MODELING AND SIMULATION OF SECURE DATA TRANSFER IN HIGH LEVEL LANGUAGE USING QUANTUM COMMUNICATION PROTOCOL

Manoj E Patil[1], Dr. Swati Sharma[2]
[1]Phd Research Scholar, [2]Associate Professor,
Department of Computer Engineering, Jodhpur National University Jodhpur.

ABSTRACT: Security is the main issue in the data transfer between the two nodes or multiple nodes over the network. In our traditional communication there are very large number of protocols and security mechanisms available. But still these security mechanisms can be compromised by using the very high computing power processors. Quantum cryptography will be the promising secure communication using quantum physical laws. Quantum communication itself makes the communication more promising and reliable in terms of security. Many quantum cryptography protocols are proposed till date for secure communication including a popular 'Three-Stage Quantum Cryptography Protocol' [1]. In the current quantum cryptography protocols, the unit of data is a binary bit. Here the proposed communication system will be capable of transferring the data in the form of character rather than the bit by bit data transfer. This methodology uses the simple logic ie the high level language is used for the data transfer. The flag is also added for improving the capacity of the protocol for the english language. This paper also focus on the disadvantages of the BB84 protocol, Three-Stag Quantum Cryptography Protocol and Modified Four Stage Quantum Communication protocol. This proposed protocol will increase the data transfer speed as well as the security of the data transfer.

KEY WORDS: threshold quantum cryptography, three-stage quantum cryptography protocol, light intensity, encoding system, Malus's Law.

I. INTRODUCTION

Data communication is the most important part of the digitization. That data traverse through the communication channel for long distance and for a long time. During this transit of the data through the communication channel there is the possibility of information interception. The important data may leaked and the organization my be in trouble. To secure this data form the intruder there are many more cryptographic methods proposed. Basically the cryptography is divided into two parts, symmetric keys cryptography and asymmetric key cryptography. These methods basically work on the mathematical formulas and use the same or different keys for encryption and decryption. But now a days the computers are coming with the huge computing power. Due to this the traditional cryptographic methods may be compromised. To overcome this disadvantage new cryptographic method is proposed called as Quantum Cryptography. Quantum Cryptography [2] is an approach for secure communications by applying the properties of quantum physics. In traditional classical cryptography mathematical techniques are used to restrict eavesdroppers. The quantum cryptography is focused on the physics of information. According to quantum physics information is abstract. It acquires the physical properties of the medium on which it is stored or through which it is communicated. For example information will be governed by the laws of magnetic field when it is written on hard disk, and it will be governed by the laws of light when it is transmitted optically. Quantum cryptography provides a way of secure communication, as its security is guaranteed directly by the laws of quantum physics. The field of quantum cryptography began after the formative work of Charles Bennett and Gilles Brassard in 1984. They proposed the BB84 algorithm [11]. Today quantum cryptography is supposed to become a dominant part of communication domain. Threshold Quantum Cryptography [5] (TQC) protocols systems are secure as long as the number of photons that are exchanged between the Sender and Receiver are below a specified threshold. "TQC speaks of a (p-k-n) threshold system where, system is completely secure as long as numbers of photons exchanged are less than p. When the numbers of photons are between p and k, system is partially secure, and when it exceeds k, the system is insecure." Subhash Kak' implement the three stage quantum cryptography protocol (TSQC) [1] first time in the lab. Implementation details are given in these Paper [4] [8] [10]. Current implementation of this protocol tolerates multiple photons in the secure communication process. This make it superior to BB84 protocol [11] and its variants who require prefect single photon source for their secure implementation. Modified Four Stage Quantum Communication protocol (MFSQC) is proposed in this paper. It is the extension of Subhash Kak's TSQC protocol. The fundamental modifications are proposed in TSQC protocol so that the later can transfer data in high level language rather than currently adopted bit by bit data transfer approach.

