I. J. Computer Network and Information Security, 2020, 4, 41-50
Published Online August 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2020.04.04

Design and Implementation of Reliable Encryption Algorithms through Soft Error Mitigation

Jamuna S
Dayananda Sagar College of Engineering, Bangalore, India
E-mail: jamuna-ece@dayanandasagar.edu

Dinesha P
Dayananda Sagar College of Engineering, Bangalore, India
E-mail: drdinesh-ece@dayanandasagar.edu

Kp Shashikala
Dayananda Sagar College of Engineering, Bangalore, India
E-mail: shashikala-ece@dayanandasagar.edu

Kishore Kumar K
Dayananda Sagar College of Engineering, Bangalore, India
E-mail: kishorekalluri8@gmail.com

Received: 04 February 2020; Accepted: 06 March 2020; Published: 08 August 2020

Abstract: Designing a reliable system on reconfigurable devices has become a significant factor for implementing mission critical applications like communication protocols, automotive, nuclear reactor control, and remote applications. With the improvement in fabrication technology, logic density of the field programmable gate arrays has increased rapidly. Because of decrease in feature size, integrated circuits are becoming vulnerable to errors and also the ageing component results in run time faults. FPGAs when used in harsh conditions like high radiation and temperatures, there is a possibility of getting affected by transient faults or the soft errors. In digital communication, safety and confidentiality of data is achieved through a suitable encryption algorithm. Encryption is most important aspect when it comes to security. Reliable design techniques are very much necessary for maintaining the system's normal function. Many of the available techniques are based on redundancy logic causing area overhead for the design. Through this paper, an implementation is illustrated for managing soft errors or the single event upsets. Proposed methodology identifies and avoids the errors occurring at the logic resources where the encryption algorithms are mapped on the device. Thus encryption algorithms work normally without getting affected by the errors. During the simulation process, errors are injected at the configuration memory frames and monitored using a Single event-upset manager (SEM) controller. The proposed design is implemented on Zedboard using Xilinx Vivado 2017.4.

Index Terms: Encryption, Fault Tolerance, SEM Controller, Partial Reconfiguration, FPGA.

1. Introduction

Nowadays, field programmable gate arrays (FPGA) are used in implementing a wide variety of applications starting from a simple logic function realization to space missions. The functionalities mapped on FPGAs need to give proper expected output without getting affected by disturbances occurring in the surrounding environment as well as in the hardware itself. Possible disturbances which can affect the implemented systems are the faults. These may be temporary or permanent in nature. Temporary faults occur mainly because of variations in the environmental conditions- temperature, pressure and high energy radiations etc [1]. Reasons for permanent faults are electro-migration and aging of the device. Soft errors are also referred as single /multiple event upsets. Permanent faults include stuck-at-0/1 faults. In order to make a system reliable, a mechanism to detect faults and avoid their negative consequence on the system's normal function is most important. Handling temporary faults is somewhat easy as compared to managing permanent faults. An efficient technique or methodology for handling both temporary and permanent faults is need of the hour. Many techniques have been developed for managing fault effects across FPGAs.

In data communication, cryptography strengthens security by encrypting and decrypting data. There are various algorithms for encryption which are classified as symmetric (if same key used) and asymmetric key (if different key used) encryption. Advanced Encryption Standard (AES), Blowfish, Twofish, Rivest Cipher-5 (RC5), 3-Data Encryption Standard (3DES) algorithms are the commonly used symmetric type algorithms [2]. In the proposed design AES and Twofish algorithms are considered.

Rijmen and Jhon Deamen developed AES algorithm hence also named as Rijndeal algorithm. It is considered to be the best alternative for Data Encryption Standered (DES). AES [3, 4, 5] hold well with both software and hardware. AES has fixed block size i.e. 128-bit and has three different key lengths i.e. 128, 192 and 256 bits. AES has 10 rounds for 128 bits key and 12 rounds for 192 bits key and 14 rounds for 256 bits key. It is successor of SAFER, Blowfish and Square. Similar to AES, Twofish [6, 7, 17] also has a fixed block size and different key lengths extendable up to 256-bitswith a total of 16 rounds. Twofish has a feistel structure.

