BB84 Protocol

Sriram Devata
2019113007

Algorithm Analysis And Design

Abstract

This document gives an overview of the BB84 protocol for the implementation of Quantum Key Distribution(QKD) and the relevant principles needed to understand it.

Contents

1 Introduction 3

2 Background 3

2.1 Qubits 3

2.2 Measurement of a Qubit 3

2.3 Measurements In Different Bases 4

2.4 Quantum Communication Channel 4

3 Overview of the Procotol 5

4 Simulation Code 6

5 Analysis 6

1 Introduction

All cryptography algorithms depend on secure sharing of keys. Though symmetrical cryptography algorithms are faster over asymmetrical cryptography algorithms, the risk of the shared key being intercepted makes them an inferior choice to an asymmetrical algorithm.

When two parties (for simplicity, assume these parties to be Alice and Bob) are trying to establish communication by sharing keys to encrypt future information exchange, there's a risk of an eavesdropper (for simplicity, assume the eavesdropper is called Eve) intercepting the communication and figuring out the key that Alice and Bob decide to use. Besides having no point of encoding and decoding the information, Alice and Bob are not aware if their key has been compromised and would have the false belief that they have established a secure line of communication.

Using the BB84 protocol, Alice and Bob will know if Eve is eavesdropping and will not use the compromised key for further communication.

2 Background

2.1 Qubits

In any computational devices, a building block is a two-state system (0, 1). In quantum mechanics, any system can exist in a *superposition* of possible states. A qubit is a 2-state quantum system. It can exist in either of the possible states, or in a superposition of the two states. In general, the state of a qubit can be described as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \text{ with } \alpha, \beta \in C \text{ and } |\alpha|^2 + |\beta|^2 = 1$$

2.2 Measurement of a Qubit

The superposition $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is the *private* information of a qubit. In order for us to know the state of the qubit, we have to make a measurement. When we make a measurement, we end up with one bit of information - if the qubit collapsed to the state $|0\rangle$ or $|1\rangle$. It collapses to the state $|0\rangle$ with probability $|\alpha|^2$ and collapses to the state $|1\rangle$ with probability $|\beta|^2$.

Once the qubit collapses to a state after we make a measurement, the superposition of the qubit is lost and it now exists in the collapsed state. This means that it is not possible to find the values $|\alpha|^2$ and $|\beta|^2$ by making multiple measurements on a qubit to get a probability distribution.

A qubit can be visualized as a vector on a plane. The state of any qubit can be expressed as a linear combination of two orthogonal states. Two standard basis sets are the Z-basis states $\{|0\rangle, |1\rangle\}$ and the X-basis states$\{|-\rangle, |+\rangle\}$.

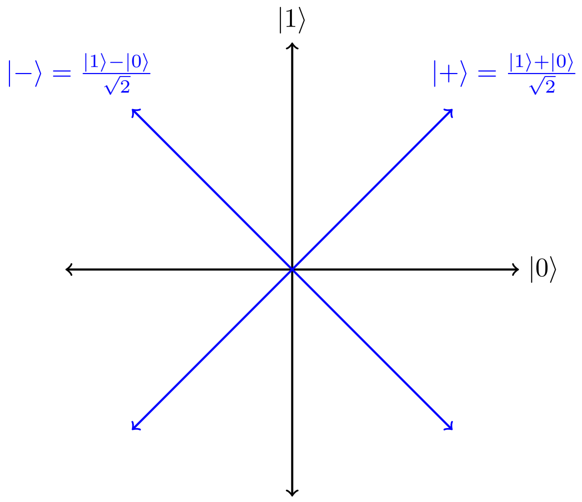

$|1\rangle$
$|-\rangle = \frac{|1\rangle-|0\rangle}{\sqrt{2}}$
$|+\rangle = \frac{|1\rangle+|0\rangle}{\sqrt{2}}$
$|0\rangle$

Figure 1: The Standard(Z) basis and the Signed(X) basis

In general, we can choose any two orthogonal states and express the state of a qubit as a linear combination of these two states.

2.3 Measurements In Different Bases

A central component of the BB84 protocol is the collapse of the qubit when it is measured in a basis different from the basis it was encoded in. For example, if the bit 0 was encoded onto a qubit in the Z basis and is measured in the X basis, the result of the measurement would be 0 or 1 with equal probability.

