DESIGN AND DEVELOP BB84 PROTOCOL

Octavian RĂDUCANU, Cristina BODOGA

Technical University of Moldova, Str. Studenților 7, Chisinau, Moldova

Since ancient times, methods of coding information have been used to ensure confidentiality. Roman Emperor Caesar proposed among the first a substitution-based encryption algorithm. Today it is called Caesar Cipher. The idea was simple, replacing the letters according to a key initially established and known to both the source and the recipient. Today, however, the amount of information is growing exponentially, computers have made available to mankind the computing power as it never was before. Therefore, the confidentiality of the data has been attacked.

Quantum cryptography comes with a completely different approach to traditional systems. The distribution of keys is completely random and driven by the principles of quantum mechanics. Thus, it is almost impossible to intercept the transmission of information. Given that quantum cryptography is environmentally sensitive and requires extremely sophisticated technology, research has led to the development of several protocols. In this article, one of the most known quantum protocols called BB84 will be analyzed. This protocol is developed both in the real environment and with the help of the computer simulator. The distribution of the keys takes place between Alice (the source) and Bob (the destination). Within the physical machine, the distribution is performed using light particles called a photon. Their polarization process leads to an observable phenomenon. Thus, the source uses slots for polarization under angles defined by the device construction. And the destination uses diagonal or vertical bases for reception. In this transmission the most important is confirmation. Within the standard protocol the confirmation is made by communicating the bases that were randomly selected by Bob (the recipient). Next, a new method of confirming information, the Quantum Teleportation method, will be investigated and implemented. This method involves the direct transmission of the information, to the bits used through the same communication channel as the BB84 protocol. This medium being fiber optic. The advantages of this method of confirmation include speed, increased security, working in parallel with the protocol. But in the real environment there are deficiencies. Even if this method is functional in the simulator, there are technological deficiencies and environmental interference in the real environment. Synchronization can be easily distorted by vibration, radiation, noise.

However, if these deficiencies are eventually overcome, a new era of security of information transmission will be introduced with the system. In the following, the fundamental principles of quantum mechanics on which both the protocol and teleportation are based will be explained and implemented. Both modes of operation, both the physical machine and the simulator, will be designed and described. On the practical side, the synchronization test of the teleportation protocol will be performed using the specialized programming language and the processing core from Microsoft. Also the aim will be to improve the security of the protocol by increasing the number of bits transmitted at random as well as the conversion from bit to qubit. The supreme test being the presentation of the synchronized work on the resonance between the protocol and the teleportation method. Executing as a causal dependency between these two methods. In the real environment, afterwards if it will be possible to test the protocol together with the teleportation, more precisely it can be established and adjusted their functioning. Within the real system there is also a parameter that is used in quantum mechanics or in the simulator, time. This may be a limitation because, if the timing is not properly calibrated, the laser beams will collapse over time. Any carrier information of a particle will be blocked in this area. This deficiency will also be analyzed with some potential

solutions. The problem having no direct solution, there are only solutions that come from applied mathematical equations. Structurally, quantum logic gates for circuits will be used within the simulator. The mathematical definition will be presented with the explanation of their use and the principles of quantum mechanics that represent them. The similarities as well as some common features of both the protocol and the teleportation, from the mathematical perspective will represent research and testing. The development together with the testing will be parallel since theoretically it is far too complex to predict how the physical system will behave by applying different facto.

As a result implementation, was able to achieve higher security check in key distribution system in simulator. Because we have limited access on physical resources as memory, CPU power and in general computer power, it was necessary in experiment to set relatively low key rate generation. But because added additional quantum gate for processing bits, was able to increase security, respectively lower latency . This consequence is valuable only on relatively short keys generation. If quantum bits are in higher number simulated and processed , performance will drop significantly.

Keywords: *Quantum Cryptography, Key Distribution, Photon, Polarization*

References

1. Mart Haitjema, A Survey of the Prominent Quantum Key Distribution Protocols [Online Resource].- Access Link: https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/
2. Nikolina Ilic, The Ekert Protocol [Online Resource].Access Link: http://www.ux1.eiu.edu/~nilic/Nina's-article.pdf
3. Jennifer Seberry, Yuliang Zheng, Shared cryptographic bits via quantized quadrature phase amplitudes of light [Online Resource].Access Link: https://www.sciencedirect.com/science/article/abs/pii/0030401895006885
4. Yi Zhao, Bing Qi, Simulation and Implementation of Decoy State Quantum Key Distributionover 60km Telecom Fiber [Online Resource].Access Link: https://ieeexplore.ieee.org/document/4036338
5. Mohsen Sharifi, A Simulative Comparison of BB84 Protocol with its Improved Version [Online Resource].Access Link: https://www.researchgate.net/publication/228571205_A_Simulative_Comparison_of_BB84_Protocol_with_its_Improved_Version
6. Subhashree Basu, Modified BB84 Protocol Using CCD Technology [Online Resource].Access Link: http://file.scirp.org/pdf/JQIS_2016032215480272.pdf
7. Bechmann-Pasquinucci, S. Mertz Six-State Protocol [Online Resource].Access Link: https://www.revolvy.com/page/Six%252DState-Protocol
8. Charles H. Bennett, The B92 Quantum Coding Scheme [Online Resource].Access Links: http://www.cki.au.dk/experiment/qrypto/doc/QuCrypt/b92coding.html
9. Leilei Li, The security analysis of E91 protocol in collective-rotation noise channel [Access Resource].Access Link: https://journals.sagepub.com/doi/full/10.1177/1550147718778192
10. Alexander Ling, Ivan Marcikic, Matt Peloso, Experimental E91 quantum key distribution [Online Resource].Access Link: https://www.researchgate.net/publication/252207648_Experimental_E91_quantum_key_distribution