ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.2, Pages : 92-94 (2013)
Special Issue of NCRTECE 2013 - Held during 8-9 February, 2013 in SMK Fomra Institute of Technology, OMR, Thaiyur, Kelambakkam, Chennai

Efficient Fault Detection Scheme for Advanced Encryption Standard

[1] Harishkumar M.N., [2] Vigneshraja B. .,
[1] M.E- Student VelTech Multitech Dr.Rangarajan Dr.Sakunthala Engg College
E-mail:harishmanekkia@gmail.com, Phone No: 7871000088
[2] Asst Professor VelTech Multitech Dr.Rangarajan Dr.Sakunthala Engg College
E-mail:vigneshraja.b@gmail.com, Phone No: 9003739187

Abstract **—** The faults that occur in the hardware implementations of the Advanced Encryption Standard (AES) may cause incorrect encrypted/decrypted output. The use of appropriate fault detection schemes for the AES makes it vigorous to inner defects as well as fault attacks. In our paper, we present a lightweight concurrent fault detection scheme for the AES. In the proposed approach, the composite field S-box and inverse S-box are divided into blocks and the projected parities of these blocks are obtained. Through exhaustive searches, we have found the optimum solutions for the least overhead parity-based fault detection structures. This is a low-cost parity-based fault detection scheme for the S-box and the inverse S-box using composite fields. For increasing the error coverage, the predicted parities of the five blocks of the S-box and the inverse S-box are got. The cost of our multi-bit parity prediction approach is lower than which use single-bit parity. It also has higher error coverages. We have implemented both the proposed fault detection S-box and inverse S- box and other Counter parts in Advanced Encryption Standard. The complexities of the proposed fault detection scheme are lower.

Index Terms – AES, Composite fields, error-coverage, fault detection

I. INTRODUCTION

Among them, the schemes presented in are independent of the ways the AES S-box and inverse S-box are implemented in hardware. Moreover, there exist other fault detection schemes that are suitable for a specific implementation of the S-box and the inverse S-box. The approach in and the one in which is extended in are based on using memories (ROMs) for the S-box and the inverse S-box. Moreover, a fault tolerant scheme which is resistant to fault attacks is presented in. It is noted that our proposed fault detection approach is only applied to the composite field S-box and inverse S-box whereas; the scheme presented is using memories. Using ROMs may not be preferable for high performance AES implementations. Therefore, for applications requiring high performance, the S-box and the inverse S-box are implemented using logic gates in composite fields.

Through exhaustive searches, we obtain the least area and delay overhead fault detection structures for the optimum composite fields using both polynomial basis. In this work, we will focus on fault attacks against the Advanced Encryption Standard (AES).It is showed that a couple of encryptions, affected by a generic byte error injected before the MixColumns operation, can be enough to recover the 128-bit secret key. This is possible since the remaining operations do not interfere with each other, thus the whole resulting output can be easily exploited to build an equation system in the last round key and in the error values. Then, the fact that AES uses an invertible key scheduler allows one to compute the initial secret key easily. The attack relies on a commonly accepted fault model. The attacker is able to control the timing and the location of the fault, but he has little influence on the actual error value. We have implemented the proposed fault detection S-box.

II. PROPOSED SYSTEM

S-BOX AND THE INVERSE S-BOX STRUCTURE

Optimum structures consist of those of the optimum parity predictions. In addition, 23 XORs for the actual parities (3 XORs for adding the coordinates and 7 XORs) are utilized. Implementation complexities of different blocks of the S-box and the inverse S-box and those for their predicted parities are dependent on the choice of the coefficients and in the irreducible polynomials and used for the composite fields. The area complexity of the entire fault detection implementations becomes optimum. We have exhaustively searched and have found the possible choices for making the polynomial irreducible. These parameters determine the complexities of some blocks.

TRANSFORMATION MATRICES

S-box and the inverse S-box can be constructed using the Exhaustive algorithm. Using an exhaustive search, eight base elements in (or) to which eight base elements of are mapped, are found to construct the transformation matrix. the Hamming weights, i.e., the number of nonzero elements, of the transformation matrices. Exhaustively searched for the least overhead transformation matrices and their parity predictions combined for the inverse S-box and have derived the total complexity for the predicted parities.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.2, Pages : 92-94 (2013)
Special Issue of NCRTECE 2013 - Held during 8-9 February, 2013 in SMK Fomra Institute of Technology, OMR, Thaiyur, Kelambakkam, Chennai

MIXED INVERSE AND AFFINE TRANSFORMATION

Instead of considering the Hamming weights, sub expression sharing is suggested for obtaining the low-complexity implementations for the S-box. Transformation matrices for the inverse S-box for different values of AND and have derived their area and delay complexities. Moreover, the gate count and the critical path delay for predicted parities.

