ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

Compact and High Speed Hardware Implementation of CLEFIA

Pankaj V. Jadhav[1], Vishnu Suryawanshi[2]

ME Student, E&TC, GHRIET, Pune, India[1]

Asst.Professor, E&TC, GHRIET, Pune, India[1]

Abstract: Since 19th century, we were get aware of the process of communication. But, from the last 3 or 4 decades we knew how the communication is essential for entire living. It is just a process of conveying information from one end to another. One end is known as transmitter and other a receiver. For the success of communication, there should be presence of these both. As the use of this process goes on increasing, different methods or strategies were established. Afterwards the human being experienced that, not only the communication is important but also its safety is important. To achieve safety of communication many methods are used. But, the best method while using communication is Cryptography. Clefia is one algorithm used in Cryptography. It is 128 bit block cipher algorithm. This paper presents the different work done on Clefia by different authors. Also it proposes a method for the implementation of Compact and High Speed Hardware of CLEFIA.

Keywords: Cryptographic Techniques, Encryption, Clefia, Xilinx, FPGA.

I. INTRODUCTION

This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website. Communication means exchanging ideas, thoughts, messages, informations etc. either by speech, by writing, signals or by behavior. Communication is the word which is derived from latin word “communis”, which means to share. For the process of communication there is necessity of sender, message and receiver. There is no need that the receiver is present at the senders end. Also, it’s not necessary that the receiver must be aware of the communication process. So, the process of communication occurs in larger distances also. The process completes when the receiver gets or understood the message sent by the sender. Wireless communication is the fastest increasing part of communication industry. There is large growth over the last decade and there is approximately 2 billion users of wireless communication in world. The wireless communication network is replaced wired communication network in many industries, homes etc. The concept of mobile or wireless communication was first developed by the Bell Laboratories in 1960s and 1970s.Then in 1970s with the development of highly reliable, small size solid state radio frequency hardware the wireless communication became practically possible. Upto 1980s there is large penetration of mobile in market. However , in the last 10 years the market penetration rate of wireless communication is extremely high.

II. LITERATURE REVIEW

In [1], the author describes compact hardware implementations of CLEFIA. His work is based on novel serialized architectures in the data processing block. Three types of hardware architectures are implemented and synthesized using a 0.13 μm standard cell library. For the small implementation, the required area is of only 2,488 GE, which are about half of the previous smallest implementation as far as we know. Furthermore, only additional 116 GE enable to support decryption.

In [2], two compact hardware structures for the computation of the CLEFIA encryption algorithm are presented. One structure based on the existing state of the art and a novel structure with a more compact organization. This paper shows that, with the use of the existing embedded FPGA components and a careful scheduling, throughputs above 1Gbit/s can be achieved with a resource usage as low as 86 LUTs and 3 BRAMs on a VIRTEX 5 FPGA. In the result the LUT reduction was very big, due to which the Throughput/Slice efficiency rises up to 2.5 times, if it is compared with the related state of the art.

In [3], the author says about high-performance hardware architectures for the 128-bit block cipher CLEFIA and finds their ASIC performances. The author designed five types of hardware structures of CLEFIA by combining two loop structures and three F-functions. These designs were synthesized with a 90-nm CMOS standard cell library, and size and speed performances were evaluated. The output efficiency obtained was 400.96 Kbps/gates, which is 1.5 times greater than that of previously achieved results.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

In [4], the article presents a pipeline implementation of the blockcipher CLEFIA. The article examines three known methods of implementing a single encryption round and proposes a new fourth method. The article tells about the implementation of a key scheduler part. The article contains a detailed analysis of the data processing path for the 128-bitkey version of the algorithm and verifies its operation on two FPGA cards in practice. On the basis of one of these cards, the article proposes a prototype of an effective upper computer-compatible hardware accelerator.
In [5], the author tells about 128-bit CLEFIA structure which supports the different key lengths. The supported keys are 128, 192 and 256 bits. And the clefia is compatible with AES. This new structure of Clefia manages good immunity against known attacks. Also, it is flexibile for efficient structure in both hardware/software with the help of design methods. CLEFIA achieves a good performance profile both in hardware and software. CLEFIA is a greatly efficient structure,majorly in hardware.

In [6], some basics about cryptography are described by author.

In [7], two kinds of contemporary developments in cryptography are examined. They suggest ways to solve currently open problems at that time. They also discussed about the theories of communication and computation solve problems in cryptography.

