Enhancing 6G Network Security with Quantum Key Distribution: A Comprehensive Review/ Review article

Bassma M. Kamil

Department of Electronics and Communications Engineering, Al-Ahliyya Amman University, Jordan

bassmamaki9492@gmail.com

Abstract

With the considerable progress of sixth-generation (6G) networks further on the horizon, security has attracted much attention in the face of increasingly sophisticated threats, especially from quantum computing. Classical cryptographic schemes based on computational hardness are becoming more and more brittle, as they can easily be attacked with a quantum computer. Quantum Key Distribution (QKD) arises as a promising tool for information-theoretic security through quantum mechanics to obtain an unbreakable key by exchanging unknown bit sequences. In this paper, we provide an extensive survey on the integration of QKD both in the envisioned 6G architecture, including current implementations, technical feasibility, and deployment of QKD in fiber-based and wireless scenarios. We compare performance metrics of QKD systems in simulating 6G systems such as secret key rates, quantum bit error rates, and robustness to noise and mobility. We propose and investigate hybrid security schemes to leverage both classical PQC and QKD technologies to build multilayered security shields. We highlight the importance of the Artificial Intelligence (AI) and Machine Learning (ML) in improving QKD systems in terms of smart error correction, dynamic routing, anomaly detection, and adaptive key management, and more. In spite of efforts, the paper points out important research challenges that remain to be addressed in scalability, standardization, cross-operation comparison and demonstration. We finally summarize new directions for quantum-secured networking, offering a future research agenda which combines AI, standardization works and real testbeds to deliver a QKD shift from a lab-scale proof of concept to global-scale 6G network adoption. This review serves as a useful reference for researchers and practitioners as they develop quantum-safe, next-generation communication networks.

Keywords: 6G Networks, Quantum Key Distribution (QKD), Network Security, Artificial Intelligence (AI), Machine Learning (ML), Post-Quantum Cryptography (PQC), Quantum-Resilient Infrastructure.

1. Introduction:

The worldwide deployment of sixth-generation (6G) systems will fundamentally transform wirelesscommunications by providing a multitude of disruptive features including terabit-per-second data rates,sub-millisecond latency, ubiquitous association, and native integration of artificial intelligence (AI) [1]. Such capabilities are intended to enable future technologies such as holographic telepresence, tactile internet, and machine autonomy. Nonetheless, the addition of these functionalities enlarges the attack surface and makes it more complex, thus augmenting the risks about privacy, integrity and authentication. In addition, the currently used security solutions for this type of wireless networks are not as well suited for 6G in a multi-dimensional security approach due to the complexity of it [2]. Hence next-generation networks demand new and future-proofed security solution and this has lead to a research challenging priority.

At the same time, the development of quantum computers is a major challenge to classical cryptographic schemes. Shor's and Grover's algorithms have shown that widely used public-key cryptosystems, such as RSA and ECC, are potentially breakable in polynomial time complexity [3]. As classical cryptographic schemes mentioned above are fundamental to existing internet and mobile network security protocols, their insecurity against quantum attacks urgently calls for rethinking for the security of future communication systems, i.e., 6G. The 'store now, decrypt later' threat model adds another vector to the importance of initiating security models that are resistant to quantum capabilities from the beginning [4,5]. This need provides a drive towards quantum-safe and quantum-enhanced security.

Quantum cryptography, in particular Quantum Key Distribution (QKD), offers a hopeful answer by using the phenomena of quantum mechanics in order to be able to obtain information-theoretic security [6]. Unlike conventional encryption, which can be cracked with sufficient computer power, QKD provides secure exchange of secret keys based on the principle that any attempt to eavesdrop will disturb quantum states in a way that can be detected, alerting users to eavesdroppers and making it impossible for a hacker to copy or intercept a key without being detected. BB84, E91, and Continuous Variable QKD are few of QKD protocols that have a lot of potential for secure communication [7]. Such technologies can provide a strong level of security guarantees for critical services such as finance, defense, autonomous vehicles, smart healthcare systems and others in the 6G framework.

In this paper, our aim is to present a survey of quantum-inspired security solutions for 6G networks. The paper takes a look into the basics of quantum cryptography, to provide a typology of the current protocols, to analyze the relevance of these protocols for 6G use cases, and to assess their strengths and weaknesses faced in practical environments. Furthermore, the paper provides an overview of existing experimental demonstrations, research projects, and pilot studies that intend to incorporate quantum communication technologies in future wireless networks. This survey, by delineating SLE vulnerabilities and listing open research questions, adds to the growing discussion on how to purposefully construct secure, quantum-proof communication infrastructures for the future.

The remaining part of this work is organized as follows: In Section 2 we describe the network architecture of 6G and security requirement of 6G. In Section 3, basic notions of quantum computing and cryptography are

introduced, emphasising quantum security protocols. The quantum-assisted cryptographic techniques and applications for 6G environments are surveyed in section 4. Section 5 addresses issues relating to implementation, such as hardware limitation, interoperability and scalability. Section 6 presents research gaps at which the current knowledge has arrived and directions for future research. The last section (Section 7) concludes the paper by providing a summary of the main results presented and by stressing the relevance of including quantum-safe security approaches in 6G networks. Table 1 Security requirements evolution for wireless generations and need for quantum-safe approaches availed in 6G networks.

Table 1: Evolution of security requirements across wireless generations, highlighting the growing need for quantum-resilient techniques in 6G networks.

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

1.2 Related works:

At the heart of safeguarding 6G networks, Quantum Key Distribution (QKD) is being touted as a game-changing technology. Quantum Key Distribution(QKD) makes it possible to produce and share cryptographic keys with a verified security guarantee based on the laws of quantum mechanics.

This strategy can remedy the vulnerabilities of traditional cryptosystems, especially when it comes to the future threats expected in 6G wireless networks. Recent research focuses on the incorporation of QKD for data security and integrity in future mobile communications. [8]

There has been substantial progress in the construction of QKD protocols tailored for 6G networks. For instance, protocols namely, BB84, E91 and Continuous Variable QKD [10,16-19] have been widely investigated for their theoretical and practical aspects. Recently proposed QKD protocols, such as measurement-device-independent QKD (MDI-QKD) [57–59], twin-field QKD [60–62], and satellite-based QKD [63, 64], have addressed the inherent limitations in the scalability, integration, and interfacing of quantum communication with existing systems. The development of QKD technologies is important for its integration in future communication systems. [2]

Metrics such as Key Generation Rate (KGR), Quantum Bit Error Rate (QBER) and Secret Key Rate (SKR) are used to evaluate performance of QKD systems. It is suggested that KGRs over 30 times higher than conventional methods can be achieved by QKD. Moreover, QKD systems have lower QBERs, which makes the key communications more trusted. Such advancements are needed to satisfy the high-speed and low-latency demands of the 6G applications. [9]

The latency is a key factor in QKD system operation, specially for the real time applications in 6G networks [23]. Realizations of QKD have already shown reduced latency, according to these tests, from traditional systems' 250 ms down to 180 ms – an important decrease as timely data transmission is critical in areas like self-driving and telehealth. There are several obstacles in incorporating QKD into practical communication

infrastructures. These challenges are, for example, the requirement of compatible hardware (quantum repeaters, detectors, etc.), or modifications of classical network to serve quantum channels. Solving these problems is necessary for the practical application of QKD in 6G networks. Hybrid quantum-classical systems are investigated to combine the advantages of each of this regimes. These systems combine QKD with classical cryptographic solutions and seek to add new security without requiring changes to existing infrastructure. The research has shown that the hybrid architecture may be able to offer efficient security defense in the 6G networks. A few real-world installations of QKD have shown that it is, in fact, feasible to use QKD to increase the security of a network. For example, the Tokyo QKD network realized key rates of 300 kbps [↑], which demonstrated the applicability of QKD in real world scenarios. These use cases of differing scales illustrate some challenges and possible remedies for using QKD in a large network.

