Babylonian Journal of Networking
Vol.2025, **pp**. 80–96
DOI: https://doi.org/10.58496/BJN/2025/007; ISSN: 3006-5372
https://mesopotamian.press/journals/index.php/BJN

Research Article

Advanced 6G Network Protection Using Quantum Key Distribution: A Systematic Review

Bassma M. Kamil[1],*

[1] *Department of Electronics and Communications Engineering, Al-Ahliyya Amman University, Amman, Jordan.*

ARTICLE INFO

Article History

Received 18 Apr 2025
Revised 14 May 2025
Accepted 15 Jun 2025
Published 14 Jul 2025

Keywords

6G Networks

Quantum Key Distribution (QKD)

Network Security

Post-Quantum Cryptography (PQC)

Artificial Intelligence (AI)

Machine Learning (ML)

Quantum-Resilient Communication Infrastructure

ABSTRACT

With the advent of 6G communication systems on the horizon, ensuring that they are secure from quantum computing threats, in a post-quantum era, is of paramount importance. Quantum attacks, computational hardness-based classical cryptographic algorithms are becoming more susceptible to quantum attacks. Quantum Key Distribution (QKD) has been proposed to address this challenge, which can provide unconditional security based on quantum mechanics for establishing security cryptographic keys. In this work, we review how QKD could fit into the 6G design as part of the general siytematic vision of security exploring its potential implementations, the technical feasibility, and the applications considering both fiber and wireless scenarios. We provide a comparative investigation of performance indicators of QKD systems in simulated 6G scenarios: secret key generation rates, quantum bit error rates (QBER), resistance to noise and user mobility. In addition, hybrid security models between classical post-quantum cryptography (PQC) and QKD to achieve multilayered security protocols are demonstrated. Furthermore, the contribution that could be made by AI/ML to improve QKD performance is analyzed, with particular attention to smart error correction, adaptive key management, anomaly detection, and dynamic routing. Despite significant progress, a number of critical challenges are still open in terms of scale, standardization, interoperability and deployment. In Section VI, we offer a forward-looking research direction, highlighting the importance of the AI empowered QKD, protocols global standardization, and creation of realworld testbeds to drive the QKD from the testbed to the 6G network. It is hoped that the insights provide here will inspire research community and industry partners to build quantum-safe communication infrastructure for the future.

1. INTRODUCTION

The upcoming sixth-generation (6G) wireless networks will transform worldwide communications by providing new capabilities including terabit-per-second data rates, ultra-low latency, pervasive connectivity, and built-in AI/ML capabilities [1]. Such features are expected to facilitate disruptive applications such as holographic telepresence, the tactile internet, autonomous systems and massive IoT infrastructure. However, the complexity and heterogeneity of 6G networks dramatically enlarge the attack surface, leading to serious issues about data confidentiality, integrity, authentication and resistance against advanced cyber threats.

Classical security solutions developed for previous wireless generations are incapable to cope with security threats of the future 6G infrastructures because they are unable to treat the current multi-dimensional and dynamic threat types caused by the new technologies[2]. In addition, the very fast advancement in the area of quantum computing brings an existential threat to classical cryptographic applications. Algorithms including Shor [18] and Grover [11] have shown the theoretical potential to perform polynomial time-breaking of commonly used publickey cryptosystems including RSA and ECC [3]. As these cryptographic schemes underpin its present Internet and mobile security protocols, their threat from quantum computers has precipitated an immediate need to rethink and redesign network security for future communications systems.

The "store now, decrypt later" paradigm, on the other hand, also illustrates the importance of forward-secure security that is even secure when data has been intercepted already years ago [4,5]. This" driver"factors the use of quantum-safe and quantum-enhanced solutions that guarantee a long-term protection of data in 6G networks.

*Corresponding author. Email: bassmamaki9492@gmail.com

One of the most-promising approaches is QKD, which is based on fundamental principles of quantum mechanics for information-theretic secure key exchange [6]. Unlike classical cryptographic methods, QKD ensures that any attempt to eavesdrop results in observable errors in the quantum state, and enables the wasting of keys that are potentially breached. Protocols like BB84, E91 and Continuous Variable QKD have shown promise for deployment in security-sensitive applications such as autonomous transportation, defence, healthcare, and financial services in the 6G based networks [7].

This work provides a full systematic review of QKD-based security schemes designed for 6G networks. We discuss key concepts behind quantum cryptography, leading QKD protocols, and their applicability, including advantages and limitations, in different 6G deployment landscapes. The research further reviews experimental proofs of concept, testbeds, and trials for deploying QKD in future wireless access networks. Moreover, it underscores how AI/ML can be employed to improve QKD operations, like intelligent error correction, dynamic routing, and adpative key management.

Focusing on the current lack of research, scalability, and implementation issues, this review aims to inform the development of secure, immune and resilient quantum communication infrastructure. Table 1 summarizes the evolution of security requirements in wireless from 4G to 6G, and corroborates the importance of quantum-safe solutions such as QKD for dealing with the growing threat landscape, ultra-low latency requirements, and the complexity brought about by ubiquitous AI and densely-wired devices.

TABLE I. EVOLUTION OF SECURITY REQUIREMENTS ACROSS WIRELESS GENERATIONS AND THE EMERGING NEED FOR QUANTUM-SAFE APPROACHES IN 6G NETWORKS

Feature / Generation	4G LTE	5G NR	6G (Expected)
Encryption Type	Classical (AES, ECC)	Classical + Post-Quantum Cryptography (PQC)	Quantum-Safe Encryption + Quantum Key Distribution (QKD)
Latency Requirements	~50 ms	~1 ms	<0.1 ms
AI Integration	Not Supported	Partial AI Integration	Native AI and ML Integration
Attack Surface	Moderate	High	Very High (Massive IoT, XR, UAVs, Holography, Tactile Internet)
Quantum Threat Resilience	Not Considered	Early Research Phase	Strongly Required and Actively Pursued

2. RELATED WORKS

Quantum key distribution (QKD) has been considered as a key ingredient for secure and future-proof 6G networks. QKD uses the laws of quantum mechanics, to generate and exchange cryptographic keys with unconditional security, which can couple the vulnerabilities of classical encryption (especially to quantum attacks possible in 6G environment [8]).

Recently, the paradigm to incorporate QKD into mobile communication infrastructures has been becoming the focus of new research to protect data confidentiality, integrity and to withstand against postquantum threats. A number of protocols, including BB84, E91, and Continuous Variable QKD (CV-QKD), have been studied in great detail, both theoretically and experimentally [9]. More sophisticated protocols are offered to work around the current limitations in scalability, interoperability, and hardware integration like Measurement-Device-Independent QKD (MDI-QKD), Twin-Field QKD, satellite-based QKD [10].

Key Generation Rate (KGR), quantum bit error rate (QBER), and secret key rate (SKR) are three metrics usually considered in the performance analysis of QKD systems. Studies have shown that QKD can implement KGRs that far outpace those for classical systems, along with lower error rates—a crucial characteristic of the URLLC that 6G applications need ([9]). Quantum key distribution (QKD) in empirical implementations has achieved a reduced transmission time—from ca 250ms in classical to approx 180ms—this has implications on applicability to real-time applications such as autonomous driving or remote surgery [11].

However, there are still many technical and architectural challenges. These include the need for quantum-compatible hardware (detectors, repeaters), for channel calibration, and for the restoration of QKD within the classical infrastructure. To address this, hybrid quantum classical security models were presented, which combines QKD with the new field of post-quantum cryptography (PQC) in the hope to provide increased security without the need for a complete infrastructure replacement.

A number of demonstrations in the real world, for example, the Tokyo QKD network have proved that QKD is indeed in practice, with resources to 300 kbps dokey generation rates. These case studies highlight both the potential and the lingering challenges of scaling QKD for large, mobile 6G networks.

In the future, it is necessary to bring QKD to an even more efficient and scalable level and to integrate QKD globally – with satellite based QKD and quantum repeaters, for example. In order to harness QKD for the future secure communication systems, interdisciplinary research will play an important role. Tables Table 2 and Table 3 summarize, in comparison, some relevant works in the literature. Table 2 It gives a summary of major several studies with respect to methodology applied, metric calculated and obtained results. Table 3 addresses deployment scenarios, real benefits, limitations, and 6G applications.