In [8], the author says that at the present state there are more efficient structure for cryptographic techniques are dedicated structures. These structures allows only single algorithm to process. For the existing multi-algorithm processors there is requirement of high costs and lesser efficiency structures. Use of reconfigurable technologies requiresextra costs in efficiency and in there configuration process also. The proposed solution provides the support for multi-algorithm by using common components and hence getting common result.

In [9], the author explains about Cryptography and its classification. They described the different types of cryptography, like Symmetric Cryptography, Asymmetric Cryptography and Threshold Cryptography. Also, they have presented 2 sub types of Asymmetric Cryptography which are known as Identity Based Cryptography and Elliptic Curve Cryptography.

In [10], the author tells about a new differential fault analysis known as DFA on CLEFIA of 128-bit key. The same attack uses 2 pairs of fault-free and faulty ciphertexts. And it finds the 128-bit secret key. The attacker need not to know about the original data. The more efficient discovered fault attack on CLEFIA, requires fault induction at the 15th round of encryption. It can be performed with 2 pairs of fault-free and faulty ciphertexts and brute-force search of around 20 bits. The simulation results have been presented to validate the same mentioned attack. The simulation results says that the attack can retrieve the 128-bit secret key in around one minute of running time. For the input requirements and the complexity the mentioned attack is most efficient.

In [11], the author says about a new lightweight cipher called L Block. L Block can achieve good security margin against known attacks, such as differential cryptanalysis, linear cryptanalysis, impossible differential cryptanalysis and related-key attacks etc. The L Block can be implemented efficiently in hardware environments and also in software platforms like 8-bit microcontroller.

In [12], the author says about meet-in-the-middle that is MITM. This attack occurs on block ciphers. Though there are significant improvements of the MITM attack, still its application is restrictive. Many MITM attacks implements only on block ciphers consisting of a bit permutation based key schedule such as KTANTAN, GOST, IDEA, XTEA, LED and Piccolo. The author extend the MITM attack so that it is possible to apply to a wider class of block ciphers. In their approach, MITM attacks on block ciphers.

In 13], the author generates impossible differential cryptanalysis on the 128-bit block cipher CLEFIA. Clefia was proposed in 2007, with 9-round impossible differentials for CLEFIA, and the result of an impossible differential attack using them. The author describes that, for 128-bit key, it is possible to apply the impossible differential attack to 12 rounds of CLEFIA. For 192 bits of key lengths and 256 bits, it is possible to apply this attack to 13-round and 14-round CLEFIA.

In [14], the author proposes complexity analysis formulas for mounting several attacks. Also, he tells about developing new things for optimizing impossible differential cryptanalysis. These ideas include for example the testing of parts of the internal state for reducing the number of involved key bits. They also develop in a more general way the concept of using multiple differential paths, an idea introduced before in a more restrained context. These enhancements increases the previous attacks against well-known ciphers such as CLEFIA-128.

In [15], the author describes different basics related to the cryptography.

In [16], the author proposes that CLEFIA is an efficient lightweight cipher which delivers advanced copyright protection and also authentication in computer networks. It is also applied in the secure protocol for transmission that contains SSL and TLS. Since it was proposed in 2007, some work about its security against differential fault analysis has been developed which reduces the number of faults and improves the time complexity of attack. This attack is very efficient if a single fault is injected into the last several rounds of the CLEFIA, and it allows to recover the whole secret key. In that paper, they present a fault detecting techniques of the CLEFIA block cipher. Their result in that study could detect the faults with very less cost when faults are even injected into the last 4 rounds.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

In [17], the paper says that Efficient implementation of block ciphers is important to achieve both high security and high-speed processing. So, the architecture provides an analysis of system performance. Also resource utilization to demonstrate the efficiency against other implementations.

III. PROPOSED WORK

As shown in figure 1 the flowchart of Clefia consists of different rounds of process. Depending upon the used key size for algorithm there is requirement of specific number of rounds [13]. That is for 128 bit Clefia, the required number of rounds are 18. Similarly, for 192 bit Clefia, the required number of rounds are 22 and for 256 bit Clefia, the required number of rounds are 26. The figure 2 shows the block diagram for Clefia implementation [13]. As shown in figure 1 the flowchart of Clefia consists of different rounds of process. Depending upon the used key size for algorithm there is requirement of specific number of rounds. That is for 128 bit Clefia, the required number of rounds are 18 [13]. Similarly, for 192 bit Clefia, the required number of rounds are 22 and for 256 bit Clefia, the required number of rounds are 26 [13].

