INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 4, April 2026 | ISSN: 2456-4184 | IJNRD.ORG

HIGH-PERFORMANCE SECURE IOT DATA TRANSMISSION

[1]Guntakindapalli Pavan Kumar Reddy, [2]G.S. Harinarayanan, [3]Rayapaneni Jagan
[1]Student, [2]Student, [3]Student
[1,2,3]Department of Computer Science and Engineering
[1,2,3]Dhanalakshmi College of Engineering, Chennai, India

Abstract: The rapid expansion of the Internet of Things (IoT) has introduced significant challenges in securing data transmitted between connected devices. Existing encryption systems based on SM3 and SM4 algorithms, while functional, suffer from limited global compatibility, high energy consumption, and separation of encryption and authentication functions, making them less suitable for resource-constrained IoT environments. This paper presents the design and implementation of a low-power, low-cost RISC-V processor integrated with an AES-GCM (Galois/Counter Mode) encryption accelerator and Elliptic Curve Cryptography (ECC) for secure key management. The proposed system is designed using Verilog HDL and implemented on the Xilinx FPGA platform using Xilinx Vivado. AES-GCM provides authenticated encryption in a single hardware operation, eliminating the need for a separate hashing step. ECC enables efficient public-key operations with smaller key sizes, well-suited to constrained IoT devices. Simulation results demonstrate significant improvement in encryption security and key management efficiency over the existing SM3/SM4-based system, with minimal impact on performance and power consumption.

Index Terms: *Internet of Things (IoT), RISC-V Processor, AES-GCM (Galois/Counter Mode), Elliptic Curve Cryptography (ECC), Authenticated Encryption, Verilog HDL, FPGA, SM3, SM4, Hardware Accelerator.*

I. INTRODUCTION

The rapid proliferation of Internet of Things (IoT) devices has revolutionized industries and daily life, enabling seamless communication between devices and fostering new possibilities in automation, monitoring, and control. However, as IoT systems increasingly handle sensitive and critical data, the security and reliability of data transmission have emerged as major concerns. Cyberattacks on IoT devices and networks can lead to breaches of privacy, financial losses, and operational disruptions, underscoring the urgent need for robust, efficient, and secure encryption mechanisms tailored for IoT environments [1].

One of the primary challenges in securing IoT systems is achieving a balance between robust encryption and resource efficiency. IoT devices are often constrained in terms of power, processing capability, and cost, necessitating lightweight solutions that provide strong encryption without overwhelming limited device resources. The Advanced Encryption Standard (AES) has proven effective in addressing this challenge, offering strong security, high-speed operation, and straightforward key management [2].

This paper presents the design and implementation of a low-power, low-cost RISC-V processor integrated with an AES-GCM encryption accelerator and ECC for public-key operations. The RISC-V architecture, known for its simplicity, scalability, and open-source nature, serves as an ideal foundation for IoT applications. The proposed system replaces the existing hybrid encryption approach based on SM3 and SM4, addressing all its limitations within a unified, globally accepted cryptographic framework [3].

II. EXISTING SYSTEM

The existing system employs a hybrid encryption scheme combining the SM3 hashing algorithm and the SM4 block cipher within the encryption accelerator of the RISC-V processor. The accelerator block receives 128-bit input data and a 128-bit key. SM4 produces a 128-bit encrypted output while SM3 produces a 256-bit hash output. These two outputs are merged in the encrypted data generation block to produce a final 384-bit encrypted output [1].

A. SM3 Algorithm

SM3 is a cryptographic hash algorithm that generates a 256-bit hash value. For a message m of length l (l < 2128), SM3 performs padding followed by iterative compression. The padded message is split into 512-bit

blocks and processed iteratively using a compression function CF, producing the final 256-bit hash value used as a message authentication code (MAC) to verify data integrity and authenticity.

