VLSI DESIGN AND IMPLEMENTATION OF LOW COST SELF TEST OF CRYPTO SYSTEM

Aravinth. V*[1] and Chelladurai.T[2]

[1]PG Scholar, [2]Assistant Professor

Department of Electronics and Communication Engineering,

PSNA college of Engineering and Technology,

Dindigul -624619, India.

Abstract: **The testability of the cryptographic cores brings in an extra dimension to the process of digital circuits testing –security. The benefits of the classical methods such as the scan-chain method introduce new vulnerabilities concerning the data protection. The Built-In Self-Test (BIST) is considered to be the most suitable countermeasure for this purpose. Testability is a major issue, particularly for secure chips. Design-for- Testability techniques based on scan chains proved to be a highway for potential attacks. BIST approaches appear as good alternatives since they do not rely on visible scan chains. In this paper we propose a generic BIST solution for block-cipher devices. Re-using embedded resources for implementing built-in-self-test mechanisms allows test cost reduction. In this paper we demonstrate how to implement cost efficient built-in self-test functions from the crypto algorithm hardware implementation in a secure system. Self-test of the proposed implementation is also presented. A statistical test suite and fault-simulation are used for evaluating the efficiency of the corresponding crypto core as pseudo-random test pattern generator; an analytical approach demonstrates the low probability of aliasing when used for test response compaction.**

*Keywords:***Scan chain method, Statistical test suite, Fault-simulation, Pseudo-random test random test pattern generator.**

I.INTRODUCTION

Now a days, data security is a challenging issue of data communications that deals with many fields including secure communication channel, strong data encryption technique and trusted third party to maintain the database. Cryptography is a new concept of protecting data transmission over a chip level. The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret keycan decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable. The goals which cryptography tries to provide are, as we have discussed, confidentiality, integrity and availability of information. While modern cryptography is growing increasingly diverse, cryptography is fundamentally based on problems that are difficult to solve. A problem may be difficult because its solution requires some secret knowledge, such as decrypting an encrypted message or signing some digital document.

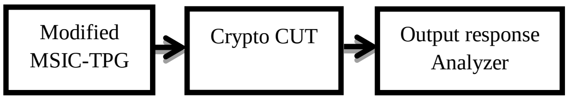


Fig.1 Basic blocks of crypto-BIST

To achieve an secure data transmission in processor various encryption algorithms are discovered. Among them most popular encryption algorithms are Advanced Encryption Standard, Data Encryption Standard, HASH algorithm, Rivets Shamir Adleman (RSA), HMAC, MD5 and RC5 etc. The task of testing a VLSI chip to guarantee its functionality is extremely complex and often very time consuming. In addition to the problem of testing the chips themselves, the incorporation of the chips into systems has caused test generation's cost to grow exponentially. A widely accepted approach to deal with the testing problem at the chip level is to incorporate built-in self-test (BIST) capability inside a chip. This increases the controllability and the observability of the chip, thereby making the test generation and fault detection easier. There are various test pattern generators has been used such as LFSR (Linear Feedback Shift Register), pseudorandom test pattern generator, and SIC (Single Input Change) etc. It is challenge to fusion security and testing for improved performance. The specific things are integration of both crypto with testing architecture. For the integration we use different approach for both testing and cryptography which has discussed in previous. Three things we have decide to do. First, design an testing platform separately, second, design an Cryptography systems separately. Third, design a combined CRYPTO-TEST system also to analyse it's parameters and performance**.**

II.METHODOLOGY

In recent times designers focus more on providing protection against attackers and testing for errors. Hence it is challenge to fusion security and testing for improved performance. We are going to design new testing architecture and also new crypto system. The specific thing is integration of both crypto with testing architecture. For the integration we are using different approach for both testing and cryptography. Re-using embedded resources for implementing built in self-test mechanisms allows test cost reduction. A basic block of integrated crypto system and self-testing of processor is shown in Fig.2.

SEA ALGORITHM

Here we are going to use Scalable Encryption Algorithm (SEA) for cryptographic core. Why we are using this algorithm in the sense the computational complexity in this algorithm is lesser and also for integration it is flexible than other algorithms. Thus the performance in area, power, speed and latency has increasing in our design system. Let as see the detail description about the SEA algorithm.