In most of the previous design implementations, only one encryption algorithm at a time is been considered unlike the proposed work. But flexibility for the system can be brought by including more than one encryption algorithms. This can be realised by using two or more algorithms in one design but it increases the resource utilization and also power. To overcome this there is an interesting feature in FPGA called Partial Reconfiguration(PR) [8] is used in implementation. PR allows accommodating two or more algorithms in a single design but activating one at a time in only one specified area hence reducing both resources and power. Proposed work is mainly based on this concept.

StaticRAM(SRAM) based FPGAs consists of mainly Configurable logic block(CLBs), DSP, blockRAM(BRAM) and also an embedded processor i.e. for 7 series FPGA ARM processor. Normally the logic resources (CLBs) will be configured in the programmable logic region as per the user design. It means that the internal configuration memory which is the base for the LUTs will be configured as per the required design. Configuration memory is a structure made of SRAM cells and is susceptible to radiation effects. Whenever the device is exposed to radiations, single/multiple event upsets are caused there by changing the original configured data. When configuration data is modified by the induced faults, the actual output changes. To avoid system's failure, proposed work uses an error mitigation mechanism using a built-in IP called Soft Error Mitigation (SEM) [9] available in Xilinx Vivado IDE. Errors are injected in the random locations of the configuration memory that affect the design and also are corrected.

The paper is organized as follows: section II, outlines previous related work; section III, briefly describes the SEM Controller; section IV, describes the proposed design implementation; section V, briefs Results and discussion; The conclusion and future work are followed in section VI.

2. Previous Related Work

Many researchers have proposed different techniques to manage soft errors in FPGAs. [10-15] Adewale Adetomi et al [10], designed ICAP Controller with a selective-area soft error Mitigation Engine. They tried to scan selective-area of the FPGA instead of entire device which saved them the time available for reconfiguration. Designed SEM controller is able to detect and correct soft errors however; SEM IP was not used for injecting the errors. This was the limitation. Swagata Mandal [11] have proposed a new error correcting code to protect configuration memory of FPGAs from soft error, which gives better performance compared to the other commonly used error correcting codes. They also proposed hardware architecture with partial reconfiguration for the designed code. S. Nidhin et al [12] worked on error injection in the logic function modifying VHDL code. For analyzing the concept redundancy and duplication with compare were used.

Verification was done by simulation with fault injection. Hamming code was utilized for double error detection and single error correction across the configuration memory. They have not implemented on the hardware kit. Mohamed Elhady KESHK et al, [13] proposed a method for injecting and mitigating faults based on essential bits of FPGA. Dynamic partial reconfiguration was used for selecting a type of modulation block. Built-in SEM IP and the ICAP interface was used for mitigating the errors. Through Matlab program, errors were injected at run time. They mainly targeted on reducing time needed for injecting and mitigating the errors. Aitzan Sari et al, [14] have concentrated on soft error effects occurring across built-in soft processors of the FPGA device. Their designed platform acts as an open-source frame work facilitating fault injection and fault monitoring. Fault identification was done as an application execution profiling. Naifeng Jing1et al, [15] have considered soft error management across routing of FPGAs. They developed a masking mechanism for managing faults. This technique is based on in-Place inversion of look-up table(LUT) logic polarities. It aims at masking faults across multiplexers of device interconnect.

3. Soft Error Injection and Mitigation

Configuration memory of the XILINX FPGA holds the data for mapping the required design on to the available LUTs. In a six input LUT, sixty four 1-bit memory locations are available. These LUTs are made of SRAM cells. When these memory cells are exposed to high energy particles, bit errors are induced there by flipping the contents configuration memory. Since it is an environment related incident, it becomes very difficult to model this error induction process.

