ISSN 2277-2685

IJESR/April-June. 2026/ Vol-16/Issue-2/990-994

Full Length Article

Low-Power and Area Optimized AES-CMAC Architecture with LP-LFSR for Secure Data Authentication

Muddada Rohini[1], Dr. Papa Rao Challagundla[2], Jyothula sowjanya[3]

[1]M.Tech Student, GVR&S College of Engineering and Technology, Budampadu-522017, Guntur (Dt), A.P., India.
[2,3]Associate professor, GVR&S College of Engineering and Technology, Budampadu-522017, Guntur (Dt), A.P., India.
Mail Id: rohini.muddada@gmail.com[1] , drcprao2025@gmail.com[2] , jyothulasowjanya@gmail.com[3]

Accepted 01-06-2026

Abstract— *Secure communication systems use cipher-based Message Authentication Codes like Advanced Encryption Standard AES-CMAC to protect data, communications, and user authentication. Due to frequent toggling during key generation and simultaneous processing, classic AES-CMAC systems consume a lot of power and hardware. This research presents a power- and area-efficient AES-CMAC design to address these concerns. This design uses an optimized LP-LFSR for pseudo-random key generation. The design's capacity to process four 128-bit blocks in parallel makes 512-bit data stream encryption and authentication efficient. The LP-LFSR refreshes the key register at predefined clock intervals to reduce dynamic power consumption and switching activity while retaining functionality. The FPGA-based Verilog implementation combines AES encryption, CMAC authentication, decryption, and verification. While retaining frequency and low latency, experimental results show 5.64% and 10.75% lower power consumption and LUT utilization than traditional systems. Due to its balanced security, space, performance, and power efficiency, the suggested architecture is appropriate for low-power VLSI applications, embedded systems, and the IoT.*

Keywords— *AES, Low-Power LFSR (LP-LFSR), Cryptographic Authentication and Verilog HDL***.**

I. INTRODUCTION

The fast development of digital communication systems, IoT devices, cloud computing, and embedded platforms has boosted demand for energy-efficient and safe cryptographic solutions. AES is one of the most used encryption systems due to its hardware implementation, fast throughput, and strong security [1], [2]. Traditional AES systems, which offer secrecy, lack message authentication and integrity verification. AES and the Cipher-based Message Authentication Code (CMAC) allow secure communication and authenticated encryption to overcome these constraints [3], [4]. AES-CMAC on FPGAs can perform high-speed parallel processing, however the continual switching and repetitive key generation procedures increase device complexity and dynamic power consumption [5], [6].

This work offers a Low-Power Linear Feedback Shift Register-based AES-CMAC architecture for secure FPGA applications to address these issues. The suggested architecture processes four 128-bit message segments simultaneously, providing 512-bit data stream encryption and authentication. By refreshing the pseudo-random key register at predefined clock intervals, the LP-LFSR maintains cryptographic capabilities while reducing dynamic power consumption and switching transitions. All architecture is implemented in Verilog HDL and synthesised with Xilinx Vivado. LP-LFSR-based AES-CMACs have lower anticipated power consumption and LUT utilisation than traditional systems, according to experiments. This design also maintains a constant operating frequency and low propagation delay. Consequently, the proposed design provides a viable compromise between security, speed, hardware complexity, and power efficiency for cryptographic applications that are based on FPGAs and VLSIs that are lightweight.

II. LITERATURE REVIEW

The primary focus of recent research on FPGA-based cryptographic designs has been to

enhance the performance, security, and power efficiency of AES implementations. The Rijndael algorithm, which was subsequently standardised as the Advanced Encryption Standard (AES), was devised by Daemen and Rijmen due to its effective hardware implementation and robust security [1]. Hodjat and Verbauwhede proposed a fully pipelined AES processor on FPGA to achieve high throughput, although it increased hardware complexity and power consumption due to extensive parallelism [2]. McLoone and McCanny further improved AES performance using optimized pipelined FPGA architectures for high-speed encryption [3]. Subsequent works have explored low-area and high-speed AES implementations; however, most of these designs focus primarily on encryption performance without providing integrated authentication and integrity verification.

