POST-QUANTUM SECURITY FOR 6G – OPPORTUNITIES AND CHALLENGES

Thomas Zasowski

ABSTRACT

Quantum computers have made huge progress in recent years. In this tutorial paper, we explain why they pose a threat to encryption methods that are used in today's communication networks. As there is the unique opportunity of 6G becoming the first cellular standard where post-quantum security could be considered from the very beginning, we present approaches to achieve post-quantum secure communications. Benefits and drawbacks of quantum key distribution (QKD) and post-quantum cryptography (PQC) are compared. Suggestions are made on how these approaches can be considered resulting in a post-quantum-safe 6G standard.

INTRODUCTION

The development of quantum computers has made significant progress in recent years, with steady increases in the number of qubits and advancements in qubit stability. The primary purpose of quantum computers is to process extremely complex problems, such as molecular simulations, which would take centuries to solve using classical computers. As many encryption algorithms also rely on very complex mathematical problems, some of these algorithms will be broken when quantum computers become powerful enough. 6G now offers a unique opportunity to consider mitigation measures already in the standardization phase instead of a complex and time-consuming upgrade of security mechanisms, which needs to be implemented into already existing networks.

QUANTUM COMPUTERS MADE HUGE PROGRESS OVER RECENT DECADES

QUBIT SCALING AND ERROR CORRECTION

Significant progress has been made in the development of quantum computers over the last decades. In 1998, IBM and a few universities demonstrated a quantum computer with 2 qubits. 25 years later, IBM announced a quantum computer with 1121 qubits.

However, the number of qubits is only one measure of improving the performance of quantum computers. As qubits are prone to errors, reducing error rates and improving error correction are equally important. Due to this reason and its better scalability, for instance IBM decided to shift further development activities to a 133-qubit system in 2023.

PHYSICAL VS. LOGICAL QUBITS

The previously mentioned qubit numbers refer to physical qubits. Physical qubits are prone to errors due to unstable states. Hence, tens to thousands of physical qubits are combined into one logical qubit, while researchers investigate solutions for more efficient quantum error correction to reduce the number of required physical qubits per logical qubit. For instance, in 2024, Google announced Willow, a quantum system with 105 physical qubits which features extraordinary quantum error correction capabilities. Still, 97 physical qubits out of the 105 are needed for 1 logical qubit to achieve a relatively low error rate.

At the end of 2024, Quantinuum announced the availability of a quantum computer with 50 logical qubits. For comparison, about 40 logical qubits can be simulated on high performance computers currently.

SEVERAL BENEFICIAL USE CASES ...

With this number of qubits, certain optimization problems can be solved, already, such as the optimal distribution of cargo in airplanes or optimal placement of air-conditioning and heating ducts in buildings. To enable more impactful business applications, such as medical drug discovery, quantum computers with millions or even hundreds of millions of logical qubits are required.

... AND A SUBSTANTIAL THREAT

However, quantum computers cannot only be used for solving difficult optimization problems or

Digital Object Identifier: 10.1109/MCOMSTD.XXXX.XXXXXX
Date of Current Version: XX XXXX XXXX
Date of Publication: XX XXXX XXXX

Thomas Zasowski is with Swisscom, CH-3050 Bern, Switzerland (email: thomas.zasowski@swisscom.com)

2471-2825 © XXXX IEEE. Applicable copyright

This article has been accepted for publication in IEEE Communications Standards Magazine. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MCOMSTD.2026.3697812

simulations that are out of reach for computation by classical computers. There is also the threat of many of today's encryption methods becoming insecure once powerful quantum computers, also referred to as cryptographically relevant quantum computers (CRQC), become available.

Still a Way to Go

As of 2026, quantum computing is still in its infancy. It can be compared to the early days of classical computing, where computers filled entire rooms while not being very powerful. Just as the numbers of transistors in classical computers steadily increased, also quantum computers are expected to continuously improve. However, it is very difficult to predict when quantum computers will be powerful enough to break today's encryption methods.

Why are Quantum Computers a Threat to Certain Today's Encryption Methods?

Many of today's encryption methods are based either on asymmetric cryptography or on symmetric cryptography.

For asymmetric cryptography, two different keys, a public and a private one, are used for encryption and decryption. In the example shown in Figure 1, Alice uses Bob's public key to encrypt the data. Only Bob can decrypt the data using his private key. In contrast, with symmetric cryptography, Alice and Bob use the same key for encryption and decryption. However, they must exchange this key beforehand in a way that nobody but them has access to the key.

