Technology Innovation Institute

ASSURING PRIVACY AND CONFIDENTIALITY IN A QUANTUM-ENABLED FUTURE

WHITEPAPER

2025

Authors:

Dr. Victor Mateu
Acting Chief Researcher, Cryptography Research Center
Technology Innovation Institute

Dr. James Grieve
Senior Director, Quantum Research Center
Technology Innovation Institute

Introduction

The development of public key cryptography techniques in the mid-1970s was critical to the growth of decentralized systems of trust underpinning the modern Internet and cloud computing.
These made it possible to authenticate parties, share secrets, and communicate securely across untrusted networks. These capabilities are combined to ensure the confidentiality and integrity of communications, stored data, software and firmware updates. They have also played an essential role in developing blockchain and decentralized ledger technology.

Security experts anticipate that the dawn of cryptography-relevant quantum computers (CRQCs) in the next five to fifteen years will breach the trust underpinning the digital economy. Telecom, commerce, finance, utility, manufacturing, government and health systems are all at risk. This event is called Q-day in security circles. Many challenges in quantum computing will need to be overcome for this to occur. There has been incredible progress in recent years, and at this point, there is general optimism in the quantum computing field that it can and will be done.

A particular concern is that sensitive data with long-duration privacy and confidentiality concerns may be susceptible to compromise in the future through store now decrypt later (SNDL) attacks, also called harvest now decrypt later (HNDL). This includes banking information, government communications, health data, and commercial secrets. In addition, blockchain cryptographic infrastructure presents unique challenges that must be addressed
to ensure end-to-end trust in these systems.

Thus, enterprises and governments must migrate to new quantum-safe infrastructure long before Q-day when CRQCs emerge. The practical adoption of these innovations requires a systemic assessment of existing systems rather than focusing on new cryptographic algorithms alone.

Owing to the potential severity of this risk, the security industry is actively developing cryptographic techniques and secure networks that could help thwart these attacks using post-quantum cryptography (PQC) algorithms and quantum key distribution (QKD) infrastructure. PQC is believed to be more robust than current classical approaches against quantum attacks. QKD protects the exchange of encryption keys at the physical level. These approaches can bolster security against quantum attacks in complementary ways.

Introduction

The US National Institute of Standards and Technology (NIST) standardized the first PQC algorithms in late 2024.[1] The security community is starting to implement these across new protocols that safeguard confidentiality, integrity and authentication to prepare for a quantum secure future. At the same time, researchers, telecom providers, and banks are starting to test and implement QKD systems. Ongoing work on crypto agility approaches will help adopt quantum secure algorithms across existing infrastructure.

Just because PQC algorithms and QKD infrastructure are implemented in some places does not mean the system as a whole will necessarily be secure. Also, upgrades will not protect data encoded with existing cryptography schemes harvested by adversaries today for future decryption.
Thus, organizations are starting to develop tools for assessing the footprint of existing cryptographic algorithms and simulating migration scenarios to guide the process using emerging cryptographic discovery and inventory tools.

It is imperative to address these broader issues through a systematic and automated approach today to plan for the seamless rollout of new PQC algorithms and QKD infrastructure more quickly and efficiently.

Figure 1. The "store now, decrypt later" attack scenario, in which an adversary stores encryped data until the eventual availability of a large-scale quantum computer.

[1] "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," NIST, Aug. 2024, Accessed: Mar. 05, 2025. [Online]. Available: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

The quantum problem

Governments have been using private key encryption methods for decades. These are called symmetric cryptography since the same key is used to scramble and recover secrets. They can protect the secrecy of messages as long as an adversary does not intercept the key or crack the mathematical algorithm used to encode the secrets.

In the mid-1970s, multiple researchers discovered public key methods supporting new encryption approaches for key exchange, and digital signatures across untrusted networks. They are called asymmetric because in this case, one entity needs to use the public key to encrypt, and the other entity needs to use the private key to decrypt. They have different keys, so they are not symmetric.
Early examples include the RSA and Diffie-Hellman methods, and other public key variants like DSA are also used today.

