RESEARCH ARTICLE OPEN ACCESS

Mixed Scanning and DFT Techniques for Arithmetic Core

Athira S , Manu Prasad
M Tech student, Assistant professor,
Electronics and communication department

ABSTRACT

Elliptic curve Cryptosystem used in cryptography chips undergoes side channel threats, where the attackers deciphered the secret key from the scan path. The usage of extra electronic components in scan path architecture will protect the secret key from threats. This work presents a new scan based flip flop for secure cryptographic application. By adding more sensitive internal nets along with the scan enable the testing team can find out the bugs in chip after post-silicon and even after chip fabrication. Also present a new mixed technique by adding DFT(design for testing or Dfx unit) unit and scan unit in same chip unit without affecting the normal critical path ,i.e. without affecting speed of operation of chip, latency in normal mode. Both Scan unit and DFT unit are used for testing the sequential and combinational circuits present in 32 Bit Arithmetic core. Here a proposed PN code generation unit as scan in port to increase the code coverage and scan out port efficiency. The proposed system will written in verilog code and simulated using Xilinx Tool. The hardware module core is synthesized using Xilinx Vertex 5 Field Programmable Gated Array (FPGA) kit. The performance utilization is reported with the help of generated synthesis result.

Keywords: *VLSI; Verilog; Testing; FPGA*

I. INTRODUCTION

Cryptography is the method of storing and transmitting data in a particular form so that only whom it is intended can read and process it. There are two techniques can be used in Cryptography. First one is Encryption and second one is Decryption. The conversion of plaintext into cipher text is called Encryption, then back again known as Decryption. In cryptography cryptosystem refers to a suite of cryptographic algorithms needed to implement a particular security service, most commonly for achieving confidentiality. That is the information cannot be understood by anyone for whom it was unintended.

Elliptic curve cryptography (ECC) offers best optimized solution with minimum resources like low power, low memory, high throughput and minimum key length. The Public key encryption technique based on elliptic curve theory. It can be used to create faster, smaller, and more efficient cryptographic keys.ECC helps to establish security with lower computing power and battery resource usage. ECC used in cryptography chips undergoes side channel threats, where the attackers deciphered the secret key from the scan path. The Usage of extra electronic components in scan path architecture will protect the secret key from threats. This work presents a more secure ECC Cryptosystem and a new scan based flip flop for secure cryptographic application. By adding more sensitive internal nets along with the scan enable the testing team can find out the bugs in chip after post-silicon and even after chip fabrication. Also present a new mixed technique by adding DFT (design for testing or Dfx unit) unit and Scan unit in same chip unit.

In general testing is finding out how well something works. Software *testing* is a process of executing a program or application with the intent of finding the software bugs. Here both Scan unit and Dfx unit are used for testing the sequential and combinational circuits present in 32 Bit Arithmetic core.

The paper is organized as follow: In Existing system, architecture of secured elliptic curve crypto chip. In proposed system, architecture of more secured elliptic curve system and system architecture. Then finally Simulation and synthesis report for the proposed system is presented .Encapsulation of the proposed work is given in the conclusion.

II. EXISTING SYSTEM

In general there are few scan based architecture which are introduced against side channel scan attack. In paper [4], an additional NOT gate is added to the flipped element. The functionality of the Not gate is controlled through the multiplier. Simultaneous launch of memory register element along with scan flip-flop at certain places in architecture shown in paper [5], but it is not been practically proved. In paper [6] robust method is introduced through modifying the particular functionality of flip flop in the scan path but this method undergo reset based attack and implementation uses additional model scan control block in the circuit. Due to overhead of component in [6], method based dynamic changes of flip flop in the circuit using latch is introduced in paper [7], but this process needs large number of clock cycles to complete the process .In paper [1] a secured elliptic curve cryptosystems for scan based VLSI architecture used , The output from second flip flop is inverted and given as one of the input to the XOR gate. The another input for XOR gate is the non inverted form of output from second flip flop. Both input produces the scan out values always 1 Computed output cannot able to make any comparison with the previous output due to similarity in scan out The secured elliptic curve cryptosystem through changing the functionality of the scan path. Here a more secure elliptic curve crypto system can be proposed .In this case the number of flip-flops and number of tapping points are increased. Which make a more complicate for hackers.

