The Quantum Countdown: Why Your Data Needs Protection Now

Executive Summary

Encryption and authentication are essential for protecting data from unauthorized access and preventing tampering. In both cases, it is critical to consider the duration of protection required: is it sufficient that unauthorized parties cannot access or alter the data *today*, or must the data remain secure a longer period?

For encrypted communications sent over the Internet or broadcasted via radio, organizations must recognize that attackers may store intercepted data for decryption attempts in the future.

During the 21st century, cryptography experienced relative stability, with most attacks targeting implementation flaws rather than fundamental weaknesses in the algorithms themselves. However, we are now entering a paradigm shift where quantum computers pose a serious threat to all classical, well-established algorithms.

By combining the proven security of classical algorithms with new algorithms designed to resist quantum attacks, hybrid cryptographic schemes provide robust protection for long-term data security.

This whitepaper outlines strategies for organizations to safeguard their data against the emerging threat of quantum computing and explains why hybrid schemes represent the most effective approach for protecting sensitive information over time.

Introduction

The Race Towards Quantum Superiority

Quantum computers promise transformative advances across science, from drug discovery to complex simulations. However, the introduction of a **cryptographically relevant quantum computer (CRQC) will be both profound and disruptive**[1], as it could break or severely weaken classical encryption methods, enabling both offensive cyber operations and decryption of sensitive communications.

History illustrates the strategic value of withholding advanced technology. For example, the Diffie-Hellman key exchange[2], developed years earlier by Britain's GCHQ, was only made public in 1976. Similarly, a government in possession of a CRQC might **delay disclosure**, leveraging it strategically for intelligence or cyber operations until other powers achieve comparable capabilities.

During such period of *assumed* exclusive access, operations would likely focus on activities that are difficult to detect, like decryption of captured communication. By not revealing the existence of the CRQC it would be possible to quietly maintain a strategic advantage for as long as possible.

The Data Harvesting Threat

Announcement of **data breaches involving harvesting of sensitive data have become a part of everyday life**. These attacks are frequently carried out by so called Advanced Persistent Threat (APT) groups[3]. Examples include *Salt Typhoon*[4], which has targeted telecommunication infrastructure, and *Hafnium*[5], which has targeted law firms and other organisations handling sensitive data. Such groups are often linked to **China's Ministry of State Security (MSS),** while other are associated with the **Russian**, **Iranian**, or **North Korean** governments[6].

A further structural threat arises from the use of **Chinese equipment in critical parts of telecom infrastructure**[7]. Any hidden backdoor or design flaw could be exploited to harvest communications at massive scale. This risk is heightened by Chinese laws that may compel companies to cooperate with state intelligence agencies.

In addition to these ongoing intrusions, the **Edward Snowden disclosures in 2013**[8] revealed that also Western intelligence agencies were conducting extensive, large-scale harvesting of global communications. These programs intercepted Internet traffic, metadata, and encrypted messages for long-term storage, demonstrating that systematic data collection has been a reality for more than a decade.

This creates profound long-term risks for sensitive data, including:

- Government communications
- Healthcare and patient records
- Intellectual property and research data
- Financial transactions

- Corporate strategy, legal documents, and proprietary information

To understand the practical implications, take a moment to reflect on the impact if an attacker suddenly gained access to everything you have written or transmitted:

i. Today
ii. Yesterday
iii. last year
iv. ten years ago

Similarly, consider the consequences if someone could falsify a signature or alter the contents of a document from these same points in time.

Because the future threat landscape is uncertain, organizations must design for longevity. If data must remain secure for one year, it is sensible to engineer protections that last ten.

Impact of Quantum Algorithms on Classical Cryptography

Quantum algorithms pose specific, well-understood threats:

- **Shor's algorithm**[9, 10]**:** efficiently factoring integers and computing discrete logarithms, breaking classical Public Key Cryptography, including:
  - **RSA** – *Rivest–Shamir–Adleman*: key encryption and digital signature algorithm based on the factorization of large prime numbers.
  - **ECC** – *Elliptic Curve Cryptography*: key encryption and digital signature algorithm based on discrete logarithms over elliptic curves, offering strong security with smaller key sizes than RSA.
  - **DH** – *Diffie–Hellman*: A key exchange protocol that allows two parties to securely establish a shared secret over an insecure channel.
- **Grover's algorithm**[9, 10]**:** reduces the effective security of symmetric ciphers by accelerating brute-force attacks.

While symmetric algorithms can be strengthened by increasing key sizes, asymmetric cryptography requires entirely new primitives.

Post-Quantum Cryptography

Lattice-Based Cryptography

Lattice-based cryptography[11] is one of the most extensively studied domains in modern cryptography and forms the foundation of several PQC algorithms selected by the U.S. based National Institute of Standards and Technology (NIST). Its historical development provides strong confidence in its long-term resilience.

The study of lattice problems began with work by Miklós Ajtai and others[12], who formalized the hardness of problems such as the Shortest Vector Problem (SVP) and Closest Vector Problem (CVP). Ajtai's 1996 worst-case to average-case reduction was a breakthrough, providing unprecedented theoretical security guarantees.

During the early 2000s, lattice-based encryption schemes matured into practical, efficient, and commercially deployed cryptosystems.

As result of the NIST PQC competition, lattice-based algorithms were selected for standardization due to their strong security proofs and implementation maturity.

Benefits of Standardized PQC Algorithms

NIST is finalizing PQC standards that include lattice-based and hash-based algorithms for public-key encryption, key encapsulation, and digital signatures.