TABLE II. COMPARATIVE ANALYSIS OF KEY RELATED WORKS ON ENHANCING 6G NETWORK SECURITY USING QKD

Study Focus	Methodology	Key Metrics	Key Findings
Role of QKD in 6G security	Literature Review	Security guarantees, integration	QKD enhances 6G security via quantum-safe key exchange.
QKD Protocols for 6G	Theoretical and simulation studies	BB84, E91, CV-QKD	Twin-field QKD and MDI-QKD improve range and robustness.
QKD performance evaluation	Experimental studies	KGR, QBER, SKR	High key rates (>120 keys/sec), low error rates in test networks.
Latency in QKD-based 6G	Empirical latency testing	Transmission delay, error margin	Reduced latency from ~250 ms to ~180 ms—suitable for real-time applications.
Infrastructure integration challenges	Architectural modeling	Hardware requirements, channel use	Need for quantum-compatible components in network infrastructure.
Hybrid QKD-Classical Security Systems	Hybrid model design	Compatibility, encryption strength	Hybrid models ensure strong security while preserving backward compatibility.
Practical deployments (e.g., Tokyo)	Case studies and benchmarking	Key rate, deployment scale	Achieved 300 kbps; demonstrated real-world feasibility.
Future trends and research gaps	Projection and analysis	Scalability, satellite integration	Emphasis on satellite QKD and scalable repeaters for global deployment.

TABLE III. APPLICATION-ORIENTED COMPARISON OF QKD APPROACHES FOR SECURING 6G NETWORKS

Deployment Context	Key Advantages	Main Limitations	Application Areas
Theoretical modeling	Provides future-proof cryptographic foundation	Lacks real-world implementation data	General 6G security frameworks
Protocol simulation environments	Validates robust protocols like MDI-QKD and twin-field QKD	Limited scalability at global scale	Secure control signaling
Lab-scale QKD testbeds	Achieves high key rates, low QBER	Restricted to small-scale experiments	Smart grids, autonomous transport
Time-sensitive networks	Reduced latency for real-time data exchange	Inefficient over long distances	Tactile Internet, telemedicine
Hybrid optical-classical links	Enables secure integration with minimal infrastructure change	Requires expensive quantum hardware	Urban communication backbones
Hybrid encryption systems	Balances classical and quantum encryption strengths	Synchronization complexity	IoT devices, edge networks
Tokyo QKD network	Demonstrates metro-scale deployment feasibility	Cost and regional limitations	Smart cities, financial sector
Satellite-based QKD	Offers global-scale secure key distribution potential	Early-stage development	Satellite networks, cross-border 6G applications

3. FUNDAMENTALS OF 6G NETWORKS

3.1 Overview of 6G

The 6G systems are intended to provide order-of-magnitude gains beyond what 5G technology can achieve, including terabit class peak data rate up to 1 Tbps, millisecond or microsecond range latency and ten times the energy efficiency of 5G [12]. These improvements are not only evolutionary, but revolutionary, as they make futuristic services, like holographic real-time communication, UHD immersive media, tactile Internet, and massivem ADVERTISEMENT human–machine interaction, possible. In order to enable these new generation applications, 6G must guarantee ultra-high capacity and, at the same time, uncapped ultra-Reliability and ultra-Low latency (URLLC) as well as relentless fault resistance and extreme reliability. They will be realized through advancements in spectrum using such as the terahertz (THz) and visible light communications as well as in backend infrastructure such as AI-native and edge-intelligent networks [10].

Unlike its predecessors, 6G is conceived as an integrated technology system that interconnect communications, sensing and computing into an intelligent whole. This "network of intelligence" will allow the network to become context-aware, self-optimizing and responsive to real-world environmental changes in real time. The near data source edge computing and AI-based decision making will be critical to reduce latency and enable real time autonomous operation [13].

Furthermore, the emergence of high-frequency bands, e.g., terahertz (THz) and visible light communication (VLC), is expected to increase the amount of bandwidth and to offer ultra-fine-grained environmental sensing capabilities [4]. These emerging bands will also bring new propagation requirements for 6G systems to consider. Security/privacy are of course built into the 6G ‘ether’. In the era of ubiquitous access, security-by-design is a necessity as wireless networks are increasingly used in important sectors and private domain as well. Unlike previous versions where security was considered to be anachronistic, 6G aims to embed trust, resilience, and privacy-preservation in the heart of the network. There are ongoing research works to answer to the needs of the changing threat landscape in the field of developing technologies like post-quantum crypto (PQC), distributed ledgers (DL) and zero-trust architecture of networks [11]. The service is decentralized, such as mobile edge computing, and presents additional challenges that need dynamic and flexible security mechanisms to cope with the threats when the harmful events occur [6].

Worldwide cooperative activities are carried out to shape the 6G vision. As part of this goal international organizations (e.g., ITU-T, 3GPP, ETSI), together with academic and industry entities, are making efforts to standardize the technical and architectural principles of 6G, and several research programs and experimental testbeds have been announced worldwide (e.g., consortiums and projects from China, the USA, South Korea and the European Union) \cite{r7}. These initiatives strive not only to create technological basis, but also regulatory and ethical guidance towards the responsible roll-out of 6G networks [12]. Table 4 depicts the transition of performance, architecture and security principles in different wireless generations and how the radical transformations are anticipated for 6G.

TABLE IV. EVOLUTION OF WIRELESS NETWORK CAPABILITIES FROM 4G TO 6G

Feature	4G LTE	5G NR	6G (Expected)
Peak Data Rate	~1 Gbps	~10 Gbps	≥ 1 Tbps
Latency	~50 ms	~1 ms	< 0.1 ms (microsecond-level)
Frequency Band	Sub-6 GHz	Up to mmWave	THz bands, Visible Light Communication (VLC), mmWave
AI Integration	Not Supported	Partial Integration	Native, Intelligent, Distributed AI
Reliability	Moderate	High	Ultra-Reliable Low-Latency Communication (URLLC)
Integrated Technologies	None	Emerging Sensing	Convergence of Communication, Sensing, and Computing
Security Architecture	Add-on Security	Layered Security	Built-in Security with PQC and QKD

3.2 Key Technologies in 6G

The wireless 6G is not a simply speed-up and latency-reduction of wireless communications; it is the integration of several gamechanging technologies and concepts that are able to offer a smart, high-rate, and secure communication area. Several promising technologies are expected to become cornerstone techniques in achieving 6G vision.

A key innovation of THz communication is the potential to function in the terahertz (THz) band, spanning from 0,1 to 10 THz. The spectrum has the potential to deliver ultra high data rates needed for futuristic immersive applications like holographic streaming and real timeXR (Extended Reality) environment. Nevertheless, there are lots of challenges for THz signals, including high path loss, molecular absorption and range limitations. To solve such problems, sophisticated technologies such as ultra-massive Multiple Input Multiple Output (MIMO), adaptive beamforming and intelligent reflecting surface (IRS) are being deployed to improve signal power and coverage [13].

6G also has profound AI incorporation into the network architecture. Augmented by AI AI won’t be an additional add-on — it will be a built-in part of the system to support predictive maintenance, dynamic resource allocation, and real-time traffic optimization. Yet, more importantly AI may be able to aid automated threat detection and response, which is critical for having self-healing, secure and rugged networks [14].

Another revolutionary technology for 6G is the IRS (Intelligent Reconfigurable Surfaces), which is a type of programmable metasurface capable of controlling the wireless propagation environment, reflecting, refracting, or absorbing signals in a deterministic way. Their extensive use indoor as well as outdoor will significantly enhance spectral efficiency, reliability of the link and coverage in dense urban areas [15]. These technologies are helping to form there-four building blocks that constitute the 6G architecture, namely ultra-fast transmission, energy-efficient communication, AI-intelligence, and built-in security and privacy. As shown in Fig. 1, there are four key supporting "legs" of 6G network technologies: speed, intelligence, efficiency, and security, and technological innovations supporting each of these four.