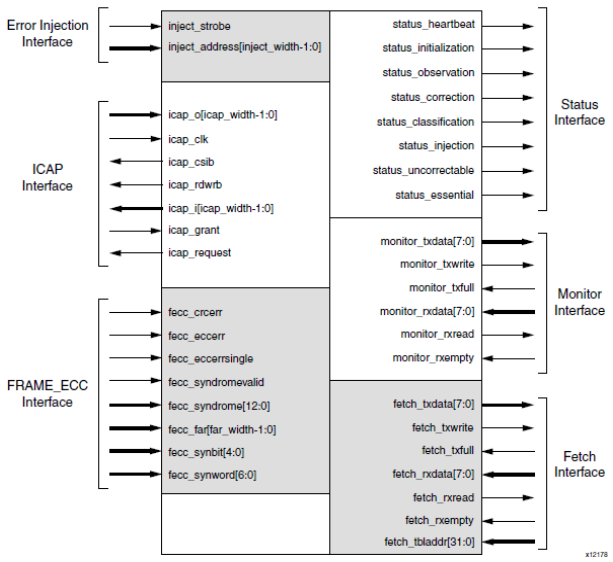

Fig.1. SEM controller block diagram [4]

Injecting errors by using radiation sources is costly and time consuming. And also accessing the configuration memory is a tedious process. So with the help of SEM IP available in Vivado IDE, soft errors can be injected and monitored easily. It allows user to inject errors and correct them simultaneously. SEM injects errors or faults similar to ionization radiation at frame level. Since the ionization radiation flips the data present in configuration memory, SEM also does the same i.e. in a selected frame, it injects fault by flipping the data present at selected word and bit. SEM monitors all the frames in a FPGA at real time. SEM makes use of FRAME_ECC and ICAP [3] to detect the errors and to access configuration memory respectively as shown in fig. 1.

Frame_ECC [16] used to detect single and double errors by calculating a 13 bit syndrome value. The syndrome value will be zero if there no errors present in the frame as shown in fig. 2.

Errors are injected using inject strobe and inject address. Inject strobe allows to inject the error and inject address is the address where error should be injected; this can be either linear frame address or physical frame address.

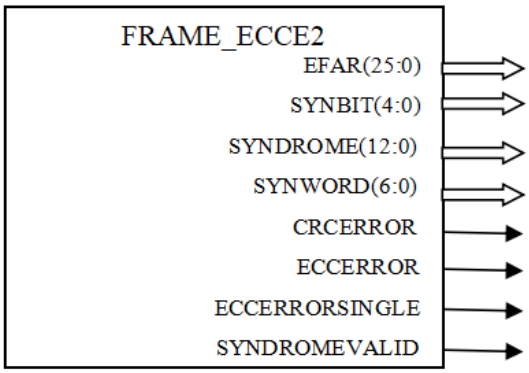

Fig.2. Frame_ECC block diagram

For correcting errors SEM has three different strategies namely Repair, Enhanced Repair and replace which are in detail explained in [9].

4. Design Methodology

In the proposed design, two encryption algorithms are defined as partial blocks so that depending on the requirement any one of them can be activated at a time. This is done for providing flexibility for the user. Fig 3 depicts the overall concept. Two separate sections of PS and PL of the FPGA are shown. SEM controller IP is included with the encryption modules to inject and correct errors and a VIO interface to monitor the provide inputs and monitor the outputs. The two encryption algorithms of AES and Two-fish are mapped in the PR region. Out of these two, any one algorithm will come in to action at a time. The error injection and correction through SEM are performed using UART and RS232. In SEM there are two states i.e. IDLE and OBSERVATION state.

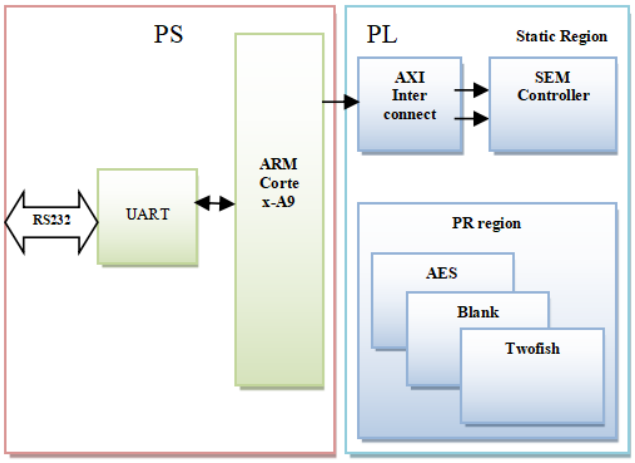

Fig.3. Block diagram of proposed design

AES and Twofish algorithms are designed and configured separately as per the partial reconfiguration design flow process. Initially the whole design is mapped on to the Zedboard and using SDK, Processor Configuration Access Port (PCAP) is disabled so that ICAP can take control of configuration memory.

