NOKIA BELL LABS

The road to quantum-safe networks

White paper

Werner Coomans, Dimitrios Schoinianakis, Richard Sohn, Sylvain Chenard, Aritra Banerjee, and Martin Charbonneau

Increasingly powerful quantum computers make the threat to current cryptographic systems loom large. The timeline for a cryptographically relevant quantum computer (CRQC) is uncertain, but the cybersecurity migration needed to counter this threat is the largest we've ever faced and will take considerable time and effort.

Telecommunication networks, responsible for transporting our data, are a crucial element in this equation. However, there is no one-size-fits-all solution to make a network "quantum-safe". In this paper, we therefore set out to provide some high-level structure and clarification to the quantum migration challenge that network operators are facing. We will address key technical concepts and how they fit the bigger picture of solutions. For example, we will talk about symmetric vs. asymmetric cryptography, post-quantum cryptography, quantum-key distribution, and hybrid solutions. We will also look more closely at the quantum threats and vulnerabilities in current networks, and we will point out the first steps to take and the tools you can use on the way to mitigation. The paper is intended to provide some clarity in the jungle of quantum security technologies and particularly, their impact on telecommunication networks.

Contents

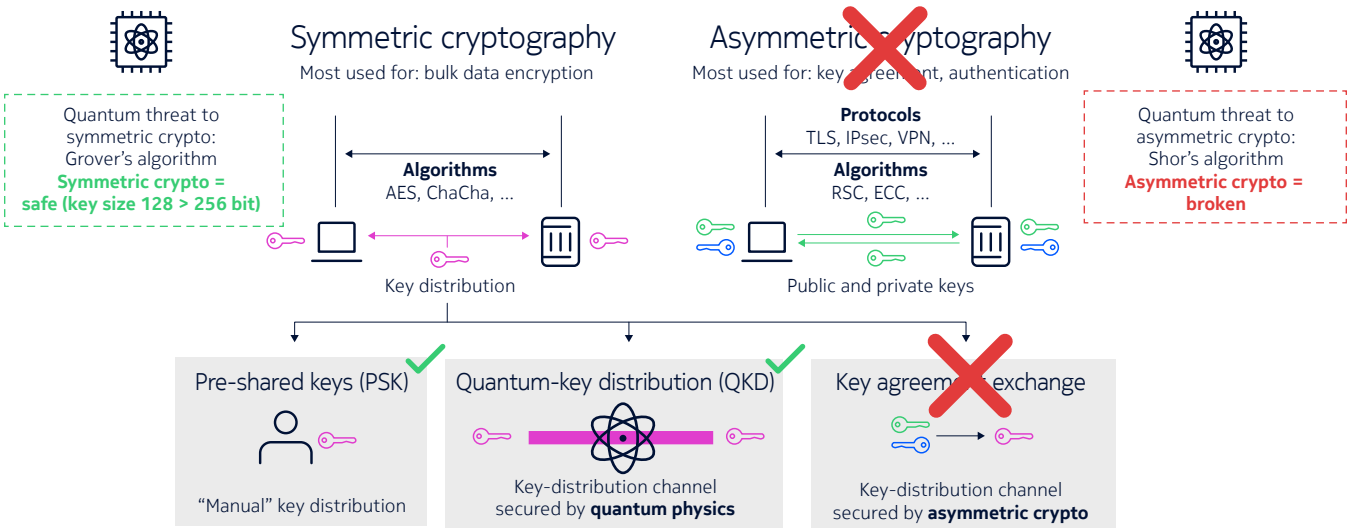
Not all cryptography can be broken by quantum computers

In the 1990s, Nokia Bell Labs researcher Peter Shor invented a new algorithm for prime factorization, specifically designed to run on quantum computers. Using Shor's quantum algorithm, a sufficiently powerful quantum computer would be able to crack encryption algorithms that are widely used today. Recent advancements in quantum computers heighten the threat of a "cryptographically relevant" quantum computer. However, not all cryptographic algorithms are vulnerable to this threat.

There are two types of cryptography (see Figure 1):

- Symmetric cryptography uses the same secret key for both encryption and decryption of the data. This common key needs to be known by both the sender and receiver and therefore relies on a secure way to distribute it to the endpoints.
- Asymmetric cryptography encrypts and decrypts data using different keys. These keys are generated in pairs (a public and a private key), and each side only needs to know the public key of the other party. This is often referred to as "public-key cryptography".

Figure 1: Only asymmetric cryptography (a.k.a. public-key cryptography) can be broken by future quantum computers using Shor's quantum algorithm. Symmetric cryptography, though vulnerable to Grover's quantum algorithm, remains safe



Quantum computers only pose a threat to asymmetric cryptography. Primitive quantum computers have been available for a while, but they are still far from being able to break today's asymmetric ciphers. Although the exact timeline is uncertain, experts envisage a cryptographically relevant quantum computer becoming available within 10–30 years. [1]

1 Global Risk Institute: 2024 Quantum Threat Timeline Report

To address this threat, a new generation of quantum-safe asymmetric cryptography, called post-quantum cryptography (PQC), is being actively researched and developed. The "post-quantum" designation shows that these new algorithms have—so far—been proven to be unhackable, even by a quantum computer. The first versions of such PQC algorithms were standardized in 2024.

