Cent. Eur. J. Comp. Sci. • 3(4) • 2013 • 173-186
DOI: 10.2478/s13537-013-0112-2

VERSITA

Central European Journal of **Computer Science**

PSP: Parallel sub-pipelined architecture for high throughput AES on FPGA and ASIC

Research Article

K. Rahimunnisa[1*], P. Karthigaikumar[2†], N. Anitha Christy[1], S. Suresh Kumar[3], J. Jayakumar[4]

1 *Karunya University,*
Department of Electronics and Communication Engineering, Coimbatore 641 114, India

2 *Karpagam College of Engineering,*
Department of Electronics and Communication Engineering, Coimbatore 641 032, India

3 *Dr. NGP Inst. of Technology,*
Department of Electrical and Electronics Engineering, Coimbatore 641 048, India

4 *Karunya University,*
Department of Electrical and Electronics Engineering, Coimbatore 641 114, India

Received 07 August 2013; accepted 17 November 2013

Abstract: As the technology is growing day by day, information security plays a very important role in our lives. In order to protect the information, several cryptographic algorithms have been proposed. The aim of this paper is to present an effective Advanced Encryption Standard (AES) architecture to achieve high throughput for security applications. The Parallel Sub-Pipelined architecture (PSP) is proposed in order to obtain high throughput. The proposed architecture is also compared with loop unrolled, pipelined, sub-pipelined, parallel and parallel pipelined architecture in terms of throughput. The AES algorithm using Parallel Sub-Pipelined architecture was prototyped in FPGA (Field Programmable Gate Array) and ASIC (Application Specific Integrated Circuit).The proposed architecture yielded a throughput of 59.59 Gbps at a frequency of 450.045 MHz on FPGA Virtex XC6VLX75T which is higher than the throughput yielded in other architectures. In ASIC 0.13 μm technology, the proposed architecture yielded a throughput of 25.60 Gbps and in 0.18 μm, it yielded a throughput of 20.56 Gbps.

Keywords: cryptography • AES • FPGA • ASIC • parallel sub-pipelined • throughput

1. Introduction

The increase in the use of computer and communication system for data and money transfer has increased the risk of theft of information. Hence, there is a need for fast and secure digital communication networks to achieve secrecy and integrity of information. Cryptography provides different algorithms for securing and authenticating the transmission of

* *E-mail: krahimunnisa@gmail.com*
† *E-mail: p.karthigaikumar@gmail.com (Corresponding author)*

information over insecure channels. There are several crypto algorithms for protecting the user information. Some of the symmetric key algorithms (same key for encryption and decryption) are Blowfish, DES, Triple DES, AES, SAFER, IDEA, RC4, etc. In the year 2001, National Institute of Standards and Technology (NIST) [1] announced that the Rijndael algorithm is the winner of the competition to replace Data Encryption Standard (DES). AES is a symmetric key algorithm which was developed by Dr. Joan Daemen and Dr. Vincent Rijmen. This algorithm has input data of length 128 bits and the key can be of length 128/192/256 bits. The hardware implementation of AES algorithm is more advantageous than the software implementation. The hardware implementation [2] provides a higher throughput and security than the software implementation of cryptographic algorithms. Hence, in this paper, hardware implementation of AES algorithm is performed in the FPGA and ASIC. FPGA combines the flexibility and ease of upgrade, which characterize the software implementations with improved physical security. An ASIC is a customised integrated circuit. A single tiny ASIC [3] can be designed to undertake specific functions which can replace a large number of individual electronic components and hence reduce the production cost for the total product. This paves the way to have several advantages like reducing system costs, big savings on space, big reductions in power consumption, big savings on assembly and testing costs and better control of electrical parameters This paper is structured as follows. Section 2 reviews the Basic AES Encryption/Decryption algorithm which involves the various steps in the AES algorithm along with the possible attacks. Section 3 gives the relevant works of various authors reported in the literature. Section 4 briefly describes the proposed Parallel Sub-Pipelined architecture of the AES algorithm. The implementation results are discussed in Section 5. The conclusion and the future work are stated in the last section.

2. AES algorithm

The need for highly secure algorithms is very essential for data transfer operations in applications like e-commerce. Advanced Encryption Standard algorithm is approved by FIPS as the standard algorithm. Though many attacks are being done on this algorithm to crack the key or plain text, these efforts have been proved futile. The following section gives a brief introduction on types of attacks on AES and their outcome.

2.1. Cryptanalysis of AES algorithm

According to [4], potential cryptanalysis performed on AES was not fruitful in retrieving the key or the plain text. The authors in [1] prove that differential cryptanalysis and linear cryptanalysis performed on AES will not be able to break and proves to be more secure. In algebraic attacks the system is expressed as a multivariate polynomial equations which can be solved to find the key [5]. The eXtended Linearization (XL) algorithm [6] and the eXtended Sparse Linearization (XSL) algorithm [7] were aimed at solving the systems of equations obtained through cryptanalysis. But the number of equations with thousands of unknown variables makes these less feasible for computing the key. In side channel attacks the variations in observable parameters are noted and cryptanalysis is done on these parameters. Only timing attacks are non invasive, all other side channel attacks like power analysis attack, fault injection attack, electromagnetic radiation are invasive. The probabilities of these attacks are normally less because of the requirement of precise measuring equipments and the requirement of encrypting device itself. Also there are many countermeasures available to overcome these side channel attacks, like increasing latency, masking of data, shuffling of data after every access etc. Though Related key attack [8] was able to crack few rounds of AES 192 and AES 256, a complete attack to break the AES 128 and retrieving its key has not been possible as of now. These results don't provide a promising cryptanalysis to break the AES-128 algorithm hence we believe that AES-128 algorithm is quite promising indeed.

2.2. AES encryption/decryption

The design of AES in this paper is based on Substitution Permutation Network [9], which takes a block of 128 bit plain text and 128 bit key as input to the encryption part and they are placed in a state array. There are four different

[1] *J. Daemen, V. Rijmen, AES Proposal: Rijndael, Version 2, http://www.esat.kuleuven..ac.be/vijmen/rijndael, 1999*

steps namely Add round key, Substitute Bytes, Mix Column and Shift Rows as shown in the Fig. 1. These four steps are iterated ten times for a 128 bit key AES and in the last round the Mix column operation is eliminated. Initially, Add round key round will be performed between the 128 bit input data and 128 bit input key, which is nothing but EX-OR(Exclusive OR) of Plain text and Round Key input and then the resulting data will be processed in the following steps as shown in Fig. 1.

