Springer Analog Integrated Circuits and Signal Processing Journal manuscript No.
(will be inserted by the editor)

Making Use of Semiconductor Manufacturing Process Variations: FinFET-based Physical Unclonable Functions for Efficient Security Integration in the IoT

Venkata P. Yanambaka · Saraju P. Mohanty · Elias Kougianos

Received: XXX / Revised: XXX / Accepted: XXX

Abstract In a typical design environment, semiconductor manufacturing variations are considered as challenges for nanoelectronic circuit design engineers. This has led to multi-front research on process variations analysis and its mitigations. As a paradigm shift of that trend the present article explores the use of semiconductor manufacturing variations for enhancing security of systems using FinFET technology as an example. FinFETs were introduced to replace high-κ transistors in nanoelectronic applications. From microprocessors to graphic processing units, FinFETs are being used commercially today. Along with the technological advancements in computing and networking, the number of cyber attacks has also increased. Simultaneously, numerous implementations of the Internet of Things (IoT) are already present. In this environment, one small security flaw is enough to place the entire network in danger. Encrypting communications in such an environment is vital. Physical Unclonable Functions (PUFs) can be used to encrypt device to device communications and are the main focus of this paper. PUFs are hardware primitives which rely on semiconductor manufacturing variations to generate characteristics which are used for this purpose. Two different designs of a Ring Oscillator (RO) PUF are introduced, one with low power consumption trading off device performance and one high-performance trading off device power consumption. There is an 11% decrease in power consumption with the low power model along with a

Computer Science and Engineering, University of North Texas, Denton, TX 76203.
Tel.: +1 940-565-3276
Fax: +1 940-565-2799
E-mail: vy0017@unt.edu

Computer Science and Engineering, University of North Texas, Denton, TX 76203.
Tel.: +1 940-565-3276
Fax: +1 940-565-2799
E-mail: saraju.mohanty@unt.edu

Engineering Technology, University of North Texas, Denton, TX 76203.
Tel.: +1 940-891-6708
Fax: +1 940-565-2666
E-mail: elias.kougianos@unt.edu

simple design and fabrication. Performance of the device can be increased with almost no increase in power consumption.

Keywords FinFET, Process variation, Physical Unclonable Function (PUF), Internet of Things (IoT), Security, Encryption

1 Introduction

The first general purpose programmable microprocessor, the Intel® 4004 was released in April 1970. It was used in calculator manufacturing and had 2250 transistors integrated in it [12]. It was manufactured in a 10 μm technology. After its release, the need for more powerful microprocessors grew and research progressed in that direction at a rapid rate. In 1975, Gordon Moore predicted that the number of transistors in an Integrated Circuit (IC) will double every two years, which became known as Moore's law and has held for the next half century. This is possible with rapid technology scaling and integration, but there were some hurdles in the process. Until transistors reached 90 nm technology, there were fewer issues with scaling. Beyond 90 nm, the channel length reduction gave rise to short channel effects. Leakage and other performance issues in transistors were more pronounced when technology reached the 45nm mark [5]. The dielectric material had to change to allow for more scaling. Hence a high-κ material was used which caused charge carrier scattering when used with the usual poly-Si gate and a metal gate was used instead. Thus, high-κ Metal Gate transistors were born. But this solution was temporary. From 22 nm downwards, the high-κ Metal Gate combination could not be used. To address this issue planar transistors were transformed into a 3D structure.

Fin Field Effect Transistors were introduced to reduce the leakage caused due to the short channel effects and the rapid transistor scaling. The structure of a FinFET with 3 Fins is shown in Fig. 1. Compared to a planar transistor, the source and drain of the FinFET are projected into the third dimension. The protruded source and drain into the gate look like fins and hence the name FinFETs [16]. The fin itself in a three dimensional structure that acts as channel. Hence the width of the channel of the transistor is equal to twice the height of the fin. The respective channel width to length ratio is increased which acts as a solution to the short channel effects. The gate also wraps on the fin, which is the channel. This gives more control over the charge carriers flowing through the channel. FinFETs are considered a reliable solution for the scaling problem. Currently FinFET manufacturing has reached the 14 nm technology node [19] and is available in commercial markets.

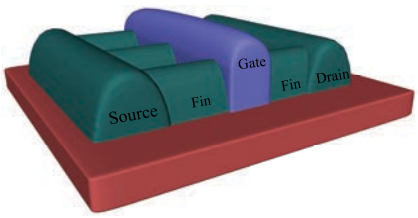

Fig. 1 Structure of FinFET with Three Fins.

High performance device design is growing with the introduction of FinFETs. Newer processors include around 8 billion transistors compared to the 2250 in the 4004. Along with transistor scaling, another area attracting research is the Internet of Things (IoT). A simple implementation of an IoT environment could be a network of devices communicating with each other to reduce human involvement in everyday activities as much as possible. The IoT is considered as one of the six most "Disruptive Civil Technologies" by the US National Intelligence Council [20]. Fig.2 presents an example of the IoT actively working in a home environment. The Iot mainly increases the quality of life and simplifies many activities with automation and networking [3,16]. Radio Frequency Identification (RFID), mobile phones, sensors, etc. started the device to device communication. That marked the beginning of the IoT. Devices are already being implemented where a single button can order goods online automatically. The "Internet of Things" term is accredited to "The Auto-ID Labs", a network of academic laboratories in this field. The IoT environment is already implemented in many areas [17].

