Post-Quantum Cryptography

Danica Cariaga Amber Thomas

October 21, 2021

Abstract

Quantum computers are on track to break our current encryption algorithms. Having strong encryption standards is necessary to protect data for private communications, company data, military secrets, and other sensitive data. With quantum computers cracking algorithms, private data will be exposed, and can be used against victims in cyber and physical attacks. By finding quantum-resistant cryptographic algorithms, it will make it difficult for quantum computers to disrupt future encryption methods. Post-quantum cryptography aims to be compatible with classical and quantum computers. An important contribution to post-quantum cryptography is lattice-based cryptography. In this emerging field, post-quantum protocols must be developed with consideration for quantum key distributions and facilitating new research that collaborates with existing infrastructure and researchers.

Keywords: post-quantum computing, post-quantum cryptography, cryptography, cryptographic algorithms, qubits, lattice-based cryptography, migration, distributed web-systems, post-quantum protocols, quantum-resistant, Shor's algorithm

Introduction

As technology advances, quantum computers are being developed and the scope of their application can be applied to anything computing related. Quantum computers speed up

superpolynomially. For perspective, a conventional computer would need about 300 trillion years to crack a 2048-bit digital key with the RSA encryption algorithm and would take a quantum computer only about 10 seconds. With that said, data privacy and security faces threats of exposure due to quantum computing and encryption cracking.

For background, quantum computers are machines based on quantum physics which can have more than one state of being at the same time but can only have one result, similar to Schrodinger's cat when that cat has been viewed. This means it can compute many streams of data at once. Because of this, Shor's algorithm, a polynomial-time quantum algorithm, is used in quantum computing to effectively crack the ubiquitous RSA encryption algorithm. Shor's algorithm is for integer factorization and is used as a current standard for computational effectiveness.

As quantum computers do not currently have the computing capacity, in the future they can be used with Shor's algorithm on collected data. That is, data is being collected now in preparation to be cracked later when the computing capacity is available. It is estimated that within one to two decades, quantum computers will achieve the capacity to crack our current encryption standards. This paper discusses the topics relating to migration, algorithms, and standardization protocols for post-quantum cryptography.

Literary Review

A key focus for Post-Quantum Cryptography is the migration from classical cryptographic algorithms to quantum cryptographic algorithms. The development of quantum-resistant public-key cryptographic standards and the algorithm selection process is currently underway. The algorithm migration is more complicated than other migrations we have faced in

the past so early awareness, education and planning are essential. We can begin much of the post-quantum transition work that needs to be done even before we know which specific algorithms the National Institute of Standards and Technology (NIST) will choose to standardize.

Distributed web systems can lead to hardware-oriented cryptography. These networks allow for effective hardware systems and can allow for a more secure approach to quantum authentication. Qubit level encryption, similar to that deployed using cryptographic hashing, may be possible with a distributed architecture. Quantum recursiveness can be used for recursive hashing in parallel qubit-based processing systems that can be interconnected to add an encryption layer that will become more complex over time. Because qubits are sometimes manipulated through high beam laser and super conductivity, they can also be converted back to 0's and 1's through polarized beams. Developing quantum recursive hashing and data encoding algorithms can allow for a multi-path layer cryptography on a hardware-oriented level.

Lattice-Based Cryptography is more resistant against quantum-based attacks. The structure of a lattice is a set of points in n-dimensional space and uses a set of vectors. In a pair of vectors, one associates with the public key, and the other with the private key. Lattice-Based Cryptography is considered ideal due to its worst-case hardness, relatively efficient implementation, and simplicity. Its promise is attributed to its application where cryptography is used such as message encryption, digital signatures, and hashing. In the quantum-computing realm, lattice-based cryptography's importance lies in its resistance to Shor's algorithm. Additionally, lattice-based cryptography can and has been proven to be secure by its mathematical security proofs.

Methodology

A proposed solution for Post-Quantum Cryptography can be broken into 3 categories: Discovery, Implementation and Ongoing Research.

It is important to discover where current cryptographic instances need to be updated or replaced due to the quantum encryption cracking threat. All guidance, standards and protocols must be reviewed to ensure that they will meet post-quantum cryptography standards and protocols. It is essential to educate government agencies, other industries and organizations about post-quantum algorithms transitions, and how it will impact their systems and assets. Then they will need to review their cryptographic standards that are relevant to their specific activities. Once these activities have been discovered they may work with standards organizations that have updated methods to prepare for post-quantum computing migration.

