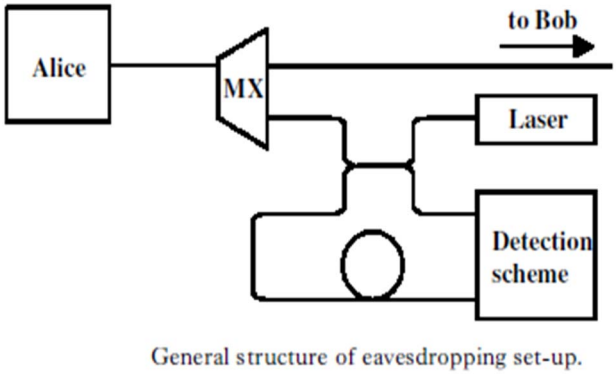
When the optically polarized pulse hits the QKD system it leads to the generation of an electron-hole pair which creates a disruption in the system (Fig. 4a). The output of the disruption is recorded by a comparator device placed in the circuit and is finally plotted as the output. Now if the threshold value is less than the initial condition given then the disruption caused will be much less or no disruption will occur[15] [13] [14]. When the threshold value is sufficiently high then one of the devices becomes inactive and we get the comparator output. The graph of Time vs. Avalanche Current, Detector Output is plotted. (Fig. 4b)

Under optimal threshold value, the Diode behaves like a Detector which detects the output of the comparator.

To retain the Perfect Eavesdropping condition, the attacker gains the permission of the Quantum bit which is only transferred to the attacker's computer, thus leaving the eavesdropper undetected by changing the relative shift of the secret key. The attacker implements a comparison over the received key and the Phase-Shifted key and records the error if any otherwise the expression for the Shift will be:

$$(H(\alpha_1) \otimes H(\alpha_2)) + (H(\alpha_3) \otimes H(\alpha_4)) = \gamma' \qquad (2)$$

Here in this Shift equation 'H' is the Hadamard Operator being applied to all the devices to compare the Shift bitwise. The error will be in the expression where the compromised device is present.



General structure of eavesdropping set-up.

Figure 3: (Structure of the Attacker Setup)

A. Position Shift Authentication of the Model

Let us consider we have two checkers C_0 and C_1, whose job is to compare the position shift and let we have a device which proves a particular position Q which lies at a random position in space-time and is denoted as P_{pos}. During the verification Phase, C_0 sends a primary quantum bit $H_\theta|X_i$ to Q, and C_1 sends the bit $H_\theta|X_j$ to Q. Now the transmission of these Qubits is arranged in such a way that θ is received by the Prover Q at a particular interval of time. To verify the position Q has to determine the data received on the basis θ to obtain the position $X_{i,y}$ and in turn the device may send back the received X to both the Checkers C_0 and C_1, these checkers will authenticate whether the data transmitted has been received in correct position and in specific time interval. Now let us consider another set of Checker P_0, P_1, Prover Z_0, and Z_1 and let the Position remain same. Let the Checker P_0 be between Z_0 and Q and let P_1 between Z_1 and Q. (Fig. 5) .When the data is transmitted P_0 intercepts the quantum bit, but the checker does not know the value of θ. If by any means the devices try to get the corresponding value she might get it wrong and the Prover will not be able to provide the correct value of $X_{i,j}$. Also, if the data is transmitted to P_1, the device will ultimately get the wrong value of θ and the Prover will not be able to send the actual value to the device. So, to solve this problem P_0 or P_1 needs to read and record the value of the Qubits until they receive the value of θ. But according to the principle of Quantum Mechanics –if we try to measure the value of a particular Qubits, superposition occurs and the value gets reduced to unity. So, actually, in this Experiment, Alice or Bob will never be able to know the actual basis of the attacker as it is dismantled in the case.

