Hybrid Oscillator Arbiter PUF Using Manufacturing Variations for Robust Security in the Internet of Things

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

Smart Electronic Systems Laboratory (http://smohanty.org/SESL), University of North Texas, USA. Email: saraju.mohanty@unt.edu

Abstract

- The Internet of Things is a lot of attracting attention.
- But security is the major concern in the connected devices.
- Physical Unclonable Functions are hardware-assisted security primitives.
- High Performance and Low Energy consumption are the key factors of PUF.

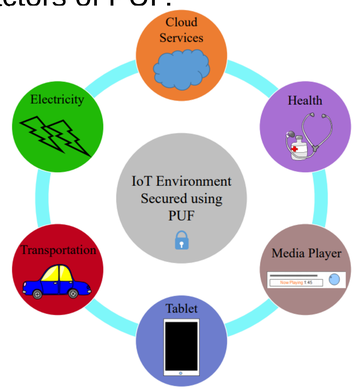


Fig. 1 Internet of Things

Physical Unclonable Function

- A Physical Unclonable Function uses the manufacturing variations introduced during the fabrication process of an IC.
- Because of these manufacturing variations, no two devices have the same geometry which introduces discrepancies in outputs.

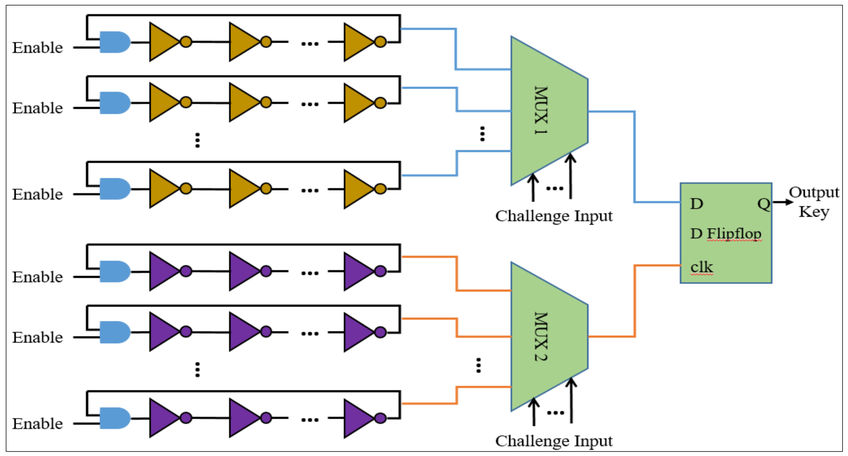


Fig. 2. Hybrid Oscillator Arbiter Physical Unclonable Function

Design of Proposed Physical Unclonable Function and Deployment in Device

- Fig. 2 shows the design of a Hybrid Oscillator Arbiter PUF which has ring oscillators as its core components.
- Due to the variations during fabrication, the oscillation frequencies are not the same for all oscillators. The oscillations are compared using a D-flipflop which outputs the PUF key.
- On top of that, environmental variations add more variability to the design of a PUF making it produce a new key every time the PUF module is run. Once a key is generated, it cannot be generated again even with the same input to the PUF module.

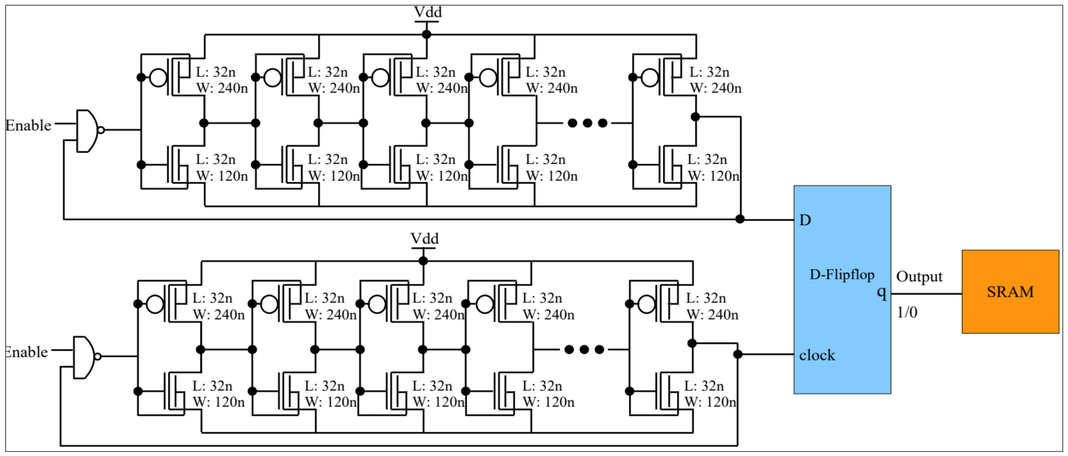


Fig. 3. Circuit Level Representation of Hybrid Oscillator Arbiter PUF

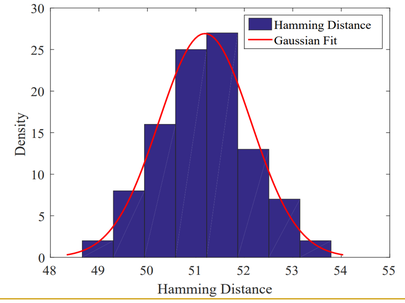
Simulation Results of The Design

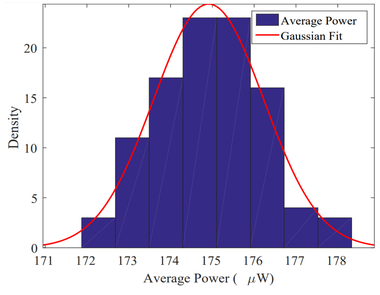
- Uniqueness: The same key should not be obtained using any other PUF design. Uniqueness is calculated using the Hamming Distance.
- Average Power: Average Power consumed by the entire circuit.
- Reliability: Environmental variability should not affect the working of a PUF module. Such effects include aging effects, temperature and power supply variations.

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	175.5 µW
Hamming Distance	51.5%
Time to generate key	150 ns

Conclusion

- A Hybrid Oscillator Arbiter Physical Unclonable Function design is presented.
- Deploying this design of PUF in an IoT environment is the subject of the future research.
- Side Channel Resilient designs of PUF should also be implemented.





References

- V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and J. Singh, “Secure Multi-Key Generation Using Ring Oscillator based Physical Unclonable Function”, in Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), 2016, pp. 200--205.
- M. O’Neill, “Insecurity by Design: Today’s IoT Device Security Problem,” *Engineering,* vol. 2, no. 1 , 2016, pp. 48–49.