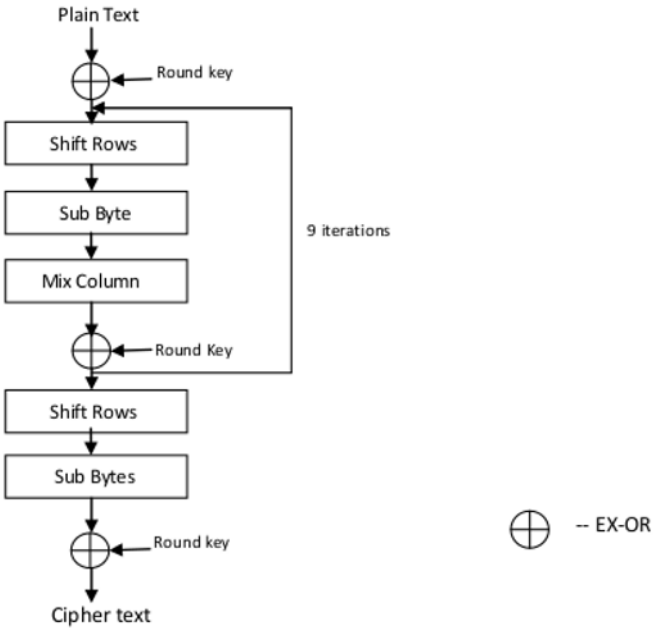

Figure 1. Encryption part of AES algorithm.

The result of the Add Round Key [10] is placed in the State array. The State array consists of a 4 x 4 array in which 8 bits of the result are occupied in each location. Sub Byte round will substitute bits from the S-box by matching the rows and columns of a predefined SBox. Mix Column will multiply the column with a fixed predefined polynomial [11]. Shift Row will shift the row to the left cyclically based on row number. The output of the Encryption part of the AES algorithm is the Cipher text, which is sent as input to the decryption part of the AES algorithm. Similarly, the decryption of the AES algorithm consists of Add Round Key, Inverse Substitute Byte, Inverse Mix column and Inverse Shift Rows as shown in the Fig. 2. In the decryption process, the cipher text is sent as input and plain text is obtained as output which is the initial input data [12].

3. Related work

The implementation of the cryptographic algorithm in hardware has been carried out for the past few years. Several architectures have been proposed to implement the AES algorithm by different authors. In the paper [13], Chi-Jeng Chang presents a 32 bit AES implementation with a low area of 156 slices and a throughput of 876 Mbps in FPGA Virtex 2P (XC2VP2) device. Loop Unrolled Architecture is used in this implementation and Sub-Byte/Mix Column is performed by Look Up Table, followed by combinational circuit XOR's. Chih-Peng Fan [14] proposed a sequential and fully pipelined AES realization using Xilinx ISE 7.1 synthesizer and uses an efficient Add Round Key architecture for real time key generations. In sequential AES design, the throughput of 0.876 Gbps is achieved with an operational frequency of 75.3MHz and in the Pipelined AES design, throughput of 28.4 Gbps is achieved with an operational frequency of 222 MHz. Issam Hammad [15] proposed architecture for high speed AES encryptor using composite field arithmetic. This architecture has multistage sub-pipelined architecture that allows a high throughput. This architecture achieves a throughput of 39.053 Gbps for 9 Pipelining stages with an operational frequency of 305.1 MHz. This design

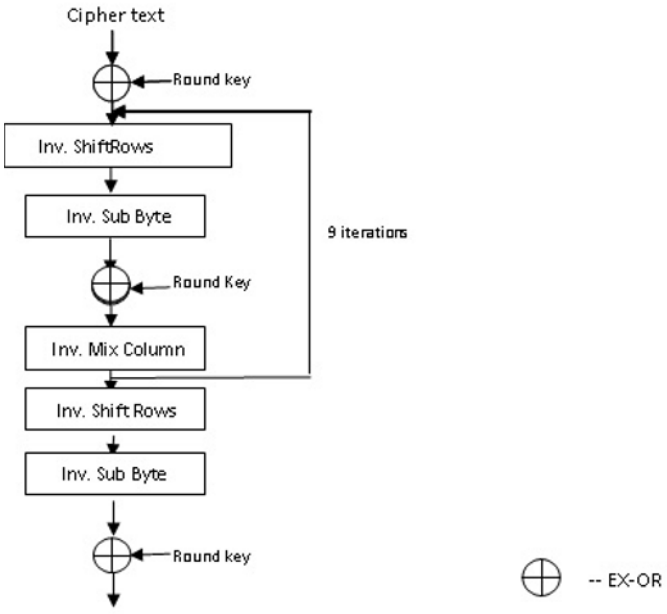

Figure 2. Decryption part of AES algorithm.

also achieves a throughput of 27.94 Gbps on Xilinx Virtex 2 device with an operational frequency of 218.3 MHz. Alireza Hodjat [16] describes a fully pipelined AES Encryption Processor on a single chip FPGA. This architecture utilises loop unrolling, inner round and outer round Pipelining techniques and achieves a throughput of 21.54 Gbps on Xilinx Virtex 2 Pro device. This design occupies 84 Block RAM's, 5177 slices with a latency of 31 cycles and the throughput per area rate is 4.2 Mbps/slice. Ingrid Verbauwhede [17] implemented a fully pipelined architecture of AES processor in 0.18 μm technology and achieved a throughput of 30 Gbps. By pipelining the composite field implementation of the byte substitution phase of the AES algorithm, the area consumption is reduced up to 35 percent. By designing an offline Key scheduling unit for the AES algorithm, the area has been further reduced by 28 percent, which results in a total reduction of 48 percent without any change in throughput. Sumanth Kumar Reddy [18] implemented an AES crypto processor for higher throughput. The processor uses a combinational logic for inner round Pipelining. Furthermore, this algorithm uses composite field arithmetic in obtaining less area and implemented a fully sub pipelined encryptor/decryptor with 3 sub stage pipelining in each round. The architecture achieves a throughput of 25.89 Gbps on Xilinx Virtex 5 device and reported that this throughput is 48.78% more effective than the previous FPGA implementations. The Algorithm is implemented in ASIC 90 nm and 0.18 μm technology, wherein the algorithm achieved a throughput of 58.18 Gbps and 30.47 Gbps respectively. E.J. Swankoski [19] proposed a parallel architecture in which internal hardware functionality is reused without duplicating. This provides a reasonably compact single block, which is ideal for duplication. This allowed multiple users to share the same hardware, as spatial isolation is achieved by the physical separation of individual encryption blocks. This algorithm achieved a throughput of 18.80 Gbps and occupies an area of 23979 slices in Virtex 2 pro FPGA device with 10 parallel blocks. Xinmiao Zhang [20] presents novel high speed architectures for the hardware implementation of the AES algorithm. In this paper, composite field arithmetic is employed to reduce the area requirements and different implementations for the inversion in subfield GF (24) are compared. The author implemented a fully Sub Pipelined encryptor with 7 sub stages in each round and achieved a throughput of 21.56 Gbps on Xilinx XCV1000 device.

