# Proof Carrying Approximate Circuits using Physical Unclonable Function

**[1]Divya. K, [2]Marichamy.P**

[1]PG Student, [2]Professor & Dean,
Department of ECE,
PSR Engineering College, India

***Abstract*: The Physical Unclonable Function which is used to protect the components from the unauthenticated users. The main objective is to avoid the piracies made by the third party access. For this purpose the PUFs are used as a security protection block which generates the license key to unlock the circuit. By using PUF in the approximate circuits the area and time consumption is reduced. The Security level has been enhanced in the approximate circuits with the use of PUF.**

***Index Terms*: Approximate Circuits, PUF, License Key, look up tables, XOR logic.**

## I. INTRODUCTION

Very Large Scale Integration is that the way toward making a microcircuit by joining many MOS transistors onto one chip. Hardware Security is weakness assurance that comes quite close to actual device rather than programming that is introduced on the equipment of a framework. In VLSI frameworks, equipment IP piracy is the major issue. Security has become a significant trouble for integrated circuits (ICs) due to globalize and reevaluated seaward creation. Moreover, a maker could make additional chips by cloning during the assembling stage subsequent to getting the plan by IC reverse engineering. Cutting edge IC reverse engineering is progressed to the point that the chips could be reverse designed inside half a month. There are devoted organizations engineering of new modern chips. Along these lines, a plan is needed to frustrate the creation of illegal cloned by reverse engineering.
Hardware obfuscation is a way to deal with fore stalls IC theft and reverse engineering. Hardware obfuscation could be ordered into two kinds: Logic or functional blocking and cover. If the module isn't enacted by the originator, the chip won't work as expected. During the post-manufacture enactment measure on believed configuration house, the chips can be initiated by opening the obfuscation capacity with a secret key that might have signed into on-chip wires. Those opened chips would then be able to be offered to the open market.

### *Physical Unclonable Function*

Using Physical Unclonable Function blocks to achieve a high level security by using encryption techniques. The PUF blocks are used for the generation of random numbers that can be used to encrypt the gates used in the circuits. The physical unclonable Function is used in the Approximate Circuits and the output of a circuit is taken as a proof of a circuit. The PUF block generated the license key which is stored in the memory. The license key should be correct to unlock the circuit otherwise the circuit will kept locked until the correct license key is given [5]. A PUF is a physical item that for a given input and condition (challenge), gives physically characterized "advanced unique mar" yield (reaction) that fills in as a one of a mankind identifier, frequently for a semiconductor gadget, for example, a microchip. PUFs are frequently founded on special physical varieties which happen normally during semiconductor fabricating.

The preserve key cannot be recovered without direct admittance to the on-chip breakers, for example, with examining assaults. Hence, a assailant cannot overproduce without information on the key. Moreover, format level procedure, for example, cell disguise could be utilized as equipment muddling and faker contacts are utilized to secure against aggressors. The format of standard cells with various functionalities s made to seem indistinguishable in the cover method. Covering can make it harder to recognize disguised doors with mechanized picture devices.

### *PUF principle*

A solution for apply secure storage while providing a better level of protection than conventional techniques which involves usage design may sound just like the security. PUF depend upon tiny manufacturing variations lead to devices conflict. The thought is that at least two gadgets that are indistinguishable intentionally will even have different electrical highlights. The difference within the electrical features is unpredictable and can't be estimated through monitoring. Solid PUFs have a huge information yield space, making portrayal illogical and consequently considerably more secure. Be that as it may, simultaneously, it makes some PUF-based confusion approaches infeasible. It is ideal to have a confusion conspire that can exploit these solid PUFs to improve the security of the methodology. In this paper, PUF based Proof-Carrying Approximate Circuits is proposed. The PUF reaction is utilized to open the capacity of the chip.

The remainder of the paper is coordinated as follow: the segment 2 portraits the related work done in the previous years and the segment 3 shows the present work developed in this paper. The output and the result analysis are clearly represented in segment 4. At last the paper is concluded in segment 5 separately.

## II. RELATED WORKS

In 2007, Yours Alkabana, Et Al, proposed to overcome Hardware piracy problem they use a remote activation scheme to protect the intellectual property of the Integrated Circuit(IC) to avoid piracy. The Unclonable Random Unique Blocks (RUBs) are

allows the circuit with the high protection from the third party [2]. Srinivas Devadas, Et Al, discussed about RFID secure authentication issues like cloning of RFID tags and replay attacks by focusing on silicon PUFs consists of MUX and arbiter [4]. An RFID has a secret key for the secure authentication of challenge-response pairs with minimally – sized circuits.