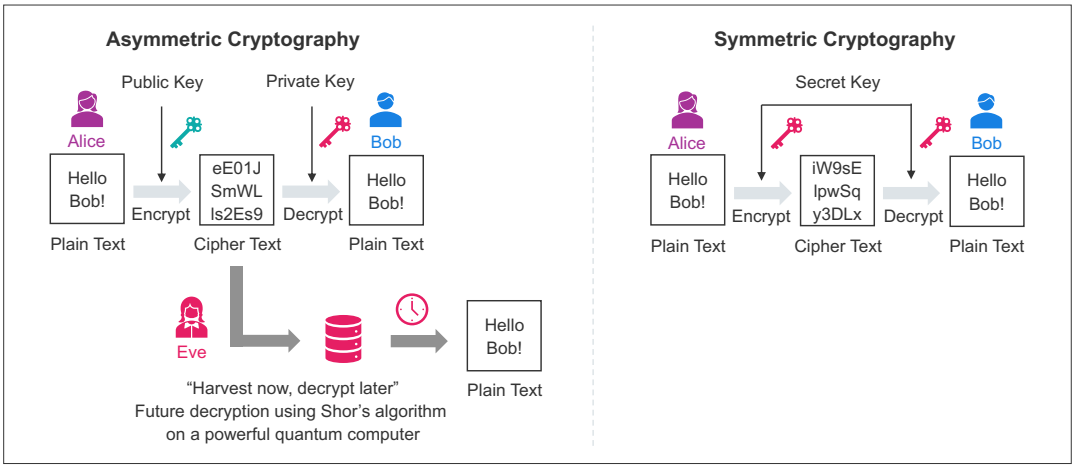

FIGURE 1. While asymmetric encryption can be broken by Shor's algorithm, symmetric encryption is considered as quantum-resistant

Asymmetric encryption algorithms, such as RSA, often rely on a relatively easy mathematical operation whose reverse operation, e.g. deriving the two prime numbers from their product, is extremely difficult and time-consuming with classical computers. In 1994, the Shor algorithm [1] was presented to factor large numbers into their prime factors on quantum computers within a short time, making such algorithms insecure. Applying the discrete logarithm algorithm from the same publication, elliptic curve cryptography (ECC) can be easily broken as well. Hence, many existing asymmetric encryption algorithms become obsolete with the presence of CRQC.

The exact number of qubits required to break asymmetric encryption depends on encryption algorithm, key length and specific realization of Shor's algorithm. For instance, researchers presented an approach for RSA 2048 that requires 20 million physical qubits to break this algorithm within 8 hours [2]. Assuming 100 physical qubits per logical qubit, this would correspond to 200'000 logical qubits. Recent work suggests that, under specific assumptions, RSA-2048 factoring may be achievable with only 1,730 logical qubits [3], highlighting the sensitivity of resource estimates to algorithmic and hardware models.

Why is it a Problem if Quantum Computers are not powerful enough Today?

Although quantum computers are not yet powerful enough to decrypt current encryption methods, attackers may store encrypted data deserving special protection, such as medical, banking or military data, and decrypt it as soon as CRQC will be

This article has been accepted for publication in IEEE Communications Standards Magazine. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MCOMSTD.2026.3697812

available as depicted in Figure 1. This attack is known as “harvest now, decrypt later” or “store now, decrypt later”.

How much time to act?

The latest point in time to take counteractions has been defined by the “Mosca Inequality” [4]. If the time required to implement a quantum-safe solution (known as "migration time") and the duration needed to secure data (termed as "shelf-life time") exceed the estimated emergence of CRQC (defined as "quantum threat time"), it is possible that the crucial date to act may already have passed as shown in Fig. 2. In the provided example, the combined migration time of 5 years and data shelf-life of 10 years exceed the assumed quantum threat time of 12 years. This results in a 3-year exposure window during which legacy data may be vulnerable to quantum-enabled decryption.

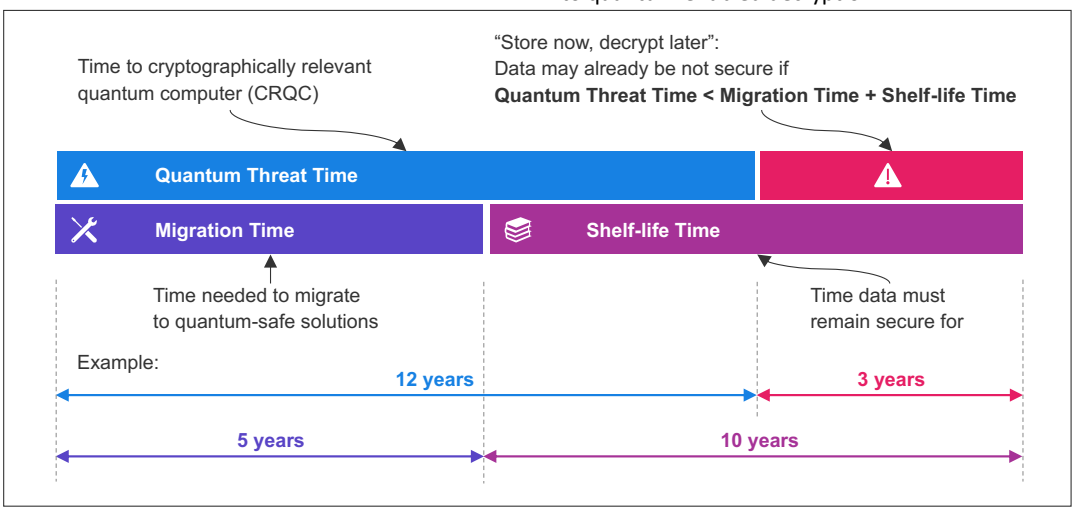

FIGURE 2. The «Mosca Inequality»

The “shelf-life time” is often given by regulatory or other legal requirements and hence cannot be changed in such cases. The “quantum threat time” is determined by the quantum computing development efforts. Even experts do not agree on a specific date, yet when CRQC will be available. In a survey from 2024 [5], about 60% of the experts assume that CRQC will be present in 2038 with a likelihood of more than 50% (see Figure 3).

