IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791(Impact Factor: 1.479)
www.ijreat.org

Fault Detection Technique For S-Box In AES Algorithm

M.P.Gomathi[1], M.Tamilselvi[2], N.Jayapal[3]

[1]*PG SCHOLAR, ECE Department, Kongunadu College of Engineering and Technology, Trichy, India*

[2]*PG SCHOLAR, ECE Department, Kongunadu College of Engineering and Technology, Trichy, India*

[3]*Asst.Professor, ECE Department, Kongunadu College of Engineering and Technology, Trichy, India*

Abstract

Security of the info transmission is one among the prime factors in communication networks.So, authentication, non-repudiation, information integrity associated confidentiality are the necessary elements of an info security. The principle of AES encryption algorithm and the detailed description of the FPGA design and implementation are proposed. The limitation of the current AES implementation methods is that the throughput is small. In allusion to this problem, this project applies assembly-line technology in the designation and gains the best optimized area and speed. The novel CFA AES S-boxes of the field is derived. The best construction is chosen when a sequence of recursive and subject optimization processes. What is more, for every composite field constructions, there exist eight attainable isomorphic mappings. Therefore, when the exploitation of a brand new common sub expression elimination algorithmic rule, the isomorphic mapping that leads to the minimum area is chosen. It implements AES encryption algorithm in hardware description language. A data corruption may be occurring due to SEU and to avoid this Hamming error correction code is used. The experiment result shows that high throughput is obtained.

***Key Words**:Advanced Encryption Standard (AES), Composite Field Arithmetic (CFA), S-box, SEU (Single Event Upset)*

1 INTRODUCTION

Communication and transfer of information within the present days invariably necessitate the utilization of encryption. Besides its uses in Military and Government's secret communication, cryptography is in addition used for shielding many kinds of civilian systems like internet e-commerce, Mobile networks, ATM machine transactions, copy protection and plenty of. Encryption is achieved by following a scientific formula named as cryptography formula. An encryption formula provides Confidentiality, Authentication, Integrity and Non-repudiation. Confidentiality is that the demand that data is unbroken secret from those who do not appear to be authorised to access it. Authentication is that the understanding that the message thus originates from the reputed sender. Integrity is that the demand that information is unaltered and complete. Non repudiation implies that the sender or receiver of a message cannot deny having sent or received the message.

Cryptography plays a very important role within the security of knowledge transmission. The event of computing technology imposes stronger needs on the cryptography schemes. The Data Encryption Standard (DES) has been the U.S. government customary since 1977. However, now, it may be cracked quickly and inexpensively. In 2000, the Advanced Encryption Standard (AES) replaced the DES to fulfill the ever-increasing needs for security. This normal specifies the Rijndael formula, a symmetrical block cipher that may method information blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle extra block sizes and key lengths; but they're not adopted during this normal.

Faults that occur in VLSI chips are classified into two categories: transient faults that eventually diminish the permanent faults. The origin of those faults might be internal phenomena within the system, like threshold changes, shorts,

opens, etc., or external influences, like electromagnetic wave. These faults have an effect on the memory similarly because the combinatory components of a circuit and are detected using concurrent error detection (CED). Cryptographical chips are sensitive to natural faults within the hardware. A little variety of excited faults will cause an outsized variety of output bits of AES to be faulty. Recently, attackers have injected faults into cryptographical circuits to steal secret data similarly.

2 RELATED WORKS

In [1], parity-based fault detection architecture of the S-box and the Inverse S-box for designing high performance fault detection structures of the AES are proposed.

In [2], 128-bit AES encryption and decryption using Rijndael Algorithm are designed and synthesized using verilog code and implemented with the help of FPGA.

In [3], the modifications in each round of the AES algorithm are done. The complexity of the encryption method is improved andthe pattern in the algorithm cannot be predicted by the attackers. In each transformation, the 8-bit values are divided into 4-bits and then they are grouped with the different 4-bits and then the transformation process is performed. This method provides the algorithm with strong diffusion and confusion.

