

EFFICIENT HARDWARE IMPLEMENTATION OF LED BLOCK CIPHER

P.FELISS RAJA SOFIA
PG SCHOLAR
DEPT OF ECE
R.M.K ENGINEERING COLLEGE
CHENNAI
felissofia@gmail.com

Dr T.BLESSLIN SHEEBA ME., Phd
Professor
DEPT OF ECE
R.M.K ENGINEERING COLLEGE
CHENNAI
tbs.ece@rmkec.ac.in

Abstract: Resource constrained devices such as RFID and sensor nodes contain sensitive and confidential information. Such devices are used in many applications leading to an ever increasing need to provide high speed security. In order to satisfy these constraints in the small embedded applications which have limited resources, lightweight symmetric LED block cipher plays a major role in the bulk data encryption. In this paper implementation of a hardware efficient symmetric LED (Light Encryption Device) block cipher design that increasing speed using high speed parallel sub-pipelined architecture is proposed. This approach is done for block size of 128-bits and key size of 128-bits. The trade off between the low resource requirement and cryptographic strength is balanced here. It is tested by encrypting and decrypting a single 128 bit block. The algorithm was designed using VHDL. To verify the digital design at the software platform modelsim simulator Altera 6.5e is used and synthesized using the Xilinx synthesizer and targeted in low cost FPGA device Spartan 6.

Keywords-Lightweight cryptography, FPGA, LED Block Cipher, Security, Confidentiality.

energy consumption. Even though the evolution of cipher has no practical impact, it has more theoretical background.

After the advent of the internet the security of data and protection of privacy have become a major concern for day to day life, although researchers and mathematicians have been trying to address this problem since the end of the World War II, when cryptology science came out from the ambit of the army to enter the Bell Laboratories.

The cryptography must ensure the tradeoff between security and low resource requirement. Information Security play an important role in our lives to satisfy the day by day life. The increase in use of computer and communication system for the data and money transfer has increased the risk of theft of information. In order to provide security there is a need of secure communication of the algorithm must ensure that fast and secure digital communication, the data is kept secret, the entity of data is preserved, the user identity is genuine [1]. Cryptography provides different algorithm for securing and authenticating the transmission of information over the channels. RFID and sensor nodes contain sensitive information and confidential information such device are used in many application but these miniature device are not possible to run in traditional cryptography which require large memory and greater power. In order to satisfy these constraint Lightweight cryptography is used.

“As light as feather and hard as dragon scale”

was Bilbo Baggins description for Mithril, a legendary material in J.R.R. Tolkiens famous novel “The Lord of the Rings” .The main objective of lightweight cryptography aims to yield very lightweight implementations that are virtually “light as a feather”, “Hard as dragon scales” is a good paraphrase for this aspect, because it emphasizes that there are sufficient security levels [7]. Symmetric key cryptography and asymmetric cryptography are the two types of cryptography. The Symmetric key cryptography use the same key for both encryption as well as decryption,

C

1. Introduction

Cryptography is an important aspect of communications security and is becoming increasingly important as a basic building block for computer security.. Cryptography began thousands of years ago. It's also found in old kingdom of Egypt circa during 1900BC. Some clay tablets from Mesopotamia are clearly meant to protect information one dated near 1500BC was found to encrypt a craftsman's recipe for pottery glaze, presumably commercially valuable. Today more and more sensitive data is stored digitally. Personal emails, bank accounts and medical records are confidential information that data must kept secure. The use of systems with more complexity, which are usually more secure, has a result low throughput rate and more

while the counterpart Asymmetric key use a public key for encryption and a private key for decryption. The Symmetric key encryption is further classified into two types Block cipher and stream cipher. The stream cipher encrypt data bit by bit whereas the block cipher can encrypt block of data. The main operations of cryptographic algorithm are that the encryption and decryption takes place under the action of fixed block sizes called as plain text. Some of the lightweight cryptographic algorithm present today are AES, DES, HIGHT, PRESENT, KTANTAN, AND KATAN, KLEIN, PRINCE, TWINE, TEA AND XTEA and LED. Among all these, the LED block cipher stay ahead in terms of security even without key schedule. When compared to other existing lightweight block cipher, the LED block cipher is more resistant to classical attacks and also to the related key attacks [1]. In this paper, the section 2 gives a overview of LED algorithm. Section 3 gives the implementation of proposed architecture. Section 4 gives an overview of hardware implementation. Section 5 explains the various performance matrices of the algorithm.

