ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 7, July 2017

A new encryption methodology of aes algorithm using high speed s-box

[1] Sarala S Shirabadagi, [2] Swetha Nadagoud
[1] BITM VTU,Ballari,Karnataka, [2] BITM VTU,Ballari,Karnataka

Abstract - **Cryptography plays an important role in the security of data. Encryption ensures data integrity by protecting the data from being corrupted or modified.RSA and DSA are the most commonly used methods for the authentication. Encryption uses symmetric and asymmetric encryption algorithms such as Triple-DES and Blowfish for maintaining the confidential. The AES is widely used for encryption of audio/video data contents in real time. Due to the significance of the AES algorithm and the numerous real-time applications, the main concern of this paper is to present new efficient hardware implementations for this algorithm.AES uses four operations, namely SubBytes, ShiftRows , MixColumns and Key Additions transformations. SubBytes transformation is done through S-BOX. This paper describes full custom design of high speed S-BOX for AES encryption algorithm and its implementation in FPGA and ASIC. The proposed AES architecture has delayed improvement of approx. 1.6 ns along with area improvement of 287 FPGA slices when implemented in the Spartan-6 FPGA of Xilinx. The full custom design of the S-BOX has been done in 180 nm technology in Cadence using novel XOR gate which has high speed and low power consumption . The designed S-BOX chip consumes 22.6 µW and has 8.2 ns delay after post layout simulation.**

Index Terms: Advanced Encryption Standard(AES), Data Encryption Standard(DES), Substitution Box(S-Box), Field programmable array(FPGA)

I.INTRODUCTION

Cryptography plays a vital role within the security of knowledge. It permits US to store sensitive data or transmit it across insecure networks so unauthorized persons cannot scan it. The urgency for secure exchange of digital knowledge resulted in massive quantities of various encoding algorithms which may be classified into 2 groups: uneven encoding algorithms (with public key algorithms) and even encoding algorithms (with personal key algorithms). even key formulas square measure normally a lot of quicker to execute electronically than uneven key algorithm. encoding uses even and uneven encoding algorithms like Triple-DES and Blowfish for maintaining the confidential. as luck would have it, varied techniques are developed to stay the information secure and personal. The essential technology underlying just about all machine-driven network and pc security applications is understood as encoding. Encoding was primarily used for military and undercover work use. The requirement for secure transactions in e-commerce, virtual personal networks and secure electronic messaging has rapt encoding into the industrial realm. Encoding ensures knowledge integrity by protective the information from being corrupted or changed. Substantiation and hash-function techniques square measure won't to give the information integrity. Authentication of users is provided by encoding by checking the identity of the user. RSA and therefore the Digital Signature Algorithm(DSA) square measure the foremost ordinarily used ways for the authentication. The Advanced encoding customary (AES) algorithmic program has revealed by authority as a draft FIPS-197 in 2001. There area unit varied hardware implementations were prompt for it, among all the implementation largely they need targeted the AES with 128-bits key size . This key size is taken into account to be applicable for many of the industrial applications, wherever mistreatment higher key sizes is taken into account as way over resources. It involves higher space implementations with longer interval and dangerous to implement for little scale devices. Key sizes of 192-bit and 256 bits area unit used largely in high secret military applications to substantiate the most level of security.

NIST control 2 conferences to debate the submissions (AES1, August 1998 and AES2, March 1999), and in August 1999 they proclaimed that they were narrowing the sector from fifteen to five: MARS, RC6, Rijndael, Serpent, and Twofish. All 5 algorithms, normally mentioned as "AES finalists". authority proclaimed that Rijndael had been handpicked because the projected AES [1]and created it formally customary.

A. PROBLEM STATEMENT

To develop HDD security technique labeled as disk trust. Disk trust technology uses PDE, creates

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 7, July 2017

authorized invisible volume on HD and implements SKC with Rijindael [1] to secure the data stored on secured volume. The main objectives for efficient AES algorithm designs are: (a) To propose the high speed S-BOX and its implementation in FPGA and ASIC. (b) In Composite Field Arithmetic, XOR is used in addition so, XOR has been designed using minimum number of transistors and it has high noise margin and low power. (c) Full custom design of SBOX for AES Encryption algorithm. (d) Implementation of high speed architecture of AES algorithm.

