GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

VLSI DESIGN AND IMPLEMENTATION OF LOW-COST SELF-TEST OF CRYPTOSYSTEM-A SURVEY

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

PG Scholar, Department of Electronics and Communication Engineering, PSNA college of Engineering and Technology, Dindigul-624622, India[*1]

Assistant Professor, Department of Electronics and Communication Engineering, PSNA college of Engineering and Technology, Dindigul-624622, India[2]

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 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 *key* can 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. 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, Rivest 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. In this survey, various encryption algorithms and test pattern generations are discussed; hence 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. The three things we have decide to do in future. First, design an testing platform separately, second, design an Cryptography systems separately. Third, design a combined CRYPTO-TEST system also to analyze it's parameters and performance**.**

II. RELATED WORKS

Feng Liang, Luwen Zhang, Shaochong Lei, Guohe Zhang, KaileGao, and Bin Liang [2] proposed a novel TPG that generates multiple single input changes (MSIC) vectored in a pattern for BIST. This proposed TPGM is a low-power TPG. Each input vector applied to the scan chain is an SIC vector. This paper composed Johnson counter and scalable SIC Counter which is used to obtain a minimum transition sequence. MSIC TPG is scalable for both the test-per-clock and the test-per-scan schemes. Since the MSIC sequence have the features of

uniform distribution and low input transition density. For test-per- clock scheme SIC sequences directly applied to the CUT (Circuit under Test) with the grid. For the test-per-scan scheme SIC vector is inverted into low transition vector for every scan chain. MSIC TPG has its own advantage based on its two schemes which is stable to Scan length and negligible its test overhead.

Bo Yang, Kaijie Wu, and Ramesh Karri [1] proposed a novel scan DFT architecture called Secure-scan DFT that maintains the high test quality of traditional scan DFT without compromising the security. This architecture can easily be integrated into the scan-based DFT design flow as the test synthesis. After that the Mirror Key Registers (MKRs) can be specified to the corresponding bit of the secret key. The secure control circuit, and the multiplexers between the MKR and the secret key can be inserted. The proposed secure-scan architecture minimizes the area overhead to small.

Giorgio Di Natale, Marion Doulcier, Marie-Lise Flottes, and Bruno Rouzeyre [3] described a generic built-in self-test approach for devices implementing symmetric encryption algorithms. This paper proposed architecture with no visible scan chain and achieves 100% fault coverage on crypt cores with very small area overhead. They proposed a self-test procedure. Such procedure feed the core with its own output and let the device run for a certain number of encryptions. It achieves 100% FC by comparing the output of the final encryption with a pre-computed signature.

Jeremy Lee, Mohammad Tehranipoor, Chintan Patel, Jim Plusquellic[4]Proposed the technique for scan based side channel attacks to neutralize the power and that has been used to expose vital information through the scan chain as a countermeasure called Lock and Key. This technique gives a supple security strategy without extensive changes to scan test practices to modern designs .In this method the scan chains are subdivided into small sub chains and access to sub chains are randomized when being accessed by an unauthorized user because of test security controller inclusion. These designs are independent while maintaining low area overhead and because of that this method is flexible and straightforward to implement for varying degrees of security.

Jean Da Rolt, Giorgio Di Natale, Marie-LiseFlottes and Bruno Rouzeyre[5] proposed a novel DFT technique for scan design to ensure security without relying on costly test infrastructures to switch from mission to test modes called scan-protection scheme and this scheme based on the concept of withholding information that provides testing facilities both at production time and over the course of the circuit's life. The idea behind is to compare test responses within the chip. Both input vectors and expected responses are scanned into the circuit and the comparison between expected and actual responses is done at vector level. This technique has no impact on test quality and no impact on modelled fault diagnostic. When compared to regular scan test. It avoids the usage of authentication test mechanism, minimize area overhead and it can be applied to IP cores as well.

Geng-Ming Chiu and James Chien-Mo Li, Member, IEEE [6] proposed secure test wrapper (STW) provides protection against scan based controllability and observability attacks and this design is compatible with the IEEE 1500 standard. STW protects not only internal scan chains but also primary inputs and outputs, which may contain encryption keys also known critical information during the system operation. To reduce the STW area, flip-flops in the wrapper boundary cells are reused AS LFSR for generating the secure test wrapper key. Experimental results based on an AES core exhibit that STW provides very high security at the price of only 5% area overhead.

