International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

High Speed Advanced Encryption Standard Using Pipelining

Mradul Upadhyay[1], Utsav Malviya[2]

[1]Research Scholar, Embedded System and VLSI Design GGITS, Jabalpur, Madhya Pradesh, India

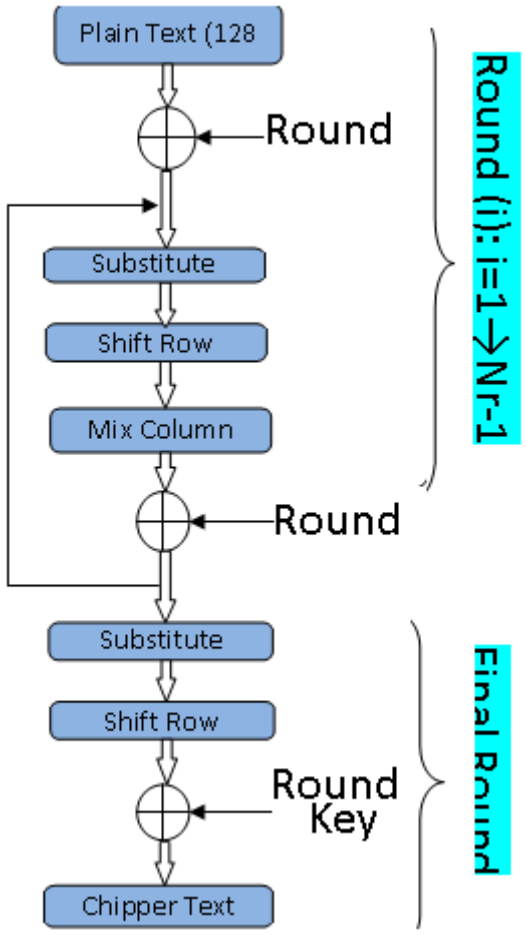
[2]Assistant Professor, Electronics & Communication, GGITS Jabalpur, Madhya Pradesh, India

Abstract: ***In this paper we have proposed high throughput by swapping the AES algorithm internal stages in this proposed work shift row is operated before sub bytes (substitution bytes) .In this proposed operation the AES encryption operation will not effect, with this process is streamlines the processes a 4 block of data rather then 16 block. The advantage of this is we can save area. This process repeats for 10 cycles and with the help of this we can encrypt 128 bits data with higher throughput. We have evaluated this performance of higher throughput and hardware area in Xilinx's 12.2 vertex 4 XC4VFX140-11FF1517.***

Keywords: Advanced Encryption Standard (AES), Register Transfer Logic (RTL), Very High Speed Integrated Circuit Hardware Description Language (VHDL), Galois field (GF), Byte Substitution (Sub Byte)

1. Introduction

Advanced Encryption Standard (AES) is used for security purpose in Military application. All Cryptographic algorithm are used for security services for various application all the encryption technique are used in government and secret military communication. The basic algorithm of AES can easily understand by the flow chart given below:



The AES used for encrypt and decrypt 128 bit plain text block. To encrypt this plain text we required 3 modes: 128 bit, 192 bit 256 bit. Each has corresponding number of round. To encrypt the data we required 128 bit matrix and each row contains four bytes of group. The 4*4 Matrix is given below.

$$X = \begin{bmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{bmatrix}$$

Figure 1: Matrix

The AES algorithm consists of four different simple operations.

- Byte substitution (Sub Bytes)
- Shift Row
- Mix column
- Add Round Key

1.1 Sub Bytes:

All bytes are processed separately and it is a non linear byte substitution. Sub byte is invertible and constructed by the composition of following two transitions;

Inversion in the GF(2^8) field and modulo an irreducible polynomial is given by:
$M(x)= x^8 + x^4 + x^3 + x + 1$

Affine transformation defines by as following:
$Y = AX^{-1} + b$
Where A is 8*8 fixed matrix and b is 8*1 vector matrix.
Shift Row**:**
In this stage

- The first row is not change.
- The second row is circular shifted by 1 byte to the left.
- The third row is circular shifted by 2 byte to the left.

- The fourth row is circular shifted by 3 byte to the left.

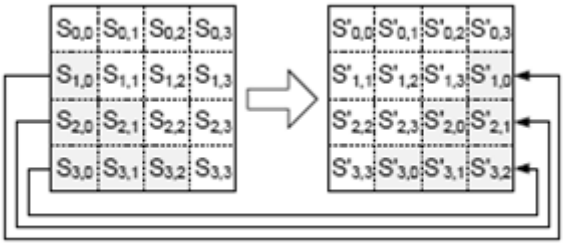


Figure 2: Shift Row

1.2 3 Mix column

The mix column transformation operates column by column and these columns will be consider as a four term polynomial. The column are consider as four term polynomial over GF(2^8) are multiplied x^4+1 with the fixed polynomial a(x) is given by:

a(x): $\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$

1.3 Add Round Key:

In this transformation the 128 bit of stage are bitwise xor with the 128 bit of the round key. The operation is viewed as a column wise operation between the 4 bytes o a state column and one word of the round key.

