Design and Analysis of AES-CBC Mode for High Security Applications

M.Vaidehi
Research Scholar,
Karpagam University,
Coimbatore.

Dr. B.Justus Rabi
Principal,
Toc H Institute of Science & Technology.
Arakkunnam, Ernakulam, Kerala, India.

Abstract— **The challenge in securizing communications networks is to obtain flexible means able to deal with the intensive computation needed by the cryptography algorithms. A representative example of this algorithm is the Rijndael. The 128-bit AES block cipher combines a 128-bit key and a 128-bit plaintext data block to get a 128-bit block of cipher text data. The Electronic Code Book (ECB) mode is the simplest encryption mode. In this mode, the message is split into blocks and each one is separately encrypted. So, therefore identical plaintext blocks are encrypted to identical cipher text blocks. This drawback generates vulnerabilities like modification of ciphered messages. In order to solve this problem, more complex modes of operation combine the data of the previous ciphered blocks and use Initialization Vectors (IV) to make each ciphered message unique. The AES Cipher-Block Chaining (CBC) mode includes these features. Before encrypting a block, it is XORed with the cipher text of the previous cipher text block. In this paper, the design and analysis of AES-CBC mode is presented to find the fault during the encryption process. Simulation is performed to analyze the chip size reduction**

Keywords **- AES, CBC mode, Initialization Vectors, Electronic Code Block**

I. INTRODUCTION

Earth observation (EO) satellites take images of the Earth with smart and sophisticated imaging sensors. Multispectral images of the Earth captured by optical on-board cameras can be used in monitoring of the environment and disasters, vegetation control, map marking, urban planning, etc. The latest trend now is towards small EO satellites, as they require smaller budgets to build and launch and also involve less maintenance costs [1]. A typical EO small satellite weighs approximately 100 kg and the orbit average power generated by solar panels is 30 to 60 W. The imaging payload units of such satellites comprise imagers, mass memory, and high-rate data transceivers and consume up to 70% of the average orbit power. At present, more and more EO satellites are equipped with on-board encryption to protect the data transmitted to the ground station. However due to confidentiality and security reasons the coverage of this topic in the open literature is very limited [3].

Encryption, by far the most widely adopted security service in terrestrial networks, is used to protect data from unauthorized users. Although there are many encryption products and algorithms, the use of these products and algorithms on-board satellites has been overlooked until recently. But now satellite manufacturers are realizing the importance of on-board encryption to protect valuable data, especially after cases, which have proved that intrusion into satellite data is not an impossible task. At present, more and more EO satellites are equipped with on-board encryption to protect the data transmitted to the ground station. Ever since DES was phased out in 2001 and its successor, the Advanced Encryption Standard (also known as Rijndael) took its place, various AES implementations have been proposed both in software and hardware [2].

The Rijndael algorithm approved as the Advanced Encryption Standard (AES) by the US National Institute of Standards and Technology (NIST) is a block cipher, which encrypts one block of data at a time. To encrypt multiple blocks, modes of operation have been defined by NIST. AES is being adopted by many organizations across the world. Because of its simplicity, flexibility, easiness of implementation, and high throughput AES is used in many different applications ranging from smart cards to big servers. In fact, hardware implementations of AES are well suited to resource-constrained embedded applications like satellites [5].

There are various hardware implementations of the AES algorithm on platforms like application specific integrated circuits (ASICs) and field programmable gate arrays (FPGAs) that achieve a significant throughput ranging from a few Mbit/s to Gbit/s.Thus the requirements of small EO satellites for high-rate data transmission are met by existing AES implementations. However, in addition to high throughput, immunity of the encryption process against faults is very important in satellites. Satellites operate in a harsh radiation environment and consequently any electronic system used on board, including the encryption processor, is susceptible to radiation-induced faults. Most of the faults that occur in satellite on-board electronic devices are radiation-induced bit flips called single event upsets (SEUs).If faulty data is transmitted to the ground station, the user's request for data retransmission has to wait until the next satellite revisit period, with revisit time varying from a couple of hours to weeks. In order to prevent faulty data transmissions, there is a need for an error-free encryption scheme on board.

IEEE Conference Number - 33344
July 8, 2014, Coimbatore, India.

