Reconfigurable Robust Hybrid Oscillator Arbiter PUF for IoT Security based on DL-FET

Venkata P. Yanambaka
Dept. of Computer Science and Engineering
University of North Texas, USA.
Email: vy0017@unt.edu

Saraju P. Mohanty
Dept. of Computer Science and Engineering
University of North Texas, USA.
Email: saraju.mohanty@unt.edu

Elias Kougianos
Engineering Technology
University of North Texas, USA.
Email: elias.kougianos@unt.edu

Prabha Sundaravadivel
Computer Science & Engineering
University of North Texas, USA.
Email: ps0374@unt.edu

Jawar Singh
Electronics & Comm. Engineering
PDPM IIIT Jabalpur, India.
Email: jawar@iiitdmj.ac.in

***Abstract*—The Internet of Things (IoT) is currently a main focus of research across disciplines. In a household IoT environment, almost all devices are connected to the internet. In the case of a smart city, most of the city homes and departments are managed through the network. One small security vulnerability is enough to take down an entire city or parts of it. Hence communications should be encrypted. Physical Unclonable Functions are commonly used for this purpose. A PUF key is not stored anywhere thus providing the advantage of secrecy. In the current paper, two designs of a reconfigurable PUF are proposed, a speed optimized reconfigurable hybrid oscillator arbiter PUF and its power optimized counterpart. Both designs can be introduced into two different categories of IoT devices, one where high performance is needed and one with low power consumption. The Hamming distance of the speed optimized and power optimized designs is 47% and 48% with power consumption of 167.5 μW and 143.3 μW, respectively.**

***Index Terms*—Dopingless Junctionless FET, Physical Unclonable Function, Ring Oscillator, Arbiter PUF, IoT**

I. Introduction

In the digital era, we use encryption to protect data and the decryption key is typically stored in memory. Non-volatile memory (NVM) is used for the storage but is not resistant to certain invasive physical attacks [1]. To save the NVM from those attacks, tamper-proofing mechanisms should be employed which take chip area as well as power. In the case of smaller devices, chip area and power consumption are the two parameters that cannot be compromised. The Internet of Things (IoT) was proposed to be one of the disruptive technologies of modern era [2], [3]. The IoT necessitates improved security.

The Physical Unclonable Function(PUF) was introduced to overcome the issue of attacks on devices deployed in unmonitored and insecure locations [4]. The main advantage of Physical Unclonable Function is that the key is not stored in memory. A PUF uses manufacturing variations in devices to generate the key. The key generated can be utilized for many different reasons, for encryption and decryption or IP protection [5], and so on. A PUF module is given a challenge input and a corresponding output is generated. The generated output can only be generated again in the same PUF module with the same challenge input. If the same challenge input is given to a different PUF, a different output key will be generated.

Many different architectures have been proposed for PUFs [6]. Some of the designs are Arbiter PUF [7], SRAM PUF [8], and Ring Oscillator PUF [9]. In the current paper, a Ring Oscillator is used as a base design for the PUF. The novel contributions of the paper are presented in Section II and the rest of the paper is organized as follows: Section III summarizes related prior research in this area, Sec. IV presets the designs of PUF that are being proposed, Sec. V presents the design of the configuration module, Sec. VI presents the experimental results for the designs and Sec. VII gives conclusions and future research directions.

II. Novel Contributions

In an IoT environment, many devices will be connected to the Internet simultaneously. PUF modules are introduced into each of the devices which can increase the security. Keys generated by PUF modules can be used to encrypt the device to device communication or end-to-end communication. The following are the two novel designs of PUF that are being proposed in this paper:

- Speed Optimized Reconfigurable Hybrid Oscillator Arbiter Physical Unclonable Function.
- Power Optimized Reconfigurable Hybrid Oscillator Arbiter Physical Unclonable Function.

The speed optimized design is proposed so it can be introduced in devices where the speed of operation is of importance but not the power consumption. Network switches and modems are such examples. The power optimized design is proposed where the speed of operation is traded-off for the power consumption and chip area, primarily for mobile applications.

III. Related Prior Research

Research in developing new architectures for IoT and better networks to connect many devices to help them work together has been done for a long time [1]. A new health monitoring system was proposed in [10]. Different applications of the IoT and the security measures were presented in [11]. In the paper, test cases were built by the authors and various threats were demonstrated.

