ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 2, Issue 3, March 2013

Detection of Fault-Injection Attacks on Cryptographic Devices

Vamsi Krishna Kosuri[1], Dr. Fazal NoorBasha[2].

***Abstract*— with this document, we have proposed a simulation model to identify the fault injection attacks on Public key and Private Key Cryptographic devices, which are more susceptible to fault-injection attacks. As multiplier is the requisite element for all Cryptographic devices whenever an intruder has injected a fault, the multiplier data corrupts automatically and in this work the basic multiplier is designed with Booth encoded Wallace tree and the fault detection unit is proposed to design with Multi-modulus multilinear arithmetic code and then it is simulated to notice the respective changes across the multiplier data whenever there is a fault-injection and the procedure is tested and verified using Xilinx14.1.**

***Index Terms* — Fault-injection attacks, Multipliers, Public key and Private Key Cryptographic devices, Xilinx14.1 Vivado.**

I. INTRODUCTION

Cryptographic applications like ATM and other commercial electronics are more susceptible to side-channel attacks [1],[8]in which the fault injection attacks are more crucial at today's Deep Sub Micron Technology. Hence the identification and modeling of these attacks from the intruders are critical, playing a vital role and became a challenge for current trend of system designs. Therefore it is necessary to design the systems which are able to identify and to detect these intruder attacks on Cryptographic devices.

It is obvious that the multiplier is the fundamental block for Public key and Private key encrypted devices and they must be designed more secure in order to overcome these fault injection attacks, in this regards various proposals are exists to design these multipliers more secure to intruder fault injection attacks. One of the considerations for this proposed document is to design the basic multiplier with multi modulus multi linear architecture [1] and to enhance its features to add some identification mechanism against fault injection and the same can be modeled with advanced core FPGA.

Public-key cryptographic devices are vulnerable to fault-injection attacks. As countermeasures, a number of secure architectures based on linear and nonlinear detecting codes were proposed. Linear codes provide protection only in opposition to primitive adversaries with flawed attack capabilities, on the other hand nonlinear codes provides protection against strong adversaries, but at the price of high area overhead (200% - 400%).The proposed plan is a novel error detection technique based on protection technique of a multiplier which is a basic building block of many public-key cryptographic devices which is under nonlinear code error detection, Cryptographic devices are mainly suffers with various side channel attacks includes for timing analysis, power analysis and fault injection attacks[13].

The current Deep Sub Micron technology [12] is resilient to introduce timing attacks and power attacks but the chances to the intruder are to introduce fault injection attacks [3],[4] over the Cryptographic devices is becoming a new challenge to identify and it must need to be model to enhance the security for Cryptographic areas.

Since the multiplier will plays a vital role in all major Cryptographic algorithms, and also as per the design concerns it occupies much more area so as to consumes more power therefore the multiplier design parameters such as speed, area and power must count into account for reliability issues of the Cryptographic devices. An assortment of multiplier architectures are proposed for Cryptographic algorithms to guarantee the security of the devices, in this regards various error detecting techniques are also proposed some of them are, linear arithmetic codes, includes parity codes, Hamming codes, AN-codes etc. Non linear arithmetic codes [2],[7] like, Robust Codes and Multi linear arithmetic codes [5], each category has their strengths and limitations, therefore a proper study and observation is required to select a suitable detection algorithm.

Generally multiplier occupies more space when physical design[9],[11], is concerned and also as the increased bit size results more occupancy of chip area, the other factor which effects the efficiency of the multiplier is its partial product, consequently there is a strong reason that multiplier design for applications like Cryptography is always critical and crucial and hence design of multiplier with good tradeoff between area, power and speed is essential especially for Deep Sub Micron era.

In order to achieve this tradeoff the multiplier structure should be designed in such away that it produces the required product terms with less number of partial products

***1.Kosuri Vamsi Krishna** is a Student of MTech VLSI, department of ECE, KL University, Vaddeswaram, Guntur, AP, India – 522022.*
(Phone: +91 8885922257; email: krishna.kosuri@gmail.com).

