International Journal of LNCT
Volume-5 Issue-26 October -2021
ISSN: (Online):2456-9895

Design an Efficient Fast and Secure Modified LED Encryption method using VHDL

Maisara Waseem [1], Dr. Vijay Yadav [*2]

[#] *Department of Electronics and Communication, Engg.*

LNCT Bhopal

***Abstract*—there are many data encryption standards designed for secure data transmission. With the increasing size of data over network it become critical to design the light weight cipher (LWC) encryption method. Thus in this paper prime concern is to design the modified efficient LED (Light encryption device) block based encryption method using the VHDL behavioural modelling methodology. Existing block ciphers are initially reviewed and are serial ones. Then Paper proposed to design a parallel partial architecture for implementing the LWC based LED cipher. In the modified LED the sub cells have used 16 PRESENT sbox's for creating the new STATE matrix in parallel architecture. During the design the clock driven machine control block is adopted for generating iteration counts. It is found that proposed modified LED is faster and delay efficient too.**

Key Words: LED, Light weight encryption, Block Ciphers, AES, cryptography. VHDL

I. INTRODUCTION

Data security has become an important task due to the proliferation of data over the network. It is therefore very necessary to design fast and effective data encryption algorithm. This crypto encryption will be lightweight and able to protect data from cyber threats. The most widely used encryption standard is AES (standard advanced encryption) [1]. This work focuses on building a faster algorithm for computer implementation based on behavioral simulation using hardware definition language. The biggest challenge for encryption is designing a delay method and a more efficient environment. These are things focused the most in this paper.

AES is used in some way for some of these encryption algorithms, but the problem is the need for large area (resources). So for devices with low hardware such as RFID tags, new algorithms should be adopted to provide encryption, LED block cipher is one way [1, 2, 4, 6, 8, and 15]. A block LED cipher is a modified form of AES level. Existing algorithms use all the steps and cycles of the LED encryption algorithm respectively so, their resource usage is very low, they use the algorithm with 217 pieces of Virtex 7 FPGA. As a result of this LED launch [1] the delay is quite high. It is therefore very necessary to design the LED light encryption based on the fraction and use of LUTs.

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.

II. RELATED WORK

There are many versions of block based ciphers designed for improving the performance and specially designed for light weights shown in Classification in Figure 1.

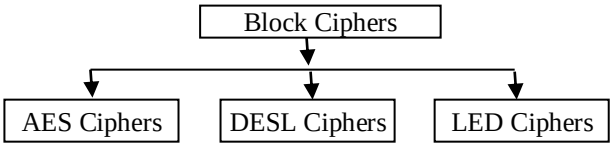

Figure 1 Classification of Block ciphers

The J. Guo et.al [4] designed a new block-based cipher called LED. The method designed for the use of hardware has three additional features. These offerings include ultra-light key schedules, key-resistant cipher attacks, and: the method used for device level security. S Subramanian [1] Cryptographic properties provide a variety of security properties for critical use models. However, unless the reliability of the structures is guaranteed, such safety structures may be damaged by natural or serious errors. In this paper, we look at the two lower block ciphers that can be used in certified encryption algorithms, namely, LED and HIGHT cipher blocks. Honey Devaraj, et al [5] proposed design encryption for internal-based security systems using locally efficient LEDs. Multiple similar block based cipher algorithms has been considered in past [9, 11, 13, 14, 16 and 17]

A. Benefits of LED

Major advantages of LED cipher over other block ciphers are that it is small and faster than PRESENT, it is highly secure light weight cipher. The LED is implementable over wide key size of 64 to 128 bits and offers very easy key scheduling.

B. Summary of Review

Finally summary of review are presented in the Table 1

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

III. OVERVIEW OF LED CIPHER

The section therefore briefly describes the overall permissive view for the keyed cipher Keyed used for LED encryption heavily inspired from the AES algorithm architecture.

