BB84 Quantum Key Distribution Protocol

Pritheesh Panchmahalkar

Bobby B. Lyle School of Engineering

Southern Methodist University

Dallas, TX

ppanchmahalkar@smu.edu

*Abstract*—In this paper, we discuss one of the first Quantum Key Distribution Protocols, BB84 protocol proposed by Bennett and Brassard in 1984. Quantum Key Distribution is the mechanism of sharing a secret key among two parties that wish to encrypt their data using the shared secret key and encryption algorithms of their choice. BB84 uses both quantum channel and a public channel for communication of messages to agree upon a common key. We also discuss how an eavesdropper can be detected based on the no cloning theorem of the quantum mechanics and also focus on the various approaches for the last phase of the BB84 protocol called as the reconciliation phase which reduces the Quantum Bit Error Rate (QBER).

*Keywords—BB84, Quantum Key Distribution, QKD protocol, Quantum Bit Error Rate (QBER), Reconciliation phase, Qubit*

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. For a cryptographic symmetric encryption algorithm to be used, the end users need to use a shared key. To share the key, techniques like Diffie-Hellman key exchange use mathematical computations. Quantum key distribution uses the quantum physics to ensure security of the key shared among the two parties. It generates a random key for encryption and decryption algorithms. QKD uses two channels for communication; an authenticated classical channel and a quantum channel. Qubits are transmitted in the quantum channel as photons. The Qubits are quantum bits, which result by encoding the bits (0s or 1s) using one of the two orientations.

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 tries to intercept their communication and read their messages. For a secure communication, Alice and Bob need a shared key to encrypt their communication using a symmetric key algorithm, say, AES. Quantum properties allow Alice and Bob to communicate in public channels even if Eve tries to intercept their communication.

1. BB84 QUANTUM KEY DISTRIBUTION PROTOCOL

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 a Quantum key distribution mechanism, quantum channel and an authenticated classical channel are used for communication between Alice and Bob to generate a new private key. Both the channels are public and are subject to eavesdropping. The quantum channel is not used for any meaningful communication but is used to send random bits between users who do not share any kind of secret information initially. Based on the sequence of messages exchanged in the quantum channel and the ordinary classical channel, the end users come to an agreement for a shared private key. If an eavesdropper happens to measure the photons being exchanged in the quantum channel, then the original information that is transmitted by a user is disturbed based on No cloning theorem[TODO:]. If a quantum state is read or measured, then the quantum state is disturbed hence modifying the actual information being sent. There is a high probability to detect the eavesdropping in the quantum transmission. If eavesdropping is detected, then the current process of generating a key is stopped and the whole process is started again to generate a new key, or they could choose to defer the process. After they agree upon a shared private key, they use it as a one-time pad to encrypt their communication or any other required cryptographic purposes which require secret communication.

Alice first generates a random bit string consisting of bits 0s and 1s. The generation of the random bit string should have the following properties.

1. It should be a random process i.e., there shouldn’t exist a pattern to guess the next bits after observing a few bits.
2. Should have roughly equal length of 0s and 1s.
3. Should not have 0s and 1s appearing for long length successively.

She generates another random sequence of bases, rectilinear (+) or diagonal (x) which is the same length as the random bit string. The random generation of bases should also have the same properties as for the generation of random 0s and 1s. She encodes the generated random bit string using the random sequence of bases which generates photons in one of the four possible states. A basis is an orientation. It could be one of two:

1. Diagonal Basis and,
2. Rectilinear Basis.

These photons represent one bit of string based on the generated basis. For a rectilinear basis, one is represented by 90-degree photon and zero is represented by a 0-degree photon. For a diagonal basis, one is represented by 135-degree photon and zero is represented by a 45-degree photon.

TABLE I. BASIS ENCODING

|  |  |  |
| --- | --- | --- |
| Basis | Bits | |
| 0 | 1 |
| Rectilinear (+) | → | ↑ |
| Diagonal (x) | ↗ | ↖ |

Table I shows the encoding procedure for the bits based on the basis. Alice transmits these encoded photons to Bob over a quantum channel one by one and records the bit, basis and timestamp before transmission. At this point in time, Alice only shares the photons, but the generated bit sequence is private and only known to Alice. Alice may record the timestamp to detect any unusual delay in transmission which could be due to eavesdropping by Eve. At this point in time, Alice has shared only the polarized state i.e., the encoded bits with Bob.