Asymmetric schemes are not as fast as symmetric ones. Symmetric approaches are not as flexible as asymmetric ones. Thus, they are often combined in different ways to take advantage of their respective merits. Asymmetric methods are used for authorization across insecure systems and then distributing symmetric keys for more efficient communication. Even though symmetric encryption is more resilient to quantum attacks, it might be compromised through attacks on asymmetric schemes used to communicate the shared secret.

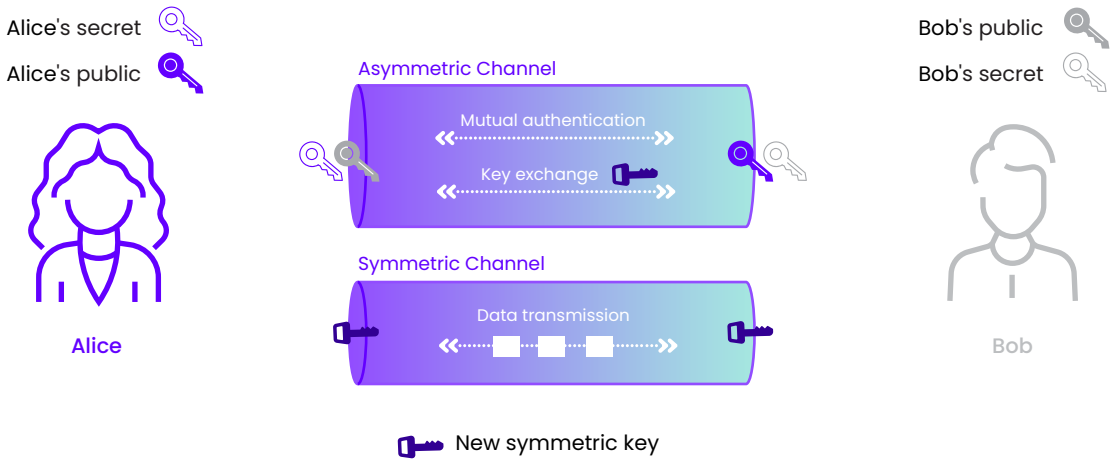

Figure 2. Illustration of symmetric and asymmetric key exchange paradigms.

[2] Peter Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," Proceedings of the 35th Annual Symposium on Foundations of Computer Science (1994), 124-134.
[3] L. Grover, "A fast quantum mechanical algorithm for database search" Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (STOC 1996), 212-219, 1996.

The quantum problem

CRQC could threaten the security of both symmetric and asymmetric approaches. In 1994, Peter Shor proposed a quantum computing algorithm (Shor's Algorithm) that could compromise the integrity of many asymmetric encryption techniques.[2] Two years later, Lov Grover discovered another technique that could speed up a search for the keys in symmetric encryption schemes.[3] Grover's Algorithm provides an exponential improvement, but the core problem remains exponential in complexity. In practice, this means the security remains the same by just doubling the size of the keys.The catch is that to threaten present-day encryption schemes, both algorithms would require very large-scale and reliable quantum computers, which are much more advanced than the state of the art at that time. Thirty years later, no one has built a quantum computer capable of cracking any relevant cryptographic scheme using these algorithms.

Two decades after the discovery of Shor's and Grover's algorithms, security researchers began to take the problem more seriously. In 2015, Michele Mosca, a quantum computing and security researcher at the University of Waterloo, developed a thorough analysis of the risks of CRQC on security infrastructure.[4] In particular, he considered the risks of SNDL attacks against national secrets, banking transactions, and health records that require a long confidential shelf life.

Mosca's Theorem posits that the urgency of moving to quantum computing-resistant security depends on the following:

- **Shelf-lifetime:** How many years must data remain secure?
- **Migration time:** How long will it take to upgrade systems securely?
- **Threat timeline:** Estimated time until potential adversaries acquire CRQC.

