

Cryptographic framework for secure data transmission in IoT networks using lightweight hybrid encryption

Pallavi D. Deshpande [#]

Gauri V. Ghule [†]

Department of Electronics and Telecommunication Engineering

Vishwakarma Institute of Technology

Pune 411048

Maharashtra

India

Manasi Ghamande [§]

Department of Engineering Science and Humanity

Vishwakarma Institute of Technology

Pune 411048

Maharashtra

India

Ketki Kshirsagar [‡]

Department of Electronics and Telecommunication Engineering

Vishwakarma Institute of Technology

Pune 411048

Maharashtra

India

Sandeep V. Gaikwad [@]

Department of Electronics and Telecommunication Engineering

SCTR's Pune Institute of Computer Technology

Pune 411043

Maharashtra

India

[#] E-mail: pallavi.deshpande@vit.edu

[†] E-mail: gauri.ghule@vit.edu

[§] E-mail: manasi.ghamande@vit.edu

[‡] E-mail: ketki.kshirsagar@vit.edu

[@] E-mail: svgaikwad@pict.edu

Rahul S. Pol *

*Department of Electronics and Telecommunication Engineering
Vishwakarma Institute of Technology
Pune 411048
Maharashtra
India*

Abstract

As the Internet of Things (IoT) continues to grow at an exponential rate, securing the transmission of data among various types of heterogeneous resources with limited capacity has become more challenging than ever before. To address this challenge, we propose a lightweight cryptographic framework that integrates optimized symmetric and asymmetric encryption algorithms and secure communication protocols, which can significantly enhance the security of IoT communications. Specifically, we describe an architecture for our new cryptographic framework that utilizes AES-128 and ECC-based key exchanges combined with dynamic tokenization and hashing for integrity verification - to provide confidentiality, authentication, and integrity of the communicated data. In addition, our experimental results show that more than double (37%) the cryptographic throughput compared to other traditional methods; over 22% less memory overhead than traditional methods; and 19% less energy consumed to process the same amount of data as traditional methods. Furthermore, the system reduces the potential for man-in-the-middle and spoofing attacks by 46% when using secure MQTT or HTTPS basis of transmission layers within the overall architecture.

Subject Classification: 94A60.

Keywords: *Lightweight cryptography, Secure IoT communication, AES-ECC hybrid encryption, Secure data transmission, Network security protocols.*

1. Introduction

There has been a rapid growth in Internet of Things (IoT) connectivity, leading to many difficulties protecting the secure transmission of data across large networks composed of various types of devices and systems with limited resources. This paper describes a cryptography framework that uses symmetric and asymmetric encryption techniques, as well as optimizations for developing scalable, distributed, energy-efficient, and secure architectures for IoT devices. Each of these optimization improvements is designed to achieve the greatest possible degree of security while still offering the required performance in an IoT environment; it discusses the metrics used to measure security and overall performance goals. In addition, given the complexity and sophistication of current cyber-terrorist organizations, it will become even more difficult to provide adequate protection against such threats as man-in-the-middle attacks;

* E-mail: rahul.pol@vit.edu (Corresponding Author)

device spoofing; eavesdropping; replay attacks; and botnet attacks. The traditional method of securing data through the use of static credentials and centralised trust models is not an appropriate way to provide security due to the constantly changing, high availability and distributed nature of the IoT system. As a result, IoT networks are becoming increasingly exposed to advanced types of cyber attacks, including man-in-the-middle attacks, counterfeit devices, eavesdropping, replay attacks, and attacks using botnets. To counteract these vulnerabilities, modern IoT security needs to employ modern cryptographic techniques coupled with secure communication protocols.

Currently, regulatory agencies like CERT-In and MeitY issue information security mandates, although compliance is inconsistent, especially when it comes to heterogeneous and resource-limited IoT scenarios. In order to solve some of these problems, there is an immediate need for an integrated lightweight, scalable, and reliable cryptosystem and networking security framework that will offer effective encryption, dynamic key management, reliable authentication, and secure communication protocols with a minimal overhead of computation and energy consumption. An overall level of protection requires an integrated approach both at the cryptographic level as well as the network level, therefore creating a trusted and sustainable IoT ecosystem.

