ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Design of Silicon Physical Unclonable Function for Authentication Of A Multicore Device.

Sudhanya P*, and P Muthu Krishnammal.

Sathyabama University, Chennai, India.

ABSTRACT

Physical Unclonable Function (PUF) is a promising method of secure identification and authentication of devices. PUF provide cheap, efficient and secure authentication. A PUF will generate a specific bit pattern response for a specific challenge. Since the response depends on the inherent properties, the attacker cannot replicate the PUF device even by knowing its design. In this paper a new delay based Silicon PUF design has been proposed and logically simulated to obtain its results. The newly designed PUF can be used in medical field for securing the RFID tags.

Keywords: Physical Unclonable Function (PUF), Process variations, Delay, Authentication, Fault Diagnosis, Voting Mechanism.

**Corresponding author*

INTRODUCTION

In the present scenario, IC security is an important area of concern. We can identify a number of hardware design threats such as counterfeiting, reverse engineering, tampering etc. As the cryptography or other techniques are expensive and needs external memory to store the IDs, PUFs (Physical Unclonable Functions) can be preferred over them to defeat such threats.

Using the inherent physical properties of a system for identification and security is not a new idea. The identification of people using fingerprints started in 19th century. In the same way intrinsic properties of a circuit can be used to identify and secure the integrated circuits. PUF, Physical unclonable functions, are also known as, physically unclonable functions. PUFs are physical entity which is substantiated on a physical structure. A PUF's, response should be very hard to predict. A PUF device should be easy to fabricate but practically it should not be possible to clone even with the same fabrication process.

A physical unclonable function generally performs a functional operation or it can be considered as a procedure performed by a particular (physical) system. The input to a PUF is called a challenge and the output a response. The applied input and its measured output are generally called a challenge-response pair or CRP.

The main PUF properties include reliability, uniformity and uniqueness.

- Reliability: For particular challenges with respect to varying supply voltage and temperature, the response of the PUF should be consistent.
- Uniformity: Uniformity implies that, there should be an equal distribution of 1's and 0's in the output. It is also called randomness. An ideal PUF would show a uniformity of 50%.
- Uniqueness: The responses to the same challenge should be different, for two instances of the same PUF design.

The creation of unique keys or signatures demands this property.A PUF duplicated on another chip should create a signature with a hamming Distance of around fifty percentages, which implies half the bits are totally different.

Generating volatile chip-specific signatures at runtime is a necessary advantage of Physical Unclonable Function (PUF). The PUF excludes the necessity of an expensive non-volatile memory for key storage. A robust security shield against attacks is provided by the PUFs and they are cost effective.

PUFs find many applications in IC world because of its inexpensive and unique nature such as

- System Identification
- Secret key generation
- Random Number Generation
- Cryptography
- RFID tags for medical applications

Previous Works

A variety of PUF designs have appeared over the past fifteen years. The PUF classification can be done based on manufacturing material or based on the number of CRPs. PUFs can be divided into strong PUFs and weak PUFs based on the number of CRPs. The strong PUF includes the optical PUF, arbiter PUF, lightweight secure PUF, etc. The weak PUF mainly includes the memory-based PUF, RO PUF and glitch PUF.

Based on the material of manufacturing, the PUFs can be divided into Silicon and non-Silicon PUFs. TheNon-Silicon PUFs mainly includes the optical PUF, paper PUF, acoustical PUF, CD PUF, RF-DNA PUF, magnetic PUF, and phosphor PUF.

Silicon PUFs are more interesting in terms of manufacturing cost and readiness in integrating with computing and communication devices. Silicon PUFs utilize the uncontrollable manufacturing process variations to produce a novel signature for each IC. According to the different sources of variation, there are three major silicon PUFs available. They are memory-based PUFs, analog electronic PUFs, and delay-based PUFs.

Analog Electronic PUFs mainly include ICID, the coating PUF, silicon nano key, LC-PUF and power grid PUFs. Memory-Based PUFs mainly includes SRAM PUF, Butterfly PUF, latch PUF, flip-flops PUF, Bi stable ring PUF, MECCA PUF etc. Delay-Based PUFs mainly includes Arbiter PUF, Ring Oscillator PUF, Anderson PUF, memristor PUF, Thyristor based PUF etc.Different types of delay based PUFs are explained below.