Probably the Right Point in Time to Check for Criticality of Data and Systems

Only the “migration time” can be optimized individually in the given inequality. Hence it might be worth considering strategies to reduce the “migration time” as many organizations likely envision practical difficulties in shortening the migration time. One common approach is called Crypto Agility. Crypto Agility refers to the ability to quickly migrate to another cryptographic algorithm without requiring costly and time-consuming changes to the remaining infrastructure.

As CRQC may be available in 15 to 20 years and as there exist data with a “Shelf-life Time” of 10 years (e.g. medical or tax records), it seems to be the right point in time to consider the move towards Crypto Agility. Crypto Agility should also be considered as key element in the 6G standardization as more powerful quantum computers or new attacks may require a swift exchange of encryption algorithms in future.

Are we doomed? No secrets anymore?

Unlike asymmetric encryption, symmetric encryption like AES is assumed to be secure even in the presence of CRQC if the keys are sufficiently long. In 1996, Grover’s algorithm [6] was presented that reduces the effort to find the correct symmetric key. Instead of O(N) checks for a key length N, only O(√N) checks are required. Hence, the implications of Grover’s algorithm can be mitigated by simply doubling the key size. However, the challenge of symmetric encryption lies in the efficient and secure distribution of the keys. Apart from key exchange via courier, which doesn’t scale, Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) are the two main approaches for this task.

This article has been accepted for publication in IEEE Communications Standards Magazine. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MCOMSTD.2026.3697812

Quantum Key Distribution (QKD) for Key Exchange

While the theoretical foundations of Quantum Key Distribution (QKD) have existed for decades, a distinction must be made between academic protocols and industrial standards. Currently, there is no single international standard that defines the physical layer. Instead, standardization bodies have focused on the architectural framework and the interfaces required to integrate QKD into classical telecommunications stacks. Unlike classical key-agreement schemes, QKD is technically a key-growing protocol. An initial shared authentication key secures the classical channel. From this seed, QKD generates fresh keys whose secrecy is information-theoretic and independent of previous rounds.

QKD relies on quantum physical effects, usually the polarization properties of photons, to distribute encryption keys securely between two end points. Hence for transmission either a fiber or a wireless optical link is required. While multiple photons might be used in continuous variable QKD (CV-QKD), only pulses containing a single photon are used in discrete variable QKD (DV-QKD). This limits the range of use in mobile networks. Standard end user equipment as e.g. mobile phones cannot be equipped with QKD. However, due to the substantial capacity increase with 6G, it can be assumed that base stations and the mobile core network must be connected via fiber, making QKD a viable option for encryption in these parts of the network.

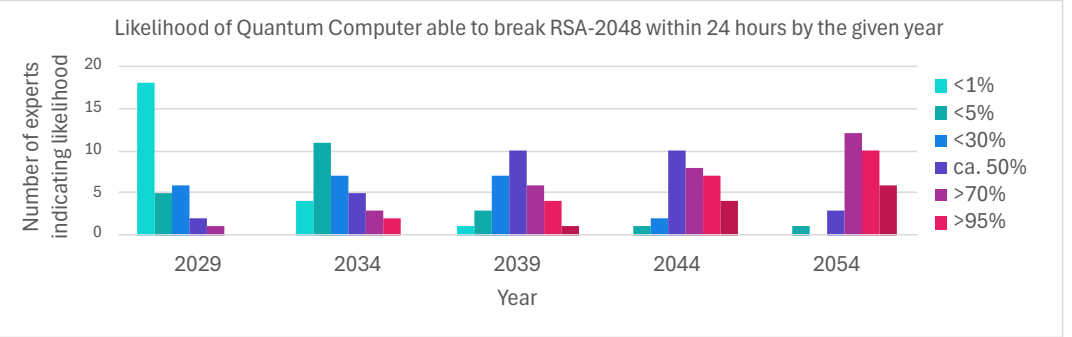

FIGURE 3. Experts' estimates on the availability of CRQC from Quantum Threat Timeline Report 2024

There exist different approaches to realize QKD systems. Let's assume for the simplified explanations of the different QKD protocols below that Alice wants to exchange a symmetric key with Bob as depicted in Figure 4, while Eve is an attacker trying to eavesdrop the key.

