Novel FinFET based Physical Unclonable Functions for Efficient Security Integration in the IoT

Venkata P. Yanambaka*, Saraju P. Mohanty†, Elias Kougianos‡
Nano Systems Design Laboratory (NSDL, http://nsdl.cse.unt.edu), Computer Science and Engineering
University Of North Texas, Denton, TX 76207, USA.
Email: *venkataprasanthyanambaka@my.unt.edu, †saraju.mohanty@unt.edu, ‡elias.kougianos@unt.edu

***Abstract*—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 the communication 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. Two different designs of a Ring Oscillator (RO) PUF are introduced, one with low power consumption trading off device performance and one with high performance trading off device power consumption. There is a 10% decrease in power with the low power model along with a simple design and fabrication. With a trade off of 3.25% of power consumption, the performance of the device can be improved.**

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

I. Introduction

The Internet of Things (IoT) is considered as one of the six most "Disruptive Civil Technologies" by the US National Intelligence Council [1]. The IoT in a home environment is considered in this paper. The IoT mainly describes an environment where all smart devices are able to talk to one another [2]. Fig.1 presents an example of the IoT actively working in a home. The IoT has become one of the main focus of research because of the numerous advantages it has and the major impact it can have on quality of life [3], [4].

In the near future, all devices at home will be communicating with each other, and people will control all the components in a house with their mobile phones. Unauthorized access to such a network will put that home in danger [5]. One of the solutions to this problem is to encrypt the end to end communication between devices. This paper examines the communication among devices present in the specific network with the use of Physical Unclonable Functions (PUFs) to ensure security.

Novel Contributions of this Paper: The encryption key is generated by a PUF which is used to encrypt the communications end to end. The main advantage of the PUF is that the key is not stored anywhere in the memory. Different types of PUF designs are available for use in the IoT [6]. An RO based PUF is used in this paper. Two different PUF designs are presented, one of which can be ideal for small devices like smart-watches and the other 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 rest of this paper is organized as follows: Section II presents related research in this field, Section IV presents the design of a one bit hybrid oscillator based arbiter PUF. Section III presents the proposed designs of Ring Oscillator (RO) PUFs. Section VI concludes the paper and presents suggestions for future research.

II. Related Prior Research

The IoT is the main focus of research for many researchers and numerous applications are being introduced every year. Different implementations of IoT are presented in [3]. A clear survey fo IoT has been performed in [3]. [7] uses the IoT and implements an energy efficient and user friendly architecture for the health industry. A thyroid monitoring system that is dynamically optimized was proposed in that paper. The IoT is also used in surveillance activity. One such application is presented in [8] which presents an architecture for secure imaging.

Security in the IoT using PUFs is already being investigated. Many types of PUF designs are available such as reconfigurable PUF, Ring Oscillator PUF, Arbiter PUF SRAM

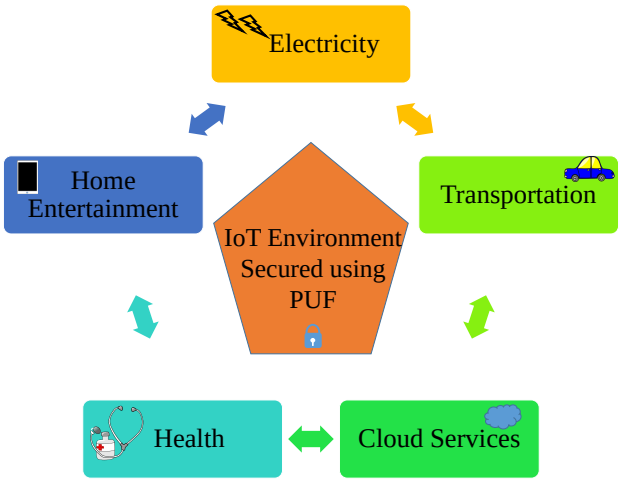

Fig. 1. Internet of Things at home.

PUF, etc. [9], [10], [6]. [11] presents an implementation of PUF using the variability of RRAM but its functionality is affected by voltage and temperature variations. [12] presents a reconfigurable PUF using Ring Oscillators. [13] proposed a new design to address the aging and the environmental effects affecting the PUF reliability. [14] proposes a protocol for authenticating different devices connected in an IoT network to avoid various types of attacks. Different Security problems in IoT are described in [15].

