COMPX304 Assignment 2: Quantum Key Exchange

Stefenie Pickston

28-04-2022

Abstract

In order to encrypt information over an insecure channel, a symmetrical encryption scheme such as a XOR cipher can be used. However, in a symmetrical encryption scheme both the sending and recieving parties must have the same key, which must also be transmitted over the insecure channel without being intercepted by a malicious eavesdropper.

A method to solve this problem is to use a quantum key exchange, where qubits are exchanged instead of regular bits. Qubits are subject to quantum physics.

This assignment will use a 'simplified' version of qubits to mimic quantum mechanics.

This report will cover the software design of a quantum key exchange algorithm, a man in the middle attack on it, the tests conducted and discussion of the test results.