A New Reconfigurable Hardware Architecture for Cryptography Applications using AES by different Substitution box (S-Box) and Random Round Selection

G.Venkatesan*, Prof.J.Raja Paul Perinbam**

*Meenakshi engg. College ,Chennai
**Professor at R.M.K. Engineering College,Chennai.

Abstract
This paper proposes a high performance AES architecture with MUX based substitution box (S-Box) and random round selection. The byte substitution is an important part of the Advanced Encryption Standard (AES) and it is implemented using Field Programmable Gate Array (FPGA). The objective of this paper is to present an efficient realization of S-Box using hardware description language (HDL). The novel implementation of proposed AES architecture is analyzed and compared with the existing AES implementations. This proposed architecture implementation shows high speed and low area. The design is coded and downloaded into Xilinx Virtex-2 2v1500ff896 FPGA. The results obtained shows that this architecture provides an improved performance about 20% and reduction of 38% device utilization.

Key words:
AES, FPGA, SB, SR, MC

1. Introduction

AES is a cryptographic algorithm, developed by Joan Daemen and Vincent Rijmen and was chosen by National Institute of Standards and Technology of the United States (*NIST)* from many AES algorithms. This AES is used to protect the electronic data and it replaces Data Encryption Standard (DES) algorithm [1], [2]. Since then the AES algorithm has been widely implemented. Many implementations are done in software. This approach seems to be too slow for fast applications such as routers, gateways and some wireless communication systems.
It is also vulnerable to attacks. In contrast, in the pure hardware implementation, the higher data rate (Gbits/second) could be obtained by parallelization and pipelining [3], [4], [5].
The implementations are physically secure since tampering by an outside attacker is difficult. It's also a cost-effective solution for many application specific systems. The AES IP cores are also available commercially in the ASIC and FPGAs [6], [7]. AES is a 128 bit symmetric data block cipher with 128, 192 or 256 bits key lengths that applied mathematical description over the Galois finite field GF (28). The data block is considered as a square matrix of bytes copied into a state array, which is modified at each stage of encryption or decryption. After the final stage, the state array is copied into an output matrix and it has four basic steps of operation; Sub Bytes, (or S-Box), ShiftRow, MixColumn and AddRoundKey. These four steps are also known as layers. The four layer steps describe one round of the AES. Number of rounds is made vary according to the key size. The figure 1 shows the AES core block diagram. The AES with 128-bit key size operates iteratively on those four basic steps for 10 rounds. However, the first and the final rounds are arranged in a slightly different manner compared to others. All four layers have their corresponding inverse operations. The deciphering is, therefore, the reverse order of the ciphering process.

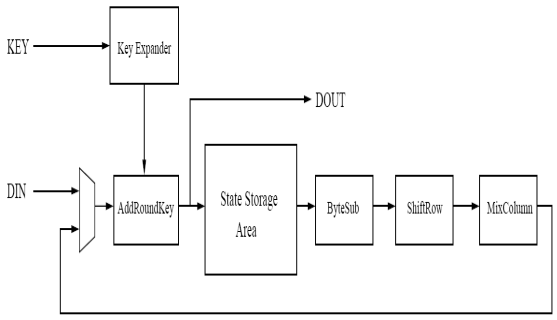

Fig1. AES core block diagram

2. Implementation of the Proposed Method using FPGA

In the proposed design, IN MUX is used to select the 128 bits of direct input or 128 bits of feedback from mixed column of one round AES. The selection of the IN MUX can be obtained from the eleven state statemachine. Each state is considered for one round. State machine is designed in such a way that to increase security by the way of selection of round in four ways. The round selection can select based on the 2bit initial seed value. The different

Manuscript received December 5, 2011
Manuscript revised December 20, 2011

selection is given in the table 1. The figure 2 shows the proposed new AES architecture.

Table 1: Different round selection.

