Chapter

Quantum-Resilient Cryptographic Techniques for AI-Driven 6G Communication

A.F.M. Shahen Shah, A.F.M. Suaib Akhter and Muhammet Ali Karabulut

Abstract

The rise of 6G communication networks, powered by artificial intelligence (AI), promises a new era of connectivity with ultra-fast data speeds, intelligent applications, and seamless integration across a wide range of devices. However, the immense volume of sensitive data handled by these ultra-dense networks brings heightened concerns about privacy and security. Quantum cryptography, which leverages the principles of quantum mechanics, offers groundbreaking potential for securing communications; yet, the advent of quantum computing poses significant threats to traditional cryptographic systems. This challenge underscores the need for quantum-resilient cryptographic solutions. This review delves into the intersection of quantum-resilient cryptographic techniques and AI-driven 6G communication networks. It provides a detailed examination of existing quantum-resistant algorithms, evaluates their suitability in AI-enabled 6G systems, and highlights critical challenges and potential future directions. By addressing the pressing demand for secure and resilient communication frameworks, this study contributes to the development of 6G systems that can withstand the security threats posed by the quantum computing era.

Keywords: artificial intelligence, quantum cryptography, quantum-resilient cryptographic techniques, security threats, 6G

1. Introduction

Today's fast-growing quantum computing capabilities risk the reliability of traditional encryption methods and constitute a huge security risk to future communication networks. Data security is especially important in new generation communication infrastructures like 6G, which are powered by artificial intelligence and feature enormous data rates. In this context, quantum-resistant cryptography (QRC) is a study field that seeks to assure secure communication by developing and implementing cryptographic algorithms that are resistant to the computational capability of quantum computers. Quantum-resistant cryptographic systems provide security mechanisms that can withstand future quantum attacks by depending on mathematical issues that are impervious to quantum algorithms like Shor's algorithm.

These techniques will play a vital role in protecting confidentiality, data integrity, and authentication in 6G communication networks.

6G communication is the next-generation wireless communication technology that is currently under active development and is expected to offer significant improvements over 5G technology. 6G aims to provide higher speeds, lower latency, and higher capacity. For example, 6G aims to reach data rates of up to 1 Tbps and reduce latency to less than 0.1 ms. These developments will pave the way for next-generation applications such as holographic telepresence, real-time digital twins, and seamless human-machine interaction. The core technologies of 6G include terahertz frequency bands, artificial intelligence (AI) integration, and advanced antenna technologies.

With features such as high speed, low latency, and extensive coverage, 6G communication networks provide an effective platform for the growth of AI-based applications. However, the integration of AI in these networks, particularly with the development of Internet of Things (IoT) devices, raises substantial data security and privacy concerns. At this juncture, QRC is important to ensure that the interaction between 6G and AI is secure. AI algorithms can improve system reliability and efficiency by optimizing QRC procedures, key management, and intrusion detection. On the other hand, QRC helps to protect sensitive data and provide dependable communication by ensuring the secure operation of AI-based 6G apps. Therefore, the co-evolution of 6G and AI will accelerate the development and proliferation of QRC and play an important role in constructing a secure digital future.

With the rapid growth of the information age, technological innovations such as AI, 6G, and QRC are vital to determining the future of our digital world. The interplay of these technologies presents unique prospects for developing a safe, intelligent, and efficient communication infrastructure. 6G provides real-time data analysis and decision-making by delivering the high bandwidth and low latency required for AI applications. On the other hand, AI is utilized to build and optimize QRC algorithms, resulting in stronger protection systems against complex cyber-attacks. QRC serves as the foundation for a dependable and secure digital environment by protecting critical data transported across 6G networks and AI algorithms from future quantum computing threats. The synergistic interaction of these technologies will accelerate innovation, especially in areas such as autonomous vehicles, smart cities, and personalized healthcare, and will provide significant transformations in every aspect of society and the economy.

1.1 Background and motivation

The rise of 6G communication networks, powered by AI, promises a new era of connectivity with ultra-fast data speeds, intelligent applications, and seamless integration across a wide range of devices [1]. However, the immense volume of sensitive data handled by these ultra-dense networks brings heightened concerns about privacy and security. Quantum cryptography, which leverages the principles of quantum mechanics, offers groundbreaking potential for securing communications; yet, the advent of quantum computing poses significant threats to traditional cryptographic systems. This challenge underscores the need for quantum-resilient cryptographic solutions. This chapter explores the intersection of quantum-resilient cryptographic techniques and AI-driven 6G systems, offering a comprehensive analysis of existing quantum-resistant algorithms, their feasibility in AI-enabled 6G environments, and the associated implementation challenges. Furthermore,

it explores future research directions to address vulnerabilities in securing these advanced networks. By tackling the critical need for robust and adaptive security frameworks, this study contributes to the development of future-proof security solutions for a hyperconnected world.

The 6G technology under development aims to reach data speeds of up to 1 Tbps, which represents a significant increase over the current 5G technology. These higher speeds will further increase security vulnerabilities and therefore further emphasize the importance of quantum-resistant cryptographic techniques.

2. Overview of 6G communication networks

This part examines the revolutionary shift from 5G to 6G communication networks, emphasizing the technological innovations that reshape connectivity, network features, and applications. Although 5G has proven to be a significant advancement in providing quicker speeds, reduced latency, and improved device connectivity, 6G imagines a more cohesive and smart communication network. By integrating AI and utilizing terahertz frequency bands, 6G aspires to provide unmatched speed, reliability, and coverage, enabling advanced applications such as holographic telepresence, real-time digital twins, and smooth human-machine collaboration. This segment explores the transition from 5G to 6G, highlighting its essential characteristics, foundational technologies, and the critical function AI serves in promoting flexibility, effectiveness, and safety in this advanced networking framework [2, 3]. A clear and concise view of how 6G surpasses its predecessors in performance, efficiency, and application scope is presented in **Table 1**.

