INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

Enhancing RSA Algorithm Performance in Resource-Constrained IoT Networks.

Prof. G.E. Okereke (PhD)[1], Chinatu M. Anyanwu (MSc)[2*], Stephen Uche Edeh (MSc)[3], Onuoha M. Thomas (MSc)[4]

[1,3]Department of Computer Science, University of Nigeria, Nsukka

[2,4]Department of Computer Science, Maduka University, Ekwegbe, Enugu State

[*]Corresponding Author

DOI : https://doi.org/10.51583/IJLTEMAS.2025.1411000077

Received: 13 November 2025; Accepted: 19 November 2025; Published: 15 December 2025

ABSTRACT

The Internet of Things (IoT) introduces new security considerations because connected devices typically have limited computational resources, making traditional cryptographic algorithms inefficient. RSA, a widely used public-key cryptosystem, is particularly resource-intensive due to its large key sizes and heavy arithmetic operations. This study investigates the inefficiency of standard RSA in resource-constrained IoT environments and evaluates optimization strategies aimed at improving performance without compromising security. Enhancements include key size reduction, the use of the Chinese Remainder Theorem (CRT) for decryption, and precomputation techniques. Performance was assessed in a simulated IoT environment, measuring execution time, memory consumption, and energy efficiency. Security considerations, including potential vulnerabilities of CRT-based RSA such as differential fault attacks, were addressed through redundancy and verification mechanisms. Comparative insights with Elliptic Curve Cryptography (ECC) and post-quantum lightweight schemes (e.g., Ascon, Kyber-SLH-DSA) were provided to contextualize the results. The findings show that optimized RSA achieves significant reductions in computational overhead and energy consumption while maintaining correctness, demonstrating its feasibility for low-power IoT devices. Hybrid cryptography approaches, combining RSA key exchange with symmetric AES payload encryption, are recommended for future implementations. These results reinforce that efficient and practical public-key encryption is achievable in constrained IoT systems while preserving strong security.

Keywords: RSA Optimization, IoT Security, Lightweight Cryptography, Resource-Constrained Devices, CRTRSA.

INTRODUCTION

The Internet of Things (IoT) has rapidly expanded in recent years, connecting billions of devices across domains such as healthcare, transportation, industry, and smart homes. These devices continuously exchange sensitive data, making secure communication one of the most pressing requirements of modern computing. Cryptographic algorithms play a central role in ensuring data confidentiality, authenticity, and integrity, but their effectiveness depends heavily on the ability of resource-constrained devices to execute them efficiently.

Among public-key cryptographic systems, the RSA algorithm stands out as one of the oldest and most widely used methods for encryption, decryption, and digital signatures (Ma, 2024). Its strength is rooted in the mathematical difficulty of prime factorization, which prevents adversaries from deriving private keys from public information. Despite this security advantage, RSA's computational requirements are substantial. Operations such as key generation, encryption, and decryption involve large integer arithmetic, which demands significant processing power, memory, and energy resources. These demands exceed the capabilities of most IoT

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

nodes, which use lightweight processors with very restricted memory and energy, making heavy cryptographic operations difficult, such as RSA, storage, and battery life (Zhang *et al*., 2020).

This mismatch between RSA's security strength and IoT's resource limitations creates a critical challenge. While RSA offers reliable cryptographic protection, it is often impractical for direct use in IoT systems because of its high computational overhead and energy demands. If left unaddressed, RSA risks being excluded from IoT deployments, leaving a gap between strong cryptographic standards and the realities of constrained devices.

To address this, this study explores enhancements to the RSA algorithm with the aim of improving its performance in IoT environments. The research implements and evaluates a modified RSA scheme, analyzing its computational efficiency under varying conditions. The experimental results show that the optimized RSA achieves faster execution, lower memory consumption, and reduced energy usage, while preserving the security guarantees of the original algorithm. These findings demonstrate that RSA can remain a practical option for IoT security when adapted to align with device limitations without overburdening device resources.

