International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Implementation of Enhanced Hardware Digital System Design by Protecting Hardware Trojans using Concurrent Error Detection Technique

[1]Dr. S. Nithyadevi, [2]Mr. S. Senthilkumar, [3]Biji Rose, [4]Dr. A. Vijayalakshmi, [5]T. Velmurugan, [6]Dr. S. A. Sivakumar*, [7]Dharmesh Dhabliya

Submitted: 01/12/2023 **Revised**: 25/01/2024 **Accepted**: 03/02/2024

Abstract: Malicious threat attacks of hardware design which are caused by third parties during Integrated Circuit(IC) fabrication process has been considered as primary security issue. Due to this attack the malicious alteration is occurred in electronic hardware design which results in failure or loss of information. This is called Hardware Trojan. To prevent the attacks during synthesis, a Concurrent Error Detection (CED) technique which is based on 128 bit encryption key generator derived from Code Division Multiple Access (CDMA) is proposed in this paper. This proposed technique is used to protect the Digital Systems from Hardware Trojan attacks and also faults can easily be detected.

The proposed technique can also be used for split-manufacturing methods in all digital circuits with minimum area overhead and less hardware complexity. The simulation results prove that the proposed method can be applicable for implementing the design in System On Chip (SoC).

Key words: *Concurrent Error Detection (CED) techniques, Code Division Multiple Access (CDMA), Hardware Trojan, System On Chip (SoC)*

1. Introduction

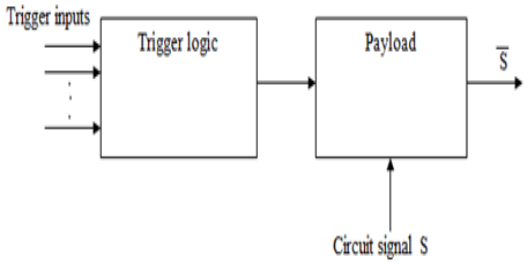
Hardware Trojan harms are regarded as a serious security risk in the process of fabricating integrated circuits (ICs). These types of attacks target the intentional alteration of an integrated circuit (IC) during the design or manufacturing process in an unreliable test service, design, or tool that involves erratic individuals, components, or design tools [12]. These malevolent alterations have the ability to extend an integrated circuit's undesirable functional characteristics or provide escape routes or hidden channels that allow the leakage of private data.

An attacker or adversary may have a greater chance of introducing fraudulent logic into an internal circuit of an IC through external means. Thus, adding more logic alters the inside circuit; these malicious modifications are known as Hardware Trojans. This existence undermines the output conditions of an Integrated Circuits and entire circuit will go into malfunction [9].

In order to facilitate test generation for Trojan detection [10], Comparator and Multiplexers have been used in Triggering circuits of combinational system and Counters have been used in Sequential circuits [11].

In most systems, hardware Trojans typically attempt to circumvent or compromise critical security aspects, including surreptitiously divulging confidential information and secret keys to adversaries, altering the contents of specific registers, or causing disruptions by disabling, deranging, or destroying either the entire hardware system or its individual components. Conventional hardware testing approaches face challenges in effectively identifying Trojans due to the low likelihood of triggering them during functional testing. Furthermore, Trojans [7] have less of an effect on side channels like static and dynamic power because to their modest size relative to the total dimensions of the chip.

[1]*Assistant Professor Sri Krishna College of Technology, Coimbaatore-641042*
nithyadevi.s@skct.edu.in
[2]*Assistant Professor Sri Krishna College of Engineering and Technology, Coimbatore-641008*
senthilkumars@skcet.ac.in
[3]*Assistant Professor (SG), Department of Electronics and Communication Engineering, Dr. N. G. P Institute of Technology, Coimbatore*
bijirose@drngpit.ac.in
[4]*Associate Professor Department of ECE, Hindustan College of engineering and technology, Coimbatore*
vijayalakshmi.adhi@gmail.com
[5]*Assistant Professor Department of ECE Builder engineering college, Kangayam*
ecevel@gmail.com
[6]*Associate Professor Department of Electronics and Communication Engineering Dr. N. G. P Institute of Technology, Coimbatore*
[6]*drsasivakumar@gmail.com**
[7]*Department of Information Technology Vishwakarma Institute of Information Technology, Pune, India*
[7]*Dharmesh.dhabliya@viit.ac.in*
**Corresponding Author: drsasivakumar@gmail.com*