III. 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.

A. Traditional Multiplexer Arbiter PUF

The design of a traditional one bit arbiter PUF is shown in Fig. 2: 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 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 faster than 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. But the chip area consumed is high compared to the ring oscillators. The power consumed is also comparatively high. To overcome these, the two designs of Hybrid Oscillator Arbiter PUF are proposed.

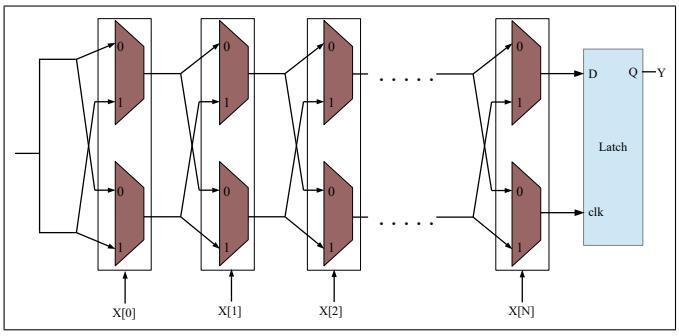

Fig. 2. One bit Arbiter PUF.

B. Traditional Ring Oscillator PUF Design

The design of a FinFET based traditional RO PUF is shown in Fig. 3 [16]. 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 oscillator. As shown in the figure, the output from $\frac{N}{2}$ oscillators are given to one multiplexer, MUX1 and the output from $\frac{N}{2}$ 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 results are tabulated in Table II. 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.

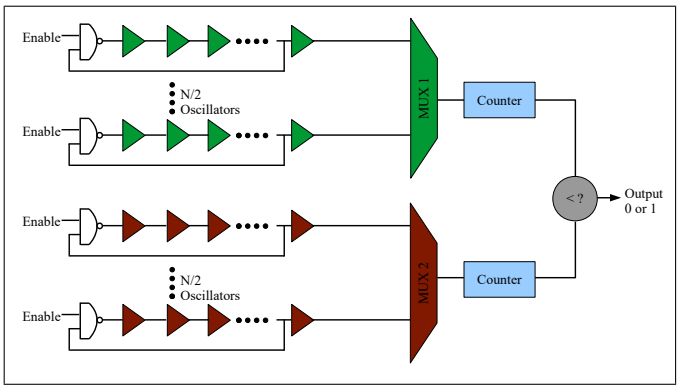

Fig. 3. Traditional RO based PUF.

C. Proposed Energy-Optimal Hybrid Oscillator Arbiter PUF

The design of the FinFET based Power Optimized Hybrid Oscillator Arbiter PUF is shown in Fig. 4. 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, $\frac{N}{2}$ ring oscillators are given as inputs to the multiplexer MUX1. The other half of ring oscillators 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 III.

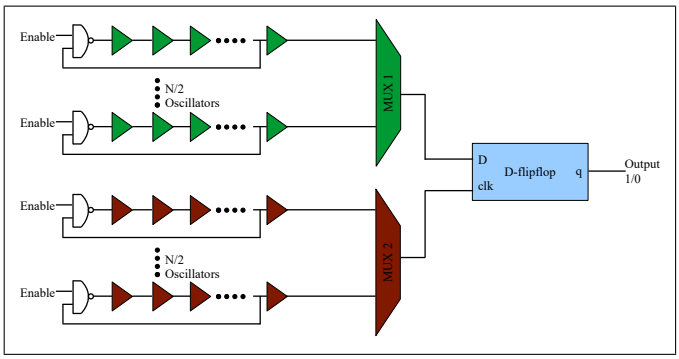

Fig. 4. Novel Power Optimized Hybrid Oscillator Arbiter PUF.

IV. FinFET Based Design of the Physical Unclonable Functions

A double gate FinFET is used to design the traditional RO PUF and both the novel Hybrid Oscillator Arbiter PUFs for a fair comparison. Fig.5 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. 2 presented in Section III-A. 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 the geometric parameters are varied with a variation (standard deviation) of 10% over nominal. 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. Table I shows the nominal values of the parameters that were considered.