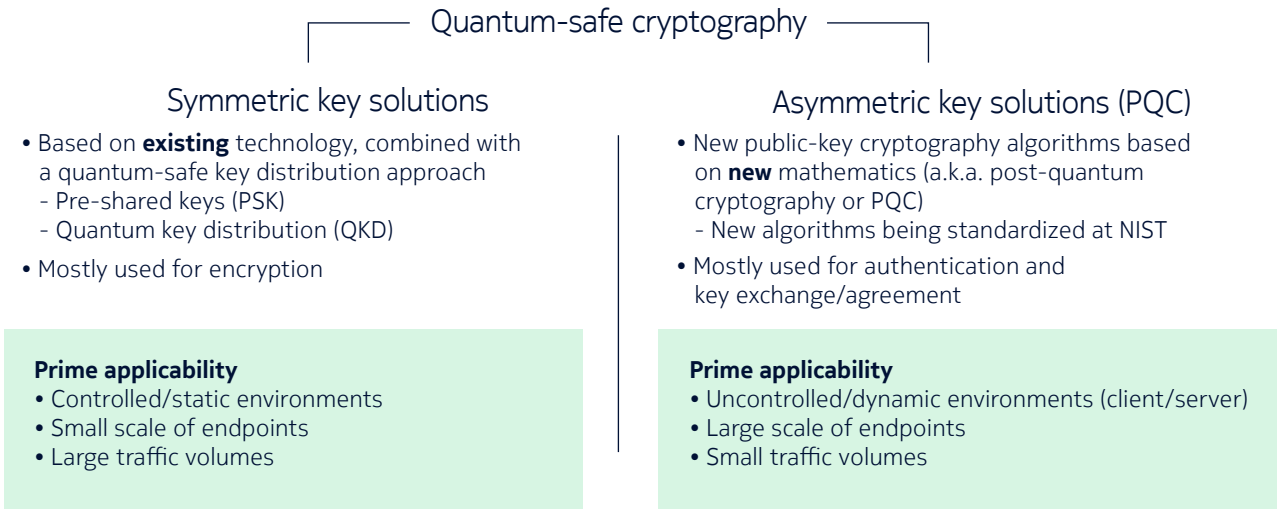
Symmetric cryptography remains safe. Another quantum algorithm created by Shor's contemporary and fellow Nokia Bell Labs researcher, Lov Grover, reduced the time needed to hack symmetric encryption. Despite this, symmetric encryption is believed to be safe when using a sufficiently large key size (minimum 128 bits). [2]

Nevertheless, the most common method to set up a shared secret key in symmetric cryptography is by using asymmetric cryptography. The benefit of this is that the two end-points do not require a secure key infrastructure or any pre-configuration of keys to obtain the symmetric session key. These key-exchange mechanisms, often used for symmetric cryptography, are hence vulnerable to Shor's quantum algorithm. **Therefore, for symmetric cryptography to be fully quantum-safe, its key distribution mechanism also needs to be quantum-safe.**

There's no "one-size-fits-all" solution

Symmetric and asymmetric cryptography are typically used for different purposes today (see Figure 2). Symmetric cryptography is mostly used for the encryption of static connections carrying large volumes of data, owing to the larger computational complexity of asymmetric cryptography. Asymmetric cryptography, on the other hand, is mostly used for authentication and for the exchange of symmetric keys in ephemeral connections between endpoints that are not preconfigured (combining the advantages of symmetric and asymmetric cryptography). Both symmetric and asymmetric cryptography can achieve quantum safety, albeit through distinct methods.

Figure 2: Both symmetric and (new) asymmetric cryptography can be used to obtain quantum-safe cryptography, but each has different prime applicability areas



2 Although the exact key size was subject to debate in the industry, NIST declared a 128-bit key size to be quantum-safe. Some other organizations do recommend using a 256-bit key size for applications with heightened security requirements, like the defense industry.

Quantum-safe symmetric solutions

Quantum-safe symmetric solutions are already commercially available today. Their applicability is in controlled/static environments with a small number of endpoints and a large volume of traffic (e.g., transport network links or enterprise connectivity). Two necessary conditions for making a symmetric encryption scheme "quantum-safe" are:

1. A sufficiently large secret key size (≥128 bits)
2. A quantum-safe approach for establishing this shared secret key.

There are multiple ways to establish a shared secret key in a quantum-safe manner:

- Using pre-shared keys (PSK), relying on a manual provisioning process or automatic centralized symmetric key distribution. The PSK is not necessarily used to encrypt the data itself. Data is often encrypted by another key (the security association key or SAK) that is securely distributed leveraging encryption from a PSK (used as a key encryption key or KEK) over an out-of-band channel.
- Using post-quantum cryptography (PQC)-based Key Encapsulation Mechanisms (KEMs)
- Using quantum-key distribution (QKD), leveraging quantum-physical properties. Two QKD-capable endpoints can establish a common secret key across a dedicated quantum communication channel that is immune to eavesdropping. However, it's important to note that, for now, QKD is a partial solution that needs to be complemented by other methods.

Quantum key distribution: a partial solution

Although sometimes perceived as a complete solution for quantum-safe networking, QKD occupies a specific place in the quantum-safe solution landscape: it is a partial solution for generating a shared secret key for symmetric encryption. QKD also uses an additional classical channel of communication[3] that requires authentication (to ensure information is exchanged with the correct entity on the other side). Authentication on this channel, however, requires to use another cryptographic method such as asymmetric cryptography or preshared keys.

Terrestrial QKD also still faces some practical limitations impeding its adoption. It is severely restricted by distance limitations over terrestrial networks (current operation is limited to ~100 km over optical fiber), and requires special-purpose equipment. Furthermore, it is highly susceptible to denial-of-service attacks, as any manipulation of the quantum states of the transmitted photons destroys the ability to exchange a key over the QKD link.

As a result, the US National Security Agency (NSA) currently recommends against using QKD for securing transmission of data in US national security systems[4] until these limitations are overcome. On the other hand, countries in the European and Asia-Pacific regions are very actively developing and deploying QKD technology[5] and related standards (e.g., in ETSI). Satellite QKD is one avenue that is currently under active exploration. Since Earth-to-satellite attenuation is lower than optical fiber losses,[6] using satellites as intermediate trusted nodes can extend the range of the QKD to thousands of kilometers.

3 In QKD, the classical side channel over which additional information needs to be exchanged (e.g., the measurement basis orientation that was used) needs to be authenticated. Without authentication of the classical channel, QKD is vulnerable to a man-in-the-middle attack.

4 https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

5 China currently operates the largest QKD network, spanning thousands of kilometers, and Europe plans to deploy a QKD network spanning the European continent (EuroQCI).