4. Proposed PSP architecture for high throughput

In this work a new architecture to implement AES in FPGA and ASIC, with high throughput is presented. The proposed architecture shown in the Fig. 3 combines the Parallel, Pipelined and Sub-Pipelined architecture to achieve high throughput. The Parallel Sub-Pipelined architecture has the advantage of both the Parallel and Sub-Pipelining architecture. In this architecture, the 128 bit input data is split into four blocks of 32 bits each and is processed parallelly as shown in Fig. 3.

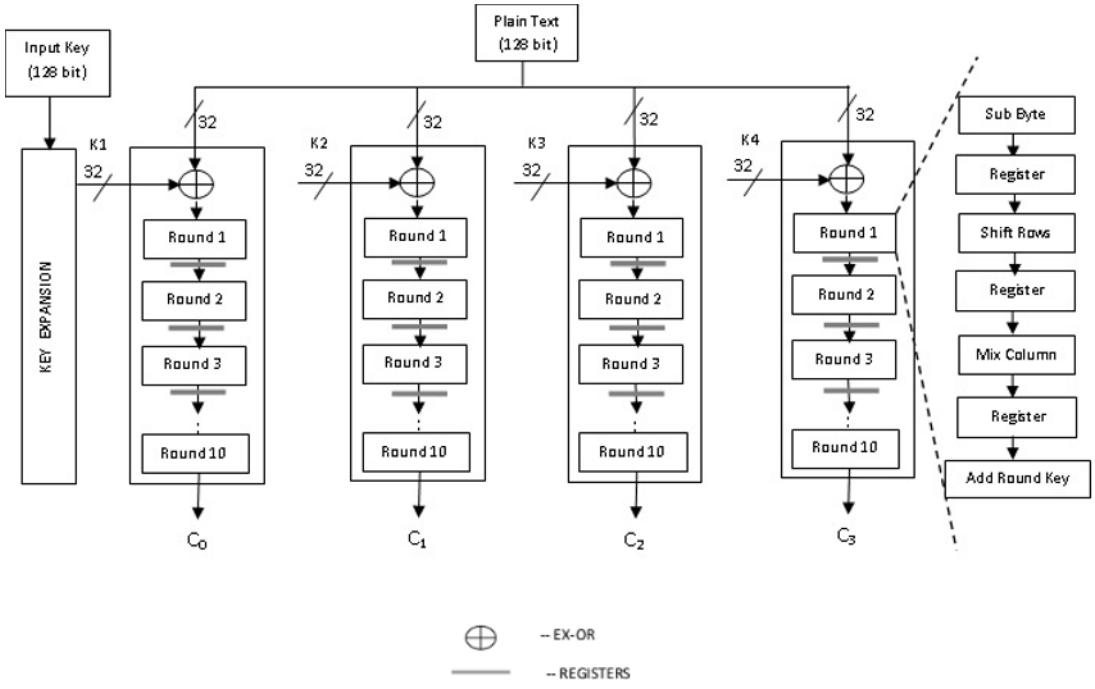

Figure 3. Parallel sub-pipelined architecture.

Registers are inserted to store the intermediate values and they act as a buffer as they can be used for further processing in the processing element. The 32-bit data is processed in four individual processing elements and is sent through the subsequent stages. In this architecture, none of the hardware components remain idle, which overcomes the drawback of the Loop Unrolled Architecture. In the Loop Unrolled architecture, one input data is processed at a time and it consumes more time to process and the speed is relatively low. But, in the proposed architecture, more input data can be processed by means of Pipelining and Parallel concept which overcomes the above disadvantages. In the Parallel Sub-Pipelined architecture, the 128 bit input is divided into four 32 bits and is sent through four set of parallel blocks initially and is processed separately in hardware components. The input 128 bit key is sent to the Key Scheduling module and different keys are generated for ten rounds. The different keys are generated by sending the key generated from the current round as input to the next key scheduling unit as shown in Fig. 4. The keys K1, K2, K3, K4 are the 32 bit data to the Initial Add round key round.

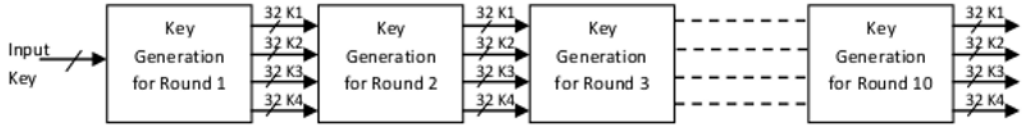

Figure 4. Key generation round.

The input 128 bit key is sent to the key generation unit and it generates another 128 bit key which is divided into four 32 bits and used for processing the first round data in the PSP structure. The key generated in round 1 is then sent to the key generation unit for round 2. Similarly the key generation is done for 10 rounds. For the first clock, the four 32 bits are sent into the four parallel blocks and round 1 is processed. For the next clock, the output bits from the round 1 are sent into the next round and a new set of inputs will arrive at the four set of input parallel blocks. Hence, more inputs can be processed at the same time. This architecture will be very efficient in terms of throughput and it can be used in many crucial/critical applications such as Ethernet, Hard disk and in Military services. The detailed structure and operation of different architectures involved in the proposed architecture are explained in the following subsection.

4.1. Pipelined architecture

In the Pipelined architecture [21], registers are inserted in between each round as shown in Fig. 5.