Eric Love, Et Al, design and analyze to provide a new IP acquisition and delivery protocol which can help consumers to quickly validate the trustworthiness from IP vendors [8]. In 2013, the machine learning techniques are developed by pseudo random numeric solutions which are used as an additive delay model, and Silicon data CRPs, from FPGAs and ASICs. The strong PUFs examined the Arbiter PUFs, Ring Oscillator PUFs [12].

The logic obfuscation is the most popular IP protection technique. Jiliang Zhang, Et Al, designed the PUFs mechanism which can be used to unlock the function of the chip; without the PUF response is correct the function would not perform correctly, the circuit will be kept locked until the correct key unlock it [13]. In 2015, Jiliang Zhang, Et Al, aims to modify the original FSM of the Hardware Intellectual Property to produce an augmented FSM [14]. The binding scheme supports multiple hardware cores to be integrated on a single FPGA design. It will protect the design from attacks such as cloning, copying, misusing and unauthorized integration.

PUFs have timing and delay information hidden in the IC and PUF output is unique for each IC. The PUFs have exponential number of challenge response pairs. The response is unique for each IC for each challenge [15]. The trusted party authenticate IC, then randomly chosen challenges to the IC to get the unpredictable responses. On the automation of the Proof Carrying Hardware Intellectual Property framework for data protection in third-party IPs Mohammad Mahdi Bidmeshki, Et Al, developed a method of Information Flow Tracking can be used to ensure the hardware design in secure in terms of information flow policies [16].

In 2016, a two –level Finite State Machine (FSM) can be used to authenticate a chip. In self-correcting FSM the key is not public, only the authenticated users have the correct key. The proposed approach prevents counterfeiting and also it is low-cost compared to BCH codes [17]. Swagath Venkataraman, Et Al, developed the Systematic Methodology for Automatic Logic Synthesis of Approximate circuits [19]. SALSA arranges an approximate version of the circuit that follows to the pre-specified quality bounds. SALSA disconnect the synthesis from the target error metric makes the approach more genetic and simply adoptable.

## III.METHODOLOGY

IC piracy can be an enormous security threat, wherever malevolent manufactures will produce unapproved extra chips or doubtless take the information of an idea through take the information of an idea through reverse engineering endeavors. As a step, hardware obfuscation lots as a rule retain a bit of the set up by replacement it with configurable modules. Implementing the configurable module to be stuffed in with the preserved key knowledge empowers a post-assembling effort of each verify chip, nevertheless with a demand to specific the threat of a free regular key. To guarantee that each chip includes a rare key, Physically Unclonable Functions (PUFs) area unit projected to be incorporated with hardware obfuscation and what is more utilized for manufacturing a allow key. To exceptionally set the key for each chip the fashioner needs to fully describe the PUFs for all the chips.

In this paper, we have a tendency to contend that an out of this world aggressor inside things of a producer will fully portray all the frail PUFs, and utilize any free key to interrupt the obfuscation system. This work proposes study PUF-based hardware obfuscation conspire by making a allow key to adequately forestall IC piracy even on account of a free key from some motivated chip. Within the projected conspire, the one of a kind per chip includes of 2 sections; Key1, the substances of the selections items, and Key2, the substance of the LUT. PUFs are projected for other forms of applications together with coding, for detection malicious alterations of style elements and for activating vender specific options on chips, every of the applications contain a singular set of necessities concerning the protection properties of the PUF.

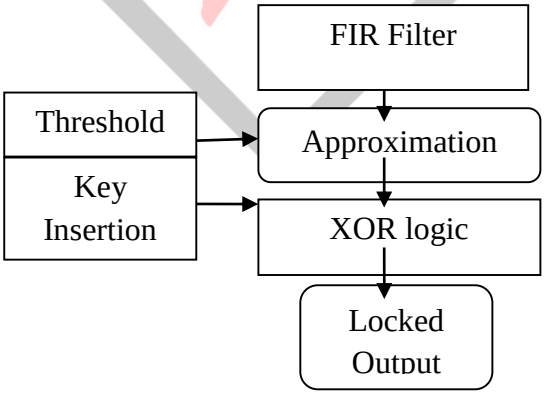


**Fig. 1: Block diagram of PUF based Proof Carrying Approximate Circuits**

### A) Encryption

PUFs produces secret keys for coding that attempt to 'machine learn' individual path delays for a chip as the simplest way of predicting the entire response of the PUF. This may be true for coding as a result of the responses to challenges area unit generally not 'readable' from an interface on the chip. All in all, the lot of access a given application offers to the PUF remotely the lot of versatility it should have to ill-disposed assault components.

