ISSN: 2395-1680 (ONLINE)
DOI: 10.21917/ijme.2018.0104

IMPLEMENTATION OF A HYBRID RING OSCILLATOR PHYSICAL UNCLONABLE FUNCTION

N. Sivasankari[1] and A. Muthukumar[2]
[1]*Department of Electronics and Communication Engineering, Mepco Schlenk Engineering College, India*
[2]*Department of Electronics and Communication Engineering, Kalasalingam University, India*

Abstract

Developing a hybrid ring oscillator based Physical Unclonable Function (PUF) in FPGA is the main work of this paper. Each structure has its own virtuous characteristics thus the desirable characteristics are selected from each PUF then they are combined together to get the hybrid PUF structure. Mainly PUF structures are used as random number generator which should be same at all the generation times. This property makes the circuit suitable for secure cryptographic structure applications. In this paper hybrid ring oscillator structure is proposed for enhancing uniqueness and reliability. The experiments were conducted on Xilinx FPGA's with the certain challenging set and produce unique response only for the concerned chip. In the experimental analysis, the proposed design increases the circuit complexity, but the power consumption seems to be same with the traditional designs.

Keywords:

Hardware Security, Uniqueness, Random Number Generation, Intrinsic PUFs, IP Protection, IC Authentication

1. INTRODUCTION

In the forthcoming years, the identity number generation and process of creating authentication to the corresponding person becomes a very important task. To increase authenticity and confidentiality, many techniques have been used in the field of cryptography. Still there is a possibility of adversary's actions such as man in the middle attack, malicious code injection or vital code part deletions. To overcome this issue Biometrics is the only solution for creating unique identity generation, but when the biometric chip is replaced or modified, the whole system responds only to the adversary. Nowadays, usage of RFID tags has become the important part for security. In RFID tags, small amount of storage is available for storing information. Within that restricted storage area, feeding large biometric information is not possible. Additionally, adversaries can also clone the chip of RFID in easy manner. The only solution for the problems in RFID tag is to make the unique chip for each person. Physical Unclonable Functions (PUFs) is an emerging cryptographic primitive to produce device fingerprint. A Physical Unclonable Function (PUF), which is a unique challenge-response function, is an emerging hardware primitive for secure applications. PUF make use of manufacturing process variations in a die to generate exclusive signatures out of a chip. This enables chip authentication and cryptographic key generation. PUFs properties are bounded to the underlying hardware. It can be easily evaluated by authorized parties within the device only. The responses are not easily predictable by adversary. It is tamper evident and have a resistance to physical attacks. The chip uniqueness can be implemented by PUF method. Hence an enhanced PUF method has been proposed. Recent works [1]-[7] on PUF show that it is possible to avoid the malicious attacks and maintain the confidentiality and authenticity within the crypto processor of PUF. The Fig.1 shows the functional description of PUF circuit.

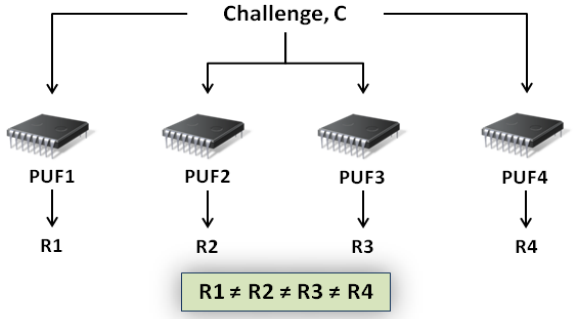

Fig.1. Functional description of PUF

This paper is organized as follows: Section 2 explains various types of PUFs available, with the help of literature survey. Section 3 narrates the concept of controlled inverters and explains how it is modified in proposed ring oscillator PUF for our work. Section 4 shows the results and discussion for the proposed hybrid ring oscillator PUF. It is followed by conclusion with future direction of PUF work in section 5.

