CSIT (June 2020) 8(2):185–191
https://doi.org/10.1007/s40012-020-00293-5

S.I. : VISVESVARAYA

# PUF: a new era in IoT security

**Bibhash Sen**[1]

Received: 27 May 2019 / Accepted: 26 May 2020 / Published online: 17 June 2020


**Abstract** Physically unclonable function (PUF) is one of the most advocated security primitives which extracts the uncontrollable intrinsic physical property of the fabrication process to generate secret bits for authentication, random number generation and key generation. Ring oscillator (RO) PUF is the widely adopted PUF design to implement in FPGA platform, but it is highly error prone to environmental noise (i.e. temperature and voltage). The configurable RO (CRO) PUF is advocated to resolve this issue without increasing the area overhead. This paper proposes an enhanced CRO framework which uses latch instead of inverter to build an RO. The use of dedicated latch (i.e. available in an FPGA) in place of inverter eliminates the restriction to use odd number of delay units (inverters) in an RO configuration. The proposed design efficiently utilizes the resources found in a configurable logic block to increase the number of RO configurations while using the same area. Also, it provides the flexibility to include a latch in an RO configuration which in turns improve the reliability and the security as well. Experimental results on Xilinx Spartan 3E FPGA establish that the proposed design exhibits high stability despite varying environmental conditions without using any error correcting code or post-processing technique.

**Keywords** Physically unclonable function · Internet of things (IoT) · Ring oscillator · Hardware security · Reliability

## 1 Introduction

The Internet of Things (IoT) has been foreseen to be the core technology, which would make smart cities and smart homes feasible in the future. Virtually any device that is connected to other devices and accessible to end users presents a danger. The personally identifiable information (PII) which is often used for secure authentication mechanisms can be compromised to create attacks that can have various implications, starting from simple annoyance to catastrophic consequences. The leakage of PII is also of further relevance as they leak physical locations and movements, rather than virtual identifiers. These may be utilised for grievous intelligent terrorism and criminal activities. The risks stem from aspects such as insecure wireless communications, broadcasting user identification information, incapability of supporting strong encryptions, and use of the custom authentication process. Also, the semiconductor industry has been able to weather the fallout from the global financial crisis and realize several years of healthy, growthin part because of the widespread adoption of smartphones and tablets. It also created demand for the networking (mobile and wireless applications) of physical objects (internet of things, IoT) through the use of embedded sensors, actuators, and other devices that can collect or transmit information about the objects. According to a McKinsey study, security and privacy are considered as the critical challenges to IoT growth in the future. A key focus area is the security of IoT devices that are accessible by end users. Software security, alone, has

Area of research work: Hardware Security, Physical Unclonable Function (PUF) for Field Programmable Gate Arrays (FPGA), Hardware Trojan, Assistive Technology.

✉ Bibhash Sen
bibhash.sen@cse.nitdgp.ac.in

[1] Computer Science and Engineering Department, National Institute of Technology Durgapur, Durgapur, India

proven inadequate to protect against known threats, but now today's FPGA SoCs can be used to implement a scalable security scheme that extends all the way down to the IC level.

Hardware security can play very critical role in this direction. The physically unclonable functions (PUFs) are extremely promising primitives for hardware security, in the sense that they are by definition random, physically unclonable, and hence infeasible to be computed by adversaries who do not have possession of the PUF hardware. PUFs have been explored in context to the application for authentication in smart grids, which are a primary application of IoT. The use of PUFs for providing other hardware fingerprints which can be used for lightweight authentication. In addition to the threats above, any user-accessible device is also vulnerable to intellectual property (IP) theft and reverse-engineering of the product. When an end-user hacks a networked device without sufficient hardware security, IP theft of the design can occur. Protecting IP is one example of design safety. Design security also includes the ability to prevent someone from reverse engineering a product. Without hardware-based security, a user-accessible product can have its IP stolen. The configuration bitstreams should be encrypted and protected in a secure design. Devices that have tamper protection, zeroization, and safe key storage can significantly reduce the chances of a successful attack. The hardware should be able to identify unauthorized access when tampering is detected. On the other hand, a root of trust is the starting point for hardware security. A root of confidence is a hardware device. It should have all the features of design security that were previously mentioned. With an established hardware root of trust, then higher-level security functions can be used safely. Also, Valuable data need protection both in storage and in transit. One must ensure they have a secured design and a root of trust so that secure data communication can be established.

