Computing&AI Connect
ISSN: 3006-4163
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

SCIFINITI PUBLISHING

OPEN ACCESS

Research Article

Quantum-Safe Networks for 6G an Integrated Survey on PQC, QKD, and Satellite QKD with Future Perspectives

Shiang-Jiun Chen,[1] Yi-Hsueh Tsai ✉,[12*]

[1] National Taipei University of Technology; Taipei, Taiwan, [2] Institute for Information Industry; Taipei, Taiwan
annette@ntut.edu.tw, yihsuehtsai@g.ntu.edu.tw

Chen, Shiang-Jiun 0009-0002-7542-2374
Yi-Hsueh Tsai 0009-0007-9676-9365

Abstract

Quantum computing presents significant issues to the current cryptographic landscape, especially with the upcoming deployment of 6G networks. Traditional cryptographic algorithms, such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), are vulnerable to quantum-based attacks, leading to the need for Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), and Satellite-based QKD solutions. This paper offers a comprehensive review of these quantum-safe technologies, discussing their integration within the context of 6G networks. Key performance indicators (KPIs), scalability issues, and hybrid cryptographic solutions are analyzed, along with the potential of Satellite-based QKD in securing global communications. The paper also explores use cases in healthcare, financial services, defense, and autonomous systems, evaluating future research directions and issues in scaling these quantum-safe technologies across industries.

Keywords

quantum computing, rivest-shamir-adleman, elliptic curve cryptography, post-quantum cryptography, quantum key distribution, quantum-safe networks

Introduction

The rapid development of quantum computing has become a significant threat to existing cryptographic systems, especially widely used standards like Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) [1]. Quantum machines, using algorithms like Shor's, can solve complex mathematical problems such as large number factorization and discrete logarithms [2-4], which can break encryption systems. Similarly, Grover's algorithm issues symmetric encryption methods like the Advanced Encryption Standard (AES) [5], significantly reducing their security. For instance, AES-128's security could drop to the equivalent of 64 bits, making AES-256 the minimum requirement for quantum resistance. In response to these looming threats, Post-Quantum Cryptography (PQC) [6] has been developed to resist quantum attacks by utilizing techniques like lattice-based and hash-based cryptography [7]. Lattice-based cryptography is founded on mathematical problems, such as the Shortest Vector Problem (SVP) and Learning With Errors (LWE), that are considered exceptionally difficult for quantum computers to solve. These problems are distinct from those that quantum algorithms can efficiently address, and to date, no quantum algorithm has been discovered that can effectively solve them. Hash-based cryptography does not rely on number-theoretic problems. Instead, it depends on the security of hash functions, with

* Corresponding Author: Tsai, Yi-Hsueh
Name, affiliation, yihsuehtsai@g.ntu.edu.tw
Tel.: + 18586337590

key properties such as preimage resistance, second preimage resistance, and collision resistance. The security of these functions is based on the difficulty of reversing them, a problem that remains exceptionally challenging for quantum computers. While quantum computing may accelerate certain attacks on hash-based signatures, these systems are better equipped to withstand quantum threats than traditional number-theoretic cryptosystems. As quantum computing technology progresses, hash-based cryptography is expected to play a vital role in achieving post-quantum security.

However, adopting PQC faces issues, such as larger key sizes and difficulties with integration into existing infrastructure.

The advent of 6G networks, designed to deliver ultra-reliable low-latency communications (URLLC), massive machine-type communications (mMTC), and enhanced mobile broadband (eMBB), increases the risks posed by quantum computing [8]. The overall landscape of quantum threats and defense strategies pertinent to 6G is an active area of research [9]. Critical applications like autonomous driving and telemedicine, which require real-time communication, could be disrupted by quantum adversaries, leading to severe consequences [10, 11]. Recent studies also highlight that scalable and secure key management in QKD networks is essential to protecting such latency-sensitive systems against quantum threats [12]. Similarly, mMTC will connect numerous IoT devices in environments like smart cities and logistics, but many lack sufficient cryptographic resources, leaving them vulnerable to quantum attacks [13]. Additionally, eMBB will enable high-speed data transmission for applications such as VR, AR, and 8K video, increasing the volume of sensitive data at risk [8]. Recent work highlights the importance of secure key management strategies for these latency-sensitive environments [9], ensuring the resilience of 6G infrastructures against quantum risks.

Satellite-based Quantum Key Distribution (SatQKD) [14] adds an essential layer of quantum-safe security, particularly for long-distance key exchanges. Satellites equipped with QKD systems can securely transmit cryptographic keys between ground stations [15], guaranteeing that any attempt to intercept the exchange is detected instantly. Combined with PQC, SatQKD strengthens the security of data transmitted over satellite communication networks, bolstering the security of 6G infrastructures. This technology is becoming increasingly viable, addressing key issues securing high-speed, long-distance communication networks, especially in defense, global navigation, and broadcasting sectors.

PQC, QKD, and SatQKD are essential components of quantum-safe networks designed for 6G technology. These innovations aim to provide robust security against potential quantum computing threats, ensuring the integrity and confidentiality of communications. PQC protects data from future cyberattacks, while QKD facilitates secure key exchanges through quantum mechanics. Additionally, SatQKD extends these benefits to satellite communications, enhancing security for data transmitted over long distances. Together, these features form a comprehensive security framework for advancing 6G networks. For more details, please refer to Table 1.

Table 1: Key Features of Quantum-Safe Networks for 6G.

Feature	Description
PQC (Post-Quantum Cryptography)	Techniques for quantum-resistant encryption
QKD (Quantum Key Distribution)	Secure key exchange leveraging quantum mechanics
SatQKD (Satellite QKD)	Long-distance QKD with satellite-based systems

As 6G networks expand, the potential threat landscape grows, particularly in highly digitized sectors like energy, transportation, and finance. A quantum attack on critical infrastructure could cause severe operational disruptions and financial losses [16]. Additionally, the "harvest now, decrypt later" strategy poses a persistent threat, as encrypted data intercepted today could be decrypted by quantum computers in the future, exposing sensitive information [17].

In conclusion, the rise of quantum computing presents dual threats to both cryptographic standards and the security of 6G networks. To mitigate these risks, industries must adopt quantum-resistant solutions like PQC and QKD, including satellite-based QKD, to ensure long-term data integrity, confidentiality, and security in the quantum era.

Background and motivation

A. Evolution of cryptographic threats

The rapid evolution of cryptography has paralleled advancements in computational power and the complexity of cyber threats. Classical cryptographic methods like RSA and ECC have long safeguarded sensitive data based on the difficulty of mathematical problems such as factoring large integers and solving discrete logarithms. However, the rise of quantum computing now threatens these systems. Using Shor's algorithm [3-4], Quantum computers can break RSA and ECC, while Grover's algorithm [5] can halve the security strength of symmetric encryption methods like AES. As a result, cryptographic standards are under pressure to adapt to these emerging threats.

Recognizing this challenge, the National Institute of Standards and Technology (NIST) launched a Post-

Quantum Cryptography (PQC) initiative in 2016 [18]. This global effort aims to develop algorithms that resist classical and quantum attacks. As quantum technology advances, replacing vulnerable cryptographic systems with PQC solutions is becoming necessary [19-21]. However, the transition to PQC is complex, requiring hybrid cryptographic models that combine classical and quantum-safe systems to ensure a smooth migration and uninterrupted security. Industries such as healthcare, finance, and defense must adopt these new cryptographic standards to avoid the potentially catastrophic consequences of data breaches, financial losses, and infrastructure failures. As quantum computing becomes viable, the urgency to implement these solutions will only grow.

