International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 24 (2017) pp. 14148-14153

Designing a High-End Cryptographic Engine for Multi-Core Processor Arrays of FPGA

S.Neelima
Research Scholar, Department of Electronics and Communication Engineering,
Avinashilingam institute for home science and higher education for woman,
Faculty of Engineering, Coimbatore-641103, Tamil Nadu, India.
Orcid id:0000-0001-6466-9987

Dr R.Brindha
Professor in Electronics and Communication Engineering,
Avinashilingam institute for home science and higher education for woman,
Faculty of Engineering, Coimbatore-641103, Tamil Nadu, India.

Abstract

Now, the number of homeowners and speakers has increased the security requirements to cover the transfer of user data outside the channel. Critical cryptographic algorithms are fundamental to overall security. In December 2001, the American Institute for Standards and Technology (NIST) Rajndel developed an adaptive encryption standard (AES) algorithm to comply with the Data Encryption Standard (DES). AES can check current registration standards. The AES algorithm is a block that can encode and decode digital information. Here we are concentrating on how to optimize system position over time and how to get 5.751Gbps and a small area. The plan has been developed on Zynq devices (xc7z020-2clg484) and tested on Zedboard. According to another AES analyser, this strategy is three times higher than most other systems. To hide or delete files with an AES algorithm, the file must start a complex configuration process. As a result, the software for your AES algorithm is fast and time consuming. The increase in stored and imported data in recent years has caused this issue more seriously when it is important to hide / copy the data.

Keywords: AES Encryption

INTRODUCTION

The synthesis is mysterious and mysterious. The information obtained must be maintained and protected against attacks. Analysis is a method of copying text into encrypted text to get data against hackers. A system configuration for decryption. Cryptographic encryption algorithms for storage and banking, Personal Network, Enterprise and many others. Then you need to save the information about the problem. The algorithm defines an important role in the security system. One of the most important channels for the encryption system depends on the nature of the input data that are classified as a stream block and encryption stream.Sharing is an algorithm that is used secretly. Blocked lock is an encryption algorithm derived from data in action. The text is divided into numerical blocks, and each processing process begins each time. Algorithms that work with the share that works on the data stream and works a bit.The known standard of data-encoding (DES) is the known cryptographic algorithm. The encryption algorithm (Des) was the first block of the NIST (National Institute of Standards and Technology), which was approved in 1974. A weak encryption of default damage data (DES) for different counter attacks is dangerous. In 2001, NIST recommended the Rijndael encryption algorithm as a general standard (AES) [1] to replace the encrypted data standard (Des) [2].

SURVEY ON CRYPTOGRAPHY SCHEMES.

The Advanced Encryption Standard Encryption Algorithm (AES) can process data block decoding. The AES (Quality Encryption Software) algorithm is a short and long-term configuration process. For example, a high-quality encryption algorithm (AES) can be used to customize the hardware: application description (ASIC) and target products (FPGA). FPGAs prevent such a thing more efficiently than ASIC while repairing. Many software packages are installed on the AES (High Quality Standard Software) software. However, the material orientation can be flexible, flexible and flexible. This book presents three different types of high-quality high-density encryption standards and small similarities, pipelines and graphic designs.

The Advanced Encryption Standard (AES) defines the Rijndael algorithm and is a symmetrically locked digit. It manages 128-bit data blocks with different key lengths of 128, 192 and 256 bits. The round number is determined by the size of the key (128 192 256 bits). The comprehensive encryption standard consists of four different steps, which are repeated in the number of revolutions. These four steps are byte substitution, low line, mixed column and key addition. When using a 128 bit size, the number of revolutions of the repeated algorithm (No) is ten. The following table shows the required

length and key revolutions for the corresponding key length. In this document, the key size used is 128 and the

Table I. A Long Key

Key Size(bits)	No.of Rounds
128	10
192	12
256	14

The AES algorithm processes 128 bits and provides 128-bit password output. Figure 1 shows the different phases of AES encryption and decoding. As shown in the Figure , decryption is the reverse process of encryption. The key of the final round is applied to the first round of the decryption process. The password keys used are in the order of 128, 192 and 256 bits. One-byte process algorithm, 8-bit order. In the AES algorithm, all byte values are displayed as a combination of individual bit values in brackets such as {b7, b6, b5, b4, b3, b2, b1, b0}.

