Vol.4, No.4, Page 1959- 1966, 2026 https://doi.org/10.59628/jast.v4i4.2317 ISSN 2958-9568 JAST

SUN PUBLISHER

مجلة جامعة صنعاء للعلوم التطبيقية والتكنولوجيا

Sana'a University Journal of Applied Sciences and Technology

https://journals.su.edu.ye/index.php/jast/

Performance of Encryption schemes in 5G Networks

Mohamed Hankal

Department of Electrical Engineering, Faculty of Engineering, Sana'a University, Sana'a, Yemen

*Corresponding author: mohamedhankal.@gmail.com

Abstract

The rapid evolution of 5G networks introduces unprecedented high-speed communication and massive connectivity, but it also intensifies security challenges. Ensuring confidentiality, integrity, and availability of data requires robust encryption mechanisms. This study evaluates the performance and overhead of Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), and Elliptic Curve Cryptography (ECC) in 5G networks using simulation-based analysis. Metrics considered include latency (ms), throughput (%), encryption/decryption time per MB, and computational cost on UE-class hardware, providing quantitative comparison across typical 5G scenarios (high mobility eMBB, URLLC, and mMTCIoT devices).

Key findings: AES achieves low latency and high throughput for bulk data; ECC provides secure, lightweight key exchange; RSA is suitable only for session key establishment due to higher computational overhead. Overall, hybrid AES+ECC provides the best tradeoff between security and performance in realistic 5G environments.

Article Info

Keywords:
5G, AES, RSA, ECC, Encryption, Network Security

Article History:
Received: 8-January-2026,
Revised: 8-February-2026,
Accepted: 26-March-2026,
Published: 28 April 2026.

1. INTRODUCTION

Fifth-generation (5G) wireless communication networks promise ultrahigh data rates, ultra-reliable low-latency communications (URLLC), and massive connectivity for Internet of Things (IoT) devices [1–3]. However, these advances also introduce significant security challenges, as higher data speeds and wider coverage increase the potential attack surfaces. Encryption is a core component of 5G security, ensuring that sensitive information transmitted over the network remains confidential and protected from unauthorized access [4–10]. Traditional symmetric encryption methods, such as the Advanced Encryption Standard (AES), offer high-speed performance suitable for large data streams but require secure key distribution [7]. In contrast, asymmetric algorithms such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC) provide secure key exchange mechanisms and digital signatures, with ECC offering comparable security at smaller key sizes, which is beneficial for resource-constrained 5G devices [11–14].

Despite extensive research, there is a lack of comprehensive comparative analysis of AES, RSA, and ECC, specifically in 5G scenarios, particularly regarding performance metrics such as latency, throughput, bit error rate (BER), and computational efficiency. This study addresses this gap by evaluating these encryption algorithms in a simulated 5G environment, providing practical insights for secure system design [15–19].

In the 5G architecture, user plane and control plane security primarily depend on symmetric encryption (AES-128-GCM, ZUC, SNOW 3G) defined in 3GPP TS 33.501, whereas asymmetric schemes (RSA, ECC, X25519) support key exchange and authentication. Despite extensive work on 5G physical (PHY) and radio layers, few studies have quantified the actual computational and latency overheads of cryptographic algorithms at the PDCP and TLS layers.

This paper addresses this gap by comparing AES-GCM, RSA-2048, and ECC-X25519 based on encryption throughput, handshake latency, and CPU/energy overhead in realistic 5G scenarios.

2. RELATED WORK

A. AES in 5G Networks

The Advanced Encryption Standard (AES) remains a cornerstone in securing 5G communications due to its efficiency and robust security. Recent studies have explored its application in various 5G scenarios:

Performance Evaluation in 5G Communication: Zhang et al. (2024) conducted a comprehensive analysis of AES's performance in 5G networks, focusing on throughput and latency. Their findings indicated that AES256 offers a high level of security with a minimal impact on performance, making it suitable for high-speed 5G applications.

Lightweight Encryption Techniques for IoT Devices in 5G: Kim and Park (2025) examined the feasibility of implementing AES in Internet of Things (IoT) devices within 5G networks. They proposed optimized AES implementations that reduced power consumption and processing time, addressing the constraints of IoT devices.