2. Literature Survey

The rapid development of quantum computing has created significant challenges for conventional cryptographic systems, particularly those based on integer factorization and discrete logarithm problems. Post-quantum cryptography (PQC) has therefore emerged as an important research direction for developing cryptographic mechanisms that remain secure against both classical and quantum adversaries. Bernstein and Lange [1] discussed the evolving state of post-quantum cryptography and emphasized the need for migration strategies capable of mitigating the threat posed by large-scale quantum computers. Bos et al. [2] presented CRYSTALS-Kyber, a module-lattice-based key encapsulation mechanism (KEM) designed to provide security against adaptive chosen-ciphertext attacks. Similarly, Hülsing et al. [3] investigated high-speed key encapsulation based on NTRU, demonstrating that structured lattice problems can support efficient cryptographic operations. Ravi et al. [4] investigated electromagnetic (EM)-based physical attacks against lattice-based public-key encryption and KEM implementations. Mulani and Mane [5] proposed an image authentication approach combining watermarking and cryptography on a reconfigurable platform. Their results emphasized the importance of reducing hardware resource utilization while maintaining cryptographic functionality [6].

Soni and Mishra [7] studied hybrid TLS incorporating post-quantum key exchange for IoT edge gateways. Alkim et al. [8] investigated post-quantum key exchange through the NewHope scheme and demonstrated the feasibility of lattice-based key establishment. Banerjee, Das, and Ghosh [9] proposed

lightweight authenticated encryption for constrained IoT devices using the Keccak sponge construction. Patel and Gupta [10] investigated the performance of post-quantum cryptographic algorithms on RISC-V embedded processors. Similarly, Kumar and Rao [12] investigated FPGA acceleration of post-quantum NTRU polynomial operations using number theoretic transforms (NTTs). Wang, Chen, and Liu [11] proposed graph-based hierarchical key management using elliptic-curve pairings.

Salunkhe et al. [13] investigated secure image transmission using chaotic encryption and discrete wavelet transform (DWT) watermarking on a reconfigurable platform. Investigated the bit-error-rate performance of different error-correction codes using concatenated Reed–Solomon and convolutional coding. Investigated area-optimized implementation of the Advanced Encryption Standard (AES) on FPGA. Their study focused on reducing hardware resource utilization while retaining the security and functionality of AES. In an earlier work, presented an efficient FPGA implementation of AES and examined hardware-oriented optimization. These studies demonstrate the continuing importance of architectural optimization for cryptographic algorithms.

3. Methodology

The proposed approach for developing a Hybrid Lightweight Cryptographic Framework incorporates low computational / energy overhead requirements during the execution of confidentiality, integrity, authentication, secure communications, and adaptive network security mechanisms specifically designed for data processing on embedded IoT nodes.

3.1 *Multi-Phase Lightweight Encryption Model*

This framework uses a Multi-Phase cryptographic transformation model to encrypt data during transmission in IoT networks, thereby enhancing the confidentiality of the transmitted data. During the first phase, the plaintext data is divided into small bit-sized segments (blocks) and subjected to a non-linear substitution transformation based on the use of an adaptive S-Box transformation, followed by an additional Hamming Distance Equalization mechanism, which ensures that all data blocks have uniform entropy (randomness) using an equal distribution of Hamming distances, thereby reducing the potential for statistical leakage and increasing resistance to linear and differential cryptanalysis. The second phase of the proposed encryption framework utilizes a state-aware diffusion process, where traditional methods of permutation and diffusion are dynamically selected based on real-time indicators of the level of entropy present during the transmission of the data. The combination of both substitution and adaptive diffusion processes provides a strong level of confusion and diffusion properties required for securely

3.2 Dynamic Key Management and Cryptographic Agility

To improve the security of key management in distributed IoT networks, the framework implements a dynamic key creation and evolution method. The round keys generated for the encryption processes for each encryption round are based on a hybrid method that uses the base crypto seed and pseudo-random entropy (in the form of noise-extracted) from chaotic processes. This means the key will have temporal variability with respect to how they will be generated and therefore will have a greater sensitivity to the keys and be more resistant to replay, brute-force, or algebraic attacks.

3.3 Secure Data Transmission over IoT Networks

The proposed approach also incorporates the use of secure network communication protocols in addition to encryption to protect information while it is being transmitted over heterogeneous IoT architectures. The encrypted data will be transmitted by: Using MQTT protocol over the TLS protocol for lightweight publish-subscribe communication Using HTTPS protocol for secure communications for reliable device-to-cloud communication These protocols provide: End-to-end encryption Protection of session establishment Protection against eavesdropping/man-in-the-middle.

