Middle-East Journal of Scientific Research 24 (S1): 173-176, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.S1.35

# Efficient Implementation of (LED) Light Encryption Device Using Pipeline Architecture

*P. Felsis Raja Sofia and T. Blesslin Sheeba*

Dept of ECER.M.K. Engineering College, Kavaraipettai, Thiruvallur, India

**Abstract:** To satisfy resource constraints in the small embedded applications which have limited resources, lightweight symmetric LED block cipher plays a major role in the bulk data encryption and offer smallest silicon footprint among comparable block cipher. 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 a block size of 128-bits and a key size of 128-bits. The trade of 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.

**Key words:** Lightweight cryptography · FPGA · LED Block Cipher · Security · Confidentiality

## INTRODUCTION

Cryptograph play a vital role in encryption and decryption of data.Cryptography enables to store sensitive information or transmit it across insecure networks so it cannot be read by anyone than the intended recipient. The science of securing data is called cryptography, where the counterpart cryptanalysis is the science of breaking secure communication and analyzing.In general, cryptography embraces both cryptography and cryptanalysis.

The terms are;

**Plain Text:** An attacker can read a message easily because it is in natural form is called plain text.Cipher text: Message altered which is unreadable by anyone except the intended recipients.

**KEY:** Sequence which controls the operation and behavior of the cryptographic algorithm.

**Encryption:** Converting from plaintext to cipher text is called encryption.

**Decryption:** The process of restoring from the cipher text.

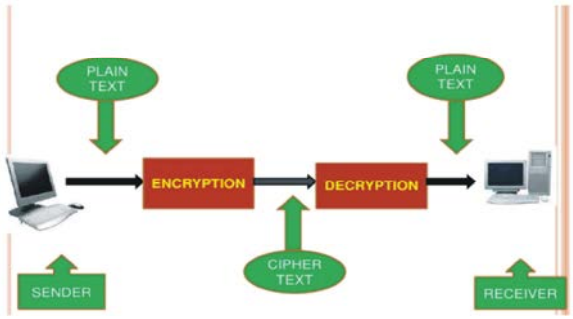


Fig. 1: Encryption and Decryption process

**Types of Cryptography:** The main types of cryptographic schemes are;

**Symmetric Key Cryptography:** It is also referred conventional encryption. Symmetric key encryption uses the same key for encryption as well as decryption. In the symmetric key cryptography, the security directly depends on the key. The symmetric cryptography is further classified into

- Stream cipher
- Block cipher

Bit by Bit encryption takes place in stream cipher and block of data encryption in block cipher.

**Corresponding Author:** P. Felsis Raja Sofia, Department of ECER.M.K. Engineering College, Kavaraipettai, Thiruvallur, India.

**Asymmetric Key Cryptography:** Asymmetric key encryption uses different keys for encryption and decryption. One of these keys should be kept private, called public-key and the other can be made public, calledpublic key. A private key is used for encrypting the message-digest in such an application private-key algorithm is called message digest encryption algorithm. A public key is typically used for encrypting the secret key in such an application private-key algorithm is called key encryption algorithm.

**Lightweight Cryptography:** The miniature device such as RFID and sensor nodes contain confidential information where the traditional cryptographic algorithm cannot satisfy the constraints in such a case lightweight cryptographic algorithm have been used. “As light ass feather and hard as dragon scale” Was Bilbo Baggins description for Mithril, a legendary material in J.K.R. Tolkiens famous novel “The Lord of the Rings” . On one hand Lightweight cryptography aims to yield very lightweight implementations that are virtual “As light as a feather”. “Hard as dragon scale” is good paraphrase for this aspect, because it emphasizes that there is sufficient security level [1].Some of the lightweight block ciphers are AES, DES, HIGHT, PRESENT, KTANTAN, TEA and PRINCE. Even without key schedule LED is ahead in terms of security. It is also more resistant to classical attacks and related key attacks.

**Related Works:** Many cryptographic algorithms have been implemented to provide security. But in this paper, we have implementeda hardware efficient symmetric Light Encryption Device(LED) to increase the speed by using pipeline architecture.

**Advanced Encryption Standard (AES):** AES was first developed by Joan and Vincent Rijmen in 2000 , uses the Rijndael block cipher. Depends on the key the number of rounds varies. The steps involved in the algorithms are Substitute bytes, Shift Rows, Mix Columns Add Round Key.