**B) Authentication**

Authentication could also be enforced by having the PUF generate a secret key for encrypting communication between the designer and booster. The helper knowledge is later transmitted to the token as needed for authentication within the field to alter precise regeneration of the key. PUFs are projected for various types of uses together with coding, for distinctive malicious changes of set up components and for enacting merchandiser express highlights on chips.

For PUF architectures throughout that machine learning is effective, the projected protocols incorporate obfuscation mechanisms to stop direct management of the PUF and observation of its responses. The second attack mechanism is same except than the individual carries out a 'man-in-middle' attack. In the proposed scheme, the distinctive key per chip consists of 2 parts: Key 1, the content of the choice bits, and Key 2, the content of the LUT taken into account the worst case that the aggressor has achieved a replica of the complete key, Key 1, Key 2, for a specific chip. Obviously, this key cannot be used on to activate alternative chips. So as to recover the master key, the aggressor needs to examine the CRP space of the set of the PUF that's employed by the designer for the leaker chip.

***PUF characterization of chips***

When getting a leaked Key 1, Key 2 from some chip, the aggressor would be able to establish the set of the PUF that's employed by the designer for that chip (from analyzing Key1). However, as all the characterization channels of the PUFs are removed at the top of the activation method, characterizing the PUF isn't any longer accessible.

At the producing stage, the characterization channel area unit accessible to the aggressor. However, since the chips don't seem to be activated nevertheless, the aggressor cannot have the "leaker key" to assist indicates that set out of the PUF are used. The huge CRP space of the strong PUFs ensures that it's prohibitive expensive to thoroughly examine all the CRPs even for one PUF.

***SAT- based attacks***

While not a right away thanks to acquire the CRP space of the PUFs, the aggressor will model the complete security block (Obfuscator, PUF and therefore the LUT) with a virtual LUT, and so attempt to notice the content of such LUT by applying carefully designed primary inputs to an operating chip and analyzing the values of the first outputs. The key plan to overcome such SAT primarily based attacks is to carefully choose the withheld perform at the planning stage, so the outputs of the LUTs become powerfully correlate. The proposed scheme in this work can work many SAT-based prevention schemes to achieve a stronger framework. Furthermore, the designer can increase the number of a q dummy fan-outs fed to the obfuscator, so as to increase the code of SAT-based attacks by enlarging the size.

An attacker with no data relating the key of the OCs cannot reason the correct license to unlock the pirated/overproduced chips. Hence, the designer is that the only one who will issue the license to activate the chip. Once the chip is high-powered on, the PUF response can XOR with the license to come up with the right key bits for OCs, then the generated key bits are keep within the flip-flops to unlock the chip.

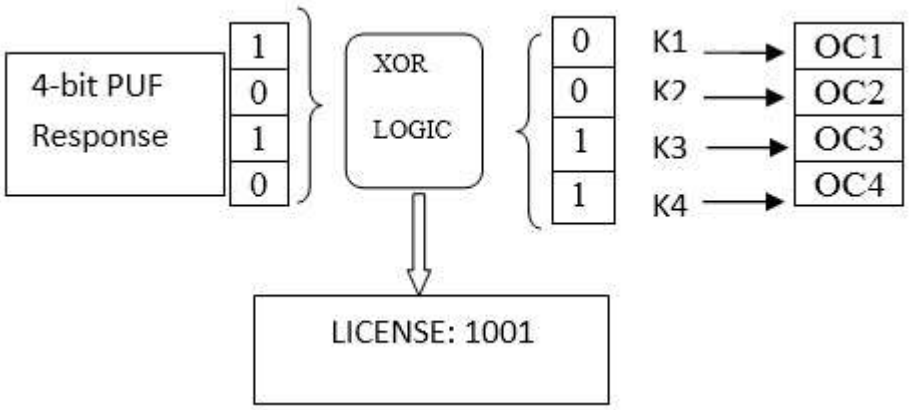


**Fig.2: PUF based obfuscation and the generation of the licenses**

The designer usually computes the error correcting code (ECC) to regulate for any bit flips to the PUF output (response) because the PUF output is tough to maintain completely stable due to the noise or different sources of physical uncertainty. The Error Correcting Code has been enforced for the minimum overhead of the input response. Likely the 4-bit input is given to the XOR logic block so that these key bits are indulged with the 4-bit encryption. ECC are promptly accessible in modern writings summed up. The mistake amended PUF reaction is utilized to open the capacity of the chip; while not the correct PUF reaction, the capacity would not perform accurately. Hence, the circuit is unbroken locked till the correct key opens it. It got to be detected that gave licenses will likewise be public and distinctive PUF reactions can be utilized to figure numerous licenses.

