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

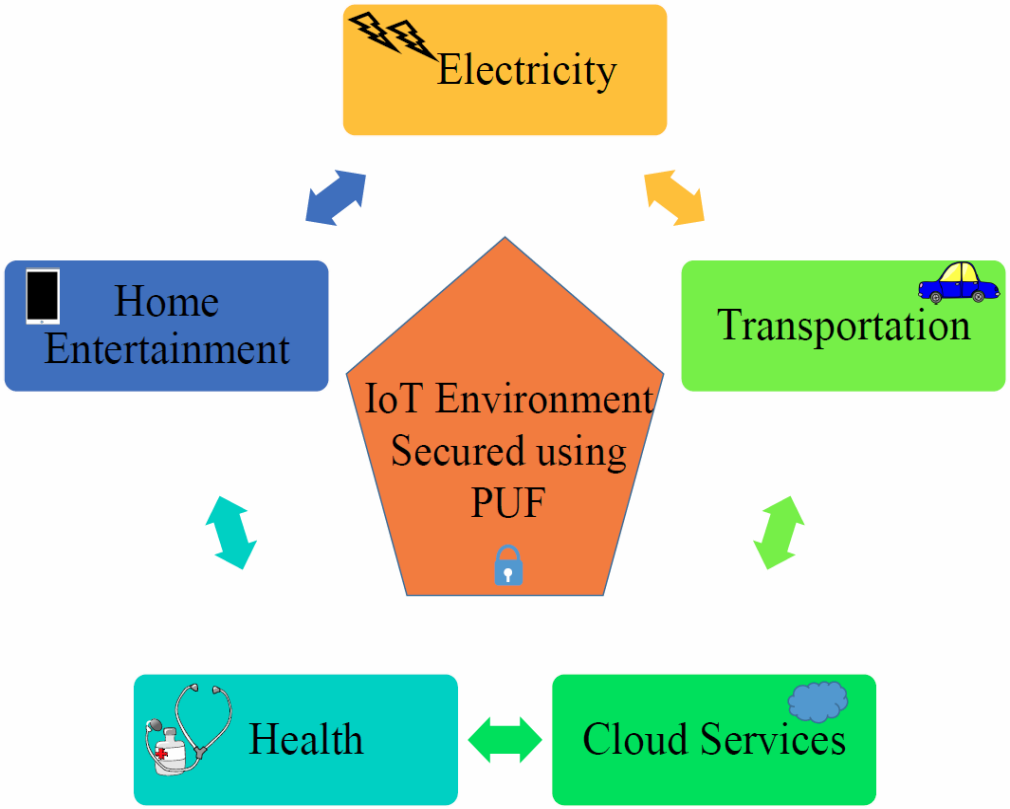
V. P. Yanambaka[1], S. P. Mohanty[2], E. Kougianos[3]
NanoSystem Design Laboratory (NSDL, http://nsdl.cse.unt.edu)
University of North Texas, Denton, TX 76203, USA.[1,2,3]
Email: vy0017@unt.edu[1], saraju.mohanty@unt.edu[2], elias.kougianos@unt.edu[3,]

Outline of the talk

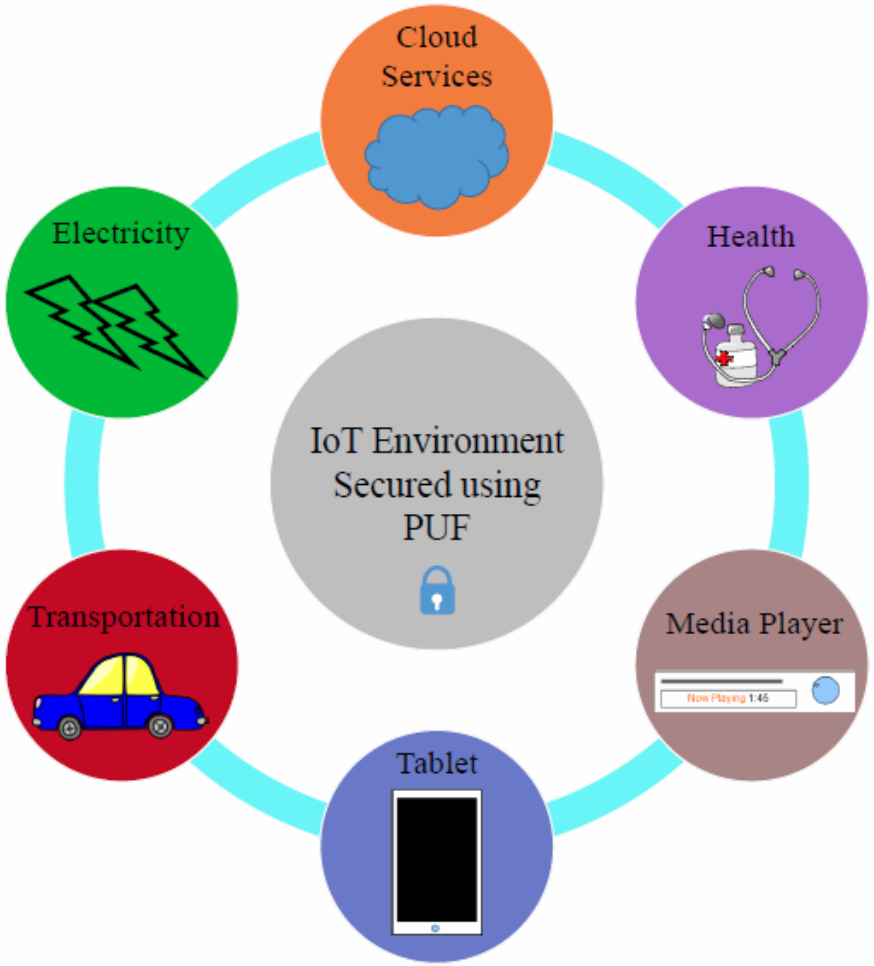
- Internet of Things
- Attacks on IoT Environment
- Novel Contributions
- Physical Unclonable Function
- Proposed Designs of Physical Unclonable Function
- Results and FoMs
- Conclusion and Future Research

Internet of Things

- All the devices will be communicating with each other in the near future
- Human interaction will become very minimal.



Internet of Things – Problems?



Focus of Current Paper

Focus of Current Paper

- Many applications are implemented using IoT environment.
- Healthcare, Home automation and Smart-Cities connect various smart devices, sensors and connecting modules.
- All these require less chip area designs and low power consumption modules.

Focus of Current Paper

- If connected to same server, multiple different keys needed to be generated.
- It should also be fast.
- All devices need different encryption keys that need to change if necessary.
- This can be achieved using Physical Unclonable Function.

Physical Unclonable Function

- PUF uses variability of different devices in manufacturing phase.
- Transistors are subject to many process and mismatch variations affecting the device geometry.
- Physical Unclonable Function takes advantage of those variations to generate a key.