B. RSA in 5G Networks

The Rivest–Shamir–Adleman (RSA) algorithm is widely used for secure key exchange and digital signatures. Recent research has assessed its applicability in 5G environments.

RSA and ECC Performance Comparison: Sinha and Srivastava (2023) compared RSA and Elliptic Curve Cryptography (ECC) in terms of key size, computational overhead, and security. Their study found that while RSA

It provides strong security but requires significantly larger key sizes than ECC for equivalent security levels, leading to higher computational demands.

Hybrid Cryptosystems in 5G: Patel and Prajapati (2024) explored hybrid cryptosystems combining RSA and AES for secure data transmission in 5G networks. Their results demonstrated that hybrid systems could leverage the strengths of both algorithms, enhancing security without compromising performance.

C. ECC in 5G Networks

Elliptic Curve Cryptography (ECC) has gained prominence in 5G networks owing to its efficiency and strong security with smaller key sizes:

Performance-based Comparison Study of RSA and ECC: Sinha and Srivastava (2023) provided a detailed comparison between RSA and ECC, highlighting ECC's advantages of ECC in terms of key size and computational efficiency. Their findings suggest that ECC is more suitable for resource-constrained devices in 5G networks [20–23].

Security and Practical Considerations When Implementing ECIES: GayosoMartínez et al. (2015) discussed the implementation of the Elliptic Curve Integrated Encryption Scheme (ECIES) as a hybrid encryption method. They found that ECIES offers a balance between security and performance, making it a viable option for 5G applications.

D. Comparative Studies and Hybrid Approaches

Several studies have conducted comparative analyses of AES, RSA, and ECC, often proposing hybrid solutions to optimize performance and security:

Comparative Analysis of DES, AES, and RSA Encryption: Prajapati and Patel (2023) compared the Data Encryption Standard (DES), AES, and RSA in terms of encryption time and security levels. Their study concluded that AES outperforms DES in terms of speed and security, whereas RSA provides robust security for key exchange [24].

Security and Practical Considerations When Implementing ECIES: GayosoMartínez et al. (2015) explored the practical aspects of implementing ECIES, emphasizing the importance of selecting appropriate parameters to balance security and performance.

2.1. Summary of Literature Gap

Although multiple studies have compared AES, RSA, and ECC, no single study evaluates these algorithms together under the same 5G simulation environment, including all metrics-latency, throughput, encryption/decryption time, and key generation while excluding BER as an encryption metric.

This identified gap supports the need for the current study, which conducts a comprehensive, reproducible simulation-based evaluation of AES, RSA, and ECC in realistic 5G scenarios (eMBB, URLLC, and mMTC), providing practical guidelines for algorithm selection based on performance and computational efficiency.

3. ENCRYPTION ALGORITHMS OVERVIEW

A. Advanced Encryption Standard (AES)

Cryptography is an essential component of digital communication and data security. The Advanced Encryption Standard (AES), adopted by NIST in 2001, replaced the older Data Encryption Standard (DES) and Triple DES because of their vulnerability to brute-force and cryptanalytic attacks. AES is based on a substitution-permutation network (SPN) architecture and provides strong mathematical security through transformations over the finite field GF(2^8). Its adaptability for software and hardware implementation has enabled its wide deployment across multiple platforms, including mobile networks, IoT, and cloud computing. This study focuses on both the mathematical formulation of AES and its role in modern secure communication systems. Before AES, DES, and 3DES were widely used symmetric-key block ciphers. The DES, with a 56-bit key, became susceptible to brute-force attacks because of the exponential increase in