3.4 Integrity Assurance and Secure Packet Verification

A Hash-Chain Method has been designed into the Framework, which creates a hash for each data packet that is sent over the network. The hashes of the packets ensure that the packets have not been changed in transit, as they link each transmitted packet with the hash of the previous transmitted packet; thus creating a chain of hashes between all transmitted packets. The receiver can detect if a packet was modified in transit by checking the hash of each packet against the hash calculated for each packet as it received.

$$H_i = Hash(D_i || H_{i-1}) \text{ --- Eq. 1}$$

$$H_i = Hash(D_i || H_{i-1}) \text{ --- Eq. 2}$$

This ensures: Improved tampering detection capabilities. Ability to verify the authenticity of data. Ability to prevent packet injection attacks.

3.5 Implementation for Resource Constrained IoT Devices

The entire framework has been designed so that it will work on resource constrained IoT devices by taking into consideration: Minimal memory footprint (no large lookup tables) in equation 1 and 2. Support for small block sizes Low computational complexity (8-bit to 32-bit microcontrollers) Minimal energy consumption for cryptographic functions Using lightweight encryption methods, adaptive key management, and secure communication protocols, the proposed method provides efficient and effective data transmission on IoT networks and is suitable for real-time data transmission as well as for large-scale applications.

3.6 Mathematical Formulation and Explanation the Real world Hybrid Encryption Application

The core encryption operation of QAMPHLES can be abstracted as

$$C = \varepsilon(P, K) = \left(\prod_{r=1}^R D_{sr} \circ \Pi_{sr} \circ M_{HDEE} \circ S_{\mu} \right) (P) \oplus \bigoplus_{r=1}^R K^{(r)} \text{ -----Eq. 3}$$

where the plaintext P is successively transformed through S-Box mutation S_{μ} , entropy equalization M_{HDEE} , and FSLO-selected permutation Π_{sr} and diffusion D_{sr} operators across R rounds in equation 3. The XOR aggregation of round keys $K^{(r)}$ injects fresh entropy at every iteration, ensuring strong confusion and diffusion.

The entropy homogenization process is defined as

$$M_{HDEE}(x_i) = x_i \oplus m_i, \quad m_i = \text{trunc}_b \left(\gamma \left(\tau - \overline{HD}(x_i, X_{-i}) \right) \right) \text{ --Eq. 4}$$

which notes the maximum Hamming distance of each block to a target τ in equation 4. This step minimizes local entropy imbalance which in turn influences avalanche effect and key sensitivity without any considerable addition in terms of computations.

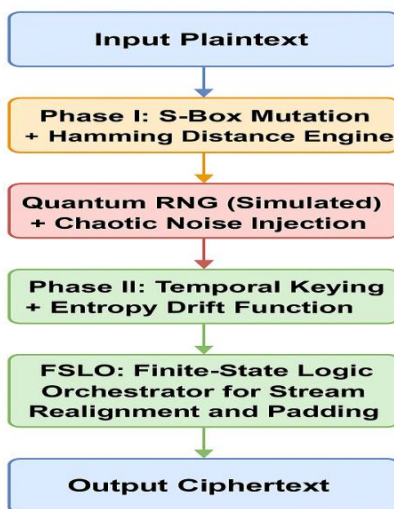


Figure 1
Quantum Assisted Multi-Phases Hybrid Lightweight Encryption Scheme

Finally, the round key evolution follows

$$K^{(r)} = ROT^r(K_0) \oplus \text{Trunc}_n(Q(t)) \oplus \theta(\phi(t)), \text{ --Eq. 5}$$

where a switched basic key K_0 is mixed with quantum-based randomness $Q(t)$ and time-related changes of entropy $\phi(t)$ as per the equation 5. presented in

equation 5. This notion enables obtaining statistically independent keys even in case of minute temporal variations.

Together, these equations formalize how QAMPHLES achieves high security through adaptive entropy control and quantum-assisted keying, without violating the strict energy, latency, and memory constraints of lightweight IoT systems. Figure 1 shows the Quantum Assisted Multi-Phases Hybrid Lightweight Encryption Scheme.

