Secure Multi-Key Generation Using Ring Oscillator based Physical Unclonable Function

Venkata P. Yanambaka
Department of Computer Science and Engineering
University of North Texas, USA.
Email: venkataprasanthyanambaka@my.unt.edu

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

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

Jawar Singh
Electronics and Communication Engineering
PDPM IIIT Jabalpur, India.
Email: jawarsingh2002@gmail.com

***Abstract*—Advancements in the computational power of devices has paved the way for a new generation of communicating devices and new and better architectures which are already being implemented currently. The Internet of Things (IoT) is one of them. In an ideal IoT all devices will be connected to a common network interface and will be able to communicate with each other to perform tasks that need a human interaction presently. Security in such an interface is of the highest priority. For encryption of messages between devices, unique key generation is important. Physical Unclonable Functions (PUFs) can be used to generate a unique key for this encryption. This paper presents two designs of PUFs which can generate a new key every time the circuit is run and hence this approach is called "Multi-Key Generator PUF" (MKG-PUF). Once a key is generated, it cannot be generated again even with the same device. Due to the process variations and environmental effects, the keys generated will be random. Power optimized and speed optimized designs are proposed in this paper. The power optimized design utilizes 30% less power compared to the speed optimized design but generates the keys slowly. The speed optimized design consumes more power but can generate the keys in a fraction of the time needed by the power optimized design.**

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

I. Introduction

Technology has advanced in many aspects of day-to-day life [1]. FinFETs are now being used commercially for manufacturing high performance and low power consuming devices. The current transistor size is 14nm [2]. FinFETs are three dimensional transistors where the source and drain are elevated to the third dimension. The fin itself acts as the channel. In case of high-κ metal gate transistors, the minimal size of the channel has led to short channel effects which are compensated in the FinFETs. As the channel width is equal to twice the height of the fin, the overall area of electron movement has increased accommodating more charge carriers in the channel. Due to the reduction in power dissipation, the overall temperature dissipation is also reduced. Fan-less designs of new commercial computational devices have being made possible by the introduction of FinFETs. When all these sensing devices are connected to each other the resulting network is called the Internet of Things (IoT), as illustrated in Fig. 1 [3], [4]. Wireless sensor networks (WSN) is an example in which active devices are connected and continuously exchange data in which security can be of paramount importance [5], [6].

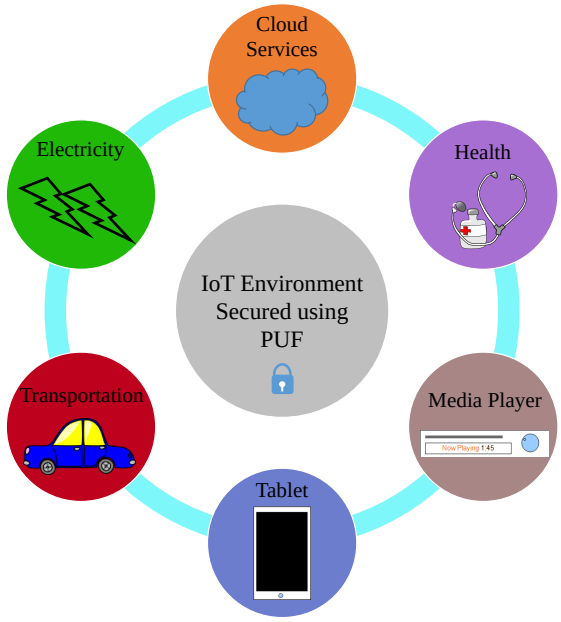


Fig. 1. Illustration of the Internet of Things (IoT).

A Physical Unclonable Function (PUF) uses the manufacturing variations in different devices to generate unique keys for different applications [7]. There are various designs of PUFs for use in different applications [8]. In the current design a Ring Oscillator (RO) is selected to generate multiple keys with a single PUF module. Among oscillator designs, the RO is the most vulnerable to environmental and power supply variations.