2.1 Role of artificial intelligence in 6G

Artificial Intelligence (AI) is set to significantly influence the creation and functioning of 6G communication networks. As networks grow in complexity, AI guarantees that 6G systems remain efficient, adaptable, secure, and able to satisfy the requirements of new technologies. The role of AI in 6G covers various areas, including resource management and optimization, predictive analytics, and improved security measures. **Figure 1** shows the role of AI in 6G.

Dynamic resource management: AI facilitates instantaneous resource distribution in 6G networks, guaranteeing the efficient allocation of bandwidth, energy, and computing resources. Through the examination of network traffic trends, user activities, and surrounding conditions, AI guarantees optimal resource utilization. This ability is essential for sustaining performance in situations with significant data requirements, like holographic communication and immersive virtual environments [6].

Network optimization: AI algorithms play a crucial role in enhancing the performance and efficiency of 6G networks. By utilizing machine learning, AI detects bottlenecks, forecasts demand variations, and adaptively modifies network setups to enhance throughput and reduce latency. AI aids in energy efficiency by turning network components on or off according to usage, thereby enhancing the sustainability objectives of 6G [7].

Anomaly detection and security: In 6G networks, AI significantly enhances security by identifying and mitigating cyber threats in real-time. AI-based anomaly detection systems monitor network behavior to detect irregular patterns, such as unauthorized access or distributed denial-of-service attack (DoS) attacks. By swiftly addressing

Aspect	4G (LTE)	5G	6G
Data Rate	Up to 1 Gbps	Up to 10 Gbps	1 Tbps or more
Latency	~50 ms	~1 ms	<0.1 ms
Frequency Spectrum	Below 6 GHz	Sub-6 GHz and mmWave (24–100 GHz)	Terahertz (0.1–10 THz)
Network Density	Thousands of devices per square km	Millions of devices per square km	Billions of devices per square km
Connectivity	Mobile broadband	Enhanced broadband, IoT, URLLC	Ubiquitous connectivity, extreme IoT
Energy Efficiency	Moderate	Improved	Highly energy-efficient (green networks)
AI Integration	None	Limited	Fully integrated into network architecture
Use Cases	HD video streaming, web browsing	AR/VR, autonomous vehicles, smart cities	Holographic communication, real-time digital twins, telepresence
Sustainability	Not energy-efficient	Moderate	High focus on energy and environmental efficiency
Security Mechanisms	Basic encryption and authentication	Advanced encryption, limited AI security	AI-driven threat detection and self-healing systems
Coverage	Mostly terrestrial	Terrestrial with limited satellite support	Global, including terrestrial, satellite, and deep-sea connectivity
Technology Enablers	OFDMA, MIMO	Massive MIMO, beamforming, network slicing	Cell-free massive MIMO, reconfigurable surfaces, integrated sensing & communication

Table 1.
A clear and concise view of how 6G surpasses its predecessors in performance, efficiency, and application scope [4, 5].

threats, AI helps maintain the integrity and strength of 6G systems, which face increasing targeting due to their vast scale and vital applications [8].

Traffic management: With billions of devices linked to 6G, AI-driven traffic management guarantees seamless data flow and prioritizes essential applications. AI is capable of categorizing data traffic, forecasting congestion areas, and distributing resources properly to ensure quality of service. For instance, in a medical environment, AI can favor telehealth solutions instead of nonessential data flows to guarantee continuous service [9].

Predictive maintenance: Predictive maintenance is yet another field where AI excels in 6G networks. Through the examination of both real-time and historical performance data, AI can forecast possible system failures and arrange maintenance in advance. This decreases downtime, cuts costs, and guarantees continuous connectivity for users [7].

In summary, AI acts as the foundation of 6G networks, facilitating their agile, smart, and safe functioning. Incorporating it into the fundamental structure of 6G guarantees that these networks can address the demands of a hyperconnected environment, facilitating the emergence of next-generation applications and services [10].

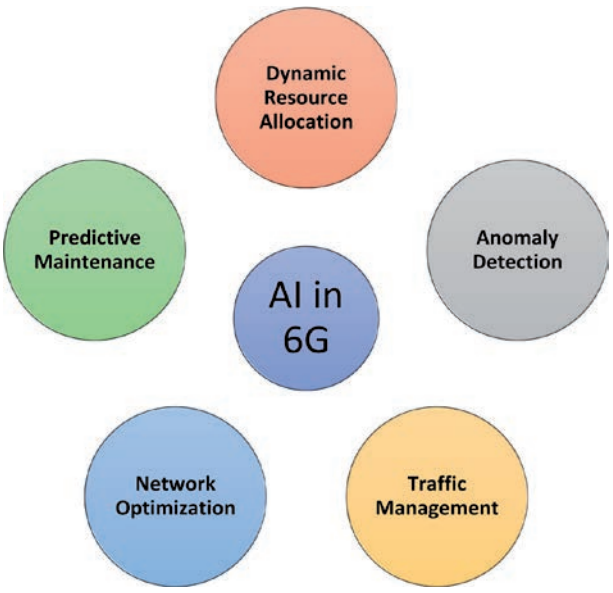


Figure 1.
Role of artificial intelligence in 6G.

