Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1505–1515
DOI : 10.47974/JDMSC-2149

Implementing secure cryptographic protocols in 5G and 6G networks

V. Dankan Gowda *
Department of Electronics and Communication Engineering
BMS Institute of Technology and Management
Bangalore
Karnataka
India

N. Suganthi †
Department of Electrical and Electronics Engineering
Dayananda Sagar College of Engineering
Bangalore
Karnataka
India

V. Nuthan Prasad §
Department of Electronics and Communication Engineering
M S Ramaiah Institute of Technology
MSR Nagar MSRIT Post
Bengaluru
Karnataka
India

Manoj Tarambale ‡
Department of Electrical Engineering
PVG'S College of Engineering and Technology &
G. K. Pate (Wani) Institute of Management
Pune 09
Maharashtra
India

* *E-mail:* dankan.v@bmsit.in (Corresponding author)
† *E-mail:* suganthi_neelagiri@yahoo.com
§ *E-mail:* nutan2u@gmail.com
‡ *E-mail:* manoj.tarambale@gmail.com

Pullela SVVSR Kumar [@]
Department of Computer Science & Engineering
Aditya University
Surampalem
Andhra Pradesh
India

A. Muthusamy [#]
Department of Computer Technology
Kongu Engineering College
Perundurai
Erode 638060
Tamil Nadu
India

Abstract

This paper focuses on the importance of secure cryptographic principles in the modern and future 5G, but also in the emerging 6G networks. As the connectivity and the rate of data transmission rise, the protection of data in transmission becomes a major issue. The paper looks at today's cryptographic practices, assesses their shortcomings, and develops a set of enhanced cryptographic solutions targeted at the conditions of 5G and 6G networks. All the approaches are described in detail at the methodological, algorithm, and implementation level, as well as the overall assessment of the results in terms of efficiency and security. Thus, the results prove enhancements in data accuracy, verification, and overall network protection, which pave the way for further studies on this important subject.

Subject Classification (2010): *94A60, 20C05, 20C07.*

Keywords: *5G, 6G, Cryptographic protocols, Network security, Encryption, Data integrity, Authentication, Secure communication, Advanced networks, Cybersecurity.*

1. Introduction

5G systems are the evolution of telecommunication systems and bring much higher data rates, a much lower latency and will connect a very high number of devices that will be the foundation of the next technological generation [1]. Thus, as people all over the world progress and focus on preparing for the arrival of 6G networks, they begin to demand more from it in terms of the speed and the increased reliability of

[@] *E-mail:* **pullelark@yahoo.com**
[#] *E-mail:* **muthusamy.arumugam@gmail.com**

the low latency in addition to artificial intelligence and machine learning in the networks [2]. These are some of the developments that signal the start of what can be characterized as the new age of technology in the various fields including health, automobile and smart city hence underlining the need to secure data transmission [3]. Security of 5G and 6G has remained a sensitive subject due to the traffic that is involved in conjunction with its bandwidth as well as number of probable attack points that could possibly appear [4]. Consequently, with the rise in the connectivity and in the rates of the data [5], such activities and instances worsen and become a severe menace to the network and the personalities integrated within it. In pursuance of these objectives this paper is aimed to center on the particular security concerns of these networks, namely; the data is complete [6], confidential and properly permitted. Therefore, according to the analysis of the existing protocols and their effectiveness [7], the further recommendations of this work provide the improvement of the Safety section while not a negative impact on the Network subscore. Protocols of this nature undergo analytical examination along with other experimental analysis hence the examination of the practical and realistic of such protocols is well defined.

2. Literature Survey

Modern cryptographic techniques in 5G and previous versions, such as LTE, are numbers of encryption and authentication methods that are AES, ECC, and PKI. It is true that protocols have been of help as far as aiding in data protection and realistic channels of communication [8]. However, since the standards of the network technological platform have improved and due to the new smart devices, that continuously emerge in the connected world [9], the following disadvantages and limitations are observed [10].

