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

Venkata P. Yanambaka*, Saraju P. Mohanty†, Elias Kougianos‡, and Jawar Singh§
NanoSystems Design Laboratory (NSDL), University of North Texas, Denton, TX 76207, USA.*†‡
Electronics & Communication Engineering, Indian Institute of Information Tech, Design & Manufacturing, Jabalpur, India.§
Email: vy0017@unt.edu*, saraju.mohanty@unt.edu†, eliask@unt.edu‡, jawar@iiitdmj.ac.in§

***Abstract*—In the IoT, 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.**

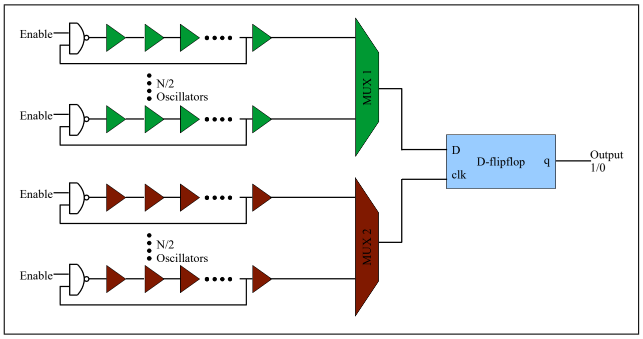

Fig. 1. Novel Power Optimized Hybrid Oscillator Arbiter PUF.

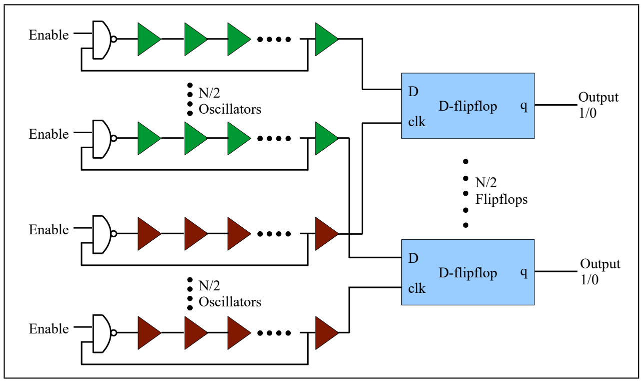

Fig. 2. Novel Speed Optimized Hybrid Oscillator Arbiter PUF.

Security in the IoT using PUFs is actively being investigated. Many types of PUF designs are available such as reconfigurable PUF, Ring Oscillator PUF, Arbiter PUF SRAM PUF, etc. [1], [2]. In this paper, we present two novel designs of RO PUF, one being high performance and the other being low power.

The design of the FinFET based Power Optimized Hybrid Oscillator Arbiter PUF is shown in Fig. 2. 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 design of FinFET Speed Optimized Hybrid Oscillator Arbiter PUF is shown in Fig. 2. 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.

Two Figures of Merit are considered, the Average Power and Time Period. Both FoMs are calculated for each of the designs the Traditional RO PUF design consumes more power than the Power Optimized Hybrid Oscillator Arbiter 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. 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.

References

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

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