3. Security challenges in 6G networks

As 6G technology evolves to meet the demands of a hyperconnected world, its advanced capabilities introduce a new set of security challenges. The integration of AI, edge computing, and terahertz communication expands the threat landscape, requiring novel security solutions to ensure reliability, privacy, and scalability. Emerging use cases, such as autonomous systems, smart grids, and extended reality, bring unique vulnerabilities that demand tailored approaches. This section explores these challenges, starting with the stringent requirements of 6G applications and their implications for security.

3.1 New 6G requirements

Future 6G applications will demand stricter requirements and extended network capabilities compared to 5G [11]. These requirements will enable diverse key use cases while shaping how security measures are implemented in 6G. For Enhanced Ultra-Reliable, Low-Latency Communication (eURLLC), latency-sensitive security workflows must ensure service quality. High reliability necessitates efficient security to protect service availability. In Further Enhanced Mobile Broadband (FeMBB), extreme data rates pose challenges for traffic processing, attack detection, and pervasive encryption. Distributed security solutions, such as local traffic processing using Distributed Ledger Technology (DLT), can alleviate these challenges by offering transparency and redundancy. Similarly, Ultra Massive Machine-Type Communication (umMTC) will drive stringent security needs for the Internet of Everything (IoE), requiring scalable AI/ML-based privacy solutions for resource-constrained and highly mobile devices operating across different administrative domains.

3.2 New applications

6G will drive numerous new technologies and applications, including UAV-based mobility, Connected Autonomous Vehicles (CAV), Smart Grid 2.0, Collaborative Robots, Hyper-Intelligent Healthcare, Industry 5.0, Digital Twins, and extended reality [12]. Each application demands tailored security measures to address its unique requirements and counter advanced attackers. For example, smart grids may need robust encryption, while autonomous vehicles require secure real-time communication protocols.

3.3 Privacy

Privacy protection will be a cornerstone of 6G networks but will face several challenges [13]. The enormous volume of small data exchanges and the integration of intelligence at the network edge increase the risk of data exposure and regulatory difficulties. Additionally, resource-constrained mobile devices running sophisticated applications will face challenges in incorporating privacy-protecting mechanisms. AI/ML introduces both opportunities and risks for privacy, as ML models can either enhance privacy or become targets for attacks such as data poisoning, reverse engineering, and adversarial interference.

3.4 AI and machine learning exploits

AI will be the backbone of 6G network management, optimizing traffic, detecting anomalies, and ensuring seamless connectivity. However, AI itself introduces new risks:

- *Adversarial attacks*: Malicious actors can manipulate AI models with poisoned data or adversarial inputs, compromising network performance and security.
- *Model theft*: Trained AI models can be stolen through side-channel attacks, leading to intellectual property theft and network disruptions.
- *Bias exploitation*: Inaccuracies in training datasets can be exploited to bypass security measures, resulting in misclassification of threats [14].

3.5 Post-quantum cryptographic threats

6G networks must be resilient to quantum computing, which threatens to break traditional cryptographic schemes such as rivest–shamir–adleman (RSA) and elliptic curve cryptography (ECC):

- *Need for quantum-resilient algorithms*: Transitioning to post-quantum cryptography (PQC) requires secure and efficient algorithms capable of handling the demands of high speed, high-volume 6G communication.
- *Integration complexity*: Updating legacy systems and ensuring seamless compatibility with PQC standards presents significant challenges [15].

3.6 Security in software-defined networks (SDN) and network slicing

6G networks rely heavily on SDN and network slicing for flexibility and efficiency, but these features also introduce vulnerabilities:

- *Slice-specific threats*: Each network slice, tailored to a specific use case, may have unique security requirements. A breach in one slice could potentially compromise others.

- *Centralized control risks*: The SDN controller, as a single point of management, becomes an attractive target for attackers [16].

3.7 Physical layer security

6G's reliance on THz communication and massive multiple-input, multiple-output (MIMO) systems brings new physical layer security concerns:

- *Eavesdropping risks:* High-frequency signals are susceptible to eavesdropping due to their directional propagation.

- *Jamming attacks:* The dense deployment of devices and reliance on shared spectrum make 6G networks more vulnerable to jamming [17].

3.8 Cyber-physical system (CPS) security

6G networks will be integral to critical infrastructure, including healthcare, transportation, and energy systems. Securing these cyber-physical systems is critical:

- *Life-critical applications*: A breach in CPS could endanger lives, such as in autonomous vehicles or remote surgeries.

- *Supply chain attacks*: Compromising hardware or software during manufacturing can introduce vulnerabilities at scale [18].

3.9 Regulatory and standardization challenges

6G development is progressing rapidly, but the absence of standardized global security protocols poses risks:

- *Fragmented standards*: Inconsistent security frameworks across countries could leave gaps exploitable by attackers.

- *Slow adoption*: Regulatory bodies may lag behind technological advancements, leading to unsecured deployments [19].

4. Quantum cryptography: An overview

4.1 Principles of quantum mechanics in cryptography

Quantum cryptography utilizes the distinctive concepts of quantum mechanics to enable secure communication. Essential principles comprise:

- *Superposition:* Quantum bits (qubits) can occupy various states at the same time, allowing for intricate encoding methods. This concept is essential for the improved security and computational capabilities of quantum systems [20].

- *Entanglement:* Linked quantum particles guarantee that any disturbance to one particle is observable in its entangled partner. This feature allows for secure communication pathways, where any interference affects the entangled state [21, 22].

- *No-cloning theorem:* An exact duplicate of an unknown quantum state cannot be made, which allows for the detection of eavesdropping. This theorem is essential for safeguarding the integrity of transmitted quantum information [23].