Physical Unclonable Function

- Security using hardware.
- Why Physical Unclonable Function (PUF)?
  - Key not stored anywhere in memory.
  - Not possible to generate on an other machine.
  - Robust and Low Power.
  - Can use different architectures with different designs.

Types of PUF

- Many different architectures of PUF
  - Static Random Access Memory PUF.
  - Ring Oscillator PUF.
  - Memristor Crossbar PUF.
  - Arbiter PUF.
  - XOR PUF, etc.,

Novel Contributions of This Paper

- Two Designs of Physical Unclonable Function are Proposed :
  - Power Optimized Hybrid Oscillator Arbiter PUF
  - Speed Optimized Hybrid Oscillator Arbiter PUF
- Each of the designs is specifically designed to be incorporated in the respective IoT application.

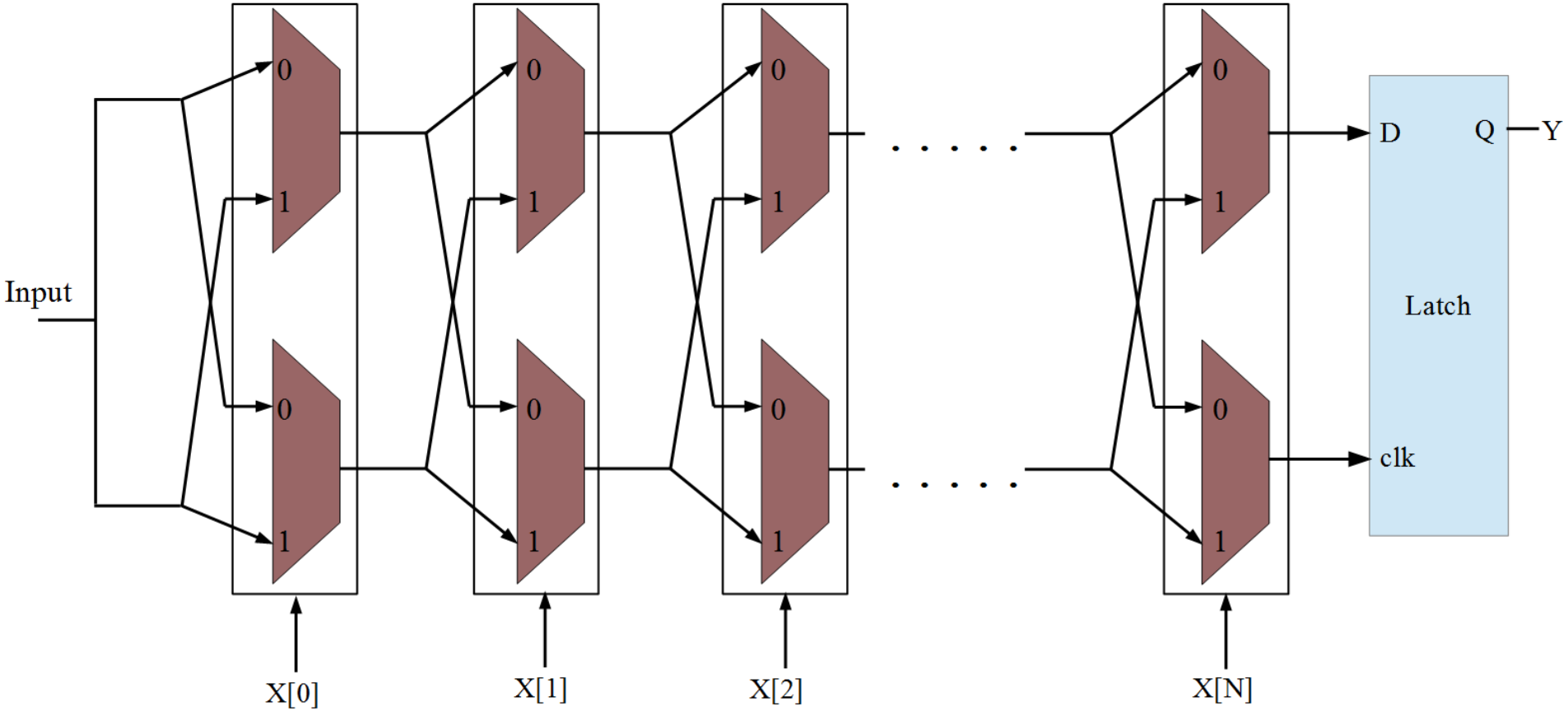
Process & Mismatch Variation

- Process Variation and Mismatch Variation is unavoidable while manufacturing any device.
- Especially geometry of the device being manufactured is greatly affected.
- Physical Unclonable Function takes advantage of those variations to generate an encryption key.

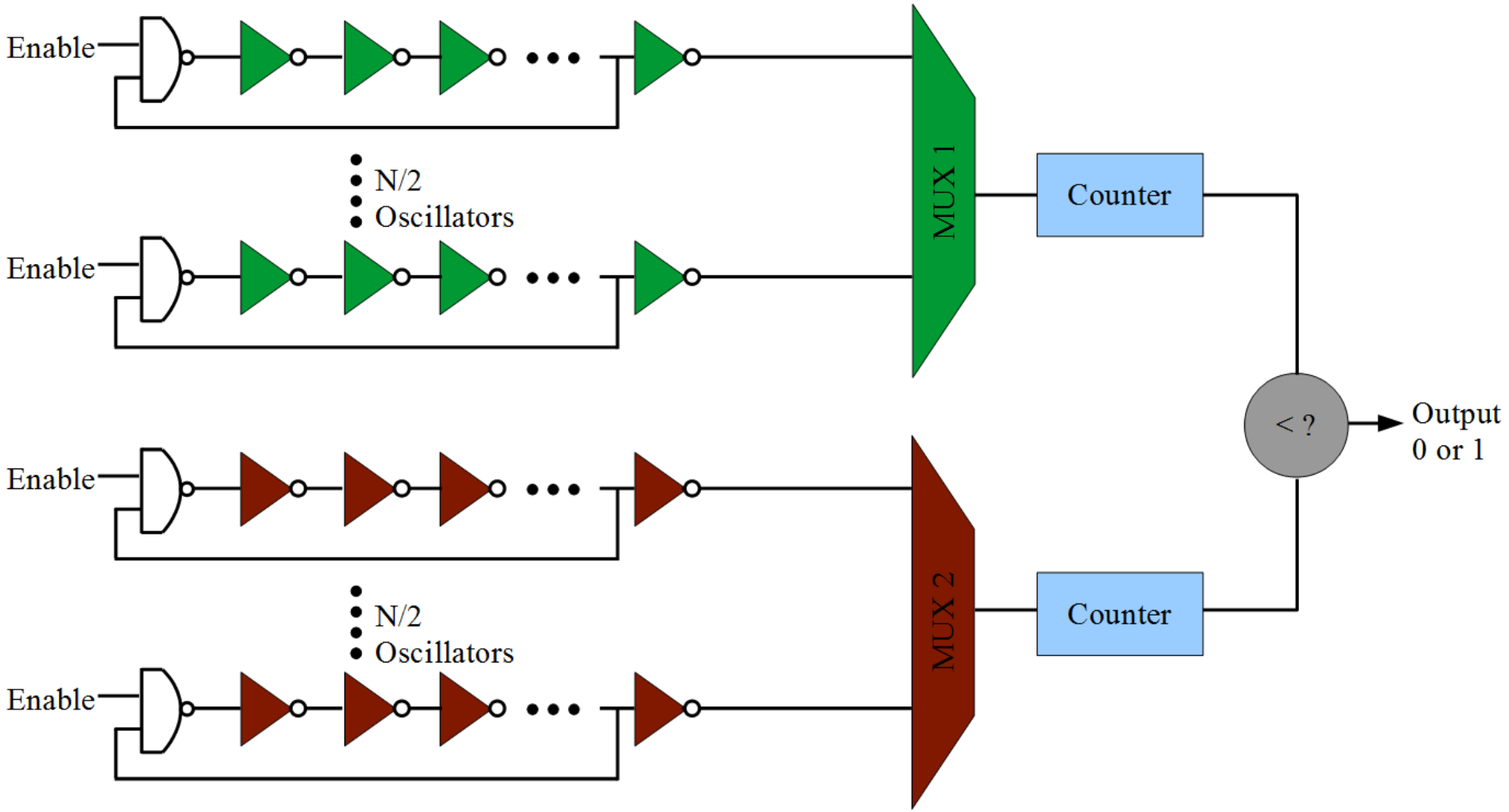
How PUF Works?