For security in IoT devices, PUFs can an be easy and efficient solution [4]. Different designs of PUF were proposed using various devices. An SRAM based PUF was presented in [8]. The Arbiter PUF was explored in [7]. Various types of emerging PUF designs are presented in [4]. Two designs of PUFs were presented in [12]. The ring oscillator architecture was used in [12]. A design of PUF using the current starved architecture of RO was presented in [13].

The PUF designs proposed in the current paper were designed using the Dopingless Junctionless transistor. Dopingless transistors were proposed in [14]. A temperature analysis and aging analysis was performed on the transistors and an extensive study was presented in [15].

A comparison of FinFET based and Dopingless FET based PUF designs is presented in [16]. In the current paper, a new configuration module is introduced into the design. The configuration module is added at every inverter stage. Based on the selected challenge bit, the oscillation frequency is changed. Hence in this case, besides using the manufacturing variations of the inverters, a delay is added due to the configuration module using which the frequency of the ring oscillators is changed.

IV. DL-FET based Reconfigurable Hybrid Oscillator Arbiter PUF

A. Speed Optimized Reconfigurable Hybrid Oscillator Arbiter PUF

Fig. 1 shows the design of a Speed Optimized Reconfigurable Hybrid Oscillator Arbiter PUF. This speed optimized design is introduced into devices where the processing should be fast to allow more data to be encrypted. For example, in a household IoT environment, a number of devices are connected to the Internet at the same time. All or some of them might be accessing the network and hence the router or the network switch connecting them should have faster processing capability and be able to encrypt the data. A PUF that can generate the keys at the rate of communication is necessary. If it is not possible, the speed of the network can be bottlenecked.

The ring oscillator PUF and the arbiter PUF designs are combined to create the hybrid oscillator arbiter PUF. The speed optimized design presented in the prior work does not have the capability of generating multiple keys once the circuit is fabricated, hence it is not possible to reconfigure. The present design solves that issue by introducing a configuration module between the inverters. Each configuration module contains two challenge bits. This increases the chance of reconfigurability exponentially. Further description of the configuration module is presented in Sec. V. Introduction of this module in the design will create some delay in the oscillations. Depending on which challenge bit is selected, at each stage, the delay introduced will vary. The ring oscillators along with the configuration modules will be generating the oscillations needed. The signals from oscillators will be fed to the D flipflop. The oscillators are divided into two groups. One oscillator from each set is selected and the signals generated are fed to the D-input and clock signal of the flipflop. As there are differences in the oscillations, the signals will not be the same at both the D-input and the clock signal. Depending on the voltage at the flipflop inputs at a certain time, the output of the flipflop will vary. The outputs of all the flipflops will give the PUF key. Due to the configuration modules, the delay can be changed and the PUF output can be changed when needed.

B. Power Optimized Reconfigurable Hybrid Oscillator Arbiter PUF

Fig. 2 shows the design of the Power Optimized Reconfigurable Hybrid Oscillator Arbiter PUF. The power optimized design is used in day-to-day applications where the power consumption of the devices needs to be as low as possible. The power optimized design consumes less power compared to the speed optimized design. This can be introduced into smart-watches, mobile phones, etc. In an IoT environment, there will also be other devices like clocks, smart TVs, etc. In the case of a network switch the number of PUF modules introduced can be more than one. With this power optimized design, both less power consumption compared to the speed optimized design and the increased number of configurations can be achieved at the same time.

This design is also similar to the one presented in the previous subsection. The ring oscillator PUF and the arbiter PUF designs are combined to form the current design. Then the configuration module is introduced. The configuration module will introduce the necessary delay in the oscillations. But here, to decrease the space utilized and the power consumed, the number of D flipflops used are decreased to one and two multiplexers are used. The outputs from the two multiplexers are fed to D-input and clock signals of the flipflop. Half the multiplexers are given to MUX1 and the other half to MUX2. So each signal from the ring oscillators is selected and fed to the flipflop. Depending on the voltage level present at the clock and the input, an output bit is generated. Another set of ring oscillators is selected and fed to the flipflop to get another bit. This process is repeated to get the complete PUF key. Hence some time is traded-off for reduced power consumption of the module. But the order in which the signals are fed to the flipflop can be changed to generate a new key which is not used. Hence the reconfigurability of the PUF module is increased. The challenge bits of the configuration module also contribute to the reconfigurability of the PUF.

