A peek at Quantum Cryptography

To the Quantum Future: Final Week

August 1, 2023

Quantum Cryptography is an emerging field at the intersection of Data Security and Quantum Algorithms. We shall introduce an important task in Quantum Cryptography, called **Quantum Key Distribution (QKD)**.

If not familiar with classical key sharing, one can gather the essence of the same via the standard Diffie-Hellman key exchange protocol. Similar to classical key sharing, QKD is the task whose goal is to share a *random* secret key between two parties A and B. No one except the two parties in question knows anything at all, to put it informally, about the secret key. For all you know, it could be absolutely anything with equal probability.

BB84 (named for its inventors, Bennett & Brassard, who came up with it in 1984) is a simple algorithm for QKD. Here we study and implement a simple version of BB84 with IBM Qiskit.

A sidenote: One wonderful thing about QKD is the fact that it can be easily experimentally verified.

Reading material

- QCQI, Sections 12.6.3 until the B92 protocol. The EPR protocol can be studied if interested.
- Make sure to study Box 12.7!

Implementation details

Implement the BB84 algorithm in Python, treating a message as a list of 1-qubit `QuantumCircuits`. Simulate qubit measurements using Qiskit's simulator.

A comprehensive help document (for reference, you must try to write as much code yourself) can be found here to help you with the implementation.