IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 19 May 2025, accepted 1 June 2025, date of publication 5 June 2025, date of current version 16 June 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3577086

TOPICAL REVIEW

Quantum Key Distribution in Multiple Fiber Networks and Its Application in Urban Communications: A Comprehensive Review

GERMAN GRANADOS, WASHINGTON VELASQUEZ, (Senior Member, IEEE), RICARDO CAJO, (Senior Member, IEEE), AND MARIA ANTONIETA-ALVAREZ, (Member, IEEE)
Facultad de Ingeniería Eléctrica y Computación, Escuela Superior Politécnica del Litoral (ESPOL), Campus Gustavo Galindo, Guayaquil, Ecuador
Corresponding author: Maria Antonieta-Alvarez (aalvare@espol.edu.ec)

This work was supported by the Escuela Superior a del Litoral.

ABSTRACT Information security faces unprecedented challenges in the digital age, particularly in the face of cyber threats and the emergence of quantum computing. This research examines QKD as a solution for secure communications in urban fiber networks. The study analyzes QKD protocols, including BB84 and Twin-Field QKD, implementing a 46-node metropolitan quantum network and key distribution over distances greater than 1002 kilometers. Various transmission media, such as multicore optical fibers and free-space communication, were evaluated, demonstrating high-capacity quantum communication with advanced noise mitigation techniques. The results reveal significant advances in quantum communication security, highlighting the potential of QKD to provide theoretically secure key distribution based on quantum mechanical principles. The research addresses challenges such as transmission loss, environmental disturbances, and network scalability, laying the groundwork for future implementations in metropolitan networks. This work contributes significantly to the standardization of evaluation protocols and metrics, which is crucial for the global adoption of QKD in a world increasingly dependent on cybersecurity, especially in developing smart cities.

INDEX TERMS Quantum key distribution, urban communications security, quantum cryptography, quantum communication protocols, post-quantum cryptography.

NOMENCLATURE

AES	Advanced Encryption Standard.
BB84	Bennett-Brassard 1984.
DI-QKD	Device-Independent Quantum Key Distribution.
SNS-TF-QKD	Sending-or-Not-Sending Twin-Field.
FWM	Four-Wave Mixing.
QD	Quantum Dot.
QKD	Quantum Key Distribution.
PQC	Post-Quantum Cryptography.
RSA	Rivest-Shamir-Adleman.
SNS	Sending or Not Sending.
SpRS	Spontaneous Raman Scattering.
TF-QKD	Twin-Field Quantum Key Distribution.
QBER	Quantum Bit Error Rate.
WDM	Wavelength Division Multiplexing.
PNS	Photon-Number-Splitting.
MCF	Multicore Fiber.
CHSH	Clauser-Horne-Shimony-Holt.

The associate editor coordinating the review of this manuscript and approving it for publication was Giovanni Angiulli.

I. INTRODUCTION

In the digital era, information security is crucial, with key distribution serving as a fundamental aspect of secure communications. Classical cryptographic systems, widely utilized today, depend on symmetric and asymmetric key distribution methods to ensure data confidentiality and integrity [1], [2], [3], [4], [5], [6], [7]. Symmetric key systems, such as the AES [8], provide fast encryption but encounter

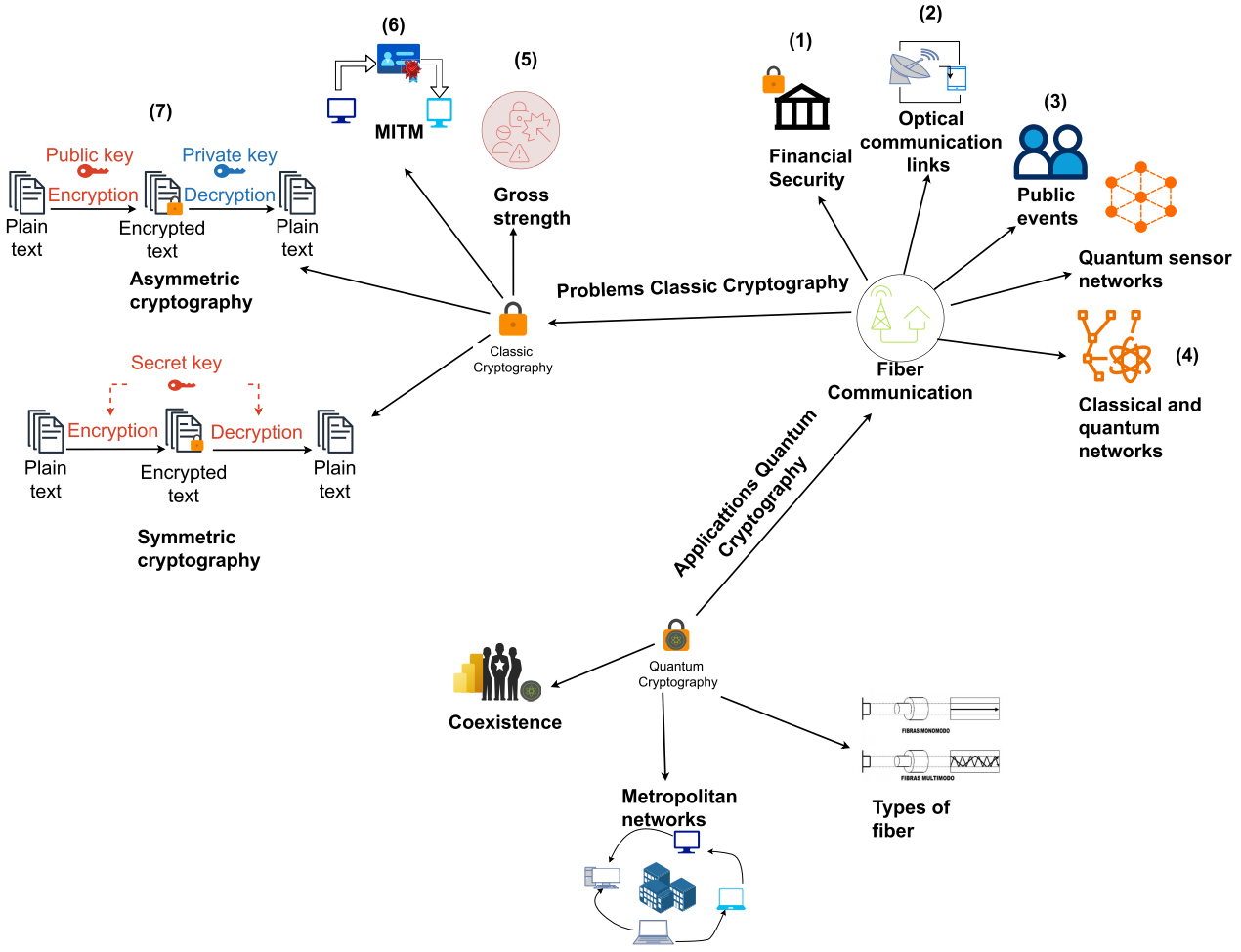

FIGURE 1. Applications and security challenges of QKD (QKD) in urban networks.

difficulties in securely distributing the initial key. On the other hand, asymmetric systems, like RSA and Diffie-Hellman [9], [10], allow for key exchange without a secure channel but are susceptible to mathematical attacks, such as factoring large numbers. The public Key Infrastructure offers a framework for key management, but is complex and costly to maintain.

These classical methods, rooted in computational complexity, have historically proven effective but now display significant vulnerabilities in the face of emerging threats [11], [12]. The rise of quantum computing presents a major challenge to classical cryptography. Quantum algorithms, such as Grover's algorithm, can reduce the security of symmetric systems from 2^{128} to 2^{64} operations, effectively halving their strength. Shor's algorithm threatens asymmetric systems by effectively solving factoring and discrete logarithm problems, rendering RSA and Elliptic Curve Cryptography vulnerable [12], [13], [14], [15], [16], [17]. Recent studies indicate a 300% increase in sophisticated cyberattacks targeting urban communication infrastructure between 2020 and 2024 [18], [19], [20], [21], highlighting the urgent need for robust security solutions.

These vulnerabilities underscore the limitations of classical cryptography in providing long-term security [9], [12], especially in dense urban networks where critical communications, such as financial transactions and smart city operations, require enhanced protection. QKD [22], [23], [24], [25], [26], [27] emerges as a promising solution to address these issues, employing quantum mechanical principles to deliver theoretically unbreakable security. Unlike classical methods, QKD enables secure key distribution without relying on computational assumptions, making it resilient to quantum attacks [28], [29], [30], [31].

Urban environments, characterized by dense fiber-optic networks and high communication demands, present unique opportunities as well as challenges for QKD deployment [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45]. While point-to-point QKD implementations have been thoroughly researched [46], [47], multi-node QKD networks in urban settings remain relatively

unexplored [48], [49], [50], [51], [52], particularly concerning practical integration and scalability. This review aims to evaluate the effectiveness and feasibility of QKD protocols in urban fiber networks, focusing on their integration into existing infrastructures and addressing scalability challenges.

QKD offers a range of applications in urban communication networks, as shown in Figure 1. These applications include:(1) *Financial and Banking Security*, which protects sensitive transactions and client data; (2) *Mobile Networks*, securing smartphones in multi-user environments and coordinating 5G services; (3) *Public Event Security*, ensuring secure communications during large-scale events; and (4) *Telecommunications*. These applications highlight QKD's potential to meet various security needs in metropolitan areas, enabling dynamic, multi-node secure communications while coexisting with classical signals [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45].

Unlike previous studies that emphasize point-to-point QKD, this work provides a comprehensive analysis of multi-node QKD networks in metropolitan areas, examining protocols such as BB84 [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45] and Twin-Field QKD [53], transmission media like MCFs, and coexistence strategies with classical signals. By synthesizing experimental results and identifying standardization needs, this study contributes to the advancement of secure communication technologies for smart cities. Its originality lies in its focus on urban multi-node networks, offering insights into practical deployment challenges and proposing a framework for evaluating QKD performance metrics. This review is aimed at researchers and network engineers who are focused on deploying QKD in urban environments. These areas present unique challenges due to high noise levels, diverse infrastructure, and strict security requirements. The review also addresses policymakers who are developing security standards for smart cities, offering insights into effective deployment strategies and the need for standardization. By providing a comprehensive analysis of multi-node QKD networks, this work bridges the gap between theoretical advancements and practical implementation, promoting secure, scalable, and noise-resilient communications for the future of smart cities.