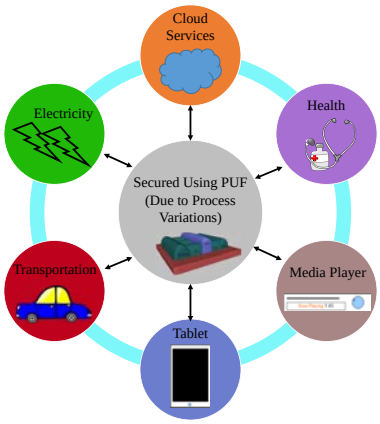

Fig. 2 Internet of Things at Home.

The rest of the paper is organized as follows: Section 2 explains how manufacturing variations are taken advantage of to design Physical Unclonable Functions (PUFs), and Section 3 presents the novel contributions of the paper. Section 5 gives an overview of the designs proposed and Section 6 presents the circuit level design of a Hybrid Arbiter Oscillator PUF. Simulation results are presented in Section 7 and conclusion and directions for future research are presented in Section 8.

2 Use of Manufacturing Process Variations for PUF based Security: The Big Picture

With all IoT devices potentially communicating with each other, there is a great possibility of malicious attacks. Cyber attacks are increasing daily. In a household, almost all devices will be connected to a network and a small vulnerability is sufficient for an attacker to gain access and take control. This might endanger the entire household. Sometimes the devices are deployed in areas where they can be easily accessed by the attacker [8]. In such devices, if the cryptographic key is stored in non Non-Volatile

Memory (NVM), it can be easily obtained by the attacker. Hence, an alternative to the key storage in memory should be implemented. A PUF is a proven alternative in such case.

A PUF is a circuit that takes advantage of manufacturing variability to uniquely form random characteristics between input and output [28]. Manufacturing variations are inevitable in any fabrication process and these physical variations in the circuit will be unique for each device. Therefore, the behavior of each device will be unique for the same given input. The input and output of a PUF are called collectively the challenge response pair (CRP). Fig. 3 shows the working characteristics of a PUF. The manufacturing variations naturally occur in the transistor or any other devices produced during the fabrication process. In the case of Fig. 3, a FinFET with three fins is shown, which is subjected to manufacturing variations. With those devices, different circuits are designed, such as Static RAMs (SRAMs) or Ring Oscillators (ROs). A PUF based on these designs is manufactured. The PUF takes in challenge inputs and gives out responses for those challenge inputs. The CRP for two RO PUFs will be different even if the challenges are the same. Hence a key need not be stored; it will be generated anytime needed and due to the high number of CRPs, even if the attacker has access to the device itself, it will be difficult to get the key needed to decrypt the communication between the client and the server.

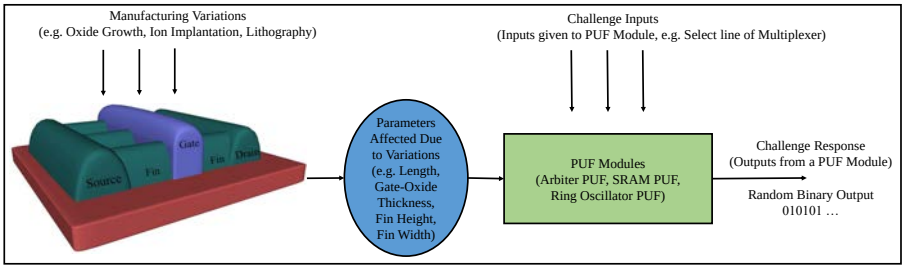

Fig. 3 Working Characteristics of the Physical Unclonable Function.

Process variations are inevitable in the fabrication of any device, especially transistors. Process variations can occur at different stages of fabrication, such as implantation, photolithography, oxidation or deposition. Due to these manufacturing variations, the geometry of the device is affected which will cause changes in the output of the device itself [1]. Fig. 4 shows the $I-V$ characteristics of an n-Type FinFET with process variations. Subsequently, an inverter is designed with these FinFETs and is subjected to DC Monte Carlo simulations. Fig. 5 shows the DC transfer characteristics of such an inverter under manufacturing variations. The dimensions of the n- and p- type FinFETs used for these simulations are shown in Table 3, and further discussion is given in section 5.3. For the Monte Carlo simulations, a variation (standard deviation) of 5% of the mean ($\sigma = 0.05\mu$) and a Gaussian distribution for the geometric dimensions was assumed. A total of 500 Monte Carlo runs were performed. From the simulations, it is clear that even if the design of the inverter is the same, under process variations there can be a significant change in the device characteristics and the input-output relationship. A PUF uses the same concept to produce different CRPs. Various PUF designs are available based on the architecture used, such as SRAM PUF, Memristor

PUF, Ring Oscillator PUF, etc. A PUF generates an output key which can be used in cryptographic applications. The advantage is that the same key cannot be generated without the device itself. Hence in an IoT environment where the client device is not monitored regularly, this can be used to generate a key for communication or authentication purposes. PUFs are also used in IP protection where a challenge response pair is generated by the manufacturer to validate the authenticity of the device [8].

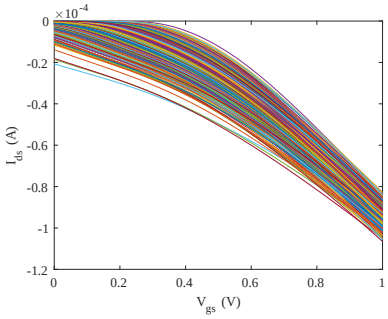

Fig. 4 n-type FinFET $I-V$ Characteristics with Process Variation Taken into Account.

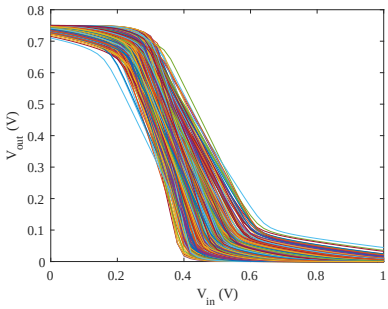

Fig. 5 Inverter DC Transfer Function Monte Carlo Simulation Results.

