www.uzresearchers.com

THE ROLE OF EXACT SCIENCES IN
THE ERA OF MODERN DEVELOPMENT

SAFEGUARDING DIGITAL SECURITY: ADDRESSING QUANTUM COMPUTING THREATS

Akmalov Zayniddin Mexriddinovich
Independent academic researcher

***Abstract**: In an era of rapidly advancing technology, the rise of quantum computers has sparked both excitement and concern. While quantum computing holds immense promise for solving complex problems, it also poses significant threats to the foundation of modern cryptography and cybersecurity. The formidable computational power of quantum machines has the potential to render commonly used encryption algorithms obsolete, leaving sensitive data and secure communication vulnerable to attacks. To counter these emerging threats, researchers and organizations are actively exploring innovative approaches to secure digital systems. Two prominent strategies have emerged: Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC). These cutting-edge methods aim to fortify encryption protocols and maintain the confidentiality, integrity, and authenticity of sensitive information in the face of quantum computing breakthroughs. This article delves into the realm of quantum computing threats, shedding light on the challenges they pose to traditional cryptographic techniques. We will explore the principles behind Quantum Key Distribution (QKD) and its ability to establish secure communication channels based on the fundamental laws of quantum mechanics. Additionally, we will delve into the world of Post Quantum Cryptography (PQC), which seeks to develop encryption algorithms capable of withstanding attacks from both classical and quantum computers. By comprehending the advances in QKD and PQC, we can grasp the strategies being developed to safeguard digital security in the quantum age. Though the journey towards fully quantum-resistant encryption is not without hurdles, ongoing research and collaboration aim to forge a new era of robust and resilient cryptographic systems.*

Key words: *quantum computers, cryptography, cybersecurity, encryption algorithms, threats, Quantum Key Distribution (QKD), Post-Quantum Cryptography (PQC), digital security, confidentiality.*

Introduction: Let's delve into the details of how quantum computers could potentially break asymmetric encryption algorithms like RSA and ECC. RSA (Rivest-Shamir-Adleman) is a widely used asymmetric encryption algorithm that relies on the difficulty of factoring large composite numbers into their prime factors. The security of RSA is based on the assumption that factoring large numbers is computationally difficult, even for powerful classical computers. However, Shor's algorithm, which is a quantum algorithm, can efficiently factor large numbers on a quantum computer. By leveraging the properties of quantum superposition and entanglement, Shor's algorithm can find the prime factors of a composite number exponentially faster than the best-known classical algorithms. If a powerful enough quantum computer becomes available, it could use Shor's algorithm to factorize the large numbers used in RSA, essentially breaking the encryption. This would allow an attacker to retrieve the private key and decrypt any data encrypted with the corresponding public key.

Elliptic Curve Cryptography (ECC) is another widely used asymmetric encryption scheme that relies on the mathematical properties of elliptic curves. ECC provides a level of security comparable to RSA but with shorter key lengths, making it more efficient for resource-constrained devices. Similarly to RSA, ECC is vulnerable to attacks by quantum computers. Quantum computers could use algorithms like Shor's algorithm or variants adapted for elliptic curve problems to compute the private key from the public key, compromising the security of the encryption.

Other encryption method that is widely used in cybersecurity today is hash functions, such as SHA-256. Hash functions are cryptographic algorithms that take an input (message) of any size and produce a fixed-size output, known as a hash value or digest. These functions are designed to be one-way, meaning it should be computationally infeasible to determine the original input from the hash value. Hash functions are widely used in various security applications, including digital signatures, password storage, data integrity verification, and more. Quantum computers, leveraging Grover's algorithm, have the potential to break some commonly used hash functions. Grover's algorithm is a quantum search algorithm that can search an unsorted database of N items in roughly √N steps, significantly faster than the best-known classical algorithms. The impact of quantum computers on hash functions is twofold: Preimage and second preimage attacks: A preimage attack refers to finding a message that matches a given hash value. A second preimage attack refers to finding a different message that produces the same hash value as a given input. Grover's algorithm can be used to accelerate these types of attacks. For example, if an attacker obtains a hash value and wants to find the original input message, a quantum computer using Grover's algorithm could potentially find a preimage in roughly √N steps, compared to the classical brute-force search of N steps. This reduces the security margin of the hash function and increases the risk of successful attacks.

Collision attacks: A collision occurs when two different inputs produce the same hash value. Hash functions are designed to minimize the probability of collisions, but they are not theoretically immune to them. Grover's algorithm can also be applied to search for collisions more efficiently than classical algorithms. If a powerful enough quantum computer becomes available, it could find collisions in hash functions like SHA-256 more quickly than classical computers. This could lead to potential security breaches, particularly in applications where collisions are explicitly or implicitly exploited, such as digital certificates and digital signatures.

