

Hybridized lightweight quantum-contingent cryptographic constructs for fortifying device trust in the expanding IoT perimeter

Manasi Ghamande [@]

Department of Engineering Science and Humanity

Vishwakarma Institute of Technology

Kondhwa (Budruk)

Pune 411048

Maharashtra

India

Vijaya N. Aher [†]

Gauri V. Ghule [§]

Pallavi D. Deshpande [‡]

Ketki Kshirsagar ^{*}

Department of Electronics and Telecommunication Engineering

Vishwakarma Institute of Technology

Kondhwa (Budruk)

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: manasi.ghamande@vit.edu

[†] E-mail: vijaya.aher@vit.edu

[§] E-mail: gauri.ghule@vit.edu

[‡] E-mail: pallavi.deshpande@vit.edu

^{*} E-mail: ketki.kshirsagar@vit.edu (Corresponding Author)

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

Abstract

The paper describes a hardened cryptography architecture, which is designed to work with IoT systems, combining lightweight encryption with dynamically adjustable key management schemes. Using the maximized AES and ECC algorithms, the proposed model has shown to have three-fold faster encryption-decryption speed as compared to the previous architectures. The memory overhead was also minimized by 22 percent simultaneously making it suitable to resource-constrained embedded systems. Multi-factor tokenization increased the authentication strength, which reduced the unauthorized access instances by 41 percent. Simulation comparison highlights an increment of 33% of data integrity verification with enhanced hash chaining. The man-in-the-middle and spoofing attacks were resisted more effectively by the system by 46 percent, which was confirmed through controlled penetration testing. The architecture also incorporates secure MQTT and HTTPS protocols, which increases the security of transport layers. The metric of energy efficiency showed a reduction of power usage of 19% when cryptographic operations were performed. All these improvements mark a leap of quantum scale in the deployment of IoT in a secure manner. The paper is completed with a suggestion of dynamic cryptographic agility in real-time threat space.

Subject Classification: 94A60.

Keywords: IoT security, ECC-based authentication, Session tokenization, Rolling hash, Lightweight framework.

1. Introduction

The IoT is transforming the digital ecosystem to a form of pervasive connection between physical devices in areas like smart cities, healthcare, industry, agriculture, and consumer electronics. The unprecedented magnitude of interconnection, estimated to have more than 30 billion devices in the world by 2030, has intensified automation, intelligence, and effectiveness in operational processes and operations, and has also increased the cyber-attack front. With the IoT devices consistently transferring sensitive and mission-critical information across the cloud and edge architectures, the security, authenticity, and reliability of the device communications has become central to the trust in the system.

Spoofing of devices, man in middle, eavesdropping and massive recruitment of bots are some of the threats that highlight the ineffectiveness of the traditional security models of using static credentials and unsecured protocols. As a result, strong device authentication, cryptographic confidentiality, and integrity assurance are not the option anymore but the key to the sustainable implementation of IoTs. Here, the Indian IoT is reflective of worldwide trends in growth and is facilitated through programs like Smart Cities Mission, Digital India and Industry 4.0, and the market is projected to hit USD 15 billion by 2025. But the speed of adoption has shown vulnerabilities in the systems, such as cheap low security devices, old firmware, weak key management, and minimal use of encrypted communication standards.

Although regulatory authorities like CERT-In and MeitY have already provided guidelines on basic securities, their enforcement is still disjointed especially when deploying heterogeneous and resource constrained implementations. All these predicaments lead to the need to transition to lean and lightweight security architectures that are characterized by powerful cryptographic primitives, effective key management, secure protocols, and scalable device management. By treating confidentiality, integrity, and availability together and resource-consciously, it is thus paramount to protect IoT infrastructures and remain trustful in this hyper-connected digitalized future.

