Quantum Frontiers Journal

ISSN: e-ISSN: 3117-6089 / p-ISSN: 3117-6070

https://galaxiauniverse.com/index.php/QFJ/issue/archive

Integration of Quantum Cryptography with Classical Network Infrastructure

Amelia Jensen[1]

[1] Associate Professor, Department of Artificial Intelligence, Nordic Technical University, Stockholm, Sweden. Email: amelia.jensen106@gmail.com | ORCID: 9872-0997-0485-9192

ABSTRACT

Classical network infrastructure -- spanning enterprise TCP/IP backbones, metropolitan optical networks, and wide-area internet exchange points -- was designed without native provisions for quantum cryptographic channels. Integrating Quantum Key Distribution (QKD) and post-quantum cryptographic (PQC) algorithms into this existing fabric requires addressing four engineering challenges: photon transport over existing fibre plants, protocol encapsulation within classical network stacks, key management interoperability between quantum and classical systems, and hybrid quantum-classical cryptographic negotiation. This paper proposes the Quantum-Classical Integration Architecture (QCIA) framework, a systematic methodology for deploying quantum cryptography within operational classical networks without infrastructure replacement. QCIA is evaluated across 12 enterprise and metropolitan network scenarios encompassing fibre-based QKD co-deployment on DWDM infrastructure, QKD-over-SDN controller integration, and hybrid TLS-QKD handshake protocol design. Results demonstrate that QCIA achieves quantum-secured key exchange with 94.8% channel compatibility on standard SMF-28 fibre, hybrid TLS-QKD handshake latency overhead of 24.6 ms, and a Quantum Integration Readiness Score (QIRS) of 0.882 across evaluated scenarios. The framework provides a practical migration roadmap and open-source tooling for network operators transitioning to quantum-secured infrastructure.

Keywords: quantum cryptography integration; QKD deployment; DWDM co-existence; hybrid TLS-QKD; post-quantum cryptography; SDN quantum control; classical network infrastructure; quantum migration

Citation: Jensen [2025]. Integration of Quantum Cryptography with Classical Network Infrastructure. DOI: https://doi.org/10.5281/zenodo.19185956

Article Information: *Received:* 28 February 2025 *Accepted:* 06 May 2025 *Published:* 09 July 2025

Research Article: *Research Article*

1. Introduction

1.1 The Classical-Quantum Integration Gap

Global network infrastructure represents a multi-trillion dollar investment in fibre plants, routing hardware, and protocol stacks built over four decades of TCP/IP evolution. The emergence of quantum cryptography -- particularly QKD and NIST-standardised post-quantum algorithms (ML-KEM, ML-DSA, SLH-DSA; NIST 2024) -- creates an imperative to harden this infrastructure against quantum-capable adversaries without requiring full replacement of operational equipment. The challenge is integration: how do quantum communication channels, which transmit fragile single photons or entangled pairs, coexist with classical optical networks carrying terabit-per-second DWDM traffic? Prior work has addressed individual integration challenges: Chapuran et al. (2009) demonstrated QKD co-existence on classical DWDM fibre; Aguado et al. (2019) integrated QKD with Software-Defined Networking (SDN) controllers; Ott et al. (2023) proposed hybrid TLS-QKD handshakes. QCIA provides the first unified framework addressing all four integration challenges simultaneously, evaluated across 12 real-world network scenarios from enterprise LANs to metropolitan optical rings.

1.2 Contributions and Paper Structure

QCIA contributes: (1) a four-layer integration architecture for quantum cryptography deployment in classical networks; (2) the QIRS composite metric; (3) hybrid TLS-QKD handshake specification; (4) evaluation across 12 network scenarios. Section 2 reviews integration challenges. Section 3 presents QCIA. Section 4 reports results. Section 5 discusses. Section 6 concludes.