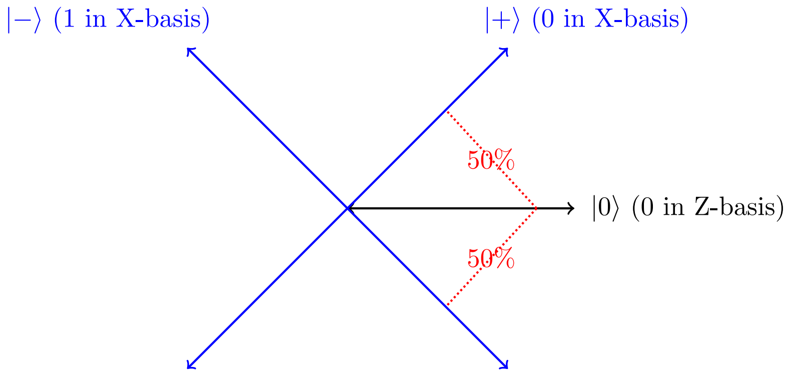

$|-\rangle$ (1 in X-basis)
$|+\rangle$ (0 in X-basis)
50%
$|0\rangle$ (0 in Z-basis)
50%

Figure 2: Measuring Z-basis 0 in the X-basis

2.4 Quantum Communication Channel

Classical communication channels can transmit classical information. Bits can be encoded as high or low voltages. This cannot be used sending and receiving qubits. To transmit quantum information, BB84 utilizes a separate Quantum communication channel to send and receive the states of qubits. The practical implementation of such a communication channel can be a fibre-optic cable that conserves the polarisation of photons. The state of a qubit can be encoded in the polarization of a photon. We can map the possible polarization states of a photon to the vector representation of a qubit.

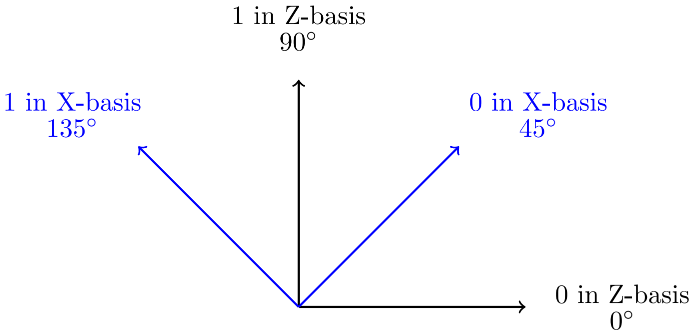


Figure 3: Mapping the Polarization of a Photon to Qubit states

In this particular quantum communication channel, the bits encoded in different bases and the resulting qubits can be shown as ↖, ↑, ↗ and →.

Bit to encode	0						1					
Encoding Basis	Z			X			Z			X		
Photon Polarization	→			↗			↑			↖		
Measurement Basis	Z	X		Z		X	Z	X		Z		X
Measured Bit	0	0	1	0	1	0	1	0	1	0	1	1

Table 1: Qubits when encoded and measured in different bases

3 Overview of the Procotol

The protocol initially assumes that there are two channels(quantum and classical) of communication available to Alice and Bob, and Eve is able to intercept information in both the channels. Alice chooses a random string of bits, and decides to encode each of these bits as a qubit, in either the Z-basis or X-basis at random. She keeps track of the initial bit string and the set of bases she chose to encode each bit. She sends the resulting qubits over to Bob through the quantum channel.

As Bob receives the qubits, he measures each of the qubit in either the Z-basis or X-basis at random. He keeps track of the bits he measures and the bases he chose to measure each qubit. Bob now sends the set of bases he chose to measure each qubit and sends it to Alice. Alice responds to this by telling Bob the qubits for which Bob chose the same bases to measure in. Alice and Bob discard the bits where they both chose different bases to encode and measure.

Alice and Bob take a small subset of the bits and compare them. Assuming that there is proper noise correction and there is no measurement errors, if Eve didn't eavesdrop, Alice and Bob would end up with the same bits. They discard this subset of bits, and use the rest of the bits to form a secret key for further communication.

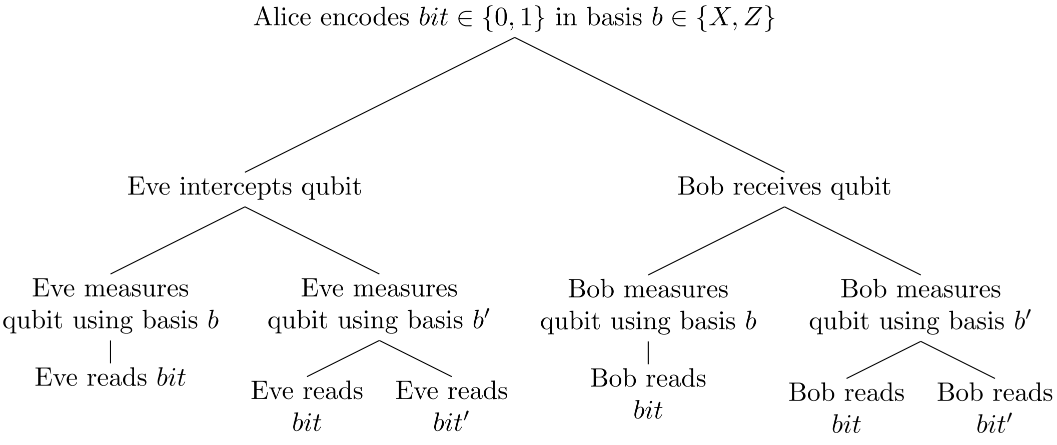
If the small subset of bits do not agree with each other, it would indicate that an eavesdropper, Eve, has intercepted the message, and the communication isn't secure. This is because if Eve wants to figure out the key, she would have to make measurements on the qubits sent by Alice in either of the bases chosen at random. According to the no cloning theorem, she can't make a replica of Alice's qubit to forward to Bob and make a measurement on her copy of the qubit. She either has to send the qubit she has measured, or guess the basis and send a new encoded qubit to Bob.