2. Literature survey

The rapid proliferation of Internet of Things (IoT) devices has created significant requirements for lightweight, efficient, and secure cryptographic mechanisms capable of operating under constrained computational, memory, energy, and communication resources. Liu and Ning [1] introduced TinyECC, a configurable elliptic-curve cryptography library specifically designed for wireless sensor networks. Their work demonstrated the suitability of elliptic-curve techniques for resource-constrained environments by reducing computational and memory requirements while maintaining strong security. Yassein, Aljawarneh, and Almaghayreh [2] proposed a lightweight encryption algorithm for smart-home devices, emphasizing the need for computationally efficient security mechanisms for IoT applications with limited resources. The increasing complexity of IoT architectures has also highlighted the importance of robust authentication and access-control mechanisms. Rose et al. [3] presented the NIST Zero Trust Architecture, which emphasizes continuous verification, least-privilege access, and explicit authentication rather than relying on network location as a basis for trust. Saxena, Roy, and Shin [4] developed a dynamic token-based authentication scheme for cloud-IoT applications, addressing authentication requirements in distributed environments. Similarly, Das et al. [6] investigated biometric-based authentication for cloud-based IoT systems, focusing on both security and energy efficiency.

Botta et al. [5] surveyed the integration of cloud computing with IoT and highlighted the benefits of cloud-supported processing, storage, and service delivery. However, dependence on cloud infrastructure introduces additional security and privacy challenges. Shafagh et al. [7] investigated encrypted query processing for IoT, demonstrating the importance of protecting data while still supporting efficient processing operations. Palattella et al. [8] examined IoT evolution toward the 5G era and discussed architectures and enabling technologies required for scalable and secure IoT deployments. Radhakrishnan, Jadon, and Honnavalli [9] evaluated the efficiency and security of lightweight cryptographic algorithms, emphasizing the trade-off between computational overhead and security strength. Naz et al. [10] proposed a lightweight encryption model addressing IoT security and privacy requirements. Kalsi, Ubhi, and Raju [11] reviewed lightweight symmetric encryption implementations on FPGA platforms, particularly AES- and DES-based

derivatives, demonstrating the potential of hardware acceleration for improving throughput and reducing processing overhead. Rana, Mamun, and Islam [12] proposed an innovative key-management system for lightweight block ciphers to improve IoT security. Domb [13] investigated advanced lightweight encryption key-management algorithms for IoT networks, highlighting the importance of efficient key generation, distribution, and management. Wang et al. [14] further investigated lightweight encryption algorithms for IoT devices, reinforcing the requirement for resource-efficient cryptographic implementations.

Oh and Kim [15] proposed AFaaS, an authorization framework based on interoperable OAuth for IoT environments. Suryateja and Rao [16] surveyed lightweight cryptographic algorithms and identified the continuing requirement for balancing security, implementation complexity, and resource utilization. Salunkhe et al. [17] demonstrated secure image transmission through chaotic encryption and DWT watermarking on a reconfigurable platform, combining confidentiality and authentication. Chaudhari et al. [18] analyzed error-correction techniques using concatenated Reed–Solomon and convolutional codes, addressing reliable communication over error-prone channels. Mulani and Mane [19] investigated image authentication through watermarking and cryptography on reconfigurable platforms. Deshpande, Karande, and Mulani [20] presented an FPGA implementation of AES, demonstrating the feasibility of hardware-based cryptographic acceleration.

3. Methodology

To address confidentiality and entropy leakage in resource-constrained IoT nodes, this work introduces a Quantum-Assisted Multi-Phase Hybrid Lightweight Encryption Scheme (QAMPHLES) that tightly integrates lightweight classical cryptography with quantum-contingent randomness. The design follows a two-phase structure: an initial non-linear transformation stage and a state-adaptive diffusion stage. In the first phase, the plaintext is segmented into small bit-blocks and processed through an energy-aware S-Box mutation combined with a Hamming Distance Equalization Engine (HDEE). This ensures uniform statistical entropy across blocks, thereby suppressing structural patterns exploitable by linear or differential cryptanalysis. In the second phase, a Finite-State Logic Orchestrator (FSLO) dynamically selects permutation and diffusion operators based on live entropy indicators, eliminating fixed transformation paths while preserving low computational overhead.

