Hybrid Quantum Security: Integrating QKD and PQC in Brownfield Optical Networks

Alberto Comin

Airbus Central Research and Technology, Munich, Germany
E-mail: alberto.comin@airbus.com

Received 09 December 2025; Accepted 11 December 2025

Abstract

The future security of digital communications will increasingly rely on the integration of Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC), indicating a necessary convergence rather than a competitive relationship between these two technologies. Following the publication of NIST FIPS 203, 204 and 205, the industry now possesses standardised algorithmic tools for migrating away from RSA and elliptic-curve cryptography (ECC). At the same time, for critical infrastructure facing "harvest-now, decrypt-later" adversaries, purely software-based measures provide only computational, not information-theoretic, security. We argue that the optimal solution is a hybrid architecture, in which PQC provides authentication and cryptographic agility across heterogeneous endpoints, while QKD supplies an additional physical-layer shield for high-value links. The central engineering challenge is brownfield coexistence: deploying QKD over existing lit telecom fibers that carry high-power classical traffic.

We review three spectral coexistence strategies to mitigate Spontaneous Raman Scattering (SpRS) – O-band separation, dense C-band DWDM integration with guard bands, and an "inverted" spectrum approach where data uses the O-band and QKD uses the C-band – and we discuss emerging physical media such as hollow-core and multi-core fibers. At the protocol layer, we discuss hybrid key encapsulation and the role of crypto-agile gateways in

Quantum Information Technologies Journal, Vol. 1_1, 105–122.
doi: 10.13052/qitj2795-0492.116

combining keys from classical, PQC and QKD sources [1]. Finally, we survey industrial pilots (e.g., SK Telecom, EuroQCI / OPENQKD) and outline open challenges in cost, standardisation and operations. The goal is to provide practitioners with a realistic, engineering-oriented overview of how PQC and QKD can be combined in brownfield optical networks.

Keywords: Quantum Key Distribution (QKD), Post-Quantum Cryptography (PQC), Brownfield Networks, Coexistence, Hybrid Security, WDM.

1 Introduction

The security of digital communications is undergoing a profound transition. For decades, the confidentiality and authenticity of internet traffic have relied on public-key primitives such as RSA and elliptic-curve cryptography (ECC). The prospect of large-scale quantum computers capable of running Shor's algorithm threatens to break these schemes, motivating an urgent search for quantum-resistant alternatives.

On the algorithmic side, the National Institute of Standards and Technology (NIST) has completed the first round of its Post-Quantum Cryptography (PQC) standardisation process and, in 2024, published Federal Information Processing Standards (FIPS) 203, 204 and 205 for lattice-based and hash-based key establishment and signatures [2–4]. This milestone transitions PQC from academic research into regulated engineering and provides software vendors, device manufacturers and network operators with concrete algorithms to deploy.

In parallel, Quantum Key Distribution (QKD) has matured from physics experiments into field trials and early commercial deployments [5–7]. Unlike PQC, which is computationally secure under hardness assumptions, QKD can deliver keys with information-theoretic security (ITS) against unbounded adversaries, provided implementation assumptions hold. This makes QKD particularly attractive for critical infrastructure such as governmental backbones, financial data-center interconnects and telecom core networks, where the confidentiality lifetime of data may exceed the safe lifetime of any specific hardness assumption.

Public discussions around PQC and QKD are often framed as a binary choice: "software vs hardware", or "crypto vs physics". In practice, these technologies are complementary: PQC is required everywhere RSA/ECC are currently used: browsers, Virtual Private Networks (VPN), software updates, IoT endpoints. QKD is only feasible on certain links (fiber-connected,

relatively static), but on those links it can provide an additional layer of protection against long-term, harvest-now-decrypt-later adversaries by making the keys themselves information-theoretically secure.

In this article we adopt the perspective that, for high-value links, the relevant question in 2025 is no longer whether to combine PQC and QKD, but how to do so in a cost-effective way.

> *The primary bottleneck is physical: QKD systems typically operate at single-photon levels, whereas classical channels in telecom fibers are launched around 0 dBm (≈1 mW). The resulting dynamic range of many orders of magnitude makes quantum channels extremely sensitive to in-fiber noise. Telecom operators cannot afford to dedicate a new dark fiber to every quantum link; instead, QKD must coexist with classical traffic in brownfield optical networks. This coexistence problem has become a focus of recent research and standardisation efforts* [5–9].

The remainder of the paper is organised as follows. Section 2 summarises the new PQC standards and their role in hybrid architectures. Section 3 reviews coexistence strategies for QKD on lit fibers, including O-band separation, C-band Dense Wavelength-Division Multiplexing (DWDM), inverted spectrum allocations, and emerging hollow-core and multi-core fibers. Section 4 discusses hybrid key management and ETSI TS 104 015. Section 5 examines industrial pilots and identifies architectural patterns. Section 6 outlines open challenges and research directions, and Section 7 concludes.