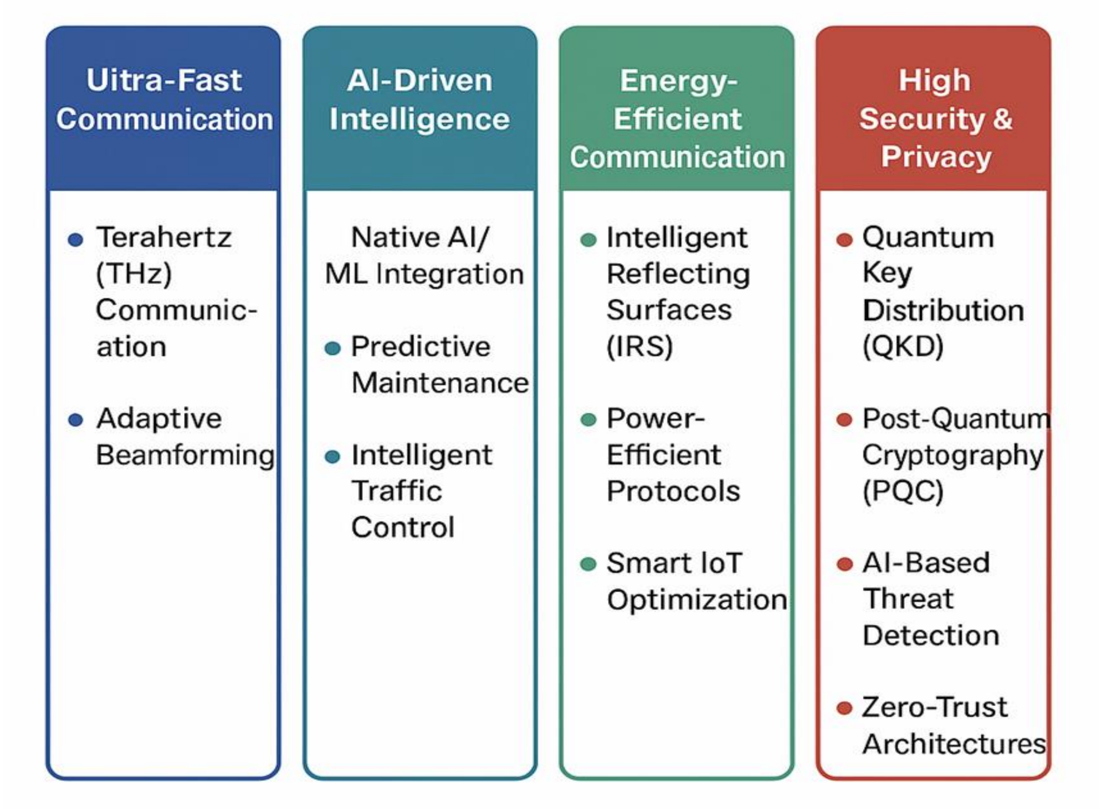
Uitra-Fast Communication
Terahertz (THz) Communic-ation
Adaptive Beamforming
AI-Driven Intelligence
Native AI/ ML Integration
Predictive Maintenance
Intelligent Traffic Control
Energy-Efficient Communication
Intelligent Reflecting Surfaces (IRS)
Power-Efficient Protocols
Smart IoT Optimization
High Security & Privacy
Quantum Key Distribution (QKD)
Post-Quantum Cryptography (PQC)
AI-Based Threat Detection
Zero-Trust Architectures

Fig. 1. Key Enabling Technologies of 6G Network Architecture

3.3 Security Challenges in 6G Networks

Although 6G networks offer revolutionary improvements in speed, latency, connectivity and intelligence,6Gstater networks also bring an array of new and complex security challenges. The extensive architecture of 6G – with ultra-dense connectivity, inter-satellite links, and decentralization – significantly widens the attack surface of the network. With the expansion of wireless networks, attacks like eavesdropping, spoofing, jamming and Distributed Denial-of-Service (DDoS) attack will become larger and more sophisticated [16].

The use of AI and ML in the core network functions allows them to autonomously operate, predict trends and optimize in real-time. But those same technologies are also creating new weaknesses. Adversarial Machine Learning (AML) is the most notable threat, where attackers sow misleading data to influence model responses. Attacks such as data poisoning and model inversion compromise the reliability of AI services in the most important applications such as healthcare, transportation and defense [17].

The changes to the computing paradigm from centralized to edge and fog complicates the security in 6G. In contrast to 6G, the centralized processing 6G is working independently, which is expected to make it more vulnerable with localized compromise when it helps isolate data servers from data senders. For instance, Sybil attacks can destroy trust in an edge environment, when a malicious actor pretends to be many nodes. Identity management and scalable authentication of millions of different edge devices may be a most challenging problem [16].

Moreover, the down-the-road menace of quantum computing should not be overlooked either. Many traditional public key cryptography systems (e.g., RSA and ECC) can be broken by quantum computers, strong quantum computers have yet to be developed. To address this issue, 6G systems have to migrate to post-quantum cryptographic mechanisms as well as employ Quantum Key Distribution (QKD) that offers a proven security based on the quantum physics. QKD allows for secure key exchange that is invulnerable to both classical and quantum attacks.

The massive density of 6G devices expected (10 million devices per square kilometer or more), requires lightweight, scalable and energy-efficient security solutions. Conventional security solutions can be resource-consuming and infeasible for limited devices including sensors, wearables and autonomous robots. Therefore, AI based, real-time adaptive security architectures will be needed in order to identify and react to malware or threats, without dropping performance and battery life.

Finally, security in 6G will also involve trust relationship building in various multi-stakeholder domains, which must involve context-aware dynamic and autonomous security policies. Static, uniform security postures will be insufficient. New models including continuous authentication, behavior-based intrusion detection, and collaborative threat intelligence sharing will underpin secure architectures for the future [18]. In summary, the main 6G technological domains most exposed to new security attacks are summarized in table 5.

TABLE V. EMERGING SECURITY CHALLENGES IN 6G NETWORKS ACROSS KEY TECHNOLOGICAL DOMAINS

Category	Security Challenge	Example Threats
AI/ML Integration	Vulnerability to adversarial learning	Data poisoning, model inversion
Device Density	Massively expanded attack surface	DDoS attacks, unauthorized access, identity spoofing
Network Decentralization	Complex trust and access control	Sybil attacks, compromised edge devices
Quantum Threats	Obsolescence of classical cryptography	Post-quantum attacks on RSA, ECC, etc.
Edge Computing	Data confidentiality and integrity risks	Eavesdropping, data tampering at local nodes

3.4 Comparison with 5G Security Paradigms

The 5G networks brought major advancements in network security thanks to evolution in encryption and better authentication models; however they still rely on traditional cryptography, which is weak against quantum decryption attacks. With advancement of quantum-computing, deficiencies of 5G security are more noticeable [18].

By contrast, 6G will be expected to provide quantum-safe cryptographic algorithms and Quantum Key Distribution (QKD) mechanisms from the beginning, offering long-term security protection against adversaries utilizing quantum tools of their own. This transition represents a general change in the understanding and realization of security in mobile networks.

Another important differnece is that of trust model. Though 5G is mainly perimeter security, taking access as a security guaranteed to be secure once it is within the network boundaries, 6G is expected to be zero-trust security architecture, meaning that authentication and verification need to occur all the time for all users, devices, and applications, no matter the location or tier of the network [19]. Combining with software-defined networking (SDN) and network slicing, this model requires context-aware, adaptive, and dynamic security solutions that must react to threats in real-time within a non-centralized environment.

And the use of AI in security varies similarly. In 5G, AI is used passively, reactively used (for example, anomaly detection). But 6G imagines it with AI deeply embedded, which is already working in real time to analyze threats, make decisions and adjust tools automatically. A summary comparison of security paradigms is presented in Table 6 between 5G and future 6G network.