B. HIGH SPEED AES DESIGN

The Advanced coding customary (AES) has further new dimension to cryptography with its potentials of safeguarding the IT systems. This technique features a fine delay - path from S-Box process. The AES rule will be enforced on a varied vary of platforms underneath totally different constraints .This paper presents the planning of Associate in Nursing ultrahigh speed AES processor to get cryptographically secured data at a rate of multi-ten GBPS. The planned style addresses ensuing generation IT security requirements: the resistance against all crypto-analytical attacks and high speed with low latency. This work optimizes AES rule to eliminate algebraically operations from the datapath that contributes to realize radical high speed and to scale back the latency. The AES processor is meant victimization Verilog HDL then simulated victimization FPGA platform. The performance of the processor is compared thereupon of different researchers in terms of speed and latency that shows its superiority over them. The soft core will be reused to convert it to ASIC to realize far better performance.

C.ARCHITECTURE AND IMPLEMENTATION OF S-BOX

There are four transformations in the AES algorithm among all the transformation, SubBytes is complex and non-linear. There are two techniques found to implement S-BOX, one using RAM and another using composite field arithmetic architecture. The implementation of the composite field S-BOX is accomplished using combinational logic circuits rather than using pre-stored S-BOX values. S-BOX substitution starts by finding the multiplicative inverse of the number in GF(galois field), and then applying the affine transformation. Implementing a circuit to find the multiplicative inverse in the finite field GF is very complex and costly, therefore, has suggested using the finite field GF to find the multiplicative inverse of elements in the finite field GF .

The S-Box is at the major of any AES implementation and is measured a full complexity design consuming the main portion of the power and energy inexpensive of the AES hardware. The substitute way is to design the S-Box circuit using combinational logic directly from its arithmetic operations. This method has a fine delay - path from S-Box processing. The AES algorithm can be implemented on a varied range of platforms under different constraints. A full-custom chip is more suitable for compact small foot-print design. The Galois Field arithmetic for S-Box, it is very clearly evident that the implementation of S-Box/InvS-Box needs a large number of XOR operations.

The novel XOR has been designed using minimum number of transistors and it has high noise margin and low power consumption as compared to existing XOR designs. This method has a fine delay – path from S-Box processing. The AES algorithm can be implemented on a varied range of platforms under different constraints The new approach to minimize the silicon - area of S-Box design demonstrated by using a new 2-input XOR gate for low-power composite field arithmetic to reduce the power dissipation and delays for the complete circuit.

II. PROPOSED AES ALGORITHM

A. IMPLEMENTATION OF ARCHITECTURE FOR S-BOX

The new architecture of S-BOX has proposed after 3 modifications in conventional architecture of S-BOX. (a) Introduced an operator (op) after merging of some blocks. (b) Implementation of multiplicative inverse in GF using multiplexor. (c) Reduced the critical path of multiplication in GF.

A. INTRODUCED AN OPERATOR (OP) AFTER MERGING OF SOME BLOCKS.

An operator (op) has introduced after merging of blocks like squarer, multiplication with constant λ, a GF (2^4) multiplier and a four bits XOR. The equation of op has introduced using Galois field irreducible conversion technique and in the form of an input bit

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 7, July 2017

stream. One major operation involve here is finding the multiplicative inverse in GF (2^8).
This can be done by breaking the GF (2^8) elements in GF (2^4). I.e. Any arbitrary polynomial in GF (2^8) can be represented as bx+c using an irreducible polynomial x2+Ax+B. Here, b is the most significant nibble and c is the least significant nibble . The multiplicative inverse can be found by using the following expression.

$(bx+c)^{-1}=b(b^2B+bcA+c^2)^{-1}x+(c+bA)(b^2B+bcA+c^2)^1$
$=b(b^2\lambda+c(b+c))^{-1}x+(c+b)(b^2\lambda+c(b+c))^{-1}$ -(1)

We can reduce the blocks in the proposed architecture from its conventional architecture of SBOX.

B.IMPLEMENTATION OF MULTIPLICATIVE INVERSE IN GF (24) USING MULTIPLEXOR.