2 Post-Quantum Cryptography as the New Baseline

2.1 NIST PQC standards (FIPS 203, 204, 205)

The first Post-Quantum Cryptography (PQC) standards issued by the National Institute of Standards and Technology define three core algorithms [2–4]:

- **FIPS 203:** A module-lattice-based Key Encapsulation Mechanism (ML-KEM) derived from CRYSTALS-Kyber. ML-KEM is intended as the default key-establishment primitive to replace RSA and elliptic-curve Diffie–Hellman (ECDH) in Transport Layer Security (TLS), VPNs and related protocols.

- **FIPS 204:** A Module-Lattice-Based Digital Signature Algorithm (ML-DSA) derived from CRYSTALS-Dilithium. ML-DSA is designed as the primary quantum-resistant digital signature standard.
- **FIPS 205:** A Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) derived from SPHINCS+. SLH-DSA is based on hash-based constructions and is intended as a hedge in case lattice-based signatures are compromised.

These algorithms form the software shield in a hybrid PQC+QKD architecture: they are deployable on commodity hardware, supported by standard libraries and protocols, and backed by regulatory guidance.

2.2 PQC role in hybrid quantum-safe networks

Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) can be viewed as complementary rather than competing technologies. PQC is essential for securely authenticating QKD at scale. Conversely, QKD provides the necessary information-theoretic security guarantees that PQC alone cannot offer for long-term key secrecy on critical, high-value communication links.

In a hybrid network, Post-Quantum Cryptography (PQC) assumes various roles that extend beyond a mere substitution for RSA/ECC [1, 10].

- Extending security to the "last mile": QKD hardware is unlikely to be deployed on mobile devices, Wi-Fi links, or many access networks in the near term. PQC, by contrast, is software-deployable on endpoints ranging from servers to smartphones. This enables a hybrid architecture in which QKD protects backbone segments between data centers, while PQC secures traffic from those data centers out to end users, as shown in Figure 1a.
- Authentication for QKD: QKD protocols assume an authenticated classical channel between endpoints to prevent man-in-the-middle attacks. Historically this authentication relied on pre-shared symmetric keys or classical public-key signatures. In a post-quantum context, PQC signatures such as ML-DSA can authenticate QKD control channels in a quantum-safe way, as shown in Figure 1b.
- Cryptographic agility remains essential after the transition to post-quantum cryptography, since PQC simply shifts security to a different set of hardness assumptions. Modern hybrid key-exchange designs therefore run two independent key-establishment mechanisms in parallel – typically a classical Elliptic Curve Diffie-Hellman Ephemeral

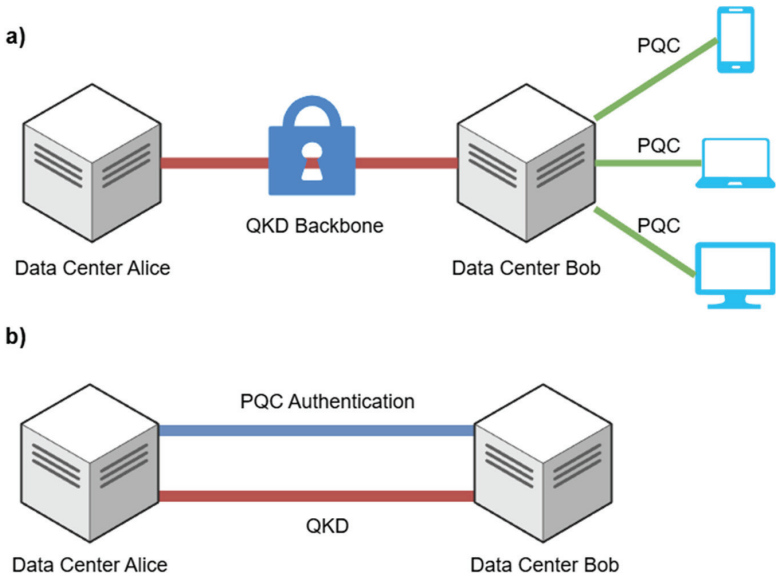

Figure 1 Simplified architecture illustrating the complementary roles of Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) in a hybrid network. a) QKD protects backbone segments between data centers, while PQC secures traffic from those data centers out to end users. b) PQC can authenticate QKD control channels in a quantum-safe way.

(ECDHE) exchange and a post-quantum KEM such as ML-KEM – and then combine their resulting shared secrets using a Key Derivation Function (KDF) or the TLS 1.3 key schedule. Current IETF drafts for hybrid TLS follow exactly this pattern: the ECDH and PQC shared secrets are concatenated and input into the standard key schedule to derive session keys [11]. By the same principle, hybrid architectures could combine multiple PQC algorithms, or even PQC and QKD-derived keys, ensuring that the compromise of any single component does not jeopardize the security of all established session keys.