TABLE VI. COMPARATIVE OVERVIEW OF SECURITY FEATURES IN 5G AND 6G NETWORKS

Security Feature	5G	6G (Expected)
Encryption	Classical cryptography (e.g., RSA, ECC)	Quantum-safe algorithms (e.g., lattice-based) and Quantum Key Distribution (QKD)
Trust Model	Perimeter-based	Zero-trust architecture with explicit authentication at all levels
AI Integration for Security	Limited, anomaly-based detection	Native AI for real-time threat prediction and autonomous response
Authentication Mechanisms	Centralized (e.g., SIM-based, PKI)	Distributed identity using blockchain and decentralized identifiers
Quantum Vulnerability	High vulnerability to quantum decryption	Resilient via post-quantum cryptography and QKD
Identity Management	Operator-managed SIM-based systems	Decentralized identity frameworks, including self-sovereign ID models
Security Policy Management	Manual and rule-based	Context-aware, AI-driven, dynamically adaptable security policies
Edge Computing Security	Basic edge node protection	AI-enhanced with lightweight cryptographic schemes for resource-constrained devices
Attack Surface	Moderate—control remains centralized	Very high due to massive IoT, device diversity, and decentralization—requires multi-layered defense
Resilience and Recovery	Lacks built-in resilience features	Built-in redundancy, blockchain-based consensus, and self-healing mechanisms

4. QUANTUM KEY DISTRIBUTION (QKD)

4.1 Quantum Cryptography

Quantum cryptography is a pioneering technology, which exploits the basic principles of quantum physics to provide information-theoretic security for communication purposes. Quantum cryptography, in contrast to methods based on conventional encryption algorithms (such as AES), also leverage the laws of physics (namely, superposition and entanglement) to communicate secure keys and guarantees the secrecy of data sent over a quantum channel.

The most established and common use of quantum cryptography is Quantum Key Distribution (QKD) that provides a secure way to exchange shared cryptographic keys between two parties, even if the communication channel is untrusted or attacked in a compromised way [20]. Quantum cryptography is based on two fundamental principles of quantum physics:

a) Heisenberg Principle of Uncertainty: A quantum state must be disturbed in measuring it, and a legitimate user is able to detect eavesdroppers.

b) No-Cloning: which means it is not possible to make an identical copy of a quantum unknown state, making qubits resistant to an unobserved in- terception and duplication of the qubits to bypass the system [21].

This yields the interesting property that if anyone tries to eavesdrop the quantum information, he needs to intercept the information and the eavesdropping introduces observable abnormalities and lead to strong security verification in the presence of eavesdropping for the communicating entities to react in time to the security threat.

Moreover, quantum entanglement is essential for some QKD schemes. Entangled particles show correlated quantum states and the measurement of one particle immediately affects the state of the entangled partner. In the case of net-pairings, any oblivious observer who polices this entanglement will disturb this correlation, with the result that one can detect whether or not any observations on the entangled system have been made [22,23].

4.2 QKD Protocols

Over the past few decades, several QKD protocols have been developed, each leveraging different quantum phenomena to achieve secure key distribution. Among these, BB84 and E91 are the most established and foundational.

3.2.1 BB84 Protocol

The BB84 protocol is the first and best studied QKD protocol by Bennett and Brassard in 1984. In BB84, Alice sends qubits encoded in one of four polarization states of light, which she selects uniformly at random by using two mutually unbiased bases: rectilinear ($|0\rangle$, $|1\rangle$) and diagonal ($|+\rangle$, $|-\rangle$). The receiver, Bob, measures each qubit in his randomly chosen basis.

After the bits are sent, Alice and Bob publicly compare which bases were used fall us neither the actual bit values and discard the bits for which the bases results is different. The output is a common secret key. It is also observable that if any of the signals are intercepted during the quantum channel, it will result in measurement-induced disturbances by the eavesdropper (Eve), thus introducing detectable errors which can be detected in error rate analysis in a subsequent reconciliation step [24].

3.2.2 E91 Protocol

Proposed by Artur Ekert in 1991, the E91 protocol is based on entanglement, rather than on the direct transmission of qubits. In this protocol a source of entangled photons sends one photon to Alice and the other to Bob. If Alice and Bob measure their own photons by a suitable bases, the observations have strong correlations by quantum entanglement.

Security of E91 is certified by Bell's theorem – more precisely, the violation of Bell's inequality. When an eavesdropper intercepts the entangled photons, the quantum correlations are destroyed, and Alice and Bob are notified of an intrusion. This leads to the fact that E91 is a common method for use cases, which require high confidence in security of QKD [25].

Table 7 summarizes and compares both the fundamental QKD protocols (BB84 and E91) based on their operational mechanism, the provided security and practicability.

TABLE VII. COMPARISON OF BB84 AND E91 QUANTUM KEY DISTRIBUTION PROTOCOLS

Feature	BB84 Protocol	E91 Protocol
Year Introduced	1984	1991
Underlying Principle	Quantum superposition	Quantum entanglement
Key Distribution Method	Measurement of randomly polarized qubits	Use of entangled photon pairs with correlated outcomes
Security Basis	No-cloning theorem, Heisenberg uncertainty principle	Bell's inequality violation
Eavesdropping Detection	Error rates during basis comparison	Disturbances in entanglement correlations
Implementation Complexity	Lower—requires single-photon sources	Higher—requires entangled photon sources and detectors

4.3 QKD Network Architectures

The architectural elements of so called quantum key distribution (QKD) networks are the basis of the secure way for transmitting sensitive information long distance based on quantum principles between small and large scale systems. These networks are integral to quantum secure exchanges of cryptogr aphic keys, and in operation are invulnerable to both classical and quantum computational attacks. According to the scale, purposes and technical limitations, multiple QKD architectures are proposed and implemented.

(a) Point-to-Point QKD Networks

The point to point (P2P) one is the simplest and straight forward QKD form. The protocol features two party, typically referred to as Alice and Bob, sharing a dedicated quantum channel, which is typically assumed to be an optical fibre or free-space optics.

Although this architecture provides high security and low complexity it is limited by distance scalabilty. Quantum signals, in particular single photons, become attenuated and suffer from decoherence, which restricts the potential transmission range. In a practical implementation, the maximum range over optical fibers for QKD is typically limited to 100–150 km, as beyond this point significant signal degradation is suffered [6].

b) QKD networks with Quantum Repeaters

In order to break the range restriction of the point-to-point QKD, quantum repeaters, i.e., QKD relay nodes which cascade to extend the coverage of QKD, have been suggested in the literature. Quantum repeaters break the whole distance into smaller ones and use entanglement swapping and quantum memory techniques to generate entanglement over longer distances.

This method supports worldwide QKD networks that could act as the basis for a quantum Internet. Nevertheless, quantum repeaters are predominantly experimental devices, and have to cope with problems related to hardware complexity, error correction, and maintaining the fidelity [7].

c) Exemplars of Satellite-Based QKD Networks

Satellite-based QKD enables a promising strategy to achieve global QKD service beyond the limitations of terrestrial resources. Quantum keys can be distributed between >1,000 km remote ground stations thanks to the use of low-Earth orbit (LEO) satellites.

This was realized in the space-to-earth direction, already by the Chinese Micius satellite (launched in 2016), where it proved that one can distribute quantum entanglement and perform QKD between space and ground stations. In this architecture, the problems of the attenuation of fibers are not present and hence allow the implementation of intercontinental and interplanetary quantum-secured communications [8]. Figure 2: Three most basic network topologies for QKD: direct point-topoint connections, Q-repeater-enhanced segments for long range land communication, and satellite quantum key exchange.

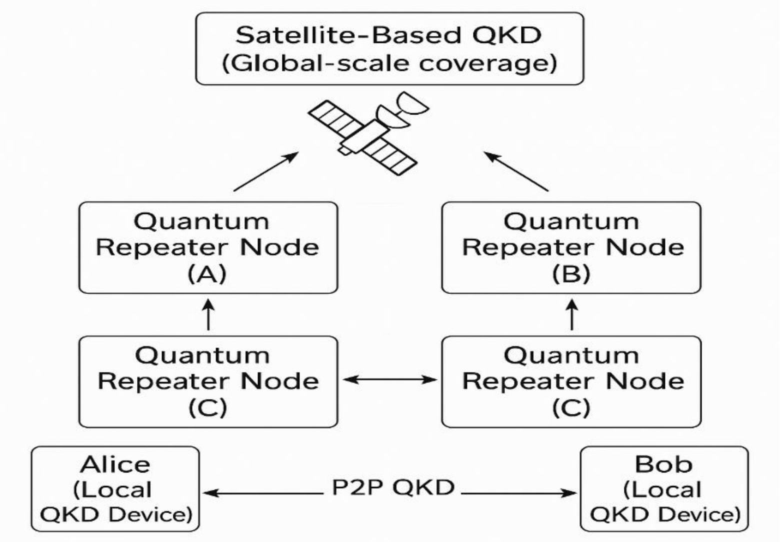
Satellite-Based QKD (Global-scale coverage)
Quantum Repeater Node (A)
Quantum Repeater Node (B)
Quantum Repeater Node (C)
Quantum Repeater Node (C)
Alice (Local QKD Device)
P2P QKD
Bob (Local QKD Device)

Fig. 2. Architectures of QKD Networks

4.4 Benefits and Limitations of QKD

The Quantum Key Distribution (QKD) is considered one of the most remarkable security solution which provides an information-theoretic secure directive using the fundamental physics from quantum mechanics rather then the computational remainder assumptions. Contrary to classical cryptography, which may be broken by quantum computing, QKD offers unconditional security that remains secure against the most sophisticated quantum attacks that are only developed later.

