Jestr

Journal of Engineering Science and Technology Review 9 (5) (2016) 142 - 144

JOURNAL OF
Engineering Science and Technology Review

Research Article

www.jestr.org

Safety and Security for Shared Storage Media

A. P. Kakarountas*

Lab. of Computer & Information Systems, Business School, TEI of Ionian Islands, Lefkada – 31100, Greece.

Received 30 June 2015; Accepted 25 January 2016

Abstract

This paper considers the newly presented standard IEEE P1619 for securing data on shared storage media, and the risk of a potential malfunction of the hardware, due to transient and temporal fault occurrence. A new core implementing a P1619 compatible core is presented, featuring on-line concurrent testing. The design flow that was followed is a mixture of formal bottom-up and top-down design flows. The presented solution addresses unexpected malfunction due to temporal and/or transient faults, which may result to critically erroneous operation.

Keywords: Data storage, security, cryptography, safety, concurrent testing.

1. Introduction

A standard for ensuring security on shared storage media has been presented by IEEE, namely the IEEE P1619 [1], which specifies the fundamental cryptographic primitives and the structure of any compatible crypto core that applies block-cipher encryption algorithms to explicitly defined blocks of data for shared storage media. Hence, it allows encryption of data considering owner (user) and location characteristics, strengthening security to shared storage media against copy-paste attacks and typical methods of cryptanalysis. The standard has attracted the attention of market vendors, as a good solution to the demands of the consumers for higher security levels in storage devices, without incorporating trivial encryption techniques or key management processes for various operating systems. The manufacturers have already developed products based on P1619 [2], which are available in the market.

Although security is ensured through strong encryption of the data blocks, the proposed system is becoming more vulnerable to safety issues. A potential implementation of a hardware core following a typical design flow for ASIC or FPGA technologies will result in a susceptible system to transient and/or temporal faults, which may in turn damage severely blocks of data. Since encryption is performed on wide data blocks, any undesirable single bit upset [3], either at the data or worse at the key, may result in complete loss of the information, without the ability for a roll back or recovery process. In order to address similar situations, due to temporal and/or transient faults, this paper proposes a crypto core, based on Totally Self-Checking (TSC) circuits and sub-systems, allowing Concurrent Error Detection (CED). The design flow that was followed is a mix of formal bottom-up and top-down design flows as described in a following section.

2. P1619 implementations in hardware

Few implementations complying with the P1619 standard are found in the technical literature and even fewer in the IP cores' market worldwide. Most of the existing implementations are based on the following architecture (with one core for both data encryption and decryption).

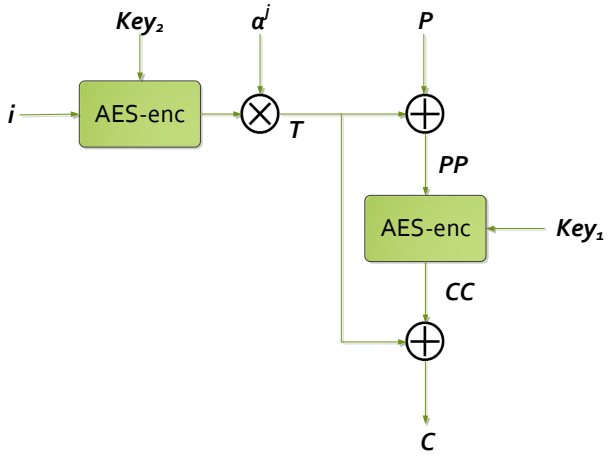

Fig. 1. P1619 structure based on XTS-AES [8]

The dominant target characteristic of the available implementations (either in ASIC [4] or FPGA technologies [5]) is high performance. However, although this target requires special design effort for the system in whole, a technological dependency is observed since the designers are aiming at modifying the XTS-AES core [6] in order to achieve high operation frequency. Such a design approach results in technology-dependant implementations, since AES has been fully explored in the last decade and only few modifications, of low impact, are still reported to the scientific literature. The most recent advancements of P1619 hardware implementations were reported in [7],[8].