3 QKD in Brownfield Optical Networks: Coexistence Strategies

QKD systems encode quantum states on single photons or weak coherent pulses, typically at telecom wavelengths. When these quantum signals share fiber with intense classical channels, several impairments arise:

- Spontaneous Raman Scattering (SpRS): Inelastic scattering of classical photons generates broadband noise across the spectrum.
- Four-wave mixing and cross-phase modulation: Nonlinear effects in DWDM systems can create additional noise in the quantum channel.
- Amplified Spontaneous Emission (ASE): Optical amplifiers, such as Erbium-Doped Fiber Amplifiers (EDFAs) introduce broadband noise.

A classical channel launched at $\sim$0 dBm can generate enough Raman noise that the effective noise floor in the quantum channel becomes orders of magnitude above the single-photon level, severely degrading the secret key rate or even preventing key generation [5–7]. Coexistence strategies seek to reduce the noise seen by the quantum receiver while preserving classical capacity.

We classify coexistence approaches into three spectral strategies and two emerging media, as shown in Figure 2.

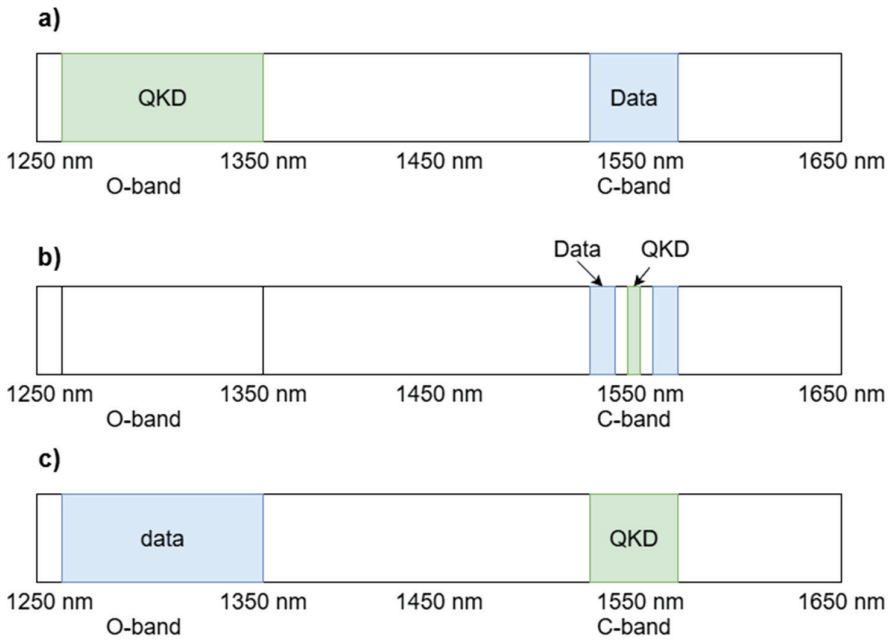

Figure 2 Spectral allocation strategies for QKD coexistence. (a) QKD in the O-band and data in the C-band. (b) Both QKD and data in the C-band with guard bands between them. (c) classical data in the O-band and QKD in the C-band.

3.1 Spectral separation (O-band QKD, C-band data)

A straightforward approach is to place quantum and classical channels in widely separated wavelength bands:

- Quantum channel(s) in the O-band (1260–1360 nm).
- Classical data (DWDM) in the C-band (1530–1565 nm) and possibly the L-band.

Raman scattering in silica fiber predominantly generates Stokes-shifted photons at longer wavelengths. High-power C-band pumps therefore scatter noise mainly into longer-wavelength bands, with weak anti-Stokes scattering back into the O-band. O-band quantum channels are thus largely shielded from C-band Raman noise [7].

The O-band suffers higher fiber attenuation ($\sim$0.3–0.4 dB/km) than the C-band ($\sim$0.2 dB/km) in standard G.652 fiber. For QKD, which is very sensitive to loss, this limits the reach of individual links to metropolitan distances (tens of kilometres), even when using state-of-the-art detectors. Multiple studies have demonstrated O-band QKD coexisting with C-band traffic over $\sim$20–40 km links, but extending beyond that becomes challenging without trusted nodes or future quantum repeater technologies [7, 12]. At present, only trusted-node architectures are brownfield-ready; quantum repeaters remain a research topic.

This method is attractive for short metro loops where spare O-band spectrum is available and where operators can accept the reach limitation in exchange for simpler coexistence engineering.

3.2 Dense C-band DWDM integration

In many networks, operators prefer to keep all traffic in the C-band, where amplifiers, ROADMs and transceivers are standardised and cost-optimised. In this in-band coexistence method, the QKD wavelength is placed within the C-band DWDM grid.