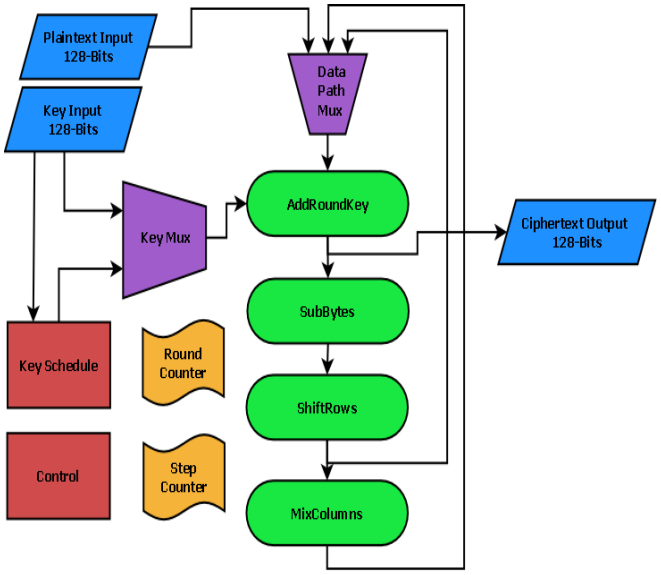

Figure 1: Block of encryption and decryption AES.

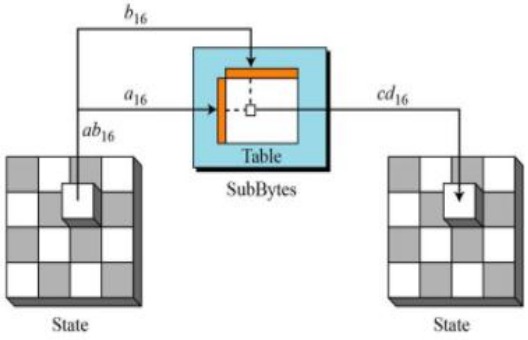

Figure 2: Transformation of Sub Byte.

By using polynomial representations, these bytes are displayed as finite field elements. AES operates with a 128-bit data block that is regulated in the form of a state flag, denoted by 4 bytes with 2 bytes. The four basic data formations for data encryption are:

A. SubByte

SubByte transformation is a replacement of nonlinear bytes. Each byte of the state is replaced by another byte of a replacement box called S-Box. The S-Box operation consists of a multiplicative and then a affine transformation. The affine transformation consists of a matrix multiplication, followed by the addition of vectors. Figure 2 shows the transformation in bytes.

1) Inverse SubByte: In the inverse SubByte, the inverse S-box is applied to each status byte. This can be done by applying inverse secondary bytes.

B. ShiftRows

In the ShiftRows transformation; The first line of a country remains unchanged. Then, the second, third and fourth rows are cyclically shifted to the left by one, two and three bytes, as shown in Figure

1) Reverse ShiftRows: The first line of the country remains unchanged. The second line is exactly a byte cycled. The second and third lines are shifted to two and three bytes, respectively.

C. MixColumns

The MixColumns transformation is a linear operation, with each column being processed independently. Each column is considered a polynomial and then multiplied by a fixed polynomial module (see Figure 4). The step of MixColumns does not exist in the final phase of the AES algorithm.

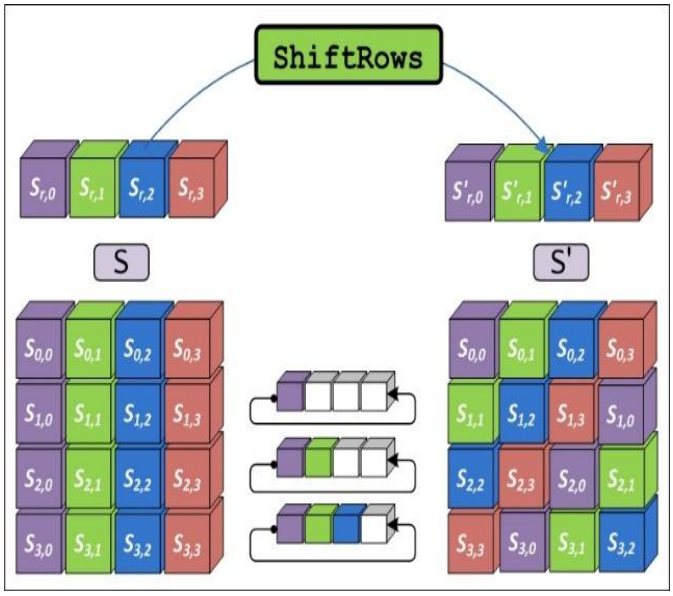

Figure 3: Turn the offset lines.

