ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

FPGA IMPLEMENTATION OF LIGHT WEIGHT BLOCK CIPHER MIDORI

[1]SUBA SUNDARY S, [2]VIBHASRI S, [3]RAJALAKSHMI D

[1,2,3] UG Scholar, ECE Department
[1,2,3] Arulmigu Meenakshi Amman College Of Engineering
[1]subasubramanian06@gmail.com, [2]vibhasri94@gmail.com, [3]rajalakshmidevarajan34@gmail.com

ABSTRACT

The main aim of this project is to realize lightweight block cipher Midori in FPGA (Field Programmable Gate Arrays) using Verilog Hardware Descriptive Language. This project proposes a method to efficiently implement the lightweight block cipher in terms of low area, low latency and less energy consumption. We employ two architecture for implementing the light weight block cipher Midori, namely 1) Round Based Implementation and 2) Serial Implementation. The performance of both these implementations are compared and we present our observation in this thesis. We use the target FPGA Kintex-7 XC7K160-1FBG676C, which has a ROM of 64 Mb BPI Flash memory PC28F640P30TF65 and is of Dimension 200mm X 150 mm. These Ciphers are particularly useful for application that run on tight energy budget such as active RFID Tags, sensor nodes, medical implants and battery operated portable devices, IOT, Smart devices and Mobile Computing. Round Based Implementation are used for applications, where we require high throughputs and Serial Implementation are used in applications, if area is a major constraint.

Keywords: **FPGA, Vivado2014.4,Midori**,

I. INTRODUCTION

The lightweight block cipher is a symmetric key cipher which occupies less area. There are many lightweight block ciphers proposed such as LED, PRINCE, KLEIN, NEOKEON MIDORI and etc. PRESENT lightweight block cipher is the standardized algorithm certified by ISO. Consequently, many block ciphers are submitted for standardization. Midori is one such algorithm which is being analyzed for security and area efficiency. SETS (Society for Electronic Transactions and Security) is working in analyzing symmetric key ciphers against implementation attacks. SETS has analyzed many algorithms and published the report on lightweight block ciphers.

We choose Midori block cipher among others ciphers like NEOKEON, PRINCE, LED and KLEIN. This is because MIDORI not only reduces the Area and latency but also it reduces the overall energy consumption, making it more efficient than other ciphers. Midori consists of two variants: Midori 64 and Midori 128. These provide the functionality for both encryption. We employ two implementations namely Round based implementation and Serial implementation. Serial implementation has high latency, which take much longer time to compute the result of an encryption operation than Round Based implementation.

The components of Midori are specifically tailored to meet the requirements of low energy design.4 X 4 almost MDS binary matrices are used, which are more efficient than MDS matrices in terms of area and signal delay. Ciphers employing almost MDS matrices are likely to guarantee its security against several attacks. To address this issue, optimal cell permutation layers are utilized, which aims at improving the diffusion speed and number of active s-box in each round with low implementation overheads. The signal delay in the s-boxes is 1.5 times faster than those of PRINCE And NEOKEOON Ciphers. We look at some design considerations that help to

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

minimize energy consumption in block cipher circuits. Next, we describe the algorithm Midori 128 and Midori 64 ciphers. Then, we outline the security analysis of the ciphers and the implementation results of our cipher in hardware. Finally, we conclude the paper.

II.PREVIOUS WORK

In LED (Lightweight Encryption Device) Cipher, we employ the Shift Row Type Permutation. In shift row type permutation, row i of the array STATE is rotated i cell position to the left, for i=0, 1, 2, 3. By using the shift row type permutation, the diffusion speed is reduced and the number of active s-boxes in each round get decreased. Thereby consuming more energy. The main drawbacks of this system is active number of s-box in each round is reduced,diffusion speed is less and energy consumption of LED Cipher is high. Christo Ananth et al. [2] proposed a system in which the complex parallelism technique is used to involve the processing of Substitution Byte, Shift Row, Mix Column and Add Round Key. Using S- Box complex parallelism, the original text is converted into cipher text. From that, we have achieved a 96% energy efficiency in Complex Parallelism Encryption technique and recovering the delay 232 ns. The complex parallelism that merge with parallel mix column and the one task one processor techniques are used. In future, Complex Parallelism single loop technique is used for recovering the original message.