B. Post-quantum cryptography (PQC)

PQC is specifically designed to protect against the emerging threat of quantum computing, which can potentially dismantle traditional cryptographic systems. Governments, enterprises, and researchers prioritize developing PQC to ensure long-term security against classical and quantum attacks [6, 18-21]. This effort is crucial as quantum computing threatens current encryption methods.

One of the most promising approaches in PQC is lattice-based cryptography, which relies on complex mathematical problems believed to resist quantum attacks [19-20, 22-23]. Lattice-based cryptography has become a leading solution in post-quantum cryptography due to its strong resistance to classical and quantum attacks. The security of lattice-based methods is built on the difficulty of solving mathematical problems like the Shortest Vector Problem (SVP) and Learning with Errors (LWE) [24], which become exponentially harder as dimensions increase, making them resistant even to quantum algorithms like Shor's [3-4]. This robustness positions lattice-based cryptography as a key player in future quantum-resistant encryption. Algorithms like Cryptographic Suite for Algebraic Lattices (CRYSTALS)-Kyber and CRYSTALS-Dilithium offer quantum-safe solutions for key exchanges and digital signatures. They are strong candidates for standardization due to their efficiency and security [25]. CRYSTALS-Kyber and CRYSTALS-Dilithium, two prominent lattice-based algorithms, are finalists in the standardization of NIST Post-Quantum Cryptography (PQC). CRYSTALS-Kyber offers quantum-resistant public key encryption and key exchange [19], while CRYSTALS-Dilithium offers secure digital signatures [20, 21]. Both rely on the LWE problem and are strong candidates for securing communications and authentication in the post-quantum era. While lattice-based cryptography offers significant advantages, key size remains a challenge. Public keys in these schemes can be much larger than those in traditional cryptographic systems, posing issues for storage and bandwidth, especially in constrained environments like IoT [26]. Additionally, while general performance is efficient, some applications, like homomorphic encryption, can be computationally demanding, requiring further optimization for widespread adoption. Despite these hurdles, lattice-based cryptography is a strong contender for securing critical applications in a quantum world. Its versatility in supporting various cryptographic primitives and its proven security against quantum attacks make it one of the most promising solutions for guaranteeing the long-term protection of sensitive communications and data.

Other PQC approaches include hash-based cryptography, which uses cryptographic hash functions to resist quantum threats [27]. Algorithms like XMSS and SPHINCS+ provide quantum-resistant digital signatures, though they often require larger keys and signatures, posing issues for deployment [28, 29]. Despite these drawbacks, the inherent security guarantees of hash-based cryptographic systems make them a valuable component of the PQC landscape. Code-based cryptography, exemplified by the McEliece cryptosystem [30], offers long-standing security but suffers from impractical public key sizes. Multivariate polynomial cryptography, such as the Rainbow signature scheme, is another area of PQC research [31]. While it offers computational efficiency, it faces specific vulnerabilities that limit its security compared to lattice- and hash-based systems. As PQC advances, striking a balance between security and performance remains a significant challenge, particularly in resource-limited settings such as the Internet of Things (IoT) [26].

The transition to PQC will require substantial infrastructure changes, particularly for industries dependent on public-key cryptography. Hybrid approaches combining classical and post-quantum systems will help ensure a smooth migration. As quantum computing advances, the standardization efforts by NIST and the global community will be crucial in securing future communications [18].

Case studies: real-world implementations of PQC and QKD

A. Healthcare and telemedicine

In the healthcare industry, protecting patient data is critical, especially as the adoption of telemedicine, wearable health devices, and remote diagnostics continues to grow. Digitalizing healthcare services has increased the need for secure transmission and storage of sensitive medical data. With 6G networks set to enable faster and real-time communication for medical applications, the vulnerabilities in classical cryptographic systems become a significant concern, particularly as quantum computing approaches viability. The risks posed to patient records, medical imaging, and telemedicine are considerable and require proactive security measures [32-34].

PQC offers a solution to these issues, guaranteeing healthcare data security even in a post-quantum world. Quantum-resistant encryption algorithms like CRYSTALS-Kyber can safeguard patient data stored in electronic health records (EHRs), ensuring secure transmission across healthcare providers [35, 36]. As 6G networks expand, implementing PQC will be critical for protecting data shared between hospitals, insurance companies, and cloud storage platforms. Telemedicine, which increasingly relies on real-time consultations and remote monitoring, can benefit from hash-based cryptography like XMSS and SPHINCS+, guaranteeing the integrity of transmitted data during video consultations or robotic-assisted surgeries [37,38].

Quantum Key Distribution (QKD) also promises to secure healthcare networks, particularly in protecting sensitive data like genetic information or clinical trial results. QKD ensures that encryption keys are securely distributed and can detect any interception attempts, adding an essential layer of security for long-term patient data. Wearable health devices and the Internet of Medical Things (IoMT) also benefit from PQC, as these technologies generate vast amounts of real-time data that must be securely transmitted over 6G networks [39-42].

Incorporating quantum-safe technologies into healthcare systems will improve patient privacy, data integrity, and overall security, especially in light of the increasing frequency of cyberattacks targeting the healthcare sector [43]. PQC and QKD will play a vital role in guaranteeing that healthcare providers comply with emerging security standards, such as those mandated by HIPAA in the United States, guaranteeing patient data remains secure in the post-quantum era [44].

B. Smart factory and satellite communication

The smart factory sector is a key candidate for adopting PQC due to its growing dependence on interconnected systems and real-time data exchange. Smart factories use IoT devices, autonomous systems, and data processing to optimize manufacturing operations. The security of these systems is critical to protecting against industrial espionage, intellectual property theft, and operational disruptions. As quantum computing advances, traditional cryptographic systems like RSA and ECC, commonly used to secure smart factory communications, will become increasingly vulnerable. To protect data integrity and confidentiality, PQC algorithms like CRYSTALS-Dilithium and Rainbow offer robust, quantum-resistant solutions for safeguarding machine-to-machine (M2M) communications and guaranteeing the authenticity of software updates [45, 46].

Satellite communications face similar security concerns, given their pivotal role in defense, telecommunications, and global navigation satellite systems (GNSS) industries. Secure satellite links are essential for transmitting sensitive information, including military commands, navigation data, and global communications [47]. Quantum computing poses a significant threat to the cryptographic protocols safeguarding these transmissions, raising the risk of eavesdropping or unauthorized access. Integrating PQC into satellite communication systems can ensure data integrity and prevent attackers from intercepting or manipulating satellite transmissions. Furthermore, PQC will be crucial for securing sensitive satellite payloads, such as surveillance and weather data [48].

QKD also holds significant potential in satellite communications by securing cryptographic key exchanges between ground stations and satellites [49]. QKD can detect any attempts to intercept or manipulate the key exchange, providing robust protection for critical communications, particularly for government and military applications. When used with PQC, QKD ensures the secure transmission of satellite control commands, making these systems resilient despite future quantum threats [50].

Both smart factories and satellite communications face long-term issues related to data security, particularly in the context of "harvest now, decrypt later" strategies. Malicious actors may intercept encrypted data today to decrypt it when quantum computers become more powerful. Adopting quantum-safe cryptographic solutions will mitigate these risks and ensure compliance with future security standards.

Methods

A. Combining PQC with symmetric cryptography

While PQC offers a long-term solution to quantum attacks, a hybrid approach combining PQC with traditional symmetric encryption like AES-256 provides an efficient and practical solution during the transition period before quantum computers fully mature. This hybrid model capitalizes on the strengths of both quantum-resistant public key cryptography and the proven security of symmetric encryption systems [51, 52]. AES-256, even in the face of Grover's algorithm, remains secure due to its resilience against quantum attacks, reducing 256-bit security to 128-bit, which is still strong by modern standards [53]. By integrating PQC for key exchange, using algorithms like CRYSTALS-Kyber or NTRUEncrypt, and AES-256 for data encryption, organizations can deploy quantum-safe solutions without overhauling their existing infrastructure [54]. This approach allows for immediate security while leveraging the efficiency of symmetric encryption, particularly in bandwidth-limited or resource-constrained environments such as IoT devices.