To illustrate the key plan of approach, we have a example for generating the license in figure 2. Taking four OCs as OC1-OC4 and K1-K4 are the key bits of the OCs. Assume K1-K4=0011, the OC can be used to replace any inverters or insert any wires. Assume that the PUF output value is 1010. To probably active the chip, the 4-bit PUF output 1010 should be XOR'd with a 4-bit license that is able to generate the results of 0011 (in this case, the license should be 1001), The chip may be properly unlocked with the

calculated license and the PUF response. The non-volatile on-chip memories would be used to store the PUF challenges, the license, and therefore relevant ECC bits on every pertinent activated IC.

## IV.RESULTS AND DISCUSSIONS

The proposed circuit is simulated and synthesized by using Modelsim and Xilinx 12.1 respectively. The simulation results of layout and the waveforms are shown in the figure 3 and figure 4.The table 1 shows the result of existing and proposed area consumption. The figure 5 and 6 are synthesis report of existing and proposed system.

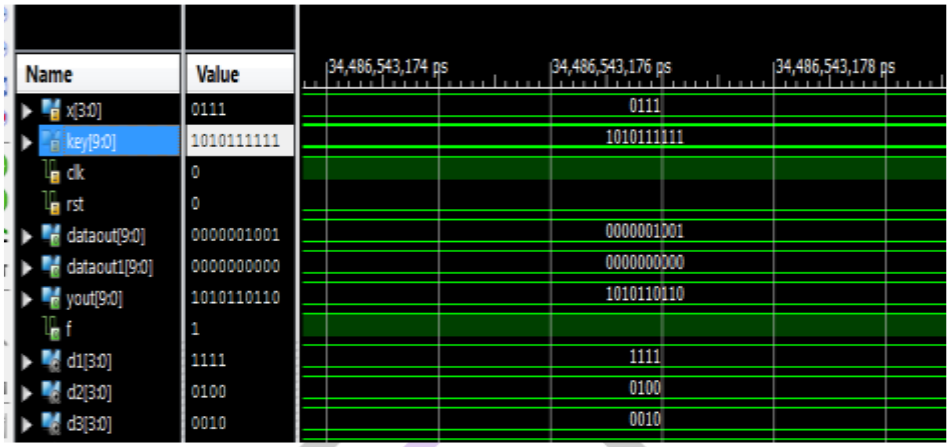


Fig.3: Simulation output with PUF

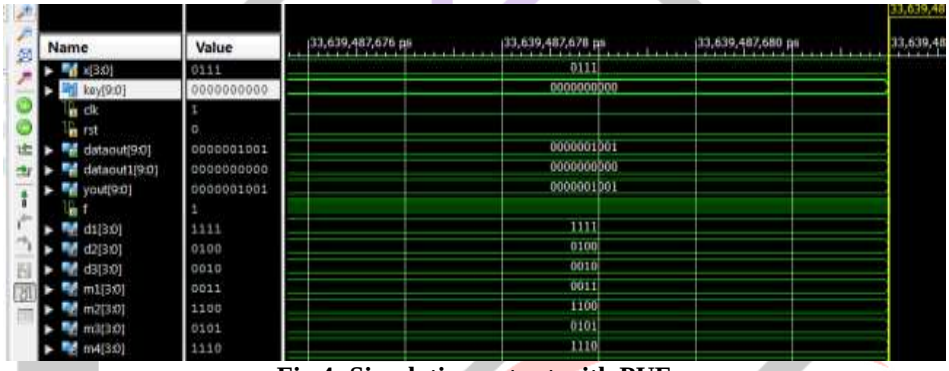


**Fig.4: Simulation output with PUF**

The figure 3 represents the simulation result of the proof carrying approximate circuit which does not use the Physical Unclonable function. In the result outputs data out and yout are different. It will show that the design key is given incorrectly. The figure 4 represents the simulation result of the proof carrying circuit uses the Physical Unclonable Function. This figure will show that the data out and are same. Hence the correct key is used which is a PUF.