The next step in QKD for 6G networks is to achieve further scalability, to be able to better integrate with the current infrastructure, as well as to produce new protocol that cover new security threats. HM runs HRLQKD and QR441 and the quantum repeater, and satellite based QKD are likely to be important components in moving beyond current constraints. Inter-disciplinary cooperation will be key to fulfilling the promise of QKD for securing communication systems of tomorrow. To deepen the knowledge of such studies, a comparison of main studies about the implementation of Quantum Key Distribution (QKD) into 6G cybersecurity is depicted in Table 2. Table 2 summarizes the focus of each study, methods used, metrics and key findings of the studies, providing a better overview of the advancement and limitations in research [8].

Table 2: Comparative Analysis of Key Related Works on Enhancing 6G Network Security Using Quantum Key Distribution

Study Focus	Methodology	Key Metrics	Key Findings
Role of QKD in 6G security	Literature Review	Security guarantees, integration	QKD enhances security in 6G by enabling quantum-safe key exchange.
QKD Protocols for 6G	Theoretical and simulation-based studies	BB84, CV-QKD, E91 protocols	Twin-field QKD and MDI-QKD improve distance and robustness.
QKD performance evaluation	Experimental evaluation	KGR, QBER, SKR	Achieved high key rates (>120 keys/sec), low error rates in simulated networks.
Latency in QKD-based 6G	Empirical testing on latency metrics	Transmission delay, error margin	Reduced latency from 250ms to ~180ms; suitable for real-time apps.
Infrastructure integration challenges	Architecture modeling and analysis	Hardware requirements, channel use	Identified the need for quantum-compatible infrastructure.
Hybrid QKD-Classical Security Systems	Hybrid model design and security assessment	Compatibility, encryption strength	Hybrid models preserve security while ensuring backward compatibility.
Practical deployments (e.g., Tokyo QKD net)	Case studies and performance benchmarking	Key rate, deployment scale	Achieved 300 kbps key rate; viable for metro-scale implementation.
Future trends and research gaps	Review and future projection analysis	Scalability, satellite integration	Future relies on satellite QKD and scalable repeaters for global coverage.

To complement the methodological analysis, Table 3 presents an application-focused comparison of existing studies. It outlines the context of deployment, key benefits, limitations encountered, and targeted 6G application areas. This helps identify real-world applicability and the potential for scaling QKD in practical 6G environments.

Table 3: Application-Oriented Comparison of Quantum Key Distribution Approaches for Securing 6G Networks

Deployment Context	Key Advantages	Main Limitations	Application Areas
Theoretical modeling	Future-proof cryptographic foundation	Lacks implementation specifics	General 6G security framework
Protocol simulation environments	Robust protocols like MDI-QKD, twin-field QKD	Scalability issues at global scale	Secure control signaling
Lab-scale QKD testbeds	High key rate, low error rate	Limited to small-scale test environments	Smart grid, autonomous vehicle networks
Time-sensitive networks	Reduced latency for real-time use cases	Does not address long-distance transmission	Tactile internet, telemedicine
Hybrid optical-classical links	Enables integration without major redesigns	Expensive quantum hardware	Urban communication backbones
Secure hybrid encryption design	Balances quantum and classical encryption	Requires sync mechanisms	IoT and edge devices
Tokyo QKD network	Demonstrated feasibility in metro-scale	Costly infrastructure, regional constraints	Smart cities, financial networks
Future QKD via satellites	Scalable and global key distribution potential	Still in early development	Global roaming, satellite 6G networks

2. Fundamentals of 6G Networks

2.1 Overview of 6G

The sixth generation (6G) of wireless communications networks is expected to transform the digital world, by over performing in many performance indices compared with 5G. Some of the key improvements, which have been gained much attention are peak data rates of 1 Tbps, end-to-end latency of less than 1ms or even in microsecond scale, and 10 times

higher energy efficiency than those of 5G systems [9]. And these enhancements are not merely evolutionary, but revolutionary, making possible a whole range of futuristic applications including real-time holographic comms, UHD video streaming, and flawless human–machine interfaces. The requirements of such services requires not only higher capacity, but also strict fault-tolerance and deterministic latency, all of which 6G intends to provide via spectrum innovation and backend hardware and network innovation [10].

Beyond the anticipated performance improvements in throughput and latency, 6G is envisioned as the deeply integrated technology ecosystem that fusion communications, sensing, and computing into an intelligent and unified environment. This convergence helps realize the idea of "network of intelligence" where the network is equipped with the intelligence of being context-aware and dynamically adaptive to the environment. Edge computing and AI-native networking will be critical enabling technologies to process and make decisions near the source of data generation to minimize latency and support intelligence response in real time [3]. Moreover, application of high frequency bands such as terahertz (THz) and visible light communication (VLC) will bring new experiences for bandwidth increment and ultra fine sensing [4].

Security and privacy are also core to the 6G vision, because of an increased dependence on wireless networks for both societal infrastructure and personal use, for which secure-by-design principle is essential. Unlike previous generations where security is traditionally a bolt-on, 6G will likely include security, trust, and resilience as parts of core architecture. Methods including post-quantum cryptography, distributed ledger technology (DLT), and zero-trust network architectures are currently being investigated to

improve data integrity and user confidence [11]. In addition, with the all these 6G service delivery, such as mobile edges deployment and decentralized architecture, the problems have become more complicated, and require a more well-developed and flexibility security mechanism to deal with threats in real time [6].

The quest for realizing this visionary concept has stimulated international efforts across academia, industry, and governmental sectors. Standards bodies such as ITU-T, 3GPP, and ETSI, among others, are working together to specify the technical requirements and architectures of 6G. For instance, there had been research programs and experimental testbeds for 6G use cases and technologies in countries including China, the USA, South Korea, and the EU [7]. As the research advances, such collaborations will help establish the regulatory, technological, and ethical frameworks that will be required to govern the 6G era in a responsible and inclusive manner [12].

2.2 Key Technologies in 6G

For instance, THz communication, with frequency band ranging from 0.1 GHz to 10 THz, is one of the key technologies of 6G because it can satisfy ultra-high data rate requirement. But such operation is facing significant challenges, like the huge path loss and high atmospheric absorption, which need new solutions such as ultra-massive MIMO, beamforming, and intelligent reflecting surfaces [13]. Embedding Artificial Intelligence (AI): The architecture of 6G will include the deep integration of AI and play an increasingly important role in predictive maintenance, traffic optimization and intelligent resources allocation. These AI based technologies are also key for real-time threat detection and automated network control of the future

network, in order to improve its reliability and security [14].