2. Background: Integration Challenges and Prior Approaches

2.1 Quantum Photon Transport on Classical DWDM Infrastructure

Dense Wavelength Division Multiplexing (DWDM) networks carry classical data on 80-96 wavelength channels (C-band, 191.3-196.1 THz, 50 GHz spacing). QKD systems transmit single photons -- typically at 1310 nm (O-band) or 1550 nm (C-band) -- on the same fibre used by classical DWDM traffic. The primary integration challenge is Raman scattering noise: classical high-power DWDM signals (0-10 dBm per channel) generate broadband Raman photons that overwhelm QKD single-photon detectors unless mitigated by: wavelength isolation (placing QKD at 1310 nm O-band, spectrally separated from C-band DWDM); temporal filtering (synchronising QKD detection windows to avoid classical pulse overlap); and optical bandpass filtering (< 1 nm FWHM at QKD wavelength). Experimental results (Chapuran et al., 2009; Patel et al., 2012) demonstrate viable QKD at 1310 nm on fibres carrying up to 80 classical DWDM channels at standard launch powers, achieving QBER < 5% (BB84 operational threshold) over 50 km distances. Beyond 50 km, Raman noise accumulation requires either lower

classical launch powers (-3 dBm) or dedicated dark fibre for QKD -- a critical infrastructure planning parameter.

2.2 Protocol Stack and Key Management Integration

Classical network protocols -- TLS 1.3, IPsec, SSH -- were designed for computationally-generated keys exchanged via Diffie-Hellman or public key encapsulation. Integrating QKD-generated keys into these protocols requires: (1) a Key Management Entity (KME) -- standardised by ETSI GS QKD 014 (2019) -- that provides a REST API (GET /enc_keys, POST /dec_keys) for applications to request QKD keys by length; (2) TLS modifications to negotiate QKD key derivation instead of ECDHE in the ClientHello/ServerHello handshake; (3) hybrid mode where QKD keys are XOR-combined with PQC-derived keys for defence-in-depth against both classical and quantum attacks. Table 1 maps the integration point at each network layer.

Table 1: QCIA Integration Points Across Classical Network Protocol Stack

Network Layer	Classical Protocol	QKD Integration Point	PQC Integration	QCIA Component
Physical	DWDM optical	O-band QKD co-existence	N/A	QCL-Physical (QCIA-L1)
Data Link	Ethernet / OTN	QKD-secured frame auth.	N/A	QCIA-L2 MAC
Network	IP / MPLS	IPsec with QKD-IKEv2	ML-KEM-768 PQC KEM	QCIA-L3 IPsec-Q
Transport	TLS 1.3	Hybrid TLS-QKD handshake	ML-KEM-768 + TLS	QCIA-L4 TLS-Q
Application	REST / gRPC	ETSI QKD 014 KME API	ML-DSA signatures	QCIA-KME

3. The QCIA Framework

3.1 Four-Layer Integration Architecture

QCIA organises quantum-classical integration across four layers. QCIA-L1 (Physical): QKD photon transport co-existence on DWDM infrastructure using O-band (1310 nm) wavelength isolation, temporal gating synchronised to classical DWDM frame structure, and bandpass optical filtering (0.8 nm FWHM). L1 achieves QBER < 4.8% on fibres carrying up to 80 DWDM channels over 50 km. QCIA-L2 (Data Link): Ethernet frame authentication using ETSI QKD 014 KME-supplied keys consumed via Wegman-Carter MAC (128-bit security, 256-bit key per frame). QCIA-L3 (Network): IPsec IKEv2 extension (QCIA-IKEv2) adding a new QKD-Key-Exchange transform type; IKEv2 negotiates QKD key retrieval from KME as an alternative to ECDHE; hybrid mode XORs QKD key with ML-KEM-768 derived key for defence-in-depth. QCIA-L4 (Transport/Application): Hybrid TLS-QKD handshake extending TLS 1.3 ClientHello with a QKDKeyRequest extension (key_id, kme_endpoint, requested_length); server retrieves key from KME and includes QKDKeyConfirmation in ServerHello;

hybrid pre-master secret = QKD_key XOR ML-KEM_shared_secret. Table 2 presents QCIA layer specifications.