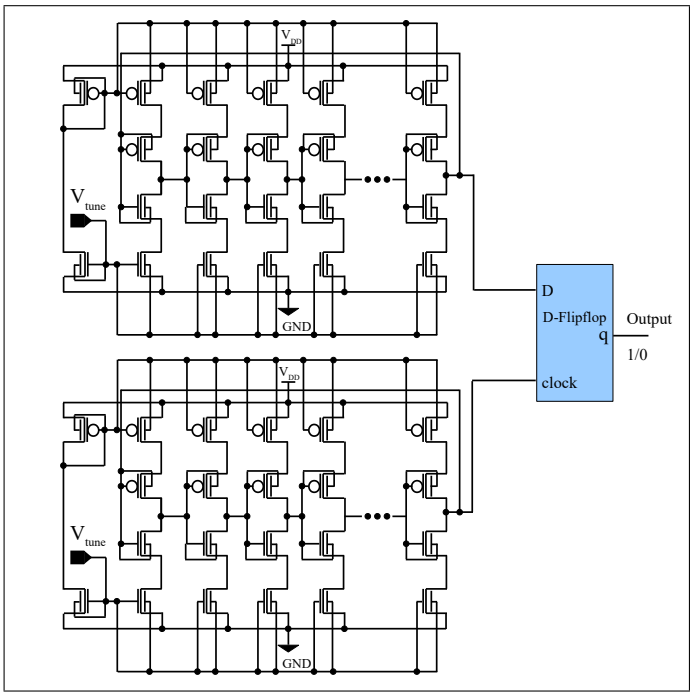

Fig. 5. One bit FinFET Based Hybrid Oscillator Arbiter PUF.

TABLE I. Nominal values for the FinFET device parameters.

Parameter	Nominal Value
pFET Length	32n
nFET Width	240n
nFET Length	32n
pFET Width	12n
pFET Threshold Voltage	-250mV
nFET Threshold Voltage	310mV
pFET Oxide Thickness	1.65n
nFET Oxide Thickness	1.75n
Supply Voltage	0.9V

A. Proposed Speed-Optimal Optimized Hybrid Oscillator Arbiter PUF

The design of FinFET Speed Optimized Hybrid Oscillator Arbiter PUF is shown in Fig. 6. Due to process variations, the frequency of the generated oscillations will be different in each of the 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.

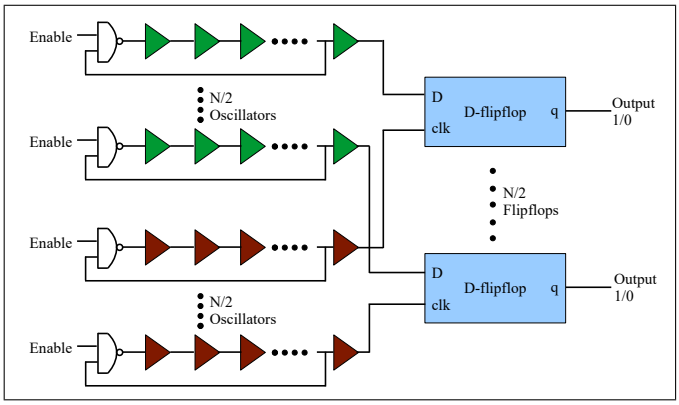

Fig. 6. Novel Speed Optimized Hybrid Oscillator Arbiter PUF.

V. Experimental Results

Table II, Table III and Table IV present the transistor sizes used to design the RO and the respective results obtained. Two figures of merits were considered, Time Period and the 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 the 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 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. 7 represents the frequencies of ring oscillators in all 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. The quality of a PUF can be estimated using three factors: Uniqueness, Reliability and Attack Resilience.