Filtration and guard bands. To prevent adjacent channels from overwhelming the quantum receiver, the QKD wavelength is typically surrounded by guard bands – empty DWDM slots (e.g. 100–200 GHz) on either side – and isolated using cascaded optical filters (WDM demultiplexers, notch filters, narrowband band-pass filters). Experimental setups report total out-of-band isolation exceeding 100 dB [6, 12].

Discrete-Variable QKD (DV-QKD) uses single-photon detectors that integrate all photons within a timing window, making them sensitive to

broadband noise unless sharp optical filtering is applied. Continuous-Variable QKD (CV-QKD), by contrast, uses homodyne or heterodyne detection with a strong local oscillator (LO). The LO defines a narrow spatial-temporal mode; only light in that mode contributes significantly to the measured quadratures. This coherent receiver acts as a mode-selective filter, rejecting much of the Raman and ASE noise outside the LO's mode [9].

Recent work by Hajomer et al. demonstrated CV-QKD coexistence with a fully populated Coarse Wavelength-Division Multiplexing (CWDM) system over 120 km of fiber, using natural mode filtering of the LO and robust phase-noise mitigation [9].

At the same time, the security analysis of CV-QKD in realistic settings is still an active area of research. While composable security proofs against general attacks exist, their assumptions and finite-size treatments are more intricate than for many DV-QKD protocols [13, 14]. This justifies a cautious statement that "security proofs are still evolving" when discussing deployable CV-QKD systems.

Overall, dense C-band integration is appealing where operators wish to minimise changes to existing DWDM infrastructure and can justify the added filtering and complexity.

3.3 Inverted spectrum (O-band data, C-band QKD)

An alternative, recent approach in fiber optic communication is to invert the typical allocation of frequency bands for data and Quantum Key Distribution (QKD). In this method, high-capacity classical data transmission, employing coherent modems, is moved to the O-band. Conversely, the QKD channel is situated in the C-band, leveraging its lower signal attenuation and compatibility with existing single-photon detection hardware. This inverted spectrum method was experimentally validated by Beppu et al. over 80 km of fiber [8]. Their demonstration successfully achieved simultaneous transmission of a 33.4 Tb/s classical superchannel in the O-band and a DV-QKD channel in the C-band. The C-band quantum channel offered distinct advantages, including extended reach, due to reduced fiber attenuation compared to the O-band, and minimized Raman noise. This noise reduction occurs because the powerful O-band signals scatter predominantly into higher wavelengths, leaving the C-band relatively undisturbed.

This trial represents one of the highest reported capacity–distance products for QKD coexistence to date and highlights the potential of non-traditional wavelength allocations in brownfield scenarios.

Implementing the inverted approach in existing networks is challenging because it is not a plug-and-play solution. It necessitates O-band coherent transceivers and potentially new amplification methods. While this might be viable for new greenfield 6G/metro deployments, retrofitting it into older, C-band-only systems could prove difficult. Despite these hurdles, this approach highlights that shifting the classical channels is sometimes less complicated than shifting the quantum channel.

3.4 Emerging media: hollow-core and multi-core fibers

Beyond spectral strategies in standard single-mode fiber, new fiber types, such as Hollow-Core Fiber (HCF) and Multi-Core Fiber (MCF), offer physical isolation between quantum and classical channels.

Hollow-core nested antiresonant fibers guide light predominantly in air rather than glass. This dramatically reduces nonlinear effects, including Raman scattering. Alia et al. demonstrated DV-QKD coexisting with 1.6 Tb/s of C-band classical data launched at 0 dBm over HCF, with negligible degradation of secret key rate compared to the QKD-only case [5]. In contrast, the same configuration in standard single-mode fiber was limited to total launch powers around -20 dBm before QKD performance collapsed. This corresponds to roughly two orders of magnitude higher tolerable classical power in HCF compared to SMF, a striking figure that underscores the potential of engineered fiber for coexistence.

HCF also reduces latency because light travels faster in air than in silica, with one-way latency reductions of order 1.5 μs per kilometre. This makes HCF doubly attractive for latency-sensitive financial links that also demand strong security.

In MCF, several cores are embedded in the same cladding. By dedicating one core to QKD and others to classical data, one obtains inherent spatial isolation [28]. Core-to-core crosstalk in modern MCFs is typically 50–70 dB, substantially reducing the noise seen in the quantum core. Kong et al. analyse QKD coexistence in HCF, MCF and SMF, and propose wavelength allocation schemes that further enhance performance [7].

