Detection and Diagnosis of Fault Using Light-Weighted Midori Blocks

C. Thirumarai Selvi, R. S. Sankarasubramanian, and M. MuthuKrishnan

Abstract Modified block ciphers increase the performance and lower the time duration for high-speed applications. High-speed applications are mainly required for wearable medical devices, and compact devices which are implantable in the human body. Various security algorithm suffers due to inclusion of malicious and natural faults. The proposed model modifies the Midori block as light-weighted nature. This proposed algorithm introduces lower latency and less hardware complexity. The proposed model adds diagnosis algorithm in different stages of the work flow. Diagnosis algorithm reduces the fault value to the minimum. The fault diagnosis systems implemented with nonlinear S-box layer and beat structures. The beat structure includes 64-bit and 128-bit Midori symmetric key ciphers. The designed systems are benchmarked on a field programmable gate array (FPGA) with injected faults. The proposed light-weighted block cipher blocks yields, good energy efficiency rate and implemented using VHDL code.

Keywords Fault correction · Lower block cipher · Field programmable logic array gate (FPGA) · Midori blocks

1 Introduction

The main algorithm used for obtaining higher security protection with lower area consumption and to lower the energy consumption is light-weighted cryptography. These techniques have been used in many applications which have the following domain. They can be embedding system, wireless communication [1], RFID (Radio frequency identification tags) and other medical applicable devices. But obtaining

C. Thirumarai Selvi (✉)
Sri Krishna College of Engineering and Techology, Coimbatore, Tamil Nadu, India
e-mail: thirumaraiselvi@skcet.ac.in

R. S. Sankarasubramanian
PSG Institute of Technology and Applied Research, Coimbatore, Tamil Nadu, India

M. MuthuKrishnan
KIT-Kalaigarkarunanidhi Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India

A. Sivasubramanian et al. (eds.), *Futuristic Communication and Network Technologies*,
Lecture Notes in Electrical Engineering 792,
https://doi.org/10.1007/978-981-16-4625-6_16

lower energy consumption is a difficult process which is the drawback of the system. These technology have been used in implantable and mobile medical devices. The efficiency can be increased by the use of dischargeable batteries. The dischargeable batteries are difficult to remove the surgical operations. However, in the wireless technology by using the RFID tags and the sensor is the major reason for usage of light-weighted cryptography. By using these algorithm in the wireless technology, it will decrease the area consumption which would increase the efficiency of the system and decrease the source power. Thus, the requirements are given by the light-weighted ciphers [2]. By using the light-weighted ciphers, security level can be increase with the decrement in the optimal energy level. This light-weighted blocks lower the hardware difficulties. The main step noted in the light-weighted block [3] is the advance encryption standard (AES) that have limited the area and the power dissipation. In the proposed method, Midori Algorithm is used that has the required security level with the lower power optimization. The Midori which consists of S number of boxes that are obtained from the AES and other light-weighted block ciphers. Midori [4, 5] have been classified as two types. It has 4-bit S-boxes that are classified as ones variable. Midori which is the light-weighted block ciphers that can have the acceptable range of cells. The permutations of each cells are separated by using the certain distance calculation. These distance calculation method has classified as the MDS which is known as the maximum distance separable. It will arise due to the lower implementation of the values and the higher immunity against the several causes. The fault diagnosis in the cryptography is based on the crypto-architectures that have the center of values. As the existing work have implemented, the time and hardware redundant variation approaches. These variations which consists of variations in the different platforms due to the different light-weighted architectures [6–13]. In the lower weighted Midori domain, there doesn't exist any existing work and the main advantage of the proposed work is the higher value of accuracy of fault diagnosis as compared with the different existing methods. In the previous work, there exists the two-folded algorithms. These algorithms consist of two stages namely fault detection and fault diagnosis. During the first stage, there exists the comparison of logic-gate based and look up table (LUT). These two existing algorithm consists of the error detection techniques. The error detection depends upon the S number of boxes in the Midori algorithm. The key advantage of employing the Midori block is its low energy consumption, which allows it to meet other constraints such as area, power, or latency. The methods of implementation of Midori algorithm are that the implementation and the performance measuring schemes are different from the other algorithm. Second stage of the proposed algorithm is that it can implement the lower head detection and the performance rate can also increases. This is achieved by changing the blocks and the error containing values. Thus, to obtain the fault diagnosis, careful observation of the implementation is needed to achieve the required data value. The proposed algorithm will define the simulation results as the higher error coverage. The higher error coverage can be stated as the ratio of the number of error which is detected as a input and the number of injected error faults. From the proposed algorithm, the error detection can be achieved without any fault error [14]. These error diagnosis can be achieved by the detection of faults with the high-coverage value. From the proposed

