ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 5, May 2013

IMPLEMENTATING PROTECTED AND LESS COMPLEX CRIPTO DEVICES WITH HIGH FAULT EXPOSURE

Jaladi Harshini [1], R. Ravi Kumar[2]

Student, IV/IV B.Tech, Department of ECE, KL University, Vaddeswaram, Guntur, Andhra Pradesh, India[1]

Associate Professor, Department of ECE, KL University, Vaddeswaram, Guntur, Andhra Pradesh, India [2]

Abstract: The main motive of this Thesis is to design a secured crypto device with less complication and high protection by means of "ADVANCED AES" Algorithm along with self test procedure. The discriminating application of technological and associated procedural safeguards is an significant liability of every Federal organization in providing sufficient security to its electronic data systems and coming to self test concept there are two main functions that must be performed on-chip in order to implement built-in self-test (BIST): test pattern generation and output response analysis. The most common BIST schemes are based on pseudorandom test pattern generation using linear feedback shift registers (LFSR'S) and output response compaction using signature analyzers. To accomplish high security for a system we are using the crypto devices technique.

Keywords: CRYPTOGRAPHY, BIST, LFSR, AES, TPG, SA

I. INTRODUCTION

Most of the user now a day's using wireless communication for fast sending and receiving the mails in less time and in less cost. When this way of communication is going on, the unauthorized people who have the intension to know about our conversion will hack the information within that frequency. After hacking the information the hacker can know about what we are discussing. This leads to leakage of information. Nowadays, secure circuits are commonly used for applications such as e-banking, pay tv, cell phone... Because they hold personal data and must process secure operations, security requirements such as source/sink authentication, data integrity, confidentiality, or tamper resistance are maintained by means of several dedicated components. Confidentiality is ensured through cryptographic mechanisms generally implemented on co-processors. These mechanisms encode/decode plaintexts/cipher texts with the help of secret keys that must be preserved from compromise. Testing a secure circuit requires a specific attention since any undetected malfunction may induce a vulnerability and any extra test mechanism may induce new security vulnerabilities. For instance, generation of deterministic test patterns and design for testability such as scan design provide very high fault coverage. This mechanism minimizes the probability to deliver a supposedly secure system, but actually faulty chip, which could fail to protect the secret data. However, the scan path itself may compromise the security of the system since it provides facilities for controlling or observing sensitive data. Specific secure scan design methodologies can prevent abusive usage of the scan path but requires extra area and design effort. Conversely, the built-in self test (BIST) approach does not require visible scan chains. When the test mode is started, scan chains are fed from on-chip test resources and scanned-out test responses are compacted into a signature. The only test output is this compacted signature or the comparison result of this signature with a pre-computed "gold" one. The BIST strategy is considered as a good alternative if it provides acceptable fault coverage and low area overhead (apart from its recurrent cost, extra area for BIST implementation may in turn be subject to faults and, consequently, must be keep as low as possible). Re-using a cryptographic core ("crypto core") as test pattern generator (TPG) or signature analyser (SA) for other cores in the system prevents the insertion of any other dedicated hardware. However efficiency in terms of pattern generation and response compaction must be evaluated. There are two main functions that must be performed on-chip in order to implement built-in self-test (BIST): test pattern generation and output response analysis. The most common BIST schemes are based on pseudorandom test pattern generation using linear feedback shift registers (LFSR) and output response compaction using signature analysers.

The AES ciphers a block of 128 bits plaintext into a 128 bits cipher text with the help of a 128, 192 or 256- bits secret key K. The 128-bits plaintext is organized into a 4*4 matrix of 16 bytes. After a first XOR operation between K and the plaintext, the algorithm consists in several rounds: 10, 12 or 14 rounds according to the key length 128, 192 or 256 bits. Every round except the last one is composed of four operations: Sub bytes is a substitution of text bytes with the help of substitution tables called Sboxes, Shift Rows consists in circular shifts on the matrix lines, Mix Columns is a multiplication by a known matrix in the Galois field, and Add Round Key is a XOR operation between the partially ciphered text and the round key RKi; RKi being derived from the initial secret key K. The last round does not execute the Mix Columns operation. Without loss of generality, we assume hereafter 128- bits key and thus 10 rounds. Figure 1

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 5, May 2013

presents the base iterative implementation of the AES algorithm. It is mainly composed of a Key Generation module and a Round module. After 10 iterations of the Round module, the controller set the Encryption signal that loads the cipher text into the output register R2.