MULTIPLICATION AND ADDITION OPERATION

S-box and the inverse S-box consists of a multiplication, an addition, a squaring and a multiplication by constant. One can perform modulo-2 addition of the coordinates of the result of the multiplication by reordering and factoring of the result in the predicted parities. Only the multiplication by constant is affected for different values. We have exhaustively searched for and obtained the optimum implementation for different values.

MODULO-2 ADDITION OPERATION

The complexity of the predicted parity for this block is the same for any possible. Considering the discussions presented in this section for different combinations for polynomial basis. We present the following for the optimum parity predictions.

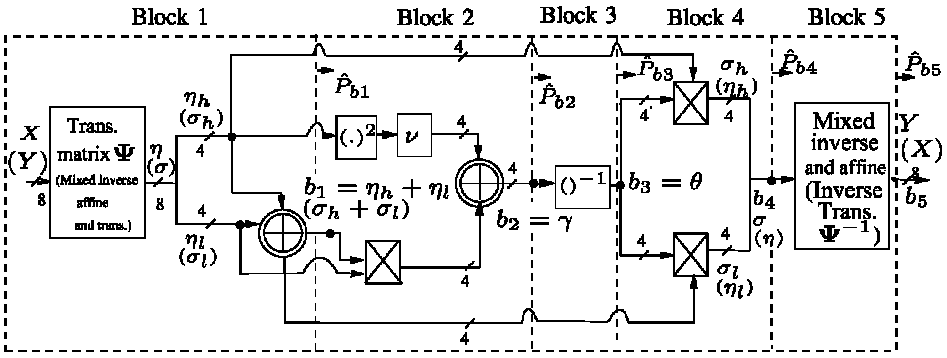

Fig 1. The S-box (the inverse S-box) using composite fields and polynomial basis and their fault detection blocks.

III FAULT DETECTION SCHEME

In this section, we describe the S-box and the inverse S-box operations and their composite-field realizations. The S-box and the inverse S-box are nonlinear operations which take 8-bit inputs and generate 8-bit outputs. In the S-box, the irreducible polynomial of $P(x) = x^8 + x^4 + x^3 + x + 1$ is used to construct the binary field $GF(2^8)$. Let $X = \sum_{i=0}^{7} x_i \alpha^i \in GF(2^8)$ and $Y = \sum_{i=0}^{7} y_i \alpha^i \in GF(2^8)$ be the input and the output of the S-box, respectively, where α is a root of P(x), i.e., $P(\alpha) = 0$. Then, the S-box consists of the multiplicative inversion, i.e., fields $GF(2^8)/GF(2^4)$. It is noted that the result of $X = \eta_h u + \eta_l$ in Fig. 1 is obtained using the irreducible polynomial $u^2 + \tau u + \nu$ of (respectively $u^2 + \tau' u + \nu'$). The multiplicative inversion in Fig. consists of composite field multiplications, additions and an inversion in the sub-field $GF(2^4)$ over $GF(2)/x^4 + x + 1$. The decomposition can be further applied to represent $GF(2^4)$ as a linear polynomial over $GF(2^2)$ and then $GF(2)$ using the $X^{-1} \in GF(2^8)$, followed by an affine transformation. Moreover, let $Y \in GF(2^8)$ and $X \in GF(2^8)$ be the input and the output of the inverse S-box, respectively. Then, the inverse S-box consists of an inverse affine transformation followed by the multiplicative inversion.

The composite fields can be represented using or polynomial basis. The S-box and inverse S-box for the polynomial and normal bases are shown in Fig1. As shown in these figures, for the S-box using polynomial basis the transformation matrix Ψ(respectively Ψ') transforms a field element X in the binary field $GF(2^8)$ to the corresponding representation in the composite irreducible polynomials of $\upsilon^2 + \Omega\upsilon + \Phi$ and $\omega^2 + \omega + 1$, respectively. As a result, it is understood that the implementation of the multiplicative inversion can be performed using the field represented by $GF((2^4)^2)$, see for example the field represented by $GF(((2^2)^2)^2)$ and has been used in the literature, the decomposition is performed using the irreducible polynomials of $\upsilon^2 + \Omega'\upsilon + \Phi'$ and $\omega^2 + \omega + 1$. For calculating the multiplicative inversion, the most efficient choice is

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.2, Pages : 92-94 (2013)
Special Issue of NCRTECE 2013 - Held during 8-9 February, 2013 in SMK Fomra Institute of Technology, OMR, Thaiyur, Kelambakkam, Chennai

to let $\Omega = \tau = 1\,(\Omega' = \tau' = 1)$ in the above irreducible polynomials. Then, we have the following for the multiplicative inversion of the S-box using polynomial basis (Fig. 1).

