Summary of Key Concepts

Quantum Key Distribution: Part II

Week of December 3, 2023

Resources

- QXQ YLC Week 10 Lab Notebook [STUDENT] v1.ipynb
- 4. QXQ YLC BB84 Cheat Sheet

Key Terms

Key Term	Definition
Hacking	Hacking refers to the methods used to gain unauthorized access to data.
Active Attack	Active attacks modify or destroy information.
Passive Attack	Passive attacks do not affect data. Their purpose is to collect information.
No Cloning Theorem	The No Cloning Theorem states that it is impossible to make a perfect copy of a pure quantum state. The reason for this goes back to the properties of quantum mechanics.

Lecture

Learning Objectives

1. *Recognize* what hacking is, including the difference between active and passive attacks.
2. *Recognize* the role of Eve in BB84, particularly in a measurement attack.
3. *Recognize* that Alice and Bob can almost always detect Eve if they share enough bits due to the no-cloning theorem.

Key Ideas

1. Theoretically, it is impossible to make a passive attack against BB84 protocol since the nature of quantum mechanics turns it into an active attack.
2. The No Cloning Theorem makes it impossible to perfectly replicate a quantum state.
3. QKD, unlike most other quantum algorithms, is possible to implement now.

Lab

Learning Objectives

1. *Recognize* how to implement BB84 in cirq, particularly including a measurement attack by Eve.

2. *Recognize* how to adjust Eve's attack in BB84 in cirq.

Key Ideas

1. Alice and Bob are able to detect Eve because no matter which attack she uses, she alters the state of the qubits that Alice sends to Bob.

2. The more qubits Alice and Bob compare, the more likely they are to catch Eve.