PUFs Using Manufacturing Variations for Robust Security in the IoT

Venkata. P. Yanambaka[1], Saraju P. Mohanty[2], Elias Kougianos[3]

Smart Electronic Systems Laboratory

(SESL, http://smohanty.org/SESL)

University of North Texas, Denton, TX 76203, USA.

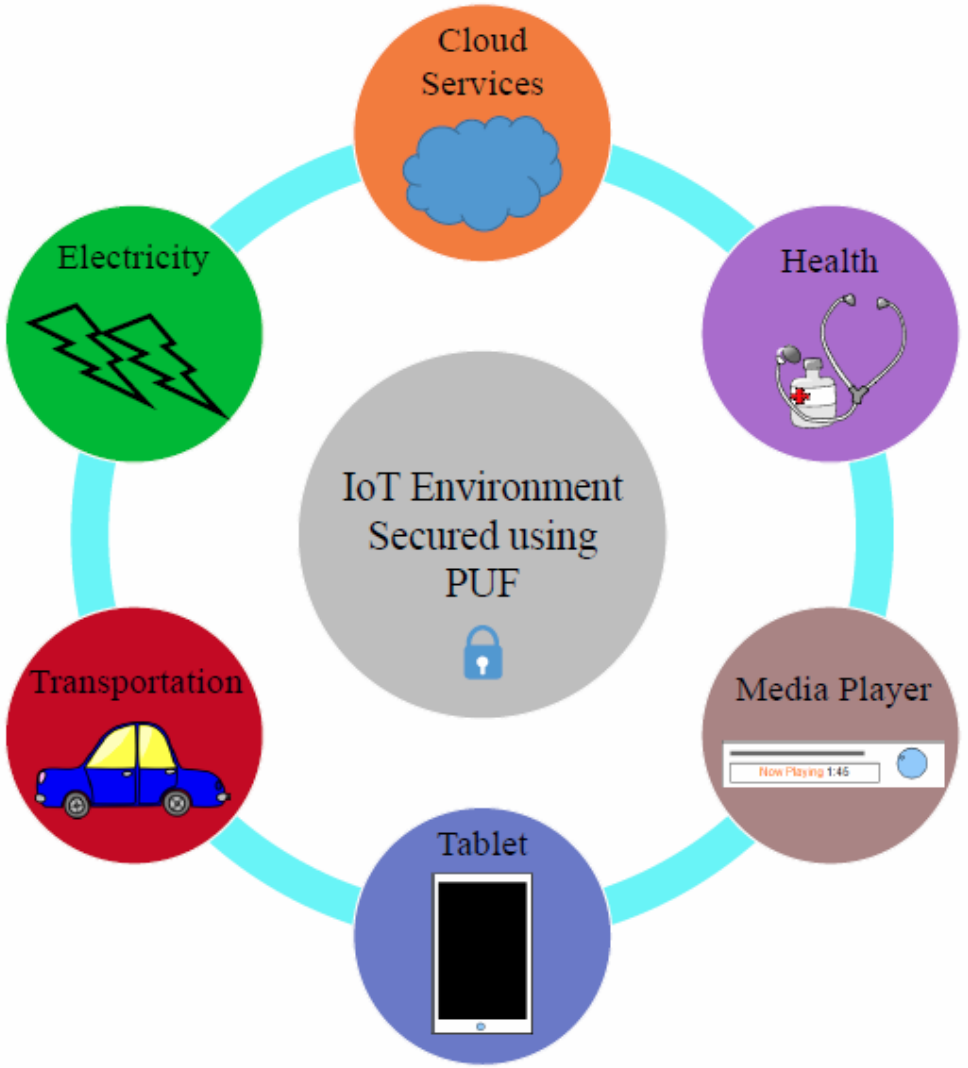
Email: vy0017@unt.edu[1], saraju.mohanty@unt.edu[2], elias.kougianos@unt.edu[3]

Outline

- Internet of Things (IoT)
- Security in IoT
- Physical Unclonable Function (PUF) ?
- Hybrid Oscillator Arbiter PUF
- Performance Metrics
- Conclusions and Future Research

Internet of Things

- Every electronic device in an environment communicates with each other.
- Human interaction will become minimal.
- Such network of devices is Internet of Things (IoT).