B. SM4 Algorithm

SM4 is a block cipher algorithm with a block length and key length both of 128 bits. It uses an unbalanced Feistel structure and iterates its round functions 32 times in both encryption and key expansion. The decryption structure is the same as encryption, except the round keys are used in reverse order. SM4 provides symmetric data encryption to ensure confidentiality of transmitted data.

C. Disadvantages of Existing System

The existing SM3 and SM4 based system has the following limitations: (1) Both algorithms are primarily Chinese national standards with limited global compatibility. (2) SM4 handles encryption alone, requiring SM3 to be computed separately for authentication, complicating implementation. (3) SM3 is computationally intensive, less suitable for resource-constrained IoT devices. (4) Fewer hardware accelerator libraries are available for SM3/SM4 compared to AES. (5) The dual-algorithm approach consumes more processing cycles and power, a significant drawback for battery-operated IoT devices [1].

III. PROPOSED SYSTEM

The proposed system replaces SM3 and SM4 with AES-GCM for authenticated encryption and ECC for public-key key management. Both modules are integrated as hardware accelerators within the RISC-V processor and implemented using Verilog HDL on the Xilinx FPGA platform [3][4].

A. AES-GCM Encryption Accelerator

The Advanced Encryption Standard (AES) is a symmetric block cipher adopted by NIST in 2001, operating on 128-bit data blocks with key lengths of 128, 192, or 256 bits. AES applies transformations over multiple rounds: 10 rounds for 128-bit key, 12 for 192-bit, and 14 for 256-bit. Each round applies four transformations on a 4×4 byte state array: SubBytes (non-linear S-Box substitution), ShiftRows (cyclic row shifts), MixColumns (polynomial multiplication over GF(28)), and AddRoundKey (XOR with round key from Key Generator). AES is implemented in Galois/Counter Mode (GCM), providing both encryption and authentication in a single operation through an authentication tag, eliminating the separate SM3 hashing step [2][3].

B. Elliptic Curve Cryptography (ECC)

ECC is integrated for public-key operations including key exchange and management. ECC achieves robust security with significantly smaller key sizes compared to other asymmetric schemes such as RSA, making it highly efficient for resource-constrained IoT environments. The combined use of AES-GCM for data encryption and ECC for key management ensures both data confidentiality and secure key distribution [3].

C. RISC-V Processor Architecture

RISC-V is an open-standard ISA that can be freely adopted and modified, ideal for custom IoT processor designs. The implemented processor follows a single-cycle datapath comprising a Program Counter (PC), Instruction Memory, Control Unit, Register File, and ALU. The PC increments by 4 after each clock cycle. The Control Unit decodes the opcode to generate control signals. The ALU performs arithmetic and logical operations. The encryption accelerator connects directly to the ALU output, producing encrypted output in the proposed AES-GCM configuration [3][4].

IV. COMPARISON: EXISTING VS. PROPOSED SYSTEM

Table 1: Existing System (SM3 + SM4) vs. Proposed System (AES-GCM + ECC)

Parameter	Existing System (SM3 + SM4)	Proposed System (AES-GCM + ECC)
Encryption Method	SM4 – 128-bit symmetric block cipher	AES-GCM – Authenticated Encryption
Integrity / Hashing	SM3 – 256-bit hash (separate step)	GCM Authentication Tag (built-in)
Key Management	Separate mechanism required	ECC-based key exchange
Global Compatibility	China national standard only	NIST worldwide standard
Authentication	Requires additional separate step	Built-in with GCM authentication tag

Power Efficiency	Moderate	High (hardware accelerated)
IoT Suitability	Limited – less ecosystem support	High – low-power optimized design
Implementation	Verilog HDL on Xilinx FPGA	Verilog HDL on Xilinx FPGA (Vivado)

V. IMPLEMENTATION

A. Hardware Description Language

Both the RISC-V processor and the AES-GCM encryption accelerator are designed using Verilog HDL, adhering to the design principles of low power and low cost. FPGA-based prototyping enables rapid development, testing, and iteration while providing insights into resource utilization, power consumption, and encryption speed [3].

