Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security

Venkata P. Yanambaka, *Student Member, IEEE*, Saraju P. Mohanty, *Senior Member, IEEE*, and Elias Kougianos, *Senior Member, IEEE*

***Abstract*—Time to market is a vital aspect of electronic product development. When it comes to device technology, the time needed for the device fabrication processes to stabilize is relatively long. At the early stages of any device technology development, manufacturing variations are extensive. They are inevitable and unpredictable. Such manufacturing variations can be used advantageously to improve security and protect hardware and software IP. A physical unclonable function (PUF) uses the device manufacturing variations to extract unique and non-replicable keys which can be used for various applications such as cryptography and IP protection. This paper presents a hybrid oscillator arbiter PUF which uses the manufacturing variations of dopingless field-effect transistors (DLFETs) to achieve non-replicability and the results are compared with the more established FinFETs. The scalability of DLFETs is higher compared to current transistor technologies and the power consumption is lower. There is a 25% reduction in power consumption when compared to a 14 nm FinFET technology. The PUF designs presented in this paper are speed-optimized and power-optimized hybrid oscillator arbiter PUFs. The power-optimal design can be deployed in systems where power consumption should be low and the speed-optimal design can be implemented when speed of operation plays a vital role. Hence, these two designs can be deployed in two different application domains of current technologies such as the of Internet of Things.**

***Index Terms*—Manufacturing process variations, dopingless junctionless FET, physical unclonable function (PUF), ring oscillator, system security, hardware-assisted security.**

I. Introduction

THE 90 nm CMOS technology node was one of the major breakthroughs when it was released [1] but scaling beyond, to the 65 nm and 45 nm nodes, introduced serious issues such as significant leakage in transistors. Conventional dielectric materials were not sufficient and high-κ dielectric materials were introduced [2]. Even with the high-κ materials, the scaling problem could not be addressed beyond 32 nm. Hence the transistors were transformed from a two dimensional structure to a three dimensional device, the FinFET [3]. With the FinFETs introduced, a single chip can now be packed with almost 21 billion transistors [4]. In a FinFET, the source and drain are projected into the third dimension so that the effective length of the channel will be twice the height of the fin. This will reduce short channel effects. With the 16 nm node, FinFETs also started exhibiting high leakage thus necessitating a new solution.

Junctionless transistors were introduced as a promising solution for these problems [5], [6] but there are some issues with the junctionless FET, such as poor switch-off capability, high parasitic capacitance (due to higher doping), low on-state current and higher gate work function [7], [8]. These issues were addressed by the introduction of the Dopingless FET (DLFET) [9]. Higher band to band tunneling and random dopant fluctuations (RDF) are addressed in dopingless FETs using a thin intrinsic silicon nanowire to form the drain and source instead of heavily doped drain, channel and source [10]. Due to the DLFET structure, the scalability of the device increases, while exhibiting low leakage currents, as discussed in Section II.

After the introduction of every new technology, there will be a significant time before it can be commercially marketed [11]. FinFET devices were commercially released in 2012 but the investigation of process variations of FinFETs started a decade earlier [12]. A discussion of process and mismatch variations have been serious issues in all fabrication processes.

The manufacturing variations are unavoidable and unpredictable. They are naturally occurring variations due to the manufacturing process. A Physical Unclonable Function (PUF) makes use of these variations to generate random numbers, as shown in figure 1. Based on the design implemented, the output of a PUF will be binary string. Since the PUF will generate the random numbers using the manufacturing variations, they cannot be replicated using any other circuit and another input. Hence these random numbers can be used for various purposes such as Intellectual Property (IP) Protection, security, and encryption. Moreover, PUFs can be used for enhancing security in the Internet of Things (IoT). In an IoT environment, the devices will not be monitored continuously. In such cases, it will not be safe to store the key for encryption and decryption in a memory at the device [13], [14]. A PUF will generate the keys continuously, without having to retrieve

Manuscript received March 14, 2018; accepted March 19, 2018. Date of publication March 22, 2018; date of current version May 8, 2018. Preliminary research relevant to this paper has been presented in the following peer-reviewed conference: [38]. *(Corresponding author: Saraju P. Mohanty.)*

V. P. Yanambaka and S. P. Mohanty are with the Department of Computer Science and Engineering, University of North Texas, Denton, TX 76207 USA (e-mail: venkataprasanthyanambaka@my.unt.edu; saraju.mohanty@unt.edu).

E. Kougianos is with the Department of Engineering Technology, University of North Texas, Denton, TX 76207 USA (e-mail: elias.kougianos@unt.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSM.2018.2818180

0894-6507 © 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

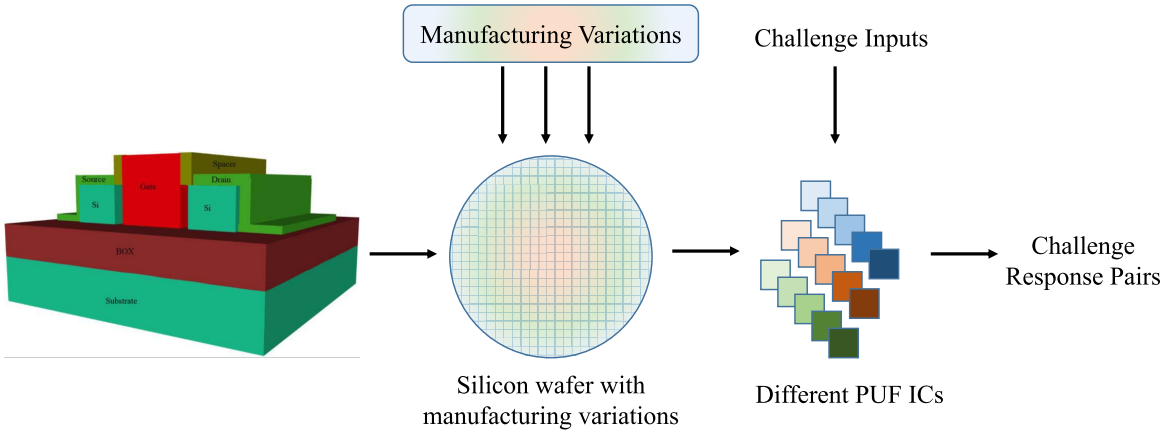


Fig. 1. Manufacturing Variations used for Physical Unclonable Functions.

them from memory and an exponentially high number of input and output combinations will make it difficult for the attacker to gain access to the message being transmitted or stored.