The main block diagram of the hardware Trojan is shown in Fig 1. Trigger and Payload are the two main building parts of a hardware Trojan [5]. The Trojan is triggered, and the payload alters the internal circuit signal. Analogue and digital hardware Trojans can be distinguished based on the trigger circumstance.

While the Digital Trojans are activated by a Boolean logic function [8], the Analogue Trojans are triggered by analogue factors like temperature, latency, or the ageing impact of the device.

The Trojan trigger activation can be designed by Attacker for extremely uncommon internal node circumstances of Integrated Circuit.

These uncommon sequences generally not used during testing. Attacker is capable of inserting many Trojans in various forms and sizes. Through a hidden side channel, the implanted Trojan hardware spills data, making it possible for nefarious individuals to collaborate and decipher the encryption key.

Power usage can be impacted by malicious modifications. Reverse engineering is not appropriate for Trojans because hardware Trojans alter layout masks due to the insertion of harmful logic delay, which increases in the integrated circuit. The perfect circuit functionality is affected by two undesirable Trojans namely Fault and hardware Trojans. Inaccuracies in a design that arise from flaws acquired during production, hardware Trojan horses are intentionally placed by an enemy with the intention of causing harm.

Trojans are divided into two types specifically combinational Trojan and sequential Trojan based on its activation. Fig.2 describes a circuit of combinational logic type of Trojan which includes Triggering circuits namely Multiplexers, AND gate and Comparator used for causing errors.

Hardware The Trojan consists of two blocks: the payload and the trigger. The Trojan is triggered, and the payload modifies its internal circuitry.

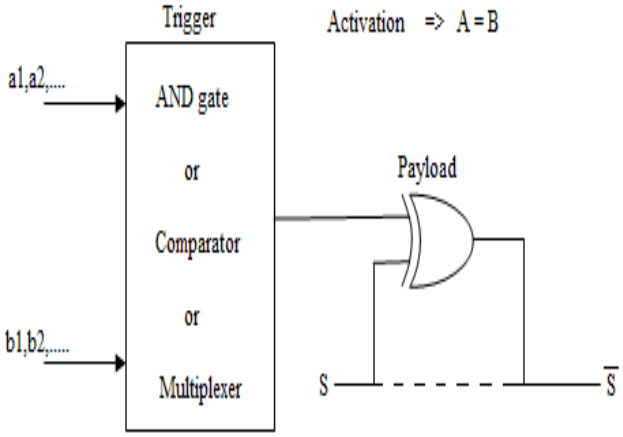


Fig. 2. Combinational Trojan

Fig.3. describes a sequential Trojan which experiences a series of condition changes before to causing a malfunction. Counters are used as triggering circuits in sequential Trojan.

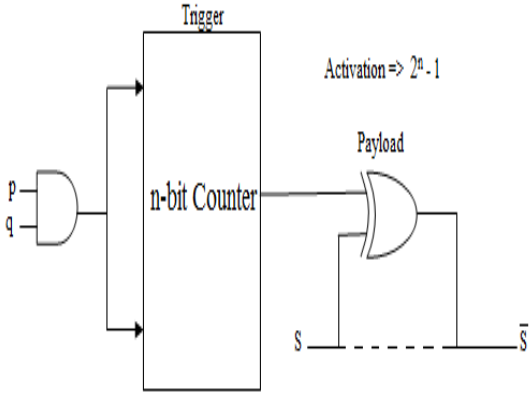


Fig. 3. Sequential Trojan

Presence of hardware Trojans in internal circuit of an IC is because of entrusted parties involvement and outsourced designs and tools [14]. Hardware Trojan activation process is referred as Triggering, its effect on IC considered as Payload. The payload component modifies an IC's internal signal when the Trojan is engaged. When the Trigger Logic is True, Trojan is activated for rarely occurring internal node sequences.