6 Because atmosphere density rapidly decreases with altitude, the largest part of the light trajectory is through near-vacuum.

Other important aspects for secure symmetric encryption

In addition to the key-distribution mechanism, some other aspects that deserve proper consideration for achieving secure symmetric solutions are:

- Key rotation: periodically refreshing keys limits the volume of data encrypted by a single key, making it harder to hack and limiting the blast radius in the case of successful hacking.
- Key entropy: ensuring sufficient key randomness (entropy) by, e.g., using a physics-based random number generator that never repeats itself. This increases key unpredictability, crucial for countering brute-force and cryptanalytic attacks.
- Separation of duty between the Network Operations Center (NOC) and the Security Operations Center (SOC), with SOCs focusing on cybersecurity and NOCs on network performance. The NOC is responsible for managing the service creation and deletion of connections, while the SOC manages the associated service security policies, which include encryption and policy management. This division improves security and network efficiency, ensuring clear accountability and access control, and reducing operational complexity.

Quantum-safe asymmetric solutions (PQC)

PQC will replace current asymmetric cryptography, which is used in more dynamic and uncontrolled environments with many endpoints. Since asymmetric cryptography is more complex than symmetric cryptography, they are often used together for data encryption. This combines the best of both worlds, establishing the secret key with asymmetric algorithms while doing the encryption with symmetric algorithms.

PQC is based on new mathematical algorithms conjectured to be difficult to solve, even with quantum computers. Those new PQC schemes will be used, for example, for exchanging keys in protocols like Transport Layer Security (TLS), and digital signatures used for authentication, code-signing or message digests (with different uses being addressed by different PQC algorithms).

Standardization landscape

Since 2016, the US National Institute of Standards and Technology (NIST)[7] has been running an open competition and standardization effort for evaluating and selecting PQC algorithms, which do not rely on quantum computing and run on traditional computing platforms. NIST released the first PQC standards in August 2024.[8] NIST has currently standardized three algorithms, one for encryption and two for digital signatures).[9] NIST adopts a comprehensive strategy that defines multiple standards based on different mathematical approaches and provides backup solutions in case one approach proves vulnerable (weakened and/or broken) in the future. More PQC standards from NIST/IETF are expected in the coming years.[10]

We expect the Internet Engineering Task Force (IETF) to complete their first internet protocol standards in 2025, using these new NIST algorithms. After that, other groups that make standards (SDOs) like 3GPP and ITU-T are expected to adopt the recommendations from NIST and IETF when they make changes to network protocol standards. Because NIST's PQC algorithms have significantly larger key and ciphertext sizes than their traditional counterparts, this may require updates to other aspects of network protocols like, e.g., to address potential packet fragmentation issues.

7 National Institute of Standards and Technology, an agency of the United States Department of Commerce

8 https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

9 Encryption algorithm: ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism), digital signature algorithms: ML-DSA (Module-Lattice-Based Digital Signature Algorithm) and SLH-DSA (Stateless Hash-Based Digital Signature Algorithm). An additional DSA algorithm will be standardized soon. See https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

10 NIST recently announced its selection of a fifth algorithm, with a finalized standard expected by 2027 [https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption]

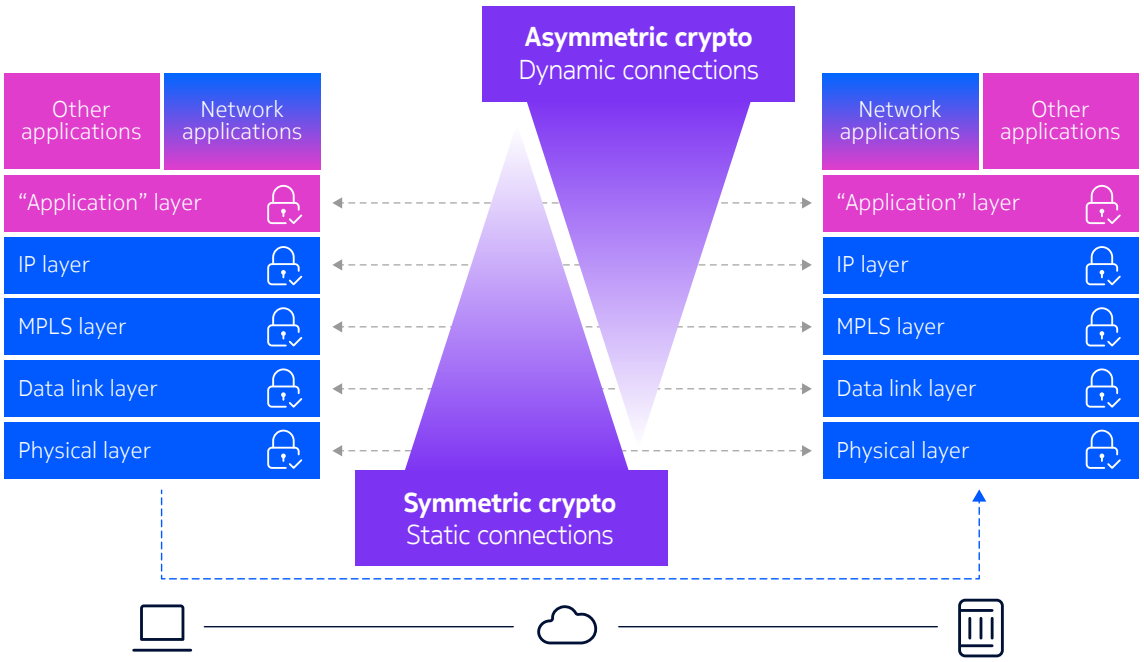
Quantum vulnerability in current telecom networks

In this section, we will take a deeper look at how telco networks operate today and pinpoint their vulnerability to quantum threats. Symmetric and asymmetric cryptography are predominantly used in different layers of the network stack (see Figure 3). Symmetric approaches are often used in the lower layers (e.g., data link and network layers) for encryption over static connections, while asymmetric approaches are more often used in the upper layers (e.g., transport and application layers) to perform key exchange and/or authentication. The telecom application layer hosts a lot of network applications (e.g., underpinning web services, streaming services, voice-over-IP, and mobile core and radio network functionality). Asymmetric cryptography is often used by these network applications to protect transmissions end-to-end, spanning multiple hops across physical networks.