## 2 State-of-the-art

Concerned by the security threats to hardware and embedded systems, the integrated circuit community is turning to building a secure Internet of Things products and applications which will play a major role in the development of the IoT market and emerging nanotechnologies for continued device improvements. In 1999, Intel, Microsoft, IBM, Hewlett-Packard, and several other companies formed the Trusted Computing Group Platform or TCG to work on creating a new computing platform for the next century that provides for improved trust in the PC platform. The TCG published the Trusted Platform Module (TPM) specification, currently in version 1.2, and a similar protection profile (PP) for the Common Criteria (CC), which represents efforts to develop formal criteria for evaluating its security.

Nowadays, the majority of IoT devices use WiFi technology for connectivity. WiFi is more vulnerable to attacks than wired LAN [14]. The current WiFi protocols, like WEP and WPA, are vulnerable to several threats [6]. The most secure WPA2 protocol can also be compromised in several ways [5]. WiFi is still vulnerable to several attacks like MAC spoofing, de-authentication, rogue access point, evil-twin attack etc. [5, 6, 13]. These attacks are mostly performed during the connection establishment phase. These attacks are possible mainly because of two reasons: a) incapability of current WiFi protocols to ensure security in physical layer b) use of secret password/pin [15]. Furthermore, IoT devices have to work with minimal human intervention in the possibly insecure environment, so these limitations can severely affect (i.e. invasive attack, tampering attack) the security of an IoT device. In this context, PUF can overcome these limitations with less resource and computation overhead.

On the otherhand, The basic RO PUF proposed in [16], derives a single bit response by comparing the frequency of two symmetric ring oscillators but it is susceptible to voltage or temperature variation (i.e environmental variation). Various RO PUF designs have been investigated so far to mitigate the effect of environmental variations adding extra hardware [16, 18, 19]. The configurable RO (CRO) PUF (Fig. 1) has the ability to minimize the effect of environmental variations without imposing extra hardware burden. The first CRO PUF was introduced in [10]. It uses MUXes available in the CLB to generate more configuration to improve reliability. However, only 8 RO configurations can be produced using the CRO PUF proposed in [10]. An improved CRO design is proposed in [17], which can produce 256 RO configurations. However, both the designs lack flexibility to choose a particular delay element (inverter) [10]. In [4], a highly flexible CRO design is proposed, which provides the flexibility to select a delay element. But, the flexible CRO PUF proposed in [4], put restrictions on selection of an RO configuration which reduces its configurability. All the CRO PUF designs investigated so far utilizes inverter as the major delay element. Recently, Zhang et. al. proposed a novel CRO PUF design which utilizes XOR as a delay element in place of inverter [20].

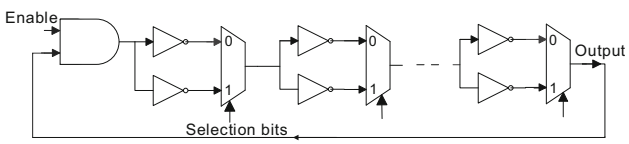


**Fig. 1** A Configurable RO

My research endeavour targets to increase reliability and configurability of CRO PUF while utilizing latch as a delay element. Finally, a PUF based protocol is proposed for secure WiFi authentication of IoT devices [8]. The augmentation of the proposed protocol with the current WiFi protocols can provide security against the aforesaid security threats [11] [12]. The protocol works during the connection establishment phase. Once the authentication is performed rest of the task relies on the underlying standard WiFi protocol.

## 3 Technical achievement & future scope

A new latch based CRO PUF framework, which efficiently utilizes hardware resources is established [7, 9]. Instead of inverter, the proposed design utilizes latch present in the CLB which results a significant improvement in CRO configurability. The proposed design deploys dedicated latch instead of the inverter, so the LUTs are free to hold other logic. This free LUTs are utilized to increase the number of configurations. Figure 2 presents the logic diagram of the proposed RO.

The proposed CRO has the flexibility to include or not to include a latch in a CRO configuration, which in turns also improve the reliability. Moreover, unlike the conventional CRO the proposed design does not restrict the RO configurations. In conventional CRO the number of inverters (delay elements) in a configuration must be odd, whereas, in the proposed CRO an RO configuration may contain odd as well as even number of latches. In the proposed design, latch has been considered as a delay element.