2. Methodology

The AES can be viewed as a encryption algorithm and in our proposed methodology we will do some changes in the basic AES algorithm and improve it's performance. The first change is we will swapping two block that is sub byte and shift row with this change the avalanche effect will improve and the second change we will perform is the introduction of pipeline in the basic AES algorithm with this change the throughput will increase and the area (slices) will reduce.

2.1 Swapping of Blocks

In the AES algorithm the blocks "sub byte" and "shift row" are swapped together but the operation of AES algorithm will not be affected when the shift row blocks is operated before the byte substitution block then the avalanche effect of the AES algorithm will be increases.

2.2 Avalanche Effect

It is the important characteristics for encryption algorithm. This property can be seen when changing ne bit in the plain text and then watching the change in the outcome of at least half of the bits in the cipher text. One purpose of the avalanche effect is that when changing in the one bit there is a large change then it is harder to perform an analysis of cipher text when trying to come up with an attack.

Consider a function F1$\{i, j\}^n$ here $\{i, j\}^n$ satisfy avalanche criteria when one input is change at least half of bit in the output bit change. Where i, j are the input and output bits. As per avalanche criteria:

Total charge in $j^{n/2}$ avalanche variable computed over whole input size 2^n in range $0 \leq w(a_j) \leq 2^n$ from the above equation we can calculate avalanche parameter of i as :

With above formula it can be proved that probability of change the output bit when only one or i^{th}bit of the input is changed is half.

1.3 Pipeline

In our design we uses the pipeline architecture of the AES pipeline stages as well as it divides the AES into ten AES pipeline stages as well as it divides the AES into ten stages yielding an overall of 110 pipeline stages then resulting speed in terms of throughput rate and implementation area is evaluated and compared with existing design implementation in terms of same gate technology factor. In our design we uses register in between every block of AES. The register is behaves like memory and used to store some data for some instant of time:

1.4 Throughput

Throughput can be calculated by using following equation:
Throughput = (Total plaintext in byte encrypted)/(Total execution time)*100

Table 1: Throughput comparison

Existing technique	*File size*	*%*
AES	50KB	70%
DES	50KB	60%
Blowfish	50KB	38%
Caesar cipher	50KB	2%
Vigenere cipher	50KB	4%
Platfair cipher	50KB	8%

3. Results

In this section we will discussed about all the result come from our proposed work. In our proposed work we will give a clock cycle for all the four blocks will operate according to the clock cycle in the input. In our proposed design the number of slices will be reduce and slices utilization percentage is also reduce. The main parameters of our results are number of slices, throughput and frequency. The result come from simulation (synthesize summary) and the RTL view of proposed design is given below.