QKD has one of it's biggest strengths in its ability to detect eavesdropping intrinsically. Any eavesdropping upon quantum keys inevitably influences the quantum state, because of the Heisenberg Uncertainty Principle that guarantees the presence of detectable imperfections of the key exchange. This enables not only confidentiality but also active intrusion detection, so that QKD becomes a promising candidate for critical and privacy sensitive 6G applications.

Despite its potential, there are many practical and engineering obstacles that prevent the large-scale commercialization of QKD. The most critical issue is transmission distance: quantum signals become unstable in long fibers by photon decoherence and attenuation. Quantum repeaters, although designed to enhance coverage, exist at the experimental stage and are not commercially available.

In addition, QKD infrastructure requires sophisticated technology and is expensive. The specialized use of precision equipment–single photon detectors, quantum entanglement sources, cryogenic cooling– can make deployments cost prohibitive, and extensions to larger scale terrestrial networks is expensive.

A further issue is that QKD systems are vulnerable to side-channel attacks that take advantage of unintended information leakages resulting from hardware imperfections. For example, adversaries can utilize differences in detector efficiencies or filtering timing to deduce secret key bits. Hence the security of QKD in practice relies not merely on quantum aspects but also on sound hardware engineering and physical security auditing. As summarised in Table 8, QKD offers a fundamental departure from classical secure communication in line with the 6G vision, nevertheless, its realisation in practice requires the resolution of significant challenges through research, technology development and standardisation.

TABLE VIII. BENEFITS AND LIMITATIONS OF QKD

Category	Benefits	Limitations
Security	Unbreakable by quantum or classical attacks; real-time eavesdrop detection	Susceptible to side-channel attacks due to hardware imperfections
Performance	Future-proof encryption beyond post-quantum cryptography	Distance-limited key exchange without quantum repeaters
Implementation	Can operate alongside classical cryptosystems for hybrid security setups	Requires high-cost, high-precision quantum hardware infrastructure
Scalability	Suitable for global QKD via satellite and fiber integration in 6G	Challenging mass deployment in dense urban and mobile environments

5. INTEGRATION OF QKD IN 6G NETWORKS

5.1 Architectural Models for QKD Integration

As 6G seeks to reshape the future of secure communications, Quantum Key Distribution (QKD) will need to be integrated into the emerging system architecture with practical and scalable considerations. Instead of replacing existing infrastructure, hybrid classical-quantum model is a potential solution. It makes use of quantum links for key distribution and classical channels for data communication. This model allows for an incremental rollout of QKD, ionizing existing telecom investment in a non-reliance upon a wholesale retrofit [26].

Yet another proposed scheme is that of centralized management of QKD, where a service called Quantum Key Management Server (QKMS) securely disseminates the keys generated from quantum in the 6G network across the end nodes. Then, those QKMS nodes, which are deployed on the main network or data centers, can use PTP-based QKD or quantum repeater to securely deliver distributed key to mobile base stations and edge devices. Note that this trusted-node model, so far applicable to small networks, is non-scalable, and, more importantly, it gives rise to trust on the nodes, and can challenge the otherwise unconditionally secure nature of QKD [2].

Scalability and mobility may be alleviated in the future by integrating satellite QKD systems and Software Defined Networking (SDN) into the architectures. Satellite QKD avoids range limitations intrinsic to terrestrial optical fibers, and allows directly transmitting quantum-secured keys around the globe. Meanwhile, SDN will enable the QP to be controlled dynamically, allocate bandwidth and manage keys according to real-time traffic requirements. This flexibility is crucial for enabling the variety of 6G use cases (e.g., URLLC and mMTC) [27].

5.2 Hardware and Implementation Considerations

The application of QKD in 6G networks brings impressive hardware challenges. Key elements like single-photon sources, and detectors need to be made micro in size and co-integrated with conventional radio hardware in particular at BS and UE. These devices, which are essential to both qubit generation and detection, must exhibit high detection efficiency, low noise and operate at gigabit transmission rates. However, obtaining such performance in a mobile and energy-limited environment is still a considerable challenge [28].

A second important requirement is the inclusion of QRNGs. These provide strong entropic keys and are to be implemented in network devices like routers, access points, and potentially smartphones. Novel technologies, such as photonic integration, are being explored to integrate these components into small footprint and low power QKD modules that are suitable for mobile edge computing in 6G [5].

Furthermore, quantum-compatible transceivers and network interfaces - such as tunable lasers, entangled photon sources, and polarization controllers - must be co-designed with classical optical and RF systems. These elements should be highly resilient to environmental dynamics such as mobility, vibrations and noise, especially in scenarios involving UAVs, vehicular networks and satellite-based systems [29]. Fig. 3: A complete architecture model for integrating QKD in 6G secure communication systems including the ground, satellite, and SDN-enabled planes.

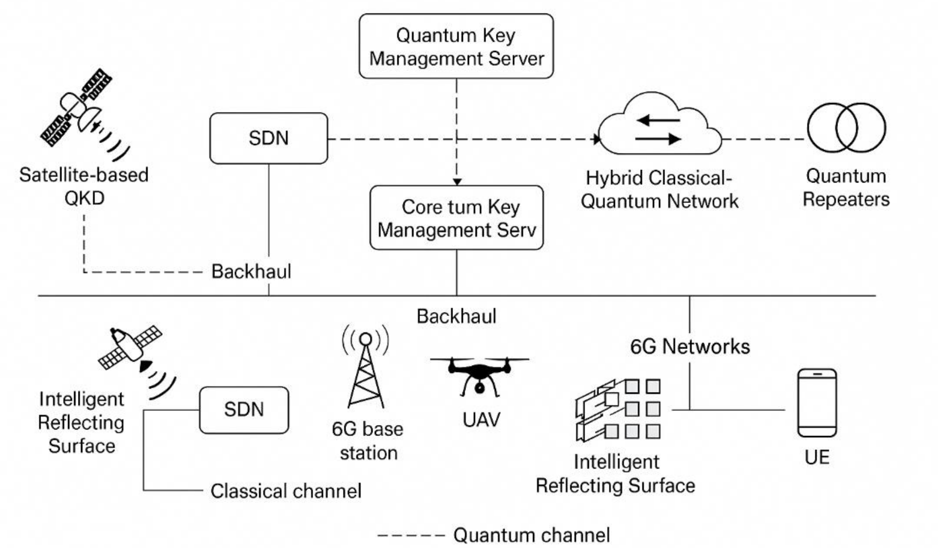
Quantum Key Management Server
Satellite-based QKD
SDN
Hybrid Classical-Quantum Network
Quantum Repeaters
Core tum Key Management Serv
Backhaul
Backhaul
6G Networks
Intelligent Reflecting Surface
SDN
6G base station
UAV
Intelligent Reflecting Surface
UE
Classical channel
Quantum channel

Fig. 3. Architectural Model for Integration of Quantum Key Distribution into Secure Communication Networks

5.3 Software and Protocol Adaptations

A successful usage of QKD in 6G would demand for major modifications on the software layer. All conventional cryptography like RSA and Diffie-Hellman would need to be refactored or replaced in order to use keys derived from QKD. For example, it is possible to adapt the current implementation of IPSec or TLS protocols to use session keys provided by externally QKD modules for providing forward secrecy in the post-quantum world [30].

Quantum Key Management Systems (QKMS) serve as middleware to manage the issuing, revoking, and synchronization of quantum keys between different devices and applications. Software-defined policies are to be created to perform context-aware quantum key usage and priority in QKD protection for mission-critical applications (e.g., autonomous vehicles, smart cities, or healthcare IoT) [28].