III. PROPOSED WORK

This work presents a new scan based flip flop for secure cryptographic application. By adding more sensitive internal nets along with the scan enable the testing team can find out the bugs in chip after post-silicon and even after chip fabrication. Also proposing a new mixed technique by adding DFT(design for testing) unit and Scan unit in same chip unit without affecting the normal critical path ,i.e. without affecting speed of operation of chip, latency in normal mode .Both scan unit and dfx unit are used for testing the sequential and combinational circuits present in 32Bit Arithmetic core.

The proposed system consist of Scan generation block and other several units like Arithmetic Core unit ,Scan unit, DFT unit , and MUX are Shown in Fig 3.1

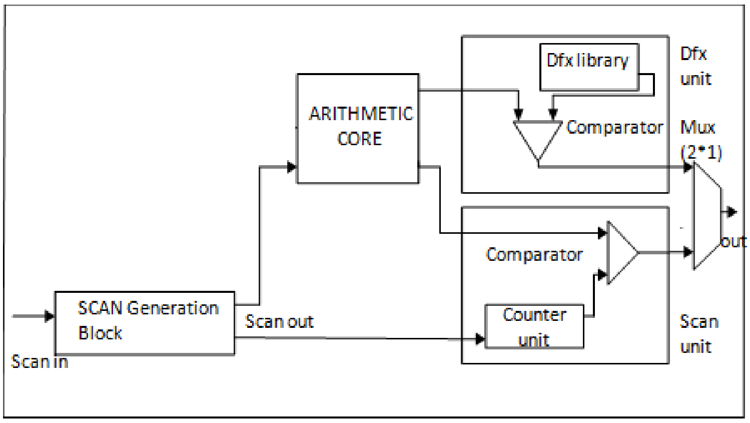


Fig 3.1 Proposed System(System Architecture)

The Arithmetic core unit represent the Functional Unit. It consist of instruction Register , Input Register and mainly a central processing unit (CPU) which consists of Control unit and ALU. And the ALU consist of adder unit only, this has been shown in Fig 3.2

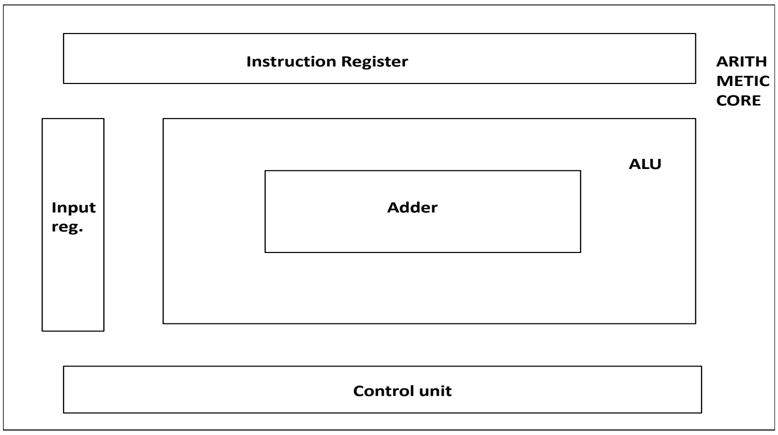


Fig 3.2 Arithmetic Core

A) Modified Scan Generation Block

The modified scan generation block consist of 18 Flip-flops and a XOR gate. Here the output of 18th Flip-flop is connected to the input of XOR gate and a feedback mechanism can be used. It is shown in Fig 3.3