AES-CMAC was standardised as a message authentication method utilising block cyphers in order to address safe authentication [5], [6]. Recent research has studied LFSR-based pseudo-random key generation methods to improve cryptographic system security and hardware delay. LFSR-based key generation was employed in RECO-LFSR's reconfigurable low-power cryptographic processor for IoT [7]. Area-efficient LFSR designs minimise hardware complexity and switching activity, according to Salehi [8]. However, constant register updating increases dynamic power consumption, hindering standard LFSR-based techniques. These restrictions inspired this work's Low-Power LFSR (LP-LFSR)-based AES-CMAC architecture. By refreshing the key register at specified clock intervals, this design lowers switching activity and allows efficient and safe concurrent authentication of 512-bit data streams.

III. AES-CMAC using LP-LFSR

The proposed work presents a secure and low-power FPGA-based cryptographic architecture that uses AES-CMAC in conjunction with a Low-Power Linear Feedback Shift Register (LP-LFSR). Verilog HDL is utilised to implement the whole system, while Xilinx Vivado is used for synthesis. The architecture has three key components: AES encryption, AES-CMAC authentication, and AES-CMAC with LP-LFSR. The proposed approach enables authenticated encryption of a 512-bit data stream by processing four distinct 128-bit message blocks at the same time. While CMAC employs chained AES operations to provide message authentication and integrity verification, AES is employed for secure encryption [1-3].

At the outset, the initial plaintext block m1 is encrypted with AES and a 128-bit key K:

$$c1 = AES(m1,K) \quad (1)$$

Before encryption, the second and third message blocks are XORed with the ciphertexts of the preceding message blocks.

$$x1 = m2 \oplus c1 \quad (2)$$

$$c2 = AES(x1,K) \quad (3)$$

$$x2 = m3 \oplus c2 \quad (4)$$

$$c3 = AES(x3,K) \quad (5)$$

In the final step, the final message block is combined with the generated subkey and the previous ciphertext before final encryption:

$$x3 = c3 \oplus mn \oplus gkey \quad (6)$$

$$Cn = AES(x3,K) \quad (7)$$

The authenticated CMAC output is represented by the final ciphertext cn. The LP-LFSR dynamically generates a 128-bit pseudo-random encryption key that is supplied to all AES encryption stages. The key that is generated is denoted as K is LP-LFSR (seed).The suggested LP-LFSR reduces needless switching transitions by updating only at predetermined clock intervals, in contrast to traditional LFSRs that update every clock cycle. The suggested LP-LFSR employs the following feedback operation:

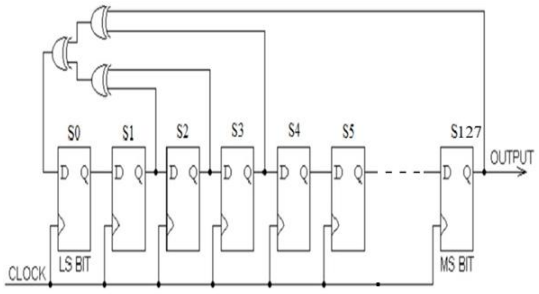

Fig 1. Low power LFSR

A counter mechanism is used to regulate the register updating process. Only when the count is 8 does the LP-LFSR update; otherwise, the prior register state is maintained, thereby reducing switching activity and dynamic power consumption.

While retaining secure authenticated encryption capabilities, the suggested LP-LFSR-based AES-CMAC design dramatically lowers switching activity and predicted power consumption. Results from experimental synthesis show that the design delivers lower power consumption and lower LUT utilization when compared to traditional AES-CMAC systems. For FPGA-based secure communication systems, Internet of Things devices, embedded cryptographic processors, and low-power VLSI security applications, the suggested architecture offers an effective trade-off among security, hardware complexity, operational speed, and power efficiency.