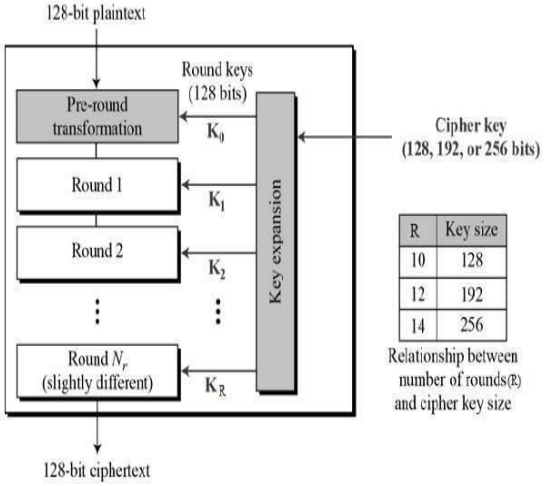

Fig. 1 Flowchart for 128- bit Clefia Structure

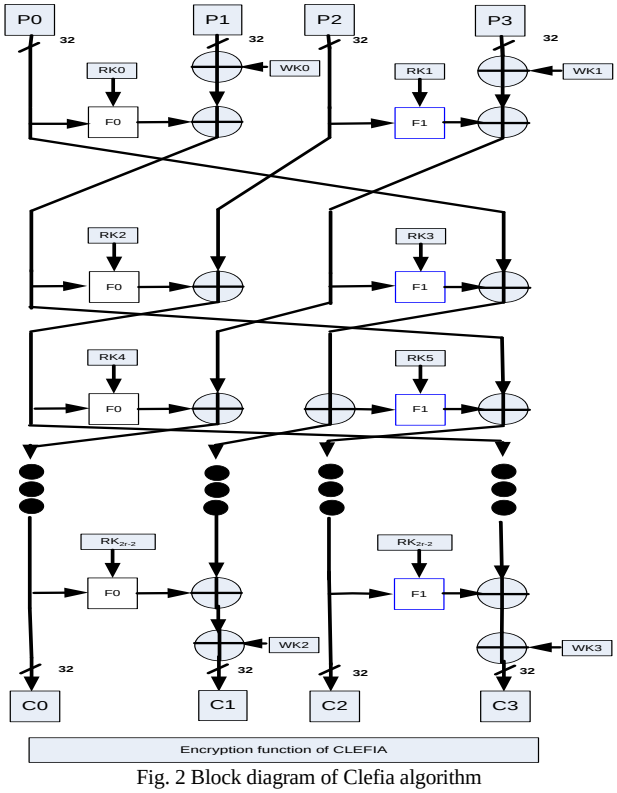

Fig. 2 Block diagram of Clefia algorithm

The figure 2 shows the block diagram for Clefia implementation.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

There are two F- Functions, F0 and F1. The functional block F0 and F1 are shown in figure 3 and figure 4 respectively.