In [5], the pipelined architecture of the AES algorithm is proposed. It increases the throughput of the algorithm and the speed is increased. Here, a register by means of which the direct contact between two rounds are avoided.

3 PROPOSED WORK

The proposed work aims to analyze each the present and new architectures that lead towards the foremost optimum composite field AES S-box doable. There are four major concerns in constructing the CFA combinatorial circuit, particularly the sector of mapping, basis illustration, field polynomials and isomorphic mapping. We have a tendency to initial deduce and gift a new composite field AES S-box constructions. Second, we have a tendency to explore all of the eight attainable isomorphic mappings for every composite field construction. To be precise, we have a tendency to apply a brand new Common Subexpression Elimination (CSE) algorithmic program to scale back the world needed within the isomorphic mappings. To this finish, the CFA AES S-boxes are regenerated into direct computation modules that are expressed using algebraic normal form (ANF) representations, consisting of solely AND and XOR operations.

4AES ALGORITHM

The Rijndael algorithmic rule used for the AES standard implements a symmetric-key cryptological function within which each the sender and receiver use a single key to write in code and decipher the knowledge. AES operates on a 4×4 array of bytes, termed the state (versions of Rijndael with a bigger block size have extra columns within the state). Every standard round includes four elementary algebraic function transformations on arrays of bytes. These transformations are: byte substitution, shift row, mix column, and round Key addition. The AES algorithm is shown in Fig-1.

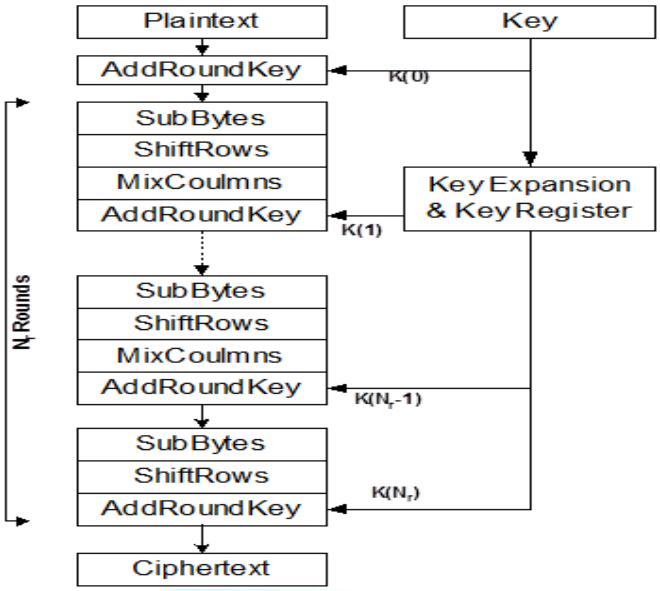

Fig-1:AES Algorithm

4.1 Sub Bytes

The first transformation in every round is that the bytes substitution known as Sub Bytes that is enforced by 16 S-boxes. It's a nonlinear substitution step wherever every byte is replaced with another per the look-up table. Every s-box transformation performs multiplicative inversion for numbers 00H-FFH in GF (2^8) followed by affine transformation. For inverse S-box transformation, the inverse affine transformation takes place initial before computing the multiplicative inverse. The S-box and inverse S-box of the AES is shown in fig-2 and it splits into 5 blocks. Out of those five blocks, three blocks perform multiplicative inversion and the remaining two blocks performs the affine transformation, based on Galois field operation.