3 Novel Contributions of this Paper

The encryption key is generated by a PUF and is used to encrypt the end-to-end communications. The main advantage of the PUF is that the key is not stored anywhere in memory. Different types of PUF designs are available for use in the IoT [26]. An RO based PUF is used in this paper. Compared to other PUF designs, the RO PUF will be easy to manufacture. The main advantage of the proposed RO PUF in this paper over the other PUF designs is that less area is needed and with N Ring Oscillators, N bits can be obtained, unlike other designs. Hence, power consumption can be much lower for generating the same number of bits. Two different PUF designs are presented, one which can be ideal for small devices like smart-watches and another which is ideal for high

speed demanding devices like routers and network adapters. The novel contributions of this paper are the following two distinct designs:

- A novel energy-optimal hybrid oscillator arbiter PUF.
- A novel speed-optimal hybrid oscillator arbiter PUF.

The current paper is an extension of the work presented in [29]. 14nm technology FinFETS are used in the current paper in contrast to 32nm FinFETs used in [29]. The use of the 14nm technology gives an advantage in power consumption and chip area reduction and is more in line with current state-of-the-art manufacturing processes.

4 Related Prior Research

FinFETs have proven to be a promising replacement to the planar transistors with less leakage and more scalability beyond the 32 nm regimes. Now the FinFET has reached 14nm in commercially available processors and devices [19]. But one of the main issues in scaling the devices beyond 20 nm is the device to device manufacturing variations. At such small transistor sizes, there will be many factors contributing to the variations. A study of the process variation effects on sidewall roughness effects was presented in [1]. Computer Aided Design models in 3D were used for the simulation of devices and the devices were subjected to Monte Carlo variations and results were presented in [1]. To study the impact of these variations on memory devices, 6T and 10T Static Random Access Memory (SRAM) cells were designed and simulation results were presented in that paper. The impact of process variation of nanotube devices and nanowire devices is presented in [22]. A 128 Mb high density 6T SRAM was fabricated and presented in [25]. The SRAM was fabricated using the 14 nm FinFET technology and the proposed design of the SRAM shows a significant reduction in power consumption. This reduction in power consumption can be very helpful in the case of a battery operated applications. In [16], many of the circuits were subjected to Process, Voltage and Temperature (PVT) variation analysis, including memory and oscillators. For the current paper, a 15nm FinFET PDK released by NCSU [4] is used.

Different implementations of the IoT are presented in [3]. With the efficient use of cloud services, the storage and analysis of data provided by various IoT devices and sensors has become easier [11]. Implementation of an energy efficient and user friendly architecture for the health industry and the IoT were presented in [27]. A thyroid monitoring system that is dynamically optimized was proposed in that paper. The IoT is also used in surveillance. One such application is presented in [10] which proposes an architecture for secure imaging.

Many types of PUF designs are available such as reconfigurable PUF, Ring Oscillator PUF, Arbiter PUF, SRAM PUF, etc. [7,9,26]. Various architectures at nanoscale used to design a PUF are presented in [8]. An implementation of a PUF using the variability of RRAM is presented in [6] but its functionality is affected by voltage and temperature variations. A reconfigurable PUF using Ring Oscillators is presented in [14]. A new design to address aging and environmental effects affecting the PUF reliability is presented in [23]. In [2], a protocol for authenticating different devices connected in an IoT network to avoid various types of attacks is proposed. Different security problems in the IoT are described in [21]. An elliptic curve based protocol was proposed using the PUF in [28]. In that paper, the PUF was designed on an FPGA and the proposed algorithm was implemented. An elliptic curve based protocol that is secure and also fast is presented in [28].

5 Proposed Physical Unclonable Function Designs

In this section we present two novel designs of RO PUF, one being high performance and the other being low power. These are ideal for the two types of devices that are present in the IoT environment. The power optimized Hybrid Oscillator Arbiter PUF is useful in low power consuming devices where the battery capacity is limited, for example in a smart-watch. The speed optimized Hybrid Oscillator Arbiter PUF is useful where there are no constraints on power consumption and where there is a need for high speed, for example in network routers and controllers. Each of the designs is used in different domains and is ideal for the conditions that are mentioned.

5.1 Traditional Multiplexer Arbiter PUF

The Hybrid Oscillator Arbiter PUF is similar to the Arbiter Multiplexer PUF. The design of a traditional one bit arbiter PUF is shown in Fig. 6: a number of multiplexers are connected in series as presented. The output from two multiplexers is fed to the clock and input signals of a latch. The gate delays produced by the transistors will produce a time delay between the two signals. This time period variation between the signals will produce different outputs from the D flipflop. If the signal given to the clock reaches before the signal given to the input, the output will be high (1). If the signal given to the clock is slow compared to the signal given to D, the output will be low (0). The signals $X[0], \cdots, X[N]$ are the select signals (or the challenges) given to the multiplexers. However, the chip area consumed is large compared to the ring oscillator designs. The power consumed is also comparatively high. To overcome these, the two designs of Hybrid Oscillator Arbiter PUF are proposed. The main advantage of this arbiter PUF is that from a single PUF module various keys can be generated.

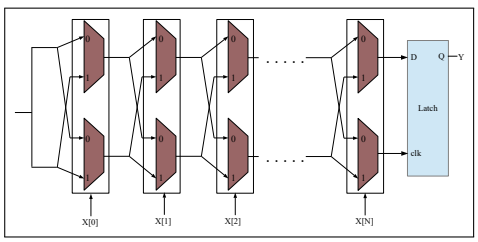

Fig. 6 One bit Arbiter PUF.