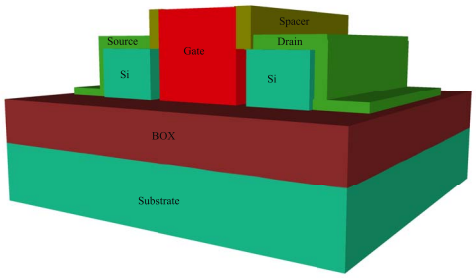
This paper is organized as follows: Section II presents a brief discussion of the geometry and structure of the DLFET. Section III provides an overview of the PUF and the use of manufacturing variations for security. Section IV summarizes related research that is being conducted in the areas of PUFs and the IoT. Section V presents the novel contributions of the paper in comparison to the works presented in Section IV. The design of the PUF is presented in Section VI and the circuit level implementation is presented in Section VII. Simulation results are presented in Section VIII. Section IX presents the conclusions.

II. Geometry and Structure of the Dopingless FET

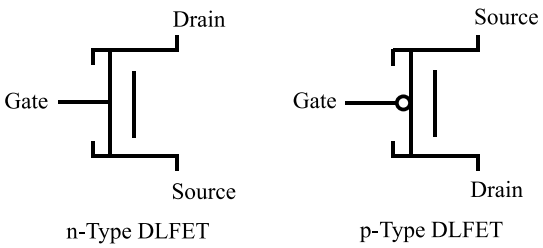
Figure 2a shows the geometry and figure 2b shows the symbols for n-type and p-type DLFETs. The DLFET does not utilize any external ion implantation. An undoped single uniform structure is used from source to drain. In the DLFET, a thin intrinsic silicon nanowire is used between the metal electrodes and gate, source and drain regions. A high-κ material (HfO_2) is considered as dielectric material, resulting in negligible leakage current. The p-type and the n-type doping regions can be formed using work function engineering inside the undoped thin silicon. The difference between the work function of the undoped silicon film and the metal incorporated for source and drain will be a deciding factor for making the region p-type or n-type [10], [15]. Electrons and holes are accumulated in the respective regions artificially and this process is called "charge-plasma". The work function difference will create a charge so that the charge carriers are accumulated in the source and drain regions.

III. Use of Manufacturing Process Variations for PUF-Based Security: The Big Picture

The Internet of Things (IoT) has been a major area of research in recent years. The IoT is a disruptive technology and is expected by 2020 to have major impact on society [16].



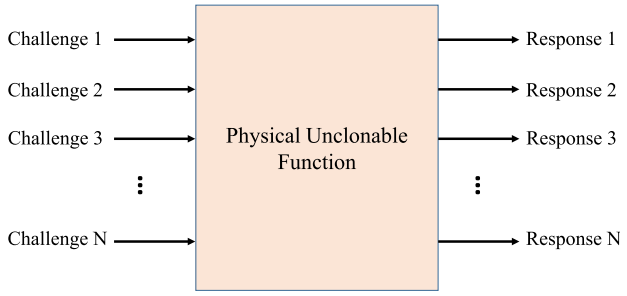
(a) Physical structure of the DLFET



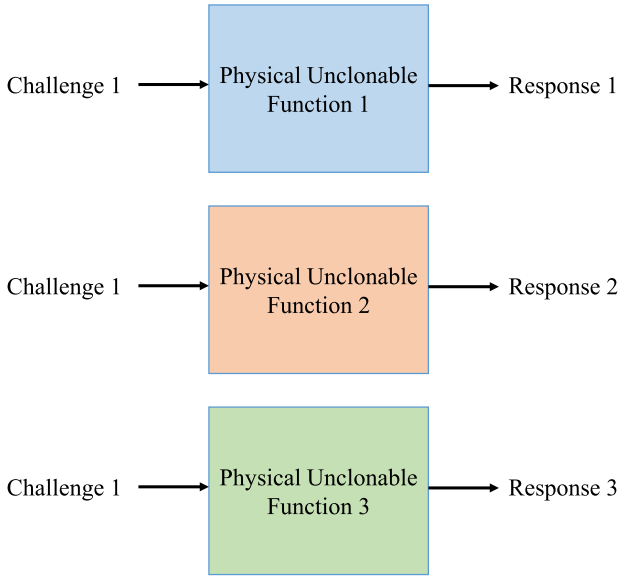
(b) DLFET symbols

Fig. 2. DLFET structure and symbols.

With the large improvements in cutting edge technologies in almost all disciplines, the end user experience has drastically changed in the past decade. Every year, new applications are becoming available with better performance, high throughput and low power consumption [11]. In an IoT environment, all devices are connected to each other through the Internet or a local network. This decreases the human interaction in most work, automating almost everything, and in turn increasing accuracy. But the devices that are deployed remotely in an IoT environment are without any human monitoring or security and can be potentially easily accessible to an attacker. IoT devices use the Internet or a local network to connect to other devices or the cloud. If the key to encrypt the communications or the data being collected is stored in a non-volatile memory, it can be accessed by the attacker in many ways and can be exploited to compromise the data and communications. A PUF uses the manufacturing variations, which are neither avoidable nor predictable, to generate the key. As shown in figure 1, after

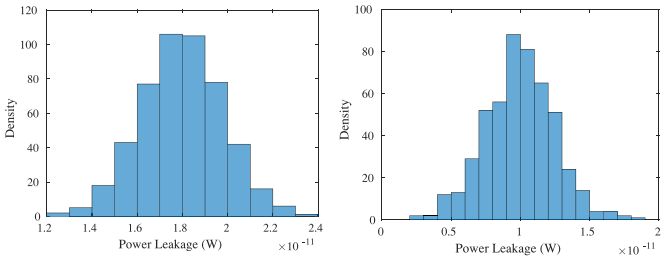


(a) Different challenges to the same PUF result in different responses.



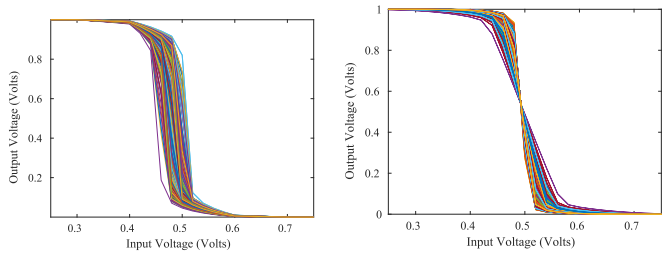
(b) The same challenges to different PUFs result in different responses.

Fig. 3. Working principle of a PUF.



(a) DLFET (b) FinFET

Fig. 4. Leakage power of n-Type FET.



(a) DLFET (b) FinFET

Fig. 5. Inverter DC characteristics.