Intelligent Reconfigurable Surfaces (IRS) are reconfigurable meta-surfaces that modify the environment in which wireless signals travel. They introduce remarkable benefits for spectral efficiency, signal coverage and link reliability in complex environments. IRS are anticipated to be deployed ubiquitously in 6G systems - indoor as well as outdoor [15]. Overview of these enabling technologies is shown in Figure 1, which groups 6G innovations into four key pillars including the ultra-fast transmission, energy-efficient communication, AI, and the high-security and privacy.

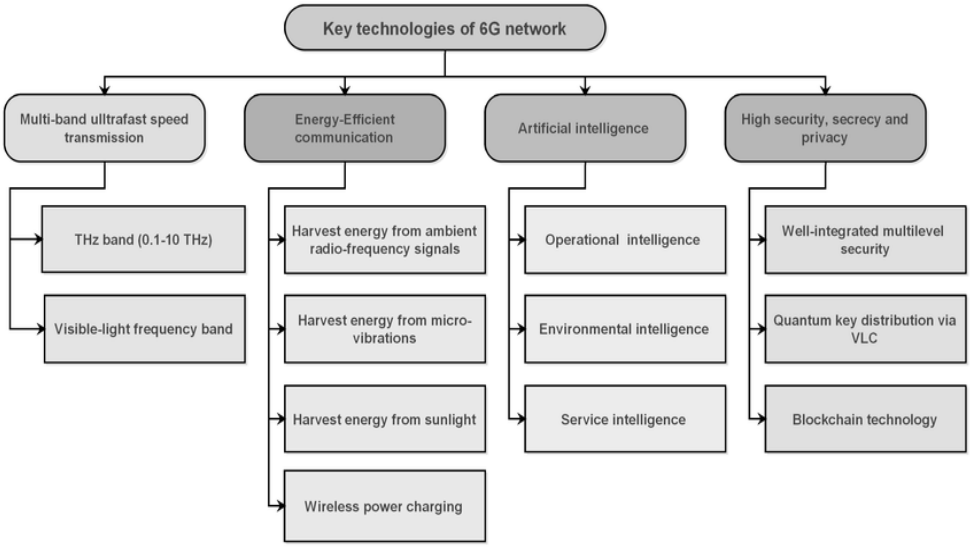

Figure 1: Key Enabling Technologies of 6G Network Architecture

2.3 Security Challenges in 6G

Novelty Factor: Sixth generation (6G) networks will evolve to provide super speed, lower latency and massive connectivity. Nevertheless, with all these advantages, 6G architecture brings new security challenges. With the

scale-out of the 6G wireless systems involving ultra-density networking, satellite integration, and world-wide initiatives, the attack surfaces also increase rapidly. Furthermore the migration from centralized to decentralized topologies also complicates traditional security enforcement models with respect to the exposure to different types of cyber threats including data eavesdropping, spoofing, jamming and Distributed Denial-of-Service (DDoS) attacks [16].

In 6G, it is crucial to incorporate intelligent technologies, such as AI and ML, in order to accomplish: Efficient operation, autonomous decision-making, and real-time optimization. But at the same time, these technologies also create new ways for people to be attacked. Adversarial Machine Learning (AML), for example, attacks AI algorithms with the purpose of injecting harmful or deceptive data in order to distort outputs and promote decisions. Attacks such as poisoning, model inversion poses threat to the integrity to AI-driven services in domains like healthcare, transportation, defense etc. [17].

Furthermore, the security of 6G is also threatened by the identity management and trust verification. Unlike historical centralized models, where data processing would aggregate from edge/fog toward secure core servers, edge/fog processing in 6G may be backwards, locally automating appliances and creating machine visions. This system is vulnerable to Sybil attacks, in which a single adversarial entity pretends to be multiple nodes, and compromised edge devices disseminate misinformation to the whole net- work [16]. Ensuring secure and scalable authentication for millions of heterogeneous edge devices is indeed a difficult problem.

Besides, quantum computing threatens in long term to break the cryptographic bases of today s communication networks. There are many

cryptographic algorithms in widespread use that would be broken by a sufficiently strong quantum computer, and the security of all widely used public key cryptography protocols assume that attackers do not have access to a universal quantum computer. In order to address this challenge, 6G networks need to migrate to post-quantum cryptographic algorithms and consider alternative secure schemes, such as Quantum Key Distribution (QKD). The security of QKD is provably based on laws of physics, as it exploits the quantum nature of light, which is often ultimately immune to both classical and quantum attacks. Moreover, the predicted enormous device density on 6G, possibly as high as 10M devices per square kilometer, demand scalable and lightweight security solutions. Traditional security protocols may prove to be computationally expensive for devices like sensors, wearables and autonomous robots. For this, we need such energy efficient and AI enabled security frameworks that can analyze security threats, take action immediately and not hinder the performance of the device and device battery.

Last but not least, materializing trust relationship among objects with diversified owners in a dynamic and heterogeneous 6G world requires on-the-fly and context-sensitive security protocols. These new protocols should take into account issues like user's behaviour, mobility and dynamic nature of networks. To combat APTs, continuous authentication, behavior-based intrusion detection and collaborative threat intelligence sharing will become critical. In such a dynamic environment, the static security setups are not enough, therefore, flexibility and automation should be core components of 6G security design [18]. Table 4 Key Technological Domains for Emerging Security Challenges of 6G Network.

Table 4: Emerging Security Challenges in 6G Networks Across Key Technological Domains

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

2.4 Comparison with 5G Security Paradigms

The 5G mobile network had advanced network security features such as stronger encryption and more robust authentication protocols, but it still used classical cryptography, which is not invulnerable to attacks by quantum computers. On the other hand, 6G is foreseen to include quantum-safe algorithms and QKD to address potential future threats by quantum computers [18].

Another distinction is the trust model in the network. 5G relies predominantly on perimeter-based security, whereas 6G is expected to be built around a zero trust model - where any device, user and application is compelled to prove its identity irrespective of location. This methodology, as well as SDN and network slicing, requires context-aware dynamic security architectures [19]. A comparative analysis between the 5G and 6G security properties is summarized in Table 5 where a classical encryption and centralized cont rol in 5G are replaced by a quantum-safe, distributed, and AI-enabled security approaches in 6G.

