Summary of Key Concepts

Quantum Key Distribution: Part I

Week of November 26, 2023

Resources

- QXQ YLC Week 9 Lab Notebook [STUDENT].ipynb
- QXQ YLC Week 9 Homework Notebook [STUDENT].ipynb
- 4. QXQ YLC BB84 Cheat Sheet
- Python choices function documentation
- Python dictionaries documentation
- Python for loops documentation
- The Original BB84 Paper

Key Terms

Key Term	Definition
Algorithm	A specific procedure for solving a computational problem.
Quantum Algorithm	Quantum circuits for solving a computational problem.
Protocol	A set of standard rules that allow electronic devices to communicate with each other.
Quantum Protocol	The rules that allow multiple quantum computers to communicate and work together.
Cybersecurity	An emerging field of technology that protects our computer and network systems from bad actors.
Cryptography	The set of techniques for secure communication in the presence of eavesdroppers.
Secret Key	A password for secure, *encrypted* communication.
Channel	A way of communicating that can be either public or private. This includes emails, phones, fiber optics, and more.
Encryption	"Hiding" or encoding messages using a secret key so no one without the key understands them.
Decryption	"Unhiding" or decoding messages using the same secret key that was used to encrypt them.
Quantum Key Distribution	A way to share passwords (secret keys) for communication more securely than we possibly can classically.
BB84	A quantum key distribution scheme that relies on quantum superposition and measurement to detect Eve.
Encoding in the Z Basis	Encoding bits into the 0 and 1 states of qubits, which lie along the Z axis of the Bloch sphere.
Encoding in the X Basis	Encoding bits into the + and - states of qubits, which lie along the X axis of the Bloch sphere.

Lecture

Learning Objectives

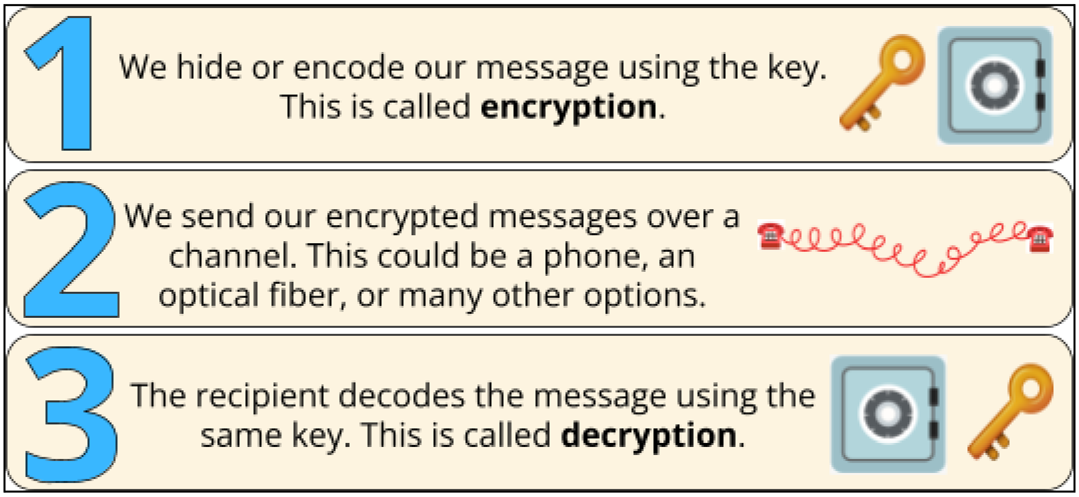
1. *Recognize* what quantum algorithms and protocols are.
2. *Recognize* what quantum key distribution is.
3. *Recognize* the steps of the BB84 protocol.

Key Ideas

1. An **algorithm** is a specific procedure for solving a computational problem. It is like a recipe for a computer.
2. A **quantum algorithm** accomplishes this using quantum circuits.
3. A **protocol** is a set of standard rules that allow electronic devices to communicate with each other. It is like the rules that allow multiple chefs to communicate and work together.
4. A **quantum protocol** allows multiple quantum computers to communicate and work together. The three most famous quantum protocols are:
    a. **Quantum Teleportation**: Send quantum information more efficiently using quantum computers and sending classical bits.
    b. **Superdense Coding**: Send classical information more efficiently using quantum computers and sending qubits.
    c. **Quantum Key Distribution**: Create a secure password for classical communication by sending qubits and classical bits.