This article is organized into seven sections. Section II discusses the methodological foundations of QKD, providing background on quantum cryptographic principles. Section III explores QKD implementation in urban fiber networks, focusing on practical deployment considerations. Section IV evaluates the performance of QKD systems, analyzing key metrics and experimental results. Section V analyzes challenges, such as the cost-benefit comparison between QKD and PQC, as well as future directions for research. Section VI synthesizes the findings and addresses the research questions. Finally, Section VII synthesizes key findings and offers recommendations for advancing QKD in urban environments.

II. METHODOLOGICAL FOUNDATIONS OF QKD

The broad subject of QKD necessitates methodical and exacting examination. This study uses a mixed methodology that combines qualitative assessment of security frameworks, comparative analysis of implementations, and a systematic literature survey. Examining the connections between network designs, distribution protocols, and security methods is made possible by the holistic approach.

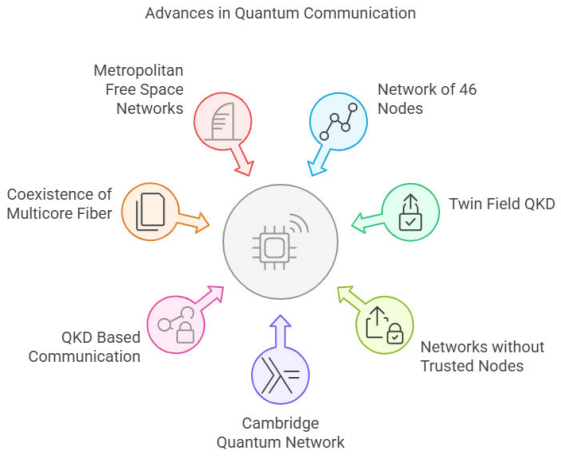

FIGURE 2. Advances in QKD.

A. RESEARCH OBJECTIVE

The main objectives of this review include the comparative effectiveness of different QKD protocols in terms of key generation rates and resistance to attacks, 1) evaluate the effectiveness of quantum technologies in the creation of fault-tolerant networks, 2) analysis of the feasibility of QKD implementations in different transmission media, and 3) identify best practices for the coexistence of quantum and classical communications.

B. RESEARCH QUESTIONS

The research's central inquiry denoted as the Main Question (MQ) and its associated Sub-Questions (SQ) form the foundation of the study. Considering theoretical and practical implementation considerations, this subject tackles the crucial difficulty of incorporating QKD technologies into existing communication infrastructures. The purpose of the sub-questions is to methodically dissect the several operational and technical facets that comprise the primary challenge. *SQ*1 investigates the essential performance of various methods, offering a foundation for evaluating their viability in practice. Finding the best options for various implementation scenarios requires this comparison study. On the other hand, *SQ*2 focuses on the effects of transmission media and discusses the implementation's physical components. Given that one of the earliest areas in which QKD was used practically was in metropolitan networks, this problem is especially pertinent. Understanding each technology's unique

TABLE 1. Research questions.

Identifire	Issue
MQ	How can QKD technologies be effectively implemented in existing communication networks while maintaining their fundamental security?
SQ1	What is the comparative effectiveness of different QKD protocols regarding key generation rates and attack resistance?
SQ2	How do different transmission media impact the practical implementation of metropolitan QKD networks?
SQ3	What mitigation strategies most effectively ensure coexistence between quantum and classical signals?
SQ4	What are the main challenges in implementing QKD networks without trusted nodes?
SQ5	What metrics are most appropriate for evaluating the performance of QKD systems in different deployment scenarios?

constraints and possibilities is made possible by examining various transmission media.

*SQ*3 is essential for real-world applications. This problem acknowledges that QKD networks need to be integrated with current communication infrastructures rather than functioning independently. Research is vital for mitigation methods to be successfully implemented in the real world. *SQ*4 mentions one of the most cutting-edge and exciting features of QKD technology, which is addressed by concentrating on the difficulties of networks without trusted nodes. Creating secure networks that do not depend on potentially weak points depends on this problem. Finally, *SQ*5 talks about the critical necessity for measurement and assessment criteria, which is addressed in the section on evaluation metrics. The establishment of industry standards and the objective assessment of various implementations depend on this issue, illustrated in Table 2.

These research questions direct the methodical investigation of the technical, operational, and security facets of QKD implementations. They offer a methodical framework for studying anything from theoretical underpinnings to real-world implementation difficulties. These questions' relationships with one another guarantee thorough treatment of the subject, and their specificity enables in-depth examination of each vital facet. The resulting research framework makes it easier to identify areas that need more development and evaluate current technology. The questions ' formulation provides a strong basis for rigorous scientific research in the field of QKD, which permits both qualitative and quantitative analysis.

C. QKD PROTOCOLS OVERVIEW

This subsection provides a foundation for the analysis by outlining the key QKD protocols evaluated in this review: BB84 with decoy states, SNS-TF-QKD, and DI-QKD. A detailed comparison of these protocols can be found in Section IV and Table 2, with subsequent sections referencing their performance in specific contexts.

- **BB84 with Decoy States:** Introduced by Bennett and Brassard in 1984, the BB84 protocol uses polarized photons to share secure keys. It incorporates decoy states to enhance security against PNS attacks. This protocol is widely implemented in urban networks, providing scalability and compatibility with existing fiber infrastructure [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45].
- **SNS-TF-QKD:** A variant of Twin-Field QKD, SNS-TF-QKD allows long-distance key distribution without the need for trusted relays, utilizing phase-matching techniques and ultra-low-loss fibers. This makes it ideal for inter-city and metropolitan networks [54]
- **DI-QKD:** Relies on Bell inequalities, such as CHSH, to guarantee security without depending on the hardware, making it ideal for high-security urban applications [55].

These protocols are assessed across different transmission media and applications in Sections III and IV, with performance metrics summarized in Table 2.

D. ARTICLE SELECTION AND ANALYSIS METHODOLOGY

The current study employs a systematic literature selection approach based on the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) [56] methodology, ensuring a rigorous and transparent review process. Four comprehensive digital databases were utilized to capture the breadth of QKD research:

(1) IEEE Xplore. **(2)** Web of Science (WoS). **(3)** Scopus. **(4)** arXiv.

The literature selection process incorporated three systematic iteration stages: First Iteration: Initial screening eliminated non-relevant documents based on broad thematic alignment with QKD research. Second Iteration: Detailed title and abstract screening removed duplicate or irrelevant studies, ensuring focused research selection. A comprehensive full-text review validated selected publications' scientific rigor and relevance, as evidenced by figure 3. Search parameters combined strategic keywords such as ''Quantum Key Distribution'', ''QKD protocols'', ''Quantum communication networks'', and ''Secure key distribution''. Advanced search options excluded book chapters, brief communications, and non-scientific documents. Our methodical approach ensures a comprehensive and systematic review of QKD literature, providing a robust foundation for analyzing current technological developments and identifying future research directions.

These papers were carefully selected through an exhaustive literature review and served as the basis for our research. Among them are contemporary studies such as [55] on DI-QKD and classic works such as [27], which lay the theoretical foundations of QKD safety. The literature selection process adhered to strict relevance, scientific impact, and

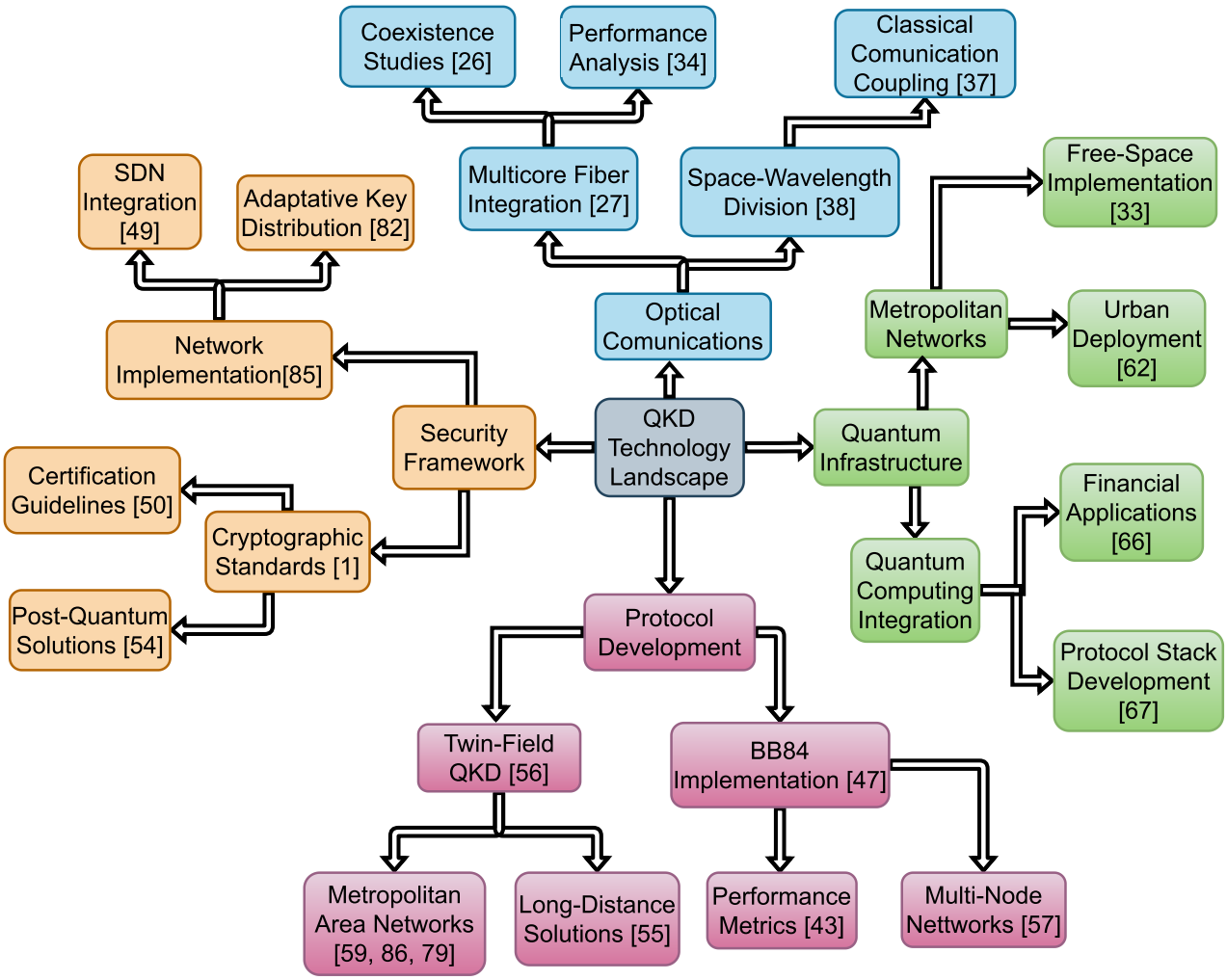

FIGURE 3. Advanced QKD: research areas and applications.

methodological diversity criteria to provide comprehensive coverage of the area.