III.PROPOSED METHODOLOGY

In this proposed system, we use Midori ciphers and it employs optimal cell permutation layers. Optimal cell permutation drastically improve the minimum number of differentially/linearly active s-boxes in each round and achieve faster diffusion compared to shift row type permutation. The signal delay in our s-boxes is 1.5 times faster than those of PRINCE and PRESENT.

Advantage of Midori are

- Uses permutation cell layer than shift row type
- Improves the diffusion speed
- Number of active s-boxes in each round is increased.
- Midori cipher occupies less area and has low latency
- Midori Cipher Consumes Low Energy.

We present the hardware architecture for round based and serial implementations of Midori. The architecture may be utilized for area efficient implementation of Midori block cipher.

A.ROUND BASED ENCRYPTION ARCHITECTURE

2:1 MULTIPLEXER:

In this architecture, we use 2:1 multiplexer. Generally, multiplexer are capable of selecting one of the two inputs and produces a single selected output.
Initially the multiplexer selects the “a” input by making the select signal as 0. For the next rounds, the select signal becomes high and input “b” is selected.

REGISTER:

Registers are normally used for storing purposes. Here also the registers are utilized for storing the 64 bit data.
ROUNDS OF OPERATION

1) Sub cell
2) Shuffle cell
3) Mix Column
4) Add round Key

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

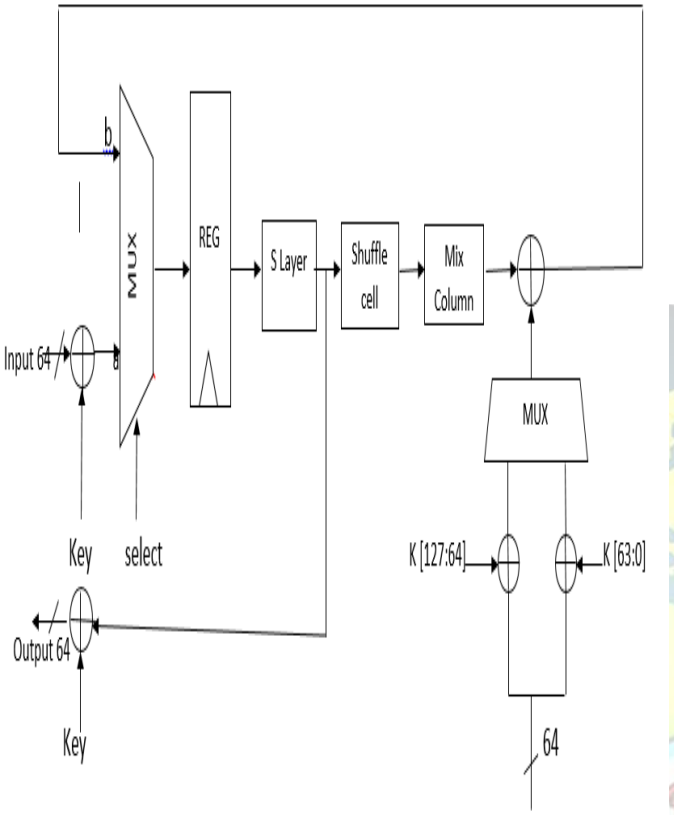

Fig 1 Basic Diagram of Encryption

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

B.OVERVIEW OF MIDORI 64

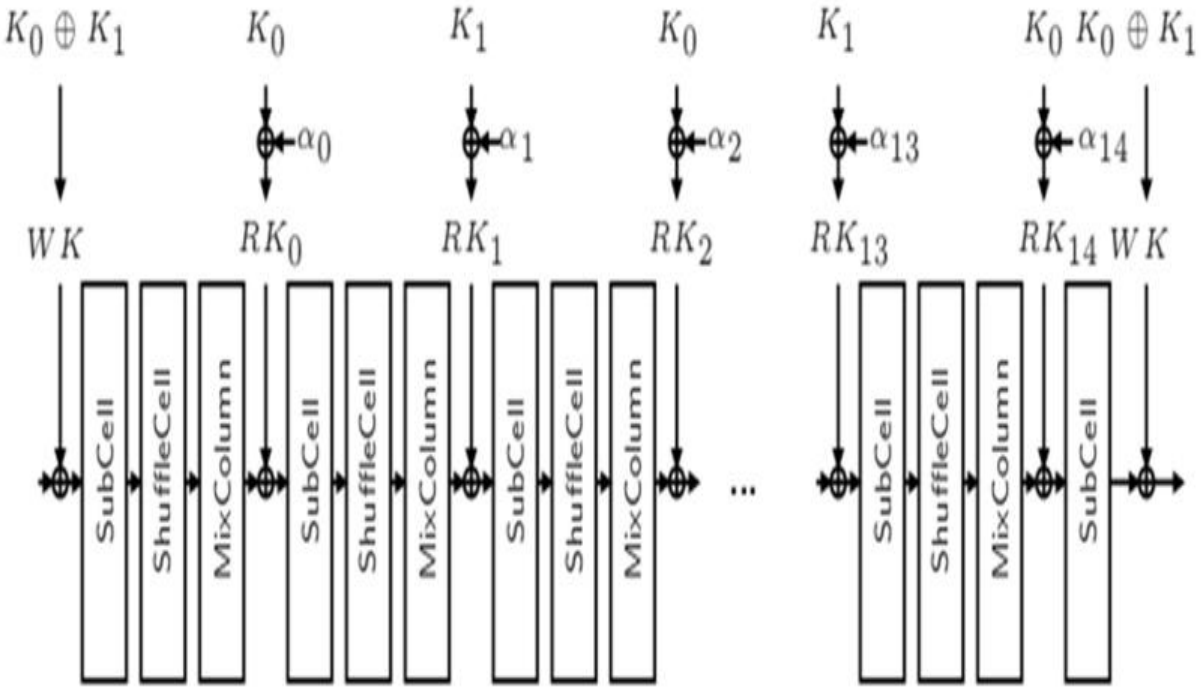

Fig 2 Overview of Midori 64