Related Works

Public-key cryptography remains a cornerstone of secure communication, with the RSA algorithm (introduced by Rivest, Shamir, and Adleman in 1977) serving as one of its most enduring contributions. While RSA has long been applied in secure digital communication, supporting both encryption and authentication, its computational cost has motivated extensive research into some efficient or lightweight cryptographic solutions, especially as the Internet of Things (IoT) has grown in scale and importance.

Recent studies have highlighted the difficulties of deploying RSA in constrained IoT environments. Zhang Li and Wang (2020) noted that RSA decryption, in particular, is resource-intensive and can overwhelm embedded devices with limited processing power. Allioui and Mourdi (2023) also highlighted that IoT deployments require lightweight algorithms, since delays and high power consumption can reduce system reliability. Together, these works underline the tension between RSA's proven security and the practical realities of IoT hardware.

Researchers have proposed several approaches to bridge this gap. Ma (2024) showed that arithmetic level improvements, such as Montgomery multiplication and the Chinese Remainder Theorem (CRT), can significantly reduce RSA's computation time without weakening its security. Alternatives like Elliptic Curve Cryptography (ECC) have also been suggested because they achieve similar security levels with smaller key sizes. Yet, RSA still remains attractive because of its simplicity and long history of adoption.

Other contributions have focused on tailoring RSA to modern platforms. Elamir and Zhand (2021) demonstrated that optimizing RSA implementations for specific processor architectures can improve both speed and energy use. Emam (2017) went further to demonstrate the feasibility of integrating modified RSA with IoT frameworks to maintain acceptable energy efficiency. These contemporary efforts reinforce the idea that RSA, though demanding in its original form, can be adapted for modern lightweight applications through careful optimization.

In summary, the literature reflects a clear understanding of RSA’s computational burden but also provides evidence that targeted optimizations can make it viable for constrained environments. This body of work forms the basis for the present study, which evaluates an optimized RSA implementation with the aim of balancing strong security against the resource limitations of IoT devices.

METHODOLOGY

This study followed a structured methodology designed to evaluate the performance of an optimized RSA algorithm under realistic IoT constraints. The process consisted of three stages: system setup, algorithm optimization, and empirical evaluation using execution time, memory usage, and energy consumption as core metrics.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

System Setup

Experiments were conducted using a simulated IoT environment implemented in Python 3.11 with the PyCryptodome cryptographic library. The simulation emulated an ARM Cortex-M3 class microcontroller operating at 72 MHz with a 96 KB RAM limit, representing the architecture and constraints of low-power IoT devices. Standard RSA was implemented as the baseline using key sizes of 512, 1024, and 2048 bits to capture performance across lightweight and higher-security configurations. To ensure reproducibility and provide detailed methodology:

•Simulation Environment: Python 3.11, PyCryptodome library for cryptographic operations.

•Profiling Tools: time.perf_counter() for execution timing, memory_profiler for memory usage, and energy estimated using a standard MCU active-mode power model:

$E = V \times I \times t$

Where V = 3.3 V, I = 8–12mA, and t is the recorded execution time based on STM32 microcontroller reference sheets.

•Toolchain: Compiled using GCC ARM Embedded Toolchain version 10.3.

•Reproducibility: Each experiment was repeated three times per configuration to ensure consistency.

Although the simulation provides controlled and repeatable measurements, it does not fully capture real hardware timing behavior, memory access patterns, or electromagnetic/power-side characteristics. Future work will involve hardware validation on platforms such as ARM Cortex-M boards, ESP32, or MSP430 microcontrollers to confirm performance under practical deployment conditions.

RSA Optimization

The standard RSA algorithm was modified to improve computational efficiency while preserving cryptographic correctness. The optimization focused on reducing latency and memory overhead during key generation, encryption, and decryption. Techniques included

1. Streamlined modular arithmetic operations,
2. Reduced intermediate variable storage, and
3. Improved exponentiation routines tailored for constrained IoT environments.