B. Xilinx Vivado Development Environment

The Xilinx Vivado IDE was used for synthesis, simulation, implementation, and debugging. The design was synthesized into a gate-level netlist and mapped onto the Xilinx Zynq-7000 family FPGA (Part: xc7z007sclg400-1, Package: clg400, Speed Grade: -1). Functional and timing simulations were conducted using Vivado's integrated simulator to verify correctness before bitstream generation [3].

C. Simulation Results

Simulation results from Xilinx Vivado demonstrate that the proposed AES-GCM encryption accelerator integrated into the RISC-V processor achieves correct and verified encryption output. The proposed system simulation waveforms show inputs in1[127:0] and in2[127:0] with the correct ciphertext[127:0] output, verified against AES test vectors. The proposed AES-GCM system produces a compact 128-bit authenticated ciphertext, compared to the 384-bit output of the existing SM3+SM4 system, confirming correct hardware operation with improved efficiency [3].

VI. ADVANTAGES AND APPLICATIONS

The proposed system provides the following advantages: Strong Security through AES-GCM combined encryption and authentication with ECC key exchange; Energy Efficiency through RISC-V hardware acceleration; High Performance enabling real-time secure communication; Cost-Effectiveness through RISC-V open-source design; and Compact Design through ECC small key sizes suitable for constrained IoT devices [3].

Application domains include Smart Homes (securing smart locks and cameras), Healthcare (protecting wearable health monitor data), Industrial IoT (securing factory sensor networks), Smart Cities (traffic management and public safety systems), and Transportation (vehicle-to-vehicle and vehicle-to-infrastructure communication) [3].

VII. CONCLUSION

This paper presented the design and implementation of a secure and efficient data transmission system for IoT using a RISC-V processor integrated with an AES-GCM encryption accelerator and ECC for public-key operations. The proposed system addresses all limitations of the existing SM3/SM4 approach by providing globally compatible, authenticated encryption in a single hardware-accelerated operation. Verified on Xilinx Vivado, the system confirms functional correctness and improved security performance. Future work will explore further power optimization and deployment in critical domains such as healthcare, automotive, and industrial IoT.

REFERENCES

[1] Wang Tong, Cui Wen Peng, Li Tong, Wang Liang, Li Hao, and Chi Ying Ying, "The Research of the SM2, SM3 and SM4 Algorithms in WLAN of Transformer Substation," 2019 3rd International Conference on Electronic Information Technology and Computer Engineering (EITCE), 2019.

[2] Yuan-Hsi Chou and Shih-Lien L. Lu, "A High Performance, Low Energy, Compact Masked 128-Bit AES in 22nm CMOS Technology," 2019 International Symposium on VLSI Design, Automation and Test (VLSI-DAT), 2019.

[3] Duc-Thinh Nguyen-Hoang, Khai-Minh Ma, Duy-Linh Le, Hong-Hai Thai, Tran-Bao-Thuong Cao, and Duc-Hung Le, "Implementation of a 32-Bit RISC-V Processor with Cryptography Accelerators on FPGA and ASIC," IEEE Ninth International Conference on Communications and Electronics (ICCE), 2022.

[4] Mao-Hsu Yen, Cheng-Hao Tsou, Tzu-Feng Lin, Yih-Hsia Lin, Yuan-Fu Ku, and Chien-Ting Kao, "VLSI Implementation of RISC-V MCU with a variable stage pipeline," IEEE 6th International Conference on Knowledge Innovation and Invention (ICKII), 2023.
[5] H. Zhenbo, Teach You to Design CPUs Hand-in-Hand; RISC-V Processor, People's Posts and Telecommunications Press, Beijing, China, 2018.
[6] H. Fu, G. Bai, and X. Wu, "Low-cost hardware implementation of SM4 based on composite field," Proceedings of the 2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference, Chongqing, China, May 2016, pp. 260-264.