Arbiter PUFs

The arbiter PUF is a well-studied design, published in 2004 [5]. In the general sense, an arbiter PUF sets up a set of closely-matched race tracks with an arbiter at the end to determine which signal reached the end first-typically this is a D Flip-Flop with one signal attached to the clock pin and another attached to the data pin. The basic arbiter PUF is as shown in Figure 1.

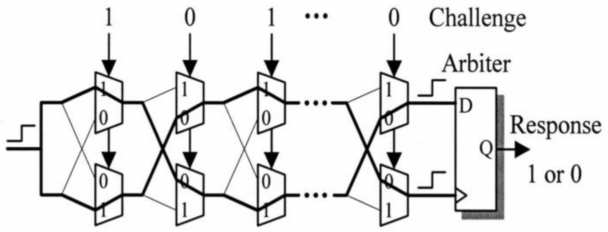


Figure 1: Basic Arbiter PUF

Ring Oscillator PUF

The ring oscillator (RO) is one of the earliest and mature classes of delay-based silicon PUFs, first introduced in [6, 7], and it is popular PUF designs on FPGAs, since absolute symmetry is not necessary to create an oscillator, and the error associated with making a single measurement is amortized across many oscillator cycles.

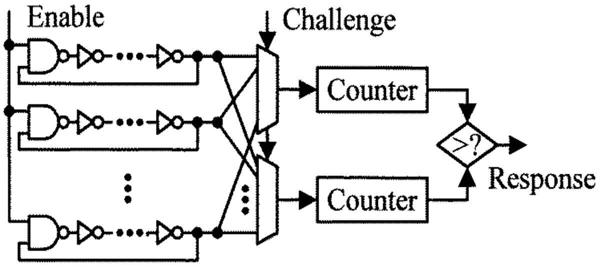


Figure 2: RO PUF with Differential configuration

The "differential" measurement with RO PUF has been shown to give better results than the basic RO design. A typical RO PUF with such a configuration is shown in Figure 2.

Anderson PUF

The Anderson PUF [9] is the first PUF designed for implementation on FPGAs. Unlike many PUFs designed for FPGAs, it uses the carry chain multiplexers present in certain FPGA components. A simplified depiction of Anderson's PUF is shown in Figure 3.

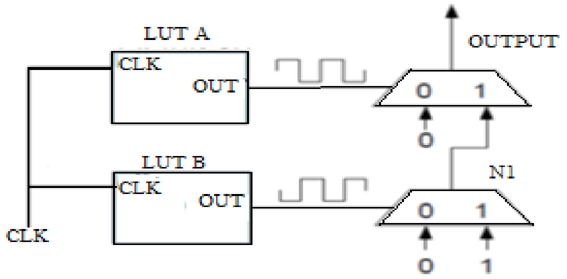


Figure 3: Structure of Anderson PUF

Memristor PUF

Memristors are electrical elements that are used to relate magnetic flux linkage and charge. A write-time primarily based memristive PUF is given in [13] that leverages variability within the SET time of the memristors. A 1 bit memristive PUF cell is shown in Figure. 4.

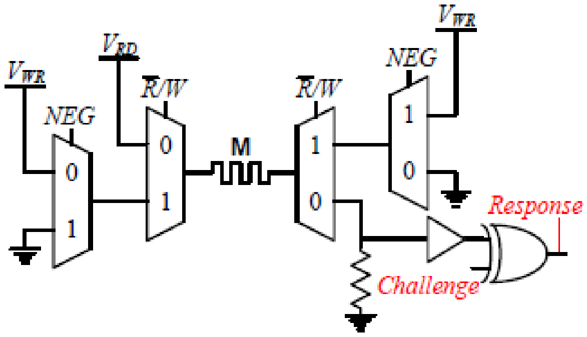


Figure 4: A 1-bit memristive memory-based PUF cell

Thyristor based PUF

A new thyristor sensor based PUF was introduced in [10] and the Figure.5 shows the architecture of the thyristor-based PUF. The new thyristor based PUF system comprised of thyristor-based sensors, Time Difference Amplifier (TDA), voting mechanism, Time Difference Comparator (TDC), and diffusion algorithm circuit. In this system the set of select line bits are the challenge and an output ID bit is considered as the response. Here the thyristor delay elements are used to capture the manufacturing process variations and the thyristor-based sensor is composed of these delay elements. Each thyristor sensor could produce two slightly different delay-time values that are dependent on discharge current of thyristor delay elements.