work, the permanent faults such as stuck-at faults, fault error can be occurred. These causes are the main reason for the VLSI manufacturing defects. The manufacturing defects [15] are due to the break in the intension during the run time. During the test generation, pattern will be generated to identify the faults within the system. The long transient faults can be identified by the leakage in the information and the changes in the output occurs due to the computation techniques. The faults attack are saved in the register for the further references. This action will discontinue the counter operation. The proposed algorithm can be implemented using the Field Programmable Logic Array (FPGA) in the Xilinx Vertex software. By using the proposed software, the work can be expected toward the constrained level. The proposed work consists of various steps which will give the detailed explanation about the fault detection and diagnosis using the Midori light-weighted blocks.

2 Proposed Method

The proposed work block diagram is shown in Fig. 1. The variants such as Midori-128 and Midori-64 have 128-bit secret key (K) and use two 64-bit sub keys K_0 and K_1 and the W_K are derived through modulo-2 addition of these 64-bit sub keys, respectively. In Midori64, the derivation of the round key is reiki = K (imod2) EX-ORαi, where $0 \leq i \leq 14$. In Midori128, $W_K = K$ and Reiki = K EX-orbetai, $0 \leq I \leq 18$, in which

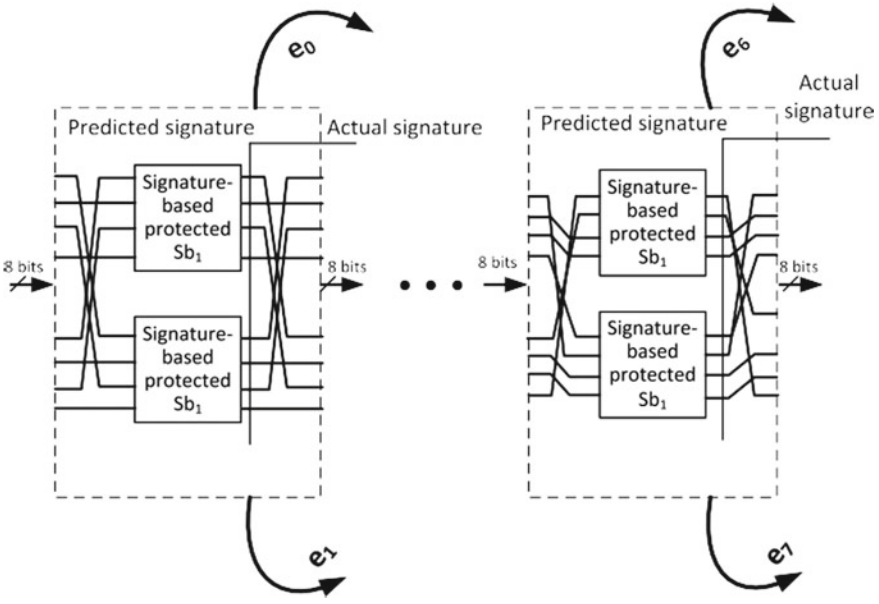

Fig. 1 Proposed method S-box transmission

Fig. 2 Three instances scheme transmission

$$\alpha_0 = \beta_0 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

$$\alpha_{14} = \beta_{14} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

$$\beta_{18} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

betai = αi for $0 \leq I \leq 14$ (see Fig. 2). Hence, the round key matrix is either "1"or "0" as ˆSignature.(Reiki) = Signature. (K) EX-OR Signature. (betai/αi).

