Post Quantum Cryptography

Brandon LaPointe

Spring 2023

1 Post-Quantum Cryptography: A Summary

Post Quantum Cryptography involves the potential use of future quantum computing technologies 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 "Big Three"

The "Big Three" cryptosystems are the most widely used public-key encryption methods today. The "Big Three" includes RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC). RSA, which stands for Rivest, Shamir, and Adleman, is widely used for secure data transmission and digital signatures. The security of RSA is based on the difficulty of factoring large integers into their prime factors. Diffie-Hellman, on the other hand, is used for secure key exchange in a public channel. The security of Diffie-Hellman is based on the discrete logarithm problem. Elliptic curve cryptography (ECC) is similar to RSA in that it relies on the difficulty of solving a mathematical problem, namely the elliptic curve discrete logarithm problem, for its security. ECC is often used in applications where computational power and storage are limited, such as mobile devices and smart cards. Despite their widespread use and effectiveness, these cryptosystems are all vulnerable to attacks by quantum computers.

3 The General Number Field Sieve vs. Shor's Algorithm

For classical computers, the best-known factoring algorithm is the General Number Field Sieve (GNFS). GNFS has a sub-exponential time complexity, which means that as the size of the number being factored increases, the time it takes to factor the number grows much slower than the size of the number itself. However, even with the best implementation and hardware available, GNFS can only factor numbers up to a certain size in a reasonable amount of time. As the size of the number increases, the time it takes to factor the number becomes prohibitively long.

On the other hand, Shor's algorithm is a quantum algorithm that can factor numbers exponentially faster than classical algorithms like GNFS. Shor's algorithm has a time complexity of $O((logN)^3)$, where N is the number being factored. This means that as the size of the number being factored increases, the time it takes to factor the number grows much slower than with classical algorithms. For example, it would take a classical computer using GNFS several hundred years to

factor a 2048-bit RSA key, while a quantum computer running Shor's algorithm could do it in a matter of minutes.

The impact of quantum computers on modern computing is significant, particularly in the field of cryptography. The fact that we have a quantum algorithm for breaking the "big three" public key cryptosystems is a major development because these are the most widely used encryption schemes in use today. AES, on the other hand, is a symmetric key encryption algorithm that is widely used for encrypting data at rest and in transit, and it is believed to be secure against quantum attacks as there is no known quantum algorithm that can solve the problem significantly faster than classical computers yet. However, the impact of quantum computers on RSA, Diffie-Hellman, and ECC is significant.

4 The Future of Security

Since Shor's algorithm can factor large numbers and compute discrete logarithms in polynomial time, it means that the "Big Three" cryptosystems will become vulnerable to attack by quantum computers once they reach a certain size of qubits. The exact size at which this becomes a problem is a matter of debate, but it is generally believed that quantum computers with a sufficient number of qubits could break RSA and ECC with key sizes of 2048 bits or less, and Diffie-Hellman with key sizes of 3072 bits or less with relative ease. These estimates of a "sufficient number" of qubits range from anywhere from several hundred to several thousand physical qubits. While quantum computers are not a threat to all encryption schemes, the development of post-quantum cryptography is an active area of research to address this issue by finding new cryptographic algorithms that are resistant to quantum attacks.

5 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, or in other words, injected with some randomness so that it becomes difficult to distinguish between the original equation and the perturbed version. 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 difficulty and time complexity of solving systems of multivariate polynomials, which is believed to be difficult for both classical and quantum computers.

6 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 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.

7 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 "Big Three" encryption methods, RSA, Diffie-Hellman, and ECC, which are widely used today, will become vulnerable to quantum attacks once quantum computers reach a sufficient number of qubits. Lattice-based cryptography, code-based cryptography, and multivariate polynomial cryptography are all promising approaches to post-quantum cryptography that are being actively researched. The development of these new cryptographic systems will be crucial to ensuring the security and privacy of our digital communications in the coming decades.

8 References

By. (n.d.). Intel hits key milestone in Quantum Chip Production Research. Intel. Retrieved March 30, 2023, from https://www.intel.com/content/www/us/en/newsroom/news/intel-hits-key-milestone-quantum-chip-research.html

Flint, R. (2023, January 8). Do we need to worry about China breaking RSA encryption technologies with quantum computers? - quantum computing news and features. Quantum Zeitgeist. Retrieved March 30, 2023, from https://quantumzeitgeist.com/do-we-need-to-worry-about-china-breaking-rsa-encryption-technologies-with-quantum-computers/#: :text=A%20recent%20research%20paper%20from,rely%20upon%20for%20digital%20security.

McKinsey & Company. (2022, May 4). When-and how-to prepare for post-quantum cryptography. McKinsey & Company. Retrieved March 30, 2023, from https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography

Migrating to post-quantum cryptography - whitehouse.gov. (n.d.). Retrieved March 30, 2023, from https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

Post-Quantum Cryptography initiative: CISA. Cybersecurity and Infrastructure Security Agency CISA. (n.d.). Retrieved March 30, 2023, from https://www.cisa.gov/quantum Post-quantum cryptography: Anticipating threats and preparing the future. ENISA. (2022, October 19). Retrieved March 30, 2023, from https://www.enisa.europa.eu/news/enisa-news/post-quantum-cryptography-anticipating-threats-and-preparing-the-future

The Quantum Computer and its implications for public-key ... - entrust. (n.d.). Retrieved March 30, 2023, from https://www.entrust.com/-/media/documentation/whitepapers/sl20-1026-001-ssl_quantumcomputers-wp.pdf?la=en&hash=11184A80B0523E918F674EFF0C68137A

Quantum computing and Post-Quantum Cryptography - U.S. Department of ... (n.d.). Retrieved March 30, 2023, from https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF

RSA, DSA, and ECC Encryption Differences — Sectigo® Official. (n.d.). Retrieved March 30, 2023, from https://sectigo.com/resource-library/rsa-vs-dsa-vs-ecc-encryption