Post Quantum Cryptography

Brandon LaPointe

Spring 2023

1 Post-Quantum Cryptography: A Summary

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. With the National Institute of Standards and Technology (NIST) planning on publishing its new post-quantum cryptographic standard in 2024, this upcoming future of security is closer than it seems.

2 The Future of Security

Post-quantum cryptography has become a pressing issue due to the rapid development of quantum computing technology. Quantum computers are capable of breaking traditional cryptographic systems that are based on mathematical problems that can be solved efficiently by classical computers, such as factoring large numbers and computing discrete logarithms. These problems form the basis of widely used encryption protocols, such as RSA and Elliptic Curve Cryptography (ECC).

The impact of quantum computers on cryptography is significant because quantum computers can use Shor's algorithm to solve these problems quickly. This means that the security of the communication channels protected by these encryption protocols will no longer be guaranteed. Post-quantum cryptography offers a solution to this problem by developing new cryptographic algorithms that are resistant to quantum attacks. This involves designing new cryptographic primitives and protocols that can operate securely on both classical and quantum computing systems. The aim is to find mathematical problems that are computationally intractable for quantum computers, even with the use of Shor's algorithm.

3 Potential Candidates

One of the most promising approaches to post-quantum cryptography is based on lattice-based cryptography. Lattice-based cryptography is a relatively new field that is based on the use of lattices, which are geometrical structures that can be used to encode information in a way that is difficult for quantum computers to crack.

The most popular lattice-based cryptographic algorithm is the Learning With Errors (LWE)

problem. This algorithm uses the difficulty of finding a small, random error in a set of linear equations that have been perturbed with some noise. The security of the LWE problem is based on the hardness of approximating the shortest vector in a high-dimensional lattice, which is believed to be a difficult problem for both classical and quantum computers.
Another promising post-quantum cryptographic approach is based on code-based cryptography. This approach uses error-correcting codes to create a hard problem for quantum computers. The security of these codes is based on the difficulty of decoding a random linear code, which is believed to be a difficult problem for quantum computers.
Multivariate polynomial cryptography is another post-quantum cryptographic approach that uses the difficulty of solving non-linear equations to create hard problems for quantum computers. This approach is based on the hardness of solving systems of multivariate polynomials, which is believed to be difficult for both classical and quantum computers.

4 What's Holding Us Back?

Despite the rapid development of quantum computing technology, there are still significant challenges that need to be overcome before we can build large-scale, fault-tolerant quantum computers that can solve practical problems. One of the main challenges is the issue of quantum decoherence, which causes quantum states to rapidly lose their coherence and become entangled with the environment. This makes it difficult to maintain the fragile quantum states that are needed for quantum computation. Quantum states are the possible states of a quantum system, such as an atom or a photon. Unlike classical systems, quantum systems can exist in multiple states simultaneously, a property known as superposition. In other words, a quantum system can be in multiple states at once, with each state having a different probability of being observed when measured. The state of a quantum system is described by a mathematical object called a wave function, which encodes the probabilities of observing different outcomes when the system is measured.
Another challenge is the problem of scaling up quantum systems to large numbers of qubits, which requires significant advances in quantum hardware and control technology. Qubits, or quantum bits, are the basic units of information in quantum computing. They are the quantum analog of classical bits, which can be either 0 or 1. Qubits, on the other hand, can be in a superposition of both 0 and 1 at the same time, which is what gives quantum computers their potential for massive parallelism and speedup. Qubits can be realized using a variety of physical systems, such as atoms, ions, superconducting circuits, and photons. The state of a qubit is described by a quantum state, which is a superposition of the two basis states, 0 and 1. When measured, a qubit collapses into either the 0 or 1 state, with the probability of each outcome determined by the coefficients of the superposition. Additionally, there are still many open questions in the theory of quantum computing, including the development of new quantum algorithms and the study of the limits of quantum computation. Overcoming these challenges will be crucial to unlocking the full potential of quantum computing technology and realizing its promise for revolutionizing fields such as cryptography, materials science, and drug discovery.

5 Conclusion

In conclusion, post-quantum cryptography is a rapidly evolving field that is essential for maintaining the security of communication channels in the face of quantum computing technology.

The field is based on the development of new cryptographic primitives and protocols that can withstand quantum attacks. Lattice-based cryptography, code-based cryptography, and multivariate polynomial cryptography are all promising approaches to post-quantum cryptography. The development of these new cryptographic systems will be crucial to ensuring the security and privacy of our digital communications in the coming decades.

6 References Used **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.

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

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

"$PostQuantumCryptography$: $DefendingagainstFutureAdversaries.$"$Intel,$
$https$: $//www.intel.com/content/www/us/en/research/news/post-quantum-cryptography.html.$

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