Measurement 278 (2026) 121738

Contents lists available at ScienceDirect

Measurement

journal homepage: www.elsevier.com/locate/measurement

Quantum-secured distributed measurement systems for critical infrastructures operations

Leopoldo Angrisani, Mauro D'Arco *, Matteo D'Iorio, Fabrizio Lo Regio

University of Naples Federico II - Department of Information Technology and Electrical Engineering, Naples, Italy

ARTICLE INFO

Keywords:
Distributed measurement system
Quantum cryptography
Quantum key distribution
Critical infrastructures
Secure communication
Quantum network

ABSTRACT

In the context of homeland security, protecting critical infrastructures (CIs) is paramount, given emerging threats that exploit cyber–physical systems and quantum computers. As CIs rely on distributed measurement systems (DMSs), they require stringent security protocols for remote transmission of commands and measurement results. This paper proposes a novel architectural paradigm for DMSs that integrate quantum key distribution (QKD) to ensure information-theoretic security (ITS). Specifically, a hardware-agnostic architecture is introduced to reconcile quantum cryptography with industrial applications, addressing the conceptual and systemic integration of quantum technologies with DMSs. The proposed solution decouples metrological logic from hardware, facilitating a secure interface between QKD layers and measurement nodes. Two key management modalities, client-initiated and server-initiated, are proposed to address diverse operational requirements; the former minimizes latency, while the latter ensures superior synchronization. Experimental validation is provided by leveraging the facilities of a quantum metropolitan area network (QMAN) that is currently under deployment. The characterization reveals that the proposed architecture effectively reconciles the stochastic, low-throughput nature of QKD with DMSs demands. The system demonstrates operational autonomy, maintaining data integrity during QKD outages. Finally, this work establishes a trajectory from hybrid models toward quantum-resistant networks for CIs.

1. Introduction

Protecting critical infrastructures (CIs), such as power grids and telecommunication networks, is becoming fundamental for modern homeland security [1]. While once optimized for operational efficiency, the contemporary geopolitical instability has effectively shifted attention toward systemic vulnerabilities of CIs [2]. To manage dispersed assets, distributed measurement systems (DMSs) become indispensable [3] for the coordinated acquisition and management of measurement data and control commands through multiple interconnected nodes [4], addressing the growing complexity of large-scale industrial and infrastructural applications. Such systems increasingly mirror the evolution of decentralized and cooperative systems in terms of node coordination and integrity [5,6]. While improving scalability and accessibility, these architectures also introduce significant vulnerabilities [7].

As CIs integrity is contingent upon the DMSs, the latter expands the system attack surface, exposing assets to sabotage, service disruption, and unauthorized access [8]. Recent cyberattacks, such as the 2016 *Industroyer* power outages in Ukraine [9] and the 2017 *TRITON* attack on petrochemical safety systems [10], highlight the physical risks of such exploits. This challenge is further exacerbated in the emerging era of quantum computing, where the classical cryptographic schemes face potential obsolescence and increasing vulnerability [11].

Within this evolving threat landscape, quantum key distribution (QKD) has emerged as a cornerstone technology for unconditionally secure communications [12]. Unlike traditional computational methods, QKD relies on quantum mechanics to ensure secrecy and detect eavesdropping [13]. By leveraging quantum-derived keys, DMSs can evolve into resilient networks capable of withstanding quantum-capable adversaries. Despite the experimental validation of point-to-point QKD [14], quantum facilities remain largely decoupled from the functional management of critical systems.

A prevailing limitation is the tendency to evaluate quantum security in isolation, focusing on data transport while neglecting the stringent real-time constraints of measurement instrumentation and operational efficiency [15,16]. Furthermore, the architectural divide between proprietary quantum facilities and the heterogeneous environments of industrial monitoring has prevented a comprehensive paradigm for QKD-enabled DMSs. The absence of a framework thus represents a significant barrier to the deployment of quantum-secured measurement

* Corresponding author.
E-mail address: darco@unina.it (M. D'Arco).

https://doi.org/10.1016/j.measurement.2026.121738
Received 23 February 2026; Received in revised form 13 April 2026; Accepted 30 April 2026
Available online 5 May 2026

systems in mission-critical environments. Bridging this gap requires an architectural design in which security does not undermine the operational efficacy that defines the functional integrity of the measurement process; as the integration of quantum security may introduce overhead and delays that potentially degrade system performance [17].

While significant research has focused on enhancing QKD physical-layer metrics, such as secret key rates and detector efficiency [18,19], the functional integration of these technologies into the operational logic of DMS remains significantly underdeveloped. Such advancements, although foundational to the evolution of quantum networks, frequently treat the application layer as a passive data recipient, often overlooking the stringent operational constraints and real-time requirements of industrial environments [20,21]. Based on these considerations, this work proposes a novel architecture that integrates quantum communication facilities directly into the monitoring and control of DMSs for critical infrastructures. This work shifts the focus from quantum-layer optimization toward the practical interoperability of commercial quantum devices with legacy industrial software infrastructures. The framework ensures the integrity of data and configuration commands. The system's efficacy was validated via a secure link within a quantum metropolitan area network (QMAN) prototype [22], serving as a real-world urban testbed for real-time quantum-secured metrology. The innovative contribution of this paper is multifaceted:

1. Integration paradigm: A framework for integrating QKD into DMSs, protecting sensitive measurement data and control logic is defined.
2. Hardware-agnostic architecture: An architecture that decouples application logic from the quantum hardware, ensuring interoperability across heterogeneous networks, is proposed.
3. Security-oriented implementation: It is shown how control software commonly used in industrial environments (LabVIEW) can interface with quantum cryptographic engines to gain quantum-level security.
4. Validation: Communication and key retrieval latencies affecting the prototype of a QMAN are evaluated to confirm the viability of real-time monitoring.

The paper is organized as follows: Section 2 covers theoretical foundations; Section 3 details the proposed architecture and implementation; Section 4 presents the experimental case study via QMAN; in Section 5 the results are described in detail; Section 7 summarizes findings and future research directions.

2. Background

2.1. Distributed measurement systems (DMS)

DMSs are measurement systems in which sensing, acquisition, and processing functionalities are deployed across interconnected, geographically separated nodes. DMSs have become indispensable for the management of CIs, providing the foundational sensory layer essential for the continuous oversight of assets vital to public safety and economic stability [23]. Practical applications of DMSs are in smart grids, where they facilitate energy management [24], in train and subway control systems, where they ensure safe and efficient operation by automating spacing, speed, and braking, in urban drainage systems, where they are employed in conjunction with real-time hydraulic modeling to mitigate flood risks [25].

