International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Detect and Correct Single Event Upset of the AES Algorithm in On Board Satellite

Md. Riyaj[1], Vipin Gupta[2]

[1]M. Tech Scholar, Suresh Gyan Vihar University, Jaipur, India
[2]Assistant professor, Suresh Gyan Vihar University, Jaipur, India

Abstract: ***The AES cryptography algorithm can be used to encrypt /decrypt blocks of 128 bits and is capable of using cipher keys of 128, 196 or 256 bits wide (AES 128, AES 196 and AES 256). The AES can be implemented in either software or hardware. The AES is a symmetric key algorithm in which both the sender and the receiver use a single key for encryption & decryption. The encrypted satellite data can get corrupted before reaching the ground station due to various faults. One major source of fault is the harsh radiation environment, Therefore any electronic system used on board satellites such as processors; memories are very susceptible to faults induced by radiation. In this paper we analyzed the propagation of faults that occur during transmission due to noise is carried out in order to avoid data corruption and faults are rectified by using hamming Error correction code algorithm. This reduces the data corruption and increases the performances as a result.***

Keywords: AES, DES, SEU, TWOFISH

1. Introduction

The meaning of the cryptography in the past is only encryption and decryption using secret keys. But now a days modern cryptography means asymmetric-key cryptography (public-key cryptography) and symmetric key cryptography (called as private-key cryptography). Only one key is used in private key algorithms both for encryption and decryption where as two key is used in public key algorithms both for encryption and decryption. A no. of cryptographic algorithm such as DES, ECC, advanced encryption algorithm, twofish algorithm, blowfish algorithm and other algorithms [1] . The advanced encryption standard (AES) is the important published cryptographic algorithms. Many computations cycles is required in AES algorithm. AES uses four operations in different rounds such as sub bytes, shift rows, mix columns and additional key round transformations. In military satellites, security is essential. In satellite fault tolerance is very important. Due to radiation fault is induced in the on board electronic systems such as memories, processors etc. before sending the data to ground faults must be detected and corrected. If ground station receives faulty data the users request for data retransmission. Due to radiation, single bit flips called single event upsets (SEU) is induced in satellite on board electronic devices. In the 1960's the IBM researcher team researches on one project and result of this project was cipher and this cipher is known as LUCIFIER. In 1977 this cipher was finally adopted as the data encryption standard. 128 bit key size used in LUCIFIER and this key size reduced to 56 bits for data encryption standard. DES receives 64 bit key as input and the last eight bits are used for parity checking. DES is based on Feistel block cipher. In the early 70^{s} IBM researcher HORST FEISTEL developed a block cipher which is known as feistel block cipher. Feistel block cipher consist of a number of operations such as bit shuffling, non linear substitutions (s-boxes) and exclusive OR operations. All operations are in one round. DES receives two inputs –the plain text and the secret key. DES is a symmetric key cryptography in which only one key is used for both encryption and decryption.

2. Literature Review

DES block cipher encrypts data [2] 64 bits at a time. The DES algorithms have three different types of operations Rotations, Substitutions and initial and final permutations. The DES algorithm performs 16 rounds (rotations) of a function between initial and final permutations. Each rotations consists permutations and substitution of the text bit and the inputted key bit, and final permutation to get 64 bit cipher text. The DES algorithm is not successful due to its low security. In DES algorithm high security is obtained by increasing the number of rotation.

Twofish [1] algorithm is based on a feistel network and can receive a key upto 256 bits. Two fish algorithms has four key 8 by 8 bit s-boxes, a fixed 4 by 4 maximum distance, a pseudo-hadamard transform key schedule and bitwise rotations. AES for advance encryption standard which is based on robust security properties. It is very easy to implement in both hardware and software. In public key cryptography, a modern branch of cryptography in which a pair of key known as public key and private key is used for encryption and decryption respectively. AES algorithm is based on symmetric key cipher in which a single key is used by sender and receiver for encryption and decryption. AES basically an iterative algorithm. Each repetition is called a round. There are 10, 12 and 14 rounds for the key lengths 128, 192 and 256 respectively. The use of large key size increase the cryptographic strength but it requires a greater number of processing rounds. Generally 128 bit AES is enough for most of the purpose and it is commonly used. It requires two rounds for process 128 bit data block slit into 16 bytes. These bytes are mapped to a 4*4 matrix called the state. Internal functions of AES algorithm depend on the state. Full implementation of AES is divided into two parts: one is the cipher and other is key expander. Cipher performs encryption and decryption on clocks of input data, while key expander component is responsible for preparing input key for use by cipher.