TABLE I
DEVICE PARAMETERS OF DOPINGLESS FET [18]

Parameters	Dopingless FET
Silicon Film Thickness (T_{si})	10 nm
Effective Oxide Thickness (EOT)	1 nm
Gate Length (L_g)	20 nm
Width (W)	1 μm
Source/Drain extension	10 nm
Metal work function/doping for source/drain	3.9 eV (Hafnium)
Metal work function/doping for gate	4.66 eV (TiN)
Doping	$10^{15}/cm^3$

the fabrication process when a wafer is cut into different ICs, each will have its own manufacturing variations. Each of the devices, on the same IC or a different IC will have slightly different output for the same input, even if this difference is small.

For a PUF, circuits like ring oscillators, SRAM, and arbiters are fabricated and are tested their suitability. Due to the variations, the outputs will not be identical even on identical circuits. Using these varied outputs, cryptographic keys can be generated. The input given to a PUF is a challenge, and the output obtained is a response. Both of them are combined in a Challenge Response Pair (CRP). As shown in figure 3a, if the same challenge input is given to the same PUF module, there will be no change in the output. If the challenge input is changed for the same module, there will be a different output. As also shown in the same figure, if the same challenge input is given to a different PUF, a different output will be generated. Hence, a key generated with a specific challenge input on a module cannot be replicated on any other PUF module.

Even with the attacker having access to the PUF module, without the challenge input, it becomes difficult to decrypt the data or compromise the intellectual property. There are various architectures of PUFs and different methodologies were proposed to isolate the challenge input that is being transmitted by the server from the attacker [17]. Besides communication encryption and data encryption, PUFs are also widely used in IP protection. A unique identification key will be generated and stored, which can be used for IP protection and validation in the future.

To illustrate these ideas, simulations were performed in the Cadence Virtuoso suite. Models for the DLFETs were obtained from first-principle TCAD simulations using SILVACO ATLAS/Device 3D as detailed in [9]. The TCAD simulations were then used to generate calibrated Verilog-A models for the circuit simulator. Monte Carlo simulations were performed for 500 runs and the $I-V$ characteristics were plotted with the geometric parameters varied by 10% (i.e., standard deviation was 10% of the mean during Monte Carlo sampling). The leakage power of the n-Type DLFET and the n-Type FinFET were compared. Leakage of the FinFET is higher compared to that of a DLFET. Figure 4 shows the comparison with the manufacturing variations simulated. Figure 5 shows the comparison of variation of FinFET and DLFETs in the case of an inverter. These show the variability of the transistors which can be suitable for PUF design. Table I provides the nominal parameters.

IV. Related Prior Research

Extensive research has being conducted in reduction in leakage power. The leakage issues and short channel effects for CMOS transistors and high-κ metal gate transistors are presented in [11]. A PVT analysis of circuits like SRAMs with different technologies is also presented in the same reference. A PVT analysis of FinFETs in analog applications is presented in [19]. The Dopingless FETs structure, working and fabrication methodology along with an SRAM implementation was presented in [9]. In the same work, a stress test was conducted on the respective transistors to check the aging resistance of the devices. The transistors show promising resistance to aging effects. In [10], a comparison of the DLFET with the junctionless transistor was presented. The main issues with the junctionless transistors were presented in [9] and, as a potential solution, the DLFET was introduced. A temperature analysis on the DLFETs is performed in [20] and [21].

Using the manufacturing variations as a foundation, PUFs have been designed. Different architectures of PUFs have been proposed for various applications and implementations [22]–[26]. Each of the architectures can be categorized into weak PUFs and strong PUFs [14]. Many different architectures were surveyed in [14]. An SRAM PUF was presented in [27]. Besides transistors, other devices are also being used to develop PUF modules. A memristor-based PUF was presented in [26] and [28]. Some of the PUFs were proven to be susceptible to various attacks. Developing an attack resilient PUF has been a challenge in almost all architectures. In order to avoid attacks on PUFs, various algorithms were proposed. In [17], an elliptic curve based PUF authentication protocol was proposed and evaluated.

The Ring Oscillator (RO) PUF is easy to implement and also occupies smaller chip area and consumes less power comparatively to other architectures. Conventional RO PUF design is presented in [29]. In [30] and [31], the design of the hybrid oscillator arbiter PUF was proposed. Two different designs, power optimized and speed optimized PUFs were presented for implementation in different applications, from hand-held devices to high performance computing. The design of a PUF to generate multiple keys is presented in [32].

The IoT is already being implemented in many environments and in the near future the entire home will be automated, making it a smart home. Research is being conducted extensively in that area. In [33], a health monitoring system is presented which incorporates the IoT, connects different devices and automates the process of monitoring and diagnosing of thyroid function. Modules which can be placed on the patient and a module for the doctor were developed and Bluetooth technology was used for the communication between the patient module and the doctor module. In [34], different security issues in the IoT were presented. A very detailed description of uses of PUF in security applications is presented in [35].

V. Novel Contributions

This paper presents two designs of PUFs using the DLFET and the results are compared to the same designs using 14 nm FinFET technology. These designs are the following:

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

The speed optimized design, as the name suggests can be deployed in applications where the speed of operation is vital like routers and network switches. The power optimized design can be deployed in applications where the speed can be traded off for power conservation like smart devices which operate on a battery. Both devices can be deployed in respective application domains of the Internet of Things.

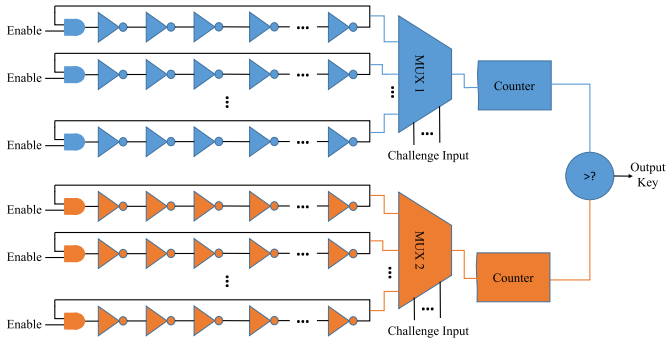


Fig. 6. Conventional RO-PUF Design.

VI. Design of Physical Unclonable Functions

This section presents the different PUF designs. The two designs take advantage of the manufacturing variations that are introduced during fabrication. The designs are derived from two different architectures of PUFs. The two conventional designs are presented first and then the new designs of PUF are presented.

A. Conventional Ring Oscillator PUF Design

The conventional Ring Oscillator Physical Unclonable Function (RO-PUF) design is presented in Fig. 6. As the name suggests, the RO-PUF contains N ring oscillators. In this case, for N oscillators, an $N/2$ bit key will be produced. The ring oscillators are connected to two counters through multiplexers which count the number of oscillations given by the ROs. The multiplexers feed the oscillations to the counters. The select lines of the multiplexers in this case become the challenge input to the PUF design itself. As shown in the figure, half of the oscillators are connected to one counter and the remaining half are connected to the other counter. The counted oscillations are then compared with each other.