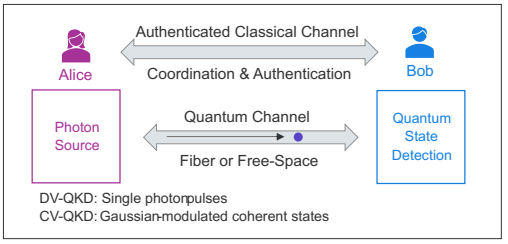

FIGURE 4. QKD setup with quantum channel and authenticated classical channel

Discrete Variable Quantum Key Distribution (DV-QKD) on basis of BB84 [7]

Applying DV-QKD, Alice randomly sends pulses containing a single photon either using a polarization filter with basis "rectilinear" or "diagonal" via a fiber. Bob randomly selects a receive filter either using basis "rectilinear" or "diagonal".

A classical authenticated channel is required for basis reconciliation and post-processing. After comparing their bases over this classical channel, Alice and Bob discard the transmitted bits with different bases and thus obtain a shared key based on the remaining ones as shown in Figure 5.

This article has been accepted for publication in IEEE Communications Standards Magazine. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MCOMSTD.2026.3697812

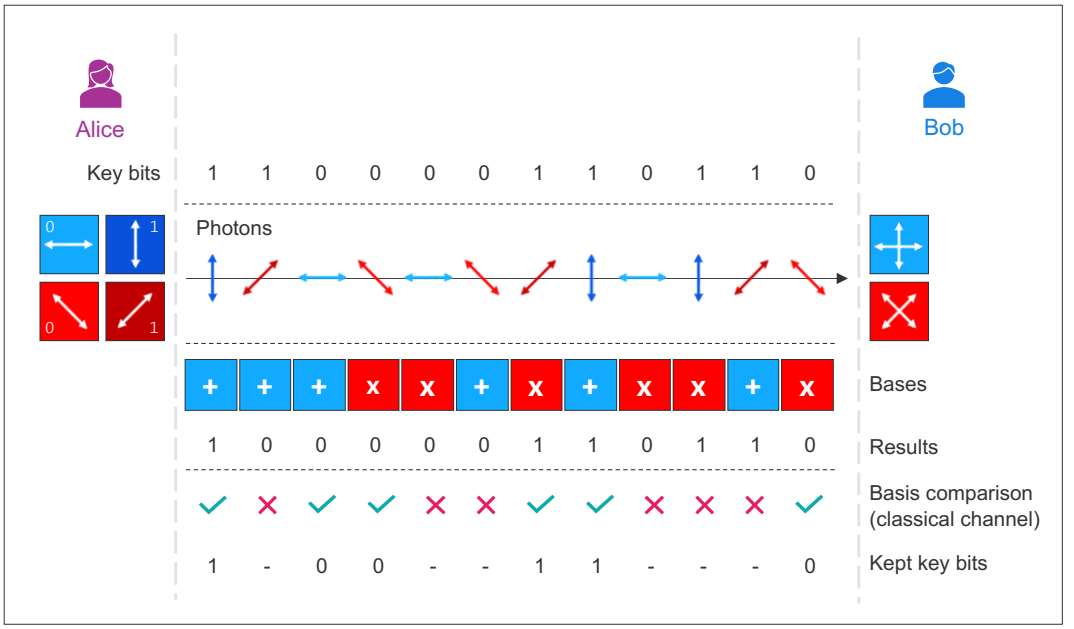

FIGURE 5. Schematic illustration of BB84 key derivation

This single-photon requirement gives security but limits the maximum distance between Alice and Bob. The distance is limited by fiber attenuation and detector inefficiency. Due to the no-cloning theorem, standard optical amplifiers cannot be used to mitigate this as it is done in classical optical communications. Instead, quantum repeaters are needed to extend the reach.

If Eve tries to measure the state sent in the photon not knowing the original basis to encode the qubit, she will fail half of the time. According to the measurement postulate of quantum mechanics, each incorrect measurement irreversibly disturbs the quantum state, introducing detectable errors in the correlations between Alice and Bob. By comparing a random subset of their data, Alice and Bob can estimate this error rate and thus determine whether the quantum channel has been compromised. The no-cloning theorem further guarantees that Eve cannot make perfect copies of the transmitted states to measure later once the encoding bases are revealed. Consequently, while eavesdropping attempts can disrupt the key exchange, they cannot yield the secret key without being detected.

Entangled Quantum Key Distribution (eQKD) on basis of E91 [8]

With eQKD, two entangled photons are sent from a photon source to Alice and Bob. Due to the entanglement of the two photons, as soon as the state of one photon is measured, the state of the other photon is known. For instance, if Alice measures a photon with polarization “horizontal”, she knows that Bob’s photon has the polarization “vertical”. Hence, if Alice and Bob use the same basis, they know the state of each other’s photon. If they use different bases, the information can be used to determine if an attacker Eve has been present during the transmission by leveraging Bell’s inequality.