Typically adopting a client–server paradigm, DMSs rely on centralized nodes for task coordination, instrumentation control, and data aggregation [26]. In typical deployments, measurement commands and results are exchanged over classical communication channels using TCP/IP-based protocols [27]. While this model ensures interoperability, it introduces heavy dependencies on the underlying network. For CIs, these dependencies represent a mission-critical vulnerability, where latency, reliability, and security are paramount.

As modern DMSs increasingly leverage heterogeneous and potentially untrusted infrastructures, safeguarding communication against interception, manipulation, or replay attacks is a prerequisite for preventing sabotage of physical assets [28]. While transport layer security (TLS) serves as the de facto standard [29], its reliance on computational hardness assumptions, such as integer factorization, faces an existential threat from quantum computing [30]. Specifically, it is theoretically demonstrated that Shor's algorithm allows for large integers factorization in polynomial time, rendering ubiquitous asymmetric schemes, including RSA and elliptic curve cryptography, obsolete [31]. In fact, while the decryption of a standard 2048-bit RSA key would necessitate millions of years of classical computation, a quantum computer could theoretically need only some hours [32].

2.2. Quantum key distribution (QKD)

While symmetric encryption remains comparatively robust against quantum algorithms, sustaining only a quadratic vulnerability to Grover's algorithm, secure distribution of symmetric keys remains a critical bottleneck [33]. In this landscape, QKD provides information-theoretic security (ITS) between two trusted users [34], enabling the establishment of a shared secret key. Unlike classical public-key cryptography, which relies on the unproven computational hardness of mathematical problems, QKD is grounded in the fundamental laws of physics [35]. Consequently, the secrecy of keys is ensured even if the assumptions protecting the authentication layer are compromised, providing security regardless of adversary computing power.

The most established framework for QKD implementation is the BB84 protocol [36]. The process involves a transmitter (Alice) and a receiver (Bob) connected by a quantum channel for state transmission, e.g., optical fiber, and an authenticated classical channel for post-processing, as illustrated in Fig. 1(a). Using single photons as information carriers, Alice encodes each bit of a raw key by modulating their polarization states [37]. Security derives from non-orthogonal states grouped into two conjugate bases: the rectilinear (computational) basis $\{|0\rangle, |1\rangle\}$, and the diagonal basis $\{|+\rangle, |-\rangle\}$.[1] The encoding scheme is visualized in Fig. 1(b), which maps binary values to specific polarization orientations. Mathematically, these states are formalized as two-dimensional unit vectors within a Hilbert space, as in Eq. (1).

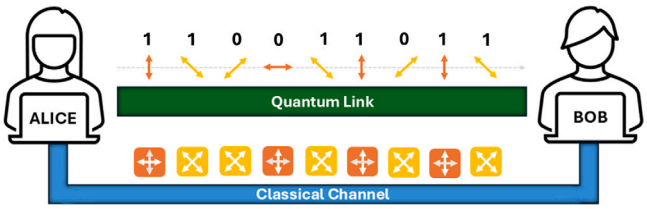
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, |+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \tag{1}$$

For each bit, Alice randomly chooses a basis to polarize the photon. Upon transmission over the quantum channel, Bob, lacking prior knowledge of Alice's encoding bases, randomly and independently selects his measurement basis for each photon; therefore, Bob chooses the correct basis 50% of the time [39]. Due to the measurement paradox of quantum mechanics, according to which the act of measuring forces the state of the photon into one of those of the adopted measurement basis, all measurements using the same basis as Alice retrieve the bits, while the results are purely probabilistic otherwise.

Security against an eavesdropper (Eve) is predicated on her lack of knowledge regarding Alice's bases. By measuring each photon with a random basis, Eve irreversibly perturbs the state whenever she selects the wrong basis, which occurs with 50% probability. To avoid detection, Eve must then resend a photon to Bob, prepared in her own basis. The no-cloning theorem prevents Eve from duplicating the original state [40]; thus, even if Bob measures using Alice's basis, a 25% error rate is introduced.

After quantum transmission, Alice and Bob perform basis reconciliation over the classical channel, disclosing the basis for each photon. Only bits where bases coincided are retained. The quantum bit error

[1] While standard BB84 uses four states, practical industrial implementations often employ the three-state BB84 protocol [38].



a)

Basis	Bit	Photon's polarization
Rectangular	0	
	1	
Diagonal	0	
	1	

b)

Fig. 1. Graphical representation of the two-state BB84 protocol: (a) Alice and Bob exchange polarized states across a quantum link and auxiliary information across the classical channel; (b) Basis and corresponding polarization states.

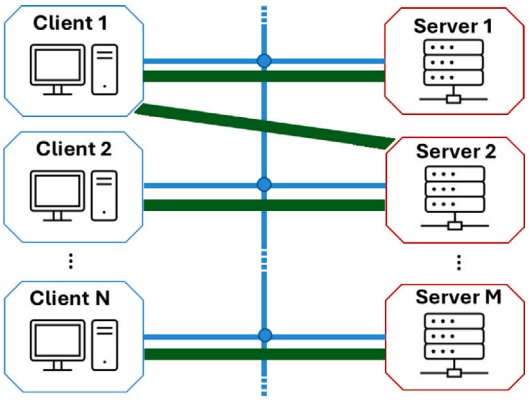


Fig. 2. Schematic representation of the proposed M2M network architecture for a QKD-secured DMS, in which the connectivity between N client nodes and M server nodes is via a quantum link (green), for the QKD, and a classical channel (blue), for data transmission and post-processing.

rate (QBER) [41], defined as the ratio between the number of erroneous bits and the total number of detected bits in the sifted key, is compared with a theoretical threshold, typically 11% [42]. Since the final key is still affected by channel noise, hardware imperfections, and potential eavesdropping [43], if the measured QBER exceeds this threshold, the parties abort the process [44]. Finally, error correction and privacy amplification are applied to reconcile discrepancies while minimizing information leakage [45].

