BB84 Quantum Key Distribution Protocol

Pritheesh Panchmahalkar

Bobby B. Lyle School of Engineering

Southern Methodist University

Dallas, TX

ppanchmahalkar@smu.edu

*Abstract*—The security of the internet depends on encryption. Quantum algorithms like Shor’s algorithm could be used to break public key cryptographic algorithms like RSA which assumes that the factorization of large numbers is computationally expensive. To counter quantum algorithms, quantum technology could be used for encryption schemes. In this paper, we discuss the first quantum key distribution scheme, BB84 quantum key distribution protocol developed by Charles Bennett and Gilles Brassard in 1984.

*Keywords—BB84, Quantum Key Distribution, QKD protocol*

1. INTRODUCTION

With quantum technology becoming a reality, we need techniques that are secure against the quantum attacks. The cryptographical methods that are resistant to the quantum attacks are referred to as post-quantum or quantum-safe cryptography. BB84 is a quantum key distribution protocol which was coined by Charles Bennett and Gilles Brassard in the year 1984 and hence the name BB84. Quantum key distribution is a mechanism of sharing a private key among two parties using two channels; an authenticated classical channel and a quantum channel.

We will use the classical cryptographical notation to represent the two parties Alice and Bob who want to communicate with each other privately, and an eavesdropper Eve who tries to intercept their communication and read their messages.

1. BB84 Quantum key distribution

Without the knowledge of the key, it is difficult to break the encryption algorithm i.e., the data is safe as long as the key is kept safe and private. Quantum key distribution provides a mechanism to distribute the key among the two parties. It takes advantage of the quantum mechanics to ensure that the key being shared is not intercepted. Even if Eve tries to intercept the data, the scheme detects that the breach and discards the key and generates a new key.

...

In this paper, we will discuss about the qubits, quantum channel, the bb84 protocol, bit error rate

##### iii References

1. I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
2. A. I. Nurhadi and N. R. Syambas, “Quantum Key Distribution (QKD) Protocols: A Survey,” 2018 4th International Conference on Wireless and Telematics (ICWT), 2018.

1. C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing," in Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing. Bangalore, India, December 10 -12,1984. pp. 175-179.
2. Y. Wang, H. Wang, Z. Li, and J. Huang, “Man-in-the-middle attack on BB84 protocol and its defence,” 2009 2nd IEEE International Conference on Computer Science and Information Technology, 2009.
3. F. Zamani and P. K. Verma, “A QKD protocol with a two-way quantum channel,” 2011 Fifth IEEE International Conference on Advanced Telecommunication Systems and Networks (ANTS), 2011.
4. S. Salemian and S. Mohammadnejad, “An error-free protocol for quantum entanglement distribution in long-distance quantum communication,” Chinese Science Bulletin, vol. 56, no. 7, pp. 618–625, 2011.
5. V. Padamvathi, B. V. Vardhan, and A. Krishna, “Quantum Cryptography and Quantum Key Distribution Protocols: A Survey,” 2016 IEEE 6th International Conference on Advanced Computing (IACC), 2016.
6. J. Bobrysheva and S. Zapechnikov, “Post-Quantum Security of Communication and Messaging Protocols: Achievements, Challenges and New Perspectives,” 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2019.
7. A. I. Nurhadi and N. R. Syambas, “Quantum Key Distribution (QKD) Protocols: A Survey,” 2018 4th International Conference on Wireless and Telematics (ICWT), 2018.
8. A. Gabriel, B. Alese, A. Adetunmbi, and O. Adewale, “Post-Quantum Crystography: A combination of Post-Quantum Cryptography and Steganography,” 2013 IEEE Third International Conference on Information Science and Technology (ICIST), 2013.

These references are tentative as I first thought I would be working on the comparing few protocols in quantum key distribution.