We concentrate on three primary categories that reflect the most essential QKD application scenarios for examining real-world implementations. We provide a detailed analysis of the Cambridge Quantum Network and the 46-node network in the metropolitan network domain, showing that QKD is feasible in urban settings. [54] and [57] achieved ground-breaking distances of 511 km and 1002 km, respectively, which are the foundation for exploring long-distance implementations. Regarding free-space QKD, we study novel approaches for adaptive spatial filtering and daytime communication.

A tiered analytical framework that blends quantitative measures and qualitative criteria is used to evaluate performance and security. Key generation rates, transmission distances, and mistake rates are quantitative measures; compatibility with current infrastructures and resilience to attacks are qualitative criteria. Thanks to this dual method, we can obtain a comprehensive insight into QKD systems' performance.

Experimental validation and theoretical modeling are used to supplement the technical analysis. To assess the coexistence of quantum and classical signals and confirm the reproducibility of the published experimental results, we employ sophisticated SpRS and FWM noise models. We can determine key success factors and best practices for the following implementations by methodically comparing various deployments.

The integrative approach of our technique, which combines academic rigor with practical application, is what sets it apart. We can discuss the essential elements and the real difficulties of applying QKD from different points of view and analysis methods. This scientific approach provides a solid basis for evaluating the current state of QKD technology and guiding its future development.

Figure 2 highlights significant advancements in QKD, encompassing various protocols such as BB84 and Twin-Field QKD, as well as transmission media like MCFs and free-space communication. It also addresses network architectures, including setups that operate without trusted

nodes. These types of networks eliminate the dependence on potentially vulnerable intermediate nodes, thereby enhancing security in urban environments [54]. The analysis incorporates both quantitative metrics, such as key generation rates and transmission distances, and qualitative criteria, like compatibility with classical infrastructure, to provide a comprehensive evaluation of QKD performance.

III. QKD FOR URBAN FIBER NETWORKS

This section explores the integration of QKD in multiple fiber networks and its pivotal role in enhancing urban communications. As metropolitan areas expand and the demand for secure communication grows, QKD emerges as a critical technology for ensuring data security in complex network environments. This section delves into the practical applications of QKD in urban settings, highlighting its potential to revolutionize secure communication infrastructures.

A. MULTIPLE FIBER NETWORKS AND QKD INTEGRATION

The integration of QKD into multi-fiber networks, especially in MCF systems, is essential for ensuring secure communications in urban environments. MCFs consist of multiple independent optical cores within a single fiber, which increases channel capacity and reduces interference, making them well-suited for QKD deployment. This section explores key QKD protocols, including BB84 with decoy states, SNS-TF-QKD, and DI-QKD, along with their integration into MCF networks. Additionally, it addresses challenges such as SpRS and crosstalk, which can disrupt quantum signals [33], [58], [59], [60], [61], [62], [63], [64], [65].

Advanced techniques, such as tunable filters and dual-core MCFs, enhance the integration of QKD. Optimized power allocation in WDM systems maintains a QBER below 5% over distances of 50 km, achieving key rates of 11 kbps even in noisy urban environments [63]. Chip-based QKD involves implementing QKD protocols on integrated photonic circuits, usually made from materials such as silicon. This approach minimizes the size and cost of QKD systems while preserving performance, making it suitable for compact and scalable applications in urban environments. Chip-based BB84 implementations using silicon photonics provide stable key rates of 866 bps over 150 km with a QBER of 0.50%, making them suitable for compact urban deployments [64]. These advancements, as detailed in Table 2 and Section IV, demonstrate the feasibility of QKD for secure and scalable urban communication networks.

B. APPLICATIONS IN URBAN COMMUNICATIONS

QKD effectively tackles the specific challenges posed by urban communications, which include high data traffic, a wide range of user requirements, and the necessity for enhanced security measures. By delivering theoretically secure key distribution, QKD plays a vital role in supporting essential applications within metropolitan areas. This includes smart city initiatives, governmental communications, and financial transactions, as demonstrated in Figure 4.

The implementation of QKD in urban settings not only enhances the security of these critical applications but also ensures that data integrity and privacy are maintained amidst the complexities and potential threats in densely populated environments. As urban areas continue to evolve and incorporate advanced technologies, the role of QKD in safeguarding communications becomes increasingly significant [12], [66], [67], [68], [69], [70], [71], [72], [73], [74].

In the Hefei metropolitan network, the BB84 protocol with decoy states enables secure voice calls for 40 user nodes simultaneously, supporting confidential communications for government agencies and research institutions. The integration of this network with MCF and WDM, as discussed in Subsection III-A, facilitates connectivity with national quantum networks, thereby enhancing urban security [57]. Similarly, the Cambridge quantum network utilizes the BB84 protocol for high-speed AES encryption, ensuring the security of data streams for thousands of urban users engaged in financial transactions and municipal services [75].

The architecture of SNS-TF-QKD without trusted relays is well-suited for large-scale urban networks. Field tests have shown its effectiveness in securing government communications by eliminating vulnerabilities in intermediate nodes. This makes it an excellent choice for urban command centers and emergency response systems. Additionally, its compatibility with existing telecom infrastructure supports various smart city applications, including traffic management and public safety [54].

DI-QKD's device-independent security offers a promising approach to protecting critical infrastructure. Experimental results indicate its potential for securing urban IoT networks and traffic control systems, effectively mitigating side-channel attacks in environments with untrusted hardware [55]. Integrating QKD into urban communication systems enhances resilience against cyber threats, ensuring secure and reliable data transmission for smart city infrastructure in metropolitan areas.

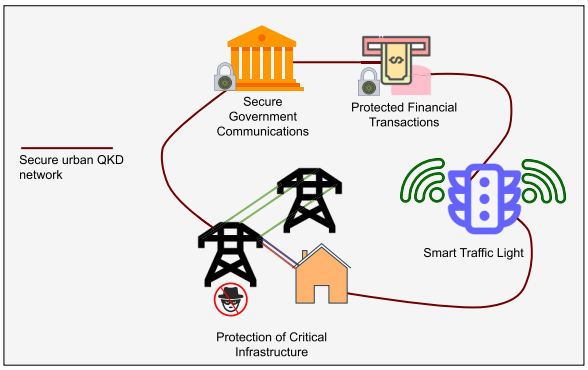

FIGURE 4. QKD applications in urban communications and smart cities.

IV. PERFORMANCE EVALUATION OF QKD

This section evaluates the performance of QKD systems across various protocols, transmission media, and network

architectures. It focuses on quantitative metrics such as key generation rates, QBER, and transmission distances. The analysis addresses the research objectives and sub-questions (SQ1–SQ5) by providing a detailed comparison of QKD protocols, their resilience to attacks, and their practical implementation in urban environments. Unlike Section III, which concentrated on integration and applications, this section emphasizes empirical performance data and security metrics to inform future QKD deployments.

A. COMPARATIVE EFFECTIVENESS OF QKD PROTOCOLS

This section compares the performance of different QKD protocols in urban and long-distance networks. We focus on key metrics such as key generation rates (the speed at which secure keys are created), transmission distances, and resistance to hacking attempts. Protocols like BB84, Twin-Field QKD, and Device-Independent QKD are evaluated to assist in selecting the best option for urban applications, such as securing financial transactions or smart city systems.

The effectiveness of QKD protocols is evaluated based on key generation rates, transmission distances, and resistance to attacks, which addresses SQ1. This comparison includes discrete variable protocols (such as BB84), continuous variable protocols, and advanced variations like SNS-TF-QKD and DI-QKD, utilizing experimental data from both urban and long-distance implementations [76], [77], [78], [79], [80], [81].

- **BB84 with Decoy States:** BB84 is widely used in urban networks and achieves key rates ranging from 6 to 60.5 kbps over a distance of 18 km with 40 nodes in Hefei [57]. In Cambridge, it can deliver 2.58 Mbps over 10.6 km [75]. Utilizing a 7-core MCF, BB84 provides 605 kbps per core over 53 km, maintaining a QBER below 5% this effectively mitigates PNS attacks through the use of decoy states [63].
- **SNS-TF-QKD:** This protocol is designed for long-distance communication, achieving a data rate of 111.74 kbps over a distance of 202 km, with a QBER of 0.944% in the Z-basis. It can reach up to 1002 km when utilizing ultra-low-loss fibers and superconducting detectors [54]. Its relay-free design enhances security for both metropolitan and inter-city networks.
- **Interlaced QKD:** Optimized for short-range free-space links, it achieves 5.7 kbps over a distance of 1.7 km during daytime, making it ideal for urban line-of-sight applications [82].
- **DI-QKD:** This protocol guarantees security that is independent of the device used. An ion-based system in Oxford generates 0.064 bits per event over a distance of 2 meters, with a QBER of 1.44% [55]. In contrast, a Munich atom-based system achieves 0.07 bits per event over 400 meters, but with a higher QBER of 7.8% [55]. Despite the lower key rates, DI-QKD is highly suitable for high-security 97
- **Chip-Based BB84:** Utilizing silicon photonics, this implementation achieves a transmission rate of 866 bps over a distance of 150 km, with a QBER of 0.50%, providing compact solutions for urban networks [64].

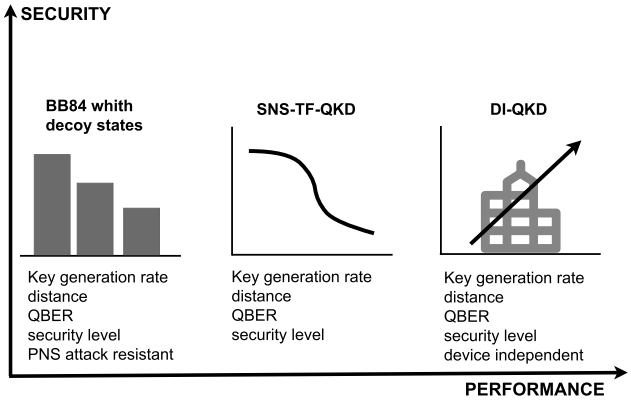

FIGURE 5. Trade-offs in QKD: efficiency, distance, and attack robustness.