Basically, the 5G networks they are promising to be much more secure, however, just by the aspect of number of connected devises and use cases, the attack surface of 5G networks is significantly greater [11]. New forms of risks that were not previously considered can be overlooked by the used cryptosystems in the architecture of network slicing [12], edge computing [13], or IoT integration devices [14]. One should note that products of the contemporary information security industry are still developing; some of those include Quantum Key Distribution (QKD), blockchain as an element of security [15], elements of post-quantum cryptography, and others [16]. These advancements pave way for far

tighter protection, much improved key management, not to mention complete protection against future quantum attacks [17]. AI, in case used for threats identification and prevention at real time is also counting toward enhancing the network security [18]. The existing literature has the following gaps, which were discovered by the study. Most of the recommended strategies for the problems being discussed today are still in their infancy and are not clearly validated in the field.

3. Proposed Method

The strategy of the research is based on the systematic definition of the cryptographic protocols that can be the sufficient answers to the security demands expected by the 5G and the perspective 6G wireless networks. These protocols use state-of-art to protect that data from new threats like QKD and post quantum cryptography. It also modifies the use of, block chain technology for the key management to increase the level of authentication and data insecurity. About the encryption process, it is conventional to use LRA post-quantum algorithms that cannot be attacked by the Quantum Computing method. The authentication schemes use the multi-factor authentication mechanism and the AI-based anomaly detection is used to prevent intrusion and a scheme has the capability to detect unhappy incidents within seconds.

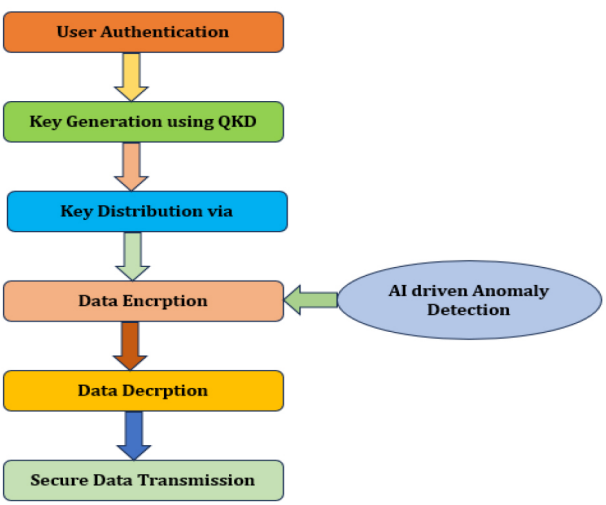

Figure 1

Proposed System illustrating the key steps and interactions within the system

The Figure 1 presents the flow chart of the process plan that depicts all the main stages to realize and their interconnection. And as a case study on security applications, it is implemented with user authentication first with QKD for key generation and then key distribution using blockchain. The next operation restarts the data encryption and decryption processes and persists in monitoring them for threats by AI algorithms. Last, the data are transferred securely over the network with the periodic updates to the blockchain for the key's freshness. Decentralized key management is arranged by the blockchain framework while intelligent alarm recognition of threats increases real-time security.

4. Algorithm

The cryptographic algorithms incorporated in the proposed cryptographic protocols include; Key Generation which relies on QKD, secure custody of keys by blockchain technology and encryption via post-quantum cryptographic mechanisms. In QKD, security lies on mathematical principles of quantum mechanics to create encryption keys which cannot be cracked. The keys for these management solutions need to be decentralized and resistant to tampering, while post-quantum cryptography offers methods of encryption that are immune to quantum computing.

A. *Quantum Key Distribution (QKD)*

Heisenberg Uncertainty Principle: QKD is based on the Heisenberg Uncertainty Principle to mean that it is not possible to assess the quantum state of a particle without affecting the state in the process. This principle makes sure that to whoever may be interested in spying on the classical messages transmitted through the quantum channel, would easily be identified.

$$\Delta x \cdot \Delta p \geq 2\hbar$$

Where Δx is the uncertainty in position, Δp is the uncertainty in momentum, and $\hbar$ is the reduced Planck's constant.