3. Proposed architecture for a QKD-secured distributed measurement system

3.1. Network topology and security assumptions

The proposed DMS leverages a client–server multipoint-to-multipoint (M2M) architecture consisting of N clients and M servers, as depicted in Fig. 2. In this configuration, each client accesses multiple servers to retrieve specific measurement assets, while servers host a suite of measurement instruments, designed to handle concurrent or sequential requests. This topology facilitates shared access to dispersed assets via a dual-channel physical layer:

- Classical channel: A standard TCP/IP connection for transmitting encrypted commands, measurement results, and QKD post-processing data [46].
- Quantum link: A dedicated physical path (fiber-optic or free-space) reserved exclusively for non-orthogonal single-photon states in QKD.

The system primarily adopts a star topology, where a central server maintains concurrent QKD sessions with clients. Since quantum links are inherently limited to point-to-point connections, achieving M2M connectivity into a scalable QKD architecture over extended distances remains a primary architectural challenge.

To circumvent the point-to-point limitations of quantum links and facilitate wide-area connectivity, several paradigms have been explored. While advanced quantum-coherent relaying solutions represent the long-term theoretical objective [47], their current technological immaturity renders trusted relays the definitive state-of-the-art for practical implementation [48]. Accordingly, the proposed framework implements a hop-by-hop key forwarding mechanism. In this configuration, intermediate nodes bridge distant terminals through sequential cryptographic operations; specifically, these relays utilize locally generated link keys to encapsulate and transmit end-to-end cryptographic material, typically via XOR-based encryption [49].

To sustain scalability and mitigate topological complexity, an external controller that manages the infrastructure nodes is essential. This higher-level entity provides the coordination required for a broad functional spectrum, integrating dynamic path computation with seamless temporal synchronization across the network.

This operational model necessitates the trusted node assumption for intermediate relays, where quantum links provide immunity to remote interception, and end-to-end security remains contingent upon the physical integrity of the central hub and relay facilities. Within this framework, a physical breach of these nodes would compromise cryptographic material in the clear. Consequently, the cumulative attack surface grows proportionally with the number of nodes. Beyond node security, the architecture is evaluated against an untrusted channel assumption, positing an adversary (Eve) with full access to the communication medium. This adversarial model encompasses both passive eavesdropping and active quantum-layer interventions, such as intercept-and-resend attacks [50]. To mitigate these threats, the framework decouples key generation from data transmission, leveraging the quantum layer for ITS and eavesdropping detection. Within this model, active attacks on the classical channel, notably Man-in-the-Middle (MitM), are addressed by assuming an authenticated public medium, ensuring that key distillation occurs exclusively between verified identities [51]. Furthermore, the model accounts for Denial-of-Service (DoS) risks, specifically physical fiber tampering to inflate the QBER and classical traffic saturation. While QKD cannot prevent service interruption, its integration into the DMS can effectively neutralize command injection and replay attacks by anchoring the application layer to unique, high-rate cryptographic material.

3.2. Node roles and hardware

A strategic design choice in the proposed architecture concerns the assignment of Alice and Bob roles across the network, implementing an economically scalable asymmetric topology where clients operate as Alice and servers as Bob. While Alice leverages cost-effective, room-temperature components, Bob can require high-performance single-photon detectors (SPD). While several detector technologies exist, superconducting nanowire SPD (SNSPD) operated at cryogenic temperatures emerge as a promising solution due to their detection efficiency and low timing jitter. Centralizing complex cryogenic infrastructure at the M servers while deploying simplified transmitters at the N client nodes effectively amortizes overhead across the entire DMS. Despite distinct roles within the topology, every node, whether client or server, shares a uniform modular architecture comprising two functional blocks:

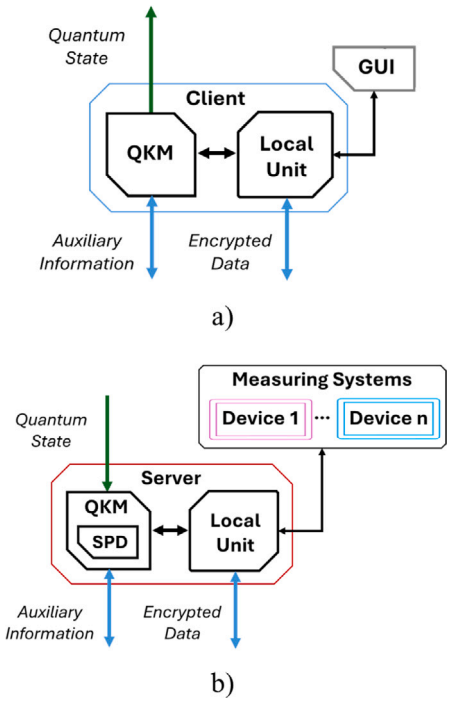


Fig. 3. Nodes hardware: (a) Client node (Alice) features a QKM, a local unit for remote control, and a graphical user interface (GUI) to access instrumentation and define measurement instructions; (b) Server node (Bob) acts as a centralized hub interfaced with measuring instruments and with a QKM consisting in single photon detectors. The quantum link (green) and the classical channel (blue) follow Fig. 2.

- **Local unit:** The node's application layer. In a server, it interfaces directly with measurement instrumentation; in a client, it functions as the remote control unit.
- **Quantum key manager (QKM):** The cryptographic driver responsible for the QKD protocol. In any link, a pair of QKMs (Alice and Bob) establishes a secret key between the local units.

Fig. 3 depicts the hardware, highlighting the simplified client transmitter and the server receiver equipped with the cryogenic SPD module.

3.3. Key management

The proposed architecture is designed to be agnostic to the underlying key retrieval logic, supporting two operational modes depending on the specific requirements of the measurement task:

1. On-demand retrieval: A QKD session is triggered by a measurement request. While ensuring freshly distilled keys, it introduces the measurement process to the inherent latency during the quantum post-processing phase.
2. Buffered generation: QKD activity runs as an autonomous background process continuously populating the key buffers with identical secret keys and the corresponding key IDs. QKMs at both endpoints are provided with local buffers. Key IDs act as unique pointers, ensuring endpoint synchronicity.

From a hardware perspective, it is important to clarify that Bob must remain operational constantly, independently of the chosen paradigm. This is due to the protracted time needed for both to reach the stable cryogenic temperature required by the SNSPDs [52] and for base alignment [53]. On-demand mode strictly concerns the logical orchestration of the quantum channel, where the server employs optical switches to multiplex specific Alice nodes.

