HAL
open science

Evaluation of Concurrent Error Detection Techniques on the Advanced Encryption Standard

Kaouthar Bousselam, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre

To cite this version:

Kaouthar Bousselam, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre. Evaluation of Concurrent Error Detection Techniques on the Advanced Encryption Standard. ETS: European Test Symposium, May 2010, Prague, Czech Republic. lirmm-00493247

HAL Id: lirmm-00493247

https://hal-lirmm.ccsd.cnrs.fr/lirmm-00493247v1

Submitted on 18 Jun 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Evaluation of Concurrent Error Detection Techniques on the Advanced Encryption Standard

K. BOUSSELAM, G. DI NATALE, M-L. FLOTTES, B. ROUZEYRE
LIRMM (Université Montpellier II / CNRS UMR 5506)
Montpellier, France
{bousselam, dinatale, flottes, rouzeyre}@lirmm.fr

***Abstract*—In nowadays technologies, circuits are more and more sensitive to aging phenomenon, as well as soft errors. Furthermore several attacks that used a fault to derive secret information have been demonstrated on cryptosystems. Concurrent fault detection is thus of prime interest for such systems. The purpose of this paper is to compare several code-based concurrent fault detection schemes dedicated to the hardware implementation of the Advanced Encryption Standard. The protection schemes under comparison are either directly issued from the literature, or built from several complementary solutions for protection of the full implementation. The evaluation of these schemes is performed in terms of costs with particular emphasis on fault injection vs errors detection capabilities.**

Keywords: concurrent fault detection, coding techniques, Advanced Encryption Standard.

Secure devices are used for storage and processing of confidential data. For that, they are designed with the ability to protect information against unauthorized access and intentional misuse. The digital security in such devices relies, among others, on data encryption. If encryption/decryption functions can be implemented in hardware for reasons of performances, the reliability of resulting IPs requires careful attention. Indeed, the security of the processed data may be compromised by permanent or transient faults affecting the expected behavior of the circuit.

Permanents faults due to manufacturing imperfections can be addressed before to put the chip into service in its application. However material aging is another source of permanent faults and must be addressed during the circuit life time. Moreover, several phenomena resulting in transient faults can affect the circuit behavior during its life time: natural soft (cosmic) errors and misuses. The latest can be intentionally induced by attackers with the aim of retrieving the secret information processed in secured devices. This type of attack, called "Differential Fault Analysis" (DFA), consists in inferring the secret data by comparing the results of a faulty encryption and a fault-free encryption [1].

The faults can be injected by different means such as temperature variation, clock frequency modification, exposure to radiations UV, X or visible light etc...

Our study deals with detection of transient faults in a standard cryptocore namely the Advanced Encryption Standard (AES). Several error detection schemes have been proposed in the literature for this particular encryption; they rely on different forms of temporal or spatial redundancies. Here, we focus on code-based redundancy mechanisms: [2], [3], [4], [5] and [6].

Those techniques act at algorithmic, round or operation level presenting various fault detection latencies. They are first compared in terms of costs (hardware/performance overhead, power consumption). Then their capability to detect errors of different multiplicities is compared. Because none of the related works reports correlation information between the error multiplicity on observable states and the transient faults likely to affect internal signals during encryption operations, we place emphasis on error detection vs fault injection. Several experiments are conducted in order to evaluate the number of resulting erroneous bits when the AES cryptocore is affected by a fault.

We then discuss the resistance of the protection schemes against state-of-the-art DFA attacks (e.g. [7]). The presented evaluation process shows that inexpensive AES implementations based on mathematical expressions requires expensive protection against fault attack because single fault injection results in large number of errors. Conversely, AES implementations based on look-up tables require (initaly) larger area but seam easiest to protect since single faults affecting these implementations result in a lower number of errors.

REFERENCES

[1] C. Giraud, "DFA on AES", 4th International Conference on AES, Springer publisher, pp. 27-41.

[2] Wu, K; Karri, R.; Kuznetsov, G. & Goessel, M., "Low Cost Concurrent Error Detection for the Advanced Encryption Standard", International Test Conference, 2004. pp 1242- 1248.

[3] Bertoni, G.; Breveglieri, L.; Koren I.; Maistri, P. & Piuri, V. "Error Analysis and Detection Procedures for a Hardware Implementation of the Advanced Encryption Standard", IEEE Trans. on Computers, Vol. 52., No.4, April 2003.

[4] Yen, C.H. & Wu, B.F. "Simple Error Detection Methods for Hardware Implementation of Advanced Encryption Standard", IEEE Trans. on Computers, June 2006, Vol. 55, No.6, pp 720-731.

[5] Di Natale, G.; Flottes M.L. & Rouzeyre, B., "An On-Line Fault Detection Scheme for SBoxes in Secure Circuits", Proc. of 13th IEEE International On-Line Testing Symposium, IOLTS 2007, pp. 57-62.

[6] Mozaffari Kermani M., Reyhani-Masoleh A., "Parity-Based Fault Detection Architecture of S-box for Advanced Encryption Standard," pp.572-580, 21st IEEE Int. Symp. on Defect and Fault-Tolerance in VLSI Systems (DFT'06), 2006.

[7] Blömer J. & Krummel, V, "Fault Based Collision Attacks on AES," FDTC 2006, pp. 106-120.