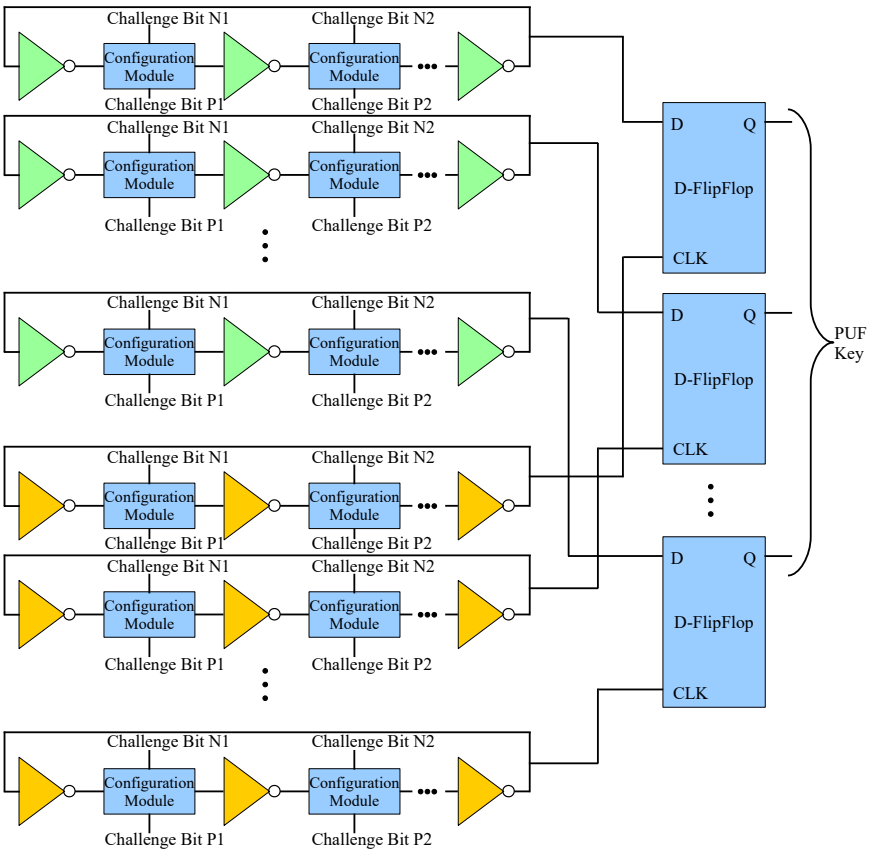

Fig. 1. Speed Optimized Reconfigurable Hybrid Oscillator Arbiter PUF.

V. Configuration Module Design

Fig. 3 shows the circuit diagram of the configuration module. The configuration module is used to provide a certain delay to the oscillations so that the oscillation frequency is not only dependent on the number of inverters used in the ring oscillator design but also in the configuration module. This helps in increasing the robustness of the entire PUF design itself. The main components of the configuration module are transistors. The transistors are introduced to increase the delay in the oscillations. There are two transistors present, n-Type DL-FET and p-Type DL-FET. Each of the transistors is selected using the four AND gates and the OR gate present in the module. The input is the oscillation coming from the inverter before it. The input is fed to both AND gates. The second input to the AND gates comes from the challenge bit input. There are two challenge bits 'C1' and 'C2'. If a challenge bit is given high, the corresponding AND gate will be fed a high input. Then the input (coming from the inverter) will be fed as an input to the corresponding transistor. Transistors T1 and T2 will be given high (1V) and low (0V) all the time at their gates. If challenge bit C1 is made high, it will be fed to both AND gates A1 and A4. A1 gets an input from the inverter and the output is fed as an input to transistor T1. Transistor T1 gives its output as an input to gate A4 which has a high input already. So the same input is forwarded to the OR gate. When C1 is high, C2 is made low. Hence no matter what the input to gates A2 and A3, the outputs of A2 and A3 will be low. Hence the signals A2 (signal from inverter prior to this configuration block) and A3 (a low signal in this case) are fed to O1. Then the output is replicated at the output but with a small delay.