These principles form the foundation of quantum cryptographic methods, offering a level of security unattainable with classical techniques.

4.2 Key distribution protocols

Quantum cryptography is best known for its application in quantum key distribution (QKD), which enables two parties to share encryption keys securely. Prominent protocols include:

- *BB84 protocol:* The initial functional QKD protocol that utilizes polarized photons for the secure encoding and transmission of information [24]. This protocol remains the cornerstone of modern QKD systems.

- *E91 protocol:* Based on quantum entanglement, this protocol guarantees that any eavesdropping efforts disturb the entangled state, indicating the breach [25].

- *Decoy state QKD:* An improvement over BB84, this method incorporates decoy states to identify photon number splitting attacks, thus boosting security and effectiveness [26].

These protocols exemplify the potential of quantum cryptography in achieving unbreakable key exchanges.

4.3 Strengths and limitations of quantum cryptography

4.3.1 Strengths

- *Unconditional security:* Security is rooted in the laws of physics rather than computational complexity, providing resilience against current and future attacks [27].

- *Eavesdropping detection:* Any attempt to intercept communication alters the quantum states, alerting the communicating parties [28].

- *Future proofing:* Resistant to quantum computer-based attacks on classical encryption methods, ensuring long-term data security [29].

4.3.2 Limitations

- *Hardware challenges*: Quantum devices require highly sensitive and precise instruments, such as single-photon detectors and entangled photon sources, for operation [30].

- *Scalability issues:* Deploying quantum cryptography on a large-scale is complex and resource-intensive due to current technological limitations [31].

- *Limited communication distance:* Signal degradation in quantum channels restricts the range of QKD systems. Efforts like satellite-based QKD are being explored to overcome this limitation [32].

While quantum cryptography offers transformative security capabilities, its practical adoption requires overcoming significant technical and logistical hurdles.

5. Quantum-resilient cryptographic techniques

With the advancement of quantum computing technology, the cryptographic algorithms safeguarding existing communication systems are becoming more and more exposed. This chapter investigates quantum-resistant cryptographic methods crucial for safeguarding 6G communication systems, highlighting post-quantum cryptography (PQC) along with its application.

5.1 Post-quantum cryptography: A primer

Post-quantum cryptography (PQC) denotes algorithms intended to withstand assaults from quantum computers while still being compatible with traditional systems. In contrast to quantum cryptography, which employs quantum mechanics principles, PQC modifies conventional cryptographic systems to protect against quantum dangers. These algorithms seek to ensure a smooth shift into the quantum age without needing specific quantum equipment. Recent initiatives by groups such as the National Institute of Standards and Technology (NIST) have been crucial in standardizing PQC techniques to protect digital communication systems [33].

5.2 Prominent quantum-resistant algorithms

Various post-quantum cryptographic algorithms have been developed, each leveraging different mathematical foundations to counteract quantum threats. Here is an overview of the most prominent approaches:

5.2.1 Lattice-based cryptography

Overview: Lattice-based cryptography relies on the hardness of problems like the Shortest Vector Problem (SVP) and Learning with Errors (LWE). These problems are computationally challenging for both classical and quantum computers, making them a strong foundation for cryptographic systems.

Advantages: High computational efficiency and versatility, supporting encryption, key exchange, and digital signature schemes.

Applications: Widely used in NIST finalist schemes like Kyber (encryption) and Dilithium (digital signatures), which offer robust security and practical implementation [34].

5.2.2 Code-based cryptography

Overview: Code-based cryptography builds on the difficulty of decoding random linear codes, as demonstrated in the McEliece cryptosystem.

Advantages: Long-standing security track record and resistance to quantum attacks.

Challenges: Requires larger key sizes, which can hinder performance in resource-constrained environments.

Applications: Suitable for environments where security outweighs constraints on memory and bandwidth [35].

5.2.3 Multivariate quadratic cryptography

Overview: Multivariate quadratic cryptography uses systems of multivariate quadratic equations over finite fields for security.

Advantages: Efficient computation and compact signature sizes make this approach attractive for specific use cases.

Challenges: Vulnerable to specialized algebraic attacks, leading to limited adoption in large-scale systems.

5.2.4 Hash-based cryptography

Overview: Hash-based cryptography relies on the collision resistance of cryptographic hash functions, with Merkle trees and eXtended Merkle Signature Scheme (XMSS) being prominent examples.

Advantages: Simple design and minimal reliance on untested mathematical assumptions, ensuring long-term security.

Challenges: Inefficient for applications requiring frequent key exchanges due to constraints like one-time key usage [36].

5.3 Comparative analysis of post-quantum algorithms

Each quantum-resistant algorithm offers unique benefits and trade-offs, making them suitable for different applications in AI-driven 6G communication:

Lattice-based cryptography: Known for its high efficiency, it requires rigorous parameter optimization to prevent side-channel attacks. It is ideal for general-purpose encryption in 6G systems.

Code-based cryptography: Provides strong security guarantees but struggles with scalability due to its large key sizes. It is suitable for high-security, low-latency applications like secure control systems.

Hash-based cryptography: Simplistic and well-understood, but its limitations in dynamic key exchanges make it less suitable for high-frequency communication networks.

The choice of algorithm depends on the specific requirements of 6G systems, including latency, bandwidth, computational resources, and energy constraints. The adoption of hybrid systems combining multiple quantum-resilient techniques is also being explored for comprehensive security solutions [37].