| Device Utilization Summary (estimated values) | | |
|---|---|---|
| **Logic Utilization** | **Used** | **Available** |
| Number of Slices | 19 | 960 |
| Number of Slice Flip Flops | 16 | 1920 |
| Number of 4 input LUTs | 31 | 1920 |
| Number of bonded IOBs | 27 | 66 |
| Number of GCLKs | 1 | 24 |

```
Minimum input arrival time before clock: 2.780ns
Maximum output required time after clock: 11.398ns
Maximum combinational path delay: 12.072ns
```

**Fig. 5: Synthesis Report for the design without using the PUF**

Figure 5 represents the synthesis result of proof Carrying circuit with less number of slices used and time constraints for producing the output. This design summary shows that the design which does not uses the PUF will produce benefits when compared to the PUF based design.

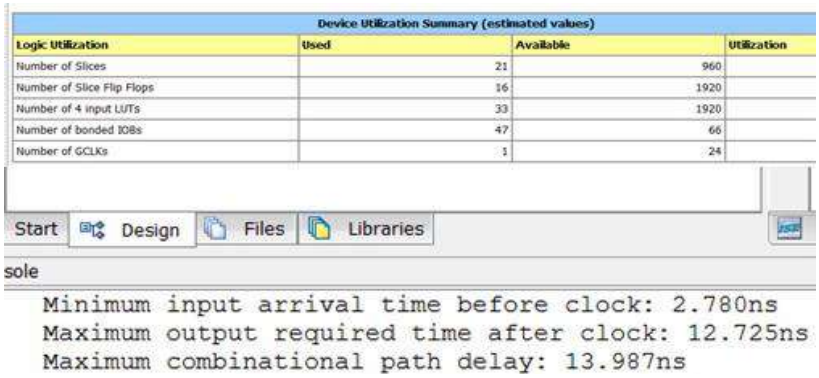


**Fig.6: Synthesis report for the design using PUF**

Figure 6, shows the synthesis result of the Physical Unclonable Function based Proof Carrying circuit with more slices and time constraints for producing the output. This report shows that the design uses the PUFs having more advantages than the previous design.

**Table.1: Comparison Table**

| Parameter | Proof Carrying Approximate Circuits without PUF | PUF based Proof Carrying Approximate Circuits with PUF |
|---|---|---|
| Slices | 19 | 21 |
| LUT | 31 | 33 |
| IOB | 27 | 47 |
| time(ns) | 12.07 | 13.98 |

The comparison table 1 represents the slices used, look up tables and time consumed for the two types of design. Time taken for the PUF based circuit is increased because the security level has been enhanced when compared to the proof carrying which does not uses the PUF.

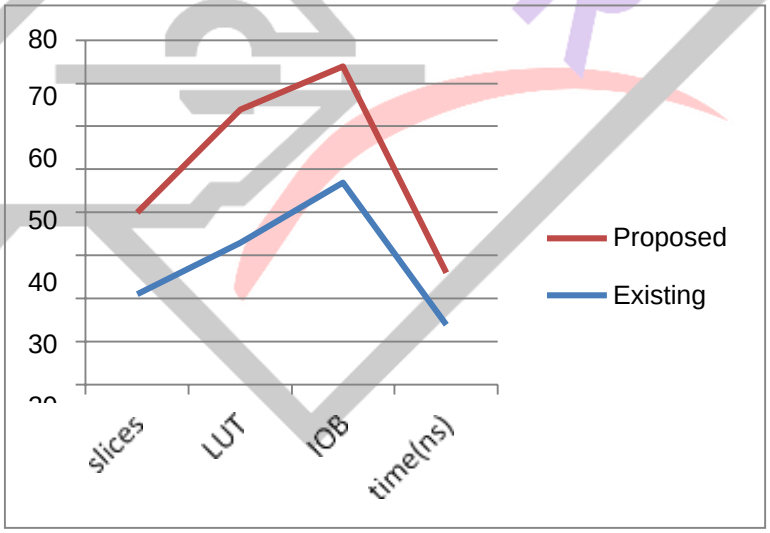


**Fig.7: Performance chart**

Figure 7 represents the performance chart for circuits with and without Physical Unclonable Function. The performance has been enhanced when using the Physical Unclonable Function in the Proof Carrying Approximate Circuits.

## V. CONCLUSION

This project focused on the security enhanced method to avoid the hardware piracy by using the Physical Unclonable Function. The PUF produces the encrypted key to access the hardware components used in the circuit, it will helps to avoid the reverse engineering, brute force attacks made by the unauthenticated users. The benchmark circuit was designed to verify the approximate circuits using the PUF. And then the synthesis report shows the improvements made by the use of PUF. The design of the Physical Unclonable Function in the approximate circuits was simulated and the output was verified.