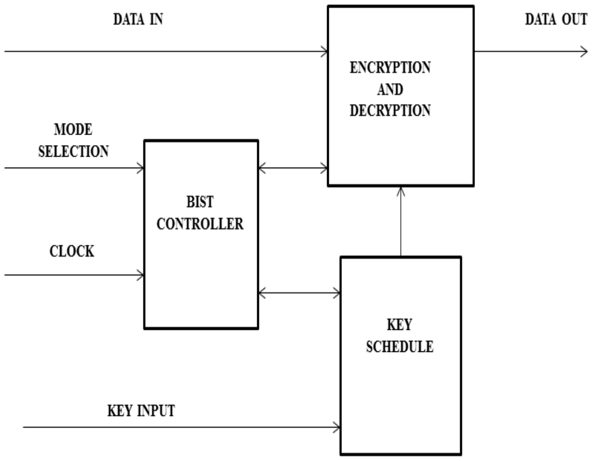


Fig.1 Block diagram of integrated cryptosystem with self-test architecture

To secure logical values in an integrated chip proposed cryptographic system utilizes encryption and decryption algorithm. The working function of encryption algorithm is shown in Fig.2. The step by step procedure of decryption algorithm is discussed below:

1. Reverse of encryption process
2. The encrypted data E and keys are known
3. Split into two halves and get rotated left part, vector form of S box i.e., SV.
4. Perform inverse word rotation operation
5. Expand the key and convert to integer form which is the right part .
6. To get the input data the left part and right part are concatenated.

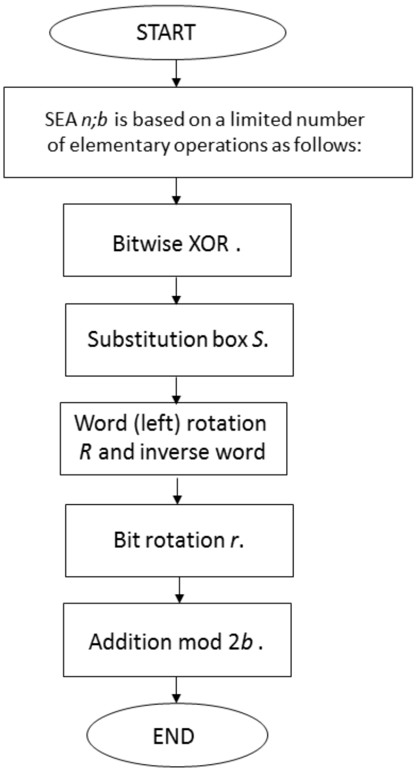

START
SEA n;b is based on a limited number of elementary operations as follows:
Bitwise XOR .
Substitution box S.
Word (left) rotation R and inverse word
Bit rotation r.
Addition mod 2b .
END

Fig.2- Flow chart of SEA Algorithm

ALGORITHM PROCEDURE

These are the main operations of this algorithm.,

```
C = SEA n; b(P;K)
f
% initialization:
L0&R0 = P;
KL0&KR0 = K;
% key scheduling:
For i in 1 to bnr =2c
[KLi ;KRi] = FK (KLi1; KRi1; C(i));
Switch KLbn =2c, KRbn =2c;
For i in dnr=2e to nr 1
[KLi ;KRi] = FK (KLi1; KRi1; C(r  i));
% encryption:
For i in 1 to dnr=2e
[Li; Ri] = FE (Li1; Ri1; KRi1);
For i in dnr=2e + 1 to nr
[Li; Ri] = FE (Li1; Ri1; KLi1);
% final:
C = Rn&Ln;
switch Ln 1, KRn 1; g
```