***2.Dr. Fazal NoorBasha** is an associate professor and in-charge, VLSI Research Group, department of ECE, KL University, Vaddeswaram, Guntur, AP, India – 522022).*
(Phone: +91 9000502785; email: fazalnoorbasha@kluniversity.in).

and to increase the speed of this task let us add some reliable algorithm on to its structure so that it could tolerate the increased bit size.

The present article is alienated into three major areas. Firstly, the design of secure multiplier and extending its design abilities such that it can hold out the intruder attacks, secondly, the testing process of the multiplier architecture to ensure its perfectness with absence and presence of fault injections and finally to simulate the modeling of the design.

The rest of this paper is structured as follows. In section II, multiplier design with extended features is described. In section III, we design and analyze the detection arrangement for fault injection attacks. In section IV, the simulation results with and with out fault injection.

II. DESIGN OF MULTIPLIER

A Wallace tree is an efficient hardware implementation of a digital circuit that multiplies two integers, devised by an Australian Computer Scientist Chris Wallace in 1964. As per the speed factor is concerned the Wallace Tree multiplier[15] is the best alternative compared to its predecessors and an n-bit Wallace Tree multipliers is on the order of $O(\log(n))$ in terms of logic gates.

The benefit of the Wallace tree is that there are only $O(\log(n))$ reduction layers, and each layer has $O(1)$ propagation delay. As making the partial products is $O(1)$ and the final addition is $O(\log(n))$, the multiplication is only $O(\log(n))$, not much slower than addition (however, much more expensive in the gate count). Naively adding partial products with regular adders would require $O(\log(n^{2}))$ time. From a complexity theoretic perspective, the Wallace tree algorithm puts multiplication in the class NC. These computations only consider gate delays and don't deal with wire delays, which can also be very substantial. The Wallace tree can be also represented by a tree of 3/2 or 4/2 adders. It is some times combined with Booth Algorithm for best yield of required out put.

Booth's multiplication algorithm is a multiplication algorithm that multiplies two signed binary numbers in two's complement notation. The algorithm was invented by Andrew Donald Booth in 1950. Booth's algorithm examines adjacent pairs of bits of the N-bit multiplier Y in signed two's complement representation, including an implicit bit below the least significant bit, $y_{-1} = 0$. For each bit y_i, for i running from 0 to N-1, the bits y_i and y_{i-1} are considered. Where these two bits are equal, the product accumulator P remains unchanged. Where $y_i = 0$ and $y_{i-1} = 1$, the multiplicand times 2^i is added to P; and where $y_i = 1$ and $y_{i-1} = 0$, the multiplicand times 2^i is subtracted from P. The final value of P is the signed product.

The representation of the multiplicand and product are not specified; typically, these are both also in two's complement representation, like the multiplier, but any number system that supports addition and subtraction will work as well. As stated here, the order of the steps is not determined. Typically, it proceeds from LSB to MSB, starting at $i = 0$; the multiplication by 2^i is then typically replaced by incremental shifting of the P accumulator to the right between steps; low bits can be shifted out, and subsequent additions and subtractions can then be done just on the highest N bits of P.[1] There are many variations and optimizations on these details.

The algorithm is often described as converting strings of 1's in the multiplier to a high-order +1 and a low-order –1 at the ends of the string. When a string runs through the MSB, there is no high-order +1, and the net effect is interpretation as a negative of the appropriate value. Because of both advantages we will consider the Booth encoded Wallace tree multiplier as a basic element of error detection unit for Cryptographic application.