* E-mail address: kazarlis@teicm.gr
ISSN: 1791-2377

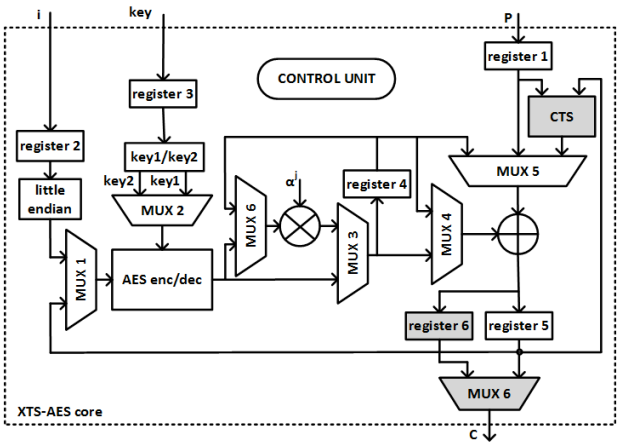

Fig. 2. State of the art P1619 implementation for dual core operation in parallel [7]

3. Totally Self-checking circuits and systems

As already mentioned, there is a continuous need for a keeping a common viewpoint for both security and safety. Thus, although security may be assured by the strong cryptographic primitives that may be used in a system, the effects of a hostile environment, or the intended actions of an attacker may result in either destruction or alteration of data.

Apart from hacker attacks that can be addressed with several countermeasures proposed in technical literature, there are also causes found in harsh environments that may result in catastrophic results. This is the nature of cause that this paper aims to confront.

Single Event Upsets (SEUs) are transient errors (soft-errors), which cause dynamic bit flips without damaging the hardware. When transient errors are frequent during normal operation, the feature of error detection is essential. CED is the most widely used mode of on-line testing [9] and is exploited to create self-checking designs. A more robust subset of self-checking circuits is the Totally Self-Checking circuits (TSCs). A thorough analysis for circuit and system design methodology was presented in [10], and it will serve as a guide to the presented approach.

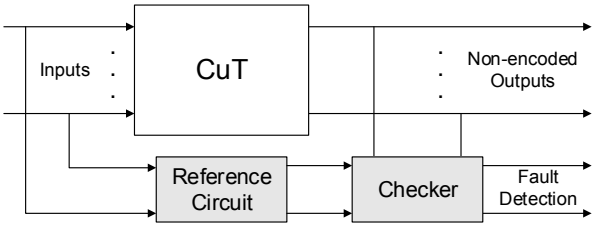

Fig. 3. The basic structure that will be followed for CED

4. System description

The system is based on a crypto core that was presented in [1], performing XTS-AES encoding, as described in [4]. Several modifications were made to increase performance [8] and various modes of operation were considered [7]. Following well defined techniques and substituting typical circuits with TSC ones [9], the proposed system is capable to detect the effects of single stuck-on faults either in combinational or sequential circuits. Special concern was given on silicon requirements (e.g. cost and area occupation).

4.1. Exploitation of TSC circuits

Practically, the application of TSC principle has several advantages over the application of generalized CED principle. The most significant advantage of a TSC system, compared to one with enabled CED, is that in the TSC one, not only the errors occurred in the data, but also potential errors that may occur inside its checking circuitry can be detected.

4.2. Encoding schemes

As presented in [10] to achieve TSC circuits and systems correct by construction, the correct mix of encoding schemes and TSC circuits should be carefully selected. For the scope of this work, extended Hamming encoding was employed to the main Data Bus and CRC code to the rest of the signals (control + address). Additionally, to decrease the area requirements, parity-bit for arithmetic and logical operations was preferred, since it offers a satisfactory level of safety of SEU.

Performing the above mentioned selections, the area penalty caused by information redundancy is kept in rational levels with the help of the hardware redundancy. Recall that CED techniques usually result in duplication or even triplication of area and cost.

4.3. Safety state

In the case of fault detection, the system signals a warning and System operation is halted. Data is then recovered exploiting the selection of the data encoding scheme. Potential inability to recover data (TSC is continuously checking the attributes of the encoded data), freezes operation, causes report for fatal error and the Padding Unit flushes.

5. Design Flow

The design flow that was adopted for developing the proposed core is a mix of formal bottom-up and top-down design flows. All components (typical circuits) are developed following a bottom-up design flow, in order to ensure correct interconnection between standard cells of the targeted integration technology. Circuits are then treated as macro-blocks that have been placed and routed. This approach results in correct by construction circuits concerning safety properties, such as TSC. Various versions of each circuit have been developed for a plethora of encoding schemes (e.g. parity, CRC etc.) All the developed circuits have been characterized in terms of area requirements, power dissipation and critical path, and are forming a library of hard IPs appropriate for use at the Register-Transfer Level (RTL).

Then the system may be described using an HDL, describing a system level representation of the core. At the RTL, bulk components are used that are replaced during synthesis and place & route processes by the characterized hard IPs of the library. Thus the system is described following a top-down design flow, exploiting the appropriate (concerning the targeted safety property) circuits that were derived by the opposite design flow that was described before. The effect is to divide the system design project, in significantly less demanding (in terms of time and effort) small design projects to form the initial hard IP library.