Substitution and permutation operations are used in each round to transmit the input data. Except the final round,

each round in AES is composed of 4 transformations: subBytes, ShiftRows, Mixcolumns and AddRoundKey during encryption. The final round does not have mixcolumns transformation while in decryption, InvsubBytes, InvshiftRows, InvmixColumns and Addroundkey are used. The following table illustrated the variation of AES algorithm A modern branch of cryptogarhy which is used in the public and private sector in different pair of element and different steps of algorithm. On case of AES algorithm it is a symmetric key chipper in which both the transmitter and the receiver use a single key use for encryption and decryption here encryption means to change the data in the code forms. And decryption means remove the coded form and receive the original data. Data block length is fixed it is 128 bit. And the key length can be 128, 192, 256 bit respectively [5]. The 128 bit data block is divided by 16 bytes in mapped 4*4 array or matrix called state [4]. Notations conventions and mathematical background: The data block length in the AES algorithm is 128 bit in the receiver and the transmitter. The sequences decide the block and the number of bits decides the length.

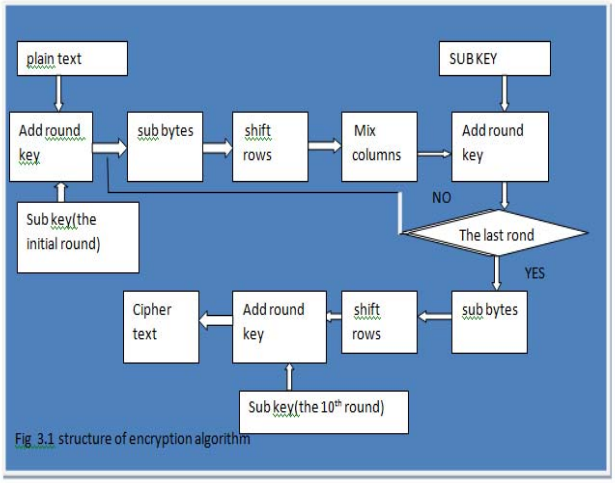

Figure 2.1: The structure of encryption algorithm

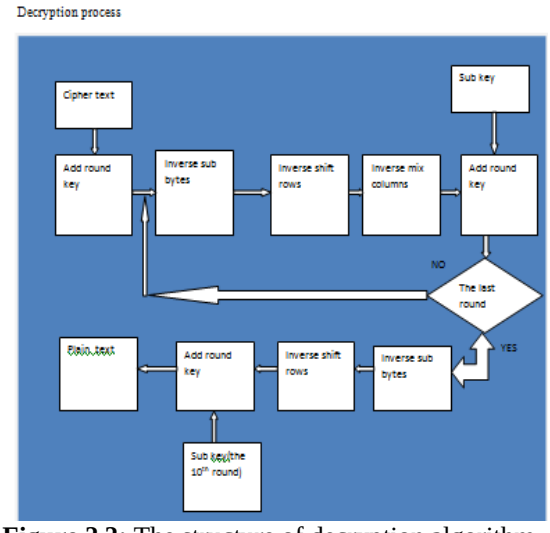

Figure 2.2: The structure of decryption algorithm

2. 1 Encryption

Sub bytes Transformation:

The sub bytes transformation is done by using the s-box (substation box) LUT (look up table).

Shift rows (Permutation)

In the shift row transformation, the first row is not shifted, second, third, and fourth row are shifted by one, two and three bytes to the left respectively.

Figure 2.3: Shift Rows

Mix Column Transformation

Obtained shift row matrix is multiplied with a constant matrix to produce a new output matrix (d_{ij}). Mix column transformation functions on [5] the state column by column, considering each column as a four-term polynomial.