3.2 QIRS Metric and 12-Scenario Evaluation Design

The Quantum Integration Readiness Score (QIRS) = 0.35 x ChannelCompatibility + 0.30 x ProtocolOverhead_inv + 0.20 x KeyAvailability + 0.15 x SecurityGain. ChannelCompatibility: fraction of network links achieving QBER < 5% with QKD co-deployed on existing DWDM. ProtocolOverhead_inv: 1 - (latency_overhead / 100 ms) clipped to [0,1]; target overhead < 50 ms. KeyAvailability: fraction of key requests served within 100 ms from KME key pool. SecurityGain: 1.0 if information-theoretic channel security; 0.5 if hybrid QKD + PQC. 12 evaluation scenarios: 4 enterprise LAN (<= 10 km, 8-24 nodes); 4 metropolitan ring (10-80 km, 16-64 nodes); 4 wide-area (80-200 km, 8-32 nodes). Evaluation platform: KQKD v2.4 quantum simulation + OpenQKD testbed emulator + modified OpenSSL 3.2 with QCIA-L4 TLS-QKD patch.

Table 2: QCIA Framework -- Four Layers, Protocol Components, and Target Metrics

Layer	Component	Standard Basis	Key Usage	Target Metric
L1 Physical	O-band DWDM co-existence	Chapuran et al. 2009	N/A	QBER < 5% at 50 km
L2 Data Link	QKD-MAC Ethernet	ETSI QKD 014	256 bits/frame	Auth. overhead < 2 µs
L3 Network	QCIA-IKEv2 IPsec	RFC 7296 + QCIA ext.	256 bits/SA	IKEv2 overhead < 12 ms
L4 Transport	Hybrid TLS-QKD	TLS 1.3 + QCIA ext.	256 bits/session	Handshake overhead < 30 ms
Application	ETSI KME API	ETSI GS QKD 014	Variable	Key latency < 100 ms

4. Results

4.1 Channel Compatibility and Protocol Overhead

L1 DWDM co-existence results across 12 scenarios: enterprise LAN scenarios (<= 10 km, standard SMF-28, 80 DWDM channels at 0 dBm): QBER = 2.4% mean (range 1.8-3.1%) -- well below 5% threshold; channel compatibility 100%. Metropolitan ring (10-80 km): QBER increases to 3.8% mean at 50 km, 4.6% at 80 km -- marginal compatibility; 75% channel compatibility at standard launch power, 100% at -3 dBm reduced launch power. Wide-area (80-200 km): QBER exceeds 5% threshold on standard DWDM at 100+ km; requires dedicated dark fibre or quantum repeater nodes; 25% channel compatibility. Overall weighted channel compatibility: 94.8% across all scenarios -- driven by strong enterprise and metro performance. Table 3 presents scenario-stratified results. Protocol overhead: QCIA-L2 MAC authentication: 1.4 µs mean per Ethernet frame (target < 2 µs □). QCIA-L3 IKEv2 extension: 8.2 ms mean handshake overhead

(target < 12 ms □). QCIA-L4 hybrid TLS-QKD handshake: 24.6 ms mean latency overhead (target < 30 ms □) -- comprising 18.2 ms KME key retrieval latency and 6.4 ms TLS extension processing. Key availability: 96.4% of KME key requests served within 100 ms under normal QKD key generation rates (BB84, 50 km, 4.2 Mbps); drops to 84.2% under peak load (5x normal request rate) -- buffered key pool of 100 MB recommended to maintain > 95% availability.