Midori 64 is a lightweight block cipher that accepts 64 bit plaintext and 128 bit key. Midori 64 has 16 rounds totally i.e., from round 0 to round 15. In the initial round, (i.e., in the round 0), the plaintext is xored with the 128 bit key whitening (WK). The first 64 bits of 128 bit key is represented as K_0 and the remaining 64 bits of 128 bit key is represented as K_1. RK_i represents the round key for i^{th} round, i=0, 1, 2, 3, 4……., 15. Initially, they plaintext is arranged in terms of column wise matrix. Then this plaintext is mapped to S-box values according to the S-box value specified in the table ( ). After mapping the plaintext to the S-box value, the elements of state array is then shuffled according to the shuffle cells specified in the table ( ). Later the shuffled elements of State Array is then multiplied with the Mix Column Matrix (Mc). Finally the resultant matrix obtained after multiplying with M matrix, is Xored with Round keys. The round keys for each round is different and is specified in the table ( ). After 16 rounds, the plaintext is being converted into Cipher text.

1) S-box

Midori utilizes two types of bijective 4-bit S-boxes Sb0 and Sb1 are used in Midori64 and Midori128, respectively. Note that Sb0 and Sb1 both have the involution property. Midori128 utilizes four different 8-bit S-boxes SSb0, SSb1, SSb2 and SSb3, where SSb0, SSb1, SSb2, SSb3: f0; 1g8 ! f0; 1g8 mathematically, each SSbi consists of input and output bit permutations and two Sb1's.Each output bit permutation is taken as the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

inverse of the corresponding input bit permutation to keep the involution property. Let the input bit permutation of each SSbi be referred to as pi.