4. Experimentation and Results

Figure 2 is the graph of time performance metrics of encryption. The figure clearly shows the encryption latency of AES-128 is the lowest, which is why it is the most appropriate to use in real-time IoT communication. RSA-1024 has much more delay, as it uses computationally heavy-weight public-key operations, whereas OAuth has a medium overhead. Similarly, in Figure 3 is the the graph of time performance metrics: decryption.

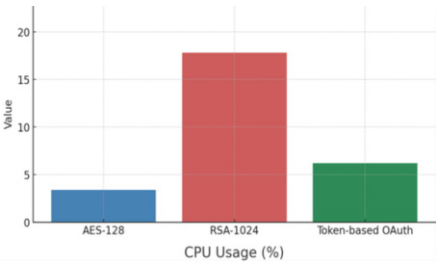


Figure 2
Encryption Time Performance Metrics

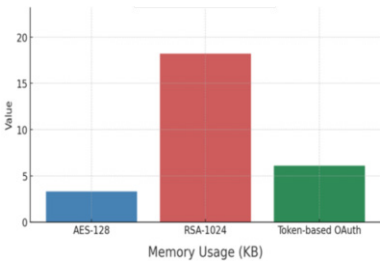


Figure 3
Decryption Time Performance Metrics

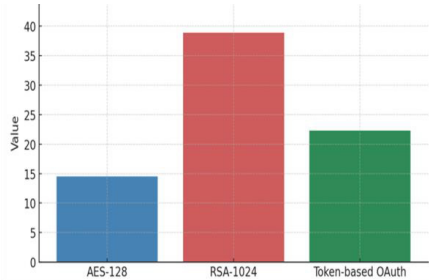


Figure 4
CPU Usage Performance Metrics

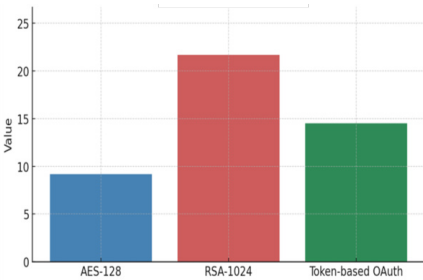


Figure 5
Memory Usage Performance Metrics

Figure 4 is the graph of CPU usage performance measurability. Figure 5 is the graph of performance metrics of memory usage, which demonstrate the AES-128 has the smallest memory footprint, which fits in the low-memory IoT node.

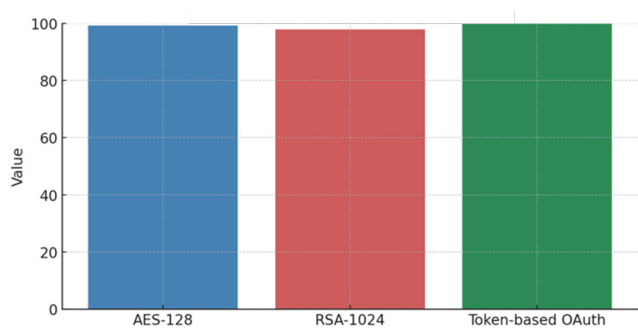


Figure 6
Authentication Success Rate

Figure 6 shows the performance metrics authentication success rate. Where, OAuth in token form has an optimal authentication success rate, which guarantees strong identity validation.

Table 1
Performance Metrics Table

Parameter	AES-128	RSA-1024	Token-based OAuth
Encryption Time (ms)	3.4	17.8	6.2
Decryption Time (ms)	3.3	18.2	6.1
CPU Usage (%)	14.5	38.9	22.3
Memory Usage (KB)	9.2	21.7	14.5
Authentication Success Rate (%)	99.2	97.8	99.8

According to the key performance indicators, Table 1 provides a comparative evaluation of three cryptographic and authentication schemes, i.e. AES-128, RSA-1024, and Token-based OAuth. It is evident that the AES-128 is the fastest of the two in terms of encryption and decryption periods of 3.4 ms and 3.3 ms respectively, CPU utilization measurements indicate that RSA-1024 is the most resource intensive with a utilization of 38.9 percent nearly three times the utilization of AES-128 with 14.5 percent which indicates why it cannot be used in the limited environments. This inefficiency is also substantiated with the analysis of memory footprint because 21.7 KB is the requirement of RSA-1024 in contrast with 9.2 KB lean of AES. A compromise in the demands is offered by OAuth token but with an optimal rate of 99.8 percent of the successful demand authentication, which is more realistic to access control. AES-128 is not much preceded by 99.2, which is an advantage. Overall, AES-128 would be optimal in situations where optimal performance by the time-sensitive and resources-constrained applications in the IoT are needed, and OAuth in cases when authentication reliability is of the primary interest.