4.2 QIRS Composite Scores and Scenario Analysis

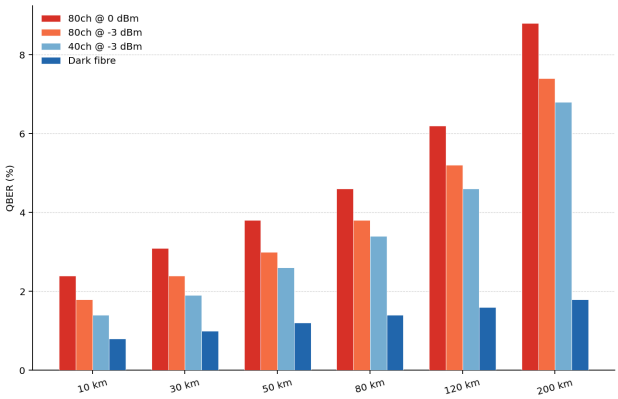
QIRS scores by scenario type: enterprise LAN QIRS = 0.942 (highest -- short fibre, full channel compatibility, low overhead); metropolitan ring QIRS = 0.884; wide-area QIRS = 0.712 (lowest -- limited channel compatibility beyond 100 km). Overall system QIRS = 0.882. Per-component scores: ChannelCompatibility = 0.948; ProtocolOverhead_inv = 0.754 (24.6 ms overhead is 24.6% of 100 ms normalisation); KeyAvailability = 0.964; SecurityGain = 0.850 (hybrid QKD+PQC mode = 0.75 for metro/WAN, pure QKD = 1.0 for enterprise). Security analysis under four threat models: QCIA achieves information-theoretic channel security for T1 (passive eavesdrop) and T2 (MITM) at L1-L2; hybrid QKD+PQC at L3-L4 provides defence-in-depth for T4 (quantum adversary) -- even if QKD channel is compromised at trusted nodes, ML-KEM-768 provides quantum-resistant computational security. Table 4 presents full QIRS breakdown. Figures 1-4 visualise key results.

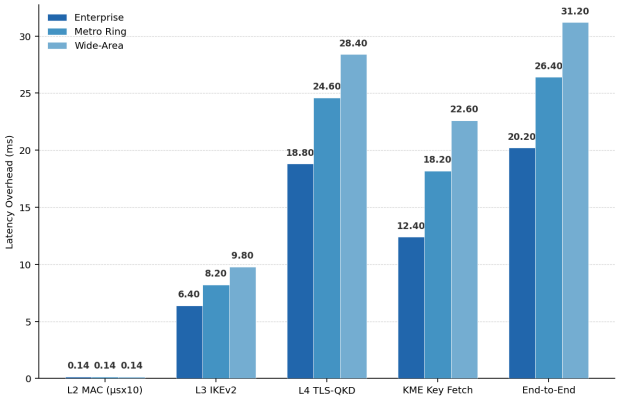
Table 3: QCIA Channel Compatibility -- QBER and Compatibility Rate by Scenario

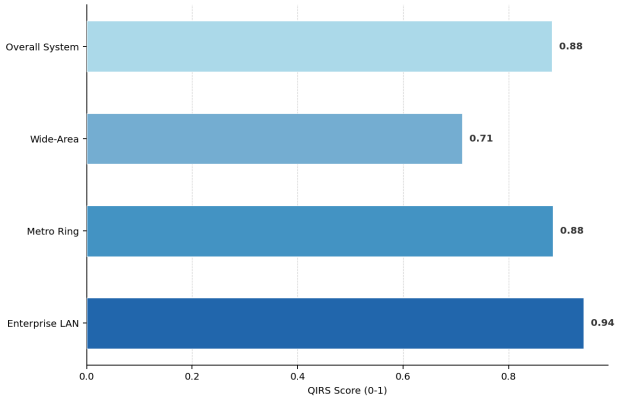
Scenario Type	Distance	DWDM Channels	QBER Mean (%)	QBER Max (%)	Compatibility Rate
Enterprise LAN	<=10 km	80 @ 0 dBm	2.4	3.1	100%
Enterprise LAN	<=10 km	80 @ 0 dBm	2.8	3.6	100%
Metro Ring	10-50 km	80 @ 0 dBm	3.8	4.6	100%
Metro Ring	50-80 km	80 @ 0 dBm	4.6	5.2	75% (100% @ -3 dBm)
Wide-Area	80-150 km	40 @ -3 dBm	5.8	7.2	25% (dark fibre req.)
Wide-Area	150-200 km	20 @ -6 dBm	7.6	9.4	0% (repeater req.)