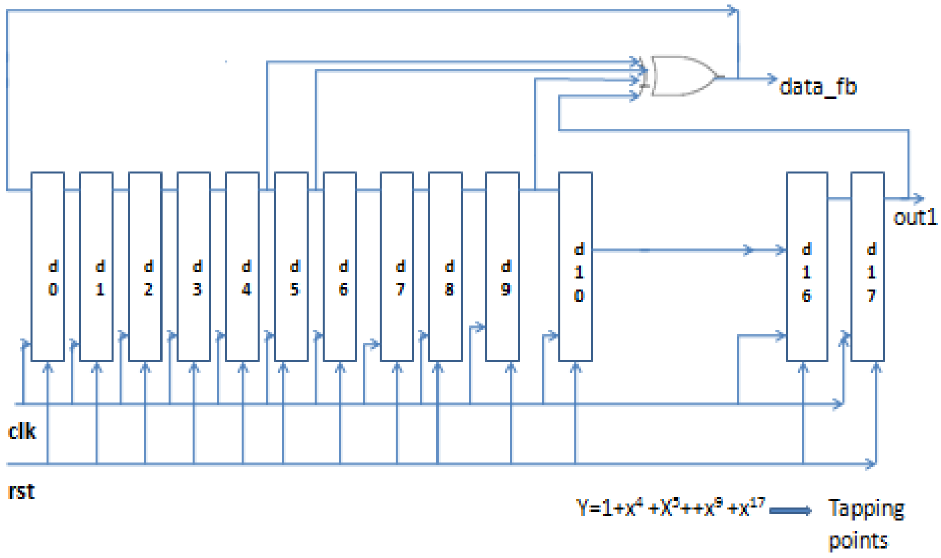


Fig 3.3 Modified Scan Generation Block

B) DFT Unit

The DFT unit consist of Dfx library and a comparator. The adder consist of mainly two inputs. Also this input will applied Reference adder. And it produces a output and it will compare with the original adder output. That is testing the combinational circuits. It is shown in Fig 3.4

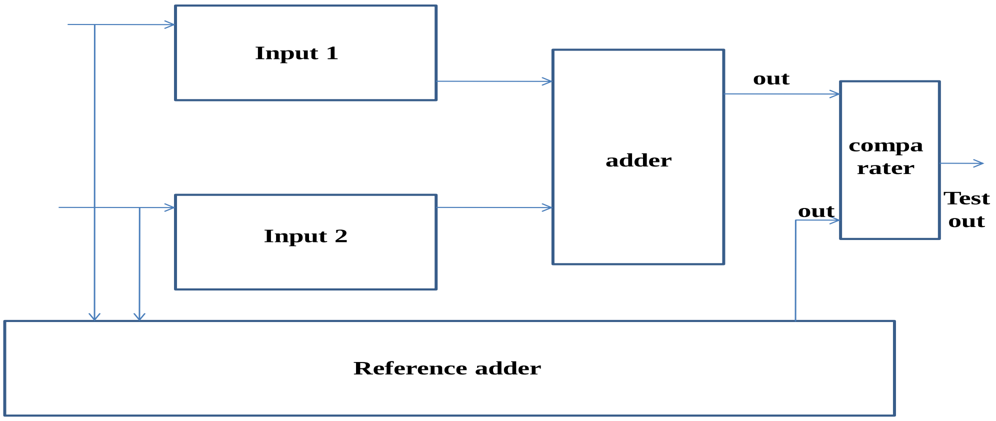


Fig 3.4 DFT Unit

C) Scan Unit

The scan unit consist of a comparator unit and a counter unit. It is shown in Fig 3.5 The scan generation block produces output which will give to the input of the core. This input can be used only for scanning. This input can also be applied to the counter block and this block produces an output. And this output will compare with the scanning output. That is testing the sequential circuits. Here the input register represents the sequential circuit.