### 3.1 Experimental result and analysis

To check the quality factor, the same LCRO PUF design has been synthesized using Xilinx ISE 14.7 and implemented on 20 similar Spartan 3E starter boards. Additionally, in 5 boards measurement is taken in differential temperature and voltage environment. The Chip Scope Pro software available with Xilinx ISE is used to monitor RO frequency. The challenge (input) response (output) pairs and the frequency of RO configurations are collected by controlling the system with a finite state machine, which is implemented using the MicroBlaze MCS core. The frequency of the different configurations of an LCRO should be different otherwise this will not lead to any additional benefit. Figure 3 represents the average frequency of all the 64 configurations of Board D487943 (serial no.). A significant change in frequency has been observed when the number of latches varies. It happens because a latch introduces more delay compared to other elements in the RO. However, the average frequency varies in the range of 85–180 MHz.

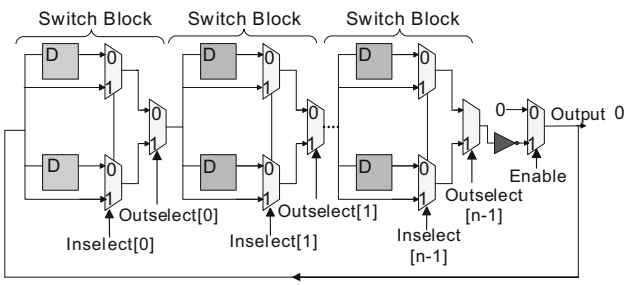


**Fig. 2** Proposed latch based CRO

Any correlation between the selected stable (i.e. reliable) RO configurations may raise security issue. Theoretically, the stable RO configurations should be equally distributed over all the RO pairs. There are 64 possible RO configurations and 99 RO pairs. So, the 64 RO configurations will be distributed over the 99 pairs. Figure 4 plots the count of selected stable RO configuration (i.e for convenience of visibility only 10 boards are shown). It can be noticed that, the selected stable RO configurations are almost random, which means observing the stable RO configurations selected in one board an adversary cannot accurately predict the stable configurations selected in other boards.

The selected stable RO configurations are used during the measurement of reliability, in any other quality measurement all the configurations are considered.

#### *3.1.1 Bit aliasing of the response bits*

Bit aliasing measures the entropy of PUF response across different PUF instances using same challenge. For *ith* challenge in *R* different devices bit aliasing is measured as

$$BitAliasing = \frac{1}{R}\sum_{j=0}^{R-1}({}^{j}r_i \times 100\%) \quad (1)$$

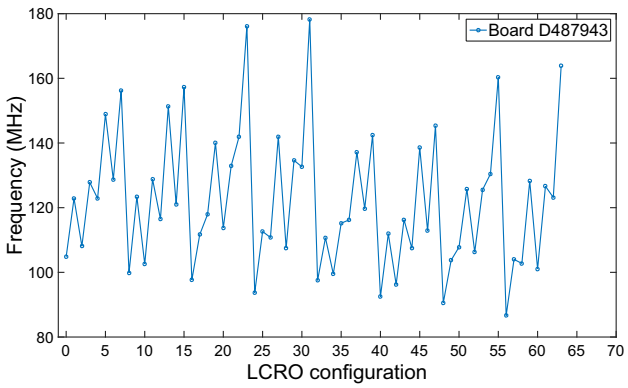


**Fig. 3** Average frequency of the 64 RO configurations of board D487943

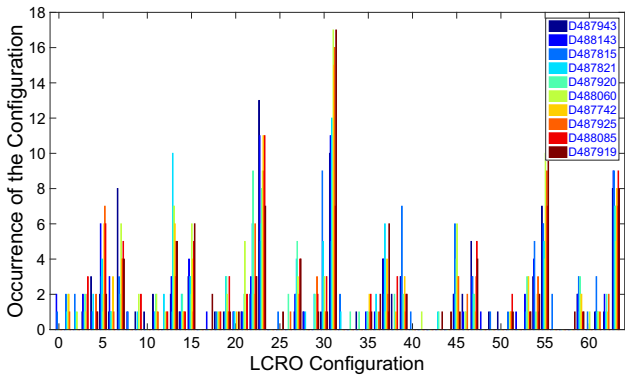


**Fig. 4** Count of selected stable RO configurations on 10 boards

where ${}^{j}r_i$ is the *ith* bit response of *jth* PUF instance. For a particular select line, ideally, bit aliasing should be 50%. Histogram of the percentage of bit aliasing is shown in Fig. 5. From the plot, it can be observed that the bit aliasing value tends to the ideal value of 50% with high probability. It signifies that the proposed design generates high-quality response with better security.

