IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Lightweight Hybrid Encryption Scheme for 8-bit RISC Embedded Systems

[1]M R Maanasa, [2]Yashwanth Gouda K Patil , [3]Prakash Hatagundi

[1]Assistant Professor, [2]Student, [3]Student

[1]Department of ECE, Sri Siddhartha Institute of Technology,SSAHE, Tumkur, Karnataka, India

[2,3]Student, Department of ECE, Sri Siddhartha Institute of Technology,SSAHE, Tumkur, Karnataka, India

Doi: https://doi.org/10.56975/ijcrt.v14i7.309965

Abstract: The rapid growth of wireless communication and Internet of Things (IoT) devices has increased the need for secure data transmission, especially in resource-constrained embedded systems. Traditional encryption algorithms such as AES and DES provide strong security but require high computational power and memory, making them unsuitable for 8-bit microcontrollers. This project presents a lightweight encryption and decryption system based on an 8-bit RISC processor for secure communication. The proposed system uses a hybrid encryption technique that combines Affine transformation, bit rotation, and key feedback mechanisms to ensure data confidentiality while maintaining low computational complexity. The ESP8266 Wi-Fi module is used to receive user input through a web interface and perform encryption. The encrypted data is then transmitted to an Arduino UNO, which acts as an 8-bit RISC processor and performs decryption using inverse operations. The system enables real time communication through serial (UART) transmission and displays both encrypted and decrypted data on an LCD module. The implementation demonstrates that secure communication can be achieved efficiently using simple mathematical operations on low cost and low power embedded platforms. This project highlights the feasibility of lightweight cryptographic techniques for applications in IoT and embedded systems where resources are limited. Keywords: 8-bit RISC processor, Encryption and Decryption, Lightweight Cryptography, Affine Transformation, Bit Rotation, Key Feedback Mechanism, ESP8266 Wi-Fi module, Arduino UNO, Secure Data Transmission, Embedded Systems, Internet of Things (IoT), and UART communication.

Index Terms - Encryption and Decryption, Lightweight Cryptography, Affine Transformation, Bit Rotation, Key Feedback Mechanism, ESP8266 Wi-Fi module, Secure Data Transmission, Internet of Things (IoT), and UART communication.

I. INTRODUCTION

The rapid growth of digital communication systems and the widespread adoption of Internet of Things (IoT) technologies have significantly increased the need for secure and reliable data transmission. In modern embedded environments, a large number of low-cost devices continuously exchange information over wireless communication networks. These embedded devices are commonly deployed in open and unsecured environments, making them vulnerable to various cyber threats such as eavesdropping, unauthorized access, data tampering, and information leakage. Therefore, ensuring data confidentiality and integrity has become an important requirement in embedded systems and IoT applications. Traditional encryption algorithms such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) provide strong security but require high computational power, larger memory resources, and increased

energy consumption. These requirements make them unsuitable for resource-constrained devices such as 8-bit microcontrollers, which are widely used in embedded systems because of their simplicity, low cost, and low power consumption [1][2][5].

Lightweight cryptography has emerged as an effective solution for secure communication in low-resource embedded systems. Lightweight cryptographic techniques focus on reducing computational complexity by utilizing simple arithmetic and logical operations while still maintaining acceptable security levels [5][6]. Several researchers have proposed lightweight encryption architectures and hardware accelerators for embedded and IoT applications [3][4]. In this project, a lightweight mini encryption and decryption unit is proposed using an 8-bit AVR RISC processor implemented on Arduino UNO based on the ATmega328P microcontroller. The proposed method combines affine transformation, bit rotation, and dynamic key feedback mechanisms to improve security with minimal hardware overhead. Affine transformation increases mathematical complexity, bit rotation improves diffusion characteristics, and key feedback introduces dynamic variations during encryption. Since these operations mainly involve simple mathematical and bitwise instructions, they are highly suitable for Reduced Instruction Set Computing (RISC) architecture, resulting in faster execution, reduced encryption time, lower power consumption, and reduced memory utilization [7][8][9].

