Center of Computer Science, Vol. 1, No. 1, April, 2026, Pages 43-51
DOI: https://doi.org/10.65591/CoCS-81-2026

Center of Computer Science

REVIEW ARTICLE

Comparative and Evolutionary Analysis of Encryption and Physical Layer Security in 5G and 6G

Shuruq Khalid Abdulredha[1*]

[1]General Directorate of Education in Babylon, Ministry of Education, Iraq.

*Corresponding author E-mail : alalaakshuruq@gmail.com

Article Info.

Article history:

Received: 14/03/2026

Accepted: 25/03/2026

Published: 01/04/2026

Abstract

The evolution from 5G to 6G wireless networks is driving a fundamental transformation in encryption technologies. While 5G networks primarily rely on advanced classical cryptography, including AES, ECC, and RSA, emerging applications such as IoT, e-healthcare, and ultra-reliable low-latency communications demand lightweight, hybrid, and context-aware security schemes. The advent of quantum computing poses significant threats to classical cryptosystems, motivating the integration of quantum-resistant security techniques, including post-quantum cryptography (PQC), quantum key distribution (QKD), and physical layer security (PLS) in 6G networks. This review synthesizes recent research on classical, hybrid, and quantum-resistant security techniques, highlighting the shift toward multi-layered and adaptive security frameworks. A comparative analysis of PLS in 5G and 6G illustrates its transition from a complementary role to a core security mechanism, especially in ultra-low-latency, massive connectivity, and heterogeneous environments. Finally, open research questions and standardization challenges are discussed, emphasizing the need for scalable, energy-efficient, and interoperable security solutions for next-generation wireless networks.

Keywords: 5G; 6G; Post-Quantum Cryptography (PQC); Quantum Key Distribution (QKD); Physical Layer Security (PLS).

1. Introduction

The evolution from 5G to 6G wireless networks is driving a transformation in encryption techniques, motivated by the need for higher data rates, ultra-low latency, massive device connectivity, and the looming threat of quantum computing. 5G networks primarily rely on advanced classical cryptography—such as AES, ECC, and RSA—augmented by lightweight and hybrid schemes to address the diverse requirements of IoT, e-healthcare, and critical infrastructure [1-4]. As quantum computing threatens to undermine traditional cryptosystems, 6G research is rapidly incorporating post-quantum cryptography (PQC), quantum key distribution (QKD), and physical layer security (PLS) to ensure future-proof confidentiality, integrity, and authentication [5-18]. This review synthesizes the latest research on encryption methods in 5G and 6G, highlighting the shift toward multi-layered, quantum-resistant, and context-aware security frameworks.
In this paper, the term "quantum-resistant" is used as a general concept referring to all techniques capable of resisting quantum attacks, while "post-quantum cryptography (PQC)" specifically denotes cryptographic algorithms designed to be secure against quantum computers.

2. Classical and Hybrid Cryptography in 5G

5G networks employ a combination of symmetric (AES, ZUC, SNOW-V) and asymmetric (ECC, RSA) cryptography for data confidentiality and authentication [19,20]. Lightweight and hybrid schemes, such as dynamic key management and hierarchical broadcast encryption, are used to support high mobility and resource-constrained IoT devices [2][21] Homomorphic encryption and quantum-walk–based cryptographic primitives are also explored for privacy-preserving applications [4,23].

3. Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) in 6G

6G research is rapidly integrating PQC algorithms to counter quantum threats [22,24]. Hybrid cryptosystems combine classical and post-quantum primitives for robust, future-proof security [16,17]. QKD is being piloted for secure key exchange in both fronthaul and core network architectures, offering information-theoretic security [25,26].

4. Physical Layer Security (PLS) and Coding-Crypto Fusion

Physical Layer Security (PLS) leverages the inherent randomness of wireless channels to provide physical layer-level encryption-like security safeguards, including secret key generation, eavesdropping encryption, and authentication based on physically non-reproducible functions (PUFs) [13, 27].

Cryptogram and cryptography fusion techniques, such as combining LDPC or polar codes with post-quantum cryptography (PQC), enhance both error correction and data confidentiality, particularly in ultra-reliable, low-latency (URLLC) communication scenarios [28, 29].

A clear evolution from traditional, centralized security mechanisms in 5G networks toward more flexible, intelligent, and quantum-computing-resistant solutions in 6G networks is observed. Table 1 summarizes this shift, providing a comparative analysis of authentication and encryption mechanisms across 5G and 6G networks.

Table 1: Comparison table of means of authentication and coding [5].