The hybrid approach also addresses concerns regarding the larger key sizes associated with many PQC algorithms. While PQC is ideal for secure key exchanges, its larger keys can introduce latency in applications requiring frequent exchanges. By relying on AES-256 for data encryption, organizations can minimize performance issues while maintaining quantum resistance. This strategy is particularly suited for high-security environments like government, finance, and defense, where maintaining confidentiality and integrity is paramount. Combining PQC with AES-256 allows these sectors to take proactive steps toward quantum safety while preserving the performance and security of their current operations.

B. DEPLOYING PQC IN EDGE COMPUTING, SMART FACTORY, AND SATELLITE COMMUNICATION

In increasingly decentralized and data-reliant environments like edge computing, smart factories, and satellite communications, deploying PQC is essential to safeguard sensitive transmissions against emerging quantum threats [55-59]. These systems, which depend on real-time processing, encounter specific security challenges as quantum computing evolves, potentially undermining traditional cryptographic algorithms like RSA and ECC. PQC provides quantum-resistant solutions to secure data transmission and processing within these domains.

One of the primary issues for adopting PQC in edge computing, smart factories, and satellite communications is the limited computational capacity of devices. Many IoT and industrial systems operate with constrained memory and processing power, making implementing larger PQC keys and computationally intensive processes complex. Efforts are ongoing to develop lightweight PQC implementations, guaranteeing that devices with minimal resources can benefit from quantum-safe encryption while maintaining efficiency [56].

Despite these issues, PQC is critical for protecting communications in smart factories, which rely heavily on secure machine-to-machine (M2M) communications to optimize manufacturing processes [57]. Integrating PQC into satellite communications is equally crucial, as it ensures the integrity of data relayed between satellites and ground stations, preventing quantum-enabled eavesdropping and interference in vital communications like military and global positioning systems.

1) Edge computing

In edge computing, data is processed closer to the source, such as IoT devices, sensors, and local nodes, which reduces latency and enhances real-time decision-making [55]. However, this decentralized approach introduces multiple security vulnerabilities, as data needs to be protected at various points throughout the network. PQC algorithms, like lattice-based CRYSTALS-Kyber, can be integrated into these devices to secure key exchanges and encryption while optimizing real-time decision-making. These quantum-resistant algorithms are well-suited for resource-constrained environments, ensuring data remains protected from quantum attacks without compromising performance. To address the limited processing power of edge devices, lightweight PQC implementations are being developed, enabling efficient operation while providing robust security against quantum threats.

2) Smart factory

In smart factories, interconnected IoT devices and automated control systems drive operations, making the security of machine-to-machine (M2M) communications crucial [26, 56-57]. PQC offers quantum-resistant protection to secure industrial control systems, safeguarding production processes, intellectual property, and operational data from future quantum-enabled cyberattacks. Smart factories rely on

low-latency, high-speed data transmission to optimize manufacturing processes. PQC can be integrated into these systems to maintain data integrity and protect against tampering or unauthorized access. Using PQC ensures that real-time commands and sensitive information remain secure, even as the number of connected devices in smart factories grows.

2) Satellite communication

In satellite communication, security is paramount due to the global nature of data transmission, particularly for critical services like military communications, navigation systems, and international broadcasting. PQC can be implemented to protect satellite communications from quantum threats, guaranteeing that sensitive data exchanged between ground stations and satellites remains secure [58]. QKD is also being explored for satellite systems to enhance cryptographic key exchanges, allowing immediate detection of any attempts to intercept or tamper with transmissions. Recent developments in SatQKD make it possible to integrate QKD with PQC, creating a more resilient and secure satellite communication framework for the future [59].

Current developments in quantum-safe networks (QSN) within GSMA, NGMN, and 3GPP

As quantum computing advances, it poses significant threats to current cryptographic algorithms, foundational to secure telecommunications. In response, key global organizations, including GSMA, and the Next Generation Mobile Networks (NGMN) Alliance, and the 3rd Generation Partnership Project (3GPP) are actively engaged in developing quantum-safe networks (QSN) to ensure the security and resilience of future communication systems, particularly 5G and beyond. These organizations are investigating quantum-resistant cryptographic algorithms, transitioning to 256-bit security, and exploring QKD as part of their strategies to mitigate the risks posed by quantum computing.

A. GSMA's vision for quantum-safe networks

The GSMA, as the principal association overseeing the global ecosystem of mobile network operators, has taken decisive action to steer the telecommunications industry toward robust quantum-safe networks. Recognizing the impending challenges quantum computing poses to current cryptographic systems, the GSMA introduced its Post-Quantum Cryptography (PQC) Guidelines in 2024. These guidelines represent a foundational step in equipping the telecommunications sector to transition to quantum-resistant cryptographic algorithms, aiming to mitigate the risks associated with emerging quantum threats [52, 60].

1) Preparing the industry for quantum threats

The guidelines emphasize preparing for quantum computing's impact on cryptography by evaluating existing systems comprehensively. Key preparatory measures include conducting a detailed cryptographic inventory to identify vulnerabilities, such as algorithms susceptible to quantum attacks. Furthermore, operators are encouraged to adopt migration strategies that underscore crypto-agility—the capacity to switch seamlessly between cryptographic protocols as post-quantum algorithms mature. This agile approach ensures resilience and adaptability in technological evolution [52, 60].

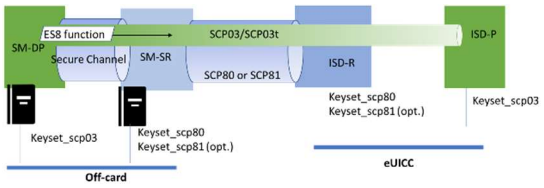

Figure 1: SM-DP/SM-SR/eUICC Channel [52]

Remote SIM provisioning, particularly in the M2M context (GSMA SGP.02 referenced in [52]), involves secure channels between the Subscription Manager Data Preparation (SM-DP), the Subscription Manager Secure Routing (SM-SR), and the embedded Universal Integrated Circuit Card (eUICC), as shown in Figure 1. SCP03/SCP03t logical channels are established through SM-SR, with SCP80/81 channels used between SM-SR and eUICC [52].

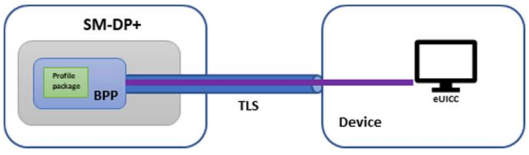

Figure 2: SM-DP+/Device Channel [52]

In the consumer specifications (GSMA SGP.22 also discussed in [52]), the architecture evolves, replacing the SM-SR with an enhanced Subscription Manager Data Preparation (SM-DP+), securing channels with TLS and Diffie-Hellman key exchange, as illustrated in Figure 2 [52]. The SM-DP+ and the Device channel is secured using TLS with ECDHE key exchange and ECDSA or RSA signatures. Profile

protection uses keys derived from Diffie-Hellman key exchange between the SM-DP+ and the eUICC.

2) Hybrid cryptographic schemes for transitional security

A cornerstone of the GSMA's recommendations is the adoption of hybrid cryptographic schemes during the transition to full quantum resistance. These hybrid approaches integrate existing algorithms, like RSA and ECC, with post-quantum cryptographic solutions, creating a dual-layered security architecture. This method not only preserves operational integrity but also provides redundancy against quantum threats, ensuring that data remains secure even as quantum capabilities evolve. The GSMA advocates for active participation in standardization efforts led by organizations like NIST, which is spearheading the global initiative to standardize quantum-resistant algorithms [60, 61].