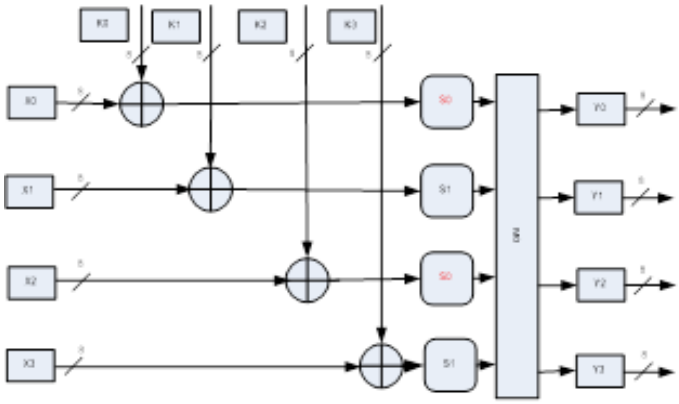

Fig 3. F0 Function

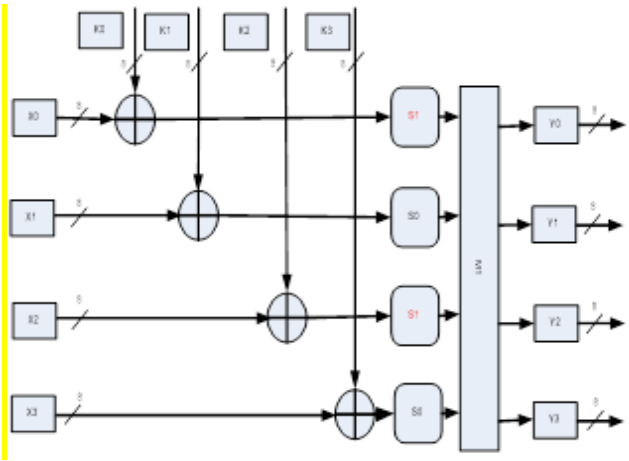

Fig 4. F1 Function

There is slight difference between the F0 and F1 functions. That is the position of S- boxes. The same kind of operation is done at both the F- functions [3].
As shown in above block diagram the plain text of 16 bytes that is 128 bits. This plain text is divided into total 4 parts. Each
part contains 32 bits of plain text data(32 bits x 4 = 128 bits). The 128 bit cipher key is very important here. So, it is used. At
the end from the cipher text is obtained and it is implemented on FPGA board.

A. Multiplication Process in F0 and F1 Functions

There are different multiplication methods used in implementation of cryptographic algorithm. Like,

- Add and Shift Method
- Booth's Algorithm
- Galois Field Method

Each of these methods has certain drawbacks. Here, we implemented another method for multiplication in Clefia algorithm.

The output data from Substitution boxes are multiplied in Diffusion Matrices M0 and M1. Let us know how it happens in these matrices.
Consider output of S0,S1,S0 and S1 is 29 02 46 and e1.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

Then M0 calculation is as follows:-

$$\begin{pmatrix} 29 \\ 02 \\ 46 \\ e1 \end{pmatrix} \begin{pmatrix} 01\ 02\ 04\ 06 \\ 02\ 02\ 06\ 04 \\ 04\ 06\ 01\ 02 \\ 06\ 04\ 01\ 02 \end{pmatrix} = \begin{matrix} Y1 \\ Y2 \\ Y3 \\ Y4 \end{matrix}$$

Y1= (29*01) $\oplus$ (02*02) $\oplus$ (46*04) $\oplus$ (e1*06)
Y2= (29*02) $\oplus$ (02*02) $\oplus$ (46*06) $\oplus$ (e1*04)
Y3= (29*04) $\oplus$ (02*06) $\oplus$ (46*01) $\oplus$ (e1*02)
Y4= (29*06) $\oplus$ (02*04) $\oplus$ (46*02) $\oplus$ (e1*01)

Here, (29*01) gets multiplied normally and gives output as 29.
But, there is quite difficulty while multiplying with multiple of 2.

1. Multiplication by 2(Multiply by x):

Let,
$a(x)= a_0+a_1x+a_2x^2+a_3x^3+a_4x^4+a_5x^5+a_6x^6+a_7x^7$ ----(1)
Let,
$b(x)= x *(b_0+b_1x+b_2x^2+b_3x^3+b_4x^4+b_5x^5+b_6x^6+b_7x^7)$
$=(b_0 x+b_1x^2+b_2x^3+b_3x^4+b_4x^5+b_5x^6+b_6x^7+b_7x^8)$
$= (b_0 x+b_1x^2+b_2x^3+b_3x^4+b_4x^5+b_5x^6+b_6x^7+b_7 (x^4 + x^3 + x^2 + 1)$
$= (b_0x+b_1x^2+b_2x^3+b_3x^4+b_4x^5+b_5x^6+b_6x^7+b_7x^4 + b_7x^3 + b_7x^2 + b_7)$
$=(b_0x+ (b_1+b_7) x^2+ (b_2+b_7) x^3+ (b_3+b_7) x^4+b_4x^5+b_5x^6+b_6x^7+ b_7)$

Comparing with equation (1)
$a_0<= b_7$; $a_1<= b_0$; $a_2<=(b_1 \oplus b_7)$; $a_3<=(b_2 \oplus b_7)$;
$a_4<=(b_3 \oplus b_7)$; $a_5<=b_4$; $a_6<= b_5$; $a_7<=b_6$;

Designing hardware circuit diagram:

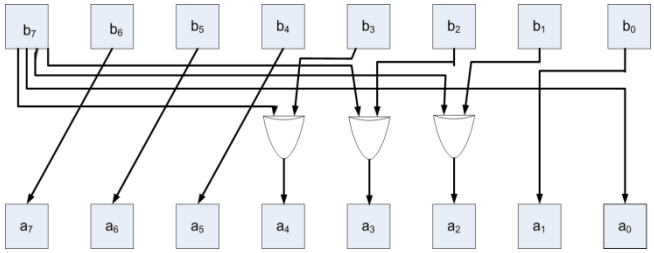

Fig. 5 Circuit diagram for Multiplication by 2

Now, suppose 1st we perform multiplication amongst 46 and 02. Then, we have to write 46 in binary form as below.