To analyze matrices of constant values, same approaches are followed. Let us consider two examples for detections of errors by round key operation. In the first example, the input key by K and the output round key by rookie. To derive 16 signatures, each one is processed underage = k*j EX-orbeta j. The nibble of k3 jk2 jk1 jk0 j for Midori64 or a byte as k_7 jk_6 jk_5 jk_4 jk_3 jk_2 jk_1 jk_0 j for Midori128. Then, signatures are Midori128, ˆSignature.(r*k*j) = Signature.(k_7 jk_6 jk_5 jk_4 jk_3 jk_2 jk_1 j(k_0 j EX-orbeta j)), where $0 \leq j \leq 15$. The received "1"or "0"elements of the round key matrix. In the second example, to create just one signature nature for error detection the modulo-2 addition of the entire elements in the state matrix is processed by one signature nature. For example, (r*k) = 15 j = 0 k*j + 15 j = 0 beta* j, and α_0 = $beta_0$,α_{14} = $beta_{14}$, and $beta_{18}$ elements of each matrix in modulo-2 addition drives "0," "1," and "0,", respectively. Hence, RK_0 and RK_{18}, the input signature natures, are intact, and RK_{14} is inverted.

3 Architecture of the Proposed Work

The structures of encryption of Midori128 detect mentioned error in which it has 20 rounds of 8bits cell size.

In this, variant has functioned to encrypt with round function and key generation. It has the SubCell operation, and the WK is modulo-2 in the last round. Then in the first and last steps, respectively (see Fig. 3). For different operations, they have derived with error detection schemes, and round function, illustrated by the predicted signature-nature of each operation.

Signature-based error detection architectures in Midori's encryption and decryption process (see Fig. 4) are carried out through a loop-like architecture by inserting a multiplexer (MUX) and a register. This will derive the signatures of input and the key. The similar functions operated in encryption and decryption, but with variation