To enable real-time communication, the ESP8266 Wi-Fi module is integrated into the system and configured as a web server. The ESP8266 receives input data through a browser interface, performs encryption, and transmits the encrypted information to Arduino UNO using UART serial communication protocol. The Arduino UNO performs decryption using inverse operations and displays both encrypted and decrypted data on an LCD module for visualization. The proposed system can also be extended for secure transmission of real-time sensor data in IoT environments. Compared to traditional algorithms, the proposed hybrid lightweight cryptographic architecture is more suitable for low-resource embedded applications where implementing complex encryption standards increases computational and hardware requirements [10]. The proposed system demonstrates better throughput, lower computational overhead, improved avalanche effect, and efficient execution on 8-bit RISC architecture. The work also provides a foundation for future enhancements such as FPGA implementation, advanced lightweight cryptographic algorithms, multi-round encryption, and secure large-scale IoT communication systems.

II. LITERATURE SURVEY

Recent advancements in embedded systems and Internet of Things (IoT) applications have significantly increased the demand for lightweight and efficient cryptographic techniques. Researchers have focused on developing secure encryption architectures that can operate efficiently on low-resource devices while maintaining acceptable levels of security. Several works have explored hardware accelerators, lightweight block ciphers, and optimized encryption mechanisms for embedded and wireless communication systems.

A RISC-V based System-on-Chip (SoC) architecture[1] is proposed for accelerating encryption and decryption operations at the edge. These architecture mainly focused on improving computational efficiency and reducing processing latency in homomorphic encryption systems. Similarly, D.-S. A resource-shared cryptographic coprocessor is designed and integrating with AES encryption/decryption with SHA-3 functionality. Their architecture reduced hardware utilization and improved resource efficiency, making it suitable for embedded applications[2]. Dayane Reis et al. [3] introduced IMCRYPTO, an in-memory computing architecture for AES encryption and decryption, where memory and computation are integrated to improve performance and reduce energy consumption.AES-RV, a hardware-efficient RISC-V accelerator was proposed with low-latency AES instruction extensions specifically designed for IoT security applications. Their work demonstrated improved execution speed and optimized hardware performance[4].

Several survey-based studies have also contributed to the field of lightweight cryptography. The comprehensive survey on lightweight cryptographic algorithms[5] highlighted the importance of lightweight security methods for IoT and embedded systems. NIST lightweight cryptography standards[6] reviewed and discussed implementation challenges, hardware constraints, and future research directions. A systematic review of lightweight cryptographic algorithms have been conducted by comparing different methods based on efficiency, security strength, and implementation complexity. Researcher [8] focused on developing and evaluating lightweight cryptographic algorithms for secure embedded systems and demonstrated the importance of balancing security and computational overhead. The time complexity

characteristics of NIST lightweight cryptographic finalists provided a comparative insights into their computational efficiency[9].

Researchers[11] introduced an PRESENT ultra-lightweight block cipher optimized for hardware-constrained systems. SIMON and SPECK lightweight block ciphers[12] was propoed which provided flexible and efficient cryptographic solutions for embedded applications.The LED lightweight encryption algorithm is developed for low-power devices with reduced computational requirements[13]. An energy-efficient AES architecture designed that minimized power consumption while maintaining encryption performance for embedded systems[14]. SPINS, a lightweight security protocol was proposed for wireless sensor networks that ensured secure communication using low-overhead encryption mechanisms[15].

In addition to lightweight block ciphers, secure end-to-end encryption methods have also been explored for IoT communication. A Curve25519 based lightweight end-to-end encryption technique was proposed for IoT devices, which improved communication security while reducing computational complexity. Their work highlighted the growing importance of lightweight security frameworks for modern wireless and IoT systems[10].

