IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, October 2026
Impact Factor: 8.2

A Study of Hybrid and Post-Quantum Security for 5G-AKA

Avanti Fulsaundar[1], Prof. P. B. Chandane[2], Dr. H. B. Jadhav[3]
Student, Computer Engineering[1]
Guide, Computer Engineering[2]
HOD, Computer Engineering[3]
Adsul Technical Campus, Ahilyanagar, India

Abstract: *Fifth-generation (5G) mobile networks support services such as smart healthcare, connected vehicles, smart homes, and the Internet of Things. Because these services exchange important personal and operational data, secure user authentication is essential. The standard 5G Authentication and Key Agreement (5G-AKA) protocol helps verify users and establish communication keys, but research has identified concerns including user traceability, attacks by a malicious serving network, and limited protection against future quantum-computing threats. This paper explains these issues in simple terms and reviews two approaches discussed in the selected research article: a hybrid method combining Advanced Encryption Standard (AES) with a Key Encapsulation Mechanism (KEM), and a fully post-quantum method based on KEM. The source study reports that both approaches aim to improve authentication security, while the hybrid option uses fewer computational resources. This paper is a literature-based explanation of the published study; it does not claim a new protocol or independent experimental results*

Keywords: 5G-AKA, authentication, post-quantum cryptography, AES, key encapsulation mechanism, network security

I. INTRODUCTION

Mobile networks have become an important part of daily life. People use them for online payments, communication, health services, connected devices, and many other applications. 5G offers high data rates and low communication delay, which makes these services more practical. At the same time, a larger number of connected devices creates more opportunities for security and
privacy problems. Authentication is the process of checking whether a device or user is genuine. In 5G networks, the 5G Authentication and Key Agreement (5G-AKA) protocol is used to authenticate a subscriber and help establish keys for secure communication. However, theselected research article explains that existing authentication methods can still face threats such as malicious serving networks, replay attacks, exposure of temporary secrets, user tracking, and insufficient forward secrecy [1].
Quantum computing is another reason to improve network security. Some widely used public-key cryptographic methods may become vulnerable if sufficiently powerful quantum computers become available. Therefore, post-quantum cryptography is being studied to protect systems against both present-day attacks and possible future quantum attacks.

II. BACKGROUND

A. 5G-AKA Authentication

The authentication process described in the source article involves three main entities: User Equipment (UE), Serving Network (SN), and Home Network (HN). The UE is the user's mobile phone or another connected device. The serving

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, October 2026
Impact Factor: 8.2

network provides network access, while the home network maintains subscriber information and helps decide whether the user should be authenticated. These entities exchange messages to verify identities and establish a session key.

B. Post-Quantum Cryptography and KEM

Post-quantum cryptography refers to cryptographic methods designed to remain secure against attacks from quantum computers.A Key Encapsulation Mechanism (KEM) allows two parties to establish a shared secret key using public-key and private-key operations. In general, one party uses a public key to create an encapsulated value and a shared key; the other party uses its private key to recover the same shared key. The shared key can then protect further communication.

C. Hybrid Security

A hybrid approach combines a conventional cryptographic technique with a post-quantum technique. In the paper being reviewed, the hybrid version combines AES, a symmetric encryption algorithm, with KEM. The other version relies on KEM for its post-quantum approach. The aim is to balance security with the processing and communication limits of mobile devices.

III. RESEARCH PROBLEM AND OBJECTIVES

The main problem is how to make 5G user authentication more resistant to current security attacks and future quantum threats without creating too much additional computational, communication, or energy cost. Some earlier schemes have security weaknesses, while others may require resources that are difficult for smaller devices to provide.

The objectives of this study are:

- To explain the security limitations associated with conventional 5G-AKA authentication.
- To understand how post-quantum cryptography and KEM can be used in authentication.
- To compare the hybrid AES-plus-KEM approach with the fully KEM-based approach described in the source article.
- To discuss the balance between security protection and system performance.

IV. APPROACH DISCUSSED IN THE SELECTED STUDY

A. Hybrid AES + KEM Approach

In the first approach, AES is combined with KEM. The use of KEM supports the establishment of shared secret keys, while AES is used as part of the hybrid cryptographic design. According to the source article, this version is intended to provide strong protection while reducing the processing burden compared with the fully KEM-based version. A hybrid design may be useful when a system needs to move gradually toward post-quantum security while keeping practical resource use in mind.