MI in GF (2^4) represented by the symbol x-1 and multiplication in GF (2^4) are the two maincomponents falls in the critical path of the design. MI in GF (2^4) consists of complex logic given by equation (2)

$q_3^{-1} = q_3+ q_3\ q_2\ q_1+ q_3\ q_0 +q_2$

$q_2^{-1} = q_3\ q_2\ q_1+ q_3\ q_2\ q_0+ q_3\ q_0 +q_2+q_2\ q_1$

$q_1^{-1} = q_3+q_3\ q_2\ q_1 +q_3\ q_1\ q_0+ q_2\ q_0 +q_2 + q_1$

$q_0^{-1} = q_3\ q_2\ q_1+ q_3\ q_2\ q_0+q_3\ q_1+q_3\ q_1\ q_0+ q_3\ q_0+q_2+q_2$
$q_1+ q_2\ q_1\ q_0+ q_1+ q_0$ ----------(2)

Where, $q3^{-1}q2^{-1}q1^{-1}q0^{-1}$ is 4-bits MI of 4-bit value q3 q2 q1 q0and + sign indicates XOR operation. It is evident that the realization of MI in GF (2^4) requires a number of exclusive-or gates. By eliminating the XOR gates, delay and area can be reduced.

C.REDUCED THE CRITICAL PATH OF MULTIPLICATION IN GF (2^2)
It is evident that there are two XOR gates and one AND gate in the critical path of GF (2^2) multiplication. The output equation can be written as in equation (3)

$z(0)=x(1)y(1) \oplus x(0)y(0)$

$z(1)= x(1)y(1) \oplus x(0)y(1) \oplus x(1)y(0)$ -----(3)

The above equation can be implemented using two 4:1 parallel multiplexers as shown in figure 1

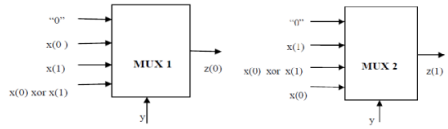

Figure1: 4:1 multiplexer for (a) LSB output and (b)

MSB output for 2 bits output of multiplication in GF

D. IMPLEMENTATION OF ARCHITECTURE OF S-BOX
Figure 2 shows the proposed architecture of S-box for AES has been implemented in Xilinx FPGA and 180nm ASIC.

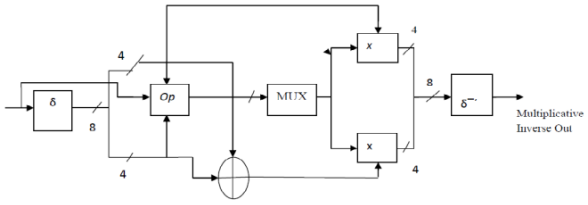

Figure 2: Multiplicative Inverse architecture

III. HIGH SPEED AES ENCRYPTION

We have designed the architecture of AES encryption which has low latency and low power consumption. The design optimization has been done by replacing conventional modules in AES architecture with a module which best suits for the area and latency reduction. our proposed architecture, in which ShiftRows and Add Round Keys are merged in Mix Columns transformation module. It means that these three transformations can be done using single clock cycle.
The proposed architecture of S-BOX with all three modifications (which discussed in the previous section II) have used for SubBytes transformation in the proposed architecture of AES encryption algorithm. Iterative architecture can be realized with low area and proposed architecture helps to raise the speed.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 7, July 2017

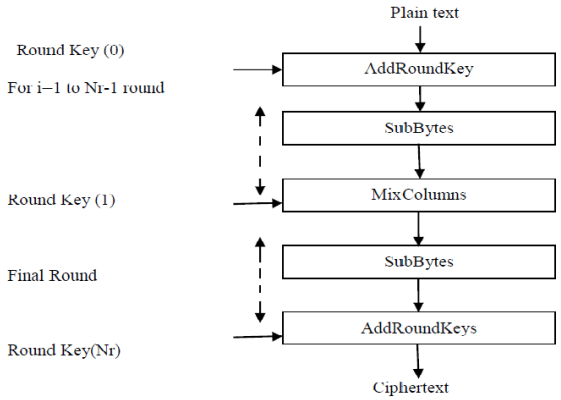

Figure 3: The proposed architecture of AES encryption algorithm

IV. FULL CUSTOM DESIGN FOR S-BOX

The S-Box (Substitution box) forms the core building block of any hardware implementation of the Advanced Encryption Standard (AES) algorithm. This chapter presents a full custom CMOS design of S-Box with low power and high speed GF (28) Galois Field inversions based on polynomial basis, using composite field arithmetic. The proposed architecture shows that XOR is the major component which is used to do the addition operation in composite field arithmetic. The optimization of the design has been done by proposing novel circuit for smaller components like XOR gate and other circuit components like Galois Field (GF) multiplier. The XOR has been designed using minimum number of transistors and it has high noise margin and low power consumption as compared to existing XOR designs. The full custom design is required for small devices like smart cards and high rate of data transmission.