Furthermore, networking software will have to be adapted to take advantage of QKD-aware routing and traffic engineering. Quantum-secured resources can be reserved programmatically for virtual network slices with different security assurance levels using SDN and NFV. For instance, a UAV fleet coordination slice may require more stringent QKD protection than a video-streaming service -optimal usage of quantum resources [29].

4.4 Compatibility analysis of 6G components with the existing componentry

In order for QKD to become practically viable in the 6G systems, it shall harmoniously interwork with the key enabling technologies, e.g., THz communication, IRS, and massive MIMO. Due to the fact that the QKD protocol itself mostly works in the optical domain, it is important to carefully design the hybrid RF-optical system, so as to make spectrum resources accessible to RF and optical systems without interfering with each other. Then the THz band could be used for ultra high speed data transfer and the QKD technique could secure the control and key exchange layers [31].

In addition, integration of QKD with Multi-Access Edge Computing (MEC) and AI-native 6G architectures will be key. The edge nodes have to provide not only computation and quantum interface, but come with local key generation and local key exchange. AI algorithms are used to optimally utilize QKD and manage the allocation of entangled resources, detect eavesdropping attempts, and dynamically adjust security policies in light of network conditions [11].

Finally, backwards compatibility with 5G infrastructure and legacy systems is crucial to ensure a smooth migration process. QKD solutions have to interact with actual cryptographic APIs and transport phase. The presence of QKD and QKEI techniques can lead to hybrid DEs, where legacy and quantum-aware nodes are protected and operated for a while in parallel between two different periods [32].

6. REVIEW OF EXISTING RESEARCH

6.1 QKD Integration in Next-Generation Networks

Quantum Key Distribution (QKD) Quantum Key Distribution (QKD) is rapidly gaining popularity as a game-changing technology for use in future secure communication systems based on foundational quantum principles. Unlike conventional cryptosystems, which are only based on computational hardness, QKD protocols (e.g., BB84 and E91) exploit the intrinsic laws of nature for their security [33].

This is an interesting advancement as it showed that QKD can be conducted using telecommunication (fiber-optic) networks with quantum and classical signals sharing the same channel. In particular, [34] also demonstrated a successful use of QKD in metropolitan fiber networks, showing that QKD is easily integrable into existing systems and can already be considered as a practical technology.

Furthermore, QKD is getting integrated with Software-Defined Networking (SDN) and Network Function Virtualization (NFV). An interesting work [4] presented an SDN-control plane for dynamic, real-time management of QKD resources that supports adaptive and policy driven key management. This hybrid structure also provides secure quantum channels concomitantly with the conventional network services, which gives secure communication systems more reliability and flexibility.

Satellite-based QKD has also been found to be a promising tool for the extension of secure communication into space. Another significant experiment realized QKE between the opposite sides of satellite-based channels over 1200 km despite the atmospheric losses and synchronization issues [35]. These results indicate the feasibility of global quantum-secure infrastructure complemented by satellites. Nevertheless, the scalability of QKD is still restricted by the key generation rate, the integration complexity, and the standardization. Bodies like the ETSI ISG QKD are pushing towards the development of certification schemes and standards for easier commercial adoption of QKD [36]. It would be important in the future to focus on optimising the hardware, fine-tuning error correcting codes for fault tolerance, and developing advanced network management protocols for full deployment in the future.

6.2 QKD performance in simulated 6G dilemma Here we consider the effect of 6G dilemma on QKD performance.

The use of QKD in 6G scenarios poses new challenges and possibilities. 6G targets ultra-high data rates, ultra-low latency, and ultra-dense connections, which requires novel security schemes. Since 6G architectures are anticipated to combine terrestrial and non-terrestrial networks, simulation tools combined with quantum channel models are being employed to assess QKD performance in such scenarios.

The QKD performance metrics including secret key rate, QBER, and latency have been analyzed through 6G traffic [37]. These simulations demonstrate the resilience of QKD to the highly dynamic and dense nature of 6G environments.

Specifically, multi-user simulations of 6G networks have included QKD-enabled links for studying coexistence with classical communication. Optimal wavelength assignment and noise mitigation schemes were shown to remarkably increase the key rates, despite large loads of classical traffic in the research in [38]. These results highlight the necessity of proactive key management which reacts to dynamic network conditions so as to maintain efficient and seamless key establishment.

Furthermore, hybrid approaches, where QKD is combined with post-quantum cryptography (PQC), have been considered in simulated 6G stacks. For instance, [39] considered stacked security architectures based on both QKD and PQC that provided additional robustness against quantum and classical adversaries. Investigations show that hybrid architectures are capable of solving the limitation on bandwidth and making the network robust enough.

However, the distance from theoretical performance to practical usage is vast. The Real-world practical problems, such as quantum channel noises, network congestion and the loose integration of movement are also required to solve in high-mobility DRN. Better simulation fidelity, testing based on real-world, and cross-disciplinary cooperation are required to transfer these results into operational 6G networks [5].

6.3 Hybrid Classical–Quantum Security Solutions

To ease the shift towards entirely quantum-secure communication, security standards have been proposed where QKD is combined with classical cryptographic protocols. They provide the proven security of QKD for key exchange together with the scalability and operational maturity of classical encryption algorithms, such as AES [1] and PQC [2].

One of the architectural approaches would be the application of QKD-assisted Virtual Private Networks (VPNs) and secure Multi-Protocol Label Switching (MPLS) in which seeds keys for symmetric encryption are quantum-generated keys. An approach [3] explored integration of QKD key refresh with PQC for enterprise related networks and found that significant enhancements may be made for key renewal rates and resilience at little or no overhead to legacy infrastructure.

Other developments are in the form of dynamic security key management protocols that intermix QKD and PQC keys according to both network condition and security requirements [40]. The intelligent switch mechanism improves the utility of resources and guarantees the great security for the bandwidth- and latency-limited condition.

Nevertheless, there are still several hurdles preventing widespread application. A lack of established proscription and interoperability between quantum and classical systems makes integration difficult. Organizations like IEEE P3340 and ETSI ISG QKD endeavor to develop standardized profiles, threat models, and testing approaches, which ensure end-to-end security in heterogeneous systems [5].

6.4 Research Gaps & Future Directions

Despite immense advancement, there still exist many open issues, which have to be resolved for successful deployment of QKD in the next-generation networks:

a) Scale and Scalability of 6G Networks: Most existing QKD systems are typically not suitable for high-mobility and large-scale (as might be expected in 6G) networks with their inherent limited key generation rate, often coupled with a short transmission distance due to quantum channel loss and hardware limitations [29].

b) Quantum–Classical Interoperability: While coexistence has been shown in a controlled setting, in the real world, the presence of noise, interference and crosstalk in networks can adversely affect QKD [31]. Adaptive schemes to direct the allocation of QKD resources in presence of such scenarios are in earlier stages [33].

c) Standardisation and Certification: Because there are no standardised methods for hybrid classical–quantum systems, the security assurance would be unclear. There are ETSI and IEEE efforts to fix this, but complete security frameworks and certification processes are on the way [5].

d) Experimental Verification: Virtually all work until now relies on simulation or on a limited-size testbed. In a complex environment that also includes satellite integration, dynamics of users-mobile and ultra-low latency needs for instance, real-world validation is necessary [26]. Large pilot projects and cooperative research are important to overcome the lab-to-field barrier.

Closing these gaps is necessary for QKD to mature from a laboratory innovation into a deployable service that is secure and interoperable for future communications.

7. FUTURE DIRECTIONS

7.1 Quantum-Secured Networking Trends

Quantum-secured networking is growing quickly thanks to accelerating progress in quantum devices, protocol enhancements and creative network designs. An important development is the study of hybrid quantum-classical computational schemes with objectives of providing scalable and adaptive security in the context of integrated networking. Quantum miniaturization of devices—ranging from chip-integrated photon sources and detectors—enables Quantum Key Distribution (QKD) for mobile and IoT devices, and brings quantum security from only static fiber-based infrastructure to a mobile environment.