Let he multiplier has M-bits P and N-bits Q as input and generate M X N -bits output R, then P and Q can be represented as $P = \sum_{k=0}^{M-1} P_k 2^k$ and $Q = \sum_{l=0}^{N-1} Q_l 2^l$ such that the output R can be interpreted as $R = P \times Q = \sum_{k=0}^{M-1} (\sum_{l=0}^{N-1} P_k Q_l 2^{k+l})$. The output R is computed by adding the partial product $P_k Q_l$ together. The simplest implementation requires an N-bit adder and take M cycles to generate the output. Another implementation of multiplier is so called adder array multipliers which achieve higher speed at the cost of larger hardware. Several other technologies have been developed to improve the speed and reduce the power consumption of multiplier. There are two widely used approaches: booth algorithm and Wallace tree compressor, Booth algorithm can do multiplication on both non-negative and negative operand by using 2's complement number. Moreover, the booth algorithm can further decrease the number of partial product which can lead to substantially delay and area reduction.

Booth's algorithm follows this scheme by performing an addition when it encounters the first digit of a block of ones (0 1) and a subtraction when it encounters the end of the block (1 0). When the ones in a multiplier are grouped into long blocks, Booth's algorithm performs fewer additions and subtractions than the normal multiplication algorithm.

Wallace tree is a way of summing of partial product bits parallel. By using the Wallace method, both the critical path and the number of adders are reduced.

The basic idea is using a full adder as a 3-2 compressor to reduce the product matrix. The Booth encoded – Wallace tree multiplier design for the proposed work is summarized in the following table which contains the details of the design platform and it's deigns specifications.

The 20-bit, Radix-8 Booth encoded -Wallace Tree multiplier is included as the key element of detecting the fault injection attacks and its Verilog Description is modeled using Xilinx14.1.

TABLE 1
SUMMARY OF BASIC MULTIPLIER DESIGN

S.No	Content	Description
1	Algorithm	Booth encoding
2	Radix	8
3	Structure	Wallace Tree
4	Multiplier size	20 –bit
5	HDL	Verilog
6	Development tool	Xilinx 14.1

The 20-bit size may accommodate more encoded data for Cryptic Device and the 40-bit product may give more analysis probability for injected faults, the following section summarizes the design considerations and analysis of functional block for detecting the injected faults.

The building block of the Booth encoded-Wallace tree multiplier is shown in the following figure

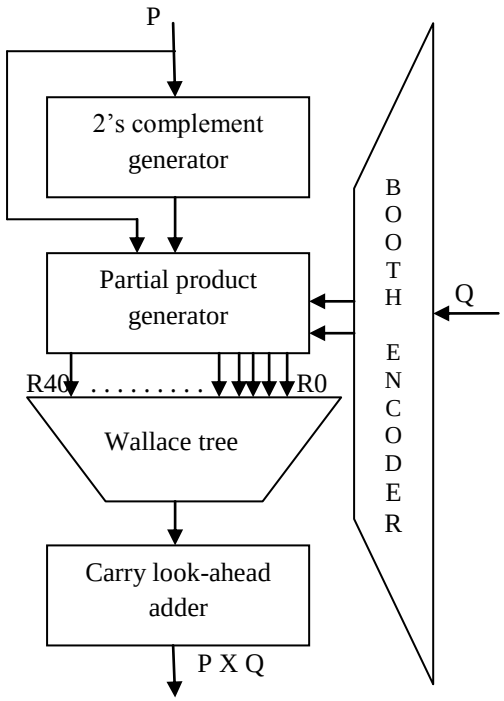

Fig.1. 20-Bit Booth Encoded Wallace Tree

III. MODELING OF FAULT DETECTION UNIT

As mentioned earlier, numerous error detecting codes [6] for Cryptographic applications are existed and their brief description is given here after.

Linear Arithmetic Codes: (ex: AN Codes, Hamming codes and Parity Codes etc.) they may work with a good accuracy but their abilities are limited because of the following reasons. They are suitable to a fastidious type of error (ex: error with odd multiplicity or byte error etc.), less sensitive to protect over unanticipated error, not recommendable to lazy channels, less and limited attack capability, not protective other than primitive adversities.