5.2 Traditional Ring Oscillator PUF Design

The design of a FinFET based traditional RO PUF is shown in Fig. 7 [15]. The ring oscillators will generate the required oscillations which are given to the inputs of a multiplexer. Due to the process variations, the frequency of the generated oscillations will be different in each of the ring oscillators. As shown in the figure, the outputs from $N/2$ oscillators are given to one multiplexer, MUX1 and the outputs from the other $N/2$ oscillators are given to the other multiplexer MUX2. At a given time, two of the different

ring oscillators are selected and the pulse signals generated are counted. The counted numbers are given to a comparator which compares the number of signals generated up to that respective point of time and gives the output accordingly as "1" or "0". A 16-bit FinFET based traditional RO PUF was implemented and its characterization was performed. The transistor sizing and results are tabulated in Table 1. The relative sizing of the transistors was made to ensure a smooth current flow through the inverters and symmetrical transfer characteristics. In a traditional RO PUF, generating the key will take time as pairs of ring oscillators are to be selected and the signals are to be given to the counter for some time to count the number of pulses generated and then compared. This lag in generation can be avoided in the proposed PUF design presented next.

Table 1 Characterization Table for Traditional PUF.

Parameter	Value	
Transistor sizes	p-Type (W:L)	n-Type(W:L)
	90nm : 20nm	45nm : 20nm
Average Power	248 μW	
Hamming Distance	50 %	
Time to generate key	150 ns (Varies with frequency of RO)	

Fig. 7 shows the design of a FinFET based traditional Ring Oscillator PUF. The ROs generate the required oscillations. The generated pulse waves, due to the manufacturing variations of the transistors, will have differences in their frequencies. N ring oscillators are used where $N/2$ ring oscillators are given to Multiplexer 1 and the other half are connected to Multiplexer 2. Two signals from each set are selected and compared with each other which gives the output 1 or 0.

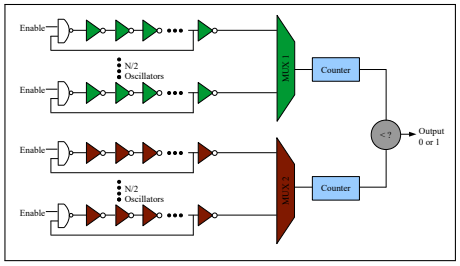

Fig. 7 Traditional RO based PUF.

The 16 bit FinFET based PUF was implemented, which requires 32 ring oscillators. To check the uniqueness and reliability of the PUF, inter-distance and intra-distance PUF challenges were performed and the Hamming distance was calculated to test the uniqueness. The inter-distance PUF of the implemented FinFET PUF is 0.500

(50%) which is the ideal Hamming distance. To calculate the inter-distance, the same challenge was given to two different PUFs and the outputs are compared. To calculate the intra-distance, the same challenge was given to the same PUF module over and over again to check any variations in the output key generated. Temperature and supply voltage fluctuations were taken into consideration to confirm that the intra-distance challenge gives out the same key.

5.3 Proposed Energy-Optimal Hybrid Oscillator Arbiter PUF

The design of the FinFET based power optimized Hybrid Oscillator Arbiter PUF is shown in Fig. 8. Like the traditional RO PUF design, the ring oscillators will generate the necessary oscillations. Due to process variations, the frequency of the generated oscillations will be different in each of the ring oscillators. In this case, to conserve energy and create a low power environment, a multiplexer is employed. As in the traditional RO PUF design, $N/2$ ring oscillators are given as inputs to multiplexer MUX1. The other half are given to the other multiplexer MUX2. The output from MUX1 is given as the input to the D flipflop. The output from MUX2 is given as the clock signal to the D flipflop. Depending on the different frequencies of ring oscillators, the output will be "1" or "0". In this case, to obtain the key will take more time than the speed optimized Hybrid Oscillator Arbiter PUF as pairs of ROs are selected and given to the D flipflop. The power optimized Hybrid Oscillator Arbiter PUF is characterized and the values are tabulated in Table 2.

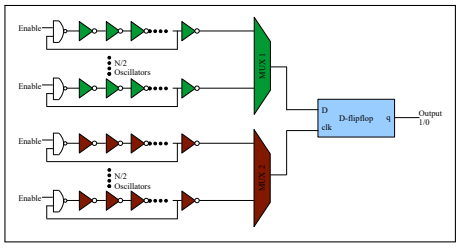

Fig. 8 Novel Power Optimized Hybrid Oscillator Arbiter PUF.

Table 2 Characterization Table for Power Optimized Hybrid Oscillator Arbiter PUF.

Parameters	Values	
Transistor sizes	p-Type (W:L)	n-Type(W:L)
	90n : 20n	45n : 20n
Average Power	219.34 μW	
Hamming Distance	48.51 %	
Time to generate key	150 ns (Varies with frequency of RO)	

5.4 Proposed Speed-Optimal Optimized Hybrid Oscillator Arbiter PUF

The design of the FinFET speed optimized Hybrid Oscillator Arbiter PUF is shown in Fig. 9. Due to process variations, the frequency of the generated oscillations will be different in each ring oscillator. In this design, the signals generated by the RO are not given to the multiplexers, but are given to the D-input and clock signal input of the D flipflop. In this case, the design may become complex compared to the previous designs due to the routing that should be followed. The signal of one RO is given as D-input and the signal from another RO is given as a clock to the same D flipflop. Depending on the frequencies of the two RO signals, the output bit will be "1" or "0". The output bits are taken after a time period of 50ns in this experiment. To achieve more bits from the same design, two outputs can be taken from the flipflop outputs, Q and $\bar{Q}$. In such a configuration, for N different ring oscillators, an N-bit key can be obtained.