Parameter	5G	6G
Authentication Protocols	5G-AKA, EAP	Context-aware, Post-Quantum, Zero Trust
Channel Coding Techniques	Polar, LDPC, CRC	LDPC, Polar, RS
Trust Architecture	SEAF, HSS (centralized)	Blockchain, AI-driven identity management
Auxiliary Security Mechanisms	USIM, AKA keys	AI biometrics, multi-factor authentication, PUF
Verification Approach	Rule-based / signature-based	Context-aware, AI-driven behavioral analysis

The following visual highlights the evolution from classical cryptography and centralized trust in 5G toward quantum-resistant, AI-driven, and context-aware security in 6G.

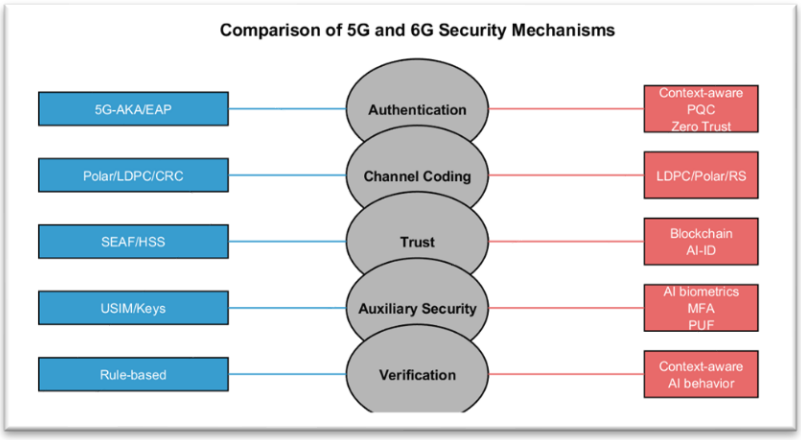

Fig.1 : illustrates a simplified comparison of the main security mechanisms in 5G and 6G networks.

5. Advanced and Application-Specific Encryption

Emerging techniques include searchable encryption for privacy-preserving data access in smart cities [31] hybrid quantum-crypto standards for Industry 5.0 [16], and triple-layered security systems for multimedia and IoT applications [4,32]. Fully homomorphic encryption is also being explored for secure computation in 6G network slicing [18].

6. Evidence-Based Analysis of Security Claims in 5G and 6G Networks

In light of recent advancements in 5G and 6G networks, a clear understanding of the key scientific claims surrounding encryption technologies and their effectiveness against both conventional and quantum threats have become increasingly important. The following table aims to provide a systematic summary of the main claims and supporting evidence as presented in recent studies, highlighting the strength of each piece of evidence and its associated scientific interpretation. This approach helps to shed light on the research gaps and practical challenges facing encryption applications in next-generation network environments.

Table 2: Evidence-Based Analysis of Security Claims in 5G and 6G Networks

Papers	Reasoning	Evidence Strength	Claim
[5] [6] [9] [11][14] [16] [17][22][24]	Quantum computing threatens classical cryptography; PQC and QKD offer future-proof security.	Strong	6G networks require quantum-resistant security solutions, including post-quantum cryptography (PQC) and quantum key distribution (QKD)
[13][27][28][29][30][33][34] [35][39]	PLS provides encryption-like protection with minimal latency, crucial for URLLC and mMTC.	Strong	Physical layer security is essential for ultra-low-latency6G use cases
[2][5][16][17][18][24][32]	Combining classical, PQC, and coding techniques addresses diverse threats and performance needs.	Moderate	Hybrid cryptographic models improve resilience and scalability
[5] [6] [9] [11][14][17][22][24] [36]	ECC and RSA can be broken by quantum computers; migration to PQC is necessary.	Moderate	5G encryption is vulnerable to quantum attacks
[8][10][13][15][16][26][33] [37]	Implementation, performance, and compatibility issues hinder widespread adoption.	Moderate	Standardization and integration of PQC/QKD face practical challenges
[19][20][38]	Differential fault and side-channel attacks can compromise certain ciphers if not properly mitigated.	Moderate	Some 5G/6G encryption schemes remain susceptible to side-channel/fault attacks

7. Research Gaps in 5G and 6G Cryptography

Despite advances, gaps remain in the standardization, real-world deployment, and performance evaluation of PQC, QKD, and PLS in large-scale, heterogeneous 6G environments. There is also a need for more research on lightweight, energy-efficient encryption for IoT and edge devices, as well as on the integration of AI-driven security mechanisms.

8.Comparative analysis of physical layer security techniques in 5G and 6Gwireless communications networks

Physical layer security in 5G vs 6G: similar foundations, different emphases and technologies Physical-layer security (PLS) in 5G and 6G share core principles but target different use-cases, channel conditions and design constraints.