Although several lightweight cryptographic methods have been proposed in literature, many existing approaches still require comparatively higher computational resources, complex hardware architectures, or dedicated cryptographic accelerators. Most existing systems focus mainly on AES-based optimization techniques or hardware-intensive implementations. In contrast, the proposed work focuses on designing a lightweight hybrid encryption and decryption architecture using simple affine transformation, bit rotation, and dynamic key feedback mechanisms implemented on an 8-bit AVR RISC processor. The proposed method reduces computational overhead, memory utilization, and power consumption while enabling real-time secure communication using UART protocol and ESP8266 Wi-Fi module. Furthermore, the system can also support secure sensor data transmission in IoT applications, making it suitable for low-cost embedded communication environments.

TABLE I. Comprehensive Review Table

Ref. No	Technique Used	Advantages	Limitations
[1]	RISC-V Encryption Accelerator	Faster encryption processing	Higher hardware complexity
[2]	AES + SHA-3 Coprocessor	Reduced hardware utilization	Complex architecture
[3]	In-Memory AES Computing	Improved efficiency	High implementation cost
[4]	AES-RV Accelerator	Low latency operation	Hardware dependency
[5]	Lightweight Cryptography Survey	Broad comparison of methods	No practical implementation
[6]	NIST Lightweight Standards	Standardized security methods	Implementation challenges
[7]	Systematic Review	Efficiency comparison	Limited real-time testing
[8]	Lightweight Embedded Security	Improved embedded security	Complexity in scalability
[9]	Time Complexity Analysis	Computational comparison	No hardware implementation
[10]	Curve25519 Encryption	Secure IoT communication	Moderate computational load

[11]	PRESENT Cipher	Very lightweight	Limited security strength
[12]	SIMON and SPECK	Flexible implementation	Security concerns in some cases
[13]	LED Cipher	Low power operation	Lower throughput
[14]	Energy Efficient AES	Reduced power consumption	AES still computationally heavy
[15]	SPINS Protocol	Secure sensor communication	Limited scalability

From the literature survey, it is observed that lightweight cryptographic techniques play a major role in securing embedded and IoT systems with limited hardware resources. Existing works mainly focus on AES optimization, lightweight block ciphers, or hardware accelerators. However, many approaches still involve increased hardware complexity, higher computational overhead, or greater power consumption. Therefore, there is a need for a simple, low-cost, and computationally efficient encryption mechanism suitable for 8-bit RISC based embedded systems. The proposed work addresses this requirement by combining affine transformation, bit rotation, and dynamic key feedback mechanisms to achieve secure communication with reduced memory utilization, faster execution, lower power consumption, and real-time UART-based communication suitable for embedded and IoT applications.

III. METHODOLOGY

The block diagram shown in Fig.1 and Fig. 2 illustrates the overall architecture and working flow of the proposed lightweight hybrid encryption and decryption system designed using an 8-bit AVR RISC processor for secure embedded and IoT communication. The system mainly consists of a user interface, ESP8266 Wi-Fi module, Arduino UNO, UART serial communication unit, and LCD display module. Initially, the user enters the message through a web browser or mobile interface, and the message is transmitted wirelessly through Wi-Fi to the ESP8266 module. The ESP8266 acts as the encryption unit and converts the received message into ASCII format so that mathematical and logical operations can be efficiently performed. To improve security and processing efficiency, the complete message is divided into smaller 4-letter blocks before encryption. The proposed system employs a hybrid lightweight cryptographic technique combining affine transformation, XOR operation, bit rotation, and dynamic key feedback mechanisms. Affine transformation introduces mathematical confusion, XOR operation improves randomness and data masking, while bit rotation enhances diffusion by rearranging bit positions. In addition, the dynamic key feedback mechanism continuously updates the encryption key for each character or block, ensuring that repeated input characters produce different encrypted outputs. This combination improves security while maintaining low computational complexity, making the system suitable for low-resource embedded environments.