Regardless of the retrieval mode, there is an intrinsic asymmetry of the QKD network due to the M2M topology, where multiple client nodes (Alice) contend for the limited resources of a centralized server (Bob). Therefore, the operational management of the keys between the N clients and M servers is critical. With this aim, two distinct key management paradigms are proposed, which govern both the initiation of the QKD protocol (in on-demand mode) and the retrieval of keys (in buffered mode).

- Client-initiated paradigm: In buffered mode, the client fetches a key ID from its buffer and dispatches the encrypted payload with it. In on-demand mode, the client's request triggers a new QKD session. However, concurrent requests in single-link architectures [48] may lead to collisions and buffer exhaustion.
- Server-initiated paradigm: In on-demand mode, the server evaluates the state of quantum links, prioritizing mission-critical nodes. In buffered mode, the server dictates the key ID and timing. This ensures specific users or time-critical instruments are never stalled by secondary traffic.

3.4. System implementation

The proposed implementation is developed as a LabVIEW application that serves as the primary engine for managing QKM buffer interactions, classical communication, and instrumentation control [54]. The architecture is deployed on a Linux-based laptop with LabVIEW 2024 and Python 3.11. A modular architecture based on software drivers, called virtual instruments (VIs), is employed: server-side VIs handle automatic test equipment (ATE) settings and queries, while client-side VIs facilitate data collection, processing, and visualization.

Software drivers invoke validated services available through a high-level application programming interface (API) for executing manufacturer-specific terminal instructions. The API structure is organized into three functional domains: (i) QKD Management, which handles key retrieval through a Command Line Interface wrapper invoked via the *System Exec* VI; (ii) Cryptographic Service executing cryptographic protocols by leveraging the LabVIEW *Python node*, which integrates external encryption libraries; and (iii) Instrument Control, which interfaces with the ATE by mapping high-level user commands to specific physical measurement operations. Transitioning from legacy drivers to these validated services ensures full interoperability across heterogeneous vendors without redesigning core measurement routines. Decoupling the measurement application from the underlying quantum infrastructure renders the architecture agnostic to the deployed quantum link and the QKD instrumentation. This allows the system to retrieve quantum keys without direct interaction with the physical layer.

Supporting both buffered and on-demand modes, the QKM allows for either continuous key generation or discrete hardware triggers without impacting measurement performance. The data exchange process is described below.[2]

1. Instruction input: Through a client-side GUI, the user selects the target instrumentation and defines measurement parameters. Upon submission, data handling and security protocols operate autonomously in the background.
2. Encryption and transmission: The client invokes the QKD Management to retrieve a key/ID pair. To ensure robustness, the Cryptographic Service executes the Advanced Encryption Standard (AES-256) via a Python-based script [55]. The LabVIEW Python node achieves interoperability between industrial logic and cryptographic libraries. Encrypted instructions and the plaintext key ID are dispatched over the TCP/IP channel.

[2] While the sequence details client-initiated buffered key management, the structure remains identical for the server-initiated paradigm.

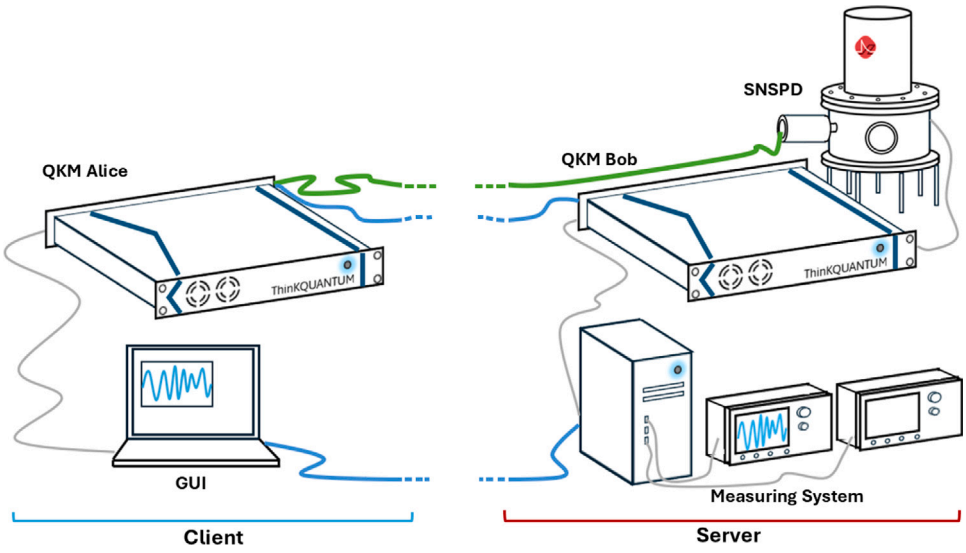


Fig. 4. Architectural layout of the proposed distributed measurement system (DMS) employing a client–server paradigm secured via quantum key distribution (QKD). The system features: an Alice quantum key manager (QKM) at the client node for control based on graphical user interface (GUI); a Bob QKM at the server node, interfaced with superconducting nanowire single-photon detectors (SNSPDs) and the automated test equipment (ATE).

Table 1
Latency in terms of mean value and standard deviation (s) for operation-specific processes of QKD and for the overall system architectures, according to client-initiated and server-initiated paradigms.

Metric	Operation-specific				Overall architecture	
	Key acquisition	*Key retrieval*	*Encryption*	*Decryption*	*Client-initiated*	*Server-initiated*
Mean value (s)	0.06	0.10	1.34	1.34	2.87	3.26
Std (s)	0.02	0.06	0.21	0.21	0.54	0.27

3. Decryption and measurement: The server uses the received ID to fetch the matching key from its buffer via the QKD Management. It decrypts the payload through the Cryptographic Service and routes the commands to the target hardware via the Instrument Control.
4. Data transmission: The acquired measurement data is encrypted by the server and transmitted back to the client. The client retrieves the decryption key, unlocks the payload, and renders the results.

4. Case study

The QKMs leverage commercial platforms by ThinkQuantum S.r.l. [56], implementing a three-state BB84 protocol, integrating SNSPDs [57,58]. While ThinkQuantum systems typically feature embedded detection, the proposed setup integrates external SNSPDs from Photec [57, 58]. The hardware and the corresponding logical interconnections between the control interface, the quantum layer, and the measurement instrumentation are depicted in Fig. 4.

