Fault Tolerance Technique for FPGA Implementation of Cryptographic Circuit

Rahul Karpe[1], Pravin Matte[2]

[1, 2] Department of Electronics and Telecommunication

[1, 2] G.H.R.C.E.M., Pune, Maharashtra, India

Abstract- *Reconfigurable devices are the programmable devices used to execute complex capacities in applications like space missions, correspondence frameworks, atomic frameworks and so forth. They are prominently known as the field programmable gate array (FPGAs).The FPGA is used in many applications such as cryptography, reliability of hardware is very much vital. The framework or system should be designed as a fault tolerant system. Fault tolerant is the capacity of a system to work typically given the state of defects or in any faults i.e. stuck-at-1, stuck- at-0. FPGAs have made it possible to consolidate adaptation to internal failure into frameworks at less expensive cost. In order to design fault tolerance technique the idea of TMR that is Triple Modular Redundancy is utilized.*

Keywords- TMR, Advance encryption standard, Cryptography.

I. INTRODUCTION

In our step by step process we utilize smart cards, ATM cards, credit cards for exchange reason. Security is similarly as strong as its weakest association. In all cases security is vital.We can without quite a bit of an extend find cryptographic devices, for instance, ATM cards wherever in our step by step lives from continuing managing an account cards to SIM cards for GSM [1][4]. One of the principal reasons why these cryptographic equipment gadgets are for the most part used? Since they are acknowledged to be more secure, this is the reason they have the execution of various cryptographic traditions. Regardless, late change of physical attack shows that a straightforward execution of cryptographic traditions does not give security any more. In brilliant cards each client has given a special unmistakable verification number and secret word is suited ID reason. This secret key is guaranteed with an encryption key which might be as bits of 0 and 1 or it might be in some other code words like picture. When we enter this password it is decoded in an interesting shape and offer it to the relating client. Regardless of occasion of a couple of shortcomings, for instance,logical fault,physical fault [6] if any of the bits is changed at that point fault will happen and the resultant decoded key won't coordinate. Subsequently for this circumstance we have to become such a model which will recognize such fault and furthermore correct it.

The impelling of a fault through to a recognizable frustration takes after a particularly described cycle. At whatever point executed, a fault may realize an oversight, which is an invalid state inside a system restrain. A mistake may bring on extra error inside as far as possible, as needs be each new error goes about as a fault and be perceivable. Exactly when mistake states are seen at as far as possible they are named as defective. This framework is named as fault error failure cycle and is a key instrument in reliability. Numerous specialists have built up a few strategies for deal with these faults. Cryptosystem utilizes AES, Chinese remaindering calculation, RSA [7] [8]. In cryptographic gadget we utilize AES calculation that is advance encryption standard [2]. In such gadget the encoding key is open and shifts from decoding key which is individual and kept as a secret. The information which is to be sending is a plain content, by utilizing key it will encode the information. Exactly when any content or mail is sent from any of the client, there is part of chances that attackers can hack the information and take off changes in the data which incorporates the faults in data consequently remembering the true objective to sidestep this wrong data transport, those encryption and decoding is consistently checked and when fault happens it should be tolerated. The data which client needs to send is plain substance data by using the key he will encode this data and get the figure content data.

This cipher text information as a matter of first importance he will send and received output on spartan6 board furthermore on the GUI screen which is produced in Matlab. For this situation no single fault is infused. After that by means of switches which are available on the spartan3 board faults are added. Those are only Stuck-at-0, Stuck-at-1 and Transient fault. At once single fault is included and faulty output can be seen on the Spartan3 board and in addition on the Graphical User Interface. In order to endure the impact of this fault, fault tolerant procedure is created and for that the idea of TMR (Triple Modular Redundancy) is utilized. In computing, triple modular redundancy is a fault-tolerance form of modular redundancy, there are three system block to perform a process and to produce a single output the result is processed by a majority-voting system.

In triple modular redundancy concept, as we are adding one of the fault at a time i.e. Stuck at 0 or Stuck at 1 or Transient fault. Accordingly we get the three outputs output1, output2 and output3.By means of this triple modular redundancy concept we will compare this three faults with each other so as to get faultless output.