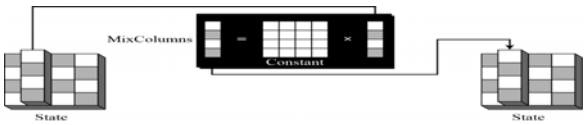

Figure 2.4: Block diagram of Mix column transformation

Add Round Key Transformation

In this transformation, the state matrix is xored with the expended round key. The initial key (128 bits) arranged in a 4*4 matrix. Each column in [6] the matrix is treated as a one word. i. e 4*4 matrix consists of 4 words or 4 columns. By using key expansion algorithm, the original key is expended to 40 more words or columns.

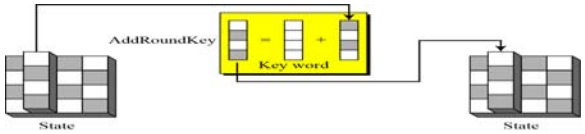

Figure 2.5: Block diagram of Add round key

2.2 Decryption

Inverse Bytes Substitution Transformation

Inverse sub byte is the inverse of the sub byte transformation, in which inverse s box is applied to each byte of the state. Inverse bytes substitution is obtained by inverse affine transformation and multiplicative inverse in GF (2^8).

Inverse Mixing of Columns Transformation

Inverse mixing of columns transformation is the inverse of the mix column transformation. State matrix is multiplied with a constant matrix to produce a new output matrix (d_{ij}). Inverse Mix column transformation functions on the

state column by column, considering each column as a four-term polynomial similar to mix column transformation.

$$\begin{bmatrix} d_{00} & d_{01} & d_{02} & d_{03} \\ d_{11} & d_{12} & d_{13} & d_{10} \\ d_{22} & d_{23} & d_{20} & d_{21} \\ d_{33} & d_{30} & d_{31} & d_{32} \end{bmatrix} = \begin{bmatrix} c_{00} & c_{01} & c_{02} & c_{03} \\ c_{10} & c_{11} & c_{12} & c_{13} \\ c_{20} & c_{21} & c_{22} & c_{23} \\ c_{30} & c_{31} & c_{32} & c_{33} \end{bmatrix} \otimes \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

Figure 2.6: Inverse Mix Columns

3. Purposed Hamming Tolerant Model

3. 1 Model Description

The purposed model is based on single error correcting Hamming code. A single bit fault [8] in a byte is detected and corrected by Hamming code. At the end of the each transformation the hamming code is predicted from the Hamming code table. The EDC (error detection and correction) model is based upon the predicting the hamming code bits at the end of each transformation from hamming code memory table.

3. 2 Hamming Code Calculation

The hamming code of the each byte of the S-ox look up table is stored in the hamming code memory. Following are the procedure to calculate the hamming code bits. The parity check bits of each byte of the s-box look up table are pre-calculated.

h (SRD [a])--> hRD [a] (A)
h ((SRD [a] f{2g})--> h2RD [a]

Where a=state byte

h ((SRD [a] f{03g})--> h3RD [a] (1)

h=calculation represent humming code

h_{RD}, h_{2RD} and h_{3RD} is the Hamming code of the S-box LUT (S_{RD}), (S_{RD}@{02}) and (S_{RD}@{03}) respectively.

Each state byte can be represented by bits b_0, b_1, b_3, b_4, b_5, b_6, b_7, b_8. 4-bit hamming code of the state byte is represented by bits (h_3, h_2, h_1, h_0)

$H_3 = b_7$ xor b_6 xor b_4 xor b_3 xor b_1
$H_2 = b_7$ xor b_5 xor b_4 xor b_2 xor b_1
$H_1 = b_6$ xor b_5 xor b_4 xor b_0
$H_0 = b_3$ xor b_2 xor b_1 xor b_0

The hamming code for S_{RD} table are pre-calculated and stored in the hamming memory table (known as h_{RD} table).

The h_{2RD} table is obtained by the parity check bits of (S_{RD}× {02}). The galois field multiplication of a state byte, a, with {02}.

h_{2RD} = h ({02}× a)

The h_{3RD} table is obtained by the parity check bits of (S_{RD}× {03}). The galois field multiplication of a state byte, a, with {03}.