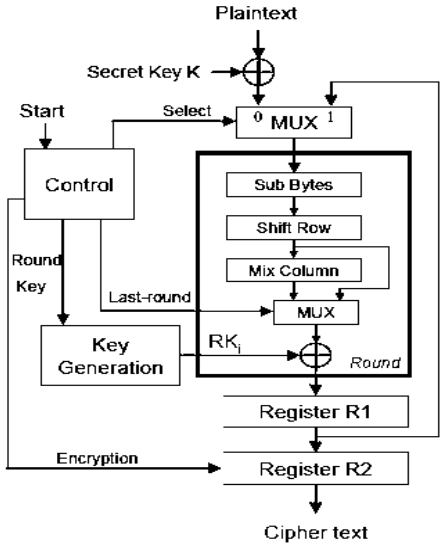


Figure 1: AES base iterative implementation

In this paper we investigate 1/ the self-testability of the AES crypto core, and 2/ its use as TPG or SA.

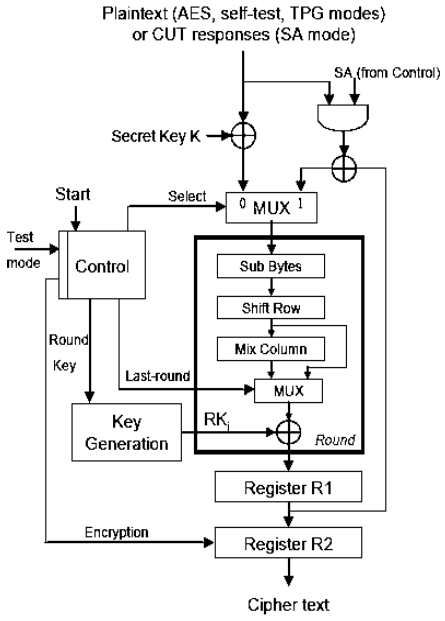


Figure 2: AES TPG/SA implementation

The three new behavioural modes (TPG/SA/SELF_TEST) entail the addition of extra control, and new operations in the data path (AND, XOR) of the base implementation. Figure 2 depicts the introduced slight changes. During the first round of the mission mode (encryption), self-test or TPG modes, the select signal is set to 0. The self-test of the core is further discussed in section 3. In TPG mode, the select signal allows to load the seed of the generator. Next, the select signal is set to 1 while the SA is set to 0. Test patterns are issued from R2 at every clock cycle with the help of the Encryption signal that enables the R2 load operation after every round. Evaluation of the so-generated test vectors is presented in the section 4. For test response compaction (SA mode), select and SA signals are set to 1. An XOR operation is performed between one response of the Core Under test (CUT) and the result of the previous round. The final signature obtain after compaction of all the test responses is loaded into the R2 register. Diagnostic facilities can be implemented using the Encryption signal for enabling the analysis of intermediate signatures. The Key Generation module is also slightly modified in such a way that during self-test, TPG and SA modes, the 10th round key is used as the primary key for the next round keys generation. Usually, the original secret K is used as primary key at the

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 5, May 2013

beginning of every encryption, or, in other words, every ten rounds. This behaviour is maintained for mission mode. Table 1 reports the areas of original and modified AES crypto cores in terms of cell number. Both architectures have been described in VHDL

II. AES SELF-TEST

This paragraph presents both theoretical results on the required test length for AES self-test and fault simulation results. Pseudo-random testing is an efficient technique for crypto cores. High fault coverage can be achieved with short pseudo-random test sequences because traditional cryptographic operations (XOR, substitution, modulo…) are easily tested with random data. Moreover, the inherent properties of these operations allow the propagation of random data through the circuit. Because the AES core is mainly made up of Sboxes (83% of the AES area for implementing the SubByte operation), we first focused on the testability of these components. The minimum deterministic test set for 100% fault coverage is 203 patterns long for one 8-input bits Sbox. An in-house fault simulator and a heuristic have been used for building up the fault dictionary and defining this minimal test set. From this number, and in order to be conservative, we compute the minimal-length random sequence that would include these 203 patterns with a given confidence: where $P[X \leq n]$ is the confidence level, k is the number of targeted patterns, p is the probability that every random pattern occurs (here p=1/28) and n is the number of random patterns that have to be sampled. In our case, 203 patterns must be obtained after n random patterns with a confidence level of 99%, i.e.: From this equation it comes that the minimal random sequence length is n = 2534 patterns. This result stands for the whole set of Sboxes in the AES core since they are tested in parallel. The same experiment have been performed for various implementations of the Sboxes and thus for different minimal deterministic test sets. In any case, the theoretical minimal length of the random sequence for including the targeted deterministic patterns ranges from 2400 to 2600 patterns. The upper bound is thus set to 2600 random patterns to test the Sboxes whatever their implementation. Concerning the other round operations: ShitRow function requires only wires for its implementation and is tested when every bit of this interconnection structure has been set to both “0” and “1” (under the assumption of stuck-at fault model). This should be easily achieved with the patterns issued from the Sboxes (bijective operations fed with 2600 random patterns). Mix Column and Add Round Key operations are mainly xor trees and should be very easily tested too using random patterns issued from the Sboxes. In order to confirm this hypothesis, we have performed a fault simulation on the proposed AES core sets in self-test mode. The test response (or signature) is only observed after simulation of the whole sequence, not at every round. The self-test structure is initialised with a randomly chosen plaintext and a secret key. This experiment has shown that all the faults have been tested after 2100 round cycles (to be compared with the 2534 random patterns theoretically required for 100% fault coverage on the first experimented Sboxes implementations). This experiment has been repeated with different plaintexts and secret keys as starting points: 2100 to 2500 patterns have been required for 100% fault coverage. We did the same experiments with two other AES logic implementations and obtained similar results. From a practical point of view, 2600 round cycles in self-test mode should be sufficient to test the whole structure with a confidence level of 99%.