[1] proposed a logic encryption technique to secure digital design against malicious logic. This technique inserts key gates to digital design, thus without key unauthorized access is not possible. Furthermore, in order to meet two important requirements—a high degree of key dependency and a high level of output corruption for incorrect keys—their method meticulously incorporates key-gates into the design and adds a few extra gates. This ensures that the encryption quality is maintained.

2. Existing Method

[3] has developed a logic obfuscation technique for Integrated Circuit security. XOR operation of OC configuration and PUF response generates a license, it protects IC from overbuilding. Logic obfuscation prevents attacker from Reverse Engineering of layout-level geometry and gate level net list [13]. Synthesis was realized using Synopsis 45nm technology with area and power overhead are 0.63% and 2.6%respectively. The usage of don't cares in RTL code by new hardware Trojans has been studied [4]. These hardware Trojans that reveal the values of internal circuit nodes. Also in this method X-analysis described by formulating proposed new hardware Trojan insertion and its detection in different cases in terms of RTL don't cares. Elliptic Curve Processor case study was formulated with 538 doesn't cares.

3. Proposed Method

Security of the digital circuits is a key factor in current digitalized world. The proposed security architecture mainly concentrates on the security of the digital system design with less hardware complexities. IC manufacturing process results in various stages where an adversary or third parties can attack or can do malicious modifications in the circuitry which results in hardware Trojans. The proposed security architecture detects the intrusion of malicious attacks in the hardware digital circuit design. The suggested security architecture uses a concurrent error detection checker and a 128-bit encryption key generator with the least amount of overhead space to detect input bit encoding and output bit decoding.

A. Logic Circuit: 16 bit adder

Consider a 16-bit adder logic circuit as shown in the Fig. 4.