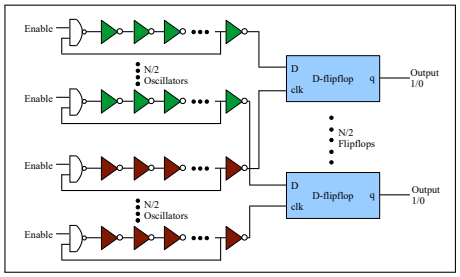

Fig. 9 Novel Speed Optimized Hybrid Oscillator Arbiter PUF.

6 FinFET Based Design of the Physical Unclonable Functions

In the multiplexer arbiter PUF design, the gate delay of the multiplexers produces a time delay for the signals reaching the latch at the end. Similar to this, in the design of the Hybrid Oscillator Arbiter PUF, two ring oscillators are connected to the input and the clock of the D flipflop. Due to the process variation in the manufacturing of the transistors, the oscillations produced will be of different frequencies. Hence, as presented in the traditional arbiter PUF, the variation in the time period of signals reaching the D flipflop will produce the different output keys.

Fig.10 shows the design of one bit of the FinFET based Hybrid Oscillator Arbiter PUF. It is similar to the Multiplexer Arbiter PUF shown in Fig. 6 presented in Section 5.1. In the presented design, the environmental changes will affect the output key generation. A single bit change can affect the encryption and decryption of data and hence the entire communication. Hence a current starved design of the ring oscillator is chosen to compensate for temperature variations. The traditional RO PUF and the Hybrid Oscillator Arbiter PUF were subjected to 100 runs of Monte Carlo variations. All geometric parameters are varied with a variation (standard deviation) of 5% over the nominal values. The nominal values are presented in Table. 3. The parameters that were varied are height and width of the transistors, oxide thickness of p-type and n-type transistors, supply voltage, and threshold voltages of both the transistors.

A temperature variation was also performed to simulate the real-time environmental effects that the device can experience.

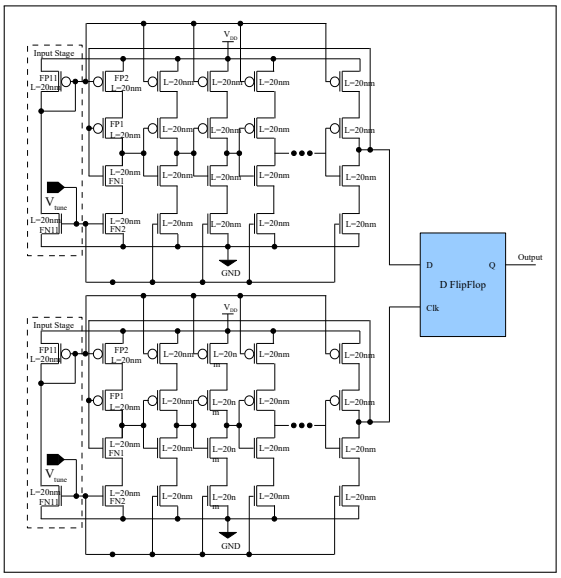

Fig. 10 One bit FinFET Based Hybrid Oscillator Arbiter PUF.

Table 3 Nominal values for the FinFET device parameters.

Parameter	Nominal Value
pFET Length	20 nm
pFET Width	90 nm
nFET Length	20 nm
nFET Width	45nm
pFET Fin Width	10 nm
nFET Fin Width	10 nm
pFET Fin Thickness	10 nm
nFET Fin Thickness	10 nm
pFET Fin Height	23 nm
nFET Fin Height	23 nm
Supply Voltage	0.9V

7 Experimental Results

15 nm FinFET models are used for simulations in this paper. The NCSU PDK is used for all simulations [4]. The models were developed as industry standard compact

models. The n-Type FinFET is subjected to Monte Carlo variation to simulate the manufacturing variations by varying the geometric parameters. Table. 3 shows the nominal values taken for the simulations. All the parameters are subjected to a 5% variation.

Table 1, Table 2 and Table 4 present the transistor sizes used to design the RO and the respective results obtained. Two figures of merit were considered: Time Period and Average Power. Time Period is the total time taken by the circuit to generate the key. Average power is taken as the sum of dynamic power and leakage power of the transistors. For simulation purposes, the ring oscillators used are the same for all three configurations: Traditional, Power Optimized and Speed Optimized PUF. 32 different ring oscillators are used to generate a 16 bit key in the case of the traditional RO PUF and a 32 bit key in both cases of Hybrid Oscillator Multiplexer based PUF. 100 Monte Carlo runs are performed on the circuit and the frequencies of different ring oscillators are calculated. Fig. 11 represents the frequencies of the ring oscillators in the 100 different runs. Temperature was varied from 24°C to 30°C and the mean supply voltage of 0.9 V was considered with a 10% standard deviation, which is representative of on-chip power supply tolerances.

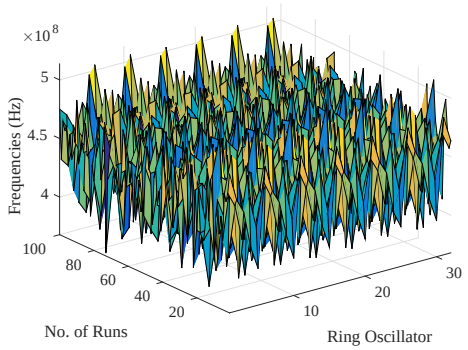

Fig. 11 Ring Oscillator Frequencies of 100 Different PUFs.

