JOURNAL OF SOUTHERN COMMUNICATION ENGINEERING
ISLAMIC AZAD UNIVERSITY BUSHEHR BRANCH

E-ISSN: 2980-9231
https://sanad.iau.ir/journal/jce

https://doi.org/...

Vol. x/ No. x/xxx

Research Article

Optimized Lightweight Cryptography for Two-Stage Adaptive Design under Reflected Normal Loss Function in the Internet of Things: Integration of Regression Models and Elliptic Curve Encryption

Hassan Mazarei [1]

[1]Department of Basic Sciences, Bushehr Branch, Islamic Azad University, Bushehr, Iran
mazarei.hasan@iau.ac.ir

Correspondence
Hassan Mazarei, Professor, Department of Basic Sciences, Bushehr Branch, Islamic Azad University, Bushehr, Iran

Email: mazarei.hasan@iau.ac.ir

Main Subjects:
Internet of Things

Paper History:
Received: 15 April 2025
Revised: 10 May 2025
Accepted: 13 May 2025

Abstract

The Internet of Things (IoT) plays a pivotal role in bridging the physical and digital worlds through billions of interconnected devices. However, its security challenges, particularly in data confidentiality and integrity, demand efficient solutions. This study proposes an optimized lightweight cryptographic method for IoT, leveraging a two-stage adaptive design under the Reflected Normal Loss Function (RNL). The proposed method integrates an enhanced Blowfish algorithm with parallelization of the *F* function, achieving a 35–40% reduction in execution time, and combines it with Elliptic Curve Cryptography (ECC) for secure key management. To ensure data integrity, the lightweight BLAKE2s hash function replaces the insecure MD5 algorithm. Simulations using the iFogSim tool demonstrated that the proposed approach reduces energy consumption by 18–22% and execution time by 20–25% compared to traditional algorithms such as RSA and AES-128 in ECB mode, without imposing significant computational overhead on IoT devices. Additionally, replacing RSA with the lightweight PRESENT algorithm enhances resistance against side-channel attacks. Aligned with the hardware limitations of IoT nodes (e.g., limited processing power and battery life), this framework adheres to the hybrid ECIES standard (RFC 6090) for secure key exchange and employs linear regression models to reduce the probability of successful brute-force attacks to below 0.1%.

Keywords: Internet of Things (IoT), Reflected Normal Loss Function, Linear Regression, Security, Lightweight Cryptography, Elliptic Curve Cryptography (ECC).

Highlights

- Proposed an optimized lightweight cryptographic method for IoT
- Enhanced Blowfish algorithm with parallelization of F function, achieving 35-40% reduction in execution time
- Integrated Elliptic Curve Cryptography (ECC) for secure key management and BLAKE2s for data integrity
- Achieved 18-22% reduction in energy consumption and 20-25% in execution time compared to traditional algorithms

Citation: [in Persian].

1. Introduction

The expansion of the IoT has created a critical need for efficient security protocols that can protect data confidentiality and integrity while respecting the limited hardware resources (processing, memory, battery life) of IoT nodes. Classic cryptography, such as RSA and DES, is often resource-intensive and thus unsuitable for these environments. Recently, advanced statistical techniques like **two-stage adaptive sampling** combined with loss functions, specifically the **Reflected Normal Loss (RNL) function**, have been introduced to statistically optimize the crucial parameters of cryptographic schemes (e.g., key size and number of encryption rounds) to minimize operational overhead. This research aims to leverage this statistical foundation by integrating advanced lightweight cryptographic algorithms, specifically to create a hybrid framework that is highly efficient, secure, and statistically optimized for the unique constraints of IoT.

2. Innovation and Contributions

The core innovations of this research focus on optimizing performance and security simultaneously in a resource-constrained environment:

- Optimized Lightweight Cryptographic Solution: We propose a novel, optimized lightweight cryptographic method explicitly designed for IoT infrastructure.
- Blowfish Algorithm Enhancement: The F function within the Blowfish algorithm is modified to enable the parallel execution of addition and XOR operations. This structural change significantly reduces time complexity, resulting in a 35−40% reduction in the algorithm's execution time.
- Hybrid Security Integration: The security scheme employs a combination of techniques: the enhanced Blowfish for high-speed data encryption, ECC/ECIES for secure private key exchange, and the lightweight BLAKE2s hash function for robust 256-bit data integrity, offering increased resistance against collision attacks.
- Performance Optimization and Validation: The resulting framework achieves an 18−22% reduction in energy consumption and a 20−25% reduction in execution time when benchmarked against traditional algorithms.

3. Materials and Methods

The proposed framework is a hybrid architecture consisting of data encryption, key security, data integrity, and statistical optimization components.

Optimized Blowfish Encryption

Blowfish is utilized for its speed and low memory footprint (less than 5 KB). The key modification is in the Feistel network's F function. The standard serial F function is a major source of time complexity. Our enhancement modifies the function to allow two addition/XOR operations to be executed in parallel (effectively reducing the time required for two serial additions to that of one). This is achieved by restructuring the S-Box lookups and arithmetic operations within the F function to fully leverage multi-threading capabilities.