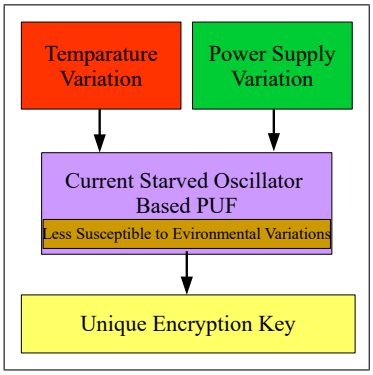
In this paper we propose two designs of PUFs as an advancement of our previous research on this topic disseminated through [9]. One is power efficient, trading off the time taken to generate the key and the other is time efficient, trading off the power consumption of the design. The Speed Optimized PUF consumes more power and can be deployed in performance

demanding applications like network switches or routers where high speed processing is necessary. Power Optimized PUF can be deployed into devices where the power consumed by the device is of higher importance than its performance.

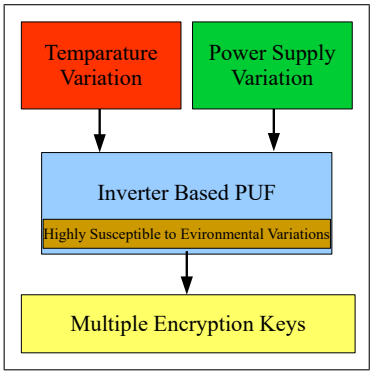
The rest of this paper is organized as follows: Section II highlights the novel contributions of the paper. Section III presents related research in this area. The design of the FinFET based Multi-key Generation PUF is presented in Section V and the two designs are presented in Section IV. Experimental results are presented in Section VI and Section VII summarizes the results and provides future directions.

II. Novel Contributions

In reference [9], a Current Starved (CS) Oscillator PUF has been presented by the authors of this paper. The current paper also uses a basic inverter based oscillator to design the PUF. However, in the CS based PUF, the whole module is less susceptible to environmental and power supply variations and hence not suitable for multi-key generation. On the other hand, the design presented in this paper uses a different architecture of oscillator to increase susceptibility. Figure 2 shows the difference between the two architectures, the one presented in [9] and the other in the current paper. **Both the PUF designs differ substantially at the circuit level and in terms of performance objectives**.



(a) Current-Starved Architecture based Oscillator [9].



(b) Proposed Inverter based Oscillator PUF

Fig. 2. Comparison of PUF Architectures.

When a current starved architecture with output switching is used, the oscillation frequency of the oscillator is not affected strongly by temperature and other environmental variations. But in the current paper, the main goal is to generate multiple or different keys every time the PUF is activated. So a normal inverter based oscillator is used to make the circuit susceptible to the power supply variations such that the oscillation frequency changes easily with a slight change in different parameters. The following are the two novel contributions of the paper:

- A speed optimized inverter based multi-key generating PUF.
- A power optimized inverter based multi-key generating PUF.

III. Related Prior Research

The current focus of research in almost all domains is high performance with low power consumption. Transistors are one of the key focus areas. Short channel effects in high-κ metal gate transistors were solved by the development of FinFETs [1], [2]. A comparative analysis of high-κ metal gate transistors and the FinFETs is presented in [2].

IoT is a concept that can be introduced into a wide range of applications. In [4], an IoT based quadrotor is presented for real time object tracking. The architecture presented in [4] uses off-shelf components to make the manufacturing easier. A 20$\times$ faster response rate is achieved by the implementation of the architecture. In [10], a IoT enabled sensor is presented for diagnosis of thyroid cancer. This sensor connects the patient and doctor using the IoT. A prototype of the proposed design was also implemented using Simulink®. In [11], different security issues are discussed that are present in an IoT environment. A protocol to authenticate different devices that are connected in the IoT is presented in [12].

There are different ways to encrypt communications between different devices in an IoT environment. Generating a unique key used for encryption is very important. A PUF can be used to generate a unique key. In [8], detailed description, properties and different implementations of PUFs has been presented. Characterization of PUFs is presented in [13]. In [14], an implementation of a PUF using the variability of RRAM is presented.

In [15], a ring oscillator PUF architecture has been presented. A reconfigurable PUF is presented in [16] which can be configured to generate different keys with different challenge bits which can give a large number of combinations. An SRAM based PUF is discussed in [17]. The main advantage of an SRAM based PUF is it can be implemented easily where SRAM is available and it can also be implemented in FPGAs. A PUF can also be implemented using multiplexers [18]. NAND gates are used to implement the multiplexers. The process and mismatch variations introduce the gate delays in the transistors. Due to this gate delay, the output generation in the NAND gates will have considerable difference between different logic gates. This delay is utilized for the PUF. When a number of multiplexers are connected in series, there will be enough delay in signals. Different such delayed signals, compared with each other are creating different bits for keys. A Ring Oscillator PUF occupies less chip area but the circuit will degrade over time. An aging resistant ring oscillator is presented in [19].

