Energy-Efficient Physical Unclonable Functions for Secure IoT Environment

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

Nano System Design Laboratory (http://nsdl.cse.unt.edu), University of North Texas, USA. Email: saraju.mohanty@unt.edu

Abstract

- The Internet of things is currently the most sought after solution for many day-to-day issues that we are facing.
- This work presents an energy efficient security solution, the **PUF,** for making the Internet of Things a safer environment.
- Low power consumption and low chip area makes it easier to be deployed anywhere.

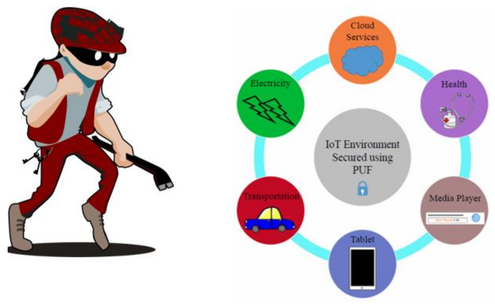


Fig. 1 IoT Security

Engineering Problem Overview

- In an IoT environment **everyTHING** is connected and where 'everything' is connected, security is one of the main concerns.
- If an environment is attacked and breached, an entire city or home can be in chaos.
- One of the efficient solutions for this issue is hardware security.
- Physical Unclonable Functions (PUF) take advantage of the manufacturing variations in an IC.
- A PUF key is never stored in memory which makes it more secure and robust.
- The input to a PUF is Challenge Input (in form of binary) and the output is Response (also binary).

Design of Proposed Physical Unclonable Function and Deployment in Device

- During the fabrication, due to various factors, variations will be introduced into the devices on the IC.
- These variations will affect the output of the devices and no two devices will give an identical output.
- In PUF design, Ring Oscillators generate oscillations but due to manufacturing variations, no two frequencies are the same.
- Multiplexers select a pair of ROs and give signals to the D-Flipflop. The PUF key is generated from the flipflop.
- To generate an *N*-bit key, *2N* ring oscillators are needed in this design.

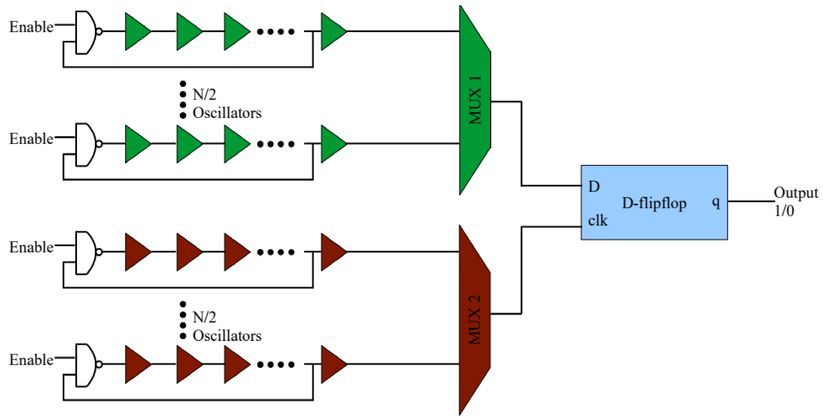


Fig. 2. Hybrid Oscillator Arbiter Physical Unclonable Function

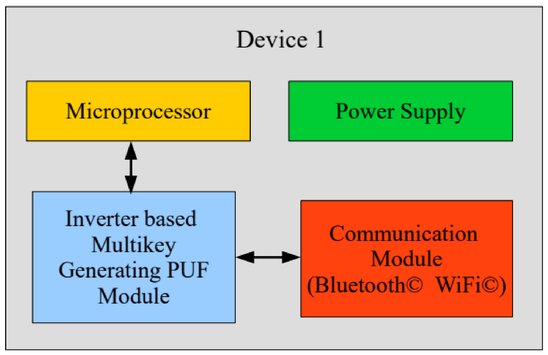


Fig. 3. Deployment of PUF in Iot Device

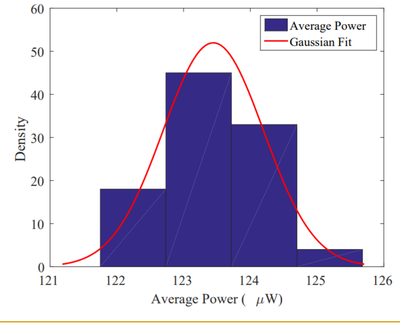
Simulation Results of The Design

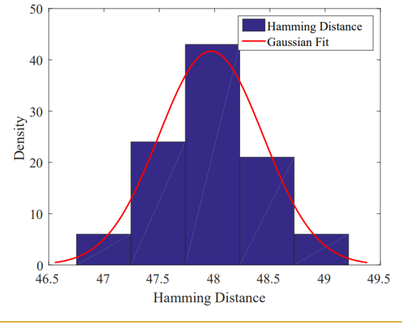
- Uniqueness: The same key should not be obtained using any other PUF design. Uniqueness is calculated using Hamming Distance.
- Average Power: Average Power consumed by the entire circuit.
- Reliability: The PUF module should give the same key. Even the environmental effects should not change the key.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

Parameter	Value
Conventional Ring Oscillator Physical Unclonable Function	
Average Power	310.8 µW
Hamming Distance	50%
Time to generate key	150 ns
Proposed Hybrid Oscillator Arbiter Physical Unclonable Function	
Average Power	123.8 µW
Hamming Distance	48.1%
Time to generate key	150 ns

Conclusion

- Energy-Efficient PUF design is presented.
- In future work, the design will be deployed in an IoT environment for real-time analysis.
- More robust designs can be implemented to increase the security of the circuit on a whole.





References

- 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, pp. 172-177.
- M. O'Neill, "Insecurity by Design: Today's IoT Device Security Problem," *Engineering,* vol. 2, no. 1 , 2016, pp. 48–49.