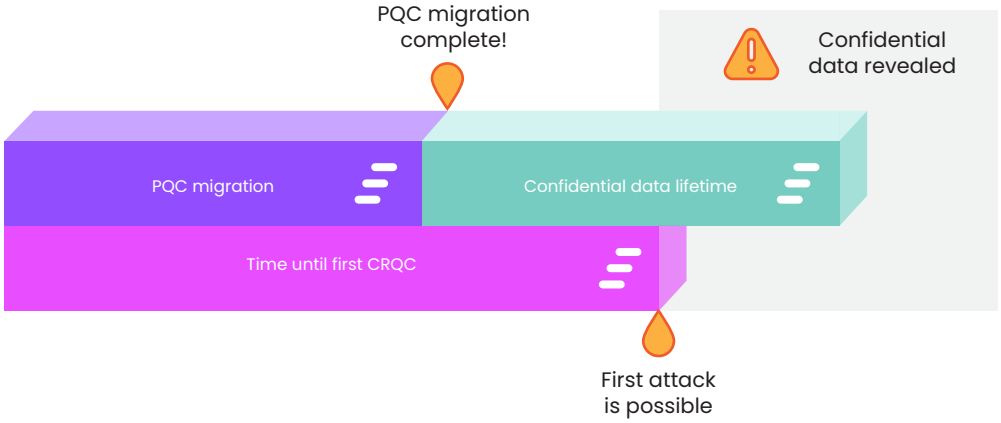

Figure 3. Mosca's theorem diagram

[4] M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?," 2015, 2015/1075. Accessed: Mar. 07, 2025. [Online]. Available: https://eprint.iacr.org/2015/1075]

The quantum problem

The implications are that even if CRQC is a decade away and it takes five years to upgrade encryption, existing sensitive information generated in the interim is at risk of compromise. In 2015, Mosca estimated a 14% chance that RSA would be vulnerable by 2026 and a 50% chance by 2031.
In 2024, Mosca et al. surveyed a panel of quantum computing experts, revealing a broader range of opinions.[5] The optimists predicted a 14% probability of a CRQC by 2029 and 34% by 2034. The pessimists predicted a 19% probability of CRQC by 2034.

To appreciate the scaling challenges facing quantum computers today, it is important to understand a few core concepts. A qubit is a simple information primitive of a 2-level quantum mechanical system, such as a quantum computer, analogous to the 2-level bits in classic computers. The number of qubits is often used to characterize relative improvements in quantum computers that may take advantage of different physical principles.

The popular press is filled with impressive-sounding claims about more qubits, which lack context. For example, quantum processors for simulated annealing from D-Wave can support thousands of qubits, but these are more constrained than universal quantum computer architectures. Some interesting research has found ways to apply quantum processors to crack toy encryption algorithms, but it has not been scaled.[6]

CRQC will likely require new designs for creating long-lived and low-noise qubits for building quantum circuits capable of implementing Grover's or Shor's algorithms. The current stability of the qubits (probability of errors occurring) prohibits large algorithms from reaching useful conclusions, and most teams agree that some error correction scheme is needed. The overhead is envisaged as a process of mapping physical qubits to logical qubits. The current generation of error-correcting codes requires a large overhead in terms of the number of physical qubits compared to the logical qubits needed for utility.

Researchers have estimated the quantum computing resources needed to compromise a 256-bit key in elliptic curve cryptography (ECC) and a and a RSA-2048 encryption key to be 2,500 and 4,000 logical qubits respectively.[7] While these numbers are interesting for illustrative purposes, practical resource estimates must also include the overheads imposed by error correction, as well as computation time. As of publication, the latest estimates suggest that RSA-2048 encryption keys can be factored using 1 million noisy physical qubits: a twenty-fold reduction in the same team's earlier estimate from 2019.[8]

Such progress highlights the remarkable pace of development in this field. Despite the relative immaturity of today's quantum machines, it is clear that continuous innovation in quantum hardware, quantum error correction and classical control techniques will one day deliver a system capable of threatening legacy cryptography. It is only a matter of time.

[5] "Quantum Threat Timeline Report 2024," Global Risk Institute. Accessed: Mar. 07, 2025. [Online].
Available: https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/
[6] "Chinese Scientists Report Using Quantum Computer to Hack Military-grade Encryption." Accessed: Mar. 12, 2025. [Online].
Available: https://thequantuminsider.com/2024/10/11/chinese-scientists-report-using-quantum-computer-to-hack-military-grade-encryption/
[7] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter, "Quantum resource estimates for computing elliptic curve discrete logarithms," Oct. 31, 2017, arXiv: arXiv:1706.06752. doi: 10.48550/arXiv.1706.06752.
[8] Craig Gidney, "How to factor 2048 bit RSA integers with less than a million noisy qubits,
" May 21, 2025, arXiv: 2505.15917v1. https://arxiv.org/html/2505.15917v1.