Due to the manufacturing variations in the fabrication phase, the oscillation frequencies will not be the same for all ring oscillators. Depending on the oscillation frequency, the comparator will generate the bits 1 and 0. With each pair of selected ring oscillators, the output bit will change because of the process variation. Hence, to generate a 128-bit key, 256 ring oscillators need to be employed in the design. The challenge input for this design is the input to the multiplexers. With the change in challenge input, the output key changes.

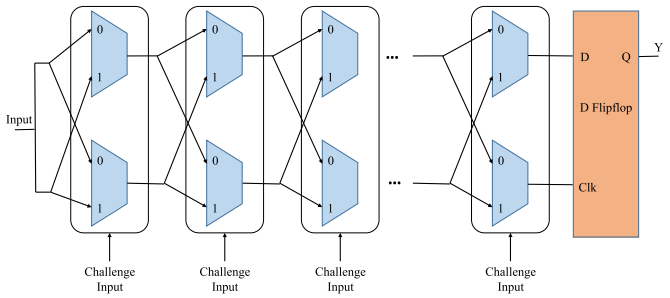


Fig. 7. Conventional Arbiter PUF Design.

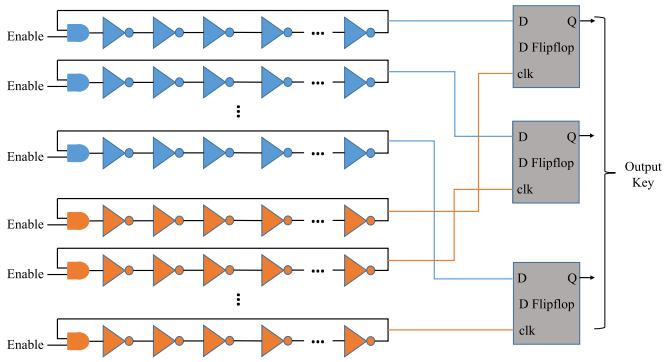


Fig. 8. DLFET Based Speed Optimized Hybrid Oscillator Arbiter PUF.

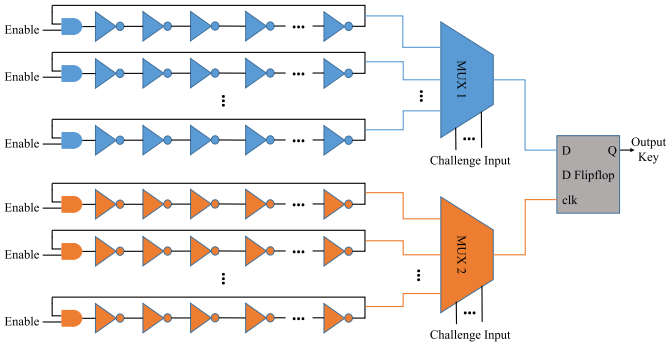


Fig. 9. DLFET Based Power Optimized Hybrid Oscillator Arbiter PUF.

Inverters are highly susceptible to temperature and environmental variations. Hence the counters are employed such that there is a little error rate while generating the output key.

B. Conventional Arbiter PUF Design

The conventional Arbiter Physical Unclonable Function (A-PUF) design is shown in figure 7. This PUF contains multiplexers connected in series, as shown in the figure. In the case of an RO-PUF design, the oscillation frequencies are affected by various factors. In the Arbiter PUF, the transistors present in the multiplexers will produce variable delays. At the end of the series, a D flipflop is present. The signal from the top multiplexers will be fed as an input to the D flipflop and the signal from the bottom series of multiplexers is fed to the clock signal of the D flipflop.

Due to manufacturing variations, the gate delay presented by the transistors will vary with each multiplexer. Hence, the flipflop input signals, the D input and the clock, will be different at a specific point of time where the output will be obtained. To generate a 128-bit key, 256 series of multiplexers are needed. As the output generation entirely depends on the gate delay, more multiplexers will be needed to generate a sufficient delay to produce a difference between the two signals, the D input and the clock signal. Hence the power consumption of the device will also be comparatively higher.

C. Dopingless Transistor Based Speed Optimized Hybrid Oscillator Arbiter PUF

The design of the speed-optimized hybrid oscillator arbiter PUF is shown in figure 8. Dopingless FETs are used for the design. The hybrid oscillator arbiter PUF design is a combination of the arbiter and the ring oscillator PUF designs. For the hybrid oscillator arbiter PUF, N ring oscillators will generate an $N/2$ bit key. The ring oscillators will produce the oscillations, but due to the manufacturing variations introduced during the fabrication process, the frequencies will not be the same for all oscillators. This is taken advantage of in designing the PUF. There are two sets of ring oscillators with $N/2$ in each set. One half of the ring oscillators are connected to the D input of the flipflops and the other half are connected to the clock signal. At a given time, the signal at the D input and the clock signal of the flipflop will not be the same due to the manufacturing variations which will give different outputs from each of the flipflops. All the output bits combined give the PUF key. With the absence of multiplexers, the speed of key generation is increased significantly.

D. Dopingless Transistor Based Power Optimized Hybrid Oscillator Arbiter PUF

The power-optimized hybrid oscillator arbiter PUF is similar to the design of the speed-optimized hybrid oscillator arbiter PUF. The main difference is the presence of multiplexers. Devices operating on battery power cannot afford to supply power to multiple D flipflops all the time. So the flipflops are replaced with one flipflop and multiplexers. The ring oscillators are divided into two sets with $N/2$ oscillators in each set. Instead of connecting them directly to the flipflops, one set of oscillators is connected to multiplexer MUX1 and the other half are connected to multiplexer MUX2, as shown in figure 9. The outputs of the multiplexers are connected to the D input and the clock signal of the D flipflops. This reduces the power consumption but increases the key generation time. The multiplexers select the oscillators and feed to the flipflop which then generates each bit of key. Due to the manufacturing variations, the signals at the D input and the clock signals will not be the same. Hence the output bits will also not be the same. This design can be used when the power consumption needs to be conserved at the cost of speed of operation.