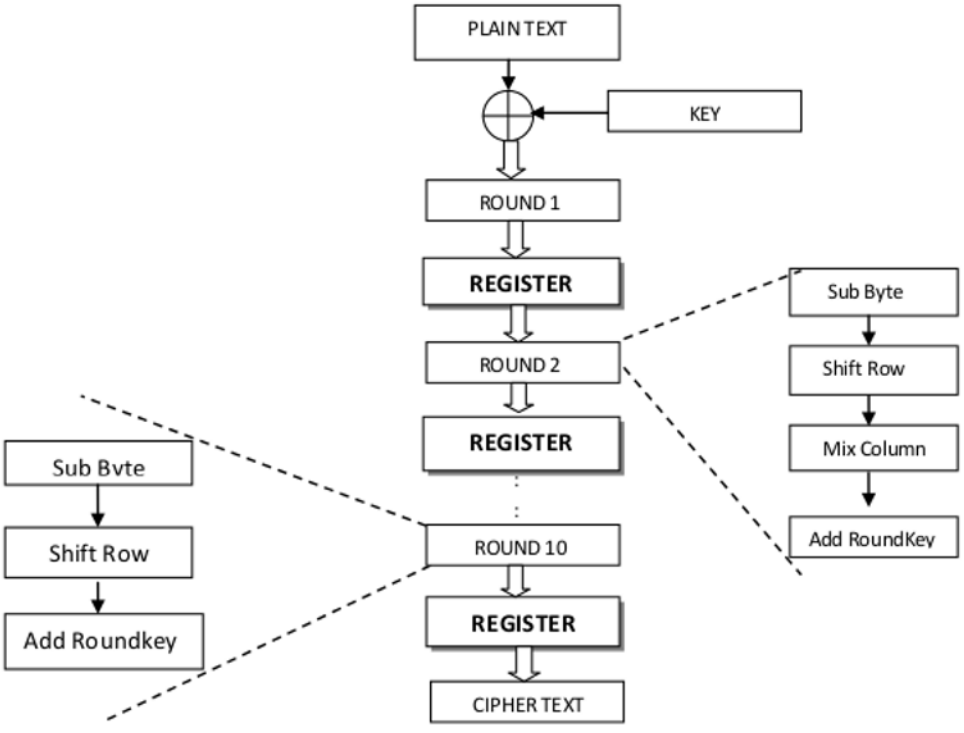

Figure 5. Pipelined architecture

The registers are used to store the intermediate values after each round. A round comprises of Substitute Bytes, Shift Rows, Mix Column and Add Round Key. When clock is equal to '1', the input will enter into the round 1 and for the next clock, the output of the first round is stored in the register and at the same time, the next input enters into the round 1.Hence, at a time more than one input can be processed. Here, the throughput achieved is 10% more than that of the Loop Unrolled architecture. In the Loop Unrolled architecture, the same hardware resources are used for n iterations, where n is the number of rounds; whereas in the Pipelined architecture, individual hardware resources are used for each round. The delay between the input data is reduced in Pipelined architecture. The throughput and area of the Pipelined architecture is higher than the Loop Unrolled architecture. In order to increase the throughput further, Sub-Pipelined architecture is used.

4.2. Sub-pipelined architecture

In the Sub-Pipelined architecture [22], the registers are inserted in both inter and the intra rounds. Hence, more than one input can be processed at a time. The registers are placed in between the rounds and inside the rounds in order to store the intermediate results. The registers are placed in between Sub Byte, Shift Rows, Mix Column and Add Round Key as shown in Fig. 6.

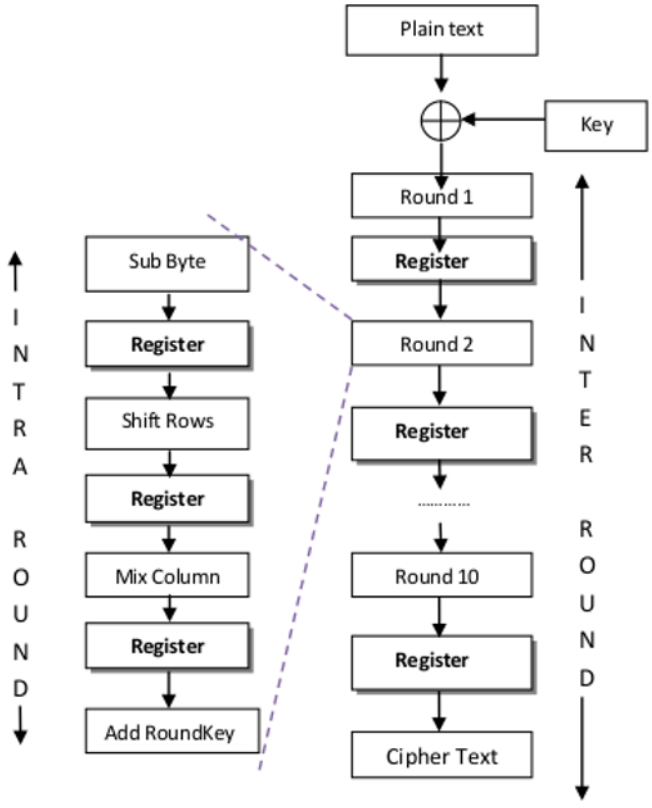

Figure 6. Sub-pipelined architecture.

This type of architecture increases the throughput further when compared to the Pipelined architecture and increases the area as well. In this architecture, when clock is equal to 1, the first set of input data (Plain text) will be processed in the Add round key. For the next clock, the first set of input will be processed in the Sub Byte round and the next set of input will be processed in the Add round Key such that none of the hardware component remains idle. In this type of architecture, the processing time is increased. In order to decrease the processing time, Parallel Architecture is used.

4.3. Parallel architecture

In the Parallel architecture, 128 bit input data is divided into four blocks of 32 bit each and is sent through four individual processing elements as shown in Fig. 7.
In this architecture, various computations are performed simultaneously [23]. This architecture is based on splitting up large components into small components thereby processing occurs simultaneously. Instead of processing one word at a time, this type of architecture processes four words parallelly at a time. This will decrease the processing time and there will be a trade-off between the throughput and area.

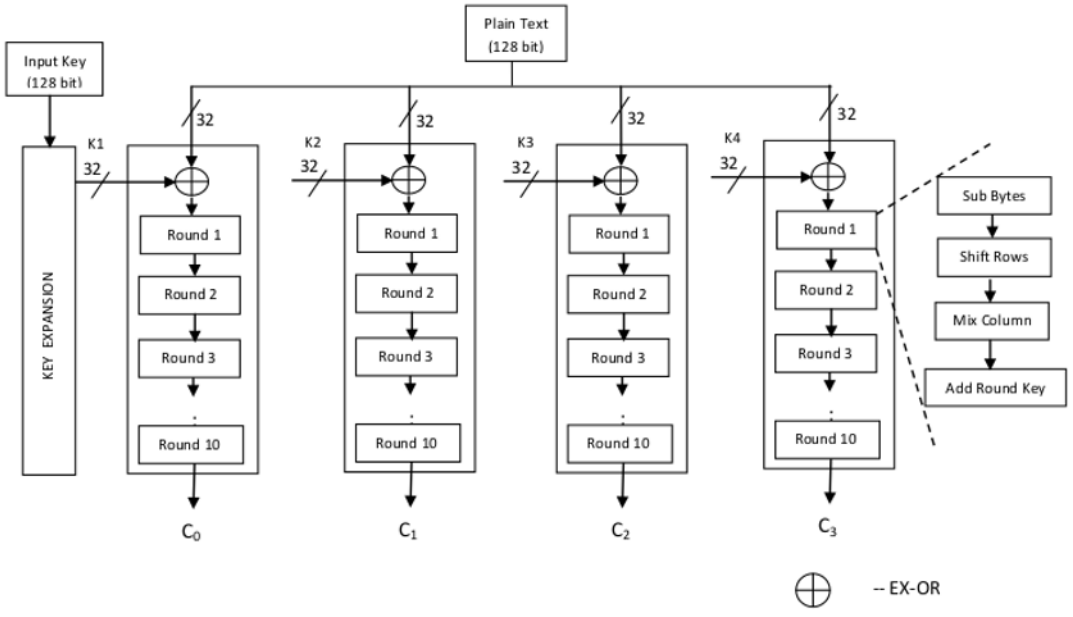

Figure 7. Parallel architecture.