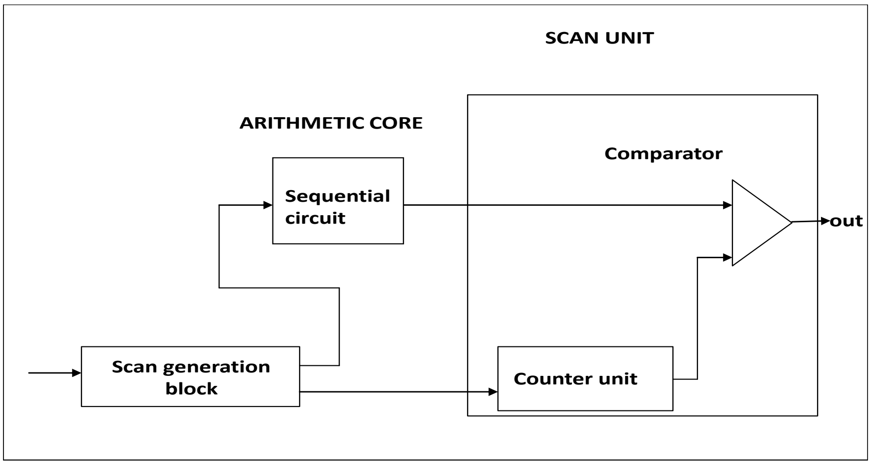
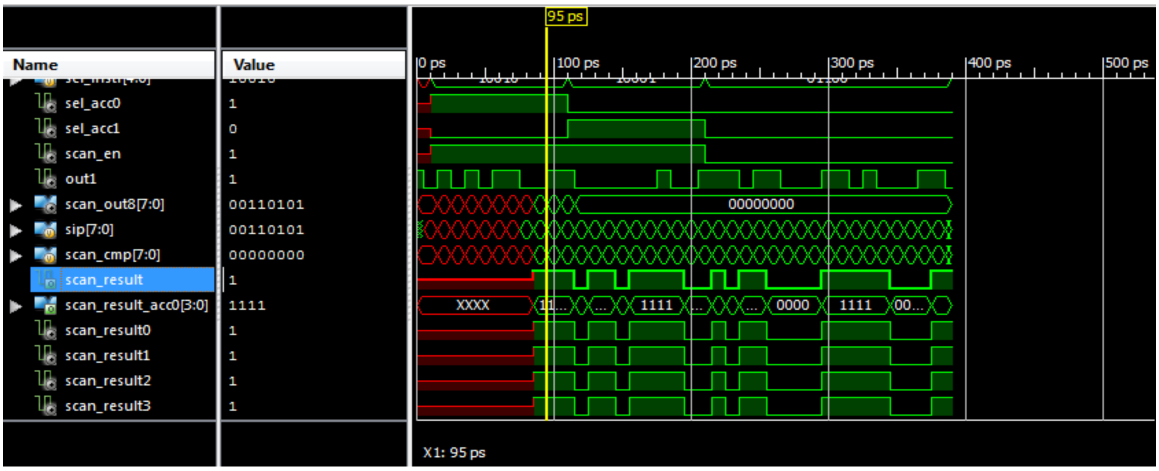