Figure 5 provides a visual summary of the balance between security and performance of the main QKD protocols analyzed in this study. Each protocol has its own strengths and weaknesses:

- **Decoy-State BB84:** offers a high key generation rate and strong resistance to PNS attacks. However, its security decreases as the transmission distance increases.
- **SNS-TF-QKD:** is notable for its ability to transmit keys over long distances with high key rates and low QBER levels. This makes it particularly suitable for metropolitan networks and intercity connections.
- **DI-QKD:** provides device independence, ensuring highly secure transmissions. However, it has significantly lower key rates, which limits its applicability in scenarios that require high real-time throughput.

This visual comparison helps in understanding which protocol is best suited for different urban scenarios, depending on the priorities for security and performance.

These results, summarized in Table 2, demonstrate BB84's adaptability to urban environments, the strength of SNS-TF-QKD for long distances, and the potential of DI-QKD for high-security applications, aiding in protocol selection based on network scale and security requirements.

B. FEASIBILITY OF QKD IMPLEMENTATION IN DIFFERENT TRANSMISSION MEDIA

The feasibility of QKD across various transmission media, including MCF, standard fiber, free-space, and hybrid systems, is evaluated in response to SQ2. Each medium has unique advantages and challenges, with performance metrics derived from experimental data.

Table 2 provides a summary of characteristics for each medium, emphasizing quantitative performance.

MCF is designed for high-capacity urban networks, achieving a transmission speed of 605 kbps per core over a distance of 53 kilometers, with a QBER below 5% in a system with 7 cores. To mitigate SpRS and inter-core crosstalk, techniques such as decoy states and filtering are

TABLE 2. Summary of QKD implementations.

Protocol	Media	Key Rate	Distance	QBER	Security Level	Status	Ref.
BB84 with Decoy States	MCF	605 kbps/core	53 km	<5%	High (PNS, SPRS resistance)	In Development	[65]
BB84 with Decoy States	Standard Fiber	6–60.5 kbps	18 km	N/S*	High (PNS resistance)	In Development	[59]
BB84 with Decoy States	Standard Fiber	2.58 Mbps	10.6 km	N/S*	High (PNS resistance)	In Development	[79]
SNS-TF-QKD	Standard Fiber	111.74 kbps	202 km	0.944%	High (Relay-free)	In Development	[56]
SNS-TF-QKD	Ultra-Low-Loss Fiber	3.11×10^{-12} bits/pulse	1002 km	N/S*	High (Relay-free)	In Development	[60]
Interlaced QKD	Free Space	5.7 kbps	1.7 km	N/S*	Medium-High (Daytime)	Experimental	[86]
DI-QKD (Ion-Based)	Fiber	0.064 bits/event	2 m	1.44%	Very High (Device-independent)	Developing	[57]
DI-QKD (Atom-Based)	Fiber	0.07 bits/event	400 m	7.8%	Very High (Device-independent)	Developing	[57]
Chip-Based BB84	Standard Fiber	866 bps	150 km	0.50%	High (PNS resistance)	In Development	[66]
Satellite QKD	Free Space (Satellite)	47.8 kbps	4,600 km	2.5%	High (Global connectivity)	Experimental	[87]
Continuous Variable QKD	Standard Fiber	10–100 kbps**	50 km	N/S*	Medium-High (Gaussian)	Developing	[80]

Note: QBER = Quantum Bit Error Rate; N/S* = Not Specified; PNS = Photon Number Splitting; **Estimated range.

employed. This allows for secure key rates of up to 2.86 Mbps in systems that utilize 37 cores [63]. Free Space provides flexibility for urban links, with Interlaced QKD achieving a speed of 5.7 kbps over a distance of 1.7 km. Atmospheric turbulence is managed using spatial filters; however, ambient light can limit overall performance [82]. Standard Fiber utilizes existing infrastructure but is currently facing losses. Chip-based BB84 achieves 866 bps over a distance of 150 km with a QBER of 0.50%, which is enhanced by decoy states and silicon photonics [64].

The choice of medium depends on distance, noise levels, and available infrastructure, with MCF performing well in dense urban networks and hybrid systems providing adaptability.

C. COEXISTENCE OF QUANTUM AND CLASSICAL COMMUNICATIONS

To address SQ3, it is essential to manage the coexistence of quantum and classical signals for the practical deployment of QKD. Noise models such as SpRS and FWM help quantify the interference. Mitigation strategies have successfully achieved a QBER of less than 5% in MCF systems, with data rates of 605 kbps per core over 53 km, and in WDM systems, with data rates of 11 kbps over 50 km [63]. Techniques like decoy states and optimized power allocation help reduce the impact of noise, facilitating seamless integration with the existing classical telecom infrastructure.

D. SECURITY METRICS AND IMPLEMENTATION CHALLENGES

Addressing SQ3 and SQ4, regarding mitigation strategies and implementation challenges, we present security metrics across different implementations in Table 2.

QKD systems demonstrate robust performance across diverse transmission media, effectively balancing security and efficiency for urban communication networks. In MCF deployments, protocols like BB84 and SSNS-TF-QKD show exceptional resilience against PNS attacks and SpRS noise. Notably, SNS-TF-QKD achieves a remarkably low QBER of 0.944% in the Z-basis and secure key rates of 605 kbps per core over a distance of 53 km in a 7-core MCF, with ongoing certification processes striving to standardize these protocols [54], [63]. In addition, free-space QKD utilizes entanglement-based methods to support urban line-of-sight links, delivering key rates of 5.7 kbps over 1.7 km while ensuring robust security under experimental certification, despite facing atmospheric challenges. DI-QKD offers unmatched security through its hardware-agnostic framework, achieving QBERs of 1.44% for ion-based systems at 2 m and 7.8% for atom-based systems at 400 m. There are continuous efforts aimed at certifying practical deployments for high-security urban environments. [55], [82]. Hybrid systems, which combine fiber and free-space channels, successfully maintain a QBER below 5% while providing key rates of 11 kbps over a distance of 50 km [63]. These systems are designed for specific network configurations and are well-suited for flexible urban integration. Overall, these advancements highlight QKD's potential to secure metropolitan infrastructures, with persistent certification efforts facilitating the pathway toward widespread adoption.

These metrics inform the choice of QKD systems for urban networks, balancing both security and performance.

V. CHALLENGES AND FUTURE DIRECTIONS

The path to practical quantum communication is fraught with complex technical challenges. Transmission loss remains a

TABLE 3. Challenges and solutions.

Technology	Main Challenges	Proposed Solutions
Fiber Optics	Losses, interference	TF-QKD, multiplexing
Free Space	Ambient light, turbulence	Adaptive filters, QDs
DI-QKD	Practical implementation	New protocols
Entanglement-Based	Efficient distribution	Improved sources
MCFs	Crosstalk, amplification	Optimized design

critical constraint, with photon signals degrading significantly across fiber channels. The delicate quantum states are particularly vulnerable to environmental perturbations, requiring sophisticated error correction and noise mitigation strategies.

Atmospheric conditions pose additional complications, particularly for free-space quantum communication. Researchers must develop advanced spatial filtering techniques to maintain quantum state integrity under varying environmental conditions. These challenges underscore the intricate balance between quantum mechanical principles and practical communication technologies.

A. TECHNICAL CHALLENGES AND PROPOSED SOLUTIONS

Transmission loss is a significant limitation in QKD systems, as photon signals can degrade considerably when transmitted through fiber channels. The fragile quantum states are especially susceptible to environmental disruptions, necessitating advanced error correction and noise mitigation techniques. In the case of free-space QKD, atmospheric factors such as turbulence and ambient light create further challenges, requiring sophisticated spatial filtering methods to preserve the integrity of the quantum states. These technical obstacles highlight the complex relationship between quantum mechanics and practical communication technologies.

Table 3 summarizes the main challenges in various QKD technologies and their proposed solutions, laying a foundation for overcoming implementation barriers.

- **Fiber Optics**: Transmission losses and interference, including SpRS, limit key generation rates. Solutions like TF-QKD and WDM improve performance by increasing key rates and reducing noise. This enhancement is illustrated by the Hefei network, which achieved key generation rates of 6 to 60.5 kbps over a distance of 18 km [57].
- **Free Space**: Atmospheric turbulence and ambient light can diminish signal quality. Adaptive spatial filtering and QD technologies enhance resilience, allowing daytime operations with key rates of 5.7 kbps over a distance of 1.7 km [82].
- **DI-QKD**: Practical implementation is hindered by low key rates (e.g., 0.064 bits per event) and experimental complexity. New protocols and advanced hardware, such as ion-based systems, have been proposed to enhance feasibility [55].
- **Entanglement-Based Systems**: Efficient distribution of entangled states is still challenging. Enhanced quantum sources and improved error correction techniques are essential for scalability.
- **MCFs**: Crosstalk and amplification issues negatively impact performance. Optimized fiber designs and filtering techniques, such as those achieving 605 kbps per core over 53 km, help address these challenges [63].

B. COST-BENEFIT CONSIDERATIONS: QKD VERSUS PQC

This subsection offers a qualitative comparison of the economic and security implications, concentrating on infrastructure requirements, scalability, and suitability for urban applications. Due to the limited availability of accurate cost data in the public domain, this analysis refrains from making speculative quantitative estimates and instead highlights key factors that are important for network engineers and policymakers.

1) ECONOMIC CONSIDERATIONS

Deploying QKD in urban environments requires significant investment in specialized infrastructure, which affects its economic feasibility.

- **Hardware Requirements**: QKD depends on specialized quantum hardware, such as superconducting nanowire single-photon detectors and quantum light sources. This requirement leads to custom manufacturing and integration into existing telecom systems [54]. Consequently, it increases complexity and resource demands compared to conventional cryptographic systems.
- **Infrastructure Modifications**: Implementing QKD in urban fiber networks often requires low-loss or MCFs to minimize transmission losses and interference, such as SpRS [54]. These specialized fibers necessitate substantial upgrades to existing infrastructure, particularly in densely populated metropolitan areas.
- **Maintenance Needs**: The sensitivity of quantum systems necessitates ongoing calibration and environmental stabilization, which increases operational overheads. This is especially challenging in urban environments with significant ambient noise and fluctuating network demands.

In contrast, PQC utilizes existing computational infrastructure, providing a more cost-effective alternative:

- **Software-Based Implementation**:PQC algorithms, particularly lattice-based schemes like Kyber standardized by NIST [83], can be implemented through software updates on standard servers and IoT devices, reducing the reliance on specialized hardware.