After encryption, the encrypted data blocks are transmitted to the Arduino UNO through UART serial communication protocol, which provides reliable and real-time communication between the ESP8266 and Arduino modules. The Arduino UNO, based on the ATmega328P 8-bit AVR RISC architecture, acts as the decryption unit in the system. The RISC architecture supports faster execution of lightweight arithmetic and logical instructions such as XOR, shifting, affine transformation(substitution cipher), and bit rotation due to its reduced instruction set and 8-bit data processing capability. The Arduino UNO receives the encrypted data block by block and performs decryption using inverse affine transformation, reverse bit rotation, inverse XOR operations, and reverse key feedback synchronization to recover the original message accurately. Since the encryption and decryption operations involve simple mathematical and bitwise computations, the proposed architecture achieves reduced encryption time, lower memory utilization, lower power consumption, and improved throughput compared to computationally intensive encryption methods. The use of UART communication also demonstrates the capability of secure real-time serial data transfer suitable for IoT and wireless embedded applications. Furthermore, the proposed system can also be extended for secure transmission of real-time sensor data such as temperature, humidity, biomedical, or industrial monitoring data in IoT environments.

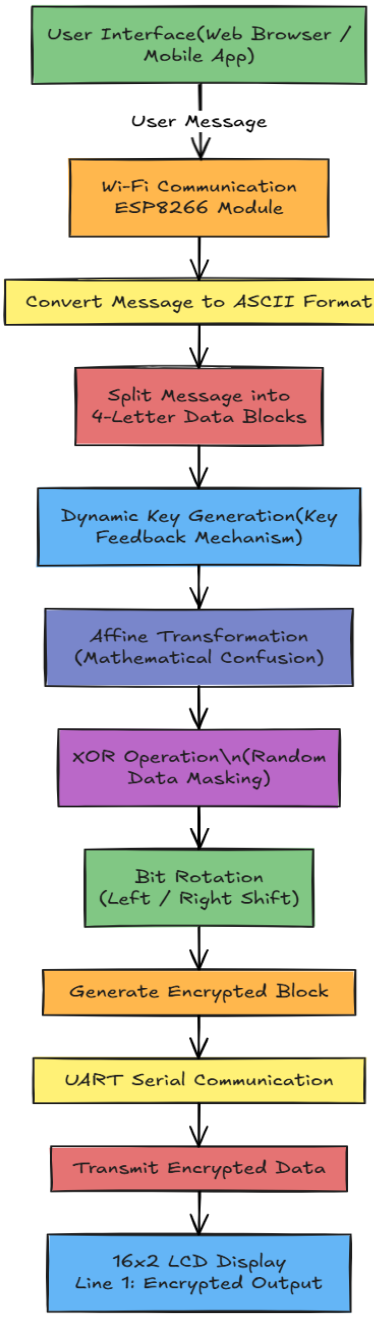

Fig. 1. Encryption block diagram with Affine Transformation.

Finally, the encrypted and decrypted outputs are displayed on a 16×2 LCD module for real-time visualization and verification of the system operation. The first line of the LCD displays the encrypted message, while the second line shows the decrypted original message. The proposed work mainly focuses on developing a lightweight cryptographic architecture rather than replacing highly secure industrial encryption standards such as AES or DES. The novelty of the work lies in the optimized combination of affine transformation, XOR operation, bit rotation, and dynamic key feedback implemented efficiently on an 8-bit RISC platform with minimal hardware requirements. Compared to traditional encryption approaches, the proposed system offers advantages such as low computational overhead, faster execution, reduced memory usage, real-time UART communication support, improved avalanche effect, and better suitability for low-cost embedded devices. The system can be further enhanced in future by integrating FPGA implementation, dynamic session-based key generation, multi-round encryption, secure IoT frameworks, entropy analysis, and advanced lightweight cryptographic techniques. Thus, the proposed system demonstrates that effective and secure communication can be achieved efficiently even on resource-constrained 8-bit embedded systems, making it suitable for educational research, lightweight IoT security applications, and embedded communication environments.