6. Applicability in AI-driven 6G networks

Incorporating quantum-resilient cryptographic methods into AI-based 6G networks is essential for providing secure, reliable, and efficient communication

in future applications. By protecting data integrity and privacy, allowing real-time encryption, and facilitating AI-driven anomaly detection, these methods tackle the increased security challenges presented by quantum computing. Moreover, strong systems for authentication, key management, and end-to-end encryption provide consistent security throughout versatile and diverse 6G settings. Finding a balance between these security measures and performance needs is crucial for real-time AI applications such as autonomous systems, smart healthcare, and immersive technologies, establishing a secure and scalable 6G environment.

6.1 Integrating quantum-resilient cryptography with AI systems

The integration of quantum-resilient cryptographic techniques into AI-driven 6G networks is essential for ensuring secure and efficient communication. Key considerations include:

Data integrity and privacy: Post-quantum cryptography (PQC) ensures that sensitive AI-generated data, such as predictive models, user analytics, and decision-making outputs, remains secure against the computational threats posed by quantum computers. For instance, lattice-based schemes like Learning with Errors (LWE) can secure critical AI datasets used in smart city infrastructures or financial modeling systems. This is particularly crucial for protecting federated learning systems, where user devices collaborate on model training without compromising data privacy [38].

Real-time encryption: AI-enabled systems in 6G, such as autonomous drones and real-time analytics platforms, require rapid encryption and decryption processes. Techniques like isogeny-based cryptography, which offer smaller key sizes, are promising candidates for achieving both security and computational efficiency in scenarios demanding real-time data exchange [39].

AI-enhanced security: Machine learning models can complement cryptographic techniques by providing real-time anomaly detection and breach prediction. For example, an AI model could monitor patterns in encrypted traffic and detect deviations indicative of potential attacks, such as quantum-assisted brute-force decryption attempts. This layered security framework combines proactive AI-driven insights with robust cryptographic protocols [40].

6.2 Security frameworks for 6G communication

Quantum-resilient cryptographic techniques are instrumental in designing robust security frameworks for AI-driven 6G networks:

- *Authentication protocols*: Lattice-based cryptography, such as the NTRUEncrypt protocol, is well-suited for secure authentication in 6G. For instance, these protocols can secure communication between IoT devices in smart homes or industrial settings, preventing unauthorized access or impersonation attacks [41].

- *Key management systems*: Dynamic 6G environments, such as autonomous vehicular networks or drone swarms, require efficient and secure key distribution mechanisms. AI can optimize these processes by predicting network changes and preemptively generating quantum-resistant keys. For example, reinforcement learning algorithms can adapt key renewal frequencies based on network conditions, ensuring seamless integration of PQC in dynamic scenarios [41].

- *End-to-end encryption*: Secure communication across devices, from IoT endpoints to centralized AI systems, can be achieved through post-quantum encryption techniques like hash-based signatures (e.g., XMSS). This is particularly important in critical applications such as military communication systems or national healthcare networks, where secure end-to-end data transmission is paramount [42].

6.3 Performance implications in real-time AI applications

Quantum-resilient cryptographic solutions must balance security with performance, especially in real-time AI applications where latency and resource efficiency are critical.

- *Autonomous systems*: Ultra-low latency is crucial for AI-driven autonomous vehicles, drones, and robotics. For example, a self-driving car in a 6G-connected smart city must exchange encrypted data on traffic conditions with nearby vehicles and infrastructure in milliseconds. Lightweight quantum-resistant algorithms like ring-LWE can provide the required balance between speed and security in these scenarios [43].

- *Smart healthcare*: 6G-enabled AI systems in telemedicine, such as real-time diagnostic platforms and robotic surgery, demand robust encryption to protect sensitive patient data while ensuring uninterrupted service. For instance, a surgical robot performing a remote operation must communicate securely with medical professionals in real-time, where any delay caused by encryption overhead could be life-threatening [44].

- *Immersive applications*: Augmented reality (AR) and virtual reality (VR) environments powered by 6G require lightweight cryptographic solutions to avoid disruptions in user experience. For instance, a VR-based remote education platform must ensure the secure streaming of interactive content to students worldwide without compromising on responsiveness. Cryptographic protocols optimized for low-power devices and edge computing can enhance these applications [45].

7. Challenges and open research directions

7.1 Technical and implementation barriers

The adoption of quantum-resilient cryptographic techniques in AI-driven 6G networks faces several technical and practical challenges:

1. *Computational overhead:* Post-quantum cryptographic algorithms, such as lattice-based and code-based cryptography, demand significantly higher computational resources compared to classical algorithms. This requirement can strain devices with limited processing power, including IoT nodes and edge devices, potentially affecting overall network efficiency and latency [46].

2. *Key size and bandwidth*: Many post-quantum cryptographic schemes require substantially larger key sizes and signature lengths. This increases storage re-

quirements and impacts transmission efficiency, particularly in bandwidth-constrained environments characteristic of 6G networks. These challenges become critical for applications involving massive IoT and ultra-reliable low-latency communication (URLLC) [47].

3. *Compatibility issues*: Incorporating quantum-resilient cryptographic methods into existing network infrastructures and communication protocols often requires significant modifications. This leads to compatibility concerns, higher implementation costs, and a complex transition phase, making backward compatibility with legacy systems a substantial hurdle [46].

4. *AI-driven optimizations*: AI-driven 6G networks rely on dynamic, adaptive configurations. Implementing AI-based optimization for managing cryptographic processes, such as key management and real-time authentication, is a complex task. The interplay between cryptographic demands and AI algorithm overheads further complicates system-level optimizations [48].