VII. Circuit Level Implementation of Hybrid Oscillator Arbiter PUF Using DLFET

In the experimental setup, a 13-stage oscillator was considered. A 32-bit key was generated. For the generation of

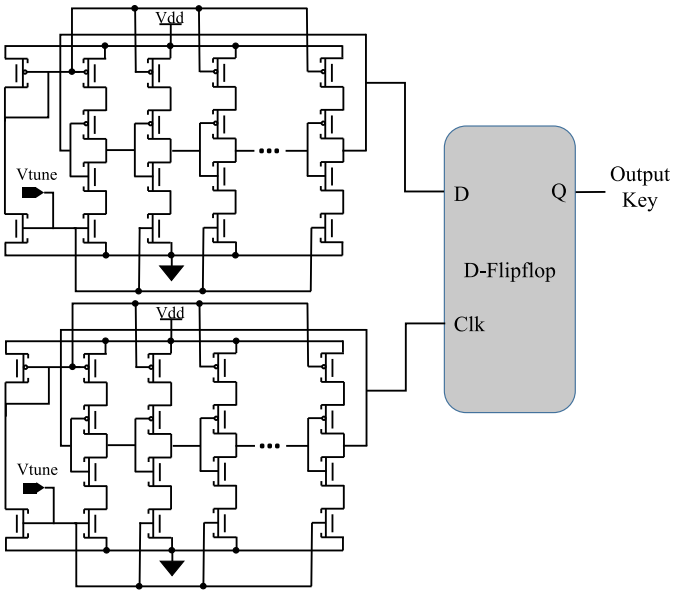


Fig. 10. Circuit implementation of the PUF.

a 32-bit key, 64 ring oscillators were needed. In the Ring Oscillator PUF, counters and a comparator were used. On the other hand, in the Hybrid Oscillator Arbiter PUF, the counters and the comparator were replaced with a D flipflop. An RS flipflop could be implemented instead of a D flipflop for lower biasing, but it was found that it was not optimal for the PUF performance. The Arbiter PUF also uses a high number of multiplexers which will increase the number of transistors and hence the overall complexity of the circuit itself. Hence, with the Hybrid Oscillator Arbiter PUF, the complexity of the circuit was decreased comparatively.

The conventional inverter is highly susceptible to temperature and power supply variations. This becomes a serious issue when implementing PUFs using inverters. When the temperature of the chip or the module changes, if a conventional inverter is used in a PUF architecture, the oscillation frequency changes. Due to the change in frequency, for a single challenge input, the response changes. Hence the error rate increases and the key cannot be used to encrypt the data. Another major issue is the aging effect of the inverter design. As the age of the inverter circuit increases, the output changes, which affects the reliability of the PUF module itself. To overcome these effects on the module, a current starved architecture is being implemented in the PUF. Figure 10 shows the circuit level design of a single bit PUF module. The current starved oscillator will generate the oscillations necessary and they are compared using the D flipflop. The flipflop will give out a single bit of the PUF. The tuning voltage V_{tune} for all the oscillators is given the same when running the simulations. To increase the complexity of the keys generated, V_{tune} can also be used as a challenge input along with the multiplexers. This complicates the implementation but will increase the security of the module. Using this architecture, the error bit rate will be low, as presented in Section VIII.

TABLE II
CHARACTERIZATION TABLE FOR POWER AND SPEED OPTIMIZED DESIGNS

Parameter	Power Optimized Hybrid Oscillator Arbiter PUF	Speed Optimized Hybrid Oscillator Arbiter PUF
Average Power	121.3 μW	151 μW
Hamming Distance	48 %	50 %
Time to generate the key	150 ns	50 ns

VIII. EXPERIMENTAL RESULTS

This section presents the experimental results of the speed optimized and the power optimized hybrid oscillator arbiter PUF designs. For a PUF to be validated, the following two properties must be satisfied: Uniqueness, and Reliability. The Figures of Merit (FoMs) considered in this section, along with the uniqueness and reliability, are the average power consumed by the module and the total time taken to generate the PUF key. These are the two main conflicting aspects in applications as the data processing should be fast while consuming as little power as possible. For high performance, some power should be traded off and for low power consumption, a performance trade off will always be needed. Table II shows a comparison of the Hamming distance between the FinFET based PUF and the DLFET based PUF.

A. Uniqueness

The uniqueness of a PUF is the ability of the module to produce different PUF keys with a change in the challenge bits. It can be quantified using the Hamming distance of the keys produced by the circuit. For an ideal PUF, the Hamming distance should be exactly 50%. Monte Carlo simulations were performed on the circuit to simulate the process and mismatch variations. 100 runs were performed and the output keys were checked for uniqueness. Figure 11 shows the frequencies of different ring oscillators in each of the runs. This shows the different frequencies each of the oscillators produce for each run and in a single run. Figures 12 and 13 show the Hamming distance between the different keys produced in different runs. The power optimized hybrid oscillator arbiter PUF consists of multiplexers and the select lines of the multiplexers can be considered as challenge bits. On the other hand, in the speed optimized PUF there is not multiplexer present and hence no challenge bits are available. This means that it will produce a single key once it is fabricated. For a fair comparison, only the process variation is considered in this case and the challenge bit variation in both designs was ignored.

B. Reliability

A PUF is not reliable if it cannot create the same key with environmental and supply voltage variations. Environmental effects like temperature variations will affect the performance of the ring oscillators. In such conditions, a PUF with the same challenge bits should be generating the same key. To test the reliability of the designs, the temperature and the power supply are varied. Figures 14 and 15 show the Hamming distance of

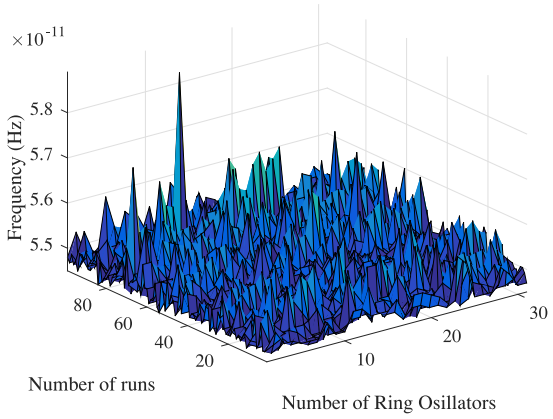


Fig. 11. Frequencies of the Ring Oscillators.

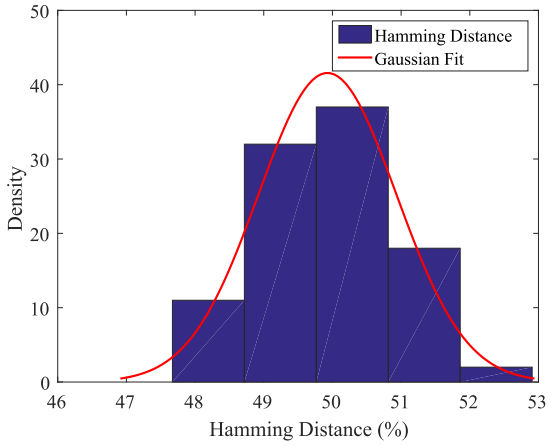


Fig. 12. Inter PUF Hamming Distance of Speed Optimized Hybrid Oscillator Arbiter PUF.