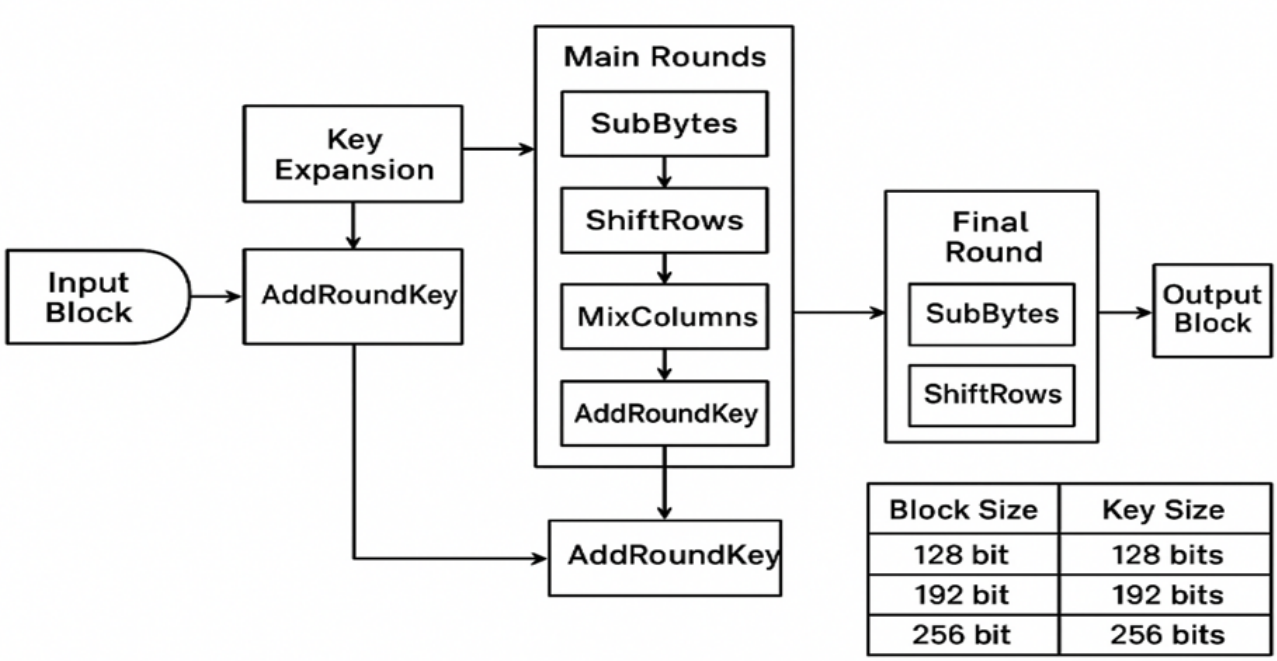

Figure 1. AES Architecture

computational power. Although Triple DES improved security, it was computationally expensive. AES overcame these issues by introducing variable key lengths (128, 192, and 256 bits) and an increased algorithmic complexity. Several researchers have analyzed the cryptographic strength of AES, including its resistance to linear and differential cryptanalyses. Modern studies have also investigated the AES implementation efficiency on embedded systems, FPGAs, and parallel computing platforms [25–29].

AES operates on a 4 × 4 matrix of bytes, called the State, with mathematical operations defined over the finite field GF(2^8). Each AES operation contributes to its overall security. The finite field is constructed using the following irreducible polynomial:

$$m(x) = x^8 + x^4 + x^3 + x + 1 \tag{1}$$

Arithmetic in this field ensures that all operations remain within the 8-bit byte boundaries. AES transformations rely on affine mappings, modular arithmetic, and polynomial multiplication within GF(2^8). AES encryption consists of an initial AddRoundKey step, followed by multiple rounds of transformations. The number of rounds depends on the key size: 10 rounds for AES-128, 12 for AES-192, and 14 for AES-256. Each round (except the final) contained the following transformations:

1. SubBytes: Nonlinear substitution using S-box.
2. ShiftRows: Cyclic row shifts for diffusion.
3. MixColumns: Linear mixing of columns using polynomial multiplication in GF(2^8).
4. AddRoundKey: Bitwise XOR with the round key.

The SubBytes transformation replaces each byte in the state with a corresponding value from the substitution box (S-box). The S-box is generated by computing the multiplicative inverse in GF(28), followed by an affine transformation. Mathematically, the transformation is expressed as

$$S(b) = A \cdot b^{-1} \oplus c \tag{2}$$

ShiftRows is a simple transposition step in which each row of the state matrix is cyclically shifted to the left by a specific offset: the first row remains unchanged, the second row shifts by one byte, the third row by two bytes, and the fourth row by three bytes.