3) Addressing integration challenges and ensuring performance

The GSMA acknowledges the operational challenges of integrating PQC into existing network architectures. These challenges include potential latency and processing overheads introduced by the computational demands of quantum-safe algorithms. The guidelines recommend meticulous planning and extensive testing to evaluate the impact of these changes on performance, particularly for latency-sensitive applications like 5G services. This proactive approach maintains service quality and user experience while transitioning to quantum-safe infrastructures [52, 60].

4) Collaboration with international standards bodies

Central to the GSMA's strategy is fostering collaboration with global standardization entities. Active engagement with NIST, the European Telecommunications Standards Institute (ETSI), and the International Telecommunication Union (ITU) ensures that the telecommunications industry aligns with globally recognized cryptographic standards. This alignment facilitates the seamless implementation of PQC across diverse ecosystems and supports the development of interoperable solutions critical for the global telecom sector's sustainability [15, 52].

5) Advancing cryptographic innovation

The GSMA underscores the importance of advancing cryptographic research and innovation. Telecom operators are encouraged to participate in research initiatives and support open-source projects on quantum-resistant solutions. This involvement accelerates the development of practical PQC algorithms and enhances the industry's capability to address the quantum threat comprehensively. By fostering a culture of innovation, the GSMA aims to equip telecom stakeholders with the tools and expertise needed for a secure quantum future [52, 60].

6) Ensuring long-term cryptographic security

The GSMA recommends adopting long-term strategies beyond immediate challenges to sustain security in a quantum-enabled world. This includes implementing quantum-safe Public Key Infrastructure (PKI) and upgrading systems for secure key management. The guidelines also emphasize the critical need for telecom operators to develop in-house expertise in quantum-safe cryptography, ensuring their teams can navigate the complexities of this transformative period with confidence and agility [15, 52].

The GSMA's proactive measures, as outlined in its 2024 PQC guidelines, serve as a pivotal framework for the telecommunications sector's journey toward quantum safety. Through a combination of hybrid cryptographic schemes, active collaboration with standards bodies, and a commitment to innovation, the GSMA equips network operators to safeguard their infrastructures against emerging quantum threats. By integrating these measures into their operations, telecom stakeholders can ensure that their networks remain resilient, secure, and capable of delivering uninterrupted services in the quantum era [52, 60].

C. NGMN's vision for quantum-safe networks

The Next Generation Mobile Networks (NGMN) Alliance, recognized as a strategic thought leader in the global evolution of mobile networks, has prioritized quantum-safe cryptography as a cornerstone of its roadmap for developing 6G technologies. Through its publication, “6G Requirements and Design Considerations,” NGMN has underscored the necessity for advanced, future-resilient security measures to counter the imminent challenges posed by quantum computing. These measures are designed to ensure that next-generation communication infrastructures remain secure and adaptable as quantum threats emerge, emphasizing integrating quantum-safe cryptography and Quantum Key Distribution (QKD) as essential components of long-term security frameworks for 6G networks [62, 64].

1) Vision for quantum-resilient networks in 6g

NGMN's vision for 6G extends beyond individual user security, encompassing safeguarding industrial applications and critical infrastructure. The Alliance emphasizes that sectors like healthcare, finance, and manufacturing, which rely heavily on digital transformation, will necessitate robust quantum-safe mechanisms to protect sensitive data and ensure operational integrity. As these industries adopt 5G and transition toward 6G, the importance of quantum-resilient networks becomes increasingly pronounced [63, 64].

2) Seamless transition and architectural integration

Central to NGMN's approach is the seamless integration of quantum-resistant algorithms into existing network protocols. The Alliance has called for developing adaptable security architectures supporting hybrid cryptographic models that combine traditional and quantum-resistant algorithms. This approach enhances the resilience of transitional security systems and ensures interoperability and scalability across various network deployments. Additionally, NGMN advocates for early-stage planning to address the potential latency and computational overheads associated with post-quantum cryptography. This strategy involves extensive testing and validation to maintain high-performance levels, particularly for latency-sensitive applications such as autonomous systems and real-time industrial operations [63, 64].

3) Collaborative ecosystem for standardization

Recognizing the importance of global standards, NGMN promotes collaboration among network operators, equipment manufacturers, and regulatory authorities to establish a unified approach to quantum-safe cryptographic standards. NGMN seeks to prevent fragmentation within the telecom ecosystem by fostering international cooperation and ensuring consistency and interoperability in security protocols across regions. This effort aligns with ongoing standardization initiatives, including those spearheaded by ETSI and ITU, contributing to the global adoption of quantum-safe practices [63, 64].

4) Future directions in trust and security

Beyond immediate measures, NGMN's focus includes fostering innovation in cryptographic technologies to address evolving quantum threats. This involves leveraging advances in secure key management and developing resilient Public Key Infrastructure (PKI) systems optimized for post-quantum environments. Furthermore, the Alliance emphasizes the need for continuous industry engagement to refine and adapt these frameworks, ensuring that 6G networks can dynamically respond to emerging challenges while maintaining robust trust mechanisms [23, 64].

NGMN's commitment to quantum-safe cryptography is pivotal in shaping the security paradigms of 6G networks. By integrating advanced cryptographic solutions, fostering international collaboration, and emphasizing future-proof security measures, the Alliance is laying the groundwork for a resilient and secure telecommunications infrastructure. These efforts address the quantum computing challenge and contribute to the broader objectives of creating a trustworthy, inclusive, and sustainable digital ecosystem for the future [23, 64].

D. 3GPP's evolution in standardizing quantum-safe networks

The evolution of quantum computing has introduced significant challenges for the telecommunications industry, particularly in maintaining the robustness of cryptographic mechanisms that underpin network security. Within the 3rd Generation Partnership Project (3GPP), there has been a growing recognition of the necessity to prepare for the potential vulnerabilities introduced by quantum computers. These vulnerabilities arise from quantum computing's ability to undermine the mathematical foundations of many widely used encryption techniques. As a result, 3GPP has intensified its focus on creating quantum-safe networks, ensuring that the communications infrastructure remains resilient in the face of these emerging threats. This focus is reflected in several pivotal technical reports and documents highlighting 3GPP's ongoing efforts to transition the telecommunications ecosystem toward quantum-resistant security models [60, 62].

A cornerstone of 3GPP's strategy is migrating from 128-bit to 256-bit cryptographic keys for encryption and integrity protection. This shift is driven by the vulnerabilities of quantum algorithms such as Grover's and Shor's. Grover's algorithm, which provides a quadratic speedup in brute-force attacks on symmetric cryptography, effectively reduces the security strength of a 128-bit key to the equivalent of a 64-bit key, making it significantly easier for attackers to breach. Consequently, transitioning to 256-bit keys mitigates this risk by ensuring that the effective

security strength remains robust against such quantum-enhanced attacks. Meanwhile, Shor's algorithm represents a more profound threat to public-key cryptography, rendering commonly used algorithms like RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) ineffective. To address this, 3GPP is exploring post-quantum cryptographic (PQC) algorithms that are not susceptible to Shor's algorithm [61, 62].

The transition to quantum-safe cryptographic standards also involves addressing several practical challenges. One of these challenges is ensuring backward compatibility. This is critical because a complete overhaul of network infrastructure to support 256-bit cryptography exclusively is impractical in the short term. 3GPP is developing mechanisms to coexist with 128-bit and 256-bit cryptographic systems to address this. This approach allows legacy systems to operate alongside upgraded systems, ensuring a gradual and seamless transition without disrupting existing network operations or compromising security [61, 62].