### 3.1.2 Uniformity of the response bits

Uniformity denotes the number of 1 in the PUF output. Ideally, the output should contain an equal number of 0 and 1. The uniformity is calculated as

$$Uniformity = \frac{1}{n}\sum_{i=1}^{n}({}^{p}r_i \times 100\%) \tag{2}$$

where ${}^{p}r_i$ is the *ith* response of PUF instance *p*, *n* is the number of responses. Ideally, uniformity should be 50%. The probability of the occurrences of uniformity is shown in Fig. 6. On average uniformity is 49.65%, which is very close to the ideal value of 50%.

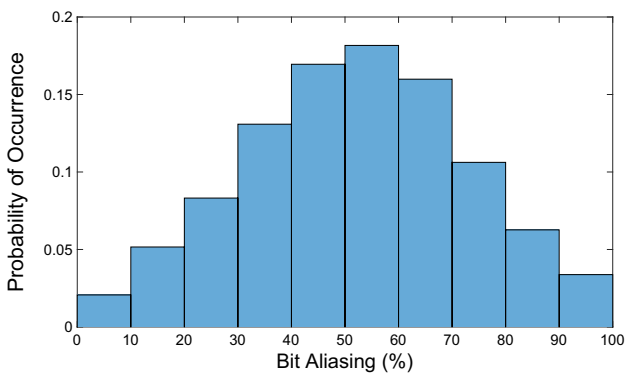


**Fig. 5** Histogram of the percentage of bit aliasing

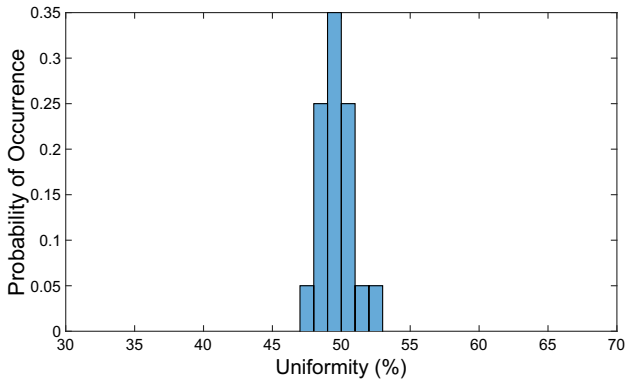


**Fig. 6** Probability of the occurrence of Uniformity(%)

### 3.1.3 Uniqueness

It is the measurement of inter die variation. It indicates the ability of PUF to differentiate two devices. The same challenge is applied to two different devices and the hamming distance between their response is calculated as uniqueness. For *M* PUF instances it is calculated as

$$Uniqueness = \frac{2}{M(M-1)}\sum_{i=1}^{M-1}\sum_{j=i+1}^{M} AHD(R_i, R_j) \times 100\% \tag{3}$$

where $AHD(R_i, R_j)$ is the average hamming distance between the response of PUF instance $R_i$ and $R_j$. Ideally, uniqueness should be 50%. On average the proposed design possesses a uniqueness of 43.40% with a standard deviation of 3.78. The minimum and maximum value of uniqueness are 33.08% and 51.70% respectively, which is sufficient to uniquely distinguish two PUF instances. The distribution of uniqueness is shown in Fig. 7.

### 3.1.4 Reliability analysis

Reliability is the most important factor to estimate PUF quality. It indicates the stability of the PUF responses

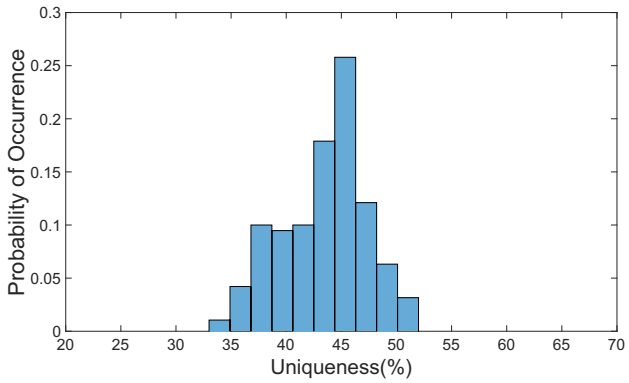


**Fig. 7** Probability of the occurrence of Uniqueness(%)

across different measurements. Ideally, a PUF instance should always produce same response to the same challenge. Reliability is quantified as

$$Reliability = \left(1 - \frac{1}{M}\sum_{i=0}^{M-1} AHD\left({}^{k}R_i, {}^{k}R_C\right)\right) \times 100\% \quad (4)$$

where ${}^{k}R_C$ is the response of *kth* PUF instance at nominal voltage and temperature. ${}^{k}R_i$ is response of *ith* measurement. $M$ is the number of measurements in different environmental conditions and *AHD* is the average Hamming distance. The ideal value of the reliability is 100%.