Basically the internal state is considered to be the 4 × 4 matrix of 4-bit cells. LED process steps are provided in

- **AddConstants:** xor dependent constants in each round to the first columns
- **SubCells:** apply Sbox of PRESENT 4 bit to each cell
- **ShiftRows:** rotate the i-th line by I positions to the left
- **MixColumnSerial:** apply a specific number of MDS to each column independently of Figure 2.

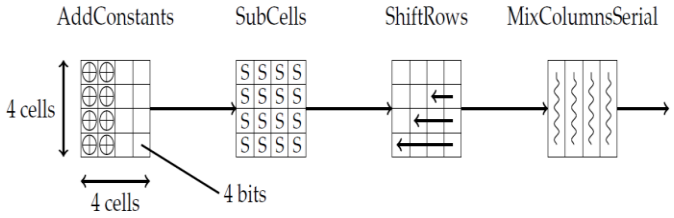

Figure 2 Sequential single round of the LED process for the encryption

A. *Constants addition*

Steps to add conditions added in sequence as

- k represents the size of the key
- In this paper k7: k0 says "00100000", as the key size is 64
- rc represents continuous, take this rc number in the table mentioned above

B. *Sub Celll Generation*

Each nibble of the array state is changed by the nibble generated by using the PRESENT S-box. Then LED cipher re utilizes the PRESENT S-box which was adopted in numbers of lightweight cryptographic algorithms.

X	0 1 2 3 4 5 6 7 8 9 A B C D E F
S[X]	C 5 6 B 9 0 A D 3 E F 8 4 7 1 2

Figure 3 showing the sub cell generation.

C. *Row Shifting*

Row i of the array state is rotated i cell positions to the left, for i = 0, 1, 2, 3.

S0	S1	S2	S3
S4	S5	S6	S7
S8	S9	S10	S11
S12	S13	S14	S15

→

S0	S1	S2	S3
S5	S6	S7	S4
S10	S11	S8	S9
S15	S12	S13	S14

D. *Mix Columns*

The Mix Columns Serial layer can be viewed as four applications of a hardware-friendly matrix 'A' with the net result being equivalent to using the MDS matrix M

$$A^4 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 4 & 1 & 2 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 1 & 2 & 2 \\ 8 & 6 & 5 & 6 \\ B & E & A & 9 \\ 2 & 2 & F & B \end{pmatrix} = M \qquad (2)$$

E. Key Schedule

For the 64-bit key, proposed modified method xored it to the internal states over the every four rounds. Our method apply a total of 8 steps (or 32 rounds)

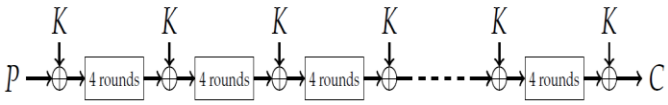

Figure 4 Basic Key scheduling

IV. Proposed Modified LED Encryption

In this paper partial parallel architecture is used to implement LED cipher, sub cells used 16 PRESENT S-box to generate the new STATE matrix in parallel, similarly all the three rows of shift column process are shifted in parallel to generate the new STATE matrix in parallel, and the same story goes with mix column operation. The flow chart of LED cipher is shown in figure. A state machine controller is designed to control the process, at every clock pulse iteration number is incremented by one, the starting value of I is 0 and the terminal value of i is 31.