A. 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. 7 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.

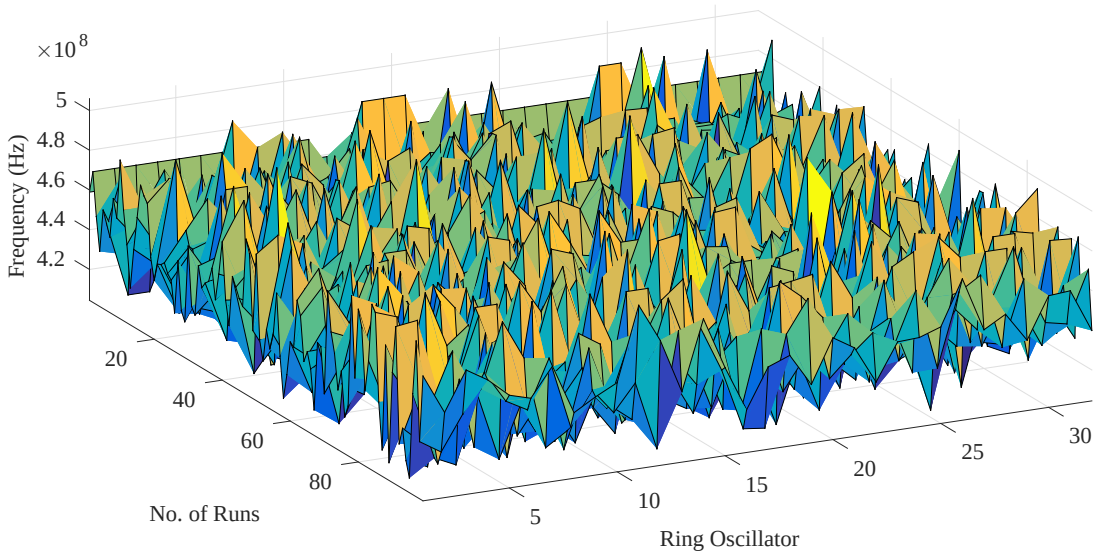

Fig. 7. Ring Oscillator Frequencies of 100 Different PUFs.

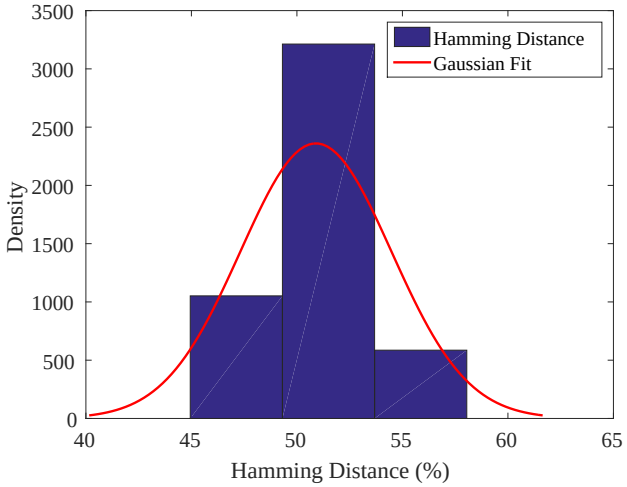

Fig. 8. Distribution of intra-PUF Hamming Distance of Power Optimized Hybrid Oscillator Arbiter PUF.

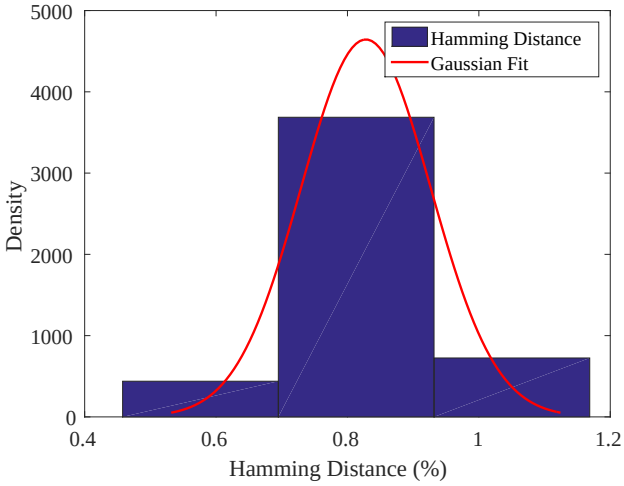

Fig. 9. Distribution of intra-PUF Hamming Distance of Hybrid Oscillator Arbiter PUF.

Figure 8 shows the distribution of Hamming distances of the Power Optimized Hybrid Oscillator Multiplexer based PUF which has a distribution from 44% to 58% with an average Hamming distance of 50.9%. The Speed Optimized Hybrid Oscillator Multiplexer based PUF has a distribution from 45% to 55% with an average Hamming distance of 52% (histogram not shown due to lack of space).

B. Reliability

Fig. 9 shows the distribution of Hamming distance with temperature and supply voltage variations. The Hamming distance was varied from 0.4% to 1.18% with a mean of 0.79%. This reliability can still be increased by employing different Ring Oscillator designs like Temperature resistant RO, and a reconfigurable PUF design.

C. Attack Resilience

The attack resilience of the PUF is the main idea in this paper. The only way an attacker is going to decode the communication is by knowing the private key. The only way to get the private key is to know the frequencies of Ring Oscillators and the different pair configuration in which they are connected to the D-Flipflop. The only way this is possible is to have access to the device itself. An attacker outside the home getting access to different devices in a home is unlikely to happen. Hence the attack resilience of this proposed PUF is high.