- Transistors are involved in most designs.
- Gate delay is the main focus.
- Gate delay produced in different transistors give distinct outputs in systems.
- Other architectures (for eg., Memristor) also take advantage of geometric variations in key generation.

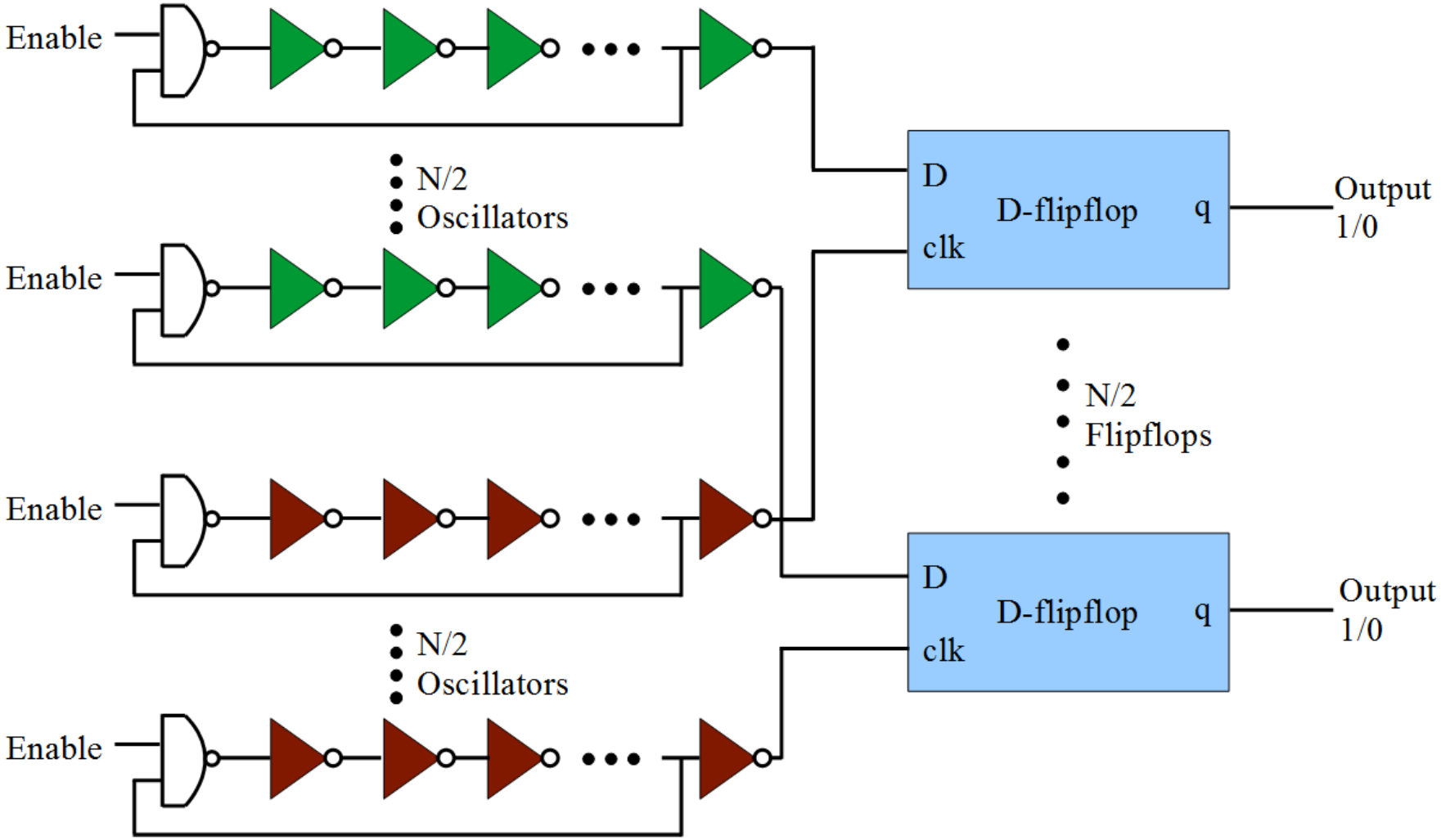
Traditional Arbiter PUF