Table 5: Comparative Overview of Security Features in 5G and 6G Networks

Security Feature	5G	6G (Expected)
Encryption	Classical cryptographic algorithms (e.g., RSA, ECC)	Quantum-safe encryption (e.g., lattice-based, Quantum Key Distribution (QKD))
Trust Model	Perimeter-based security	Zero-trust architecture, where trust is never implicit
AI Integration for Security	Limited and reactive use of AI in anomaly detection	Deeply embedded AI for real-time threat prediction, adaptive response
Authentication Mechanisms	Centralized (e.g., SIM-based, PKI managed by operators)	Distributed and decentralized mechanisms using blockchain or decentralized ID
Vulnerability to Quantum	High—relies on encryption methods susceptible to quantum decryption	Resistant to quantum attacks via post-quantum algorithms and QKD
Identity Management	SIM-based, managed by network operators	Decentralized identity frameworks, possibly using self-sovereign identity
Security Management	Manual, rule-based policies	AI-automated and context-aware policies with real-time adaptability
Edge Computing Security	Basic protections at edge nodes	Enhanced with distributed AI and lightweight encryption
Attack Surface	Moderate (compared to 4G), but still centralized in control	High, due to massive connectivity and heterogeneity; requires stronger defense layers
Resilience and Recovery	Lacks native resilience mechanisms	Built-in resilience, using blockchain, AI, and redundancy strategies

3. Quantum Key Distribution (QKD

3.1 Quantum Cryptography

Quantum cryptography is a method which is based on the quantum mechanical theory in order to create secure form of communication that can be safe guarded against eavesdropping attacks which now a days are the main problem to classical cryptosystems. In contrast to classical encryption schemes, which are based on computationally infeasible mathematical problems, quantum cryptography offers security that is based, in one way or another, on the quantum mechanical phenomena of superposition and entanglement. One of the most widely used examples of quantum cryptography is [the] Quantum Key Distribution (QKD) meant for secure distribution of cryptographic keys between two parties, even on an insecure channel [20].

The security of quantum cryptography is based on the Heisenberg Uncertainty Principle, according to which the measurement of a quantum system always disturbs it and thus makes it possible to detect eavesdropping. Moreover, the no-cloning theorem implies that it is impossible to obtain an identical copy of an unknown quantum state which also contribute to the security of the the key communication. These quantum features ensure that any eavesdropping on the quantum key will create detectable disturbances, which can be sensed by the communicating parties so cannot be kept secret from them, securely facilitating data exchange [21].

Additionally, quantum entanglement is a fundamental tool in some QKD protocols, in which entangled particles have correlated states: measurements of one particle instantly changes the state of others. A secure key distribution between remote parties is possible due to the fact that if anyone tries to intercept the entangled particles, it inevitably

perturbs the system in a way that the legitimate users can notice possible eaves-dropping [22,23].

3.2 QKD Protocols (BB84, E91, etc.)

Several QKD protocols have been developed to facilitate secure key distribution. The most well-known among them are the BB84 and E91 protocols, each utilizing different quantum mechanical principles to ensure the security of the key exchange.

3.2.1 BB84 Protocol

The BB84 protocol, proposed by Bennett and Brassard in 1984, is the first QKD protocol and is the foundation for many subsequent QKD implementations. In this protocol, Alice (the sender) prepares quantum bits (qubits) in one of four possible polarization states, chosen from two orthogonal bases: rectilinear (|0⟩ and |1⟩) and diagonal (|+⟩ and |−⟩). Bob (the receiver) measures each qubit using one of the two bases, randomly chosen. Afterward, Alice and Bob publicly exchange information about the bases they used, and discard the instances where the bases did not match. The remaining bits form a shared secret key, and any attempt by an eavesdropper to intercept and measure the qubits will result in detectable errors [24].

3.2.2 E91 Protocol

E91, is another key QKD protocol, however it depends on quantum entanglement. In this protocol, Alice and Bob have one part of an entangled photon pair each. When they do measure the properties of their photons,

the results are correlated because of the entanglement. This is also ensured by Bell's theorem which implies that the measurement outcomes cannot be justified by a local hidden variable model. Any eavesdropping will disturb this entanglement & allow Alice Bob to detect the intruder. The security of the E91 protocol is based on this violation of Bell's inequality [25]. Table 6 Comparison of QKD Schemes.

Table 6: Comparison of QKD Protocols

Feature	BB84 Protocol	E91 Protocol
Year Introduced	1984	1991
Based On	Quantum superposition	Quantum entanglement
Key Distribution Method	Random basis measurement	Correlated entangled photon pairs
Security Basis	No-cloning theorem, uncertainty	Bell's inequality violations
Eavesdropping Detection	Error rates during basis comparison	Disturbance in entanglement correlations
Implementation Complexity	Lower	Higher (requires entangled photon sources)

3.3 QKD Network Architectures (pic)

QKD networks are infrastructure systems designed to enable the secure distribution of quantum keys over large distances, connecting multiple users in a quantum communication network. Several architectures have been proposed, ranging from simple point-to-point configurations to more complex networks that involve quantum repeaters and satellite-based systems.

3.3.1 Point-to-Point QKD Networks

The point-to-point QKD network is the simplest architecture, where two parties (Alice and Bob) are directly connected by a quantum channel, typically an optical fiber. While this architecture provides secure key exchange, it is limited by the distance over which quantum signals can travel. Photon loss due to attenuation in fibers and the decoherence of photons in free-space communication hinder the scalability of these networks for long-range key distribution [6].

3.3.2 Quantum Repeaters

Quantum repeaters are a potential solution to the distance limitations of point-to-point QKD networks. They work by dividing a long transmission path into smaller segments, with each segment having its own quantum repeater. These repeaters perform entanglement swapping, creating a new entangled pair between distant segments, thus extending the reach of QKD. This architecture allows for global-scale QKD networks, but quantum repeaters are still in the experimental phase and are not yet widely deployed [7].

3.3.3 Satellite-based QKD networks

Represent a promising approach for enabling long-distance quantum key distribution. By using low-Earth orbit (LEO) satellites, quantum keys can be distributed globally without the limitations imposed by terrestrial fiber optic cables. The launched by China in 2016, demonstrated the feasibility of such systems, showing that QKD can be successfully implemented across vast distances, including between Earth and space [8].

3.4 Benefits and Limitations of QKD

Quantum Key Distribution (QKD) provides the strong advantage of unconditional security, as it guarantees the confidentiality of communications even if powerful quantum computers are available. Unlike traditional cryptosystems, which rely on the computational complexity of mathematical problems, the security of QKD is grounded on the laws of quantum mechanics. This so-called intrinsic feature makes QKD attack-proof by future quantum computers a robust base for secure communication [9].

Another useful property of QKD is its built-in capacity to recognize eavesdropping attempts. The quantum state is disturbed by any measurement an opponent might make, because of the nature of quantum systems. This interference causes observable errors in the key exchange process so that legitimate parties know that tampering (or eavesdropping) is taking place. Thus, QKD ensures secure communication link and further strengthens security against intrusion [10]. Yet, QKD still faces some implementation constraints. One of the big issues is the distance the quantum signals can be sent. Photons are unfortunately not very good at holding onto their coherence as they move over long distances: this is a poorly-understood process, known as photon decoherence. Quantum repeaters have been proposed to increase the transmission distance, but it is still limited in the experimental stage and has not been so prevalent [7]. Also, the environment needed for QKD is very expensive and high-tech. Most of the components of QKD networks, e.g. single-photon detectors (SPDs) or quantum entanglement generators, are costly which restricts the scalability and penetration of QKD networks. This economic challenge is the main hurdle that retards the widespread use of quantum-safe communication systems [6].