During reconfiguration SEM should be kept at idle state to avoid SEM detecting reconfigured region as errors. The inputs and outputs are provided using virtual input/ output IP (VIO). The complete design implementation is done on zedboard. The proposed design has been designed using Verlog-HDL.

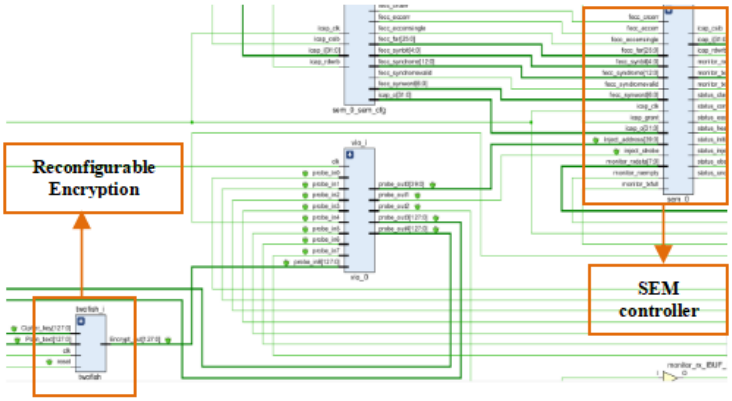

Fig.4. RTL schematic of the proposed design

The RTL schematic of the proposed design is shown in fig. 4. This is the result after the design is simulated and synthesized in the FPGA design process. SEM controller and reconfigurable encryption blocks are highlighted.

4.1. Power Estimation

The proposed design power consumption is estimated from the tool generated report as shown in Table 1. The total power is 1.737W.

Table 1. Power consumption of overall design

On-Chip Power	Power in Watts
Dynamic Power	1.592W
Device Static Power	0.145W
Total Power	1.737W

4.2. Resource Utilization Report

Table 2 shows the resource utilization summary for each internal block in the proposed design is estimated from the tool generated report.

Table 2. Utilization summary

Name	Number of Slice LUTs	Number of Slice Registers	Number of F7 Muxes	Number of F8 Muxes	Number of Slice	Number of LUT as Logic
Top	6387	3334	95	0	2105	6306
VIO	690	1629	64	0	416	690
SEM	670	584	0	0	209	613
Reconfigurable encryption	4571	399	0	0	1302	4571
dbg_hub	476	722	1	0	226	432

5. Results and Discussion

AES and Twofish algorithms are separately simulated and the results are shown in fig. 5 and 6. By giving different set of plain text and cipher key inputs, code is simulated.

For AES encryption following are considered:
Plain text: 0x0f0ffff,
Cipher key: 0x0ff,
Cipher key: 4cb227245c89afa8e431bd0098b5a846.
When inputs are changed:
Plain text: 0x0f0f0ffffff0fffffff,
Cipher key: 0x0fff0000ff,
Cipher text: 0de008bcd4694dad8903df0534100ad0.