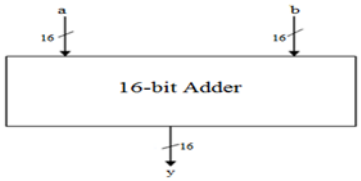


Fig. 4. 16-bit Adder Logic

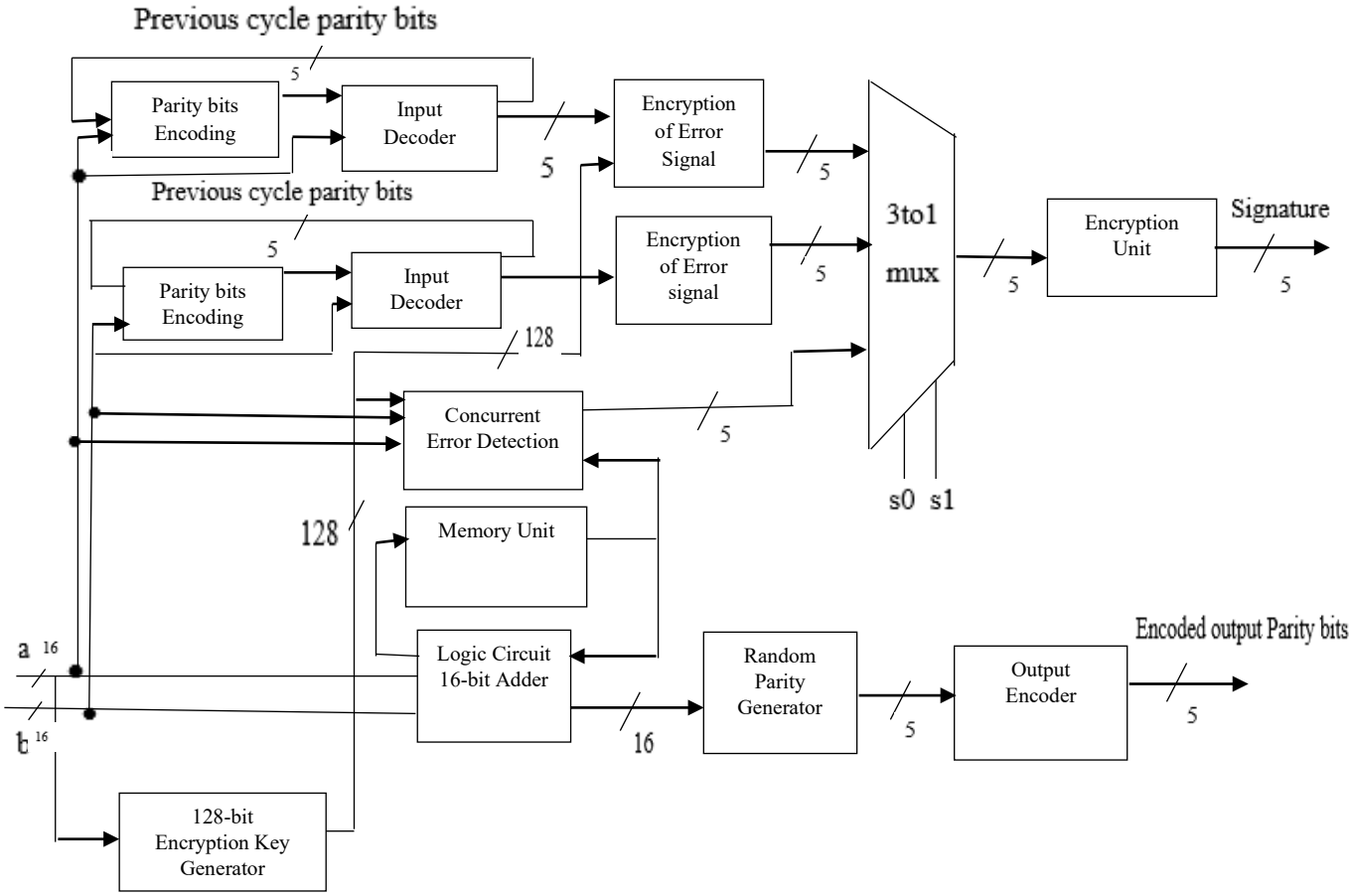


Fig. 5. Block Diagram of Proposed Security Architecture

16 bit adder logic circuit consists of two inputs as a[15:0] and b[15:0] producing y[15:0] as sum outputs. The proposed security architecture involved with 16-bit adder is shown in Fig. 5

B. Output bit Encoding

The procedure of calculating parity bits is as follows: assuming 4-bit data 1010. Using the Hamming code, a random parity code word is created.

These random parity codeword and the previous encoded output bits are fed as inputs to 2-bit XOR gate. The D-Flip flop stores the XOR gate's output for each clock cycle, which is then utilised to encode the output parity bits. The parity bits' encoded output is represented by the following codes: z[0], z[1], z[2], z[3], and z[4]. If there is an error or malicious attacks are detected, then output of the encoded parity bits changes to its compliment output. This ensures the security at the output side of the circuit.