$b_7\ b_6\ b_5\ b_4\ b_3\ b_2 b_1\ b_0$
0 1 0 0 0 1 1 0 = (46)

Now, from above circuit diagram, we can easily generate the respective value of the multiplication as,

$a_7\ a_6 a_5\ a_4\ a_3\ a_2\ a_1\ a_0$
1 0 0 0 1 1 0 0 = (8C)

So, after multiplication of 46 and 02 the result is 8C.

2. Multiplication by 4 (Multiply by x^2):

Let,

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

$b(x)= b_0x^2+b_1x^3+b_2x^4+b_3x^5+b_4x^6+b_5x^7+b_6x^8+b_7x^9$
$= b_0x^2+b_1x^3+b_2x^4+b_3x^5+b_4x^6+b_5x^7 +b_6 (x^4+x^3+x^2+1) +b_7 (x^5+x^4+x^3+x)$
$b(x) = b_0x^2+b_1x^3+b_2x^4+b_3x^5+b_4x^6+b_5x^7 +b_6 x^4+ b_6 x^3+ b_6 x^2+ b_6 +b_7x^5+ b_7 x^4+ b_7 x^3+ b_7 x)$
$=b_6 +b_7 (x)+(b_0 + b_6)x^2 +(b_1 + b_6 + b_7) x^3 + (b_2 + b_6 + b_7) x^4 + (b_3+ b_7) x^5 +b_4x^6 \quad +b_5x^7$

Comparing with equation (1)

$a_0<=b_6$, $a_1<=b_7$; $a_2<b_0 \oplus b_6$;$a_3<=b_1 \oplus b_6 \oplus b_7$; $a_4<=b_2 \oplus b_6 \oplus b_7$; $a_5<=b_3 \oplus b_7$; $a_6<=b_4$; $a_7<b_5$;

Designing hardware circuit diagram:

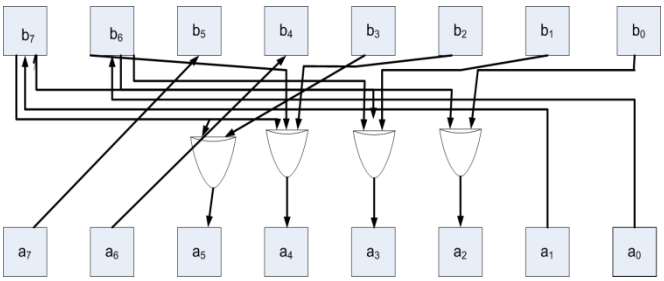

Fig. 6. Circuit diagram for Multiplication by 4

Now, suppose we are performing multiplication amongst 46 and 04. Then, we have to write 46 in binary form as below.

b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0
0 1 0 0 0 1 1 0 = (46)

Now, from above circuit diagram, we can easily generate the respective value of the multiplication as,

a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0
0 0 0 0 0 1 0 1 = (05)

So, after multiplication of 46 and 04 the result is 05.

3. Multiplication by 6 (Multiply by $x+ x^2$):

Let,
$b(x)= x+ x^2*(b_0+b_1x+b_2x^2+b_3x^3+b_4x^4+b_5x^5+b_6x^6+b_7x^7)$
$= ((b_0x+ (b_1+b_7) x^2+ (b_2+b_7) x^3+ (b_3+b_7) x^4+b_4x^5+b_5x^6+b_6x^7+ b_7)) +$
$(b_6 +b_7 (x)+(b_0 + b_6)x^2 +(b_1 + b_6 + b_7) x^3 + (b_2 + b_6 + b_7) x^4 + (b_3+ b_7) x^5 +b_4x^6+b_5x^7)$
$= (b_0 + (b_6 +b_7) (x) + (b_0 + b_1+ b_6 + b_7)x^2+ (b_1 + b_2 + b_6 + 2b_7) x^3+ (b_2+ b_3 + b_6 + 2b_7) x^4+ (b_3+ b_4+ b_7) x^5+ (b_4+ b_5) x^6 + (b_5+ b_6) x^7+ (b_6 +b_7)$