Various parts of the network, therefore, exhibit different quantum vulnerabilities. Protocols currently relying on public-key cryptography (e.g., TLS, SSH, IPsec, and protocols from the JOSE[11] framework) are vulnerable, just like protocols relying on symmetric-key cryptography (e.g., AES, SNOW, ZUC) that use quantum-vulnerable key sizes and key distribution mechanisms.

Telecom networks are composed of multiple security domains, ranging from the data plane (carries user data), the control plane (handles network signaling and controls how user data is forwarded), and the management plane (monitors and configures network resources) to the user equipment itself. The recent addition of exposure interfaces to enable network programmability through APIs adds a new attack surface. We will start by summarizing the cryptography that is currently used in these domains for mobile, fixed and transport networks, and the overall "root of trust" in network equipment.

Figure 3: The lower layers of the network stack predominantly use symmetric cryptography over static connections (e.g., AES), while the upper layers more often use asymmetric cryptography over dynamic connections for key negotiation and/or authentication (e.g., as used in TLS)



11 JavaScript Object Signing and Encryption

Securing an equipment root of trust

To establish trust in network hardware and software, vendors often include certificates and signature-verification capabilities for establishing authenticity. This yields the ability to ensure the product and the software running on it are not tampered with and can also enable secure over-the-air firmware updates through firmware signing. Digital signatures, typically based on quantum-vulnerable algorithms like RSA and ECDSA, are used to securely boot and attest workloads as safe. These signatures can securely be stored in a trusted platform module (TPM) or hardware security module (HSM), functioning as a hardware "root of trust".

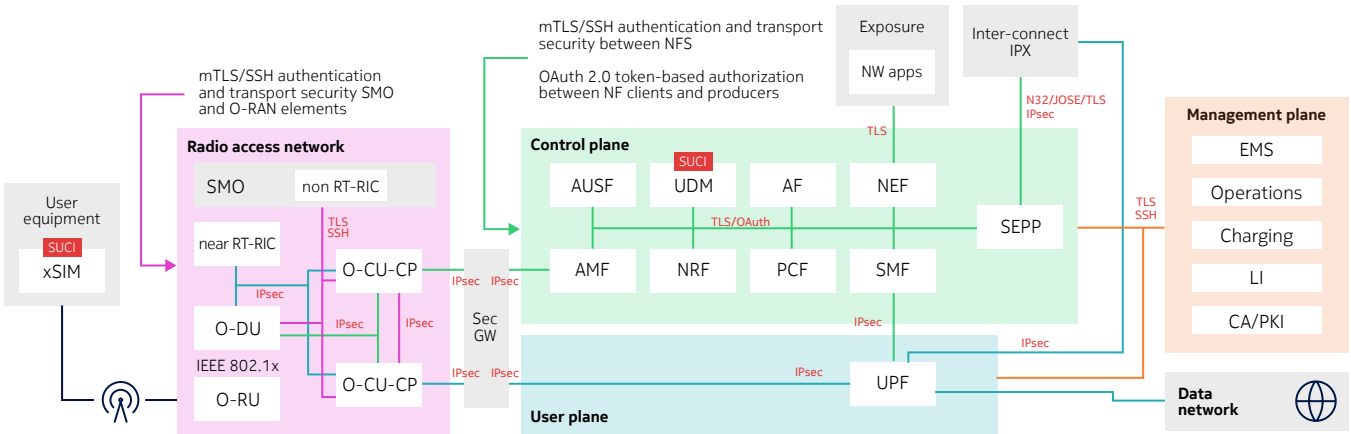
Mobile networks

In mobile networks, the data plane in the radio access network (RAN) uses symmetric encryption (AES, SNOW or ZUC) on Layer 2,[12] using a key derived from a pre-shared key that is programmed into the SIM card and that is also provisioned into the subscriber's account in the control plane. Mobile networks also extensively use IPsec for user-plane connections between the RAN and the 5G core, which often rely on a quantum-vulnerable key-exchange method (IKEv2).

The control plane relies on a range of protocols (on the IP layer and above) that are quantum-vulnerable, such as IPsec, TLS and protocols from the JOSE framework. To provide privacy protection of a subscriber's identity, the subscription identifier is encrypted using quantum-vulnerable public-key cryptography to create the subscription concealed identifier (SUCI), which is used for authentication and authorization when attaching to a mobile network.

The operator-facing management plane[13] uses protocols like TLS and SSH, while network APIs are secured using TLS. Lastly, interconnects between different mobile operator networks go through a security edge protection proxy (SEPP), which also uses TLS and protocols from the JOSE framework.

Figure 4: Overview of quantum-vulnerable interfaces (shown in red) in mobile networks



12 This encryption is on the PDCP layer (a Layer 2 protocol in 4G/5G networks)

13 Including, e.g., element management systems, business support systems, billing and charging functions, certificate managers, identity and authentication managers, and DNS/NTP/PTP servers.

Fixed networks

In passive optical networks (PONs), both the data and control plane in the access network leverage symmetric AES encryption on Layer 2[14] using pre-shared keys on the customer premises equipment (optical network unit or ONU). This encryption only applies to the segment between the ONU and the optical line terminal (OLT), which terminates the PON fiber on the network side. Traffic northbound of the OLT (to the core/aggregation network) and southbound of the ONU (to user devices) is unencrypted on the network layers. Like mobile networks, the management plane and network APIs rely on quantum-vulnerable TLS and SSH protocols.

Transport networks

Transport networks underpin the infrastructure of fixed and mobile networks, providing connectivity on the lower layers (L1-L3). Their data plane typically supports symmetric encryption at the link level, like OTNsec (L1) and MACsec (L2), or across multiple links like, ANYsec[15] (L2.5) or IPsec (L3). For example, edge routers or BNGs (in fixed networks) typically support such encryption capabilities.