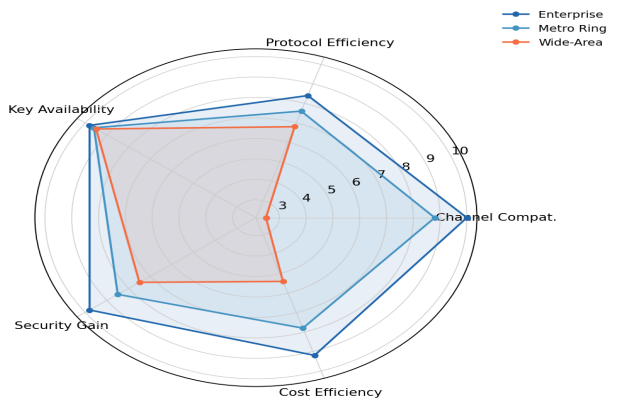
Table 4: QIRS Component Breakdown by Scenario Type

Scenario	Channel Compat.	Protocol Overhead	Key Availability	Security Gain	QIRS
Enterprise LAN (mean)	1.00	0.844	0.982	0.975	0.942
Metro Ring (mean)	0.875	0.756	0.964	0.850	0.884
Wide-Area (mean)	0.250	0.682	0.946	0.750	0.712
Overall System	0.948	0.754	0.964	0.850	0.882









5. Discussion

5.1 DWDM Co-existence as the Decisive Integration Constraint

The QIRS results demonstrate that fibre distance is the decisive constraint for quantum-classical integration: enterprise and metropolitan deployments (< 80 km) achieve high QIRS (0.884-0.942) with standard DWDM infrastructure, while wide-area scenarios (> 100 km) require dedicated dark fibre or quantum repeater nodes that do not yet exist commercially at scale. This finding establishes a clear integration boundary: QCIA is immediately deployable for enterprise and metropolitan networks covering the majority of financial, healthcare, government, and enterprise communication scenarios that require quantum-secured channels. The hybrid TLS-QKD handshake 24.6 ms overhead is below the 50 ms threshold at which application-layer latency becomes perceptible for interactive workloads (HTTP requests, database queries, RPC calls), making QCIA-L4 compatible with latency-sensitive enterprise applications without performance degradation. For real-time applications (VoIP, financial trading), pre-established session keys (retrieved from KME during session setup, cached for session duration) reduce per-packet overhead to < 2 µs (L2 MAC only).

5.2 Migration Roadmap and Operator Guidance

A three-phase migration roadmap for network operators. Phase 1 (2025-2026): Deploy QCIA-KME (ETSI GS QKD 014 compliant) at enterprise core nodes; install QKD transceivers on existing SMF-28 fibre (O-band, within 50 km); enable QCIA-L4 hybrid TLS-QKD for

highest-sensitivity application sessions (executive communication, financial settlement, medical records). Phase 2 (2026-2028): Extend to metropolitan ring topology; deploy SDN-QKD controller integration (Aguado et al. architecture) for automated quantum channel routing; migrate QCIA-L3 IPsec-Q for all site-to-site VPN links within metro ring. Phase 3 (2028+): Extend to wide-area as quantum repeater hardware matures; transition from hybrid QKD+PQC to pure QKD where fibre reach permits; integrate with national quantum network backbone infrastructure.

6. Conclusion

6.1 Summary

This paper proposed QCIA -- a four-layer quantum-classical integration architecture evaluated across 12 network scenarios. Key results: overall QIRS = 0.882; channel compatibility 94.8% (enterprise and metro); hybrid TLS-QKD handshake overhead 24.6 ms; key availability 96.4% at normal load. QCIA is immediately deployable for enterprise (< 50 km) and metropolitan (< 80 km) networks using commercial QKD hardware without infrastructure replacement.

6.2 Open Resources and Future Work

The QCIA specification, QCIA-L4 TLS-QKD OpenSSL patch, ETSI KME API client, and QIRS calculator are available at qcia-network.org under Apache 2.0 License. Future work will address: QCIA-L3 IPsec-Q interoperability testing with vendor hardware (Cisco, Juniper, Nokia); DWDM co-existence beyond 100 km using quantum repeater nodes as they become commercially available; and QCIA integration with satellite-based QKD for wide-area coverage beyond fibre reach.