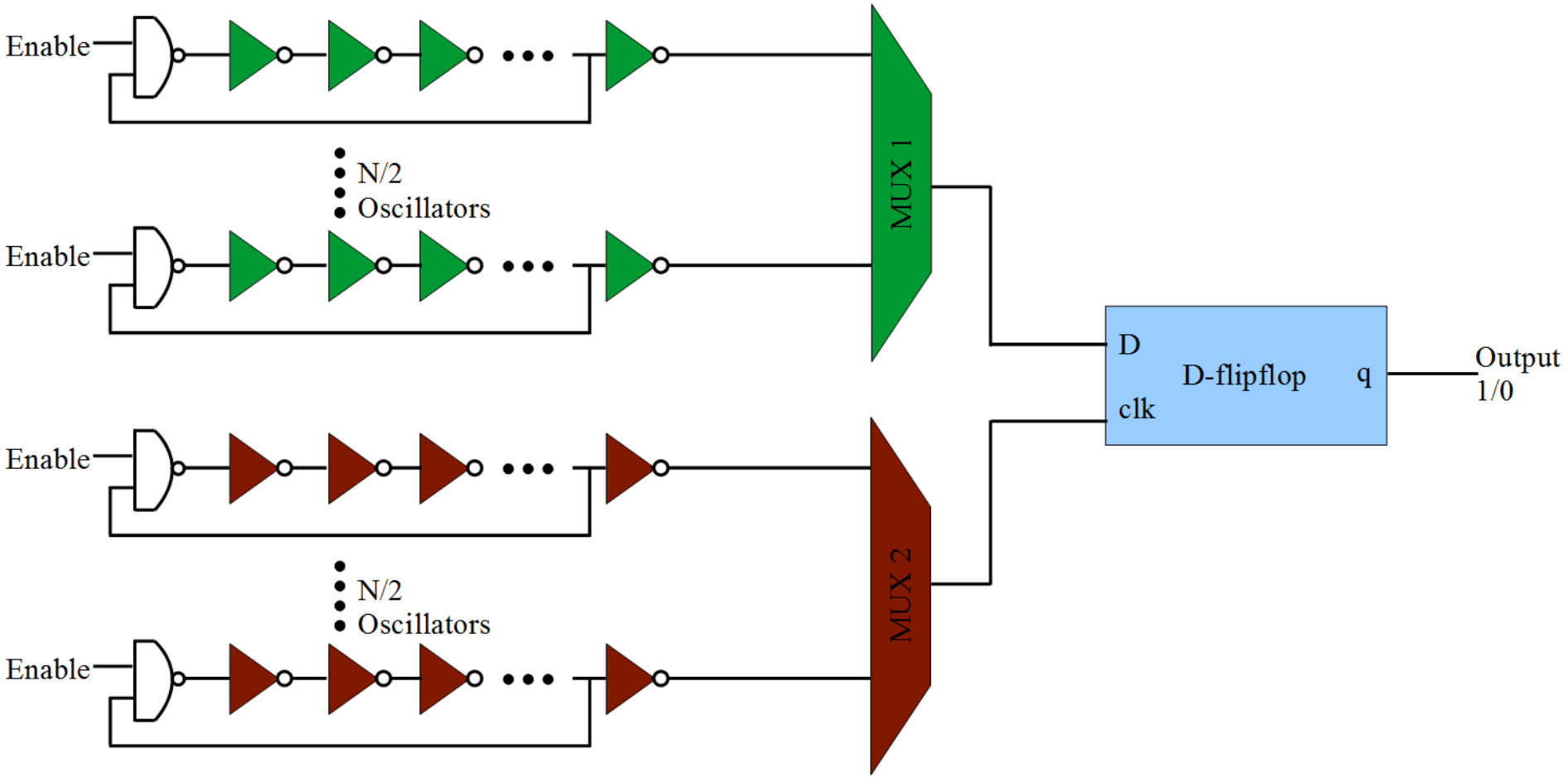
Traditional Ring Oscillator PUF



Speed Optimized Design



Power Optimized Design



Circuit Level of One Cell

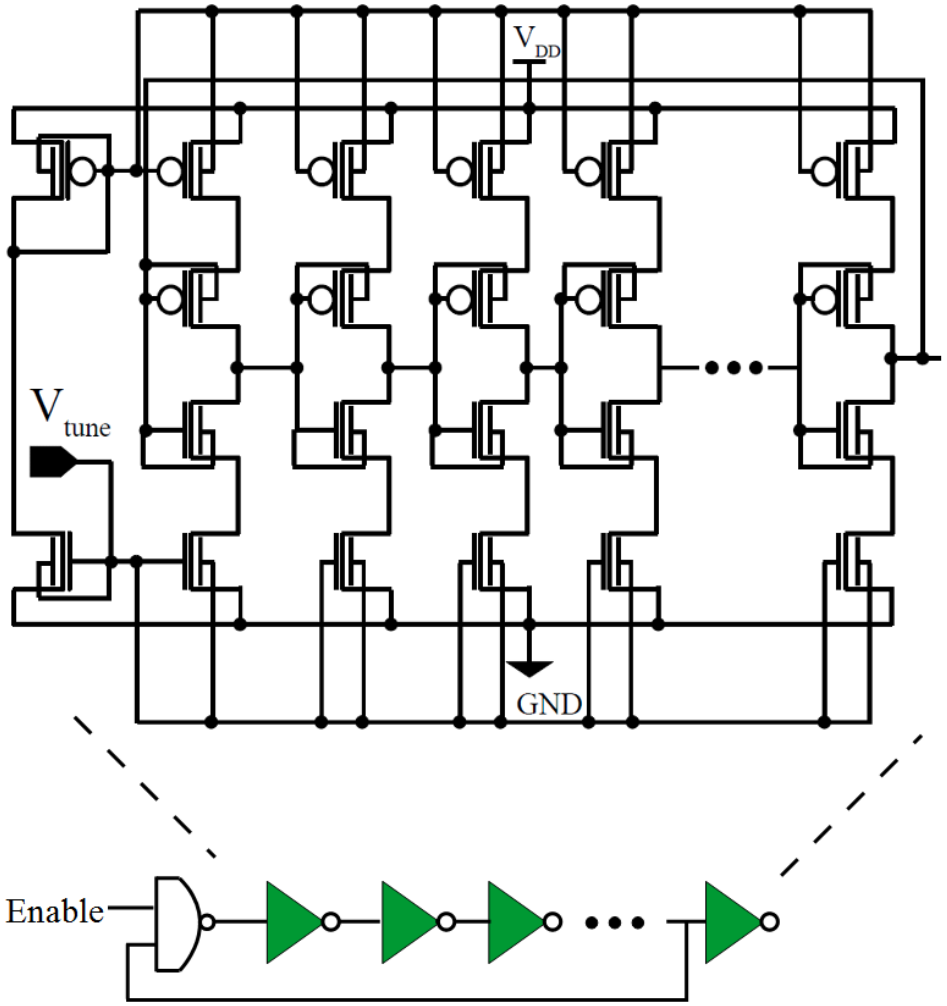


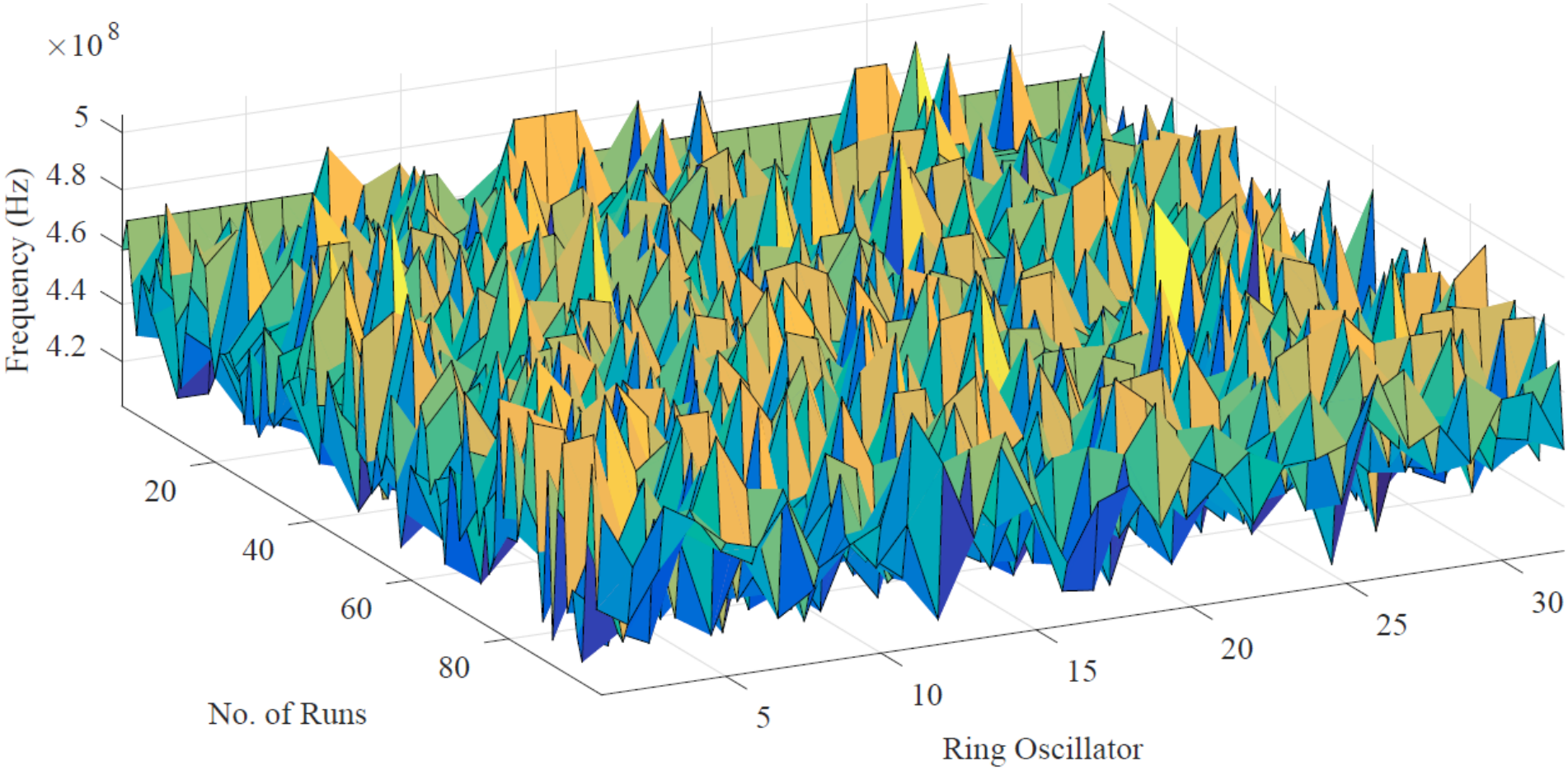
Figure of Merits

- Uniqueness
  - Hamming distance of keys generated should be 50% under ideal conditions.