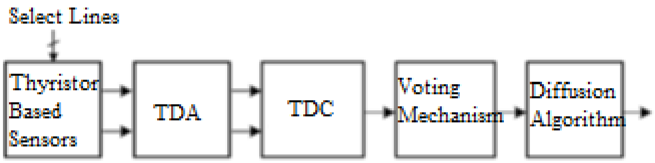


Figure 5: Basic operation of Thyristor based PUF

Multiple thyristor-based sensors are designed to be identical according to the number of bits needed in the CRPs. Time difference amplifier is used to amplify slight delay-time difference from selected thyristor-based sensors. The output of TDA is then compared to generate an ID 0/1 bit for the chip using a time difference comparator, i.e., an SR latch. A stable ID bit based on probability distribution is produced by voting mechanism circuit by sampling the output of the comparator many times. Diffusion algorithm circuit is then used to transform ID bits according to certain diffusion algorithms, which ensures that transformed IDs have a good characteristic of uniform statistical distribution.

PROPOSED SYSTEM- A NEW SILICON PHYSICAL UNCLONABLE FUNCTION FOR AUTHENTICATION OF A MULTICORE DEVICE

A new delay based Silicon PUF can be designed as shown in the flow diagram Figure.6. The newly designed system has added advantage of fault diagnosis of the multicore device using the generated signature. Authentication and fault diagnosis using the system can be carried out using two modes of operation. Two modes of operation are Normal mode (Authentication of device) and Test mode (Fault Diagnosis of system).