II. RELATED WORK

In October 2005, Russell Tessier and Wayne Burleson [1] have display an energy aware smart card architecture that works utilizing an inserted battery and precious stone is clarified. This low-control VLSI framework is consistently dynamic and gives upgraded security through intermittent inward redesign when the card is disengaged from a reader. This architecture is spurred by applications, for example, for- ward security techniques. The dynamic lifetime of the model is improved by the utilization of circuit plan energy aware architectural techniques. This smart card model interfaces to smart card reader and gives encryption scratch upgrade to improve security. The architecture has been appeared to be good with existing battery innovation.In this paper a proof of concept prototype implementation has been developed includ- ing register transfer level and gate level designs which have been synthesized to silicon.

In July 2006, Kris Tiri and Ingrid Verbauwhede [2] have the idea regarding the Small embedded integrated circuits for ex- ample smart cards are defenceless against side-channel attacks (SCA) is given. The assailant can pick up data by observing the power utilization, execution time, electromagnetic radiation, and other data spilled by the exchanging conduct of digital CMOS gates. This paper presents a digital VLSI outline stream to make secure power-analysis-attack-resistant ICs.This paper portrays how to change the library databases with the end goal that the normal single-finished static CMOS cells actualize a dynamic and differential logic style and to such an extent that more than 20,000 differential logic styles can be route in parallel. Starting late, a couple assaults that usage information spilled by the indicated side channels to find the secret key have been displayed.

In July 2007, TAN Yanghong, HE Yigang[3] have proposed a hierarchical neural networks (HNNs) method for fault diag- nosis of large-scale circuits. The exhibited systems utilizing neural networks approaches require a lot of calculation for reproducing different broken segment potential outcomes. For large scale circuits, the quantity of conceivable issues, and thus the recreations, become quickly and ended up dreary and some of the time even illogical. The technique is portrayed by redusingthe over-lapped possible spaces of responses of circuits with resistance and prompts better execution and higher right characterization. The framework is spoken to by technique for assurance cases. This venture delineates that A various levelled strategy for fault analysis of extensive scale circuits is proposed. The structures of neural systems will be excessively convoluted, making it impossible to merge to their adjust states on the off chance that they should take in all element vectors acquired by (wavelet parcel) decay when the size of circuit is substantial. The various levelled technique is portrayed by diminishing the over-lapped attainable areas of reactions of a circuit with resistance prompting better execution of neural systems and higher right grouping to the issues of the circuits.

In November 2008, Radu Muresan and Stefano Gregori [4] have present a circuit that secures smart cards against differential power examination assaults. The circuit relies on a current fixing technique and is composed utilizing a standard 0:18 m CMOS innovation and can be coordinated in a similar package with the smart card micro controller. We assess the current straightening execution and the vi- ability of the insurance against differential power analysis attack exhibiting an examination in light of transistor-level recreations utilizing trial current follows gathered from a 8 bit micro controller for smart cards executing data encryption standard for encryptions. This paper adds to laying out the obstructions of differential power examination assault and shows how a circuit with little zone and low power can fill in as a convincing countermeasure. Side channel assaults misuse the defencelessness of convention, cryptographic calculations consolidated with extra data spilled amid the operation of a cryptographic device.

In February 2012, Chong Hee Kim [5] has represents that differential fault analysis DFA finds the key of utilizing differential data amongst right and faultyfaulty cipher texts acquire by initialize fault during the action of calculation of cipher text. Among many cipher information,advanced encryption standard (AES) has been the fundamental focus of DFA as a result of its unmistakable quality. From a traditional point cryptanalysis is a abstract scientific thought. In any case, practically speaking calculations must be executed on genuine physical gadgets that are exhibited to side channel attacks like power attack,electromagnetic attack as well as fault attacks. Differential fault survey is one of the fault assaults used to break cipher utilizing differential data among right and faulty cipher texts. An assailant gets faulty cipher texts by glitch, voltage variety and giving outside effect on a gadget with laser and so forth. Due to its multifaceted nature, DFA on advance encryption standard key schedule require more matches of right and broken cipher content than DFA on advance encryption standard State. Furthermore, they have utilized a multi byte blame model, which is dicey in 16-bit design. In this paper assaults diminish the amount of sets of right and defective cipher texts in view of a one-byte blame model. Furthermore, assaults incite inadequacies one round sooner than the present ones. Thus it is shown that one more round ought to be ensured to avoid DFA on advance encryption standard .