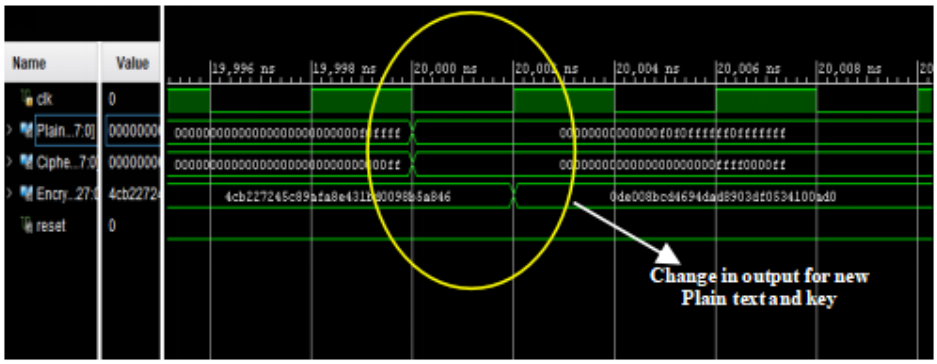

Fig.5. Output for AES encryption

For Twofish encryption following are considered:
Plain text: 0x0fff0000ffff,
Cipher key: 0x0ff00,
Cipher text: c562b3685bcc5a1df489180ef5eb2198.
When inputs are changed:
Plain text: 0x0fff0fff0fff,
Cipher key: 0x0f0f0f0,
Cipher text: 993abb67bd55ca2d477ef99ed574dd5a.

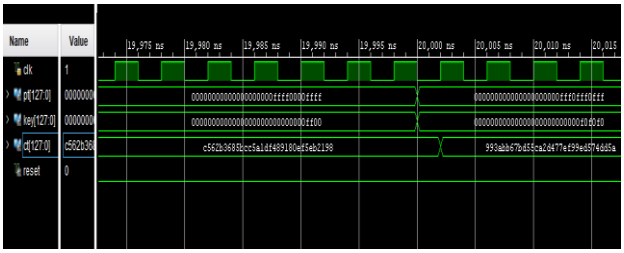

Fig.6. Output for Twofish encryption

The proposed design verified by injecting and correcting errors. Fig. 7 shows the floorplan of the implemented design.

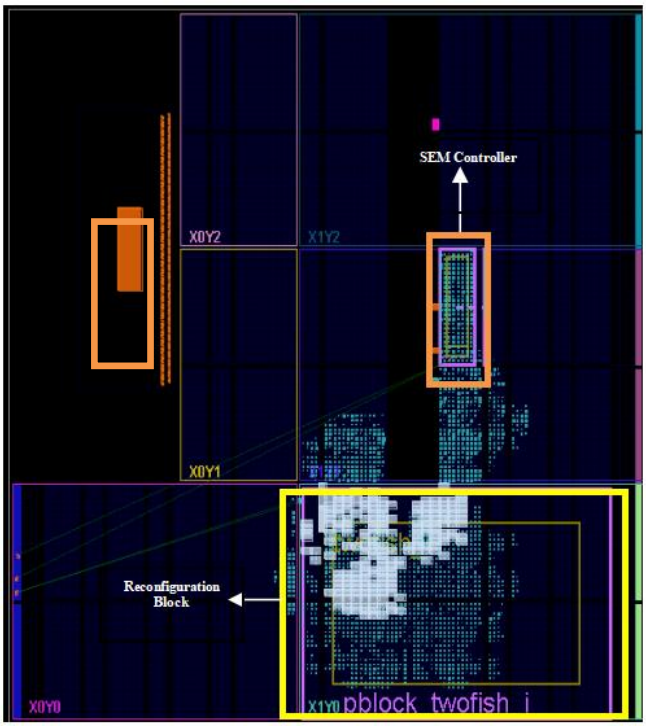

Fig.7. Implemented layout of proposed design on Zedboard

The highlighted areas shows different modules placed on the Zedboard Zynq Evaluation and Development Kit (xc7z020clg484-1) after placement and routing.

Initially when proposed design is mapped on Zedbord, VIO shows the results as shown in fig. 8 and SEM behavior can be observed on the terminal as shown in fig.9.

Name	Value	Activity	Direction	VIO
Cipher_key[127:0]	[H] 0000_0000_0000_0000_0000_0000_0000_0000		Output	hw_vio_1
Encrypt_out[127:0]	[H] 0000_0000_0000_0000_0000_0000_0000_0000		Input	hw_vio_1
Plain_text[127:0]	[H] 0000_0000_0000_0000_0000_0000_0000_0000		Output	hw_vio_1
reset	[B] 0		Output	hw_vio_1
status_classification	[B] 0		Input	hw_vio_1
status_correction	[B] 0		Input	hw_vio_1
status_observation	[B] 0		Input	hw_vio_1
status_uncorrectable	[B] 0		Input	hw_vio_1

Fig.8. VIO window showing results for initial mapped design.