IV. Proposed Inverter based MKG PUF

In this section, two designs of Inverter based Multi-key generating PUF are presented to generate a key that can be used only once and the same key cannot be generated again even with the same PUF module. Figure 3 shows the application domain of the proposed designs. During wireless communications, each session uses a different key for encryption. All devices do not have the capability to generate a new session key every single time. To compensate for new key generation, we propose this module where a new key is generated when the module is activated. Before starting a new session or connecting to a new device, the Inverter based Multi-key generating PUF module is activated and a new key is generated. Then the key is used to encrypt the communication.

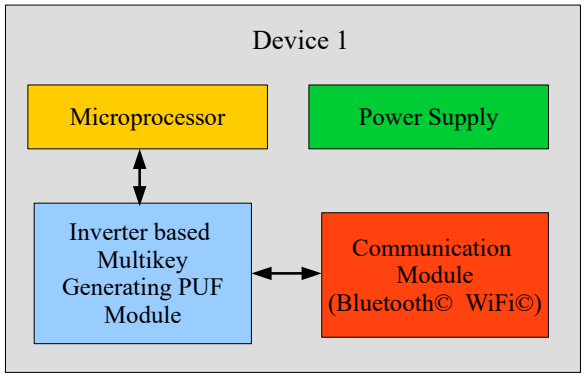


Fig. 3. Deployment of Inverter based Multi-key Generation PUF.

Figure 4 presents the speed optimized inverter based MKG PUF. This design is optimized for high performance devices where power consumption is not the main concern, such as a router. As shown in the figure, this design is similar to that of an arbiter PUF. The multiplexers are replaced by ring oscillators. A number of ring oscillators are connected to a D flip-flop. The output of the flip-flop depends on the frequency of the oscillators. Due to process and mismatch variations during manufacturing, the frequency will not be the same for all oscillators. In the speed optimized design, each pair of ring oscillators is connected to a different D flip-flop. The bit generated at the flip-flop is stored using an SRAM. In this case, the signals need not be selected one after the other which speeds up the process of key generation.

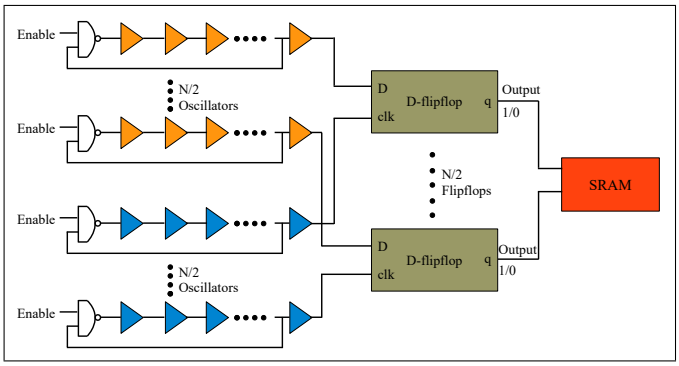


Fig. 4. Proposed Design of Speed Optimized Inverter based MKG PUF.

Figure 5 presents the power optimized inverter based MKG PUF. Development of low power devices has become a necessity as technology grows. To include a PUF module into the low power devices, we reduce the power consumption of the PUF itself. The power optimized PUF is similar to that of the speed optimized PUF. In this design, the signals are selected using a multiplexer to avoid the use of multiple D flip-flops. This design also reduces the chip area consumed by the PUF. Two different sets of ring oscillators are connected to two multiplexers. Each multiplexer will select different ring oscillators based on the select signals used. These signals are fed to the clock and input of the D flip-flop. Depending on the frequency of the signals from the oscillators, the output bit is generated which is stored in the SRAM.