VI. Simulation Results

The key generated by a PUF should be secure and not clonable by any other PUF module. To validate the authenticity of a PUF design, the following Figures of Merit are considered:

- Uniqueness
- Reliability
- Randomness

The current PUF is being introduced into the devices for which power consumption is very important. Hence power consumption is another FoM being considered in this case. On both the power optimized and speed optimized designs of PUF, a Monte Carlo analysis is performed. In the dopingless Transistors, the width of device is varied by 10%. 100 Monte Carlo runs were performed on the designs to simulate 100 different PUF modules. The characterization of two PUF designs is presented in Table I.

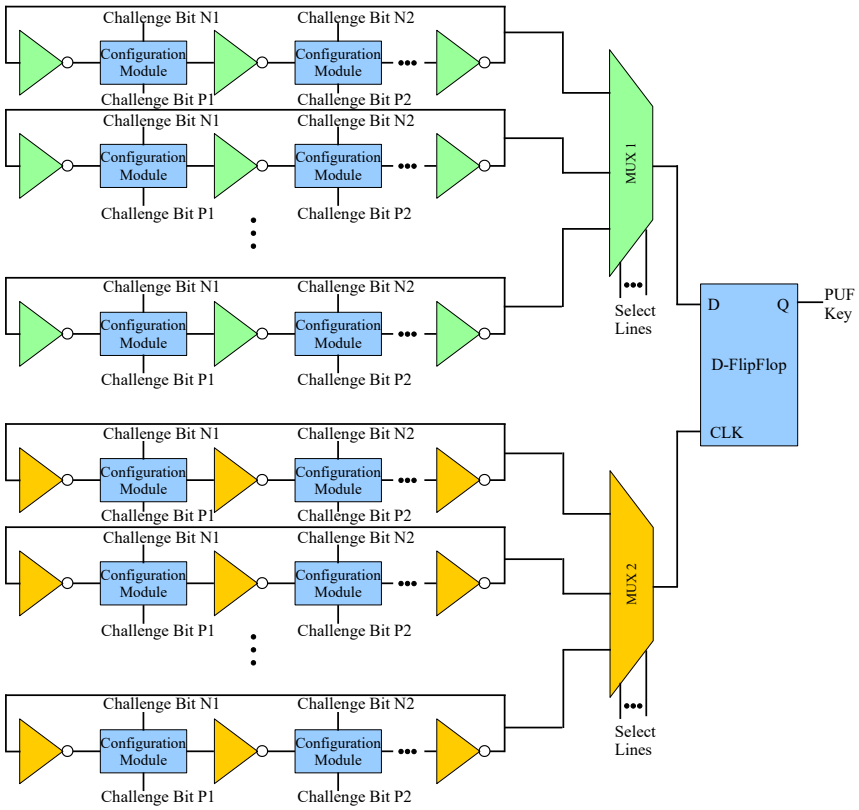

Fig. 2. Power Optimized Reconfigurable Hybrid Oscillator Arbiter PUF.

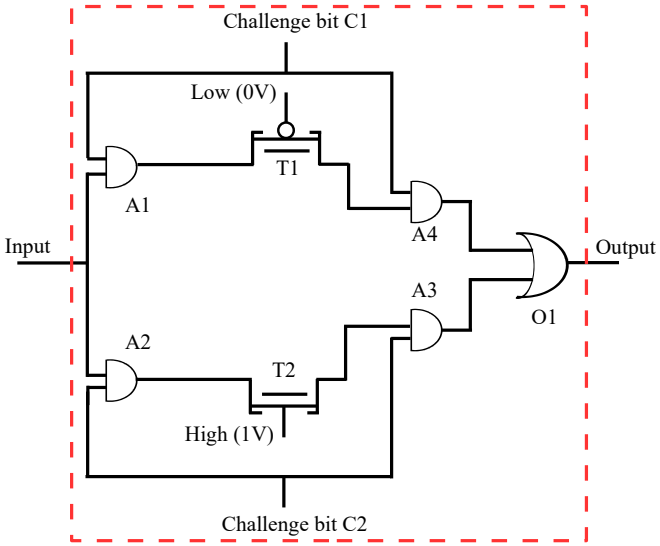

Fig. 3. Design of Configuration Module.