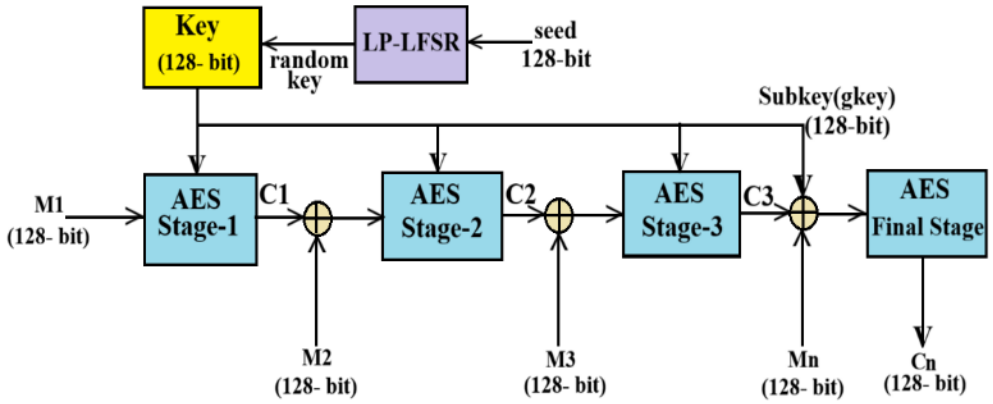

Fig2. AES CMAC using LP-LFSR

IV. RESULTS

RTL Schematic: The hardware blueprint used to compare the actual design to the intended architecture is represented by the Register Transfer Level (RTL) diagram. It displays internal block interconnections for data flow analysis and is produced using Verilog/VHDL. Fig 3 displays the RTL schematic of the suggested AES-CMAC employing LP-LFSR.

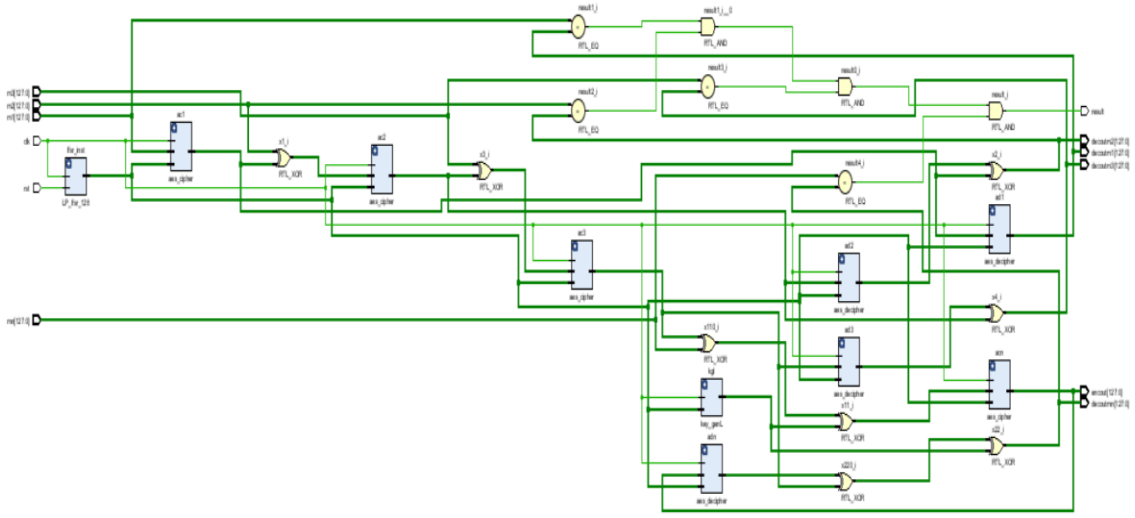

Fig3. RTL Schematic of AES CMAC using LP-LFSR

Simulation: The simulation waveform demonstrates that the proposed AES-CMAC architecture successfully processed four 128-bit message blocks. The waveform shows that the input data, control signals, and output responses are properly synchronised over several clock cycles. Throughout the simulation, proper signal transitions confirm the accuracy of the encryption and authentication operations. The data show that the recommended design is functionally accurate.