2. RELATED WORKS

The identity of any chip is defined by PUF technology. PUF is also known as hardware one-way function i.e., the response generated by one chip is not same with other chip with the same input. However, the quality factors of this PUF, which include uniqueness, reliability and attack resiliency, are negatively affected by environmental noise and systematic variations in the die. This technology can be either built at integrated circuit fabrication level (explicitly introduced randomness) or it can be constructed by some logic circuits (intrinsic randomness). The classification of PUF is shown in Fig.2.

2.1 EXPLICITLY INTRODUCED RANDOM PUFS

The production process technology is decided by particular application and availability of materials. PUF production process produce each IC's with a unique characteristic. As per [8] the production process of PUF is classified here. Optical PUF's contain a transparent substrate with light scattering particles. When the light scattering particles were irradiated with the laser beam, PUF's can create the unique speckle pattern. The uncontrolled placement of the scattering particles and interaction between the laser and the particles is unpredictable. Memristor is considered as a fourth element in passive components which exhibits different properties under different doping condition, in turn, it can produce different electrical characteristics, through that different random functions can be created. The concentration of the doping material (titanium oxide (Tio_2)) for each of the IC

must be different; which affects the resistance of the device, which can be characterized by,

$$R_{eq}(t) = \frac{w(t)}{D} \cdot R_{on} + (1 - \frac{w(t)}{D}) \cdot R_{off} \quad (1)$$

where, R_{on} is the least resistance value when more dopants are added or the whole device is doped. Similarly R_{off} is the resistance when only the small area is doped or the entire area is undoped. The width of the doped region is mentioned as w, whereas the total width is D. When the width variable $w(t) = D$, the equivalent resistance is just R_{on}. Similarly, when $w(t) = 0$, then the equivalent resistance is R_{off}. The varying nature of resistance can be utilized for creating PUFs as per [15].

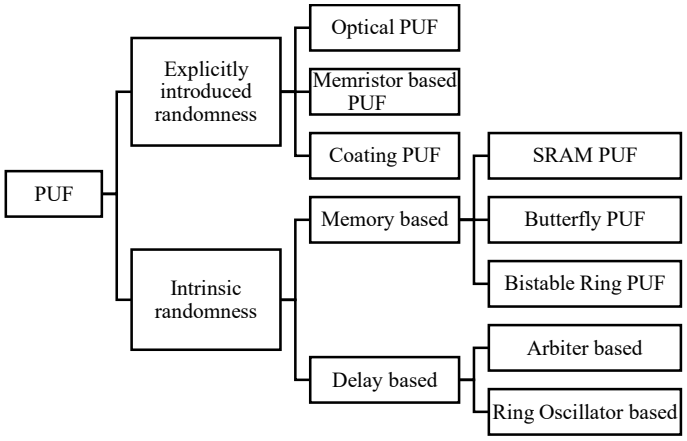

Fig.2. PUF classification

For coating PUF a dielectric material with different random permittivity (a mixture of Tio_2 and Tin) is spreaded over the top layer of the normal IC which acts as PUF [16]. An array of sensors arranged in comb like structure reveals different capacitance values. Hence the random number generation depends upon the location of dielectric particles and charging and discharging properties of capacitors.

2.2 INTRINSIC RANDOMNESS PUFS

Explicitly introduced random PUFs should be constructed during the manufacturing process, but intrinsic randomness PUFs can be included in any FPGA design module. Intrinsic randomness PUF circuits contain an array of circuits either as a form of memory elements or some set of delay elements. Hence, they are classified as memory based PUF and delay based PUF in intrinsic randomness PUFs.