The disruption of secure communication protocols is another concern related to the development of quantum computers and their impact on cybersecurity. Let's explore this in more detail. Secure communication protocols like Transport Layer Security (TLS) and Internet Protocol Security (IPsec) are widely used to provide confidentiality, integrity, and authentication for data transmitted over networks. These protocols rely on cryptographic algorithms for key exchange, encryption, and digital signatures. The security of these protocols is based on the assumption that certain cryptographic algorithms, such as the ones used for key exchange (e.g., Diffie-Hellman), encryption (e.g., RSA, ECC), and digital signatures (e.g., RSA, DSA), are computationally secure against known attacks. However, these algorithms are vulnerable to attacks by quantum computers.

Method: The "store now, decrypt later" (SNDL) strategy is a concerning method used by hackers to exploit the long shelf life of certain valuable data, such as banking details, medical records, and social security numbers. In this approach, hackers intercept the transfer of encrypted data between two points and store it for future decryption. This tactic has gained popularity among cybercriminals.

The SNDL strategy highlights the urgency of implementing robust encryption methods to protect sensitive information. While it is not possible to reverse the past, taking proactive measures to strengthen encryption can help stay ahead of potential threats. Protecting both businesses and governments from this type of attack is imperative.

Hackers employing the SNDL strategy aim to exploit secret information that would be just as damaging if it were exposed immediately or years later. Therefore, safeguarding data from this threat requires proactive measures to ensure encryption methods remain secure against future advancements in quantum computing.

Results: There are 2 main methods to prevent this: QKD and PQD Quantum cryptography, also known as quantum key distribution (QKD), is a cryptographic technique that utilizes the principles of quantum mechanics to ensure secure communication between parties. While the concept of quantum cryptography is promising and offers intriguing possibilities for secure communication, its practical implementation and widespread adoption face several challenges. One of the main limitations of quantum cryptography is the requirement for specialized hardware and infrastructure. QKD protocols typically rely on the transmission of individual photons through fiber optic cables, which requires precise and sensitive equipment. The need for such specialized hardware makes the implementation of quantum cryptography expensive and technically complex. Additionally, the performance of QKD systems is currently slower compared to classical encryption methods. The transmission of individual photons and the necessary protocols for key distribution result in lower data transmission rates. As a result, quantum cryptography is not yet suitable for applications that require high-speed data transmission. Despite these limitations, quantum cryptography is an active area of research and development. Scientists and engineers are working on improving the efficiency, reliability, and practicality of QKD systems. As technology advances and new innovations emerge, it is possible that quantum cryptography may find more applications and become more widely used in the future.

According to a blog post on the Google Cloud blog, Google is already utilizing post-quantum cryptography (PQC) security techniques to protect against "store-now-decrypt-later" attacks. The post, authored by Google Senior Cryptography Engineers Stefan Kölbl, Rafael Misoczki, and Sophie Schmieg, states that Google Cloud has implemented a PQC algorithm on its internal encryption-in-transit protocol, Application Layer Transport Security (ALTS). This ensures that communication within Google's internal infrastructure is authenticated and encrypted.

PQC

The National Institute of Standards and Technology (NIST) has been actively involved in advancing both cryptography and cybersecurity through its standardization programs. One such program is the PostQuantum Cryptography Standardization program, which was announced at the PQCrypto Conference in 2016. Its primary objective is to update cryptographic standards to include post-quantum cryptography, identifying and standardizing algorithms that can resist attacks from quantum computers. The standardization process for post-quantum cryptography involved multiple rounds of evaluation and analysis to ensure the selection of robust algorithms that can withstand quantum computing threats. In addition to the efforts in cryptography, NIST has also focused on enhancing cybersecurity practices through its Cybersecurity Framework (CSF). The CSF was initially introduced in 2014 as a set of guidelines, best practices, and standards to help organizations assess, manage, and improve their cybersecurity posture. It offers a flexible framework applicable to various industries, sectors, and organizational sizes. Recognizing the evolving cybersecurity landscape, NIST has released a draft version of the updated Cybersecurity Framework (CSF) 2.0. The draft, incorporating over a year's worth of community feedback, aims to make the framework more practical and relevant across all organizations. It reflects changes in the cybersecurity landscape and seeks to align the CSF with current and future needs. The draft framework is open for public comments until November 4, 2023, and NIST has expressed its intention not to release another draft version for comments. To gather further input, NIST has planned a workshop in the fall, providing stakeholders with another opportunity to offer feedback and comments on the draft CSF. The final version of CSF 2.0 is expected to be published in early 2024, incorporating the feedback received during the public comment period and the workshop. This updated version will enhance the effectiveness and applicability of the CSF in addressing evolving cybersecurity challenges faced by organizations worldwide.