Fig 3.5 Scan Unit

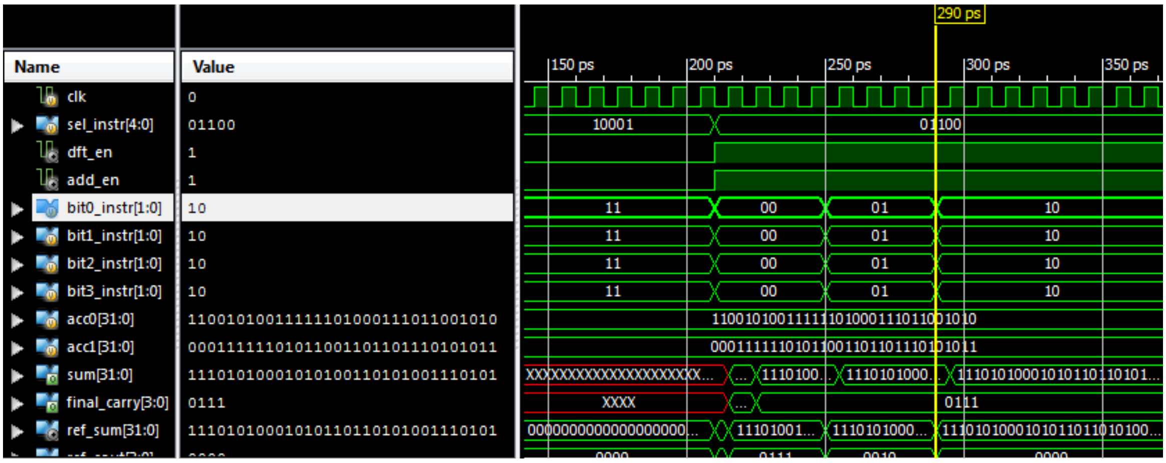
IV. EXPERIMENTAL RESULT

Implementation of proposed system is simulated in Verilog Hardware Description Language (HDL) for electronic circuit. The simulation result of tested sequential circuit is shown in Fig 4.1and the simulation result of tested combinational circuit is shown in Fig 4.2.Also the RTL schematic of the top module is shown in Fig 4.3.



Name	Value
sel_acc0	1
sel_acc1	0
scan_en	1
out1	1
scan_out8[7:0]	00110101
sip[7:0]	00110101
scan_cmp[7:0]	00000000
scan_result	1
scan_result_acc0[3:0]	1111
scan_result0	1
scan_result1	1
scan_result2	1
scan_result3	1

Fig 4.1 Simulation Result of Tested Sequential Circuit



Name	Value
clk	0
sel_instr[4:0]	01100
dft_en	1
add_en	1
bit0_instr[1:0]	10
bit1_instr[1:0]	10
bit2_instr[1:0]	10
bit3_instr[1:0]	10
acc0[31:0]	11001010011111101000111011001010
acc1[31:0]	00011111101011001101101110101011
sum[31:0]	11101010001010100110101001110101
final_carry[3:0]	0111
ref_sum[31:0]	11101010001010110110101001110101

Fig 4.2 Simulation Result of Tested Combinational Circuit

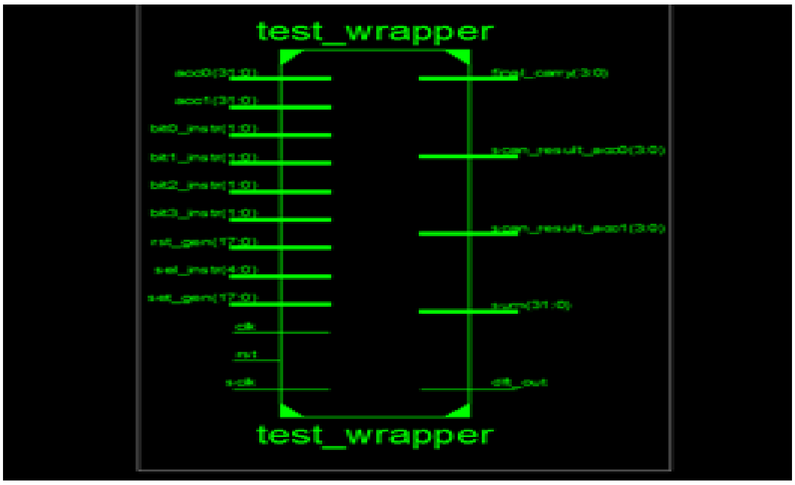


Fig 4.3 RTL schematic of the top module

V. CONCLUSION

The proposed system is a better option in scan based flip flop for secure cryptographic application. The mixed scanning and DFT techniques can be used without effect the operation speed of chip. Also proposed PN code generation unit as scan in port to increase the code coverage. In the case of modified scan generation block, it consist of more than 2 tapping points. That is 4 tapping points. Hence the security can be increased. Here a feedback mechanism can be used, hence Easy to manage and It can be tested with less effort. The Scan Generation block is mainly used to give the more secure inputs at the time of scanning. This does not effect the area.

