Muhammad Izham Bin Norhamadi
B032020039 BITZ

Tutorial 11: Assignment on Quantum Computer

Quantum computers are a type of computer that uses the principles of quantum mechanics to store and process data. Unlike classical computers, which use bits to represent information, quantum computers use quantum bits, or qubits. This allows quantum computers to perform certain types of calculations much faster than classical computers. In recent years, there has been significant progress in the development of quantum computers and their increasing capabilities. IBM recently reveals its 400 qubits-plus quantum processor alongside next-generation of quantum system. In late 2019, Zapata computing claimed to have factored 1,099,551,473,989 and released a paper describing this computation in 2021. One of the major concerns about the advancing technology of quantum computers is their potential impact on cryptography. Cryptography is the practice of secure communication, and it relies on the fact that certain mathematical problems are difficult for classical computers to solve. For example, the security of many internet transactions is based on the difficulty of factoring large numbers. However, quantum computers have the potential to solve these problems much more quickly than classical computers, which could potentially compromise the security of many cryptographic systems.

In response to this concern, researchers are actively working on developing new cryptographic techniques that are resistant to attacks by quantum computers. These techniques, known as post-quantum cryptography, are designed to protect against attacks by quantum computers and ensure the security of communication systems in the post-quantum era. Several algorithm candidates were chosen on rounds of the NIST PQC Standardization Process. The broad evaluation criteria that would be used to compare candidate algorithms throughout the process are security, cost and performance, and algorithm and implementation characteristics. One of these candidates is NTRU which stands for “Number Theory Research Unit”. NTRU is a public-key cryptosystem that was invented by Jeff Hoffstein, Jill Pipher, and Joseph H. Silverman in 1996 based on the problem of finding the shortest vector in a lattice, which is a type of mathematical structure that consists of a discrete set of points that are evenly spaced in one or more dimensions.

Muhammad Izham Bin Norhamadi
B032020039 BITZ

Though currently, quantum computers have not yet been able to crack RSA encryption, which is a widely used public-key cryptosystem that is based on the difficulty of factoring large numbers. There are several reasons why quantum computers have not yet been able to do so, one reason is that RSA keys are typically very large, with key sizes of at least 2048 bits being commonly used. This makes it difficult for quantum computers to factorize the large numbers that are used in RSA keys in a reasonable amount of time. Another reason is that quantum computers are still in the early stages of development, and they are not yet powerful enough to perform the massive calculations that would be required to factorize large RSA keys. While quantum computers have the potential to perform certain types of calculations much faster than classical computers, they are still not as powerful as classical computers for many tasks.

Besides that, there is ongoing debate among scientists and philosophers about whether quantum computers should be considered "real" or "imaginary." Some argue that quantum computers are simply a mathematical abstraction and do not correspond to any physical reality. Others argue that quantum computers are based on the principles of quantum mechanics, which have been experimentally verified and are considered to be a fundamental part of the physical world. Regardless of whether quantum computers are considered real or imaginary, it is undeniable that they have the potential to revolutionize the way we think about computation and solve problems that are beyond the capabilities of classical computers. While it is difficult to predict exactly when quantum computers will become practical for widespread use, it is clear that they hold great promise for the future of computation as researchers and engineers are actively working to overcome limitations and make quantum computers more practical and reliable.

Muhammad Izham Bin Norhamadi
B032020039 BITZ

References

Alagic, G. (2020, July). *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*. Retrieved from NIST: https://csrc.nist.gov/publications/detail/nistir/8309/final

Dyakonov, M. I. (2020). *Will we ever have a quantum computer?* Springer.

Fernandez-Carames, T. M.-L. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE access*.

IBM. (2022, November 9). *IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two*. Retrieved from Newsroom IBM: https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two

NIST. (2022). *Post-Quantum Cryptography Standardization*. Retrieved from NIST: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization

OpenSSH. (2022, April 8). *OpenSSH 9.0*. Retrieved from OpenSSH: https://www.openssh.com/txt/release-9.0

Pirandola, S. A. (2020). Advances in quantum cryptography. *Advances in optics and photonics*.