A. *Uniqueness*

Uniqueness of a PUF is the ability of the module to generate a unique key when a challenge response is given to the module. When two or more PUFs are given the same challenge bit, they should be capable of generating a unique different key. That is the uniqueness factor of PUF. To calculate the uniqueness, the keys are generated and the Hamming distance is calculated between the keys. The ideal Hamming distance between two keys is 50%. To test the uniqueness of the proposed design, 100 Monte Carlo runs were performed to simulate 100 different PUF modules. The Hamming distance between the keys produced by both PUFs, the speed optimized and power optimized design, were calculated. Fig. 4 and Fig. 5 show the inter-PUF Hamming distance.

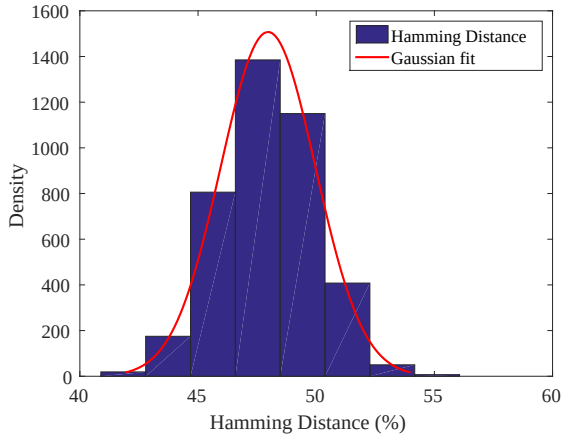

Fig. 4. Hamming distance of Speed Optimized Reconfigurable Hybrid Oscillator Arbiter PUF.

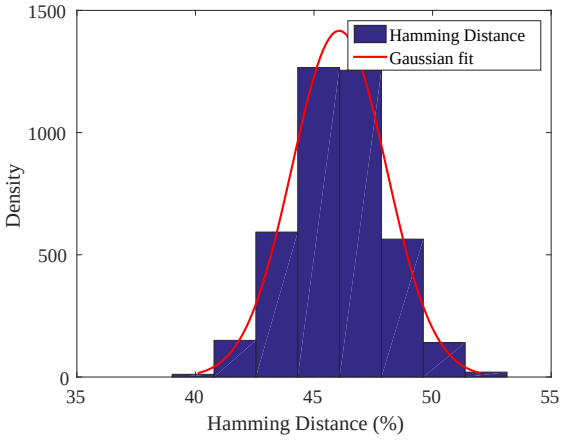

Fig. 5. Hamming distance of Power Optimized Reconfigurable Hybrid Oscillator Arbiter PUF.

B. Reliability

Reliability of a PUF is the ability of the module to generate the same key with the environmental effects and natural aging effects affecting it. There will be many different variations like power supply variations, temperature variations and so on, which will affect the working of the module. Due to these affects if the PUF key is changed, the module itself will not be reliable. The power supply and temperature were varied and 100 Monte Carlo runs were performed on the module. The ideal reliability of a PUF module is 0% as there should be no error in producing the results. But in real time this will not be the case. Fig. 6 and Fig. 7 show the intra-PUF Hamming distance.

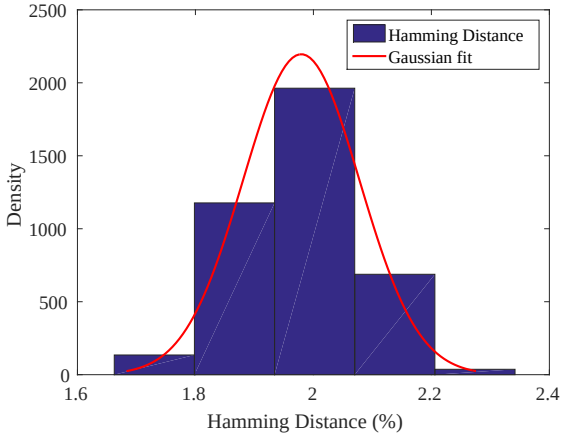

Fig. 6. Hamming distance of Speed Optimized Reconfigurable Hybrid Oscillator Arbiter PUF.