The geometric parameters are taken with a 10% variance. The mean values are the nominal values of the specific technology. The main parameters that were considered for variation were Width and Height of the fin and the oxide thickness. Along with these parameters, the temperature variation and also supply voltage variation was also considered in each of the cases. The quality of a PUF can be estimated using three factors: Uniqueness, Reliability and Attack Resilience.

7.1 Uniqueness

Uniqueness of a PUF is the ability of producing a unique key different from the other devices. In the proposed design, the output bit completely depends upon the frequencies of the Ring Oscillators. Fig. 11 is the surface plot representing the frequency variation of each of the 32 Ring Oscillators across 100 Monte Carlo Runs. From this plot, the uniqueness of different frequencies can be clearly shown. Hence all the signals reaching each of the D flipflops in the proposed design reach at different time periods.

After the bits are generated, the Hamming distance between different keys is calculated. The ideal Hamming distance for a key to be unique is 0.5 (50%). Figure 12 shows the distribution of Hamming distances of the Power Optimized Hybrid Oscillator Multiplexer based PUF which has a distribution from 40% to 58% with an average Hamming distance of 48.51%. The Speed Optimized Hybrid Oscillator Multiplexer based PUF has a distribution from 40% to 60% with an average Hamming distance of 49.60%. The Hamming distance distribution of Speed Optimized Hybrid Oscillator Multiplexer based PUF is shown in Fig. 13.

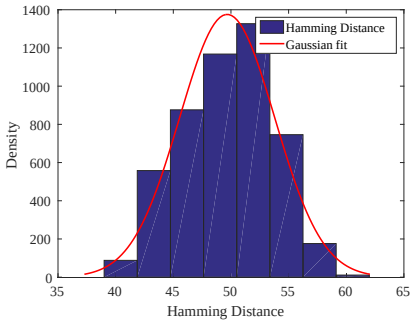

Fig. 12 Distribution of intra-PUF Hamming Distance of Power Optimized Hybrid Oscillator Arbiter PUF.

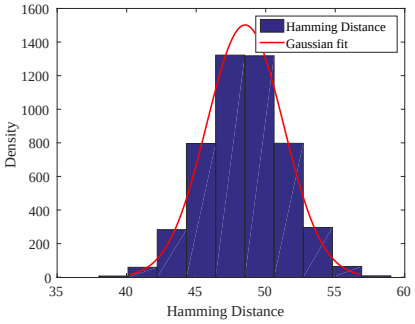

Fig. 13 Distribution of inter-PUF Hamming Distance of Speed Optimized Hybrid Oscillator Arbiter PUF.

7.2 Reliability

Reliability is the ability of a PUF to generate the same key again over a period of time resisting the temperature and supply voltage variations. In the IoT environment, for successful communication between the devices, the reliability of the PUF key generated is of high importance. Fig. 14 shows the distribution of Hamming distance with temperature and supply voltage variations. The Hamming distance was varied from 0.8%

to 4.3% with a mean of 2.5%. This reliability can still be increased by employing different Ring Oscillator designs such as temperature resistant RO, and a reconfigurable PUF design.

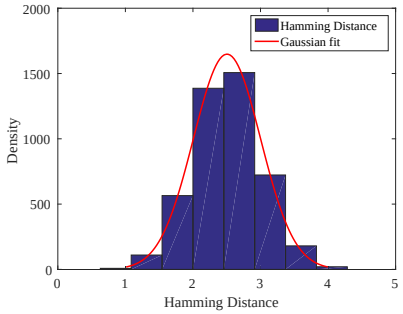

Fig. 14 Distribution of intra-PUF Hamming Distance of Hybrid Oscillator Arbiter PUF.

7.3 Randomness

Randomness is another parameter for the validation of a CRP generated using PUFs. In the key generated by a PUF module, the number of 0s and 1s should be equal and only then the key is said to be secure. For both Speed Optimized and Power Optimized Hybrid Oscillator Arbiter PUFs, the randomness is measured and presented in Fig. 15.

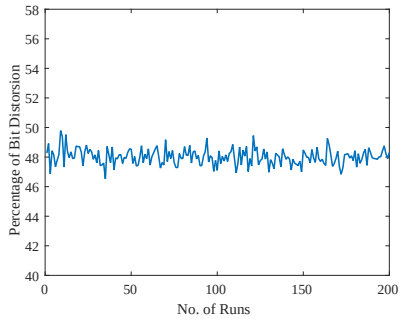

Fig. 15 Randomness of Hybrid Oscillator Arbiter PUF.

7.4 Figures Of Merit Comparison

Two Figures of Merit (FoMs) are considered, the Average Power and Time Period. Both FoMs are calculated for each of the three designs and presented in Tables 1, 2, and 4. The Traditional RO PUF design consumes more power than the Power Optimized Hybrid Oscillator Arbiter PUF. But the time consumed for the generation of the key

is also longer for the Traditional PUF than the Power Optimized Hybrid Oscillator Arbiter PUF. In traditional PUFs, more time is taken for the calculation of frequency of the different ring oscillators and this can be compensated by the proposed design. In the Speed Optimized Hybrid Oscillator Arbiter PUF, trading off the power consumption, $N/2$ D flipflops are employed to generate the key much faster.The increase in Average Power compared to the traditional PUF is 3.25%. But the time period is much smaller comparatively as the multiplexer is removed from the design. The maximum time taken is 50 nm.

Table 4 Characterization Table for Speed Optimized Hybrid Oscillator Arbiter PUF.