7.2 Standardization efforts for post-quantum cryptography

The successful implementation of post-quantum cryptography in 6G communication systems necessitates a standardized global framework to ensure interoperability, security, and efficiency.

1. *NIST post-quantum cryptography standardization*: The National Institute of Standards and Technology (NIST) is leading the global effort to identify, evaluate, and standardize post-quantum cryptographic algorithms. These efforts aim to balance the trade-offs between security, computational efficiency, and practical implementation challenges [49].

2. *Industry collaboration*: Collaboration among academia, industry, and government bodies is critical to fostering the development of practical and interoperable post-quantum cryptographic standards. Initiatives like the European Telecommunications Standards Institute (ETSI) [50] and the International Telecommunication Union (ITU) play a pivotal role in harmonizing efforts across stakeholders [51].

3. *Regulatory challenges*: Cross-border data encryption laws and regulations pose challenges to the deployment of standardized cryptographic solutions. Ensuring compliance with diverse legal frameworks is essential for the seamless adoption of post-quantum cryptography [10].

7.3 Future directions in AI and quantum-resilient security

The intersection of AI and quantum-resilient cryptographic techniques opens several promising avenues for future research and development:

1. *AI-assisted cryptography*: AI can be leveraged to enhance cryptographic algorithms by optimizing key generation, identifying vulnerabilities, and enabling adaptive defense mechanisms against evolving threats. This dynamic approach aligns well with the flexible architecture of 6G networks [52].

2. *Hybrid cryptographic models*: Combining classical, quantum, and post-quantum cryptographic techniques can create robust, multilayered security frameworks. These models can provide resilience against threats originating from both classical and quantum computing capabilities [53].

3. *Lightweight cryptography*: Developing energy-efficient post-quantum cryptographic solutions is crucial for IoT and edge devices with limited power and computational resources. Research in this domain focuses on minimizing key sizes, reducing algorithmic complexity, and improving energy efficiency without compromising security [54].

4. *Quantum cryptography integration*: Exploring the integration of quantum cryptography (e.g., quantum key distribution) with post-quantum techniques is an emerging area of research. This approach aims to create a unified security paradigm that addresses threats from both current and future quantum technologies [55].

These challenges and research opportunities emphasize the importance of interdisciplinary collaboration and innovation in safeguarding 6G networks against emerging security threats.

8. Case studies and applications

The integration of quantum-resilient cryptography into AI-driven 6G systems is being actively explored across various real-world scenarios:

8.1 Examples of AI-driven 6G use cases

- *Smart cities:* Secure communication protocols are essential for AI-driven infrastructure, such as intelligent traffic management systems and automated energy grids, to operate without the risk of data breaches. The implementation of quantum-resistant cryptographic algorithms ensures that the vast amounts of data exchanged within smart cities remain protected from potential quantum attacks [56].

- *Healthcare systems:* In smart healthcare, post-quantum cryptographic techniques safeguard sensitive medical records while ensuring the reliability of AI applications like remote surgery and diagnostics. The adoption of quantum-safe encryption methods is crucial to maintaining patient confidentiality and the integrity of medical data against future quantum threats [57].

- *Autonomous vehicles:* Self-driving cars depend on real-time communication with infrastructure and other vehicles. Quantum-resilient encryption ensures secure exchanges, preventing malicious interference that could compromise safety. The integration of post-quantum cryptography in vehicular communication systems is vital to protect against emerging cyber threats in the quantum era [58].

8.2 Practical deployment of quantum-resilient solutions

- *Quantum-secure IoT networks:* Pilot studies in IoT deployments have implemented lattice-based cryptography to secure data from sensors in smart factories,

demonstrating scalability and efficiency. These studies highlight the feasibility of deploying quantum-resistant algorithms in resource-constrained IoT devices, ensuring long-term security [59].

- *Quantum key distribution trials:* Telecommunications companies have initiated trials integrating quantum key distribution (QKD) systems with 6G infrastructure to enhance data security for AI applications. For instance, O_2 Telefónica has been exploring QKD to secure mobile networks, aiming to create quantum-safe communication channels resistant to future quantum attacks [60].

- *AI-augmented security frameworks:* AI algorithms are being utilized to monitor and adapt post-quantum cryptographic processes in dynamic 6G environments, ensuring optimized performance and security. Projects like CONFIDENTIAL6G focus on developing cryptographic quantum-resistant protocols and security-proof tools, leveraging AI to enhance confidentiality in 6G networks [61].

8.3 Lessons learned from pilot studies

8.3.1 Successes

- Post-quantum algorithms have demonstrated strong resistance to potential quantum attacks, providing a robust foundation for future-proof security in 6G networks [62].

- Hybrid cryptographic models, combining traditional and quantum-resistant techniques, have facilitated smoother transition strategies, allowing for the gradual integration of post-quantum solutions without disrupting existing systems [63].

8.3.2 Challenges

- Increased computational overhead has impacted real-time applications, particularly in resource-constrained environments, necessitating further optimization of post-quantum algorithms to balance security and performance [64].

- Lack of standardization and interoperability has posed barriers to large-scale deployment, highlighting the need for unified standards and collaborative efforts to ensure seamless integration of quantum-resilient cryptography across diverse platforms [65].

These case studies underscore the potential of quantum-resilient cryptography in securing AI-driven 6G networks, while also emphasizing the necessity for ongoing refinement and scalability to address emerging challenges in the quantum era.