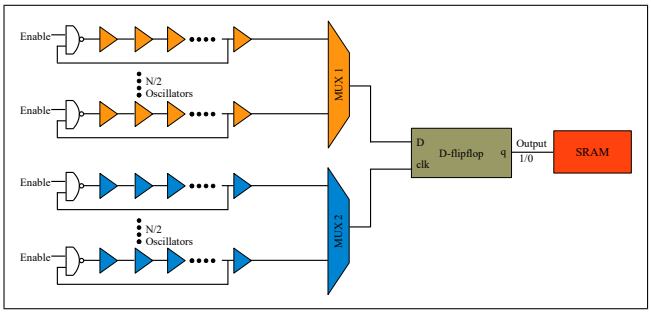


Fig. 5. Proposed Design of Power Optimized Inverter based MKG PUF.

V. Design of Inverter based Multi-key Generation PUF

The design of the inverter based Multi-Key Generation PUF is presented in Figure 6. Double Gate FinFETs are used to design the inverters. A shorted gate mode FinFET is used to increase the stability of the oscillator. In this design of PUF, to generate a N bit key, $2N$ ring oscillators are needed. A single bit generation is presented in this section. As shown in the figure, the traditional ring oscillator architecture is used instead of current mirror architecture which is very resistant to temperature variation. The two ring oscillators are connected to the input and the clock signal of the D flip-flop. The D flip-flop generates the output based on the oscillation of the ring oscillators. If the input arrives before the clock signal, the output will be low ('0'). If the clock signal arrives first, the output of the D flip-flop will be high ('1'). Simulations were performed in Spice. To simulate the process variation, Monte Carlo analysis was considered.

The nominal length and width of the pFET used are 32 nm and 120 nm. The nominal length and width of the nFET are 32 nm and 240 nm. The threshold voltage of pFET and nFET considered in the design are -250 mV and 310 mV. The nominal oxide thickness considered for the pFET and nFET is 1.65n and 1.75n. The supply voltage is 0.9 V.

Monte Carlo analysis was used to simulate the process and mismatch variations on the circuit. 100 Monte Carlo runs were performed. All the geometric variables of the transistors were varied. A 10% variation was considered and simulations were performed. The mean values for these variables were the nominal values presented above. To simulate the generation of Multi-Key generation, all geometric variables were kept constant but the power supply and the temperature of the circuit were varied. The power supply of the oscillators was

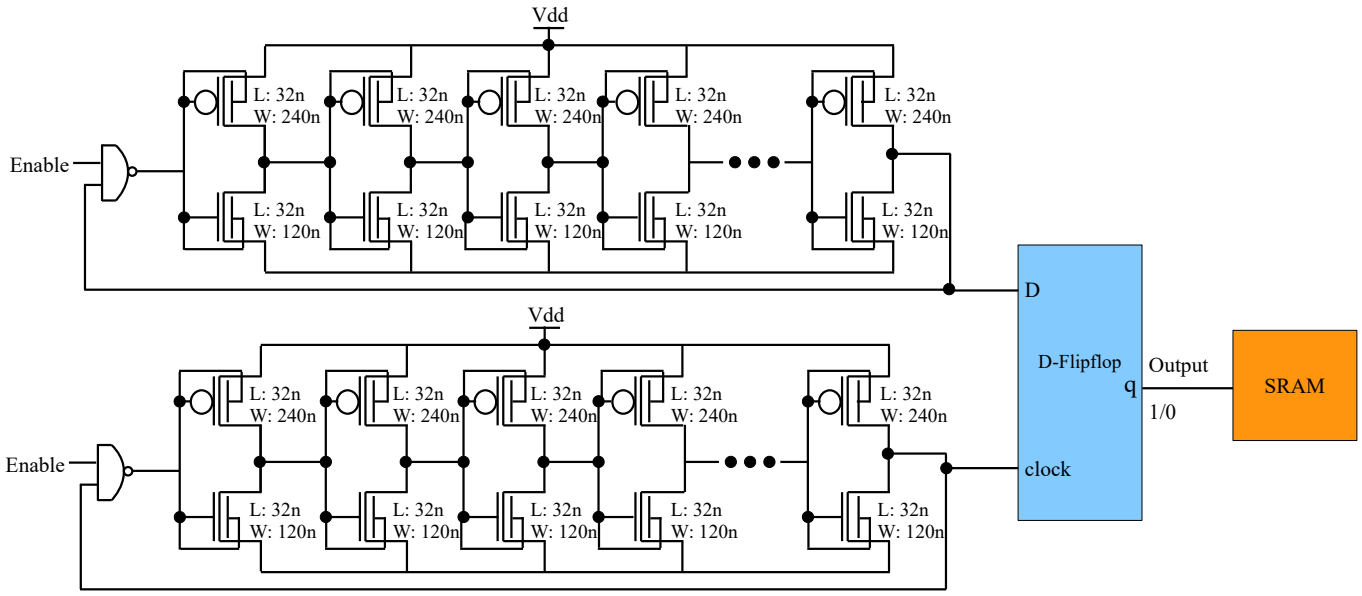


Fig. 6. Design of Inverter based MKG PUF.