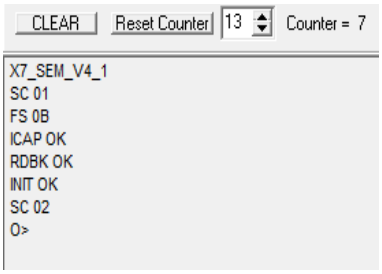

Fig.9. Terminal showing the SEM behavior.

During reconfiguration, if SEM is not in IDLE state then it gives CRC uncorrectable error as shown in fig. 10 since it is observing the changes in the frame. This is also similar while performing the TwoFish algorithm reconfiguration.

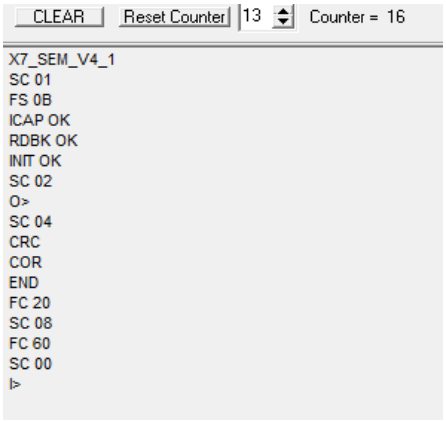

Fig.10. CRC error while performing reconfiguration

This can be corrected by resetting the SEM controller. The AES algorithm is reconfigured on to the device and output is as shown in fig. 11.

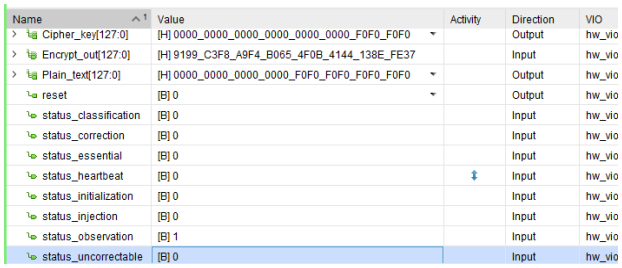

Fig.11. Output of AES algorithm

The error is injected in physical frame address of 042161F056 i.e. in 042161F frame, in 2rd word and 22nd bit and when SEM is changed to observation state it shows that Syndrome is valid and corrects the error which can be seen in fig. 12 after COR (correction). It also shows that, it is essential and correctable bit by changing the FC to 40.

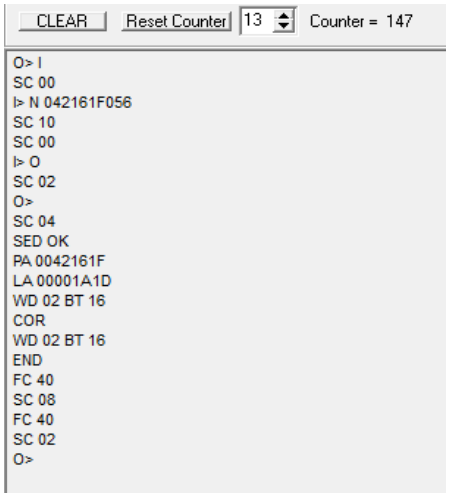

Fig.12. SEM behavior during and after error injection for AES algorithm

After error injection, the desired output changes and status essential is enabled since it is essential bit as shown in fig. 13.

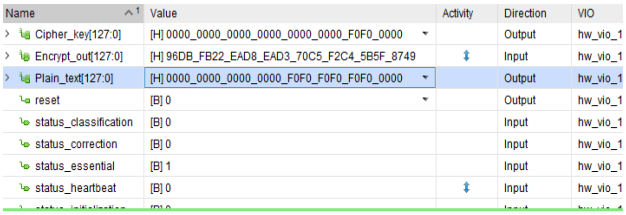

Fig.13. Output of AES algorithm after error injection

After reconfiguring Twofish algorithm, error is injected similar to the AES i.e. in physical frame address of 042151F001. Here physical frame address is 042161F, 0^{th} word and 1^{st} bit and when SEM is changed to observation state it shows that Syndrome is valid and corrects the error which can be seen in fig. 14 after COR (correction). It also shows that, it is non-essential and correctable bit since the FC 00, but error classification report i.e. SC 08 and FC 40 sets the essential bit high because in the proposed design error classification is disabled hence even non-essential bits are considered to be essential hence FC is 00.