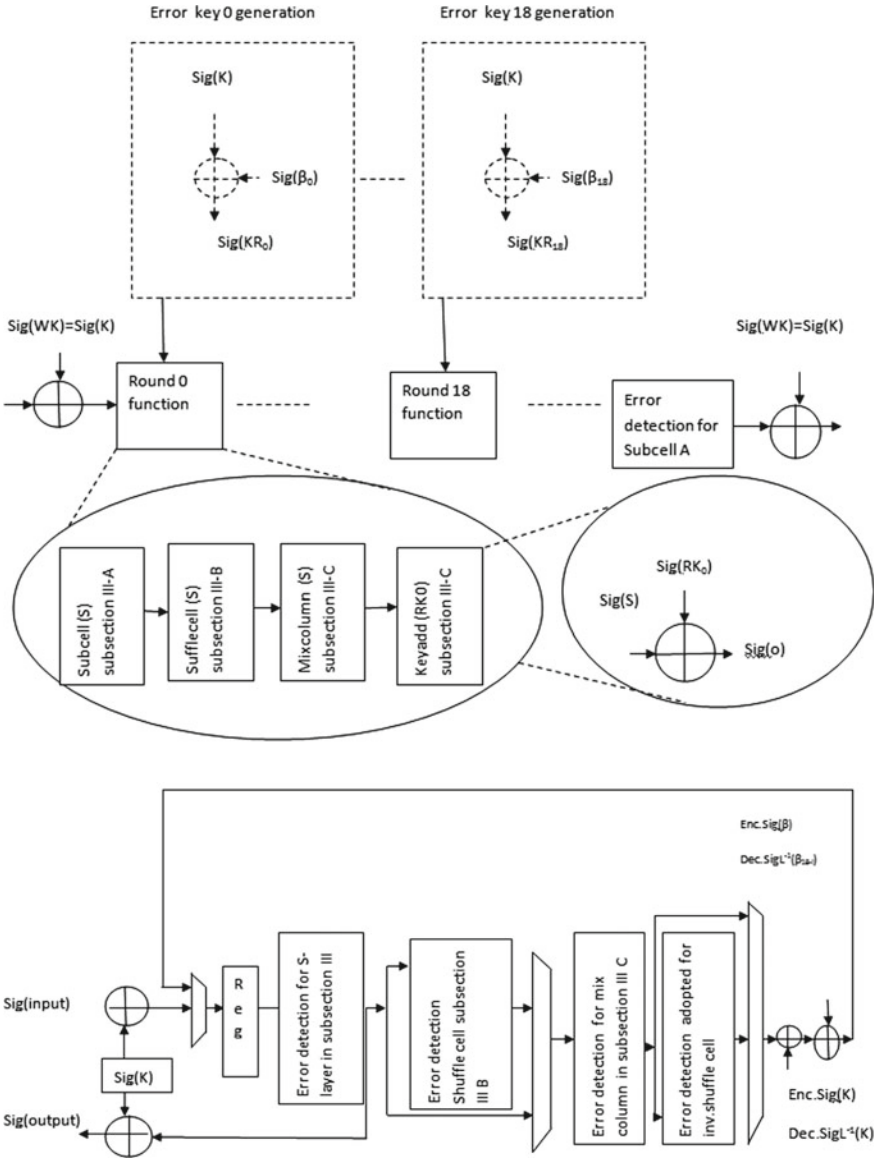

Fig. 3 Architecture of proposed work

as ShuffleCell (Sh) operation in encryption and InvShuffleCell (Sh−1) operation for decryption is adopted. In decryption key, generation process is altered, i.e., L−1 (K) instead of K and the corresponding signature natures "Signaturen."(L−1 (K)) and "Signaturen."(L). Similarly, the itch round constant is replaced by L−1 (beta*18−i), instead of betai (see Fig. 5). Rather than in other cases, in case of deriving a "black-

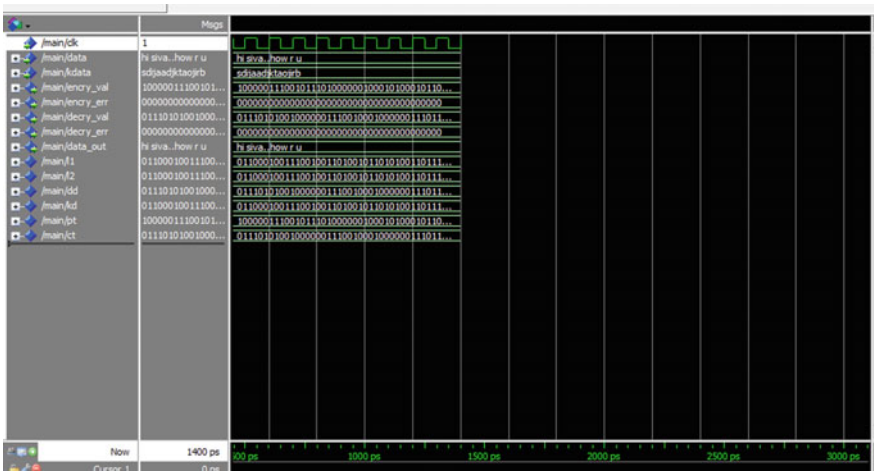

Fig. 4 Simulation of decrypted Midori block

```
Device utilization summary:
---------------------------

Selected Device : 7vx330tffg1157-3


Slice Logic Utilization:
 Number of Slice LUTs:                  816  out of  204000     0%
    Number used as Logic:               816  out of  204000     0%

Slice Logic Distribution:
 Number of LUT Flip Flop pairs used:    816
   Number with an unused Flip Flop:     816  out of    816   100%
   Number with an unused LUT:             0  out of    816     0%
   Number of fully used LUT-FF pairs:     0  out of    816     0%
   Number of unique control sets:         0

IO Utilization:
 Number of IOs:                         389
 Number of bonded IOBs:                 388  out of    600    64%

Specific Feature Utilization:

---------------------------
```