8.1 Conceptual role in 5G vs 6G

- 5G: PLS is mainly a complement to upper-layer cryptography, used to enhance secrecy, support key generation and cope with decentralized, heterogeneous, high-throughput networks [40-42].
- 6G/B5G: PLS is positioned as a first line of defense and sometimes a substitute for heavy cryptography especially for ultra-low-latency, massive IoT, non-terrestrial and near-field THz scenarios [43-47].

Physical Layer Security (PLS) technologies have undergone a structural transformation with the evolution of wireless networks from 5G to 6G, moving from a complementary role supporting traditional encryption mechanisms to a core component of multi-layered security architectures. In 5G environments, PLS solutions primarily focused on enhancing confidentiality and improving resistance to eavesdropping and jamming in heterogeneous, high-throughput communication scenarios. In 6G networks, PLS adoption has expanded to encompass more complex scenarios, such as Ultra Reliable Low Latency Communications (URLLC), the Internet of Things (IoT), non-terrestrial communications, and near-terminal terahertz (NTR) bands. This shift is driven by stringent latency and power constraints, which render exclusive reliance on traditional encryption impractical in some applications. Accordingly, the following table illustrates the functional and technical evolution of core PLS technology families, comparing their application focus in 5G versus 6G networks and highlighting relevant recent research trends.

Table 3: Evolution of Physical Layer Security Techniques Across 5G and 6G Networks.

Citations	6G/B5G focus	5G focus	Technique family
[14][27][40][41] [48]	Integration with new spectra(mmWave/THz), ultra-short packets (URLLC)	Wiretap codes, secrecy capacity in MIMO/mmWave/HetNet/NOMA	Secrecy coding (LDPC, polar, lattice)
[14][35][40][41] [42] [46[49]	Joint with RIS/IRS, near-field THz wavefront design, UAV/NTN	Secure beamforming, AN to degrade eavesdropper; HetNets, mmWave	Massive MIMO beam forming &artificial noise
[13][40] [41] [42][45]	Central for massive IoT, ultra-dense 6G access; PHY-key + crypto integration	Lightweight key agreement for decentralized 5G, IoT	Key generation from channel randomness
[13][42][45][50]	Multi-factor auth (channel, PUF, localization) for cyber-physical systems	Initial work on channel-based auth, malicious node detection	PHY-assisted authentication /PUFs
[13][27] [47][51]	RL-driven cross-layer PLS against intelligent jamming and spoofing attacks in high-density 6G environments	Basic modelling of jamming/eavesdropping	Anti-jamming, covert comms

8.2 Physical layer security in 5G networks: features and prevailing trends

Surveys for 5G highlight PLS around key 5G enablers:

- Massive MIMO, mmWave, HetNets, NOMA, full-duplex: used to create spatial/selective advantages for legitimate users via secure beamforming, interference exploitation, and secrecy-oriented resource allocation [14,40-42].
- Information-theoretic metrics: secrecy capacity, secrecy outage probability, and equivocation rate dominate performance assessment [40-42].
- Lightweight enhancements: low-complexity secure beamforming, mobile/cooperative secure schemes, PHY-assisted authentication and key generation in massive MIMO mmWave systems [42,48].

PLS is mainly tuned to 5G traffic patterns (eMBB, URLLC, mMTC) and finite-block length issues start to emerge for URLLC [27].

8.3 The shift in physical layer security towards 6G networks

6G work broadens and deepens PLS along several axes:

- Ultra-secure low-latency (USLLC): key-based PLS protocols mapped to 5G/6G OFDM waveforms achievesub-1 ms two-way private exchange by obscuring data with rotated reference signals, tightly co-designing synchronization and secrecy [29].
- New propagation regimes:
  1) Near-field THz PLS using wavefront hopping between Airy/Bessel beams to reduce eavesdropping probability with minimal performance loss [46].
  2) Non-terrestrial networks (NTN)/UAVs: PLS adapted to 3D heterogeneous topologies and infrastructure-free security needs [44].
- RIS/IRS-assisted PLS: Intelligent surfaces reconfigure channels to maximize secrecy rate or minimize eavesdropper SNR; extended to RF and optical systems, often combined with ML for complexity control [35,39,49].
- Post-quantum and lattice-based PHY encryption: full PHY-layer lattice-based scheme for 6G OFDM/QAMwhere security reduces to the closest-vector problem, giving information-theoretic-style protection against eavesdropping [14].
- Cross-layer, AI-driven PLS: reinforcement learning used to adapt beamforming, power, and jamming strategies against unknown or smart attackers in dense 6G networks [51]. RL addresses smart jammers by framing anti-jamming as an online sequential decision/game problem and learning adaptive, sometimes deceptive, strategies over channels, power, rate, mobility, and cooperative resources, without requiring an explicit model of the intelligent jammer [52].

