QKD Simulation

Gabriela Mogos
Facultad de Informatica y Electronica, Escuela Superior Politecnica de Chimborazo, Riobamba, Ecuador
gabi.mogos@gmail.com

Introduction
The goal of this study is to understand the alternatives to classical protocols for obtaining cryptographic keys that can be used as substitutes, should quantum computers be realized.

This study explores quantum alternatives to traditional key distribution protocols and involves implementations of Quantum Key Distribution protocol - Bennett-Brassard (BB84) on 2 cases: with and without cyber-attacks.

Implementation

I. Bennett-Brassard without eavesdropper
The study will present the results obtained from the Bennett-Brassard (BB84) protocols software implementation. To implement BB84 protocols, we used C++ language.

On first BB84 simulator, the emitter and the receiver will communicate safety, without the presence of the eavesdropper. To obtain the cryptographic key, both of them will execute the stages of the Bennett - Brassard protocol: bases reconciliation, reconciliation and privacy amplification secret key.

The equipment used for the deployment of simulation of BB84 protocol are computers connected by switches. Each computer has a static IP to communicate over the switch and on each computer will run specific programs: the Emitter and Receiver, respectively.

![Fig.1. Bennett-Brassard protocol ideal — without eavesdropper](image)

We tested the application on a variable number of input data (qubits) and have studied how vary QBER.

After running 10 times the simulation program QKD - ideal, we obtained the following results for an initial key with sizes ranging from 320 to 2560 qubits:
Analyzing the data obtained we can conclude that quantum bit error rate – QBER the final key is around 50%.

II. Bennett-Brassard with eavesdropper

The attack used by the enemy in BB84 simulation program is Intercept-Resend method. The Intercept-Resend attack, called the Fake-State, is the most common type attack used on quantum key distribution systems.

The Eavesdropper, interrupting the quantum channel, measure each qubit received from the Emitter and, then, the Eavesdropper transmits to Receiver other polarized qubits without leaving traces of the attack.

Use of two polarization bases, gives the Eavesdropper a chance to get about 50% of measurements compatible with qubits transmitted by the Emitter.
The probability Eavesdropper chooses the incorrect basis is 50%, and if Receiver measures this intercepted qubits, he gets a random result, i.e., an incorrect result with probability of 50%. The probability an intercepted qubits generates an error in the key string is then 50% × 50% = 25%.

Conclusions

Even if the main disadvantage of quantum key distribution algorithms present the final key is the small size compared to the initial size of the transmitted key, the focus is on getting a unique secret keys with a satisfactory size.

The final key, obtained with any of quantum key distribution scheme can be used together with one-time pad algorithm to create a perfectly safe cryptosystem.

Acknowledgment

This work was financed from Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT) of Ecuador, through Prometeo project.

References