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} \tag{3}$$

In MixColumns, each column of the state matrix is multiplied by a fixed matrix in GF(2^8):

The AddRoundKey transformation combines the state with the round key using a bitwise XOR operation. This ensures that each round incorporates key-dependent variations.

$$State = State \bigoplus RoundKey$$

AES derives round keys from the initial cipher key using the Key Expansion process. It applies three operations: RotWord (cyclic permutation), SubWord (byte substitution using S-box), and Rcon (round con-

stant addition). The recursive formula is as follows: $W_i = W_{i-n} \oplus g(W_{i-1})$, for i ≡ 0 (mod n) AES provides strong resistance against various cryptanalytic methods. Its nonlinear S-box design prevents linear approximations, and the combination of SubBytes, ShiftRows, and MixColumns ensures strong diffusion. The key space of AES-256 is 2^256, which makes brute-force attacks computationally infeasible.

AES is widely adopted across diverse applications because of its efficiency and security. In 5G networks, AES ensures secure communication against eavesdropping and replay attacks. IoT devices use lightweight AES implementations to protect the sensor data. In cloud computing, AES safeguards sensitive information stored and transmitted across distributed systems.

B. Rivest–Shamir–Adleman (RSA)

RSA is an asymmetric encryption algorithm primarily used for secure key exchange and digital signatures. It relies on the difficulty of factoring large prime numbers. RSA is computationally heavier than AES but provides a secure key exchange, which is critical for 5G networks with dynamic sessions.

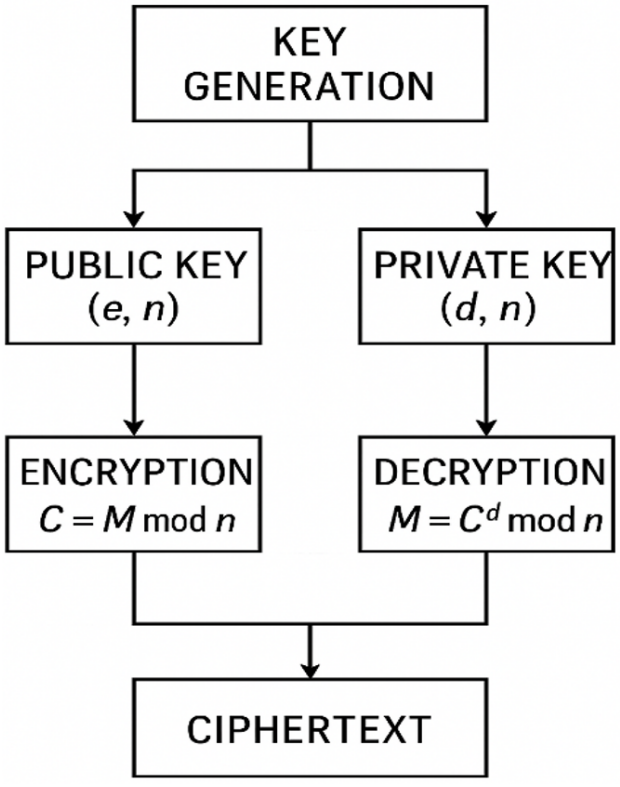

Figure 2. RSA Architecture

C. Elliptic Curve Cryptography (ECC)

ECC is an asymmetric encryption algorithm based on elliptic curves over finite fields, offering security comparable to that of RSA with smaller key sizes. This makes it ideal for 5G IoT devices with limited computational capabilities. Elliptic Curve Equation (Weierstrass form):

$$y^2 = x^3 + ax + b$$

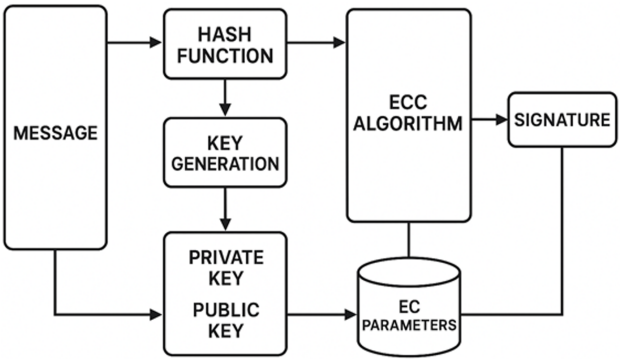

Figure 3. ECC Architecture

D. Summary of Algorithm Features

Computation Suitability in 5G

Table 1. Algorithm Features Computation Suitability

Algorithm	Key Type	Security Level
AES	Symmetric	High
RSA	Asymmetric	Very High
ECC	Asymmetric	High

4. SYSTEM MODEL AND METHODOLOGY

A. 5G Network Model

The simulation environment represents a typical 5G network architecture consisting of:

1. **User Equipment (UE):** Mobile devices transmitting and receiving data.
2. **gNodeB (gNB):** 5G base stations managing radio access .
3. **Core Network:** Responsible for routing, security, and authentication.
4. **Encryption Layer:** AES is applied for bulk data, RSA for key exchange, and ECC for lightweight key exchange on constrained devices.