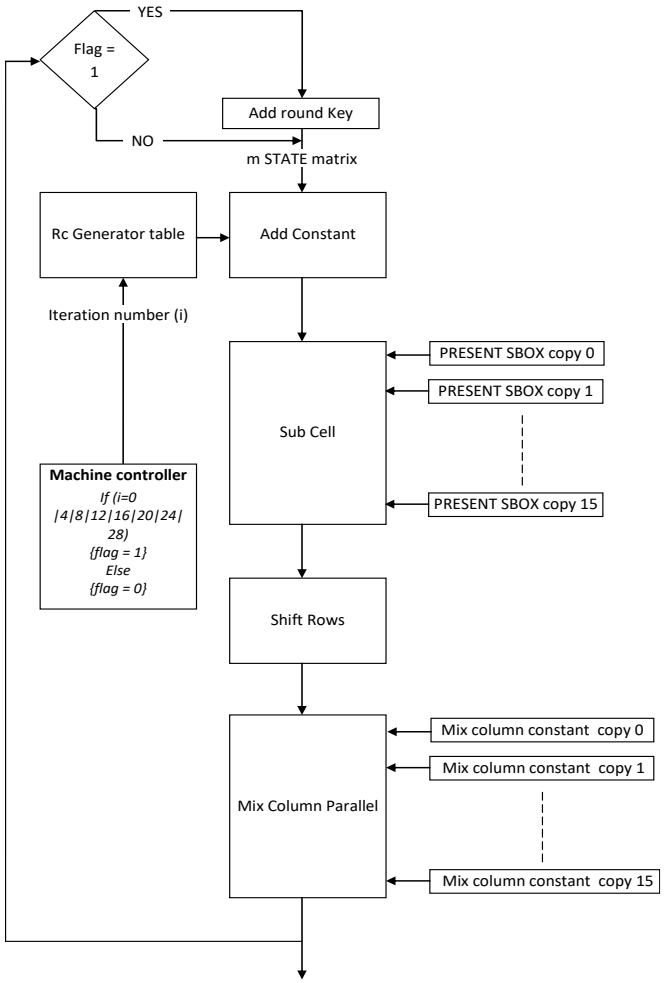

Figure 5 Flow chart of the Proposed LED algorithm.

The machine controller block is adopted to control all the processes. This machine controller is a clock driven unit which generates the iteration number. The following functions are implemented by machine controller unit:

1. Generates iteration number (i), this value is incremented at every clock pulse having initial value = 0 and terminal value = 31, so a total of 32 states are present.
2. Set and Reset flag, when i = 0, 4, 8, 12, 16, 20, 24 or 28, the flag is set, for all other values of i flag is reset.
3. The rc generator is simply a memory table having 6 bit constant values, machine controller fetches the appropriate value form the rc table and supply the same to add constant.

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

In this 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, each state matrix is implemented in parallel and output state matrix of that unit is made available in single clock cycle

V. Results and Discussion

In this paper, cryptosystem for low area devices like RFID are targeted, various cryptographic algorithms are available in literature, Authors chosen LED (Light encryption device). As this algorithm is closest implementation of AES (Advance Encryption Standard), AES is widely use in many industry standard encryption machines like SSL etc, also the AES is easy to implement on both hardware and software also it is very difficult to hack. LED used similar rounds to AES like add round key, sub cells similar to sub byte of AES, shiftrows, mix column etc