Luke Pierce and Spyros Tragoudas[7]proposed a mechanism to enforce a multilevel privilege security system for the JTAG boundary scan standard and this method is user-privilege aware, which allows for higher granularity for controlling user access of individual scan chains. They have minimized timing overhead and for this it require no modifications to the core logic of the integrated circuit. With the hardware modifications proposed are compliant with IEEE 1149.1.Themultilevel privilege system allows for in-the-field updates and debugging of the firmware while maintaining a high degree of protection for the most sensitive intellectual property in the IC.A side from the initial unlocking of the system, processing of JTAG commands
requires no additional time compared to unsecured JTAG systems.

Jim Blythe and L. Jean Camp[8] proposed mental models that directly shields the domain of cyber security and security experts primarily use five kinds of mental models such as physical, criminal, medical, warfare and market models. They implement previously identified models in order to explore their use for predicting user behaviour. They describe a general approach for implementing the models in agents that simulate human behaviour within a network security test bed, and show that the implementations produce

behaviours similar to those of users who hold them and they plan to test the impact on networked attacks of large groups of individuals behaving according to a general population of mental models.

Amitabh Das, Barıs¸ Ege, Santosh Ghosh, LejlaBatina, and Ingrid Verbauwhede[9]pursues the validity of this right and presents scan attack susceptibilities of test compression schemes used in commercial electronic design automation tools and , security of industrial test compression schemes against differential scan attacks has been evaluated. In this design test compression structures provided by tools such as Synopsys, Cadence, and Mentor Graphics design for testability are injected into the design and also a visibly available advanced encryption standard design is used. A new noise injector countermeasure is proposed and its security properties are analyzed in this paper experimental results of the differential scan attacks employed that recommend the tools using X-masking and X-tolerance are vulnerable and leak information about the secret key. Finally, a suitable countermeasure is proposed and compared to the heretofore proposed countermeasures.

Kurt Rosenfeld and Ramesh Karri[10]proposed a protection scheme to protect against some security issues surrounding JTAG by making use of trivial cryptographic primitives such as stream ciphers and incremental message authentication codes. This scheme defines four levels of protection and determines which protection level is needed to prevent it for each of the attack setups and also implementing these security enhancements such as area, test time and operational. This scheme provides a significant improvement in JTAG security with reasonable added cost and this scheme is flexible in the sense of provide high assurance or cost for important chips and lower assurance or cost for less important chips.

GauravSengar, Debdeep Mukhopadhyay, and Dipanwita Roy Chowdhury[11] proposed a new scan-chain architecture called as flipped scan-chain architecture to test cryptographic devices through inserting a certain number of inverters between randomly selected scan cells. The presence of NOT gates or inverter in the scan-data path does not obstruct the normal functionality of the device. A proper placement of inverters is necessary to prevent normal scan chain-based attacks. This proposed scan chain architecture proved that the intellectual property of a chip is protected than conventional scan chains.

F. Mace, F.-X. Standaert, and J.-J. Quisquater[12] discussed an efficient low cost encryption and decryption algorithm globally referred as SEA(Scalable Encryption Algorithm).SEA is a flexible Encryption/Decryption algorithm mainly used for embedded applications and this algorithms flexibility can be revolved into a fully generic VHDL design. Since any plain text keys and bus size van be able to directly re implemented without any simple modifications of the hardware description language with their important tools. This paper proposed AES Rijndal and ICEBERB (a cipher purposed for efficient FPGA implementations) and their performance are compared with the SEA algorithm. This algorithm computes both the round and the key round algorithm in parallel and supports both encryption and decryption at minimal cost. Finally this algorithm reduced throughput by minimizing its area utilization.

III. RESULTS AND DISCUSSION

The various cryptographic algorithms and various testing techniques for improving performance of processor by increasing speed, reducing power and minimizing its area overhead separately in this survey were studied. Among those techniques, Single Input Change (SIC) Test Pattern Generation (TPG) technique achieves better results in neglecting test overhead. For Cryptography, SEA (Scalable Encryption Algorithm) achieves better results in reducing computational complexity and its possible to integrate with other platform. Secure Test Wrapper (STW) composed both Controllability and Observability which create better protection.

IV. CONCLUSION

In this survey, it has been concluded that there are several techniques discovered for the development of cryptographic core and also testing core. Most of the papers mainly conclude on minimizing area overhead on the test and crypto system separately. Since I concluded, that a fusion of both testing and cryptography in a single chip for improving performance of reducing area and minimizing latency and increasing speed, the scheme will use integration of self test and crypto system called CRYPTO-BIST is proposed in my future work.

V. 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, 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.

[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-LiseFlottesand Bruno Rouzeyre,"Thwarting Scan-Based Attacks on Secure-ICsWith On-Chip Comparison," IEEE transactions on Very Large Scale Integration (VLSI) systems, vol. 22, no. 4, april 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 Group Systems," 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.

[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.

[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 2008.