Improving the Quantum Cryptography Experiment

Tristan Lonsway and Andrei Zhukov
Stony Brook Department of Physics and Astronomy

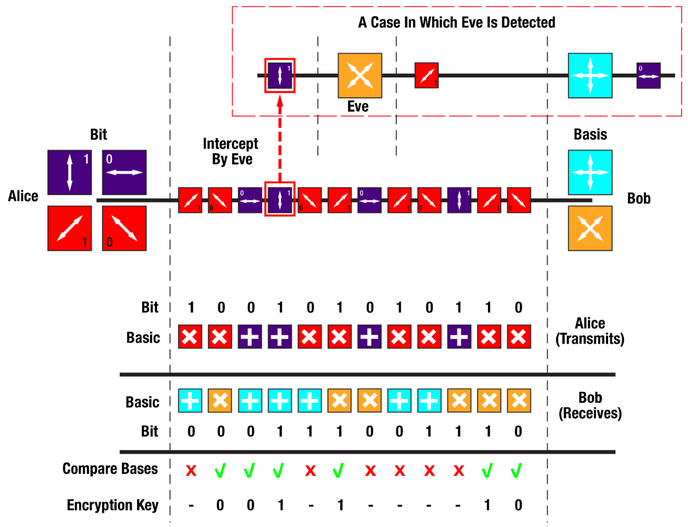
Stony Brook University

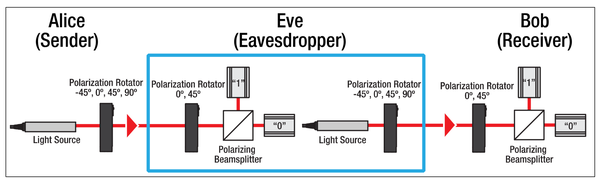
QUANTUM CRYPTOGRAPHY

- The no-cloning theorem prevents a quantum state from being identically copied, so attackers cannot eavesdrop on a quantum channel without introducing detectable errors.
- This experiment demonstrates a Quantum Key Distribution (QKD) protocol, which allows two agents to securely exchange a key for later cryptographic use. For simplicity, we simulate photonic polarization qubits with classical laser pulses.

BB84 QUANTUM KEY DISTRIBUTION

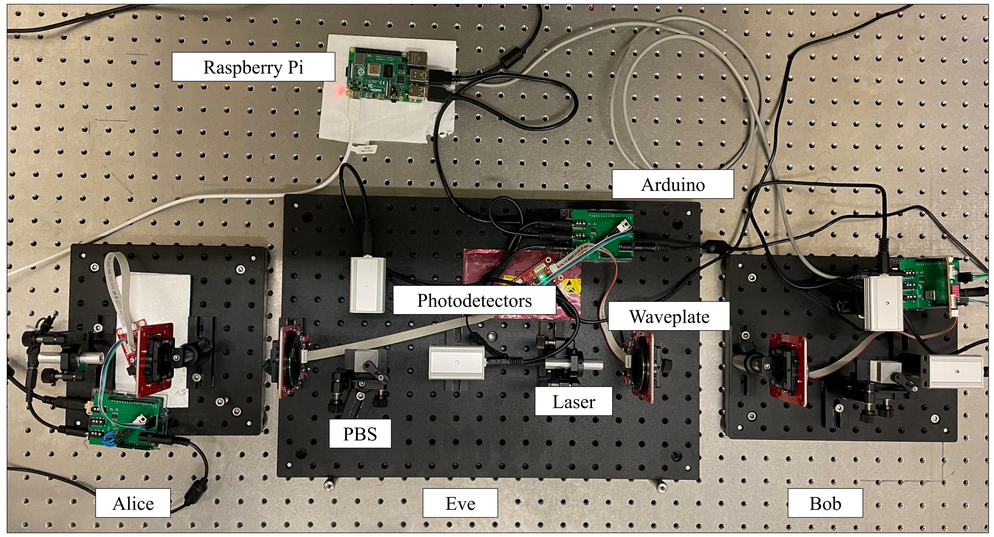
The BB84 QKD protocol shares a randomly generated secret key between a sender (Alice) and receiver (Bob) with the ability to detect a potential eavesdropper (Eve).



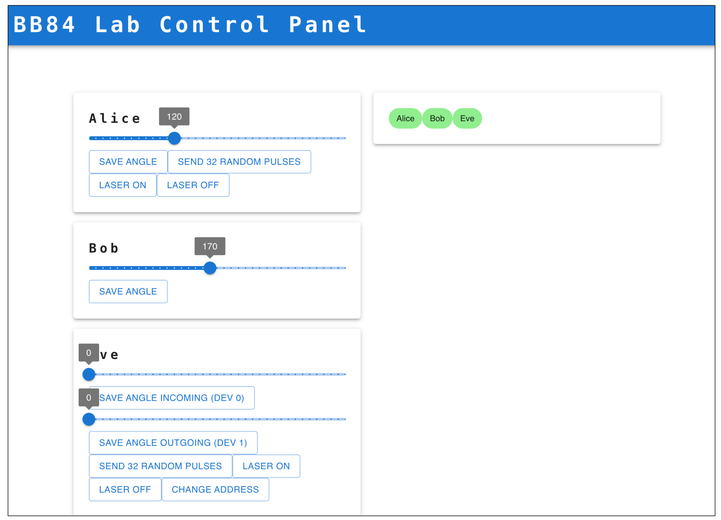


AUTOMATING THE EXPERIMENT

- Our goal was to create a simple and reliable control platform upon which more sophisticated experiments could be built.



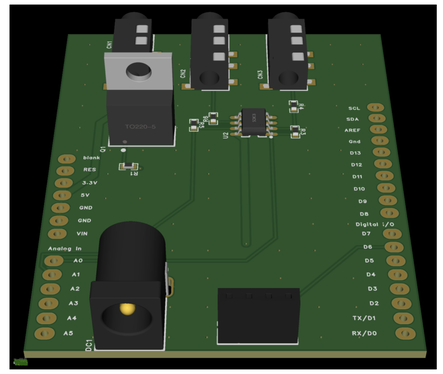
Overview of the experiment setup, with stations for Alice, Bob, and Eve



Work-in-progress browser-based user interface for the lab. Once on the WiFi network hosted by the Pi, users can access this page.

STREAMLINED INTERFACE

- The original interface for this lab consisted of directly sending commands to the individual Arduinos through the Arduino IDE serial monitor.
- We built a new browser-based interface to a Raspberry Pi computer which simultaneously controls all 3 Arduinos.



Rendering of the custom Arduino shields we designed. The shield is designed for the Arduino Rev3 board.

CUSTOM ARDUINO SHIELDS

We integrated all the necessary electronics into a custom designed PCB Arduino shield, enabling the Arduino to do the following:

- Laser control for Alice and Eve
- Rotation mount control for Alice, Bob, and Eve
- Photodetector reading for Bob and Eve

RASPBERRY PI CONTROL CENTER

- To abstract control of the individual Arduinos, we set up a Raspberry Pi with serial USB connections to each station.
- Students connect to the Pi via a wireless network it hosts. Once on the network, the lab dashboard can be accessed via a web browser.

REFERENCES

[1] “Quantum Cryptography Analogy Demonstration Kit,” www.thorlabs.com. https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=9869

[2] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” Theoretical Computer Science, vol. 560, pp. 7–11, Dec. 2014, doi: https://doi.org/10.1016/j.tcs.2014.05.025.