Educational Administration: Theory and Practice
2023, 29(3), 1746 -1750
ISSN: 2148-2403
https://kuey.net/

Research Article

A Lightweight And Secure Authenticated Encryption Design For Resource-Constrained Internet Of Things Devices

Dr. Riddhi R. Tanna[1], Dr. Rashmin S. Tanna[2]

1Department of Computer Applications, Christ College, Rajkot, Gujarat, India, Email: dr.riddhirtanna@gmail.com
2Lecturer (EC), A.V. Parekh Technical Institute, Rajkot, Directorate of Technical education, Gandhinagar, Gujarat, India Email: - dr.rashminstanna@gmail.com

Citation: Riddhi Tanna (2023). A Lightweight And Secure Authenticated Encryption Design For Resource-Constrained Internet Of Things Devices Educational *Administration: Theory and Practice*, 29(3) Doi: 10.53555/kuey.v29i3.11307

ARTICLE INFO

ABSTRACT

Internet of Things (IoT) devices deployed in home and office environments operate under stringent constraints on memory, processing capability, and energy consumption, while increasingly handling sensitive sensor and multimedia data. Conventional cryptographic algorithms, although secure, often impose computational and memory overheads that are unsuitable for constrained platforms. Prior research introduced optimized symmetric encryption schemes and hybrid key-management approaches to improve efficiency for multimedia communication. More recently, standardization efforts have emphasized lightweight authenticated encryption as a practical requirement for IoT ecosystems. This paper presents a design-centric IEEE-compliant study of a lightweight authenticated encryption framework for IoT devices, grounded in prior MAES and EMAES research and aligned with contemporary lightweight cryptography standards. The paper analyses design goals, security requirements, and implementation constraints, and proposes a configurable authenticated-encryption blueprint suitable for sensors, multimedia IoT nodes, and gateways. Comparative analysis tables and architectural illustrations are provided to position the proposed approach against existing schemes. A reproducible evaluation methodology using an existing multimedia dataset is outlined to assess efficiency, security, and feasibility. The study serves as a foundation for future implementation and experimental validation of lightweight encryption schemes in IoT environments.

Keywords: Lightweight cryptography, IoT security, authenticated encryption, MAES, EMAES, constrained devices, symmetric encryption.

I. Introduction

The proliferation of Internet of Things (IoT) technologies has transformed home and office environments into interconnected ecosystems comprising sensors, smart appliances, surveillance systems, and multimedia devices. These devices continuously exchange sensitive information, necessitating robust encryption mechanisms to protect confidentiality and integrity over wireless networks [1], [2].

The Advanced Encryption Standard (AES) remains the most widely adopted symmetric encryption algorithm due to its strong security properties and global standardization [3], [4]. However, AES implementations often incur non-negligible computational and memory overheads when deployed on resource-constrained IoT devices, particularly for multimedia-intensive workloads. In addition, traditional encryption modes frequently rely on separate authentication mechanisms, increasing complexity and energy consumption [5].

To address these limitations, Modified AES (MAES) was proposed to improve encryption efficiency for multimedia data, followed by Extended MAES (EMAES), which integrates hybrid key-management capabilities for networked environments [8]– [10]. While these approaches demonstrated improved performance over

standard AES, evolving IoT deployment scenarios and increasing device heterogeneity motivate the need for even lighter cryptographic primitives with built-in authentication.
This paper addresses this requirement by presenting a lightweight authenticated encryption design framework for IoT devices, building on MAES/EMAES principles and informed by recent lightweight cryptography standards [11], [12]. The objective is not to introduce a finalized algorithm, but to provide a secure, feasible, and implementation-ready design direction suitable for next-generation IoT deployments.

II. Background and Related Work

A. Cryptographic Requirements in IoT

IoT devices typically operate with limited CPU frequency, restricted memory, and strict energy budgets. Cryptographic primitives for such environments must minimize code size, RAM usage, and execution cycles while maintaining resistance to cryptanalytic and implementation-level attacks [1], [5].

B. AES and Performance Optimization

AES is standardized and proven secure against known classical attacks [3], [4]. However, several studies report performance bottlenecks when AES is applied to large multimedia payloads or executed on low-power platforms [6], [7]. Algorithm-level and implementation-level optimizations have been explored to reduce latency while preserving security guarantees [6].

C. MAES and EMAES

MAES enhances AES efficiency for multimedia encryption by restructuring internal operations and reducing redundant computations [8], EMAES further extends this approach by incorporating asymmetric key exchange to enable secure session establishment in distributed environments. These schemes demonstrated improved throughput and acceptable security trade-offs, making them relevant precursors to lightweight IoT encryption design.

D. Lightweight Cryptography Standards

In response to IoT security demands, the National Institute of Standards and Technology (NIST) initiated the Lightweight Cryptography (LWC) project, culminating in the selection of the Ascon family as a standard for authenticated encryption and hashing on constrained devices. Ascon's sponge-based design provides integrated confidentiality and integrity with low implementation overhead [12], [19].