The control plane consists of signaling and routing protocols for the IP and optical transport networks (OTNs). Examples include OSPF, IS-IS and BGP protocols for IP as well as GMPLS protocols for OTN. Security mechanisms, for example, used to authenticate messaging to update a router's IP routing tables, typically use pre-shared keying material (i.e., no PKI dependency). Efforts have been made to add PKI-based authentication mechanisms to exterior gateway protocols (e.g., BGPsec), with increasing adoption. The management plane and network APIs, again, often rely on TLS, SSH and SNMPv3 protocols. Depending on its configuration, SNMPv3 can already be considered quantum-safe (supporting PSK-based authentication and AES encryption).

14 This happens at the PON TC layer (equivalent of L2), allowing a 128-bit key size. The encryption is bidirectional except for GPON, where only downstream encryption is defined in ITU-T. AES-256 is supported from 50G-PON onwards.

15 ANYsec is a Nokia-brand name for an encryption algorithm leveraging the MACsec standard (IEEE802.1AE) to encrypt MPLS payloads, while leaving MPLS labels in the clear and unauthenticated.

A quantum-safe network

There is no monolithic or standardized definition of what constitutes a quantum-safe network. For this paper, we define it as the combined use of cryptographic methods to protect the entire network stack from future CRQC threats. Examples of such cryptographic methods are the use of sufficiently large key sizes and secure key distribution for symmetric encryption (e.g., QKD), PQC algorithms for authentication and key exchange. The network stack, on the other hand, covers the entirety of networking functionality, consisting of the data plane, control plane, management plane and exposure interfaces.

It's clear that the importance of having safe and trusted connections will only continue to grow, as our society's reliance on such connectivity is increasing. Consumers, enterprises, mission-critical infrastructure builders and communication service providers all want their digital communication infrastructure and data to remain secure, reliable and trustworthy in the face of this new threat. A quantum-safe network is an outcome to strive for (as opposed to a technology), using agile and resilient approaches across network and application layers. Taking advantage of solutions across multiple layers will allow telcos to adapt to unique business needs, to achieve scale and reduce risk, and to stay ahead of the curve in the face of evolving quantum security risks.

Quantum threats

There are two main types of quantum threats to networks: those targeting data and those targeting the network's functionality. The world today already faces a threat to our data, in the form of harvest-now-decrypt-later (HNDL) attacks. In such attacks, data is collected by adversaries today to be decrypted later, once a CRQC becomes available. This threat is therefore relevant to any data that needs to be kept confidential for a time longer than it would take to create the first CRQC. Countering this threat requires all confidential data traveling through a network to be encrypted in a way that is quantum-safe.

The second quantum threat type targets the network itself, i.e., the control and management plane. Such attacks would aim to alter or disrupt a network's operation or to exfiltrate data from the systems connected to a network, for example, achieving denial of service or acquiring unauthorized access to systems (by hacking traditional public key infrastructures). Addressing this threat requires ensuring that the control plane network protocols, as well as operations and management practices, use quantum-safe authentication and encryption methods.

Elements in the migration journey

Countering the security threat posed by quantum computers amounts to the largest cybersecurity transition in history. Its size and complexity are significantly greater than that of the measures required to address the "Y2K" millennium bug.[16]

In this section we discuss a few crucial elements of this migration journey, such as the role of a cryptographic inventory, hybrid solutions, the use of layering to increase resiliency, and a shift to increasingly agile implementations of cryptographic primitives.

Building a cryptographic inventory

Networks are rarely a homogenous collection of equipment. Networks consist of many distinct types of equipment (from different vendors), and communication often occurs across different management domains (e.g., public cloud). Different network layers use different security protocols (incl. different versions), often supporting multiple options and parameter settings within a single protocol. A first step in a migration towards a quantum-safe network is to increase the visibility of cryptographic assets in use across the network via the creation of a cryptographic inventory to find elements that may require mitigation. Such inventory efforts cover three aspects:

- First, industries governed by the work of SDOs (such as 3GPP and ETSI for telecom) can examine security aspects of standards and create an inventory of those needing remediation to achieve quantum safety, paying particular attention to unique or specialized cryptographic use cases defined in those standards (for example, the SUCI in mobile networks). An SDO may go further and recommend specific solutions to promote industry-wide harmonization.
- Second, software and hardware vendors can examine the cryptographic components contained in their products (and the processes that produce and support them) to create a cryptographic bill of materials (CBoM). The CBoM contains information on available algorithms, protocols, libraries and software components, aiding in understanding their readiness to support quantum-safe networks. A CBoM can be used in discussions with suppliers and with customers for collaborative planning.
- Third, an operational (or runtime) inventory based on network scanning tools shows whether quantum-safe methods are effectively being used within a network. The operational cryptographic inventory shows policy non-compliance that may result from interoperability issues, misconfiguration, stale crypto materials (e.g., keys or certificates) and provides actionable input to mitigation strategies. Such an operational inventory fosters transparency (e.g., toward regulators).

Going forward, increased adoption of cryptographic agility capabilities (see the end of this section) will further increase the value of using automated tools to keep CBoMs up to date. Use of CBoMs improves overall security hygiene, aside from their value in managing the migration to quantum-safe networks.

16 https://www.weforum.org/stories/2023/10/y2q-cybersecurity-cyberattack-quantum-computing/

Hybrid solutions

History shows that cybersecurity migrations take time. Migrations of single algorithms (e.g., replacing deprecated algorithms like MD5, DES/3DES, or SHA-1 by more secure alternatives) all required decades to complete. A full transition to PQC will take at least 10–15 years.[17] It is therefore unavoidable that networks will initially contain a mix of cryptographic methods, some of which have already been migrated to PQC, while others have not. It is important to ensure interoperability between these components during this transition period.