The proposed architecture is tailored for its integration into the 3-node quantum metropolitan area network (QMAN) currently being deployed across the city of Naples in the south of Italy. While the full QMAN fiber backbone is undergoing final deployment, the implementation of the proposed system was conducted using a dedicated optical fiber link and optical attenuators to emulate the signal loss characteristic of the network's planned 25 km span. This configuration accurately reproduces an attenuation of 15 dB, which serves as a benchmark for typical metropolitan-scale fiber deployments [58].

Experimental evaluation focuses on communication latency and key acquisition time. This case study benchmarks a single 256-bit cryptographic key per transaction, ensuring information-theoretic security, currently achievable for symmetric encryption, and future-proofing the system against quantum brute-force attempts [34]. A Tektronix TDS220 digital real-time oscilloscope configured as the ATE was interfaced via GPIB to the server node. The client issued remote commands to modulate instrument parameters and query status updates. The measurement task involved complex waveform transfers, requiring sequential orchestration of vertical scaling, time-base triggering, and high-volume data block acquisition.

5. Results

5.1. On-demand QKD benchmarks

To benchmark the on-demand network, performance metrics from the QMAN infrastructure are considered [58]. Under 15-dB loss, the system yields a secret key rate (SKR) of 5000 ± 1000 bit/s. While SKR measures the average secure throughput, it masks the operational latency of the distillation phase. Unlike bit-by-bit generation, QKD produces keys in discrete batches; ensuring cryptographic security and accurate error rate estimation requires large sifted blocks, rendering this block-oriented processing a fundamental bottleneck.

In operational scenarios, a 500-kbit block is used as a compromise to balance security and speed [59]. However, the accumulation time is substantial; initial alignment can delay key production by up to six minutes [60]. Consequently, an on-demand request for a single 256-bit AES key incurs operational delays in contrast with the real-time demands of CIs. Even under optimized steady-state conditions, where latency may drop to approximately 10 s [59–61], such latency remains prohibitive. Moreover, rapid request bursts can deplete available keys, triggering service outages [62].

Beyond latency, the on-demand paradigm suffers from stochastic outages caused by polarization realignment or environmental noise, which can drive the QBER above security thresholds and halt distribution [63]. Such outage intervals, lasting up to 10 min [58,64], result in the total suspension of secure communication.

5.2. Validation of QKD-buffered architecture

Building upon the on-demand baseline, this section evaluates the experimental performance of the buffered architecture. A continuous generation strategy with localized buffers is crucial for bridging the discrepancy between the stochastic SKR inherent to QKD and the high-throughput DMS demands. By decoupling key production from consumption, the network sustains simultaneous measurement links while nursing seamless continuity during the realignment phases or link failures.

Table 1 quantifies the temporal performance of the proposed system, providing a granular breakdown of cryptographic overhead and total latency (T_{meas}), which encompasses the end-to-end transaction from hardware interfacing to data management.

While logical sequences remain consistent, node responsibilities shift between paradigms: the client initiates acquisition in the client-led configuration, whereas the server orchestrates key selection in the server-led model. Data indicates that "Key retrieval via ID" incurs higher latency than "Acquisition", as the former requires targeted database lookups to synchronize specific key material across nodes, whereas the latter merely fetches the next available entropy block. Encryption and decryption latencies, accounting for approximately 93% of the total budget, stem from the LabVIEW Python node rather than the intrinsic algorithmic complexity or key delivery constraints. This software-bound bottleneck was a deliberate trade-off necessitated by the Linux-based QMAN infrastructure, where native LabVIEW cryptographic toolkits are either unsupported or exhibit suboptimal stability. Crucially, this modular architecture prioritizes a hardware-agnostic and flexible integration paradigm, where the framework remains extensible to emerging standards. While low-level optimizations could drastically reduce these latencies, the current implementation successfully validates the functional synergy and real-time viability of quantum-secured DMS within legacy industrial environments. Beyond software-specific constraints, the buffered QKD overhead is functionally commensurate with 2048-bit RSA handshake latencies. By substituting computationally intensive sparse asymmetric spaces with dense symmetric keys, the architecture optimizes throughput, proving that quantum-secure integration remains performance-competitive with prevailing classical industrial benchmarks.

The results highlight a performance trade-off between the two paradigms: the client-initiated architecture is the preferred choice for time-sensitive applications due to faster mean execution times. Conversely, the server-initiated paradigm exhibits a higher total mean execution time and lower standard deviation, enhancing stability.

5.3. Comparative overhead analysis

From a practical standpoint, the key buffer functions as a reservoir where QKD-driven replenishment competes with task-driven depletion. It is updated each time a QKD cycle successfully completes. A core aspect is the system's ability to maintain operational continuity even during QKD failures or other disruptions. Performance depends on the equilibrium between the generation rate, governed by the SKR, and the consumption rate, determined by the latency T_{meas} and the number of operational demands N_{op}. The dynamics of this reservoir follow a first-order deterministic rate-balance model, consistent with the resource management principles [65][3]. Specifically, the buffer state $N(t)$, for keys of n bit, is governed by:

$$\frac{dN}{dt} = \frac{SKR}{n}(1-\alpha) - \frac{N_{op}}{T_{meas}} \tag{2}$$

subject to $0 \le N \le N_{max}$, where $\alpha \in \{0,1\}$ is a binary variable representing the QKD link status ($\alpha = 1$ during outages or realignment). Given the SKR and T_{meas} values from Sections 5.1 and 5.2, for $n = 256$ bits, the buffer surplus ensures up to 9.3 h of autonomous operation during QKD outages. However, optimized T_{meas} values could reach the millisecond range, while DMSs for CIs may impose significantly higher N_{op} values requested by a single client.

Varying T_{meas} and N_{op} reveals the transition from software-limited to physics-limited regimes. As N_{op} increases or T_{meas} decreases, buffer depletion accelerates. This dynamic is illustrated in Fig. 5, which plots system resilience against measurement duration. This multivariate sensitivity analysis demonstrates how the architectural logic sustains operational integrity across diverse scenarios. Assuming a buffer capacity defined by a 60-second accumulation window, each client–server transaction consumes a single 256-bit key. For the experimental baseline ($N_{op} = 1$, $T_{meas} = 2.87$ s), resilience time exceeds 500 min, represented by the black dot, far surpassing the 17-minute maintenance window represented by the red dashed line. Even under high concurrency ($N_{op} = 50$), the architecture withstands typical QKD realignments provided T_{meas} is sufficiently high to moderate consumption. While resilience scales linearly with the measurement interval, ultra-low-latency ($T_{meas} < 100$ ms) or high-demand ($N_{op} > 50$) scenarios may reach a threshold where consumption outpaces generation. Such regimes necessitate either an SKR upgrade or dynamic key-recycling policies to maintain operational integrity.