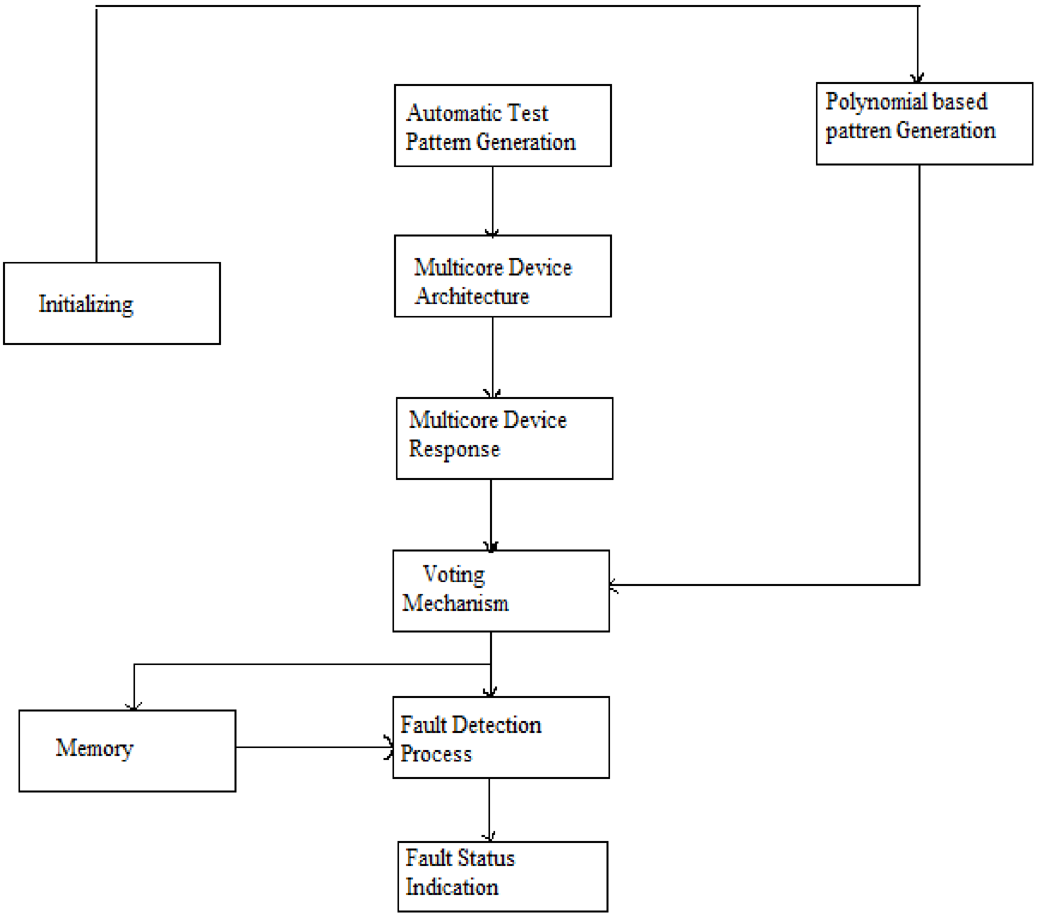

Automatic Test Pattern Generation
Polynomial based pattren Generation
Multicore Device Architecture
Initializing
Multicore Device Response
Voting Mechanism
Memory
Fault Detection Process
Fault Status Indication

Figure 6: Flow Diagram of Proposed PUF System

Modes of Operation

Normal mode (Authentication of device)

By using the inherent process variations and without excess extra hardware, signature can be produced and authorization is possible by making use of this signature or ID. The delay is created in simulated stage by comparing the response of random polynomial equation and the multi core device output. From this delay a golden signature is being generated.

Test mode (Fault Diagnosis of system)

After generating the signature, if the fault diagnosis is needed, the signatures have to be kept on the memory for comparing the results in run time. In the testing mode the stored IDs of each of the processor inside the multicore device is compared with the generated IDs from the processors and if there is any deviation in IDs, the fault is identified. The overall fault diagnosis is also possible by utilizing the single ID that is being created for the device.

STAGES IN THE PROPOSED SYSTEM

Automatic Test Pattern Generation

In this stage, automatic test patterns are generated for further processing. These test patterns are given as input to Multicore processor. Automatic patterns are generated from two 32 bit inputs using reset and clocking sequence. In order to use in different processor elements, we are using different logic to produce the patterns automatically. So according to the logic, the automatic patterns are generated for individual processors of multicore device in response to clocking sequences.

Multicore Device

The multicore device is the device which is to be authenticated or a unique signature is to be generated. This work considers a multicore processor (Arithmetic core processor) architecture which consists of an adder, a comparator, a subtractor and a multiplier unit. Along with the signature creation, we are going to identify whether any of the processor in the multicore processor is faulty or not.Each of the processor in the multicore processor produces a 64 bit output in each process. All the processor inputs are of 32 bits and are intern producing a 64 bits output.

Polynomial based pattern generation

A polynomial based random pattern generation is also used to produce a unique signature for the processor and those random patterns based on a polynomial are generated in this stage. Cryptographic systems use random sequences extensively in their applications. Sequences of zero and one bits are produced in random number generators. The unpredictability of random number sequences can increase the security of cryptographic systems. Pseudo Random Number Generators and True Random Number Generators are two types of random number generators. One-way functions are used to generate a sequence in Pseudo RNG based on a mathematical algorithm. The complexity of its algorithms and functions decides the security of pseudo random sequence. The linear feedback shift register (LFSR) are a common circuit used to generate pseudo random sequences. A non-linear feedback shift register (NFSR) will be achieved by connecting a non - linear function of the previous state of shift register to its input. Since the function is very unpredictable, the PUF produces completely randomized stream of bits. This paper proposes the design and implementation of a new PUF-which is based on generated sequence of random numbers.PUF based polynomial equation consist of D-FF connected in cascade with the same clock applied to the entire FF to make them act like a shift register. The XOR operation introduces a pattern in the next stage.

Voting Mechanism

Unique signature (ID) is getting generated by comparing the polynomial based random pattern and response of multicore device. Voting mechanism produces a 64 bit signature for the multicore device- Individual signature for each of the processor inside the multicore device and a single Signature for the multicore device. The 64-bit majority architecture is used to the data encoding process and to modify the majority function using the Boolean logic function. The signature produced is used for authentication and in fault diagnosis process.