Satellite data can further get corrupted during transmission to ground due to noise in the transmission channel. The impact of radiation on semiconductor devices on board depends on orbit altitude, orientation, and time. Reliability is the most important issue in avionics design. SEUs must be detected and corrected on board before sending the data to ground. The triple modular redundancy (TMR) technique is one of the most widely used redundancy-based SEU mitigation techniques in satellites. A TMR design consists of three identical modules, which are connected by a majority voting circuit to determine the output. However, with the TMR technique the area and power overheads triplicate in comparison with the original module. This paper addresses reliability issues of the AES algorithm. A detailed analysis of the impact of faults during on-board encryption and during transmission for the AES-CBC mode is presented [4].

II. ADVANCED ENCRYPTION STADARD–LGORITHM AND MODES OPERATION

The AES is a symmetric key algorithm, in which both the sender and the receiver use a single key for encryption and decryption. AES defines the data block length to 128 bits, and the key lengths to 128,192, or 256 bits. It is an iterative algorithm and each iteration is called a round. The total number of rounds, Nr, is 10, 12, or 14 when the key length is 128, 192, or 256 bits, respectively [9]. Each round in AES, except the final round, consists of four transformations: Sub Bytes, ShiftRows, MixColumns, and AddRoundKey [3]. The final round does not have the MixColumns transformation the decryption flow is simply the reverse of the encryption flow and each operation is the inverse of the corresponding one in the encryption process. The round transformation of AES and its steps operate on some intermediate results, called state. State can be visualized as a rectangular matrix with four rows. The number of columns in the state is denoted by Nb and is equal to the block length in bits divided by 32. For a 128 bit data block (16bytes) the value of Nb is 4, hence the state is treated as a 4×4 matrix and each element in the matrix represents a byte. For the sake of simplicity, in the rest of the paper, both the data block and the key lengths are considered as 128 bit long. However all the discussions and the results hold true for 192 bit and 256 bit keys as well [8].

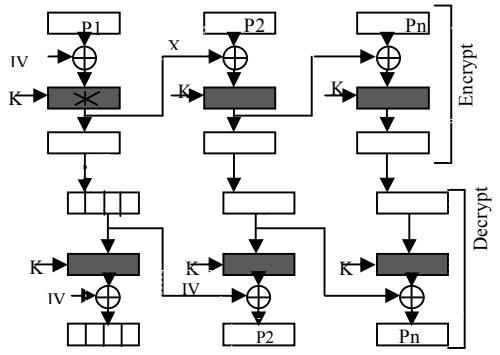

Figure 1. Fault Propagation during encryption in AES-CBC mode.

III. FAULT PROPAGATION ANALYSIS

Due to fault propagation even a single bit error during encryption of one block of AES can result in corruption of 50% of the bits in the final encrypted data on average. In addition, when using the AES feedback modes faults occurring in one block can propagate to other blocks because of the feedback. In this section propagation to subsequent blocks of single bit faults occurring both during encryption and during transmission is investigated.

A. Fault Propagation in AES-CBC Mode

Cipher Block Chaining Mode: The CBC mode, illustrated in Fig. 3, is the mode in which the plain data block is XOR-ed with the cipher data of the previous block before it is encrypted. The first block is XOR-ed with an initial vector (IV), which is a random number. In Fig.2, P1,P2…. Pn represent the plain data, C1, C2….Cn represent the cipher data and K is the key used in both encryption and decryption. The plain data blocks, the cipher data blocks, and the key are of 128 bit length each. The "E" and "D" blocks in Fig.2 denote an encryption and decryption function using the AES algorithm, respectively [9].

The effect of an SEU during encryption in the CBC mode is illustrated in Fig.2, where the SEU occurrence is marked by the star symbol * and the corrupted data blocks are represented by black boxes. If an SEU occurs while encrypting the plain block P1, the cipher block C1 will be corrupted and hence the decrypted block P1 will also be corrupted. However, this corrupted data is not propagated to the subsequent blocks despite the feedback. The reason for this is that the corrupted cipher block C1 is XOR-ed twice (with the plain block P2 before encryption and with the cipher block C2 after decryption) as shown in Fig.2.Performing the XOR operation two times with this corrupted cipher block C1 neutralizes the fault and prevents propagation of faults to subsequent blocks as shown below:

$$P \oplus X \oplus X = P \qquad (5)$$

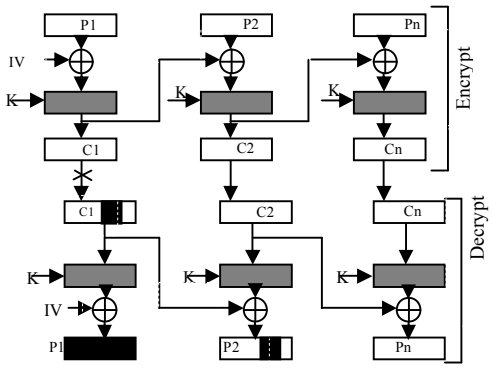

Figure 2.Transmission Fault Propagation in CBC mode

IEEE Conference Number - 33344
July 8, 2014, Coimbatore, India.

In contrast, a fault occurring in an encrypted block during transmission propagates to the next block, as shown in Fig.3, where the transmission fault is shown by the star symbol during the transmission of the cipher block C1. The decrypted block P1 is completely garbled and the subsequent decrypted block P2 will have bit errors at the same positions as the original erroneous block C1.The decrypted blocks following the second block will not be affected by the fault. Hence the CBC mode is self synchronizing [6].

IV. FAULT-TOLERANT MODEL OF THE AES ALGORITHM

This section presents a novel fault-tolerant model for the AES algorithm, which is immune to radiation-induced SEUs occurring during encryption and can be used in hardware implementations on-board small OE satellites. The model is based on a self-repairing EDAC scheme, which is built in the AES algorithmic flow and utilizes the Hamming error correcting code. The proposed Hamming code based fault-tolerant model of AES can be adapted to all the five modes of AES to correct SEUs on board. Even though the calculation of the Hamming code is carried out within the AES it does not alter any of the transformations of the algorithm and does not affect in any way the operation of AES. The disadvantage of this method is that the implementation of the codes based EDAC will require an additional encoding stage to encode the plain data blocks to code-word symbols which will inevitably add an overhead to on-board resources and processing.

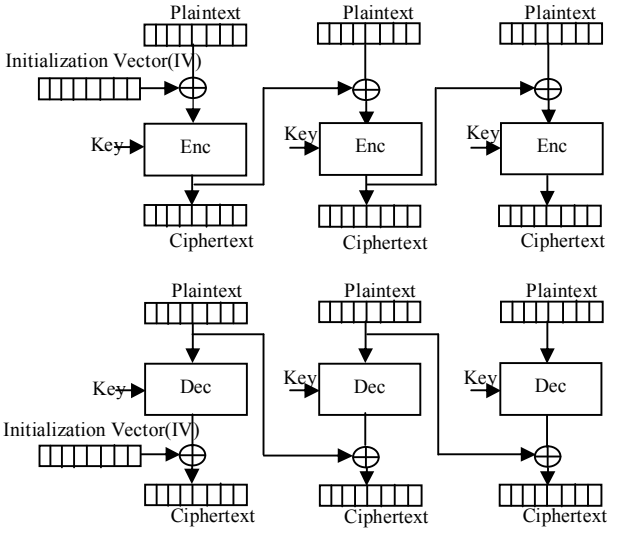

Figure 3. Cipher Block Chaining mode encryption and decryption

A. Software Simulation

In EO satellites high throughput encryption processing is required to comply with high-rate data transmission bandwidth of up to a few hundred Mbit/s . In order to meet the requirement for high throughput processing, hardware implementation is considered to be the preferred choice on board satellites. The Verilog hardware description language (HDL) is used for the coding, and ModelSim is used for the functional, presynthesis, and post synthesis simulations of the design. The HDL designs are tested extensively using the KAT and MCT vectors by NIST. Synthesis and implementation are carried out using Synplify and Xilinx ISE, respectively.