III. Design Goals and Constraints

The proposed lightweight encryption design is guided by the following goals:
1. **Security:** Provide confidentiality and integrity through authenticated encryption while resisting classical cryptanalysis and common implementation attacks [12], [14].
2. **Lightweight Operation:** Minimize computational overhead, memory footprint, and code size [5], [13].
3. **Energy Efficiency:** Reduce execution cycles and memory accesses to conserve battery power [16].
4. **Scalability:** Support both small sensor messages and larger multimedia payloads through chunk-based processing [8].
5. **Interoperability:** Integrate with existing IoT communication stacks and WLAN infrastructures [2], [18].

Typical constraints include microcontrollers with tens of kilobytes of RAM and limited hardware acceleration [5], [13].

IV. Comparative Analysis of Encryption Approaches

Table I presents a comparative analysis of AES, MAES, EMAES, and lightweight authenticated encryption approaches with respect to IoT requirements.

Table I. Comparison of Encryption Approaches for IoT Devices

Parameter	AES	MAES	EMAES	Lightweight AEAD
Encryption Type	Symmetric	Symmetric (Optimized)	Hybrid	Symmetric (AEAD)
Integrity Protection	Separate MAC	Separate MAC	Separate MAC	Built-in
Computational Cost	High	Medium	Medium–High	Low
Memory Footprint	High	Medium	Medium	Very Low
Suitability for Sensors	Low	Medium	Medium	High
Suitability for Multimedia IoT	Medium	High	High	High
Key Management	Static	Static	Dynamic	Dynamic
Standardization Status	NIST Standard	Research	Research	NIST LWC-aligned

This comparison highlights the suitability of lightweight AEAD approaches for constrained IoT devices while positioning MAES and EMAES as efficient transitional solutions.

V. Proposed Lightweight Authenticated Encryption Design

A. Architectural Overview

The proposed design follows an **authenticated encryption with associated data (AEAD)** paradigm, providing confidentiality and integrity in a single cryptographic operation [11], [12].
The architecture is structured into three profiles:

- **Profile-S (Sensor):** Ultra-lightweight configuration for low-end sensors.
- **Profile-M (Multimedia):** Balanced configuration for camera and audio-enabled IoT devices.
- **Profile-G (Gateway):** Enhanced configuration for gateways and access points with higher computational resources.

Figure 1 illustrates the overall workflow of the proposed lightweight encryption architecture.

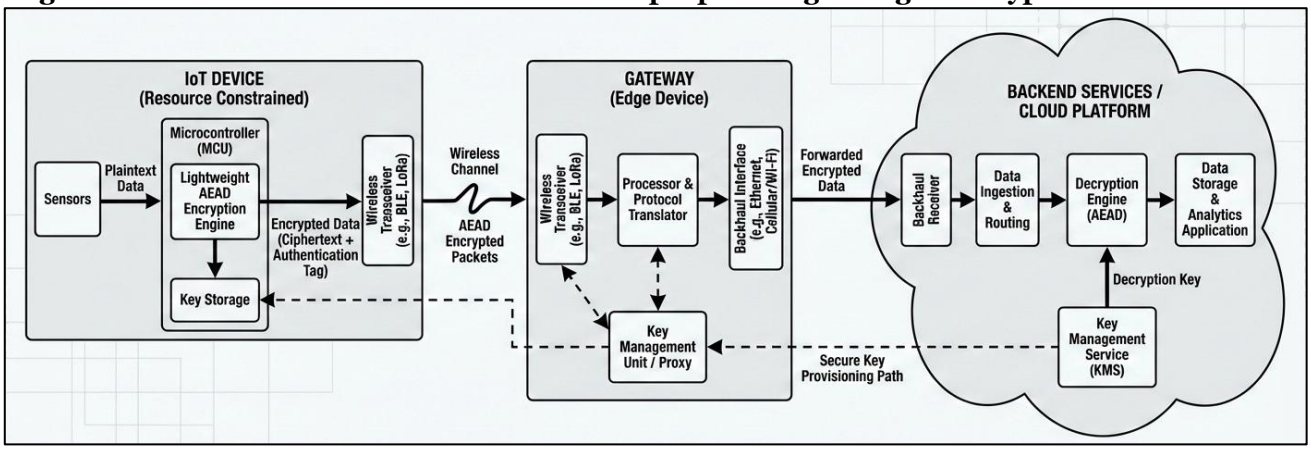

Figure 1 : Lightweight authenticated encryption workflow for secure data transmission in IoT environments.

B. Symmetric Core Design

The symmetric core is inspired by two complementary approaches:
1. **Sponge-based permutation design**, aligned with NIST lightweight cryptography recommendations [11], [12].
2. **Optimized block-based design**, leveraging insights from MAES to improve throughput where optimized software or hardware support is available [8], [9].