  - Frequencies of different Ring Oscillators are also presented to show the uniqueness

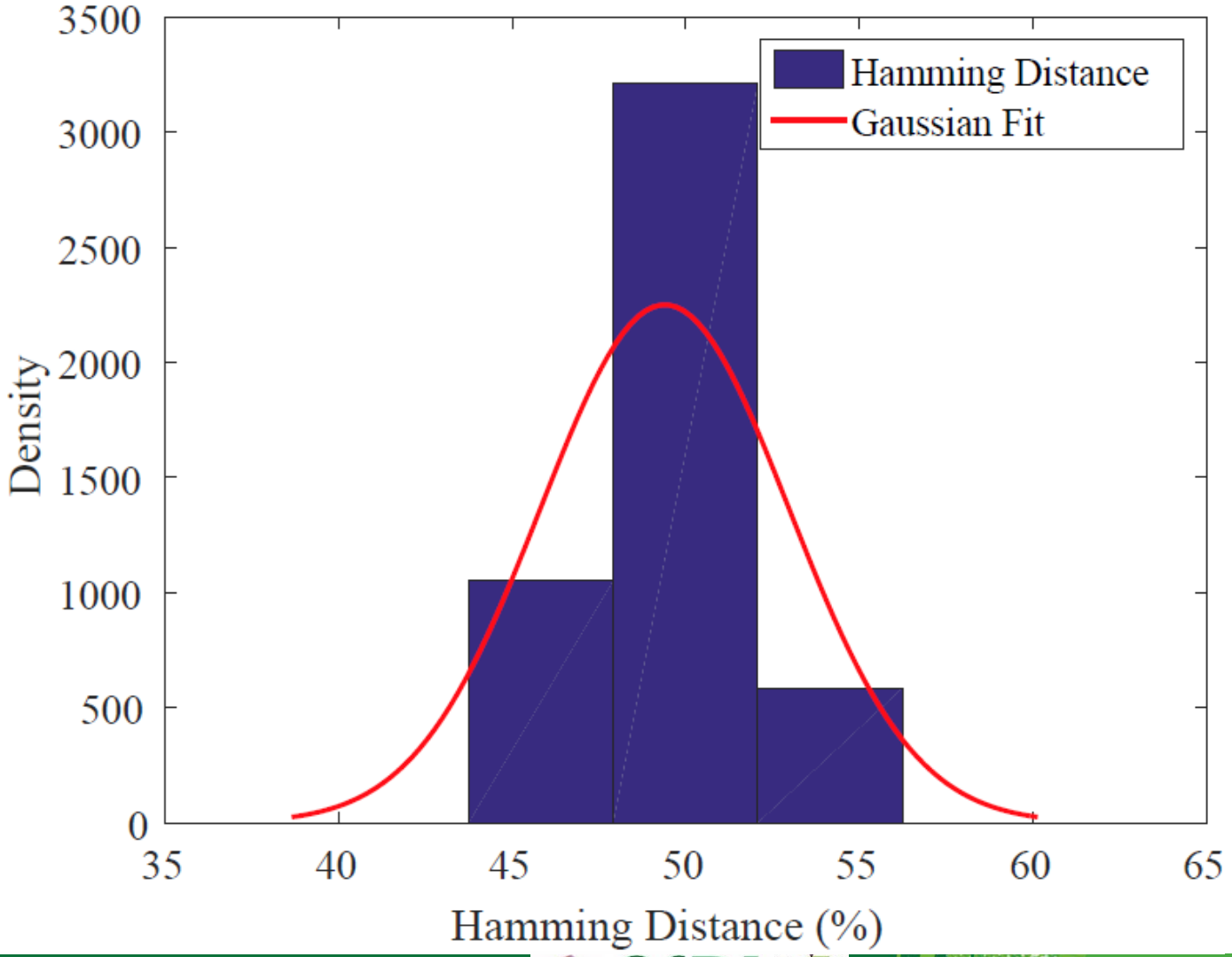
Figure of Merits

- Reliability
  - Creating same key with no change in challenge bits.
  - But in this case, same key should not be generated.
- Average Power
  - Average Power of MKG PUF is the sum of all leakage powers and the dynamic power.