C. Randomness

When the output key is generated from a PUF module, the bits should contain an equal amount of '0'and '1' bits for the key to be more robust. This property of a PUF is called randomness. To check the randomness of PUF designs, Monte Carlo simulations were performed on both designs and

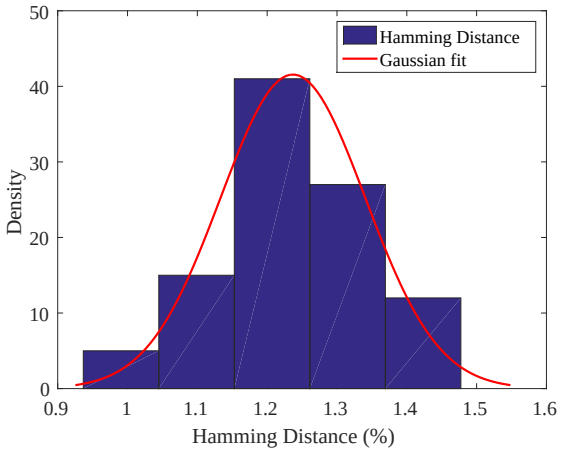

Fig. 7. Hamming distance of Power Optimized Reconfigurable Hybrid Oscillator Arbiter PUF.

keys were generated. Then the bit distribution in the keys was observed. Fig. 8 shows the randomness distribution of the keys. 50% is the ideal value in this case. The keys generated in real time will not be ideal but closer. In test results, there was a 48% mean number of zeros present in the keys generated.

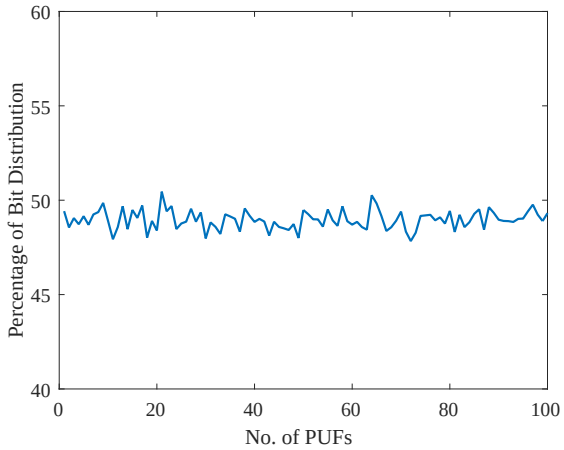

Fig. 8. Randomness of PUF.

VII. Conclusion and Future Research

Two designs of PUFs were proposed in this paper. Each of the designs can be deployed into different applications in an IoT environment. One when high processing speeds are needed and the other where the power consumption is the highest priority. The Speed Optimized Reconfigurable Hybrid Oscillator Arbiter PUF generates the output keys fast. The Power Optimized Reconfigurable Hybrid Oscillator Arbiter PUF can be deployed in applications where the power consumption of the device is a priority. The Power Optimized design consumes less power compared to the Speed Optimized Design due to the use of only one flipflop and multiplexer. In the current designs, the reconfigurability has been addressed but the power consumption can still be reduced. Future research includes

TABLE I
FIGURE OF MERITS FOR DIFFERENT PUF DESIGNS.

PUF Characteristics	Estimated Values	
PUF Design	Speed Optimized Hybrid Oscillator Arbiter PUF	Power Optimized Hybrid Oscillator Arbiter PUF
Average Power	167.5 μW	143.3 μW
Hamming Distance	48%	47%
Average Time to Generate Key	50 ns	$1 > 50$ ns

TABLE II
COMPARISON OF RESULTS WITH RELATED EXISTING RESEARCH.

Research Works	Technology	Architecture Used	Average Power Consumed	Hamming Distance (%)
Rahman et al. [17]	90 nm CMOS		–	50
Maiti et al. [9]	180 nm CMOS	Ring Oscillator	–	50.72
S. R. Sahoo et al. [18]	90 nm CMOS	Ring Oscillator	–	45.78
Maiti et al. [19]	–	–	–	47.31
Yanambaka et al. (Power Optimized) [12]	32 nm FinFET	Current Starved Oscillator	175.5 μW	50.1
Yanambaka et al. (Power Optimized) [13]	32 nm FinFET	Traditional Ring Oscillator	285.5 μW	50.9
Yanambaka et al. (Power Optimized) [16]	10 nm Dopingless FET	Hybrid Oscillator Arbiter	121.3 μW	48.0
Yanambaka et al. (Speed Optimized) [16]	10 nm Dopingless FET	Hybrid Oscillator Arbiter	151 μW	50.0
This Paper (Power Optimized)	10 nm Dopingless FET	Reconfigurable Hybrid Oscillator Arbiter	143.3 μW	47.0
This Paper (Speed Optimized)	10 nm Dopingless FET	Reconfigurable Hybrid Oscillator Arbiter	167.5 μW	48.0

exploring other architectures of PUFs. Side channel leakage resilient PUF is important for having robust PUF designs. Importantly, the deployment of PUF in real-life applications is worthy exploring as future research.

