ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

REALIZATION OF A CRYPTO COPROCESSOR WITH AES AND LFSR-BASED ENCRYPTION AND DECRYPTION IN VLSI

GEMMELI PAPARAO[1], T. PATTALU NAIDU[2]
[1]Research Scholar, AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY, TAMARAM, Narsipatnam Road, Makavarapalem Mandal -531113

[2]Assistant Professor, AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY, TAMARAM, Narsipatnam Road, Makavarapalem Mandal -531113

Abstract: AES Using LFSR (Linear Feedback Shift Register) is an approach that integrates the AES encryption algorithm with the use of LFSR-based techniques to enhance the performance, security, and hardware efficiency of the cryptographic system. AES (Advanced Encryption Standard) is one of the most widely used symmetric-key encryption algorithms, offering high security and fast encryption. However, the need for efficient hardware implementations has led to the exploration of various methods to speed up the encryption process while maintaining security.The integration of LFSR into the AES structure primarily targets the generation of pseudo-random key streams for key expansion or stream cipher generation, improving the randomness and speed of the key schedule, which is a vital part of the AES algorithm. By utilizing LFSR-based key generation techniques, the AES cipher can achieve faster processing speeds, lower hardware complexity, and reduced power consumption in embedded systems, FPGA, and ASIC implementations.

Keywords—AES, IoT , Energy Consumption , Resource Constraint Environments (RCEs) , Cryptography and LFSR.

I. INTRODUCTION

The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security to its electronic data systems. This publication specifies a cryptographic algorithm, the Advanced Encryption Standard (AES) which may be used by Federal organizations to protect sensitive data. Protection of data during transmission or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by the data.

The algorithms uniquely define the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form. The Advanced Encryption Standard is being made available for use by Federal agencies within the context of a total security program consisting of physical security procedures, good information management practices, and computer system/network access controls. Data encryption (cryptography) is utilized in various applications and environments. The specific utilization of encryption and the implementation of the AES will be based on many factors particular to the computer system and

its associated components. In general, cryptography is used to protect data while it is being communicated between two points or while it is stored in a medium vulnerable to physical theft. Communication security provides protection to data by enciphering it at the transmitting point and deciphering it at the receiving point. File security provides protection to data by enciphering it when it is recorded on a storage medium and deciphering it when it is read back from the storage medium. In this the key must be available at the transmitter and receiver simultaneously during communication.

II. LITERATURE SURVEY

The literature survey focuses its attention towards AES, particularly to utilize under low power consumption, high security, better performance and improved efficiency. The implementation feasibility in VLSI environment is also studied and analyzed in depth. Fault Analysis in AES-CBC Algorithm Using Hamming Code for Space Applications ,National institute of standard and technology (2001) presented computer security. Two FIPS publications already prove the modes of operation for two particular block cipher algorithms . Four of these modes are equivalent to the ECB, CBC, CFB, and OFB modes with the Triple DES algorithm (TDEA) as the underlying block cipher. For any given key, the block cipher algorithm of the mode consists of two function that are inverses of each other.

Francois-Xavier Standaert, Gael Rouvroy, Jean-Jacques Quisquater, and Jean-Didier Legat presented (2004) discussed about the Efficient Implementation of Rijndael Encryption in Reconfigurable Hardware. It addressed various approaches for efficient FPGA implementations of the Advanced Encryption Standard algorithm. In implementation of block ciphers, several strategies can produce effective designs. Inherent constraints of FPGAs were taken into account in order to define an efficient methodology. Inside these architectures, the authors proposed algorithmic optimizations for the substitution box, and also efficient combinations between the diffusion layer and the key addition. 25 Farhadian.A and Aref.M.R (2009) presented efficient method for simplifying and approximating the s-boxes based on power functions

III. AES (ADVANCED ENCRYPTION STANDARD)

Advanced encryption standard is the most widely used cryptographic algorithm that is compatible with hardware and software at the same time. The data input given is encrypted by AES using a key provided by the user or the developer. AES is a block cipher that transform the 128-bit input data by [19]permutations and combinations using a key of size 128-bit, 192-bit or 256-bit secret key. The National Institute of standards and Technology have announced in Jan 1997 to initiate the development of new AES cipher. In October 2001 they have announced that the new [7]Rijndal algorithm have won the competition between different algorithms developed and proposed that the new Advanced Encryption Standard will be Rijndal algorithm. From there on-wards AES is being widely used as the base of cryptography in terms of hardware and software. It have replaced the existing [7]DES and Triple DESto provide better security benefits and secure

architecture. AES is being widely used in the commercial market for different kind of data transactions. It pawed the way to make the cryptographic algorithm widespread in the market. There are several hardware architecture using the benefits of AES to perform better encryption with the help of other hash algorithms like SHA, MD5 etc.