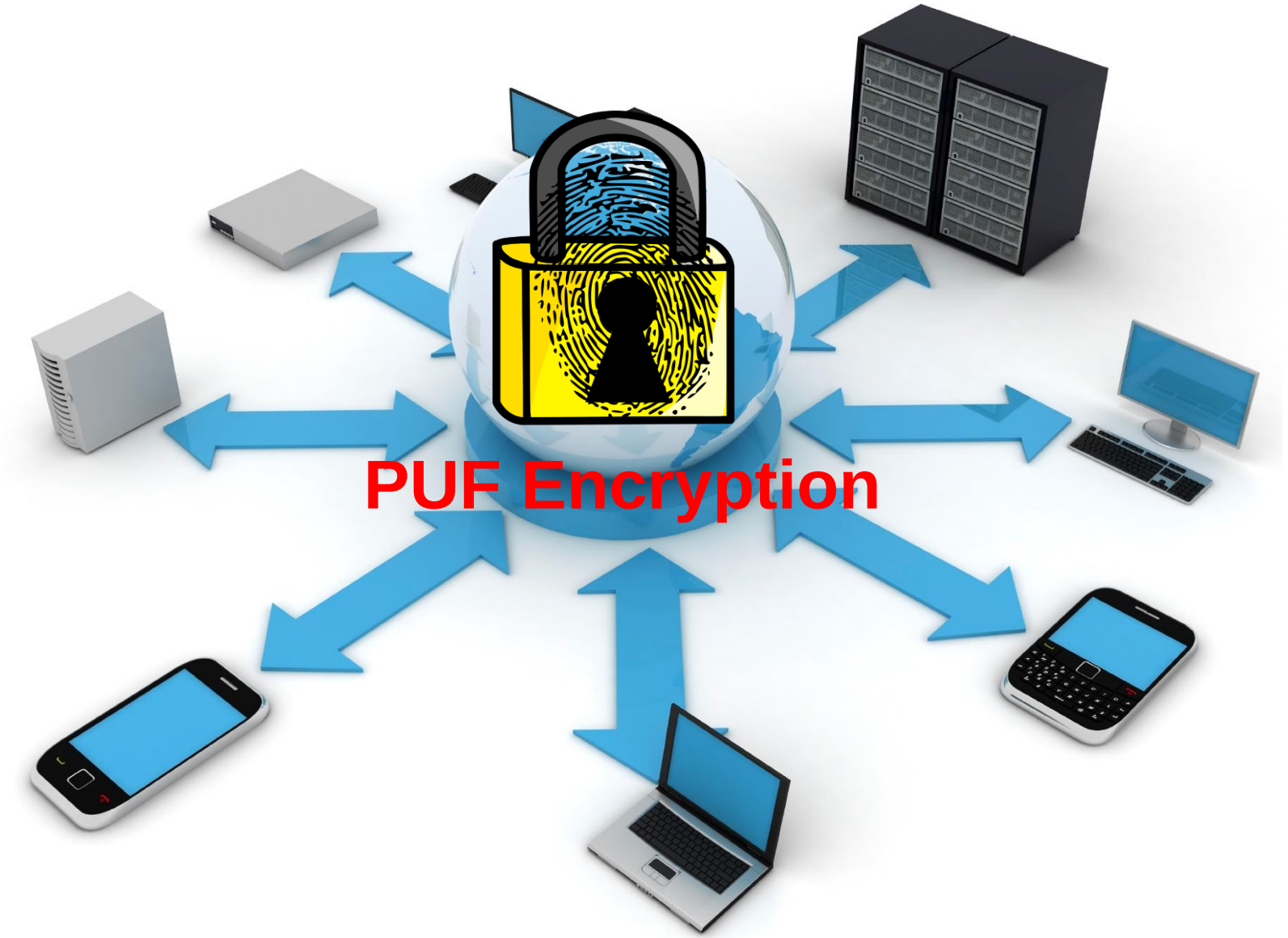


Security in Internet of Things

Lock for Security

- Earliest mechanical lock found dates back 4000 years.
- Even today, we keep things under LOCK and KEY – But Digitally.
- Digital keys are stored in Non – Volatile Memory (NVM) for cryptographic applications.

PUF vs Encryption



Physical Unclonable Function (PUF)

- Physical Unclonable Functions are simple primitives for security.
- PUFs are easy to build and impossible to duplicate (Theoretically).
- Input and Output are called Challenge Response Pair (CRP).

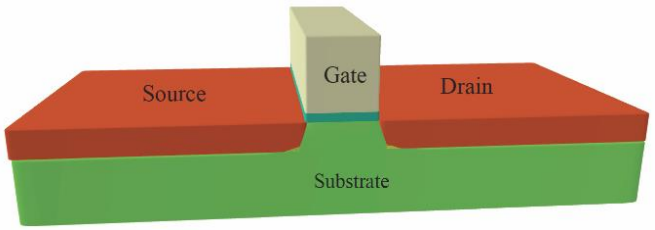
Only an authentic hardware can produce a correct Response for a Challenge.