Multi-Core Fiber (MCF) enables various coexistence strategies, typically permitting classical and quantum signals to share the same wavelength grid while occupying separate cores ("spatial WDM"). Additional spectral separation can be realized within each core. Although MCF can be deployed similarly to standard cable, providing several quasi-independent fibers, its drawbacks include elevated cost, less extensive deployment compared to Single-Mode Fiber (SMF), and associated interoperability difficulties (e.g.,

connectors, splices, fan-out devices). Both Hollow-Core Fiber (HCF) and MCF continue to be considered premium technologies. Fundamentally, they illustrate that fiber design itself constitutes an intrinsic element of the coexistence toolkit, serving as a complement to spectral and filtering methodologies.

4 Hybrid Key Management and Standards

Physical coexistence solves only part of the problem. To be operationally useful, QKD keys must be integrated into existing security architectures and key-management workflows. The European Telecommunications Standards Institute (ETSI) has recently published TS 104 015, a technical specification for efficient quantum-safe hybrid key exchanges with hidden access policies [1].

The central concept involves Hybrid Key Encapsulation, specifically a Key Encapsulation Mechanism with Access Control (KEMAC), exemplified by the "Covercrypt" construction [1]. This mechanism utilizes multiple distinct key sources – such as classical Elliptic Curve Diffie-Hellman (ECDH) or Post-Quantum Cryptography (PQC) Key Encapsulation Mechanisms (KEMs) – to encapsulate a symmetric content-encryption key. Access policies rigorously define the requisite combination of these key components for the successful reconstruction of the final key.

Within the domain of quantum-safe security, a prevalent hybrid methodology entails the combination of a classical KEM (e.g., ECDH for legacy compatibility) with a PQC KEM (e.g., ML-KEM, FIPS 203). The foundational security benefit resides in the resulting combined key's persistent protection, provided that at least one of its constituent keys remains resilient against attack. This strategic approach furnishes a robust defense against potential, unforeseen vulnerabilities inherent in either the classical or the PQC cryptographic assumptions.

The actual KEMAC constructions in ETSI TS 104 015 define more specific encapsulation and decapsulation procedures, including access control, metadata and multi-recipient features [1]. Our equation should therefore be read as a conceptual abstraction of hybrid key derivation, not as a verbatim description of the standard.

4.1 Crypto-agile gateways and SDN integration

The successful deployment of these hybrid security solutions in existing networks could increasingly depend on the use of crypto-agile key management

systems and gateways [15, 16]. These central platforms could integrate Post-Quantum Cryptography (PQC) libraries, Quantum Key Distribution (QKD) devices, and classical key servers. They would provide a unified Application Programming Interface (API) for network infrastructure, including firewalls, encryptors, and Virtual Private Network (VPN) appliances. Crucially, these systems could be responsible for enforcing security policies, such as mandating a combination of QKD and PQC for high-sensitivity data while permitting only PQC for lower-sensitivity traffic.

ID Quantique's Clarion KX platform, for example, is designed to orchestrate keys from multiple sources, including QKD and PQC, and to distribute them securely to network encryptors across telecom and enterprise networks [15]. Clarion KX has been integrated into multi-vendor testbeds and national initiatives, enabling hybrid QKD–PQC services and "Quantum-Safe Network" offerings in collaboration with carriers [15].

In EuroQCI and OPENQKD (Open European Quantum Key Distribution Testbed) testbeds, software-defined networking (SDN) controllers manage multi-vendor QKD networks and steer keys across domains [17, 18]. The combination of ETSI-style hybrid KEMs with such crypto-agile gateways is key to making hybrid PQC+QKD deployments operationally manageable.

5 Industrial Applications and Design Patterns

Hybrid PQC+QKD concepts have been validated in several large-scale pilot projects within production-like settings. We will present two key examples and deduce the recurring architectural patterns from them.

5.1 Telecom hybrid encryption services

In Korea, SK Telecom and affiliates have developed and marketed QKD–PQC hybrid encryption products, often described in marketing literature as "quantum double encryption" [17, 19, 20]. These services are implemented using a combination of technologies: PQC software adhering to NIST-selected algorithms, QKD hardware such as IDQ's Clavis XG systems, and a key-management platform responsible for generating composite keys from both these sources [29].

From a cryptographic standpoint, "quantum double encryption" should be understood as a hybrid scheme for key establishment and encryption. In this approach, keys derived from both Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) are combined, which is conceptually similar to the hybrid Key Encapsulation Mechanism (KEM) methods discussed

in Section 4.1. It is important to differentiate this from the simple sequential application of two independent encryption processes.

Initial deployments focus on securing carrier management and control traffic between key-management servers and network encryptors. Operators also offer PQC-only services for customers for whom QKD is not yet cost-effective, illustrating that the hybrid approach can be applied selectively by policy.