STATE NO	INITIAL FEED VALUE			
	00	01	10	11
S0	ROUND 0	ROUND 0	ROUND 0	ROUND 0
S1	ROUND 5	ROUND 7	ROUND 1	ROUND 9
S2	ROUND 6	ROUND 8	ROUND 2	ROUND 6
S3	ROUND 3	ROUND 9	ROUND 7	ROUND 3
S4	ROUND 4	ROUND 3	ROUND 8	ROUND 4
S5	ROUND 8	ROUND 1	ROUND 5	ROUND 5
S6	ROUND 9	ROUND 2	ROUND 6	ROUND 1
S7	ROUND 1	ROUND 6	ROUND 9	ROUND 2
S8	ROUND 2	ROUND 4	ROUND 3	ROUND 7
S9	ROUND 7	ROUND 5	ROUND 4	ROUND 8
S9	ROUND 10	ROUND 10	ROUND 10	ROUND 10

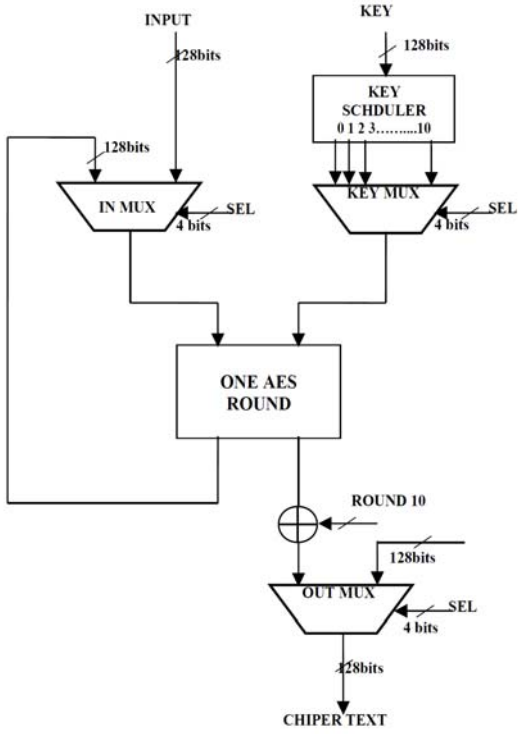

Fig 2. Proposed New AES architecture

The figure 3 shows the one round AES and one round consists of 128 bit XOR operation, Substitute Box (SB), Shift Row (SR) and Mixed Column (MC).
One AES round delivers two 128 bits output, one is from mixed column used for feedback to one round AES and other is from Shift Row.
The output of the Shift Row is XORed with 128 bits of 10th round key. The key scheduler is used to calculate the pre defined 10 round keys. All the 10 round keys is given as input to the key selection MUX.

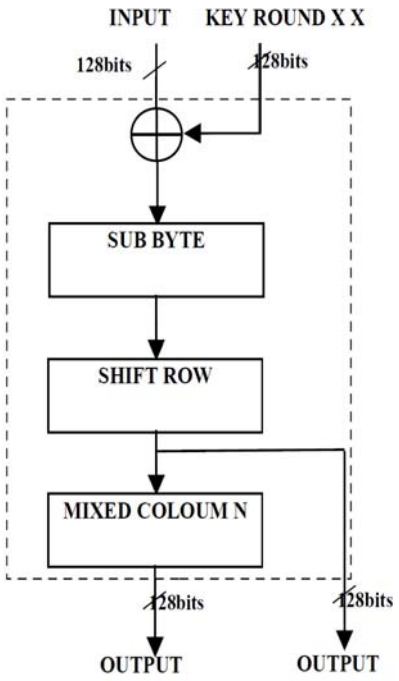

Fig 3.One round AES architecture

The figure 4 shows the state machine to give the selection lines for all the three muxes. This selection sequence is used to identify the data path between blocks. IN MUX to pass feedback and loop on the same path for 9 times, where there is no MCs in the last round.
The selection of key is used to select the different rounds of AES. The OUT MUX is used to select the output at the last round up to last round the OUTMUX deliver the default output. The correct cipher text can be identified by a single bit Done signal which is delivered by the architecture at the 10th state of state machine.