So by the majority function logic a unique signature is getting generated from the responses of the multicore device and random pattern generator response.

ROM memory

If the system is using for testing purpose, we need to store the signatures that are created for the future purpose. So the Signatures (IDs) for testing purpose are stored in the memory according to the clocking sequences.

Fault detecting process

By comparing the expected signature and the produced signature, fault diagnosis can be done. It is to identify multicore device fault status and to reduce the test process time. Output response comparator compares the golden signature from ROM memory and signature results from majority circuit level. Circuit under test was performed before the device assembly. The fault status indicates particularly gives the faulty processor, if the fault is present.

Fault indication

In the fault indication process, a logic function is used to show the fault status in characters. It takes the 4 bit value and converts it into characters to show which unit of the multicore device is faulty.

RESULTS AND CONCLUSION

The logic simulation of the circuit is done and the results are analyzed. The waveforms are as shown below. In the normal mode, from the delay produced from the outputs of multi-core device and the polynomial based random number generator, a unique ID is generated as shown in Figure. 7.

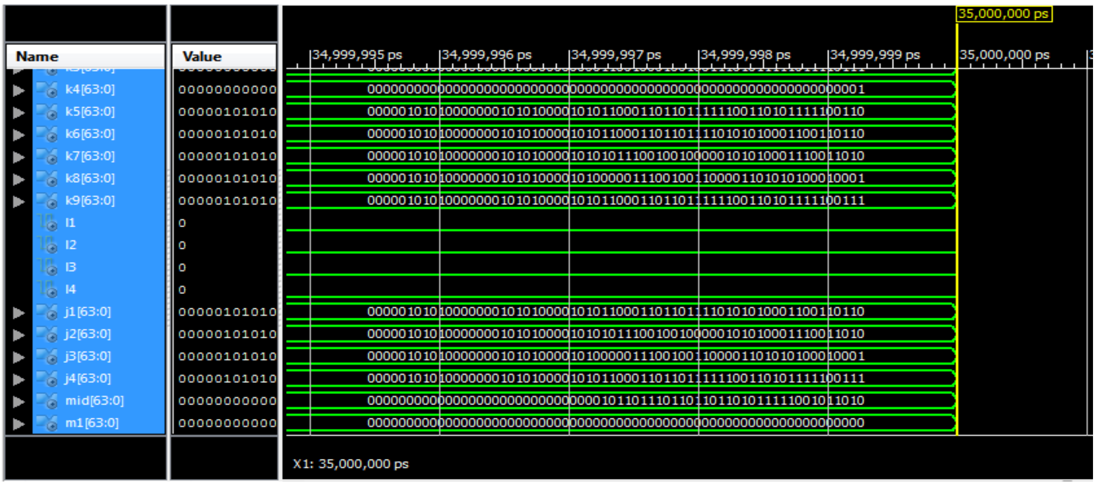


Figure 7: Single ID generation for authentication of device.

In the testing mode the fault in the system can be identified and its response can be seen in the response. If there is no fault is present, the response will show '–no' shown in Figure.8.

