Quantum Reliable Transfer QuaRT

Objective

The objective of this project is to be able to transfer files between two parties while keeping the content of these files secret.

Summary

Quantum Reliable Transfer is a peer-to-peer command line application that allows two parties to transfer files with theoretically perfect secrecy. It uses the Quantum Key Distribution BB84 protocol to generate a shared key between the sender and receiver. The generated key length is the same as the message length in order to use one-time pad encryption to provide perfect secrecy.
The application will stop if it doesn't produce enough min-entropy bits to generate a key with a provided security parameter. However, QuaRT can handle a certain amount of noise and still securely generate key with noisy qubits or some weak attack due to the protocol post processing, which uses Cascade for error correction and Toeplitz matrices-based hashing for privacy amplification.
This application uses the EC-DSA algorithm to sign and verify all classical messages, creating an authenticated channel.

Design Overview

QuaRT was designed in a very simplistic way to allow future extension and easy collaboration. It contains two main classes in two main files, sender and receiver, which control the whole execution. They are responsible for the Quantum Key Distribution protocol and in the end the exchange of files.
Every step of the BB84 protocol and post processing is isolated to create a separation of responsibilities.
The error correction protocol is implemented in a strategy class so it’s trivial to replace the error correction algorithm.
There are modules for authentication and communication that abstract the lower level structures. With this abstraction, changing the signature algorithm (i.e: to RSA) or the structure used to communicate classically (i.e: to HTTP) is trivial.