Another critical area of focus within 3GPP's quantum-safe strategy is the enhancement of key management and algorithm negotiation protocols. The increasing complexity of cryptographic operations in a post-quantum era requires robust frameworks to manage the lifecycle of cryptographic keys. 3GPP working groups are actively studying how to adapt current protocols, such as Authentication and Key Agreement (AKA), to accommodate quantum-resistant cryptography. This involves ensuring that AKA and related mechanisms can support new algorithms while maintaining interoperability across diverse network components [60, 61], reflecting broader trends toward integrating quantum-safe solutions into modern security architectures for future networks [12].

Moreover, 3GPP has closely monitored developments in the broader cryptographic research community, including initiatives led by organizations such as the National Institute of Standards and Technology (NIST). NIST's ongoing efforts to standardize PQC algorithms provide valuable insights for 3GPP. By aligning its cryptographic transition timeline with these developments, 3GPP aims to adopt mature and well-tested PQC solutions in its future network standards, such as those envisioned for 6G. This alignment ensures that 3GPP's quantum-safe measures are built on a foundation of global consensus and technical rigor [60, 61].

In addition to addressing cryptographic vulnerabilities, 3GPP is examining the implications of quantum-safe security for other aspects of network architecture. For example, post-quantum algorithms typically require larger key sizes and more computational resources, impacting network performance and latency. 3GPP is exploring optimized implementation strategies to mitigate these impacts, including hardware acceleration and hybrid cryptographic approaches. These approaches combine traditional and post-quantum algorithms to balance security and efficiency during the transition period [61,62].

In summary, 3GPP's evolution toward quantum-safe networks reflects its proactive approach to addressing the challenges posed by quantum computing. By prioritizing the transition to 256-bit keys, integrating post-quantum algorithms, ensuring backward compatibility, and adapting key management protocols, 3GPP is laying the groundwork for a secure telecommunications future. These efforts are integral to safeguarding the integrity, confidentiality, and availability of communications networks in an era increasingly shaped by quantum advancements. Through continued collaboration with global standards bodies and cryptographic experts, 3GPP remains at the forefront of building a resilient and future-proof communications infrastructure [60, 62].

E. Summary

The collaborative efforts of GSMA, NGMN, and 3GPP reflect a proactive approach to the security challenges posed by quantum computing. These organizations are laying the groundwork for quantum-safe networks by transitioning to 256-bit cryptographic algorithms, developing hybrid cryptographic schemes, and exploring Quantum Key Distribution. As quantum computing continues to evolve, the telecom industry must stay ahead of potential threats by adopting quantum-safe cryptographic measures that ensure the security and resilience of future communication systems, from 5G to 6G and beyond.

Enabling quantum-safe network (QSN) for 6G: migration and performance considerations in 3GPP

As quantum computing technology advances, it poses a significant threat to classical cryptographic algorithms that form the backbone of current communication net-

works. Introducing a Quantum-Safe Network in 6G is essential to protect against these emerging threats. This section addresses the system and operational aspects of enabling a Quantum-Safe Network [12, 65].

A. Migration to quantum-safe network

The transition from a Legacy Security Network to a Quantum-Safe Network presents several issues, including the compatibility between the 3GPP and PQC protocols and the impact on Network Operations.

1) Interworking with Earlier 3GPP Systems: Ensuring compatibility between existing 3GPP systems and new PQC protocols is crucial. This includes developing seamless migration paths that allow for a phased deployment of PQC algorithms without disrupting ongoing services. Strategies must be established for managing interworking scenarios where devices and networks use different cryptographic generations.

2) Impact on Network Operations: PQC will impact various network operations, including key management, authentication processes, and data encryption. These operations will require more computational resources, which could affect network latency and performance. Evaluating and optimizing these processes is necessary to minimize any negative impact on user experience.

B. Performance considerations

Enabling a Quantum-Safe Network for 6G networks introduces significant performance issues:

1) Increased Computational Complexity: PQC algorithms, particularly those for key exchange and digital signatures, are generally more computationally intensive than classical algorithms. This increased complexity can lead to longer processing times, potentially affecting overall network performance, especially in low-latency scenarios.

2) Larger Key Sizes: PQC typically requires larger key sizes to ensure quantum resistance, which can increase the bandwidth needed for secure communications. This may impact network efficiency, particularly in bandwidth-constrained environments. Therefore, strategies to manage and optimize bandwidth usage in PQC scenarios are essential.

3) Energy Consumption: The higher computational demands of PQC algorithms are likely to result in increased energy consumption, particularly for mobile and IoT devices. Designing energy-efficient PQC solutions that do not significantly reduce battery life is crucial.

4) Increased Latency: The initial handshake and authentication processes, critical for establishing secure connections, may take longer due to the increased computational complexity and larger key sizes associated with PQC. This could introduce additional latency, affecting applications that rely on URLLC, a key feature of 5G TSN. The variability in processing times for PQC operations can introduce jitter and affect the determinism of network communications, which is critical for many TSN applications. Ensuring consistent and predictable network performance becomes more challenging with introducing PQC.

C. Security and privacy

Quantum Safe Network aims to protect the network against quantum attacks, but it also introduces new security and privacy considerations:

1) Security of Key Management: The security of key management processes must be maintained, even as PQC is introduced. This includes guaranteeing that the keys used in PQC are generated, distributed, and stored securely, with robust protections against classical and quantum attacks.

2) Privacy Implications: As PQC is implemented, evaluating and addressing any potential impacts on user privacy is essential. This includes guaranteeing that the encryption methods used in PQC do not inadvertently expose sensitive user information or weaken existing privacy protections.In PQC, do not inadvertently expose sensitive user information or weaken existing privacy protections.

D. Integration into existing infrastructure

Enabling a Quantum-Safe Network for 6G infrastructure requires careful planning and execution:

1) Hardware and Software Upgrades: Network infrastructure, including hardware and software components, must be upgraded to enable a Quantum-Safe Network. This includes updating cryptographic modules, guaranteeing compatibility with PQC algorithms, and optimizing network devices to handle the increased computational load.

2) Testing and Validation: Extensive testing and validation are required to ensure that PQC implementations are secure and efficient. This includes testing PQC algorithms under various network conditions, evaluating their impact on performance, and guaranteeing that they meet the required security standards.

E. Summary

Enabling a Quantum-Safe Network is a critical step in future-proofing our communication systems against quantum threats. By addressing the system and operational aspects outlined in this section, we can ensure that 6G networks remain secure, resilient, and capable of meeting the demands of a quantum-safe future.

Results and Discussion

As quantum computing advances, it poses significant threats to classical cryptographic systems, especially in the context of critical 6G applications. The rising threat of quantum computing to cryptographic systems like RSA and ECC necessitates the integration of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) into 6G networks. These innovations are crucial for protecting user identities, authentication mechanisms, and encrypted communications in the face of quantum-enabled threats [1, 2].

A. Use case: PQC for 6G networks

The rising threat of quantum computing to cryptographic systems like RSA and ECC necessitates the integration of PQC into 6G networks. This use case addresses the protection of user identities, authentication mechanisms, and encrypted communications in the face of quantum-enabled threats. [65]

Pre-condition: A 6G user, Sarah Connor, subscribes to a service provided by SkyNet Telecom. Her subscription concealed identifier (SUCI) is generated using the Elliptic Curve Integrated Encryption Scheme (ECIES) with the Home Network public key [66]. However, quantum computers can break the Diffie-Hellman key exchange, leaving Sarah's SUCI vulnerable to decryption by quantum algorithms such as Shor's [67]. Figure 3 provides an overview of cryptographic applications in 5G systems and their transformation with quantum-safe mechanisms.