At the same time, new PQC algorithms from NIST have not yet been exposed to the same amount of scrutiny from the cryptographic community as older cryptographic algorithms. It is possible that these new PQC algorithms from NIST could potentially hold (as-of-yet unknown) algorithmic weaknesses making them vulnerable to attack by classical computers. A case in point is the SIKE algorithm. After it had successfully made it to the fourth and final round of the NIST PQC competition, it was hacked by Belgian researchers[18] with a regular computer. Besides the algorithm itself, its flawed implementation can also introduce vulnerabilities. This was the case for the "KyberSlash" timing attack, to which multiple implementations of Kyber (an earlier version of NIST's ML-KEM) were vulnerable.[19]

Hybrid solutions[20] that combine quantum-safe cryptography with legacy cryptography are, therefore, useful both to act as a safeguard and to facilitate interoperability. There are many ways to construct such hybrid solutions (also called post-quantum traditional or PQ/T hybrid schemes). We explain two types of hybrid solutions being considered in the industry (see Figure 5):

- **Key mixing:** A single hybrid key is generated based on inputs from multiple sources. One example is RFC8784, that makes IKEv2 (a widely used key-management protocol for IPsec) quantum-safe. RFC8784 combines[21] the current (quantum-vulnerable) key with a pre-shared key to generate a "mixed" encryption key that is quantum safe. Other examples using a conceptually similar approach are RFC9370 (also applicable to IKEv2 and combining sequentially obtained outputs of a legacy asymmetric and a PQC-based key exchange) and the hybrid key exchange mechanism in TLS1.3 (using secret key concatenation).
- **Dual signing of certificates:** A PKI certificate is signed twice, once using a legacy asymmetric algorithm and once using a PQC algorithm. The verifier only accepts the message if both signatures are valid. This has not deployed yet, as creating post-quantum certificates still faces some obstacles such as upgrading the hardware security modules (HSMs) used by certification authorities to sign certificates.

The other side of the coin is that, when compared to "pure" quantum-safe solutions, hybrid solutions may introduce added complexity and communication overhead. However, recent studies have shown that hybrid solutions, for example, hybrid PQC schemes as used in TLS1.3, perform quite well and observed performance bottlenecks are due to the classic cryptography rather than the new PQC algorithms.[22]

17 According to PQSecure

18 W. Castryck, T. Decru (2023), "An Efficient Key Recovery Attack on SIDH", In Proceedings of: Advances in Cryptology – EUROCRYPT 2023. https://doi.org/10.1007/978-3-031-30589-4_15

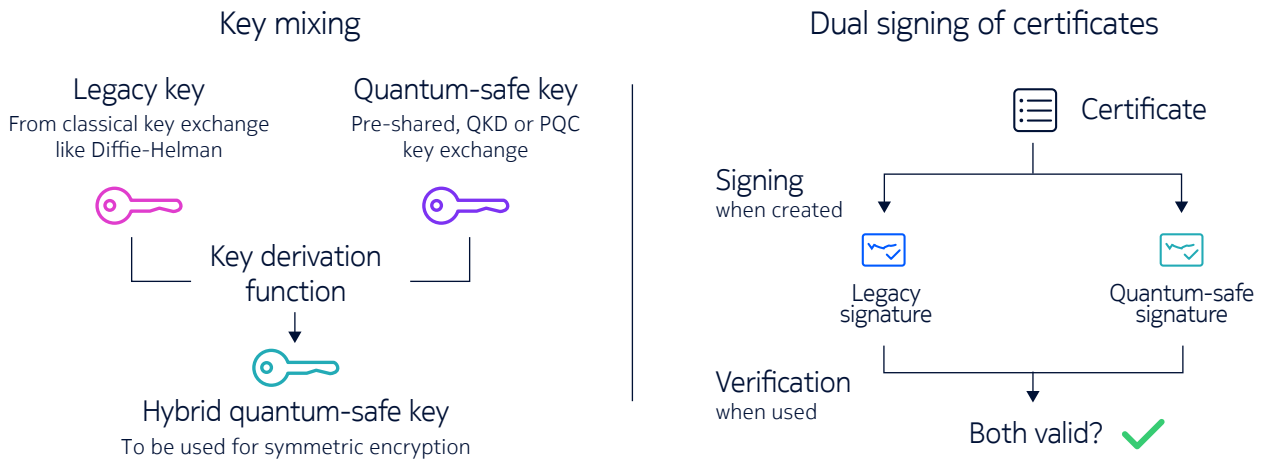
19 https://blog.cloudflare.com/fr-fr/pq-2024/

20 In cryptography, "hybrid cryptosystems" can also refer to cryptosystems combining asymmetric with symmetric cryptography. In this paper, "hybrid" refers to cryptosystems combining quantum-safe with legacy (non-quantum-safe) cryptography.

21 Using a key derivation function.

22 M. Sosnowski et al., "The Performance of Post-Quantum TLS 1.3," in Companion of the 19th International Conference on emerging Networking EXperiments and Technologies, Paris France: ACM, Dec. 2023, pp. 19–27.

Figure 5: Two examples of post-quantum/traditional hybrid schemes: key-mixing (for obtaining a quantum-safe secret key in symmetric encryption), and dual-signing (e.g., for PKI-based authentication)



Quantum resiliency through layering

A well-known security concept to increase resiliency and agility is layering or defense-in-depth. Using multiple layers of encryption, each leveraging a different encryption mechanism, avoids a single point of failure. A resilient quantum-safe network should also employ different layers of encryption, each based on different quantum-safe algorithmic primitives. A powerful example for achieving quantum resiliency involves combining application-layer cryptography (mostly using PQC algorithms) with additional layers of network-layer cryptography that use a different cryptographic primitive (symmetric-key encryption). These added layers are also resistant to quantum attacks but use a different cryptographic primitive. This is particularly important given the uncertainty surrounding the security of new PQC algorithms.