6. Limitations and discussion

The proposed framework, while demonstrating the viability of QKD-secured distributed measurement, is subject to specific constraints that must be addressed for large-scale industrial adoption. A primary consideration is the hybrid nature of the security model discussed in Section 3. Although QKD provides information-theoretic security for key generation, the protocol remains dependent on classical authenticated channel for post-processing and basis reconciliation. If the authentication layer is compromised, the entire QKD session becomes vulnerable to MitM attacks, highlighting a persistent reliance on classical cryptographic primitives for identity verification. Crucially, since quantum-derived encryption is applied to data only post acquisition, the physical measurement process itself remains unaffected. Therefore, the cryptographic layer does not affect raw data acquisition.

As highlighted in Section 5.2, the primary challenge instead involves maintaining the temporal integrity and synchronization of the DMS. In a single client–server scenario, where the client transmits instructions as a single command block, latency manifests solely as an initial communication delay and in the transmission of measurement results. Since the sequence is orchestrated internally, QKD-induced overhead does not affect measurement accuracy. In contrast, coordinated measurement tasks involving multiple spatially distributed nodes face significant challenges. In these scenarios, the latency inherent in cryptographic operations can adversely affect network synchronization. Specifically, QKD can introduce unpredictable jitter consistent with other cryptographic systems, directly affecting the distributed measurement. Should an encrypted trigger fail to reach its target within a preallocated window, the resulting phase mismatch would compromise the metrological characterization in time-triggered architectures. This shifts the fundamental problem from data security to the temporal stability of the system.

Furthermore, practical deployment obstacles remain for real-world critical infrastructures. As emphasized in Section 3, the requirement for cryogenic infrastructure introduces substantial costs and maintenance overhead. The physics-limited regimes explored in Section 5 demonstrate that as the system scales or demand (N_{op}) increases, the equilibrium between key generation and consumption becomes precarious. While the proposed hardware-agnostic architecture facilitates interoperability, the transition to a fully decentralized quantum network

[3] While stochastic processes or queuing theory could provide a more granular characterization of SKR jitter, the employed first-order deterministic approach effectively captures the dynamics [66,67].

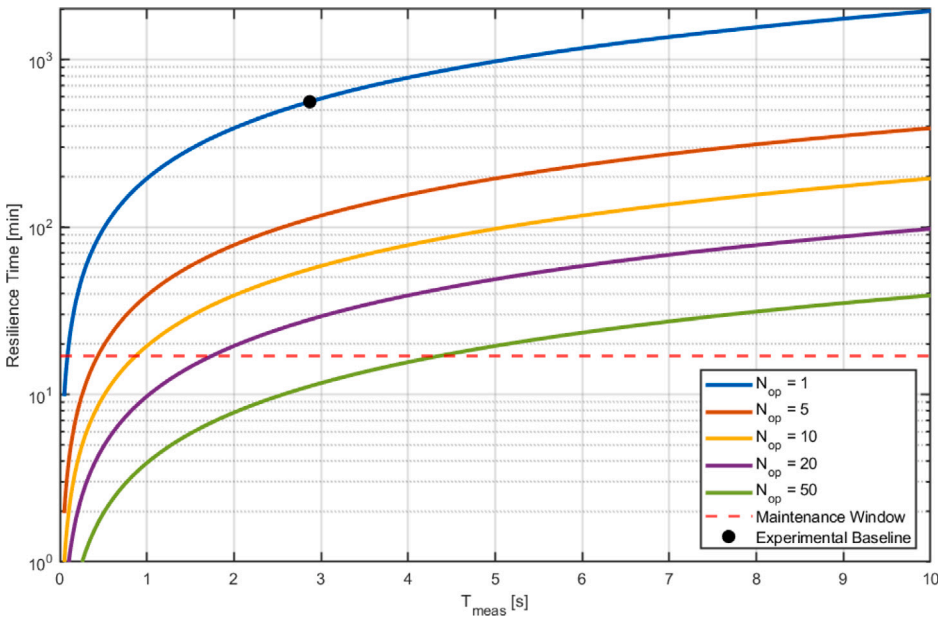


Fig. 5. System resilience time (min) during a QKD outage as a function of measurement task duration (T_{meas}) for various concurrent operational demands (N_{op}). The black marker denotes the experimental baseline (N_{op} = 1, T_{meas} = 2.87 s), which yields a survival time exceeding 500 min. The horizontal red dashed line represents the 17-minute QKD maintenance window benchmark for the adopted QMAN.

remains hindered by current hardware limits. Consequently, adoption in mission-critical environments necessitates a strategic trade-off, ensuring that maximum security does not undermine the synchronization and reliability of the measurement process.

7. Conclusion

This work presents a hardware-agnostic system for DMS secured by QKD, specifically engineered to address the systemic vulnerabilities of critical infrastructures. The proposed architecture successfully reconciles the functional requirements of industrial monitoring with the stringent demands of ITS. In an era where the functional integrity of utility and telecommunication networks is increasingly threatened by cyber–physical attacks, the proposed framework secures both sensitive measurement results and remote control commands. By decoupling high-level industrial logic from the quantum physical layer, architectural resilience and interoperability across heterogeneous hardware are ensured. The synthesis of this research highlights a fundamental architectural trade-off: while the modular, software-based integration of industrial software drivers and Python-driven cryptographic engines ensures high flexibility and ease of deployment, it introduces a software-bound latency that accounts for 93% of the temporal overhead. However, this performance cost represents a strategic compromise, as the modularity gained allows for a seamless transition toward quantum-secured protocols without requiring a complete overhaul of existing industrial control software. Furthermore, the study elucidates a critical security-performance trade-off through its buffered key management strategy. This approach effectively bridges the gap between the stochastic, low-throughput nature of physical QKD links and the high-frequency demands of real-time DMS. Empirical validation conducted on a QMAN confirmed that the system maintained real-time data exchange despite an emulated 15 dB channel loss, ensuring that the measurement system remains robust during quantum link outages or realignment phases, albeit at the cost of maintaining a local entropy reservoir. In conclusion, this work provides a technical blueprint for the next generation of mission-critical measurement networks. The experimental validation on a metropolitan-scale testbed confirms that the proposed system can maintain the integrity and synchronization of distributed data even under significant channel loss. Future research will focus on transitioning from software-limited to physics-limited regimes through low-level optimization and exploring mesh topologies to enhance the traceability and reliability of distributed measurement data across national strategic assets.