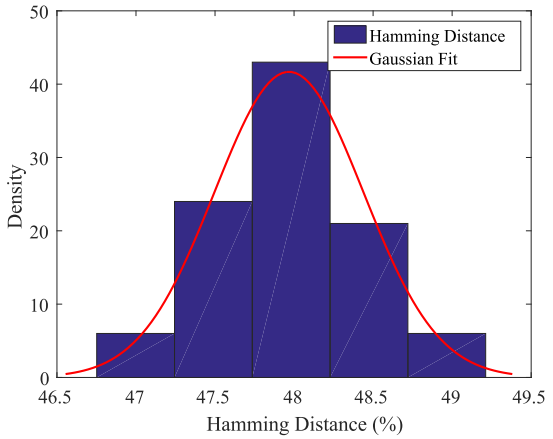


Fig. 13. Inter PUF Hamming Distance of Power Optimized Hybrid Oscillator Arbiter PUF.

the keys generated by the designs. The speed optimized PUF does not have much variation but comparatively the power optimized PUF shows more variation.

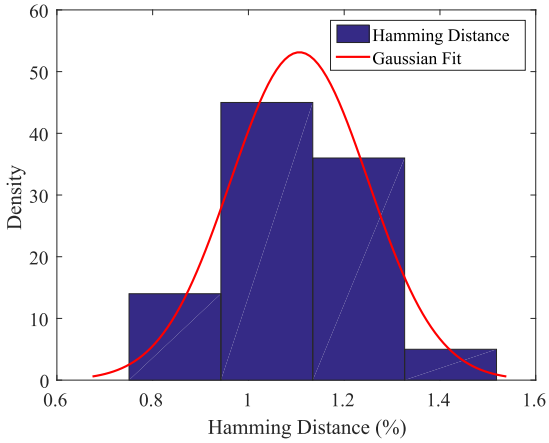


Fig. 14. Intra PUF Hamming Distance of Speed Optimized Hybrid Oscillator Arbiter PUF.

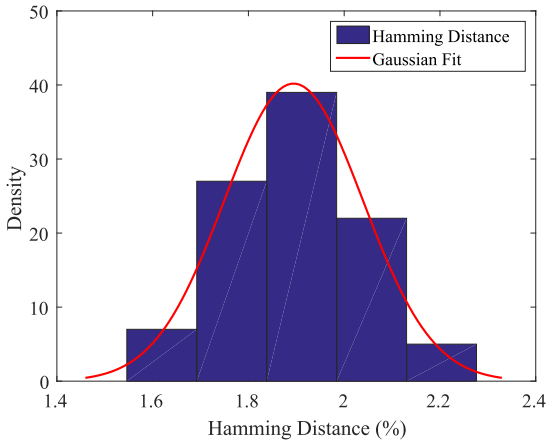


Fig. 15. Intra PUF Hamming Distance of Power Optimized Hybrid Oscillator Arbiter PUF.

TABLE III
COMPARISON OF FINFET AND DLFET TECHNOLOGIES

Power Optimized Hybrid Oscillator Arbiter PUF		
Parameter	FinFET	DLFET
Average Power	219.34 μW	121.3 μW
Hamming Distance	49.3 %	48 %
Time to generate the key	150 ns	150 ns
Speed Optimized Hybrid Oscillator Arbiter PUF		
Parameter	FinFET	DLFET
Average Power	250.15 μW	151.3 μW
Hamming Distance	49.6 %	50 %
Time to generate the key	50 ns	50 ns

C. Average Power

The average power consumed is always a major metric. In devices that run on battery, low power should be consumed or the introduced module will be of no use at that point. In applications like routers or network switches, speed should be very high to reduce data latency. Figures 16 and 17 show the power consumption of the speed optimized and power optimized hybrid oscillator arbiter PUFs. The power optimized design does show lower consumption due to the smaller number of flipflops present in the design. The average

TABLE IV
COMPARISON OF RESULTS WITH RELATED EXISTING RESEARCH

Research Works	Technology Used	Architecture Used	Average Power Consumption	Hamming Distance (%)
Rahman, et al. [36]	90 nm CMOS		–	50
Maiti, et al. [29]	180 nm CMOS	Traditional Ring Oscillator	–	50.72
Suh, et al. [37]	–		–	46.15
Maiti, et al. [23]	–	–	–	47.31
S. R. Sahoo, et al. [24]	90 nm CMOS	Ring Oscillator	–	45.78
Cherkaoui, et al. [25]	350 nm CMOS	Transient Effect Ring Oscillator (TERO)	–	49.7
Yanambaka, et al. (Power Optimized) [32]	32 nm FinFET	Current Starved Oscillator	175.5 μW	50.1
Yanambaka, et al. (Speed Optimized) [31]	32 nm FinFET	Traditional Ring Oscillator	285.5 μW	50.9
This Paper (Power Optimized)	10 nm Dopingless FET	Hybrid Oscillator Arbiter	121.3 μW	48.0
This Paper (Speed Optimized)	10 nm Dopingless FET	Hybrid Oscillator Arbiter	151 μW	50.0

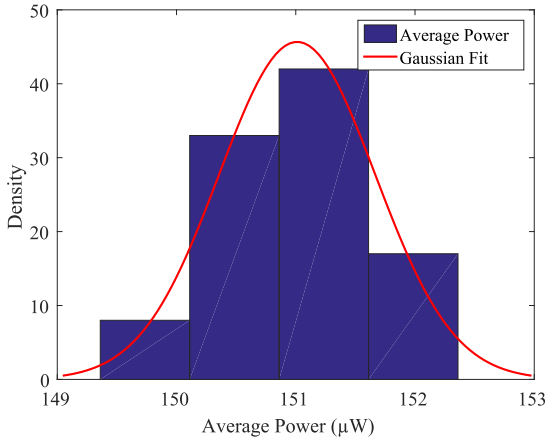


Fig. 16. Average Power of Speed Optimized Hybrid Oscillator Arbiter PUF.

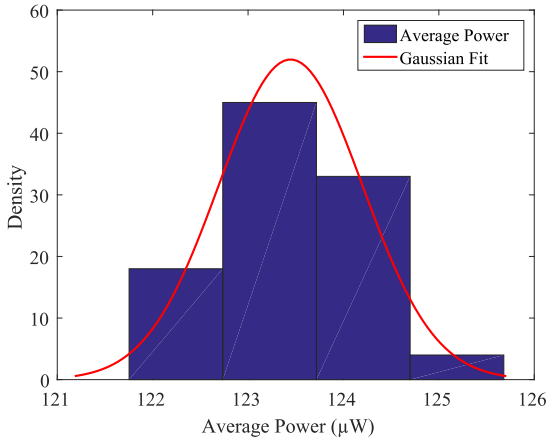


Fig. 17. Average Power of Power Optimized Hybrid Oscillator Arbiter PUF.

power is the sum of all the leakage powers and the dynamic power.