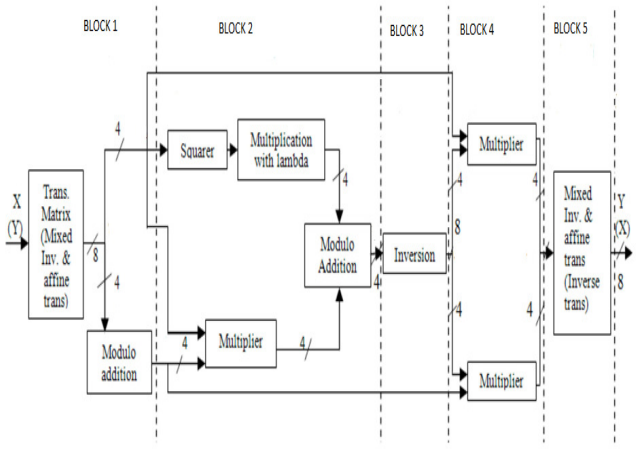

Fig-2: Construction of S-box

4.2 Shift Rows

Shift Rows is a transposition step in which every row of the state is shifted cyclically an explicit range of steps to left. For AES, the primary row is left unchanged. Within the second row, the third and fourth rows, each byte is shifted by one, two and three positions respectively as shown in fig-3. Inverse shift rows is that the inverse method of Shift rows transformation within which the bytes within the last three rows of the State are cyclically shifted over totally different numbers of steps to right.

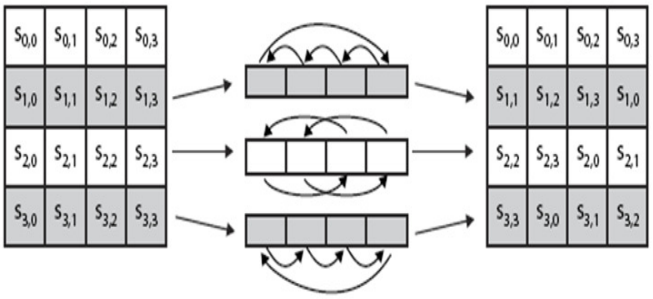

Fig-3: Shift Rows

4.3 Mix Columns

In Mix Columns, each entry in the output state is constructed by the multiplication of a column in the input state with a fixed polynomial over GF(2^8) as shown in fig-4. The Mix Column transformation is executed by repeating the operation of basic module into four times. Inverse Mix column is the inverse operation of the Mix Column transformation.

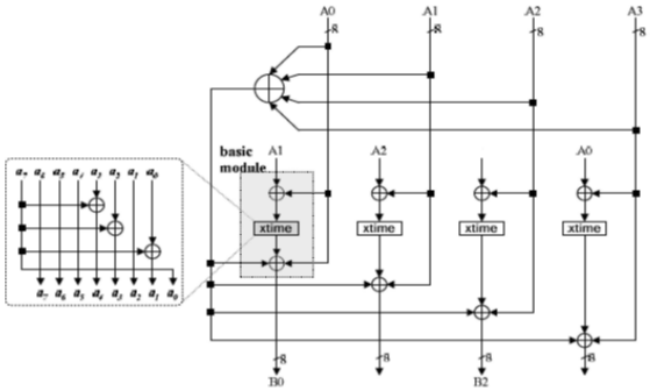

Fig-4: Mix Column Stage

4.4 Add Round Key

In this, each byte of the state is combined with the round key: each round key is derived from the cipher key using a key schedule. The round key is added to the state before starting the loop. In the Add Round Key step, each byte of the key state is combined with a byte of the round sub key using the XOR operation.

4.5 Key Expansion

It takes 128-bit (16-byte) key and expands into linear array of 44/52/60 32-bit words. It starts by copying key into first 4 words and then loop creating words that depend on values in previous & 4 places back. In 3 of 4 cases XOR operation is used.1st word in 4 includes the operation such as rotate and XOR for S-box addition and round constant on previous. The Fig-5 shows the operation involved in key expansion.