Technology Scaling

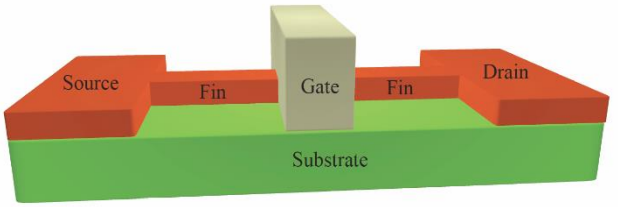
90nm CMOS

32nm CMOS

14nm FinFET

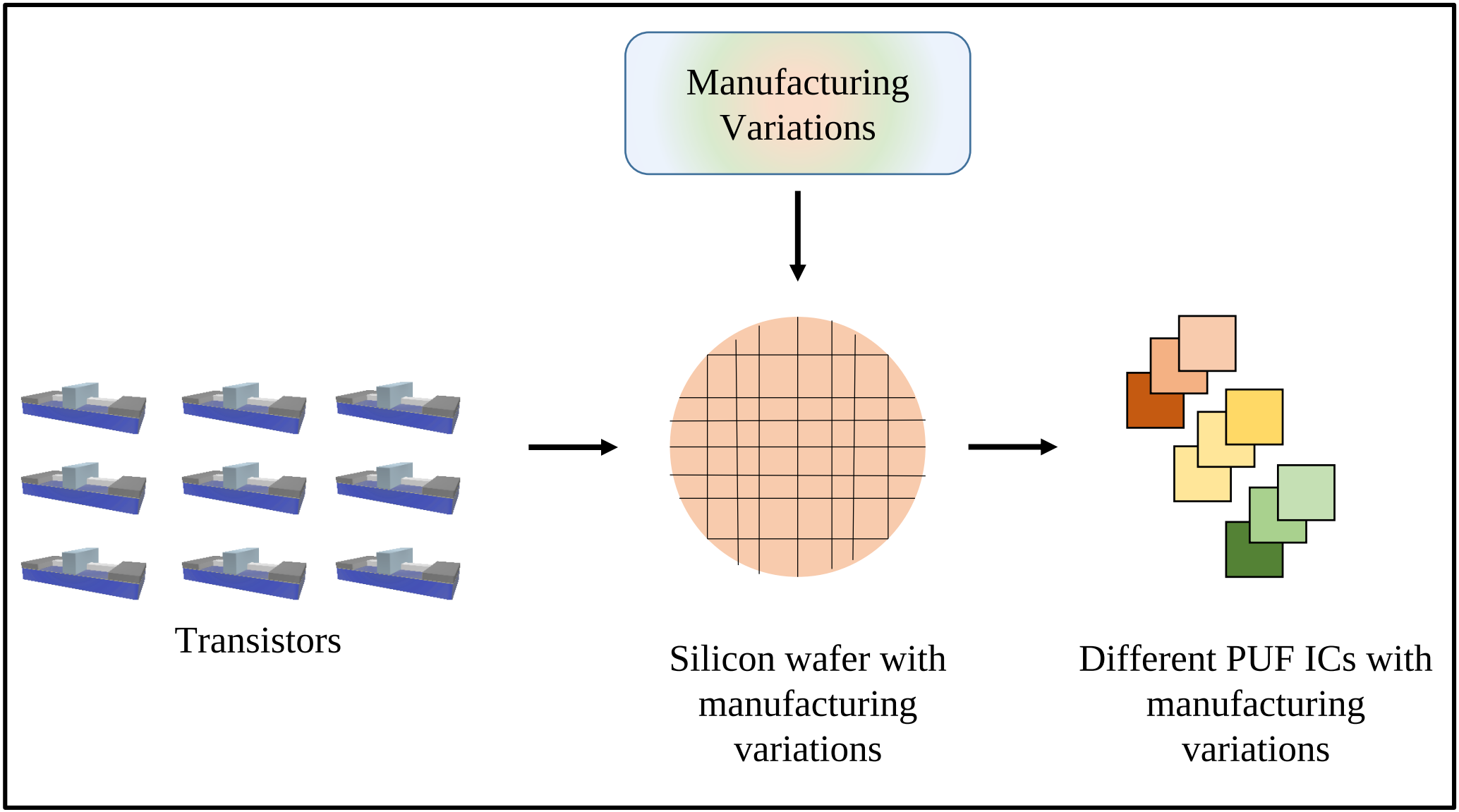