II. BACKGROUND

Quantum Cryptography started with the introduction of BB84 protocol in the year 1984 [3]. The protocol used single light photon to transfer one bit of data. To be precise, the protocol used the polarization states of photons to realize the key distribution. Quantum physics states that it is generally impossible to gain any precise information about the unknown polarization state of a single photon and once the

 Copyright 2017.All rights reserved.

polarization of the photon is measured, its polarization is irreversibly altered. So if the exact polarization of photon was not known before it was measured, a measurement will not reveal that exact polarization. This is known as No-Cloning theorem. Due to this theorem, an unknown quantum state of a single photon cannot be copied. This theorem is why quantum cryptography claims to provide unconditional security to the communication process. This theorem is the basis of every quantum cryptographic protocol. First quantum cryptography protocol, BB84 protocol, was designed to establish a secret key between two parties. The established key was then used to scramble actual communication. This key was established over the communication channel popularly(Quantum Channel). The actual communication was carried out on classical channel. As the time passed many modifications were made in the original definition of this protocol but the basic idea remained the same, "Quantum channel will be used for key distribution, and once the key is established, actual communication will be done on the classical channel using that previously shared key". This communication approach dominated quantum cryptographic domain for nearly two decades. In year 2006, Subhash Kak introduced the TSQC protocol. This protocol brought the paradigm shift, it obliterated the need of classical channel and thus broke the 20 year long tradition of using two channels for communication. A big achievement indeed! Due to the use of only a quantum channel, TSQC protocol enjoys the benefits 'no cloning theorem' during the whole communication process. The main drawback of TSQC protocol is that it needs three signals to send one bit data from source to destination, thus the name – three stage cryptographic protocol. It means that, if the ASCII character encoding system is considered – total 3 × 8 = 24 signals are to be exchanged to transmit 1 alphabet. Proposed MFSQC protocol, theoretically, is capable of doing the same work within 4 signals.

III. METHODOLOGY

The foundation of the MFSQC protocol lies in its encoding system. Instead of converting the alphabets into combination of binary bits, each character of the communication language is assigned a particular unique light intensity. The upper boundary of this light intensity is established in advance by the agreement between communicating parties. MFSQC protocol also uses a filtering polarizer at the destination, to filter out incoming light before measuring its intensity. For the scope of this paper, from here on light will mean linearly polarized light. In the MFSQC protocol intensity of output light depends upon the angle between the direction of polarization of light and the direction of the axis of filtering polarizer. This property of light is explained by Malu's law in optical physics. Thus the intensities assigned to each character in the encoding system corresponds to angles between prepared state of polarization of photons (at the Sender's end) and the axis of polarizer used as filter before measuring the output intensity (at the Receiver's end). The encoding system is illustrated in Figure 1.

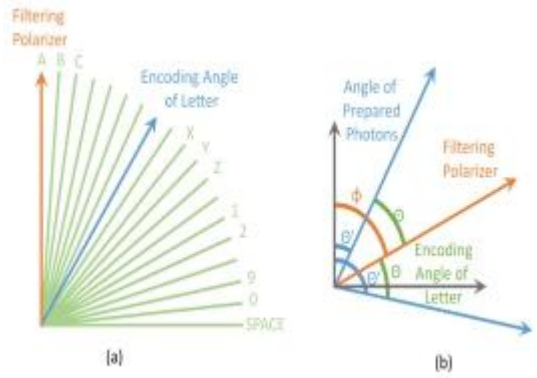

Figure 1 - Encoding of Alphabets in Angles (A) Fixed Filtering Polarizer (B) Random Filtering Polarizer.

FSQC encoding system assigns each character in the communication language, a particular angle in the range of 0o to 90o. A restricted range of 0o to 90o angles is implied because, intensity values are repeated in each quadrant of the coordinate system. For example, for the filtering polarizer aligned at say 0o and input light polarized at say θ = 60o will produce output intensity Io = Icos260o = I/4 which is exactly what is obtained for θ equal to 120o or
240o or 300o. Hence this restriction on the encoding range, between 0o to 90o, is required to ensure unique intensity values.
Section III-I uses this convention and explains the working of FSQC protocol.

IV. I MODIFIED FOUR STAGE QUANTUM COMMUNICATION PROTOCOL

The whole process of MFSQC protocol is shown in Figure 2. This process is explained in step by step manner in the algorithm given below.

- Sender will send INITIATE signal to Receiver.
- On receiving INITIATE signal Receiver will
- Choose random angle between 0o to 360o as the angle of filtering polarizer φ and will prepare photon pulse polarized at this angle.
- Then he will select a random private rotation angle φB and will rotate the photon pulse with φB and send the result towards Sender.
- Sender will apply rotation equal to her privately chosen angle φA, set the flag bit and send the modified photon pulse towards Receiver.
- Receiver will reverse his private rotation φB and send the pulse back to Sender.
- Sender will also reverse her rotation φA.
- At this moment she will have photon pulse polarized at an angle chosen by Receiver as an angle of filtering polarizer φ.
- Now she will rotate the resultant pulse with the angle θ corresponding to the letter she wants to communicate with Receiver and finally send the resultant light pulse towards him.
- This rotation θ can either be clockwise or anticlockwise. Choice will be made by Sender with coin toss.