H_{3RD} = h ({03}× a) = h_{RD} XOR h_{2RD}

Hence by using h_{2RD} and h_{RD} we can calculate h_{3RD} table. Finally when we get all the hamming bits, the next action is to detect &correct the faults by predicted hamming code bits.

3.3 Fault Detection and Correction

The Hamming code sub byte transformation matrix is obtained (predicted) by h_{RD} table [8] . The Hamming code shift rows transformation matrix is obtained by simple cyclic rotation of the Hamming code sub byte transformation matrix. The Hamming code mix column transformation matrix is predicted by with the help of just two tables h_{RD} and h_{2RD}. for each transformation predicting Hamming code is obtained by using the parity check bit tables and also the Hamming code is calculated from the output of the transformation. By comparison of predicted and calculated Hamming code we can detect and correct fault as mentioned below.

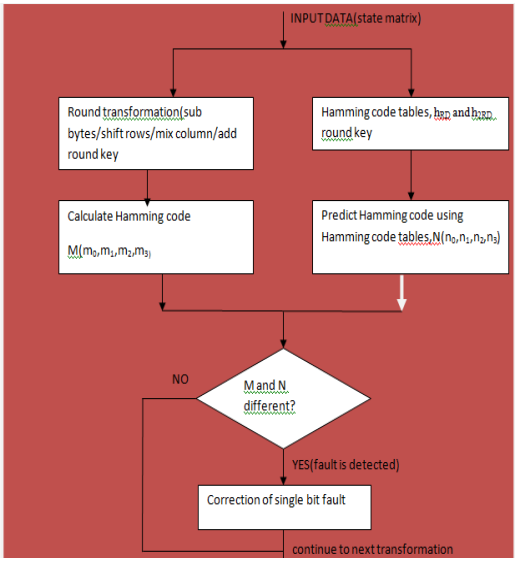

Figure 3.1: Hamming Fault Detection Model

Let the predicted check bits of the transformation input be showed by (m_3, m_2, m_1, m_0) and calculated check bits of the transformation output be showed by (n_3, n_2, n_1, n_0). By comparison of predicted and calculated Hamming check bits location of faulty bit is detected using the table 3. 1. Once the position of faulty bit is identified the fault correction is done by flipping that bit and then encryption process is continued.

Table 3.1: Hamming code Bit Match Table to Locate a Faulty Bit

Hamming code bits comparision	Faulty bit position in output
$(m_3,n_3)\&(m_2,n_2)$	0
$(m_3,n_3)\&(m_1,n_1)$	2
$(m_3,n_3)\&(m_0,n_0)$	5
$(m_2,n_2)\&(m_1,n_1)$	3
$(m_2,n_2)\&(m_0,n_0)$	6
$(m_1,n_1)\&(m_0,n_0)$	7
(m_1,n_1)	1
(m_0,n_0)	4