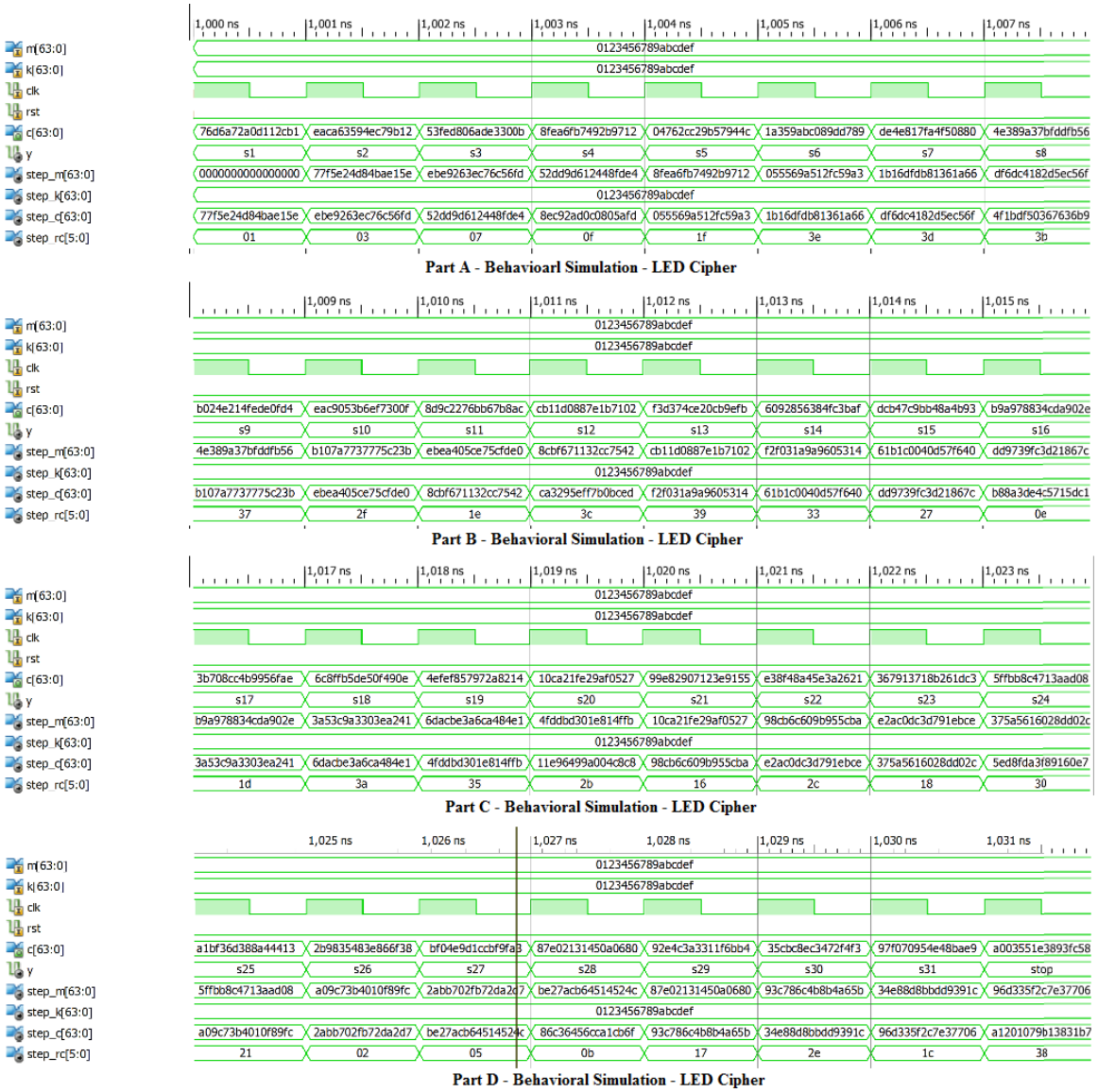

Figure 6 Results of the behavioral simulation of the proposed LED algorithm

TABLE 2 **SUMMARY OF THE TIME EVALUATION**

```
Timing Summary:
---------------
Speed Grade: -3

   Minimum period: 2.090ns (Maximum Frequency: 478.538MHz)
   Minimum input arrival time before clock: 1.008ns
   Maximum output required time after clock: 2.369ns
   Maximum combinational path delay: 0.900ns

Timing Details:
---------------
All values displayed in nanoseconds (ns)
```

Table 3: Comparative Study of Synthesis report of LED block cipher

S.No	Architecture	Area (Slices)	Delay
1	LED – Algorithm Design 1 of [1], [4]	178	5.841 ns
2	Algorithm 2 of [1] LED –signature	217	5.914 ns
3	LED – Partial parallel implementation**[This Work]**	346	2.090ns
4	**Percentage Change {S.no 1 & 3}**	**+94%**	**-179%**

5	**Percentage Change {S.no 2 & 3}**	**+59%**	**-182%**

Behavioral Simulation

In this section the results of the behavioral analysis of the simulation work are presented. Figure 6 shows the behavioral simulation of LED cipher, as observed from the simulation that a total of 32 clock cycles are required to generate the cipher text. A state machine is used to implement machine controller, there are 32 states in state machine form s0 to s31, when the machine is reset the state of state machine is s0 and at every clock cycle the state of the machine is goes from s0 to s1 to s2 and so on and different operation are performed at each state. Intermediate values of different units can also be seen from figure.