In addition, quantum repeaters and entanglement swapping have been regarded as key techniques to overpass the distance constraint in quantum communications and to realized secure long distance communication. In the network layer, which is at the foundation of great research attraction, researches are also proposed to form the multi-path key distribution and develop quantum-resilient routing protocols to increase the fault tolerance and decrease the vulnerabilities in adversarial attacks or node faults. Taken together, these developments indicate a realistic path toward integrating- quantum-secured technologies into next-generation communication networks.

7.2 Role of AI/ML in Advancing QKD

AI and ML are enabling technologies which revolutionize the optimization of QKD technologies by addressing performance bottlenecks and improving resilience. AI can be used to improve error correction and privacy amplification to achieve a higher Secret Key Rate (SKR) and a lower Quantum Bit Error Rate (QBER) in QKD. Opposite to static algorithms, adaptive techniques developed by AI, in particular reinforcement learning and NN based decoders, provide the ability to adapt in real time to an evolving quantum channel and to adversarial parties, potentially increasing robustness and efficiency of key generation.

In addition to protocol optimization, ML also enhances the hardware reliability of QKD modules such as photodetectors and sources. These quantum processors are subject to environmental variation and hardware decay. Machine learning-based predictive maintenance models, which analyze operational telemetry to forecast potential breakdowns or degradation before they happen and preempt service interruptions. Moreover, malicious activities, e.g., eavesdropping, can be detected through anomaly detection algorithms, adding layers to the security monitoring one.

As QKD scale in large networks, AI will be used as resource service allocation orchestration, network routing, and dynamic key management. Smart algorithms optimize the use of scarce quantum resources (e.g., repeaters, trusted nodes) when traffic and user mobility is volatile. In addition, ML-based key scheduling mechanisms could contribute to balance refresh rates and key distribution among heterogeneous nodes in such a way that performance and security can be secured.

AI also enables a hybrid cryptographic approach, in which a dynamic switching of quantum key sources, between classical encryption and quantum keys, is performed in real-time by means of real-time security assessments. Simulation pave the way towards design and offline testing of new QKD protocols in different networking environments based on AI and reduce development cost, and time-to-deployment. This integration of AI and quantum technology is key to migrating QKD from controlled laboratory-based scenarios to practical, intelligent and expandable secure communication infrastructure.

7.3 Toward a Quantum-Resilient Infrastructure for 6G Networks

With 6G networks on the horizon, creating a quantum-resilient infrastructure will be critical to address new threats posed by quantum computers. This infrastructure should include up to both QKD for secure key-exchange and Post-quantum Cryptography (PQC) enabling multi-layer security profiles in the protocol stacks.

Quantum-safe techniques such as secure authentication, data encryption, and network slicing must be incorporated into 6G system design in order to guarantee the confidentiality and integrity of data in the face of possible quantum-level attacks. The simultaneous studies on Quantum Compatible hardware design and Low Latency enabling Materials optimised for harsh 6G application requirements will also be addressed.

Designing systems with these capabilities requires interdisciplinary cooperation between classical network engineers and quantum physicists to define standard, interoperable frameworks that can incorporate quantum security features seamlessly. The quantum-fortified 6G infrastructure that emerges will form the basis for secure communications in the era of post-quantum computing.

7.4 Suggested Research Roadmap

In the meanwhile and in order to completely harvest the impact of quantum-based secured communications in the future networks, an agreed research agenda with collaboration is needed. Priority research areas include:

a. Improvement of the scalability of quantum hardware, in particular with high-rate single-photon sources and ultra-low-noise detectors.
b. Creating accurate quantum channel models and simulation platforms that support network-level dynamics, user mobility and noise conditions.
c. To define open standards and cross-platform interoperability frameworks for hybrid classical-quantum security integration.
d. Co-creating cross-disciplinary research reaching from quantum physics and cryptographic protocol design to network engineering for solving system-wide problems such as dynamic key formation, orchestration, and side-channel attack mitigation.
e. Scaling up testbeds and pilot deployment in real world environments to support proving technologies and refining the regulatory and industrial practices.

It will consist of a strategic roadmap to move QKD beyond theoretical concepts and experiments to deployed, scalable, and secure communication systems essential to 6G and beyond.

8. SUMMARY OF FINDINGS

In this paper, we have performed a comprehensive review of QKD based technologies in the context of emerging 6G communication networks. The review emphasized substantial progress on quantum hardware, protocol development, and hybrid quantum-classical architecture, toward overcoming central challenges such as communication distance and key generation rate.

Through simulative analysis over 6G network scenario, it is found that while QKD can guarantee the communication security, the practical implementation is challenged by practical factors such as the dynamics of mobile users, environmental noise and the dynamic networking among nodes. To deal with these problems, hybrid security models, by combining QKD with classical cryptosystems, appear to be a solution to build threat-resilient and flexible security infrastructures, which are able to survive on a wide range of threat models.

Additionally, this work recognized Artificial Intelligence (AI) and Machine Learning (ML) as the disruptive technologies, which add the most value to the QKD systems. These smart tools enable adaptive error correction, predictive hardware maintenance, and real-time network orchestration, to achieve peak key rates, reliability and operational efficiency in dynamic scenarios.

However, many fundamental problems are still unresolved for the practical QKD systems even with the existing developments. Among these are the realization of scalable quantum repeaters, the standardization of QKD protocols, and the demonstration of quantum-secured systems in commercial real-world networks. Connecting the theory with practical implementations will be an important step towards moving QKD out of the chemistry lab and into the field.

8.1. Final Remarks on QKD in the 6G Era

As the 6G vision continues to crystallize, with expected ultra-high data rates, ultra-low latency, all-pervasive AI, and extremely high density of devices, the need for a quantum-safe communication infrastructure is inevitable. QKD, based on the law of quantum mechanics, guarantees information-theoretic security against even next-generation quantum computer [9]. However, 6G integration of LiFi entails a complex set of challenges.

These challenges relate to the fact that quantum hardware should be integrated in mobile and heterogeneous infrastructures, must work in presence with classical RF signals and must satisfy the restrictions on mobile devices [11]. Furthermore, the distributed and dynamic characteristics of 6G necessitate the novel design of flexible quantum networking architectures to enable efficient routing, linking, and quantum resource management.

The collaborative adoption of QKD together with Post-Quantum Cryptography (PQC) and AI-aided network intelligence will be critical for realizing security defense in depth, adaptiveness and scalability. This hybrid QKD scheme makes the technology more than a theoretical dream – it makes the tech a practical necessity of the future internet infrastructure.

8.2. Research and Practical Implications

It is imperative for future studies to address these theoretical and practical constraints, in an attempt to bridge the gap between QKD on benches and QKD inside the context of 6G systems. Key focus areas include:

a. The development of quantum hardware technologies, eg. high-rate photon sources, low-noise single-photon detectors and quantum repeaters, to realize global-scale secure communication [13].
b. Establishing realistic quantum channel models in the presence of the physical and architectural attributes of 6G type environment, which incorporates mobility and heterogeneous groups [14].
c. Defining standard protocols and providing with an interoperability ecosystems that enable large scale deployability and industrial adoption in cooperation with academia, industry and regulators [15].
d. Integration of AI/ML towards automating key management, anomaly detection, and network resource management in self-healing quantum-secured networks [17].
e. Contributing to the establishment of pilot testbeds and large scale field trials to prove QKD performance under operational conditions, and to promote the technology pick up from R&D to manufacturing [18].

Cross-disciplinary work between quantum physicists, communication engineers, cybersecurity experts, and AI researchers is also necessary to solve systemic and interdisciplinary challenges. Work Package 1, Theorey, Experiment on theory-to-experiment-to-engineering QDSR&T in future 6G networks: Theory-to-Experiment-to-Engineering alignment for the development of Quantum-Defended Secure Routing and Transmission (QDSR&T) within future 6G networks. Fig. 4 Graphically illustrates the phased process of the development path, from the initial theoretical frameworks to full deployment of QKD for 6G networks, including hardware innovation, protocol standardization, AI integration and testbed validation.