D. Figures Of Merit Comparison

Two Figures of Merit are considered, the Average Power and Time Period. Both FoMs are calculated for each of the three designs and presented in Tables II, III, IV and Figures 10, 11, 12. The Traditional RO PUF design consumes more power than the Power Optimized Hybrid Oscillator Arbiter

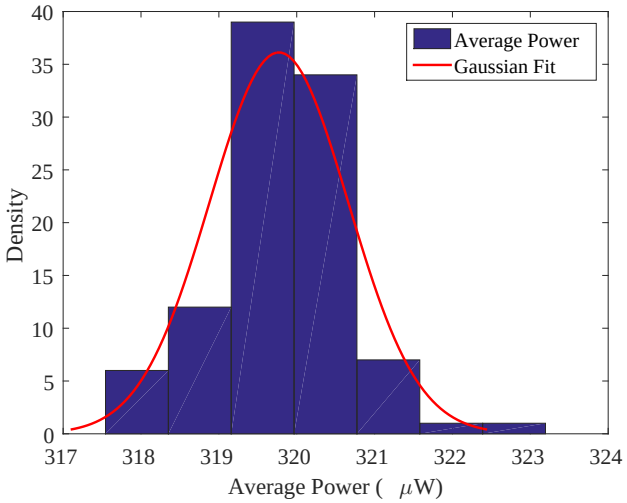

Fig. 10. Distribution of Average Power of Traditional RO PUF.

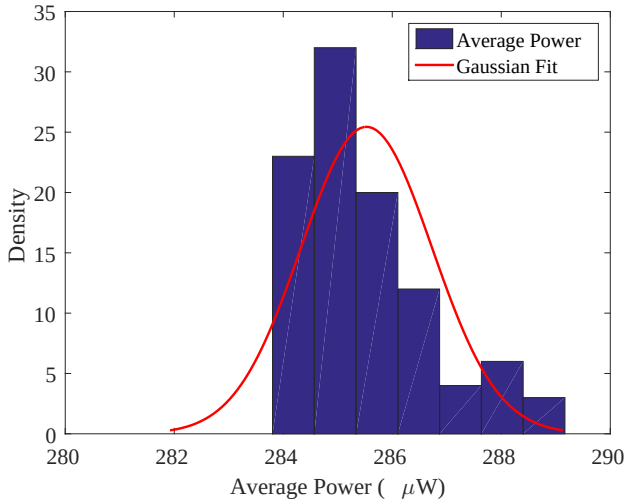

Fig. 11. Distribution of Average Power of Power Optimized Hybrid Oscillator Arbiter PUF.

PUF. But the time consumed for the generation of key is also more for the Traditional PUF than the Power Optimized Hybrid Oscillator Arbiter PUF.

TABLE II. CHARACTERIZATION TABLE FOR TRADITIONAL PUF.

Parameter	Value	
Transistor sizes	p-Type (W:L)	n-Type(W:L)
	120n : 32n	240n : 32n
Average Power	310.8 μW	
Hamming Distance	50 %	
Time to generate key	150 ns (Varies with frequency of RO)	

TABLE III. CHARACTERIZATION TABLE FOR POWER OPTIMIZED HYBRID OSCILLATOR ARBITER PUF.

Parameters	Values	
Transistor sizes	p-Type (W:L)	n-Type(W:L)
	120n : 32n	240n : 32n
Average Power	285.5 μW	
Hamming Distance	50.9 %	
Time to generate key	50 ns (Varies with frequency of RO)	

TABLE IV. CHARACTERIZATION TABLE FOR SPEED OPTIMIZED HYBRID OSCILLATOR ARBITER PUF.

Parameters	Values	
Transistor sizes	p-Type (W:L)	n-Type(W:L)
	120n : 32n	240n : 32n
Average Power	320 μW	
Hamming Distance	52 %	
Time to generate key	100 ns (Varies with frequency of RO)	

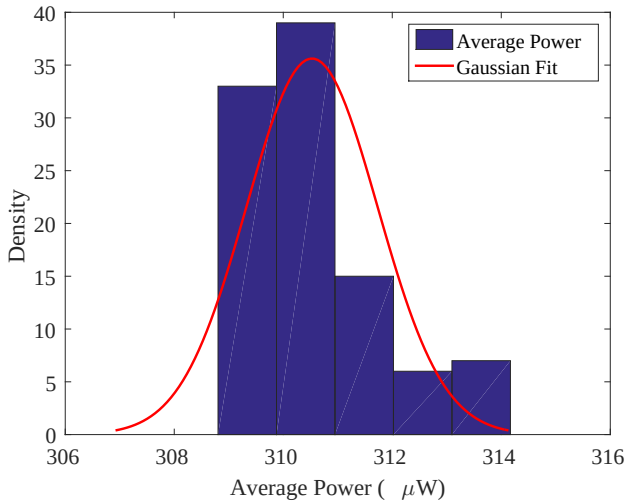

Fig. 12. Distribution of Average Power of Speed Optimized Hybrid Oscillator Arbiter PUF.