Table 1: Comparision of AES, DES, LED

| Factor | AES | DES | LED |
|---|---|---|---|
| Key LENGTH | 128,192 OR 256 | 56 | 64,128 |
| Cipher Type | Symmetric block Cipher | Symmetric block Cipher | Symmetric block Cipher |
| Network type | SPN | Feistel | SPN |
| Best known attacks | Side channel attacks | No attack has been exhibited | Meet in the middle attacks |

**Data Encryption Standard (DES):** DES was the first algorithm recommended by NIST (National Institute of Standards and Technology). The algorithm undergoes an initial permutation, sixteen rounds block cipher and a final permutation [2].

**LED (Light Encryption Device):** LED is an SPN (Substitution Permutation Network) [3] type Lightweight 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 [4]. The LED algorithm block diagram is shown in Figure 2. The steps during the encryption and decryption process depend on the keys is shown in Table 2 and Table 3.

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

**Substitute Cells:** The present S-box is used for the operation of LED. It is a 16-bit elements is shown in Table 3.

**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.

**Proposed Architecture:** The LED block cipher was implemented by Jian Guo, Thomas Perrin, Axel Poschmann and Matt Robshaw in the year 2011. It is implemented in Mentor graphics [5]. To reduce the hardware utilization iterative architecture is used and synthesized using Xilinx and it is targeted to spartan 3 devices of FPGA [6]. The parallel pipeline architecture is proposed to increase the speed in this paper is shown in Figure 4. In this architecture, the input key is divided into two blocks of 64-bit keys and processed parallelly. So more than one input can be processed at a time, thereby the speed of architecture increased at the cost of the area. The operation involved in the architecture are Add Round key, Add Constant, Substitute Cells, Shift Rows and Mix Columns [7]. To store the intermediate values buffers are used in between the round operation. For the first round (i=0) the plain text is EX-OR’ed with the key. Then it undergoes the round operation such as Add constant, substitute cells, Shift rows and Mix columns. After 12 rounds of operation, the cipher text is generated. To retrieve the original plaintext the inverse operation of encryption is processed.

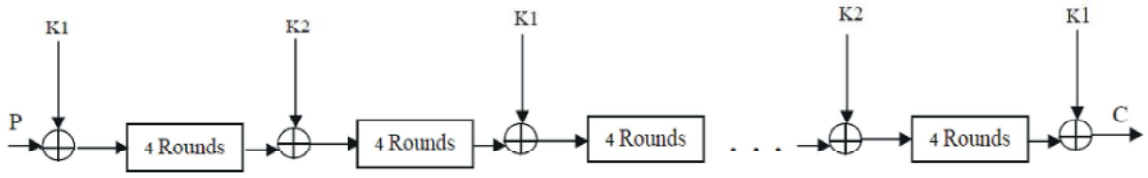


Fig. 2: Block diagram of LED

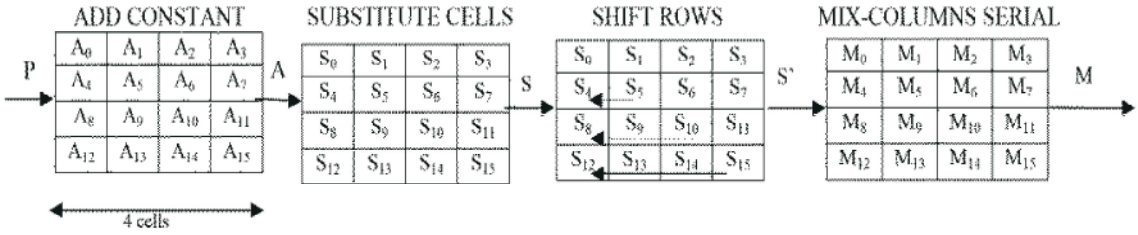


Fig. 3: Operation in LED

Table 4: 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 |

Table 2: For 64 bytes key

```
for i=1 to 8 do
{
addRoundKey(state,k1)
step(state)
}
Addroundkey(state,k1)
```

Table 3: For 128 bit key

```
for i=1 to 6 do
{
addRoundkey(state,k1)
step(state)
addRoundkey(state,k2)
step(state)
}
addRoundkey(state,k1)
```