CMOS

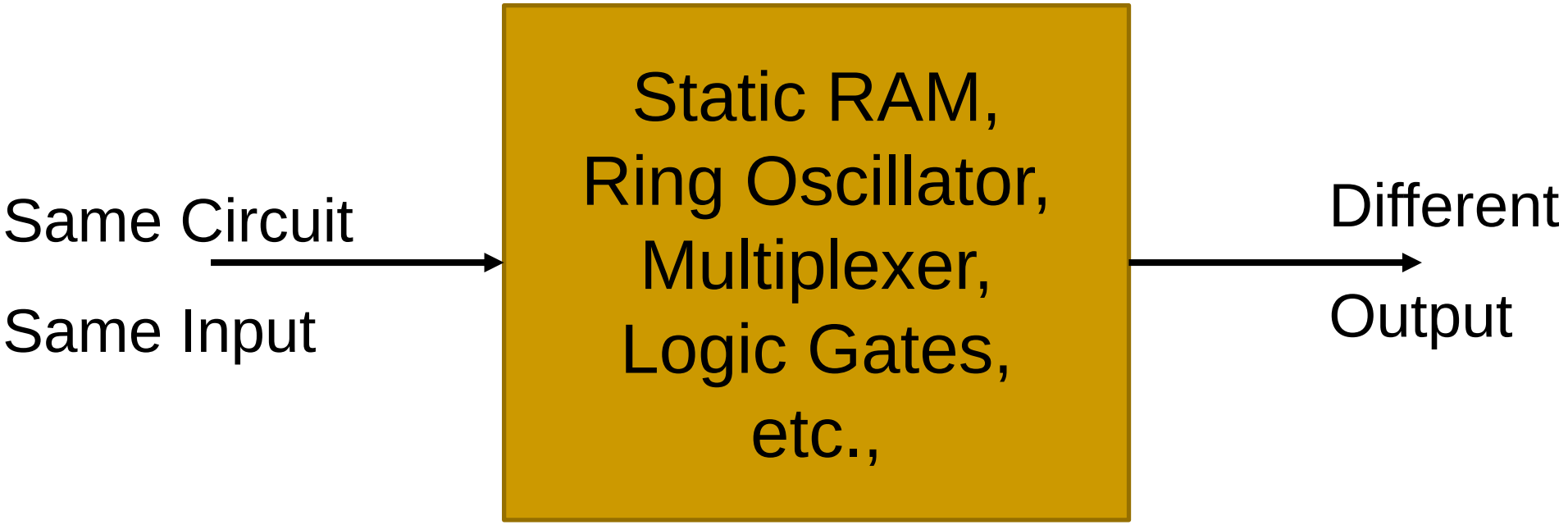


FinFET

PUF Principle

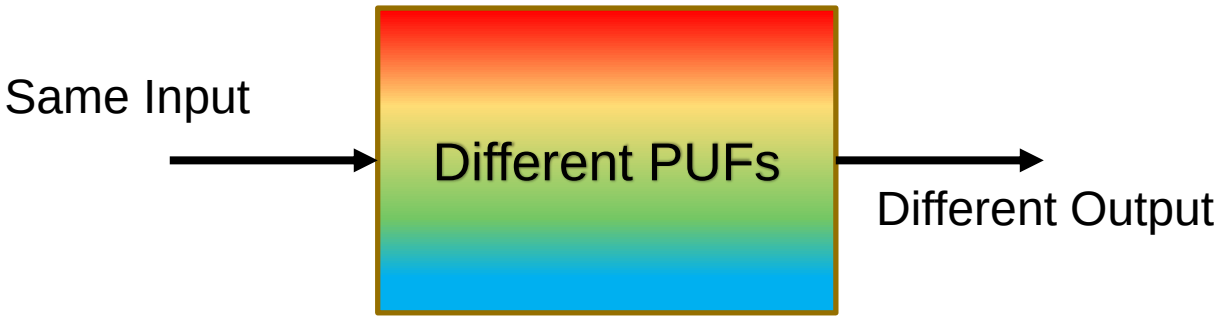


How PUF Works?



