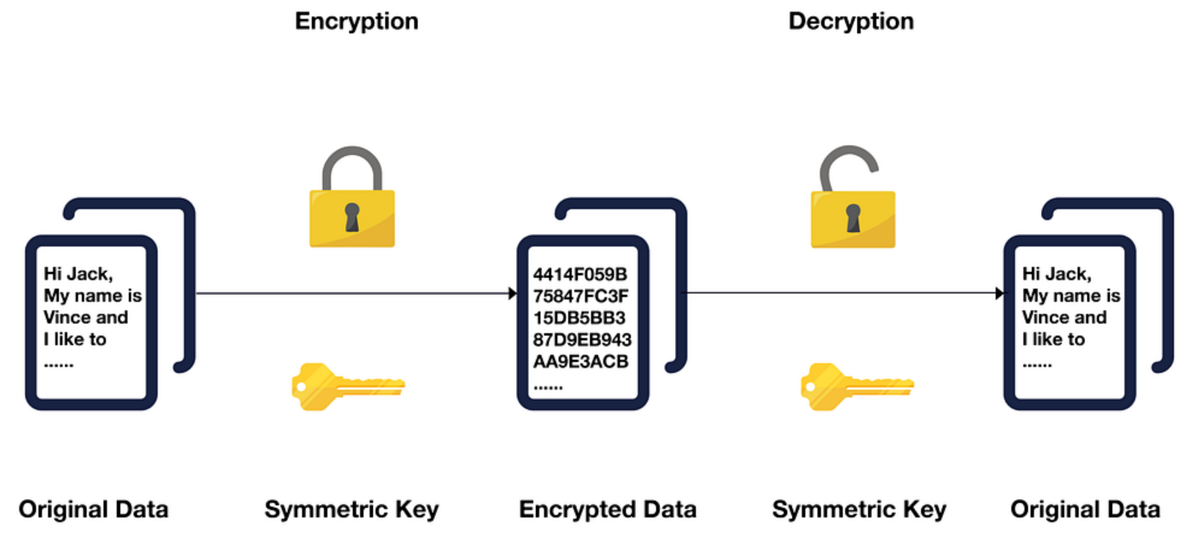
Defending Against Quantum Computer Cryptanalysis: Current Developments and Practical Challenges of Post-Quantum Cryptography

Cryptography is a complex field with high mathematical thresholds, particularly within cybersecurity. However, the widespread use of mobile devices, the rise of cryptocurrencies, and the advancement of cloud services have integrated cryptography into everyday life, protecting the digital assets and privacy of billions globally. Recently, a hot topic has been the claim that "quantum computers will destroy existing cryptographic systems," predicting that the advent of quantum computers will devastate cryptocurrencies[1], national defense, and cybersecurity[2], presenting unprecedented threats. Is this as catastrophic as it sounds? This article will explore the impact of quantum computers on existing cryptographic systems, including the extent and scope, and the reasons why "post-quantum cryptography" (PQC), which can withstand quantum computer attacks, is not yet widely used.

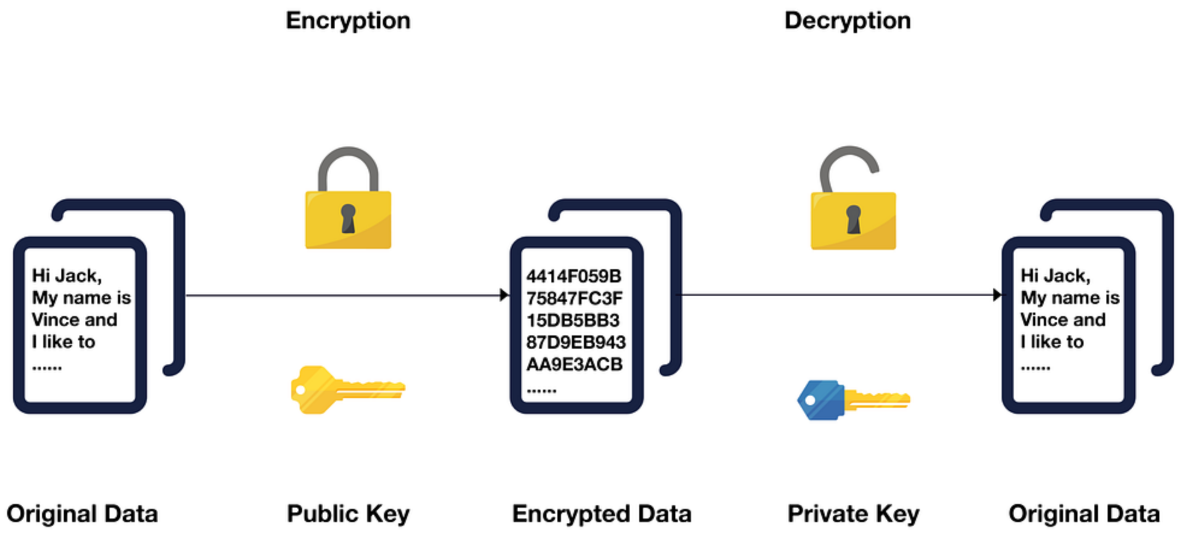
Cryptographic systems fall into two main categories: "symmetric" and "asymmetric" (or public-key) systems. In about 15 to 20 years[3], with the emergence of large-scale universal quantum computers with over 2,000 qubits[4], the threat to these two types of cryptographic systems will differ[5].