Bob receives the photons from Alice representing 1s or 0s based on their state represented by the arrows as shown in table 1. Bob also records the timestamps at which he receives the photons. It is also possible that there might be loss in information during the transmission due to imperfect detectors at the Bob’s end or a few photons could be lost in the channel during their transit. He generates new sequence of bases to measure each of the photons received from Alice. This sequence is random and independent of what the message received was. He then measures each of the received photons using the random sequence of bases. If the received photon is in rectilinear representation and the randomly generated basis is also rectilinear then the photon is measured in rectilinear as is. If the basis is diagonal, then either 45-degree or 135-degree photon is generated randomly with equal probability. But the received photon is in diagonal representation say 45-degree or 135-degree and the randomly generated basis happens to be a rectilinear basis then the photon is measured as a 0-degree or a 90-degree photon with an equal probability.

TABLE II. MEASURING PHOTON BASED ON RANDOMLY GENERATED BASIS AT BOB’S END

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bob’s basis | Received Alice’s transmitted photon | | | |
| → | ↑ | ↗ | ↖ |
| Rectilinear (+) | → | ↑ | → or ↑ | → or ↑ |
| Diagonal (x) | ↗ or ↖ | ↗ or ↖ | ↗ | ↖ |

Table II illustrates how Bob measures the received photons from Alice through the quantum channel. When Bob chooses basis that is not the same as the one chosen by Alice, and Bob measures the photon the actual information sent by Alice is lost. The received photon is in diagonal representation and the randomly chosen basis is also diagonal basis then the photon is measured with the same value. The values measured correspond to a binary 0 or 1. If the photon is either a 0-degree photon or a 45-degree photon, it corresponds to a binary zero, and if the photon is either a 90-degree photon or a 135-degree photon, it corresponds to a binary one which is similar to the way Alice encodes the binary bits using her random bases.

TABLE III. IDENTIFYING BITS

|  |  |
| --- | --- |
| Orientation | Bit Value |
| → | 0 |
| ↑ | 1 |
| ↗ | 0 |
| ↖ | 1 |

Table III illustrates how bob identifies bit information using the output obtained by measuring the Alice’s photons with his bases. Bob and Alice both have a sequence of bits they can compare and come to an agreement for a private key if no eavesdropping is detected. After measuring all the photons received Bob communicates with Alice now sends the bases, she chose to encode the bits over a public channel to Bob for the first time. She is not concerned about the privacy of bases as the communication of the key has already taken place.

Alice may analyze the timestamps received from Bob against the recorded timestamps when she sent the photons to check for unusual delay in the transmission. If the communication in the quantum channel is not disturbed, Alice and Bob should agree upon the bits encoded the photons. Bob checks the bases Alice has sent against the bases he randomly chose earlier to measure Alice’s photons. He discards the information that didn’t match the bases, Alice has sent and identifies the bits represented by the left-over information and shares it with Alice. A one-time pad is generated and can be used by Alice and Bob to encrypt their communication using one the various available encryption algorithms.

It is possible that the bits that Bob identifies are the same as generated by Alice when he chooses a different basis to measure the photon as the process is random but at the same time it is also possible that it is incorrect. Roughly on an average, more than half the bits produced after measurement of photons match the one’s generated at Alice’s end. In the presence of Eve, if she measures the photons that Alice sends, then when there is a difference in the basis with which she measures the photon and the basis Alice chooses to encode her bit, she generates a photon which is in different orientation and retransmits the measured photons to Bob. Assume that before Alice has shared her randomly generated bases with Bob, Eve intercepts the communication and retransmits her measured photons to Bob. Any measurement resulting in b bits of expected information must induce a disagreement with probability at least b.2 if the measured photon, or an attempted forgery of it, is later re-measured in its original basis. [refer 1984 paper]. Suppose that Eve measures all the photons in diagonal bases and retransmits the measured photons to Bob. In the process of measurement, Eve could be right for about half of the times. Consider the times where Eve goes wrong and if re-measured with the original bases, the retransmitted bits induce disagreements in one-fourth of those. Hence, when Eve attempts to eavesdrop and tries to measure the photons sent by Alice, she introduces more errors in the process as the information is lost whenever she measures incorrectly and can be easily detected.

Hence, to detect eavesdropping Alice and Bob can adopt the following procedure. Bob shares some of the bits with Alice over the public channel. The bits chosen by Bob are random and the size to be chosen could be around one-third to one-fourth of the original size of the key agreed upon. If all the comparisons are right, then it is safe to assume that the transmission was not disturbed and hence, they agree upon a key. If eavesdropping is detected, they simply discard the present key and start the whole process again and create a new key. In the process of eavesdropping, it is also possible that Eve could be clever and be disturbing only the subset of information and hence remaining undetected in the process. She could obtain part of information of the key and the whole process appears to be a disturbance in the quantum channel.

Summarize the whole process in list. May be rewrite the eaves dropping part.

Refer: <https://homepage.univie.ac.at/reinhold.bertlmann/pdfs/dipl_diss/PetraPajic_BA_QuantumCryptography.pdf>

Give an example after summarizing.

##### iii References

1. 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