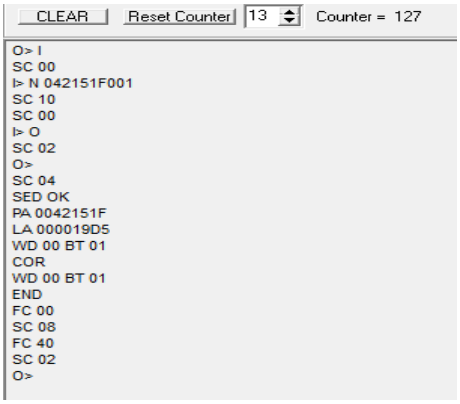

Fig.14. SEM behavior during and after error injection for Twofish algorithm

After error injection, a fault free output is obtained since the injected bit is non-essential but status essential is high since error classification is disabled as shown in fig. 15.

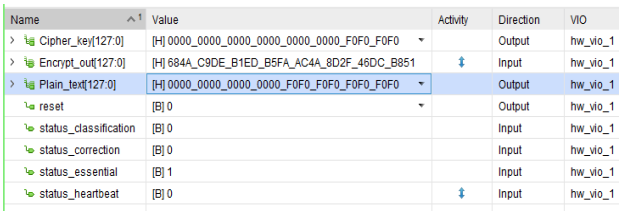

Fig.15. Output of Twofish algorithm after error injection

6. Conclusion

This paper explained about a technique for managing soft errors or the single event upsets. Errors occurring across encryption algorithms are corrected in order to increase reliability aspect of the design. Single event mitigation concept is applied to two types of encryption algorithms considering one at a time. Proposed concept is also validated by implementing it on the hardware kit- ZED board. Since partial reconfiguration is used for selecting any one of the two algorithms at runtime, resource optimization and reduction in power consumption are achieved.

As a future work permanent faults can be injected and corrected to further improve the reliability which is the most essential factor for mission critical applications.

Acknowledgement

This work is been carried out as a part of DRDO- ERIP/ER/DG-Med&CoS/990916502/M/01/1659 sponsored research work in the department. We are grateful for the financial support provided.

References

[1] B. Harikrishna and S. Ravi, "A survey on fault tolerance in FPGAs," *2013 7th International Conference on Intelligent Systems and Control (ISCO)*, Coimbatore, 2013, pp. 265-270. doi: 10.1109/ISCO.2013.6481160.

[2] "Practical cryptography", Text book Ferguson N. Schneier B. Wiley, 2003 ISBN-0471223573, 9780471223573.

[3] Ye Yuan, Yijun Yang, Liji Wu, Xiangmin Zhang , "A High Performance Encryption System Based on AES Algorithm with Novel Hardware Implementation," IEEE conference, 2018. DOI: 10.1109/EDSSC.2018.8487056

[4] S. Burman, P. Rangababu and K. Datta, "Development of dynamic reconfiguration implementation of AES on FPGA platform," *2017 Devices for Integrated Circuit (DevIC)*, Kalyani, 2017, pp. 247-251. DOI: 10.1109/DEVIC. 2017. 8073945.

[5] Snehal Wankhade and Rashmi Mahajan. "Dynamic partial reconfiguration implementation of AES algorithm," International Journal of Computer Applications, 97(3), 2014. DOI: 10.5120/16986-7084

[6] R. Yegireddi and R. K. Kumar, "A survey on conventional encryption algorithms of Cryptography," *2016 International Conference on ICT in Business Industry & Government (ICTBIG)*, Indore, 2016, pp.1-4. DOI: 10.1109/ ICTBIG. 2016.7892684.

[7] S. A. M. Rizvi, S. Z. Hussain and N. Wadhwa, "Performance Analysis of AES and TwoFish Encryption Schemes," *2011 International Conference on Communication Systems and Network Technologies*, Katra, Jammu, 2011, pp. 76-79. DOI: 10.1109/CSNT.2011.160.