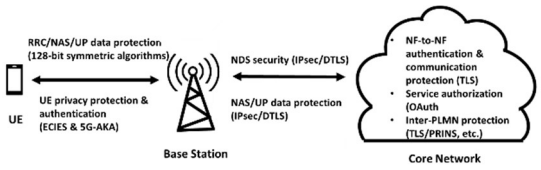

Figure 3: Application scenario of cryptographic algorithms for 5G system [70].

Attack Scenario: Using quantum computers, a hacker group intercepts and decrypts Sarah's SUCI through a technique called "SUCI Catcher [69]." They then track her location in real-time, compromising her privacy and security. Figure 4 highlights an example of quantum attacks targeting User Equipment (UE) and network infrastructure.

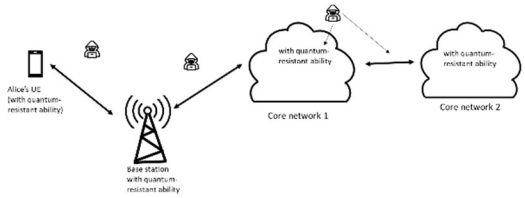

Figure 4: An example of quantum attacks to the UE and the mobile network [70].

Mitigation Strategy Using PQC: Upon detecting the risk of quantum attacks, the operator integrates PQC algorithms such as lattice-based cryptography (e.g., CRYSTALS-Kyber and CRYSTALS-Dilithium) [7, 25]. These algorithms resist quantum attacks, ensuring secure key exchanges and user identity protection.

Performance Considerations: While PQC algorithms introduce larger key sizes and additional latency, 6G networks optimize these processes using hybrid cryptographic models combining AES-256 for data encryption and PQC for key exchanges [5].

Post-condition: The network now supports Post-Quantum Cryptography, safeguarding sensitive data, user identities, and session keys from quantum-enabled threats. This ensures robust security without major disruptions to service continuity.

B. Use case: QKD for industrial 6G networks

QKD is implemented to secure time-sensitive industrial applications in 6G networks. This use case explores the protection of critical operations in a smart factory, where real-time control is vital for maintaining operational efficiency and safety [65].

Pre-condition: John Connor's additive manufacturing facility relies on 5G TSN for controlling 3D printing processes. The manufacturing of life-critical parts (e.g., medical devices and aerospace components) requires ultra-low latency and high reliability. Classical encryption methods such as RSA, used in the current TSN system, are vulnerable to quantum attacks.

Attack Scenario: A quantum attacker intercepts and decrypts the network's communications, using quantum computing to insert malicious commands that alter the dimensions or material properties of the parts being produced. This poses catastrophic risks to the quality of the manufactured components.

Mitigation Strategy Using QKD: (1) Quantum-Safe Communications: The factory implements a SatQKD system. QKD ensures secure key exchanges between ground stations and the satellite, detecting interception attempts. (2)

Secure Manufacturing Process: The quantum keys generated via QKD are integrated into the factory's 6G TSN system, securing all communication channels and preventing malicious data insertion.

Performance Considerations: (1) Latency and Jitter: Although QKD introduces minor latency due to its high computational demands, it offers superior security with real-time key distribution, making it suitable for industrial applications requiring security and low latency [68]. (2) Operational Resilience: The smart factory continues to operate efficiently, with quantum-safe measures guaranteeing that life-critical parts are manufactured without risk of tampering.

Post-condition: The facility successfully mitigates the quantum attack, securing its 6G TSN system with QKD. This demonstrates the importance of QKD in protecting real-time industrial processes in 6G networks from quantum threats.

C. Summary

These 6G use cases for the 3rd Generation Partnership Project highlight the integration of quantum-safe technologies like PQC and QKD in protecting personal and industrial data from quantum-enabled threats. The need for robust quantum-resistant solutions becomes critical as 6G networks expand to include URLLC, mMTC, and eMBB applications. These use cases emphasize performance trade-offs, security enhancements, and the necessity for hybrid cryptographic models to achieve quantum-safe 6G networks.

Conclusions

As quantum computing advances, safeguarding 6G networks requires a multi-faceted strategy incorporating PQC, QKD, and SatQKD. These technologies provide essential layers of security to counter the increasing threat posed by quantum computers to traditional cryptographic systems. PQC offers quantum-resistant encryption, while hybrid cryptographic approaches combine PQC with symmetric encryption, such as AES-256, to create immediate and long-term security solutions. QKD secures key distribution with quantum-level protection, and SatQKD extends this security to global communications via satellite systems.

The transition to these quantum-safe technologies faces several issues. Standardization is critical for the global adoption of PQC and QKD, and efforts such as the NIST PQC standardization initiative aim to establish global cryptographic standards. Scalability and integration into existing systems are also necessary to ensure that quantum-safe communication networks are practical and efficient on a large scale. Quantum repeaters and satellite infrastructure developments will play a vital role in overcoming these issues and guaranteeing that quantum-safe solutions are globally available.

A secure, quantum-resistant internet will require international cooperation across industries and borders. By integrating PQC, QKD, and SatQKD into the core infrastructure of 6G networks, industries can protect against quantum computing threats, guaranteeing the long-term security and confidentiality of global communications.

List of abbreviations

AES Advanced Encryption Standard
AR Augmented Reality
ECC Elliptic Curve Cryptography
eMBB Enhanced Mobile Broadband
EHRs Electronic Health Records
GNSS Global Navigation Satellite Systems
GSMA Global System for Mobile Communications Association
HIPAA Health Insurance Portability and Accountability Act
IoMT Internet of Medical Things
IoT Internet of Things
mMTC Massive Machine-Type Communications
NGMN Next Generation Mobile Networks
NIST National Institute of Standards and Technology
PKI Public Key Infrastructure
PQC Post-Quantum Cryptography
QKD Quantum Key Distribution
RSA Rivest-Shamir-Adleman
SatQKD: Satellite Quantum Key Distribution
SUCI Subscription Concealed Identifier
TSN Time-Sensitive Networking
URLLC Ultra-Reliable Low-Latency Communications
VR Virtual Reality

Author Contributions

Conceptualization and supervision, Yi-Hsueh Tsai and Chen, Shiang-Jiun;
methodology, Chen, Shiang-Jiun;
validation, Yi-Hsueh Tsai.;
formal analysis, Chen, Shiang-Jiun.;
investigation Yi-Hsueh Tsai and Chen, Shiang-Jiun.;
resources, Yi-Hsueh Tsai and Chen, Shiang-Jiun;
data curation, Yi-Hsueh Tsai and Chen, Shiang-Jiun;
writing—original draft preparation, Yi-Hsueh Tsai and Chen, Shiang-Jiun; writing—review and editing, Yi-Hsueh Tsai and Chen, Shiang-Jiun; project administration, Yi-Hsueh Tsai and Chen, Shiang-Jiun; funding acquisition, Yi-Hsueh Tsai and Chen, Shiang-Jiun
All authors have read and agreed to the published version of the manuscript.

Availability of Data and Materials

All data supporting the findings are included in the manuscript.

Consent for Publication

Not applicable.

Conflicts of Interest

The authors declare no conflicts of interest.

Funding

No external funding was received for this research.

Acknowledgments

We sincerely thank AT&T, GE Network Technology, and ISSDU for supporting the 3GPP contribution, S1-242126 Proposal for 6G SID: Quantum-Safe Network (QSN). We also want to thank Stephen F. Bush from GE Aerospace and Ian Deakine, the current leader of the Quantum Safe Communications and Information Initiative (QSCII) at the Alliance for Telecommunications Industry Solutions (ATIS), for sharing their extensive experience in Quantum Safe Communications. Their assistance in the 3GPP contribution was instrumental in inspiring and completing this research project.