II LIGHT ENCRYPTION DEVICE

LED is a SPN (Substitution Permutation Network) [4] type Lightweight block cipher, which is designed by Guo et al. in 2011. It uses the key size varying from 64 bits to 128 bits. The step function is performed eight times for a 64-bit key and twelve times for a 128-bit key [3].The user-provided key is used repeatedly and

provide efficient advantage in hardware implementation[2]. The overview of algorithm of Light Encryption Device is shown in Figure 1. In encryption algorithm, the steps performed in Add Roundkey are as follows the key $K=K_{63}, \dots, K_0$ is EX-OR'ed with Plain text $P=P_{63}, \dots, P_0$. In this method 128 bit key size is used. Initially the plain text is EO-OR'ed with key1 (k1) where k1 ranges from 0 to 63 bits of total key size. After the completion of rounds the key K2 is EX-OR'ed, where K2 range from 64 to 127 bits of the total key size. k1 and K2 are alternatively EX-OR'ed after every four rounds

A. S-Boxes

LED lightweight block cipher makes use of a PRESENT S-box, which has been adopted by many algorithms is shown in table 1. The goal of substitution is to reduce the correlation between input and output.

B. Shift Row

The shift row transformation consist of

- (i) not shifting the first row of the state array;
- (ii) The second row is circularly shifting by one byte to the left;
- (iii) The third row is circularly shifting by two bytes to the left; and
- (iv) The last row is circularly shifted by three bytes to the left.

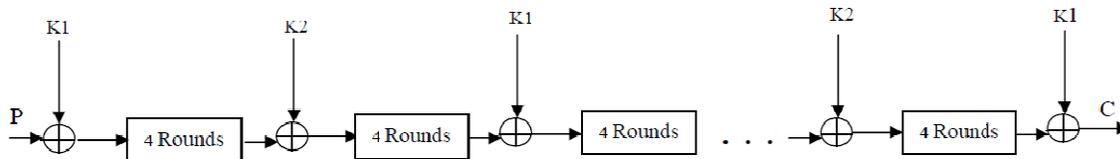


Figure 1. Light Encryption Device

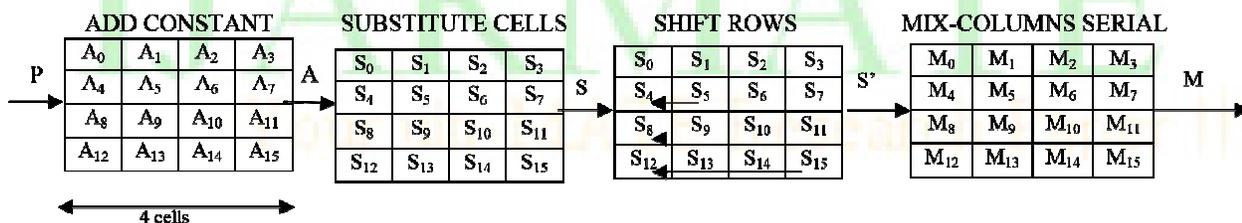


Figure 2. Operation involved in LED

Table 1 S-Box

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

C. Mix-Column Serial

Each column vector is replaced by another column vector after multiplying it with the matrix which is shown in Figure 3.

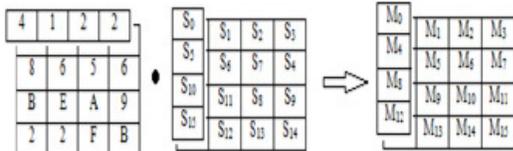


Figure 3. Mix-columns operation of LED algorithm

III IMPLEMENTATION OF LED

The hardware implementation of LED block cipher by JianGuo, Thomas Peyrin, Axel Poschmann and Matt Robshaw has been proposed in 2011 and implemented. Lightweight Encryption device block cipher is a 64-bit block cipher that uses cryptographic key sizes varying from 64-bits to 128 bits.

It is proposed to achieve high throughput through, parallel sub pipelined architecture is shown in figure 4. In this architecture the 128-bit key is divided into 2 blocks of 64-bit and it is processed parallel. To store the intermediate values the register is inserted, it act as a buffer and they can be used for further processing. By key scheduling the 128-bit key is divided into two 64-bit blocks and processed parallel by sending to set of blocks and perform ten rounds of operation. Add Constant, Substitute cells, Shift Rows and Mix columns are the modules used for the design.

In the pipelined architecture, the inputs are given to more than one round, so that more than one input can be processed at a time and thereby the throughput of the architecture get increased. The throughput thus obtained is 10% more than that of loop unrolled architecture. Further to increase the throughput the sub-pipelined architecture is used. The register are used in sub-pipelined architecture among substitute cell, shift Rows and Mix-Columns to store intermediate results. Here the processing time get increased to overcome that parallel architecture is used. Thus the parallel architecture reduces the tradeoff between the area and speed.

IV PERFORMANCE METRICES

The important parameter required for the evaluation of the implementation of this architecture are Throughput and Efficiency. The Very High Speed Hardware Description Language code is written for this architecture.