8. 4 Comparative Insights on Physical Layer Security in 5G and 6G

- Scope: 5G PLS is largely an add-on to standard security; 6G PLS is architected as integral to meeting latency, massive connectivity, and heterogeneous requirements [13,27,45].
- Technologies: 5G PLS leans on massive MIMO/mmWave/NOMA; 6G adds THz, RIS, NTN/UAVs, semantic andnear-field communications [43,44,46].

- Design philosophy: 5G emphasizes secrecy capacity under classical models; 6G emphasizes joint goals: secrecy + latency + energy + scalability, often via cross-layer and learning-based designs [29,47,51].

Overall, physical layer security (PLS) in both 5G and 6G networks is based on the same theoretical foundations, but the focus differs between the two generations. In 5G networks, the emphasis is on adapting existing PLS tools and technologies to modern radio technologies, while in 6G networks, security is radically rethought starting from the physical layer itself, where PLS is directly integrated into carrier design, network architecture, and AI-driven network strategies.

9. Comparative Analysis of Authentication and Encryption Mechanisms in 5G and 6G Networks

The transition from 5G to 6G networks is bringing about significant advancements in security mechanisms, particularly in authentication and encryption technologies. While 5G networks rely primarily on traditional encryption methods and centralized trust structures, 6G networks are expected to incorporate more flexible, intelligent, and quantum-computing solutions. These solutions include the integration of post-quantum cryptography (PQC), contextual authentication, and decentralized trust models such as blockchain technology [5].

To highlight these differences, Table 4 presents a comparative analysis of the main authentication and encryption mechanisms in 5G and 6G networks, focusing on core technologies, encryption strategies, and security capabilities.

Table 4: The Key Differences Between 5G And 6G Security Mechanisms [5].

Security Aspect	5G	6G
Authentication model	Multilevel: SIM/SUPI; EAP; 5G-AKA; SEAF as trust anchor	Context-aware authentication; Zero Trust; PQC integration (e.g., CRYSTALS-Kyber, Dilithium); blockchain-based identity
Basic protocols	5G-AKA; EAP	PQC-enhanced authentication protocols; hybrid classical–PQC schemes
Integrity checking mechanisms	Frame-level CRC	CRC; cryptographic MACs; PQC-based digital signatures
Coding techniques for authentication	LDPC (physical layer); Polar codes for control channel (URLLC)	Cross-layer integration of LDPC and RS codes for error control and source validation; PUF-based authentication; PQC-enabled coding
Role of coding	Indirect authentication via successful decoding	Combined role: data protection; source verification; quantum-attack resistance

The following infographic presents a layered comparison of security aspects, including authentication models, basic protocols, integrity checking mechanisms, coding techniques, and the role of coding. Features of 5G are displayed on the left in blue, while 6G enhancements—including post-quantum cryptography (PQC), blockchain-based identity, and zero-trust authentication—are shown on the right in green. Arrows highlight the evolution and integration of new security methods from 5G to 6G, providing a clear visual overview of the transition and technological improvements.

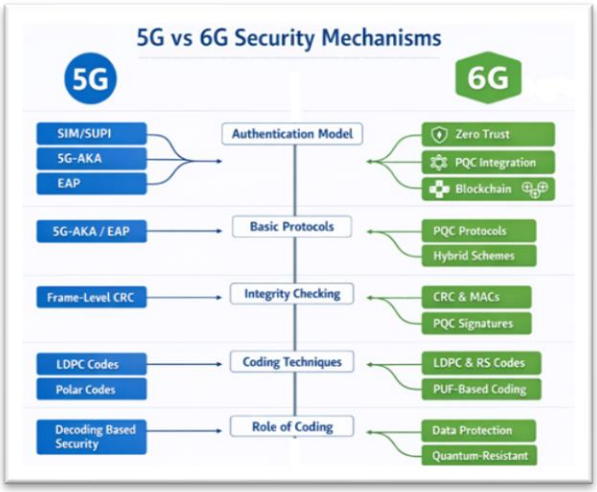

Fig. 2: illustrates the key differences between 5G and 6G security mechanisms.

10. Open Challenges and Research Questions

Given the existing challenges and research gaps in 5G and 6G network encryption, future research should focus on developing scalable, interoperable, and energy-efficient encryption frameworks that can adapt to the dynamic nature of next-generation networks. In addition to

these research gaps, practical implementation challenges must also be considered, particularly in resource-constrained environments such as IoT devices.