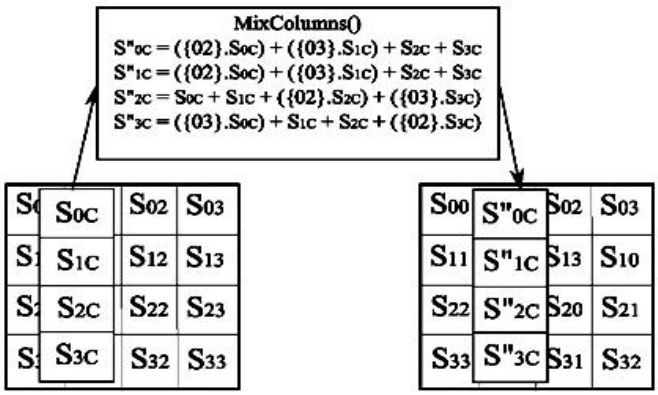

Figure 4: MixColumns Transformation.

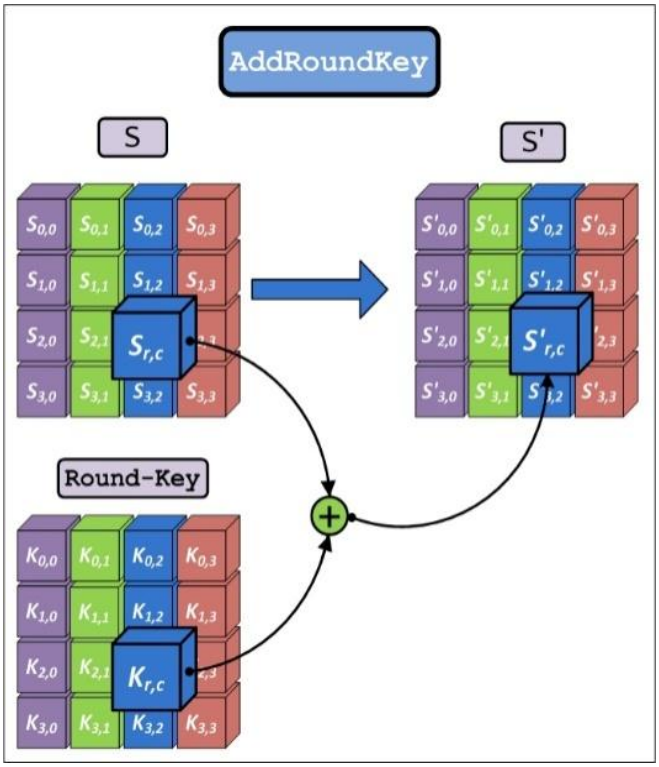

Figure 5: AddRoundKey transformation.

1. Reverse MixColumns: In reverse columns, each column is processed independently. Each column is considered a polynomial and then multiplied by a fixed polynomial (x).

$$p(x) = \{0p\}\,x_3 + \{0q\}\,x_5 + \{0\partial\}\,x + \{0\sigma\} \qquad (1)$$

D. AddRoundKey

AddRoundKey performs each status bite independently. The AddRoundKey input is a 16 byte state and a current 16 byte key. A 16-byte key is obtained by a key expansion process. The country was added to the round button with the exclusive bitwise operation (XOR). Figure 5 shows the transformation of an additional key.

E. KeyScheduling

The AES algorithm uses three keys with 128, 192 and 256 bits. Depending on the chosen key, the number of turns is determined as shown in the table.

There are three phases in each phase of the planning:

1. KeyRotWord: KeyRotWord accepts four-byte input words [b3, b2, b1, b0] and performs cyclic mimics. After performing cyclic permutation, the function returns the word [b2, b1, b0, b3].
2. KeySubWord: Performs operations for each column byte. It requires four bytes input words and is then processed in each byte. Each byte is replaced by another byte with the S-Box.
3. KeyXOR: The Rcon KeyXOR feature uses a continuous word organization. In the KeyXOR function, XOR operations are performed between the first words of the previous keyword, the words obtained from KeySubWord and the first word of the fixed rotary converter.

During the decryption process, since AES is a symmetry system, it means that the same key is used for the encryption and decryption process. that is, the keys are counted in the last round of the first decryption round. Next, the same process is repeated so that the ninth round of the encryption process is applied to the second decryption process. This has been decrypted and eventually the original content has been found.