Table 1: Area of AES-CBC Mode

Modes	LUT	Slices
AES-CBC (Encryption)	794	433
AES-CBC (Decryption)	1323	700

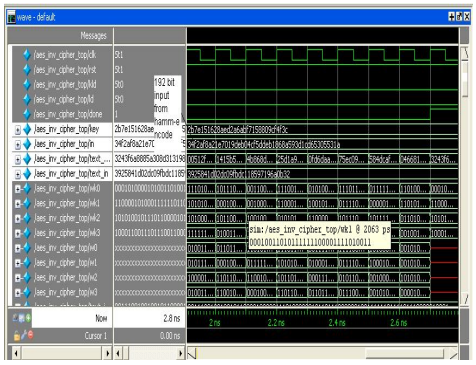

Figure 4. AES encryption using ModelSim.

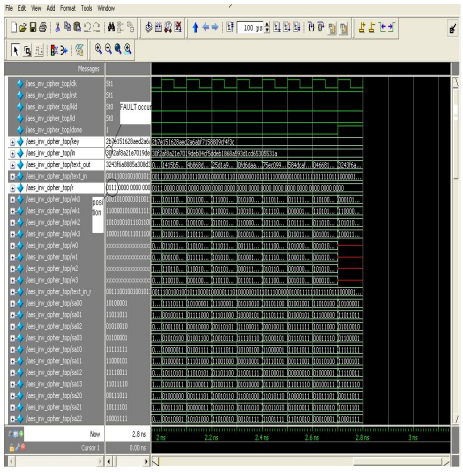

Figure 5. AES fault detection and correction using Hamming Code.

IEEE Conference Number - 33344
July 8, 2014, Coimbatore, India.

V. CONCLUSION AND FUTURE WORK

This paper examines the trustworthiness of the AES algorithm for employ on board EO small satellites. The AES mode CBC, was conversed in specify the impact of the propagation of SEU errors happening during on-board encryption is examined. In adding together, an examination of the Propagation of errors that occur during transmission due to noise is carried out. So as to keep away from data corruption because of SEUs, a fault detection and correction model of AES is presented based on the Hamming code (12, 8). The model offers an SEU self-recovering capability, which is built in the AES data path. Also it consumes a less amount of the power accessible to the payload unit. The predictable hardware overhead of the best fault-tolerant AES in terms of area .The model can be enlarged for detection and correction of multiple bit faults by using other new complicated error-correcting codes such as modified Hamming code, etc.The proposed fault detection and correction AES model aims the satellite application domain, though it can also be used in other applications aimed at hostile environments like , interplanetary exploration, nuclear reactors unmanned aerial vehicles, etc. Terrestrial applications, which need sophisticated of reliability, such as bank servers, telecommunication servers, etc. can advantage from the use of AES fault-tolerant techniques also.

REFERENCES

[1] Sun, W., Stephens, P., and Sweeting, M. N. Micro-minisatellites for affordable EO Constellations–Rapid Eye and DMC. In Proceedings of the IAA Symposium on Small Satellites for Earth Observation, Berlin, Germany, Apr. 2001, IAA-B3-0603.

[2] Surrey Satellite Technology Ltd. www.sstl.co.uk (last accessed on 18th June 2007).

[3] Directory of Earth Observation Resources. http://directory.eoportal.org/pres TopSat.html (last Accessed 18th June 2007).

[4] Sweet, K. The increasing threat to satellite communications. Online Journal of Space Communication, 6 (Nov. 2003).

[5] Mariani, R., and Boschi, G. Scrubbing and partitioning for protection of memory systems. In Proceedings of the 11th IEEE International Symposium on On-Line Testing, July 6—8, 2005, 195—196.

[6] S. Kim, Ingrid Verbauwhede, "AES implementation on 8-bit microcontroller," Department of Electrical Engineering, University of California, Los Angele s, USA, September, 2002.

[7] Guido Bertoni, Luca Breveglieri, Israel Kor "Error Analysis and Detection Procedures for a Hardware Implementation of the Advanced Encryption Standard", IEEE transactions on computers, vol. 52, no. 4, april 2003

[8] Ramesh Karri, Kaijie Wu, Piyush Mishra, and Yongkook Kim, "Concurrent Error Detection Schemes for Fault-Based Side-Channel Cryptanalysis of Symmetric Block Ciphers", IEEE transactions on computer-aided design of integrated circuits and systems, vol. 21, no. 12, December 2002

[9] HyeopgeonLee, KyounghwaLee, YongtaeShin, "Implementation and performance Analysis of AES-128CBC algorithmic WSNs", Feb.7-10, 2010 ICACT 2010.