Therefore, it is essential to identify the key open research questions that will guide future developments. The following highlights critical issues that require innovative encryption solutions, including quantum-resistant mechanisms, enhanced physical layer security, and lightweight endpoint protection techniques.

- How can PQC and QKD be efficiently integrated into large-scale 6G networks?
  Rationale: The integration must balance security, latency, and scalability across diverse applications and devices.

- What are the most effective physical layer security (PLS) techniques for URLLC and mMTC in 6G?
  Rationale: Ultra-low latency and massive connectivity demand novel and efficient PLS approaches beyond current models.

- How can lightweight quantum-resistant security techniques (e.g., PQC-based algorithms) be optimized for IoT and edge devices?
  Rationale: Resource-constrained environments require efficient and secure solutions suitable for large-scale deployment.

In conclusion, the future of 5G and 6G encryption lies in the convergence of quantum-resistant techniques (including PQC and QKD), physical layer security, and adaptive multi-layered frameworks to address the evolving requirements of next-generation wireless networks.

11. Discussion

The transition from 5G to 6G marks a paradigm shift in encryption, driven by the need to address both classical and quantum threats. While 5Grelies on robust classical cryptography, it is increasingly incorporating lightweight, hybrid, and context-aware schemes to support diverse applications and resource constraints [1-3.19]. The imminent threat of quantum computing has accelerated the adoption of PQC and QKD in 6G [5,6,9,11], with lattice-based and isogeny-based algorithms emerging as leading candidates [14,16,17,22,24]. Physical layer security and coding-crypto fusion offer additional layers of protection, particularly for ultra-low-latency and high-mobility scenarios [28-30,33-35].

Despite significant progress, challenges remain in standardizing PQC, integrating QKD with existing infrastructure, and balancing security with performance and scalability. The research highlights the importance of multi-layered, adaptive security frameworks that combine cryptography, coding, and physical layer techniques to meet the stringent requirements of next-generation networks [8,10,13,15,37].

12. Conclusion

The landscape of encryption in 5G and 6G networks is rapidly evolving, with a clear shift toward quantum-resistant, multi-layered, and context-aware security frameworks. While 5G relies on hardened classical cryptography (AES, ECC/RSA, TLS/IPsec) with early integration of quantum-aware schemes, 6G moves toward quantum-safe cryptography (PQC), quantum-key distribution (QKD), and physical-layer security. These mechanisms are often combined with advanced coding and context-aware authentication to maintain confidentiality, low latency, and robustness in massive, heterogeneous networks.

Both 5G and especially 6G will also face heightened malware “metavirus” risks due to the proliferation of devices, virtualized components, and AI-driven applications. At the same time, security will be strengthened through physical-layer techniques, quantum-safe cryptography, and intelligent, slice-aware, zero-trust architectures. The ultimate security of future networked ecosystems, including metaverse applications, will depend less on raw radio technology and more on how these emerging encryption and security capabilities are integrated end-to-end.

In practice, implementing 5G/6G security means combining zero-trust, strong identity and quantum-resilient cryptography with physical-layer protections, slice/edge isolation, and AI-driven, real-time defense, all guided by standards and rigorous risk assessment across specific 5G/6G use cases.

References

[1] J. Yang and T. Johansson, “An overview of cryptographic primitives for possible use in 5G and beyond,” *Science China Information Sciences*, vol. 63, 2020, doi: 10.1007/s11432-019-2907-4.

[2] A. Kumar, P. Singh, D. Kamble, and I. Singh, “Hybrid cryptographic approach for strengthening IoT and 5G/B5G network security,” *Scientific Reports*, vol. 15, 2025, doi: 10.1038/s41598-025-21861-2.

[3] K. Chand, R. Arokia, S. Kumar, J. V. Bojjawar, P. Veeraiyah, and T. Jayanthi, “5G Wireless Network Security: Investigating Next-Generation Mobile Communication Data Encryption Methods and Authentication Protocols,” in *2025 3rd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT)*, pp. 253–258, 2025, doi: 10.1109/dicct64131.2025.10986591.

[4] J. Jain, A. Jain, S. Srivastava, C. Verma, M. Răboacă, and Z. Illés, “Improved Security of E-Healthcare Images Using Hybridized Robust Zero-Watermarking and Hyper-Chaotic System along with RSA,” *Mathematics*, vol. 10, no. 7, 2022, doi: 10.3390/math10071071.