PROPOSED METHODOLOGY

This section describes AES encryption and decoding machines that are parallel, parallel and sequential, maintaining the areas and transmission times on the individual hardware.

A. Intelligent architecture, pipelines and designs

Three different advanced encryption standard (AES) functions are calculated in parallel, pipeline and sequential architecture. This architecture is an integrated architecture gateway (FPGA) architecture. FPGA can work in parallel. These are logical blocks separated by newly conFigure d connections. The main advantage of the AES hardware application is its adaptability. Per program, if FPGA matches. Redeployment. This adaptability has complicated the complicated application of complications. In general, the hardware is defined in the processor. According to the design of the processor, the hardware is dedicated and cannot be reconFigure d. In addition, the processor is sequential. If such an algorithm is required to calculate large calculations on the processor, processing time will be very slow and time will continue to decrease. In this proposed system, three different AES applications are recommended to run the power three times. This process is carried out in parallel, in the pipeline and in

succession. The combined processes resulting from encryption and defragmentation are performed in parallel, the data is encrypted and decoded. IT is another task of the AES algorithm, such as SubByte, ShiftRows transformation, and so on.

If you make a roundabout in this document, the measurement will be performed simultaneously. Now, a compound transfer and XORing are the circular details of the most important addition. The mixed column phase consists of a series of XORs to change the data elements in each column. The velocity of the tube was very effective.

The process shows processes that are individually processed. Also in this process in the order. In an activity, the AES algorithm such as SubByte, ShiftRows, and so on. Each operation is processed one by one, with each brochure being processed on the other hand. All these operations are performed on a single hardware device. The speed is the time the algorithm needs. The ratio is defined as, T = No at the same time X Maximum operating frequency. The importance of the maximum operating frequency is that the design can work efficiently depending on the operating frequency. If the bit rate is high, the number of fixed bits is much shorter. The performance is greater, the design is more efficient and therefore the highest. The area needs to be improved to increase the periods. This increases the capacity and increases the energy consumption. The FPGA says that the project is efficient, depending on the use of its resources. Therefore, the drawing must maintain trade between the area and the river.

The FPGA consists of slice, LUT, flip-flop, BRAM and DSP48 programs. To replace all sizes, you need S-boxes. S-Boxes can be stored in BRAM. FPGA has 1K (1024 x 18) BRAM. Depending on how the S-Box is stored, there are three different techniques that allow the area to be designed and effectively planned.

Table II: Trade Relationship

Output	S-Box stored in ROM
16 Clock	1
4 Clock	4
1 Clock	16

The number of clock cycles depends on the ROM usage, as shown in Table II. First, an S-box table is stored in the ROM and therefore requires a clock cycle for each action in each clock cycle. The system is efficient, but performance is low because productivity decreases. In the second case, four S-boxes are stored in the ROM and one column is needed in each column.For example, each column needs hours to access the ROM. Four bytes are divided into a column in a clock cycle. So here is the pillar of the wisdom act. It's an effective field, but reduces speed when one column becomes an hour. Third, the number 16 indicates that there are S boxes in ROM 18. It's time to delete 16-bit data blocks from a single clock cycle. Here the system is fast and improves performance significantly. In addition, the field is effectively selected by selecting the BRAM merge options for the xilinx14.3 property.It is very important to maintain trade between the region and its achievements. The design should no longer use areas. If you use multiple zones, power consumption increases and system performance decreases.As a result, the proposed system indicates that the third digit is more effective than the first two because it protects regions and performance. The current can be calculated using formula 2.

Value = Number of bits per hour * Maximum operating frequency (2)