2.2.1 Memory Based PUF:

The SRAM PUF works on the principle of startup behavior [2] [12] of SRAM cells. The threshold voltage mismatch (even in the same manufacturing process) of the MOS transistors creates two stable states either as '0' or '1'. It can be used directly as a key to protect sensitive data. The idea described in [2] classify the memory cells of the standard SRAMs into two disjoint events, one suitable for generating identifiers or secret keys, and the other suitable for the generation of random numbers. This classification method under different operating condition proves that misclassification of cells due to aging problems may be reduced. Kumar in [13] used Butterfly based PUF Internet Protocols for handling sessions which is feasible to implement in FPGA. Butterfly PUF (BPUF) contains two cross coupled D flip flops which act as latches. The challenge or excitation input is given as clear input for one latch, preset input for next latch. The final output is determined by the random delay variations in the challenge signal path. In eight stages Bistable Ring Oscillator PUF the possible response may be "10101010" or "01010101" based on the input challenge lines. If the reset input is '1' means all the outputs will be '0' from each BR cell. If reset input is '0' then each it works as inverter. This makes the behavior of BRO-PUF is easy for machine learning attacks and cryptanalysis. To overcome this problem, challenge lines are applied to the certain number of BR cells simultaneously as suggested by [17]. The results from all the cells are XORed together to get a single response which will prevent brute force attack.

2.2.2 Delay Based PUF:

The idea behind the delay based PUFs are that two circuit path delays try to win themselves to reach the destination path first. If the first path reaches first means the response is '1', otherwise '0'. An Arbiter PUF [4] (APUF) is composed of two identical configured delay paths that are stimulated by a clock signal. The multiplexer select lines are challenge line inputs. Each challenge line has to select two 2:1 multiplexer outputs. The edge triggered flip flop latch is used for measuring the delay difference between the two propagation paths. This difference can't be predictable due to manufacturing process variation present in the multiplexer (two AND gates and one OR gate) and latch. In Ring Oscillator PUF (RO-PUF), variations in the frequencies of identically constructed ring oscillators are utilized to build the PUF. The RO frequencies are monitored and transmitted using multiplexer. Number of inverters in each ring oscillator can be three or five or any odd numbers. In a frequency counter, the frequencies are counted and the frequency deviation in the set of ring oscillators is transformed into binary outputs by a simple comparison method. As shown in Fig.3, challenge lines act as the multiplexer select lines. Common enable signal is given to all RO structures. The multiplexer select lines are challenge lines which are going to select any of the rows from upper and lower ring oscillator set for comparison. Due to manufacturing variations each ring oscillator frequency will be varied and this variation is recorded by frequency counters and comparators. A large amount of area is occupied by two frequency counters and comparator circuit as by the circuit suggested in [3]. Hence they can be replaced by a frequency divider network as described in [16] where the modulus value is considered as response. A ring oscillator (RO) based PUF is a promising solution for FPGA platforms. In this paper typical ring oscillator structure form is modified. Hence the previous works on the ring oscillator structure is focused. The single chip secure processor introduced by Sue and Devedoss known as AEGIS secure processor [1] [9] in which the encryption key from PUF secret security kernel and main processor is implemented on the same chip. Consider a situation where ID is generated in separate module and transferred to the main module for verification and further calculation where they are communicated by cable, it can be tracked by attacker. The hackers can stole the data using cables without the knowledge of customer. Hence to avoid this cryptographic module and main processor module are built with the same module. With this AEGIS processor, PUF plays the main role of creating the random number. When the ring oscillators chosen for comparison are varying only by small amount then the performance of them will be decreased with

respect to temperature. When 1 out of *k*-masking scheme is used, the particular set of the ring oscillator pair will be selected in upper and lower paths whose frequency variation is high. With this masking scheme the performance of PUF won't be degraded with respect to temperature. But these masking circuits will occupy more area and circuits. In addition to that the fixed RO-pair frequencies can be modeled and it is vulnerable to the attacker.