Applications requiring data privacy can, hence, use their own application-layer key negotiation and encryption methods. Service providers and enterprises would add complementary quantum-safe network-connectivity layers, using different cryptographic methods like centralized symmetric key distribution and/or QKD paired with block-cipher encryption. The relationship between network-layer cryptography and application-layer cryptography is complementary, boosting the overall resiliency of the data in transit, while each layer retains its independence. Network-layer protection furthermore adds benefits in terms of scale and applicability of quantum-safe encryption to all data in transit.

Cryptographic agility

Hybrid or layered solutions provide a fallback solution in case one of the crypto algorithms is broken. But a broken algorithm requires fixing. Implementations of cryptographic algorithms should therefore become increasingly agile, i.e., able to accommodate new or updated algorithms without introducing major service disruptions (e.g., hardware swaps). This will ensure PQC-algorithm implementations can be quickly updated if proven to be cryptanalytically weak. Possible updates could range from tweaking the algorithm parameters to fully replacing the algorithm.

Using multi-layered quantum-safe protection allows one to rely on the protection provided by the network layer while updating a weakened or broken application-layer PQC algorithm. This effectively provides a network shielding effect that continuously ensures in-flight data confidentiality.

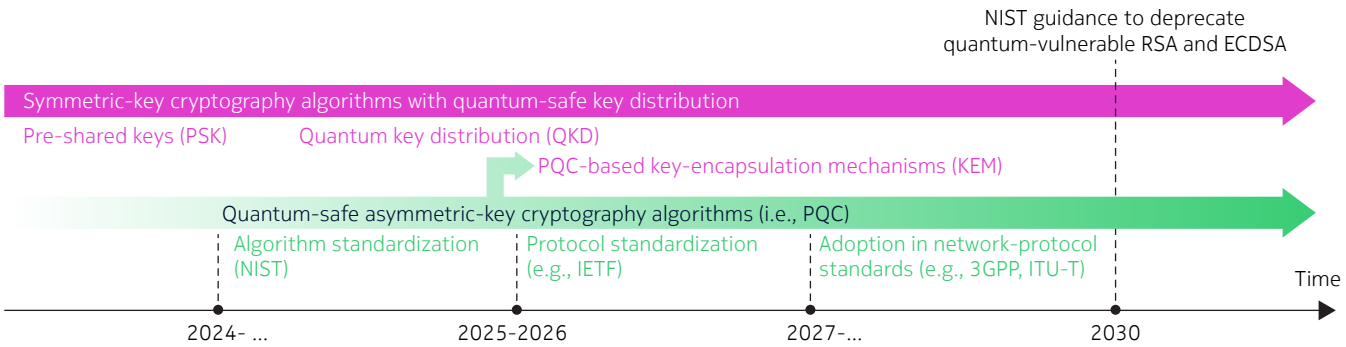
Toward a quantum-safe network

In this section, we put forward some dimensions clarifying how and what to prioritize in the face of quantum threats.

Technology availability and quantum threats

Symmetric-key based solutions using sufficiently long key sizes and high-quality key sources are quantum safe, and they are commercially available today. To establish the shared secret key, they need to rely on a quantum-safe key distribution mechanism, using either pre-shared keys (mature), quantum key distribution (maturing), or quantum-safe asymmetric protocols (maturing). Quantum-safe asymmetric algorithms (i.e., PQC algorithms) have only just been standardized by NIST, so adoption in security protocols is ongoing (e.g., at IETF). Adoption in network protocol standards (e.g., 3GPP, ITU-T) that rely on these security protocols will soon follow but will take additional time.

Figure 6: The availability of quantum-safe security solutions will increase over time



As discussed previously, we already face one quantum threat today: HNDL attacks. Countering this threat requires protecting both stored and in-flight data. Therefore, addressing this threat from a network perspective requires focus on the data plane, making harvesting of in-flight data useless. A fully quantum-resilient network, on the other hand, also requires addressing the security schemes used in the management and the control-signaling planes so that the operation of the network is safeguarded. The priority and timeline for addressing the data plane, management plane, control plane and exposure interfaces may vary according to the risks an operator may wish to mitigate. Operators in the business of selling secure network connectivity services might focus on the data plane first. Interfaces toward the management plane may also rate a higher priority. They are more exposed because they include network and security management systems (incl. regulatory compliance dependencies), and the management plane also has a weaker dependency on standardization (common management-plane protocols like TLS and SSH depend just on the IETF). The recent Salt Typhoon attack is a prime example of an attack on management plane functionality. It successfully targeted lawful intercept (LI) functionality, which is a separate system connecting to the control and data plane to collect traffic.

For the management plane and network exposure interfaces, all types of networks—mobile, fixed and transport—rely heavily on TLS and SSH protocols. These links, which often directly interface with IT environments, will all need to migrate to quantum-safe TLS and SSH versions. CBoMs can be especially useful for such interfaces to IT environments (which might already be more advanced in terms of PQC adoption), and to facilitate interoperability between systems of different vendors. Other aspects will be separately discussed below for the different segments.

Securing an equipment root of trust

Given that network hardware lifetimes easily exceed a decade, it is important to ensure its secure boot functionality is still safe during that time, i.e., quantum safe. TPMs, used to securely store signatures, must be able to execute the appropriate PQC digital signature algorithms. Similarly, hardware security modules (HSMs) must be upgraded to protect quantum-safe keys (new algorithms and resulting key sizes).

For completeness, NIST does currently recommend using stateful hash-based signature (HBS) schemes for applications with a long lifetime, and for which it is not practical to transition to a PQC digital signature scheme once deployed (e.g., authentication of firmware updates for constrained devices). These schemes are considered quantum-safe but rely on a large set of one-time signature (OTS) private keys, which require extreme care to ensure that no OTS key is ever reused.