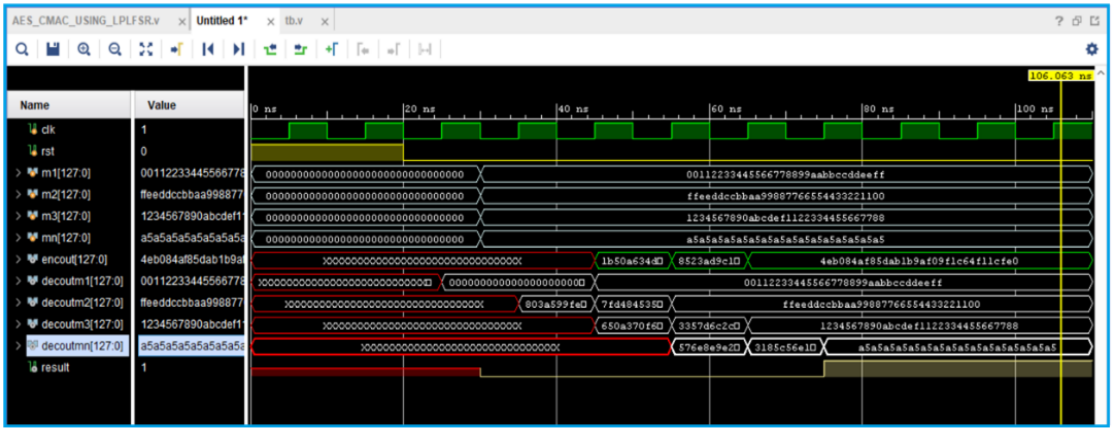

Fig 4. Simulated wave form of AES CMAC using LP-LFSR

Table I Parameter comparison

Parameter	AES	AES-CMAC	AES-CMAC using LP-LFSR
No. of LUTs	20983	97319	86975
Frequency (MHz)	51.895	48.919	49.799
Delay (ns)	47.769	2.481	2.481
Power(mWatt)	8899.847	31958.633	30155.967
Security level	High	Very high	Extreme high
Block size	128bit	128-bit per message block	128-bit per message block
Key usage	Fixed key	Fixed Authentication Key	Dynamically Randomized Keys