5. Implementation results and discussion

5.1. Evaluation metrics

The most important parameters required for evaluating the implementation are throughput and efficiency. The Hardware Description Language (HDL) code has been written for the different architectures of AES algorithm and is prototyped on Xilinx Virtex 6 XC6VLX75T device and simulated on ModelSim XE III 6.3C tool. Also, the throughput of the proposed structure is calculated for different FPGA devices and compared with others reported in the literature.

5.2. Synthesis analysis

Various existing architectures of AES algorithm such as Loop Unrolled, Pipelining, Sub-Pipelining, Parallel, Parallel Pipelining and the proposed architecture Parallel Sub-Pipelining architecture are synthesised using Xilinx ISE tool targeted for Virtex 6 FPGA device [24]. The area occupied by the Look Up Table (LUT) and registers for different architectures are shown in Fig. 8.

From Fig. 8, it is observed that the LUT (area) occupied by the architectures increases as the throughput increases. In the pipelined architecture, the pipelining registers are used; hence area occupied by the LUT slices is higher than the Loop Unrolled architecture. In the Sub-pipelined architecture, pipelining and sub pipelining registers are used; hence the area occupied increases more than the Pipelined architecture. In Parallel architecture, all the components have been increased from basic iterative AES algorithm, so the area increases to 2121 slices rapidly which is higher than the Loop Unrolled, Pipelined and Sub-Pipelined architecture. The parallel Pipelined architecture makes use of Pipelined registers, hence it occupies more area than the parallel architecture. The proposed Parallel Sub-Pipelined architecture consumes more area when compared to all the other architectures since it makes use of sub-pipelining registers and parallel architecture.

5.3. Throughput and efficiency analysis

Throughput is the speed at which the data is encrypted/decrypted. The throughput is a very important parameter in a communication process and this determines the performance of the algorithm. The throughput [25] is determined by the

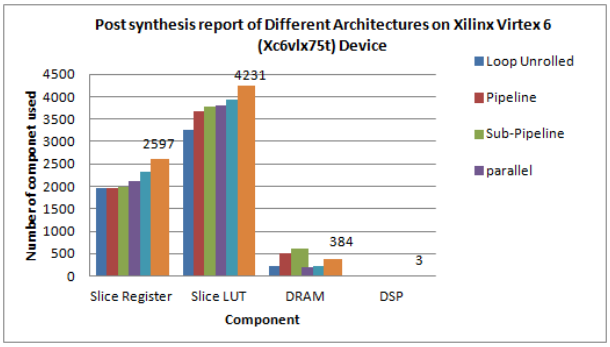

Figure 8. Post synthesis results of different architecture.

following formula,

$$\text{Throughput} = \frac{128 * \text{Number of blocks/cycle}}{\text{Period}}. \quad (1)$$

Clock Period 128- indicate the block size of the input data. The efficiency [26] is calculated by the formula,

$$\text{Efficiency} = \frac{\text{Throughput}}{\text{Area}}. \quad (2)$$

The Performance comparison of the proposed architecture with the existing architecture reported in literature is shown in the Table 1. Efficiency is the throughput per area which is denoted as Mbps/slices. The throughput and efficiency are calculated for all the architectures in order to estimate and compare the speed of the algorithm. Table 1 Performance comparison of proposed Parallel Sub Pipelined architecture with the Existing Works.

Table 1. Performance comparison of the proposed parallel sub pipelined architecture with the existing works.

S. No	Device	Author	Architecture	Throughput (Gbps)	Area (slices)	Efficiency (Mbps)
1	XC2V6000-6	[27]	Parallel Pipeline	24.92	3576	6.97
		This Work	**Parallel Sub-Pipelined**	29.73	5484	5.4
2	XC2VP7X	[28]	Loop Unrolled	3.85	2599	1.48
		This Work	**Parallel Sub-Pipelined**	31.38	5550	5.65
3	XC2VP70	[29]	Pipeline	34.7	2389	14.5
		This Work	**Parallel Sub-Pipelined**	36.38	5510	6.60
4	XC4VLX40	[30]	Iterative	0.497	1725	0.288
		This Work	**Parallel Sub-Pipelined**	39.40	6760	5.82
5	XC2VP20	[31]	Parallel Pipeline	28.44	6541	4.34
		This Work	**Parallel Sub-Pipelined**	31.38	7625	4.11
6	XC6VLX75T	**This Work**	**Iterative**	39.07	1953	20
			Pipeline	43.051	1962	21.94
			Sub-pipelined	48.531	1988	24.41
			Parallel	53.117	2121	25.04
			Parallel Pipeline	57.605	2322	24.80
			Parallel Sub-pipelined	59.59	2597	22.94

Jose M. Granado et al. [27] proposed a Parallel Pipeline Architecture which achieved a throughput of 24.92 Gbps and an area of 3576 slices on Xilinx Virtex 2 device XC2V6000.The proposed technique achieves a throughput of 29.73 Gbps which is higher when compared to [27] at the cost of increase in area. Khanob et al. [28] described two architectures, Loop Unrolled and Pipelined architecture and implemented them on Xilinx Virtex Pro2 XC2VP7X device. The Loop Unrolled architecture achieves a throughput of 3.85 Gbps and an area of 2599 slices and the Pipeline architecture achieves a

