Post Quantum Cryptography

Brandon LaPointe

Spring 2023

1 Proposal

1. Describe the topic:
   Post Quantum Cryptography involves the potential use of future quantum computing technology and its computing abilities to crack modern cryptographic standards of security. While this technology is still in the process of coming to existence, the threat of this technology to systems involving data confidentiality and integrity of security are crucial to make resilient to this potential menacing for the inevitable day that the technology gets into the wrong hands. The National Institute of Standards and Technology (NIST) plans on publishing its new post-quantum cryptographic standard in 2024.

   Post-Quantum Cryptography: A Summary

   Quantum computing is a new paradigm of computing that is based on quantum mechanics. This technology uses quantum bits (qubits) which are capable of being in multiple states simultaneously. As a result, quantum computers can perform certain calculations much faster than classical computers. This speed increase makes quantum computers a serious threat to the security of classical cryptographic systems, which are based on mathematical problems that are hard to solve for classical computers but are solvable for quantum computers. This leads to the need for post-quantum cryptography, which is designed to be secure even against quantum computers.

   Post-Quantum Cryptography is a new field that aims to design cryptographic algorithms that are secure against quantum computers. Unlike classical cryptography, which is based on mathematical problems such as integer factorization and the discrete logarithm problem, post-quantum cryptography is based on problems that are believed to be hard even for quantum computers. These problems are typically related to lattice-based problems, code-based problems, and multivariate polynomial problems.

   One example of a post-quantum cryptographic algorithm is lattice-based cryptography. Lattice-based cryptography is based on the mathematical concept of lattices, which are a grid of points in a multi-dimensional space. Lattice-based cryptographic algorithms, such as the Learning With Errors (LWE) problem, are based on the idea that it is hard to find the closest lattice point to a given vector in high-dimensional space. This makes lattice-based cryptography secure against quantum computers, since solving the closest vector problem is believed to be hard even for quantum computers.

   In conclusion, post-quantum cryptography is a new field that is necessary to ensure the security of cryptographic systems against quantum computers. The field is based on mathematical problems that are believed to be hard for quantum computers, such as lattice-based problems,

code-based problems, and multivariate polynomial problems. One example of a post-quantum cryptographic algorithm is lattice-based cryptography, which is based on the concept of lattices and the difficulty of finding the closest lattice point to a given vector.

2. List the individuals working on the project:
   Brandon LaPointe

3. Outline the goals for the project:
   Learn more on the subject matter
   Give real world examples
   Provide detailed summary for an average reader to comprehend

4. List potential references in proper formatting:
   Refer to "References Used" Section.

2 What Is Post Quantum Cryptography?

1. Brief Quantum Computing Summary

2. Threats to cryptography that arise from Quantum Computing

3. Post Quantum Cryptography Summary

3 Post Quantum Cryptography Potential

1.

4 What Is Holding Us Back? * subject to change with revision *

1.

5 References Used * Figuring out formatting and requirements. Also subject to change *

Migrating to Post-Quantum Cryptography - Whitehouse.gov. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf.

National Security Agency Frequently Asked Questions Quantum Computing ... https://media.defense.gov/2021/Au
1/-1/1/Quantum$_F AQs_2$0210804.PDF.

"$Post-QuantumCryptographyInitiative.$"$CybersecurityandInfrastructureSecurityAgencyCISA, https$: $//www.cisa.gov/quantum.$

"$Post-QuantumCryptography$: $AnticipatingThreatsandPreparingtheFuture.$"$ENISA, 19Oct.2022, https$: $//www.enisa.europa.eu/news/enisa-news/post-quantum-cryptography-anticipating-threats-and-preparing-the-future.$

"$PostQuantumCryptography$: $DefendingagainstFutureAdversaries.$"$Intel,$

$https://www.intel.com/content/www/us/en/research/news/post-quantum-cryptography.html.$

"$When--andHow--toPrepareforPost-QuantumCryptography.$" $McKinseyamp;Company$, $McKinseyamp;Company$, $22June2022$, $https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography.$