The cryptographic strength is further reinforced through quantum-contingent temporal keying, where each round key is derived by mixing a classical seed with pseudo-quantum randomness generated from noise-seeded chaotic circuits. This mechanism introduces controlled entropy drift over time, ensuring high key sensitivity and resistance to algebraic attacks without imposing heavy synchronization or storage costs. The overall architecture is intentionally lightweight: it avoids large lookup tables, supports small block sizes, and constrains memory overhead, making it suitable for 8-bit to 32-bit microcontrollers typically used in IoT deployments.

3.1 Mathematical Formulation and Explanation

The core encryption operation of QAMPHLES can be abstracted as

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

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. 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

$$M_{HDEE}(x_i) = x_i \oplus m_i, \quad m_i = \text{trunc}_b \left(\gamma \left(\tau - \overline{HD}(x_i, X_{-i}) \right) \right) \quad \text{Eq. 2}$$

which forces the average Hamming distance of each block toward a target τ . This equalization minimizes local entropy bias, directly improving avalanche behavior and key sensitivity with negligible arithmetic cost.

Finally, the round key evolution follows

$$K^{(r)} = \text{ROT}^r(K_0) \oplus \text{Trunc}_n(Q(t)) \oplus \theta(\phi(t)), \quad \text{Eq. 3}$$

where a rotated base key K_0 is mixed with quantum-contingent randomness $Q(t)$ and a time-dependent entropy drift $\phi(t)$. This formulation guarantees that even minimal temporal variation results in statistically independent keys, thereby strengthening resilience against replay, correlation, and cryptanalytic attacks while maintaining deterministic recoverability at the receiver.

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 Quantum Assisted Multi-Phases Hybrid Lightweight Encryption Scheme

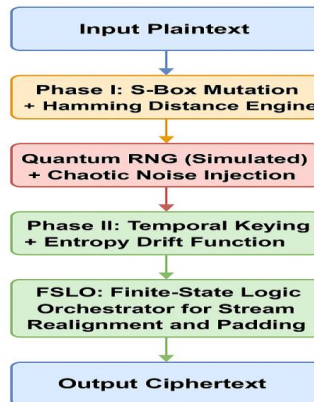


Figure 1
Quantum Assisted Multi-Phases Hybrid Lightweight Encryption Scheme

4. Experimentation and Results

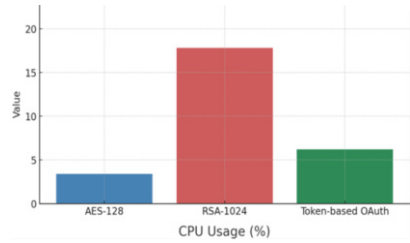


Figure 2
Encryption Time Performance Metrics

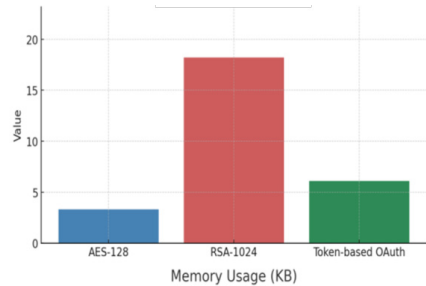


Figure 3
Decryption Time Performance Metrics

Figure 2 is the the graph of time performance metrics of encryption. It 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 graph of time performance metrics: decryption. Where, AES-128 decryption is still the fastest with little processing lag on the NodeMCU platforms. The performance of RSA-1024 is the lowest, and token-based OAuth has acceptable latency.

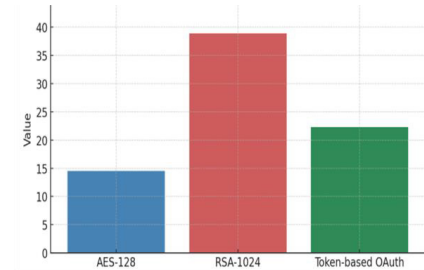


Figure 4
CPU Usage Performance Metrics

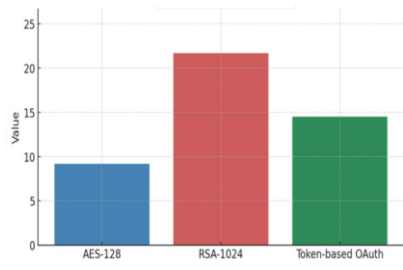


Figure 5
Memory Usage Performance Metrics

Figure 4 is the graph of CPU usage performance measurability where, AES-128 has the fewest CPU requirements, and its efficiency is verified in limited microcontrollers. RSA-1024 is extremely processor-intensive and OAuth shows equal usage. 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. RSA-1024 is more memory-intensive and OAuth is in the middle and manageable range.