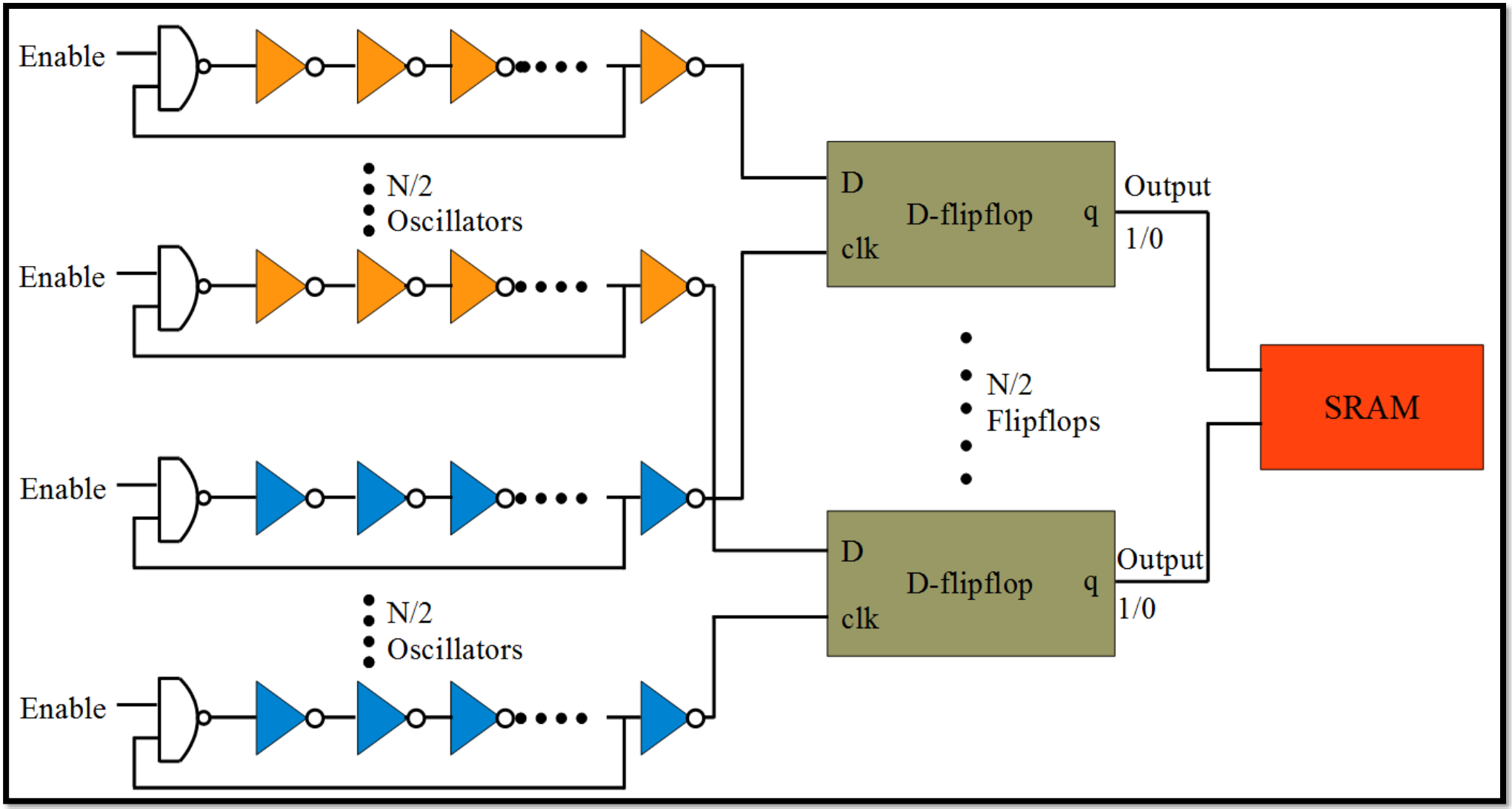
With the same circuit and the same input, we get different output due to process variations.

How PUF Works?