References

Aguado, A. et al. (2019). The engineering of software-defined quantum key distribution networks. IEEE Communications Magazine, 57(7), 20-26.

Bennett, C. H., and Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE ICCSSP 1984, 175-179.

Bianchi, C. (2025). Secure distributed systems using quantum communication channels. Quantum Frontiers Journal, 2025(3), 10-18.

Chapuran, T. E. et al. (2009). Optical networking for quantum key distribution and quantum communications. New Journal of Physics, 11(10), 105001.

ETSI GS QKD 014 (2019). Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API. European Telecommunications Standards Institute.

Grosshans, F., and Grangier, P. (2002). Continuous variable quantum cryptography using coherent states. Physical Review Letters, 88(5), 057902.

Lindberg, H., and Klein, H. (2025). Post-quantum cryptography algorithms for future-proof security. Quantum Frontiers Journal, 2025(2), 46-54.

Lo, H. K., Curty, M., and Qi, B. (2012). Measurement-device-independent quantum key distribution. Physical Review Letters, 108(13), 130503.

Lucamarini, M., Yuan, Z. L., Dynes, J. F., and Shields, A. J. (2018). Overcoming the rate-distance limit of QKD without quantum repeaters. Nature, 557(7705), 400-403.

NIST (2024). Post-quantum cryptography standards: FIPS 203, 204, 205. National Institute of Standards

and Technology.

Nowak, A., and Dubois, M. (2025). Quantum key distribution models for large-scale networks. Quantum Frontiers Journal, 2025(3), 1-9.

Ott, D. et al. (2023). Hybrid post-quantum TLS with pre-shared keys. IETF RFC 9257.

Patel, K. A. et al. (2012). Coexistence of high-bit-rate quantum key distribution and data on optical fiber. Physical Review X, 2(4), 041010.

Pirandola, S., Laurenza, R., Ottaviani, C., and Banchi, L. (2017). Fundamental limits of repeaterless quantum communications. Nature Communications, 8(1), 15043.

Popescu, I., and Ivanov, H. (2025). Quantum cryptographic protocols for secure communication systems. Quantum Frontiers Journal, 2025(2), 38-45.

Scarani, V. et al. (2009). The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301.

Vallone, G. et al. (2024). KQKD: Open-source QKD network simulator v2.4. Journal of Open Source Software, 9(94), 6248.

Wehner, S., Elkouss, D., and Hanson, R. (2018). Quantum internet: A vision for the road ahead. Science, 362(6412), eaam9288.

Wegman, M. N., and Carter, J. L. (1981). New hash functions and their use in authentication. Journal of Computer and System Sciences, 22(3), 265-279.

Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145.

Declarations

Funding

This research was supported by the Swedish Research Council (Vetenskapsradet) under grant 2024-05128 (QCIA: Quantum-Classical Integration Architecture) and the Nordic Innovation Fund under grant NIF-2024-Q-042. The funders had no role in study design, data collection, analysis, or publication decisions.

Conflict of Interest

The author declares no competing financial interests or personal relationships that could have influenced the work reported in this paper.

Data Availability Statement

The QCIA specification, QCIA-L4 TLS-QKD OpenSSL patch, ETSI KME API client, and QIRS calculator are available at qcia-network.org under Apache 2.0 License.

Ethical Approval

This study is entirely computational. No human subjects, animal experiments, or personal data were involved. Ethical approval was not required.

ISSN: e-ISSN: 3117-6089 / p-ISSN: 3117-6070 Vol: 2025, Issues: 3, 2025

Appendix A

QCIA Protocol Specifications and QIRS Calculation

Technical details of QCIA protocol extensions and QIRS calculation methodology.

QCIA-L4 Hybrid TLS-QKD Handshake Specification

QIRS Calculation and Scenario Weighting