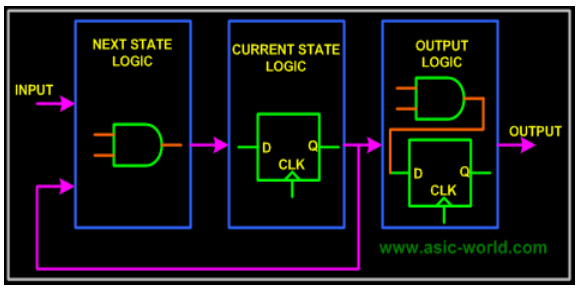

Figure 6: FSM encoding

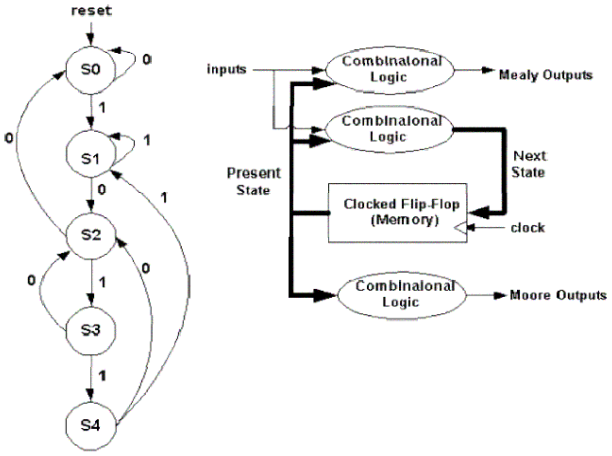

Figure 7: FSM Decryption

C. Advanced AES database

In the AES algorithm, the card is independent of the data. In this section, State Machine Technology (FSM) was used for encryption and decryption. 6 shows the minimum emergency firewall FSM algorithm, and Figure 7 shows the FSM dehydration algorithm.

D. FSM encryption

The data will not be processed during reset. If rst = 0, the system enters standby mode. By deleting the saved data in the

file, RAM when the new processing has started.The system is always in sleep mode until data "1" has been delivered. When "1" comes in the data transfer, it is said that a 16-page package is ready for encryption. This FSM diagram for an encryption module. There are also three encryption units in the encryption process. The 16 bit bits require 16 clock cycles. The first case s-1 shows the first round because the original X-ORed data is uploaded to the s-box. Thereafter, the exit sphere is obtained for each revolution of the box. Thus, the algorithm comes after the first round in the second case s-2 when 8 rounds are completed, and finally the last s3 is correct, that is. 10 ° around. At the end of 10 comments, the high-speed encryption indicates that the 16-byte data blocks are blocked. Due to the 128-bit kernel size, 10 full rotations are performed.For example, every 10 hours. a rotation in a clock cycle. Then you need 10 cycles in 10 cycles. Then it's too late and it will be over. At the same time, data block 16 makes further measurements that require 16 hours of transmission, one cycle per single cycle. When 10 rounds are completed, a total of 10 bytes are allowed. This is called hydraulic system.

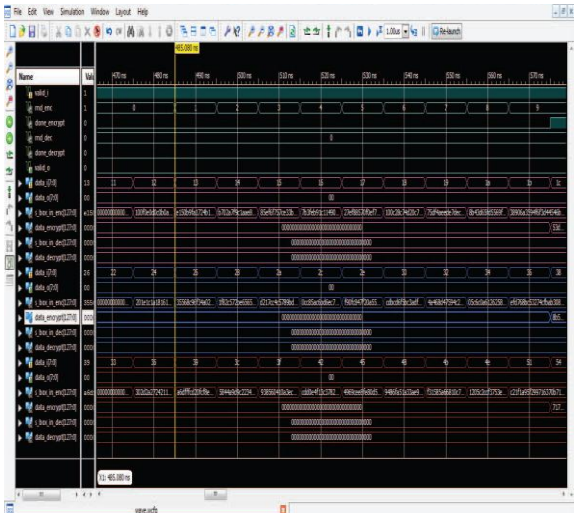

Figure 8: Encryption axes

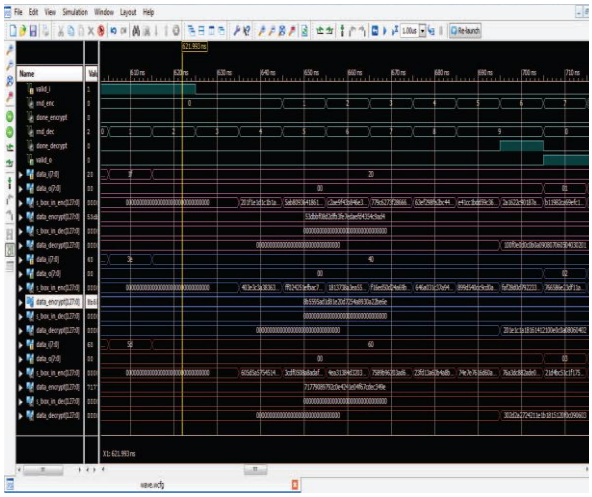

Figure 9: Descending waveform

FSM must stay 6 hours with a 6-byte ring. After resetting, encryption for the next set starts with other data. Until then, the group was already discriminated against. Now the next special encryption begins at the same time as the previous batch decryption. This is given in parallel. A transformation begins after another. Finally, the FPGA works in parallel and online.