The quantum problem

Here are some of the ways that potential quantum vulnerabilities could apply in systems, cloud computing, data management, and communications infrastructure:

• **Secure Communication:** Eavesdropping and interception attacks that capture public keys could allow attackers with CRQC to listen in on secure communication protocols like Transport Layer Security (TLS) that secure web traffic and VPN tunnels, secure messaging apps, and telecommunication networks.

• **Data Encryption and Storage:** Symmetric encryption is used to protect sensitive data at rest in databases, backups, and cloud storage, and it is believed to be resistant to quantum attacks. RSA and ECC-based key wraps or RSA-encrypted storage often protect the keys. CRQC attacks could unlock these keys for future decryption of data stored in cloud and SaaS services.

• **Digital Signatures and Integrity:** RSA and Elliptic Curve Digital Signature Algorithms (ECDSA) are used in applications like code signing, secure boot, document signing and blockchain transactions. These digital signatures verify the authenticity of software updates, authentication tokens, financial transactions, and PKI certificates.

• **Banking and Financial Services:** CRQC attacks could compromise interbank communication, long-lived transactions, and customer-facing services such as online banking and ATM network security. Attacks on the digital signature infrastructure in procurement and trading could facilitate forgery in the future.

• **Healthcare:** Healthcare data, including patient records and genomics data, must remain confidential for a patient's lifetime, making it particularly vulnerable to SNDL attacks.

• **Government:** Long-lived government national security secrets and citizens' data are similarly vulnerable to SNDL attacks in the future.

• **Critical infrastructure:** Attacks on the command-and-control links that use secure SCADA communication systems could allow attackers to compromise critical infrastructure, including energy grids, water systems, gas pipelines, and industrial equipment.

CRQC attacks could allow attackers to alter or corrupt data stored on a blockchain, gain unauthorized access to crypto wallets, disrupt consensus mechanisms, and disrupt supply chains that rely on blockchain for transparency and traceability. They could also manipulate the logic in smart contracts and exploit external dependencies in external oracles, leading to unintended consequences.

The blockchain community is addressing many of these issues by adopting PQC in the blockchains themselves. Attacks on secure boot and software update authentication infrastructure could allow attackers to steal private keys, modify blockchain apps, or disrupt consensus mechanisms. Hackers have already gained access to accidentally leaked cryptographic keys for secure boot, which is widely used on commercial computers.

PQC and QKD could help mitigate these kinds of quantum attacks in the future. Leveraging both effectively will require a detailed assessment of existing cryptographic processes, making it easier to deploy them across enterprises and governments.

Post-quantum cryptography

As previously noted, asymmetric encryption schemes like RSA, DSA, and ECDSA provided the foundations for public key cryptography used in key exchange and digital signatures across untrusted networks. These all rely on mathematical problems that could be cracked using Shor's algorithm once CRQC emerges.

Fortunately, researchers have discovered several families of mathematical problems and associated classes of cryptographic systems that cannot be cracked with Shor's algorithms.[9] Many of these date back to the 1970s. Examples include hash-based cryptography (1979), code-based cryptography (1978), lattice-based cryptography (1998), and multivariate-quadratic equation cryptography (1996). They all come with tradeoffs regarding performance, computation requirements, key size, and overhead.

NIST launched a competition across implementations of these techniques in 2016 and selected five Federal Information Processing Standards (FIPS) for Post-Quantum Computing and three have been finalized already.[10] FIPS 203 provides a key encapsulation mechanism for establishing shared secrets among two parties over a public channel. FIPS 204 and FIPS 205 each specify digital signature schemes used to detect unauthorized modifications to data and authenticate the signatory. NIST has also proposed a new round to obtain better-performing digital signature algorithms and more diversification, given that the field is now more mature.