**REFERENCES**

[1] J.W.Lee, D. Lim, B. Gassend, G. E. Suh, M. VanDijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in Proc. IEEE VLSI Circuits Symp., 2004, pp.176-179.

[2] Yousra Alkabani, Farinaz Koushanfar, and Miodrag Potkonjak, "Remote Activation of ICs for Piracy Prevention and Digital Rights management", IEEE 2007.

[3] E. Castillo, et al, "IPP@HDL: Efficient Intellectual Property Protection Scheme for IP cores", IEEE TVLSI, vol.15, no.5, pp.578-590, May 2007.

[4] Srinivas Devadas, Edward Suh, Sid Paral, Richar, Tom Ziola and Vivek Khandelwal, "Design and Implementation of PUF based "Unclonable" RFID ICs for Anti-Counter facing and Security Applications", IEEE 2008.

[5] Y. Alkabani and F. Koushanfar, "Active control and digital rights management of integrated circuits IP cores", in proc. Int. Conf. Compil., Archit., Synth. Embedded Syst, 2008, pp.227-234.

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

[7] U. Rührmair, H. Busch, and S. Katzenbeisser, "Strong PUFs: Models, constructions and security proofs," in Towards Hardware Intrinsic Security: Foundation and Practice, A.-R. Sadeghi and P. Tuyls, Eds. New York, NY, USA: Springer, 2010.

[8] Eric Love, Yier Sin and Yiogos Makris,"Proof carrying Hardware Intellectual Property: A Pathway to Trusted Module Acquisition", IEEE Transactions on Information Forensics and Security, Vol.7, No.1, February 2012.

[9] S. Venkataramani, A. Sabne, V. Kozhikkottu, K. Roy, and A. Raghunathan, "SALSA: Systematic logic synthesis of approximate circuits," in Proc. 49th Annu. Design Autom. Conf. (DAC), 2012, pp. 796–801.

[10] F. Koushanfar, "Provably secure active IC metering techniques for piracy avoidance and digital rights management," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 51–63, Feb. 2012.

[11] R. Maes, D. Schellekens, and I. Verbauwhede, "A pay- per-use licensing scheme for hardware IP cores in recent SRAM-based FPGAs," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 98–108, Feb. 2012.

[12] Ulrich Ruhrmair, Jan Solter, Frank Sehnke, Xiaolin Xu, Ahmed Mahmoud, Vera Stoyanova, Gidden Dror, Jurgen Schmidhuber, Wayne Burleson and Srinivasan Devadas, "PUF Modeling Attacks on Simulated and Silicon Data", IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, November 2013.

[13] Jiliang Zhang, "A Practical Logic Obfuscation Technique for Hardware Security", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2015.

[14] Jiliang Zhang, Yaping Lin, Yongqiang Lyu and Gang Qu, "A PUF-FSM Binding Scheme for FPGA IP Protection and Pay-Per-Device Licensing", IEEE Transactions on Information Forensics and Security, Vol. No.6, June 2015.

[15] Kavita Chandrakant Mugali, Minakshee M. Patil, "Device Authentication by Physical Unclonable Functions", International Conference on Computing Communication Control and Automation, 2015.

[16] Mohammad-Mahdi Bidmeshki, Xiaolang Guo, Raj Gautam Dutta, Yier Jin, Yiorgos Markis," Data Secrecy Protection through Information Flow Tracking in Proof- Carrying Hardware IP", IEEE Transactions on Information Forensics and Security, 2016.

[17] Yingjie Lao, Bo Yuan, Chris H. Kim and Keshab K.Parhi "Reliable PUF -based Local Authentication with Self-Correction", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2016.

[18] Z. Vasicek, "Relaxed equivalence checking: A new challenge in logic synthesis," in Proc. IEEE 20th Int. Symp. Design Diag. Electron. Circuits Syst. (DDECS), Apr. 2017, pp. 1–6.

[19] Swagath Venkataramani, Vivek Kozhikkottu, Amit Sabne, Kaushik Roy and Anand Raghunathan, "Logic Synthesis of Approximate Circuits ", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2019.

[20] Linus Witschen, Tobias Wiersema and Macro Platzner, "Proof Carrying Approximate Circuits", IEEE Transactions on Very Large Scale Integration (VLSI) systems, 2020.