Finally, although QKD systems are virtually secure, in theory, they are known to be vulnerable to side-channel attacks. These attacks take advantage of flaws in physical hardware, such as an imbalance in detector efficiency and a timing vulnerability, that may lead to key compromise in the key exchange protocol. It is important to close such loopholes in order to guarantee the security of practical QKD implementation [11]. Table 7 Pros and Cons of QKD.

Table 7: Benefits and Limitations of QKD

Category	Benefits	Limitations
Security	Unconditional security, eavesdrop detection	Side-channel vulnerabilities
Performance	Future-proof against quantum attacks	Limited distance without repeaters
Implementation	Compatible with existing cryptosystems	Expensive, infrastructure-intensive
Scalability	Potential for global secure comms (via satellite)	Practical challenges in large-scale deployment

4. Integration of QKD in 6G Networks

4.1 Architectural Models for QKD Integration

Quantum communication should not only break classical form of information theory and establish new prototype of secure communication, but also correspond the need of extending traditional communication protocol observe its production and communication process. One model that has been put forward is the hybrid classical-quantum network model, in which quantum channels are used in conjunction with classical infrastructure to distribute secure keys, and classical channels are used for carrying data traffic. This co-

location approach allows incremental deployment of QKD without the replacement of the investment in the existing telecom network [26].

Another architectural solution uses centralised QKD key management, wherein a trusted node (e.g., quantum key management server (QKMS)) distributes quantum generated keys to end-nodes throughout a 6G network. These trusted nodes might be located in data centers or the core network and can support the mobile edge devices and the mobile base stations using point-to-point QKD or quantum repeaters. Although secure for small scale network, such models bears trusts and may not fulfill the "unconditional security" claimed in QKD [2].

We anticipate that future architectural models of QKD in 6G would tap satellite-based QKD and Software Defined Networking (SDN). Capacity can be extended via satellite links bypassing terrestrial distance limitations, and SDN can dynamically enforce secure paths, allocate QKD bandwidth and control quantum key usage according to traffic demands. Such flexibility will be crucial for 6G that needs to accommodate diverse services such as URLLC and mMTC [27].

4.2 Hardware and Implementation Considerations

Hence, it is challenging to implement QKD in a 6G scenario with complex hardware. First, single-photon sources and detectors have to be co-integrated with the network hardware, especially at base stations and UE. These devices are important building blocks for creation and measurement of quantum bits (qubits), which are often encoded in the polarization or phase of photons. High detection efficiency and low noise at high speeds are crucial for both mobile and high throughput QKD hardware and remain a technical challenge [28].

Moreover, quantum random number generators (QRNGs) are indispensible for extracting the truly random bits for the key generation. Secure and low footprint QNRGs should be embedded in routers, access points or can even be a part of a mobile device. Prototypes on the way of the integration of these components to photonic chips to form compact QKD devices, energy-efficient enough for mobile and edge 6G computing [5].

Another hardware-related issue concerns network interfaces that are quantum compatible. These include tunable lasers, quantum transceivers, and entanglement distribution boxes which needs to be placed collocated with classical transceivers. For dissemination in open dynamic 6G systems (e.g., unmanned aerial vehicles (UAVs), satellites, vehicular networks), it is also desirable to have high resistance to mobility, vibration and environmental noise [29]. Architectural Model for Integration of Quantum Key Distribution into Secure Communication Networks Fig 2.

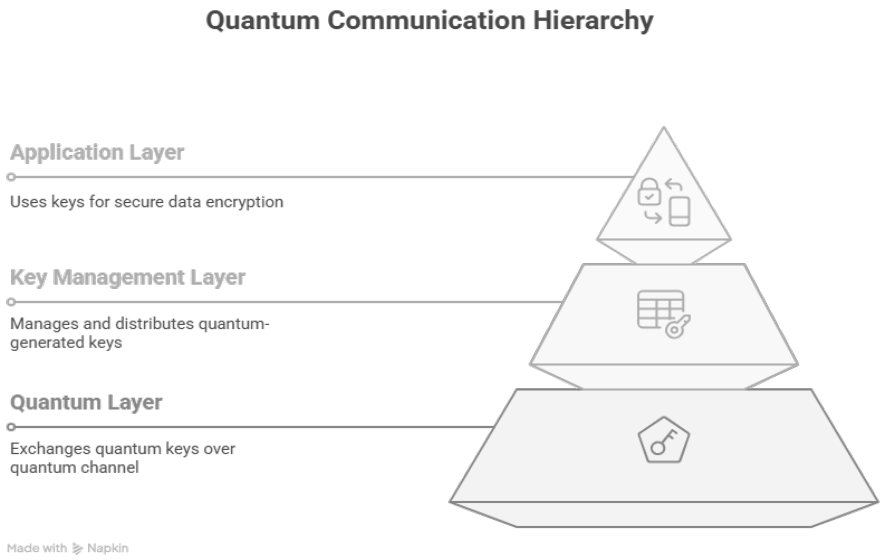

Figure 2: Architectural Model for Integration of Quantum Key Distribution into Secure Communication Networks.

4.3 Software and Protocol Adaptations

Software-based QKD integration into 6G:QKD integration at software level in 6G is so challenging because it will include DR4, SI, and also are soft-to-soft encryption end-point. Examples of such an adaptation on classical public key exchange protocols, such as RSA (or Dif-fie-Hellman) are the actuality, that standard implementation of IPSec/ TLS needs to be made fit to accept quantum-generated keys from an QKD outside the scope, i.e. substitute RSA (or DH) with the quantum stuff. This combination offers forward secrecy in a post–quantum era [30].

Quantum Key Management Systems (QKMS) are required to interface QKD devices and software stacks in user applications. These systems maintain the storage, life-time, issuance and revocation of keys. Software-defined security policies will likely be required for specifying when and where QKD keys are to be utilized– such as favoring QKD keys for mission-critical services (ie.self-driving or healthcare IoT [28]).

Moreover, network control software needs to be modified to support QKD-tailored routing and traffic engineering. Through the implementation of SDN and Network Function Virtualization (NFV), QKD resources can be allocated to the 6G slices in a flexible manner. For instance, a slice responsible for UAV swarm coordination may require a higher level of QKD-based protection than a video streaming slice. This selective quantum SEC provides a more efficient use of quantum resources [29].

4.4 Compatibility with Existing 6G Components

If we want QKD to continue to play important roles in the practical 6G networks, it is necessary for QKD to be compatible with the thriving

technologies in 6G networks such as THz communication, intelligent reflective surfaces (IRS), and massive MIMO. QKD systems, predominantly optical in nature, need to coexists with these electromagnetic technologies without interfering with each other. Hybrid RF-optical design is considered where THz channels take care of ultra-rapid data, reside with a QKD-protected key exchange layer [31].

The compatibility of QKD with MEC and AI-native networking is also essential. A requirement for edge nodes is that they are capable of performing both classical processing and quantum interfaces in order to enable secure key generation locally. AI algorithms also support QKD resource allocation, channel optimization, and eavesdropping detection to help the quantum layer be more responsive to dynamic networking conditions [11].