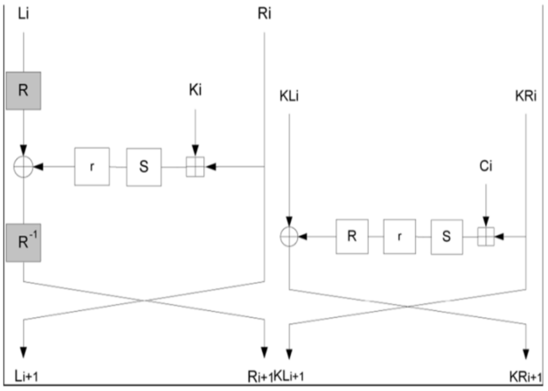


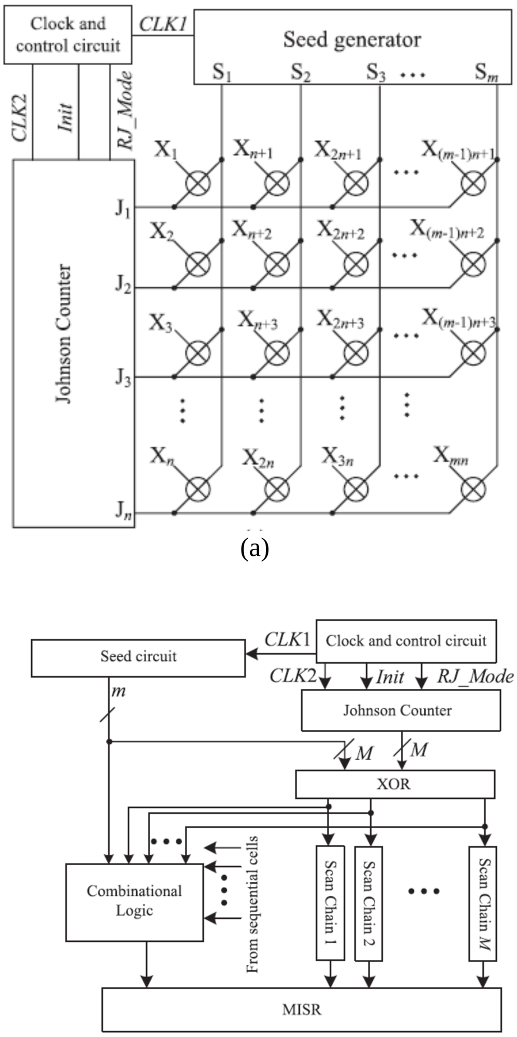
Fig.3 Basic operation encryption and decryption of SEA[12]

MODIFIED MSIC TPG

A new method to generate multiple single input change (MSIC) vectors in a pattern, i.e., each vector applied to a scan chain is an SIC vector. A reconfigurable Johnson counter and a scalable SIC counter are developed to generate a class of minimum transition sequences. A modified MSIC TPG is proposed which is flexible to both the test-per-clock and the test-per-scan schemes. The produced MSIC sequences have the favourable features of uniform distribution and low input transition density. The performances of the designed TPGs and the circuits under test with 45 nm are evaluated. Simulation results with ISCAS benchmarks demonstrate that MSIC can save test power and impose no more than 7.5% overhead for a scan design. It also achieves the target fault coverage without increasing the test length.

This modified method proposed a low-power test pattern generation that could be easily implemented by hardware. Combined with the proposed reconfigurable Johnson counter or scalable SIC counter, the Modified MSIC-TPG can be easily implemented, and is flexible to test-per-clock schemes and test-per-scan schemes. For a test-per-clock scheme, the MSIC-TPG applies SIC sequences to the CUT with the SRAM-like grid. For a test-per scan scheme, the MSIC-TPG converts an SIC vector to low transition vectors for all scan chains. Experimental results and analysis results demonstrate that the Modified MSIC-TPG is scalable to scan length, and has negligible impact on the test overhead.

The main objective of this algorithm is to reduce the switching activity. In order to reduce the hardware overhead, the linear relations are selected with consecutive vectors or within a pattern, which can generate a sequence with a sequential decompressor, facilitating hardware implementation. Another requirement is that the MSIC sequence should not contain any repeated test patterns, because repeated patterns could prolong the test time and reduce test efficiency . Finally, uniformly distributed patterns are desired to reduce the test length (number of patterns required to achieve a target fault coverage). This section aims to extract a class of test sequences that meets these requirements. Johnson counter to generate an SIC sequence in time domain.A seed generator is an *m*-stage conventional LFSR, and operates at low frequency CLK1. The test procedure is as follows.



(a)

(b)

Fig.4 MSIC-TPGs for (a) test-per-scan schemes and (b) test-per-clock schemes [1]

Modified MSIC-TPGs for Test-per-Clock Schemes

A seed generator is an *m*-stage conventional LFSR, and operates at low frequency CLK1.

1) The seed generator generates a new seed by clocking CLK1 one time.
2) The Johnson counter generates a new vector by clocking CLK2 one time.