A. NOVAL XOR GATE FOR LOW POWER FULL CUSTOM DESIGN OF S-BOX

It is clearly evident that the implementation of S-Box requires a large number of XOR operations whose efficient and low power implementation can result in a significantly improved CMOS S-Box hardware design. The numerous 2-input XOR gate designs have been described to enhance the performance for several applications. The novel XOR has been designed using minimum number of transistors. The pass transistor concept is used to design proposed XOR gate.

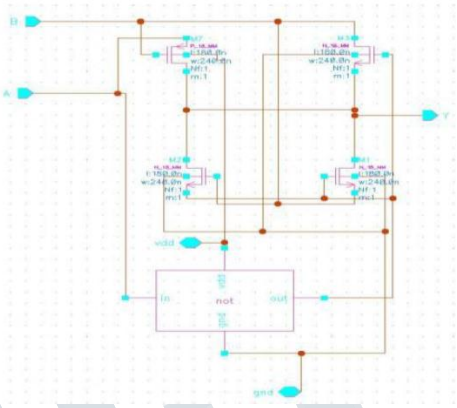

Figure 4: Schematic for novel XOR

A novel XOR has simulated in same technology and improvement can be seen in Figure4 . It has a high noise margin and low power consumption as compared to conventional XOR gate designs. The new approach to minimize the silicon - area of S-Box design demonstrated by using a new 2-input XOR gate for low-power composite field arithmetic to reduce the power dissipation and delays for the complete circuit.

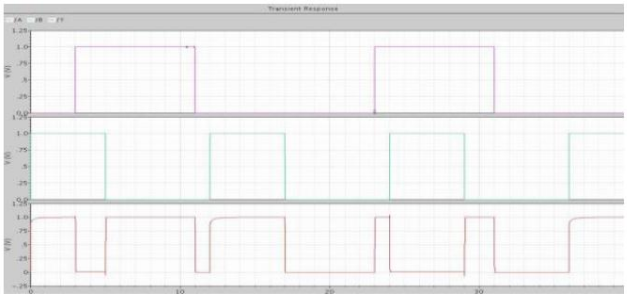

Figure 5: Simulated output for Schematic of novel XOR

A full-custom design of AES SubByte module based on sense amplifier based logic is proposed in this paper. Power consumption of this design is independent of both value and sequence of data. Therefore this design is resistant to power analysis attack. This design is implemented using SMIC 0.18

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 7, July 2017

um CMOS technology. Simulation results show that it can work at the frequency of 83.3 MHz, and its total area is about 0.85 mm2. This design is suitable for application in the hardware implementation of symmetric-key cryptographic devices that have high security demand. The proposed architecture shows that XOR is the major component which is used to do the addition operation in composite field arithmetic.
The optimization of the design has been done by proposing novel circuit for smaller components like XOR gate and other circuit components like Galois Field (GF) multiplier. The XOR has been designed using minimum number of transistors and it has high noise margin and low power consumption as compared to existing XOR designs. The full custom design is required for small devices like smart cards and high rate of data transmission.

V. RESULT

The proposed engineering was actualized utilizing the CADENCE virtuoso format configuration instrument. The strategy received was a hand crafted at the transistor level in light of a custom cell library of 0.35 CMOS primitive standard cells. A progressive approach was followed in the execution of the calculation. Custom cell plan approach was utilized for creating the design for the transarrangements. The format for every module was created and later coordinated to get the last chip. The subsystems depicted in(III) were actualized as modules at the transistor level and tried comprehensively by applying appropriate test boosts. The MOSIS CMOS configuration principles were utilized to design primitive cells utilizing the Cadence Virtuoso format editorial manager. The format was made free of Design Rule Check (DRC) blunders and Extraction mistakes. The created cells were then changed over to a netlist. The created netlist was then mimicked with HSPICE utilizing the MOSIS CMOS demonstrate parameters to produce the waveforms. The ByteSubstitution, Shift Row, Mix Column, Round Key Addition changes are executed. The outline designs of all the four changes are shown in figure 6-7.