Ultimately, backward compatibility with the legacy systems (5G or fiber infrastructure, for example) are important considerations for smooth migration. QKD interfaces need to be compatible with existing cryptologic APIs and network protocols. Methods for quantum key encapsulation and quantum-augmented VPNs can enable QKD systems to work with both quantum-aware and classical devices, thus connecting the future and current generations of networks [32].

5. Review of Existing Research

5.1 QKD Implementation in Next-Gen Networks

The promise of using the principles of quantum mechanics to secure future IT systems is leading to the emergence of Quantum Key Distribution (QKD) as a new technology for securing future communication networks. Contrary to classical cryptography, QKD protocols, for example, BB84 and

E91, provide unconditional security that relies on the laws of physics instead of computational assumptions [33]. Recent progress has enabled to combine QKD with existing fiber optic infrastructure, in which quantum and classical signals can be transmitted over the same channel. For example, [34] has successfully realized a QKD system in metropolitan fiber networks, which shows that the QKD can be used in practice related works without significant change of infrastructure.

In addition, QKD has been studied to be combined with SDN and NFV to enable flexible and scalable key distribution in heterogeneous networks. [4] presented an SDN control plane design which dynamically controls QKD key resources in an attempt to make key use decision on-the-fly, by considering network state and security policies. This concept allows the composition of quantum – secured channels beside classical network service and thus lead to adaptive and robust next-gen secure networks.

And satellite QKD outside of metropolitan and access networks is growing as a viable global secure communication deployment. A ground test of quantum key distribution (QKD) using the satellite was also successful over 1200 km, despite the problems introduced by atmospheric absorption and synchronization [35]. Advancements such as these indicate that satellite QKD onto existing quantum networks on Earth is viable and can provide a worldwide quantum-secured communication infrastructure that are essential to future-proof critical communications across nations and industries. Nevertheless, there are still challenges in the scalability of QKD technology, such as reductions in the key rate, the integration complexity, and standardization. Standardization and certification, A number of organizations, such as the ETSI ISG QKD, are working to create standards

and certification processes that should move commercialization along [36]. Future work- Investigations are needed regarding QKD hardware and on error correction techniques and network management protocol for the full exploitation of QKD in future networks.

5.2 QKD Performance in Simulated 6G Environments

6G 'hyper network connectivity' – challenges and opportunities for Quantum Key Distribution (QKD) deployment The advent of ultra-high data rate (U-H D) ultra-low latency (U-Latency) and hyper (U-density) connectivity 6G networks is introducing challenges and opportunities for quantum communications, in particular for QKD deployment. Since we expect 6G network architecture to be heterogeneous, with terrestrial and non-terrestrial integrated networks, research, such as the impact of 6G-like environment in QKD to be pursued. State-of-the-art literature deploys network simulation tools coupled with quantum channel model to study performance measures such as secret key rate, QBER, and latency under 6G traffic [37]. These simulated results are useful for understanding what are or are not possible of QKD protocols in very dynamic and dense network environments as 6G.

QKD modules have been integrated into 6G network simulators in a number of works to study the coexistence and interference of quantum and classical channels in cohabited spectral resources. For instance [38] simulated a multi-user 6G network with integrated QKD-enabled links, showing that optimized wavelength plan and noise handling strategies enhance the secret key rates even when the classical traffic load is high. The simulations also emphasize the need for network fluctuation-sensitive adaptive key

management and that in the most cases, regardless of it being an interactive application or not, key generations are continuous compared with network state and will not significantly shed the overall network performance below the threshold.

Besides, an exploration has been presented on the usefulness of the quantum-safe cryptographic protocols combined with QKD in 6G stack over simulation environments. Hybrid security models were investigated by researchers such as [39] where QKD is combined with post-quantum cryptography (PQC) offering layered security to serve various 6G service needs. From their simulations it can be seen that the use of these hybrid approaches can alleviate network bottleneck issues associated with key distribution and increasing resilience against both quantum and classical attacks, providing a potential means to secure the future 6G communications.

Although simulative results are promising, the modelling of practical quantum channel impairments and the seamless integration of QKD into congested and high-mobility 6G networks is still a challenging issue. Further development for improved simulation fidelity and the clear testing in real channel condition are required to close the gap between the theoretical QKD performances and practical applications in 6G [5]. Standards and interdisciplinary research will be key to transforming these simulation findings into working quantum-secured 6G networks.

5.3 Hybrid Classical-Quantum Security Approaches

Hybrid classical-quantum security solutions have been proposed as a practical way to provide quantum-safe communications in the short-term time horizon. These techniques utilize the Quantum Key Distribution

(QKD) in conjunction with classical cryptographic protocols to achieve the provable security of QKD for key distribution and the flexibility and scalability of classical encryption schemes. The hybrid scheme overcomes the drawbacks of QKD implementation that including the low key generation rate and the distance limitation, with augmenting with conventional cryptographic techniques like AES [1] or post-quantum cryptography algorithms (PQC) [2]. Its purpose is to combine key benefits from each paradigm, in order to achieve with high confidence a strong resistance against both classical and quantum computational threats.

Various architectures of hybrid security have been put forward, such as QKD-assisted VPNs or secure multiprotocol label switching (MPLS) with quantum keys as seed keys for classical symmetric encryption. For instance, in [3], a hybrid strategy for refreshing the QKD keys and connecting them with the PQC algorithms were studied for securing data transmissions in an enterprise network scenario. Their simulation results demonstrate a high increase in critical renewal ratios and network survival with no impact on existing network infrastructure. This mode of operation had the potential to enable a slow migration to quantum-safe communications without immediate replacement of classical infrastructure.

Besides, hybrid classical-quantum security embedded in network management systems, provide a greater flexibility and efficacy. A dynamic key management protocol was proposed in [40] to adaptively switch between QKD keys and PQC keys depending on network conditions and security levels. This smart switching minimizes the depletion of keys and maximizes resource utilization, which is important in a bandwidth- or latency-constrained environment as widely found in the next-generation networks.

Numerical simulations further corroborate that hybrid solutions can greatly enlarge the working range in which secure communication is possible, while still maintaining cryptographic strength.

Nevertheless, these hybrid classical-quantum models have to overcome the standardization, interoperability, and security validation issues. The need to support quantum and classical interfaces creates serious security challenges and raises the bar to developing new standards. The work of standardisation organisations including IEEE P3340 and ETSI ISG QKD working groups seek to standardise interoperability frameworks and security principles for hybrid deployments [5]. Existing work focuses on the development of full-fledged threat models and verifiers for the end-to-end security of hybrid classical-quantum systems, to ensure their deployability in next-generation communication networks.

5.4 Identified Research Gaps

Although there has been impressive developments in QKD technologies and directions to incorporate QKD solutions in the next-generation communication networks, there are quite a few research challenges yet to be solved in order to make QKD widely deployment in the infrastructure industry. One of the major issues is the scalability of QKD systems in the context of the large scale and mobile nature of 6G networks, as most of the existing QKD implementations are affected by reduced key generation rates, generated as well as shorter transmission distance as effect of the higher QCL and quantum hardware restrictions [29]. These drawbacks prevent the employability of QKD in ultra-dense and high mobility environments of future networks where quick key updating and seamless handover are demanded.