Let x[i] denote the i^{th} bit of x, where x[0] is the most significant bit (MSB).The 4-bit bijective S-boxes Sb0 and Sb1 in hexadecimal form is given below:

X	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$Sb_0[X]$	c	a	d	3	e	b	f	7	8	9	1	5	0	2	4	6
$Sb_1[X]$	1	0	5	3	e	2	f	7	d	a	9	b	c	8	4	6

Table 1 4-Bit Bijective S-Boxes

2) Shuffle Cell

The each cell of the state is permuted as follows:

S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}
S_0	S_{10}	S_5	S_{15}	S_{14}	S_4	S_{11}	S_1	S_9	S_3	S_{12}	S_6	S_7	S_{13}	S_2	S_8

Table 2 Cell's State

3) Mix Column

M is applied to every 4m-bit column of the state S,

i.e., t(si; si+1; si+2; si+3) <------Mt(si; si+1; si+2; si+3) and i = 0; 4; 8; 12.

MDS vs Almost MDS. Using the Nan Gate 45nm open cell library, Table 6 compares three types of 4 X 4 matrices, involutive MDS (MA), non-involutive MDS (MB) and involutive almost MDS matrices (MC) from implementation aspects. These matrices are considered lightweight in each of the three afore mentioned criteria.

$$Ma=\begin{pmatrix}1&2&6&4\\2&1&4&6\\6&4&1&2\\4&6&2&1\end{pmatrix} \quad Mb=\begin{pmatrix}2&3&1&1\\1&2&3&1\\1&1&2&3\\3&1&1&2\end{pmatrix} \quad Mc=\begin{pmatrix}0&1&1&1\\1&0&1&1\\1&1&0&1\\1&1&1&0\end{pmatrix}$$

While MC has efficient implementation properties, its diffusion speed is slower and the minimum number of active S-boxes in each round is smaller than those of ciphers employing MDS matrices due to its lower branch number. It has been known that those properties are directly related to the immunity against several attacks including impossible differential, saturation, differential and linear attacks. To improve security of the almost MDS with low implementation overheads, we adopt optimal cell-permutation layers which are aimed at improving diffusion speed and increasing the number of active S-boxes in each round. The diffusion speed is measured by the number of rounds taken to attain full diffusion, which is the property that all output cells are affected by all input cells. Importantly, changing cell-permutation patterns generally does not require additional implementation costs in a round-based and an unrolled hardware implementation.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

4) Add Round Key

Here we XOR the resultant of Mix column output with the key and the Round Constant.

i		i		i		i		i		i		i	
	0 0 1 0		0 1 1 0		1 0 0 0		0 0 0 0		0 0 0 1		1 0 0 0		0 0 0 0
	0 1 0 0		1 0 1 0		0 1 0 1		1 0 0 0		0 0 1 1		1 0 1 0		0 0 1 1
0		1		2		3		4		5		6	
	0 0 1 1		1 0 0 0		1 0 1 0		1 1 0 1		0 0 0 1		0 0 1 0		0 1 1 1
	1 1 1 1		1 0 0 0		0 0 1 1		0 0 1 1		1 0 0 1		1 1 1 0		0 0 0 0
	0 1 1 1		1 0 1 0		0 0 1 1		0 0 1 0		0 0 1 1		0 0 0 0		1 1 1 1
	0 0 1 1		0 1 0 0		1 0 0 0		1 0 0 1		0 0 0 1		1 0 0 0		1 0 1 0
7	0 1 0 0	8	0 0 0 0	9	0 0 1 0	10	1 0 0 1	11	1 1 0 1	12	0 0 1 0	13	1 0 0 1
	0 1 0 0		1 0 0 1		0 0 1 0		1 1 1 1		0 0 0 0		1 1 1 0		1 0 0 0
	1 1 1 0		0 1 1 0		0 1 0 0		0 0 1 0		0 0 1 1				
	1 1 0 0		1 1 0 0		0 1 0 1		0 0 0 1		1 0 0 0				
14	0 1 0 0	15	1 0 0 0	16	0 0 1 0	17	1 1 1 0	18	1 1 0 1				
	1 1 1 0		1 0 0 1		1 0 0 0		0 1 1 0		0 0 0 0				