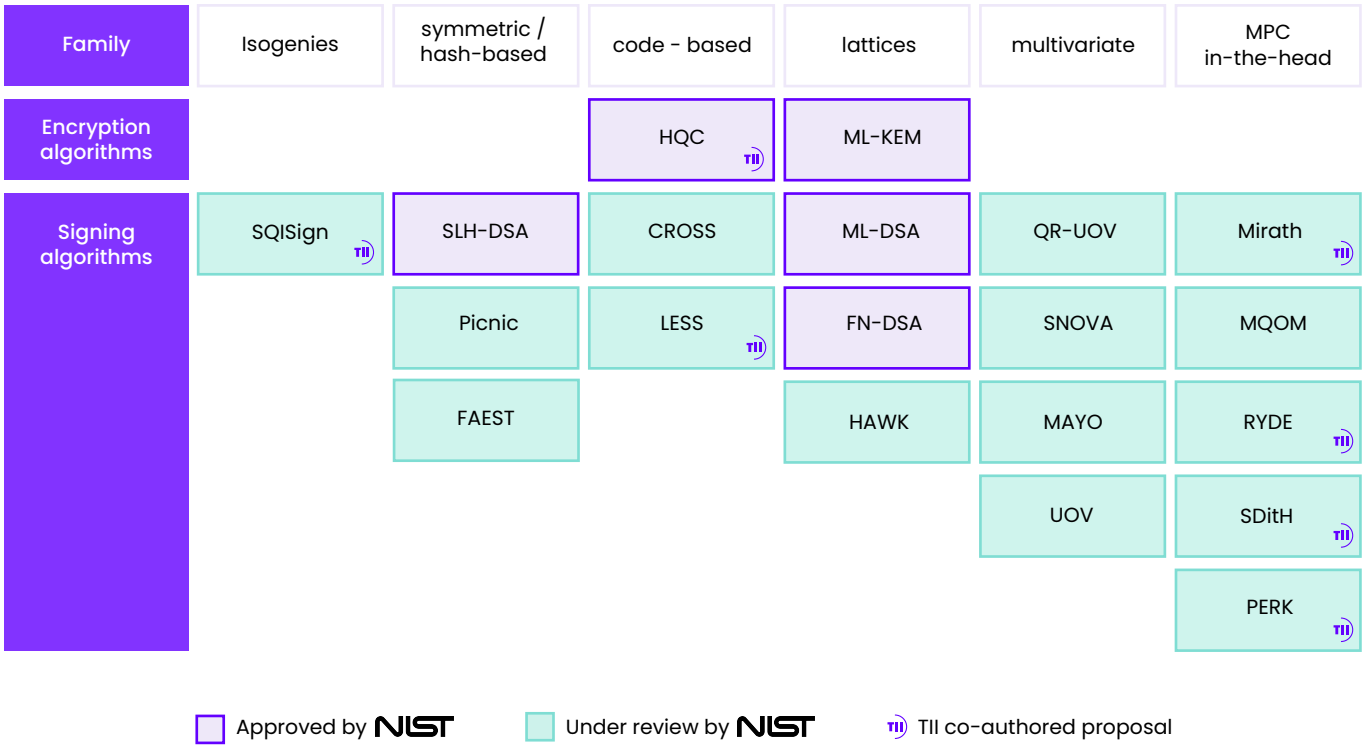

Figure 4. PQC Algorithms: Approved and Under Review by NIST

[9] D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds., Post-Quantum Cryptography. Berlin, Heidelberg: Springer, 2009. doi: 10.1007/978-3-540-88702-7.
[10] "Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography," NIST, Aug. 2024, Accessed: Mar. 12, 2025. [Online]. Available: https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved

Post-quantum cryptography

NIST has recommended that popular asymmetric cryptographic schemes be deprecated and replaced with PQC by 2030 and disallowed after 2035.[11] This timeline may be optimistic for organizations reliant on legacy systems and older hardware that may be difficult to replace easily. Earlier cryptographic migrations took well over a decade across industries.[12]

Also, complete migration is unlikely to happen simultaneously and will require support for classical algorithms for backward compatibility alongside post-quantum algorithms for some time. Systems like those with embedded cryptographic algorithms will be harder to migrate.