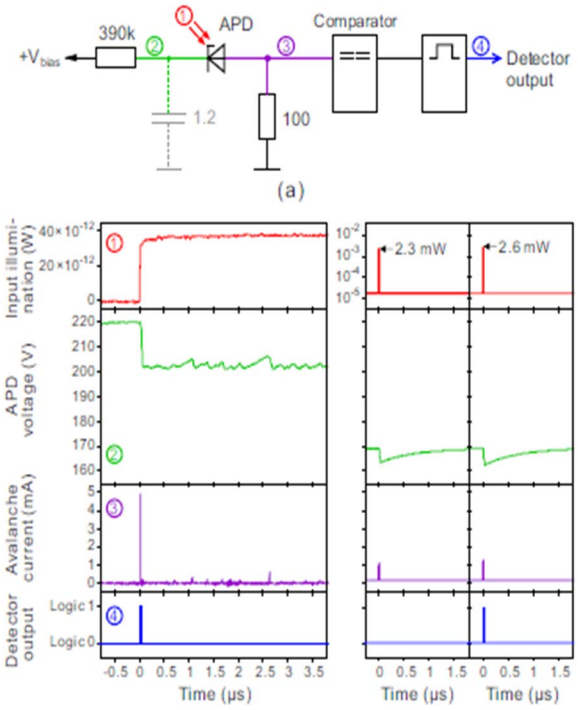


Figure 4: (Graphical Stimulation of the Entities)

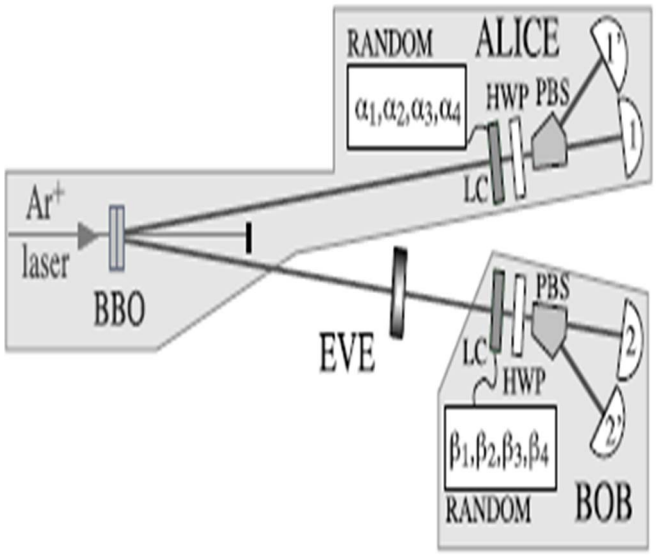


Figure 5: (Block Diagram of the Phase Key Setup)

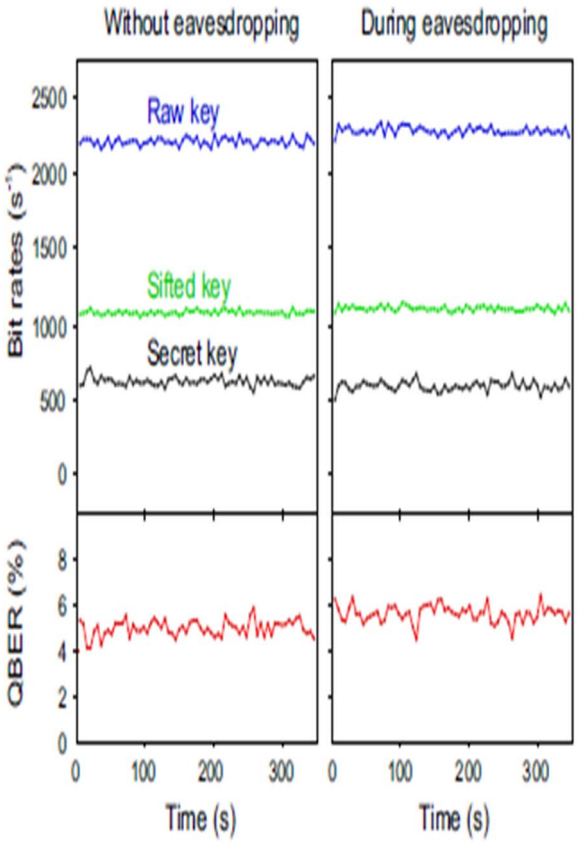


Figure 6: (Graphical Analysis of the Secret Key in the following two conditions)

The evaluation of performance first with eavesdropping and second without eavesdropping is explained in the graph (Fig. 6). The graph indicates the comparison between the actual key and the Phase-Shifted Key before and after the attack was made in the QKD system [11][16][17]. However, all the values in the graph are true only if the Qubits are not in the pre-entangled state, meaning if they are in an entangled state the experiment mechanism will fail and the attacker will not be able to change the Phase of the key in the entangled state. Thus the perfect-Eavesdropping condition will fail as we will not be able to get the threshold value greater than the initial value. Still, the Perfect-Eavesdropping condition has many inbuilt errors which maybe later rectified with efficient algorithms.