E. Decoding of FSMs

The reset and rest states are identical to those of the FSM encryption. If the algorithm is in hibernation mode, it can not specify_ done encrypt = 1. In this case, the first encryption triggers are the first round of the last encryption round. The algorithm goes to position s2 when in the last round the situation s-3 is rounded to 8 and ends, indicating that the decryption is complete. This decoding signal is high. And yet the algorithm goes into an idle state awaiting new future data.

EXPERIMENTAL ANALYSIS

This section describes the value of this process. Displays the encryption and decryption process, as shown in Figure 8. Figure 9 different types are used for different variants. 24 bits are collected and divided into one third of the 8 bits. Now the 8-bit tariff has been added to the key. Once the key is accepted, all data is currently synced. Therefore, each zone begins to collect data. The decoding process of the third part is shown in FIG9. The AES program collected each module for Modulo 8 manipulation numbers and lost 24 bits at a time and one clock. The summary report shows the most effective moment of table 2.

$$T= 239.648 * 24 = 5.751 \text{ Gbps} \text{ ----Eq 2}$$

Table 2: Utilization Summary of Resourses.

Resource utilization	Single AES[13]	FSM(Three AES)
Number of Slice Register	1658	2008
Number of fully used LUT flip-flops pairs	4360	1394
Maximum operating Frequency	165.462MHz	239.648MHz
Throughput	882.464Mbps	5.751Gbps

CONCLUSION

This paper uses 11 keys to perform three versatile AES initiatives, and the details are 16 hours and a half clock, that is, an hour's turn. The FSM system was very effective in the region and in the hand. This makes the belt's time or execution a good management of the belt. FPGA is fully implemented as a tool and system. With AES, Zynq (xc7z020-2clg484) device

runs a 5.751Gbps and focused on small area. This makes the plan more efficient and expensive. If the design can be more complex in the future and the key can be modified to improve security.

REFERENCES

[1] National Institute of Standards and Technology, "Specification for the Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication 197, November 26, 2001.

[2] National Institute of Standards and Technology, "Specification for the Data Encryption Standard (AES)", Federal InformationProcessing Standards Publication 197, November 26, 2001

[3] A.Hodjat and I.Verbauwhede, "Area-Throughput Trade-Offs for Fully Pipelined 30 to 70 Gbits/s AES Processors, "IEEE Trans.Computers, vol. 55, no.4, pp.366-372,Apr.2006.

[4] Bin Liu, Bevan M. Baas, "Parallel AES Encryption Engines for Many- Core Processor Arrays" IEEE Trans.on computer vol. 62, no. 3, March2013.

[5] L.Verbauwhede, P. Schaumont, and H. Kuo, "Design and Performance testing of a 2.29 Gb/s Rijndael Processor," IEEE J.Solid-State Circuits (JSSC), Mar.2003.

[6] D. Bernstein and P. Schwabe, "New AES Software Speed Records," Progress in Cryptology, pp. 322-336, 2008.

[7] S.Gueron, "Intel Advanced Encryption Standard (AES) Instructions Set," Jan.2010.

[8] M. Matsui and J. Nakajima, "On the Power of Bitslice Implementation on Intel Core 2 Processor," Proc. Cryptographic Hardware and Embedded 6\VWHPV, SS. 121-134, 2007.

[9] RezaRezaeianFarashshi, BahramRashidi, SayedMasoudSayedi, "FPGA based fast and high-throughput 2-slow retiming 128-bit AES encryption algorithm" Science Direct, Microelectronics Journal 2014.

[10] Hodjat and I. Verbauwhede, "A 21.54 gbits/s FullyPipelined AES Processor on FPGA," Proc. IEEE 12th Ann.Symp. Field-Programmable Custom Computing Machines, pp. 308-309, Apr. 2004.

[11] "Int'l Technology Roadmap for Semiconductors, Design," http://www.itrs.net/Links/2009ITRS/2009Chapters_2009Tables/2009_D esign.pdf, 2009.

[12] C.-J. Chang, C.-W. Huang, K.-H. Chang, Y.-C. Chen, and C.-C.Hsieh, "High Throughput 32-Bit AES Implementation in FPGA,"Proc. IEEE Asia Pacific Conf. Circuits and Systems, pp. 1806-1809, Nov. 2008.

[13] Manoj.B, Manjula N Harihar, "Image Encryption and Decryption using AES", International Journal of Engineeringand Advanced Technology, ISSN: 2249-8958, vol.1, issue-5, June 2012.