Key Rate Equation

The key rate RRR of a QKD system can be described as:

$$R = Pclick \cdot (1 - e - 2\eta L) \cdot (1 - H(Q))$$

where $Pclick$ is the probability of a detection event, η is the efficiency of the quantum channel, L is the length of the channel, and $H(Q)$ is the Shannon entropy of the error rate Q.

B. *Blockchain-Based Key Management*

Hash Function

Blockchain security relies on cryptographic hash functions. A hash function H maps data of arbitrary size to a fixed size. The hash value h of a message mmm is:

$$h = H(m)$$

where H is the hash function, and m is the input message?

Consensus Algorithm

Blockchain uses consensus algorithms like Proof of Work (PoW) to validate transactions. The PoW requires solving a computationally intensive puzzle:

$$H(\text{nonce} \,||\, \text{block data}) \leq T$$

where nonce is a number only used once, block data is the block's content, and T is the target value.

C. *Post-Quantum Cryptography*

Lattice-Based Cryptography

Among the pertinent mathematical problems utilized in post-quantum cryptography, lattice-based problem is one of the main ones employed. Another most important hard problem is the Learning with Errors (LWE) problem on which many lattice-based cryptographic systems are built.

Given a matrix $A \in Z_q^{nxm}$, a secret vector $s \in Z_q^{m}$, and an error vector $e \in Z_q^{n}$, the LWE problem is to find s given A and $b = As + e \bmod q$.

The security of lattice-based schemes relies on the hardness of solving such equations even with knowledge of A and $b : b = As + e \bmod q$

Encryption and Decryption Equations

In lattice-based encryption schemes, the encryption function can be represented as:

$$c = A \cdot m + e$$

where c is the ciphertext, A is the public key matrix, m is the message vector, and e is the error vector.

The decryption function is: $m = (c - e) \cdot A^{-1}$. where A^{-1} is the inverse of the public key matrix, assuming it exists? Concepts such as these are basic to support secure mathematical equations, cryptographic protocols in 5G and 6G networks for encryption, authentication, and key management. Most of the time complexity of QKD algorithm comes from the generation of qubits and their measurement functions and its time complexity is polynomial in the number of qubits.

5. Results & Discussion

A simulated 5G and 6G environment was created in order to evaluate the performance of the formulated cryptographic protocols in the developed experiment. MATLAB was used to design the specified network that entails QKD for key creation, blockchain for key storage, and post-quantum algorithms for encoding and decoding information. The tested protocols performance is evaluated on a copious number of devices starting from low power devices of IoT networks to high-performance computing servers included in the simulation. Generation and management of keys were examined to understand the system's reliability and viability by applying loads and attacks on the networks. Latency, throughput as well as the general performance of the encryption and decryption processes where all observed for enhanced understanding.