Continuous Variable Quantum Key Distribution (CV-QKD) on basis of GG02 [9]

In CV-QKD, Alice encodes the information in the light field’s amplitude and phase quadratures using Gaussian random numbers. Bob measures randomly either the amplitude or the phase of each signal and informs Alice about his choice. This procedure yields two correlated sets of Gaussian variables, from which Alice and Bob can extract a shared secret key through classical post-processing. The security of CV-QKD stems from the Heisenberg uncertainty principle, which implies that any attempt to measure both the amplitude and phase inevitably adds noise to the signal. To preserve genuine quantum behavior and ensure security, the transmitted states must remain weak to prevent an eavesdropper Eve from probing them without detection.

This article has been accepted for publication in IEEE Communications Standards Magazine. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MCOMSTD.2026.3697812

SO, EVERYTHING IS FINE AGAIN. OR NOT REALLY?

QKD allows for the secure exchange of symmetric keys but also presents several challenges, among them are the following:

Distance: The attenuation of light in a fiber limits the maximum distance of a single QKD link, reducing also the key rate with increasing distance. In the lab, distances of more than 800km have been already achieved for DV-QKD [10]. Typically, in currently available commercial solutions, the distance is limited to about 100-150km for DV-QKD, which is sufficient for transmission of keys between mobile base stations and the mobile core network. For longer-distances, such as within the mobile core network, communication can be achieved either through QKD via satellites or by using trusted nodes until quantum repeaters become practical and move beyond the research stage. Using trusted nodes, a node receives QKD-derived keying material from one link and forwards fresh or re-wrapped keying material to the next link. This relaying requires strict physical and logical trust assumptions. Payload traffic does not need to be decrypted at the node unless link-by-link encryption is chosen. Although, entanglement is theoretically not limited in distance, the maximum distance is also limited in real-world eQKD to a few hundred kilometers. In CV-QKD, achievable distance is limited also to about 150 km by channel loss, excess noise, and reconciliation efficiency.
Classical optical repeaters or amplifiers cannot extend quantum signals because they do not preserve the quantum states. Hence, practical quantum repeaters remain a research topic across all QKD variants.

Point-to-point: Only point-to-point links are supported with DV-QKD. Hence, a larger QKD network would consist of several point-to-point QKD links with trusted nodes between them. As already stated above, concepts and implementations are required to reduce the number of trusted nodes and to make them safe against attacks. However, researchers already identified the trusted nodes as the weak point for secure end-to-end quantum key exchange.

Unlike DV-QKD, eQKD also supports point-to-multipoint key distribution in principle. However, any optoelectronic conversion of the signal between Alice and Bob would destroy the quantum properties, hence limiting the key exchange to segments in fiber networks without such equipment. Thus, carrier-scale multi-user key distribution remains a research topic.

Special equipment: Most existing DV-QKD and eQKD solutions require special equipment such as single photon detectors, which make them very expensive. The co-existence of today's commercially available QKD systems with already deployed fiber optical systems for communication purposes in the same fiber is limited, typically requiring a dark fiber for QKD between the communicating network endpoints. Having a solution with a single fiber where the QKD signal and the payload use different wavelengths has already been demonstrated. However, further elaboration and standardization of such schemes would be highly beneficial for deployments in already existing fiber networks.

Whole solution: QKD alone is not sufficient but only part of a whole solution. Additionally, a key management system (KMS) is required for storage, management and exchange of the keys.

Attacks: QKD is theoretically secure due to the underlying quantum laws that they rely on and that cannot be conquered.
Like any optical communication system, QKD can be disrupted by a form of Denial-of-Service (DoS) if the quantum channel is physically interrupted e.g. by cutting the fiber or injecting noise, although such attacks affect availability rather than the secrecy of the exchanged keys.
Moreover, researchers have demonstrated practical side-channel attacks on existing QKD implementations, showing that keys could be extracted without Alice or Bob detecting the intrusion. Such exploits often target hardware components, e.g. vulnerabilities in avalanche photodiodes used in detection.
As for classical cyber-security solutions, researchers continuously suggest countermeasures to fix these vulnerabilities.

Standardization: To enable QKD use in future 6G networks, standardization, certification, and auditability are crucial. Although functional requirements for QKD exist, such as those developed by the International Telecommunication Union (ITU) [11], a comprehensive standard for the physical transmission of quantum keys and full system operation is still lacking. Current implementations largely follow academic concepts and remain vendor-specific, so devices based on the same theoretical protocol are not necessarily interoperable.

For widespread commercial deployment, QKD standards should address not only the physical layer mechanisms but also the complete system architecture, including key management

systems (KMS) and trusted-node concepts, to ensure secure key exchange across heterogeneous infrastructures.

Certification and security assurance are essential for deploying quantum technologies in critical communication infrastructures, including 6G networks. Progress in QKD certification is evident in ongoing European efforts, such as the EuroQCI program and related initiatives developing protection profiles and certification frameworks. A broader overview of quantum technology standardization in Europe can be found in [12].

Key Exchange by Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography (PQC) encompasses algorithms that remain secure against both quantum computer and classical computer attacks. Unlike QKD, which depends on quantum physics, PQC is entirely software-based and designed to run on classical hardware. Research and standardization, led by institutions such as NIST and ETSI, focus on lattice-based, hash-based, and multivariate-polynomial schemes. PQC offers scalability and ease of deployment within existing network and device infrastructures, making it suitable for end-user devices and over-the-air links. In a 6G context, PQC can complement QKD by securing connections where quantum channels are impractical.