References

[1] Mahto D, Yadav DK. RSA and ECC: A comparative analysis. Int J Appl Eng Res 2016;12(19):9053–61.

[2] Suo J, Wang L, Yang S, Zheng W, Zhang J. Quantum algorithms for typical hard problems: A perspective of cryptanalysis. Quantum Inf Process 2020;19(178). doi: 10.1007/s11128-020-02673-x.

[3] Shor PW. Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS). Santa Fe, NM, USA: IEEE; 1994. p. 124–34. doi: 10.1109/SFCS.1994.365700.

[4] Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev 1999;41(2):303–32. doi: 10.1137/S0036144598347011.

[5] Grassl M, Langenberg B, Roetteler M, Steinwandt R. Applying Grover's algorithm to AES: Quantum resource estimates. arXiv Preprint 2015; arXiv:1512.04965v1. Available from: https://arxiv.org/abs/1512.04965.

[6] Kumar M, Pattnaik P. Post Quantum Cryptography (PQC) - An overview: (Invited Paper). In: Proceedings of the 2020 IEEE High Performance Extreme Computing Conference (HPEC). Waltham, MA, USA: IEEE; 2020. p. 1–9. doi: 10.1109/HPEC43674.2020.9286147.

[7] Baseri Y, Chouhan V, Hafid A. Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols. Comput Security 2024;142:103883. doi: 10.1016/j.cose.2024.103883.

[8] Zaman F, et al. Quantum Machine Intelligence for 6G URLLC. IEEE Wireless Commun 2023;30(2):22–30. doi: 10.1109/MWC.003.2200382.

[9] Alin-Bogdan Popa, Pantelimon George Popescu, "The Future of QKD Networks", arXiv Preprint 2024. [Online]. Available from: https://arxiv.org/html/2407.00877v1

[10] SandboxAQ. Safeguarding Healthcare: The Urgent Need for Post-Quantum Cryptography and Zero Trust Architectures [Internet]. SandboxAQ; 2023 Oct. Available from: https://www.sandboxaq.com/post/safeguarding-healthcare-the-urgent-need-for-post-quantum-cryptography-and-zero-trust-architectures

[11] Zhuang Y, et al. Quantum computing in intelligent transportation systems: A survey. arXiv Preprint 2024; arXiv:2406.00862. doi: 10.48550/arXiv.2406.00862.

[12] E. Dervisevic, A. Tankovic, E. Fazel, R. Kompella, P. Fazio, M. Voznak, and M. Mehic, "Quantum Key Distribution Networks – Key Management: A Survey," arXiv preprint arXiv:2408.04580v1, Aug. 2024. [Online]. Available: https://arxiv.org/abs/2408.04580

[13] Alomari A, Kumar SAP. Securing IoT systems in a post-quantum environment: Vulnerabilities, attacks, and possible solutions. Internet of Things 2024;25:101132. doi: 10.1016/j.iot.2024.101132.

[14] Bedington R, Arrazola JM, Ling A. Progress in satellite quantum key distribution. npj Quantum Inf. 2017;3(30). doi: 10.1038/s41534-017-0031-5.

[15] Huttner B, Alléaume R, Diamanti E, et al. Long-range QKD without trusted nodes is not possible with current technology. npj Quantum Inf. 2022;8(108). doi: 10.1038/s41534-022-00613-4.

[16] Arslan B, et al. A study on the use of quantum computers, risk assessment and security problems. In: Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS). Antalya, Turkey: IEEE; 2018. p. 1–5. doi: 10.1109/ISDFS.2018.8355318.

[17] García CR, et al. Quantum-resistant transport layer security. Comput Commun 2024;213:345–58. doi: 10.1016/j.comcom.2023.11.010.

[18] National Institute of Standards and Technology (NIST). Post-Quantum Cryptography (PQC) [Internet]. 2024. Available from: https://www.nist.gov/pqcrypto.

[19] National Institute of Standards and Technology (NIST). FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard [Internet]. Aug 2024. Available from: https://www.nist.gov/pqcrypto.
[20] National Institute of Standards and Technology (NIST). FIPS 204 Module-Lattice-Based Digital Signature Standard [Internet]. Aug 2024. Available from: https://www.nist.gov/pqcrypto.
[21] National Institute of Standards and Technology (NIST). FIPS 205 Stateless Hash-Based Digital Signature Standard [Internet]. Aug 2024. Available from: https://www.nist.gov/pqcrypto.
[22] Micciancio D, Regev O. Lattice-based cryptography [Internet]. Jul 2008. Available from: https://eprint.iacr.org/2008/471.pdf.
[23] Khalid S, McCarthy M, O'Neill M, Liu W. Lattice-based cryptography for IoT in a quantum world: Are we ready? In: Proceedings of the 2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI). Otranto, Italy: IEEE; 2019. p. 194–9. doi: 10.1109/IWASI.2019.8791343.
[24] Sabani ME, Savvas IK, Garani G. Learning with errors: A lattice-based keystone of post-quantum cryptography. Signals 2024;5(2):216–43. doi: 10.3390/signals5020012.
[25] Mert AC, et al. KaLi: A crystal for post-quantum security using Kyber and Dilithium. IEEE Trans Circuits Syst I: Reg Papers 2023;70(2):747–58. doi: 10.1109/TCSI.2022.3219555.
[26] P C, Jain K, Krishnan P. Analysis of post-quantum cryptography for Internet of Things. In: Proceedings of the 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE; 2022. p. 1–5. doi: 10.1109/ICICCS53718.2022.9787987.
[27] Bagirovs G, Sipola T, Hautamäki J. Applications of post-quantum cryptography. In: Proceedings of the 23rd European Conference on Cyber Warfare and Security (ECCWS). 2024. doi: 10.34190/eccws.23.1.2247.
[28] Bernstein DJ. The SPHINCS+ signature framework. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). ACM; 2019. p. 2129–46. doi: 10.1145/3319535.3363229.
[29] Shahid F, Khan A. Smart Digital Signatures (SDS): A post-quantum digital signature scheme for distributed ledgers. Future Gener Comput Syst 2020;111:241–53. doi: 10.1016/j.future.2020.04.042.
[30] Singh H. Code-based cryptography: Classic McEliece. arXiv Preprint 2020; arXiv:1907.12754v2. Available from: https://arxiv.org/abs/1907.12754.
[31] Ding J, Schmidt D. Rainbow, a new multivariable polynomial signature scheme. In: Applied Cryptography and Network Security (ACNS 2005), Lecture Notes in Computer Science, vol. 3531. Springer; 2005. p. 204–20. doi: 10.1007/11496137_12.
[32] Ahad A, et al. 6G and intelligent healthcare: Taxonomy, technologies, open issues and future research directions. Internet of Things 2024;25:101068. doi: 10.1016/j.iot.2024.101068.
[33] Nasralla MM, et al. Exploring the role of 6G technology in enhancing quality of experience for m-Health multimedia applications: A comprehensive survey. Sensors 2023;23(13):5882. doi: 10.3390/s23135882.
[34] Nayak S, Patgiri R. 6G communication technology: A vision on intelligent healthcare. arXiv Preprint 2020; arXiv:2005.07532v1. Available from: https://arxiv.org/abs/2005.07532.
[35] Bansal A, Esha A, Mehra PS. A post-quantum consortium blockchain-based secure EHR framework. In: Proceedings of the 2023 International Conference on IoT, Communication and Automation Technology (ICICAT). IEEE; 2023. doi: 10.1109/ICICAT57735.2023.10263717.
[36] Mohinder MSB, Natarajan J, Prabhakar A. Novel secure authentication protocol for e-Health records in cloud with a new key generation method and minimized key exchange. J King Saud Univ Comput Inf Sci 2023. doi: 10.1016/j.jksuci.2023.101629.
[37] Li C, et al. A review of IoT applications in healthcare. Neurocomputing 2024;565:127017. doi: 10.1016/j.neucom.2023.127017.
[38] Nkereuwem E, Ansa G. Enhancing data integrity in telemedicine system using blockchain approach. REJOST 2023.
[39] Circular Economy Network. Review of security and privacy for the Internet of Medical Things (IoMT) resolving the protection concerns for the novel circular economy bioinformatics. Articles Jan 2022.
[40] Camhi J. The IoT security report: Securing new connected devices against cyber attacks. BI Intelligence, Business Insider 2015.
[41] Tank B, Patel H, Upadhyay H. A survey on IoT privacy issues and mitigation techniques. In: Proceedings of ICTCS. Udaipur, India; Mar 2016. p. 1–4.
[42] Joyia GJ, Liaqat RM, Farooq A, Rehman S. Internet of Medical Things (IoMT): Applications, benefits and future challenges in healthcare domain. J Commun 2017;12(4):240–7. doi: 10.12720/jcm.12.4.240-247.
[43] Jeyaraman N, et al. Revolutionizing healthcare: The emerging role of quantum computing in enhancing medical technology and treatment. Cureus 2024;16(8):e67486. doi: 10.7759/cureus.67486.
[44] Basha B. Enhancing healthcare data security using quantum cryptography for efficient and robust encryption. J Electr Syst 2024;20(5s):1993–2000. doi: 10.52783/jes.2535.
[45] Paul S, et al. Towards post-quantum security for cyber-physical systems: Integrating PQC into industrial M2M communication. arXiv Preprint 2021; arXiv:2021.1563v1. Available from: https://arxiv.org/abs/2021.1563.