$$(\eta_h u + \eta_l)^{-1} = [((\eta_h + \eta_l)\eta_l + \eta_h^2 \nu)^{-1}\eta_h]u + ((\eta_h + \eta_l)\eta_l + \eta_h^2 \nu)^{-1}(\eta_h + \eta_l) \quad (1)$$

$$(\eta_h' u^{16} + \eta_l' u)^{-1} = \left[\left(\eta_h'\eta_l' + \left(\eta_h'^2 + \eta_l'^2\right)\nu'\right)^{-1}\eta_h'\right]u^{16} + \left[\left(\eta_h'\eta_l' + \left(\eta_h'^2 + \eta_l'^2\right)\nu'\right)^{-1}\eta_l'\right]u \quad (2)$$

It is noted that one can replace $\eta(\eta')$ with $\sigma(\sigma')$ to obtain (1) and (2) for the inverse S-box. In the next section, we propose the low-cost fault detection scheme for the S-box and the inverse S-box.

IV CONCLUSION

In this paper, we have presented a high performance parity-based concurrent fault detection scheme for the AES using the S-box and the inverse S-box in composite fields. Using exhaustive searches, we have found the least complexity S-boxes and inverse S-boxes as well as their fault detection circuits. Our error simulation results show that very high error coverages for the presented scheme are obtained. We have also implemented the AES encryption using the proposed fault detection scheme.

REFERENCES

[1] National Institute of Standards and Technologies, Announcing the Advanced Encryption Standard (AES) FIPS 197, Nov. 2001.

[2] R. Karri, K. Wu, P. Mishra, and K. Yongkook, "Fault-based side-channel cryptanalysis tolerant Rijndael symmetric block cipher architecture," In *Proc. DFT*, Oct. 2001, pp. 418–426.

[3] R. Karri, K. Wu, P. Mishra, and Y. Kim, "Concurrent error detection schemes for fault-based side-channel cryptanalysis of symmetric block ciphers," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 21, no. 12, pp. 1509–1517, Dec. 2002.

[4] A. Satoh, T. Sugawara, N. Homma, and T. Aoki, "High-performance concurrent error detection scheme for AES hardware," in *Proc. CHES*, Aug. 2008, pp. 100–112.

[5] L. Breveglieri, I. Koren, and P. Maistri, "Incorporating error detection and online reconfiguration into a regular architecture for the advanced encryption standard," in *Proc. DFT*, Oct. 2005, pp. 72–80.

[6] M. Karpovsky, K. J. Kulikowski, and A. Taubin, "Differential fault analysis attack resistant architectures for the advanced encryption standard," in *Proc. CARDIS*, Aug. 2004, vol. 153, pp. 177–192.

[7] P. Maistri and R. Leveugle, "Double-data-rate computation as a countermeasure against fault analysis," *IEEE Trans. Computers*, vol. 57, no. 11, pp. 1528–1539, Nov. 2008.

[8] C. H. Yen and B. F.Wu, "Simple error detection methods for hardware implementation of advanced encryption standard," *IEEE Trans. Computers*, vol. 55, no. 6, pp. 720–731, Jun. 2006.

[9] G. Bertoni, L. Breveglieri, I. Koren, P. Maistri, and V. Piuri, "A parity code based fault detection for an implementation of the advanced encryption standard," in *Proc. DFT*, Nov. 2002, pp. 51–59.

[10] G. Bertoni, L. Breveglieri, I. Koren, P. Maistri, and V. Piuri, "Error analysis and detection procedures for a hardware implementation of the advanced encryption standard," *IEEE Trans. Computers*, vol. 52, no. 4, pp. 492–505, Apr. 2003.

[11] C. Moratelli, F. Ghellar, E. Cota, and M. Lubaszewski, "A fault-tolerant DFA-resistant AES core," in *Proc. ISCAS*, 2008, pp. 244–247.

[12] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Parity-based fault detection architecture of S-box for advanced encryption standard," in *Proc. DFT*, Oct. 2006, pp. 572–580.

[13] S.-Y. Wu and H.-T. Yen, "On the S-box architectures with concurrent error detection for the advanced encryption standard," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E89-A, no. 10, pp. 2583–2588, Oct. 2006.

[14] A. E. Cohen, "Architectures for Cryptography Accelerators," Ph.D. dissertation, Univ. Minnesota, Twin Cities, Sep. 2007.

[15] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "A lightweight concurrent fault detection scheme for the AES S-boxes using normal basis," in *Proc. CHES*, Aug. 2008, pp. 113–129.