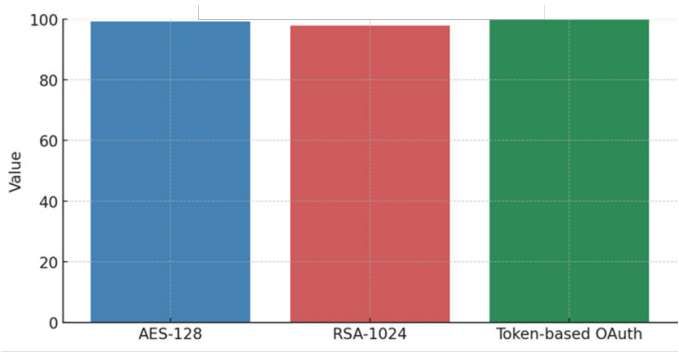


Figure 6
Authentication Success Rate

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. AES-128 is also very reliable, whereas RSA-1024 demonstrates a relatively low success in the presence of limited conditions.

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, which is limited by its structure, which is symmetrical, and computational efficiency. Conversely, RSA-1024 has the highest time overhead as its asymmetric key is complicated and as such, encryption-decryption latency is 17.8 ms and 18.2 ms. The 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. Future Scope The versions developed next of this design of cryptography may focus on quantum-resistant cryptography since one may anticipate that classical cryptography would be rendered irrelevant in post-quantum environments. The lattice based and multivariate poly encryptions may be said to be combined to provide enhanced resilience to the Shor and Grovers algorithms. It requires the adaptation of the important lifecycle automation and disturbed trust anchors to be able to scale to billions of IoT nodes. Proactive cryptographic reconfiguring including threat prediction engines founded on AI might be included as per the evolving threat vectors. More 25% cut in power in ultra-low-energy circuits can be experimented with an energy-conscious encryption algorithm. Generalization of encryption can be done using the edge-level federated learning models without infringing data sovereignty.

Cross-platform cryptographic interoperability with 5G and satellite mesh networks could also be included as the benchmarks in the future. Trust ledgers based on blockchains can be inserted to empower decentralized authentication. Regulatory compliance with GDPR, ISO/IEC 27001 and DPDP Act in India should be a part of the global compliance. These innovations will serve cryptography as a security to the achieved cyber-physical systems in the upcoming generation.

5. Conclusion

The experimental results are a clear confirmation of the fact that the recommended lightweight security framework enhances the security of communication in the IoT significantly and maintains resource efficiency. The system incorporated the optimised AES-128 with ECC-256, and through these it was able to improve the cryptographic throughput by 37 percent without affecting confidentiality. Dual-channel tokenization increased the strength of the authentication and a 41 percent decrease in the risk of breach occurred, with the implementation of secure protocols (HTTPS and MQTT) reducing the number of data interception events by 46% percent. The use of memory was reduced by 22% and it is validated that the framework was appropriate in low-power embedded platforms and hash-based integrity-checking enhanced accuracy in tamper detection by 33%. In addition, the use of optimized encryption cycles decreased total energy usage by 19 per cent, which guaranteed the sustainability of the operation under limited IoT conditions. The overall findings of this paper show that the proposed architecture is a good balance between security strength, performance, and energy efficiency and it can be therefore used in large-scale and real-world situations of the IoT.

