Quantum Computing

Computing of the Future Made Reality

Janelle Mathis

Background

- Quantum computing is an emerging technology that makes use of quantum mechanics to solve problems that would be too complex for a classical computer
- Quantum computers use qubits to run multidimensional quantum algorithms used to solve complex
- These computers have to be held in extremely cold temperatures due to quantum processors in order to operate because these computers are dealing with electrons and other sub-atomic particles
- Because quantum information is placed on a qubit, that qubit goes through two quantum phenomena: Superposition and Entanglement
- Quantum circuits help with the visualization of the algorithms used by these computers

Implementation:

Three-bit Random Number Generator

```
1   OPENQASM 2.0;
2   include "qelib1.inc";
3
4   qreg q[3];
5   creg c[3];
6
7   h q[0];
8   h q[1];
9   h q[2];
10
11  measure q->c;
```

- Source code consists of the assembly language of QASM
- Lines 1-2 are calling for QASM version and calling for extra gates
- Lines 4-5 are creating more qubits and classical bits
- Lines 7-9 are quantum instructions calling for three H gates
- Line 11 is deciding which qubit and which classical register to store the bit values in

Quantum vs. RSA

Quantum

- Post-Quantum Cryptography is still in its infancy
- Uses quantum key distribution to exchange encryption keys
- Utilizes Shor's algorithm for encryption

RSA

- Most common cryptography used today
- Uses a public key for encryption and private key for decryption
- Utilizes a totient function to create encryption and decryption

Protections

- Lattice-Based Cryptography is based on the idea that a cryptographic scheme is built on mathematical problems around lattices, which for a quantum computer is challenging to do in a reasonable period.
- Three lattice-based algorithms and encryption systems used today:
  - CRYSTALS-Kyber
  - CRYSTALS-Dilithium
  - NTRU

CRYSTALS-Kyber

- Kyber is an IND-CCA2 secure key encapsulation mechanism based on the difficulty of solving the Learning-with-Errors (LWE) problem
- IND-CCA2 stands for indistinguishability of ciphertexts under adaptive chosen attacks
- The Learning-with-Errors problem is the solving of linear equations with noise
- Kyber is one of the finalists in the NIST Post-Quantum Cryptography Project

CRYSTALS-Dilithium

- Dilithium is a digital signature lattice-based algorithm that is secure under chosen message attacks and is based on the level of difficulty of lattice problems
- Essentially, this scheme means that an attacker with access to an oracle that can sign cannot produce a digital signature of a message whose signature has not been seen yet
- Dilithium, like Kyber is one of the candidate algorithms submitted to NIST Post-Quantum Cryptography Project

NTRU

- NTRU is a public key cryptosystem that utilizes lattice theory for encryption and decryption which is based on the embedding of messages within algebraic structures
- Consists of NTRUEncrypt for encryption and NTRUSign for digital signatures
- NTRU relies on the closest vector problem and the shortest vector problem for encryption
- NTRU is faster than RSA cryptography, but is slower than CRYSTALS-Kyber and is not IND-CCA secure unlike both CRYSTALS systems

Reverse Engineering

- In 2021, a study was done to show what reverse engineering could look like on a quantum computer
- Used a reverse engineering tool called QRev to generate abstract representations of quantum programs
- QRev is broken into two modules: Q# parser and KDM (Knowledge Discovery Model) generator
- Two questions were posed and answered: can QRev generate accurate and complete KDM models and can QRev generate these models in a scalable manner

The Future of Quantum Computing

Even though it is still relatively new, quantum computing can and will offer new opportunities for areas such as random number generation, communication, cryptography, machine learning and many more.