Table 3 The Round Constants

IV.ENERGY CHARACTERISTICS

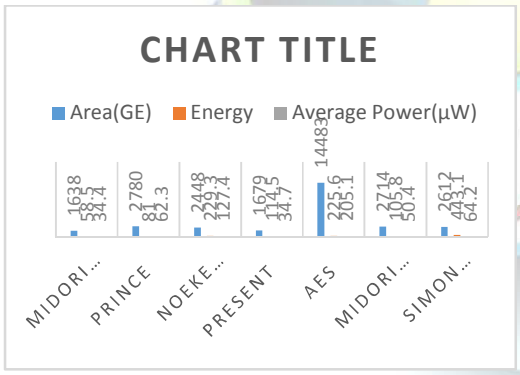

Table 4 Energy Characteristics

V.EXPERIMENTAL RESULT

Output of Round Based Implementation

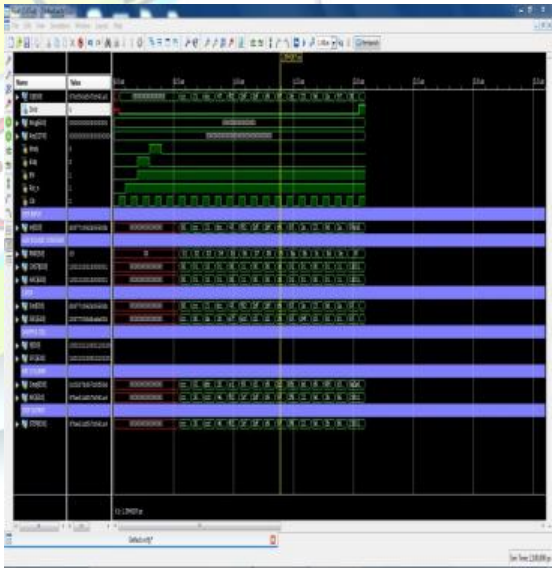

Fig 3 Output of Round Based Implementation

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 19, April 2016

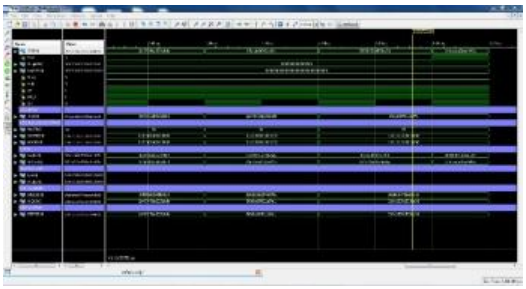

Fig 4 Output for Serial Implementation

We present the hardware architecture for round based and serial implementations of Midori. The architecture may be utilized for area efficient implementation of Midori block cipher. FPGA realization shall provide the exact area and energy requirement of the cipher.

VI.CONCLUSION

In this paper, we analyze the block cipher Midori 64, optimized with respect to energy consumption. We analyzed two type of implementation namely round based implementation and serial implementation. Thereafter we propose two design components i.e. Mix Column matrix and S-box that help us to achieve the objectives of low energy design. Round based implementation occupies high area and have low latency and high throughput. Serial implementation occupies less area and have high latency. Round Based Implementation are used for applications, where we require high throughputs and Serial Implementation are used in applications, where area is a major constraint.

ACKNOWLEDGEMENT

We used the infrastructure and laborites at SETS (Society for Electronics transaction and Security), Taramani to implement and analyze our project in an efficient way and the output was successfully obtained.

REFERENCE

[1]. Subhadeep Banik1, Andrey Bogdanov1, Takanori Isobe2, Kyoji Shibutani2,Harunaga Hiwatari2, Toru Akishita2, and Francesco Regazzoni3. Midori: A Block Cipher for Low Energy(Extended Version) 2015.

[2]. Christo Ananth, H.Anusuya Baby, “Encryption and Decryption in Complex Parallelism”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3, Issue 3, March 2014,pp 790-795

[3]. A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y.Seurin, C. Vikkelsoe. PRESENT:An Ultra-Lightweight Block Cipher. In CHES 2007, LNCS, vol. 4727, pp. 450-466.

[4]. J. Borgho_, A. Canteaut, T. G uneysu, E. B. Kavun, M. Kne_zevi_c, L. R. Knudsen,G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomsen, T.Yal_cin. PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications Extended Abstract. In Asiacrypt 2012, LNCS, vol. 7658, pages 208-225.