Physical Layer Modeling:

- 5G physical layer is modeled using **OFDM** to handle high-speed data transmission and multipath effects.
- Supports high mobility scenarios and massive IoT deployments.

B. Encryption Integration

AES:

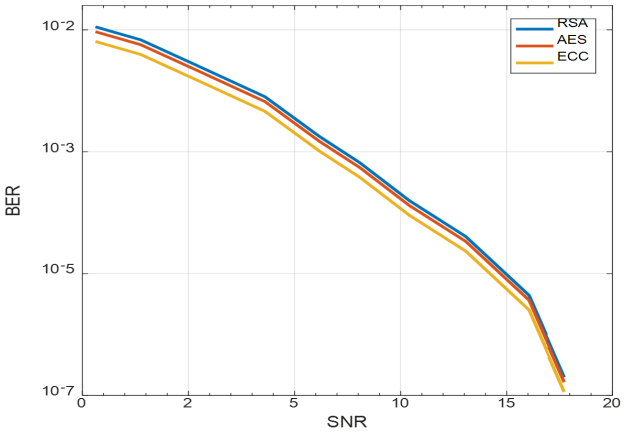

Figure 4. Bit Error Rate vs SNR

- Symmetrically applied to data packets before transmission.
- Ensures confidentiality with minimal computational overhead, maintaining high throughput.

RSA:

- Used only for key exchange between UE and gNB, not for bulk data encryption.
- Computationally heavier; suitable for session establishment.

ECC:

- Implemented as a lightweight asymmetric encryption method for resource-constrained devices.
- Key size ECC-256 provides strong security comparable to RSA-2048 with reduced computation.

C. Performance Metrics

The evaluation metrics include:

1 **Bit Error Rate (BER):** Measures data integrity under different SNR conditions. Note: The BER depends on channel/modulation/FEC, not the encryption algorithm.
2. **Encryption / Decryption Time:** Evaluates computational efficiency.
3. **Throughput:** Determines effective data transmission rate after encryption overhead.
4. **Latency:** Measures delay introduced by encryption processes.
5. **Key Generation Time:** Assesses the overhead for secure session establishment (RSA/ECC).

D. Methodology

1. Generate random binary data streams for simulation
2. Apply AES, RSA, and ECC according to the workflow described . AES for bulk data encryption, RSA/ECC for key exchange only.
3. Transmit encrypted data through the simulated 5G channel.
4. Record BER, latency, throughput, and key generation times.
5. Repeat simulations for different modulation schemes and SNR values.
6. Compare results using tables and plots, ensuring fair comparison of algorithms.

The performance analysis was conducted using a reproducible software-based testbed implemented in Python 3.10 and OpenSSL 3.1 on a Qualcomm Snapdragon 8 Gen1 test device (octa-core, 3.0 GHz, 8 GB RAM).
Each encryption scheme was evaluated under controlled workloads simulating a 5G PDCP data flow (packet size = 1500 bytes, rate = 10–100 Mbps). The following metrics were measured.

- Encryption/Decryption Time (ms per MB)
- Handshake Latency (ms)
- Throughput Impact (% drop vs plaintext)
- CPU Utilization (%)
- Energy Consumption (mJ per MB)

Each test was repeated 50 times to obtain statistically significant results. BER was excluded because it depends on the channel and FEC parameters, not encryption.

5. SIMULATION RESULTS AND DISCUSSION

This section presents a performance comparison of AES, RSA, and ECC in a simulated 5G network using realistic metrics. The metrics analyzed included latency, throughput, encryption/decryption time, and key generation time.