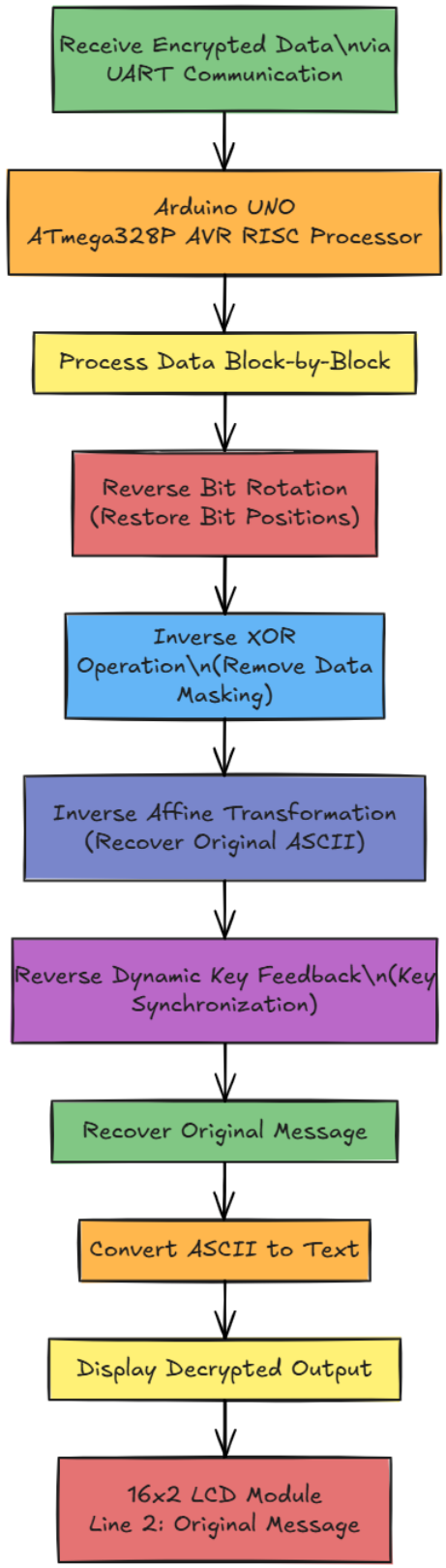

Fig. 2. Decryption block diagram with Affine Transformation .

IV. RESULTS AND DISCUSSION

The proposed system was successfully designed and implemented as shown in Fig. 3 The results in Fig. 4.confirms that the proposed system provides an effective balance between security, processing speed, and hardware efficiency, making it suitable for real-time small-data communication applications in embedded and IoT environments. The project was successfully designed and implemented using Arduino UNO, ESP8266 WiFi module, and a 16×2 LCD display for secure data transmission. The original message, “processor encryption and decryption,” was transmitted through WiFi and encrypted using the proposed lightweight hybrid algorithm based on affine transformation, bit rotation, and dynamic key feedback. The encrypted data was then successfully decrypted at the receiver side, and the corresponding

encrypted and decrypted outputs were displayed block-wise on the LCD, as shown in the figure. The system demonstrated reliable communication, fast processing speed, and low memory utilization on low-cost hardware platforms.

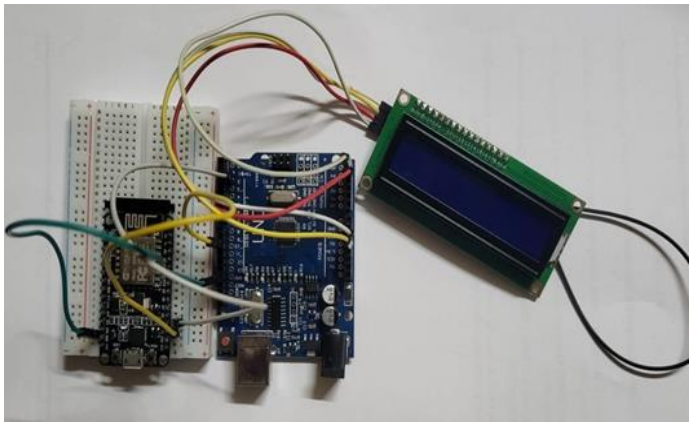

Fig. 3. Hardware Setup.