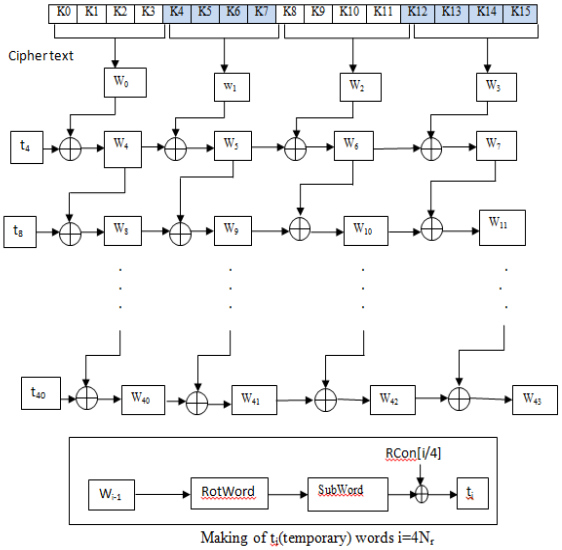

Fig-5: AES Key Expansion

5 COMMON SUBEXPRESSION ELIMINATION ALGORITHM

Common sub-expression elimination (CSE) could be a compiler optimization that searches for instances of identical expressions, and analyses whether or notit'sworthyreplacement them with a single variable holding the computed worth. The optimizationof those multiplications willresult innecessaryenhancements in numerousstyle parameters like area or power consumption.

The steps involved in CSE algorithm are as follows:
1. Identify common factors present in the transformation.
2. Select a pattern for elimination.
3. Remove all the occurrences of the selected pattern.
4. The eliminated pattern is computed only once.
5. Repeat Step 1 - 4 until none multiple patterns is present.

One of the common problems relating to the feasibleness of CSE is that the optimality of the algorithm. The optimality referred here emphasizes on the elimination of logic operators. By eliminating one pattern, it is likely to lose other possible patterns owing to the sharing of the nonzero bits. Hence, the key issue here is to pick the proper pattern and eliminate over the others which will end in maximal reduction. The proposed CSE algorithm results in optimum substructure sharing scheme for isomorphism function and affine transformation in composite field AES S-box.

6 FAULT MODEL

The types of faults are the permanent stuck-at-1 and stuck-at-0 faults. The proposed technique assumes faults due to transients and induced faults. A fault in a network is said to be masked if the function has not been changed due to the occurrence of the fault. In this we focused a design technique for detecting and correcting single/multiple error using Hamming code.

6.1 Detection and Correction of Fault

When mismatch between the output parity bits and predicted output parity bits is occurred, then it says that error has been occurred. When it is used in error correction mode using the computed syndrome, we can distinguish errors in the functional block and the PP block. Comparing the output parities and the PP bits gives a unique syndrome that shows error in the functional block or the PP block. This syndrome is decoded to identify which bit is in error and the final EXOR operation is used to correct the erroneous bit. The basic structure of the concurrent error detection and correction scheme is shown in Fig-6:

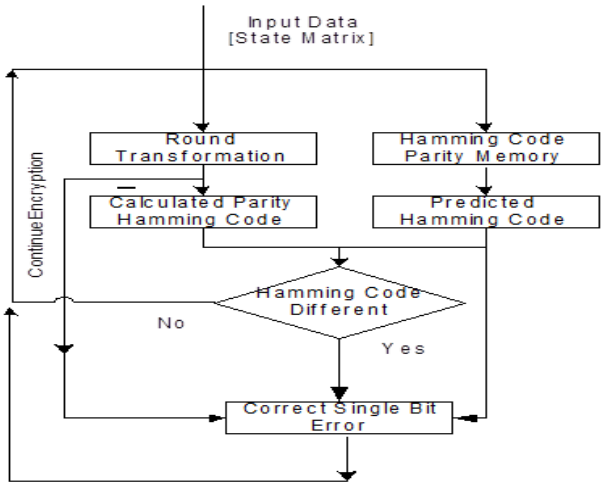

Fig-6: Function Circuit for Error Detection and Correction

The Hamming code matrix for the Sub Bytes transformation is predicted with reference to the hRD table. The Hamming code matrix prediction for Shift Rows are involved using cyclic rotation of the Sub Bytes Hamming code bits. For Mix Columns the Hamming code state matrix is predicted by means of the hRD, h2RD and h3RD parity bits and they are expressed by the equation as follows:

h0,j = h2RD[a0,j] h3RD[a1,j] hRD[a2,j] hRD[a3,j]
h1,j = hRD[a0,j] h2RD[a1,j] h3RD[a2,j] hRD[a3,j]
h2,j = hRD[a0,j] hRD[a1,j] h2RD[a2,j] h3RD[a3,j]
h3,j = h3RD[a0,j] hRD[a1,j] hRD[a2,j] h2RD[a3,j] 0 < j <4

Once the position of the faulty bit is identified, then that bit is flipped in the fault correction technique. The encryption is then continued without any interruption. The Hamming code tables are protected from SEUs by using memory protection techniques in satellite applications like memory scrubbing and refreshing.

7 RESULTS

From the synthesis result, the comparison of area requirement on CYCLONE II EP2C35F672C6 is given in table 1.

	LUT based S-box	High Throughput-low area S-box
Total LE(33,216)	208	99
Total combinational functions (33,216)	208	99
Logic registers(33,216)	8	16

Table-1: Comparison of area requirement

The simulated output for the S-box by applying affine transformation and multiplicative inverse is shown in fig-7

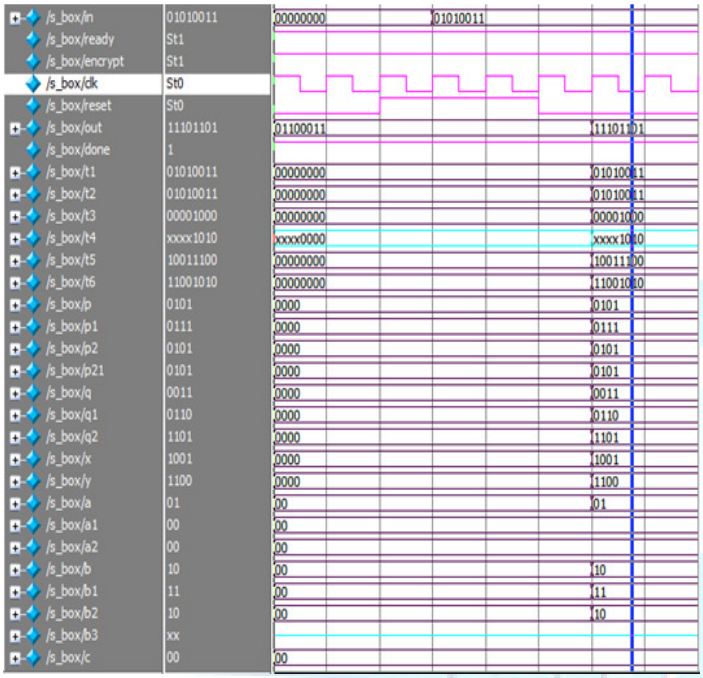

Fig-7: Simulated output for Sub Bytes

The simulated output for AES algorithm is shown in fig-8.

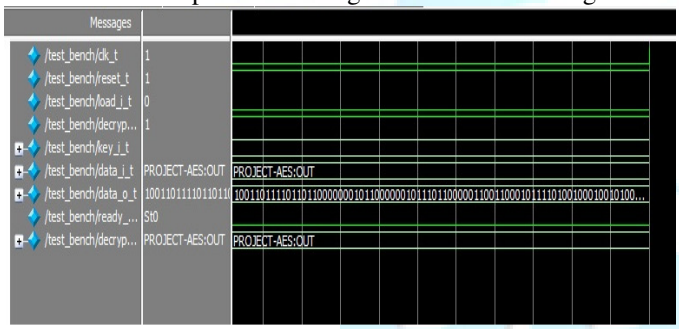

Fig-8: Simulated output for AES Encryption

The output for the error detection and correction using Hamming code is as follows. Fig-9 denotes the output that should be obtained. In Fig-10, it shows that it detects the error and corrects automatically by means of Hamming code.