Parameters	Values	
Transistor sizes	p-Type (W:L)	n-Type(W:L)
	90n : 20n	45n : 20n
Average Power	250.15 μW	
Hamming Distance	49.6 %	
Time to generate key	50 ns (Varies with frequency of RO)	

7.5 Comparison of Traditional and Hybrid PUFs

Table 5 gives a comparison of the experimental results of all three different designs of PUFs, Traditional RO PUF, Speed Optimized Hybrid Oscillator Arbiter PUF and Power Optimized Hybrid Oscillator Arbiter PUF. Replacing the counter and the comparator in the traditional RO PUF with a D flipflop will conserve energy. An Average Power consumption reduction of 11% is observed by using the Power Optimized Hybrid Oscillator Arbiter PUF. The generation of the PUF key will take the same time as that of the traditional design. The key can be generated much faster by removing the multiplexer and increasing the number of D flipflops. This will increase the average power consumption. With almost no increase in power consumption compared to the traditional design the key generation is much faster. Table 6 presents a comparison of the presented work with research presented elsewhere. The architectures of the compared works are mostly Ring Oscillator based but the technology used differs. Use of 15nm FinFET with the current architecture of PUF makes it much more robust in generating the keys and also consumes less power which can be observed from Table 5. It should be pointed out that a direct comparison between presented designs is not possible due to the different technologies, process nodes and architectures used. However, the reported Hamming distance is a good indicator of the competitiveness of the current design. Furthermore, its 15nm FinFET implementation is state-of-the-art and guaranteed to provide the smallest power consumption.

Table 5 Comparison of Figures of Merit for different PUF Designs.

Characteristics	Estimated Values		
PUF Design	Traditional RO PUF	Speed Optimized Hybrid Oscillator Arbiter PUF	Power Optimized Hybrid Oscillator Arbiter PUF
Average Power	248 μW	250.15 μW	219.34 μW
Hamming Distance	50%	49.6%	48.51%
Average Time to Generate Key	150 ns	150 ns	50 ns

Table 6 Comparison of Results with Related Existing Research.

Research Works	Technology	Architecture Used	Average Power Consumed	Hamming Distance (%)
Rahman, et al. [23]	90 nm CMOS		–	50
Maiti, et al. [15]	180 nm CMOS	Ring Oscillator	–	50.72
S. R. Sahoo, et al. [24]	90 nm CMOS	Ring Oscillator	–	45.78 %
Maiti et al. [13]	–	–	–	47.31
This paper (Speed Optimized)	14 nm	Current Starved Ring Oscillator	250.15 μW	49.6
This Paper (Power Optimized)	14 nm	Current Starved Ring Oscillator	219.34I μW	48.51

8 Conclusion and Future Research

Two novel designs of Hybrid Oscillator Multiplexer based PUFs are presented in this paper, one Power Optimized and the other Speed Optimized. The Power Optimized Hybrid Oscillator Arbiter PUF generates the key trading off the speed with an 11% decrease in power consumption compared to the traditional RO PUF. The Speed Optimized Hybrid Oscillator Arbiter PUF generates the key much faster compared to the Traditional RO PUF design with a 3.25% increase in power consumption. Both designs can be used in two different types of devices in an IoT environment, low power consuming devices and high power consuming, performance-oriented devices.

As a future research, hardware based encryption and decryption architectures will be implemented to increase the security of communication between devices. Optimization will be performed on the designed hardware for the overall low power consumption [18]. Different Ring Oscillator designs will be employed to improve the stability and temperature and voltage variation resilience. Side channel leakage resilient PUF design can also be explored in future.

Acknowledgments

The current paper is based on a previous conference presentation [29]. The current paper utilizes a 15nm FinFET PDK in contrast to the previous presentation which used a 32nm FinFET model for the design.