These deployments offer several key design insights. Firstly, they demonstrate the practical coexistence of Backbone Quantum Key Distribution (QKD) and Edge Post-Quantum Cryptography (PQC). In this setup, QKD secures a limited number of fiber segments, while PQC is employed for all other connections. Secondly, a principle of Policy-driven hybridisation is evident: high-value links are protected by both QKD and PQC, while other links utilize PQC exclusively. Finally, a significant element is the Reuse of classical infrastructure: QKD is typically integrated into existing optical links, minimising the need for new dark fibers wherever feasible.

5.2 EuroQCI and OPENQKD: multi-vendor quantum networks

The European Quantum Communication Infrastructure (EuroQCI) initiative aims to deploy a secure quantum communication infrastructure across EU member states [21–23]. Precursor projects such as OPENQKD have built multi-vendor testbeds integrating QKD from different manufacturers into SDN-controlled optical networks [16, 18].

Several key characteristics emerge from these initiatives. Typically, Quantum Key Distribution (QKD) is deployed as a backbone service, with QKD links established between major data centers or national nodes to form a quantum backbone. Conversely, Post-Quantum Cryptography (PQC) is predominantly utilized at the network edge, where client connections from these nodes to end users depend on classical and PQC-based mechanisms. Significant importance is placed on multi-vendor interoperability. Specifically, standardized key-management interfaces facilitate the operation of QKD systems from different vendors through a shared key-management layer. Finally, there is a strong focus on Hybrid use-cases, with demonstrations encompassing quantum-safe Virtual Private Networks (VPNs), data-center interconnects, and the protection of critical infrastructure.

A common pattern emerges: QKD is treated as a shared key-distribution infrastructure, analogous to an optical transport layer, while PQC operates at the IP or application layers.

6 Open Challenges and Research Directions

Despite the progress outlined above, several challenges remain before hybrid PQC+QKD becomes routine in carrier and enterprise networks.

The foremost challenge is related to cost and scalability. Quantum Key Distribution (QKD) hardware, comprising hardware components such as photon sources, detectors, and stabilisation mechanisms, is substantially more expensive than purely software-based Post-Quantum Cryptography (PQC) solutions. Current deployments are typically confined to a limited number of high-value links. A reduction in cost per kilometre, simplification of installation procedures, and enhanced integration with pre-existing optical infrastructure are imperative for achieving broader adoption [16].

Another significant constraint currently involves the necessity for trusted nodes in long-range Quantum Key Distribution (QKD). The majority of deployed QKD systems operate on a point-to-point basis and require reliance on trusted intermediate nodes to achieve extended distances. Within a trusted-node architecture, each QKD link establishes keys between adjacent nodes, and these keys are subsequently relayed or aggregated at these intermediate points. Consequently, the confidentiality of end-to-end keys is contingent not only upon the physical-layer security inherent to QKD but also upon the premise that all intermediate nodes are honest and physically secure [17, 24]. Conversely, quantum repeaters are designed to facilitate the extension of entanglement and Quantum Key Distribution (QKD) across extensive distances without necessitating trust in intermediary nodes, achieved through the utilization of entanglement swapping and quantum memories. Nevertheless, the practical implementation of quantum repeaters remains confined to the realm of research and they are not currently available for deployment in existing "brownfield" networks. Consequently, in the foreseeable future, hybrid Post-Quantum Cryptography (PQC) and QKD networks must explicitly recognize the security compromises inherent in trusted-node architectures and mitigate these through robust organizational and physical security protocols, alongside comprehensive end-to-end application-layer safeguards.

A third challenge is the increased operational complexity. Hybrid PQC+QKD networks introduce new layers of complexity, encompassing key-lifetime management for both QKD and PQC keys, continuous monitoring of QKD system health, managing alarms triggered by QKD key unavailability, and the necessary coordination with maintenance windows that impact optical paths and coexistence performance.

Standardization gaps also represent an ongoing area of development. While ETSI TS 104 015 addresses hybrid Key Encapsulation Mechanisms

(KEMs), and nascent standards are emerging for Quantum Key Distribution (QKD) interfaces and key management, comprehensive frameworks encompassing Post-Quantum Cryptography (PQC) algorithms, QKD networks, and higher-layer protocols remain under development. The harmonization of these elements with established standards, such as TLS, IPsec, MACsec, and 3GPP, presents a significant challenge [1–4].

Finally security models and certification are crucial. A key challenge is that security proofs for Quantum Key Distribution (QKD) often assume idealized devices. Therefore, the certification of practical QKD systems remains an active research and standardization area, requiring thorough consideration of side-channels, hardware imperfections, and insider threats. For hybrid schemes, careful analysis is necessary to prevent inadvertent downgrade or misconfiguration flaws. Similarly, while Continuous-Variable QKD (CV-QKD) has established theoretical composable security against general attacks, practical certification must fully account for specific hardware characteristics [13, 14].