[5] S. Dunaiev, “An integrated approach to data confidentiality in 5G/6G based on LDPC codes and post-quantum cryptography,” *Terra Security*, 2025, doi: 10.20998/3083-6298.2025.02.03.

[6] R. Zhou, H. Guo, F. Teo, and S. Bakiras, “A Survey on Post-Quantum Cryptography for 5G/6G Communications,” in *2023 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, pp. 1–6, 2023, doi: 10.1109/soli60636.2023.10425346.

[7] C. Mangla, S. Rani, N. Qureshi, and A. Singh, “Mitigating 5G security challenges for next-gen industry using quantum computing,” *Journal of King Saud University - Computer and Information Sciences*, 2022, doi: 10.1016/j.jksuci.2022.07.009.

[8] M. Zheng and Y. Xuan, “Quantum-Encrypted 6G Fronthaul Network: Enhancing Security and Efficiency in Next-Generation Wireless Communication,” *Applied and Computational Engineering*, 2025, doi: 10.54254/2755-2721/2025.21689.

[9] S. Sanon, I. Alzalam, and H. Schotten, “Quantum and Post-Quantum Security in Future Networks,” in *2023 IEEE Future Networks World Forum (FNWF)*, pp. 1–6, 2023, doi: 10.1109/fnwf58287.2023.10520624.

[10] E. Zeydan, C. Alwis, R. Khan, Y. Turk, A. Aydeger, T. Gadekallu, and M. Liyanage, “Quantum Technologies for Beyond 5G and 6G Networks: Applications, Opportunities, and Challenges,” *IEEE Open Journal of the Communications Society*, vol. 6, pp. 6383–6420, 2025, doi: 10.1109/ojcoms.2025.3591842.

[11] S. Sanon and H. Schotten, “Securing Mobile Networks in the Quantum Era: Imperative Role of Post-Quantum Cryptography,” in *2025 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, pp. 721–726, 2025, doi: 10.1109/eucnc/6gsummit63408.2025.11037057.

[12] M. Mehic, L. Michalek, E. Dervisevic, P. Burdiak, M. Plakalovic, J. Rozhon, N. Mahovac, F. Richter, E. Kaljic, F. Lauterbach, P. Njemcevic, A. Maric, M. Hamza, P. Fazio, and M. Voznák, “Quantum Cryptography in 5G Networks: A Comprehensive Overview,” *IEEE Communications Surveys & Tutorials*, vol. 26, pp. 302–346, 2024, doi: 10.1109/comst.2023.3309051.

[13] M. Mitev, A. Chorti, H. Poor, and G. Fettweis, “What Physical Layer Security Can Do for 6G Security,” *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 375–388, 2022, doi: 10.1109/ojvt.2023.3245071.

[14] W. Abdallah, “A physical layer security scheme for 6G wireless networks using post-quantum cryptography,” *Comput. Commun.*, vol. 218, pp. 176–187, 2024, doi: 10.1016/j.comcom.2024.02.019.

[15] I. Djordjevic, “Physical-Layer Security, Quantum Key Distribution, and Post-Quantum Cryptography,” *Entropy*, vol. 24, 2022, doi: 10.3390/e24070935.

[16] K. Singamaneni, A. Budati, S. Islam, R. Kolandaisamy, and G. Muhammad, "A Novel Hybrid Quantum-Crypto Standard to Enhance Security and Resilience in 6G-Enabled IoT Networks," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 18, pp. 7876–7891, 2025, doi: 10.1109/jstars.2025.3540905.

[17] V. Ulitzsch, S. Park, S. Marzougui, and J. Seifert, "A Post-Quantum Secure Subscription Concealed Identifier for 6G," in *Proc. 15th ACM Conf. on Security and Privacy in Wireless and Mobile Networks*, 2022, doi: 10.1145/3507657.3528540.

[18] S. Sanon, I. Ademi, M. Zentara, and H. Schotten, "Applicability of Fully Homomorphic Encryption in Mobile Communication," in *2024 3rd International Conference on 6G Networking (6GNet)*, 2024, pp. 234–240, doi: 10.1109/6gnet63182.2024.10765741.

[19] R. Barker and F. Afghah, "Securing Open RAN: A Survey of Cryptographic Challenges and Emerging Solutions for 5G," *arXiv*, vol. abs/2506.09418, 2025, doi: 10.48550/arxiv.2506.09418.

[20] V. Katyal, V. Bajaj, A. Parihar, and I. Singh, "AI-Driven Security Evaluation of the ZUC Stream Cipher in 5G Networks," *IEEE Access*, vol. 13, pp. 166680–166694, 2025, doi: 10.1109/access.2025.3612453.