References

1. Agrawal, N., Liu, H., Arghavani, R., Narayanan, V., Datta, S.: Impact of Variation in Nanoscale Silicon and Non-Silicon FinFETs and Tunnel FETs on Device and SRAM Performance. IEEE Transactions on Electron Devices 62(6), 1691–1697 (2015). DOI 10.1109/TED.2015.2406333
2. Aman, M.N., Chua, K.C., Sikdar, B.: Physical Unclonable Functions for IoT Security. In: Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security, pp. 10–13 (2016)
3. Atzoria, L., Ierab, A., Morabito, G.: The internet of things: A survey. Elsevier Computer Networks 54(15), 2787вЃ'Y2805 (2010). DOI 10.1016/j.comnet.2010.05.010
4. Bhanushali, K., Davis, W.R.: FreePDK15: An Open-Source Predictive Propcess Design Kit for 15nm FinFET Technology. In: Proceedings of the 15th International Symposium on Physical Desing (ISPD), pp. 165–170 (2015)
5. Bohr, M.T., Chau, R.S., Ghani, T., Mistry, K.: The High-κ Solution. IEEE Spectrum 10(10), 29–35 (2007)
6. Chen, A.: Utilizing the Variability of Resistive Random Access Memory to Implement Reconfigurable Physical Unclonable Functions. IEEE Electron Device Letters 36(2), 138–140 (2015)
7. Clavier, C., Gaj, K.: Cryptographic Hardware and Embedded Systems. Springer (2009). DOI 978-3-642-04137-2
8. Gao, Y., Ranasinghe, D.C., Al-Sarawi, S.F., Kavehei, O., Abbott, D.: Emerging Physical Unclonable Functions With Nanotechnology. IEEE Access 4, 61–80 (2016). DOI 10.1109/ACCESS.2015.2503432
9. Hori, Y., Yoshida, T., Katashita, T., Satoh, A.: Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs. In: Proceedings of the International Conference on Reconfigurable Computing and FPGAs, pp. 298–303 (2010)
10. Kougianos, E., Mohanty, S.P., Coelho, G., Albalawi, U., Sundaravadivel, P.: Design of a High-Performance System for Secure Image Communication in the Internet of Things. IEEE Access 4, 1222–1242 (2016). DOI 10.1109/ACCESS.2016.2542800
11. Kovatsch, M., Lanter, M., Shelby, Z.: Californium: Scalable cloud services for the internet of things with coap. In: Proceedings of the 2014 International Conference on the Internet of Things (IOT), pp. 1–6 (2014). DOI 10.1109/IOT.2014.7030106
12. Lammers, D.: Moore's Law Milestones. IEEE Spectrum (2015)
13. Maiti, A., Casarona, J., McHale, L., Schaumont, P.: A large scale characterization of RO-PUF. In: Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 94–99 (2010)
14. Maiti, A., Schaumont, P.: Improving The Quality of a Physical Unclonable Function using Configurable Ring Oscillators. In: Proceedings of the International Conference on Field Programmable Logic and Applications, pp. 703–707 (2009)
15. Maiti, A., Schaumont, P.: Improved Ring Oscillator PUF: An FPGA-friendly Secure Primitive. Journal of Cryptography 24(2), 375–397 (2010). DOI 10.1007/s00145-010-9088-4
16. Mohanty, S.P.: Nanoelectronic Mixed-Signal System Design. 9780071825719. McGraw-Hill Education (2015)
17. Mohanty, S.P., Choppali, U., Kougianos, E.: Everything You wanted to Know about Smart Cities. IEEE Consumer Electronics Magazine 5(3), 60–70 (2016). DOI 10.1109/MCE.2016.2556879
18. Mohanty, S.P., Ranganathan, N., Chappidi, S.K.: Peak Power Minimization Through Datapath Scheduling. In: Proceedings of the IEEE Computer Society Annual Symposium on VLSI, pp. 121–126 (2003)
19. Natarajan, S., Agostinelli, M., Akbar, S., Bost, M., Bowonder, A., Chikarmane, V., Chouksey, S., Dasgupta, A., Fischer, K., Fu, Q., Ghani, T., Giles, M., Govindaraju, S., Grover, R., Han, W., Hanken, D., Haralson, E., Haran, M., Heckscher, M., Heussner, R., Jain, P., James, R., Jhaveri, R., Jin, I., Kam, H., Karl, E., Kenyon, C., Liu, M., Luo, Y., Mehandru, R., Morarka, S., Neiberg, L., Packan, P., Paliwal, A., Parker, C., Patel, P., Patel, R., Pelto, C., Pipes, L., Plekhanov, P., Prince, M., Rajamani, S., Sandford, J., Sell, B., Sivakumar, S., Smith, P., Song, B., Tone, K., Troeger, T., Wiedemer, J., Yang, M., Zhang, K.: A 14nm Logic Technology Featuring 2nd-Generation FinFET Transistors, Air-Gapped Interconnects, Self-Aligned Double Patterning and a 0.0588 m2 SRAM cell size. In: Proceedings of the 2014 IEEE International Electron Devices Meeting, pp. 3.7.1–3.7.3 (2014). DOI 10.1109/IEDM.2014.7046976

20. National Intelligence Council: Six Technologies with Potential Impacts on US Interests out to 2025. Disruptive Civil Technologies (2008)
21. O'Neill, M.: Insecurity by Design: Today's IoT Device Security Problem. Engineering 2(1), 48–49 (2016)
22. Paul, B.C., Fujita, S., Okajima, M., Lee, T., Wong, H.S.P., Nishi, Y.: Impact of Process Variation on Nanowire and Nanotube Device Performance. In: Proceedings of the 2007 65th Annual Device Research Conference, pp. 269–270 (2007). DOI 10.1109/DRC.2007.4373749
23. Rahman, M.T., Forte, D., Fahrny, J., Tehranipoor, M.: ARO-PUF: An Aging-Resistant Ring Oscillator PUF Design. In: Proceedings of the Design, Automation Test in Europe Conference Exhibition (DATE), pp. 1–6 (2014)
24. Sahoo, S.R., Kumar, S., Mahapatra, K.: A Modified Configurable RO PUF with Improved Security Metrics. In: Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems, pp. 320–324 (2016). DOI 10.1109/iNIS.2015.37
25. Song, T., Rim, W., Jung, J., Yang, G., Park, J., Park, S., Kim, Y., Baek, K.H., Baek, S., Oh, S.K., Jung, J., Kim, S., Kim, G., Kim, J., Lee, Y., Sim, S.P., Yoon, J.S., Choi, K.M., Won, H., Park, J.: A 14 nm finfet 128 mb sram with V_{MIN} enhancement techniques for low-power applications. IEEE Journal of Solid-State Circuits 50(1), 158–169 (2015). DOI 10.1109/JSSC.2014.2362842
26. Suh, G.E., Devadas, S.: Physical unclonable functions for device authentication and secret key generation. In: Proceedings of the 44th ACM/IEEE Design Automation Conference, pp. 9–14 (2007)
27. Sundaravadivel, P., Mohanty, S.P., Kougianos, E., Albalawi, U.: 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), pp. 1–4 (2016). DOI 10.1109/EuroSimE.2016.7463377
28. Wallrabenstein, J.R.: Practical and Secure IoT Device Authentication Using Physical Unclonable Functions. In: Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 99–106 (2016). DOI 10.1109/FiCloud.2016.22
29. Yanambaka, V.P., Mohanty, S.P., Kougianos, E.: 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), pp. 172–177 (2016)