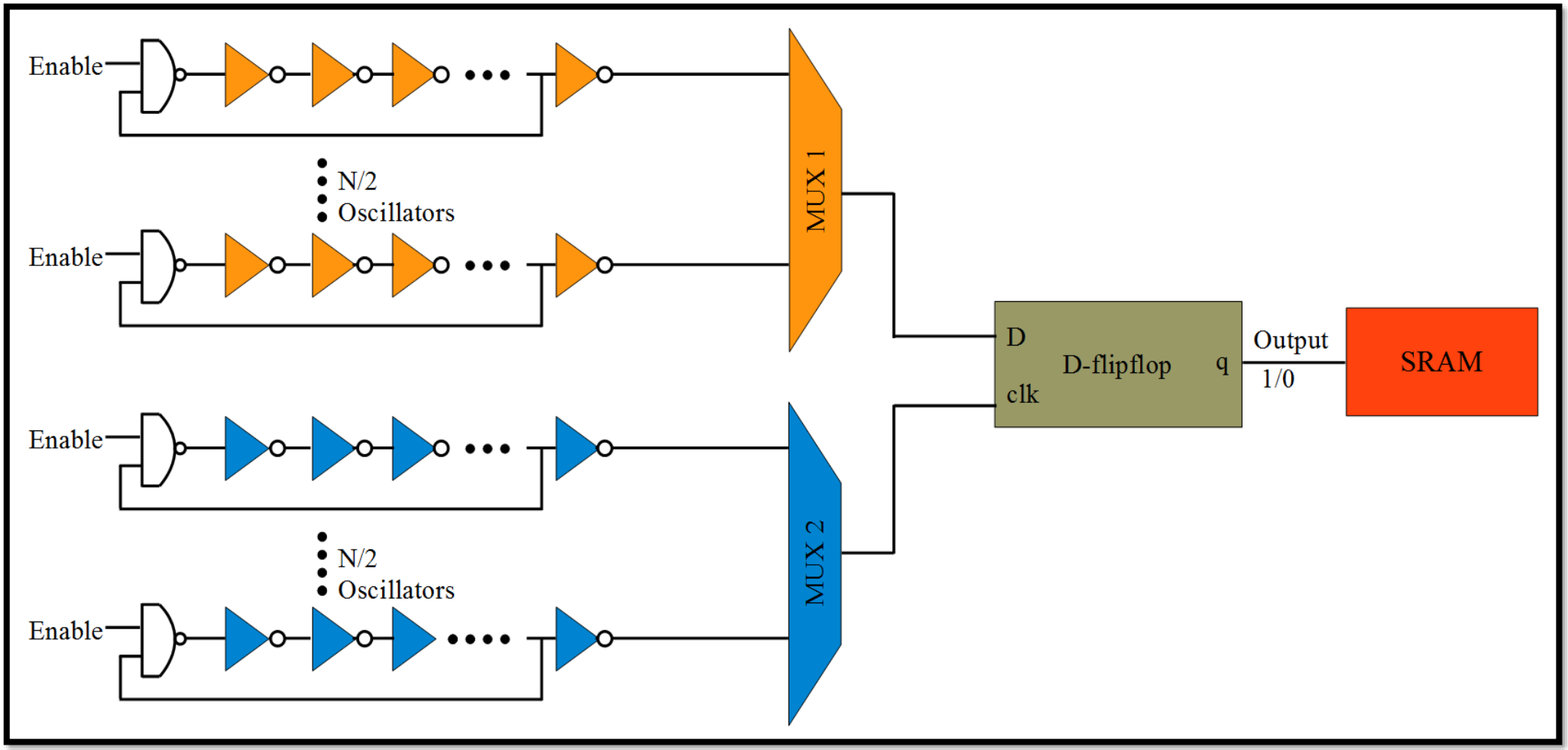


With the same circuit and the same input, we get different output due to process variations.