Fig. 5 Reduced area using Midori block

box" signature, they have to choose the check arguments for the entire encryption/decryption. At the time, it had a huge probability for encountering error indication flags. In case of the wrong alarm ratio, fine-tuned multiple signaturenatures are avoided, and it uses the error indication flags with separate transformations. The formulation as per paper is used in each check point is higher for expanse of more overhead and wrong alarms probability. Atlast, best granularity is fixed with separate 4-bit S-boxes of Midori's 8-bit S-box checking. It leads to higher wrong alarms ratios at higher overhead and higher error coverage. This provides three models of different signaturenatures to detect odd faults in addition to single stuck-at faults. Here, it is

possible to detect only VLSI defects such as burst faults and unable to find adjacent faults. Adjacent faults are diagnosed on interleaved parties at the expense of more overhead. In signaturenature-based diagnosis approach, it allows to linear codes to detect random errors of small multiplicity based on robust codes it detects any errors. The outcome of the methods to reach, reliability and hardware security.

3.1 Error Detection for Threshold Implementation of Midori

Threshold implementation (TI) for first order [16, 17] is widely used to protect light-weight block-ciphers. It also analysis the power consumption during the performance and complexity overheads. The S-box approach [5]: $A_{out}Q_{12}A_mQ_{12}$ A_{in}, where A_{out}:{0 A1B82934E 5FC6D7}$_{16}$, A_m: {84B70C3F 95 A61D2E$_{16}$, A_{in}:{8 A02DF57CE469B13}$_{16}$, and Q_{12}: {0123456789CDE FAB}$_{16.}$ Register sets have three instances of f_{Q12} over by an A_{out}. S-box combined with TI plots helps to find error, while duplicating native approach. $A_{out}Q_{12}A_mQ_{12}A_{in}$ reviles to high error coverage, no false alarms and low overhead. The performance, of signature, leads to lower overhead, while expanding the error coverage.

4 Proposed Technique Implementation in Fault Attacks

Analysis of differential fault intensity is the combinations of fault injection principles and differential power analysis derives based fault models in practical times the fault in original and redundant computations injections are rare. The insertion of few faults may possible in reduction of efforts, i.e., injecting of single faults with different intensities. The variation of a intensity simulation is used for biasing fault models by bits within higher intensities rather than using with low fault intensity. Fault categories such as single/two/three/four-bit modes. The approach to detecting error codes, signaturenatures on column are capable to throw more fault. Moreover, using parities SBUs and SBTBUs are detected fully. In addition, with burst faults, it is able to detect SBTBUs, SBQBUs and OSBs. Similar type of fault is introduce in both the original and redundant computation. This developed RESI architecture brings the null biasing effect in a fault model. Also, it injects f_0 and f_1 fault to the output registers. By the parting, both these attack schemes similarity are marked as in 23.

5 Simulating Errors by Injection with FPGA Benchmark

This section describes assessment of error coverage and benchmark overhead in the error detection structures. By transient random faults, the internal faults are modeled.