D. Time Taken to Generate the PUF Key

The time taken to generate the PUF key is another main metric which plays an important role in high performance devices. In the case of router or network switches, the number of devices connected at a time will be high. So to encrypt and decrypt every incoming and outgoing message, the PUF key generation should be fast. In such cases, to decrease latency, the multiplexers in the power optimized design were removed and a number of D flipflops are added in the speed optimized design. As each pair of oscillators has a separate D flipflop, the time needed to generate the key will be the time the circuit runs until a chosen point of time. For example, in the simulations performed, the output key was recorded after running the circuit for 50ns. In the power optimized design, the total time taken to generate the key will be more than 150ns as the multiplexers are used to select the signals from oscillators and between each selection a small time gap is given.

E. Comparison With Other Technologies

A comparative analysis of the two designs of hybrid oscillator arbiter PUF using DLFETs and FinFETs is presented in Table III. For the FinFET based design, 14 nm FinFETs are used. Similar to the design presented in the paper, a current starved architecture is used in the FinFET based PUF. Monte Carlo is used to simulate the manufacturing variations. All the geometric parameters along with the doping concentration are varied in the FinFETs. From the table, it is clear that the DLFETs are less power hungry compared to the FinFETs. Table IV shows the comparison of figures of merit from other published works.

IX. CONCLUSION

This paper presents two designs of hybrid oscillator arbiter PUFs, a speed optimized and a power optimized design using DLFETs. A fair comparison of two technologies, FinFET and DLFETs is presented in this paper to show a power reduction using these DLFETs. As a future research, an ultra low power design of PUF can be implemented as these transistors show a promise for usage in low power applications. A newer design of PUF will also be developed with these transistors which will be capable of reconfigurability and will generate multiple keys accordingly. An SRAM based PUF using these transistors can also be implemented as DLFETs are more stable, which might give an advantage in designing better SRAMs. The speed optimized design, gives only one key. As a future research, a configurable model of the speed optimized hybrid oscillator arbiter PUF can be designed and characterized.

ACKNOWLEDGMENT

The authors would like to acknowledge the help of visiting scholar Dr. J. Singh.

REFERENCES

[1] F. Pellizzer *et al.*, "A 90nm phase change memory technology for stand-alone non-volatile memory applications," in *Symp. VLSI Technol. Dig. Tech. Papers*, Honolulu, HI, USA, 2006, pp. 122–123.

[2] M. T. Bohr, R. S. Chau, T. Ghani, and K. Mistry, "The high-κ solution," *IEEE Spectr.*, vol. 10, no. 10, pp. 29–35, Oct. 2007.

[3] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Ghai, *Nanoscale High-κ/Metal Gate CMOS and FinFET Based Logic Libraries* (Nano-CMOS and Post-CMOS Electronics: Devices and Modelling), vol. 1. London, U.K.: Inst. Eng. Technol., 2015, ch. 6, pp. 169–211.

[4] *Nvidia*. Accessed: Nov. 11, 2017. [Online]. Available: http://www.geforce.com/

[5] A. Kranti *et al.*, "Junctionless nanowire transistor (JNT): Properties and design guidelines," in *Proc. Eur. Solid State Device Res. Conf.*, Sevilla, Spain, 2010, pp. 357–360.

[6] D. Gola, B. Singh, and P. K. Tiwari, "A threshold voltage model of tri-gate junctionless field-effect transistors including substrate bias effects," *IEEE Trans. Electron Devices*, vol. 64, no. 9, pp. 3534–3540, Sep. 2017.

[7] M. S. Parihar, D. Ghosh, and A. Kranti, "Single transistor latch phenomenon in junctionless transistors," *J. Appl. Phys.*, vol. 113, no. 18, 2013, Art. no. 184503.

[8] Z. Chen *et al.*, "Surface-potential-based drain current model for long-channel junctionless double-gate MOSFETs," *IEEE Trans. Electron Devices*, vol. 59, no. 12, pp. 3292–3298, Dec. 2012.

[9] C. Sahu and J. Singh, "Potential benefits and sensitivity analysis of dopingless transistor for low power applications," *IEEE Trans. Electron Devices*, vol. 62, no. 3, pp. 729–735, Mar. 2015.

[10] C. Sahu and J. Singh, *Junction and Doping-Free Transistors for Future Computing* (Nano-CMOS and Post-CMOS Electronics: Devices and Modelling), vol. 1. London, U.K.: Inst. Eng. Technol., 2015, ch. 5, pp. 139–168.

[11] S. P. Mohanty, *Nanoelectronic Mixed-Signal System Design*. New York, NY, USA: McGraw-Hill Educ., 2015.

[12] S. Xiong and J. Bokor, "Sensitivity of double-gate and FinFETdevices to process variations," *IEEE Trans. Electron Devices*, vol. 50, no. 11, pp. 2255–2261, Nov. 2003.

[13] S. Joshi, S. P. Mohanty, and E. Kougianos, "Everything you wanted to know about PUFs," *IEEE Potentials*, vol. 36, no. 6, pp. 38–46, Nov./Dec. 2017.

[14] 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.

[15] M. Panchore, J. Singh, and S. P. Mohanty, "Impact of channel hot carrier effect in junction-and doping-free devices and circuits," *IEEE Trans. Electron Devices*, vol. 63, no. 12, pp. 5068–5071, Dec. 2016, doi: 10.1109/TED.2016.2619621.

[16] "Six technologies with potential impacts on U.S. interests out to 2025," Disruptive Civil Technol., Nat. Intell. Council, Washington, DC, USA, Rep. CR 2008-07, 2008.

[17] J. R. Wallrabenstein, "Practical and secure IoT device authentication using physical unclonable functions," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud)*, Vienna, Austria, Aug. 2016, pp. 99–106.

[18] C. Sahu and J. Singh, *Junction and Doping-Free Transistors for Future Computing* (Nano-CMOS and Post-CMOS Electronics: Devices and Modelling), vol. 1. London, U.K.: Inst. Eng. Technol., 2015, ch. 6, pp. 139–168.

[19] D. Ghai, S. P. Mohanty, and G. Thakral, "Comparative analysis of double gate FinFET configurations for analog circuit design," in *Proc. 56th IEEE Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Columbus, OH, USA, 2013, pp. 809–812.

[20] V. Shrivastava, A. Kumar, C. Sahu, and J. Singh, "Temperature sensitivity analysis of dopingless charge-plasma transistor," *Solid-State Electron.*, vol. 117, pp. 94–99, Mar. 2016.