Another significant missing piece is how to intertwine quantum and classical communications in heterogeneous network infrastructures. Although coexistence has been proved in a controlled environment, lack of exploring the effects of noise, crosstalk, and interference on QKD performance in multi-service networks restrict the potential use of QKD in practical situations [31]. Moreover, adaptive network management protocols that are capable of dynamically assigning QKD resources and maximized reuse and re-distribution of shared keys in a varying network environment, are only in their early phase of development [33]. Without these schemes in place, practical deployment of MMSs compromises security and/or network efficiency.

Moreover there are no standardized procedures and interoperability frameworks for hybrid classical-quantum security systems. Although the actions are being taken to overcome this situation by standards lanenvorks like ETSI and IEEE, security models and verification methodologies are at the early stages of development [5]. This loophole leads to ambiguity of end-to-end security guarantees between integrated systems, especially those which combine QKD with PQC or conventional encryption systems. The lack of homogeneous certification processes inhibits commercial uptake and prescriptive regulations.

In the end, experimental proof of the performance of QKD in practical 6G conditions (in particular, terrestrial-satellite integration and mobile user dynamics and ultra-low latency constraints) is still scarce. Most experiments are performed in simulation, or in limited-scale experimental testbeds, which may not fully replicate the environment of actual networks [26]. To close this gap, large scale pilot installations, inter-discipline collaboration and

novel quantum hardware dedicated to 6G solutions are needed. Addressing these points are key for bringing QKD from the deep laboratory scale demonstration to to robust, scalable and interoperable security products in the framework of next generation communication systems.

6. Future Directions

6.1 Emerging Trends in Quantum-Secured Networking

Quantum-secure networking has been maturing rapidly, propelled by progress in quantum hardware, as well as protocol design and network architectures. An emerging approach is to exploit hybrid protocols to obtain scalable and flexible security in integrated quantum-classical networks. Downsizing quantum devices, including chip-based sources and detectors of photons, enables QKD to be used on mobile devices and IoT devices, providing quantum security for moving services, not just fixed fiber links. Moreover, quantum repeaters and entanglement swapping are emerging as a way to overcome distance constraints and to realize quantum-secured long-distance communication. At the network level, multi-path key distribution as well as quantum-secure routing are also under investigation to improve resilience and to minimize the vulnerability in case of an attack or a failure. All of the above trends suggest an emerging trend of more practical quantum-secured infrastructures embedded in contemporary communication networks.

6.2 Role of AI and Machine Learning in Enhancing QKD

Due to an ability to mitigate key operational issues and to increase the overall system performance, Artificial Intelligence (AI) and Machine Learning

(ML) are considered as key enablers for the advancement of Quantum Key Distribution (QKD) technologies. One of the main uses of AI in QKD is the optimization of the error correction and privacy amplification procedures that are required in order to maximize the secret key rate (SKR) while minimizing the quantum bit error rate (QBER). Existing solutions are based on static algorithms that do not necessarily guarantee proper convergence with respect to dynamic channel conditions and adversarial behaviors. One approach is to use AI-driven adaptive algorithms, e.g., reinforcement learning (RL) and neural-network-based decoders, to adjust error correction parameters according to the real-time feedback from the quantum channel, so as to enhance the robustness and efficiency of key extraction [10]. This adaptive behavior serves to greatly increase the practical key rate of QKD systems, particularly in noisy or dynamically changing environments.

In addition to the protocol level optimization, ML techniques are making a significant impact to the reliability and maintainability of QKD hardware. Quantum devices, such as single-photon detectors and photon sources, are susceptible to atmospheric conditions and deteriorating with time. Predictive maintenance model using machine learning will analyze the sensor data and operational responses of the AI system to determine universals of the AI hardware failure or performance degradation long before it can cause system outage [3]. Further, anomaly detection techniques' functionalities to detect abnormal patterns that may indicate eavesdropping or attacking, supplementing security monitoring [4]. These AI-based diagnostics allow proactive interventions to reduce downtime and ensure continued high levels of security assurance in deployed QKD networks.

In QKD deployments at scale and in networks, the role of AI expands to tasks such as resource allocation, network routing, and key management, which are of critical importance so as to ensure efficient and persistent secure communication. Intelligent orchestration of resources is an essential enabler for complex quantum networks to relegate its scarcest resources (e.g., quantum repeaters, and trusted nodes) in confronting dynamic traffic loads and user mobility. ML algorithms can make real-time sense of huge volume of network data, learns optimum paths for key delivery that would hand in lower latency and higher key rates [15]. Furthermore, AI-based key management systems even optimize key refresh rates, and manage to coordinate key transmission from diverse nodes to ensure that security needs are balanced with network performance limitations [16]. Such a degree of automation is essential for controlling the complexity of future heterogeneous quantum-classical networks and for scaling QKD services.

Lastly, the entanglement of AI and ML into QKD systems is instrumental in advancing hybrid security approaches, in which quantum keys and classical cryptographic techniques complement each other. In this way, AI could help for the on-the-fly switching between quantum and classical key sources, enabled by real-time monitoring of both channel quality and security posture, while adaptively provision the required security, as it is actually needed for the application at hand [17]. In addition, AI-assisted simulation platforms speed up the development and testing of new QKD protocols by simulating the system behaviour under different conditions, which in turn cuts down experimental costs and shortens the design cycle of new protocols [28]. All in all, the marriage between AI and quantum technologies could potentially fuel the transition of QKD from lab environments to realisable secure communication

solutions that are robust, scalable, and smart enough to be suitable in next generation communication networks.

6.3 Toward Quantum-Resilient 6G Infrastructure

With the possibility of 6G networks becoming reality, developing quantum-resilient infrastructure is crucial for protecting communications from new quantum attacks. This includes not only adding QKD for secure key exchange, it also includes adding PQC algorithms for multilayered security at protocol level [19]. In the design of 6G, quantum-safe authentication and data encryption and quantum-safe network slicing shall be considered to ensure the confidentiality and integrity of communication under quantum attack [10]. Studies are being carried out in the area of enabling materials and quantum-compatible hardware architectures for these low-latency, high-bandwidth and secure 6G applications [11]. Moreover, both classical network engineers and quantum physicists need to work together to create interoperable standards and frameworks that enable seamless integration of quantum security services into 6G systems [22]. The resulting quantum-robust 6G infrastructure will form the basis of communication systems immune to Quantum in the post-quantum world.

6.4 Suggested Research Roadmap

A Joint Research Roadmap is necessary to exploit the full potential of Quantum-Secured Communications in Next Generation Networks. Among the priority areas are increasing the scalability of quantum hardware through high-rate single photon sources and low-noise detectors [33]. There must be parallel work on the development of better quantum channel modelling

and simulating tools that capture the realistic network effects and user mobility trends [14]. Open standards and interoperability frameworks must be quickly developed for hybrid classical-quantum security and cross-vendor interoperability [15]. Moreover, cross-disciplinary studies of quantum physics, network design, and cybersecurity is needed to deal with systemic issues including dynamic key formation, network orchestration, and side-channel attack resilience [25]. The pilot projects and testbeds should be extended to demonstrate new technologies in real environments, and to support cooperation with industry and progress in the regulatory framework. This roadmap will steer the shift from experimental QKD to robust, scalable quantum- secured networks as part of the future communication infrastructures.