E. Comparison of Traditional and Hybrid PUFs

Table V gives a comparison of the experimental results of all the 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 a lot of energy. A total of around 10% Average Power consumption is reduced by using the Power Optimized Hybrid Oscillator Arbiter PUF. Generation of 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. A trade off of 3.25% is made in power consumption compared to the traditional design but the key generation is much faster. Table VI presents the comparison of the presented work with research presented elsewhere.

TABLE V. COMPARISON OF FIGURE OF MERITS 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	310.8 μW	320 μW	285.5 μW
Hamming Distance	50%	52%	50.9%
Average Time to Generate Key	150 ns	50 ns	150 ns

TABLE VI. COMPARISON OF RESULTS WITH OTHER PUBLICATIONS.

Research Work	Technology	Average Power Consumed	Hamming Distance (%)
Rahman et al. [13]	90 nm	–	50
Maiti [16]	180 nm	–	50.72
Suh [6]	–	–	46.15
Maiti et al. [17]	–	–	47.31
This paper	32 nm	285.5 μW	50.9
This Paper	32 nm	320 μW	52

VI. CONCLUSION AND FUTURE RESEARCH

Two novel designs of Hybrid Oscillator Multiplexer based PUFs Functions 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 a 10% 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 these designs can be used in two different types of devices in an IoT environment, low power consuming devices and the 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.

REFERENCES

[1] National Intelligence Council, "Six technologies with potential impacts on us interests out to 2025," *Disruptive Civil Technologies*, 2008.

[2] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities," *IEEE Consumer Electronics Magazine*, vol. 5, no. 3, pp. 60–70, July 2016.

[3] L. Atzoria, A. Ierab, and G. Morabito, "The internet of things: A survey," *Elsevier Computer Networks*, vol. 54, no. 15, p. 27872805, October 2010.

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

[5] N. Sklavos, *Securing Communication Devices via Physical Unclonable Functions (PUFs)*. Wiesbaden: Springer Fachmedien Wiesbaden, 2013, pp. 253–261.

[6] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *44th ACM/IEEE Design Automation Conference*, June 2007, pp. 9–14.

[7] P. Sundaravadivel, S. P. Mohanty, E. Kougianos, and U. Albalawi, "An energy efficient sensor for thyroid monitoring through the iot," in *17th International Conference on Thermal, Mechanical and Multi-Physics Simulation and Experiments in Microelectronics and Microsystems (EuroSimE)*, 2016, pp. 1–4.

[8] E. Kougianos, S. P. Mohanty, G. Coelho, U. Albalawi, and P. Sundaravadivel, "Design of a high-performance system for secure image communication in the internet of things," *IEEE Access*, vol. 4, pp. 1222–1242, 2016.

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

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

[11] A. Chen, "Utilizing the Variability of Resistive Random Access Memory to Implement Reconfigurable Physical Unclonable Functions," *IEEE Electron Device Letters*, vol. 36, no. 2, pp. 138–140, Feb 2015.

[12] A. Maiti and P. Schaumont, "Improving The Quality of a Physical Unclonable Function using Configurable Ring Oscillators," in *Proceedings of the International Conference on Field Programmable Logic and Applications*, 2009, pp. 703–707.

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

[14] M. N. Aman, K. C. Chua, and B. Sikdar, "Physical Unclonable Functions for IoT Security," in *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*, 2016, pp. 10–13.

[15] M. O'Neill, "Insecurity by Design: Today's IoT Device Security Problem," *Engineering*, vol. 2, no. 1, pp. 48–49, 2016.

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

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

[18] S. P. Mohanty, N. Ranganathan, and S. K. Chappidi, "Peak Power Minimization Through Datapath Scheduling," in *Proceedings of the IEEE Computer Society Annual Symposium on VLSI*, 2003, pp. 121–126.