The reliability of the proposed design is evaluated in normal as well as extreme operating conditions. In nominal operating condition (i.e $25°C$ and $1.2V$), repeated measurement of responses does not show any bit flip which means in the normal operating condition the proposed design possesses 100% reliability. In five boards, responses are extracted in different voltage and temperature level to estimate the effect of environmental variations on reliability. The temperature and voltage (i.e core voltage) ranges are $\{25°C, 35°C, 45°C, 65°C\}$ and $\{.8V, 1.0V, 1.2V, 1.4V, 1.6V\}$ respectively.

The implemented PUF produces 100% reliable responses despite temperature variations, so the results of temperature variation are not listed. But, it has been observed that the voltage has a significant impact on RO frequency. The RO frequency increases or decreases as the core voltage increases or decreases. However, bit flip only happens, if the frequency change alters the sign of the frequency difference [16]. Number of bit flips (i.e out of 99 responses) in different voltage regions are shown in Table 1. On average the reliability of the implemented PUF against voltage variation is $(100 - 0.51) = 99.49\%$, with a maximum and minimum value of 100% and 97.98% respectively .

Hardware overhead and number of reliable response bits are the well-known trade-offs for PUF characterization. The proposed PUF design generates almost 100% reliable response despite extreme environmental noise which eliminates the need for any additional resources for error correcting code or post-processing. On average, the proposed PUF produces almost a one bit reliable response from a single CLB. Moreover, the design generates 64 RO configurations from single CLB, so the number of response bits can also be increased by using a reliability threshold [4]. The reliability comparison with the state of the art CRO PUFs is shown in Table 2. The comparison results show that the proposed design has better reliability against environmental variation compare to the other designs. The proposed design utilizes latch instead of inverter which in turn allow to use the free LUTs for improving the configurability [1, 2].

The main achievements are summarized below

- A latch based CRO (LCRO) PUF is proposed which provides the flexibility in selection of a particular delay unit with an increase in number of configurations.
- The proposed LCRO PUF eliminates the restriction in selection of RO configuration by replacing inverter with latch. The design exploits more intrinsic variations while using same area as the basic RO.
- A PUF based lightweight authentication protocol is developped towards the secure WiFi authentication of IoT devices which ensures the security using 3 pairs of challenge-response during the connection establishment.
- Finally, LCRO PUF is implemented on Xilinx Spartan 3E FPGA. The experimental results depict, the implemented PUF is able to generate highly stable response despite environmental variation without using any error correcting code or post-processing technique.

### 3.2 Future scope

The usage of a wireless physical communication, which allows attackers easier interception of communications, together with the Internet of Things (IoT) also leads to unprecedented opportunities for attackers to reveal confidential information and to manipulate data. It is crucial to find efficient and effective methods to counteract such attacks. In order to address these challenges, first, a deep security analysis of the existing technologies is needed to

**Table 1** Number of bit flips due to voltage variation (T=25°C)

| | .8V | 1.0V | 1.2V | 1.4V | 1.6V |
|---|---|---|---|---|---|
| Board D487943 | 0 | 0 | 0 | 0 | 0 |
| Board D488143 | 1 | 1 | 0 | 0 | 0 |
| Board D487815 | 0 | 0 | 0 | 0 | 0 |
| Board D487821 | 2 | 2 | 0 | 2 | 2 |
| Board D487920 | 0 | 0 | 0 | 0 | 0 |

**Table 2** Comparison of average reliability

| CRO design | Reliability | Delay unit |
|---|---|---|
| Basic CRO PUF [10] | 99.14% | Inverter |
| Improved CRO PUF [17] | 98.98% | Inverter |
| Highly flexible RO PUF [4] | NA | Inverter |
| Low cost CRO [3] | 98.41% | Inverter |
| XOR based CRO [20] | 97.72% | XOR |
| Proposed CRO PUF | 99.49% | Latch |

help discover the root causes as well as find analysis techniques that allow verifying the security of the system.