[21] M. Panchore, J. Singh, S. P. Mohanty, and E. Kougianos, "Compact behavioral modeling and time dependent performance degradation analysis of junction and doping free transistors," in *Proc. 2nd IEEE Int. Symp. Nanoelectron. Inf. Syst. (iNIS)*, 2016, pp. 194–199.

[22] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs," in *Proc. Int. Conf. Reconfigurable Comput. (FPGAs)*, 2010, pp. 298–303.

[23] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of RO-PUF," in *Proc. IEEE Int. Symp. Hardw. Orient. Security Trust (HOST)*, Anaheim, CA, USA, 2010, pp. 94–99.

[24] S. R. Sahoo, S. Kumar, and K. Mahapatra, "A modified configurable RO PUF with improved security metrics," in *Proc. 2nd IEEE Int. Symp. Nanoelectron. Inf. Syst.*, 2016, pp. 320–324.

[25] A. Cherkaoui, L. Bossuet, and C. Marchand, "Design, evaluation, and optimization of physical unclonable functions based on transient effect ring oscillators," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1291–1305, Jun. 2016.

[26] M. Uddin *et al.*, "Techniques for improved reliability in memristive crossbar PUF circuits," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI)*, Pittsburgh, PA, USA, Jul. 2016, pp. 212–217.

[27] C. Clavier and K. Gaj, *Cryptographic Hardware and Embedded Systems*, C. Clavier and K. Gaj, Eds. Lausanne, Switzerland: Springer, 2009.

[28] G. S. Rose and C. A. Meade, "Performance analysis of a memristive crossbar PUF design," in *Proc. 52nd ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, San Francisco, CA, USA, Jun. 2015, pp. 1–6.

[29] A. Maiti and P. Schaumont, "Improved ring oscillator PUF: An FPGA-friendly secure primitive," *J. Cryptography*, vol. 24, no. 2, pp. 375–397, 2010.

[30] V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making use of semiconductor manufacturing process variations: FinFET-based physical unclonable functions for efficient security integration in the IoT," *Analog Integr. Circuits Signal Process. J.*, vol. 93, no. 3, pp. 429–441, Dec. 2017.

[31] V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Novel FinFET based physical unclonable functions for efficient security integration in the IoT," in *Proc. 2nd IEEE Int. Symp. Nanoelectron. Inf. Syst. (iNIS)*, 2016, pp. 172–177.

[32] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and J. Singh, "Secure multi-key generation using ring oscillator based physical unclonable function," in *Proc. 2nd IEEE Int. Symp. Nanoelectron. Inf. Syst. (iNIS)*, 2016, pp. 200–205.

[33] P. Sundaravadivel, S. P. Mohanty, E. Kougianos, and U. Albalawi, "An energy efficient sensor for thyroid monitoring through the IoT," in *Proc. 17th Int. Conf. Thermal Mech. Multi Phys. Simulat. Exp. Microelectron. Microsyst. (EuroSimE)*, Montpellier, France, 2016, pp. 1–4.

[34] M. O'Neill, "Insecurity by design: Today's IoT device security problem," *Engineering*, vol. 2, no. 1, pp. 48–49, 2016.

[35] N. Sklavos, "Securing communication devices via physical unclonable functions (PUFs)," in *Proc. Inf. Security Solutions Europe*, Brussels, Belgium, 2013, pp. 253–261.

[36] M. T. Rahman, D. Forte, J. Fahrny, and M. Tehranipoor, "ARO-PUF: An aging-resistant ring oscillator PUF design," in *Proc. Design Autom. Test Europe Conf. Exhibit. (DATE)*, Dresden, Germany, 2014, pp. 1–6.

[37] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Design Autom. Conf.*, San Diego, CA, USA, 2007, pp. 9–14.

[38] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, P. Sundaravadivel, and J. Singh, "Dopingless transistor based hybrid oscillator arbiter physical unclonable function," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI)*, Bochum, Germany, 2017, pp. 609–614.

Venkata P. Yanambaka (S'12) received the Bachelor of Technology degree in electronics and communications from the Priyadarshini College of Engineering and Technology, India, in 2014. He is currently pursuing the Ph.D. degree with the System Electronic Systems Laboratory, Department of Computer Science and Engineering, University of North Texas. His research interests are in security in Internet of Things, energy-efficient circuits and systems, and application-specific systems design. He has authored of a 12 research articles which include multiple journals/transactions articles. He is a regular reviewer of various peer-reviewed journals and conferences.

Saraju P. Mohanty (SM'08) is a Professor with the University of North Texas. His research is in "Smart Electronic Systems" which has been funded by the National Science Foundations, Semiconductor Corporation, and the U.S. Air Force. He has authored 250 research articles, three books, and invented four U.S. patents. His Google Scholar citation with an H-index 29 and i10-index 84. He is the Editor in Chief of the *IEEE Consumer Electronics Magazine*. He serves as the Chair of Technical Committee on very large scale integration, IEEE Computer Society. He has been recognized as a IEEE Distinguished Lecturer by the Consumer Electronics Society in 2017. He was a recipient of the Glorious India Award in 2017 for his exemplary contributions to the discipline, the Society for Technical Communication 2017 Award of Merit for his outstanding contributions to the *IEEE Consumer Electronics Magazine*, the 2016 PROSE Award for best Textbook in Physical Sciences and Mathematics from the Association of American Publishers for his *Mixed-Signal System Design* book published by McGraw-Hill in 2015, and the 2016–2017 UNT Toulouse Scholars Award for sustained excellent scholarship and teaching achievements.

Elias Kougianos (SM'07) received the B.S.E.E. degree from the University of Patras, Greece, in 1985 and the M.S.E.E. degree, M.S. degree in physics, and the Ph.D. degree in EE from Lousiana State University, in 1987, 1988, and 1997, respectively. He is a Professor with the Department of Engineering Technology, University of North Texas (UNT), Denton, TX, USA. From 1988 to 1997, he was with Texas Instruments, Inc., Houston and Dallas, TX, USA. Initially he concentrated on process integration of flash memories and later as a Researcher in the areas of technology CAD and very large scale integration CAD development. In 1997, he joined Avant! Corporation (now Synopsys), Phoenix, AZ, USA as a Senior Applications Engineer and in 2001, he joined Cadence Design Systems, Inc., Dallas, TX, USA as a Senior Architect in Analog/Mixed-Signal Custom IC Design. He has been with UNT since 2004. His research interests are in the area of analog/mixed-signal/RF IC design and simulation and in the development of very large scale integration architectures for multimedia applications. He has authored or co-authored over 100 peer-reviewed journal and conference publications.