[21] R. Pothumarti, K. Jain, and P. Krishnan, "A lightweight authentication scheme for 5G mobile communications: a dynamic key approach," *Journal of Ambient Intelligence and Humanized Computing*, 2021, doi: 10.1007/s12652-020-02857-4.

[22] A. Atutxa, A. Sanz, E. Salegi, M. Huarte, J. Astorga, and E. Jacob, "Authentication of the QKD classical channel through Post-Quantum Cryptography in a multi-site 5G/6G quantum-safe communication network," in *2025 International Conference on Quantum Communications, Networking, and Computing (QCNC)*, 2025, pp. 648–654, doi: 10.1109/qcnc64685.2025.00108.

[23] A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. Venegas-Andraca, "Secure Data Encryption Based on Quantum Walks for 5G Internet of Things Scenario," *IEEE Transactions on Network and Service Management*, vol. 17, pp. 118–131, 2020, doi: 10.1109/tnsm.2020.2969863.

[24] Q. Khan, S. Purification, and S. Chang, "Post-Quantum Key Exchange and Subscriber Identity Encryption in 5G Using ML-KEM (Kyber)," *Information*, 2025, doi: 10.3390/info16070617.

[25] P. Dhakal, B. Dawadi, and N. Adhikari, "Performance Analysis of Different Quantum Key Distribution Protocols for Optimised Security and Efficiency," *IET Quantum Communication*, 2025, doi: 10.1049/qtc2.70015.

[26] P. Zhang, R. Oliveira, Z. Davidson, E. Salas, E. Kosmatos, A. Stavdas, A. Lord, J. Rarity, R. Nejabati, and D. Simeonidou, "Daylight quantum key distribution over free-space optics for future security networks," *Journal of Optical Communications and Networking*, vol. 17, pp. B61–B70, 2025, doi: 10.1364/jocn.553171.

[27] Y. Ji, J. Yu, Y. Yao, K. Yu, H. Chen, and S. Zheng, "Securing wireless communications from the perspective of physical layer: A survey," *Internet of Things*, vol. 19, p. 100524, 2022, doi: 10.1016/j.iot.2022.100524.

[28] R. Shankar and M. Mishra, "Reinforcing 6G Network Security by Combining AES and Polar Codes at the Physical Layer," in *2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI)*, vol. 3, 2025, pp. 1642–1646, doi: 10.1109/iccsai64074.2025.11064175.

[29] A. Yerrapragada, T. Eisman, and B. Kelley, "Physical Layer Security for Beyond 5G: Ultra Secure Low Latency Communications," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 2232–2242, 2021, doi: 10.1109/ojcoms.2021.3105185.

[30] S. Guo, Y. Zhang, J. Guo, S. Zhao, J. He, Y. Shen, and X. Jiang, "A High-Entropy Physical Layer Key Generation Scheme for 5G Systems," *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 8357–8372, 2025, doi: 10.1109/tifs.2025.3588684.

[31] J. Shi, Y. Yu, Q. Yu, H. Li, and L. Wang, "Toward Data Security in 6G Networks: A Public-Key Searchable Encryption Approach," *IEEE Network*, vol. 36, pp. 166–173, 2022, doi: 10.1109/mnet.006.2100714.

[32] T. Srour, M. El-Bendary, M. Eltokhy, and A. Abouelazm, "Triple-layered security system: reliable and secured image communications over 5G and beyond networks," *Scientific Reports*, vol. 15, 2025, doi: 10.1038/s41598-025-10022-0.

[33] R. Kumar and S. Arnon, "Review of Physical Layer Security in Integrated Satellite–Terrestrial Networks," *Electronics*, 2024, doi: 10.3390/electronics13224414.

[34] P. Devi, M. Bharti, and D. Gautam, "A survey on physical layer security for 5G/6G communications over different fading channels: Approaches, challenges, and future directions," *Vehicular Communications*, vol. 53, p. 100891, 2025, doi: 10.1016/j.vehcom.2025.100891.

[35] M. Khoshafa, O. Maraqa, J. Moualeu, S. Aboagye, T. Ngatched, M. Ahmed, Y. Gadallah, and M. Di Renzo, "RIS-Assisted Physical Layer Security in Emerging RF and Optical Wireless Communications Systems: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 27, pp. 2156–2203, 2024, doi: 10.1109/comst.2024.3487112.

[36] V. Chamola, A. Jolfaei, V. Chanana, P. Parashari, and V. Hassija, "Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography," *Computer Communications*, vol. 176, pp. 99–118, 2021, doi: 10.1016/j.comcom.2021.05.019.