Key Management and Integrity

The symmetric key used by the enhanced Blowfish is secured using Elliptic Curve Cryptography (ECC), specifically by implementing the hybrid ECIES standard (RFC 6090). This eliminates the security risk associated with transmitting the private symmetric key over the network. For data integrity, the lightweight BLAKE2s hash function is employed, which provides a 256-bit output and consumes 15% less energy than MD5, offering superior protection against collision attacks.

Statistical Optimization

The system utilizes RNL within a two-stage adaptive scheme to estimate the optimal key parameters (e.g., key length and number of rounds) that minimize the loss function associated with resource consumption. Furthermore, Linear Regression models and Bayesian inference are integrated to reduce the probability of successful brute-force attacks to less than 0.1%, thus dynamically adapting the security strength based on network conditions

Performance Metric	Comparison vs. Traditional Algorithms (RSA/AES-128 ECB)	Improvement Source
Energy Consumption	18−22% Reduction	Lightweight components (Enhanced Blowfish, ECC, BLAKE2s)
Execution Time (Overall)	20−25% Reduction	Parallelized the F function, reduced the overhead of lightweight encryption
Blowfish F Function Speed	35−40% Reduction	Parallelization and modification of internal arithmetic operations
Brute-Force Attack Probability	Reduced to <0.1%	RNL-based Two-Stage Design and Linear Regression Modeling

4. Results and Discussion

The proposed framework was simulated and evaluated using the **iFogSim tool**. The results confirmed the effectiveness of the hybrid approach in addressing the security-efficiency challenge in IoT.

5. Conclusion

This study successfully developed an optimized lightweight hybrid cryptographic framework tailored for resource-constrained IoT environments. The framework integrates an enhanced, parallelized Blowfish algorithm with ECC for secure key exchange, and BLAKE2s for data integrity, all governed by a statistical two-stage adaptive design under the Reflected Normal Loss Function. The simulation results validate the effectiveness of the proposed approach, demonstrating substantial reductions in both energy consumption (18−22%) and execution time (20−25%) compared to traditional methods, thus providing a practical and highly secure solution for data protection in the Internet of Things.

6. Acknowledgement

The author would like to acknowledge the support of the Department of Basic Sciences, Bushehr Branch, Islamic Azad University, Bushehr, Iran.

References

[1] Tun, S. Y. Y., Madanian, S., & Mirza, F. (2021). Internet of things (IoT) applications for elderly care: a reflective review. Aging clinical and experimental research, 33(4), 855-867.

[2] Gope, Prosanta. Hwang, Tzonelih. (2020). A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system. Journal computers & security. Elsevier.

[3] Gangireddy, V. K. R., Kannan, S., & Subburathinam, K. (2021). Implementation of enhanced blowfish algorithm in cloud environment. Journal of Ambient Intelligence and Humanized Computing, 12(3), 3999-4005.

[4] Quilala, T. F. G., Sison, A. M., & Medina, R. P. (2018). Modified blowfish algorithm. Indones. J. Electr. Eng. Comput. Sci, 11(3), 1027-1034.

[5] Chandra, S., Paira, S., Alam, S. S., & Sanyal, G. (2014, November). A comparative survey of symmetric and asymmetric key cryptography. In 2014 international conference on electronics, communication and computational engineering (ICECCE) (pp. 83-93). IEEE.

[6] Medileh, S., Laouid, A., Euler, R., Bounceur, A., Hammoudeh, M., AlShaikh, M., ... & Khashan, O. A. (2020). A flexible encryption technique for the internet of things environment. *Ad Hoc Networks*, *106*, 102240.

[7] Xue, W., Luo, C., Shen, Y., Rana, R., Lan, G., Jha, S., ... & Hu, W. (2020). Towards a compressive-sensing-based lightweight encryption scheme for the Internet of Things. *IEEE Transactions on Mobile Computing*, *20*(10), 3049-3065.

[8] Rana, M., Mamun, Q., and Islam, R. (2022). "Lightweight cryptography in IoT networks: A survey." Future Generation Computer Systems, 129, 77-89.

[9] Zhang, X., Tang, S., Li, T., Li, X., Wang, C. (2023). "GFRX: A New Lightweight Block Cipher for Resource-Constrained IoT Nodes." Electronics, 12, 405.

[10] Lightweight Cryptography for Internet of Things: A Review (2024). EAI Endorsed Transactions on Internet of Things.

Declaration of Competing Interest: Authors do not have conflict of interest. The content of the paper is approved by the authors.

Author Contributions: Hassan Mazarei: Conceptualization, Methodology, Software, Validation, Formal Analysis, Investigation, Resources, Data Curation, Writing—Original Draft Preparation, Writing—Review & Editing, Visualization, Supervision, Project Administration.

Declaration of Competing Interest: Authors do not have conflict of interest. The content of the paper is approved by the authors.