Organizations should avoid proprietary or homegrown cryptographic algorithms for the following reasons:

- **Rigorous, Global Cryptanalysis:** NIST PQC candidates have undergone years of open, public scrutiny by the global cryptographic community. Proprietary algorithms rarely receive comparable analysis, making undiscovered vulnerabilities far more likely.

- **Transparency and Trust:** NIST's selection process is transparent and inclusive, involving academic institutions, industry experts, and government laboratories. Proprietary solutions may hide design flaws or implementation weaknesses.

- **Interoperability:** Industry-wide adoption requires consistent standards. NIST algorithms are already being integrated into Internet Engineering Task Force (IETF) drafts, major open-source libraries, hardware roadmaps, and commercial products.

- **Regulatory Alignment:** Governments and regulators increasingly mandate quantum-safe migration strategies aligned with NIST standards.

- **Reduced Long-Term Risk:** Cryptographic history shows that proprietary encryption often fails under scrutiny.

- **Avoiding Vendor Lock-In:** Standards allow multiple interoperable implementations.

Hybrid Cryptography

As further outlined in **IETF RFC 9794**[13], hybrid cryptography combines a classical algorithm with a PQC algorithm. In a hybrid scheme, security depends on both components—meaning an attacker must break *both* the classical and the PQC algorithm to compromise the system.

Classical public-key algorithms have benefited from decades of cryptanalysis, standardization, and large-scale real-world deployment. Their strengths, limitations, and operational characteristics are well understood and highly predictable.

PQC algorithms are promising and backed by strong theoretical foundations, but they have not yet experienced the same depth of analysis or breadth of real-world exposure as classical cryptography.

Hybrid models therefore provide a balanced and risk-mitigating approach by ensuring:

- Protection against existing classical adversaries
- Protection against future quantum-capable adversaries

Conclusion

Quantum computing will profoundly affect the foundations of modern cryptography. Given the rapid advancements in the field, **organizations should act now** to ensure their security infrastructures remain robust today and quantum-resilient tomorrow.

Transitioning cryptographic systems is a complex, multi-year process that requires organizations to inventory assets, update protocols, ensure interoperability, and validate performance and security. For large enterprises, this effort often spans several years.

Messaging systems are especially vulnerable to **"harvest now, decrypt later"** attacks. Sensitive data is routinely collected by state-linked hacker groups associated with the China, Russia, Iran, and North Korea. The use of Chinese telecom equipment in critical network infrastructure adds additional risk, as backdoors or legal obligations could enable mass interception of communications. Snowden's 2013 disclosures showed that also Western intelligence agencies have long conducted large-scale global communications harvesting, including encrypted traffic.

Hybrid cryptography offers the most reliable and practical path toward quantum-safe security by providing protection against current classical threats while building resilience against future quantum-enabled adversaries.

References

1. **Preparing for Quantum-Safe Cryptography**, an NCSC whitepaper about mitigating the threat to cryptography from development in Quantum Computing.
   Published 11 November 2020.
   https://www.ncsc.gov.uk/pdfs/whitepaper/preparing-for-quantum-safe-cryptography.pdf sdfds

2. **Diffie-Hellman key exchange**
   https://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange

3. **Advanced Persistent Threat groups (APT)**
   https://en.wikipedia.org/wiki/Advanced_persistent_threat

4. **Hafnium**, an APT group allegedly linked to the Ministry of State Security in China
   https://en.wikipedia.org/wiki/Hafnium_(group)

5. **Salt Typhoon**, an APT group allegedly linked to the Ministry of State Security in China
   https://en.wikipedia.org/wiki/Salt_Typhoon

6. **Nation-State threats,** by U.S. Cybersecurity & Infrastructure Security Agency (CISA). Advanced Persistent Threat groups are often linked to the government of China, Iran, Russia or North Korea.
   https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors

7. **Top EU official urges more countries to ban China's Huawei, ZTE from 5G networks.** A structural threat originating from the use of Chinese equipment in critical parts of telecom infrastructure.
   https://www.cnbc.com/2023/06/16/eu-urges-more-countries-to-ban-chinas-huawei-zte-from-5g-networks.html

8. **Edward Snowden NSA files: secret surveillance and our revelations so far**. The Guardian summarizes the data leakage on 21 August 2013.
   https://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations

9. **Post-Quantum Cryptography for Engineers.** The threat from Shor´s algorithms on classical Public Key Cryptography such as RSA, ECC, Diffie-Hellman, and Grover´s algorithms on symmetric ciphers.
   Published 26 August 2025.
   https://www.ietf.org/archive/id/draft-ietf-pquip-pqc-engineers-14.html

10. **Understanding Shor´s and Grover´s Algorithms and Their Impact on Cybersecurity.** An overview of the threats from Shor´s and Grover´s algorithms.
    https://www.fortinet.com/resources/cyberglossary/shors-grovers-algorithms

11. **Lattice-based Cryptography.** A survey on the security of the lattice-based NIST finalists, published 8 April 2025
    https://eprint.iacr.org/2025/304.pdf

12. **Lattice-based Cryptography**
    https://en.wikipedia.org/wiki/Lattice-based_cryptography

13. **RFC 9794: a new standard for post-quantum terminology**, by NCSC publications. Published 2 October 2025
    https://www.ncsc.gov.uk/blog-post/new-standard-for-post-quantum-terminology