4 Simulation Code

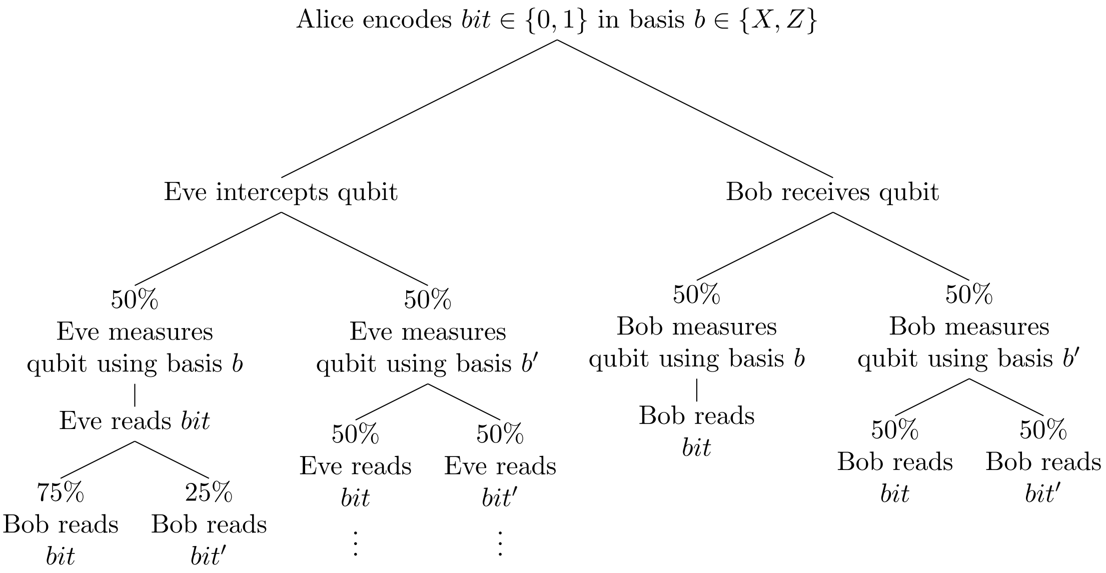
An implementation of the BB84 protocol in Qiskit can be found as an interactive example here.

5 Analysis

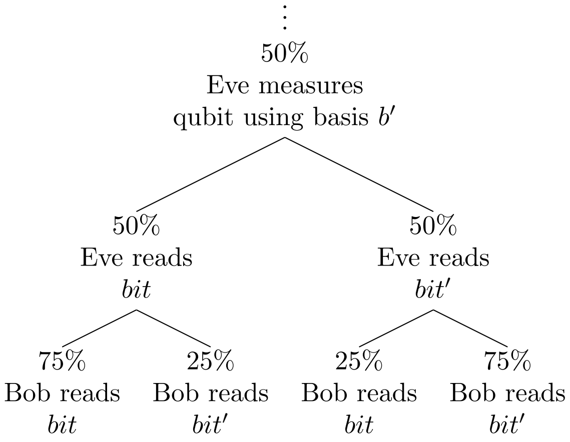
For each bit that Alice encodes, the following flowchart illustrates the bit that Bob will measure if Eve doesn't intercept the qubit, and the bit that Eve measures if Eve intercepts the qubit.


Alice encodes $bit \in \{0,1\}$ in basis $b \in \{X,Z\}$
Eve intercepts qubit
Bob receives qubit
Eve measures qubit using basis b
Eve reads bit
Eve measures qubit using basis b'
Eve reads bit
Eve reads bit'
Bob measures qubit using basis b
Bob reads bit
Bob measures qubit using basis b'
Bob reads bit
Bob reads bit'

Since both Eve and Bob choose the basis to measure in randomly, there is a 50% chance that they choose the right basis. If they choose the wrong basis, there is a 50% chance that they measure the correct bit. In the BB84 protocol implementation attached with this document, Eve forwards the qubit that she already made the measurement on to Bob. This means that in the case when Eve chose the wrong basis and the qubit collapsed to bit', Bob measures bit and bit' with different probabilities.


Alice encodes $bit \in \{0, 1\}$ in basis $b \in \{X, Z\}$
Eve intercepts qubit
Bob receives qubit
50%
Eve measures qubit using basis b
Eve reads bit
75%
Bob reads bit
25%
Bob reads bit'
50%
Eve measures qubit using basis b'
50%
Eve reads bit
50%
Eve reads bit'
50%
Bob measures qubit using basis b
Bob reads bit
50%
Bob measures qubit using basis b'
50%
Bob reads bit
50%
Bob reads bit'

In the case where Eve intercepts the qubit and measures using the basis b',



Such an analysis will help us to choose optimal initial bit string length and the subset of the bit string to choose, to bring the number false negatives of an eavesdropper within the error threshold.