9. Conclusion

With the spread of 6G communication networks and the acceleration of AI integration, the importance of quantum-resistant cryptographic techniques is increasing. In order to build a secure and reliable digital ecosystem, the development of QRC

algorithms and their integration into 6G infrastructure is of great importance. In this way, a communication network that is protected against the potential threats of quantum computers can be established, and the confidentiality of sensitive data can be secured. The combined use of AI and QRC will form the basis of smart and secure communication systems of the future and accelerate the digital transformation of society. By exploring the synergistic link between 6G, AI, and QRC, future research on how to improve their integration for safe and intelligent communication systems will be guided.

Author details

A.F.M. Shahen Shah[1*], A.F.M. Suaib Akhter[2] and Muhammet Ali Karabulut[3]

1 Department of Electronics and Communication Engineering, Yildiz Technical University, Istanbul, Turkey

2 Department of Computer Engineering, Sakarya University of Applied Science, Sakarya, Turkey

3 Department of Electronics Engineering, Turkish Air Force Academy, National Defense University, Istanbul, Turkey

*Address all correspondence to: shah@yildiz.edu.tr

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Shah AFMS. A survey from 1G to 5G including the advent of 6G: Architectures, multiple access techniques, and emerging technologies. In: Proc. of IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA: IEEE; 2022. pp. 1117-1123

[2] Raihan A. An overview of the implications of artificial intelligence (AI) in sixth generation (6G) communication network. Research Briefs on Information and Communication Technology Evolution. 2023;**9**:120-146

[3] Telecoming. 2025. Available from: https://www.telecoming.com/blog/the-road-to-6g-evolution-of-5g-technology/

[4] Mihret E, Haile G. 4G, 5G, 6G, 7G and future mobile technologies. Journal of Computer Science and Information Technology. 2021;**9**(2):75

[5] Kshirsagar PR, Reddy DH, Dhingra M, Dhabliya D, Gupta A. A review on comparative study of 4G, 5G and 6G networks. In: In 2022 5th International Conference on Contemporary Computing and Informatics (IC3I). Uttar Pradesh, India: IEEE; 2022. pp. 1830-1833

[6] Ponnusamy V, Vasuki A. AI-enabled intelligent resource management in 6G. In: AI and Blockchain Technology in 6G Wireless Network. Springer Nature Singapore: Singapore; 2022. pp. 71-92

[7] Suresh K et al. Sustainable resource allocation and base station optimization using hybrid deep learning models in 6G wireless networks. Sustainability. 2024;**16**(17):7253

[8] Saeed MM et al. Anomaly detection in 6G networks using machine learning methods. Electronics. 2023;**12**(15):3300

[9] Tariq M, Naeem F, Poor HV. Toward experience-driven traffic management and orchestration in digital-twin-enabled 6G networks. arXiv preprint arXiv:2201.04259. 2022

[10] Chataut R, Nankya M, Akl R. 6G networks and the AI revolution—Exploring technologies, applications, and emerging challenges. Sensors. 2024;**24**(6):1888

[11] Alwis CD. et al. Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research. IEEE Open Journal of the Communications Society. 2021;**2**:836-886

[12] You X et al. Towards 6G wireless communication networks: Vision enabling technologies and new paradigm shifts. SCIENCE CHINA Information Sciences. 2021;**64**(1):1-74

[13] Wang M et al. Security and privacy in 6G networks: New areas and new challenges. Digital Communications and Networks. 2020;**6**(3):281-291

[14] Ylianttila M et al. 6G white paper: Research challenges for trust, security and privacy. arXiv preprint arXiv:2004.11665. 2020

[15] Chamola V, Jolfaei A, Chanana V, Parashari P, Hassija V. Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography. Computer Communications. 2021;**176**:99-118

[16] Cunha J et al. Enhancing network slicing security: Machine learning, software-defined networking, and network functions virtualization-driven strategies. Future Internet. 2024;**16**(7):226

[17] Ara I, Kelley B. Physical layer security for 6G: Toward achieving intelligent native security at layer-1. IEEE Access. 2024;**12**:82800-82824

[18] RS, P. An intelligent dynamic cyber physical system threat detection system for ensuring secured communication in 6G autonomous vehicle networks. Scientific Reports. 2024;**14**(1):20795

[19] Alsaedi WK, et al. Spectrum Options and Allocations for 6G: A Regulatory and Standardization Review. IEEE Open Journal of the Communications Society. 2023;**4**:1787-1812

[20] Clarke J, Wilhelm FK. Superconducting quantum bits. Nature. 2008;**453**(7198):1031-1042

[21] Einstein A, Podolsky B, Rosen N. Can quantum-mechanical description of physical reality be considered complete? Physical Review. 1935;**47**(10):777-780

[22] Bell JS. On the Einstein-Podolsky-Rosen paradox. Physics Physique Физика. 1964;**1**(3):195-200

[23] Wootters WK, Zurek WH. A single quantum cannot be cloned. Nature. 1982;**299**:802-803

[24] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, India: IEEE; 1984

[25] Ekert AK. Quantum cryptography based on Bell's theorem. Physical Review Letters. 1991;**67**(6):661-663

[26] Hwang W-Y. Quantum key distribution with high loss: Toward global secure communication. Physical Review Letters. 2003;**91**(5):057901

[27] Scarani V, Bechmann-Pasquinucci H, Cerf NJ, et al. The security of practical quantum key distribution. Reviews of Modern Physics. 2009;**81**(3):1301-1350

[28] Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Reviews of Modern Physics. 2002;**74**(1):145-195

[29] Shor PW. Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings of 35th Annual Symposium on Foundations of Computer Science. 1994. pp. 124-134