CRediT authorship contribution statement

Leopoldo Angrisani: Writing – review & editing, Supervision, Methodology, Funding acquisition, Conceptualization. **Mauro D'Arco:** Writing – review & editing, Supervision, Methodology, Funding acquisition, Conceptualization. **Matteo D'Iorio:** Writing – original draft, Visualization, Software, Data curation, Conceptualization. **Fabrizio Lo Regio:** Writing – review & editing, Writing – original draft, Validation, Software, Methodology, Data curation, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work was financially supported by the Italian Ministry of Enterprises and Made in Italy (MIMIT) through the project SHINE-QC (CUP B69J25000260005).

Data availability

Data will be made available on request.

References

[1] T.G. Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, John Wiley & Sons, 2019.

[2] E.D. Vugrin, D.E. Warren, M.A. Ehlen, A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane, Process. Saf. Prog. 30 (3) (2011) 280–290.

[3] S. Corbellini, E. Di Francia, S. Grassini, L. Iannucci, L. Lombardo, M. Parvis, Cloud based sensor network for environmental monitoring, Measurement 118 (2018) 354–361.

[4] P. Daponte, M. Di Penta, G. Mercurio, TransientMeter: A distributed measurement system for power quality monitoring, IEEE Trans. Power Deliv. 19 (2) (2004) 456–463.

[5] A.T. Khan, X. Cao, S. Li, Z. Milosevic, Blockchain technology with applications to distributed control and cooperative robotics: A survey, Int. J. Robot. Control. 2 (1) (2019) 36–48.

[6] A.T. Khan, S. Li, X. Cao, Control framework for cooperative robots in smart home using bio-inspired neural network, Measurement 167 (2021) 108253.

[7] C. Bourelly, D. Capriglione, C. Carissimo, F. Milano, L. Tari, Measurement and applications: The role of communication technologies in developing distributed measurement systems and measurement applications, IEEE Instrum. Meas. Mag. 26 (4) (2023) 19–26.

[8] C. Alcaraz, S. Zeadally, Critical infrastructure protection: Requirements and challenges for the 21st century, Int. J. Crit. Infrastruct. Prot. 8 (2015) 53–66.

[9] P. Kozak, I. Klaban, T. Šlajs, Industroyer cyber-attacks on Ukraine's critical infrastructure, in: 2023 International Conference on Military Technologies, ICMT, IEEE, 2023, pp. 1–6.

[10] A. Di Pinto, Y. Dragoni, A. Carcano, TRITON: The first ICS cyber attack on safety instrument systems, Proc. Black Hat USA 2018 (2018) 1–26.

[11] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Modern Phys. 92 (2) (2020) 025002.

[12] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, The security of practical quantum key distribution, Rev. Modern Phys. 81 (3) (2009) 1301–1350.

[13] R. Renner, Security of quantum key distribution, Int. J. Quantum Inf. 6 (01) (2008) 1–127.

[14] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, et al., An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature 589 (7841) (2021) 214–219.

[15] X. Cao, P. Li, Y. Wang, C. Hua, A.T. Khan, Zeroing neural network for real-time operational research and computational intelligence: An ordinary differential equation based approach, Comput. Intell. 41 (4) (2025) e70099.

[16] R.-P. Braun, M. Ritter, R. Doering, M. Geitz, Berlin openqkd testbed evaluating quantum key distribution in provider networks, in: Proceedings of the 2023 8th International Conference on Systems, Control and Communications, 2023, pp. 41–51.

[17] M. Bertocco, F. Ferraris, C. Offelli, M. Parvis, A client-server architecture for distributed measurement systems, IEEE Trans. Instrum. Meas. 47 (5) (2002) 1143–1148.

[18] R.H. Hadfield, Single-photon detectors for optical quantum information applications, Nat. Photonics 3 (12) (2009) 696–705.

[19] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, A. Shields, Quantum key distribution without detector vulnerabilities using optically seeded lasers, Nat. Photonics 10 (5) (2016) 312–315.

[20] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, et al., Quantum key distribution: a networking perspective, ACM Comput. Surv. 53 (5) (2020) 1–41.

[21] S. Bajrić, Enabling secure and trustworthy quantum networks: current state-of-the-art, key challenges, and potential solutions, IEEE Access 11 (2023) 128801–128809.

[22] S. Francesconi, D. Ribezzo, N. Biagi, I. Vagniluca, C. De Lazzari, T. Occhipinti, D. Bacco, A. Zavatta, Quantum communications for real-world use cases, in: 2024 24th International Conference on Transparent Optical Networks, ICTON, IEEE, 2024, pp. 1–4.

[23] J. Moteff, P. Parfomak, Critical Infrastructure and Key Assets: Definition and Identification, Tech. Rep., Lybrary of congress Washngton DC Congressial Research Service, 2004.

[24] A.E. Saldaña-González, A. Sumper, M. Aragüés-Peñalba, M. Smolnikar, Advanced distribution measurement technologies and data applications for smart grids: A review, Energies 13 (14) (2020) 3730.

[25] J. Koiwanit, et al., Accuracy of distributed systems towards industry 4.0: smart grids and urban drainage systems case studies, GEOMATE J. 14 (43) (2018) 70–76.

[26] F. Pianegiani, D. Macii, P. Carbone, An open distributed measurement system based on an abstract client-server architecture, IEEE Trans. Instrum. Meas. 52 (3) (2003) 686–692.

[27] A.G. Blank, TCP/IP Foundations, John Wiley & Sons, 2006.

[28] D. Grimaldi, M. Marinov, Distributed measurement systems, Measurement 30 (4) (2001) 279–287.

[29] E. Rescorla, RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3, RFC Editor, USA, 2018.

[30] M.A. Khan, S. Javaid, S.A.H. Mohsan, M. Tanveer, I. Ullah, Future-proofing security for UAVs with post-quantum cryptography: A review, IEEE Open J. Commun. Soc. (2024).

