Post-Quantum Cryptography

Rupaben Odedara
Subject: INCS-741, Prof. Tokunbo Makanju New York Institute of Technology, Vancouver, BC.

***Abstract*—The use of cryptography today is at serious risk as quantum computing develops further. The security of sensitive data and communication could be threatened by quantum computers' potential to defeat conventional cryptography techniques. This study examines post-quantum cryptography, a topic that aims to create cryptographic algorithms impervious to quantum computer attacks. The article introduces quantum computers and their basic concepts while emphasizing the dangers they represent to the cryptography procedures used today. The discussion of quantum-resistant ciphers then proceeds, covering their attributes and several design strategies. As part of its investigation into the quantum-resistant ciphers under consideration for standardization, the National Institute of Standards and Technology (NIST) is working to create a standard for quantum-resistant cryptography. The findings highlight how crucial it is to switch to quantum-resistant cryptography systems to maintain sensitive data's long-term security and confidentiality.**

I. INTRODUCTION

Cryptography, the science of securing information, has played a pivotal role in ensuring the confidentiality, integrity, and authenticity of sensitive data and communication in the digital age. However, the rapid advancement of quantum computing technology poses a significant challenge to the current practice of cryptography [1]. In response to this threat, post-quantum cryptography, also known as quantum-resistant or quantum-safe cryptography, has emerged as a field dedicated to developing cryptographic algorithms that can withstand attacks from powerful quantum computers. These post-quantum algorithms aim to ensure the long-term security of sensitive information, even in the face of quantum computers' computational power and unique properties [4]. To provide security against potent quantum computers, this research study examines the significance of quantum-resistant cyphers and offers insights into how they protect private data. This article examines the idea of post-quantum cryptography, the dangers posed by quantum computers, and the continuous efforts being made by organizations like the National Institute of Standards and Technology (NIST) to standardize quantum-resistant algorithms. Additionally, research analyzes the types of quantum-resistant ciphers being considered for standardization.

II. POST-QUANTUM CRYPTOGRAPHY

A. Quantum Computers

An interesting and quickly evolving area of technology, quantum computers use the concepts of quantum physics to carry out computations fundamentally differently from conventional computers. Quantum computers use qubits, which can exist in a superposition of 0 and 1, unlike classical computers that use bits representing either 0 or 1. Qubits are typically subatomic particles like electrons or photons, making their generation and management a complex engineering and scientific challenge [5].Quantum computers utilize entanglement, enabling instantaneous correspondence between coupled qubits regardless of physical distance. Their ability to simulate molecular behavior is an exciting application. However, the full potential of quantum computers may take years to realize, as universities and companies face challenges in finding qualified researchers and essential suppliers.

Quantum computers pose a threat to current cryptography by exploiting the computational complexity of mathematical problems used in traditional encryption methods. Their unique quantum features can compromise the security provided by these methods.

B. Quantum Computing's Impact on Cryptography

As quantum computing advances through additional research and development, quantum computers could potentially defeat many of the encryption techniques used by businesses today. Because quantum computers may be able to conduct calculations that can decrypt them, quantum assaults may put symmetric and asymmetric cryptographic encryption methods at danger[3].

- The widely used RSA (Rivest-Shamir-Adleman) method focuses on the challenge of factoring big numbers into their prime factors. RSA is widely utilized for secure communication and digital signatures in many applications.
- The Shor algorithm, utilized by quantum computers, poses a significant threat to cryptographic systems that rely on factorization. Its ability to parallelize computations enables rapid factorization of large numbers, potentially compromising the security of RSA and similar algorithms.
- Quantum computers threaten Elliptic Curve Cryptography (ECC), a widely used public-key method. ECC relies on the high computational complexity of the elliptic curve discrete logarithm problem, which can be solved by quantum computers using the same technique.

Table I describes how quantum computer impact from large scale to other cryptography algorithm. Exploring quantum-resistant algorithms that are independent of mathematical vulnerabilities susceptible to quantum attacks.