Table 1 Proposed MIDORI-128 method error coverage details

Type of faults	Injected faults	Detected faults	Error coverage (%)
Stuck-at zero	10,000	9909	99.09
	100,000	99,870	99.87
Stuck-at one	10,000	9908	99.08
	100,000	99,762	99.76

The errors are detected through multiple stuck-at fault injections. Then, the transient and permanent internal faults are identified after simulation. The natural and malicious faults are known as single and multiple stuck-at faults. In reality, technological constraints have led to multiple faults. So, single stuck-at faults are found to be ideal in nature. In the linear and nonlinear components of Midori, single-bit errors are detected in nibbles (Midori-64) and bytes (Midori-128). The proposed single stuck-at faults concludes to 100% error coverage. Hence, simulation is neglected. The proposed approaches give the detection of odd faults with the property of inheritance signaturenature is used with subsets as single stuck-at faults. It is an irregular system to detect all potential fault attacks, but the difficulty in mounting is achieved by proposing architecture. The architecture in different subparts alarms for the errors. The transient faults and permanent internal permanent faults and transient faults were simulated by injecting faults. This is developed with the help of Midori128 encryption. By injecting, 10,000 or 100,000 faults for the encryption process and monitored. Table 1 plots the error coverage which shows the increase in injection points and thus higher error prediction is calculated. Two experiments are implemented as follows: (a) Linear-feedback shift registers (LFSRs) used for detecting random multiple faults, with maximum tap polynomials. These polynomial projects the type, location and the total faults (b) Increased number of fault injections are used to get closer and realistic error coverage. Hence, 10,000 faults are injected to improve the performance.

Parity-interleaving or parity-swapping yields reduced are and power consumption, while operating with S-boxes. Reduction of error coverage results due to inputs swapping and column mixing in the S-boxes.

6 Simulation Results

Modified light-weighted blocks will lead to the changes in the accuracy rate and the delay time. The simulation results of the proposed work are presented from Figs. 6 and 7. These results represent the reduced area and increased speed. Also, the encrypted message using the modified light-weighted block is given in the results.

```
Timing Summary:
---------------
Speed Grade: -3

   Minimum period: No path found
   Minimum input arrival time before clock: No path found
   Maximum output required time after clock: No path found
   Maximum combinational path delay: 2.565ns

Timing Details:
---------------
All values displayed in nanoseconds (ns)
```

Fig. 6 Reduced time using Midori block

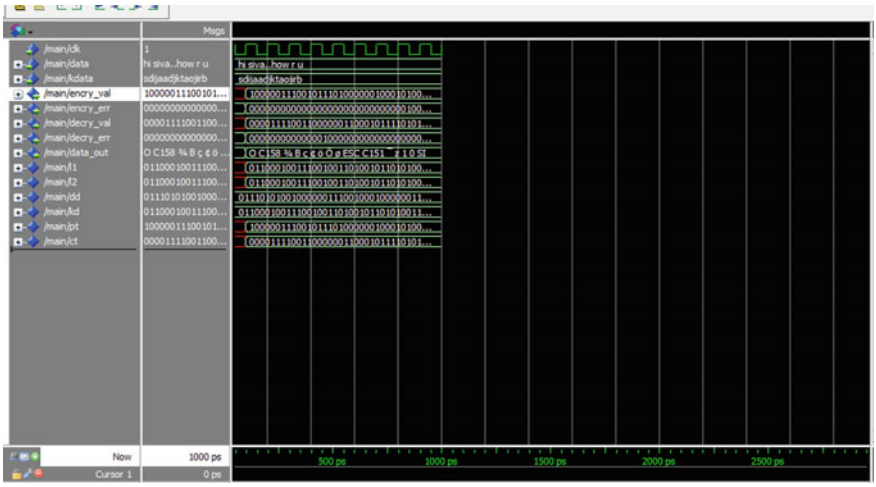

Fig. 7 Simulation of encrypted Midori block

7 Conclusion

Thus, the proposed method has the lesser area coverage, and there is the reduction in the time consumption. This reduction will have the better accuracy as comparison with the existing algorithm. The light-weighted Midori block will have the lesser values of the error. The fault detection can be shown in the encryption and decryption process of the proposed work. In future scope, the Midori blocks can be increased for achieving the more accuracy.