throughput of 6.16 Gbps and an area of 3119 slices which proves that Pipeline architecture is better than the Loop Unrolled Architecture. The proposed architecture that is Parallel Sub Pipeline architecture achieves a throughput of 31.38 Gbps which is much higher than the Loop Unrolled and Pipelined architecture. The proposed technique consumes more area due to the presence of sub-pipelining registers when compared to [28]. Yulin Zhang et al. [29] proposed a Pipelined architecture that achieves a throughput of 34.7 Gbps and an area of 2389 slices on Xilinx Virtex II Pro XC2VP70 device. The proposed parallel Sub-Pipeline architecture achieves a throughput of 36.38 Gbps which is higher than the throughput achieved [29]. This architecture occupies an area of 5510 slices which is quite higher than the area referred in [29] due to the increased use of registers. In the paper [30], Nalini et-al discussed that the iterative algorithm of AES which achieves a throughput of 0.497 Gbps and an area of 1725 slices on Xilinx Virtex 4 device XC4VLX40.The proposed technique achieves a throughput of 39.40 Gbps and an area of 6760 slices. The iterative algorithm processes a single input data at a time whereas the proposed technique processes more than one input data at a time. S. M. Yoo et al. [31] implemented Parallel Pipeline Architecture on Xilinx Virtex 2 device XC2VP20 and achieved a throughput of 28.44 Gbps and an area of 6541 slices. From the table 1, it is evident that the parallel Sub-pipeline achieves a throughput of 31.38 Gbps which is higher than the throughput in [31] .This architecture consumes an area of 7625 slices and is more when compared to [31] because of its architecture. Also in this paper, different architectures of AES algorithm has been synthesized on Xilinx Virtex 6 device XC6VLX75T. Since this aim of this research paper is to obtain the high throughput using parallel sub-pipelined architecture, the throughput of the proposed architecture with existing work of various authors alone is presented in Figure 9.

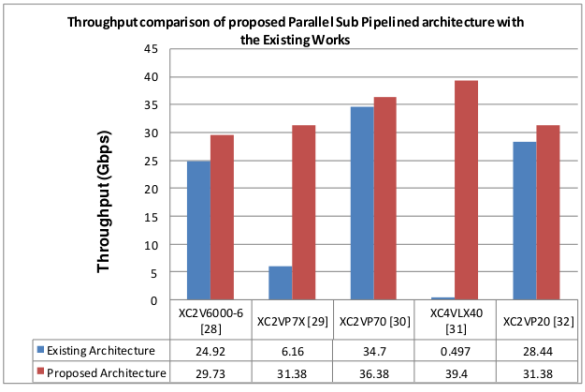

Figure 9. Throughput comparison of proposed architecture with existing works.

From the Figure 9 and Table 1, it has been observed that the Proposed technique ie., Parallel Sub Pipeline Architecture achieves a high throughput of 59.59 Gbps with a frequency of 450.045 MHz, at the cost of area and there is not much variation in efficiency except [29] because of high throughput.

5.4. Area analysis

There is a trade-off between the throughput and the area. The Loop Unrolled architecture utilises less area but the throughput is reduced. In pipelining architecture, the throughput is increased but occupies more area due to the use of registers. In Sub-Pipelining architecture, the throughput is increased further than the pipelined architecture [32]. Due to the increased number of registers, this architecture also consumes more area. When using the Parallel architecture, the hardware components are increased, ultimately the area occupied by the slice is also increased. The proposed parallel sub-pipelining architecture also consumes more area than all the other architectures but achieves more throughput than all the existing architectures. The area can be reduced by optimization techniques without affecting the throughput. These techniques can slightly modify the internal architecture [33]. Some techniques are using Composite field arithmetic in the Sub-Byte round instead of using Look Up Table (LUT) and On the fly key expansion technique in Key expansion unit.

5.5. Image encryption/decryption

The proposed architecture is also tested for different set of input images. In this research, the gray scale images of different sizes are taken and are resized to 128 x128 sizes. The gray scale images are converted to binary images using MATLAB. Now, the pixel values of the binary images are 1's and 0's which are then sent as input to the proposed architecture of AES encoder. In the AES encoder, the plain text/ input bits are converted to the Cipher/Encrypted data. The encrypted data is again sent to the MATLAB to see the encrypted image using the FILE operation. The encrypted image's pixel values are then sent to the AES decoder. In the AES decoder, the encrypted data is converted to the decrypted data / Plain Text which is again linked to the MATLAB to obtain the decrypted image through the FILE operation in VHDL. The decrypted image obtained will be the binary image which is again converted to gray scale image by using MATLAB command. The resulting will be the reconstructed image which will be same as the Original image. The different input images (a), its encrypted images (b), decrypted binary images (c) and the reconstructed images (d) are shown in Fig. 10.

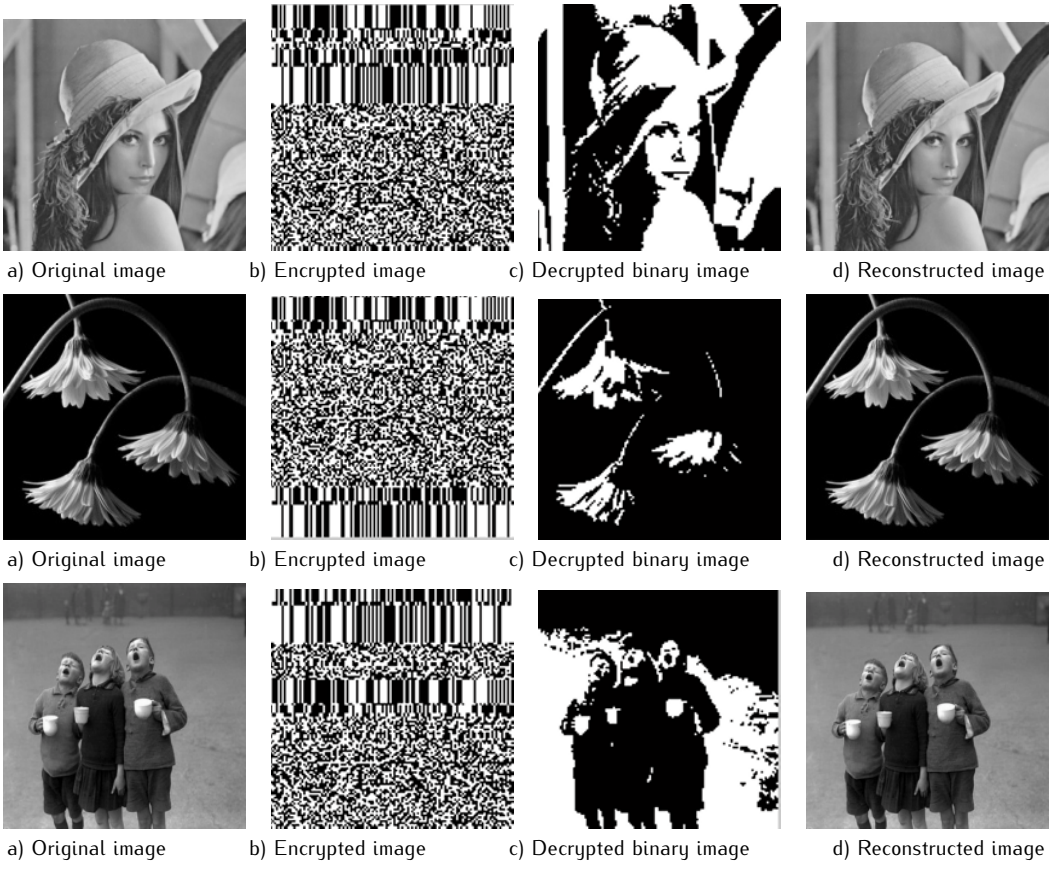

Figure 10. Image encryption/decryption using the proposed architecture of AES.