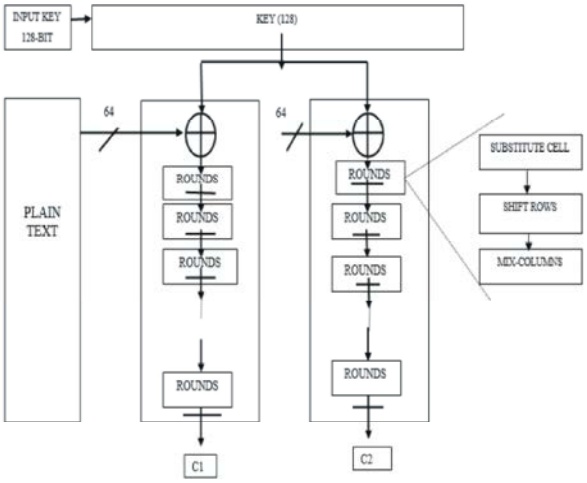


Fig. 4: Parallel pipeline architecture

**Hardware Implementation:** In this proposed approach for effective implementation of Lightweight cryptographic LED, algorithm is preferred. FPGA Field Programmable Gate Arrays introduced in 1985 by Xilinx Company, is a set of programmable device consist of CPLDs. The three main parts are set programmable logic cells, a programmable interconnection network and set of input-output cells. ASIC Application Specific Integrated circuits is an integrated circuit customized for particular use. Depends on the constraint and application either FPGA or ASIC is preferred. 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 [8].

## RESULTS AND DISCUSSIONS

The LED algorithm is designed using the VHDL language and it is simulated using ModelSim simulator Altera 6.5e and synthesized using Xilinx synthesizer.

Table 5: Synthesis Report

| TARGET FPGA device | Virtex xc6slx 150-3fgg676 |
|---|---|
| Optimizing goal | speed |
| Maximum operating frequency | 45.738 MHz |
| No of slice registers | 384 out of 184304 |
| No of Slice LUTs | 25193 out of 92152 |
| Number used as logic | 25193 out of 92152 |
| Number of bonded IOBs | 386 out of 396 |
| Number of BUFG/BUFGMUXs | 1 out of 16 |
| Number of MUXCYs used | 7296 out of 46076 |
| Encryption /Decryption Throughput | 281Gbps |
| Total memory usage | 914 MB |


Fig. 5: Comparison of Number of slice registers

The targeted FPGA device used is Virtex xc6slx 150-3fgg676. The total number of slice register used in this technology is 384. The number of Slice LUTs used here is 25193.The number of BUFG/BUFGMUXs is 1. The total memory usage for this architecture is 914MB. The Synthesis report of Xilinx is shown in Table 5. The comparison of Number of slice registers for AES and LED is shown in Figure 5. The comparison of a number of bonded IOBs is shown in Figure 6.


Fig. 6: Comparison of number of bonded IOBs

Table 6: Comparison AES and LED parallel Sub pipelined Architecture

| S.No | Architecture | Throughput | AREA (SLICES) | EFFICIENCY |
|---|---|---|---|---|
| 1 | Parallel Sub-pipelined AES | 59.59Gbps | 2597 | 22.92 |
| 2 | Parallel Sub Pipelined LED | 281.022Gbps | 384 | 73.182 |

## CONCLUSION

Cryptography algorithms are omnipresent in modern communication in which the information security, such as confidentiality of communication or reliable authentication is absolute necessities. 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 concentrates on the improvement of throughput and area of the implementation Algorithm. The throughput and area of parallel sub-pipelined AES is compared with that of LED where LED is found to be more efficient is shown in Table 6. Therefore LED is suitable for small embedded applications. In Future, the area of the device can be reduced by optimizing the rounds in the algorithm.

## REFERENCES

1. Axel York Poschmann, 2009. "Lightweight Cryptography: Cryptographic Engineering for a pervasive world",.
2. http://www.xilinx.com/products/silicon-devices/fpga/spartan-6.htm
3. Swarnendu Jana, Jaydeb Bhaumik and Manas Kumar Maiti, 2013. "Survey on Lightweight Block Cipher", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, 3(5).
4. Mika Fujishiro, Masao Yanagisawa and Nozomu Togawa, "Scan-based Attack on the LED Block Cipher Using Scan Signatures", 978-1-4799-3432-4/14/$31.00 ©2014 IEEE.
5. Jian Guo, Thomas Peyrin, Axel Poschmann and Matt Robshaw, 2011. "The LED Block Cipher", Cryptographic Hardware and Embedded Systems, Springer-Verlag.
6. Raja, Raja R. and D. Pavithra, 2013. "Implementation of Hardware Efficient Light Weight Encryption Method", International conference on Communication and Signal Processing, April 3-5, 2013, India, ©2013 IEEE.
7. National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES), " Federal Information Processing Standard (FIPS) 197, 2001.
8. Florian Mendel, Vincent Rijmen, Deniz Toz, Kerem Var_c_ "Differential Analysis of the LED Block Cipher".