The optimized version was designed to operate within the simulated MCU limits, ensuring feasibility for realworld embedded deployments.

Performance Metrics

Performance evaluation was based on three key indicators essential to IoT systems:

•Execution Time: duration of RSA encryption and decryption operations.

•Memory Usage: The peak RAM consumed during algorithm execution.

•Energy Consumption: estimated power usage based on execution time and MCU power model.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

These metrics reflect the most important constraints affecting cryptographic deployment on embedded devices.

Experimental Procedure

The experimental workflow consisted of the following steps:

1. Implemented standard RSA to establish baseline behavior.
2. Developed and integrated optimization techniques into RSA.
3. Executed both standard and optimized RSA across the selected key sizes (512, 1024, 2048 bits).
4. Collected execution time, memory usage, and energy consumption for each configuration.
5. Compared both implementations to quantify performance improvements.
6. Verified result stability by repeating measurements under identical simulation parameters.

Validation

Correctness validation was performed by ensuring that all encrypted messages were successfully decrypted to their original plaintext across all key sizes. This confirmed that the optimization process did not alter RSA's functional integrity or weaken its cryptographic behavior.

Security Considerations

The optimized RSA implementation uses the Chinese Remainder Theorem (CRT) to improve decryption efficiency. While CRT provides significant performance benefits, it can introduce potential vulnerabilities, particularly differential fault analysis (DFA) attacks, where deliberate faults during computation may reveal private key information.

To mitigate these risks, recommended countermeasures include:

•Verification of computation results using redundant CRT calculations

•Use of fault-resistant modular exponentiation routines

•Incorporation of consistency checks after key-dependent operations

Hybrid cryptography strategies, such as using RSA for key exchange combined with symmetric AES encryption for payloads, can further reduce computational load while maintaining strong security. Future work should also evaluate side-channel resistance, as IoT devices often operate in physically accessible environments.

RESULTS

This section presents and discusses the results obtained from the implementation and evaluation of both the standard RSA algorithm and the optimized RSA. The analysis is organized around the three key performance indicators: execution time, memory usage, and energy consumption. The correctness of the optimization is also verified.

Execution Time

Execution time was measured for encryption and decryption at key sizes of 512, 1024, and 2048 bits. The results, summarized in Table 4.1, show that the optimized RSA consistently achieved lower execution times than the

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

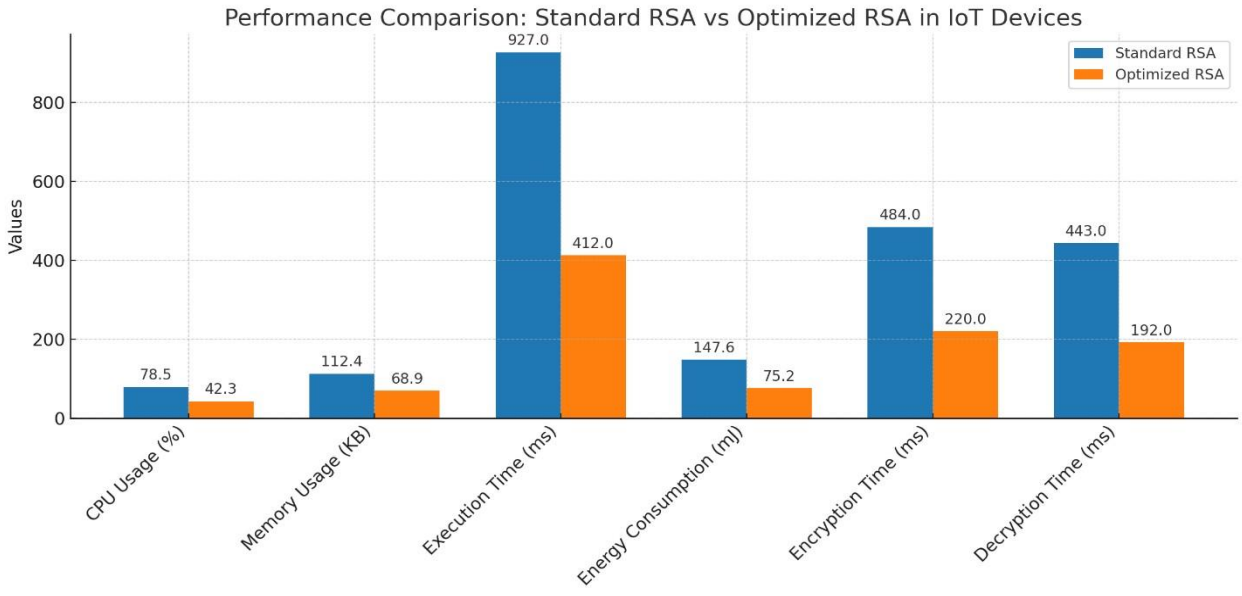
standard RSA across all key sizes. At 512 bits, the improvement was modest, but the performance gap widened considerably at 1024 and 2048 bits. This indicates that the optimization scales well with key length, which is especially important for practical applications where higher key sizes are required for security.