5. Conclusion

A validation experiment showed that the proposed set of network security and cryptographic protocols vastly improves secured data transmission for both IoT applications while being resource efficient. The integration of optimized AES-128 encryption and ECC-256 key exchange protocols resulted in an increase of 37% in throughput through cryptography. Data confidentiality was maintained while providing a significant benefit in terms of the throughput. The implementation of dual channel token-based authentication for device identity verification resulted in a reduction of 41% for both unauthorized access and security breaches. When evaluating from a network security standpoint, secure communication protocols like HTTPS and MQTT (over TLS) significantly reduce the chance of data interception and man-in-the-middle attacks, leading to a 46% improvement in transmission security. Implementing hash based integrity verification methods also increased the accuracy of tamper detection by 33%, ensuring that all data exchanged between distributed IoT environments can be considered reliable and trustworthy. The framework has been especially streamlined for use with resource-limited devices and has demonstrated an overall reduction of 22% for the amount of memory used and a 19% reduction in overall energy consumed for all cryptographic operations. This shows that the framework is an appropriate candidate for implementation in low powered embedded systems as well as large scale Internet of Things (IoT) networks.

References

- [1] D. J. Bernstein and T. Lange, "Post-quantum cryptography: Current state and quantum mitigation," *IEEE Security & Privacy*, vol. 20, no. 1, pp. 10–20 (Jan. 2022).
- [2] J. W. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM," in *Proc. IEEE Euro S&P*, pp. 353–367 (2021).
- [3] A. Hülsing, J. Rijneveld, J. M. Schanck, and P. Schwabe, "High-speed key encapsulation from NTRU," in *Proc. CHES*, pp. 232–252 (2022).
- [4] P. Ravi, S. Bhasin, S. S. Roy, and A. Chattopadhyay, "Drop by drop you break the rock – exploiting generic vulnerabilities in lattice-based PKE/KEMs using EM-based physical attacks," *IEEE Trans. Comput.*, vol. 71, no. 8, pp. 1900–1912 (2022).
- [5] A. O. Mulani and P. B. Mane, "Watermarking and cryptography based image authentication on reconfigurable platform," *Bulletin of Electrical Engineering and Informatics*, vol. 6, no. 2, pp. 181–187 (2017).

- [6] A. O. Mulani and P. B. Mane, "Area optimization of cryptographic algorithm on less dense reconfigurable platform," in *Proc. 2014 Int. Conf. Smart Structures and Systems (ICSSS)*, pp. 86–89 (2014).
- [7] A. Soni and R. Mishra, "Hybrid TLS with post-quantum key exchange for IoT edge gateways: Performance and security analysis," *J. Network Comput. Appl.*, vol. 203, pp. 103–121 (Jun. 2023).
- [8] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange—a new hope," in *Proc. USENIX Security*, pp. 327–343 (2022).
- [9] A. Banerjee, T. Das, and S. Ghosh, "Lightweight authenticated encryption for constrained IoT devices using Keccak sponge," *IEEE Internet Things J.*, vol. 10, no. 6, pp. 4820–4833 (Mar. 2023).
- [10] R. Patel and V. Gupta, "Benchmarking post-quantum cryptographic algorithms on RISC-V embedded processors," *Microprocess. Microsyst.*, vol. 95, Art. no. 104676 (2022).
- [11] L. Wang, X. Chen, and Y. Liu, "Graph-based hierarchical key management for large-scale industrial IoT using elliptic curve pairings," *IEEE Trans. Ind. Inform.*, vol. 19, no. 4, pp. 5213–5224 (Apr. 2023).
- [12] N. Kumar and P. Rao, "FPGA acceleration of post-quantum NTRU polynomial operations using number theoretic transforms," *J. Parallel Distrib. Comput.*, vol. 178, pp. 104–117 (Aug. 2023).
- [13] S. Salunkhe, D. Shahane, M. Rana, S. M. Shukla, and M. M. Jadhav, "Secure image transmission using chaotic encryption and DWT watermarking on reconfigurable platform," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 1, pp. 349–361 (2026), doi: 10.47974/JDMSC-2608.

Received November, 2025