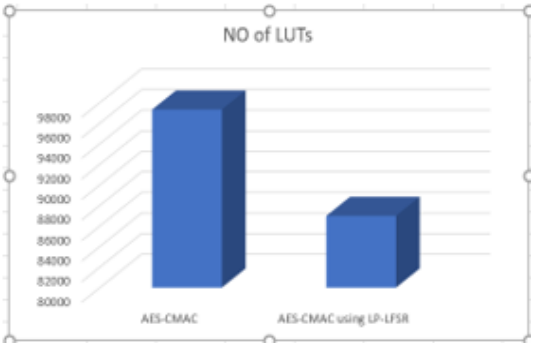

Fig 5. LUT comparison barograph

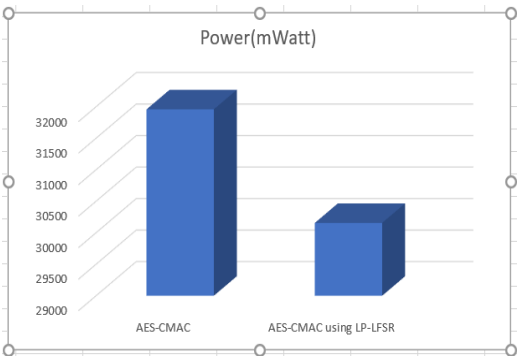

Fig 6. Power comparison barograph

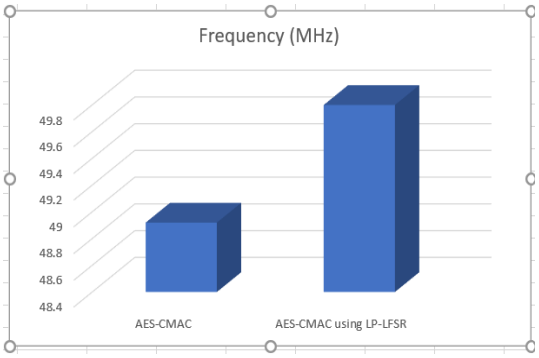

Fig7.Frequency comparison barograph

the parameter analysis, the proposed AES-CMAC with LP-LFSR has higher area and power efficiency than the previous design. The design maximises hardware use by reducing switching activity and increasing performance. The proposed technology reduces total power consumption while ensuring a consistent operating frequency. These findings validate the architecture's suitability for low-power secure communication applications.

CONCLUSION

A low-power AES-CMAC architecture with an optimized LP-LFSR for effective dynamic key generation and decreased switching activity was proposed in this work. In addition to increasing hardware efficiency, the suggested architecture allows for the concurrent processing of four 128-bit message blocks, enabling high-throughput encryption and authentication of a 512-bit data stream. In comparison to the traditional AES-CMAC architecture, experimental findings demonstrate notable gains with a 10.63% reduction in LUT utilization and a 5.64% reduction in power consumption, all while maintaining a constant operating frequency and dependable performance. Further power optimization employing cutting-edge low-power techniques like clock and power gating, ASIC implementation for real-world deployment analysis, enhanced parallelism for faster throughput, and integration of more secure key generation techniques are all part of this work's future scope. The architecture will also be more appropriate for edge computing, the Internet of Things, and new low-power secure communication systems by strengthening defense against side-channel attacks and modifying the design for lightweight cryptographic standards.

REFERENCES

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

[2] A. Hodjat and I. Verbauwhede, “A 21.54 Gbits/s Fully Pipelined AES Processor on FPGA,” *IEEE Symposium on Field-Programmable Custom Computing Machines*, 2004.

[3] M. McLoone and J. V. McCanny, “High-Performance Single-Chip FPGA Rijndael Algorithm Implementations,” *IEEE Workshop on Signal Processing Systems*, 2001.

[4] T. Manoj Kumar et al., “A Low Area High Speed FPGA Implementation of AES Architecture for Cryptography Application,” *Electronics*, vol. 10, no. 16, 2021.

[5] M. Dworkin, “Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication,” NIST SP 800-38B, 2005.

[6] RFC 4493, “The AES-CMAC Algorithm,” RFC 4493 – The AES-CMAC AlgorithmM. McLoone and J. V. McCanny, “High-Performance Single-Chip FPGA Rijndael Algorithm Implementations,” *IEEE Workshop on Signal Processing Systems*, pp. 383–392, 2001.

[7] S. A. Salehi, “Area-Efficient LFSR-Based Stochastic Number Generators with Minimum Correlation,” *IEEE Design & Test*, vol. 41, no. 1, 2024.

[8] J. Kaur, A. C. Canto, M. M. Kermani, and R. Azarderakhsh, “A Comprehensive Survey on the Implementations, Attacks, and Countermeasures of the Current NIST Lightweight Cryptography Standard,” *arXiv preprint arXiv:2304.06222*, 2023.

[9] NIST, “Advanced Encryption Standard (AES),” FIPS PUB 197, National Institute of Standards and Technology, 2001.

[10] M.Dworkin, “Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication,” NIST Special Publication 800-38B, 2005.

[11] A. Hodjat and I. Verbauwhede, “A 21.54 Gbits/s Fully Pipelined AES Processor on FPGA,” *IEEE Symposium on Field-Programmable Custom Computing Machines*, pp. 308–309, 2004.