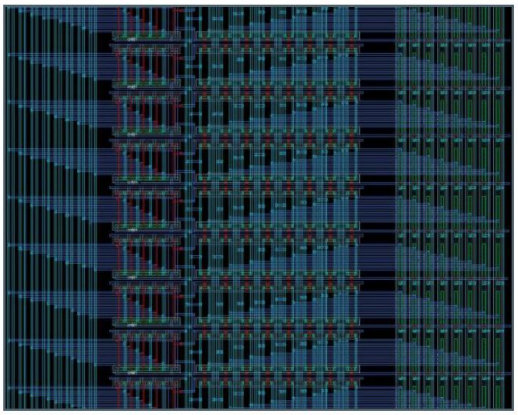

Figure6:Multiplicative Inverse Layout for Encryption and Decryption

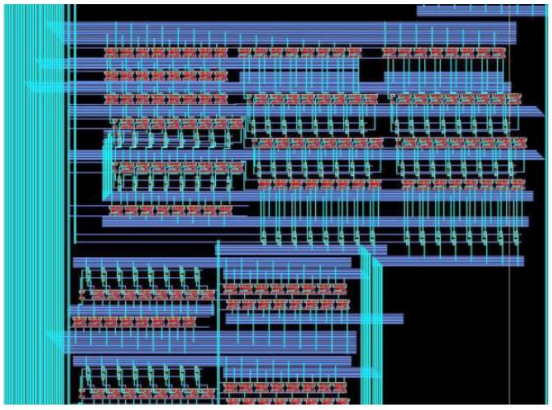

Figure 7: Mix Column and Inverse Mix Column Transformation Layout for Encryption and Decryption

VI. CONCLUSION and FUTURE WORK

We have proposed optimized VLSI architecture of Sbox for AES algorithm. The architecture of s-box in composite field has been modified in order to have high speed and low areas. Using the proposed s-box, AES architecture has been implemented using the merging technique in FPGA. The proposed AES architecture has delayed improvement of approx. 1.6 ns along with area improvement of 287 FPGA slices when implemented in the Spartan-6 FPGA of Xilinx. The full custom design of the s-box has been done in 180 nm technology in Cadence using novel XOR gate which has high speed and low power consumption as compared to existing one. The designed s-box chip

consumes 22.6 μW and has 8.2 ns delay after post layout simulation.The proposed architecture uses feedback logic. We perform both the encryption and decryption modules, with datablock and key equal to 128 bits.

A. FUTURE WORK

1.Full custom design of AES.
2.Tape out of full custom AES.
3.Video encryption in real-time using proposed design implemented in FPGA.
4.Text data encryption in real-time using proposed design implemented in FPGA.
5.Enhance the speed of data transmission.
6.Enhance the security of data transmission

REFERENCES

[1] Rudra, P.K. Dubey, C.S. Jutla, V. Kumar, J.R. Rao, and P. Rohatgi. "Efficient Rijndael Encryption Implementation with Composite Field Arithmetic", Workshop on Cryptographic Hardware and Embedded Systems (CHES2001), pages 175–188, May 2001.

[2] B.A. Forouzan and D. Mukhopadhyay, Cryptography and Network Security, 2nd Ed.,Tata McGraw Hill, New Delhi, 2012.

[3] Chih-Pin Su, Tsung-Fu Lin, Chih-Tsun Huang, and Cheng-Wen Wu, "A High-Throughput Low-Cost AES Processor," IEEE Communications Magazine, Vol.41 (12), pp.86-91, Dec. 2012.

[4] Data Encryption Standard (DES), FIPS PUB (46- 3), Oct. 25, 1999 FederalInformation Processing Standard

[5] Edwin NC Mui, "Practical Implementation of Rijndael S-Box Using Combinational Logic," Custom R&D Engineer Taxco Enterprise Pvt. Ltd.

[6] Federal Information Processing Standards Publication 197 (FIPS 197), available online, http://csrc.nist.gov/publications/fips/fips197/fips197.pdf.