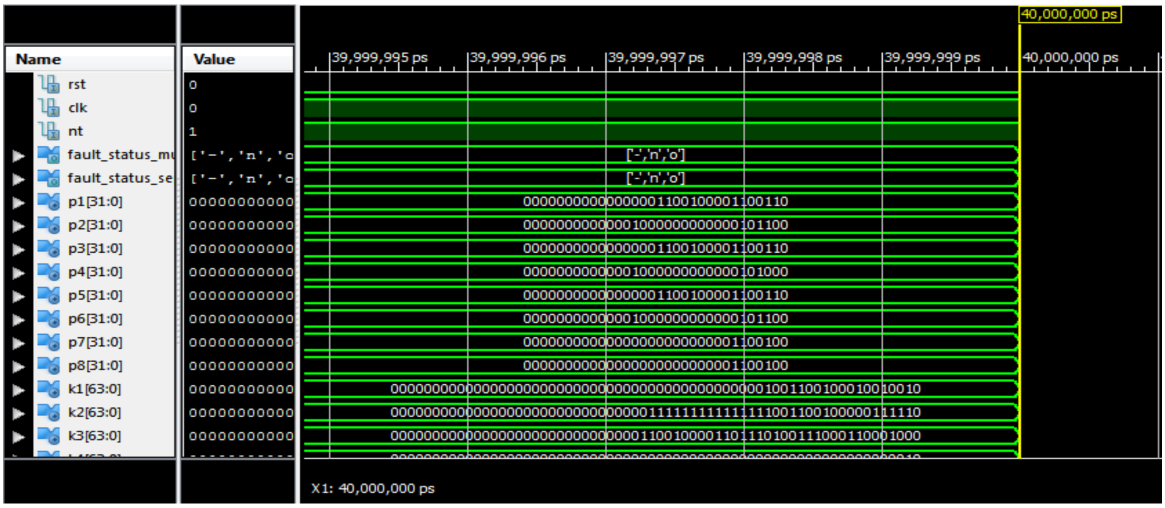
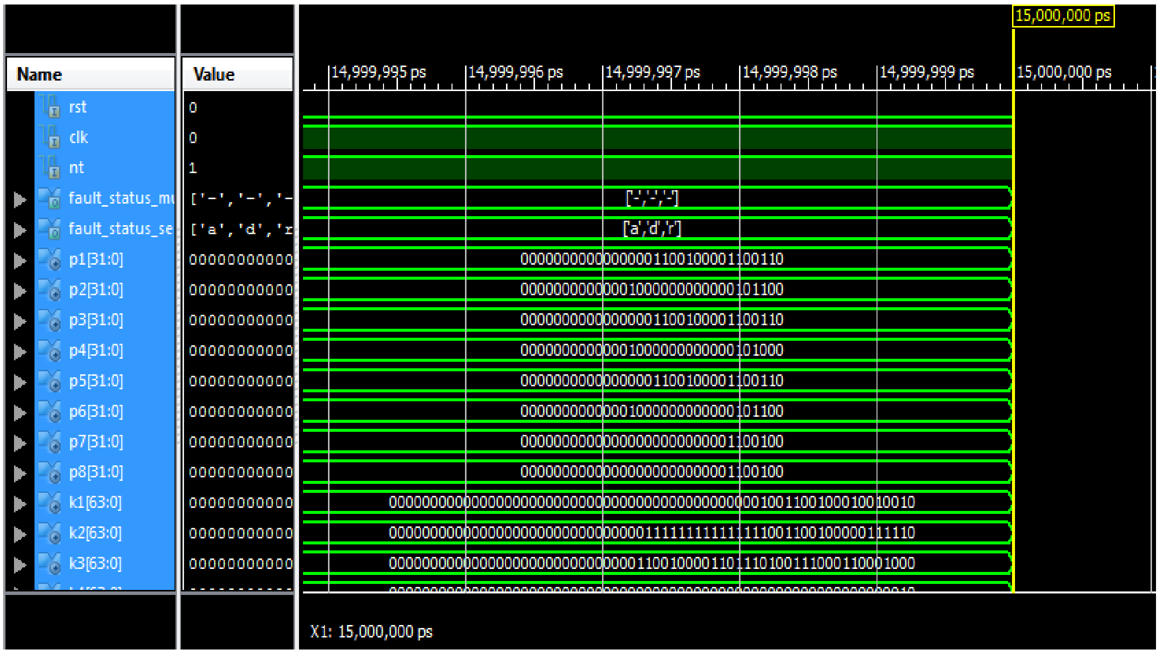


Figure 8: Fault status indication in testing mode with no fault.