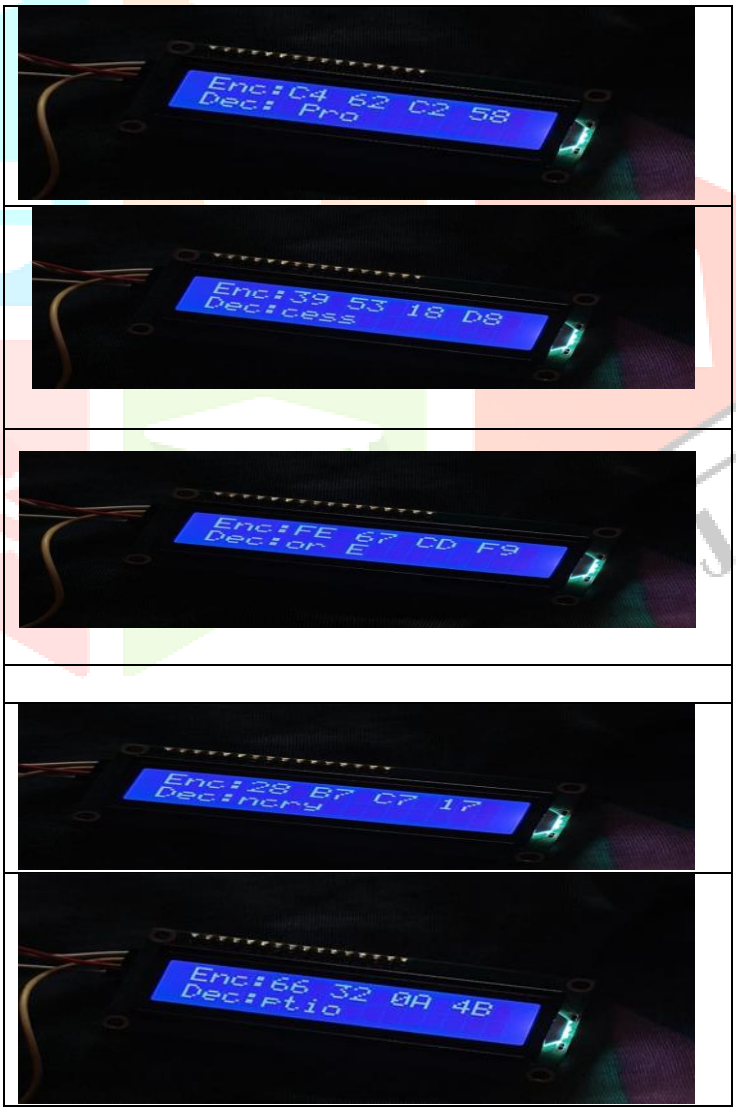

Fig. 4. Results of Proposed system and User Interfcae

The proposed approach is compared to conventional complex encryption techniques. These system is more suitable for resource-constrained embedded systems due to its lightweight nature and efficient performance.

TABLE II. Comparision with Proposed system

Parameter	**AES**	**DES**	**Proposed Method**
Processor Requirement	High	Moderate	Low
Memory Utilization	High	Moderate	Low
Power Consumption	High	Moderate	Low
Computational Complexity	High	Moderate	Low
Encryption Speed	Moderate	Moderate	High
Throughput	Moderate	Moderate	High
Hardware Cost	High	Moderate	Low
Suitability for IoT	Limited	Limited	Highly Suitable
Lightweight Nature	No	Partial	Yes
Real-Time UART Communication	Not Focused	Not Focused	Supported
Sensor Data Encryption	Possible	Possible	Supported Efficiently
Avalanche Effect	High	Moderate	Improved
Ease of Implementation	Complex	Moderate	Simple
Suitable for 8-bit RISC	Limited	Limited	Highly Suitable