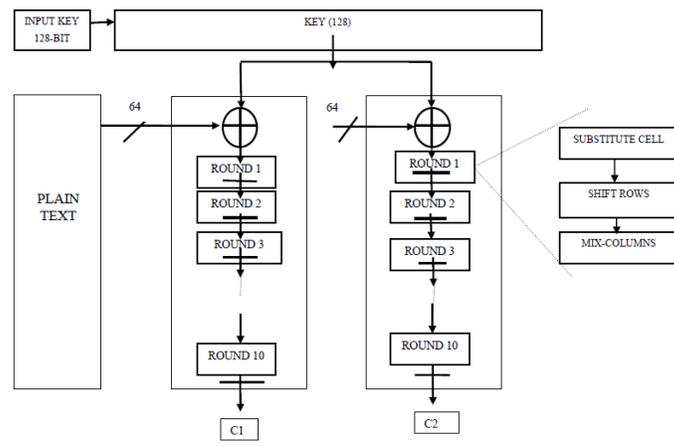


Figure 4. Sub-pipelined parallel Light Encryption Device architecture

Throughput and efficiency analysis

The speed at which the data is encrypted and decrypted is throughput. The performance of the algorithm is mainly determined by the Throughput.

The throughput [10] can be calculated by the formula

$$\text{Throughput} = \frac{128 * \text{Number of blocks/cycle}}{\text{Period}}$$

The efficiency [11] is calculated

$$\text{Efficiency} = \frac{\text{Throughput}}{\text{Area}}$$

Area Analysis

In general, there is a tradeoff between the throughput and area. In pipeline architecture the area get increased at the cost of speed. Due to the increased number of register in between the rounds the area get increased by sub pipelined architecture. The proposed architecture also consume more area compare to other cryptography architecture. It is necessary to decrease

V RESULT AND DISCUSSION

The symmetric lightweight efficient LED algorithm is designed using VHDL and simulated using modelsim simulator Altera 6.5e and synthesized using the Xilinx synthesizer and targeted in FPGA device Spartan 6. The modelsim simulation results of LED block cipher Encryption and Decryption is shown in Figure 5 and Figure 6 respectively. In this work FPGA device

SPARTAN 6 is targeted. Spartan-6 devices are the most cost-optimized FPGAs, offering industry leading connectivity features such as high logic-to-pin ratios, small form-factor packaging, and a diverse number of supported I/O protocols. Built on 45nm technology, the devices are ideally suited for a range of advanced bridging applications found in automotive infotainment, consumer, and industrial automation.

The algorithm is verified using the input which is shown below (in Hexadecimal representation)

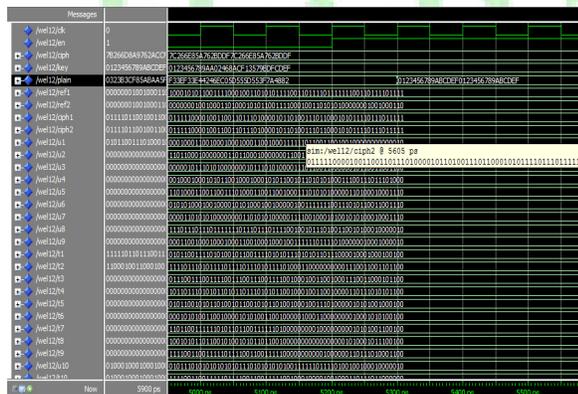
Plain text :
 0123456789ABCDEF0123456789ABCDEF
 KEY :
 01234567898048D159E26AF37BEBCEDEF
 Cipher Text:
 7C266E85A762BDDF7C266E85A762BDDF

VI CONCLUSION AND FUTURE WORK

Cryptography algorithm are omnipresent in modern communication in which the information security, such as confidentiality of communication or reliable authentication is absolute necessities. Efficient implementation techniques are necessary in order to provide high-security cryptographic algorithms.