Addressing these issues will require sustained collaboration between quantum physicists, cryptographers, network engineers, vendors and standardisation bodies.

7 Conclusion

The advent of standardised PQC algorithms and increasingly mature QKD technology has shifted the focus of quantum-safe communications from if to how these tools should be combined. For most applications, PQC will serve as the universal replacement for classical public-key cryptography, providing quantum-resistant authentication and key establishment on general-purpose hardware. For selected high-value links in critical infrastructure, QKD offers an additional information-theoretic layer of protection against long-term, harvest-now-decrypt-later adversaries.

In brownfield optical networks, one of the key technical challenges will be the coexistence of quantum and classical channels on the same fiber. In this article, we have reviewed three major spectral strategies – O-band separation, dense C-band DWDM integration, and an inverted O-band data/C-band QKD allocation – as well as emerging hollow-core and multi-core fibers that address the problem at the physical-media level [25–27]. In parallel, protocols such as ETSI TS 104 015 and crypto-agile gateways enable hybrid key derivation, blending keys from classical, PQC and QKD sources to achieve defense-in-depth.

Industrial pilots by telecom operators and European consortia demonstrate that hybrid PQC+QKD architectures are already feasible today on a limited scale. Over the coming years, networks are likely to evolve toward a heterogeneous mix of standard single-mode fiber, specialised hollow-core routes and multi-core cables, orchestrated by crypto-agile key-management systems. In such networks, PQC and QKD will not be competitors but complementary building blocks in a layered, quantum-safe security architecture.

References

[1] ETSI. (2025). ETSI TS 104 015 V1.1.1 (2025–02): Cyber Security; Quantum-Safe Cryptography; Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies. European Telecommunications Standards Institute.

[2] National Institute of Standards and Technology (US). 2024. Module-lattice-based key-encapsulation mechanism standard, National Institute of Standards and Technology (U.S.), Washington, D.C. NIST FIPS 203.

[3] National Institute of Standards and Technology (US). 2024. Module-lattice-based digital signature standard, National Institute of Standards and Technology (U.S.), Washington, D.C. NIST FIPS 204.

[4] National Institute of Standards and Technology (US). 2024. Stateless hash-based digital signature standard,. National Institute of Standards and Technology (U.S.), Washington, D.C. NIST FIPS 205.

[5] Alia, O., R. S. Tessinari, S. Bahrani, T. D. Bradley, H. Sakr, K. Harrington, J. Hayes, Y. Chen, P. Petropoulos, D. Richardson, F. Poletti, G. T. Kanellos, R. Nejabati, and D. Simeonidou. 2022. DV-QKD Coexistence With 1.6 Tbps Classical Channels Over Hollow Core Fibre. J. Lightwave Technol. 40: 5522–5529.

[6] Schreier, A., Alia, O., Wang, R., Singh, R., Faulkner, G., Kanellos, G., Nejabati, R., Simeonidou, D., Rarity, J., & O'Brien, D. (2023). Coexistence of quantum and 1.6 Tbit/s classical data over fibre-wireless-fibre terminals. Journal of Lightwave Technology, 41(16), 5226–5232. https://doi.org/10.1109/JLT.2023.3258146.

[7] Kong, W., Y. Sun, T. Dou, Y. Xie, Z. Li, Y. Gao, Q. Zhao, N. Chen, W. Gao, Y. Hao, P. Han, Y. Liu, and J. Tang. 2024. Enhanced Coexistence of Quantum Key Distribution and Classical Communication over Hollow-Core and Multi-Core Fibers. Entropy 26: 601.

[8] Beppu, S., D. J. Elson, S. Murai, A. Murakami, H. Yamamuro, Y. Wakayama, N. Yoshikane, and T. Tsuritani. 2025. Coexistence Transmission of 33.4-Tb/s O-band Coherent Classical Channels and a C-band QKD Channel over 80 km. In Optical Fiber Communication Conference (OFC) 2025 Optica Publishing Group, San Francisco, California. Tu3D.2.

[9] Hajomer, A. A. E., I. Derkach, V. C. Usenko, U. L. Andersen, and T. Gehring. 2025. Coexistence of Continuous-Variable Quantum Key Distribution and Classical Data over 120 km Fiber. Phys. Rev. Lett. 135: 170804.

[10] Zeng, P., D. Bandyopadhyay, J. A. M. Méndez, N. Bitner, A. Kolar, M. T. Solomon, Z. Ye, F. Rozpędek, T. Zhong, F. J. Heremans, D. D. Awschalom, L. Jiang, and J. Liu. 2024. Practical hybrid PQC-QKD protocols with enhanced security and performance.

[11] Stebila, D., S. Fluhrer, and S. Gueron. 2025. Hybrid key exchange in TLS 1.3, https://www.ietf.org/archive/id/draft-ietf-tls-hybrid-design-15.txt.