In 2016, the National Institute of Standards and Technology (NIST) published a call for proposals for post-quantum cryptography algorithms. From the initially more than 80 submitted proposals, only 3 algorithms, including one key encapsulation mechanism (KEM) and two digital signature algorithms, have been published as standards in August 2024. A fourth algorithm was expected to be standardized by the end of 2024, which was not the case, and a fifth algorithm was announced at the beginning of 2025 to be finally standardized in 2027. The three new standards received new names after the draft phase and are:

FIPS 203 (formerly Kyber, now ML-KEM [13]), which is a KEM based on structured lattices. It shows good all-around performance and security properties.

FIPS 204 (formerly Dilithium, now ML-DSA [13]), which is a digital signature based on structured lattices. Due to its good all-around performance and security in combination with a relatively simple implementation, NIST recommends it as primary signature algorithm to be used.

FIPS 205 (formerly Sphincs+, now SLH-DSA [13]), which is a digital signature based on stateless hash-based cryptography with performance below that of FIPS 204.

All these new PQC standards are based on mathematical problems that are assumed to be difficult even in the presence of quantum computers. There exists no proof yet that these algorithms will remain secure indefinitely. Hence, as with today's encryption algorithms it may happen in future that either clever solutions will be found or that quantum computers become powerful enough to solve these mathematical problems in a relatively short time, resulting in becoming insecure.

Therefore, three more algorithms are still in the standardization process and could be considered as a kind of fallback in case that the standardized algorithms turn out to be vulnerable at a later point in time.

The Latency-Performance Trade-off

While currently the mathematical security of the PQC algorithms standardized by NIST can be assumed, its implementation within the 6G Radio Access Network (RAN) might impact the performance. 6G aims for Ultra-Reliable Low-Latency Communication (URLLC) with a target latency of less than 1 ms.

Computational Overhead and Handshake Latency

The transition from ECC to lattice-based schemes like ML-KEM impacts the initial handshake. While ML-KEM is computationally efficient, the size of the public keys and ciphertexts is a concern. For example, ML-KEM typically uses kilobyte scale public keys, an order of magnitude increase over the tens of bytes sized public keys, common in today's ECC based standards.

For 6G standardization, this means:

Message size: The maximum transmission unit (MTU) of control plane protocols must be specified such that large PQC keys do not exceed it. If a key must be split across multiple radio link control (RLC) segments, it increases the probability of packet loss and retransmission, directly threatening the URLLC reliability mandate.

Energy consumption: For mMTC (massive Machine Type Communications) devices in the 6G ecosystem, the transmission of kilobyte-sized keys instead of byte-sized ones leads to higher radio-frequency (RF) energy expenditure, shortening the battery life of sensors designed to last a decade.

This article has been accepted for publication in IEEE Communications Standards Magazine. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MCOMSTD.2026.3697812

Strategic Measures for PQC Performance Optimization

To mitigate the drawbacks described above, for 6G standardization we propose a transition from a "static" security model to an "adaptive" one. This involves leveraging the inherent flexibility of the 6G architecture.

Dimension	Quantum Key Distribution (QKD)	Post-Quantum Cryptography (PQC)
Security Foundation	Based on quantum mechanical principles; security derived from the laws of physics.	Based on mathematical hardness assumptions resistant to quantum algorithms; no absolute proof of immunity.
Key Exchange Mechanism	Keys generated through transmission of quantum states over fiber or free-space optical links.	Keys exchanged through classical communication using standardized lattice-based or hash-based algorithms.
Required Physical Infrastructure	Needs fiber or satellite optics and special equipment (e.g. single-photon detectors).	No specific infrastructure needed; relatively easy deployable in existing systems and devices.
Scalability	Point-to-point with typically <150 km; trusted nodes for longer distances.	Supports global Internet scale.
Standardization Status (2026)	ETSI ISG-QKD, ITU-T Y.3800-series, ISO/IEC 23837 in progress. Physical-layer interoperability still limited.	NIST FIPS 203 (KEM), 204 (DSA), 205 (DSA) published; additional algorithms pending; integration into IETF TLS 1.3, 3GPP SA3 studies advancing.
Threats / Vulnerabilities	Hardware side-channel attacks (e.g. detector blinding).	Mathematical breakthroughs could defeat certain schemes; implementation bugs or side-channel attacks possible.
Auditability and Certification	Complex due to proprietary hardware; few certification paths available; emerging ETSI guides.	Straightforward — uses cryptographic FIPS and ISO frameworks; readily auditable.
Cost / Economic Viability	Today high CAPEX/OPEX; feasible for national or operator-grade backbone.	Low cost; widely applicable across all network tiers.
Best-Fit Deployment in 6G	Core network, data-center interconnects, satellite backhaul, mission-critical government links.	End user devices, RAN/user plane protection, IoT, URLLC.
Main Benefits	Physics-guaranteed security, eavesdropping detection, independence from mathematical assumptions.	Ease of deployment, software-only implementation, flexible integration, scalable quantum-resistance.
Challenges to Address	Reduce system cost, extend operational range, strengthen standardization and certification frameworks.	Migration of the current security eco system to PQC, minimize key-size overhead and energy impact, continuously monitor mathematical robustness of selected schemes.