[11] A. Regenscheid, "Transition to Post-Quantum Cryptography Standards," National Institute of Standards and Technology, Gaithersburg, MD, NIST IR 8547 ipd, 2024. doi: 10.6028/NIST.IR.8547.ipd.
[12] A. Jadhav, "Perspectives on Migration Toward Post-Quantum Cryptography," EE Times. Accessed: Mar. 12, 2025. [Online]. Available: https://www.eetimes.com/perspectives-on-migration-toward-post-quantum-cryptography/

Quantum Key Distribution

Today, one of the safest ways to share keys is to employ a trusted human carrier to securely deliver a key between parties. Now, vendors are exploring how special-purpose fiber optic and satellite networks can leverage quantum principles to do something similar. Several QKD networks have already been deployed to assess integration and implementation challenges.

QKD protocols are unconditionally secure at the physical level, which is impossible to achieve with algorithms alone. They promise an efficient alternative for out of band key distribution, exchanging keys, cheaper and quicker than vetting trusted couriers and flying them worldwide. Vendors, banks, security agencies, and researchers have begun investigating their potential for providing an additional layer of proven security to their networks and complementing PQC algorithms running on the higher network layers.

QKD uses quantum properties to encode secret keys in photons (particles of light). If an eavesdropper tries to intercept the signal, their action will necessarily change the quantum state, thus revealing the eavesdropping attempt. After exchanging the quantum signals, the two parties compare a subset of their measurements to estimate the fraction of errors (corrupted bits), which are assumed to have resulted from attempted eavesdropping. After appropriate postprocessing, the parties are left with a shared secret key.

Some security organizations, such as the US National Security Agency (NSA), have advocated that QKD should not be used for securing data in national security systems until several limitations are overcome.[13] Many of these concerns also apply to PQC and practical physical infrastructure security today, and may be overblown or are being actively mitigated within the QKD community.

For example, much like the new PQC KEM standards, QKD provides a way to exchange keys securely but does not provide a mechanism to authenticate that the sender is who they say they are. Both must be combined with strong authentication techniques to prevent man-in-the-middle attacks.[14]

Today, QKD deployments are at an early stage internationally, focusing on small-scale networks and point-to-point secure communications. In the future, the construction of rich, multi-hop routing connections like those that have fostered the growth of the Internet will change as the technology matures and QKD can help fill in some of the current gaps and limitations that can arise when using PQC alone to secure systems.

[13] "National Security Agency/Central Security Service > Cybersecurity > Quantum Key Distribution (QKD) and Quantum Cryptography QC." Accessed: Mar. 12, 2025. [Online]. Available: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC
[14] "Quantum key distribution and authentication: Separating facts from myths," Amazon Science. Accessed: Apr. 14, 2025. [Online]. Available: https://www.amazon.science/blog/qkd-and-authentication-separating-facts-from-myths