TABLE I
IMPACT OF QC ON COMMON CRYPTO ALGORITHMS. FROM REPORT ON POST-QUANTUM CRYPTOGRAPHY, 2016

Cryptographic algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	-	Hash Functions	Larger output needed
RSA	Public key	Signatures, Key Establishment	No Longer Secure
ECDSA, ECDH	Public key	Signatures, Key Exchange	No Longer Secure
DSA (finite field cryptography)	Public key	Signatures, Key Establishment	No Longer Secure

C.Exploring Quantum Resistant Ciphers: Safeguarding Data in the Quantum Computing Age

It is impossible to overestimate the significance of quantum-resistant ciphers in post-quantum encryption in the era of quantum computing. The foundation of secure communication and data security, traditional cryptographic methods are susceptible to attacks from powerful quantum computers [2]. The need for the creation and use of quantum-resistant ciphers is driven by the growing vulnerability of existing algorithms to the creation of quantum computers. As a result, researchers and cryptographers have been actively exploring the development of quantum-resistant ciphers to safeguard data in the quantum computing age [2]. The impact of such computational power on traditional cryptographic algorithms is substantial, as these algorithms rely on the presumed difficulty of these problems for their security. Thus, quantum-resistant ciphers become indispensable in providing long-term security in the face of quantum computing advancements. One example of Lattice-based cryptography is a quantum-resistant cipher that relies on challenging problems in lattice theory, such as the Shortest Vector Problem (SVP) and the Learning with Errors (LWE) problem. These problems are complex for classical and quantum computers to solve efficiently. [2].

D.NIST's Standardization Efforts for Post-Quantum Cryptography and Considered Types of Quantum Resistant Ciphers for Standardization

After thorough evaluation in the third round of the NIST PQC Standardization Process, NIST has selected four algorithms as candidates for standardization. For most use cases, NIST will recommend implementing CRYSTALS-KYBER for key-establishment and CRYSTALS-Dilithium for digital signatures. First one is CRYSTALS-Kyber algorithm, which is used for general encryption when accessing secure websites. Because of its shorter encryption keys and efficient operation, NIST chose this algorithm. NIST has chosen other three algorithms for digital signatures used in identity authentication and remote document signing: CRYSTALS-Dilithium, FALCON, and SPHINCS+. Because of its efficiency, CRYSTALS-Dilithium is recommended as the primary algorithm, whereas FALCON is appropriate for smaller signatures. Because of its unique mathematical approach, SPHINCS+ acts as a backup choice. In Fig.1 NIST Announced timeline and remaining fourth round announce date.

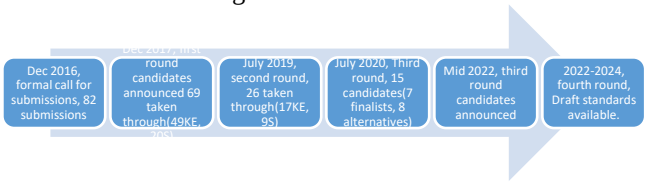

Fig. 1. Timeline of NIST from Status report on the second round of the NIST post-quantum cryptography standardization process.

TABLE 2
NIST THIRD-ROUND FINALISTS FROM STATUS REPORT ON THE SECOND ROUND OF THE NIST POST-QUANTUM CRYPTOGRAPHY

Public-Key Encryption/KEMs	Digital Signatures
Classic McEliece	CRYSTALS-DILITHIUM
CRYSTALS-KYBER	FALCON
NTRU	Rainbow
SABER	

TABLE 2: The remaining seven finalist candidates will compete for standardizations at the conclusion of the third round [6].

V. CONCLUSION

In conclusion, the rise of quantum computing poses a significant threat to traditional cryptographic methods, necessitating the development of post-quantum cryptography. Quantum-resistant ciphers and NIST's standardization efforts offer promising solutions to ensure the long-term security of sensitive data and communication in the quantum computing age. It is imperative to adopt these advancements to safeguard against the potential risks posed by quantum computers.

REFERENCES

[1] Bernstein, D., Lange, T. Post-quantum cryptography. Nature 549, 188–194 (2017). https://doi.org/10.1038/nature23461
[2] Chen, L., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., ... & Smith-Tone, D. (2016). Report on post-quantum cryptography (Vol. 12). Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.
[3] Barker, W., Polk, W., & Souppaya, M. (2020). Getting ready for post-quantum cryptography: explore challenges associated with adoption and use of post-quantum cryptographic algorithms. The Publications of NIST Cyber Security White Paper (DRAFT), CSRC, NIST, GOV, 26.
[4] NIST announces the first four quantum-resistant cryptographic algorithms. NIST. (2022, July 7). https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
[5] Giles, M. (2021, October 20). Explainer: What is a quantum computer?. MIT Technology Review.https://www.technologyreview.com/2019/01/29/66141/what-is-quantum-computing/
[6] Moody, D., Alagic, G., Apon, D. C., Cooper, D. A., Dang, Q. H., Kelsey, J. M., ... & Alperin-Sheriff, J. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process.