[12] Gao, T., L. Rickert, F. Urban, J. Große, N. Srocka, S. Rodt, A. Musiał, K. Żołnacz, P. Mergo, K. Dybka, W. Urbańczyk, G. Sęk, S. Burger, S. Reitzenstein, and T. Heindel. 2022. A quantum key distribution testbed using a plug & play telecom-wavelength single-photon source. Applied Physics Reviews 9: 011412.

[13] Leverrier, A. 2015. Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States. Phys. Rev. Lett. 114: 070501.

[14] Leverrier, A. 2017. Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction. Phys. Rev. Lett. 118: 200501.

[15] ID Quantique. (2024). Clarion KX Platform: A unified quantum-safe key exchange platform for end-to-end post-quantum security [Brochure/Product page]. Retrieved from https://www.idquantique.com.

[16] WiN-Lab (DFN-Verein). (2024). Quantum Key Distribution Testbeds – Overview of QKD testbeds 2020–2024. Deutsches Forschungsnetz.

[17] Farrugia, N., D. Bonanno, N. Frendo, A. Xuereb, E. Kosmatos, A. Stavdas, M. Russo, B. Montrucchio, M. Menchetti, D. Bacco, S. Marigonda, F. Stocco, G. Morgari, and A. Manzalini. 2024. European Quantum ecOsystems – Preparing the Industry for the Quantum Security and Communications Revolution. In 2024 International Conference

on Quantum Communications, Networking, and Computing (QCNC) IEEE, Kanazawa, Japan. 336–340.

[18] OPENQKD Consortium. (2024). OpenQKD: Open European Quantum Key Distribution Testbed – Project overview and results. Retrieved from https://openqkd.eu.

[19] Korea JoongAng Daily. (2024, October 15). SK Telecom unveils QKD–PQC hybrid quantum encryption product. Korea JoongAng Daily. Retrieved from https://koreajoongangdaily.joins.com.

[20] SK Broadband. (2023). SK Broadband launches hybrid quantum security service. Korea Economic Daily Global Edition. Retrieved from https://www.kedglobal.com.

[21] Geitz, M., R. Döring, and R.-P. Braun. 2023. Hybrid QKD & PQC Protocols implemented in the Berlin OpenQKD testbed. In 2023 8th International Conference on Frontiers of Signal Processing (ICFSP) IEEE, Corfu, Greece. 69–74.

[22] European Commission. (2024). European Quantum Communication Infrastructure – EuroQCI. Retrieved from https://digital-strategy.ec.europa.eu.

[23] EuroQCI. (2025). EuroQCI: Towards a pan-European quantum communication infrastructure. European Commission Factsheet.

[24] Poppe, A., M. Peev, and O. Maurhart. 2008. Outline of the SEQOQC Quantum-Key-Distribution network in Vienna. Int. J. Quantum Inform. 06: 209–218.

[25] Poletti, F. 2014. Nested antiresonant nodeless hollow core fiber. Opt. Express 22: 23807.

[26] Zahidy, M., D. Ribezzo, C. De Lazzari, I. Vagniluca, N. Biagi, R. Müller, T. Occhipinti, L. K. Oxenløwe, M. Galili, T. Hayashi, D. Cassioli, A. Mecozzi, C. Antonelli, A. Zavatta, and D. Bacco. 2024. Practical high-dimensional quantum key distribution protocol over deployed multicore fiber. Nat Commun 15: 1651.

[27] Wu, Q., D. Ribezzo, G. Di Sciullo, S. Cocchi, D. Ann Shaji, L. Alves Zischler, R. Luis, P. Serena, C. Lasagni, A. Bononi, T. Hayashi, A. Gagliano, P. Martelli, A. Gatto, P. Parolari, P. Boffi, D. Bacco, A. Zavatta, Y. Zhu, W. Hu, Z. Xu, M. Shtaif, A. Marotta, F. Graziosi, A. Mecozzi, and C. Antonelli. 2025. Integration of quantum key distribution and high-throughput classical communications in field-deployed multi-core fibers. Light Sci Appl 14: 274.

[28] Zaitcev, A. I., O. V. Kolesnikov, T. V. Kazieva, L. N. Isaeva, and K. Y. Yerokhin. 2023. Quantum Key Distribution Through a Multi-Core Optical Fiber. In 2023 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF) 1–4.
[29] ID Quantique. (2025). Clavis XG series QKD obtains national security certification [Press release]. Retrieved from https://www.idquantique.com

Biography

Alberto Comin holds a PhD in Physics from the University of Milan, Italy. He is currently based at Airbus Central Research and Technology in Munich, Germany. His previous professional experience includes roles at the Italian Institute of Technology, the Lawrence Berkeley National Laboratory, and Sincrotrone Trieste.