[8] Xilinx "Partial Reconfiguration User Guide" UG 702.

[9] Xilinx "Soft Error Mitigation Controller" Product Guide, PG036.

[10] A. Adetomi, G. Enemali and T. Arslan, "A fault-tolerant ICAP controller with a selective-area soft error mitigation engine," *2017 NASA/ESA Conference on Adaptive Hardware and Systems (AHS)*, Pasadena, CA, 2017, pp. 192-199. doi: 10.1109/AHS.2017.8046378.

[11] S. Mandal, R. Paul, S. Sau, A. Chakrabarti and S. Chattopadhyay, "A Novel Method for Soft Error Mitigation in FPGA Using Modified Matrix Code," in *IEEE Embedded Systems Letters*, vol. 8, no. 4, pp. 65-68, Dec. 2016. doi: 10.1109/LES.2016.2603918.

[12] T. S. Nidhin, A. Bhattacharyya, R. P. Behera, T. Jayanthi and K. Velusamy, "Dependable system design with soft error mitigation techniques in SRAM based FPGAs," *2017 Innovations in Power and Advanced Computing Technologies (i-PACT)*, Vellore, 2017, pp. 1-6. doi: 10.1109/IPACT.2017.8244907.

[13] M. E. Keshk and K. Asami, "fault injection in dynamic partial reconfiguration design based on essential bits", jast, vol. 11, no. 2, pp. 25-34, jul. 2018.

[14] A. Sari and M. Psarakis, "A fault injection platform for the analysis of soft error effects in FPGA soft processors," *2016 IEEE 19th International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS)*, Kosice, 2016, pp. 1-6.doi: 10.1109/DDECS.2016.7482459.

[15] N. Jing, J. Lee, W. He, Z. Mao and L. He, "Mitigating FPGA interconnect soft errors by in-place LUT inversion," *2011 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, San Jose, CA, 2011, pp. 582-586. doi: 10.1109/ICCAD.2011.6105389.

[16] Xilinx "7 Series FPGAs Configuration User Guide" UG470.

[17] Yuwen Zhu, Hongqi Zhang, Yibao Bao "Study of the AES Realization Method on the Reconfigurable Hardware," 2013 International Conference on Computer Sciences and Applications. DOI: 10.1109/CSA.2013.23.

Authors' Profiles

Jamuna S is working as a professor in the department of ECE, Dayananda Sagar College of Engineering, Bangalore, India since 2008. She has done M.Tech in VLSI design and embedded systems from VTU, Belgaum and PhD from JNTU, Hyderabad. Her research domain includes VLSI design, verification and testing. She is currently, executing a funded project as principal investigator in the department. Research funds are sanctioned from DRDO, New Delhi, India.

Dinesha P is a Professor in Department of ECE, Dayananda Sagar College of Engineering, Bangalore, India. He received his Ph. D degree from University of Mysore, India, in the year 2014. His research interest is in VLSI Design (Digital Design), Digital System Design and Nanotechnology (Applications of conducting polymer composites).

KP Shashikala is an associate professor in Dayananda Sagar College of Engineering; Bangalore, India .She did her Bachelors in Electronics from MSRIT, Bangalore. Masters in Digital Communication from BMSCE, Bangalore, and Doctorate in Palmprint Biometrics from Rayalseema University Kurnool, AP. Her areas of interests include Biometrics, Image processing and Digital Communication.

Kishore Kumar K is working as a Junior Research Fellow in the department of ECE, Dayananda Sagar College of Engineering, Bangalore, India. He has done M.Tech in VLSI design and embedded systems from Bangalore Institute of Technology, Bangalore. His research domain includes VLSI design and Verification.

How to cite this paper: Jamuna S, Dinesha P, Kp Shashikala, Kishore Kumar K, "Design and Implementation of Reliable Encryption Algorithms through Soft Error Mitigation", International Journal of Computer Network and Information Security(IJCNIS), Vol.12, No.4, pp.41-50, 2020. DOI: 10.5815/ijcnis.2020.04.04