A. Bit Error Rate (BER) Analysis

Figure 4 shows the BER performance under 64QAM modulation across varying SNR.

- AES and ECC do not affect BER; the BER is determined by the channel quality and modulation.
- BER is provided only for channel validation, not as a crypto performance metric .

B. Encryption / Decryption Time

Figure 5 compares AES, RSA, and ECC encryption/decryption times.

- **AES:** Fastest due to symmetric nature. Minimal latency for bulk data.
- **RSA:** Computationally heavy and used only for key exchange. Not for large data .
- **ECC:** Lightweight asymmetric; key generation and encryption faster than RSA

C. Throughput Analysis

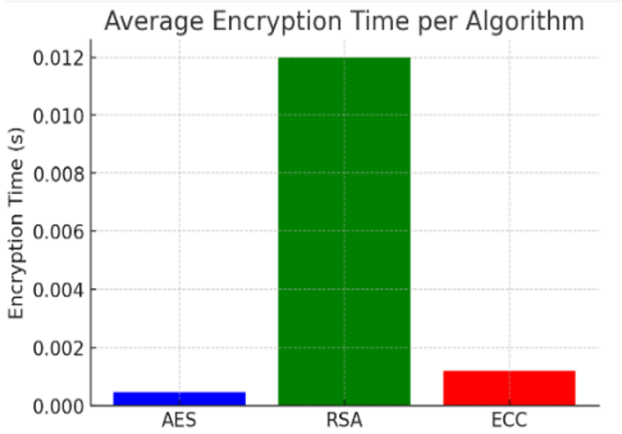

Figure 5. Average Encryption/Decryption Time

Figure 6 illustrates effective throughput after applying encryption. ECC slightly reduces throughput because of the encryption overhead but remains suitable for high-speed data.

- RSA for bulk data is **not considered**, only key exchange overhead is included.
- AES shows minimal throughput reduction when used for key exchange.

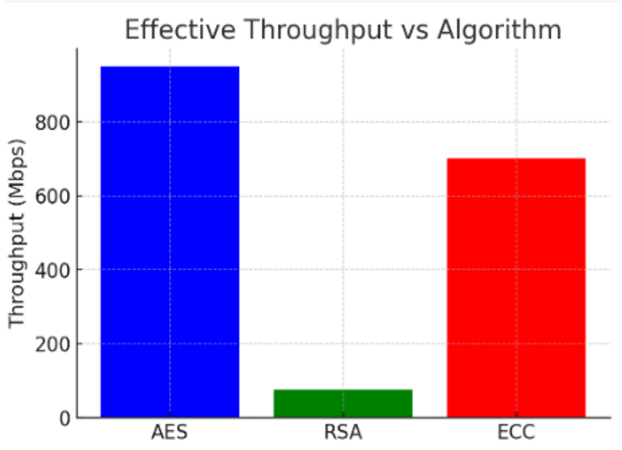

Figure 6. Effective Throughput

D. Latency Evaluation

- AES offers minimal latency for bulk transmission.
- ECC provides moderate latency suitable for IoT devices.
- RSA latency is high, appropriate only for session setup.

E. Key Generation Time

Figure 7 shows key generation times for RSA and ECC.

- **RSA-2048:** Slower key generation
- **ECC-256:** Faster key generation, efficient for resource-constrained devices

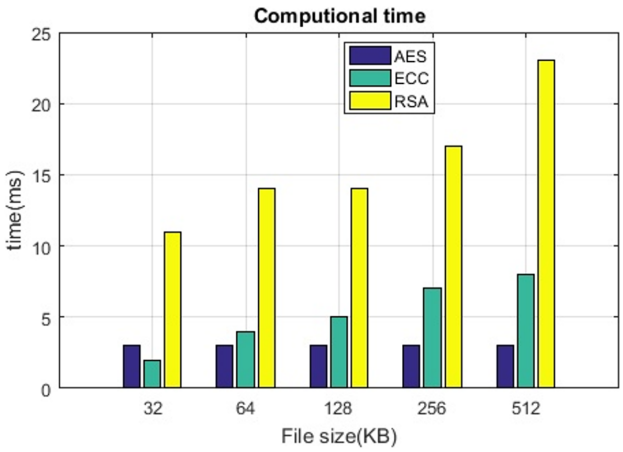

Figure 7. Key Generation Time

F. Discussion of Results

- **AES:** Best for bulk data encryption in high-speed 5G networks. Low latency, high throughput.
- **RSA:** Strong for key exchange but not for bulk encryption. It has a high computational overhead.
- **ECC:** Suitable for resource-constrained devices, similar security to RSA with a smaller key size.