In March 2015, Mostafa Taha and Patrick Schaumont [6] have illustrate that Side channel analysis (SCA) misuses the data spilled through accidental yields, for example power consumption, to uncover the secret key of cryptographic modules. The genuine risk of SCA lies in the capacity to mount assaults over little parts of the key and to total data over various encryptions .In this paper, a nonexclusive structure of lightweight key redesigning that can ensure the current cryptographic principles and assess the base necessities for heuristic SCA-security. At that point an entire answer for ensure the execution of any standard method of Advanced Encryption Standard.

In 2012,K. Jarvinen, C. Blondeau, M. Tunstall [8],presents an expansion of the byte fault attack on signature plans displayed by Giraud et al. this work broadens their attack in various ways, however the fundamental center is an optional fault model propelled by existing fault injection comes about. Rather than expecting faults are uniformly distributed (i.e., a given bit is flipped with probability 1 by 2), we consider the situation where faults are one-sided (i.e. the probability differs from 1 by 2). This outcomes demonstrate that injecting one- sided shortcomings permits an attacker to uncover security- critical information with essentially less faults or fundamen- tally speedier search through the remaining candidates.

III. SYSTEM MODEL

The overall system consists of PC, serial to USB convertor, Reconfigurable FPGA, Fault injection circuit, LED, LCD display. After analysing advantages and drawbacks of different method, we are proposing new method that combines fault injection and fault tolerant technique together to enhance the security [5] and protection. Following figure shows complete block diagram of our proposed system.

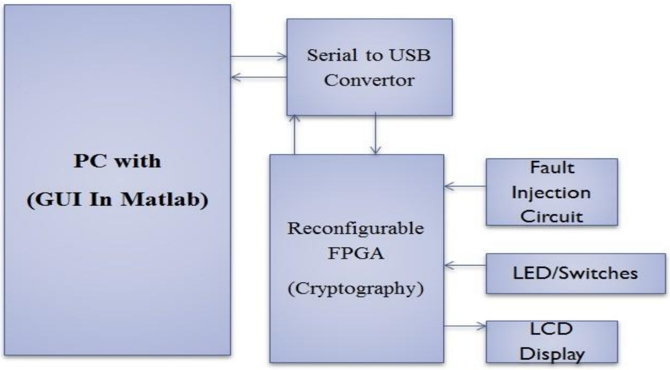
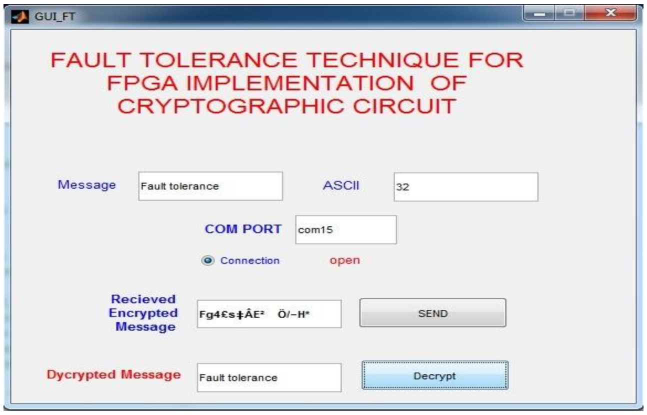


Figure 1. Block Diagram of Proposed System

The working of every segment is given below:

- Matlab is used for making the graphical user interface (GUI) and taking the contribution through serial to par- allel port.
- Reconfigurable FPGA is playing out the task by taking the contribution from Fault injection circuit.
- In FPGA cryptographic, operations are performed to fault tolerant.