varied from 0.7 V to 1.1 V. The temperature was varied from 27^oC to 30^oC. The variation in temperature considered was not very high to be close to a realistic scenario. Figure 7 shows the DC characteristics of a FinFET based inverter when subjected to Monte Carlo analysis. This shows the variation by a FinFET based inverter with the same nominal or mean values. The output bits of 100 different PUFs were compared to each other. For this, the geometric variables of the transistors are varied along with the temperature and the power supply. The experimental results are presented in Section VI.

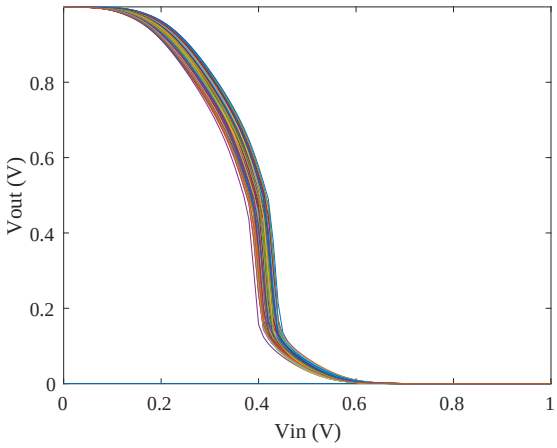


Fig. 7. DC Analysis of Inverter with Process and Mismatch Variations.

VI. Experimental Results

To characterize the design of a PUF, two Figures of Merit (FoM) are considered, the Hamming distance and average power consumption. Average power consumption is calculated as the sum of leakage power, dynamic power and the gate leakage of the transistors. The PUF can be characterized using its uniqueness, reliability and power consumption. *Uniqueness* of a PUF is the ability of the module to generate different keys with every new challenge bit. The challenge bit in the case of an arbiter PUF is the input given at the select lines of different multiplexers. In the case of the inverter based MKG PUF, the uniqueness is checked such that for every Monte Carlo run, a new key is generated. In the process of simulations, along with the variables of the transistor, the power supply and the temperature are also varied to get the best possible results. Then the Hamming distance of the keys is calculated. The ideal Hamming distance between the keys to consider them safely unique is 0.5. Figures 8 and 9 show the Hamming distance distribution of the two designs, the speed optimized inverter based MKG PUF and the power optimized inverter based MKG PUF. The Hamming distance is presented in percentages in the histograms. In both designs, the Hamming distance follows a Gaussian distribution.

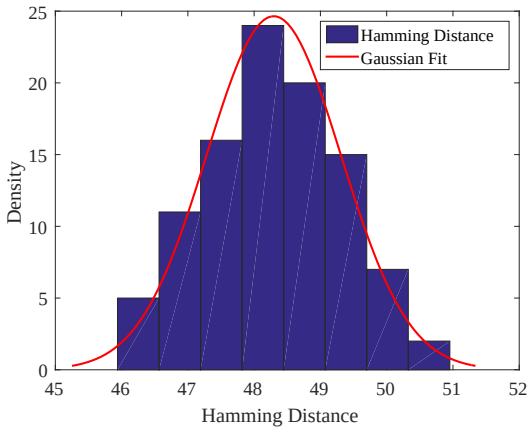


Fig. 8. Hamming Distance of Speed Optimized Inverter based MKG PUF.

Reliability of a PUF is the ability of the module to generate the same key again with the same challenge bits.

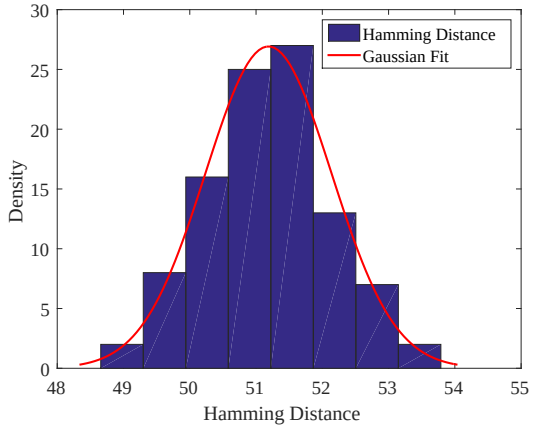


Fig. 9. Hamming Distance Power Optimized Inverter based MKG PUF.