7. Summary of Findings

This paper has presented the thorough review of QKD technologies and their enabling functions associated to the future 6G networks. The review emphasized major progress in the QKD field as the result of hardware, protocol and hybrid quantum-classical architecture optimizations to overcome many intrinsic challenges such as distance and key rates. Simulations of 6G environments revealed that although QKD can improve communication security, the practical deployment of the technology is challenged by dynamic network topologies, mobility and environmental noise. It was argued that hybrid security approaches based on the interplay between QKD and classical security mechanisms are crucial to build security-proof architectures which suit to different threat models. Furthermore, the integration of AI and ML was recognised as a disruptive element for obtaining the best performance from

QKD, implementing trajectory-dependent error correction, preventive maintenance of hardware, and adaptive network control. Despite current efforts, significant challenges remain in practical QKD systems, such as scalable quantum repeaters, QKD protocol standardization, and real-world experimental verifications on commercial-scale networks for the transition from laboratory demonstrations to practical devices.

Final Thoughts on QKD in 6G advent of 6G networks envisions enormous data rates, ultra-low latency, massive connections of devices, and ubiquitous AI integration, posing challenges of new extremes that call for the establishment of an inherently secure communication infrastructure that is secure against any quantum attacks coming in the future. QKD exploits the laws of quantum physics to offer key agreement methods that are proven to be secure against arbitrary computational advancements such as quantum computers attacks [9]. But to deploy QKD in 6G era, this requires one to handle a number of complex challenges, including integrating quantum hardware with mobile and wireless infrastructure, managing the interplay of classical-radio frequency (RF) and quantum RF in heterogeneous environment, and dealing with the resource constraints in mobiles [11]. Additionally, the dynamic, distributed environment of 6G networks call for novel quantum networking architectures that facilitate flexible routing, multiplexing, and quantum resource management. The interplay of QKD with classical post-quantum cryptography (PQC) as well as AI-enhanced network intelligence is essential for layered, adaptive, and scalable security solutions. This hybrid QKD allow QKD to be not only a theoretical ideal but also a realistic part of the overall security mechanism of next-generation 6G communication.

The Implications for the Research and its Practical Application of Future studies will have to strive to overcome the practical, as well as theoretical, obstacles in order to develop the full potential for QKD in 6G systems. This includes promoting quantum hardware technologies ranging from high-rate photon sources, low-noise detectors, to quantum repeaters to extend secure communication across the globes [13]. In addition, the development of advanced quantum channel models which can accurately capture the physical and network-level characteristics of 6th generation mobile network (6G), is necessary to enable efficient QKD protocols under mobile, wireless and heterogeneous environment [14]. Efforts toward standardization and interoperability are required for large scale uptake and commercialization and therefore require the collaboration of industry and academia and regulatory bodies [15]. Exploration of tighter AI and ML coupling is also needed to automate key management, anomaly detection, and real-time resource allocation in support of self-healing/adaptable quantum networks. [17] Funders should support construction of scalable testbeds and pilot projects that can demonstrate QKD performance under field conditions sooner rather than later, promoting technology transfer from research to infrastructure [18]. Furthermore, it will be necessary to foster cross-disciplinary cooperation, involving quantum physics, communication engineering, cybersecurity and AI, in a mission to address systemic issues and provide secure communication facilities. The integration of these research and practical results will be indispensable in laying a solid foundation for QDSR&T 6G networking. The Research Roadmap for Scalable QKD in 6G is illustrated in Figure 3.

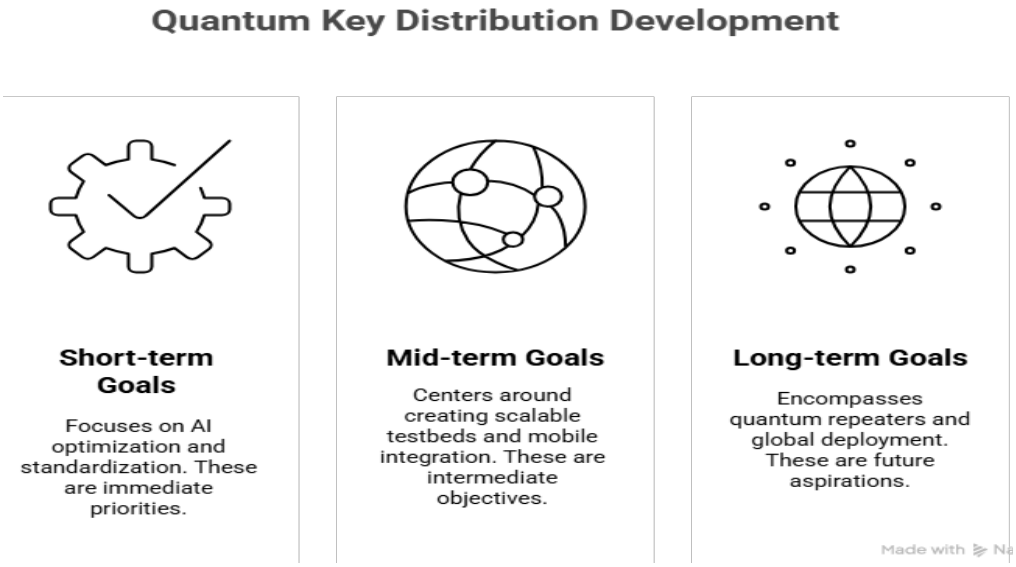

Figure 3: Research Roadmap for Scalable QKD in 6G

8. Conclusion

Progression towards sixth-generation (6G) networks offers unprecedented performance gains, however also exposes communication infrastructures to evolving security risks; none so much as quantum computing. This extensive review has considered QKD as a fundamental technique for securing 6G networks. With the assistance of quantum mechanics, QKD provides unconditional security of key exchange, which can be used to overcome weaknesses of classical cryptography. By examining QKD protocols, integration architectures and hybrid security models, this work seeks to emphasise QKD's ability to "play nice" with incumbent systems whilst confronting challenges of latency, scale and deployment. In addition, convergence of QKD with Artificial Intelligence (AI) and Machine Learning (ML) potentially creates new avenues to adaptive key management, anomaly

detection, and intelligent routing, thereby toward highly secured, automated 6G infrastructures. While there has been significant progress, a number of important research challenges remain, such as the development of efficient quantum repeaters, the definition of standardised protocols and the validation of quantum devices in real-world conditions. Filling such gaps will require close collaboration between quantum physics, cybersecurity and telecommunications engineering. Next-generation 6G networks will need to deliver not just fast and smart connectivity, but also be founded on security-by-design. In the post-quantum era, quantumsecure communication systems will require the integration of QKD (as well as post-quantum cryptography and AI) for the technology to be resilient.

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.