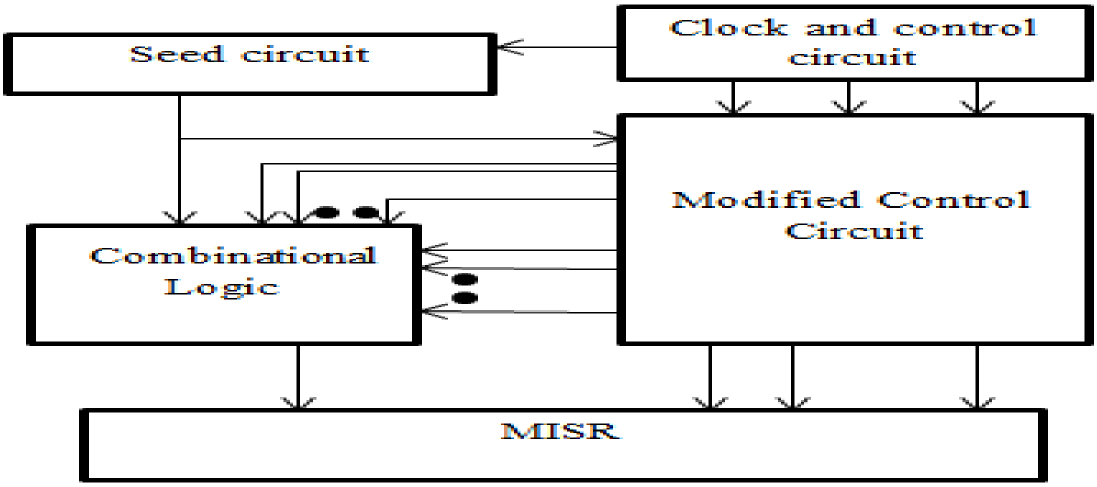


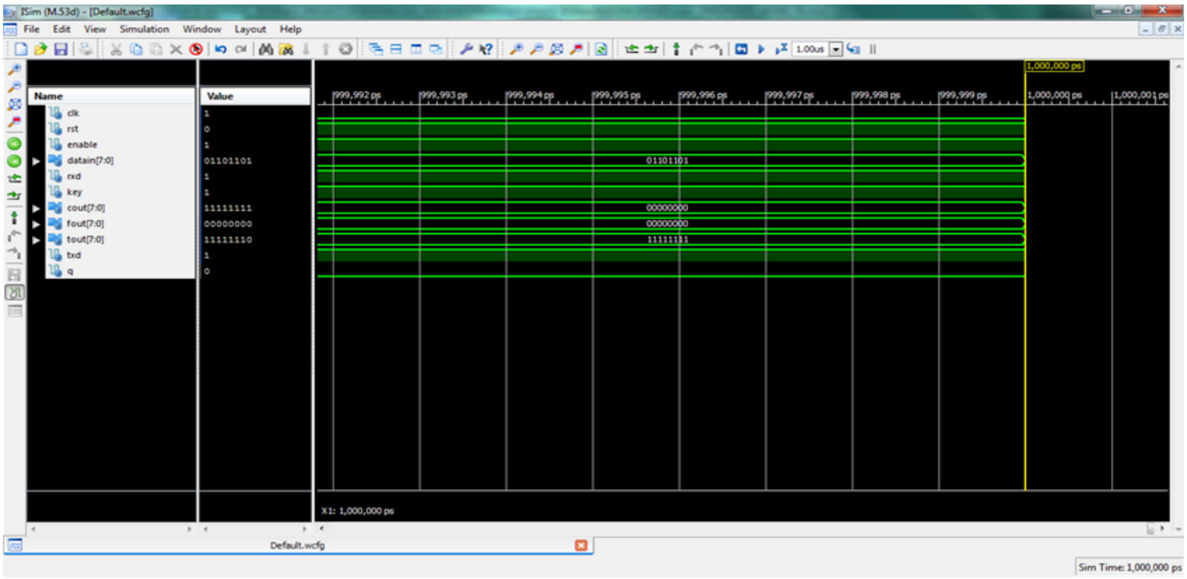
Fig.5 Modified MSIC-TPGs for Test-per-Clock Schemes

3) Repeat 2 until 2*l* Johnson vectors are generated.
4) Repeat 1–3 until the expected fault coverage or test length is achieved.