Speed Optimized Hybrid Oscillator Arbiter PUF



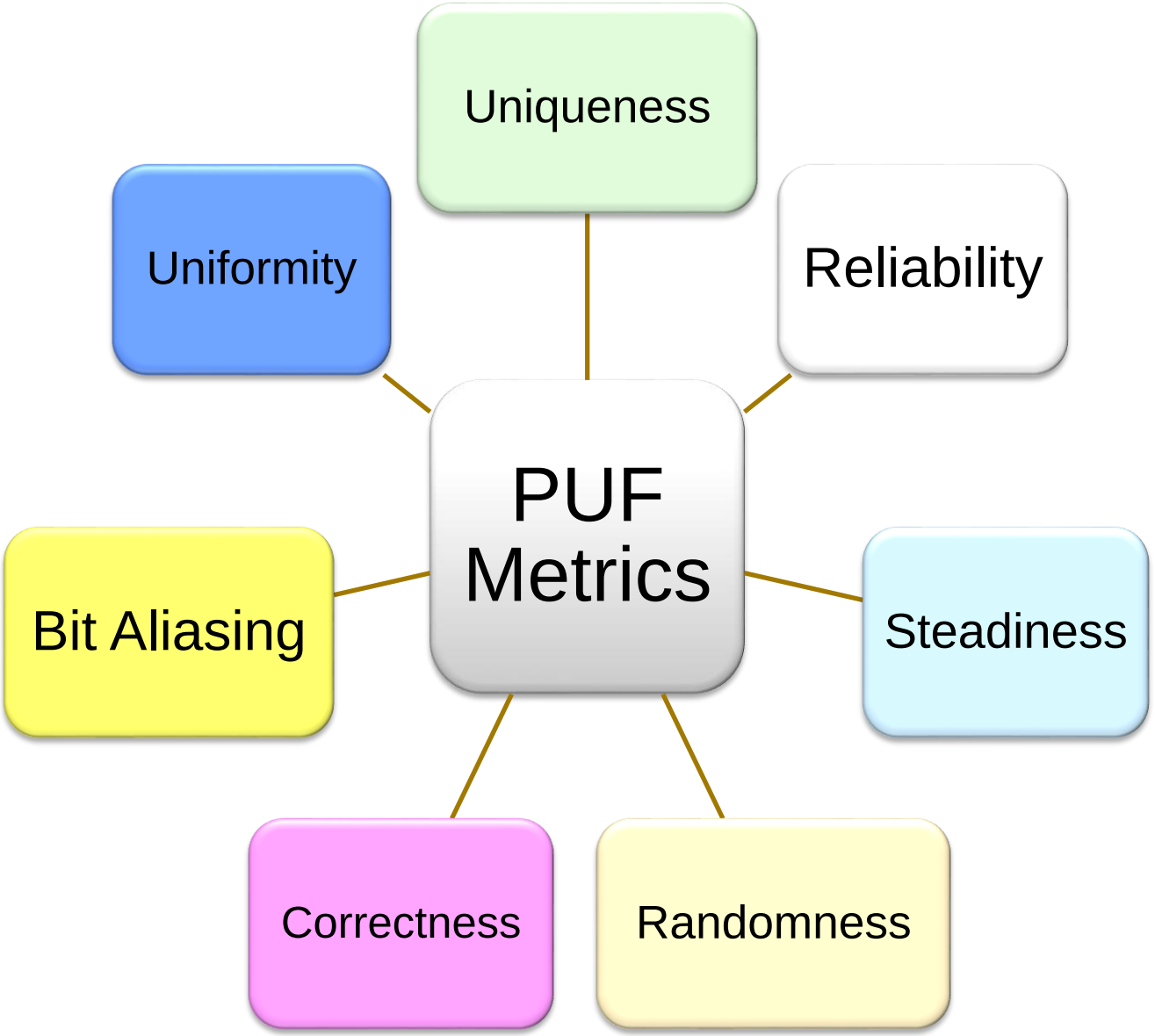
Power Optimized Hybrid Oscillator Arbiter PUF



Performance Metrics …

Can any circuit become PUF?

Performance Metrics



Reliability and Uniqueness

Research Works	Technology	Architecture Used	Reliability (Hamming Distance%)	Uniqueness (Hamming Distance%)
Rahman et al. [4]	90nm CMOS	--	0.92	50
Maiti et al. [3]	180nm CMOS	Ring Oscillator	--	50.72
S. R. Sahoo et al. [2]	90nm CMOS	Ring Oscillator	--	45.78
This Design [1]	14 nm FinFET	Speed Optimized Design	**1.25**	**47.31**
This Design [1]	14 nm FinFET	Power Optimized Design	**2.3**	**52.04**

Conclusion and Future Research

- PUF is a promising Hardware Security Solution.
- Design a Side Channel Resilient PUF.
- Implementation in IoT require Low Power Consumption Designs.
- Implementation in Network requires High Performance Designs.

References

[1] S. P. Mohanty, and E. Kougianos, “Novel FinFET based Physical Unclonable Functions for Efficient Security Integration in the IoT”, in *Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, 2016, pp. 172--177.

[2] S. R. Sahoo, S. Kumar, and K. Mahapatra, “A Modified Configurable RO PUF with Improved Security Metrics,” in *Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems*, 2016, pp. 320–324.

[3] A. Maiti and P. Schaumont, “Improved Ring Oscillator PUF: An FPGAfriendly Secure Primitive,” Journal of Cryptography, vol. 24, no. 2, pp. 375–397, 2010.

[4] 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.

THANK YOU