- **Compatibility with Existing Systems**: PQC integrates smoothly with protocols like TLS, allowing for quick deployment across urban networks, including 5G and IoT infrastructures, without the need for significant infrastructure overhauls. [83].
- **Lower Maintenance Overhead**: PQC requires regular software updates, which are less resource-intensive than the hardware maintenance needed for QKD, making it more suitable for large-scale urban applications. [83].

While QKD involves higher economic demands due to its specialized requirements, PQC takes advantage of existing infrastructure, making it more accessible for widespread deployment in resource-constrained urban environments.

2) SECURITY BENEFITS

QKD and PQC provide different security characteristics, each tailored for specific urban use cases.

- **QKD Security**: QKD offers information-theoretic security grounded in the principles of quantum mechanics, making it resistant to all types of computational attacks, even those that may arise from future quantum computers. For example, protocols such as BB84 and SNS-TF-QKD can achieve QBERs as low as 0.944% and key rates of up to 605 kbps per core. This makes them highly suitable for protecting critical communications, including financial transactions and government operations [54], [63].
- **PQC Security**: PQC is based on mathematical problems that are thought to be resistant to attacks from quantum computers, such as lattice-based cryptography. However, its security is not information-theoretic, meaning it could be vulnerable to unexpected advancements in algorithms. While NIST's PQC standards offer practical security for most applications, they don't provide the same absolute guarantees as QKD [83].

The trade-off between the theoretical security of QKD and the practical security of PQC is a crucial consideration for urban deployments, where the required level of security varies depending on the application.

3) URBAN SCENARIOS AND RECOMMENDATIONS

The decision between QKD and PQC depends on the specific needs of urban communication networks.

- **High-Security Applications**: QKD is particularly well-suited for critical infrastructure, including urban command centers, financial hubs, and government communications. In these high-stakes environments, the potential risk of data breaches makes the investment in specialized infrastructure worthwhile.
- **Cost-Sensitive Applications**: PQC is preferred for large-scale, lower-criticality networks, such as municipal IoT systems or public Wi-Fi, where cost and scalability are priorities. Its compatibility with existing infrastructure makes it ideal for smart city applications, like traffic monitoring.
- **Hybrid Approach**: A hybrid strategy that combines QKD for high-security nodes, such as financial institutions, with PQC for peripheral networks, like smart meters, optimizes both security and economic efficiency. This approach utilizes the strong security offered by QKD for critical applications while employing PQC to cost-effectively scale across broader urban networks.

This qualitative analysis examines the economic and security trade-offs between QKD and PQC, offering a framework for stakeholders to make informed decisions regarding their deployment in urban environments without relying on unverified cost estimates.

C. FUTURE RESEARCH DIRECTIONS

The future of QKD in urban communications needs to address both technical and economic challenges to improve its practicality and scalability. Important research directions include:

- **Quantum Repeaters**: Creating efficient quantum repeaters, such as those utilizing silicon-vacancy centers, can extend the range of QKD without relying on trusted nodes, thereby improving scalability in urban networks [84].
- **Standardization**: Implementing universal certification protocols, such as ETSI GR QKD 003, is essential for ensuring interoperability and trust in QKD deployments [85].
- **Hybrid Systems**: Enhancing the integration of quantum and classical signals through advanced WDM and filtering techniques, achieving QBERs below 5% over a distance of 50 km [63].
- **Cost Reduction**: Investigating chip-based QKD implementations that achieve stable key rates of 866 bps over a distance of 150 km, aiming to reduce infrastructure costs. [64]. Public-private partnerships, as illustrated by the Cambridge network, can help facilitate larger-scale deployments [75].
- **Satellite QKD**: Enhancing satellite-based QKD for inter-city connectivity, achieving key rates of 47.8 kbps over 4,600 km, to support urban fiber networks [86].

These advancements will facilitate the adoption of QKD in smart city infrastructures by overcoming technical limitations and economic barriers, thus ensuring secure, scalable, and noise-resilient communications.

VI. DISCUSSION

This section synthesizes findings to address Sub-Questions (SQ1–SQ5) with a focus on the implications for urban QKD deployment.

SQ1: Comparative Effectiveness of QKD Protocols. The scalability of BB84 makes it suitable for dense urban networks, such as those in Hefei, enabling applications like municipal services [57]. On the other hand, the relay-free design of SNS-TF-QKD is ideal for inter-city connections and urban command centers, as it enhances security [54]. DI-QKD offers secure communication even when the devices

used are not fully trusted. It is based on fundamental principles of quantum physics instead of relying on perfect hardware, which enhances its security in situations where trust in equipment is limited. However, it operates at lower key rates [55]. A hybrid approach that utilizes BB84 for metropolitan networks, SNS-TF-QKD for long-distance links, and DI-QKD for critical infrastructure can optimize urban deployment Table 2.

SQ2: Impact of Transmission Media. MCF facilitates high-capacity urban networks, while free-space technology offers flexibility for short-range connections. Hybrid systems provide versatility, making them ideal for dynamic smart city infrastructures Table 2. MCF is particularly suited for densely populated cities [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45].

SQ3: Coexistence of Quantum and Classical Signals. Noise mitigation strategies, such as SpRS/FWM filtering and optimized power allocation, enable seamless integration with classical telecom infrastructure, which is crucial for urban networks that share fiber resources [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45].

SQ4: Challenges in Networks Without Trusted Nodes. SNS-TF-QKD and DI-QKD remove the need for trusted nodes, improving security against urban-specific threats such as side-channel attacks Table 2 [54], [55]

SQ5: Performance Evaluation Metrics. Standardized metrics such as key rate, QBER, and certification status are crucial for evaluating QKD systems. The ongoing certification efforts for MCF-based protocols, along with experimental advancements in free-space systems, emphasize the necessity for industry collaboration to create universal standards [64], [82].

A. KEY LIMITATIONS AND MITIGATION STRATEGIES

The comparative analysis of QKD protocols, transmission media, and coexistence strategies, as discussed in Sections III and IV, highlights significant advancements in securing urban communication networks. However, several limitations and practical challenges must be addressed to ensure scalable and cost-effective deployment in metropolitan environments. This subsection critically evaluates these limitations and their implications for specific urban scenarios, as well as potential mitigation strategies. Additionally, it explores emerging architectures that could influence future QKD deployments.

1) PROTOCOL TRADE-OFFS AND URBAN IMPLICATIONS

The trade-offs among various QKD protocols—BB84, SNS-TF-QKD, and DI-QKD—have significant implications for urban applications, influenced by factors such as cost, scalability, and regulatory constraints. This high scalability makes it suitable for dense metropolitan networks like the Hefei network, which supports up to 40 user nodes [57]. Additionally, BB84's compatibility with existing telecommunications infrastructure helps minimize deployment costs, making it an excellent option for smart city applications, including municipal services and financial transactions. However, its dependence on trusted relays introduces potential vulnerabilities in high-security situations. Therefore, careful certification of nodes is necessary to meet urban cybersecurity regulations. In contrast, SNS-TF-QKD utilizes a network design without trusted nodes. This technology enhances security for inter-city connectivity and is particularly beneficial for large-scale urban command centers. Its high key rates make it suitable for real-time applications, such as emergency response systems. However, the requirement for ultra-low-loss fibers and superconducting nanowire single-photon detectors increases deployment costs, which can be a barrier for municipalities with limited budgets. Additionally, regulatory frameworks, such as those established by the European Telecommunications Standards Institute (ETSI), can complicate deployment due to strict requirements for interoperability with classical networks. DI-QKD offers strong security without relying on trusted hardware and can achieve quantum QBER as low as 1.44% in ion-based systems [55]. This makes it particularly suitable for critical infrastructure, such as urban IoT networks and traffic management systems, where concerns about untrusted hardware arise. However, the low key generation rates—approximately 0.064 bits per event—significantly hinder its applicability in real-time scenarios that necessitate high data throughput, like live video surveillance in smart cities. Furthermore, the experimental complexity of DI-QKD can drive up costs and delay scalability, requiring substantial investment in research and development to align with urban deployment timelines. These trade-offs emphasize the importance of adopting a hybrid approach tailored to urban environments. For cost-sensitive applications, the BB84 protocol provides a practical solution. In contrast, SNS-TF-QKD is better suited for high-security, long-distance links, while DI-QKD is designed for niche, high-stakes scenarios. Policymakers need to balance these considerations with regulatory requirements, such as the European Union's cybersecurity directives, which mandate the implementation of quantum-resistant technologies for critical infrastructure by 2030 [85].

2) CERTIFICATION BARRIERS

Certification remains a significant challenge for urban QKD deployments, as highlighted in Table 2. Currently, MCF-based BB84 and SNS-TF-QKD systems are undergoing certification, while experimental certification has been achieved for free-space systems. However, the certification of device-independent DI-QKD is still in development, primarily due to its low key rates and experimental complexity. Technical challenges include the necessity for standardized protocols to ensure interoperability among diverse urban networks, especially in MCF and WDM systems. For example, ETSI's QKD Industry Specification Group has developed standards such as ETSI GR QKD 003 (2022) that outline the requirements for the integration of QKD modules; however, these standards have not yet been universally adopted [85]. Additionally,

regulatory challenges further complicate the certification process, as urban deployments must comply with national and international cybersecurity frameworks, including guidelines from the U.S. National Institute of Standards and Technology (NIST) and the International Telecommunication Union's (ITU-T) Y.3800 series for quantum-safe networks [87], [88].

Timelines for certification vary. MCF-based systems are projected to achieve standardization by 2027, largely due to pilot projects like the Hefei network [57]. However, the certification for DI-QKD may extend beyond 2030 because it depends on advanced quantum hardware, such as ion or atom-based systems. To overcome these challenges, collaboration between the industry and standardization bodies like ETSI, ITU-T, and ISO/IEC is crucial. Public-private partnerships, such as those demonstrated in the Cambridge quantum network [75], can expedite the certification process by funding testbeds and aligning technical requirements with regulatory mandates.