A Modified MSIC- TPG FOR Test-per-ClockSchemes is shown in Fig.5. This modified circuit consists of Johnson counter, XOR gate and set of scan chain connected in cascade. This arrangement minimizes area and complexity and further integration with SEA Crypto-core helps to reduces computational complexity compared with MSIC-TPG.

The test procedure for test-per-Scan Schemes is as follows.

1) The seed circuit generates a new seed by clocking CLK1one time.
2) RJ_Mode is set to "0". The reconfigurable Johnson counter will operate in the Johnson counter mode and generate a Johnson vector by clocking CLK2 one time.
3) After a new Johnson vector is generated, RJ_Mode and Init are set to 1. The reconfigurable Johnson counter operates as a circular shift register, and generates *l* codewords by clocking CLK2 *l* times. Then, a capture operation is inserted.
4) Repeat 2–3 until 2*l* Johnson vectors are generated.
5) Repeat 1–4 until the expected fault coverage or test length is achieved.

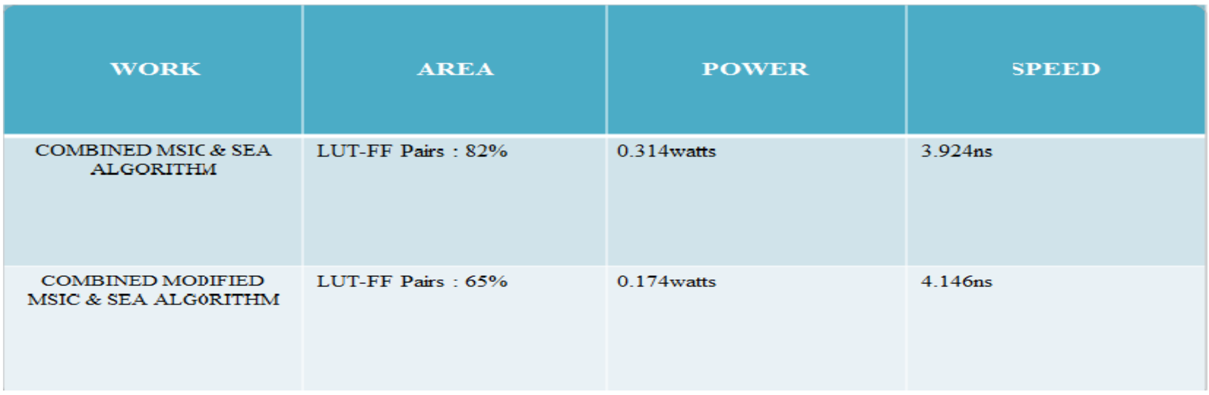


```
Name          Value
clk           1
rst           0
enable        1
datain[7:0]   01101101
rxd           1
key           1
cout[7:0]     11111111
fout[7:0]     00000000
tout[7:0]     11111110
txd           1
q             0
```

Fig.6 Simulation of modified MSIC-TPG with SEA algorithm

III.RESULTS AND DISCUSSION

Fig.6 shows simulation output of Modified MSIC-TPG with SEA Algorithm executed in Modelsim. The input to the Modified MSIC-TPG with SEA algorithm are clk, rst, enable, datain[7:0], rxd and key. The obtained outputs are cout[7:0], fout[7:0] and tout[7:0]. Table.1 represents area, power and speed of proposed work compared with MSIC-TPG. The areaof MSIC-TPG with SEA algorithm is 111 including Flip-flops and Lookup table pair is reduced.



WORK	AREA	POWER	SPEED
COMBINED MSIC & SEA ALGORITHM	LUT-FF Pairs : 82%	0.314watts	3.924ns
COMBINED MODIFIED MSIC & SEA ALGORITHM	LUT-FF Pairs : 65%	0.174watts	4.146ns

Table.I Comparison of combined MSIC & SEA Algorithm with combined Modified MSIC & SEA Algorithm

IV.CONCLUSION

This work was started with the intension of integrating the cryptographic and testing core in a single chip. The proposed system is used to design the crypto processer with Built in Self-Test (BIST) core with low power and low memory usage. Since the proposed algorithm SEA (Scalable Encryption Algorithm) used for this analysis. A ModifiedMSIC test pattern generator was proposed. It can be easily implemented, and is flexible to test-per-clock schemes and test-per-scan schemes by working with reconfigurable Johnson counter and a scalable SIC counter. A Modified MSIC-TPG is scalable to scan length, and has negligible impact on the test overhead and minimizes the delay. Integrating these two cores in a single chip may decrease the computational complexity, area, power and also processing time. Even though the testing core design is modified, it is further possible to simplify the design using various testing techniques.