TABLE 1. Comparison of QKD and PQC

Security-Aware Network Slicing

Network slicing, which has been introduced with 5G, is also considered as a fundamental pillar of 6G, allowing a single physical infrastructure to support multiple virtual networks with different service level agreements (SLAs). We propose using slice-specific security policies as a primary optimization measure. Instead of a "one-size-fits-all" PQC approach, slices with different purposes or optimization criteria could utilize different cryptographic suites.

For instance, in a URLLC slice (e.g. for industrial robotics), with priority on low latency, one might use "lightweight" PQC with smaller public keys or even rely on pre-shared symmetric keys refreshed during non-critical periods.

In an eMBB (enhanced Mobile Broadband) slice (e.g. for AR/VR) one could most likely tolerate slightly higher handshake latency relying on standard ML-KEM-768 for robust protection. And in an mMTC slice (e.g. for smart meters) power consumption is of highest importance. Hence, one may utilize extremely infrequent PQC handshakes or delegate security to an "edge gateway" that handles the heavy PQC computation on behalf of the simple sensors. Such approach would prevent the high overhead of PQC from "polluting" the performance of slices that require sub-millisecond responses.

Adaptive Key Refreshment

In 5G, re-keying is often triggered by timers or handovers, which may result in a «signaling storm». This effect might be omitted in 6G by context-aware re-keying.

Risk-based triggers: Instead of refreshing keys in regular time intervals, the 6G core might trigger a new PQC handshake only when a risk threshold is met (e.g., after a certain volume of data is transmitted or when a device moves to a less-trusted geographical area).

Overhead vs. exposure: Extending the time between PQC handshakes reduces signaling overhead but increases the "cryptographic exposure window." Standardization should define the maximum permissible "security gap" for different service classes.

Handshake resumption and 0-RTT PQC

To avoid the heavy cost of a full PQC exchange for every connection, session resumption techniques may be applied similar to those found in TLS 1.3 but optimized for the radio interface. After the initial heavy ML-KEM handshake, the network issues a "quantum-safe ticket." Subsequent reconnections could use this ticket to derive new session keys using much faster symmetric cryptography, effectively achieving zero round-trip time (0-RTT) handshakes for the majority of user sessions.

THE WAY FORWARD

Cryptographic assets require special focus, particularly given the rapidly changing cryptographic landscape due to the presence of CRQC. Implementing a comprehensive crypto inventory is essential. A crypto inventory can be considered as an overview of all cryptographic material and algorithms deployed in an organization, including ciphers and key lengths. It provides transparency regarding potential security issues and facilitates the orchestration of security updates. Reviewing and maintaining this inventory across the various levels protocols, software and infrastructure ensures compliance and supports auditing processes. As crypto inventories are not limited to 6G and mobile networks only, the ability of embedding a 6G crypto inventory into a general companies' crypto inventory should be kept in mind during the standardization.

Once a crypto inventory is in place, ensuring cryptographic agility becomes crucial for maintaining flexibility in response to evolving threats. It must be considered in the standardization that cryptographic algorithms can be changed without significant infrastructure modifications. This involves transitioning from hardcoded algorithms to configurable options, while ensuring these configurations are secured rigorously. Embedding agility into cryptographic strategies allows the mobile network to remain future-proof and to swiftly move to new algorithms if needed.

6G WITH A HYBRID PQC-QKD SETUP

6G is expected to deliver ultra-high data rates, sub-millisecond latency, and native support for AI-driven orchestration and tactile Internet applications [14]. To address cyber-threats that are caused by quantum computers, symmetric encryption like AES should be considered in general to allow for quantum resilience. The choice of symmetric encryption can be tailored for each network slice. New encryption algorithms with longer key lengths will most likely be required with the advance of more powerful quantum computers.

For exchange of keys and signatures, both PQC and QKD should be considered. Fiber-based segments of 6G backhaul and core networks are promising candidates for deploying QKD, while PQC can protect wireless access, edge nodes and user equipment. Building on hybrid PQC-QKD models proposed in recent literature [15], a feasible 6G architecture is illustrated in Figure 6, where key exchange is performed via PQC or a hybrid PQC-QKD setup according to segment-specific requirements.

From today's perspective, PQC appears to be the more comprehensive solution, capable of protecting

This article has been accepted for publication in IEEE Communications Standards Magazine. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/MCOMSTD.2026.3697812

nearly all connections up to the end-user device. Its software-based nature allows it to scale effectively across the billions of diverse devices and the mobile networks that will constitute the 6G ecosystem.
Nevertheless, we propose considering QKD as an option for mission-critical communications or as a second security mechanism in the mobile core network.