3) EMERGING ARCHITECTURES: SATELLITE QKD AND QUANTUM MEMORY-BASED REPEATERS

Emerging technologies, such as satellite QKD and quantum memory-based repeaters, offer promising solutions to current limitations in secure communications and aim to enhance urban QKD networks. Notably, satellite QKD has been successfully demonstrated, achieving secure key distribution over distances greater than 4,600 kilometers, with average secret key rates of 47.8 kilobits per second during typical satellite passes [86]. In urban environments, satellite QKD can complement fiber-optic systems by enabling secure connections between cities or serving as backup links for metropolitan networks during fiber outages. For instance, a hybrid satellite-fiber network could secure government communications across multiple urban centers, effectively addressing scalability challenges in densely populated areas. However, atmospheric variability presents significant obstacles to the widespread adoption of this technology. The integration of QKD satellites with fiber systems provides an effective approach to improving secure connectivity between different locations, particularly in crowded urban settings.

Recent advancements in quantum memories, particularly those using silicon-vacancy (SiV) centers in diamond coupled with nanocavities, enable the storage and manipulation of quantum states with high fidelity. These systems boast coherence times that exceed 200 microseconds. Such technologies enhance the capability for Bell state measurements and secure the distribution of quantum keys over long distances, thereby improving the efficiency and security of quantum networks without the need for reliable repeaters. Although there are still challenges related to cost and experimental complexity, these developments mark significant progress toward the practical implementation of scalable quantum networks in the near future [84].

Integrating these architectures into urban QKD networks necessitates strategic planning. Pilot projects, such as those proposed for smart cities [57], should be established to test hybrid satellite-fiber systems and quantum repeaters in real-world urban environments. Collaboration with industry leaders and standardization bodies will be crucial to developing cost-effective, interoperable solutions that comply with urban regulatory frameworks.

4) MITIGATION STRATEGIES FOR SCALABILITY AND COST

To tackle scalability and cost challenges, several strategies have been proposed. First, utilizing existing telecom infrastructure, as demonstrated by the Cambridge network's use of standard fiber for BB84 [75], reduces deployment costs while ensuring compatibility with classical signals. Second, chip-based QKD implementations have achieved 866 bps over 150 km with a QBER of 0.50% [64], providing compact and cost-effective solutions for urban networks. Third, public-private partnerships can support large-scale deployments, as observed in the Hefei network [57]. Finally, regulatory incentives, such as subsidies for quantum-secure infrastructure under the EU's Digital Decade initiative, can help offset costs and speed up the adoption of these technologies [85]. These strategies should be adapted to urban environments. For instance, in densely populated cities with high data traffic, the high capacity of MCF justifies its deployment costs, making it suitable for applications such as real-time traffic management. On the other hand, cost-conscious municipalities might prefer chip-based BB84 for smaller-scale networks, like municipal services. Additionally, regulatory compliance, especially with NIST's PQC standards [83], will play a crucial role in guiding deployment decisions, ensuring that QKD aligns with global cybersecurity objectives.

VII. CONCLUSION

This review enhances the discussion on quantum-secure urban communications by summarizing key technical advancements, emerging challenges, and practical strategies for the deployment of QKD in smart cities. Unlike previous studies that concentrated solely on theoretical performance, we address the crucial gap between experimental successes and real-world implementation through three innovative contributions:

A. SUMMARY OF KEY INSIGHTS

1) **Protocol Optimization**: The record-setting 1002-km SNS-TF-QKD implementation [40] and successful metropolitan BB84 deployments [5], [42] demonstrate that long-distance quantum communication is now technically feasible. However, DI-QKD's low key rates over short distances [40] highlight an ongoing trade-off between device-independent security and practical usability.
2) **Infrastructure Integration**: Our analysis shows that advanced noise mitigation techniques such as SpRS/FWM filtering and optimized power allocation in WDM systems have enabled QKD to coexist with classical signals at distances up to 50 km

with QBERs below 5% [5]. Silicon photonics-based chip implementations further enhance scalability by reducing system size and power consumption while maintaining acceptable performance metrics [6].

3) **Security-Practicality Balance**: While NIST's Post-Quantum Cryptography (PQC) program emphasizes mathematical resilience against quantum attacks [83], QKD offers a fundamentally different form of security rooted in quantum physics. Nevertheless, certification frameworks for MCF and DI-QKD remain underdeveloped, creating a gap in standardization that must be addressed to ensure interoperability and trustworthiness in real-world applications.

B. LIMITATIONS AND FUTURE DIRECTIONS

Despite these advancements, several challenges hinder the widespread adoption of QKD in smart city infrastructures:

Technological Maturity: Current single-photon detectors require cryogenic cooling, significantly increasing operational complexity and energy consumption [5]. In addition, noise effects such as SpRS and inter-core crosstalk in MCF systems pose significant limitations to signal integrity [63]. Emerging technologies like silicon photonics and passive detection methods show promise but require substantial research investment to reach commercial viability [6].

Standardization Delays: Although ETSI has outlined a roadmap for MCF-based QKD certification (GR QKD 003), expected finalization is projected for 2027 [89]. Similarly, ITU-T's Y.3800 series aims to establish global compatibility by 2025 [80]. These timelines lag behind the current pace of technological development, particularly for protocols like DI-QKD, which currently lack any universally accepted certification framework [40].

Energy Efficiency: Existing QKD nodes consume 10–100 times more power than their classical counterparts due to the need for cryogenics and high-power lasers [5]. However, recent pilot projects in Hefei suggest that hybrid architectures combining QKD with classical infrastructure could reduce energy consumption by up to 40% within the next decade [42].

C. ACTIONABLE ROADMAP

To transition QKD from experimental success to large-scale urban deployment, we propose the following strategic steps:

Regulatory Alignment: Establish a joint task force among NIST, ETSI, and ITU-T by 2025 to harmonize QKD and PQC standards. This initiative should leverage existing draft guidelines from ISO/IEC JTC1/SC27 [89], aiming to create a unified certification framework by 2027.

Focused Pilots: Target high-security zones in 3–5 cities (e.g., Singapore, Zurich) for MCF-based QKD deployments by 2026. These pilots should utilize funding models inspired by the EU Quantum Flagship program to accelerate industrial adoption and regulatory validation.

Detector Innovation: Prioritize government and private grants—such as those from NSF or DARPA—for the development of room-temperature single-photon detectors with efficiency above 50% and jitter below 100 ps by 2028 [5]. Such improvements would significantly reduce the operational costs and complexity of QKD nodes.

D. INTERDISCIPLINARY CONVERGENCE

Future research must adopt an interdisciplinary approach to address the broader implications of QKD in smart cities:

AI-Driven Optimization: Machine learning algorithms can enable real-time QBER adjustment and adaptive noise suppression in dynamic urban environments, enhancing the robustness of QKD systems in multi-node configurations [5].

Policy Frameworks: Given the transnational nature of many urban communication networks, future work should include geopolitical risk assessments and policy design informed by quantum-safe clauses similar to GDPR provisions [89].

Hybrid Security Architectures: Co-designing QKD with lattice-based PQC will provide layered defense mechanisms against both classical and quantum threats. This dual-layer strategy supports a smooth transition to post-quantum secure communications while leveraging the information-theoretic advantages of QKD [83].

This roadmap presents QKD as a scalable pillar of urban quantum resilience, relying on coordinated advancements in technology, policy, and standardization.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, Oct. 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0304397514004241

[2] S. Khan, F. Luo, Z. Zhang, F. Ullah, F. Amin, S. F. Qadri, M. B. B. Heyat, R. Ruby, L. Wang, S. Ullah, M. Li, V. C. M. Leung, and K. Wu, "A survey on X.509 public-key infrastructure, certificate revocation, and their modern implementation on blockchain and ledger technologies," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 4, pp. 2529–2568, 2023.

[3] S. T. Mantey, M. F. Ramos, N. A. Silva, A. N. Pinto, and N. J. Muga, "Frame synchronization for quantum key distribution systems," in *Proc. GLOBECOM-IEEE Global Commun. Conf.*, Dec. 2022, pp. 5237–5242.

[4] D. Chen, L. Wei, C. YaLiang, P. Qing, and S. Lei, "Reference-frame-independent measurement-device-independent quantum key distribution using hybrid logical basis," *Quantum Inf. Process.*, vol. 17, no. 10, pp. 1–11, Oct. 2018.

[5] P. K. Lala, "An efficient key distribution protocol based on BB84," *Amer. J. Comput. Res. Repository*, vol. 2, no. 2, pp. 33–37, Jan. 2014.

[6] T. Zhou, M. Xu, D. Qin, X. Nie, X. Li, and C. Li, "Computing offloading based on TD3 algorithm in cache-assisted vehicular NOMA–MEC networks," *Sensors*, vol. 23, no. 22, p. 9064, Nov. 2023.

[7] A. C. H. Chen, "Post-quantum cryptography anonymous scheme - PQCWC: Post-quantum cryptography winternitz-chen," 2024, *arXiv:2410.03678*.

[8] J. Kaur, S. Lamba, and P. Saini, "Advanced encryption standard: Attacks and current research trends," in *Proc. Int. Conf. Advance Comput. Innov. Technol. Eng. (ICACITE)*, pp. 112–116, Mar. 2021.

[9] W. Diffie and M. Hellman, "New directions in cryptography (1976)," Tech. Rep., 2021.

[10] T. Yang, Y. Zhang, S. Xiao, and Y. Zhao, "Digital signature based on ISRSAC," *China Commun.*, vol. 18, no. 1, pp. 161–168, Jan. 2021.

[11] J. J. Tom, N. P. Anebo, B. A. Onyekwelu, A. Wilfred, and R. E. Eyo, "Quantum computers and algorithms: A threat to classical cryptographic systems," *Int. J. Eng. Adv. Technol.*, vol. 12, no. 5, pp. 25–38, Jun. 2023.

[12] A. Mehmood, A. Shafique, M. Alawida, and A. N. Khan, "Advances and vulnerabilities in modern cryptographic techniques: A comprehensive survey on cybersecurity in the domain of machine/deep learning and quantum techniques," *IEEE Access*, vol. 12, pp. 27530–27555, 2024.

[13] M. N. Khan, A. Rao, and S. Camtepe, "Lightweight cryptographic protocols for IoT-constrained devices: A survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4132–4156, Mar. 2021.

[14] P. Kocher, "Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems," in *Proc. Annu. Int. Cryptol. Conf.*, Jan. 1996, pp. 104–113.

[15] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment," *Sensors*, p. 5941, May 2023.

[16] M. Bhavsar, K. Roy, J. Kelly, and O. Olusola, "Anomaly-based intrusion detection system for IoT application," *Discover Internet things*, vol. 3, no. 1, p. 5, May 2023.