Implementation activities begin with algorithms to identify sensitive information protected with cryptographic key establishments. These algorithms are part of an automated tool that will inventory cryptography usage by identifying hardware and software modules, libraries, and embedded code. It is important to prioritize the encrypted data based off the affected components and assets from the algorithm. Post-Quantum Cryptography implementation will then lead to real-world trials and testing of modified systems using the NIST standards which are currently on round 3 trials.

Lastly, ongoing research is vital given the nature of the development of quantum computing and quantum algorithms. Different parameters and computational requirements of new algorithms such as key, ciphertext and signature sizes, memory, processing cycles and network latencies will all vary from our current cryptographic algorithms. New research will be needed to secure communications and should also include frameworks for cryptographic agility.

New tools need to be researched that can be configured and controlled by updated cryptographic standards and protocols. Academia can help research post-quantum authentication, key management, web applications, mobile and IoT computing.

Results and Discussion

Potential measurable outcomes such as security proofs for lattice-based cryptography can be quantified by mathematical computations. The algorithms can also be quantified by the time it would take to be cracked. The post-quantum encryption methods can be tested against using Shor's algorithm to determine its effectiveness. Migration progress can be tracked by post-quantum cryptography standards and protocols being implemented in government, industries, and other organizations as well as the creation of automated tools to implement them. Within migration implementation, the distributed web-system would be measured through the qubit processing and its conversion back to binary.

Conclusion and Remediation

Cryptographic models implemented need to withstand extended periods of time in the future. Data use needs to be considered as these models will be able to secure sensitive information during the time in storage. Furthermore, these encryption methods need to be strong to prevent harvested data from being exposed. Through lattice-based cryptography, preparation to migrate to a post-quantum cryptography model can begin now. Following NIST guidelines, migration will be easier when post-quantum cryptography methods are implemented and tested from the current cryptographic algorithms to algorithms that are resistant to quantum computer-based attacks.

Sources

Asif, Rameez. "Basic types of Post-Quantum Cryptography (PQC)" MDPI, 5 Feb. 2021, https://www.mdpi.com/2624-831X/2/1/5/htm

Barker, William, and Murugiah Souppaya. “Migration to Post-Quantum - Nccoe.org.” National Cybersecurity Center of Excellence (NCCoE), https://www.nccoe.org/sites/default/files/library/project-descriptions/pqc-migration-project-description-final.pdf.

Campagna M., LaMacchia B., & Ott D. (2020) Post Quantum Cryptography: Readiness Challenges and the Approaching Storm. https://cra.org/ccc/resources/ccc-led-whitepapers/#2020-quadrennial-papers

Computer Security Division, Information Technology Laboratory. “Post-Quantum Cryptography: CSRC.” CSRC, 14 June 2021, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

“Cryptography in a Post- Quantum World - Accenture.” Accenture, 4 Oct. 2018, https://www.accenture.com/_acnmedia/pdf-87/accenture-809668-quantum-cryptography-whitepaper-v05.pdf.

Micciancio, Daniele, and Oded Regev. “Lattice-Based Cryptography.” *NYU CIMS*, 22 July 2008, https://cims.nyu.edu/~regev/papers/pqc.pdf.

Nassief, Andrew M. K. “Distributed Web Systems Leading to Hardware Oriented Cryptography and Post-Quantum Cryptologic Methodologies.” IACR Cryptology EPrint, 14 Dec. 2019, https://www.academia.edu/41405212/Distributed_Web_Systems_Leading_to_Hardware_Oriented_Cryptography_an_Post_Quantum_Cryptologic_Methodologies.

"NSAs Cybersecurity Perspective on Post Quantum Cryptography Algorithms." National Security Agency/Central Security Service > Cybersecurity > https://www.nsa.gov/Cybersecurity/NSAs-Cybersecurity-Perspective-on-Post-Quantum-Cryptography-Algorithms/.

Shankland, Stephen. "Quantum Computers Could Crack Today's Encrypted Messages. That's a Problem." CNET, CNET, 24 May 2021, https://www.cnet.com/tech/computing/quantum-computers-could-crack-todays-encrypted-messages-thats-a-problem/.

Staff, NQCO. "NSA Updates FAQ on Post-Quantum Cybersecurity." National Quantum Initiative, 10 Aug. 2021, https://www.quantum.gov/nsa-updates-faq-on-post-quantum-cybersecurity/.