6. Implementation

The system was developed in VHDL, and implemented in TSMC 40nm technology. It was verified for correct operation via simulation. Due to the duality of most of the components, the core exploits the spare in time component to generate the reference circuit's output. This way, high performance is sacrificed in order to achieve safety.

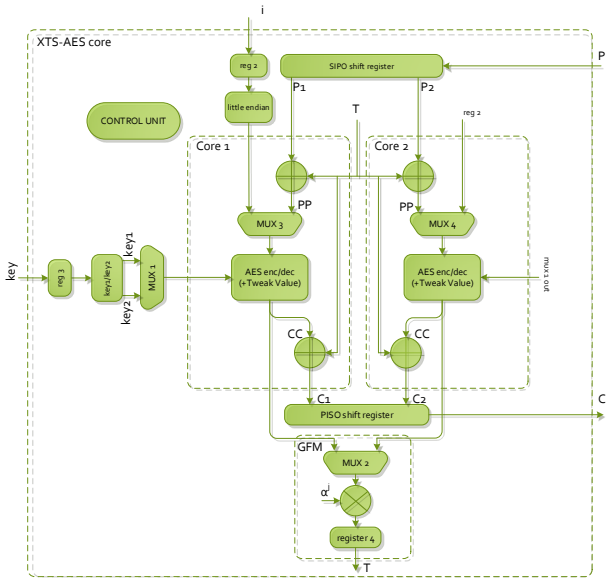

Fig. 4. The system's architecture (without the representation of hardware redundancy). Notice that two cores co-exist, supporting each other and changing in time the role of the CuT and Reference circuit. [8]

7. Results and Discussion

The area was kept below x2 compared to the most competitive in performance implementation. This is more than satisfactory in the case of CED systems. Although integration cost is increased, security and safety are assured at the highest degree. Furthermore, although performance was not a critical issue and didn't affect design decisions, at any phase of the development, it was kept in competitive figures, as it may be seen at the following table.

Table 1. Comparison of the proposed system to competitive implementations

	Technology	Area (eq.gates or slices)	Throughput (Gb/s)
[11]	ASIC	70k – 410k	2 – 16
[12]	ASIC	53k	3
[13]	ASIC	30k – 50k	7
[14]	ASIC	70k	3.7
[15]	FPGA (Virtex-4)	1594	2.2
[15]	FPGA (Virtex-5)	17 RAM16	2.8
[7]	ASIC	90k	37.3
proposed	ASIC	120k	9.8

8. Conclusion

An IEEE P1619 compatible crypto core based on TSC circuits was presented in this paper. The system is capable to detect in real-time single bit upsets, and address them by entering a safe mode. This is the first appearance of such a system in the international technical literature (to the best of the author knowledge).

This paper was presented at Pan-Hellenic Conference on Electronics and Telecommunications - PACET, that took place May 8-9 2015, at Ioannina Greece.

References

[1] IEEE Project 1619 (2007).
[2] L.Hars, IEEE Computer. **40**, 103 (2007).
[3] G.Messenger and M.Ash, Single Event Phenomena, Springer (2006).
[4] E.Hatzidimitriou, and A.P.Kakarountas, Proc. Mediterranean Electrotechnical Conf., Valetta, Malta, pp.597-601 (2010).
[5] C.Mancillas-Lopez, D.Chakraborty, F.Rodriguez-Henriquez, IEEE Trans. Comput. **59**, 1547 (2010).
[6] M.A.Alomari, K.Samsudin, A.R.Ramli, Proc. Stud. Conf. Research and Development, Serdang, Malaysia, pp.172-175 (2009).
[7] A.P.Kakarountas, E.Hatzidimitriou, P.Kitsos, Proc. Int. Symp. Communications, Control, and Signal Processing, Athens, Greece, pp.574-577 (2014).
[8] E.Hatzidimitriou, MD Thesis, Univ. Patras (2013).
[9] P.Lala, Self-Checking and Fault Tolerant Digital Design, Morgan Kaufman Publishers, San Francisco, USA (2001).
[10] A.P.Kakarountas, K.S.Papadomanolakis, C.E.Goutis, Designing CMOS Circuits for Low Power, Kluwer Academic Publishers, London, UK, p.205–234 (2002).
[11] www.ellipticsemi.com/products-clp-47.php.
[12] www.ellipticsemi.com/products-clp-33.php.
[13] www.ipcores.com/AES_XTS_IP_core.htm.
[14] www.ipcores.com/GXM3core.htm.
[15] www.heliontech.com/aes_xex.htm.