[17] S. Rajapaksha, H. Kalutarage, M. O. Al-Kadri, A. Petrovski, G. Madzudzo, and M. Cheah, "AI-based intrusion detection systems for in-vehicle networks: A survey," *ACM Comput. Surveys*, vol. 55, no. 11, pp. 1–40, Nov. 2022.

[18] A. Kuzior, H. Yarovenko, P. Brożek, N. Sidelnyk, A. Boyko, and T. Vasilyeva, "Company cybersecurity system: Assessment, risks and expectations," *Prod. Eng. Arch.*, vol. 29, no. 4, pp. 379–392, Dec. 2023.

[19] P. Cao and L. Teng, "A chaotic image encryption algorithm based on sliding window and pseudo-random stack shuffling," *Nonlinear Dyn.*, vol. 112, no. 15, pp. 1–31, Aug. 2024.

[20] M. U. Rehman and A. Shafqiue, "Robust encryption framework for IoT devices based on bit-plane extraction, chaotic sine models, and quantum operations," *Internet Things*, vol. 27, Oct. 2024, Art. no. 101241.

[21] V. Smith, M. Mendoza, and I. Ullah, "Data security techniques using vigenere cipher and steganography methods in inserting text messages in images," *J. Inf. Syst. Technol. Res.*, vol. 3, no. 3, pp. 92–100, Sep. 2024.

[22] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal, "Experimental quantum key distribution certified by bell's theorem," *Nature*, vol. 607, no. 7920, pp. 682–686, Jul. 2022.

[23] V. L. Krutyanskiy, M. Galli, V. Krcmarsky, S. Baier, D. A. Fioretto, Y. Pu, A. Mazloom, P. Sekatski, M. Canteri, M. Teller, J. Schupp, J. Bate, M. Meraner, N. Sangouard, B. P. Lanyon, and T. E. Northup, "Entanglement of trapped-ion qubits separated by 230 meters," *Phys. Rev. Lett.*, vol. 130, no. 5, Feb. 2023, Art. no. 050803.

[24] X. Hu, Y. Guo, B. Liu, C. Li, and G. Guo, "Progress in quantum teleportation," *Nature Rev. Phys.*, vol. 5, no. 6, pp. 339–353, May 2023.

[25] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin, "Quantum repeaters: From quantum networks to the quantum Internet," *Rev. Modern Phys.*, vol. 95, no. 4, Dec. 2023, Art. no. 045006.

[26] S. Storz et al., "Loophole-free bell inequality violation with superconducting circuits," *Nature*, vol. 617, no. 7960, pp. 265–270, May 2023.

[27] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim, and H. Weinfurter, "A device-independent quantum key distribution system for distant users," *Nature*, vol. 607, no. 7920, pp. 687–691, Jul. 2022.

[28] R. Zia-Ul-Mustafa, S. S. Boroujeni, C. Guerra-Yanez, Z. Ghassemlooy, H. L. Minh, and S. Zvanovec, "Quantum key distribution for visible light communications: A review," in *Proc. 13th Int. Symp. Commun. Syst., Netw. Digit. Signal Process. (CSNDSP)*, Jul. 2022, pp. 589–594.

[29] J. Mietzner, A. Harlakin, P. A. Hoeher, T. Fast, C. Liedtke, R. Heinze, and R. Greule, "Joint light planning and error-rate prediction for dual-use lighting/visible light communication," *IEEE Photon. J.*, vol. 14, no. 6, pp. 1–13, Dec. 2022.

[30] R. Verma, S. Agrawal, and A. Jaiswal, "Modulation signaling-based continuous variable quantum key distribution for indoor visible light communications," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2023, pp. 1–6.

[31] R. Zia-Ul-Mustafa, H. L. Minh, Z. Ghassemlooy, and S. Zvánovec, "Machine learning-based channel allocation for secure indoor visible light communications," in *Proc. 14th Int. Symp. Commun. Syst., Netw. Digit. Signal Process. (CSNDSP)*, Jul. 2024, pp. 506–511.

[32] W. Kong, Y. Sun, Y. Gao, and Y. Ji, "Coexistence of quantum key distribution and optical communication with amplifiers over multicore fiber," *Nanophotonics*, vol. 12, no. 11, pp. 1979–1994, May 2023.

[33] W. Kong, Y. Sun, Y. Gao, and Y. Ji, "Core and wavelength allocation of sending-or-not-sending quantum key distribution for future metropolitan networks over multicore fiber," in *Proc. Opt. Fiber Commun. Conf. (OFC)*, Jan. 2022, pp. 1–15. [Online]. Available: https://opg.optica.org/abstract.cfm?uri=OFC-2022-Th2A.37

[34] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the qinternet," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 839–894, 2nd Quart., 2022.

[35] C. Cai, Y. Sun, and Y. Ji, "Simultaneous long-distance transmission of discrete-variable quantum key distribution and classical optical communication," *IEEE Trans. Commun.*, vol. 69, no. 5, pp. 3222–3234, May 2021.

[36] D. Herman, C. Googin, X. Liu, Y. Sun, A. Galda, I. Safro, M. Pistoia, and Y. Alexeev, "Quantum computing for finance," *Nature Rev. Phys.*, vol. 5, no. 8, pp. 450–465, Jul. 2023.

[37] J. Illiano, M. Caleffi, A. Manzalini, and A. S. Cacciapuoti, "Quantum Internet protocol stack: A comprehensive survey," *Comput. Netw.*, vol. 213, Jun. 2022, Art. no. 109092.

[38] G. G. Rozenman, N. K. Kundu, R. Liu, L. Zhang, A. Maslennikov, Y. Reches, and H. Y. Youm, "The quantum Internet: A synergy of quantum information technologies and 6G networks," *IET Quantum Commun.*, vol. 4, no. 4, pp. 147–166, Dec. 2023.

[39] R. Liu, G. G. Rozenman, N. K. Kundu, D. Chandra, and D. De, "Towards the industrialisation of quantum key distribution in communication networks: A short survey," *IET Quantum Commun.*, vol. 3, no. 3, pp. 151–163, Sep. 2022.

[40] P. Yue, J. An, J. Zhang, J. Ye, G. Pan, S. Wang, P. Xiao, and L. Hanzo, "Low Earth orbit satellite security and reliability: Issues, solutions, and the road ahead," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 3, pp. 1604–1652, 3rd Quart., 2023.

[41] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, "Continuous-variable quantum key distribution system: Past, present, and future," *Appl. Phys. Rev.*, vol. 11, no. 1, p. 011318, Mar. 2024.

[42] A. Widomski, S. Stopinski, K. Anders, R. Piramidowicz, and M. Karpinski, "Precise on-chip spectral and temporal control of single-photon-level optical pulses," *J. Lightw. Technol.*, vol. 41, no. 19, pp. 6255–6262, Oct. 1, 2023.

[43] S. Baskar, M. K. Roberts, and K. Sridhar, "Long-distance secure communication based on quantum repeater deployment with quantum-key distribution," in *Proc. 3rd Int. Conf. Artif. Intell. For Internet Things (AIIoT)*, May 2024, pp. 1–6.

[44] C. Xie, Y. Sun, Y. Gao, and F. Sun, "Synergistic resource allocation with key generation and consumption matching in quantum secured multicore fiber optical networks," in *Proc. Asia Commun. Photon. Conf. (ACP) Int. Conf. Inf. Photon. Opt. Commun. (IPOC)*, Nov. 2024, pp. 1–6.

[45] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, Jun. 2005, Art. no. 230504.

[46] H. Zhang, X. Zhang, J. Eng, M. Meunier, Y. Yang, A. Ling, J. Zuniga-Perez, and W. Gao, "Metropolitan quantum key distribution using a GaN-based room-temperature telecommunication single-photon source," 2024, *arXiv:2409.18502*.

[47] H. Kaur and J. S. P. Singh, "Software defined network implementation of multi-node adaptive novel quantum key distribution protocol," *AIMS Electron. Electr. Eng.*, vol. 8, no. 4, pp. 410–430, 2024.

[48] R. Bavdekar, E. J. Chopde, A. Agrawal, A. Bhatia, and K. Tiwari, "Post quantum cryptography: A review of techniques, challenges and standardizations," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2023, pp. 146–151.

[49] R. Müller, W. Meier, and C. F. Wildfeuer, "Area efficient modular reduction in hardware for arbitrary static moduli," 2023, *arXiv:2308.15079*.

[50] R. Shajahan, K. Jain, and P. Krishnan, "A survey on NIST 3rd round post quantum digital signature algorithms," in *Proc. 5th Int. Conf. Mobile Comput. Sustain. Informat. (ICMCSI)*, Jan. 2024, pp. 132–140.

[51] K. Samunnisa, S. V. Gaddam, and K. Madhavi, "Enhancing cloud security: A hybrid honeycomb-lattice encryption model for quantum resistance," Tech. Rep.

[52] J. Oliva del Moral, A. deMarti iOlius, G. Vidal, P. M. Crespo, and J. E. Martinez, "Cybersecurity in critical infrastructures: A post-quantum cryptography perspective," *IEEE Internet Things J.*, vol. 11, no. 18, pp. 30217–30244, Sep. 2024.

[53] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," *Nature Photon.*, vol. 15, no. 8, pp. 570–575, Aug. 2021.

[54] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, D. Ma, C. Zhang, W.-X. Pan, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, C.-Y. Lu, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, and J.-W. Pan, "1002 km twin-field quantum key distribution with finite-key analysis," *Quantum Frontiers*, vol. 2, no. 1, p. 16, Nov. 2023.

[55] V. Zapatero, T. van Leent, R. Arnon-Friedman, W.-Z. Liu, Q. Zhang, H. Weinfurter, and M. Curty, "Advances in device-independent quantum key distribution," *npj Quantum Inf.*, vol. 9, no. 1, p. 10, Feb. 2023.

[56] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, and D. Moher, "Updating guidance for reporting systematic reviews: Development of the PRISMA 2020 statement," *J. Clin. Epidemiology*, vol. 134, pp. 103–112, Jun. 2021.

[57] T.-Y. Chen et al., "Implementation of a 46-node quantum metropolitan area network," *npj Quantum Inf.*, vol. 7, no. 1, p. 134, Sep. 2021.

[58] E. E. Moghaddam, H. Beyranvand, and J. A. Salehi, "Resource allocation in space division multiplexed elastic optical networks secured with quantum key distribution," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 9, pp. 2688–2700, Sep. 2021.