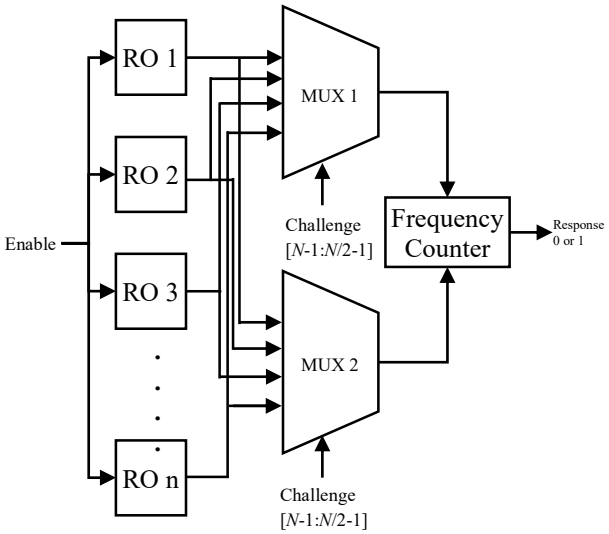

Fig.3. Typical Ring oscillator

This problem is overcome by Maiti's [10] reconfigurable PUF where each inverter block contains two NOT gates and 2:1 multiplexer where challenge bits acts as select lines. For a ring oscillator with three stages (each stage two inverters) 8 different configurations are possible. Minimum delay is noted for '000' challenge line and '111' challenge line exhibits maximum delay path. The various paths are selected only by challenge lines. Xin et al. [11] expands the idea of Maiti by inserting additional multiplexer in the ring oscillator package and by splitting the challenge lines for selecting inverters in the ring oscillator packages and multiplexer selection. Xin increases the number of possible configurations to 256. In all the ways the RO PUF works on the process of comparing frequencies. For each RO PUF one output bit is produced. For *n* output bits *n* RO PUF packages should be constructed. This PUF matrix value should be unique for every chip. Further it can't be traced by any of the mathematical modeling attack. In this paper ring oscillator based PUF concept with modification known as challenge line delay logic is proposed and discussed in section 5. In addition to that the delay in ring oscillator is increased by a basic logic of bistable ring oscillator PUF. In section 6 the results are compared with typical Ring Oscillator based PUF.

3. PROPOSED WORK

In cryptography PUFs can be used for generating seed for random number generation and unique identification for hardware devices. Hence to get the uniqueness, the circuit should be complicated enough that it cannot be producible. The structures of existing PUFs have been discussed. But within the existing structure how to get more random and unpredictable result is an art. Based on differential equations how to extract entropy is discussed in [6]. The operation of normal inverters is known to all. To increase the complexity control inverters are used. Controlled inverters or programmable delay lines [6] are used for giving the propagation delay in inverting. They are programmed based on challenge line inputs. The ultimate goal is to get unpredictable response from primitive PUF structure. The MUX select lines '11111' gives the longest path delay in the circuit, while the select lines '00000' gives the shortest delay path. The control line inverters are given in Fig.5. The delay lines in turn affect the response of the system in unique way which cannot be fabricated. The detailed description and operation of programmable five stage inverter is shown in Fig.5.