Steps In AES Algorithm

• Key Expansions : The input key is expanded for the number of rounds plus one for the [6]addround key step in each stage. The keys are obtained by from the cipher key by the Rijndael's key schedule. • Initial Round a) AddRoundKey : Each byte of the state is combined with the round key block using bitwise XOR.

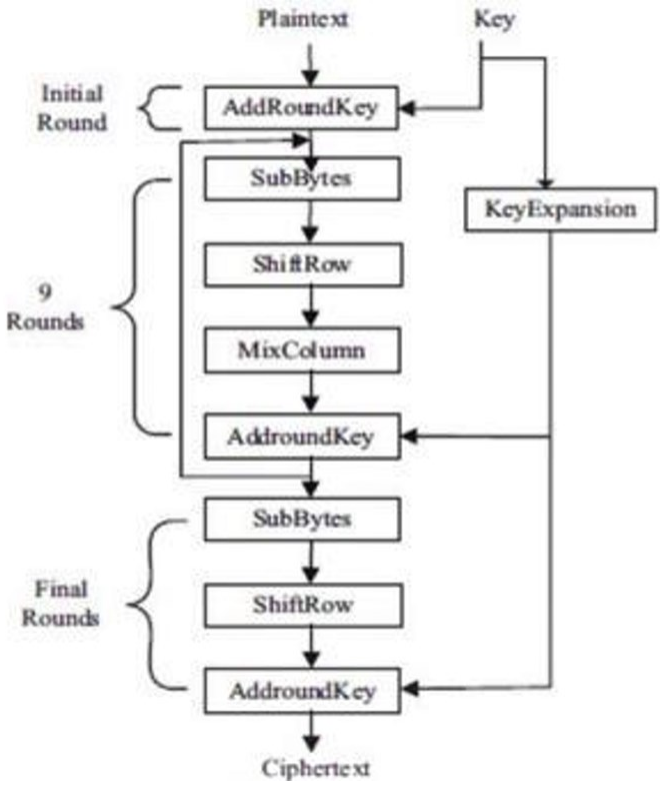


Fig. 1. Working of AES

SUB-BYTES: This non linear byte substitution operation will operate on each byte independently. The [20]substitution table or the [4]sbox is invertible and is constructed by the combination of two transformations:

i) Multiplicative inverse is taken in the Rijndael's finite field.

ii) Then doing the affline transformations.

SHIFT ROW STEP: In this step each columns are shifting row wise. The initial row is not getting shifted, it will be same as previous. The 2nd row is left shifted to left one time, the 3rd row two times and the 4th row three times.

MIX COLUMNS: By treating each column as a four-term polynomial the mix column operation makes the transformation on the state column by column. The columns are considered as polynomials over [5]GF 28 and multiplied modulo x4 +1 with a fixed polynomial a(x),

given by

$$a(x) = \{03\}x3+\{01\}x2+\{01\}x+\{02\} \quad (1)$$

KEY EXPANSION: The initial key we provide as the input to AES will not be sufficient for the proceeding 10 rounds . The key ex-pander algorithm follows an [10]Key expander (or generator) operation basically follows five steps to generate a unique key for each round in AES. Every key produced will be same width as that of input key. The inputto key expander circuit will be the key from the LFSR here, thereby making the keys also unpredictable by the attacker.

ADDROUNDKEY: The main function of the Add Round Key is to associate the keys generated by the key expander step to XOR with the output got from the mixcolumn step. The initial 128 bit key is expanded by the key expansion method to increase the key size for multiple rounds. The round key length will be matching with the block size length, that is 16 bytes. The output of addround key is got by XORing of Key expansion output and the Mix columns output. The output given above is encrypted output of output1. The output of the Add Round Key step is given as input to the next round to process. The feedback creates a loop and runs for 10 rounds of this stage.

The Cipher and Decipher process is explained in the pseudo code in Figure.4 and Figure.5. The individual transformation – Byte substitution, Shift row, Mix column and Add round key- processes the state and is described in the following subsection. As shown in the Figure.4, all Nr rounds are identical with the exception of the final round, which does not include Mix column transformation and as such same in the decipher process shown in the Figure.5. Let us now see the detailed description of each of the four stages used in AES. For each stage both encryption and decryption transformation will be explained. This is followed by a discussion of key expansion process used in AES.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

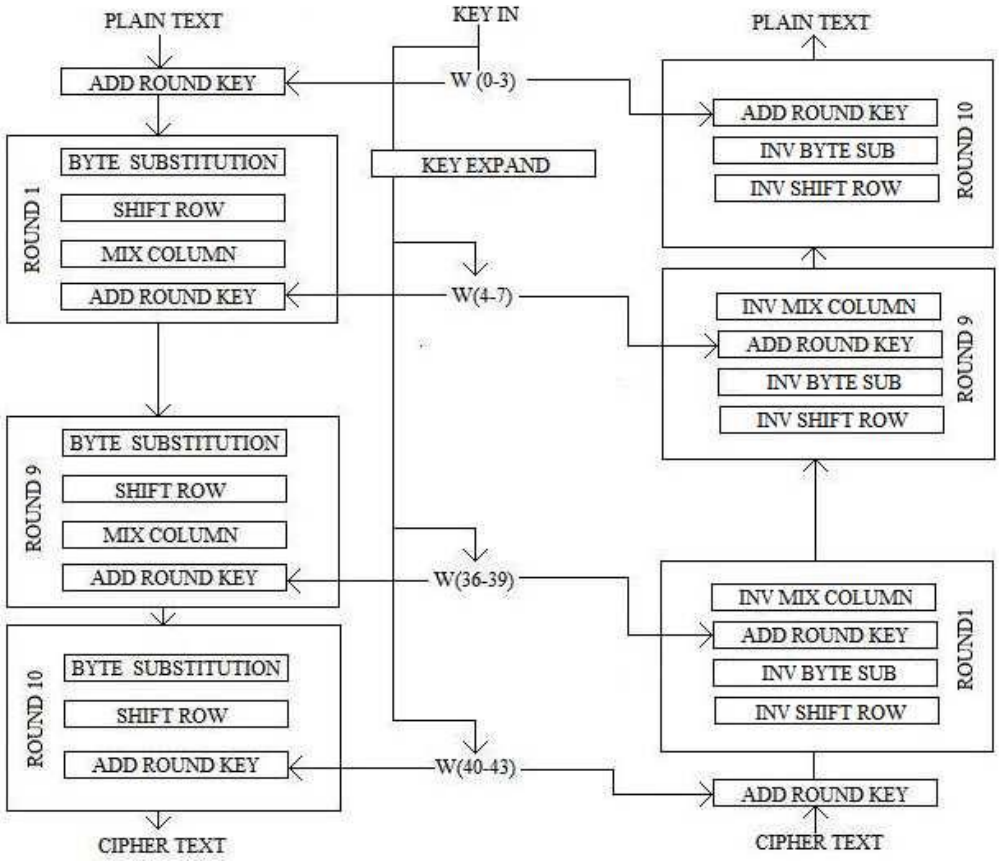


Fig 2.AES Encryption and Decryption

In AES Algorithm is working with one key, to improving the security of the design here we are adding one module for supplying key randomly, for applying random key we are taking random number generator module in this project.

we present the methodology for implementing AES encryption using Linear Feedback Shift Registers (LFSR). The methodology focuses on integrating LFSRs into the AES encryption process to enhance key generation and improve hardware efficiency. The approach involves modifying the key expansion process of AES by utilizing an LFSR-based key generation system. The process is designed to maintain the security and efficiency of AES while optimizing performance in terms of speed, area, and power consumption, especially for embedded systems and hardware-based implementations such as FPGA and ASIC.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

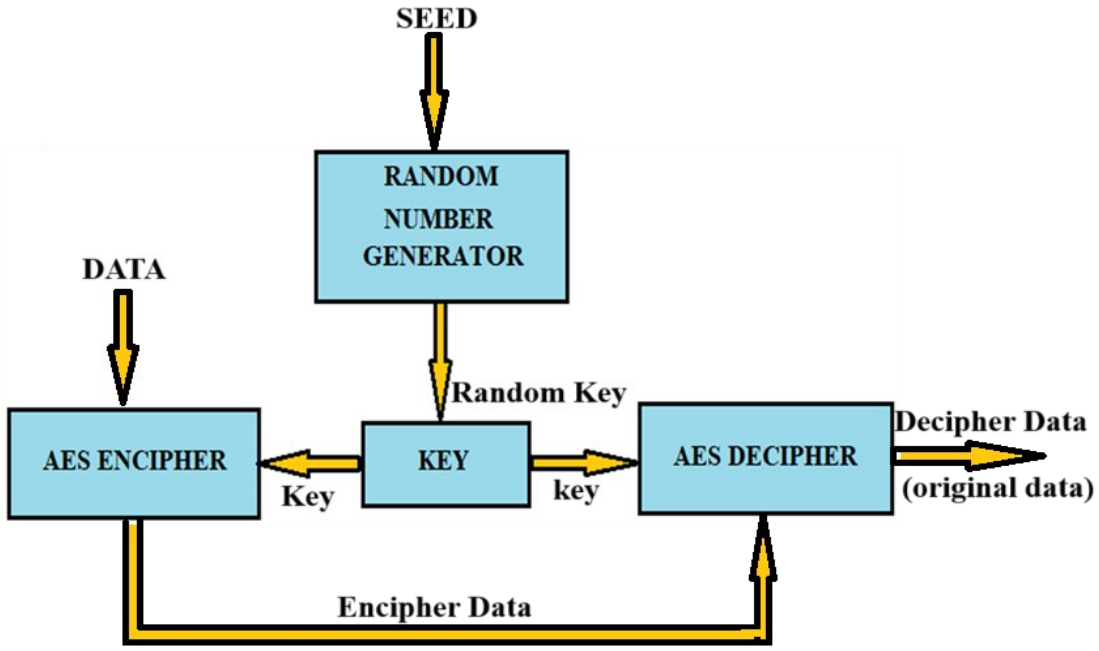


Fig 3. block diagram proposed design

AES (Advanced Encryption Standard) is a symmetric encryption algorithm that operates on blocks of data (128 bits) using a secret key of 128, 192, or 256 bits. The encryption process involves several rounds of transformations, including substitution, permutation, and key addition. The key expansion phase generates round keys from the original key to be used in each round of the encryption process. Traditionally, key expansion involves the use of S-boxes and Rcon values, which may increase the complexity of hardware implementations.We propose the use of an LFSR-based key generation mechanism to replace traditional key expansion methods. The LFSR is used to generate pseudo-random sequences, which are then used to expand the original key, providing a faster and more efficient key generation process.

The main goal of this step is to utilize an LFSR to generate key material for AES encryption. An LFSR is a shift register with feedback that produces a pseudo-random sequence of bits. The LFSR is characterized by its feedback polynomial and initial state, which determine the sequence of bits it generates.

IV. RESULTS

RTL SCHEMATIC: The RTL schematic is abbreviated as the register transfer level it denotes the blue print of the architecture and is used to verify the designed architecture to the ideal architecture that we are in need of development .The hdl language is used to convert the description or summery of the architecture to the working summery by use of the coding language i.e verilog ,vhdl. The RTL schematic even specifies the internal connection blocks for better analyzing .The figure represented below shows the RTL schematic diagram of the designed architecture

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

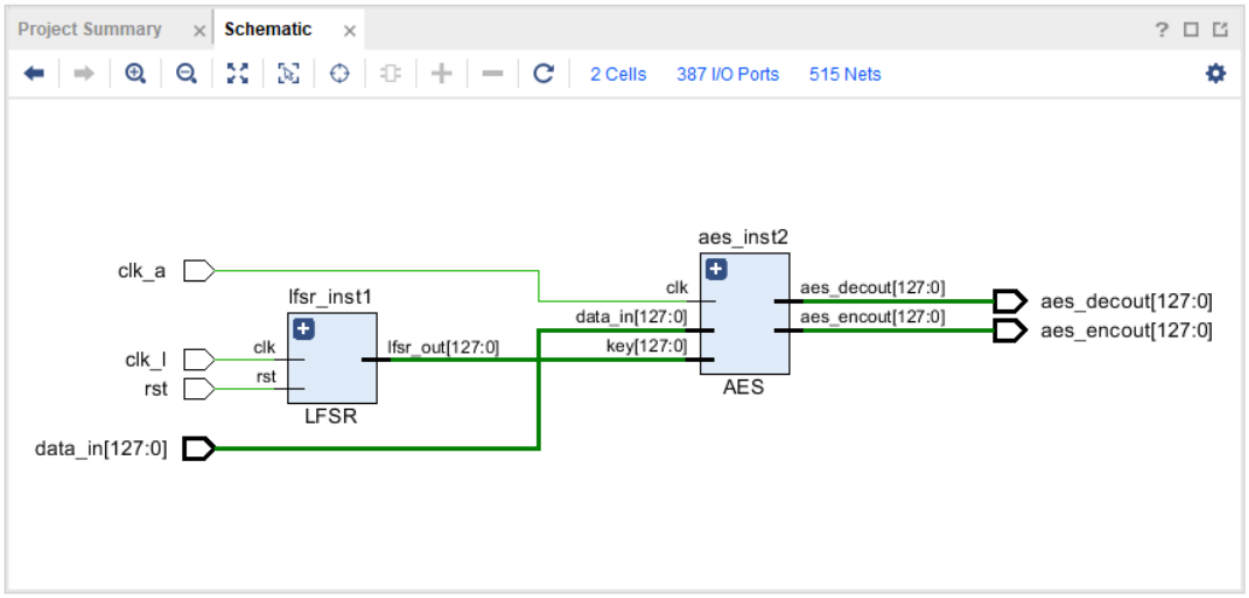


Fig 4. RTL Schematic1 of AES with LFSR

SIMULATION: The simulation is the process which is termed as the final verification in respect to its working where as the schematic is the verification of the connections and blocks. The simulation window is launched as shifting from implantation to the simulation on the home screen of the tool ,and the simulation window confines the output in the form of the wave forms. Here it has the flexibility of providing the different radix number systems.

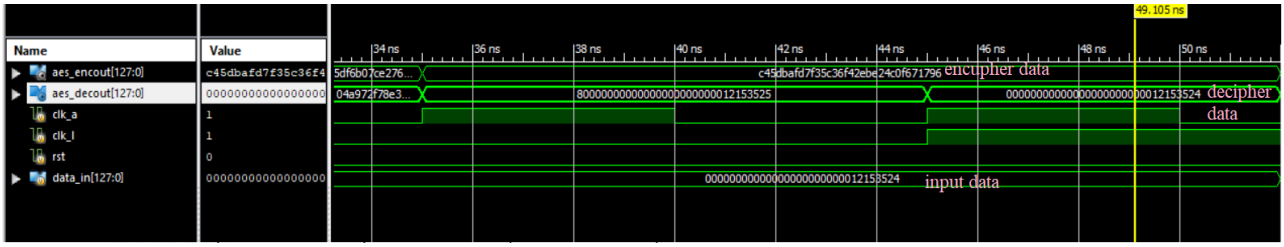
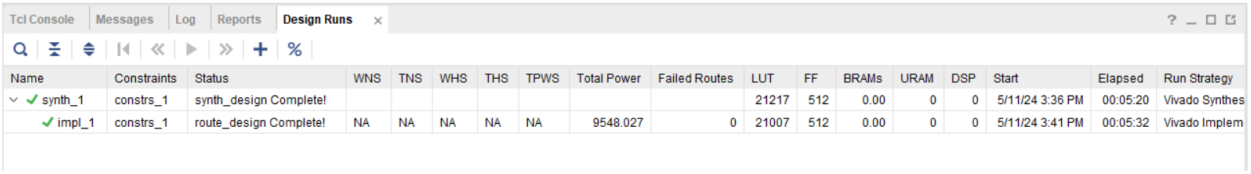


Fig5. Simulated Waveforms of AES with LFSR

PARAMETERS: Consider in VLSI the parameters treated are area, delay and power, based on these parameters one can judge the one architecture to other.The parameter is obtained by using the tool XILINX Vivado and the HDL language is verilog language.



Name	Constraints	Status	WNS	TNS	WHS	THS	TPWS	Total Power	Failed Routes	LUT	FF	BRAMs	URAM	DSP	Start	Elapsed	Run Strategy
synth_1	constrs_1	synth_design Complete!								21217	512	0.00	0	0	5/11/24 3:36 PM	00:05:20	Vivado Synthes
impl_1	constrs_1	route_design Complete!	NA	NA	NA	NA	NA	9548.027	0	21007	512	0.00	0	0	5/11/24 3:41 PM	00:05:32	Vivado Implem

Table1 : hardware utilization.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

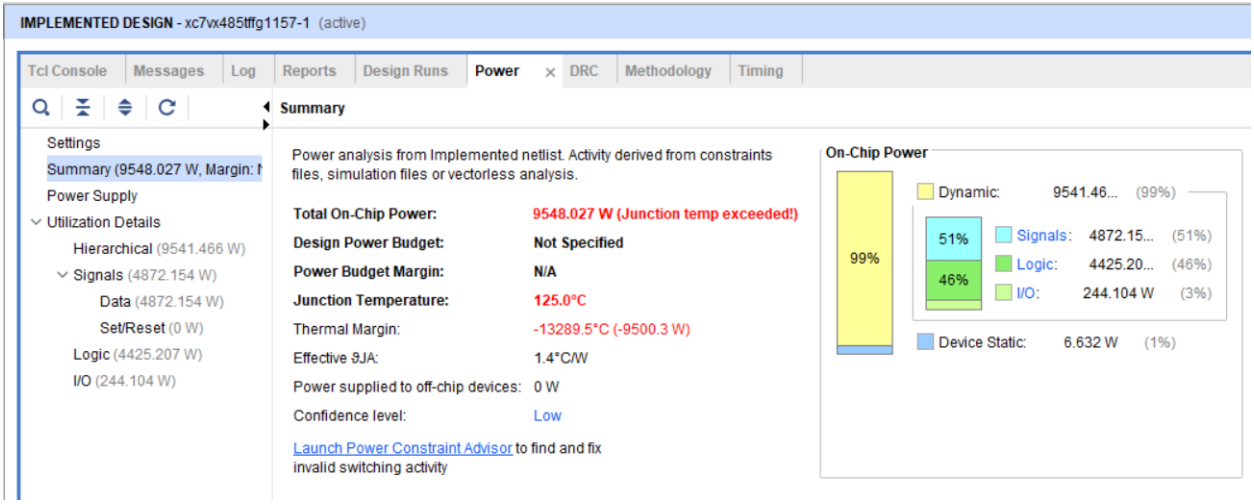


Table 2 : power report of design

V. CONCLUSION

In this project, we have given 128 bits input and 128 bits security key and observed how it is delivered at the output with security.The integration of Linear Feedback Shift Registers (LFSRs) with AES encryption represents an innovative approach to enhancing the performance and efficiency of cryptographic systems. By replacing the traditional key expansion method with an LFSR-based key generation, this method significantly improves the speed of key generation, reduces hardware complexity, and lowers power consumption—making it an ideal solution for resource-constrained environments, such as embedded systems, IoT devices, and mobile platforms. The AES with LFSR-based key generation offers a promising approach to achieve high-performance, low-power, and secure encryption for a wide range of applications, making it a viable option for modern cryptographic solutions in hardware and embedded systems.

REFERENCES

[1] Madakam, Somayya, R. Ramaswamy, and Siddharth Tripathi. “Internet of Things (IoT): A literature review.” Journal of Computer and Communications 3, no. 05 (2015): p.164.

[2] Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. “A survey of security issues in wireless sensor networks.” IEEE Communications Surveys Tutorial (2006).

[3] Veeramallu, B., S. Sahitya, and Ch LavanyaSusanna. Veeramallu, B., S. Sahitya, and Ch LavanyaSusanna. “Confidentiality in Wireless sensor Networks.” International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013.

[4] Eisenbarth, Thomas, and Sandeep Kumar. “A survey of lightweightcryptography implementations.” IEEE Design & Test of Computers 24.6 (2007).

[5] Banik, Subhadeep, Andrey Bogdanov, and Francesco Regazzoni. “Exploring energy efficiency of lightweight block ciphers.” International Conference on Selected Areas in Cryptography. Springer, Cham, 2015.

[6] Bogdanov, Andrey, et al. “PRESENT: An ultra-lightweight block cipher.” CHES. Vol. 4727. 2007.
[7] Borghoff, Julia, et al. “PRINCEa low-latency block cipher for pervasive computing applications.” International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin Heidelberg, 2012.
[8] Beaulieu, Ray, et al. “The SIMON and SPECK lightweight block ciphers.” Design Automation Conference (DAC), 52nd ACM/EDAC/IEEE. IEEE, 2015.
[9] Suzaki, Tomoyasu, et al. “TWINE: A Lightweight Block Cipher for Multiple Platforms.” Selected Areas in Cryptography. Vol. 7707. 2012.
[10] Li, Wei, et al. “Security analysis of the LED lightweight cipher in the internet of things.” Jisuanji Xuebao(Chinese Journal of Computers) 35.3(2012): p.434-445.
[11] Shibutani, Kyoji, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai. “Piccolo: An ultra-lightweight blockcipher.” In CHES, vol. 6917, pp. 342-357. 2011.
[12] Wu, Wenling, and Lei Zhang. “LBlock: a lightweight block cipher.” In Applied Cryptography and Network Security, pp. 327-344. Springer Berlin/Heidelberg, 2011.
[13] Daemen, Joan and Rijmen, Vincent. “The design of Rijndael: AES-the advanced encryption standard.”, Springer Science & Business Media, 2013.
[14] Descriptions of SHA-256, SHA-384, and SHA-512. http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384- 512.pdf.
[15] Al Hasib, Abdullah, and Abul Ahsan Md Mahmudul Haque. “A comparative study of the performance and security issues of AES and RSA cryptography.” Third International Conference on Convergence and Hybrid Information Technology, 2008. Vol.2.
[16] Feldhofer, Martin, Johannes Wolkerstorfer, and Vincent Rijmen. “AES implementation on a grain of sand.” IEE Proceedings-Information Security 152, no. 1 (2005): p.13-20.
[17] Moradi, Amir, Axel Poschmann, San Ling, Christof Paar, and Huaxiong Wang. “Pushing the limits: a very compact and a threshold implementation of AES.” In Eurocrypt, vol. 6632, pp. 69-88. 2011.
[18] Hocquet, Cdric, Dina Kamel, Francesco Regazzoni, Jean-Didier Legat, Denis Flandre, David Bol, and Franois-Xavier Standaert. “Harvesting the potential of nano-CMOS for lightweight cryptography: an ultra-lowvoltage
65 nm AES coprocessor for passive RFID tags.” Journal o Cryptographic Engineering 1, no. 1 (2011): p.79-86.
[19] Kerckhof, Stphanie, Franois Durvaux, Cdric Hocquet, David Bol, and Franois-Xavier Standaert. “Towards green cryptography: a comparison of lightweight ciphers from the energy viewpoint.” Cryptographic Hardware and Embedded SystemsCHES 2012 (2012): p.390-407.
[20] Batina, Lejla, et al. “Dietary recommendations for lightweight block ciphers: power, energy and area analysis of recently developed architectures.” International Workshop on Radio Frequency Identification: Security and Privacy Issues. Springer, Berlin, Heidelberg, 2013.

ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025
[21] Banik, Subhadeep, Andrey Bogdanov, and Francesco Regazzoni. “Exploring the energy consumption of lightweight blockciphers in FPGA.” International Conference on ReConFigurable Computing and FPGAs (ReConFig), 2015 , pp.1-6.
[22] Kong, Jia Hao, Li-Minn Ang, and Kah Phooi Seng. “A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments.” Journal of Network and Computer Applications 49 (2015): p.15-50.
[23] Wenceslao Jr, Felicisimo V., et al. “Modified AES Algorithm Using Multiple S-Boxes.” The Second International Conference on Electrical, Electronics, Computer Engineering and their Applications (EECEA2015). 2015.
[24] Kawle, Pravin, et al. “Modified Advanced Encryption Standard.” International Journal of Soft Computing and Engineering (IJSCE) 4 (2014).