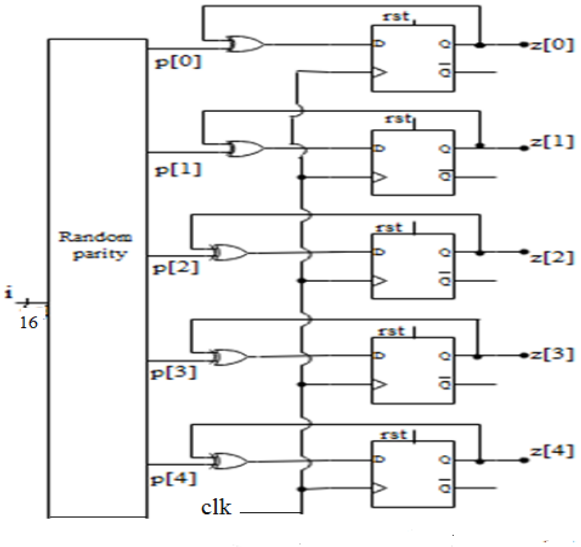


Fig. 6. Output bit encoding circuitry

C. Input bit Decoding

Fig. 7. illustrates the circuit diagram of input bits decoding. In this circuit, 16-bit input data 'a' and 5-bit encoded parity bit data 'p' both are applied to input bits decoding block. Error signals are generated by comparison of expected and actual parity bits, error signals are represented by the term 'e'. But these error signals are easily understandable to attacker, thus encryption of error signals are must for security. To generate 128-bit encryption key 's', 16-bit input applied to 128-bit encryption key generator module, it is used to encrypt the error signals. Encryption key has 128 bits, therefore 2^{128} sequences are possible for one clock cycle. These 2^{128} possible sequences for one cycle give more randomness to the system. Out of 128-bits in encryption key, 5-bits are chosen randomly for encryption. In this particular case 15, 30, 45, 90, 125 positions are taken from 128-bit encryption key for encryption process.

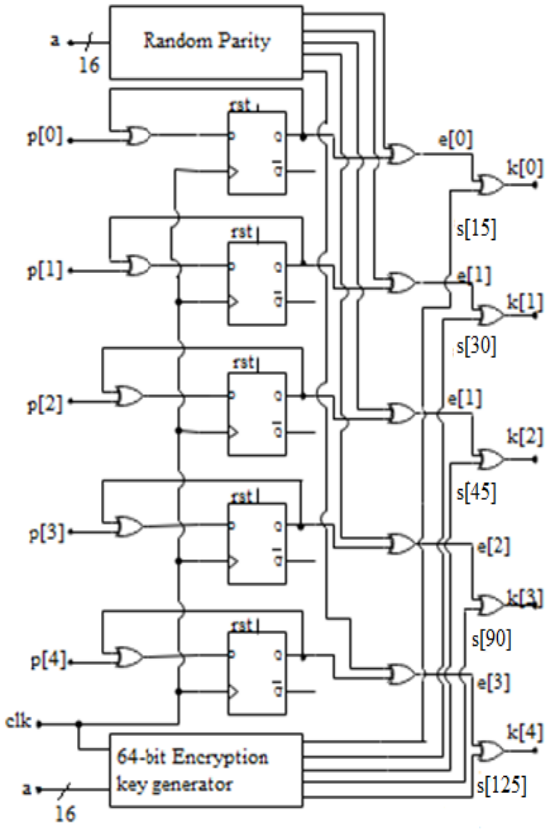


Fig. 7. Input bit Decoding circuitry

Encoding of input parity bits shown in Fig. 8. In this circuit, 16-bit input ‘a’ is given to random parity module and produces 5 parity bits for each input pattern. Encoding of five parity bits have been done by applying these parity bits and another set of five parity bits which are computed in previous clock cycle to five 2-bit input XOR gates. The result is obtained as encoded input parity bits, it is represented by ‘p’.

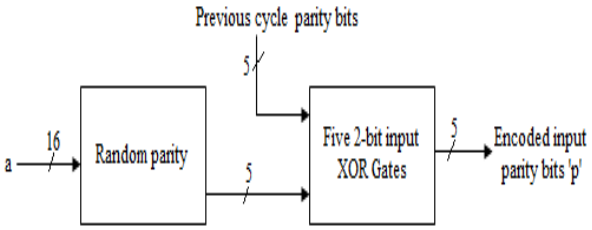


Fig. 8. Encoding of input parity bits

D. 128-bit Encryption key generator

Randomness of the digital system implies the security to the digital system in which more randomness provides greater security to the digital system. In existing method Linear Feedback Shift Register (LFSR) was used as random pattern for encoding error signals, In proposed method , to encode error signals with better security , an encryption key generator has been designed, it is called as 128-bit Encryption key generator. Every clock cycle, it creates a 128-bit encryption key.