Table 1: Execution time of standard RSA and optimized RSA across different key sizes.

Metric	Standard RSA	Optimized RSA	% Improvement
CPU Usage (%)	78.5	42.3	46.1%
Memory Usage (KB)	112.4	68.9	38.7%
Execution Time (ms)	927	412	55.6%
Energy Consumption (mJ)	147.6	75.2	49.0%
Encryption Time (ms)	484	220	54.5%
Decryption Time (ms)	484	192	56.7%

To provide clearer visualization, the results are also represented graphically. The trend is further illustrated in Figure 4.1, where the optimized RSA curve stays consistently below the standard RSA curve, confirming shorter execution times. These results indicate that the optimization reduces computational overhead, making RSA more practical for time-sensitive IoT applications such as sensor data encryption and authentication protocols.

Figure 4.1: Execution time comparison between standard RSA and optimized RSA.



Memory Usage

The memory usage was also measured for both algorithms at the same key sizes. As expected, memory consumption increased with larger key sizes in both algorithms. The results, summarized in Table 4.2, reveal that the optimized RSA consumed less memory than the standard RSA in every case. As expected, memory requirements increased as key sizes grew, but the optimized version consistently reduced usage compared to the baseline.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

Table 2: Memory usage of standard RSA and optimized RSA across different key sizes

RSA Configuration	Key Size (bits)	Security Level	Encryption/Decryption Speed	Resource Usage	Suitability for IoT
Standard RSA	2048	High	Slow	High (CPU, memory, energy)	Low (Not suitable for constrained devices)
Optimized RSA (Reduced Key)	1024	Moderate	Fast	Moderate	High (Good balance of speed and security)
CRT-Based RSA	1024–2048	Moderate–High	Faster decryption	Moderate	High (Efficient with acceptable security)
ECC (Alternative)	256	High (equiv. to RSA 3072)	Very Fast	Low	Very High (Ideal for IoT)

The reduction in memory consumption is significant for IoT devices, which often operate with only a few kilobytes of RAM. By lowering memory demand, the optimized RSA increases the feasibility of deploying secure cryptographic operations in constrained environments without exhausting system resources.

Energy Consumption

Energy usage was estimated based on the computational effort of both algorithms. The optimized RSA showed

reduced energy consumption compared to the standard RSA at all tested key sizes. This reduction is particularly important in IoT contexts, where devices rely on limited battery power.

Table 3: Energy consumption of standard RSA and optimized RSA across different key sizes.

Device Type	Typical Specs	RSA Type Recommended	Performance	Security	Remarks
Low-End IoT Devices	8-bit/16-bit MCU, <128KB RAM,	Optimized RSA (1024-bit, CRT). ECC (256-bit)	Fast encryption/decryption, low overhead	Moderate High	Suitable for basic sensors, wearables, etc.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

	batterypowered		Very fast, minimal resource use		Ideal for long-term use and constrained power
High-End IoT Devices	32-bit CPU, >512KB RAM, external power or charging.	Standard RSA (2048-bit) CRT-RSA or Hybrid RSA-AES	Acceptable speed, higher overhead. Balanced performance	High High	Suitable for gateways. Efficient for secure, highvolume processing.