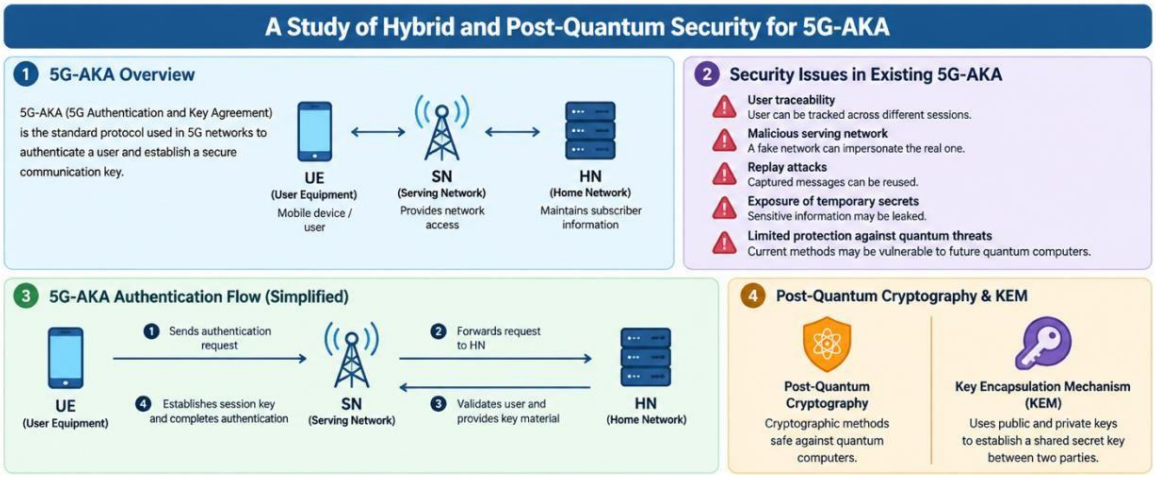
B. Fully KEM-Based Approach

The second approach uses KEM as the basis of the post-quantum authentication design. It aims to reduce reliance on classical public-key cryptography that may be threatened by quantum computing. This version provides an alternative for systems that want a fully post-quantum-oriented design, although the source study reports that it requires more computation than the hybrid version.

C. Security Checks and Evaluation

The selected article reports using formal security analysis, including the Real-Or-Random (ROR) model and the Scyther verification tool. It also compares the proposed versions with existing protocols and evaluates computational cost, communication overhead, and energy use. These are the results reported by the original authors; no separate testing or implementation was performed for the present student paper.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, October 2026
Impact Factor: 8.2



V. COMPARISON AND DISCUSSION.

Both approaches are designed to strengthen authentication and protect session keys. The hybrid approach combines AES and KEM, whereas the second approach relies on KEM. The source article reports that both versions provide comparable security goals, but the hybrid approach has lower computational cost and uses resources more efficiently [1]. This difference matters because mobile devices and Internet of Things equipment may have limited processing power and battery capacity.

A fully post-quantum approach has the advantage of placing post-quantum cryptography at the centre of the design. However, performance must still be considered before it can be used widely. A hybrid approach can be a practical transition option, but its actual suitability depends on the security requirements, implementation details, and standards adopted by network operators. No cryptographic design should be treated as completely secure merely because it uses a post-quantum algorithm; it must be carefully reviewed and tested.

The source article also highlights the importance of considering an insecure communication channel between the serving network and home network. This is relevant to practical situations such as roaming, where relying on a permanently secure link may not always be realistic. Authentication protocols should therefore be assessed under realistic network conditions as well as theoretical security models.

Feature	Hybrid (AES + KEM)	Post-Quantum (KEM Only)
Security against current attacks	High	High
Protection against quantum threats	High	High
Computational resources	Lower	Higher
Communication overhead	Lower	Higher
Suitability for mobile devices	Better	More challenging

VI. APPLICATIONS AND CHALLENGES

Stronger 5G authentication can be relevant to smartphones, connected vehicles, smart healthcare devices, industrial networks, and Internet of Things systems. These applications may transmit private or safety-related information, so reliable identity verification and session-key protection are important.

Several challenges remain. Post-quantum algorithms can involve larger keys or additional processing. Network operators must consider compatibility with existing systems, communication overhead, energy use, and the cost of updating equipment. Further testing in real deployments is needed to understand performance under different traffic levels and device capabilities

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, October 2026
Impact Factor: 8.2

VII. CONCLUSION

This paper reviewed the security problem addressed by the selected research article on transitioning 5G-AKA toward hybrid and fully post-quantum security. Conventional authentication protocols face continuing challenges, and quantum computing creates a reason to prepare for stronger cryptographic protection. The two approaches discussed are a hybrid AES-plus-KEM method and a fully KEM-based method. As reported by the original authors, both aim to improve security, while the hybrid version has a lower computational cost. The most suitable option will depend on the required level of protection and the resources available in the target network. Future work should include careful independent evaluation, practical deployment testing, and continued review as post-quantum standards and technology develop.

ACKNOWLEDGEMENT

The author acknowledges the published research article used as the main source for this literature-based paper.

REFERENCES

[1] E. Choudhary, A. K. Yadav, R. Kumar, and M. Liyanage, "A Practical Approach to Transitioning 5G-AKA Toward Fully and Hybrid Post-Quantum Security for 5G and Beyond Communication," IEEE Open Journal of the Communications Society, vol. 7, pp. 2980–2999, 2026, doi: 10.1109/OJCOMS.2026.3677962.
[2] 3rd Generation Partnership Project (3GPP), "Security Architecture and Procedures for 5G System," 3GPP TS 33.501, 2020