References

1. Kermani MM, Zhang M, Raghunathan A, Jha NK (2013) Emerging frontiers in embedded security. In: 2013 26th international conference on VLSI design,12th international conference

on embedded systems. IEEE, pp 203–208
2. Eisenbarth T, Kumar S, Paar C, Uhsadel L (2007) A survey of lightweight-cryptography implementations, IEEE Des Test Comput 24(6):522–533
3. Moradi A, Poschmann S, Ling C, Paar, Wang H (2011) Pushing the limits: a very compact and a threshold implementation of AES. In: Proceedings of EUROCRYPT, pp 69–88
4. Banik S, Bogdanov A, Regazzoni F (2015) A block cipher for low energy (extended version), Proc Cryptol ePrint Arch, pp 411–436
5. Moradi S (2016) Side-channel analysis protection andlow-latencyinaction-case study of prince and midori. [online]. Available: https://eprint.iacr.org/2016/481.pdf
6. Mozaffari-Kermani M, Azarderakhsh R, Lee CY, Bayat-Sarmadi S (2013) Reliable concurrent error detection architectures for extended Euclidean-based division OverGF(2^m). In: IEEE Trans Very Large Scale Integr (VLSI) Syst 22(5):995–1003
7. Jing Z, Zengrong L, Lei C, Shuo W, Zhiping W, Xun C, Chang Q (2012) An accurate fault location method based on configuration bitstream analysis. In: NORCHIP 2012. IEEE, pp 1–5
8. Sarkar S, Hembram PK, Purkait P, Das S (2016) Acquisition and pre-processing of three phase induction motor stator current signal for fault diagnosis using FPGA, NI Compact-RIO real time controller. In: 2016 IEEE Uttar Pradesh section international conference on electrical, computer and electronics engineering (UPCON). IEEE, pp 110–114
9. Hsu CL, Chen TH (2009) Built-in self-test design for fault detection and fault diagnosis in SRAM-based FPGA. IEEE Trans Instrument Meas 58(7):2300–2315
10. Jamshidpour E, Shahbazi M, Poure P, Gholipour E, Saadate S (2013) Fault tolerant operation of single-ended non-isolated DC-DC converters under open and short-circuit switch faults. In: 2013 15th European conference on power electronics and applications (EPE). IEEE, pp 1–7
11. Guo C, Zhang Y, Chen L, Zhou T, Li X, Wang M, Wen Z (2012) A novel application of FPGA-based partial dynamic reconfiguration system with CBSC. In: 2012 VIII Southern conference on programmable logic. IEEE, pp 1–4
12. Ghalaty NF, Yuce B, Taha M, Schaumont P (2014) Differential fault intensity analysis. In: 2014 Workshop on fault diagnosis and tolerance in cryptography. IEEE pp 49–58
13. Patranabis S, Chakraborty A, Nguyen PH Mukhopadhyay D (2015) A biased fault attack on the time redundancy countermeasure for AES. In: International workshop on constructive side-channel analysis and secure design. Springer, Cham, pp 189–203
14. Wang G, Wang S (2010) Differential fault analysis on PRESENT key schedule. In: 2010 international conference on computational intelligence and security. IEEE, pp 362–366
15. Biham E, Shamir A (1997) Differential fault analysis of secret key cryptosystems. In: Annual international cryptology conference. Springer, Berlin, Heidelberg, pp 513–525
16. Tunstall M, Mukhopadhyay D, Ali S (2011) Differential fault analysis of the advanced encryption standard using a single fault. In: IFIP international workshop on information security theory and practices. Springer, Berlin, Heidelberg, pp 224–233
17. Ali SS, Mukhopadhyay D (2013) Improved differential fault analysis of CLEFIA. In: 2013 workshop on fault diagnosis and tolerance in cryptography. IEEE, pp 60–70