Non linear Arithmetic Codes: (ex: Robust Codes) they are again divided into robust arithmetic residue codes and robust algebraic codes, these are best suitable to built Cryptographic devices which uses the AES (Advanced Encryption Standards) and recommendable [14] especially devices uses arithmetic operations. They had advantages like: ability to overcome the weakness of Linear Codes, message dependability, best supportive for lazy channels, good fault detection capability and provision of equal protection over all error patterns. Still these codes are limited for practical implementation since, huge overhead of hardware because of need for encoding and decoding units.

Multi Linear Arithmetic Codes: the main principle of this category "is randomly selecting a code from multiple linear codes for each encoding and the corresponding decoding operations ". These codes will provides the advantages like good error detection capability, less amount of hardware overhead, no need of non linear operations for encoding and decoding, negligible amount of bad errors and the best mates for lazy channels. There fore in order to describe the error attacker model we recommend Multi linear Arithmetic Codes as the prime principle along with Booth Encoded Wallace tree as a basic element of the operation. Further reduction of hardware overhead can be achieved with multi modulus multi linear arithmetic codes. Generally the fault injection [10], can be represented as shown in the following figure.

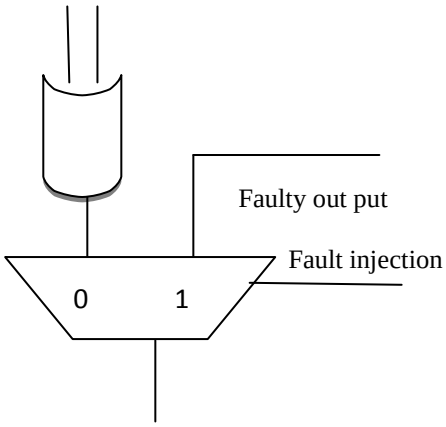

Fig.2: Fault injection in to gate.

The fault detection unit mainly contains three major blocks as described here, the basic multiplier, the error interpreter and the error detector.

Basic multiplier: Primary building block as described in section II.

Error Interpreter: This produces modulo operations on the two multiplier inputs.

Error Detector: Includes modulo operation on two multiplier inputs, selective element and a comparator unit.

The final arrangement is given in the following figure. The Booth encoded Wallace tree will produces the 40-bit product which is an input to the Error Detector, the Error interpreter whose inputs are modulus of primary inputs and with the help of a selective network any of modulo product can be given to the Detector, Error Detector unit contains again a modulo generator and a comparator network.

Whenever the fault is injected the predictor whose modulo operations are compared with another modulo values from original basic multiplier across the Error Detector, if the comparator output is zero which gives there is no fault injection else a fault injection can be noticed.

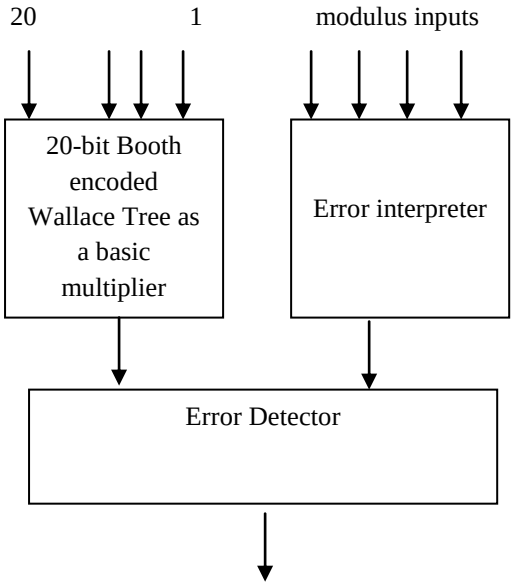

Fig.3 Fault Detection Model

As a consequence whenever there is a fault injection, correspondingly the product data may changes randomly, and depending on the bit size of the multiplier the error can be tracked with successive comparison technique. The description of this unit is done with Verilog and simulated and synthesized using Xilinx14.1; the results are analyzed in the next sections.

IV. SIMULATION RESULTS

The Verilog RTL Description of the above article is simulated using Xilinx14.1 (ISE-Simulator), and results are observed separately with and without fault inputs, it is noticed that at some instance of simulation time the product values are differs with and without fault presence the various results are shown in the following figure.4 and figure.5.