IV. CONCLUSION

Thus, in this paper, we proposed and implemented the Perfect-Eavesdropping Condition for the Position-based Quantum Cryptography. However, the condition is only satisfied if we use the setup and the devices in the optimal threshold value and the transmitted quantum bits must not be entangled state otherwise the experiment will not be possible. We proved that the actual Position of the bit is unknown to the attacker before Eavesdropping but after the successful "clicking" of the circuit Eve came to know about the transmitted data and it is well efficient. The necessary conditions were satisfied for the Attack to happen and Eve was successful in authenticating the information without being detected.

Acknowledgment

All the authors have no conflicts of interest. The work is self-funded and would not be so successful in representing without the help of the co-authors. I would also like to thank our Teachers for their immense help and corporation. I would also like to thank my parents, Abhijit Gupta and Tripti Gupta for supporting me during the hard times and keeping faith in me throughout.

References

[1] Ilja Gerhardt, Qin Liu, Ant´ıa Lamas-Linares,Johannes Skaar, Christian Kurtsiefer,and Vadim Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system"

[2] Benioff, Paul "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines". Journal of statistical physics 22 (5): 563–591. 1980

[3] Manin, Yu. I.Vychislimoe i nevychislimoe [Computable and Noncomputable] (in Russian). Sov. Radio. pp. 13–15. 1980 Retrieved 2013-03-04.

[4] Feynman, R. P.u "Simulating physics with computers". International Journal of Theoretical Physics 21 (6) (1982).: 467–488.

[5] Deutsch, David "Quantum theory, the Church- Turing principle and the universal quantum computer". Proceedings of the Royal Society A. 400 (July 1985).

[6] Finkelstein, David (1968). "Space-Time Structure in High Energy Interactions". In Gudehus, T.; Kaiser, G. Fundamental Interactions at High Energy. New York: Gordon & Breach.

[7] Gershon, Eric (2013-01-14). "New qubit control bodes well for future of quantum-computing".

[8] Quantum Information Science and Technology Roadmap for a sense of where the research is heading.

[9] Simon, D.R. (1994). "On the power of quantum computation". Foundations of Computer Science, 1994 Proceedings, 35th Annual Symposium on: 116-123.

[10] Nielsen, Michael A.; Chuang, Isaac L. Quantum Computation and Quantum Information. p. 202.

[11] Waldner,Jean-Baptiste (2007). Nanocomputers and Swarm Intelligence. London: ISTE. p. 157.

[12] Di Vincenzo, David P. (1995). "Quantum Computation". Science 270 (5234): 255–261.

[13] Lenstra, Arjen K. (2000). "Integer Factoring" (PDF). Designs, Codes and Cryptography19 (2/3): 101–128.

[14] Daniel J. Bernstein, Introduction to Post- Quantum Cryptography. Introduction to Daniel J. Bernstein,

[15] Johannes Buchmann, Erik Dahmen (editors). Post-quantum cryptography. Springer, Berlin, 2009.

[16] Samuel L. Braunstein, "Quantum Teleportation Fortschr. Phys. 50, 2002, 5-7,608-613"

[17] Kobayashi, H.; Gall, F.L. (2006). "Dihedral Hidden Subgroup Problem: A Survey".Information and Media Technologies 1 (1): 178–185.

[18] Bennett C.H., Bernstein E., Brassard G., Vazirani U., "The strengths and weaknesses of quantum computation". SIAM Journal on Computing 26(5): 1510–1523 (1997).

[19] Quantum Algorithm Zoo – Stephen Jordan's

[20] http://newatlas.com/china-quantum- cryptographycommunications-satellite/44965

[21] S. Kundu *et al*., "Quantum computation: From Church-Turing thesis to Qubits," *2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York, NY, 2016, pp.1-5. doi: 10.1109/UEMCON.2016.7777805

Corresponding Author:

Sayantan Gupta

Sayantan Gupta (14.10.1997) has a keen interest in Quantum Computing, Quantum Artificial Intelligence, Quantum Machine Learning, Quantum Methods, Digital Image Processing, Cloud Computing and has published various research papers in International Journals and Conferences.