III. DIFFERENCE BETWEEN PROPOSED & EXISITING SYSTEM:-

PROPOSED SYSTEM (AAES)	EXISTING SYSTEM(AES)
1. RCON is fixed. 2. MIXED MULTIPLICATION is also fixed. 3. It can handle Data up to: 64 bits & SKey up to: 56 bit. 4. Not much secure, since all blocks are not dependent. 5. KEY is same for all blocks. 6. KEY,USER are dependent 7. It Feistel network	1. RCON is not fixed. 2. MIXED MULTIPLICATION is also not fixed. 3. It can handle Data up to: 128,192,256 bits & Key up to: 128,192,256. 4. More secure, since all blocks are dependent. 5. KEY is not same for all blocks. 6. KEY,USER are independent 7. Substitution permutation network

IV. TEST PATTERN GENERATION

This section questions the randomness of the patterns issued from the proposed AES-based TPG, called “1-AES-round” TPG in the following. Inherent property of the basic operations involved during AES encryption and statistical analysis of the data issued from the base crypto algorithm demonstrate that the whole AES encryption process is a very good 128-bits random number generator. It can be used for instance as random number generator for stream ciphering operations implemented in the same system. However in this study, the whole AES mission mode was used to provide

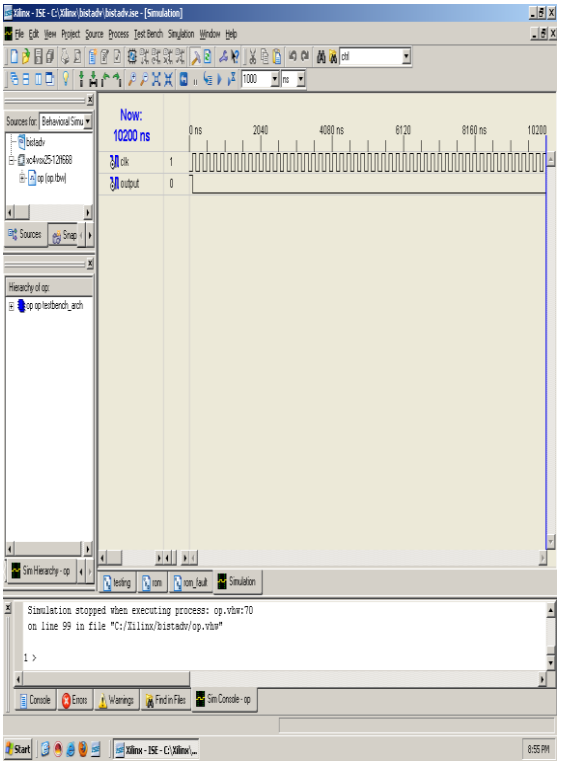
ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 5, May 2013

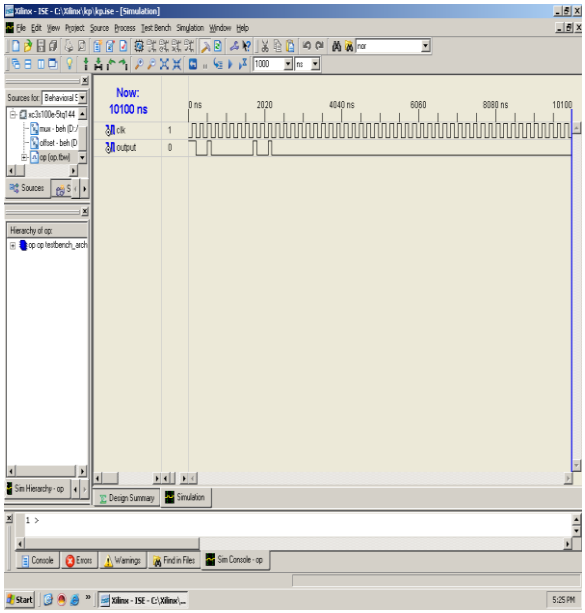
a new random word at every encryption cycle (i.e. every 10 rounds). The main drawback of this approach is that a test pattern is generated every ten clock cycles. Here, in the proposed TPG mode implementation, one pattern is issued at every round, or in other words at every clock cycle.