5. **Quantum Key Distribution** is a way to share passwords (secret keys) for communication more securely than we possibly can classically.
    a. This is part of a large field known as **cybersecurity** and is specifically a **cryptography** protocol or “scheme”.

6. Cryptography protocols typically follow these three steps:

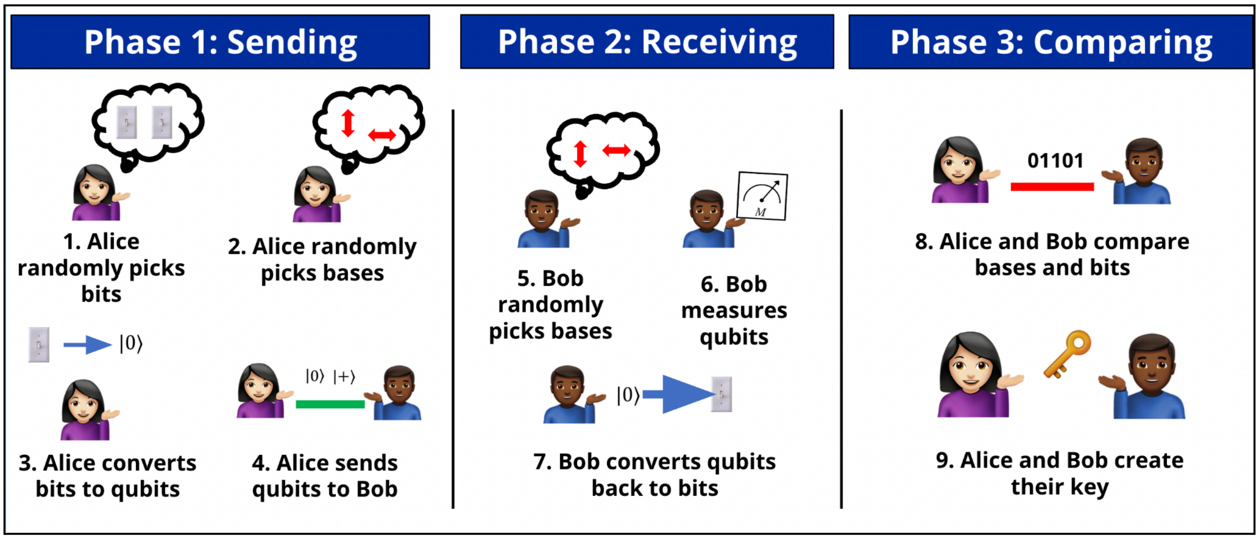


1 We hide or encode our message using the key. This is called **encryption**.

2 We send our encrypted messages over a channel. This could be a phone, an optical fiber, or many other options.

3 The recipient decodes the message using the same key. This is called **decryption**.

7. **BB84**, founded by Charles **B**ennett and Gilles **B**rassard in 19**84**, is a Quantum Key Distribution protocol that relies on quantum superposition and measurement to detect an Eavesdropper. It follows these steps:



Phase 1: Sending

1. Alice randomly picks bits

2. Alice randomly picks bases

3. Alice converts bits to qubits

4. Alice sends qubits to Bob

Phase 2: Receiving

5. Bob randomly picks bases

6. Bob measures qubits

7. Bob converts qubits back to bits

Phase 3: Comparing

8. Alice and Bob compare bases and bits

9. Alice and Bob create their key

Lab

Learning Objectives

1. *Recognize* how to use three useful python tools: the choices function, dictionaries, and loops.

2. *Recognize* how to implement the steps of BB84 between Alice and Bob using cirq.

Key Ideas

1. The python **choices function** allows us to to randomly select any number of elements from a given list such as:
    a. Bits for a key.
    b. Bases to encode qubits.

2. A python **dictionary** is effectively a list, but you can use more than indices. We typically call the general index a key and the element it refers to a value, forming **key, value pairs**.

3. **Loops** allow us to rerun the same code a given number of times instead of having to retype it over and over again.