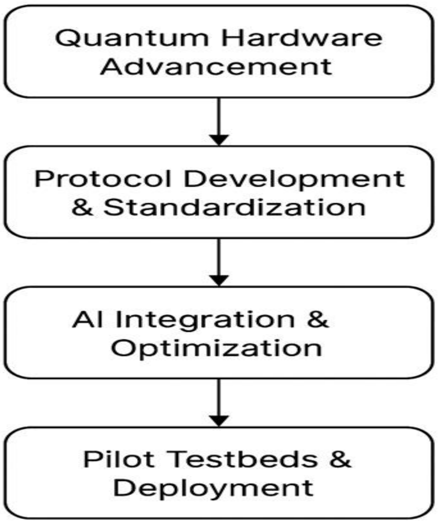
Quantum Hardware Advancement
Protocol Development & Standardization
AI Integration & Optimization
Pilot Testbeds & Deployment

Fig. 4. Research Roadmap for Scalable QKD in 6G.

8. CONCLUSION

The path to 6-th generation (6G) wireless networks is expected to bring revolutionary data rates, ultra-low latency, and new levels of connectivity. But these advances come with increased exposure of network infrastructures to ever more advanced security threats, most significantly those introduced by quantum computing. This extensive review put QKD as a corner-stone technology for 6G communications. Based on the laws of quantum mechanics, QKD can be used to achieve unconditionally secure key distribution, which overcomes the security issues which underpin classical cryptography. Different aspects of QKD compose this study that range from its protocols, possible integration with classical system and its functions in hybrid security architectures. The results demonstrate the flexibility of QKD with respect to the integration with operational communication systems, and the successful addressing of key obstacles including latency, scalability, and deployability. Furthermore, the coupling to Artificial Intelligence (AI) and Machine Learning (ML) brings a new perspective to QKD applications. AI/ML-empowered QKD supports intelligent, adaptive QKD functionalities, e.g., key management, anomaly detection, and resource-efficient routing, and is a promising aspect to secure, automate, and self-healing 6G infrastructure. Nevertheless, a number of open problems remain to be addressed. These are quantum repeaters, standardised QKD protocols and the demonstration of quantum hardware in a real-world, practical network environment. To resolve these gaps, interdisciplinary work needs to be performed in areas between quantum physics, cybersecurity and telecommunication engineering. In the end, the vision of 6G needs to go beyond just being fast and automated. The most important priority for any new strategy is that secure-by-design is hard-coded into it from the start, to make sure that communication infrastructures are secure in a post-quantum world. It will be necessary for a combined deployment of QKD, PQC, and AI-driven intelligence to enable the foundation of future-proof quantum-safe communication systems.

Conflict of Interest

The authors declare that there is no conflict of interest.

Funding

This article does not contain any funding

Acknowledgment

The author would like to express gratitude to the institution for their invaluable support throughout this research project.

References

[1] M. Giordani, M. Polese, A. Roy, D. Castor, and M. Zorzi, “Toward 6G networks: Use cases and technologies,” *IEEE Commun. Mag.*, vol. 58, no. 3, pp. 55–61, Mar. 2020.

[2] W. Saad, M. Bennis, and M. Chen, “A vision of 6G wireless systems: Applications, trends, technologies, and open research problems,” *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May/Jun. 2020.

[3] H. Tataria et al., “6G wireless systems: Vision, requirements, challenges, insights, and opportunities,” *Proc. IEEE*, vol. 109, no. 7, pp. 1166–1199, Jul. 2021.

[4] P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Santa Fe, NM, USA, 1994, pp. 124–134.

[5] M. Mosca, “Cybersecurity in an era with quantum computers: Will we be ready?,” *IEEE Security Privacy*, vol. 16, no. 5, pp. 38–41, Sep.–Oct. 2018.

[6] N. Gisin et al., “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar. 2002.

[7] V. Scarani et al., “The security of practical quantum key distribution,” *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Sep. 2009.

[8] S. Dang, O. Amin, B. Shihada, and M. S. Alouini, “What should 6G be?,” *Nature Electronics*, vol. 3, no. 1, pp. 20–29, Jan. 2020.

[9] T. S. Rappaport et al., “Overview of millimeter wave communications for fifth-generation (5G) wireless networks—with a focus on propagation models,” *IEEE Trans. Antennas Propag.*, vol. 65, no. 12, pp. 6213–6230, Dec. 2017.

[10] M. Chen et al., “Artificial Intelligence for Wireless Networks: A Tutorial on Neural Networks,” *IEEE Commun. Surv. Tutor.*, vol. 22, no. 2, pp. 1265–1294, 2020.

[11] E. Basar et al., "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116753–116773, 2019.

[12] Z. Zhang et al., "6G wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 28–41, Sep. 2019.

[13] L. You et al., "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *Sci. China Inf. Sci.*, vol. 64, no. 1, pp. 1–16, 2021.

[14] S. Pirandola et al., "Advances in Quantum Cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, 2020.

[15] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–664, 1991.

[16] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing*, Bangalore, India, 1984, pp. 175–179.

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

[18] T. C. Ralph, A. P. Lund, and H. L. Haselgrove, "Experimental quantum communication systems," *New J. Phys.*, vol. 6, no. 1, pp. 63–73, 2004.

[19] L. Zhang et al., "Quantum key distribution network with a quantum repeater," *Nat. Photonics*, vol. 14, pp. 221–226, 2020.

[20] L. Gyongyosi and S. Imre, "A survey on quantum computing technology," *Comput. Sci. Rev.*, vol. 31, pp. 51–71, 2019.

[21] Z. Zhang et al., "Quantum secure networking for 6G: Challenges and solutions," *IEEE Netw.*, vol. 36, no. 4, pp. 72–79, Jul.–Aug. 2022.

[22] Y. Liu et al., "Integrated quantum photonics for quantum communication: Challenges and prospects," *Nat. Rev. Phys.*, vol. 4, pp. 412–428, 2022.

[23] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Inf.*, vol. 3, no. 1, pp. 1–13, 2017.

[24] M. Peev et al., "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, p. 075001, 2009.

[25] J. Qiu et al., "Software-defined quantum communication network architecture for 6G," *IEEE Wireless Commun.*, vol. 29, no. 4, pp. 90–96, Aug. 2022.

[26] I. Chlamtac and W. Wang, "Terahertz communications: Challenges and research opportunities," *IEEE Access*, vol. 7, pp. 107600–107620, 2019.

[27] Y. Li et al., "Intelligent secure communication in 6G: New paradigms and AI-driven solutions," *IEEE Netw.*, vol. 36, no. 6, pp. 73–79, Nov.–Dec. 2022.

[28] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, 2018.

[29] M. Giordani et al., "A Tutorial on BEYOND 5G Networks: Evolution and Innovation," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 1636–1677, 3rd Quarter 2020.

[30] I. F. Akyildiz, A. Kak, and S. Nie, "6G and Beyond: The Future of Wireless Communications Systems," *IEEE Access*, vol. 8, pp. 133995–134030, 2020.

[31] H. Shrobe et al., "6G Security and Privacy: Challenges and Research Directions," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 6, pp. 1799–1817, Jun. 2021.

[32] M. Chafii et al., "Security and Privacy Challenges in Beyond 5G Networks: A Survey," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1571–1594, 2021.

[33] L. Uden, A. Salim, and R. F. A. Costa, "6G: Vision, Challenges and Research Directions," in *Proc. Int. Conf. Information Technology & Systems (ICITS)*, 2022, pp. 345–354.

[34] A. Checko et al., "Standardization and Policy Requirements for Future 6G Networks," *IEEE Netw.*, vol. 36, no. 6, pp. 138–144, Dec. 2022.

[35] K. A. Patel et al., "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," *Appl. Phys. Lett.*, vol. 104, no. 5, p. 051123, 2014.

[36] L. Shen et al., "Software-defined networking based control plane for quantum key distribution networks," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 474–487, Mar. 2020.

[37] J.-P. Bourgoin et al., “A comprehensive design and performance analysis of low Earth orbit satellite quantum communication,” *New J. Phys.*, vol. 15, p. 023006, 2013.

[38] Y. Zhang, X. Chen, and J. Wu, “Performance analysis of quantum key distribution in 6G-enabled integrated networks,” *IEEE Access*, vol. 9, pp. 123456–123469, 2021.

[39] R. Kumar, T. Nguyen, and M. Pal, “Hybrid quantum-safe security framework for 6G networks: Simulation and performance evaluation,” *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 1, pp. 410–423, Jan.–Mar. 2022.

[40] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009.