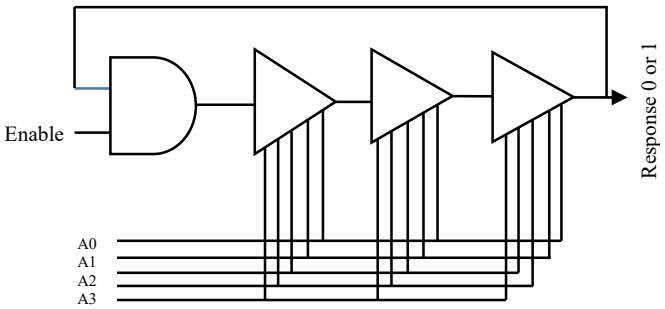

Fig.4. Challenge lines based controlled inverters

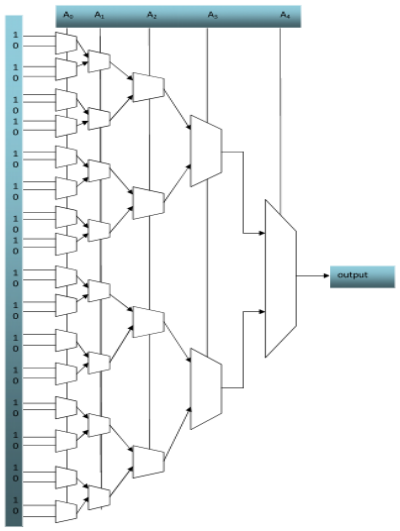

Fig.5. Five stage controlled inverter logic

Instead of using this kind of inverter based delay lines, shift register based delay line can also be used [7]. In case of shift registers delay line, each shift register is initialized by fixed values, and based on challenge lines logic output function will be defined. There is one another possibility of increasing complexity in this controlled inverter when the stored SRAM values in first stage multiplexer are not stored as fixed values of 1's and 0's, then the output from controlled inverter not only depends on the first control line but also of other control lines. If the first input in control line is '0' means the first input from all the multiplexer will be selected. If it is zero means the remaining inputs will not affect the performance of the control lines, but it introduces a delay lines in various paths.

3.1 CHALLENGE LINE BASED HYBRID RING OSCILLATOR:

Our proposed circuit structure is given in Fig.6, which makes use of complex programmable delay lines (challenge lines) concept in ring oscillator structure.

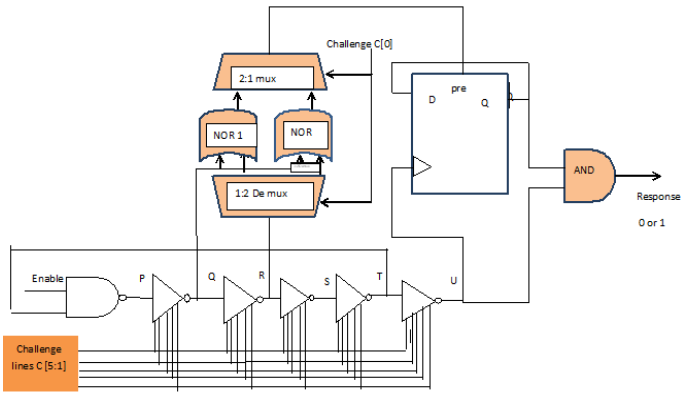

Fig.6. Hybrid PUF structure

One additional twist is included by replacing the reset pin in [14] by output of the successive inverter after NAND gate. For creating 64 bit response the module is replicated by 64 times. If enable input is '0', the output of NAND gate will indicate the value of '1'. If it is '1', as per Fig.5 the output of the first inverter be P= $\overline{T.Enable}$. The output values of successive inverters are based on the most significant bit of challenge line.

Coming to the MUX part primitive structure, (Mux and Demux and NOR gate), the DeMUX outputs may be either R. $\overline{c[0]}$ or $R \cdot c[0]$, where $c[0]$ is the challenge line least significant bit. When this entered into the NOR gate1 the output will be $\overline{Q \| (R \& \overline{c[0]})}$ and NOR gate 2 output will be $\overline{Q \| (R \& c[0])}$. The output of the NOR gates will be selected by 2:1 mux with the same challenge line $c[0]$. D flip flop gets the input from the previous Q output. At the same time the flip flop is triggered by output from ring oscillator set. The 'U' output serves for two purposes. (1) Clock input for D flip flop, (2) One of the input for AND gate. If both are equal to one then only the response bit will be '1' otherwise '0'.

4. RESULTS AND DISCUSSION

The proposed PUF architecture is implemented in Xilinx 7000FPGA and simulated using Modelsim-Altera 6.4a. Sixty four lines of ring oscillator structures are concatenated and simulated. Unless using delay lines for some of the inputs the outputs from all lines are equal in frequency counter (i.e.) the individual RO-PUF inverter delay values are changed during the time of simulation. The results obtained from Modelsim by giving delay is shown in Fig.7. PCB board implementation is shown in Fig.10. In performance analysis uniqueness indicates that the particular ID is generated for the particular set of challenges at all times. In this work 64 bit response is taken. The uniqueness (i.e.) how a PUF response can be uniquely generated is defined as their average pairwise Hamming distance as,

$$u = \frac{2}{k(k-1)} \sum_{i=1}^{K-1} \sum_{j=i+1}^{K} r_{i,j} \oplus r_{,,m} \qquad (2)$$

It is found out that out of the measurement of 50 times the uniqueness is 65.4%. For a set of challenge lines 384, the hamming distances between the obtained output responses of various PUF instances were calculated. For an ideal PUF the uniqueness should be 50%. In this work, the challenge lines itself used as programmable lines hence for each PUF circuit the deciding power mostly goes to LSB and MSB bits. The uniqueness results are varied depending upon the number of inverters. If the stages are increased then the output flipping also increases. The responses are taken for 50 times. The results are discussed by considering the following two conditions.