In a digital system, input and output bits are used to encode and decode data transmission across circuits. Hence the attacker may not able to understand the data within the circuits and modification of internal signal value is very much difficult for adversary.

128-bit Encryption key generator is designed from the idea of spread spectrum interpretation of Code Division Multiple Access (CDMA). In CDMA, Orthogonal Codes are XORed with the chip sequence for accurate and secure data communication, in the similar technique, in the proposed method, 4-bit orthogonal codes are XORed with spreading of input sequence to generate 128-bit encryption key for cycle. Analysis of this 128-bit Encryption key generator is done by using spread spectrum basics and orthogonal codes.

4. Simulation Results

Xilinx ISE 14.1 is the simulation tool utilised for compilation. The simulation will be run on a test bench that has been built. Numerous security applications of the suggested security architecture help against harmful assaults. This article presents the implementation of the suggested security architecture's modules in Verilog HDL. Several modules are used in the security architecture to carry out the input and output bit decoding, CED, and 128-bit encryption key generation. The simulation results and RTL schematic are displayed in the test bench wave forms below.

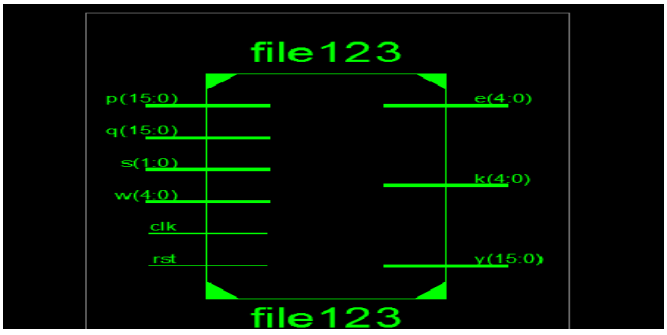


Fig. 9 RTL design of proposed work

Concurrent Error Detection is the inspiration for the suggested security method (CED) [15]. In Fig. 9, the CED approach is displayed. The output parity bits for each input to the 16-bit multiplier are predicted by the Output Characteristic Predictor (OCP) in CED. Actual parity bits are computed from 16-bit Multiplier output. The checker describes an error if actual and predicted parity bits are not same. In this case, obfuscate error signal encryption is required. CED is alone not sufficient for detecting Trojan logic from the observations.

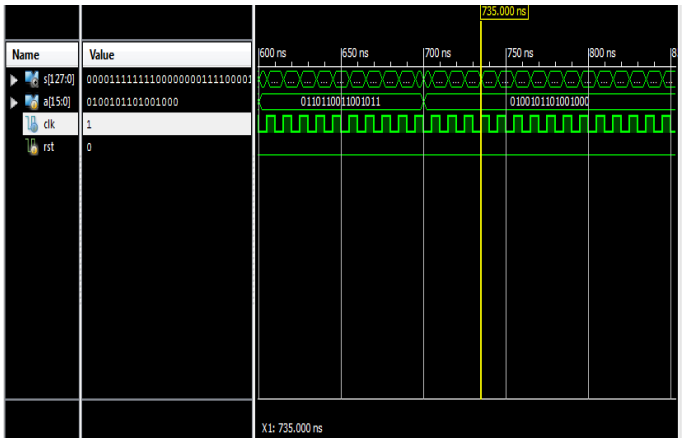


Fig. 10.128-bit Encryption key generator

Table 1. Proposed work Device Utilization Summary

Logic Utilization	Used	Available	Utilization
slice registers	28	126800	0%
Slice LUTs	108	63400	0%
Fully used LUT-FF pairs	26	51	23%
Bonded IOBs	67	210	31%
BUFG/BUFGCTRLs	1	32	3%