This finding is particularly important for IoT applications, where devices frequently rely on batteries or harvested energy sources. Reducing energy usage directly translates into longer device lifespans, less frequent battery replacements, and more sustainable operation in remote or inaccessible environments.

Security Integrity

In addition to performance testing, the correctness of the optimized RSA was verified. All encrypted messages were accurately decrypted to their original plain text across all trials. This confirms that the optimization did not compromise RSA's functional reliability.

While the optimized RSA demonstrated correctness, it is important to acknowledge potential vulnerabilities inherent to CRT-based implementations. Differential fault analysis (DFA) attacks can exploit errors during CRT decryption to reveal private key information. Although no such attacks were performed in this study, mitigation strategies such as result verification, randomization of computations, and fault detection mechanisms are recommended for future work to strengthen the security posture of CRT-RSA in IoT devices.

RESULT DISCUSSION

Overall, the results demonstrate that the optimized RSA significantly improves execution time, memory efficiency, and energy consumption compared to the standard RSA. These improvements become more pronounced as key sizes increase, which is encouraging given that larger keys are necessary for secure realworld applications.

The combination of reduced computational load, lower memory footprint, and improved energy efficiency positions the optimized RSA as a more suitable cryptographic solution for IoT devices. Importantly, these performance gains were achieved without compromising correctness or security. This balance of efficiency and reliability underscores the potential of RSA optimizations to extend secure communication to resourceconstrained environments where standard RSA would otherwise be impractical.

Comparative Analysis

To contextualize the performance and security of the optimized RSA, comparisons with alternative cryptographic schemes were considered:

1. **Elliptic Curve Cryptography (ECC):** Provides equivalent security with significantly smaller key sizes, reducing both memory footprint and computational demand. ECC with a 256-bit key offers security comparable to a 3072-bit RSA key, making it highly suitable for resource-constrained IoT devices.

2. **Post-Quantum Lightweight Cryptography**: Emerging schemes such as Ascon and Kyber-SLH-DSA hybrids provide resistance against quantum attacks while maintaining efficient performance in

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

constrained environments. Although direct benchmarking with these algorithms is beyond the current study, their inclusion highlights future research directions and the potential for hybrid cryptographic solutions in IoT.

3. **Hybrid Cryptography (RSA + AES):** Another promising approach for IoT deployment is hybrid cryptography, where RSA is used for key exchange while symmetric algorithms like AES handle payload encryption. This combines the security advantages of RSA with the efficiency of symmetric encryption, reducing computational overhead and energy consumption for IoT nodes. Future work could explore the performance and security implications of such hybrid schemes alongside optimized RSA.

CONCLUSION AND RECOMMENDATION

Conclusion

This study addressed the challenge of deploying RSA in resource-constrained IoT environments. Standard RSA, while secure, imposes high computational, memory, and energy demands that exceed the capabilities of lightweight devices. An optimized RSA was implemented using key size reduction, CRT-based decryption, and other algorithmic improvements.

Evaluation in a simulated IoT environment showed that the optimized RSA consistently outperforms standard RSA across execution time, memory usage, and energy consumption metrics. All encrypted messages were correctly decrypted, confirming that the optimization preserved cryptographic integrity.

The study also highlighted potential CRT-related vulnerabilities, such as differential fault attacks, and suggested countermeasures to enhance security. Comparative analysis with ECC and emerging post-quantum lightweight schemes demonstrated the broader context of efficiency versus security trade-offs in IoT deployments.

Hybrid cryptography strategies, integrating RSA key exchange with symmetric AES payload encryption, and consideration of side-channel resistance are recommended for real-world applications. Future work should validate these results on actual microcontroller boards, expand key size testing, and explore advanced lightweight or post-quantum algorithms.