REFERENCES

[1] S. P. Mohanty, *Nanoelectronic Mixed-Signal System Design*. McGraw-Hill Education, 2015, no. 9780071825719.

[2] National Intelligence Council, "Six Technologies with Potential Impacts on US Interests out to 2025," *Disruptive Civil Technologies*, 2008.

[3] E. Kougianos, S. P. Mohanty, G. Coelho, U. Albalawi, and P. Sundaravadivel, "Design of a High-Performance System for Secure Image Communication in the Internet of Things," *IEEE Access*, vol. 4, pp. 1222–1242, 2016.

[4] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Emerging Physical Unclonable Functions With Nanotechnology," *IEEE Access*, vol. 4, pp. 61–80, 2016.

[5] J. X. Zheng and M. Potkonjak, "A Digital PUF-Based IP Protection Architecture for Network Embedded Systems," in *Proceeding of the 10th ACM/IEEE Symposium on Architectures for Networking and Communications Systems*, 2014, pp. 255–256.

[6] S. Joshi, S. P. Mohanty, and E. Kougianos, "Everything You Wanted to Know about PUFs," *IEEE Potentials Magazine*, vol. 36, July-August 2017.

[7] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs," in *Proceedings of the International Conference on Reconfigurable Computing and FPGAs*, 2010, pp. 298–303.

[8] C. Clavier and K. Gaj, *Cryptographic Hardware and Embedded Systems*, C. Clavier and K. Gaj, Eds. Springer, 2009.

[9] A. Maiti and P. Schaumont, "Improved Ring Oscillator PUF: An FPGA-friendly Secure Primitive," *Journal of Cryptography*, vol. 24, no. 2, pp. 375–397, 2010.

[10] P. Sundaravadivel, S. P. Mohanty, E. Kougianos, and U. Albalawi, "An Energy Efficient Sensor for Thyroid Monitoring Through the IoT," in *Proceedings of the 17th International Conference on Thermal, Mechanical and Multi-Physics Simulation and Experiments in Microelectronics and Microsystems (EuroSimE)*, 2016, pp. 1–4.

[11] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, "Learning Internet-of-Things Security "Hands-On"," *IEEE Security Privacy*, vol. 14, no. 1, pp. 37–46, Jan 2016.

[12] V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Secure Multi-Key Generation Using Ring Oscillator based Physical Unclonable Function," in *Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, 2016, pp. 200–205.

[13] ——, "Novel FinFET based Physical Unclonable Functions for Efficient Security in Internet of Things," in *Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, 2016, pp. 172–177.

[14] C. Sahu and J. Singh, "Potential Benefits and Sensitivity Analysis of Dopingless Transistor for Low Power Applications," *IEEE Transactions on Electron Devices*, vol. 62, no. 3, pp. 729–735, 2015.

[15] V. Shrivastava, A. Kumar, C. Sahu, and J. Singh, "Temperature Sensitivity Analysis of Dopingless Charge-Plasma Transistor," *Solid-State Electronics*, vol. 117, pp. 94–99, 2016.

[16] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, P. Sundaravadivel, and J. Singh, "Dopingless Transistor based Hybrid Oscillator Arbiter Physical Unclonable Function," in *Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2017.

[17] M. T. Rahman, D. Forte, J. Fahrny, and M. Tehranipoor, "ARO-PUF: An Aging-Resistant Ring Oscillator PUF Design," in *Proceedings of the Design, Automation Test in Europe Conference Exhibition (DATE)*, 2014, pp. 1–6.

[18] S. R. Sahoo, S. Kumar, and K. Mahapatra, "A Modified Configurable RO PUF with Improved Security Metrics," in *Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems*, 2016, pp. 320–324.

[19] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A Large Scale Characterization of RO-PUF," in *Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2010, pp. 94–99.