[59] F. Beutel, F. Brückerhoff-Plückelmann, H. Gehring, V. Kovalyuk, P. Zolotov, G. Goltsman, and W. H. P. Pernice, "Fully integrated four-channel wavelength-division multiplexed QKD receiver," *Optica*, vol. 9, no. 10, p. 1121, Aug. 2022.

[60] W. Kong, Y. Sun, X. Ren, Y. Gao, and Y. Ji, "Space-wavelength-division-multiplexing-based synergistic transmission in quantum key distribution coexisting with classical communications," in *Proc. Eur. Conf. Opt. Commun. (ECOC)*, Sep. 2022, pp. 1–4.

[61] M. R. Dibaj, P. Mehdizadeh, M. S. Ghasrizadeh, H. Beyranvand, J. C. Hernandez-Hernandez, J. A. Hernández, D. Larrabeiti, and F. Arpanaei, "From strings to streams: A multi-period analysis of QKD over EONs, showcasing multi-band vs. multi-fiber solutions," in *Proc. 33rd Int. Telecommun. Netw. Appl. Conf.*, Nov. 2023, pp. 169–175.

[62] P. Mehdizadeh, M. R. Dibaj, H. Beyranvand, and F. Arpanaei, "Quantum-classical coexistence in multi-band optical networks: A noise analysis of QKD," *IEEE Commun. Lett.*, vol. 28, no. 3, pp. 488–492, Mar. 2024.

[63] W. Kong, Y. Sun, Y. Gao, and Y. Ji, "Core and wavelength allocation schemes for noise suppression in quantum key distribution over multicore fiber," *IEEE J. Sel. Topics Quantum Electron.*, vol. 29, no. 1, pp. 1–12, Jan. 2023.

[64] K. Wei, X. Hu, Y. Du, X. Hua, Z. Zhao, Y. Chen, C. Huang, and X. Xiao, "Resource-efficient quantum key distribution with integrated silicon photonics," *Photon. Res.*, vol. 11, no. 8, p. 1364, May 2023.

[65] X. Liu, D. Luo, Z. Luo, S. Li, Z. Zhang, and K. Wei, "Refrence-frame-independent quantum key distribution over 250 km of optical fiber," 2024, *arXiv:2405.16558*.

[66] V. S. Barletta, D. Caivano, M. D. Vincentiis, A. Pal, and M. Scalera, "Hybrid quantum architecture for smart city security," *J. Syst. Softw.*, vol. 217, Jul. 2024, Art. no. 112161.

[67] F. Hossain, K. Hasan, A. Amin, and S. Mahmud, "Quantum machine learning for enhanced cybersecurity: Proposing a hypothetical framework for next-generation security solutions," *J. Technol. Inf. Commun.*, vol. 4, no. 1, p. 32222, Dec. 2024.

[68] D. Said, M. Bagaa, A. Oukaira, and A. Lakhssassi, "Quantum entropy and reinforcement learning for distributed denial of service attack detection in smart grid," *IEEE Access*, vol. 12, pp. 129858–129869, 2024.

[69] P. R. Babu, S. A. Kumar, A. G. Reddy, and A. K. Das, "Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges," *Comput. Sci. Rev.*, vol. 54, Nov. 2024, Art. no. 100676.

[70] R. Alluhaibi, "Quantum machine learning for advanced threat detection in cybersecurity," *Int. J. Saf. Secur. Eng.*, vol. 14, no. 3, pp. 875–883, Jun. 2024.

[71] A. H. M. B. Hussain, M. M. Hasan, N. U. Prince, M. M. Islam, S. Islam, and S. B. Hasan, "Enhancing cyber security using quantum computing and artificial intelligence: A review," *algorithms*, vol. 10, no. 3, pp. 448–456, Jun. 2021.

[72] F. Raheman, "The future of cybersecurity in the age of quantum computers," *Future Internet*, vol. 14, no. 11, p. 335, Nov. 2022.

[73] T. Q. Duong, J. A. Ansere, B. Narottama, V. Sharma, O. A. Dobre, and H. Shin, "Quantum-inspired machine learning for 6G: Fundamentals, security, resource allocations, challenges, and future research directions," *IEEE Open J. Veh. Technol.*, vol. 3, pp. 375–387, 2022.

[74] K. K. Rangan, J. Abou Halloun, H. Oyama, S. Cherney, I. A. Assoumani, N. Jairazbhoy, H. Durand, and S. K. Ng, "Quantum computing and resilient design perspectives for cybersecurity of feedback systems," *IFAC-PapersOnLine*, vol. 55, no. 7, pp. 703–708, Jan. 2022.

[75] J. F. Dynes, A. Wonfor, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. Yuan, A. R. Dixon, J. Y. Cho, Y. Tanizawa, H. Greißer, I. H. White, R. Penty, and A. J. Shields, "Cambridge quantum network," *NPJ Quantum Inf.*, vol. 5, no. 1, p. 101, Nov. 2019.

[76] J. Lai, F. Yao, J. Wang, M. Zhang, F. Li, W. Zhao, and H. Zhang, "Application and development of QKD-based quantum secure communication," *Entropy*, vol. 25, no. 4, p. 627, Apr. 2023.

[77] A. Mukherjee, V. Kumar, P. Halder, A. Kumar, R. L. Sharma, P. K. Rathore, A. K. Gupta, P. K. Dalela, and R. Upadhyay, "Quantum key distribution over existing optical fibre carrying traffic," in *Proc. 16th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2024, pp. 968–972.

[78] R. Alléaume et al., "Using quantum key distribution for cryptographic purposes: A survey," *Theor. Comput. Sci.*, vol. 560, pp. 62–81, Dec. 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0304397514006963

[79] T. Niraula, A. Pokharel, A. Phuyal, P. Palikhel, and M. Pokharel, "Quantum computers' threat on current cryptographic measures and possible solutions," *Int. J. Wireless Microw. Technol.*, vol. 12, no. 5, pp. 10–20, Oct. 2022.

[80] P. Sharma, K. Choi, O. Krejcar, P. Blazek, V. Bhatia, and S. Prakash, "Securing optical networks using quantum-secured blockchain: An overview," *Sensors*, vol. 23, no. 3, p. 1228, Jan. 2023.

[81] P. Sharma, A. Agrawal, V. Bhatia, S. Prakash, and A. K. Mishra, "Quantum key distribution secured optical networks: A survey," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 2049–2083, 2021.

[82] A. Kržić et al., "Towards metropolitan free-space quantum networks," *NPJ Quantum Inf.*, vol. 9, no. 1, p. 95, Sep. 2023.

[83] M. V. Yesina, Y. V. Ostrianska, and I. D. Gorbenko, "Status report on the third round of the NIST post-quantum cryptography standardization process," *Radiotekhnika*, vol. 2022, no. 210, pp. 75–86, Sep. 2022.

[84] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin, "Experimental demonstration of memory-enhanced quantum communication," *Nature*, vol. 580, no. 7801, pp. 60–64, Apr. 2020.

[85] J. M. Sáez, A. Pastor, R. C. Palancar, D. López, J. F. Chavarria, V. M. Ayuso, and J. P. B. Mendéz, "Current status, gaps, and future directions in quantum key distribution standards: Implications for industry," in *Proc. Int. Conf. Quantum Commun.*, Jul. 2024, pp. 341–345.

[86] Y.-A. Chen et al., "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, Jan. 2021.

[87] *Security Considerations for Quantum Key Distribution Network*, ITU-T, Geneva, Switzerland, Mar. 2020.

[88] *Overview on Networks Supporting Quantum Key Distribution*, ITU, Geneva, Switzerland, Oct. 2019.

[89] J. Gulati and R. Raman, "Quantum key distribution: Harnessing the power of BB84 for secure communications in the post-quantum era," in *Proc. Int. Conf. Trends Quantum Comput. Emerg. Bus. Technol.*, Mar. 2024, pp. 1–6.

GERMAN GRANADOS received the Engineering degree from the Escuela Superior Politécnica del Litoral (ESPOL), Guayaquil, Ecuador, in 2018, and the M.Sc. degree in visual analytics and big data from the Universidad Internacional de La Rioja (UNIR), Spain, in 2023. He is currently pursuing the Ph.D. degree in electrical engineering with a focus on telecommunications with ESPOL. He is a Research Technician with the Mobile Communications Research Group (GICOM), ESPOL. His research interests include quantum communications and their applications.

WASHINGTON VELASQUEZ (Senior Member, IEEE) received the Ph.D. degree in telematics system engineering and the master's degree in telematics services and network engineering from the Universidad Politécnica de Madrid, Madrid, Spain. He is currently a Professor with the Faculty of Electrical and Computer Engineering, Escuela Superior Politécnica del Litoral, Guayaquil, Ecuador. He has authored/co-authored several articles in indexed journals and has led projects related to sensing and networking. He also holds international certifications in UBIQUITI, HUAWEI, and MIKROTIK. His research interests include telemetry, remote control, smart cities, SDN, and big data.

RICARDO CAJO (Senior Member, IEEE) received the M.Sc. degree in industrial automatic control from the Escuela Superior Politécnica del Litoral, Guayaquil, Ecuador, and the Ph.D. degree in engineering from Ghent University. Currently, he is a University Lecturer with ESPOL in the field of electronics and automation engineering. His academic background is complemented by a notable research activity, reflected in various scientific publications in journals, conferences, and book chapters. He is also recognized as an Outcomes-Based Educator specializing in engineering education. He is included in the International Professional Register of Engineering Educators (ENTER), with a registration valid, from January 2025 to January 2029. This recognition underscores his commitment to equipping future engineers with essential skills and knowledge, ensuring that educational practices align with industry standards, and fostering innovation in the field. His primary areas of research interests include the control of autonomous vehicles, such as UAVs, UGVs, and USVs, as well as fractional-order control (FOC) systems, multi-agent systems, and model-based predictive control. He has played a crucial role as a Reviewer in high-impact journals, such as IEEE TRANSACTIONS ON SYSTEMS, MAN AND CYBERNETICS: SYSTEMS, IEEE TRANSACTIONS ON AEROSPACE AND ELECTRONIC SYSTEMS, IEEE SYSTEMS JOURNAL, and IEEE TRANSACTIONS ON CYBERNETICS.

MARIA ANTONIETA-ALVAREZ (Member, IEEE) received the Ph.D. degree in information technology from Politecnico di Milano, Milan, Italy, in 2019. Since 2012, she has been with the Faculty of Electronic and Computer Engineering, ESPOL Polytechnic University, Guayaquil, Ecuador, where she is a Researcher and a Professor. Her research interests include signal processing and quantum communication, particularly in quantum security.