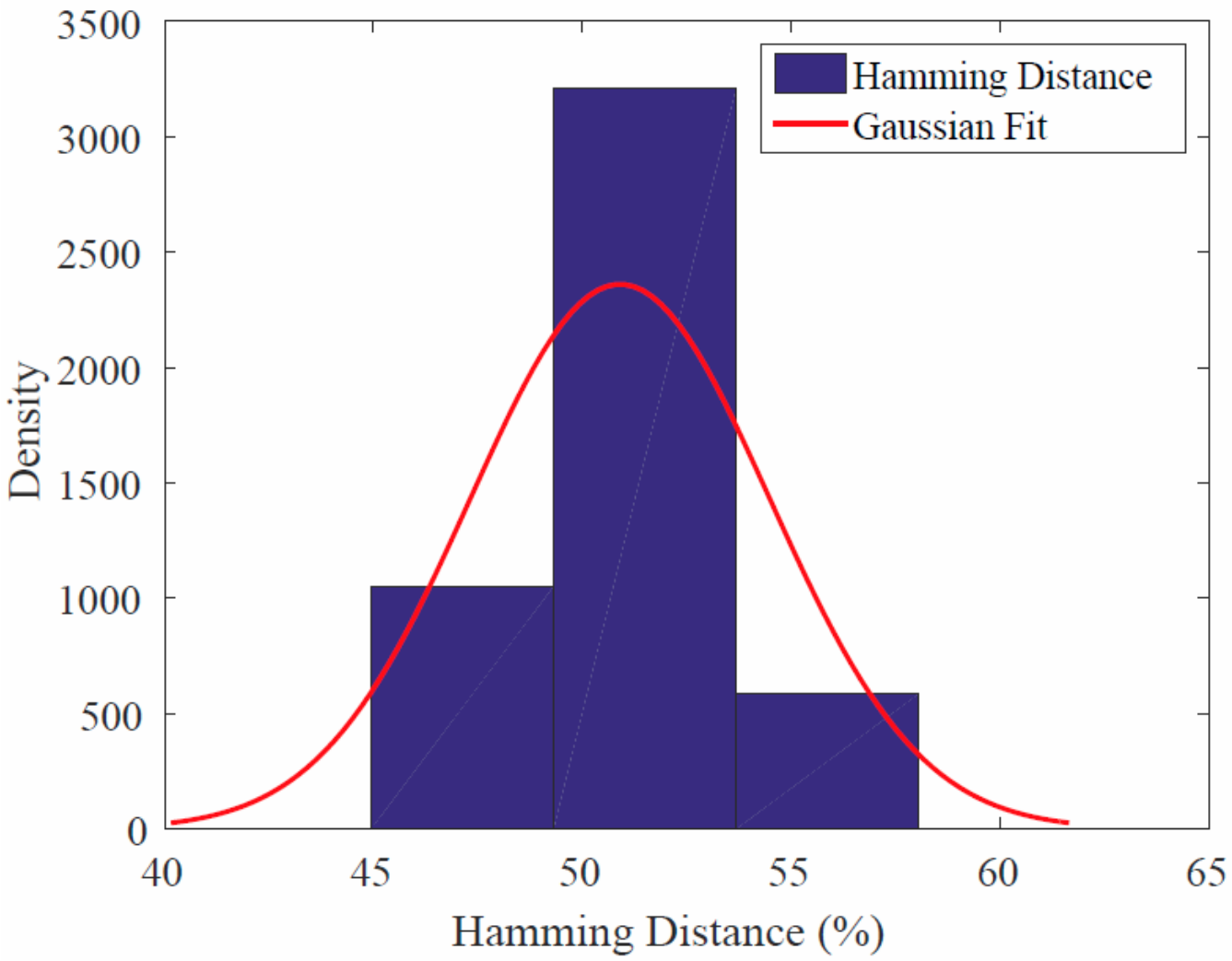
Oscillation Frequencies of ROs



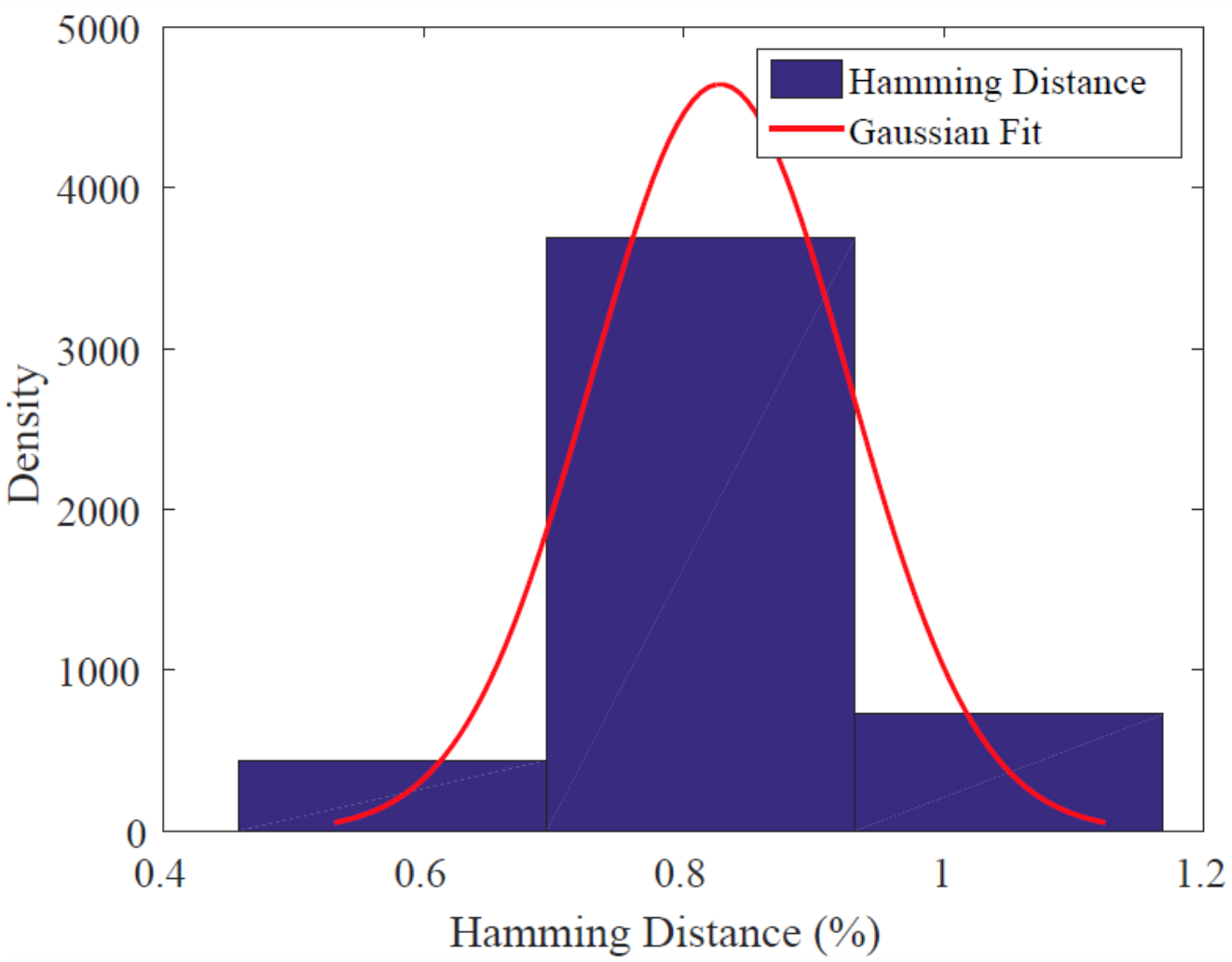
Hamming Distance – Speed Optimized



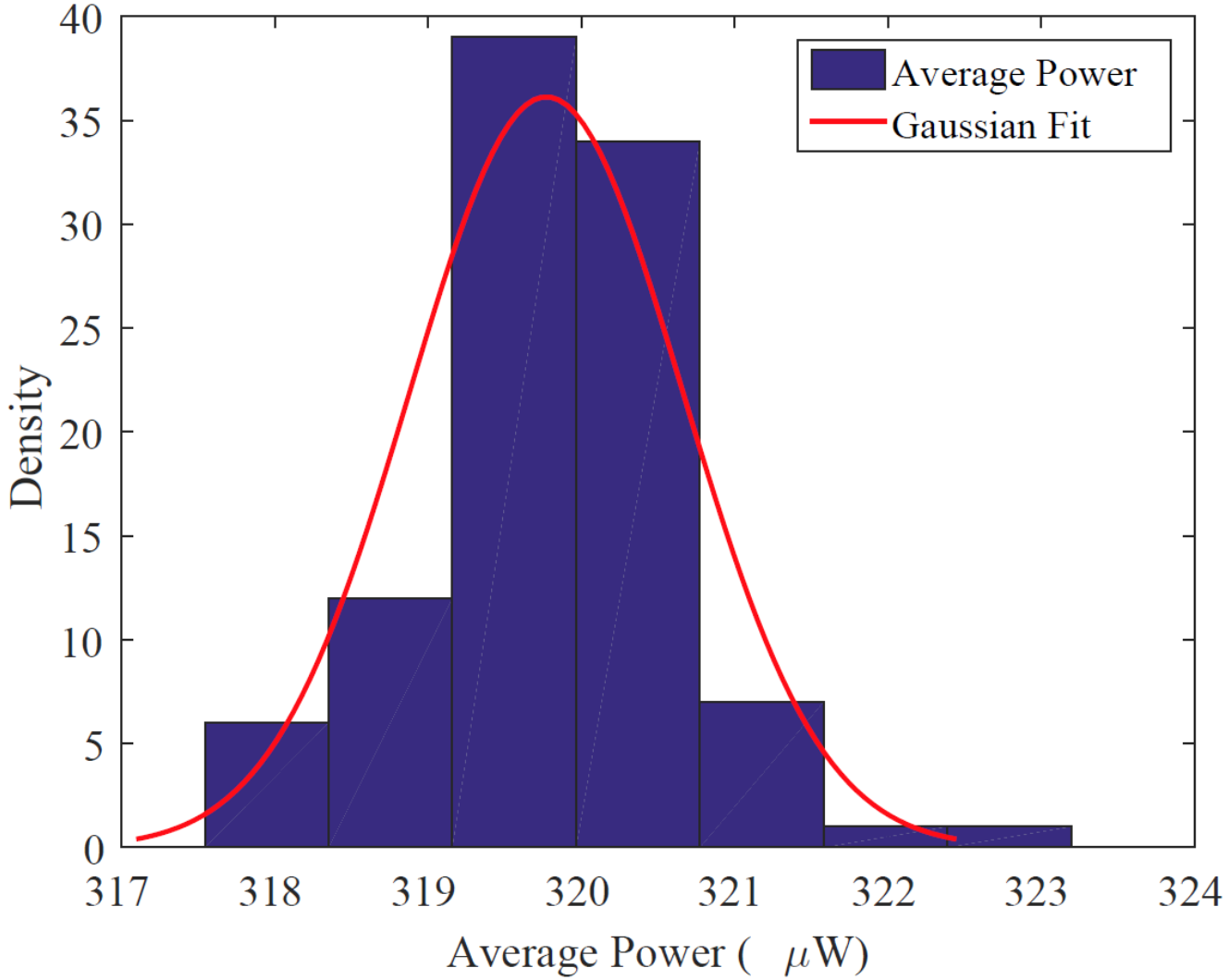
Hamming Distance – Power Optimized



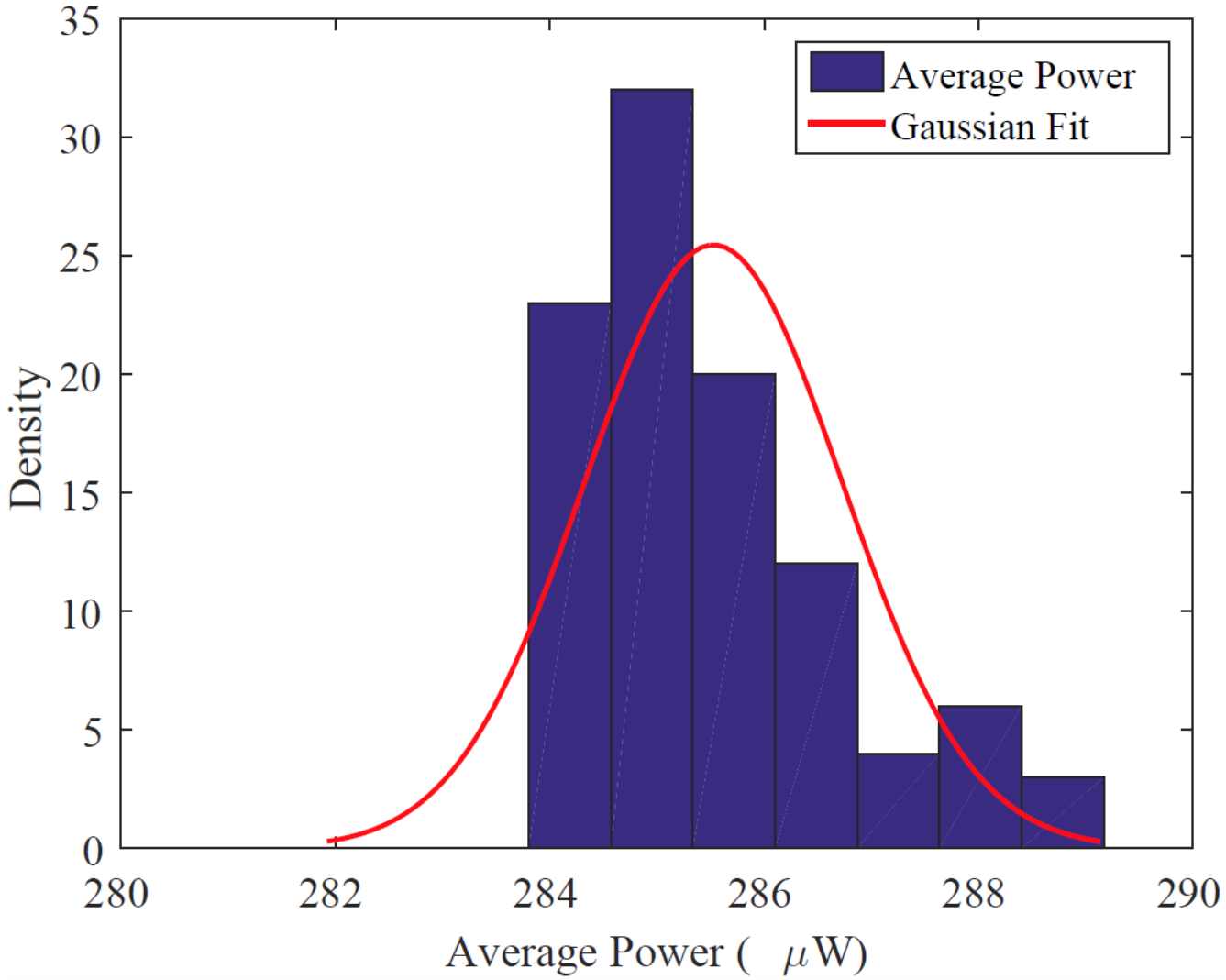
Intra – PUF Hamming Distance



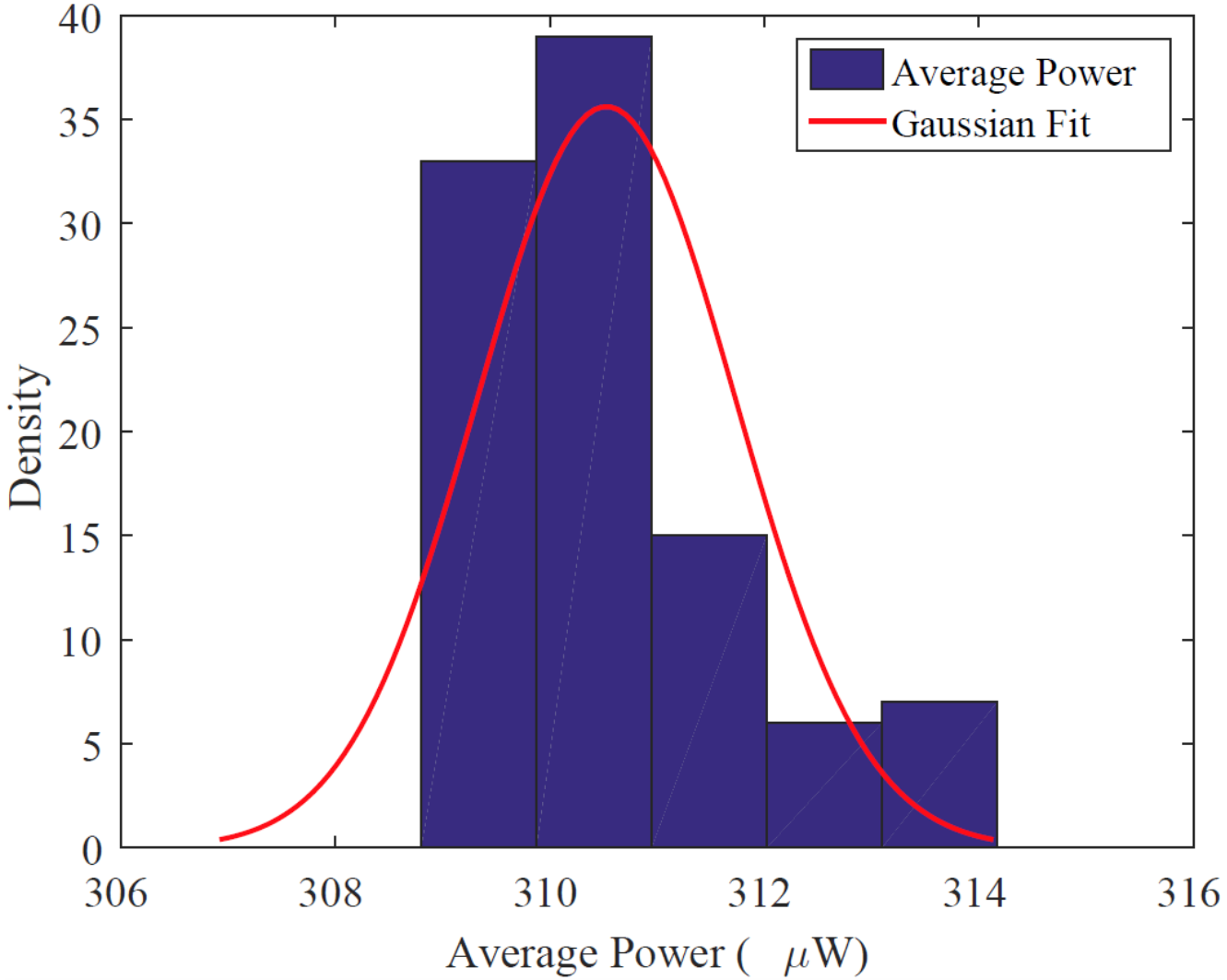
Traditional RO Average Power



Speeds Optimized Design Average



Power Optimized Design Average Power



Power Optimized Design Average Power

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

Conclusion

- Two designs of PUF were proposed :
  - Power Optimized Hybrid Oscillator Arbiter PUF.
  - Speed Optimized Hybrid Oscillator Arbiter PUF.
- PUF for both low power devices and high performance devices.
- Can be integrated into the devices.

Future Research

- Design ultra low-power models of each.
- Speed optimized design generates one key per module.
- Designing Configurable Hybrid Oscillator Arbiter PUF.
- Incorporate more stable Ring Oscillator design.

THANK YOU