Introduction

Nowadays it is important to have a method to secure the content of messages/information, in order to prevent it from being extracted by unauthorized parties. Systematic schemes for encryption and decryption are called ciphers and were developed all over the years. The interest in cryptology considerably expanded during and after the two world wars, however it was the introduction of the Internet that brought cryptography to the people. Cryptographic technologies now enable, emails, phone and financial communications to be safe on a daily basis. Modern cryptography can also enable authentication, digital signatures and secure multi-party computations. To achieve this goal an algorithm is used to combine a message with some addition information, known as the key, and produce a cryptogram. For a cryptosystem to be secure, it should be impossible to unlock the cryptogram without the key. For a long time, the cryptosystems were divided between two main classes depending on whether the two entities communication with each other, Alice on the transmission side and Bob on the reception, used the same key or not. However, the classic systems are threatened by the advances in the computational power to decode the algorithms used in this type of protocols.

To be able to overcome the adversities, quantum cryptography has a role to play in such alternative systems. Due to the quantum world being inherently probabilistic, different outcomes in quantum experiment occur with different probabilities. And so, instead of using a bit, which regardless of its physical representation, it is always read as either a 0 or a 1, it is used a quantum bit. The qubit represents a unit of quantum information and is described by a state vector in two-level quantum mechanical system which is formally equivalent to a two-dimension Hilbert space. The qubit can be a 0,1 or a superposition of both states which represents the main difference between the classical bit. It is also necessary to look at the set of rules that the quantum physics implies:

-> One cannot take a measurement without perturbing the system.

-> One cannot determine simultaneously the position and the momentum of a particle with arbitrarily high accuracy.

-> One cannot simultaneously measure the polarization of a photon in the vertical-horizontal basis and simultaneously in the diagonal basis.

-> One cannot draw pictures of individual quantum processes.

-> One cannot duplicate an unknown quantum state.

The basic idea is to exploit this quantum mechanical principles and develop quantum key distribution systems with a high level of security.

Motivation

Objectives

The main objectives are divided in the two stages of an implementation of a QKD using DV with polarization encoding. On the transmission side

Results

Structure of the document

QKD using DV with polarization Encoding

Taking in account the properties of the quantum world listed before, the first protocol for quantum cryptography was proposed in 1984 by Charles H. Benett, of IBM and Gilles Brassard, of the University of Montreal, hence the name BB84, as this protocol is known. First, we need to assume the environment in which Alice and Bob are set is highly secure. However, these two entities are connected by a quantum channel, optical fibers, which represents to be insecure when communications are done. An eavesdropper, Eve, is allowed to control this quantum channel, but she cannot check the laboratories in which Alice and Bob are set. Alice encodes her random bits on the polarization state of single photons using two sets of basis. The first one, Alice uses the horizontal polarization to represent the bit "0" the vertical polarization to represent the bit "1". In the diagonal basis, she uses 45º polarization to represent the bit "0" and 135º to represent the bit "1". For each transmission, Alice chooses in a randomly way in which basis she is going to encode her random number, from the previous set, proving the impossibility of Eve to determine its polarization state. If Eve tries to make a measure in the quantum channel, using a rectangular basis, then she is going to destroy information that is encoded in the diagonal basis.

At Bob's side, without him knowing Alice's basis selection, he randomly chooses either one of the two set of basis to measure the photon coming from the transmission side. If him and Alice chose the same basis, then they can generate correlated random bits. However, if the use different ones their bit values are uncorrelated. To solve this problem, after all the measure photons, he and Alice compare the bases used in the communication through an authenticated public channel. They discard all the random bits generated with unmatched bases and keep the ones that matched.

A quantum key distribution protocol is divided into a quantum transmission stage and reception one where the processing of information is done. This includes the stages of quantum state preparation, transmission, detection, bases comparison and error correction. This type of QKD systems have an intrinsic QBER, which could be originated from the imperfections of polarization control system, background noises, detectors noise.

In the system implemented in the IT laboratory, the receptor could not to a processing of in the incoming information in real time and only worked with one base. In the transmission stage, the current design only allows low speeds in the order of 1Khz to 8Khz. However, the detectors are only limited in the order of the Mhz to the Ghz to there is no reason to have the system working at such low speeds.

Receiver

Transmitter

Conclusions