[31] P.W. Shor, J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. 85 (2) (2000) 441.

[32] C. Gidney, M. Ekerå, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, Quantum 5 (2021) 433.

[33] J. Preskill, Quantum computing in the NISQ era and beyond, Quantum 2 (2018) 79.

[34] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, et al., Using quantum key distribution for cryptographic purposes: A survey, Theoret. Comput. Sci. 560 (2014) 62–81.

[35] S. Kak, Quantum key distribution using three basis states, Pramana 54 (5) (2000) 709–713.

[36] A.I. Nurhadi, N.R. Syambas, Quantum key distribution (QKD) protocols: A survey, in: 2018 4th International Conference on Wireless and Telematics, ICWT, IEEE, 2018, pp. 1–5.

[37] G. Milburn, Photons as qubits, Phys. Scr. 2009 (T137) (2009) 014003.

[38] C.-H.F. Fung, H.-K. Lo, Security proof of a three-state quantum-key-distribution protocol without rotational symmetry, Phys. Rev. A—Atomic, Mol. Opt. Phys. 74 (4) (2006) 042342.

[39] X. Ma, C.-H.F. Fung, M. Razavi, Statistical fluctuation analysis for measurement-device-independent quantum key distribution, Phys. Rev. A—Atomic, Mol. Opt. Phys. 86 (5) (2012) 052305.

[40] N.J. Cerf, P. Grangier, From quantum cloning to quantum key distribution with continuous variables: a review, J. Opt. Soc. Am. B 24 (2) (2007) 324–334.

[41] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography, Rev. Modern Phys. 74 (1) (2002) 145.

[42] H.-K. Lo, X. Ma, K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. 94 (23) (2005) 230504.

[43] Ø. Marøy, M. Gudmundsen, L. Lydersen, J. Skaar, Error estimation, error correction and verification in quantum key distribution, IET Inf. Secur. 8 (5) (2014) 277–282.

[44] C. Lee, I. Sohn, W. Lee, Eavesdropping detection in BB84 quantum key distribution protocols, IEEE Trans. Netw. Serv. Manag. 19 (3) (2022) 2689–2701.

[45] Y. Watanabe, Privacy amplification for quantum key distribution, J. Phys. A 40 (3) (2006) F99.

[46] D. Elkouss, J. Martinez-Mateo, V. Martin, Information reconciliation for quantum key distribution, 2010, arXiv preprint arXiv:1007.1616.

[47] H.-J. Briegel, W. Dür, J.I. Cirac, P. Zoller, Quantum repeaters: the role of imperfect local operations in quantum communication, Phys. Rev. Lett. 81 (26) (1998) 5932.

[48] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J.F. Dynes, et al., The SECOQC quantum key distribution network in vienna, New J. Phys. 11 (7) (2009) 075001.

[49] A.T. Khan, X. Cao, S. Li, B. Hu, V.N. Katsikis, Quantum beetle antennae search: a novel technique for the constrained portfolio optimization problem, Sci. China Inf. Sci. 64 (5) (2021) 152204.

[50] C.H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theoret. Comput. Sci. 560 (2014) 7–11.

[51] M.N. Wegman, J.L. Carter, New hash functions and their use in authentication and set equality, J. Comput. System Sci. 22 (3) (1981) 265–279.

[52] X. Hu, Y. Cheng, C. Gu, X. Zhu, H. Liu, Superconducting nanowire single-photon detectors: recent progress, Sci. Bull. 60 (23) (2015) 1980–1983.

[53] Z. Yuan, A. Shields, Continuous operation of a one-way quantum key distribution system over installed telecom fibre, Opt. Express 13 (2) (2005) 660–665.

[54] Z. Wang, Y. Shang, J. Liu, X. Wu, A labview based automatic test system for sieving chips, Measurement 46 (1) (2013) 402–410.

[55] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, E. Roback, Report on the development of the advanced encryption standard (AES), J. Res. Natl. Inst. Stand. Technol. 106 (3) (2001) 511.

[56] ThinkQuantum, QKD products, 2026, https://www.thinkquantum.com/quky. (Accessed February 2026).

[57] PHOTEC, Photon Technology, Superconducting Nanowire Single Photon Detector System, 2026, https://www.cnphotec.com/en/solution/solution_snspd. (Accessed February 2026).

[58] C. Bruscino, M. Peluso, P. Ercolano, C. Zhang, D. Salvoni, A. Giuliana, M. Venturini, D. Bacco, F. Santagiustina, T. Occhipinti, et al., Multi-nodes quantum network in metropolitan area of naples, in: 2025 25th Anniversary International Conference on Transparent Optical Networks, ICTON, IEEE, 2025, pp. 1–4.

[59] A. Vanghetti, Optimal parameter selection for a QKD protocol in noisy channels (Ph.D. thesis), University of Padua, 2025.

[60] A. De Toni, E. Bortolozzo, A. Emanuele, M. Venturini, L. Calderaro, M. Avesani, G. Vallone, P. Villoresi, Long-term analysis of efficient-BB84 4-node network with optical switches in metropolitan environment, 2025, arXiv preprint arXiv:2510.16867.

[61] I. Cerutti, A. Leqis, F. Bonavitacola, Quantum Key Distribution (QKD) Experimental Assessment, Tech. Rep, Publications Office of the European Union, 2023.

[62] M. Dianati, R. Alléaume, M. Gagnaire, X. Shen, Architecture and protocols of the future European quantum key distribution network, Secur. Commun. Netw. 1 (1) (2008) 57–74.

[63] D. Stucki, M. Legre, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, et al., Long-term performance of the SwissQuantum quantum key distribution network in a field environment, New J. Phys. 13 (12) (2011) 123001.

[64] E. Dervisevic, A. Tankovic, E. Kaljic, M. Voznak, M. Mehic, Design of a key management system for efficient key supply in quantum key distribution networks, J. Opt. Commun. Netw. 18 (2) (2026) 98–113.
[65] M. Razavi, An Introduction to Quantum Communications Networks: Or, How Shall We Communicate in the Quantum Era?, Morgan & Claypool Publishers, 2018.
[66] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S.X. Ng, L. Hanzo, The evolution of quantum key distribution networks: On the road to the qinternet, IEEE Commun. Surv. Tutor. 24 (2) (2022) 839–894.
[67] L. Kleinrock, Queuing systems, volume i: Theory, 1975.