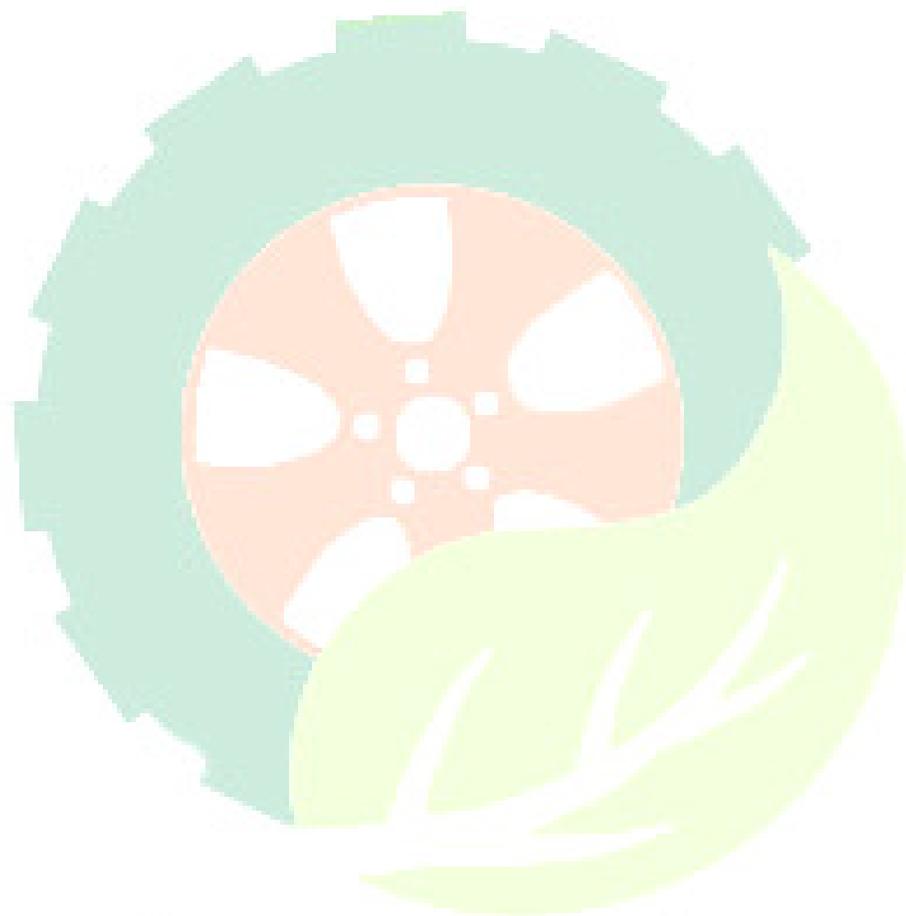
Figure 5. Simulation of encryption module



Hence in this work, encryption of serial and parallel sub-pipelined of Lightweight LED block cipher was successfully simulated using modelsim simulator Altera 6.5e and synthesized using the Xilinx synthesizer and targeted in FPGA device Spartan 6. This work is mainly concentrate on the improvement of throughput of the Algorithm. Further the area of the device can be reduced by reducing the number of rounds in the algorithm.

REFERENCES

- [1] R. RajaRaja and D. Pavithra, "Implementation of Hardware Efficient Light Weight Encryption Method", International conference on Communication and Signal Processing, April 3-5, 2013, India, ©2013 IEEE.
- [2] JianGuo, Thomas Peyrin, Axel Poschmann, and Matt Robshaw, "The LED Block Cipher", Cryptographic Hardware and Embedded Systems, Springer-Verlag, 2011,
- [3] Mika Fujishiro, Masao Yanagisawa and NozomuTogawa "Scan-based Attack on the LED Block Cipher Using Scan Signatures", 978-1-4799-3432-4/14/\$31.00 ©2014 IEEE
- [4] Swarnendu Jana, JaydebBhaumik, Manas Kumar Maiti "Survey on Lightweight Block Cipher", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-5, November 2013
- [5] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," Federal Information Processing Standard (FIPS) 197, 2001.
- [6] J. Daemen and V. Rijmen, "The block cipher Rijndael, " Smart Card research and Applications, LNCS 1820, Springer-Verlag, pp. 288-296.
- [7] Axel York Poschmann, "Lightweight Cryptography: Cryptographic Engineering for a pervasive world", 2009.
- [8] MickaelCazorla, Kevin Marquet and Marine Minier "Survey and Benchmark of Lightweight Block Ciphers for Wireless Sensor Networks,"Universite de Lyon, INRIA, INSA-Lyon, CITI-INRIA, F-69621, Villeurbanne, France
- [9] Zheng Gong, SvetlaNikova, and Yee Wei Law "KLEIN: A New Family of Lightweight Block Ciphers", Springer VerlagBerlin,Heilderberg, 2012.
- [10] M.K.Sirin,D.K.Mahesh,D.Y.Rama,HighThroughput-LessAreaEfficientFPGAImplementationofBlockCipher AESAlgorithm,InternationalConferenceonAdvancedComputing,CommunicationandNetworks,Chandigarh,
- [11] H.Qin,T.Sasao,Y.Iguchi,AnFPGADesignofAEEncryptionCircuitwith128-bitKeys,Proceedingsofthe15thACMGreatLakesSymposiumonVLSI(GLSVLSI),Illinois,Apr il17-19,2005



IJARMATE

Your *ulti-MATE* Research Paper !!!