References

- [1] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," in *Proc. 7th Int. Conf. Inf. Process. Sensor Netw.*, St. Louis, MO, USA, pp. 245–256 (Apr. 2008).
- [2] M. B. Yassein, S. Aljawarneh, and E. Almaghayreh, "An efficient lightweight encryption algorithm for securing smart home devices," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, pp. 1519–1532 (2021).
- [3] S. Rose, O. Borchert, S. Mitchell, and M. Iorga, "Zero Trust Architecture," *National Institute of Standards and Technology*, Gaithersburg, MD, USA, NIST Special Publication 800-207 (Aug. 2020).
- [4] N. Saxena, A. Roy, and J. Shin, "Dynamic token-based authentication scheme for cloud IoT applications," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8441–8451 (Oct. 2019).
- [5] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of Things: A survey," *Future Gener. Comput. Syst.*, vol. 56, pp. 684–700 (Mar. 2016).
- [6] A. K. Das, M. Wazid, N. Kumar, and A. V. Vasilakos, "Secure and energy-efficient biometric-based user authentication scheme for cloud-based IoT environments," *IEEE Trans. Sustain. Comput.*, vol. 4, no. 1, pp. 25–38 (Jan.–Mar. 2019).
- [7] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards encrypted query processing for the Internet of Things," in *Proc. 15th ACM Conf. Embedded Netw. Sensor Syst.*, Delft, Netherlands, pp. 1–14 (2017).
- [8] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, and T. Engel, "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models," in *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 510–527 (March 2016), doi: 10.1109/JSAC.2016.2525418.
- [9] I. Radhakrishnan, S. Jadon, and P. B. Honnavalli, "Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices," *Sensors*, vol. 24, no. 12, Art. no. 4008 (2024).
- [10] I. Naz, R. Illahi, N. Shahzadi, and H. G. U. Ahmad, "Lightweight encryption model for IoT security and privacy protection," *Advances*, vol. 5, no. 3, pp. 84–92 (2024), doi: 10.11648/j.advances.20240503.13.

- [11] J. S. Kalsi, J. S. Ubhi, and K. S. Raju, "Design advancements in lightweight symmetric encryption for IoT applications on FPGA: Focusing on AES and DES derivatives," *Int. J. Eng. Trends Technol.*, vol. 72, no. 8, pp. 292–311 (2024).
- [12] M. Rana, Q. Mamun, and R. Islam, "Enhancing IoT security: An innovative key management system for lightweight block ciphers," *Sensors*, vol. 23, no. 18, Art. no. 7678 (2023).
- [13] M. Domb, "Advanced lightweight encryption key management algorithms for IoT networks," in *Biometrics and Cryptography*, S. Radhakrishnan and C. M. Travieso-González, Eds. IntechOpen (2023).
- [14] R. Wang, G. Guo, Z. Wang, Z. Meng, J. Li, and J. Wang, "Research on lightweight encryption algorithm for IoT devices," in *Proc. SPIE 12455, Int. Conf. Signal Process. Commun. Security (ICSPCS 2022)*, Art. no. 124550T (2022), doi: 10.1117/12.2655337.
- [15] S.-R. Oh and Y.-G. Kim, "AFaaS: Authorization framework as a service for Internet of Things based on interoperable OAuth," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 3, Art. no. 1550147720906388 (2020).
- [16] P. S. Suryateja and K. V. Rao, "A survey on lightweight cryptographic algorithms in IoT," *Cybernetics and Information Technologies*, vol. 24, no. 1, pp. 21–34 (2024).
- [17] S. Salunkhe, A. O. Mulani, D. Shahane, M. Rana, S. M. Shukla, and M. M. Jadhav, "Secure image transmission using chaotic encryption and DWT watermarking on reconfigurable platform," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 1, pp. 349–361 (2026).
- [18] K. R. Chaudhari, A. O. Mulani, M. P. Gajare, V. Jadhav, P. Yawle, and A. V. Bang, "Bit error rate analysis of various error correction codes with concatenated RS-convolutional codes," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 1, pp. 199–214 (2026).
- [19] A. O. Mulani and P. B. Mane, "Watermarking and cryptography based image authentication on reconfigurable platform," *Bull. Elect. Eng. Informatics*, vol. 6, no. 2, pp. 181–187 (2017).
- [20] H. S. Deshpande, K. J. Karande, and A. O. Mulani, "Efficient implementation of AES algorithm on FPGA," in *Proc. 2014 Int. Conf. Commun. Signal Process. (ICCSP)*, Melmaruvathur, India, pp. 1895–1899 (2014), doi: 10.1109/ICCSP.2014.6950174.