V. CONCLUSION

This paper presented a lightweight hybrid encryption and decryption system using an Arduino UNO based 8-bit AVR RISC processor for secure embedded and IoT communication. The proposed system combines affine transformation, XOR operation, bit rotation, and dynamic key feedback mechanisms to achieve secure data transmission with low computational complexity, reduced memory utilization, lower power consumption, and faster execution speed. The ESP8266 Wi-Fi module enables real-time wireless communication using UART protocol, where encrypted data is securely transmitted and decrypted using inverse operations. The implementation demonstrates that lightweight cryptographic techniques can provide effective security for resource-constrained embedded systems without requiring complex hardware or high computational resources. The proposed method also improves throughput and avalanche effect while supporting secure real-time sensor data communication for IoT applications.

Overall, the system provides a low-cost, energy-efficient, scalable, and practical lightweight cryptographic solution suitable for embedded and IoT environments, while also offering scope for future enhancements such as FPGA implementation, advanced lightweight encryption methods, and secure large-scale IoT communication systems.

REFERENCES

[1] Z. Azad, G. Yang, R. Agrawal, D. Petrisko, M. Taylor, and A. Joshi, "RISE: RISC-V SoC for En/decryption Acceleration on the Edge for Homomorphic Encryption," IEEE paper (also available in archives).

[2] D.-S. Kundi, A. Khalid, A. Aziz, C. Wang, M. O'Neill, et al., "Resource-Shared CryptoCoprocessor of AES Enc/Dec With SHA-3," IEEE Transactions on Circuits and Systems I: Regular Papers, Vol. 67, No. 12, Dec. 2020.

[3] Dayane Reis, Haoran Geng, Michael Niemier, Xiaobo Sharon Hu, "IMCRYPTO: An InMemory Computing Fabric for AES Encryption and Decryption,", 2021.

[4] Van Tinh Nguyen, Phuc Hung Pham, Vu Trung Duong Le, et al., "AES-RV: HardwareEfficient RISC-V Accelerator with Low-Latency AES Instruction Extension for IoT Security," 2025.

[5] Suzan Sallam and Babak D. Beheshti, "A Survey on Lightweight Cryptographic Algorithms," IEEE Paper / Research Survey, 2021.

[6] Jasmin Kaur, Alvaro Cintas Canto, Mehran Mozaffari Kermani,"A Comprehensive Survey on Lightweight Cryptography Standard (NIST)," IEEE / ArXiv, 2023.

[7] Mohsin Khan, Elisavet Kozyri, Håvard Dagenborg,"Systematic Review of Lightweight Cryptographic Algorithms," IEEE / ArXiv, 2026.

[8] Brahim Khalil Sedraoui, Abdelmadjid Benmachiche,"Developing and Evaluating Lightweight Cryptographic Algorithms for Secure Embedded Systems," IEEE / ArXiv 2026.

[9] Najmul Hasan, Prashanth BusiReddyGari,"Time-Complexity Characterization of NIST Lightweight Cryptography Finalists," 2026.

[10] S. Ullah, M. A. Khan, A. Almogren, M. Alrubaian, M. Zuair, and I. U. Din, "Curve25519 Based Lightweight End-to-End Encryption for IoT Devices," *IEEE Access*, vol. 9, pp. 123456–123468, 2021.

[11] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, Vienna, Austria, Sep. 2007, pp. 450–466.

[12] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK Lightweight Block Ciphers," in *Proceedings of the 52nd Annual Design Automation Conference (DAC)*, San Francisco, CA, USA, 2015, pp. 1–6.

[13] J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, "The LED Block Cipher," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, Nara, Japan, Sep. 2011, pp. 326–341.

[14] A. Aysu, E. Gulcan, and P. Schaumont, "Energy Efficient AES Implementations for Embedded Systems," *IEEE Transactions on Computers*, vol. 63, no. 12, pp. 3017–3029, Dec. 2014.

[15] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security Protocols for Sensor Networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, Sep. 2002.