Quantum Key Distribution

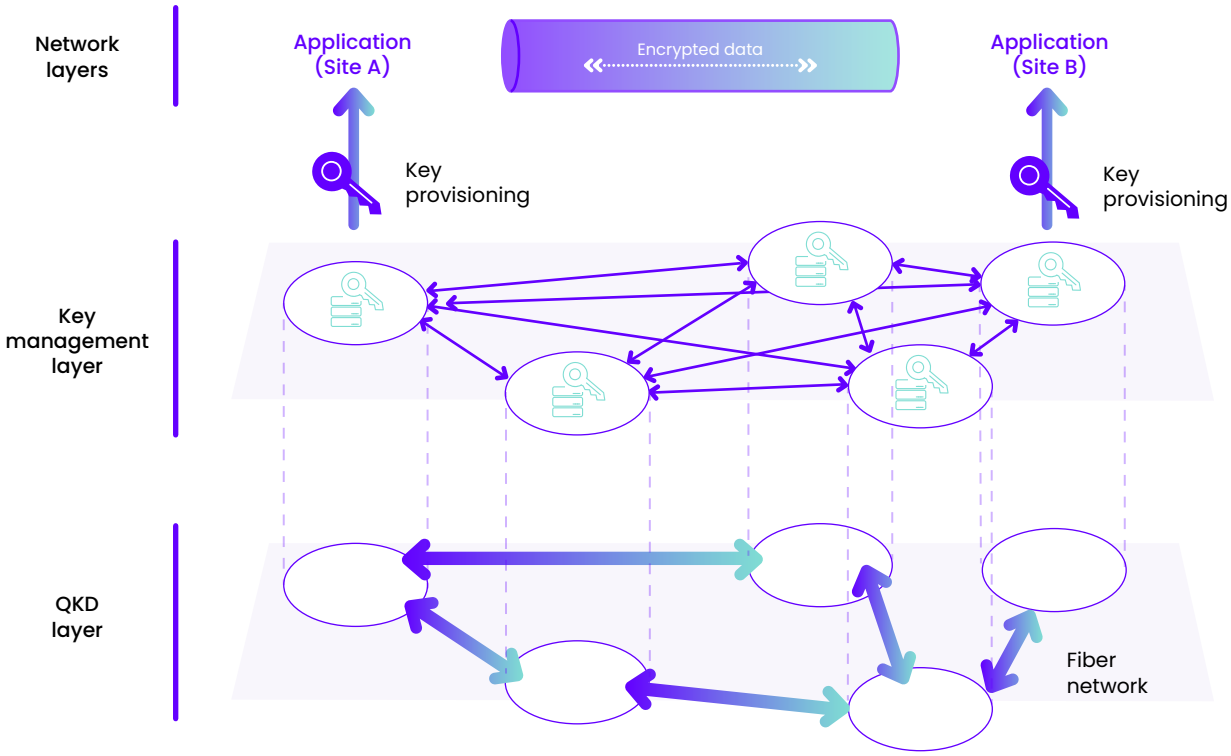

Figure 5. QKD network layer diagram

QKD developers confront an important challenge in managing the various vulnerabilities that can arise while designing and constructing secure QKD systems, which also applies to PQC algorithms. A much larger body of experts is familiar with validating software-based security systems than hardware-based security in QKD systems. This gap must be addressed through more comprehensive training programs to familiarize engineers with QKD's specific strengths and vulnerabilities.

The QKD community is exploring various approaches to overcome these challenges by creating and evolving certification programs for QKD through standards organizations like British Standards Institute (BSI), International Organization for Standardization (ISO), European Telecommunication Standards Institute (ETSI), and International Telecommunication Union (ITU). For example, PQC might be used to support authentication to reduce the threat of a man-in-the-middle or insider threat attack. (PQC key exchange requires some authentication, too.) Also, a complex trusted node network might take advantage of path diversity to combine keys in a way that diversifies trust.

Most analyses consider only small deployments, and the need to trust intermediary nodes is a frequent complaint. These issues could be reduced substantially in the context of a complex network.

Synergistic Deployment of PQC and QKD

An ideal security strategy would integrate both PQC and QKD to diversify the basis of security and make it harder for attackers to compromise systems. QKD would protect the data against surveillance, regardless of whether the PQC algorithm is later broken with a quantum computer. Hybrid classical-PQC cannot offer such guarantees.

The two technologies can be implemented in parallel or sequentially, depending on the final user's needs. These deployments should be decoupled as much as possible to support flexibility for different use cases.

There are many instances where QKD makes good sense today. For example, organizations that already have a private fiber network may find it easier to migrate to QKD first and then migrate to PQC when they have the resources. Finding ways to use both will ensure organizations have a more flexible set of options in implementing a defense-in-depth approach once Q-day arrives.

Organizations like NIST and the BSI are concerned that enterprises and government agencies will take an either-or approach. They want to ensure that PQC migration has priority. Implementing PQC and QKD can very well be done in parallel.

Crypto agility

As previously mentioned, previous large-scale cryptographic migrations have taken more than a decade. An essential challenge is that cryptographic algorithms are directly baked into application code and hardware security modules. Bryan Sullivan proposed the concept of crypto agility as a way of separating cryptographic primitives in 2009.[15] Various research teams have since explored how this might be applied to software infrastructure more broadly to streamline the transition to PQC.