Mobile access networks

Mobile networks internally have a strong reliance on public key infrastructure (see Mobile networks on p. 8). Adoption of quantum-safe primitives in the data plane of mobile networks will leverage 3GPP's inclusion of PQC algorithms in future releases. 3GPP Rel-19 strengthens symmetric-key algorithms (AES, SNOW, ZUC) by adding support for 256-bit key sizes for the connection between the UE and the RAN. With regard to the control plane, the adoption of NIST PQC algorithms in 3GPP network protocols using protocols based on asymmetric cryptography (e.g., TLS, IPsec) is planned for 3GPP Rel-20 and Rel-21. In other words, 5G will become quantum-safe in upcoming 3GPP releases, while 6G is targeted to be quantum safe from the start.

Operators will need to evaluate the migration needs of 3G, 4G/LTE and IMS networks, which also make use of TLS, IPsec and JOSE. While telecom-specific interfaces in such networks may be unlikely to see standard updates, it is possible that some upgrades may be needed (e.g., to TLS1.3) to support compatibility with far-end systems and to satisfy regulatory mandates.

Fixed access networks

The last-mile connection over PON is protected by symmetric AES encryption covering both the data plane and the control plane. In GPON, however, only the downstream traffic is encrypted. This encryption already supports quantum-safe 128-bit key sizes, and the latest ITU PON standard (G.hsp) allows support for up to 256-bit keys. Although secure key-exchange and authentication mechanisms are defined in standards (e.g., based on secret PSK), their adoption varies. As this encryption only applies to the ONU-OLT link, aggregation networks between the OLT and BNG/edge router should also adopt network-layer encryption (e.g., MACsec, ANYsec) to ensure end-to-end network encryption of the data plane.

Transport networks

In transport networks, quantum-safe solutions are already available to protect the data plane with symmetric cryptography using sufficiently large key sizes. These can be used in data-center interconnectivity, backhaul of fixed- and mobile-network traffic in more central parts of the network (including mm-wave mobile backhaul), and even last-mile applications for government, using dedicated equipment on customer premises. All network segments relying on transport functionality (e.g., aggregation network) can, in principle, benefit from these same symmetric quantum-safe data-plane mechanisms, except for the last-mile connectivity provided by the access network technology (mobile or fixed). IPsec connections can already be made quantum safe by using a quantum-safe IKEv2 (e.g., RFC8784 or RFC9370) leveraging a hybrid scheme. In the control plane, interior gateway routing protocols (OSPF, IS-IS) can be configured to use quantum-safe authentication mechanisms based on preshared material. The exterior gateway protocol BGPsec, on the other hand, introduced a public key infrastructure called Resource PKI or RPKI. The digital signature algorithms used there would need to migrate to quantum-secure algorithms to face off quantum attacks.

Conclusion

In conclusion, the transition to quantum-safe networks is a complex and multifaceted challenge that requires a comprehensive approach. Although the exact timeline is uncertain, as quantum computers become increasingly powerful, the threat to current cryptographic systems grows. The required migration amounts to the largest cybersecurity transition in history, which will take considerable time and effort. It involves the development and deployment of new cryptographic algorithms, protocols and technologies and necessitates changes to network architectures, operational practices and security policies. It is, therefore, essential to start the migration to quantum-safe solutions today.

There is no one-size-fits-all solution to ensure the quantum safety of a network. Whereas solutions relying on asymmetric cryptography (e.g., RSA, ECDH) require migration to new PQC algorithms, symmetric cryptography (e.g., AES) can already be quantum safe today when combining large key sizes with a quantum-safe key distribution mechanism. QKD is just one potential avenue to achieve this. But the use of different security protocols and cryptographic primitives by different layers in the network stack also carries the potential for a resilient multi-layered approach to achieve quantum-safe networks.

This transition also presents an opportunity to set up a new level of best practices for security, ensuring that networks are not only quantum safe but also more resilient and adaptable to future threats. To accomplish this, it is crucial to:

1. Develop and deploy quantum-safe cryptographic algorithms and protocols
2. Create and maintain a cryptographic inventory to track and manage cryptographic assets
3. Implement hybrid solutions that combine quantum-safe cryptography with legacy cryptography
4. Use layering and defense-in-depth approaches to increase resiliency
5. Foster cryptographic agility, enabling quick updates and replacements of cryptographic algorithms
6. Ensure the security of the entire network stack, including the data plane, control plane and management plane.

By taking a proactive and comprehensive approach to quantum-safe networking, we can ensure the long-term security and integrity of our networks, protecting the confidentiality, integrity and authenticity of data in the face of emerging quantum threats.

Abbreviations

CBoM	Cryptographic bill of materials
CIP	Critical information protection
CPE	Customer premises equipment
CRQC	Cryptographically relevant quantum computer
CSP	Communication service provider
DSA	Digital signature algorithm
HBS	Hash-based signatures
ICT	Information and communication technology
NSA	National Security Agency
PoC	Proof-of-concept
PON	Passive optical network
PQC	Post-quantum cryptography
PSK	Pre-shared keys
QC	Quantum computer
QKD	Quantum key distribution
QS	Quantum-safe
QSN	Quantum-safe network
RAN	Radio access network
SaaS	Software as a service
SDO	Standards developing organization
SUCI	Subscription concealed identifier

Further reading

1. NIST public draft on “Transition to Post-Quantum Cryptography Standards.” Online: https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf
2. GSMA list of government initiatives on quantum-safe networks. Online: https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region
3. Quantum Threat Timeline Report 2024 by Global Risk Institute (expert survey on the anticipated timeline to realize a CRQC). Online: https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report
4. IETF RFC draft “Post-Quantum Cryptography for Engineers.” Online: https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-engineers
5. Cloudflare blog on post-quantum cryptography digital signature algorithms. Online: https://blog.cloudflare.com/another-look-at-pq-signatures
6. TNO, The PQC Migration Handbook. Online: https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf
7. OWASP Foundation, CycloneDX, Authoritative Guide to cryptographic bill of materials (CBoM). Online: https://cyclonedx.org/guides/OWASP_CycloneDX-Authoritative-Guide-to-CBOM-en.pdf

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs, which is celebrating 100 years of innovation.

With truly open architectures that seamlessly integrate into any ecosystem, our high-performance networks create new opportunities for monetization and scale. Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID214685 (April)