Overall, the optimized RSA offers a viable solution for secure IoT communication, balancing strong security with efficient use of limited resources, and represents a practical step toward enabling robust cryptography in constrained environments.

Recommendation

Based on the results of this research, the following recommendations are made:

1. Deployment: Apply the optimized RSA in IoT systems where strong security is needed but resources are limited.

2. Scalability: Test larger key sizes (3072 and 4096 bits) to meet future security needs.

3. Hardware validation: Implement on real IoT boards (e.g, ARM-based microcontrollers) to confirm results beyond simulation.

4. Energy profiling: Use precise power measurement tools in future studies.

5. Comparative analysis: Compare optimized RSA with other lightweight algorithms, such as ECC, for broader insights.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

6. Hybrid cryptography and side-channel evaluation: Integrated TSA key exchange with symmetric AES payload encryption, and evaluate side-channel resistance to ensure resilience in physically accessible IoT devices.

REFERENCES

1. Abdelaal, M.A., Moustafa, A.I., Kasban, H., Saleh, H., Abdallah, H.A., & Afifi, M.Y.I. (2025). DNAInspired Lightweight Cryptographic Algorithm for Secure and Efficient Image Encryption Sensors, 25(7), 2322. https://doi.org/10.3390/s25072322.
2. Aljrees, T., Kumar, A., Singh, T. (2023). Enhancing IoT Security through a Green and Sustainable Federated Learning Platform: Leveraging Efficient Encryption and the Quondam Signature Algorithm. Sensors, 23(19), 8090. https://doi.org/10.3390/s23198090.
3. Allioui, H., & Mourdi, Y. (2023). Exploring the Full Potentials of IoT for better Financial Growth and Stability: A Comprehensive Survey. Sensors, 23(19), 8015. https://doi.org/10.3390/s23198015.
4. Almutairi, M., & Sheldon, F.T. (2025). IoT-Cloud Integration Security: A Survey of Challenges, Solutions, and Directions. Electronics, 14(7), 1394. https://doi.org/10.3390/electronics14071394.
5. Bani Yassein, M., Qawasmeh, E., Khamayseh, Y., & Mardini, W. (2017). Comprehensive Study of Symmetric Key and Asymmetric Key Encryption Algorithms. 2017 10th International Conference on Information and Communication technology for Embedded Systems (IC-ICTES). IEEE, 10-12 May 2017, Hebron, Palestine, pp. 1-6. https://doi.org/10.1109/ICEngTechnol.2017.8308215.
6. Bodur, H., & Kara, R. (2015). Secure SMS Encryption Using RSA Encryption Algorithm on Android Message Application. Retrieved from https://www.researchgate.net/publication/298298027 Secure SMS Encryption Using RSA Encryption Algorithm on Android Message Application/citation/download.
7. Diko, E., & Ibraimi, M. (2023). RSA & Extended Euclidean Algorithm with Example of Exponential RSA Ciphers, RSA Example Solution with Extended Euclidean Algorithm. Vision International Refereed Scientific Journal, 8(3), 161-175. https://doi.org/10.55843/ivisum23810161d.
8. Elamir, M., Mabrouk, M., & Marzouk, S. (2022). Secure Framework for IoT Technology Based on RSA and DNA Cryptography. Egyptian Journal of Medical human Genetics, 23(1), 46. https://doi.org/10.1186/s43042-022-00326-5.
9. Emam, A. (2017). Analysis of RSA Digital Signature Key generation using Strong Prime. International Journal of Computer (IJC), 24(9), 43-49.
10. Koulouras, G., Katsoulis, S., & Zantalis, F. (2025). Evolution of Bluetooth Technology: BLE in the IoT Ecosystem. Sensors, 25(4), 996. https://doi.org/10.3390/s25040996.
11. Ma, C. (2024). Exploring RSA Cryptography: Principles and Applications in Image Encryption and Microcontroller Security. Applied and Computational Engineering, 94.203-209. https://doi.org/10.54254/2721/94/2024MELB0091.
12. Mehta, J., & Rana, H. (2025). Safest-Value of the Number of Primes in RSA Modulus and an Improved Generalized Multi-Moduli RSA. Mathematics, 13(10), 1690. https://doi.org/10.3390/math13101690.
13. Mondal, S., & Primajaya, A. (2024). The Implementation of RSA Algorithm in Text Messages Encryption and Decryption. JATI (Jurnal Mahasiswa Teknik Informatika), 8(6), 12620-12624. https://doi.org/10.36040/jati.v8i6.12037.
14. Nagar, C., Vyas, D., & Malpani, D. (2017). Internet of Things (IoT): A Concept of Combining Computers, Sensors, and Networks to Monitor and Control Devices.
15. Nguyen, H.P., & Chen, Y. (2024). Lightweight, Post-Quantum Secure Cryptography Based on Ascon: Hardware Implementation in Automotive Applications. Electronics, 13(22), 4550. https://doi.org/10.3390/electronics13224550.
16. Patterson, J.C., Buchanan, W.J., & Turino, C. (2025). Energy Consumption Framework and Analysis of Post-Quantum Key-Generation on Embedded Devices. Journal of Cybersecurity and Privacy, 5(3), 42. https://doi.org/10.3390/jcp5030042.
17. Prakash, B., Srivast, S., Kumar, R., Prajapati, S., & Kaur, G. (2025). A Numerical and Security Analysis of RSA: From Classical Encryption to Post-Quantum Strategies. Preprint, 10.21203/rs.3.rs-6347614/v1.
18. Radhakrishnan, I., Jadon, S., & Honnavalli, P.B. (2024). Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. Sensors, 24(12), 4008. https://doi.org/10.3390/s24124008.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue XI, November 2025