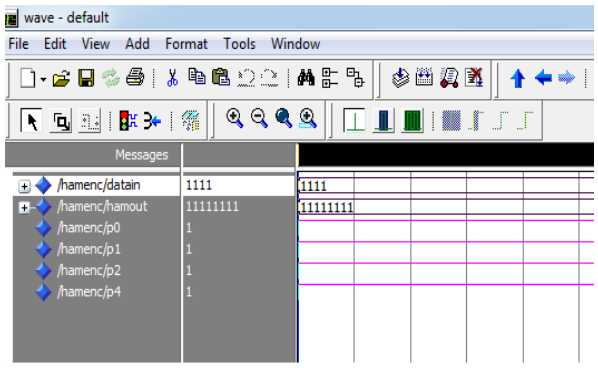

Fig-9: Simulated output without error

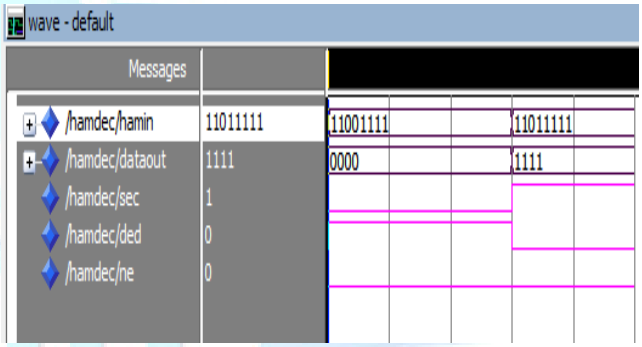

Fig-10: Simulated output for error detection and correction

CONCLUSION

Thus the high throughput S-box has been designed which minimize hardware size. In comparison with the existing method, the throughput of the proposed s-box has been increased. This work includes the derivation of a new composite field AES S-box to achieve an optimally balanced construction in terms of area and critical path. The proposed work includes the capability of detecting and correcting the errors using hamming code. The applications of these techniques are satellite communication in which Single Event Upset can be neglected.

REFERENCES

[1] Jemima Anlet P, Jagadeeswari M, "Parity Based Fault Detection Approach for the Low Power S-Box and Inverse S-Box," International Journal of Computer Technology and Electronics Engineering (IJCTEE), ISSN 2249-6343,Volume 2, Issue 2, 2012

[2] Pitchaiah M, Philemon Daniel, and Praveen, "Implementation of Advanced Encryption Standard Algorithm," International Journal of Scientific & Engineering Research, ISSN 2229-5518, Volume 3, Issue 3, March 2012.

[3] PriyankaPimpale, RohanRayarikar, SanketUpadhyay, "Modifications to AES Algorithm for Complex Encryption," IJCSNS International Journal of Computer

Science and Network Security, Vol.11 No.1 0, October 2011.

[4] Rahimwmisa K, Sureshkumar S, and Rajeshkumar K, "Implementation of AES with New S-Box and Performance Analysis with the Modified S-Box," International Conference on VLSI, Communication & Instrumentation(ICVCI) Proceedings published by International Journal of Computer Applications (IJCA), 2011.

[5] Subashri T, Arunachalam R, GokulVinoth Kumar B, and Vaidehi V, "Pipelining Architecture of AES Encryption and Key Generation with Search Based Memory," International journal of VLSI design & Communication Systems (VLSICS), Vol.1, No.4, December 2010.

[6] Wong M.M. Wong M.L.D. Nandi A.K. and Hijazin I. "Construction of Optimum Composite Field Architecture for Compact High-Throughput AES S-Boxes" IEEE Trans. Very Large Scale Integer.(VLSI) systems,vol.20., No.6, 2012

[7] SupratimSaha, "Low Power AES Algorithm Implementation For Wireless Communication," International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 2 Issue 8, August 2013