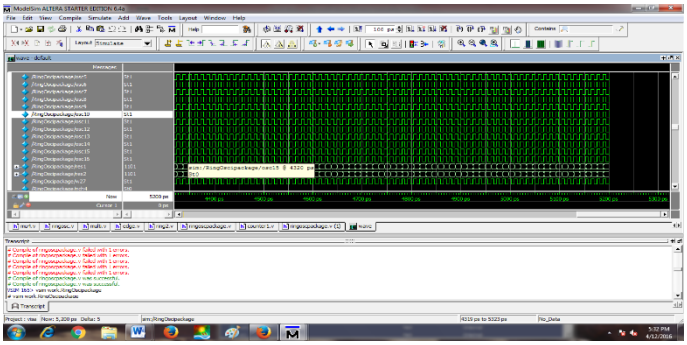

Fig.7. Output in modelsim

- First the supply voltage was fixed, and the number of inverters are increased. The number of stages of inverters are increased from n = 5, 7, 9, 11 and 13. The supply voltage for the inverters is varied with fixed number of inverters is taken as 5.
- For reliability, the number of inverters is fixed and supply voltage is varied. The supply voltage for each of the inverters is varied from 5 to 7.

The variation of bits flipping with respect to number of inverters is shown in Fig.8.

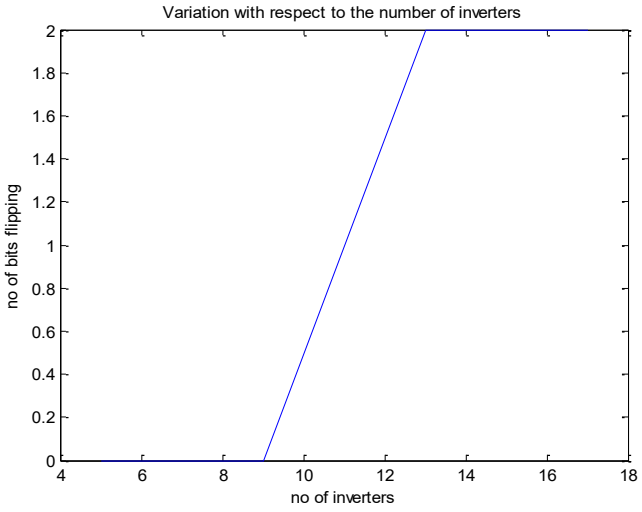

Fig.8. Number of inverters vs. Bits flipping

The variation of bits flipping with respect to supply voltage is shown in Fig.9. It indicates that due to voltage fluctuations hamming distance variations are reduced.