For general encryption, used when we access secure websites, NIST has selected the CRYSTALS-Kyber algorithm. Among its advantages are comparatively small encryption keys that two parties can exchange easily, as well as its speed of operation.

For digital signatures, often used when we need to verify identities during a digital transaction or to sign a document remotely, NIST has selected the three algorithms CRYSTALS-Dilithium, FALCON and SPHINCS+ will become standard of encryption from 2024 The Post-Quantum Cryptography Standardization program by NIST (National Institute of Standards and Technology) is a comprehensive effort to update cryptographic standards to include post-quantum cryptography.

The Google team explains that while currently deployed public key cryptography algorithms like RSA and Elliptic Curve Cryptography are secure against existing threats, they are expected to be broken by large-scale quantum computers in the future. To address this issue, the cryptographic community has developed post-quantum cryptography (PQC) alternatives that can resist attacks from quantum computers.

Google has chosen the NTRU-HRSS KEM algorithm as its preferred option due to its performance, reputation, and vetting. The team is adopting a hybrid approach by combining the NTRU-HRSS and X25519 schemes to create a single mechanism. This hybrid design ensures that an adversary attempting to break the mechanism would need to compromise both underlying schemes.

As the field of quantum cryptography is rapidly evolving, Google acknowledges the need for ongoing exploration and development of PQC solutions. The company actively participates in the standardization efforts for post-quantum cryptography, with Googlers co-authoring one of the selected signature schemes (SPHINCS+) and having proposals being considered by NIST in their PQC KEM competition (BIKE and Classic McEliece). Google plans to re-evaluate its algorithmic choices based on factors such as the clarification of Kyber's intellectual property status and the publication of selected standards from the fourth round.

In summary, Google is already implementing post-quantum cryptography techniques within its infrastructure to defend against future quantum threats. The company is actively involved in the standardization process and will continue to explore and refine its approach to quantum-resistant security.

Conclusion: In conclusion, the development of powerful quantum computers poses significant threats to current cryptographic algorithms used in asymmetric encryption, hash functions, and secure communication protocols. These threats arise from the ability of quantum computers to efficiently solve certain mathematical problems that underpin the security of these algorithms. To mitigate these vulnerabilities, researchers are actively working on developing and standardizing post-quantum cryptographic algorithms that are resistant to attacks from both classical and quantum computers. These efforts include exploring new approaches such as lattice-based, code-based, multivariate polynomial, and hash-based cryptography. Standardization bodies like NIST are leading the evaluation and selection process for these algorithms. The transition to post-quantum secure communication protocols involves challenges such as optimizing performance, ensuring compatibility with existing systems, and raising awareness among stakeholders. Education and awareness programs are being developed to help organizations understand the risks and plan for the adoption of post-quantum security. Overall, the ongoing efforts to develop post-quantum cryptographic algorithms and their subsequent adoption are crucial for ensuring the long-term security of communication systems in the face of advancing quantum technologies. By staying ahead of potential quantum threats, we can maintain the confidentiality, integrity, and authenticity of data in a future where quantum computers become more powerful.

References:

1. https://www.linkedin.com/pulse/risks-store-now-decrypt-later-safeguarding-datauncertain-haroon/
2. https://thequantuminsider.com/2023/08/24/nist-releases-four-pqc-algorithms-forstandardization/#:~:text=After%20three%20rounds%20of%20evaluation,Dilithium%2C%20FALCON%2 C%20and%20SPHINCS%2B.

3. https://thequantuminsider.com/2022/11/21/google-already-using-pqc-to-protect-internal-communications/
4. https://www.siliconrepublic.com/enterprise/quantum-apocalypse-store-now-decrypt-later-encryption
5. Bernstein, D. J., Lange, T., & Schwabe, P. (2017). Post-quantum cryptography. Nature, 549(7671), 188-194.
6. Aisenberg, M. (2019). Post-Quantum Cryptography: An Overview of Algorithms and Standardization Efforts. IEEE Security & Privacy, 17(6), 81-87.
7. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, 212-219.
8. Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 124-134.
9. National Institute of Standards and Technology (NIST). Post-Quantum Cryptography. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography
10. Alagic, G., Amiri, S., & Moody, D. (2020). Post-Quantum Cryptography: Current Developments and Future Directions. IEEE Security & Privacy, 18(4), 28-37.
11. Ding, J., & Yang, B. Y. (2017). Code-based cryptography: A survey. Designs, Codes and Cryptography, 82(1-2), 179-200.