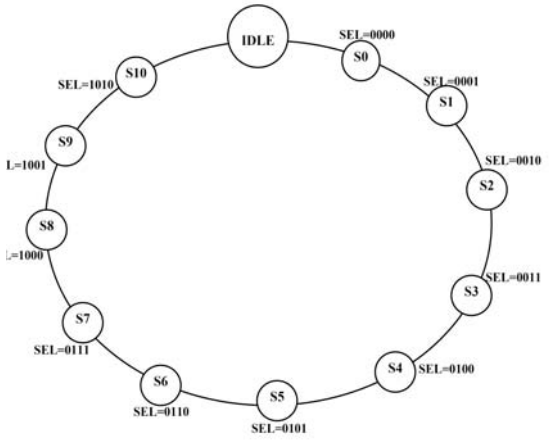

Fig 4. State machine to control the Datapath.

3. S-BOX Using Reduced memory by MUX

3.1. Lut based method

The Sub Word (Sub Bytes) transformation is implemented with a ROM, called S-Box. This ROM is a synchronous memory and thus it requires one clock cycle to produce an output. Therefore, the process to generate a round key is logically divided into two processing cycles. During the first one, the RotWord transformation is performed and an address is generated for the S-Box ROM. At the second cycle, the ROM's output is XORed with the proper Rcon value and subsequent XORs of this result produce the remaining 3 words of the round key. All four words are then stored at the unit's register file.
In addition to Substitute Byte, Mix Column can be implemented using LUT approach. An LUT combining Substitute Byte and Mix Column is called a T-Box.

3.2. Combinational method

Rijndael involves arithmetic on GF (28) elements. In the straightforward implementation inversion, multiplication and substitution are the operations that determine the overall complexity. The most common approach is to use look up table approach for these operations. A major drawback is that the size of the memory may be the bottle neck. Another approach is to use combinational logic to implement the multiplicative inversion and affine transformation for the Substitute Byte transformation. Inversion in GF (28) can be implemented using inversion in GF (24) or GF (22) accompanied by Galois field addition and multiplication. The composite field inversions are found to be more effective than GF (28) and are used to implement compact AES implementation [9].
In contrast to Rijmen's proposal which suggests the optimal normal basis representation of finite field representation, the use of polynomial representation of finite field elements results in far more flexible architecture without the necessity of the complex conversion from one representation to another. In this method hardware area can be reduced but the delay is high compared with the LUT method.

3.3. Proposed MUX based method

In this method all the sub byte values are obtained directly from the input values by inserting the inverters in the input which are the output bits changed, then this input is given to the MUX whose selection lines are controlled by the input signal. This architecture has given reduced area and higher speed. The figure 5 shows the MUX based sub byte implementation.

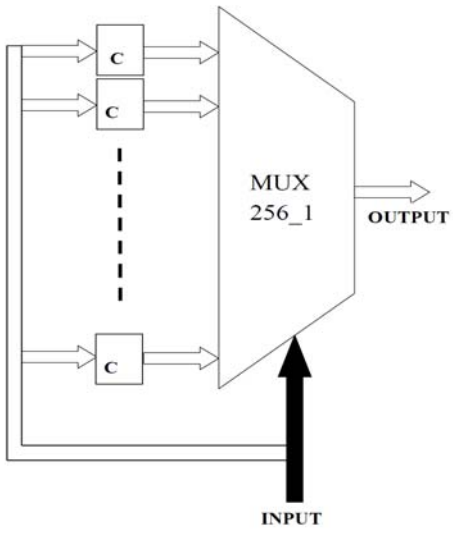

Fig 5. Proposed Sub Byte Architecture.

3.4. ShiftRows Step

The Shift Rows transformation can be expressed as an arrangement of the matrix using an address expression for each element. The address expression calculates row dependant circular shift of rows. Without a dedicated hardware resource the circular shift operation uses directions only.

3.5. MixColumns Step

The Mix Columns transformation maps one column of the input state to a new column state. The transformation is based on a four-byte input. The proposed design uses the mathematical properties of multiplication by a fixed constant in GF(28), optimally utilizing combinational logic circuit. The optimized hardware implementation considers its four byte input as a polynomial over GF (28) and is capable of performing a multiplication of the input with the constant polynomial. This zero clock cycle parallelism reduces the entire MixColumn transformation to combinational logic, efficiently exploited by us in our implementation.

4. Implementation Results and Analysis

The proposed system was implemented in VHSIC hardware description language (VHDL), and its functionality was verified by using Modlesim 6.4g. The simulation result of our encryption is shown in Figure 6.