 Copyright 2017.All rights reserved.

- Receiver will now measure the intensity of the incoming photon pulse after passing it through the polarizer aligned at an angle φ, thus receiving intensity corresponding to the letter sent by Sender.
- The Receiver also check the flag along with the incoming signal intensity.
- Steps 2 through 6 will be repeated until STOP signal comes from Sender.
- When Sender is done with the communication she will send STOP signal to Receiver ending the conversation.

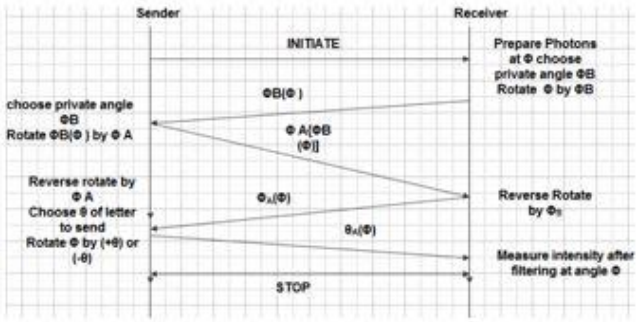

Figure 2 – Modified Four Stage Communication Protocol.

V. DISCUSSION

In the MFSQC protocol, presented in, angle of filtering polarizer (φ) will be randomly selected by Receiver for each character. Sender will prepare light pulse taking this angle as reference. Thus the first requirement of the protocol is to securely communicate Receiver's secret angle with Sender for each character. Steps 1 through 5 (a), of the algorithm, does this work. Sender then prepares the light pulse, for the character to be communicated, with respect to the received angle. At this stage before sending the actual encoded data on the network Sender has the chance to judge the security of quantum channel, this option is not available in TSQC protocol. If she is satisfied with the integrity of communication channel, then only she sends the encoded light pulse to Receiver. This is the most distinguishing feature between TSQC and FSQC protocols. Receiver then measures the intensity after passing the incoming light through a filtering polarizer aligned at φ.

Overall result of the protocol proposed in Section III-I will be that Receiver will get the intensity of light corresponding the letter sent by Sender at the output.

The actual polarization angle of photons that is exposed over network is random which depends on three factors.

- φ the angle of the polarizing filter chosen by Receiver which is random.
- θ the angle corresponding to letter that has to be sent as part of message and
- The random choice of Sender whether to add (clockwise rotation) or to subtract (anti-clockwise rotation) the offset angle ($|\varphi - \theta|$) from the reference angle of measurement (φ).

Thus even though an eavesdropper, Eve, somehow figures out the polarizing angle of sent photons (which itself is very unlikely) she will not get the correct intensity at output unless she knows the angle of polarizing filter for that alphabet. The information about the encoding angle is divided in three parts. Thus to figure out the actual filtering angle with certainty, Eve will have to gather valid data in each of the first three stages of communication. No cloning theorem makes this impossible. In addition to that Eve will have to attempt decrypting the message at runtime because she could not save the quantum states for later experimentation. This imposes time constraint on Eve's activities. The siphoning attack as suggested in Paper [6] will not work here because diverting the portion of photon pulse will change the intensity of light thus messing up the correct output intensity. Strategy to replace siphoned photons with photons of random polarization, as mentioned in Paper [7], will also fail because Receiver is not measuring the incoming photon pulse directly. First the light pulse is passed through filtering polarizer and then it is measured. This mechanism of FSQC protocol is useful to detect the presence of random polarization photons. The most an eavesdropper, Eve, can do is to block the communication channel by continuously siphoning photons. She could not modify the message as per her wish because she does not know the final measurement angle, thus any intervention be her side will produce gibberish at the receiver side providing integrity of communication. In TSQC protocol sensitive message is divided into 3 parts (1 per stage of communication). Unless the eavesdropper has access to all three of these parts she cannot decode the message. MFSQC protocol makes this process even difficult for the eavesdropper by dividing the message in 4 parts. Unlike TSQC protocol, MFSQC protocol gives Sender the chance to judge integrity of the communication channel before sending actual data. If she finds that channel was compromised during key exchange (she can do this by measuring light intensity as mentioned in Paper [6]) she can abstain herself form sending the data. This feature makes FSQC protocol much more superior than current TSQC protocol. TSQC protocol and its variants iAQC, ISA [9] requires 3 signals to be sent over network to securely transfer 1 bit of data, which means total $8 \times 3 = 24$ signals have to be sent to transfer 1 alphabet. MFSQC protocol proposed in this paper requires only 4 signals to securely transmit 1 alphabet. When it comes to knowing the angle of filtering polarizer chosen by Receiver, even Sender does not know what the angle is. She only modifies the photon pulse obtained in Step 5 (a) of protocol explained in Section III-I. Light pulse at step 5 (a) is polarized at the angle of polarization filter chosen by Receiver for current character. The encoding system of FSQC protocol is restricted to 90o window because absolute value $|\cos 2\theta|$ (Malu's Law) is unique for this window only. Thus the intensity is unique for this window only.