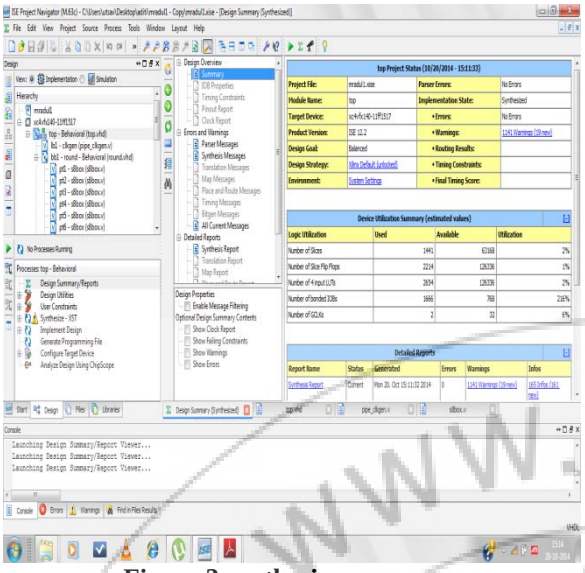


Figure 3 synthesize summary

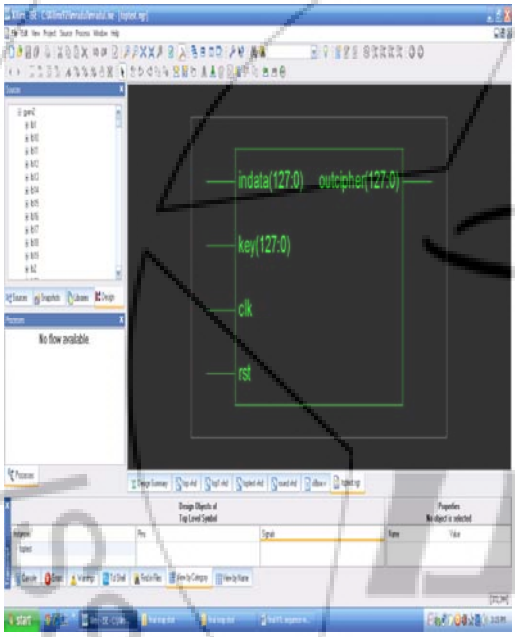


Figure 4 RTL view

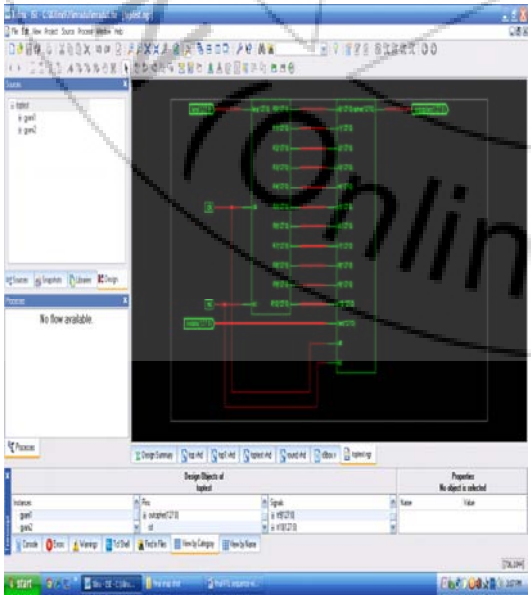


Figure 5: RTL view (Internal)

4. Result Comparison

Table 2: Comparison of the implemented design of the module with reference design

Module	*Our*	*Base paper 1*	*Base paper 2*	*Base paper 3*	*Base paper 4*
Area ((Slices)	1441	3420	1853	4720	17450
Frequency (MHz)	527.426	263.92	140.390	245	242.15
Throughput (MBPS)	1323	2815	352	2909	3090

5. Conclusion

The proposed work has implemented several modules of advanced encryption standard and the simulation done on Xilinx ISE simulator. In the proposed work pipeline is introduce into the AES method. The target device FPGA vertex 4 has been used for the validation of the proposed AES.

In the proposed work number of slices used for advanced encryption standard is reduced and the throughput is increased, in this work we have used a pipeline for all 4 stages of AES, with the help of pipeline structure the area is reduced and time taken for encryption is also reduced. We used a register in between two stages then the area (slices) is reduced and throughput is increased compare to the reference design [1]. This AES is more secured compare to previous one because in this work the combination of key is more random.

References

[1] Dr R.V. kshirsagar,M.V.Vyawahare "FPGA Implimentation of High Speed VLSI Architecture For AES Algorithm "2012 IEEE.
[2] Hassen Mestiri, Noura Benhadjyoussef, Mohsen Machhout and Rached Tourki "An FPGA Implimentation of the AES with fault detection Countermeasuer"2013 IEEE.
[3] Mr. Atul N Borkar "FPGA implementation of AES Algorithm" 2011 IEEE.
[4] Kaijie Wu, Ramesh Karri, Grigori Kuznetsov, Michael Goessel "Low Cost Concurrent Error Detection for the Advanced Encryption Standard" 2004 IEEE.
[5] Shaaban sahmoud , Wisam Elmasry , Shadi Abudalfa "Advancement the security of AES against modern attacks by using variable key block cipher " IAJET vol. 3 no 1 march 2012.
[6] Alan Kaminsky , Micheal Kurdziel , Stanislaw Radziszowski "An overview of cryptanalysis research for the AES" IEEE 2010.
[7] Ashwini M. Deshpande, Mangesh S. Deshpande and Devendra N. Kayatanavar "FPGA Implementation of AES Encryption and Decryption " IEEE June 2009.
[8] *Advanced Encryption Standard (AES)*, Nov. 26, 2001.
[9] Kris Gaj, and Pawel Chodowiec "Hardware performance of the AES finalist's survey and analysis of results", George Mason University. Proc. 3rd Advanced Encryption Standard (AES) Candidate Conference, New York, 2000:1-5.

[10] A. Elbirt "Recon_gurable Computing for Symmetric-Key Al-gorithms", Ph.D. thesis, Department of Electrical Engineering, Worcester Polytechnic Institute, 2002.
[11] Elena Trichina, and Tymur Kokishko "Secure AES Hardware Module for Resource Constrained Devices", Security in Ad-hoc and Sensor Networks. First European Workshop. ESAS 2004, Heidelberg ,Germany, August 6, 2004; (3313):215- 229.
[12] Sumio Morioka, and Akashi Satoh "An Optimized S-BOX Circuit Architecture for low power AES Design", IBM Research, Tokyo Research laboratories, CHES 2002; (2523):172-186.
[13] N. Sklavos, O. Koufopavlou, "Architectures and VLSI Implementations of the AES-Proposal Rijndael", IEEE Transactions on Computers, Vol. 51, Issue 12, pp. 1454-1459, 2002.
[14] Akashi Satoh, and Sumio Morioka "Unified Hardware Architecture for 128-Bits Block Ciphers AES and Camellia", IBM Research, Tokyo Research laboratories, CHES 2003; (2779):304-318.

Author Profile

Utsav Malviya did his AMIE in Electronics and Communication and M. Tech (Gold Medalist) from DAVV, Indore. Currently, he is working as Asst. Prof. in GGITS, Jabalpur. His area of interest includes Embedded Systems, Microcontroller, microprocessors, MATLAB and Verilog.

Mradul Upadhyay is Research Scholar in Embedded System and VLSI Design, GGITS, Jabalpur, and did BE from GGCT, Jabalpur.