REFRENCES

[1]Feng Liang, Luwen Zhang, Shaochong Lei, Guohe Zhang, KaileGao, and Bin Liang," Test Patterns of Multiple SIC Vectors: Theory and Application in BIST Schemes" IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS 1.

[2]Bo Yang, Kaijie Wu, and Ramesh Karri,"Secure Scan: A Design-for-Test Architecture for Crypto Chips," IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS, VOL. 25, NO. 10, OCTOBER 2006

[3]GauravSengar, DebdeepMukhopadhyay,andDipanwita Roy Chowdhury , "Secured Flipped Scan-Chain Modelfor Crypto-Architecture," IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS, VOL. 26, NO. 11, NOVEMBER 2007.

[4] Jeremy Lee, Mohammad Tehranipoor, Chintan Patel, Jim Plusquellic," Securing Designs against Scan-Based Side-Channel Attacks," IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 4, NO. 4, OCTOBER-DECEMBER 2007.

[5] Jean Da Rolt, Giorgio Di Natale, Marie-LiseFlottes and Bruno Rouzeyre ,"Thwarting Scan-Based Attacks on Secure-ICsWith On-Chip Comparison," IEEE TRANSACTIONS PRIL 2014.

[6] Geng-Ming Chiu and James Chien-Mo Li, "A Secure Test Wrapper Design Against Internal and Boundary Scan Attacks for Embedded Cores," IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 20, NO. 1, JANUARY 2012.

[7] Luke Pierce and Spyros Tragoudas,"Enhanced Secure Architecture for Joint Action Test GroupSystems," IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 21, NO. 7, JULY 2013.

[8] Jim Blythe and L. Jean Camp, "Implementing Mental Models," IEEE Symposium on Security and Privacy Workshops.

[9] Amitabh Das, Barıs¸ Ege, SantoshGhosh, LejlaBatina, and Ingrid Verbauwhede,”Security Analysis of Industrial Test Compression Schemes,” IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS, VOL. 32, NO. 12, DECEMBER 2013.

[11] GauravSengar, DebdeepMukhopadhyay and Dipanwita Roy Chowdhury ,”Secured Flipped Scan-Chain Modelfor Crypto-Architecture,” IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS, VOL. 26, NO. 11, NOVEMBER 2007.

[12] F. Mace, F.-X.Standaert, and J.-J. Quisquater ,”FPGA Implementation(s) of a ScalableEncryption Algorithm,” IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 16, NO. 2, FEBRUARY 200

[13] F.-X. Standaert, G. Piret, G. Rouvroy, J.-J.Quisquater, “FPGA Implementations of the ICEBERG Block Cipher”, in the proceedings of ITCC 2005, Nevada, April 2005.

[14] P Kitsos, O Koufopavlou, G Selimis and N Sklavos,” Low power cryptography “VLSI Design Lab, Electrical and Computer Engineering Department, University of Patras, Greece.

[10] Kurt Rosenfeld and Ramesh Karri ,”Attacks and Defenses for JTAG,” This article has been accepted for publication in IEEE Design and Test of Computers but has not yet been fully edited.

[15] XIE, Haiyong, ZHOU, Li, BHUYAN, “An Architectural Analysis of Cryptographic Applications for Network Processors.” Department of Computer Science and Engineering, Univ. of California, Riverside,Feb 2002.

[16] H. Bonnenbergt A. Curigert N. Felbert H. Kaeslintt X. Lait,” VLSI Implementation Of A New Block Cipher “„ in ICCD ’91, IEEE International Conference on Computer Design: VLSI in Computer and Processors 1991, pp. 510-513.

[17] Adam J. Elbirt, W. Yip, B. Chetwynd, and C. Paar,”An FPGA-Based Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists”, in IEEE Transactions On Very Large Scale Integration (VLSI) Systems, Vol. 9, No. 4, August 2001 , pp.545-557