Comparing with equation (1)
$a_0<=b_6 \oplus b_7$, $a_1<=b_0 \oplus b_7$; $a_2<=b_0 \oplus b_1 \oplus b_6 \oplus b_7$; $a_3<=b_1 \oplus b_2 \oplus b_6 \oplus 2b_7$; $a_4<=b_2 \oplus b_3 \oplus b_6 \oplus 2b_7$; $a_5<=b_3 \oplus b_4 \oplus b_7$; $a_6<=b_4 \oplus b_5$; $a_7<=b_5 \oplus b_6$;

So, like above circuit diagrams, we can generate hardware circuit diagram for this multiplication. Now, suppose we are performing multiplication amongst e1 and 06. Then, we have to write e1in binary form as below.

b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0
1 1 1 0 0 0 0 1 = (e1)

From the above generated equations we can generate the result of multiplication as below.

a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0
0 1 1 1 1 1 0 0 = (7C)

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

Hence, for this multiplication the result is 7C. Similarly, the other multiplications can be performed. And finally we get results for Y1, Y2, Y3 and Y4. Which are the actual cipher text outputs for this 128 bit clefia.

IV. SIMULATION AND RESULTS

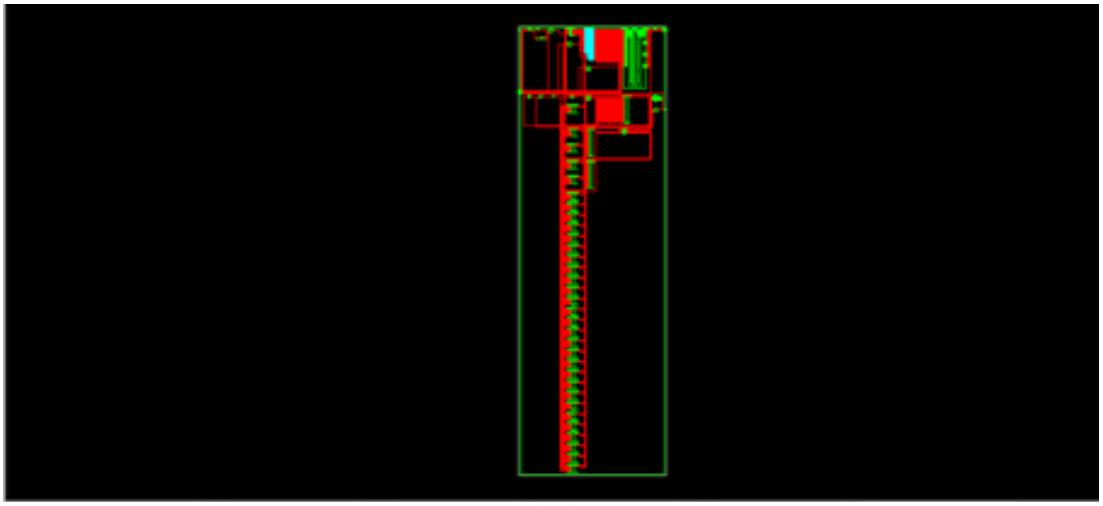

Fig. 7 Circuit diagram for for Encryption Process

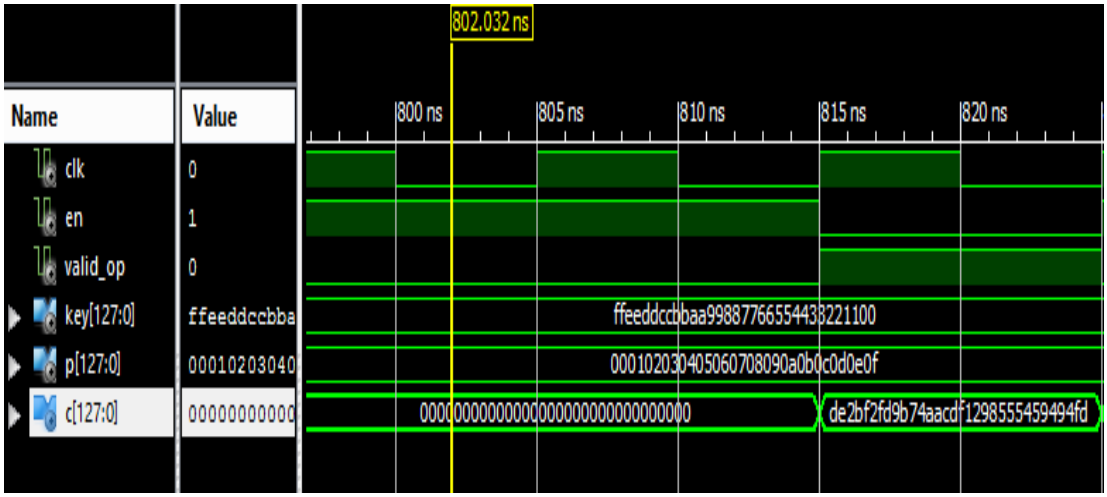

Fig. 8 Output window for 128 bit input data

By using this method the required number of logic gates reduces greatly, so the circuit becomes compact if we compare with respective previous circuits. Also, the speed of operation is also increases as the gates are less.
That is this implementation is providing a compact and high speed clefia structure.

V. CONCLUSION

The purpose of this proposed system is to implement a high speed and compact hardware structure of CLEFIA. In this paper a Clefia block cipher is presented. It uses a very important technique called as Diffusion and Switching Mechanism (DSM). The method used in Diffusion matrices gives a compact and high speed clefia structure.

REFERENCES

[1] ToruAkishita and HarunagaHiwatari "Very Compact Hardware Implementations of the Block cipher CLEFIA ". *Sony Corporation.*
[2] Paulo Proença and Ricardo Chaves *"*Compact CLEFIA Implementation On FPGAs*". 2011 21st International Conference on Field Programmable Logic and Applications.*