CED is suitable to detect only single faults in the circuit. For instance, in the event that the output data has a certain number of logic 1s and logic 0s, the CED technique forecasts the parity bits for the data. It can easily be noticed, when an attacker try to add hardware Trojan logic which modifies output data bits of the logic circuit. An attacker or adversary should not able to resolve the OCP, on other hand the attacker modifies the logic circuit outputs and OCP outputs, hence the checker doesn't find any errors.CED method generally considered that fault is at only one block, but these assumptions are not sufficient for hardware Trojan detection

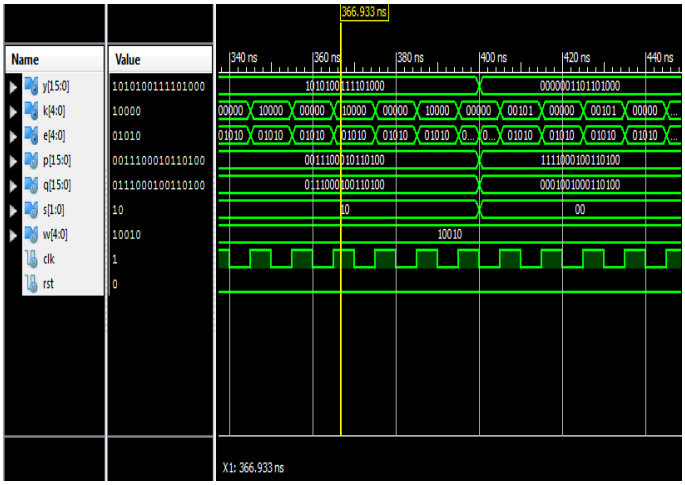


Fig. 11. Proposed work Simulation Result

because the output data can be altered by an attacker by inserting hardware Trojan logic into the checker circuit. In this case, an encryption key with large size is required to improve system randomness. In order to keep an opponent or attacker from anticipating the error signal value, a 128-bit encryption key has been employed. The output error signals correspond to the bits used for the 128-bit encryption key if no attack is found in the circuit. If not, the circuit assault is interpreted by the checker.

Table 2. Comparison between 64 bit and 128 bit Encryption Key generator

Logic Utilization	64 bit Encryption Key generator			128 bit Encryption Key generator		
	Used	Available	Utilization	Used	Available	Utilization
Slice Registers	29	126800	0%	28	126800	0%
Slice LUTs	320	63400	0%	108	63400	0%
Fully used LUT-FF pairs	28	51	8%	26	51	23%
Bonded IOBs	222	210	105%	67	210	31%
BUFG/BUFGCTRLs	1	32	3%	1	32	3%
Possible ways to encrypt error signals	$64C_5$ 76,24,512			$128C_5$ 2,64,566,400		

5. Conclusion

In IC development process the involvement of third parties reduces the manufacturing cost. Test pattern generators are unable to identify hardware Trojan due to malicious attacks. In this paper, 16-bit adder logic circuit has been proposed and implemented with security design. The 16-bit adder logic circuit gains security for input port, output port as well as on chip logic. CED continuously checks the on chip logic for every input. During checking error , signals are computed in CED and input decoding modules. These error signals describe the status of the circuit. Status implies information about whether hardware Trojan attack happened or not. If encryption key has more length more length, more number of ways encryption is possible, therefore in the proposed method 128-bit encryption key generator has been introduced. It generates a 128-bit encryption key for one clock cycle, 2^{128}possible patterns for one clock cycle. In existing work 4-bit input/output logic circuit secured by 3-bit encryption key, this is generated by 3-bit LFSR. Hardware complexity of the proposed work depends on number of parity bits. Parity bits are generated according to Hamming code in random parity. As input or output data length increases, the parity bits generation decreases. Considering a 4-bit data three parity bits are generated. In the 128-bit data, eight parity bits are generated. From the above discussion it is observed that the hardware complexity depends on number of parity bits. Only one way encryption is possible for one clock cycle in existing work. In the proposed , less hardware and tremendous security system has been implemented and compared to existing work.