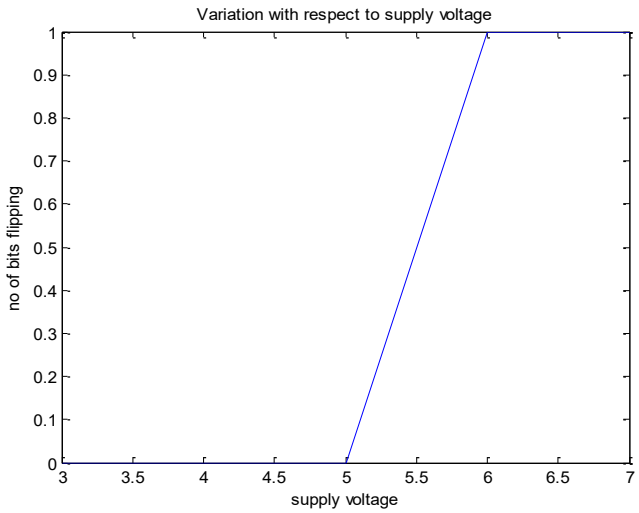

Fig.9. Supply voltage vs. number of bits flipping

The normal parameters which define the efficiency of any chip are area, time delay and power consumption. Power requirement for both typical ring oscillators and hybrid ring oscillator was same, but the time delay is increased for the proposed design. The results are tabulated in Table.1. For power analysis the device is taken fixed as XC7k70tl-2Lfbg676. The results show that the time delay additionally included due to control lines are acceptable.

Table.1. Power analysis

Type	Time delay	Power consumption
Typical RO[1]	1.004ns	1.691mW
Hybrid PUF	1.323ns	1.691mW

The synthesis report has been (The target devices have been set as Spartran, Virtex, Artix, Zynq, Kintex boards) analyzed in various devices in terms of frequency, input arrival time, output required time and path delay. The frequency analysis is given in Table.2. From the synthesis report given in Table.2, it is observed that the signal propagation time through individual device is varied. Hence finally the output propagation and ID generation will be totally different for every chip.

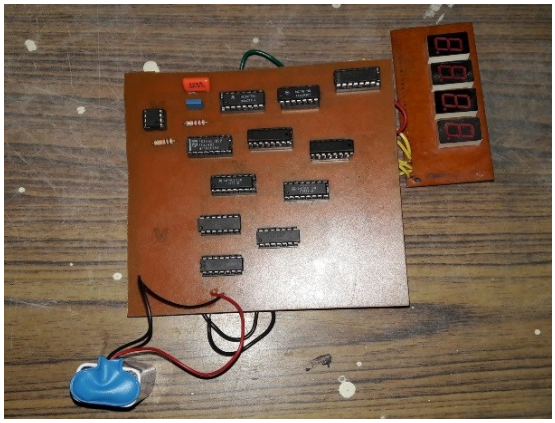

Fig.10. PCB board implementation

5. CONCLUSION AND FUTURE WORK

In the field of cryptography the hardware module PUF structure introduces a new era. Works on PUF structures are happening from the last decade, the proposed hybrid PUF structure increases the reliability and uniqueness. This takes advantage of creating MUX structure for selecting challenge lines. There are some limitations on PUF performance due to temperature variations, aging and variation of electron density in different environment conditions which induces the PUF research orientations towards that. The random number generated with this PUF structure can be utilized to implement any of the private or public key cryptosystem by designing the protocols as per the requirements.

Table.2. Timing analysis

Device Name	Frequency (MHZ)	Input arrival time (ns)	Output required Time (ns)	Path Delay (ns)
XC4vfx12-12sf363	903.261	1.888	3.810	5.385
XC7k70T-fbg676	1159.420	0.566	0.530	1.025
XC7k70tl-2Lfbg676	870.890	0.803	0.719	1.323
Xc7a100t-2Lcsg324	808.244	0.776	0.760	1.392
Xc7z010-3clg400	1159.420	0.566	0.530	1.025
Xc5vlx85-2-ff1153	839.794	1.480	2.844	4.146
Xc6vcx75t-1ff784	771.010	0.882	0.804	1.488
Xc7vx330t-1ffg1157	843.882	0.770	0.708	1.442
Xc6slx4-3tqg144	488.317	2.454	3.732	6.246
Xc6slx4l-1Ltqg144	314.451	3.438	5.238	8.887
Xc3s100e-5vq100	436.862	2.544	4.221	6.874
Xqr4vsx55-10cf1140	674.354	2.472	4.7	3.772
Xq7a100t-2Ics324	845.130	0.728	0.723	1.362

REFERENCES

[1] G.E. Suh, C.W. O'Donnell, Ishan Sachdev and Srinivas Devadas, "Design and Implementation of the AEGIS Single-Chip Secure Processor using Physical Random Functions", *Proceedings of 32nd International Symposium on Computer Architecture*, pp. 25-36, 2005.