VI. CONCLUSION

The Modified Four Stage Quantum Communication Protocol proposed in this paper modifies Subhash Kak's 'three stage quantum cryptography protocol' and may makes it probably 6 times more efficient. It also gives the Sender a chance to judge the serenity of communication channel before sending actual data. Proposed protocol can directly communicate in

 Copyright 2017.All rights reserved.

high level language like English instead of traditional binary communication approach and the number of characters capability of the protocol will be increased. Author's work in this paper provides a novel way of using light in the process of quantum communication. This communication system is especially suitable in the secure communication of bank transactions. Adopting this system for the back-end cloud server communication will reduce the network traffic immensely. This system is also perfect for communicating mission details in military.

REFERENCES

[1] S. Kak, March, 2006, "A three-stage quantum cryptography protocol," Foundations of Physics Letters, pp. 293–296. Available at: <http://arxiv.org/abs/quant-ph/0503027>[Accessed 20 November, 2014]

[2] W. P. Eleanor G. Rieffel, September. 2000, "An introduction to quantum computing for non-physicists," ACM Comput. Surv., vol. 32, no. 3, pp. 300–335. Available at: <http://doi.acm.org/10.1145/367701.367709>[Accessed 19 November, 2014]

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

[4] S. Mandal, G. Macdonald, M. E. Rifai, N. Punekar, F. Zamani, Y. Chen, S. Kak, P. K. Verma, R. C. Huck, and J. J. S. Jr., 2012, "Implementation of secure quantum protocol using multiple photons for communication," CoRR, vol. abs/1208.6198. Available at: <http://arxiv.org/abs/1208.6198> [Accessed 20 November, 2014]

[5] Kak, S., 2013, Threshold quantum cryptography. CoRR, abs/1310.6333. Available at: <http://arxiv.org/pdf/1310.6333>[Accessed 20 November, 2014]

[6] S. Kak, Y. Chen, and P. K. Verma, 2012, "iaqc: The intensity-aware quantum cryptography protocol," CoRR, vol. abs/1206.6778. Available at: <http://dblp.uni-trier.de/db/journals/corr/corr1206.html#abs-1206-6778> [Accessed 20 November, 2014]

[7] S. Chitikela, 2013, "Intensity and state estimation in quantum cryptography," CoRR, vol. abs/1302.1823. Available at: <http://arxiv.org/abs/1302.1823> [Accessed 14 November, 2014]

[8] Chen, Y.; Kak, S.; Verma, P. K.; Macdonald, G.; Rifai, M. E. & Punekar, N. 2013, Multi-photon tolerant secure quantum communication - From theory to practice., in 'ICC' , IEEE, , pp. 2111-2116 .

[9] J. H. Thomas, 2007, "Variations on kak's three stage quantum cryptography protocol," CoRR, vol. abs/0706.2888. Available at: <http://arxiv.org/abs/0706.2888> [Accessed 12 November, 2014]

[10] Mandal, S.Macdonald, G. ; El Rifai, M. ; Punekar, N. ; Zamani, F. ; Yuhua Chen ; Kak, S. ; Verma, P.K. ; Huck, R.C. ; Sluss, J., Jan, 2013, "Multi-Photon Implementation of Three-Stage Quantum Cryptography Protocol", in 'Information Networking (ICOIN), 2013 International Conference – Bangkok.', IEEE, pp 6-11.

[11] P. Basuchowdhuri, 2007, "Comparing bb84 and authentication-aided kak's three-stage quantum protocol," CoRR, vol. abs/cs/0703092. Available at: <http://arxiv.org/abs/cs/0703092> [Accessed 10 November, 2014]

[12] Valerio Scarani, C. K., 2012, The black paper of quantum cryptography: real implementation problems. Available at: <http://arxiv.org/abs/0906.4547v2> [Accessed 15 November, 2014

 Copyright 2017.All rights reserved.