The Trojan detection techniques for MSI circuits have been proposed in this work. In future it may be extended to some DSP applications and can be implemented in

MPSoCs which may result in efficient area and power optimizations to a constrained level.

References

[1] Rajit Karmakar, N. Prasad, Santanu Chattopaddhaya, Rohit Kumar and Indranil Sengupta " A New Logic Encryption Strategy Ensuring Key Interdependency". 2017 30th International Conference on VLSI Design and 2017 16th International Conference on Embedded Systems, 2017, pp. 429-434.

[2] Nandeesha Veeranna and Benjamin Carrion Schafer "Hardware Trojan Avoidance and Detection for Dynamically Re-configuarable FPGAs" 2016 International Conference on Field Programmable Technology (FPT) Dec 2016, pp. 1-4.

[3] Jiliang Zhang "A Practical Logic Obfuscation Technique for Hardware Security." IEEE Trans.Very Large Scale Integr. (VLSI) Syst., vol. 24, no. 3, March 2016, pp. 1193-1197.

[4] N. Fern, S. Kulkarni, and K. T. T. Cheng. "Hardware Trojans hidden in RTL don't cares Automated insertion and prevention methodologies". Test Conference (ITC), IEEE International, Dec.2015, pp. 1-8.

[5] K. Xiao, D. Forte, and M. Tehranipoor, "A novel built-in self authentication technique to prevent inserting hardware Trojans," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 33, no. 12, Dec. 2014,pp. 1778–1791.

[6] Swarup Bhunia, "Hardware Trojan Attacks: Threat Analysis and Countermeasures". Proceedings of IEEE, vol.2, no.8, Aug 2014, pp. 1229-1247.

[7] N. Nowroz, K. Hu, F. Koushanfar, and S. Reda, "Novel techniques for high-sensitivity hardware Trojan detection using thermal and power maps," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 33,no. 12, Dec. 2014 pp. 1792–1805.

[8] Waksman, M. Suozzo, and S. Sethumadhavan, "FANCI: Identification of stealthy malicious logic using Boolean functional analysis," Proceedings of the ACM Computer and Communications Security'13(CCS'13), Berlin, Germany, Nov. 2013, pp. 697–708.

[9] Sheng Wei and Miodrag Potkonjak "Scalable Hardware Trojan Diagnosis" IEEE Trans.Very Large Scale Integr. (VLSI) Syst., vol. 20, no. 6, june 2012, pp. 1049-1057.

[10] H. Salmani, M. Tehranipoor, and J. Plusquellic, "A novel technique for improving hardware Trojan detection and reducing Trojan activation time," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 20,no. 1, Jan. 2012, pp. 112–125.

[11] Huafeng Liu and Hongei Luo, LiweiWang "Design of Hardware Trojan Horse Based on Counter" International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering, June 2011, pp. 1-3.

[12] Baumgarten, A. Tyagi, and J. Zambreno, "Preventing IC piracy using reconfigurable logic barriers," IEEE Des. Test Comput. vol. 27, no. 1, Jan./Feb. 2010 ,pp. 66–75.

[13] M. Potkonjak, A. Nahapetian, M. Nelson, and T. Massey, "Hardware Trojan horse detection using gate-level characterization," Proceedings of the 46th ACM/IEEE Design Automation'09 (DAC'09) conference, San Francisco, CA, USA, Jul. 2009, pp. 688–693.

[14] M. Abramovici and P. Bradley, "Integrated circuit security: New threats and solutions," Article No.55, Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research'09 (CSIIRW'09), Knoxville, TENNESSEE, USA, Apr.2009, pp. 1–3.

[15] N. A. Touba and E. J. McCluskey, "Logic synthesis of multilevel circuits with concurrent error-detection," *IEEE Trans. Comput.-Aided DesignIntegr. Circuits Syst.*, vol. 16, no. 7, Jul. 1997, pp. 783–789.