QChat Description

Matt Skrzypzcyk (mdskrzypczyk)

January 22, 2018

1 Objective

The objective of this project is to explore the implementation of quantum key distribution protocols in real world messaging applications. Specifically, this project showcases the usage of the purified BB84 protocol as a method of establishing shared keys in a chat application setting as well as a demonstration of superdense coding as a means of communicating classical information through a quantum channel.

2 Summary

QChat is a peer-to-peer encrypted messaging application built on Simulaqron that makes use of quantum cryptography protocols to enable secure communications. The application allows researchers to explore simulations of quantum internet protocols and attack vectors on these protocols in adversarial settings. If provided with access to QKD hardware and a python interface, QChat could be used as a proof of concept for a real world messaging platform based on quantum computing.

3 Design Overview

In its current state, QChat is designed around a central registry server that serves as a root database for public information of users in the network. The registry server maintains the username, public key, and IP/port information of the user's server. When user's initiate their servers, they automatically register themselves with the registry server and record their contact information for peer discovery. Once a user, Alice, has registered with the root server, she can begin to query the server for her contact's, Bob, information. Once she has obtained Bob's contact information, Alice will initiate a quantum key distribution protocol with Bob to establish a shared key that can be used for encrypting furhter communications between them with AES-GCM.

In the protocol, the root registry server acts as the EPR source and distributes the qubits used for BB84 to Alice and Bob. The server is capable of manipulating the distributed qubits in any manner, which enables the simulation of adversarial scenarios in the messaging setting. QChat assumes that the classical channel is unauthenticated and users of the network utilize the root server's record of public keys to authenticate themselves to their peers.

The implementation of the purified BB84 protocol utilizes linear codes to perform information reconciliation once the BB84 states have been distributed and measurements have been tested to verify the error rate of the channel. Specifically, the binary Golay code is used for its high data rate. Afterwards, privacy amplification is performed on the reconciled information through the use of a keyless fuzzy extractor.

In addition to classical messaging mechanisms, QChat implements a means of quantum communication through superdense codes. A user, Alice, will stream her message data to her peer, Bob, by encoding pairs of bits of her message onto her qubit of her EPR pair through local operations and will then send this qubit to Bob so that he can decode the information through clever measurements.

Included with the source code is a sample of an implementation of the device independent QKD protocol. The logic of the protocol seems sound, though it was difficult to use the available measurement options in Simulaqron to implement test devices that were able to pass the CHSH test.