Home-Brew Quantum Key Distribution

Murray, Fletcher (School: Woods Cross High School)

Quantum Key Distribution (QKD) is a cutting-edge cybersecurity protocol that utilizes superposition and quantum measurement to detect an eavesdropper. However it is currently not widely available due to its expense, and the requirement of specialized equipment. The goal of this project was to implement a homemade version of QKD using cheap materials. The first stage of this project was to simulate QKD using IBM's quantum circuit programming language called Qiskit. Bits were encoded onto qubits as quantum circuits and then sent between a sender, a receiver, and a randomly listening eavesdropper. The receiver would perform a measurement on the qubit and record the result of the program. The data indicated that the program correctly detected an eavesdropper when it should, and the chance of detecting an observer increased with a longer qubit key. The second stage of this project built a physical implementation. Quantum states were encoded as the polarization of light through polarizing filters. The same process as described above in the simulation was repeated with the physical implementation by orienting polarizing filters on multiple levels of a homemade dark room. Light intensity for each qubit in a key was recorded and decoded. Keys were put through the machine and categorized on if they they correctly detected an eavesdropper (all keys behaved as predicted). A z-test was performed on the proportion of keys where the machine worked as expected. Further experimentation would involve constructing a fully automated version of the implementation using microcontrollers and motors to control the orientation of the polarizing filters. The ultimate goal of the project would be simplifying the protocol to be used to communicate between computers on network using QKD.

Awards Won: