DESIGN AN EFFICIENT FAST AND SECURE MODIFIED LED ENCRYPTION METHOD USING VHDL

Author's Name: [1]Maisara Waseem, [2]Vijay Yadav

Affiliation: [1]*Student, Lakshmi Narain College of Technology, Bhopal, Madhya Pradesh, INDIA*

[2]*Professor, Lakshmi Narain College of Technology, Bhopal, Madhya Pradesh INDIA*

E-Mail: mswaseem131@gmail.com

DOI No. – **08.2020-25662434**

Abstract

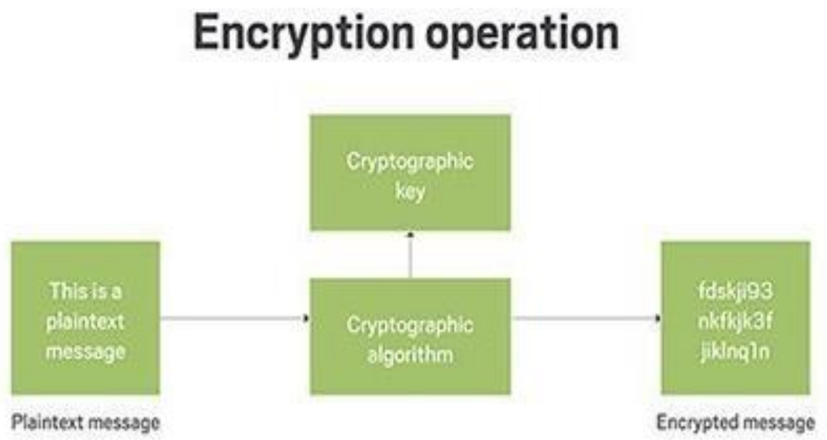
A Cryptographic architecture is the collection of hardware and software that secures and controls the use of encryption keys and similar encrypt variables. There are various data encryption methods used for secured data transmission. As the size of the data increases, it becomes difficult to transmit the secured data efficiently. Therefore, in this paper, a proposed methodology is used to design and implement a modified efficient LED (Light Encryption Device) block using the VHDL behavioural modelling. The previous research was of the Advanced Encryption Standard (AES) type and was considered as area efficient, while the current work constitutes a Feistel network structure which is suitable for low-complexity and low-power embedded security applications. In this paper, we propose well-planned and logical error detection architectures which provides faster and delay efficient modified LED.

Keywords: *AES, LED, reliability, block ciphers, VHDL.*

INTRODUCTION

To provide various security properties and functions in a structured manner, lightweight cryptographic implementations on different hardware platforms have been emerged due to the advancement and growth of constrained devices. A well planned methodology is used. These nodes require low-complexity implementations over small chip area and consume low amount of energy. Nevertheless, the Advanced Encryption Standard (AES), may not achieve such tight necessities in terms of performance and implementation metrics. Thus, lightweight security mechanisms through low-complexity implementations of cryptographic algorithms are needed. In this paper, we consider LED (light encryption device). LED has 64-128 bit block length and uses 64-bit key length. It can take single or multiple key. Thus, we propose error detection approaches for block cipher LED, considering the reliability and performance. Signature-based approaches are also used to achieve high efficiency, while maintaining high error coverage.

The most widely used encryption standard is AES (standard advanced encryption). The major concern in this paper is to focus on building a faster algorithm for computer implementation based on behavioral simulation using VHDL. Thus, fast implementation of LED encryption algorithm is proposed. The delay is reduced by partial parallel implementation.



OVERVIEW OF LED

Over past years many new cryptographic primitives have been proposed for use. In this section, we will study LED block ciphers:

LED BLOCK CIPHER

LED, an SPN type light weight block cipher was first introduced by Guo et al. in 2011. The step function performed 8 times for the 64 bit key and 12 times for the 128-bit keys. The keys used in LED block cipher may vary from 64 bits to 128 bits. The LED algorithm block diagram is shown in Figure 1. The LED block cipher is simple to analyze. The input plaintext which is of 64-bit length is arranged in a 4 × 4 array matrix called cipher state matrix. The implemented LED block cipher uses a 64-bit key. Both the cipher state matrix and the key are arranged in 4×4 matrix in the form of 16 four-bit nibbles. Each entity in the cipher state matrix and the key matrix is of 4-bit length.

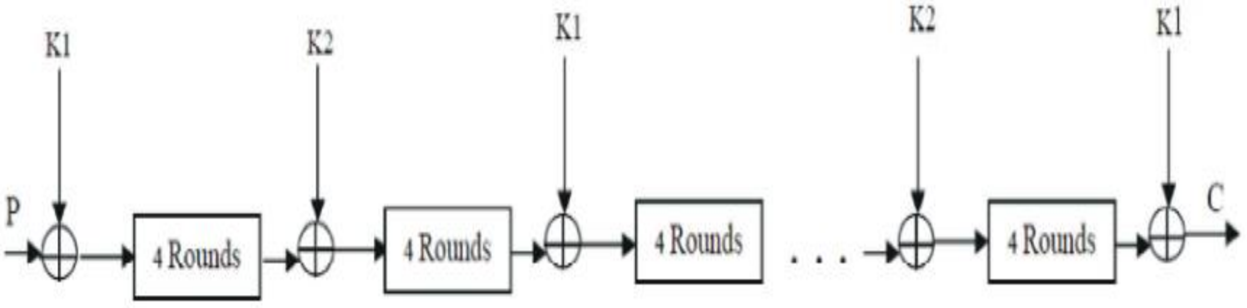


FIG. 1: BLOCK DIAGRAM OF LED ALGORITHM

The main operations in algorithms are Add Constant, Substitute cells, Shift Rows and Mix Columns.

- **Add Constants:** XOR dependent constants in each round to the first columns.
- **Substitute Cells:** It is a 16-bit element. The present S-box is used for the operation of LED.
- **Shift Rows:** The operation in shift rows rotates i-th line by i position to the left.
- **Mix Columns Serials:** Apply the special Maximum Distance Separable matrix to each column independently.

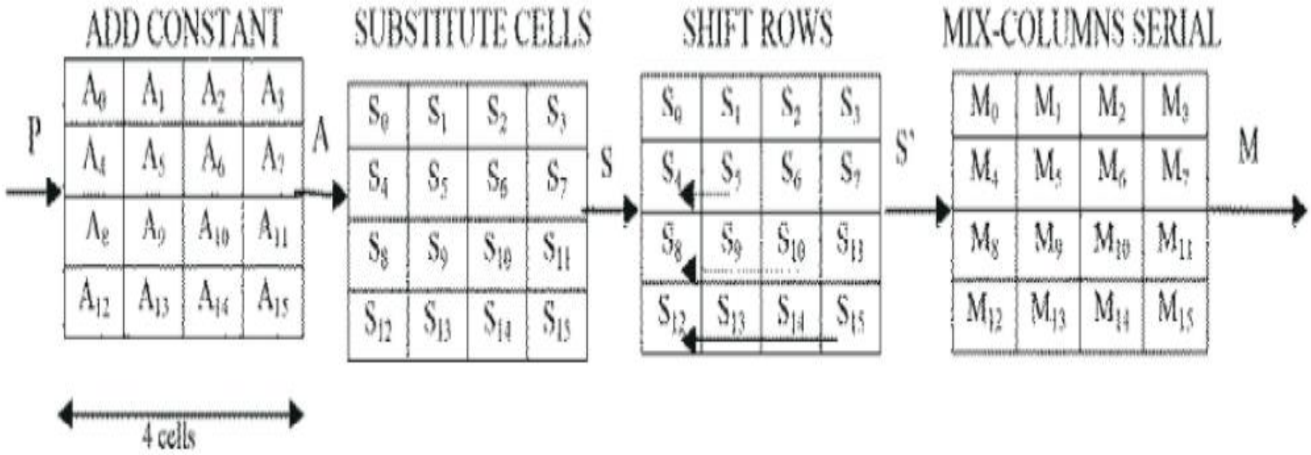


Fig. 2: operation in led

RELATED WORK

Nowadays in symmetric cryptography, an AES-like design appears to be the actual initiative for a clean and secure design. The design of LED will inevitably have many parallels with this established approach, and features such as Sboxes, Shift Rows, and (a variant of) Mix Columns.
In this paper fast implementation of LED encryption algorithm is proposed. The delay is reduced by partial parallel implementation i.e. some steps in algorithms are implemented in parallel to reduce the delay to make the algorithm faster and to simultaneously obtain increased throughput.

TABLE 1 SUMMARY OF RELATED WORK

S.no	Contribution	Description	Publication
1	Hardware Architectures for Cryptographic LED Block Ciphers [1]]	implementation of LED cipher and height cipher	S. Subramanian 2017
2	The LED Block Cipher	LED Algorithm	J. Guo et.al [4]
3.	An area efficient algorithm for embedded sputum	LED based encryption	Honey D, et al [5]
4.	Modified Light weight LED algorithm for delay efficient	Parallel Fast LED	Proposed

ADVANTAGES OF LED

1. It is small and faster.
2. It is lightweight.
3. It is highly secure.
4. It is implementable over 64 bits to 128 bits.
5. It offers very easy key scheduling.
6. It consumes low amount of energy.

PROPOSED METHODOLOGY

In this paper partial parallel architecture is used to implement LED cipher. Sub cells used 16 PRESENT S-box to generate in parallel the new STATE matrix. Similarly, all the three rows of the shift columns process are shifted in parallel to generate the new STATE matrix in parallel, and similarly continue with mix column operation. A state machine controller is designed to control the process. At every clock pulse iteration number is incremented by one. The machine controller block is adopted to control all the processes. This machine controller is a clock driven unit, which generates the iteration number.

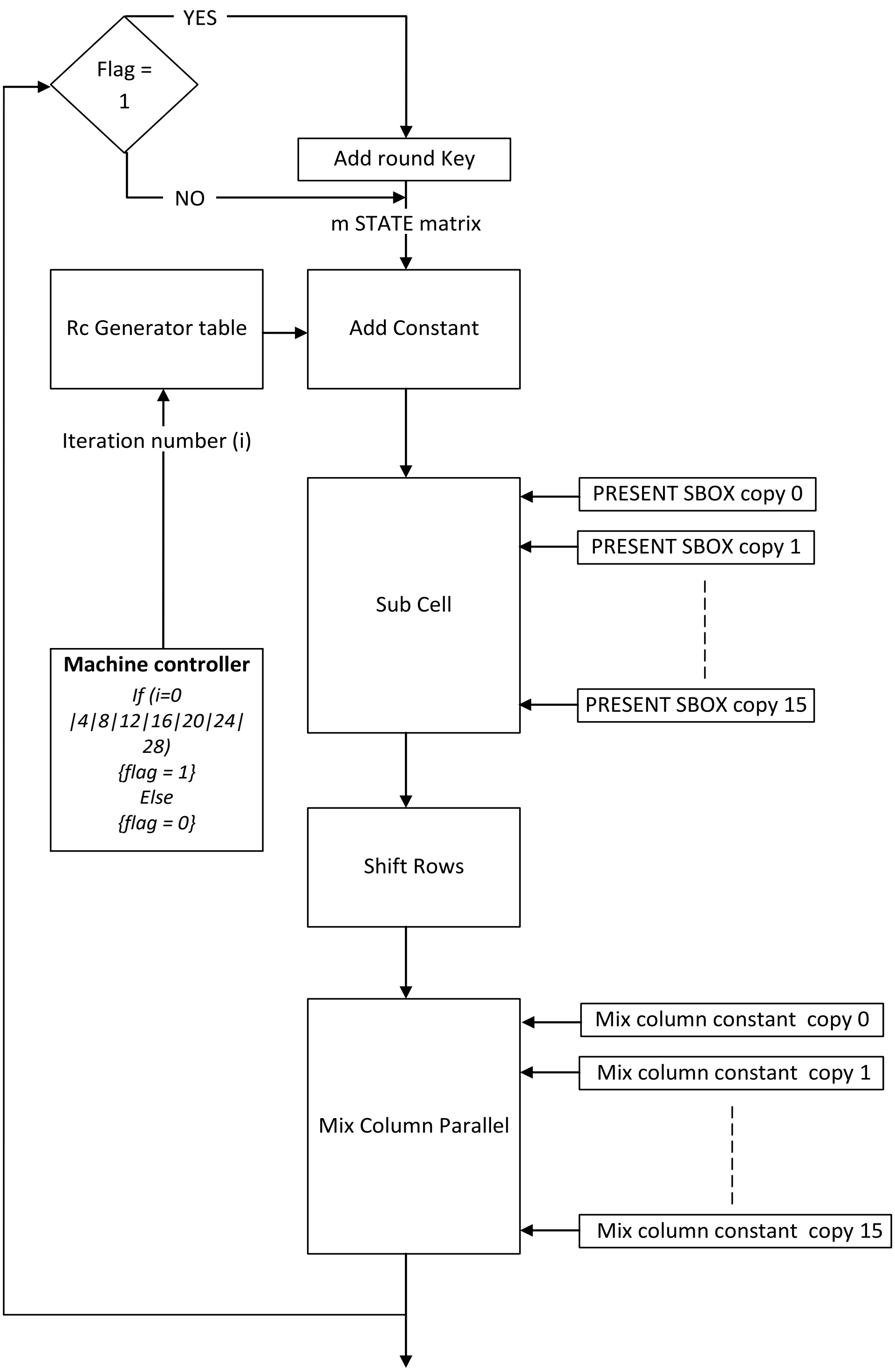


FIG. 3: FLOW CHART OF THE PROPOSED LED ALGORITHM

This is the complete design architecture which is used to implement LED cipher. This technique ensures that a single STATE matrix is generated in a single clock cycle and hence delay is reduced.

CONCLUSION

In this paper major concern is to design the delay efficient LED cipher algorithm for hardware description. After further research various hardware implementation of LED are studied and then it is found that complete serial implementation of LED tend to large delay, hence in this work we have used partial parallel and partial serial implementation of LED.

It can be concluded from synthesis report that area i.e. number of LUT slices used are increased as compared to previous designs available in literature. It can be conceded that significant less time of execution is achieved by the proposed design.

REFERENCES

1. C. H. Yen and B. F. Wu, “Simple error detection methods for hard ware implementation of Advanced Encryption Standard,” IEEE Trans. Comput., vol. 55, no. 6, pp. 720–731, Jun. 2006.
2. M. Mozaffari-Kermani and A. Reyhani-Masoleh, “Concurrent structure independent fault detection schemes for the Advanced Encryption Standard,” IEEE Trans. Comput., vol. 59, no. 5, pp. 608–622, May 2010.
3. M. Mozaffari Kermani and A. Reyhani-Masoleh, “A low-power high performance concurrent fault detection approach for the composite field S-box and inverse S-box,” IEEE Trans. Comput., vol. 60, no. 9, pp. 1327–1340, 2011.
4. Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJ, Seurin Y, Vikkelsoe C. PRESENT: An ultra-lightweight block cipher. InInternational Workshop on Cryptographic Hardware and Embedded Systems 2007 Sep 10 (pp. 450-466). Springer, Berlin, Heidelberg.
5. Riadh Ayachi , Ayoub Mhaouch, and Abdessalem Ben Abdelali, “Light weight Cryptography for Network-on-Chip Data Encryption”, Hindawi Security and Communication Networks Volume 2021,
6. Moradi A, Poschmann A, Ling S, Paar C, Wang H. Pushing the limits: a very compact and a threshold implementation of AES. InAnnual International Conference on the Theory and Applications of Cryptographic Techniques 2011 May 15 (pp. 69-88). Springer, Berlin, Heidelberg.
7. S. Subramanian, M. Mozaffari-Kermani, R. Azarderakhsh and M. Nojoumian, "Reliable hardware architectures for cryptographic block ciphers LED and HIGHT", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 36, no. 10, pp. 1750-1758, 2017.
8. Wajih El Hadj Youssef, Ali Abdelli, Fethi Dridi, and Mohsen Machhout, “Hardware Implementation of Secure Lightweight Cryptographic Designs for IoT Applications”, Security and Communication Networks Volume 2020 (2020).
9. J. Guo, T. Peyrin, A. Poschmann and M. Robshaw, "The LED block cipher", International Workshop on Cryptographic Hardware and Embedded Systems, pp. 326-341, 2011
10. M. Mozaffari Kermani and A. Reyhani-Masoleh, “A structure independent approach for fault detection hardware implementations of the Advanced Encryption Standard,” in Proc. IEEE Workshop Fault Diagnosis and Tolerance in Cryptography, Sep. 2007, pp. 47-53.
11. R. Beaulieu, D. Shors, J. Smith, S. T. Clark, B. Weeks, and L. Wingers, “Simon and Speck: Block ciphers for the Internet of things,” in Proc. Cryptology ePrint Archive, Report 2015/585, 2015.
12. C. H. Yen and B. F. Wu, “Simple error detection methods for hard ware implementation of Advanced Encryption Standard,” IEEE Trans. Comput., vol. 55, no. 6, pp. 720–731, Jun. 2006.
13. K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shi rai, “Piccolo: An ultra-lightweight blockcipher,” in Proc. Cryptographic Hardware and Embedded Systems, 2011, pp. 342–357.