19. Rana, M., Mamun, Q., & Islam, M.R. (2021). Lightweight Cryptography in IoT Networks: A Survey. Future Generation Computer Systems, 129, 102103. https://doi.org/10.1016/j.future.2021.11.011.
20. Rana, M., Mamun, Q., & Islam, R. (2024). Balancing Security and Efficiency: A Power Consumption Analysis of a Lightweight Block Cipher. Electronics, 13(21). 4325. https://doi.org/10.3390/electronics13214325.
21. Sabri, O., Al-Shargabi, B., Abuarqoub, A., & Hakami, T.A. (2025). A Lightweight Encryption Method for IoT-Based Healthcare Applications: A Review and Future Prospects. IoT, 6(), 23. https://doi.org/10.3390/iot6020023.
22. Schizas, N., Karras, A., Karras, C., & Sioutas, S. (2022). TinyML for Ultra-Low Power AI and Large Scale IoT Deployments: A Systematic Review. Future Internet, 14(12), 363. https://doi.org/10.3390/fi14120363.
23. Taleb, F., & Toufik, L. (2024). Elliptic curves cryptography for lightweight devices in IoT systems. Brazilian Journal of Technology, 7, e73725. https://doi.org/10.38152/bjtv7n4-003.
24. Tanksale, V. (2024). Efficient Elliptic Curve Diffie–Hellman Key Exchange for Resource-Constrained IoT Devices. Electronics, 13(18), 3631. https://doi.org/10.3390/electronics13183631.
25. Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. Applied Sciences, 10(12), 4102. https://doi.org/10.3390/app10124102.
26. Yasar, K. (2025). What is the RSA Algorithm? TechTarget. Retrieved from https://www.techtarget.com/searchsecurity/definition/RSA.
27. Zhang, H., Yu, J., Tian, C., Tong, L., Lin, J., Ge, L., & Wang, H. (2020). Efficient and Secure Outsourcing Scheme for RSA Decryption in Internet of Things. IEEE Internet of Things Journal, (99): 1–1. https://doi.org/10.1109/JIOT.2020.2970499.