[46] Oliva del Moral J, et al. Cybersecurity in critical infrastructures: A post-quantum cryptography perspective. arXiv Preprint 2024; arXiv:2401.03780v2. Available from: https://arxiv.org/abs/2401.03780.
[47] Tedeschi P, Sciancalepore S, Di Pietro R. Satellite-based communications security: A survey of threats, solutions, and research challenges. arXiv Preprint 2022; arXiv:2112.11324v4. Available from: https://arxiv.org/abs/2112.11324.
[48] Xu S, et al. A preliminary study of PQC implementations for satellite communication networks. arXiv Preprint 2024; arXiv:2404.05668v1. Available from: https://arxiv.org/abs/2404.05668.
[49] Lai J, Yao F, Wang J, Zhang M, Li F, Zhao W, et al. Application and development of QKD-based quantum secure communication. Entropy 2023;25(4):627. doi: 10.3390/e25040627.
[50] Hoque S, Aydeger A, Zeydan E. Exploring post-quantum cryptography with quantum key distribution for sustainable mobile network architecture design. arXiv Preprint 2024; arXiv:2404.10602v1. Available from: https://arxiv.org/abs/2404.10602.
[51] Sharma H, Kumar R, Gupta M. A review paper on hybrid cryptographic algorithms in cloud network. In: Proceedings of the 2nd International Conference on Innovation in Technology (INOCON). Bangalore, India: IEEE; 2023. p. 1–5. doi: 10.1109/INOCON57975.2023.10101044.
[52] GSM Association. Post quantum cryptography – guidelines for telecom use cases version 1.0 [Internet]. Feb 2024. Available from: https://www.gsma.com/newsroom/wp-content/uploads/PQ.03-Post-Quantum-Cryptography-Guidelines-for-Telecom-Use-v1.0.pdf
[53] Rao SK, Mahto D, Yadav DK, Khan DA. The AES-256 cryptosystem resists quantum attacks. Int J Adv Res Comput Sci 2017;8(3):1–7. Available from: http://www.ijarcs.info.
[54] Aguilera A, Garcia C, Lawo D, Imaña J, Tafur Monroy I, Olmos J. In-line rate encrypted links using pre-shared post-quantum keys and DPUs. Sci Rep 2024;14. doi: 10.1038/s41598-024-71861-x.
[55] Cicconetti C, Sabella D, Noviello P, Paduanelli GD. Quantum-safe edge applications: How to secure computation in distributed computing systems. arXiv Preprint 2024; arXiv:2405.17008v1. Available from: https://arxiv.org/abs/2405.17008.
[56] Liu T, Ramachandran G, Jurdak R. Post-quantum cryptography for Internet of Things: A survey on performance and optimization. arXiv Preprint 2024; arXiv:2401.17538v1. Available from: https://arxiv.org/abs/2401.17538
[57] Paul S, Scheible P, Wiemer F. Towards post-quantum security for cyber-physical systems: Integrating PQC into industrial M2M communication. IACR ePrint Archive 2021. Available from: https://eprint.iacr.org/2021/1563.pdf.
[58] Xu S, Alonso AV, Eisen P, Légaré J. A preliminary study of PQC implementations for satellite communication networks. In: Proceedings of the ESA Conference; 2024. Available from: https://indico.esa.int/event/528/attachments/5988/10187/A_Preliminary_Study_of_PQC_Implementations_for_Satellite_Communication_Networks.pdf.
[59] Orsucci D, et al. Assessment of practical satellite quantum key distribution architectures for current and near-future missions. arXiv Preprint 2024; arXiv:2404.05668v1. Available from: https://arxiv.org/abs/2404.05668.
[60] 3GPP TR 33.700-41. Study on enabling a cryptographic algorithm transition to 256 bits [Internet]. 2024. Available from: https://www.3gpp.org.
[61] 3GPP TR 33.841. Study on the support of 256-bit algorithms for 5G [Internet]. 2024. Available from: https://www.3gpp.org.
[62] Nokia, "3GPP S3-242820, Discussion on 3GPP Cryptographic Inventory"
[63] NGMN, "6G Trustiness Consideration", 2023. [Online]. Available: https://www.ngmn.org
[64] NGMN, "6G Requirements and Design Considerations", 2023. [Online]. Available: https://www.ngmn.org
[65] III, AT&T, GE Network Technologies, and ISSDU, "3GPP S1-242126 Proposal for 6G SID: Quantum-Safe Network (QSN) ", 2024. [Online]. Available: https://www.3gpp.org
[66] III, GE Network Technologies, and ISSDU, "S1-242126, Motivation for 6G SID: Quantum Safe Network (QSN) ", 2024. [Online]. Available: https://www.3gpp.org
[67] J. P. Mattsson and P. K. N. Nori, "Concealing the concealed identifier in 5G," in Proc. 16th Int. Conf. Availability, Reliability, and Security (ARES)*, Vienna, Austria, Aug. 2021. ACM, pp. 1–6, doi: 10.1145/3465481.3470076.
[68] X. Li, L. L. Kwan, X. Zhang, and K. Anshel, "Post-quantum Diffie-Hellman and symmetric key exchange protocols," in Proc. IEEE Inf. Assurance Workshop (IAW)*, West Point, NY, 2006, pp. 382–383, doi: 10.1109/IAW.2006.1652122.
[69] L. Barraud et al., "5G SUCI catcher: Attack and detection," in Proc. IEEE Int. Conf. Cloud Comput. Technol. Sci. (CloudCom), Naples, Italy, 2023, pp. 285–290, doi: 10.1109/CloudCom59040.2023.00053.
[70] 3GPP, "3GPP TR 22.870-011, Study on 6G Use Cases and Service Requirements," Nov. 2024. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/22_series/22.870/
[71] T. Roger et al., "Real-time gigahertz free-space quantum key distribution within an emulated satellite overpass," Sci. Adv., vol. 9, no. 48, Dec. 2023, doi: 10.1126/sciadv.adj5873