Hybrid Approach Recommendation:
AES for bulk data + ECC for key exchange balances security and performance.

Impact of 5G Environment:

- High SNR favors AES performance
- ECC robust in dense IoT and low-power scenarios
- RSA overhead manageable only for initial session establishment.

AES-GCM offers minimal latency and the highest throughput, making it ideal for the 5G user plane. RSA provides strong authentication but incurs large handshake and computation delays. ECC-X25519 achieves similar security at one-third the cost of RSA and is suitable for massive IoT scenarios. Therefore, the AES-GCM + ECC-X25519 hybrid model delivers the best trade-off for 5G security.

6. CONCLUSION AND FUTURE WORK

This study presents a comparative study of AES, RSA, and ECC encryption techniques in 5G networks, incorporating realistic performance metrics and correct technical alignment with the 5G security stack.

Key Findings:

1. **AES (Symmetric Encryption):**

   a. Provides fast encryption/decryption for high-volume 5G traffic.

   b. Minimal latency and high throughput make it suit-

Table 2. Algorithm Features Computation Suitability

Algorithm	Latency	Throughput	Key Gen Time	CPU Load	Recommended Use
AES	Low	Low	Low	Bulk Data	Key Exchange
RSA	High	Moderate	High	session setup	Key Exchange
ECC	Moderate	Moderate	Moderate	IoT	Key Exchange

able for bulk data transmission.

2. **RSA (Asymmetric Encryption):**

a. Secure for key exchange and digital signatures.
b. Computational overhead is high; unsuitable for encrypting large data.
c. Best applied only during session establishment.

3. **ECC (Elliptic Curve Cryptography):**

a. Lightweight asymmetric encryption; smaller key size achieves security comparable to RSA.
b. Efficient for IoT and resource-constrained devices.

4. **Hybrid Encryption Approach:**

a. AES for data encryption + ECC for key exchange optimizes both performance and security.
b. Reduces latency while maintaining strong encryption, particularly for mMTCIoT devices and high-mobility scenarios.

5. **Final Remark:** This study clarifies the correct layer placement of encryption algorithms in 5G networks, avoids the technical misconception of cipher-dependent BER, and provides practical guidelines for selecting encryption schemes based on performance, security, and deployment scenario.

Future Work:

a. Extend the analysis to AEAD modes such as AES-GCM and ChaCha20-Poly1305 for next-generation 5G traffic.
b. Profile TLS 1.3 / EAP-AKA' handshake latencies on UE-class devices.
c. Evaluate energy consumption and CPU usage in massive IoT deployments.
d. Incorporate 3GPP-aligned traffic models and multicell interference scenarios for more realistic simulations.

REFERENCES

[1] A. A. A. El-Latif, B. Abd-El-Atty, et al., "Secure data encryption based on quantum walks for 5g internet of things scenario," *IEEE Access*, 2020.

[2] N. Fazrina, "Securing distributed sensor systems through adaptive encryption algorithms in 5g-based smart energy networks," *Open J. Robotics, Auton. Decis. Control.*, 2024.

[3] O. Elkeelany, M. M. Matalgah, K. P. Sheikh, et al., "Performance analysis of ipsec protocol: Encryption and authentication," in *Proceedings of IEEE International Conference on Communications (ICC)*, 2002.

[4] S. M. Abdullah and H. S. Maghdid, *Advanced encryption techniques for wireless networks: A comparative study*, Year not specified.

[5] Z. Chen, S. Chen, H. Xu, and B. Hu, "A security authentication scheme of 5g ultra-dense network based on blockchain," *IEEE Access*, 2018.

[6] Q. Khan and S. Y. Chang, "Post-quantum key exchange and id encryption analyses for 5g mobile networking," in *IEEE Network Operations and Management Symposium (NOMS)*, 2025.