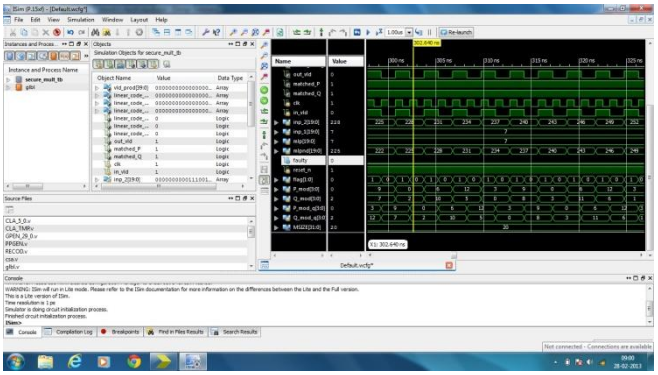

Fig.4. Simulation without Fault

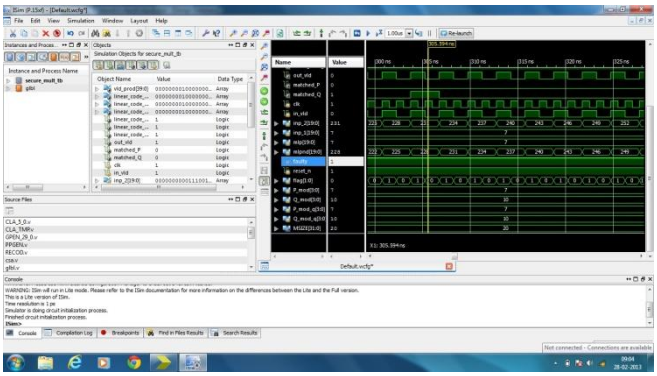

Fig.5 Simulation with Fault

When we analyze the simulation outputs it is observed that at similar instance of simulation time the data vales related to output product are different when fault is enabled.

V. CONCLUSION

This paper analyzes the simulation modeling of Fault injection attacks on Cryptographic Devices, the modified Booth encoded Wallace tree multiplier based fault detection unit is more reliable and good sensitive to Fault injection attacks, the multi modulus multi liner arithmetic block are superior and good counter parts compared to existed proposals. The hardware realization with these techniques are best measures to notice quickly the intruder attacks on the Cryptographic Devices and is possible to take necessary actions to prevent the malfunctions on Commercial Electronics.

ACKNOWLEDGMENT

We would like to thank Dr.Fazal NoorBasha, for his out standing support and also we would like to especially express gratitude EDUPLUS team for their technical advices.

REFERENCES

[1]. Zhen Wang, Mark Karpovsky and Ajay Joshi "Secure Multipliers Resilient to Strong Fault-Injection attacks using Multilinear Arithmetic Codes", *IEEE* – 2011.

[2]. K.D.Akdemir, Z.Wang, M.G.Karpovsky and B.Sunar, "Design o f Cryptographic devices resilient to fault injection attacks using nonlinear robust codes", in fault analysis in Cryptography. Newyork: Springer- verlag, 2011.

[3]. G.Canivet, P. Maistri, R. Leveugle, J.Cldire, F. Valette, and M. Renaudin, "Glitch and laser fault attacks on to a secure AES implementation on a SRAM –based FPGA", J.Cryptol., vol.24, no.2, PP. 1-22, Apr.2011

[4]. E.Trichina and R. Korkikyan, "Multi fault laser attacks on protected CRT – RSA", in proc.workshop on fault diagnosis tolerance Cryptography, 2010, pp.75-86

[5]. Z.Wang, M.G.Karpovsky, B.Sunar and A.Joshi, "Design of Reliable and secure multipliers by Multilinear arithmetic codes", information and communication security, ser.lec.notes in computer science, vol. 5927, pp.47-62, 2009

[6]. A.Krasniewski, "Concurrent error detection for finite state machines implemented with embedded memory blocks of SRAM-based FPGA's, Microprocessors and Microsystems", 2008.