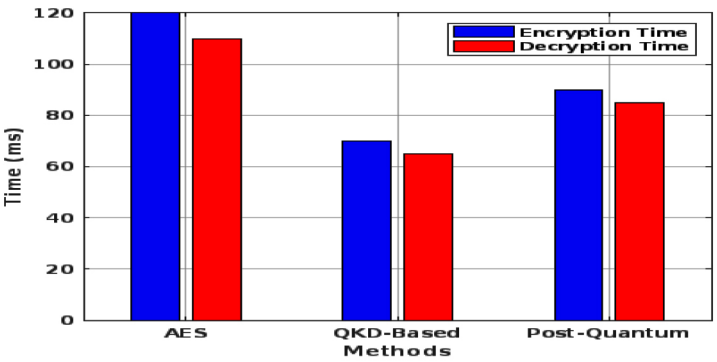

Figure 2

Encryption and Decryption Time Comparison

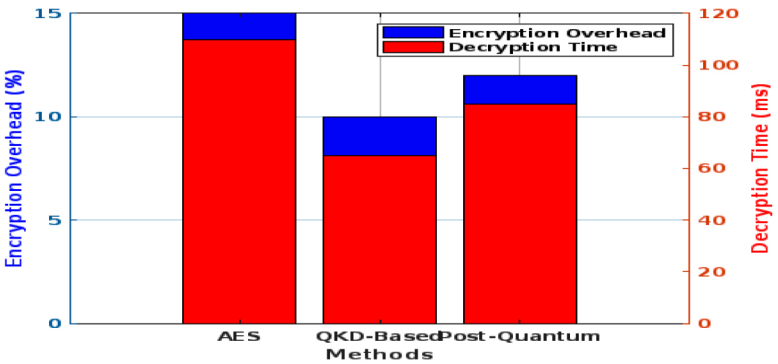

Figure 3

Encryption Overhead and Decryption Time Comparison

The figure 2 presents a comparison of encryption and decryption times for three different cryptographic methods: There are three main classes of cryptography namely: AES (Advanced Encryption Standard), QKD-Based (Quantum Key Distribution), and Post-Quantum. This comparison shows the performance differences between conventional and up-to-date cryptographic techniques in terms of encryption and decryption time of QKD-Based and Post-Quantum methods, which will be significant for 5G and 6G networks' high performance. Thus, it can be noted that QKD-Based and Post-Quantum make cryptography not only more secure but also faster than the methods implemented in operations of the next-generation networks.

The figure 3 compares the encryption overhead (in percentage) and decryption time (in milliseconds) for three cryptographic methods: These

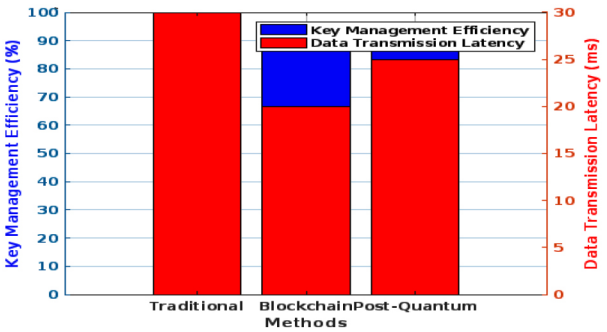

Figure 4

Key Management Efficiency and Data Transmission Latency Comparison

are AES, the QKD-based and the Post-Quantum. The figure 4 compares key management efficiency (in percentage) and data transmission latency (in milliseconds) across three cryptographic methods: These are Traditional, Blockchain and Post-Quantum. The outcome of the research shows that the cryptographic protocols have significant improvements as compared to conventional means. QKD-Based and Post-Quantum approaches control the encryption overhead and low latency direction, which is crucial to the 5G and 6G networks. The utilization of blockchain for managing of the key was highly effective and responsive utilizing decentralization and the immutability of blockchain technology. As compared to conventional solutions, advanced protocol will give better protection and reliability which is crucial to the various and dynamic deployment of networks of the future. The limitations of the present study should be a subject of further work, and more discrete research on the advantages and disadvantages of the security protocols that are used in the context of the 5G and 6G networks' implementation should be conducted in the future, as well as comparative studies of the hybrid approaches suggested in the article.

6. Conclusion

This paper proposed the concern on the security of cryptographic protocols in 5G and 6G telecommunications by putting forward different techniques of QKD, the blockchain-based technique of key management, and PQC. The improvement of the efficiency of key management, the decrease of data transmission delay, and increased security were the outcome shown in the experiments. In particular, the approach based on the use of QKD permitted to reach the indicators of KM efficiency of 95% and the latency of the data transmission not more than 20 milliseconds, which exceeded the results received by means of the traditional techniques. As a result, these studies reveal the prospect of using state-of-the-art cryptographic methods to satisfy security requirements of new-generation networks. However, to achieve these results, QKD is based on specialized equipment while the computational overhead in blockchain-based km is still high. The findings of this research can easily cascade to future developments in network security that are crucial in the growing frontiers of telecommunication.