[37] S. Hakeem, H. Hussein, and H. Kim, "Security Requirements and Challenges of 6G Technologies and Applications," *Sensors*, vol. 22, 2022, doi: 10.3390/s22051969.

[38] R. Anand, T. Isobe, A. Kundu, M. Rahman, and S. Suryawanshi, "Differential fault attack on AES-based encryption schemes: application to B5G/6G ciphers—Rocca, Rocca-S and AEGIS," *Journal of Cryptographic Engineering*, vol. 14, pp. 595–607, 2024, doi: 10.1007/s13389-024-00360-6.

[39] M. Guo, Z. Lin, R. An, K. An, D. Li, N. Al-Dhahir, and J. Wang, "Inspiring Physical Layer Security With RIS: Principles, Applications, and Challenges," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 2903–2925, 2024, doi: 10.1109/ojcoms.2024.3392359.

[40] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, pp. 679–695, 2018, doi: 10.1109/jsac.2018.2825560.

[41] J. Sánchez, L. Urquiza-Aguiar, M. Paredes, and D. Osorio, "Survey on physical layer security for 5G wireless networks," *Annals of Telecommunications*, vol. 76, pp. 155–174, 2020, doi: 10.1007/s12243-020-00799-8.

[42] J. Tang, H. Wen, K. Zeng, R. Liao, F. Pan, and L. Hu, "Light-Weight Physical Layer Enhanced Security Schemes for 5G Wireless Networks," *IEEE Network*, vol. 33, pp. 126–133, 2019, doi: 10.1109/mnet.001.1700412.

[43] L. Mucchi, S. Jayousi, S. Caputo, E. Panayirci, S. Shahabuddin, J. Bechtold, I. Morales, R. Stoica, G. Abreu, and H. Haas, "Physical-Layer Security in 6G Networks," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1901–1914, 2021, doi: 10.1109/ojcoms.2021.3103735.

[44] A. Haq, S. Sefati, S. Nawaz, A. Mihovska, and M. Beliatis, "Need of UAVs and Physical Layer Security in Next-Generation Non-Terrestrial Wireless Networks: Potential Challenges and Open Issues," *IEEE Open Journal of Vehicular Technology*, vol. 6, pp. 554–595, 2025, doi: 10.1109/ojvt.2025.3525781.

[45] E. Illi, M. Qaraqe, S. Althunibat, A. Alhasanat, M. Alsafasfeh, M. De Ree, G. Mantas, J. Rodriguez, W. Aman, and S. Al-Kuwari, "Physical Layer Security for Authentication, Confidentiality, and Malicious Node Detection: A Paradigm Shift in Securing IoT Networks," *IEEE Communications Surveys & Tutorials*, vol. 26, pp. 347–388, 2024, doi: 10.1109/comst.2023.3327327.

[46] V. Petrov, H. Guerboukha, A. Singh, and J. M. Jornet, "Wavefront Hopping for Physical Layer Security in 6G and Beyond Near-Field THz Communications," *IEEE Transactions on Communications*, vol. 73, pp. 2996–3012, 2025, doi: 10.1109/tcomm.2024.3484937.

[47] A. Sanenga, G. Mapunda, T. Jacob, L. Marata, B. Basutli, and J. Chuma, "An Overview of Key Technologies in Physical Layer Security," *Entropy*, vol. 22, 2020, doi: 10.3390/e22111261.

[48] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities," *IEEE Internet of Things Journal*, vol. 6, pp. 8169–8181, 2019, doi: 10.1109/jiot.2019.2927379.

[49] I. Hameed, A. Afridi, and M. Baek, "Enhancing Physical Layer Security in WPCNs With IRS and Controlled Jamming for 6G IoT Applications," *IEEE Access*, vol. 13, pp. 4670–4682, 2025, doi: 10.1109/access.2024.3525036.

[50] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China Communications*, vol. 14, pp. 1–14, 2017, doi: 10.1109/cc.2017.8246328.

[51] X. Lu, L. Xiao, P. Li, X. Ji, C. Xu, S. Yu, and W. Zhuang, "Reinforcement Learning-Based Physical Cross-Layer Security and Privacy in 6G," *IEEE Communications Surveys & Tutorials*, vol. 25, pp. 425–466, 2023, doi: 10.1109/comst.2022.3224279.

[52] C. Wang, Y. Chen, Z. Lin, Q. Chen, and L. Xiao, "Reinforcement Learning Based Jamming Detection for Reliable Wireless Communications," in *2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring)*, 2024, pp. 1–2, doi: 10.1109/vtc2024-spring62846.2024.10683073.