5.6. Power consumption

The proposed algorithm is also simulated in ASIC 0.13 μm and 0.18 μm technology. Table 2 shows the performance comparison of the proposed Parallel Sub-Pipeline architecture with the existing works reported in the literature. The parameters power, area and throughput are considered for comparison.

Al Wen Luo et al. [34] implemented the Pipeline architecture in ASIC 0.18 μm and consumes power of 14.0253 mW and an area of 52131.166 μm^2. When it is compared with this work, it is obvious that the parallel Sub-Pipeline architecture consumes a power of 109.25 mW which is higher than power reported in [34] .The Parallel Sub-pipeline architecture

Table 2. Performance comparison of the parallel sub-pipelined architecture with the existing works.

Author	Architecture		Technology	Total power (mW)	Area μm^2	Throughput (Gbps)
[34]	Pipeline		0.18 μm	14.0253	52131.166	-
[35]	Subpipeline	Encryption	0.18 μm	84.6	-	6.274
		Decryption		94.5	-	6.321
[36]	Pipeline		0.18 μm	9.7	-	8
[37]	Parallel		0.25 μm	150.30	-	0.543
			90 nm	7.56	-	0.615
[38]	Iterative		0.18 μm	110	819972	-
[39]	Iterative		0.13 μm	0.062	3.9 kgates	0.232
This Work	**Parallel Sub-pipelined**		**0.13** μm	**40.82**	**61225**	**25.60**
			0.18 μm	**109.25**	**95863**	**20.56**

consumes a large area and large power yet it has an advantage that it achieves a high throughput. When the proposed architecture is compared with Alma'aitah et al. [35], the Sub-Pipeline architecture consumes power of 84.6 mW during encryption and 94.5 mW during decryption which is lower than the power consumed by the proposed architecture in 0.18 μm due to the Parallel Sub pipeline architecture. This proves that the Parallel Sub-Pipelining architecture consumes high power than the Pipelining and Sub-Pipelining architecture. From the table 2, it is seen that the throughput achieved by the proposed architecture is very much higher than the throughput achieved in Sub-Pipelining architecture in [35]. Yunping Liang et al. [36] implemented Pipeline architecture in 0.18 μm technology and achieved a throughput of 8 Gbps whereas in Parallel Sub-Pipeline Architecture achieves a throughput of 20.56 Gbps. Choi H.S et al. [37] implemented Parallel architecture in 0.25 μm and 90 nm and achieves a throughput of 0.543 Gbps and 0.615 Gbps respectively. The Parallel Sub-Pipeline architecture achieves a throughput of 25.60 Gbps in 0.13 μm technology which is greater than the throughput achieved by the Parallel architecture in [37]. Lan Liu et al. [38] and Panu Hamalainen [39] implemented iterative architecture of AES in 0.18 μm and 0.13μm respectively and achieved a throughput of 0.232 Gbps. The proposed technique achieves a throughput of 25.60 Gbps and 20.56 Gbps in 0.13 μm and 0.18 μm technologies respectively. As the input is processed parallely in four processing elements, the power is cut down for the other parallel devices except for the one that is currently processing the data. Hence, it has been observed that the parallel sub-pipelining architecture achieves a high throughput and low power in 0.13 μm technology when compared to [35].

6. Conclusion and future work

In this paper, an efficient architecture for increasing the throughput of the AES algorithm has been presented. The proposed PSP architecture has been prototyped in the FPGA Virtex 6 XC6VLX75T device and has been compared with the Loop Unrolled, Pipelined, Parallel and Parallel Pipelined architecture. It is also prototyped in ASIC 0.13 μm and 0.18 μm technology. From the analysis, it has been proved that the parallel sub-pipelining architecture achieves high throughput than all the other architectures of AES algorithm. The proposed Parallel Sub-Pipelining architecture consumes more area and power, which can be reduced by the optimization techniques. The various optimization techniques are using composite field arithmetic in the sub-byte round instead of using Look Up Table (LUT) and On the fly key expansion unit can be used in the Key Expansion unit.

References

[1] National Inst. of Standards and Technology (NIST), Federal Information Processing Standard Publication 197, the Advanced Encryption Standard (AES), 2001

[2] P. Karthigaikumar, K. Baskaran, An ASIC implementation of low power and high throughput blowfish crypto algorithm, Microelectr. J. 41, 347–355, 2010