[7].K.J.Kulikoski,M.G.Karpovsky, and A.Taubin "Robust codes and Robust,fault tolerant architectures of the advanced encryption standard". Journal of systems Architecture, 53:138-159, 2007.

[8].C.H.Kim and J.J. Quisquater, "How can we overcome bothside channel analysis and fault attacks on RSA-CRT?" in FDTC'07: proceedings of the workshop on fault diagnosis and tolerance in Cryptography, Washington, DC, USA: IEEE computer society, 2007, pp.21-29.

[9].B.Skoric,S.Maubach,T.Kevenaar,and, Tuyls.Iformation-"theoretic Analysis of Coating PUF's. Cryptology" eprint Archive,report 2006/101,2006.

[10].H.bar-El, H.Choukri, D.Naccache, M.Tunstall and C.Whelan, "The Sorcerer's apprentice guide to fault attacks," proc.IEEE, vol.94, no.2, pp.370-382, Feb 2006.

[11].I.Vasyltsov,E.Hambardzumyan,y.-s.Kim,and B.Karpinskyy, "Fast digital TRNG based on metastable ring Oscillator,"in.proc.Cryptograph.hardw.Embed.syst. Workshop (CHES), 2008, pp.164-180.

[12]. Nangate lnc.,Sunnyvale,CA, "Nangate 45nm opencell library," 2009.[0nline]. Available:http://www.nangate.com.

[13]. J.M. Schmidt and M.Hutter, "Optical and EM fault attacks on CRT-based RSA:Concrete results," in proc.15th Austrian Workshop Mi-croelectron..,2007,pp.75-86.

[14].D.Roberts,T.Austin,D.Blauww,T.Mudge,and K.Flautner, "Error analysis fro the support of robust voltage scaling,"in proc.6th lnt.Symp.Quality Electron .design(ISQED),2005,pp.65-70.

[15]. C.Wallace, "A suggestion for a fast multiplier," IEEE Trans.Electron.Comput, vol.EC-13, no, 1, pp.14-17, feb.1964.

Mr. K Vamsi Krishna is a Student of MTech (VLSI), Department of ECE, KL-University, Guntur, AP, India. He worked as a Senior Embedded Engineer with Viswaksha Design Solutions Pvt Ltd for five years. His area of interest is in Cryptography, low power VLSI, FPGA architectures, CMOS VLSI design and Embedded Systems.

Dr. Fazal Noorbasha was born on 29th April 1982. He received his, B.Sc. Degree in Electronics Sciences from BCAS College, Bapatla, Affiliated to the Acharya Nagarjuna University, Guntur, Andhra Pradesh, India, in 2003, M.Sc. Degree in Electronics Sciences from the Dr. HariSingh Gour University, Sagar, Madhya Pradesh, India, in 2006, M.Tech. Degree in VLSI Technology, from the North Maharashtra University, Jalgaon, Maharashtra, INDIA in 2008, and Ph.D. Degree in VLSI Specialization from Department Of Physics and Electronics, Dr. HariSingh Gour Central University, Sagar, Madhya Pradesh, India, in 2011. Presently he is working as a Associate Professor and VLSI Systems Research Group Head, Department of Electronics and Communication Engineering, KL University, Guntur, Andhra Pradesh, India,.

He is a Scientific and Technical Committee & Editorial Review Board Member in Engineering and Applied Sciences of World Academy of Science Engineering and Technology (WASET), Advisory Board Member of International Journal of Advances Engineering & Technology (IJAET), Reviewer of International Journal of Engineering Sciences Research (IJESR), Life Member of Indian Society for Technical Education (ISTE), Member of International Association of Engineers (IAENG) and Senior Member of International Association of Computer Science and Information Technology (IACSIT). He has published over 50 Science and Technical papers in various International and National reputed journals and conferences.