Symmetric Cryptographic Systems



Quantum computers running Grover's algorithm[6] will reduce the security level of symmetric cryptographic systems by half. For example, if AES with a 128-bit key is used now, its security will be effectively reduced to 64 bits in the future, making it vulnerable to attacks with 2642^{64}264 operations. Therefore, defending against quantum computers is relatively straightforward: doubling the key length will maintain the same level of security as today. For instance, upgrading from AES 128 to AES 256 will provide equivalent security. Overall, the impact of quantum computers on symmetric cryptographic systems is limited.

Asymmetric Cryptographic Systems



In contrast, asymmetric cryptographic systems, also known as "public-key cryptosystems," will face devastating impacts. These systems include RSA encryption and signing algorithms, Diffie-Hellman key exchange, and Elliptic Curve Cryptography (ECC), all of which are widely used worldwide. Their security is based on the difficulty of problems like "integer factorization" and "discrete logarithms." However, in 15 to 20 years[3], quantum computers running Shor's algorithm could solve these mathematical problems in a short time. This means current algorithms will become obsolete and need replacement with new public-key cryptosystems. Cryptographic systems that can resist quantum computer attacks are collectively referred to as "post-quantum cryptography" (PQC). PQC algorithms are based on mathematical problems that are not easily solved by quantum computers, and thus can run on classical computers.

Post-Quantum Cryptography National Standards

In response to the quantum threat, the National Institute of Standards and Technology (NIST) in the United States has been developing national standards for post-quantum cryptography by soliciting proposals from top cryptographers worldwide. In the first round of selection in 2017, 69 algorithms were considered[6]. After the second round in January 2019, 26 algorithms remained[7], including 17 for key establishment and 9 for digital signatures. Although standards are not yet finalized, promising algorithms have already been implemented in some areas.

Three years ago, Google Chrome began using the post-quantum cryptography algorithm

NewHope for key establishment[8], suggesting that HTTPS on Chrome might have already utilized PQC. German chip manufacturer Infineon has also demonstrated a proof of concept with NewHope[9]. However, practical efficiency remains a critical factor in adopting post-quantum cryptography. Compared to existing public-key systems, PQC requires longer key lengths and produces larger digital signatures, which makes it less convenient to use. Furthermore, there are few teams proficient in implementing and applying these new algorithms, which is why they have not yet become widespread.

While various applications of quantum computers are being speculated, technology itself is neutral; its use depends on human intent. One side may use it to protect the world, while the other may use it to destroy it. Perhaps future discussions should not focus solely on the advent of quantum computers but should consider various potential applications and develop technologies and regulations to ensure a smooth and secure transition for individuals, businesses, and nations into the quantum era.

Thank you for reading this article. Feel free to applaud, share, or reply. When sharing or reprinting, please credit the source: Quan'an Intelligent Technology (IKV-Tech). We will continue to unveil the mysteries of the field of cryptography and its applications in future articles. Stay tuned.

---

[1]: "Will Quantum Computers Destroy Cryptocurrencies?" Scholars: We Should Worry About Other Areas. https://www.blocktempo.com/the-new-ways-to-save-crypto-from-a-post-quantum-world/ [2]: Quantum Computers: A Hidden Threat to Cybersecurity. https://www.businesstoday.com.tw/article/category/154685/post/201611040014/%E9%87%8F%E5%AD%90%E9%9B%BB%E8%85%A6%E7%A5%9E%E7%AE%97%20%E8%B3%87%E5%AE%89%E6%9C%89%E9%9A%B1%E6%86%82 [3]: IEKView: The Commercialization of Quantum Computing. https://ieknet.iek.org.tw/iekrpt/linkiac.aspx?rpt_idno=20120303 [4]: The Impact of Quantum Computing on Present Cryptography. https://arxiv.org/pdf/1804.00200.pdf [5]: Williams, C. P. (2010). Explorations in Quantum Computing. Springer Science & Business Media. [6]: Post-Quantum Cryptography - Round 1 Submissions. https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-1-Submissions [7]: Post-Quantum Cryptography - Round 2 Submissions. https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions [8]: Google is Working to Safeguard Chrome from Quantum Computers. https://www.theverge.com/2016/7/7/12120280/google-chrome-canary-quantum-computing-encryption-new-hope [9]: Ready for Tomorrow: Infineon Demonstrates First Post-Quantum Cryptography on a Contactless Security Chip. https://www.infineon.com/cms/en/about-infineon/press/press-releases/2017/INFCCS201705-056.html