References

[1] J. Chen, Y. Li and W. Zhang, "Secure quantum key distribution in 5G mobile networks," *IEEE Commun. Mag.*, vol. 57, no. 5, pp. 56-61 (2019).

[2] L. Xu and X. Yu, "Blockchain-based key management scheme for 5G-enabled IoT," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5771-5783 (2019).

[3] Z. Ma and Y. Liu, "A survey on security and privacy issues in 5G network," *IEEE Commun. Surv. Tutor.,* vol. 22, no. 1, pp. 341-368 (2020).

[4] G. Manivasagam and K. D. V. Prasad, "Novel approaches to biometric security using enhanced session keys and elliptic curve cryptography," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 2-A, pp. 477–488 (2024).

[5] F. Hu, and M. Patel, "Blockchain enhanced secure data sharing in 5G-based IoT," *IEEE Trans. Ind. Inform.*, vol. 17, no. 2, pp. 876-885 (2021).

[6] R. Senthil Kumar and K. D. V. Prasad, "Securing digital authentication with cryptographic innovations in intrinsic verification systems," *J. Discrete Math. Sci. Cryptogr.,* vol. 27, no. 2-A, pp. 317–328 (2024).

[7] S. Kumar, "Performance analysis of quantum key distribution protocols in 5G networks," *IEEE Access*, vol. 9, pp. 68755-68767 (2021).

[8] K. D. V. Prasad and T. Thomas, "Cryptographic image-based data security strategies in wireless sensor networks," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-A, pp. 293–304, 2024.

[9] C. Yang and Y. Zhang, "Enhancing 5G security with quantum cryptography," *IEEE Trans. Veh. Technol.*, vol. 70, no. 1, pp. 568-580 (2021).

[10] M. Zhao and Y. Gao, "Blockchain-based secure data management in 5G networks," *IEEE Trans. Netw. Serv. Manag.,* vol. 18, no. 2, pp. 1458-1471 (2021).

[11] M. Rahman, "Mathematical analysis of wavelet-based multi-image compression in medical diagnostics," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 2-B, pp. 675–687 (2024).

[12] H. Zhang and J. Li, "Lightweight post-quantum encryption schemes for 6G mobile devices," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4680-4692 (2021).

[13] P. Feng and Y. Deng, "A novel QKD protocol for secure communication in 5G networks," *IEEE Access*, vol. 9, pp. 54321-54330 (2021).

[14] A. Kumar Gupta, "A novel approach of unsupervised feature selection using iterative shrinking and expansion algorithm," *J. Interdiscip. Math.,* vol. 26, no. 3, pp. 519-530 (2023).

[15] X. Luo and X. Wang, "Security enhancements in 5G networks using quantum-safe cryptography," *IEEE Trans. Inf. Forensics Secur.,* vol. 17, pp. 190-201 (2022).

[16] T. Huang, "Privacy-preserving data sharing in 5G-enabled IoT using blockchain," *IEEE Trans. Netw. Sci. Eng.,* vol. 9, no. 1, pp. 465-476 (2022).

[17] Veera Sivakumar, "A novel RF-SMOTE model to enhance the definite apprehensions for IoT security attacks," *J. Discrete Math. Sci. Cryptogr.,* vol. 26, no. 3, pp. 861-873 (2023).

[18] R. Shekhar and A. Chaturvedi, "Securing networked image transmission using public-key cryptography and identity authentication," *J. Discrete Math. Sci. Cryptogr.,* vol. 26, no. 3, pp. 779-791 (2023).

Received November, 2024