[3] Takeshi Sugawara, Naofumi Homma, Takafumi Aoki and Akashi Satoh." High-performance ASIC Implementations of the 128-bit Block Cipher CLEFIA ".
[4] Tomasz Kryjak and MarekGorgoń."Pipeline Implementation Of The 128-Bit Block Cipher CLEFIA In FPGA". *978-1-4244-3892-1/09/$25.00 ©2009 IEEE.*

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

[5] TaizoShirai, KyojiShibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata.“ The 128-Bit Blockcipher CLEFIA (Extended Abstract) ”. *Sony Corporation.*

[6] K. B. PriyaIyer, R. Anusha and R. ShakthiPriya. “Comparative Study on Various Cryptographic Techniques”. *International Journal of Computer Applications(0975 – 8887) International Conference on Communication, Computing and Information Technology(ICCCMIT-2014).*

[7] Whitfield Diffie and Martin E.Hellman “ New Directions in Cryptography ”. *IEEE Transaction on Information Theory, Vol. IT.22, No. 6, November 1970 .*

[8] Nicolas Sklavos, João Carlos Resende, Ricardo Chaves, Francesco Regazzoni, Osnat Keren “Efficiency of Cryptography for Multi-AlgorithmComputation on Dedicated Structures ”.

[9] RoozMunjal, PinkiTanwarand NitinGoel “ Optimized Solutions to Cryptography for Securing MANETs and Analyze Using Reputation System ”. *International Journal of Advanced Research in Computer Science and Software Engineering.*

[10]SkSubidh Ali and DebdeepMukhopadhyay “Protecting Last Four Rounds of CLEFIA is Not Enough Against Differential Fault Analysis ”.

[11] Wenling Wu and Lei Zhang “LBlock: A Lightweight Block Cipher ”.

[12] TakanoriIsobe and KyojiShibutani “All Subkeys Recovery Attack on Block Ciphers: Extending Meet-in-the-Middle Approach ”.

[13] YukiyasuTsunoo , Etsuko Tsujihara, Maki Shigeri, Teruo Saito, Tomoyasu Suzaki, and Hiroyasu Kubo “Impossible Differential Cryptanalysis of CLEFIA “.

[14] Christina Boura, Maria Naya-Plasencia, ValentinSuder “Scrutinizing and Improving Impossible Di_erential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon ”.

[15] Masanobu Katagi and Shiho Moriai “Lightweight Cryptography for the Internet of Things ”.

[16] Wei Li, DawuGu, Xiaoling Xia, Ya Liu, Zhiqiang Liu “Fault Detection on the Software Implementation of CLEFIA Lightweight Cipher ”.

[17] AJ Elbirt and ChristofPaar “Efficient Implementation of Galois Field Fixed Field Constant Multiplication”.