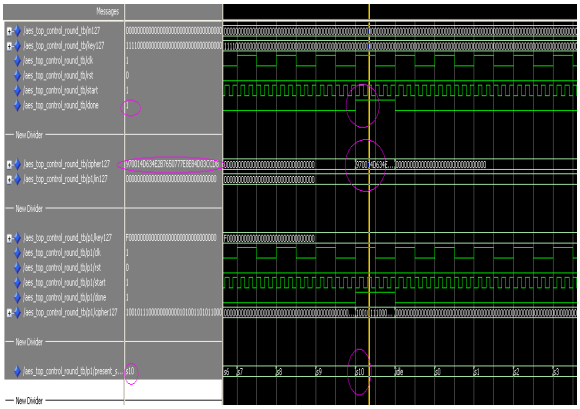

Fig 6.Proposed Sub Byte Architecture.

In order to evaluate the performance of proposed AES core, we implement three designs on Vertex 2 FPGA. We compare the performance of this design with LUT based AES and combinational AES design and also reduced memory MUX based AES. The three different AES architectures are implemented in same FPGA and compared the results. The design was synthesized on Xilinx 10.1i. The table 2 shows the comparison of area utilization in terms of number of slices and number of look up tables used and also the table shows the comparison of performance in terms of frequency and throughput. The 128-bit output from the AES module was encoded in 10 clock cycles.

The table 3 shows the three different SBOX implementation. From the table 3 the proposed substitute byte saved 80% of area from LUT based design with the same speed of operation.

Table 2. Comparison three different AES

Type of AES implementation	LUT based	Combinational	Proposed Sub byte
Device and family	Virtex 2	Virtex 2	Virtex 2
Number of Slices(7680)	5342	4998	3285
Number of 4 LUTs(15360)	10367	9681	3386
256x8-bit ROM	56	40	4
Maximum frequency	106.53MHz	72.48MHz	94.87MHz
Throughput	1.36 Gbps	0.93 Gbps	1.21 Gbps

From the result our proposed design operates at higher speed with low area utilization. The figure 7 shows the comparison chart of area used by the three architectures.

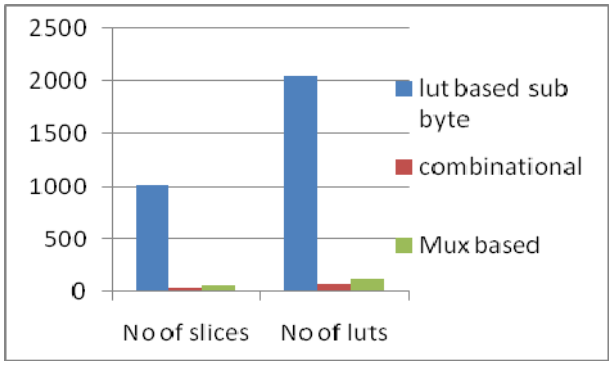

Fig 7. Comparison of area used for three different AES S-Boxes.

The figure 8 the comparison chart of performance of three architectures in terms of speed.

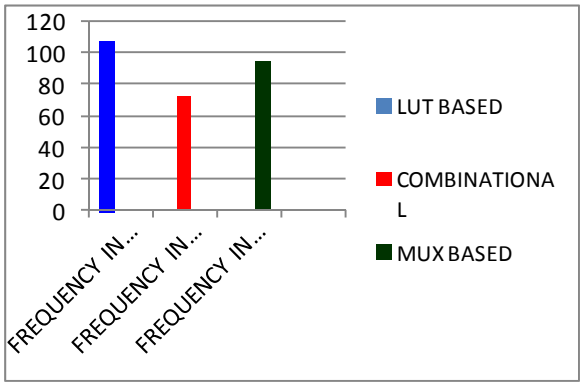

Fig 8. Comparison of speed for three different AES.