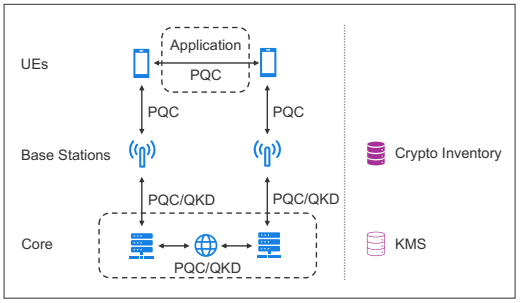

FIGURE 6. High-level architecture for quantum-resistant key exchange in 6G networks

By leveraging QKD for key exchange on the lowest infrastructure layers, specifically within the core and between core nodes and mobile base stations, 6G can achieve a pragmatic but highly secure balance. Ubiquitous, mathematical resilience is provided to the end-user and as an option absolute, physics-based protection on top for the network's vital backbone.

However, practical deployments of hybrid PQC-QKD solutions in 6G networks face distinct challenges. QKD must overcome optical-channel loss, limited key rates, and the need for standardized interfaces, while PQC introduces computational overhead and hardware-acceleration demands on resource-constrained devices. Ensuring interoperability through common management APIs, unified key-lifecycle frameworks, and performance monitoring is essential to achieve carrier-grade reliability and scalability.

CONCLUSION

Cryptographically relevant quantum computers pose a serious risk to today's asymmetric cryptography. 6G could be the first cellular technology where post-quantum resistance is considered and integrated from the very beginning of the standardization. Ideally, this would result in a mobile network solution providing an integrated, comprehensive and sustainable post-quantum resilience from the start instead of adding post-quantum resilience on different layers of an existing mobile solution at a later point in time as it most likely will happen in 4G and 5G.

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *IEEE 35th Annual Symposium on Foundations of Computer Science*, Nov. 1994

[2] C. Gidney, M. Ekera, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum 5, 433,* 2021

[3] C. Chevignard, P.-A. Fouque and A. Schrottenloher, "Reducing the Number of Qubits in Quantum Factoring," *28'th annual Quantum Information Processing (QIP) conference & CRYPTO,* 2025

[4] M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?" *IEEE Security & Privacy, Volume 16, Issue 5, pp. 38-41, Sept./Oct.* 2018

[5] M. Mosca, M. Piani, "Quantum Threat Timeline Report 2024," *Global Risk Institute, Dec.* 2024

[6] L. K. Grover, "A fast quantum mechanical algorithm for database search," *STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing, pp. 212-219,* Jul. 1996

[7] C. H. Bennett, G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *IEEE International Conference on Computers, Systems & Signal Processing, pp. 175-179*, Dec. 1984

[8] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *APS Physical Review Letters, Volume 67, Issue 6, pp. 661-663,* Aug. 1991

[9] F. Grosshans, P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," *APS Physical Review Letters, Volume 88, Issue 5,* Jan. 2002

[10] S. Wang, Z. Q. Yin, D. Y. He, et. al. "Twin-field quantum key distribution over 830-km fibre", *Nature Photonics, Volume 16, Number 2, pp 154-161,* 2022

[11] Functional requirements for quantum key distribution networks, ITU-T, Y.3801, ITU Standard, 2020

[12] O. van Deventer, N. Spethmann, M. Loeffler et. al., "Towards European standards for quantum technologies," *EPJ Quantum Technology, Volume 9, Article Number 33,* 2022

[13] NIST FIPS 203-205, Module-Lattice-Based Key-Encapsulation Mechanism Standard, Module-Lattice-Based Digital Signature Standard, Stateless Hash-Based Digital Signature Standard, National Institute of Standards and Technology, NIST, 2024

[14] H. Tataria, M. Shafi, A. F. Molisch, et. al. "6G Wireless Systems: Vision, Requirements, Challenges, Insights, and Opportunities", *Proceedings of the IEEE, vol. 109, no. 7, pp. 1166-1199*, July 2021

[15] S. Hoque, A. Aydeger, E. Zeydan. "Exploring Post Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design", *ACM Proceedings of the 4th workshop on performance and energy efficiency in concurrent and distributed systems, pp. 9-16,* 2024

BIOGRAPHY

Thomas Zasowski (thomas.zasowski@swisscom.com) received the M.Sc. degree in Electrical Engineering from Saarland University, Saarbrücken, Germany, in 2002, and the Ph.D. in Technical Sciences from ETH Zurich, Switzerland, in 2007.
He has held technical lead and management positions at Swisscom, Switzerland's leading telecom and ICT provider, where he has been involved in the development and introduction of several new

technologies, including 5G, g.fast and hybrid access networks. Since 2019, he has served as Head of Innovation, B2B, at Swisscom, where he has led multiple strategic ICT initiatives. During this period, he coordinated internal post-quantum security efforts and contributed to the development of a modular cyber-security solution that forms an integral part of the communication network. His main research interests include wired and wireless network technologies, network security, and post-quantum security.