One promising idea championed by NIST has been taking advantage of a Crypto Agility Maturity Model (CAMM) that is akin to previous software development capability maturity models (CMM).[16] CAMM defines five levels of maturity, where each level contains certain requirements that build on each other. At the bottom, hardware or software limitations may preclude any agility. At the top, organizations can easily migrate to new encryption schemes across all infrastructure and services. The Financial Services Information Sharing and Analysis Center has analyzed how ideas map to financial institutions' processes and technical challenges and defines an approach that works for each organization.[17]

The low-hanging fruit includes updating the cryptographic infrastructure of web browsers and Internet protocols. In these domains, the security community has already developed processes to respond to the discovery of vulnerabilities like the Heartbleed Bug. The vulnerability was discovered in 2014 after many years and necessitated a wide-scale migration to new cryptographic libraries.[18]

This rapid migration was possible because of the centralized control of software like web browsers and the ability to auto-update clients. In contrast, physical equipment, such as the Programmable Logic Controllers (PLC) used in industrial equipment, satellites, planes, trains, and utilities, is much harder to update.

[15] Sullivan, B, "Cryptographic Agility." Accessed: Mar. 12, 2025. [Online]. Available: https://learn.microsoft.com/en-us/archive/msdn-magazine/2009/august/cryptographic-agility
[16] J. Hohm, A. Heinemann, and A. Wiesmaier, "Towards a maturity model for crypto-agility assessment," vol. 13877, 2023, pp. 104–119. doi: 10.1007/978-3-031-30122-3_7.
[17] F.-I. Inc, "Building Cryptographic Agility in the Financial Sector." Accessed: Mar. 07, 2025. [Online]. Available: https://www.fsisac.com/pqc-crypto-agility
[18] "Heartbleed Bug." Accessed: Mar. 13, 2025. [Online]. Available: https://heartbleed.com/

Building cryptographic process digital twins

Transitioning to a secure post-quantum future will require evaluating how enterprises and governments use cryptographic processes today with an eye toward migrating to new algorithms, quantum infrastructure, and crypto agility in the future. NIST has been exploring tools and best practices for assessing the use of cryptographic processes as part of its Migration to PQC roadmap.[19]

NIST's Cryptographic Discovery work is evaluating tools that will allow organizations to check the current state of their cryptographic inventory. It is also assessing how these can improve risk management and prioritize migration efforts. NIST has evaluated at least ten tools in its lab environment and continues to develop best practices for using automated discovery tools. Cryptographic migration digital twins connect to the asset inventory solutions to map the current infrastructure, adding relevant data not shared in the production environment.

There is a more challenging problem for understanding cryptographic processes, owing to various cryptographic system implementations and limited cryptographic process observability tools. More research will be required to identify the appropriate metadata needed to capture and visualize cryptographic processes. These kinds of tools will also need to support continuous monitoring, dependency mapping, critical asset prioritization, governance, automated compatibility checks, and planning capabilities to help organizations improve their crypto agility maturity.

[19] "Migration to Post-Quantum Cryptography | NCCoE." Accessed: Mar. 13, 2025. [Online].
Available: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

Collaborating on quantum resilience

Quantum computer researchers are making great strides in advancing technology to address many sustainability, health, and science challenges. These advances will also result in the first CRQCs that present immense risks to the security and integrity of the digital economy. It may take a few years to a few decades for the first CRQCs to emerge.

Global collaboration is required to protect the confidentiality and integrity of IT and blockchain infrastructure in a quantum safe future. Security standards organizations like NIST and BSI are advocating a focus on PQC. Researchers at TII and other organizations are also exploring how PQC and QKD can co-evolve and be ready when required.

In the meantime, vendors, companies and governments will need to develop better tools to assess their cryptographic infrastructure and start planning for migration to quantum-resistant solutions. This will require working with experts and communities to find better and more secure ways to implement solutions such as PQC and QKD.

Preparing for the Q-day requires going beyond a one-off migration effort. It demands finding ways to support a process of continuous innovation and collaboration to stay ahead of the evolving quantum threat.