Table 3. Comparison of three different S-BOXes

Type of AES implementation	LUT based	Combinational	Proposed Sub byte
Device and family	Virtex 2	Virtex 2	Virtex 2
Number of Slices(7680)	1024	41	64
Number of 4 input LUTs(15360)	2048	73	128
256x8-bit ROM	16	-	1
combinational path delay	7.745ns	14.211ns	7.745ns

5. Conclusion

In this paper, we have presented a novel FPGA implementation reconfigurable architecture for AES utilizing high performance S-Box and random selection of rounds to increase the security. This implementation shows that a hardware resource reduction can be achieved through

the use of new sub byte. The parallel architecture does not lead to a significant increase in hardware usage because it is predominantly made up of combinational logic circuits. The proposed new AES architecture was analyzed and implemented on Xilinx Virtex-2 2v1500ff896 FPGA. The obtained results are compared with two different AES implementations. The results show that the proposed architecture provides an improved performance with 20% higher in maximum clock frequency as well as efficient utilization of FPGA hardware resources.

References

[1] S. Mangard, M. Aigner and S. Dominikus, "A highly regular and scalable AES hardware architecture", IEEE Trans. Computers, vol. 52, no. 4, 2003, pp. 483-491.
[2] Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, 2001.
[3] J, Daemen and V.Rijmen, "The design of Rijndael AES-The advanced encryption standard", Springer, 2002.
[4] A. Aziz and N. Ikram, "Memory efficient implementation of AES S-boxes on FPGA", J. Circuits, Systems, and Computers, vol. 16, no. 4, 2007, pp. 603-611.
[5] M. T. Tran, D. K. Bui and A. D. Duong, "Gray S-Box for Advanced Encryption Standard", in Proc. of International Conference on Computational Intelligence and Security, vol. 1, pp. 253-258, 2008.
[6] E. S. Abuelyman and A. A. S. Alsehibani, "An optimized implementation of the S-Box using residue of prime numbers", Inter. J. Computer Science and Network Security, vol. 8, no. 4, 2008, pp. 304-309.
[7] I. Harvey, "The effects of multiple algorithms in the Advanced Encryption Standard", nCipher Corporation Ltd., 2000.
[8] F. R-. Henriquez, N. A. Saqib and A. D-. Perez, "4.2 Gbits/s single chip FPGA mplementation of AES algorithm", Elect. Lett, vol. 39, no. 15, 2003, pp. 1115-1116.
[9] V. Rijmen. Efficient Implementation of Rijndael.Sbox.www.esat.kuleuven.ac.be/_rijmen/ ...Rijndael/ sbox.pdf.
[10] J. Zambreno, D. Nguyen and A. Choudhary, "Exploring area/delay tradeoffs in an AES FPGA implementation", in Proc. of International Conference on Field Programmable Logic and its Applications, Lecture Notes in Computer Science, Springer-Verlag, Vol. 3203, pp. 575-585, 2004.
[11] D. S. Kundi, S. Zaka, Q. Ain and A. Aziz, "A compact AES encryption core on Xilinx FPGA", in Proc. of 2nd International Conference on Computer, Control and Communication, pp.1-4, 2009.

Raja Paul Perinbam was born in Tamilnadu state, India in 1948. He received his B.E. Degree in Electrical and Electronics Engineering from University of Madras in 1970, M.Sc.(Engg) Degree in Applied Electronics from Anna University in 1973, and the Ph.D. Degree from IIT Madras in 1984. He was in the Faculty of Information and Communication Engineering, Anna University from 1975 to 2008. He is presently a Professor, Department of Electronics and Communication Engineering., R.M.K. Engineering College, Chennai. He has been a R&D consultant for various UPS based companies. His research interests are Embedded Systems, VLSI Design, Power Electronics and Signal Integrity.

Venkatesan was born in Tamilnadu state, India in 1977. He received his B.E. Degree in Instrumentation and Control Engineering from University of Madras in 2000. He Joined A.M.A. College of Engineering , Kanchipuram as a Lecturer in the Year 2000. He has more than 11 years of teaching Experience . He has been a Senior Lecturer in Electronics and Instrumentation Engineering , Meenakshi College of Engineering, Chennai-78 Since 2002 . The college is affiliated to Anna University, Chennai. He is presently doing M.S. (by Research) at College of Engineering, Guindy, Anna University, Chennai. .His research interests are Cryptography, VLSI Design. and Analog Electronics.