GUI stand for graphical user interface, we add some text convert it into the ASCII value and send it to the USB to serial convertor. After designing GUI, save this window by right clicking on each button choose view callback in that callback option then the matlab editor window will be displayed and corresponding code for respective button will be displayed. We can write the code in this window as per our requirement. Simulation of GUI is shown in figue 2. In this, we select COM port when we connect serial to USB converter, after that we check the connection is open or close. Then we type the message and send the data.After sending this message, we get the encrypted output and by pressing decrypt button we get the same message.


GUI_FT

FAULT TOLERANCE TECHNIQUE FOR
FPGA IMPLEMENTATION OF
CRYPTOGRAPHIC CIRCUIT

Message: Fault tolerance

ASCII: 32

COM PORT: com15

● Connection open

Recieved Encrypted Message: Fg4£s‡ÂE² Ö/–H*

Dycrypted Message: Fault tolerance

Figure 2. GUI

FPGA is nothing but our cryptographic circuit. Cryptogra- phy mainly includes:

- Plaintext - the first message which we need to send.
- Cipher text - the coded message which is only a mix of our plaintext information and key.
- Cipher- calculation for changing plaintext to Cipher text.
- Key information used in cipher known only to sender and receiver.

As shown in figure 3, A message in its original form is known as plaintext. The mangled information is known as cipher text. The process for producing cipher text from plaintext is known as encryption. The reverse of encryption is called decryption. While cryptographers invent clever secret codes, cryptanalysts attempt to break these codes. These two disciplines constantly try to keep ahead of each other. Ulti- mately, the success of the cryptographers rests on the plaintext, cipher text ,plaintext encryption, decryption Cryptographic systems tend to involve both an algorithm and a secret value. The secret value is known as the key.

AES[5] and also most encryption calculations is reversible, as shown in figure. This implies nearly similar strides are performed to finish both encryption and decoding backward request. The AES calculation works on bytes, which makes it more straightforward to execute and clarify. As specified before AES is an iterated block cipher. Every one of that implies is that similar operations are performed commonly on an altered number of bytes. These operations can without much of a stretch be separated to the following functions:

1) ADD ROUND KEY
2) BYTE SUB
3) SHIFT ROW
4) MIX COLUMN

In fault injection block we use TMR technique i.e. triple modular redundancy, which is as shown in below figure. As shown in diagram data is nothing but text which we have to send it. Same data is given to all, one of them we add some fault like stuck-at-0, stuck-at-1, or transient fault. For adding fault we use some switches. By using detection and correction block it will check the output of given data and compare them. After comparing it will check and correct it and here we get proper output. To encode information we utilize AES algorithm. AES is an iterated symmetric block cipher, which implies that AES works by repeating the same defined steps multiple times.

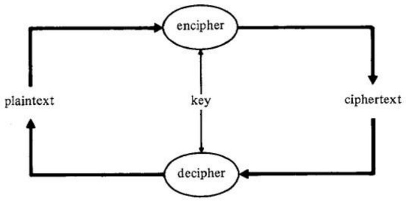


Figure 3. Secret Writing

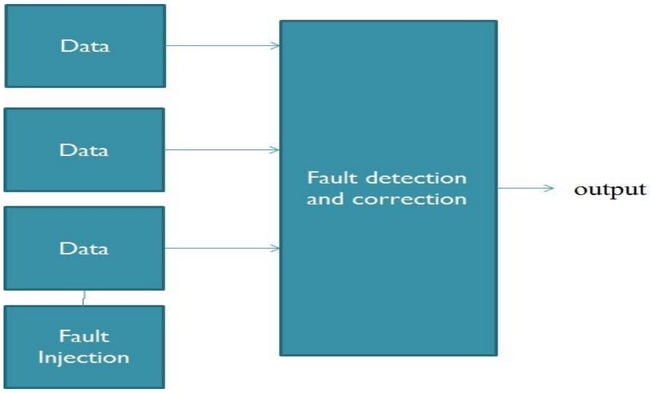
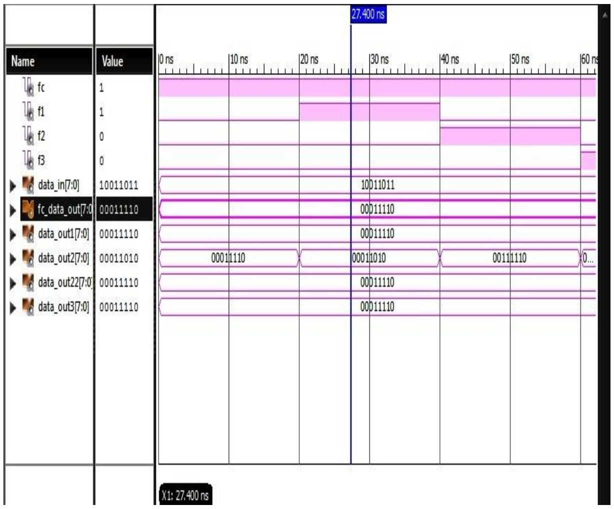