## 4 Research goals for next 4–5 years

My current research interests are divided into two broad categories, such as PUF based secure architecture for IoT applications and development of different assistive technology for differently enabled person.

As part of PUF based secure architecture research, works are being carried out on design of efficient PUF using FPGA and robust, secure system for IoT applications. Already, a flexible configurable RO-PUF based on latch logic circuit is designed. Reliability issues associated with PUF logic circuit is to explored. Also, the proposed PUF logic will be applied to implement the effective solutions for **keyless** cryptography and hardware trojan detection. Also, a proven, standardized means is to developed for securing communications between the device, the security-focused hardware element, and external entities such as mobile network servers and other systems interfacing to the IoT system.

As part of research endeavour of assistive technology for differently enabled Person, works are being carried out on on Cognitive load assessment of Visually Impaired Person. Life with any sort of physical or mental impairment is very difficult and each trivial day to day activity becomes a challenge. For example, for a visually impaired person (VIP), selecting the right shirt to wear may be a challenge. In the course of understanding and adapting skills to make use of the new assistive technology, a specially challenged person may have to bear quite an amount of mental effort or cognitive load. So, our motive or duty should be, not only to provide an assistive technology but to provide the best both in terms of suitability to the situation as well as adaptability. Hence, we should strive to develop new and helpful assistive technologies but at the same time more importantly, much have to be done to mitigate the cognitive load associated with any technology and hence increase its acceptability. Before the deployment of any technology for the specially-abled people, the level of cognitive load it imposes on the person should be well ascertained.

## 5 Publication

1. S. Banik, S. Roy and **B. Sen,**"Application-Dependent Testing of FPGA Interconnect Network," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 10, pp. 2296–2304, Oct. 2019, https://doi.org/10.1109/TVLSI.2019.2925932.
2. S. Banik, S. Roy and **B. Sen,**"An Integrated Framework for Application Independent Testing of FPGA Interconnect. J Electron Test 35, 729–740 (2019). https://doi.org/10.1007/s10836-019-05827-7.
3. M. H. Mahalat, N. Ugale, R. Shahare and **B. Sen,**"Design of Latch based Configurable Ring Oscillator PUF Targeting Secure FPGA," 2018 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC), Verona, Italy, 2018, pp. 261–266, https://doi.org/10.1109/VLSI-SoC.2018.8644737.
4. A. Mondal, M. H. Mahalat, A. R. Medapati, S. Roy and **B. Sen**, "XOR based Methodology to Detect Hardware Trojan utilizing the Transition Probability," 2018 8th International Symposium on Embedded Computing and System Design (ISED), Cochin, India, 2018, pp. 215–219, https://doi.org/10.1109/ISED.2018.8704062.
5. M. H. Mahalat, S. Saha, A. Mondal and **B. Sen,**"A PUF based Light Weight Protocol for Secure WiFi Authentication of IoT devices," 2018 8th International Symposium on Embedded Computing and System Design (ISED), Cochin, India, 2018, pp. 183-187, doi: https://doi.org/10.1109/ISED.2018.8703993.
6. S. Banik, S. Roy and **B. Sen**,"Test Configuration Generation for Different FPGA Architectures for Application Independent Testing," 2019 32nd International Conference on VLSI Design and 2019 18th International Conference on Embedded Systems (VLSID), Delhi, NCR, India, 2019, pp. 395–400, doi: https://doi.org/10.1109/VLSID.2019.00086. .

**Acknowledgements** The research grant provided by the YFR fellowship greatly helped to boost my research work. I have developed two laboratory essential for my research work, (i) Hardware security Laboratory. (ii) Assistive Technology Laboratory (Under process). Also, I have attended and presented a research paper in 26th IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC 2018), 8–10 October, Verona, Italy and Two research scholars supervised by me attended the 32nd IEEE International System-on-Chip Conference (SOCC 2019), 3–6 September, 2019, Singapore under the aegis of contingency grant of YFRF.