C. Key and Nonce Management

A 128-bit symmetric key is recommended for constrained devices, with optional support for larger keys on capable nodes [11]. Nonce uniqueness is enforced using counters or session-derived values to prevent replay and nonce-reuse attacks [12].

D. Support for Multimedia Data

Large multimedia payloads are processed in authenticated chunks, enabling streaming operation without requiring full payload buffering in memory [8], [15].

VI. Security Analysis

A. Confidentiality and Integrity

The AEAD construction ensures that any modification to ciphertext or associated data is detected during decryption. Security assumptions align with established lightweight AEAD primitives [11], [12].

B. Resistance to Known Attacks

Non-linear permutations and authenticated processing provide resistance to differential and linear cryptanalysis. MAES-based optimizations are applied cautiously to preserve diffusion and confusion properties [6], [8].

C. Implementation Considerations

Side-channel resistance is addressed through constant-time implementations and avoidance of data-dependent memory access. Masking and noise-based countermeasures may be employed in higher-security deployments [13], [14].

VII. Evaluation Methodology and Feasibility

A. Dataset

Evaluation is planned to use the 180-record multimedia dataset previously published by the author, comprising text, image, audio, and video samples [15].

B. Metrics

Key evaluation metrics include:

- Encryption and decryption time
- Throughput
- Memory usage
- Energy consumption per byte [16]
- Data fidelity metrics (PSNR, SSIM) [8]

Table II summarizes IoT constraints and corresponding design responses.

Table II. IoT Constraints and Lightweight Encryption Feasibility

Constraint	Typical Range	Design Response
RAM	16–128 KB	Compact state, chunked processing
Flash	< 512 KB	Small code footprint
CPU	< 200 MHz	Reduced rounds, simple operations
Energy	Battery-powered	Single-pass AEAD
Latency	Real-time	Stream-friendly design
Security Lifetime	5–10 years	Conservative parameters

VIII. Discussion and Future Work

Future work will focus on implementing the proposed design on representative IoT hardware, conducting experimental performance evaluations, and exploring hardware acceleration. Formal cryptographic proofs and resistance to advanced side-channel attacks remain important research directions [13], [14], [20].

IX. Conclusion

This paper presented a comprehensive, design-oriented study of a lightweight authenticated encryption framework for IoT devices. Building on prior MAES and EMAES research and aligned with modern lightweight cryptography standards, the proposed approach balances security, efficiency, and feasibility. Comparative analysis, architectural illustrations, and evaluation planning demonstrate its suitability for next-generation IoT deployments.

References

L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854–864, Dec. 2016, doi: 10.1109/JIOT.2016.2581263.

J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*. Berlin, Germany: Springer, 2002.

National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," *FIPS PUB 197*, Nov. 2001. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, Jan. 2015, doi: 10.1016/j.comnet.2014.11.008.

R. S. Tanna, R. R. Tanna, and J. Bhadeshiya, "Improvement in the execution time of AES algorithm by modifications in S-box and MixColumns for multimedia applications," *International Journal of Research in Engineering, IT and Social Sciences*, vol. 8, no. 4, pp. 65–68, 2018.

R. C. Somaiya, A. M. Gonsai, and R. S. Tanna, "WLAN security and efficiency issues based on encryption techniques," *International Journal of Research in Engineering, IT and Social Sciences*, vol. 6, no. 9, pp. 27–32, 2016.

R. Somaiya and A. Gonsai, "Design and implementation of a new encryption algorithm in MATLAB for multimedia files," *Vidhyayana – An International Multidisciplinary Peer-Reviewed E-Journal*, vol. 6, no. 6, 2021.

C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2: Lightweight authenticated encryption and hashing," *Journal of Cryptology*, vol. 34, no. 3, 2021, doi: 10.1007/s00145-021-09398-9.

T. Eisenbarth, Z. Gong, T. Güneysu, and S. Heyse, "Microcontroller implementations of lightweight block ciphers," *ACM Transactions on Embedded Computing Systems*, vol. 16, no. 1, 2017, doi: 10.1145/2994539.

P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology – CRYPTO '99*, LNCS 1666, pp. 388–397. Springer, 1999, doi: 10.1007/3-540-48405-1_25.

D. Butin, J. Großschädl, and D. Zoni, "Post-quantum cryptography on embedded systems: A performance evaluation," *ACM Transactions on Embedded Computing Systems*, vol. 18, no. 5s, Art. no. 65, 2019, doi: 10.1145/3358225.

R. Roman, J. Lopez, and R. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security issues," *ACM Computing Surveys*, vol. 52, no. 2, 2019, doi: 10.1145/3305260.

M. S. Turan, E. Barker, W. Burr, and L. Chen, "Recommendation for lightweight cryptography," *NISTIR 8114*, National Institute of Standards and Technology, 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf

J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. Schanck, P. Schwabe, and D. Stehlé, "CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM," *IEEE European Symposium on Security and Privacy*, 2018, pp. 353–367, doi: 10.1109/EuroSP.2018.00032.