V. SIMULATION RESULTS

A. CRYPTOGRAPHY WITH NO FAULTS



B. SIMULATION REPORT FOR A CRYPTOGRAPHY WHICH CONSISTS OF FAULTS



VI. CONCLUSION

In the context of secure circuits, BIST approaches appear as good alternatives since they do not rely on visible scan chains. However they require extra hardware extra hardware for implementing test pattern generation, signature analysis and corresponding control logic. In this project, a solution is presented that consists using an AES-based cryptographic core commonly embedded in secure systems. Three additional modes are added to the current mission of the AES crypto core, one for self-test, one for pseudo-random test pattern generation and one for signature analysis. Efficiency of these three modes has been demonstrated. Extra cost in terms of area is very low even compared to the implementation of a BILBO register. Because only one AES core may be originally embedded in the system, it will be interesting to study concurrent test pattern generation and response compression. Furthermore, since secure systems requires very high quality testing strategies, it may be necessary to apply deterministic patterns to some systems cores due to their resistance to pseudo-random test sequences. Techniques such as TPG reseeding should be investigated in this case.

REFERENCES

[1] C.H. Gebotys, R.J. Gebotys. A Framework for Security on NoC Technologies. Proc of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI'03),2003.
[2] K. Okeya, T. Takagi. A More Flexible Countermeasure against Side Channel Attacks Using Window Method. CHES'2003,LNCS 2779,pp.397-410,2003.
[3] J.S. Coron. Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems. CHES'99,LNCS 1717, pp.292-302,1999. 27
[4] M. Joye,C. Tymen. Protections against differential analysis for elliptic curve cryptography: An algebraic approach. CHES'2001,LNCS 2162,pp.377-390, 2001.
[5] P.Y. Liardet, N.P Smart. Preventing SPA/DPA in ECC systems using the Jacobi form. CHES 2001, LNCS 2162,pp.391-401,2001.
[6] E. Brier, M. Joye. Weierstrass Elliptic Curves and Side-Channel Attacks. PKC 2002, LNCS 2274,pp.335-345,2002.
[7] M. Joye, J.J. Quisquater. Hessian elliptic curves and side-channel attacks. CHES 2001, LNCS 2162, pp.402-410,2001.
[8] Okeya, K., Sakurai, K., Power Analysis Breaks Elliptic Curve Cryptosystems even Secure against the Timing Attack. INDOCRYPT 2000, LNCS1977,pp.178-190,2000.
[9] K. Okeya, T. Takagi. The Width-w NAF Method Provides Small Memory and Fast Elliptic Scalar Multiplications Secure against Side Channel Attacks. CT-RSA 2003, LNCS 2612,pp.328-342,2003.
[10] W. Fischer, C. Giraud, E.W. Knudsen, J.P. Seifert. Parallel scalar multiplication on general elliptic curves over Fp hedged against Non-Differential Side-Channel Attacks. Available at http://eprint.iacr.org/2002/007/.
[11] T. Izu, T. Takagi. A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks. PKC 2002, LNCS 2274,pp.280-296,2002.
[12] B. Möller. Securing Elliptic Curve Point Multiplication against Side-Channel Attacks. ISC 2001, LNCS 2200, pp.324-334,2001.
[13] B. Möller. Securing elliptic curve point multiplication against side-channel atttacks, addendum: Efficiency improvement. Available at http://www.informatik.tudarmstadt.de/TI/Mitarb-eiter/moeller/ecc-scaisc01.pdf, (2001).
[14] B. Möller. Parallelizable Elliptic Curve Point Multiplication Method with Resistance against Side-Channel Attacks. ISC 2002, LNCS 2433,pp.402-413,2002.
[15] L. Goubin. A Refined Power-Analysis Attack on Elliptic Curve Crypto -systems. PKC 2003, LNCS 2567,pp.199-211, 2003.
[16] C.D. Walter. Seeing through Mist Given a Small Fraction of an RSA Private Key. CT-RSA 2003, LNCS 2612,pp.391-402,2003.
[17] E. Oswald, M. Aigner. Randomized Addition-Subtraction Chains as a Countermeasure against Power Attacks. CHES 2001, LNCS 2162,pp.39-50,2001.
[18] K. Itoh, J. Yajima ,M. Takenaka,N. Torii.DPA Countermeasures by improving the Window Method. CHES 2002, LNCS 2523.

BIOGRAPHY

Jaladi Harshini studying B.Tech in Electronics and communication engineering in KL University. Currently, she is dealing with signal processing. She involves in R&D works of KL University

R. Ravi Kumar, working in KL University as Associate Professor. He is having assortment of experience in communication field and realistic environment.