But the presented circuit is used for generating multiple keys. Hence in this scenario, the reliability of PUF is the ability to generate a new key every time the PUF is run and generate as few interferences as possible. Figures 10 and 11 present the Hamming distance distribution of the Speed Optimized and Power Optimized Inverter based MKG PUFs.

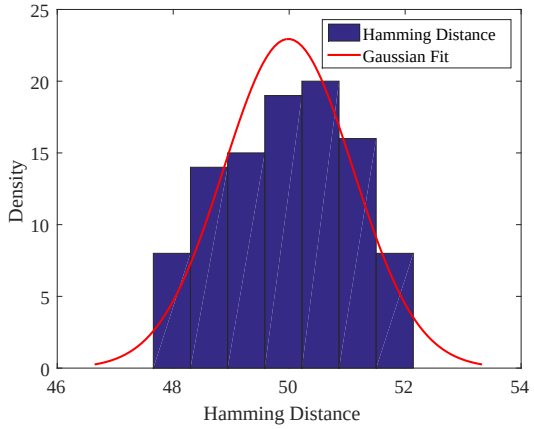


Fig. 10. Reliability of Speed Optimized Inverter based MKG PUF.

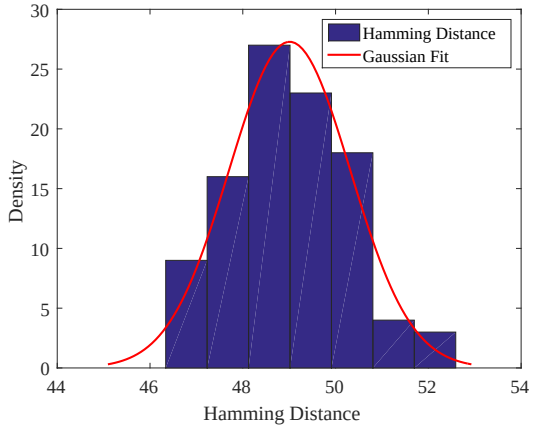


Fig. 11. Reliability of Power Optimized Inverter based MKG PUF.

The *average power* consumed is the sum of leakage powers of all the off transistors, dynamic power and the gate leakage of the transistors. Figures 12 and 13 show the power consumed by the circuits. There is a significant change in the power consumption with the use of power optimized MKG PUF. The average power reduced from 251.5 μW to 175 μW. Table I shows the transistor sizes, Hamming distance and the average power consumed by the two different designs of PUF. Table II shows a comparison of the current results with results presented in other publications.

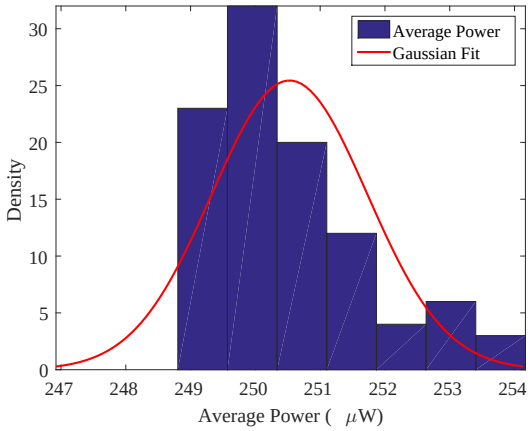


Fig. 12. Average Power of Speed Optimized Inverter based MKG PUF.

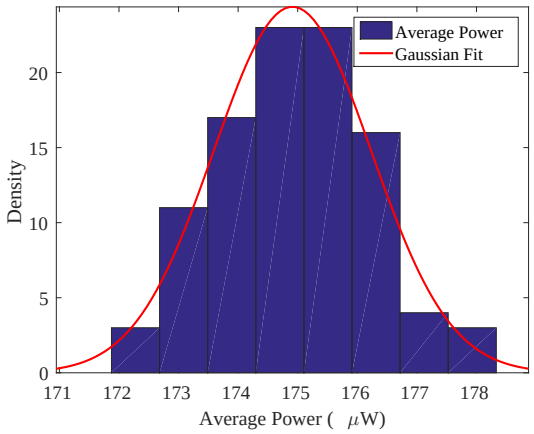


Fig. 13. Average Power of Power Optimized Inverter based MKG PUF.