4. Simulation Result

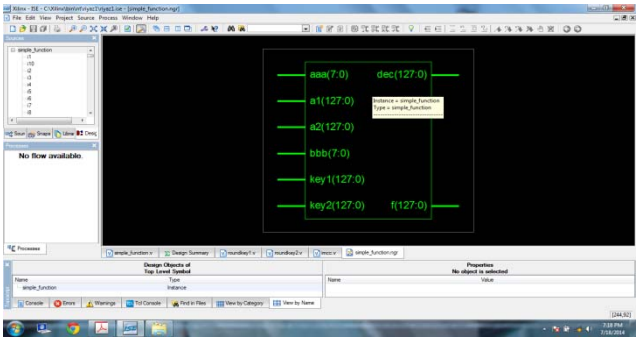

Figure 4.1: RTL Diagram for encryption and decryption

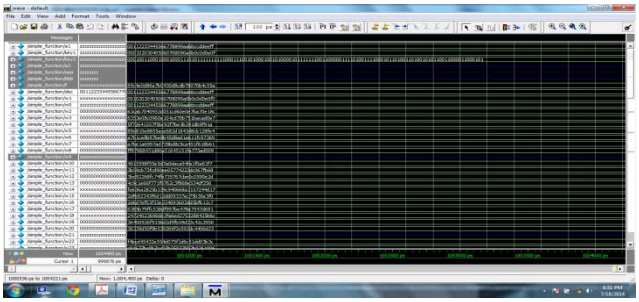

Figure 4.2: Simulation result for encryption and decryption

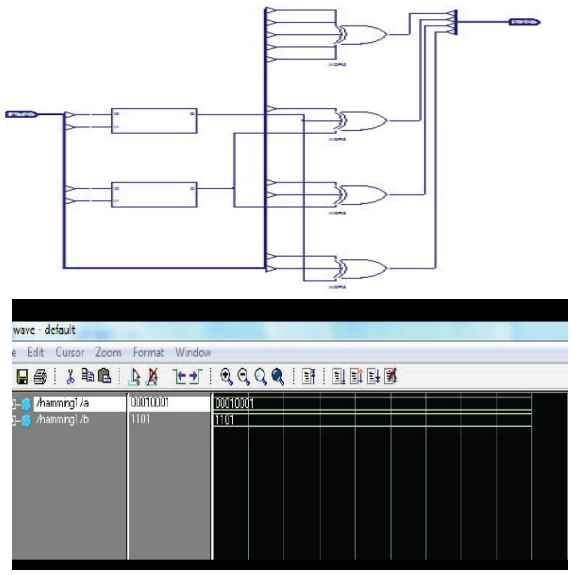

Figure 4.3: RTL Diagram for Hamming code calculation

5. Conclusion and Future Work

5. 1 Conclusion

This paper presents a unique research method of cryptographic algorithms for satellite communication. Satellite operates in radiation environment and encryption processor is sensitive to radiation and due to radiation induced faults. so the encryption algorithm should be free from radiation. to achieve error free encryption, a fault tolerant model has been proposed in this paper.

5.2 Future Work

The proposed model will detect and correct single bit errors. However this model can be extended for multiple bit errors during encryption by using hamming code, Reed-solomon codes etc. This paper was planned to connect the fault tolerant AES IP core to the LEON processor through the bus. But thesis area of research was not covered because of lack of time. The purposed model is internal to the AES algorithm. This model can be extended to implement an EDAC function that is external to the AES algorithm.

References

[1] Horatiu Paul “Twofish Encryption algorithm” conference proceeding 2004
[2] Amandeep Singh “FPGA implementation and analysis of DES and Twofish Encryption algorithms” Thaper university Patiyala, 2010
[3] A. RuhanBevi “an effective symmetric key recovery scheme for secure onboard satellite applications” in IJCSI journal 2011
[4] Mg Suresh “area optimized and pipelined FPGA implementation of AES encryption and decryption” in IJCER volume 2 Issue 7, 2012
[5] AMANDEEP KAMBOJ “high speed parallel concurrent error detection scheme for robust AES hardware” IJAREEIE Volume 2, Issue 10, October 2013
[6] SUMALATHA PATIL “Design of High speed 128 bit AES algorithm for data Encryption” IJCET special issue September 2013
[7] AMRUTHA K” advanced encryption standard algorithm implementation using Verilog HDL” IJVES Volume 4 article 6 July 2013.
[8] PRAVEEN. H. L. “satellite image encryption using AES” IJCSEE Volume 1, Issue 2, 2012
[9] Archana Garg “ efficient field programmable gate array implementation of advanced encryption standard algorithm using VHDL” Volume 4, Issue 9, September 2013
[10] Vinoth Vijay “ high performance fault detection and correction scheme for advanced encryption standard” IJSETR Volume 2, Issue 4, April 2013

Author Profile

Md. Riyaj received the B. E. degrees in Electronics and Communication Engineering from JNIT Jaipur and currently doing M-Tech VLSI in Suresh Gyan Vihar University Jaipur.

Vipin Gupta received his B. E degree in Electronics and Communication Engineering from SBCET Jaipur in 2009 and M-Tech degree in VLSI from MNIT Jaipur in 2011. He is currently working as a assistant professor in department of electronics and communication Engineering at Suresh Gyan Vihar University Jaipur.