[30] Diamanti E, Lo H-K, Qi B, Yuan Z. Practical challenges in quantum key distribution. NPJ Quantum Information. 2016;**2**:16025

[31] Tannous R et al. Quantum cryptography: Future directions and challenges. Journal of Quantum Information Science. 2022;**12**(1):45-67

[32] Liao S-K, Cai W-Q, Liu W-Y, et al. Satellite-to-ground quantum key distribution. Nature. 2017;**549**:43-47

[33] Chen L et al. Report on post-quantum cryptography. 2016

[34] Lyubashevsky V, Peikert C, Regev O. On Ideal Lattices and Learning with Errors over Rings. 2010

[35] Patarin J. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. 1996

[36] Merkle RC. A certified digital signature. 1989

[37] Campagna M, Chen L. Quantum Safe Cryptography and Security: An Introduction, Benefits, and Impact. 2014

[38] Bernstein DJ, Lange T. Post-quantum cryptography. Nature. 2017;**549**(7671):188-194

[39] Chen L et al. Report on post-quantum cryptography. Vol. 12. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology; 2016

[40] Alshaer NA, Ismail TI. AI-driven quantum technology for enhanced 6G networks: Opportunities, challenges, and future directions. Journal of Laser Science and Applications. 2024;**1**(1):21-30

[41] Abdallah W. A physical layer security scheme for 6G wireless networks using post-quantum cryptography. Computer Communications. 2024;**218**:176-187

[42] Alagic G, Alagic G, Apon D, Cooper D, Dang Q, Dang T, Kelsey J, Lichtinger J, Liu Y-K, Miller C, Moody D, Peralta R, Perlner R, Robinson A, Smith-Tone D. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. 2022

[43] Partala J. Post-quantum cryptography in 6G. Mobile Wireless Networks. 2021;**6G**:431-448

[44] Kumar A, Ottaviani C, Gill SS, Buyya R. Securing the future internet of things with post-quantum cryptography. Security and Privacy. 2022;**5**(2):e200

[45] Bhattacharya P et al. Coalition of 6G and blockchain in AR/VR space: Challenges and future directions. IEEE Access. 2021;**9**:168455-168484

[46] Hoang VT, Ergu YA, Nguyen VL, Chang RG. Security risks and countermeasures of adversarial attacks on AI-driven applications in 6G networks: A survey. Journal of Network and Computer Applications. 2024;**104031**:1-31

[47] Shaik RB, Nagaradjane P, Ioannou I, Sittakul V, Vasiliou V, Pitsillides A. AI/ML-aided capacity maximization strategies for URLLC in 5G/6G wireless systems: A survey. Computer Networks. 2024;**249**:110506

[48] Sharma D, Tilwari V, Pack S. An overview for designing 6G networks: Technologies, spectrum management, enhanced air Interface and AI/ML optimization. IEEE Internet of Things Journal. 2024

[49] Chen L, Moody D, Liu Y. NIST post-quantum cryptography standardization. Transition. 2017;**800**(131A):164

[50] ETSI. Quantum-Safe Cryptography White Paper. 2023. Available from: https://etsi.org

[51] TU-T Study Group. Security Considerations for Next-Generation Networks. ITU White Paper. 2022

[52] Ishtaiwi A et al. Artificial intelligence in cryptographic evolution: Bridging the future of security. In: Innovations in Modern Cryptography. IGI Global; 2024. pp. 31-54

[53] Fathalla E, Azab M. Beyond Classical Cryptography: A Systematic Review of Post-Quantum Hash-Based Signature Schemes, Security, and Optimizations. IEEE Access; 2024

[54] Khan AS et al. A survey on 6G enabled light weight authentication

protocol for UAVs, security, open research issues and future directions. Applied Sciences. 2022;**13**(1):277

[55] Zohaib M, Altuwaijri FS, Hyrynsalmi S. Integrating quantum computing and blockchain: Building the foundations of secure, efficient 6g technology. In: Proceedings of the 1st ACM International Workshop on Quantum Software Engineering: The Next Evolution. 2024. pp. 27-34

[56] [Internet]. 2025. Available from: https://www.ericsson.com/en/reports-and-papers/further-insights/impact-of-quantum-computing-on-5g-6g-security

[57] [Internet]. 2025. Available from: https://www.azoai.com/news/20241105/Unlocking-6G-with-QuantumSecurity-and-AI-Integration.aspx

[58] [Internet]. 2025. Available from: https://hub.telefonica.com/en/research/confidential-6g-project

[59] [Internet]. 2025. Available from: https://irr.singaporetech.edu.sg/articles/conference_contribution/A_Survey_on_PostQuantum_Cryptography_for_5G_6G_Communications/26129599

[60] [Internet]. 2025. Available from: https://www.telefonica.de/news/pressreleases-telefonica-germany/2024/11/kick-off-into-the-quantum-ageo2-telefonica-enhances-mobilenetwork-efficiency-and-securitywith-quantum-technologies-on-aws.html

[61] [Internet]. 2025. Available from: https://hub.telefonica.com/en/research/confidential-6g-project

[62] Available from: https://www.6gacademy.com/what-it-is-post-quantum-security

[63] [Internet]. 2025. Available from: https://en.wikipedia.org/wiki/Post-quantum_cryptography

[64] [Internet]. 2025. Available from: https://irr.singaporetech.edu.sg/articles/conference_contribution/A_Survey_on_PostQuantum_Cryptography_for_5G_6G_Communications/26129599

[65] [Internet]. 2025. Available from: https://decentcybersecurity.eu/evaluating-the-security-of-6g-networkswith-post-quantum-cryptography-in-2024/