TABLE I. CHARACTERIZATION TABLE FOR POWER AND SPEED OPTIMIZED DESIGNS.

Power Optimized Inverter MKG PUF		
Parameter	Value	
Transistor sizes	p-Type (W:L)	n-Type(W:L)
	120n : 32n	240n : 32n
Average Power	175.5 μW	
Hamming Distance	50.1 %	
Speed Optimized Inverter MKG PUF		
Parameter	Value	
Transistor sizes	p-Type (W:L)	n-Type(W:L)
	120n : 32n	240n : 32n
Average Power	251.5 μW	
Hamming Distance	48.3 %	

TABLE II. COMPARISON OF RESULTS WITH RELATED EXISTING RESEARCH.

Research Works	Technology	Architecture Used	Average Power Consumed	Hamming Distance (%)
Rahman et al. [19]	90 nm		–	50
Maiti [15]	180 nm	Traditional Ring Oscillator	–	50.72
Suh [7]	–		–	46.15
Maiti et al. [13]	–	–	–	47.31
Yanambaka et al. [9]	32 nm	Current Starved Oscillator	320 μW	50.9
This paper (Speed Optimized)	32 nm	Traditional Ring Oscillator	251.5 μW	48.3
This Paper (Power Optimized)	32 nm	Traditional Ring Oscillator	175.5 μW	50.1

VII. CONCLUSION AND FUTURE RESEARCH

We presented two different designs which can be deployed into respective devices where high performance is needed trading off power consumption. In the power optimized design, the power consumption can be reduced by 30% trading off a small amount of time consumed to generate the key compared to the speed optimized design. At the same time, the speed optimized design can generate the key significantly faster compared to the power optimized design but consuming 30% more power. As a future research, both designs can be converted to ultra low power consuming modules where only a fraction of power is utilized.

The future directions of this research is in multiple fronts. We intend to explore the quality of PUF design when it is realized using junction and doping free transistors [20]. We want to investigate alternative topologies for PUF circuit design which can be robust and energy-efficient. It will be interesting to evaluate the performance of specific PUFs for different nanoelectronic technology including FinFET, GNRFET, and other similar technologies. The deployment of PUF in real-life systems to provide efficient security for smart healthcare and even in smart cities in a larger context needs research and development [10].

REFERENCES

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

[2] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Ghai, *Nanoscale high-κ/metal gate CMOS and FinFET based logic libraries*, ser. Nano-CMOS and Post-CMOS Electronics: Devices and Modelling. Institute of Engineering and Technology, 2015, vol. 1, ch. 6, pp. 169–211.

[3] D. Park, "The Quest for the Quality of Things: Can the Internet of Things deliver a promise of the quality of things?" *IEEE Consumer Electronics Magazine*, vol. 5, no. 2, pp. 35–37, April 2016.

[4] 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.

[5] M. L. Rajaram, E. Kougianos, S. P. Mohanty, and U. Choppali, "Wireless Sensor Network Simulation Frameworks: A Tutorial Review," *IEEE Consumer Electronics Magazine*, vol. 5, no. 2, pp. 63–69, April 2016.

[6] M. L. Rajaram, E. Kougianos, S. P. Mohanty, and P. Sundaravadivel, "A Wireless Sensor Network Simulation Framework for Structural Health Monitoring in Smart Cities," in *Proceedings of the 6th IEEE International Conference on Consumer Electronics - Berlin (ICCE-Berlin)*, 2016.

[7] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," in *Proceedings of the 44th ACM/IEEE Design Automation Conference*, 2007, pp. 9–14.

[8] S. Joshi, S. P. Mohanty, and E. Kougianos, "Everything You Wanted to Know about PUFs," vol. xx, no. yy, p. Accepted on 11 Oct 2015, 2017.

[9] V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Novel FinFET based Physical Unclonable Functions for Efficient Security in Internet of Things," in *Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, 2016.

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

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

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

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

[18] 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.

[19] 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.

[20] 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 *Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, 2016.