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

Venkata P. Yanambaka and Saraju P. Mohanty
Department of Computer Science and Engineering
University of North Texas Denton, TX 76207, U.S.A.
{vy0017,saraju.mohanty}@unt.edu

Elias Kougianos
Department of Engineering Technology
University of North Texas, Denton, TX 76207, U.S.A.
Elias.Kougianos@unt.edu

Jawar Singh
Department of Electronics and Communication Engineering
Indian Institute of Information Tech, Jabalpur, India
jawar@iiitdmj.ac.in

Introduction

- The Internet of Things is a futuristic area where all devices can communicate with each other.
- In such an IoT environment, if any security feature is compromised, the entire environment will be in chaos.
- Hence to encrypt that environment, PUFs can be used.
- Physical Unclonable Function uses process variation in devices to generate different encryption keys.
- A PUF key is never stored in memory. For each communication, hardware encryption is performed.
- Hacking into such environment without being present at the hardware location is very difficult.
- Two designs are presented: Speed Optimized design for high speed devices like network switches and Power Optimized design for hand-held devices like smartphones.

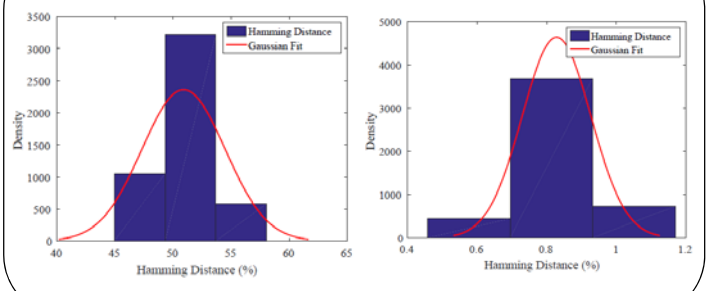
PUF Designs

- In both designs, Ring Oscillators (ROs) generate the oscillations.
- Due to process variation, there will be change in the frequencies generated.
- Hence the D-input and the clock signal will vary at any given point of time.
- Multiplexers in the Power Optimized design select a pair of ROs and give signals to D-Flipflop which consumes time but with low power consumption.
- Speed Optimized design does not have multiplexers but each pair of RO has its own flipflop which saves time in key generation.

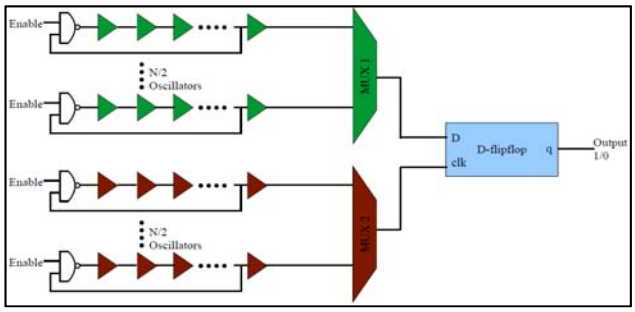
Figures of Merit

- Uniqueness: The same key should not be used in any other PUF design. Uniqueness is calculated using Hamming Distance.
- Reliability: The PUF module should give the same key. Even environmental effects should not change the key.
- Security: The module should be resistant to different attacks on the circuit.
- Each of these results are presented below.

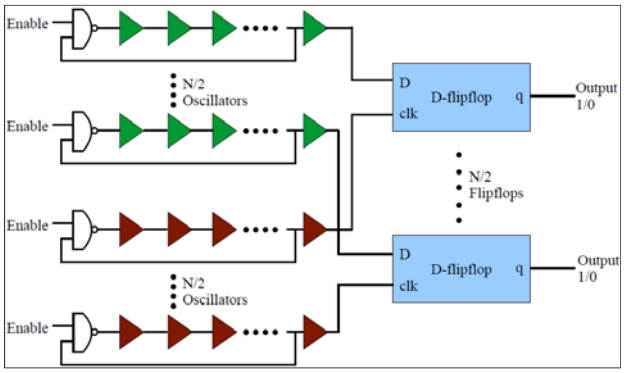
Experimental Results



Proposed PUF Topologies



Power Optimized Hybrid Oscillator Arbiter PUF



Speed Optimized Hybrid Oscillator Arbiter PUF

Experimental Results

- A comparison with traditional RO PUF is presented.
- Ideal Hamming distance is 50%.
- Power consumption is also presented for a better understanding of implementation in IoT.
- Time to generate key is a novel FoM in this presentation.

Parameter	Value
Traditional Ring Oscillator PUF	
Average Power	310.8 µW
Hamming Distance	50 %
Average Time to Generate Key	150 ns
Speed Optimized Hybrid Oscillator Arbiter PUF	
Average Power	320 µW
Hamming Distance	52 %
Average Time to Generate Key	50 ns
Power Optimized Hybrid Oscillator Arbiter PUF	
Average Power	285.5 µW
Hamming Distance	50.9 %
Average Time to Generate Key	150 ns

Conclusions

- Two designs of PUFs are presented which can be deployed in an IoT environment.
- In future, Ultra Low power designs of the same circuits can be designed.
- More robust designs can be implemented to increase the whole security of the circuit.

NSDL NanoSystem Design Laboratory UNT UNIVERSITY OF NORTH TEXAS

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING College of Engineering UNT