The fault status indication with fault in adder unit of multi-core device is shown in Figure.9 for example. If the fault is present in any of the processors in the device, the result shows it specifically. In this example, adder has fault and the results shows in ‘adr’ for adder.



```
Name                Value          14,999,995 ps  14,999,996 ps  14,999,997 ps  14,999,998 ps  14,999,999 ps  15,000,000 ps
rst                 0
clk                 0
nt                  1
fault_status_mu     ['-','-','-    ['-','-','-']
fault_status_se     ['a','d','r    ['a','d','r']
p1[31:0]            00000000000    00000000000000001100100001100110
p2[31:0]            00000000000    00000000000001000000000000101100
p3[31:0]            00000000000    00000000000000001100100001100110
p4[31:0]            00000000000    00000000000001000000000000101000
p5[31:0]            00000000000    00000000000000001100100001100110
p6[31:0]            00000000000    00000000000001000000000000101100
p7[31:0]            00000000000    00000000000000000000000001100100
p8[31:0]            00000000000    00000000000000000000000001100100
k1[63:0]            00000000000    0000000000000000000000000000000000000000000001001100100010010010
k2[63:0]            00000000000    0000000000000000000000000000011111111111111100110010000011111110
k3[63:0]            00000000000    0000000000000000000000000000011001000011011110100111000110001000

X1: 15,000,000 ps
```

Figure 9: Fault status indication in testing mode with fault in adder.

So the newly designed PUF system can be used for any processor along with the other stages of system for its authentication and fault diagnosis.

Future work

The present work describes a new design of Silicon PUF and its application for device authentication and fault diagnosis. This research work can be extended by carrying out the detailed study of the characteristics of the new proposed PUF system. The response of the system to the variation in the environmental conditions also to be further studied. The possible application of new PUF system in medical field for securing the RFID tags are also to be explored in future.

REFERENCES

[1] R. Pappu, R. Recht, and J. Taylor, “Physical one-way functions," in Science, SEP. 2002, pp. 2026-2030.

[2] A. Maiti, V. Gunreddy, and P. Schaumon, “ A systematic method to evaluate and compare the performance of physical unclonable functions," in IACR ePrint, 2011.I.S.JacobsandC.P.Bean, “Fineparticles,thinfilmsandexchangeanisotropy,” inMagnetism,vol.III,G.T.RadoandH.Suhl,Eds.NewYork:Academic,1963,pp.271–350.

[3] Lofstrom K, Daasch W R, Taylor D. IC identification circuit using device mismatch. In Proc. IEEE International Solid- State Circuits Conference, Feb. 2000, pp.372-373.

[4] Aaron Mills, Design and evaluation of a delay-based FPGA physically unclonable function, 2012.

[5] Ji-Liang Zhang, Gang Qu, Yong-QiangLv, Qiang Zhou, A Survey on Silicon PUFs and Recent Advances in Ring Oscillator PUFs. In: Journal of Computer Science and Technology 29(4): 664-678, July 2014

[6] D. Lim, J. Lee, B. Gassend, G. Suh, M. van Dijk, and S. Devadas, “Extracting secret keys from integrated circuits," Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, vol. 13, no. 10, pp. 1200 {1205, oct. 2005.

[7] B. Gassend, “Physical Random Functions," Master's thesis, MIT, MA, USA, 2003.

[8] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," In Proceedings of the 9th ACM conference on Computer and communications security, ser. CCS '02. New York, NY, USA: ACM, 2002, pp. 148-160.

[9] "Read-proof hardware from protective coatings." in Cryptographic Hardware and Embedded Systems - CHES 2006, 8th International Workshop, 2006, pp. 369-383.

[10] Chuang Bai, Xuecheng Zou, and KuiDai , '' A Novel Thyristor-Based Silicon Physical Unclonable Function'' IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, 2015.

[11] Su, Y., Holleman, J., Otis, B.: A 1.6pj/bit 96% stable chip-id generating circuit using process variations. In: Solid- state Circuits Conference, 2007. ISSCC 2007. Digest of Technical Papers. IEEE International, pp. 406{611 (2007).

[12] RoelMaes, Ingrid Verbauwhede: Physically Unclonable Functions: a Study on the State of the Art and Future Research Directions, In:Towards Hardware-Intrinsic Security, Part of the series Information Security and Cryptography pp 3-37, (2010).

[13] Garrett S. Rose, Nathan McDonald, Lok-Kwong Yan, and Bryant Wysocki, "A Write-Time Based Memristive PUF for Hardware Security Applications," in Computer-Aided Design (ICCAD), 2013 IEEE/ACM International Conference, 2013, pp. 830-833.