The proposed system is applicable for wireless communication, Online mobile banking system, SIM cards, Identifications cards in organizations. All the above system holds certain sensitive information in the chip core which requires certain amount of security. The elliptic curve cryptography system provided the high level digital security against unauthorized access from unwanted person.

REFERENCES

[1]. Mr.K.P.Sridhar,Mr.M Raguram,Dr.S.Saravanana"Secure Elliptic Curve Cryptosystems For Scan Based VLSI Architecture"ISBN,2014,IEEE

[2]. Nathan Jachimiec, Nick Iliev, and James Stine, "Strategies forVLSI Implementations of Finite Field Inversion Algorithms", 48th IEEEInternational Midwest Symposium on Circuits and Systems, (pp. 1589 -1592),2005.

[3]. Gaurav Sengar, Debdeep Mukhopadhyay and Dipanwita RoyChowdhury, Secured Flipped Scan-Chain Model For Crypto-Architecture,IEEE Transactions On Computer-Aided Design Of Integrated Circuits AndSystems, Vol. 26, No. 11,(pp. 2080 - 2084), 2007

[4]. Youhua Shi, Nozomu Togawa, Masao Yanagisawa and TatsuoOhtsuki, Design-For-Secure-Test For Crypto Cores, IEEE InternationalTest Conference,(pp. 1), 2009.

[5]. Youhua Shi, Nozomu Togawa, Masao Yanagisawa and TatsuoOhtsuki, Robust Secure Scan Design Against Scan-Based DifferentialCryptanalysis, IEEE Transactions On Very Large Scale Integration (VLSI)Systems, Vol. 20, Issue: 1,(pp. 176 - 181), 2012

[6]. Yuta Atobet, Youhua Shi, Masao Yanagisawa and NozomuTogawat, Dynamically Changeable Secure Scan Architecture AgainstScan-Based Side Channel Attack, IEEE Soc Design Conference,(pp. 155 -158),2012.

[7]. Ajay Kumar, Kunal Lala and Amit Kumar "VHDLImplementation using Elliptic Curve Point Multiplication", InternationalJournal of Advanced Research in Computer and CommunicationEngineering,(pp. 392 - 398), 2012.

[8]. Ryuta Nara, Nozomu Togawa, Masao Yanagisawa and TatsuoOhtsuki "Scan-Based Attack Against Elliptic Curve Cryptosystems" InProceedings of IEEE ,(pp. 407 - 412),January2010.

[9]. Da Rolt, J.; Das A.; Di Natale, G.; Flottes, M.-L.; Rouzeyre, B.;Verbauwhede, I.; , "A New Scan Attack on RSA in Presence ofIndustrial Countermeasures", COSADE 2012, Lecture Notes inComputer Science Volume 7275, 2012, pp 89-104.

[10]. Yang, B.; Wu, K.; Karri, R.; , "Scan based side channel attack ondedicated hardware implementations of Data Encryption Standard,"International Test Conference, 2004.

[11]. Yang, B.; Wu, K.; Karri, R.; , "Secure Scan: A Design-for-TestArchitecture for Crypto Chips," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2006.

[12]. Da Rolt, J.; Di Natale, G.; Flottes, M.-L.; Rouzeyre, B.; , "Areadvanced DfT structures sufficient for preventing scan-attacks?,VLSI Test Symposium (VTS), 2011 IEEE, pp.246-251, June 2012.

[13]. Liu, Y., Wu, K., Karri, R.; , “Scan-based Attacks on LinearFeedback Shift Register Based Stream Ciphers,” ACM Transactionson Design Automation of Electronic Systems (TODAES) 2011.

[14]. Jean Da Rolt, Bruno Rouzeyre, Marie-Lise Flottes, Giorgio Di Natale, Amitabh Das, Ingrid VerbauwhedeA .”Scan-based Attack on Elliptic Curve Cryptosystems in presence of Industrial Design-for-Testability Structures”