Figure 4. Tripple Modular Redundancy

IV. RESULTS

Cryptography assumes an imperative part while doing the security level investigation of smart cards and communication area. As it chips away at encryption and decoding keys, they are not that much simple to adjust their keys or roll out any improvement in their individual information. In any case, because of different fault as we have as of now said this encrypted data may be change. We are going to check the transmitted information and will get the information by method of GUI. Any adjustment in the information will be recognized by looking at the transmitted and received data. In order to design fault tolerance technique the idea of Triple Modular Redundancy (TMR) is utilized. For AES, we use Xilinx tool. Figure 5 shows advance encryption standard output for given 8-bit input that is ’10011011’.To encode this data we swap the first four bit with last four bit and stuck at 0 is added at second position, stuck at fifth position and transient fault is added at sixth position by using TMR technique it will correct it.



Name	Value
fc	1
f1	1
f2	0
f3	0
data_in[7:0]	10011011
fc_data_out[7:0	00011110
data_out1[7:0]	00011110
data_out2[7:0]	00011010
data_out22[7:0]	00011110
data_out3[7:0]	00011110

Figure 5. AES output

REFERENCES

[1] Russell Tessier, David Jasinski, Atul Maheshwari, Aiyap- pan Natarajan, Weifeng Xu, and Wayne Burleson, ”An Energy-Aware Active Smart Card,”IEEE Transaction on Very Large Scale Integration(VLSI) Systems,Vol. 13,No.10, Octo- ber 2005.

[2] Kris Tiri and Ingrid Verbauwhede, ”A Digital De- sign Flow for Secure Integrated Circuits,” IEEE Transaction on computer-aided design of integrated circuits and systems,Vol.25,No.7,July 2006.

[3] TAN Yanghong, HE Yigang, FANG Gefeng, ”Hierarchical Neural Networks Method for Fault Diagnosis of Large- Scale Analog Circuits,” Tsinghua Science and Technology, July 2007, IEEE Transaction on Information Forensics and security, Volume 12, Number S1, ,July 2007.

[4] Radu Muresan, Member, IEEE, and Stefano Gregori, ”Protection circuit against differential power analysis attacks for Smart Cards,” IEEE Transaction on computer, Vol. 57, No. 11, November 2008.

[5] Chong Hee Kim, Improved Differential Fault Analysis DFA on AES Key Schedule,IEEE Transaction on Information Forensics and security,Vol. 7 No. 1,February 2012.

[6] Mostafa Taha and Patrick Schaumont, ”Key Updating for Leakage Resiliency With Application to AES Modes of Operation,”IEEE Transaction on Information Forensics and Security,Vol.10,No.3,March 2015.

[7] A. Pellegrini and T. Austin, Fault-based attack of RSA authentication, in Proc. Design, Autom., Test Eur., 2010, pp. 855860.

[8] K. Jarvinen, C. Blondeau, D. Page, and M. Tunstall, ”Harnessing biased faults in attacks on ECC-based signature schemes,”in Proc.WorkshopFault Diagnosis Tolerance Cryp- tography, 2012, pp. 7282.