## References

1. Banik S, Roy S, Sen B (2019) Application-dependent testing of fpga interconnect network. IEEE Trans Very Large Scale Integr VLSI Syst 27(10):2296–2304
2. Banik S, Roy S, Sen B (2019) An integrated framework for application independent testing of FPGA interconnect. J Electron Test 35:729–740. https://doi.org/10.1007/s10836-019-05827-7
3. Cui Y, Wang C, Liu W, Yu Y, O'Neill M, Lombardi F (2016) Low-cost configurable ring oscillator PUF with improved uniqueness. In: 2016 IEEE International symposium on circuits and systems (ISCAS), pp. 558–561. https://doi.org/10.1109/ISCAS.2016.7527301

4. Gao M, Lai K, Qu G (2014) A highly flexible ring oscillator PUF. In: 2014 51st ACM/EDAC/IEEE Design automation conference (DAC), pp. 1–6. https://doi.org/10.1145/2593069.2593072
5. Huang H, Hu Y, Ja Y, Ao S (2017) A whole-process wifi security perception software system. In: 2017 International conference on circuits, system and simulation (ICCSS), pp. 151–156. https://doi.org/10.1109/CIRSYSSIM.2017.8023201
6. Kolias C, Kambourakis G, Stavrou A, Gritzalis S (2016) Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset. IEEE Commun Surv Tutorials 18(1):184–208. https://doi.org/10.1109/COMST.2015.2402161
7. Mahalat MH, Mandal S, Mondal A, Sen B (2019) An efficient implementation of arbiter PUF on FPGA for IOT application. In: 2019 32nd IEEE International system-on-chip conference (SOCC), pp. 324–329
8. Mahalat MH, Saha S, Mondal A, Sen B (2018) A PUF based light weight protocol for secure WiFi authentication of IOT devices. In: 2018 8th International symposium on embedded computing and system design (ISED), pp 183–187
9. Mahalat MH, Ugale N, Shahare R, Sen B (2018) Design of latch based configurable ring oscillator PUF targeting secure FPGA. In: 2018 IFIP/IEEE International conference on very large scale integration (VLSI-SoC), pp 261–266
10. Maiti A, Schaumont P (2011) Improved ring oscillator puf: an FPGA-friendly secure primitive. J Cryptol 24(2):375–397. https://doi.org/10.1007/s00145-010-9088-4
11. Mondal A, Mahalat MH, Mandal S, Roy S, Sen B (2019) A novel test vector generation method for hardware trojan detection. In: 2019 32nd IEEE International system-on-chip conference (SOCC), pp 80–85
12. Mondal A, Mahalat MH, Medapati AR, Roy S, Sen B (2018) XOR based methodology to detect hardware trojan utilizing the transition probability. In: 2018 8th International symposium on embedded computing and system design (ISED), pp 215–219
13. Nakhila O, Zou C (2016) User-side wi-fi evil twin attack detection using random wireless channel monitoring. In: MILCOM 2016—2016 IEEE military communications conference, pp 1243–1248
14. Sagers G, Hosack B, Rowley RJ, Twitchell D, Nagaraj R (2015) Where's the security in wifi? an argument for industry awareness. In: 2015 48th Hawaii international conference on system sciences, pp 5453–5461. https://doi.org/10.1109/HICSS.2015.641
15. Shen W, Yin B, Cao X, Cai LX, Cheng Y (2016) Secure device-to-device communications over wifi direct. IEEE Netw 30(5):4–9. https://doi.org/10.1109/MNET.2016.7579020
16. Suh GE, Devadas S (2007) Physical unclonable functions for device authentication and secret key generation. In: 2007 44th ACM/IEEE design automation conference, pp 9–14
17. Xin X, Kaps JP, Gaj K (2011) A configurable ring-oscillator-based puf for xilinx fpgas. In: 2011 14th Euromicro conference on digital system design, pp 651–657. https://doi.org/10.1109/DSD.2011.88
18. Yin CE, Qu G (2009) Temperature-aware cooperative ring oscillator PUF. In: Proceedings of the 2009 IEEE international workshop on hardware-oriented security and trust, HST '09, pp 36–42. IEEE Computer Society, Washington, DC, USA. https://doi.org/10.1109/HST.2009.5225055
19. Yu MD, Devadas S (2010) Secure and robust error correction for physical unclonable functions. IEEE Design Test Comput 27(1):48–65. https://doi.org/10.1109/MDT.2010.25
20. Zhang L, Wang C, Liu W, O'Neill M, Lombardi F (2017) Xor gate based low-cost configurable RO PUF. In: 2017 IEEE International symposium on circuits and systems (ISCAS), pp 1–4. https://doi.org/10.1109/ISCAS.2017.8050628