[3] L. Liu, D. Luke, Implementation of AES as a CMOS core, IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Canada, May 5-8, 2013
[4] A. Kaminsky, M. Kurdziel, S. Radziszowski, An Overview of Cryptanalysis Research for the Advanced Encryption Standard, Military Communication Conference, CA, Oct 31-Nov 3, 2010
[5] N. Courtois, J. Pieprzyk, Cryptanalysis of Block Ciphers with Overdefined Systems of Equations, ASIACRYPT, LNCS, Queenstown, Dec 1-5, 2002
[6] N. Courtois, A. Klimov, J. Patarin, A. Shamir, Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations, EUROCRYPT, LNCS, Kyoto, Dec 3-7, 2000
[7] A. Kipnis, A. Shamir, Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization, CRYPTO, LNCS, California, Aug 15-19, 1999
[8] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, A. Shamir, Key Recovery Attacks of Practical Complexity on AES Variants with up to 10 Rounds, EUROCRYPT, French Riviera, May 30- June 3, 2010 (Springer, 2010)
[9] S. Mangard, M. Aigner, S. Dominikus, A Highly Regular And Scalable AES Hardware Architecture, IEEE T. Comp. 52(4), 483–491, 2003
[10] O. Harrison, J. Waldron, AES Encryption Implementation and Analysis on Commodity Graphics Processing Units, 9th Workshop on Cryptographic Hardware and Embedded Systems (CHES 2007), Vienna, Sept 10-13, 2007
[11] H. Li, Z. Friggstad, An EfiňĄcient Architecture for the AES Mix Columns Operation, IEEE International Symposium on Circuits and Systems, Kobe, Japan, May 23-26, 2005
[12] G. Rouvroy, F.-X. Standaert, J.-J. Quisquater, J.-D. Legat, Compact and Efficient Encryption/Decryption Module for FPGA Implementation of the AES Rijndael Very Well Suited for Small Embedded Applications, International Conference on Information Technology: Coding and Computing, Las Vegas, April 5-7, 2004
[13] C. J. Chang, C. W. Hu, K. H. Chang, Y. C. Cheng Chen, C. C. Hsieh, High Throughput 32-bit AES Implementation in FPGA, IEEE Asia Pacific Conference on Circuits And Systems (APCCAS), Macao, Nov 30- Dec 3, 2008
[14] C. P. Fan, J. K. Hwang, FPGA implementations of high throughput sequential and fully pipelined AES algorithm, Int. J. Elec. Eng. 15(6), 447–455, 2008
[15] I. Hammad, K. El-Sankary, E. El-Masry, High Speed AES Encryptor with Efficient Merging Techniques, IEEE Embedded Syst. Lett. 2(3), 67–71, 2010
[16] A. Hodjat, I. Verbauwhede, A 21.54 Gbits/s Fully pipelined AES Processor on FPGA, Proc. of the 12th annual IEEE Symposium on Field Programmable Custom Computing Machines (FCCM'04), Boston, May 11-13, 2004
[17] A. Hodjat, I. Verbauwhede, Area Throughput Trade Offs for Fully Pipelined 30 to 70 Gbits/s AES Processors, IEEE T. Comput. 55(4), 366–372, 2006
[18] S. K. Reddy, R. Sakthivel, P. Praneeth, VLSI Implementation of AES Crypto Processor for High Throughput, Int. J. Adv. Eng. Sci, Tech. 6(1), 22–26, 2011
[19] E. J. Swankoski, R. R. Brooks, V. Narayanan, M. Kandemir, M. J. Irwin, A Parallel Architecture for Secure FPGA Symmetric Encryption, Proceedings in 18th International Symposium on Parallel and Distributed Processing Symposium, New Mexico, April 26-30, 2004
[20] X. Zhang, K. K. Parhi, High speed VLSI Architectures for the AES Algorithm, IEEE T. VLSI. Syst. 12(9), 957–967, 2004
[21] M. Fayed, W. M. El-Kharashi, F. Gebali, A high speed, Fully Pipelined VLSI Architecture for real time AES, 4th International Conference on Information and Communications Technology (ICICT), Egypt, Dec 1-2, 2006
[22] H. Li, J. Li, A high performance sub-pipelined architecture for AES, IEEE International Conference on Computer Design: VLSI in Computers and Processors (ICCD), Cambridge, October, 2005
[23] L. Henzen, W. Fichtner, FPGA Parallel–Pipelined AES-GCM core for 100G Ethernet applications, Proceedings of ESSCIRC, Seville, September 13-17, 2010
[24] S.-S. Wang, W.-S. Ni, An Efficient FPGA Implementation of Advanced Encryption Standard Algorithm, Proceedings of International Symposium on Circuits and Systems, Vancouver, May 23-26, 2004
[25] M. K. Sirin, D. K. Mahesh, D. Y. Rama, High Throughput-Less Area Efficient FPGA Implementation of Block Cipher AES Algorithm, International Conference on Advanced Computing, Communication and Networks, Chandigarh, June 2-3, 2011
[26] H. Qin, T. Sasao, Y. Iguchi, An FPGA Design of AES Encryption Circuit with 128-bit Keys, Proceedings of the 15th ACM Great Lakes Symposium on VLSI (GLSVLSI), Illinois, April 17-19, 2005
[27] J. M. Granado Criado, M. A. Vega Rodriguez, J. M. Sanchez Perez, J. A. Gomez Pulido, A new methodology to

implement the AES algorithm using partial and dynamic reconfiguration, Integration 43, 72–80, 2010
[28] K. Thongkhome, C. Thanavijitpun, S. Choomchuay, A FPGA Design of AES core architecture for portable hard disk, 8th International Conference on Computer Science and Software Engineering (ICSSE), Thailand, May 11-13, 2011
[29] Y. Zhang, X. Wang, Pipelined Implementation of AES Encryption based on FPGA, IEEE Conference on Information Theory and Information Security (ICITIS), Beijing, Dec 17-19, 2010
[30] N. C. Iyer, P. V. Anandmohan, D. V. Poornaiah, V. D. Kulkarni, High throughput, low cost, fully pipelined architecture for AES crypto chip, India Conference, Annual IEEE, India, Sept 15-17, 2006
[31] S. M. Yoo, D. Kotturi, D. W. Pan, J. Blizzard, An AES crypto chip using a high speed parallel pipelined architecture, Microproc. Microsy. 29, 317–326, 2005
[32] T. Good, M. Benaissa, 692-nW Advanced Encryption Standard (AES) on a 0.13-μm CMOS, IEEE transactions VLSI Syst. 18(12), 1753–1757, 2010
[33] S. S. Naqvi, S. R. Naqvi, S. A. Khan, S. A. Malik, Application Specific Scalable Architectures for Advanced Encryption Standard (AES) Algorithm, WSEAS T. Elec. 10(5), 427–436, 2008
[34] A. W. Luo, Q. M. Yi, M. Shi, Design and Implementation of Area-optimized AES based on FPGA, International Conference on Business Management and Electronic Information (BMEI), Guangzhou, May 13-15, 2011
[35] A. Alma'aitah, Z.-E. Abid , Area Efficient High Throughput Sub-Pipelined Design of the AES in CMOS 180nm, 5th International conference on Design and Test Workshop (IDT), Abu Dhabi, Dec 14-15, 2010
[36] Y. Liang, Y. Li, C. Zhang, High Throughput Cost-Effective and Low Power AES Chip Design, 3rd International Congress on Image and Signal Processing, China, Oct 16-18, 2010
[37] H. S. Choi, H. Ch. Joong, J. T. Kim, Low Power AES Design using Parallel Architecture, International Conference on Convergence and Hybrid Information Technology, Korea, Aug 28-30, 2008
[38] S. Qu, G. Shou, Y. Hu, Z. Guo, Z. Qian, High Throughput, Pipelined Implementation of AES on FPGA, International Symposium on Information Engineering and Electronic Commerce, Ternopil, Ukraine, May 16-17, 2009
[39] P. Hamalainen, T. Alho, M. Hannikainen, T. D. Hamalainen, Design and Implementation of Low-Area and Low-Power AES Encryption Hardware Core, 9th Euromicro Conference on Digital System Design: Architectures, Methods and Tools (DSD'06), Croatia, Aug 30- Nov 1, 2006