[2] Iluminada Baturone, Miguel A. Prada-Delgado and Susana Eiroa, "Improved Generation of Identifiers, Secret Keys, and Random Numbers From SRAM", *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 12, pp. 2653-2668, 2015.

[3] M.D. Yu and S. Devadas, "Secure and Robust Error Correction for Physical Unclonable Function", *IEEE Design and Test of Computers*, Vol. 27, No. 1, pp. 48-65, 2010.

[4] Takanori Machida, Dai Yamamoto, Mitsugu Iwamoto and Kazuo Sakiyama, "A New Arbiter PUF for Enhancing Unpredictability on FPGA", *The Scientific World Journal*, Vol. 2015, pp. 1-13, 2015.

[5] S. Dolev, L. Krzywiecki, N. Panwar and M. Segal, "Optical PUF for Non Forwardable Vehicle Authentication",

Proceedings of IEEE 14th International Symposium on Network Computing and Applications, pp. 204-207, 2015.

[6] Qinglong Zhang, Zongbin Liu, Cunqing Ma, Changting Li and Jiwu Jing, "FROPUF: How to Extract More Entropy from Two Ring Oscillators in FPGA-based PUFs", *Proceedings of International Conference on Security and Privacy in Communication Systems*, pp. 675-693, 2016.

[7] J. Zhang, Y. Lin, Y. Lyu and G. Qu, "A PUF-FSM Binding Scheme for FPGA IP Protection and Pay-Per-Device Licensing", *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 6, pp. 1137-1150, 2015.

[8] Roel Maes, "Physically Unclonable Functions: Concept and Constructions", *Physically Unclonable Functions*, pp. 11-48, 2013.

[9] G. Edward Suh and Srinivas Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation", *Proceedings of ACM/IEEE 44th Annual Design Automation Conference*, pp. 9-14, 2007.

[10] A. Maiti and P. Schaumont, "Improving the Quality of a Physical Unclonable Function using Configurable Ring Oscillators", *Proceedings of* IEEE *International Conference on Field Programmable Logic and Applications,* pp. 703-707, 2009.

[11] X. Xin, J.P. Kaps and K. Gaj, "A Configurable Ring-Oscillator-Based PUF for Xilinx FPGAs", *Proceedings of Euromicro Conference on Digital System Design*, pp. 651-657, 2011.

[12] M. Cortez, A. Dargar, S. Hamdioui and G.J. Schrijen, "Modeling SRAM Start-Up Behavior for Physical Unclonable Functions", *Proceedings of IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems*, pp. 1-6, 2012.

[13] S.S. Kumar, J. Guajardo, R. Maes, G.J. Schrijen and P. Tuyls, "The Butterfly PUF Protecting IP on Every FPGA", *Proceedings of IEEE International Workshop on Hardware-Oriented Security and Trust*, pp. 67-70, 2008.

[14] Dai Yamamoto, Masahiko Takenaka, Kazuo Sakiyama and Naoya Torii, "Security Evaluation of Bistable Ring PUFs on FPGAs using Differential and Linear Analysis", *Proceedings of Federated Conference on Computer Science and Information Systems*, pp. 911-918, 2014.

[15] G.S. Rose, N. McDonald, L.K. Yan, B. Wysocki and K. Xu, "Foundations of Memristor based PUF Architectures", *Proceedings of IEEE/ACM International Symposium on Nanoscale Architectures*, pp. 52-57, 2013.

[16] P Tuyls, GJ Schrijen, B Skoric and J Van Geloven, "Read-Proof Hardware from Protective Coatings", *Proceedings of 8th International Conference on Cryptographic Hardware and Embedded Systems*, pp. 369-383, 2006.

[17] Xiaolin Xu, Ulrich Ruhrmair, Daniel E. Holcomb and Wayne Burleson, "Security Evaluation and Enhancement of Bistable Ring PUFs", *Proceedings of International Workshop on Radio Frequency Identification: Security and Privacy Issues*, pp. 3-16, 2015.