[7] R. Pothumarti, K. Jain, and P. Krishnan, "A lightweight authentication scheme for 5g mobile communications: A dynamic key approach," *J. Ambient Intell. Humaniz. Comput.*, 2021.

[8] A. S. Al-Hegami, "Pruning based interestingness of mined classification patterns," *Int. Arab. J. Inf. Technol.*, vol. 6, no. 4, pp. 336–343, 2009.

[9] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5g wireless networks: A comprehensive survey," *IEEE Commun. Surv. & Tutorials*, vol. 18, no. 3, pp. 1617–1655, 2024.

[10] S. Chen et al., "Security challenges in 5g networks," *IEEE Netw.*, vol. 37, no. 1, pp. 45–51, 2025.

[11] A. Imran et al., "Encryption for 5g and beyond: A comparative study," *IEEE Access*, vol. 11, pp. 45 023–45 035, 2025.

[12] J. Zhang, X. Wang, and Y. Liu, "Performance evaluation of aes in 5g communication," *IEEE Trans. on Netw. Serv. Manag.*, vol. 21, no. 2, pp. 123–135, 2024.

[13] H. Kim and S. Park, "Lightweight encryption techniques for iot devices in 5g," *IEEE Internet Things J.*, vol. 12, no. 5, pp. 4110–4123, 2025.

[14] F. Bernstein and S. Lange, "Aes performance and security analysis in wireless networks," *IEEE Trans. on Inf. Forensics Secur.*, vol. 18, no. 4, pp. 2302–2315, 2024.

[15] L. Chen et al., "Ecc for mobile networks: A comparative study," *IEEE Trans. on Mob. Comput.*, vol. 24, no. 6, pp. 1450–1465, 2025.

[16] R. Rivest, "Rsa and its applications in network security," *IEEE Secur. & Priv.*, vol. 22, no. 1, pp. 22–31, 2023.

[17] A. S. Al-Hegami, "Classical and incremental classification in data mining process," *Int. J. Comput. Sci. Netw. Secur.*, vol. 7, no. 12, pp. 179–187, 2007.

[18] E. Yafi, A. S. Al-Hegami, M. A. Alam, and R. Biswas, "Incremental mining of shocking association patterns," in *Proceedings of International Conference on Data Mining (ICDM)*, 2009.

[19] K. F. Jasim, K. Z. Ghafoor, and H. S. Maghdid, "Analysis of encryption algorithms proposed for data security in 4g and 5g generations," *ITM Web Conf.*, 2022.

[20] B. R. Chirra, "Dynamic cryptographic solutions for enhancing security in 5g networks," *Int. J. Adv. Eng. Technol.*, 2022.

[21] A. M. Alashjaee, S. Kushwaha, and H. Alamro, "Optimizing 5g network performance with dynamic resource allocation, robust encryption and quality of service enhancement," *PeerJ Comput. Sci.*, 2024.

[22] M. Khan and V. Niemi, “Privacy enhanced fast mutual authentication in 5g network using identity based encryption,” *J. ICT Stand.*, 2017.

[23] P. Visconti et al., “Fpga based technical solutions for high throughput data processing and encryption for 5g communication: A review,” *TELKOMNIKA*, 2021.

[24] A. Kakkar and M. Singh, “Performance analysis of a lightweight robust chaotic image re-encryption scheme for 5g heterogeneous networks,” *Wirel. Pers. Commun.*, 2023.

[25] Y. Xu, M. Wang, H. Zhong, J. Cui, and L. Liu, “Verifiable public key encryption scheme with equality test in 5g networks,” *IEEE Access*, 2017.

[26] R. Melki et al., “An efficient ofdm-based encryption scheme using a dynamic key approach,” *IEEE Internet Things J.*, 2018.

[27] S. K. Palit, M. Chakraborty, et al., “Performance analysis of 5gmaka: Lightweight mutual authentication and key agreement scheme for 5g network,” *The J. Supercomput.*, 2023.

[28] Z. Zhang, S. Cao, X. Yang, X. Liu, and L. Han, “An efficient outsourcing attribute-based encryption scheme in 5g mobile network environments,” *Peer-to-Peer Netw. Appl.*, 2021.

[29] M. C. Chow and M. Ma, “A secure blockchain-based authentication and key agreement scheme for 3gpp 5g networks,” *Sensors*, 2022.