The time summary of the algorithm of proposed partial parallel design is given in the Table 2. It can be conceded that significant less time of execution is achieved by the proposed design. This is much clear from the statistical comparison of the delay in Table 3. The performance of the proposed partial parallel LED algorithm is compared with the standard LED and the LED –signature algorithm in the literature.

The proposed LED approach provides the good improvement over the existing two approaches in terms of delay but compromise on area concerns.

VI. Conclusion

In this paper primary concern is to design the delay efficient LED cipher algorithm for hardware description. Various hardware implementation of LED are studied primary 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, each state matrix is implemented in parallel and output state matrix of that unit is made available in single clock cycle.

It can be concluded from synthesis report that area i.e. number of LUT slices are 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.

But delay in nano seconds is decreased by more than 2 folds, hence if delay, i.e. fast implementation is desired then one can opt our design at almost same area.

Acknowledgment

The authors of the paper deeply acknowledge every individual associated to research in any way. In addition authors also acknowledge. all the referred authors for their contribution in work.

References

[1] 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

[2] Devi, SistlaVasundhara & Kotha, Harika.. "AES encryption and decryption standards". Journal of Physics: Conference Series. 1228. 2019 on research gate

[3] L. Xiao-Mei and Q. Yong, "Research on LED lightweight cryptographic *algorithm based on RFID tag of Internet of thing s"*, 2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), pp. 1717-1720, 2019.

[4] 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..

[5] Honey Devaraj, Sharon Mathew, "Area Delay Efficient Encryption Design Using LED for Embedded Security", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 6, Issue 4, April 2017

[6] G. Hatzivasilis, G. Floros, I. Papaefstathiou and C. Manifavas, "Lightweight authenticated encryption for embedded on-chip systems", *Information Security Journal: A Global Perspective*, vol. 25, no. 4-6, pp. 151-161, 2016.

[7] A. Bogdanov et al., "PRESENT: An ultra-lightweight block cipher", International workshop on cryptographic hardware and embedded systems, pp. 450-466, 2007..

[8] M. Al-Shatari, F. A. Hussin, A. A. Aziz, G. Witjaksono, M. S. Rohmad and X. -T. Tran, "An Efficient Implementation of LED Block Cipher on FPGA," 2019 First International Conference of Intelligent Computing and Engineering (ICOICE), pp. 1-5, 2019,

[9] 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),

[10] Beaulieu R, Treatman-Clark S, Shors D, Weeks B, Smith J, Wingers L. The SIMON and SPECK lightweight block ciphers. InDesig8n Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE 2015 Jun 8 (pp. 1-6).

[11] 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

[12] Riadh Ayachi , Ayoub Mhaouch, and Abdessalem Ben Abdelali, "Light weight Cryptography for Network-on-Chip Data Encryption", Hindawi Security and Communication Networks Volume 2021,

[13] 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,

[14] 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

[15] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.-S. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee, "HIGHT: A new block cipher suitable for low-resource device," in Proc. CHES, 2006, pp. 46-59.

[16] S. Sun, L. Hu, P. Wang, K. Qiao, X. Ma, and L. Song, "Automatic security evaluation and (related-key) differential characteristic search: Application to Simon, PRESENT, LBlock, DES(L) and other bitoriented block ciphers," in Proc. Advances in Cryptology, 2014, pp. 158–178.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