Secure Multi-Key Generation Using Ring Oscillator Based Physical Unclonable Function

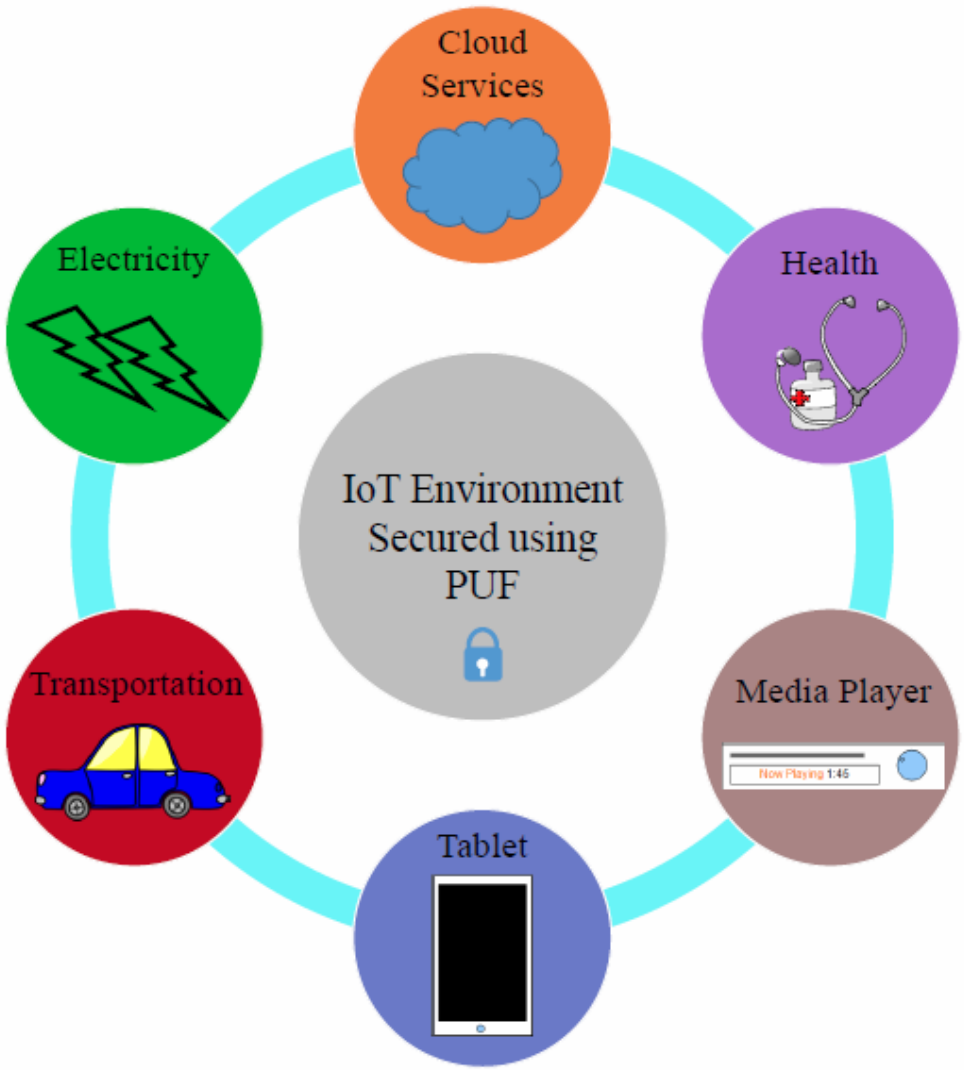
V. P. Yanambaka[1], S. P. Mohanty[2], E. Kougianos[3] and J. Singh
NanoSystem Design Laboratory (NSDL, http://nsdl.cse.unt.edu)
University of North Texas, Denton, TX 76203, USA.[1,2,3]
PDPM IIIT Jabalpur, India[4].
Email: vy0017@unt.edu[1], saraju.mohanty@unt.edu[2], elias.kougianos@unt.edu[3], jawarsingh2002@gmail.com[4]

Outline of the talk

- IoT and Attacks
- Novel Contributions
- Physical Unclonable Function
- Multi-Key Generating PUF
- Proposed Designs of Physical Unclonable Function
- Results and FoMs
- Conclusion and Future Research

Internet of Things

- In the IoT era, number of devices connected to internet are exponentially increasing.



Internet of Things

- Internet of Things (IoT) is different devices connected to each other in a network.
- IoT in a household environment is considered in this paper.
- Every appliance that we can think of can be connected to a network and to the outside world – Problem?

Issues with IoT Implementation

- "Cyber Attacks" are increasing day-by-day.
- Not even major companies are able to protect our data they have.
- Sony was attacked affecting many datacentres leading to cancellation of a movie release.
- J. P. Morgan Chase was attacked exposing customer information.

Solving the Issue

- Encryption and Decryption – One of the main areas of attacks.
- Highly encrypted data is less susceptible to attacks.
- Generating an encryption key that is less susceptible to attacks and less predictable.
- Hence the Physical Unclonable Function.

Physical Unclonable Function

- Process Variation is unavoidable while manufacturing any device.
- 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

- Simple circuit to generate a key.
- Not possible to generate the same key using any other circuit.
- With a small change in input, key changes.
- Many designs are available depending on various architectures used.

Types of PUF

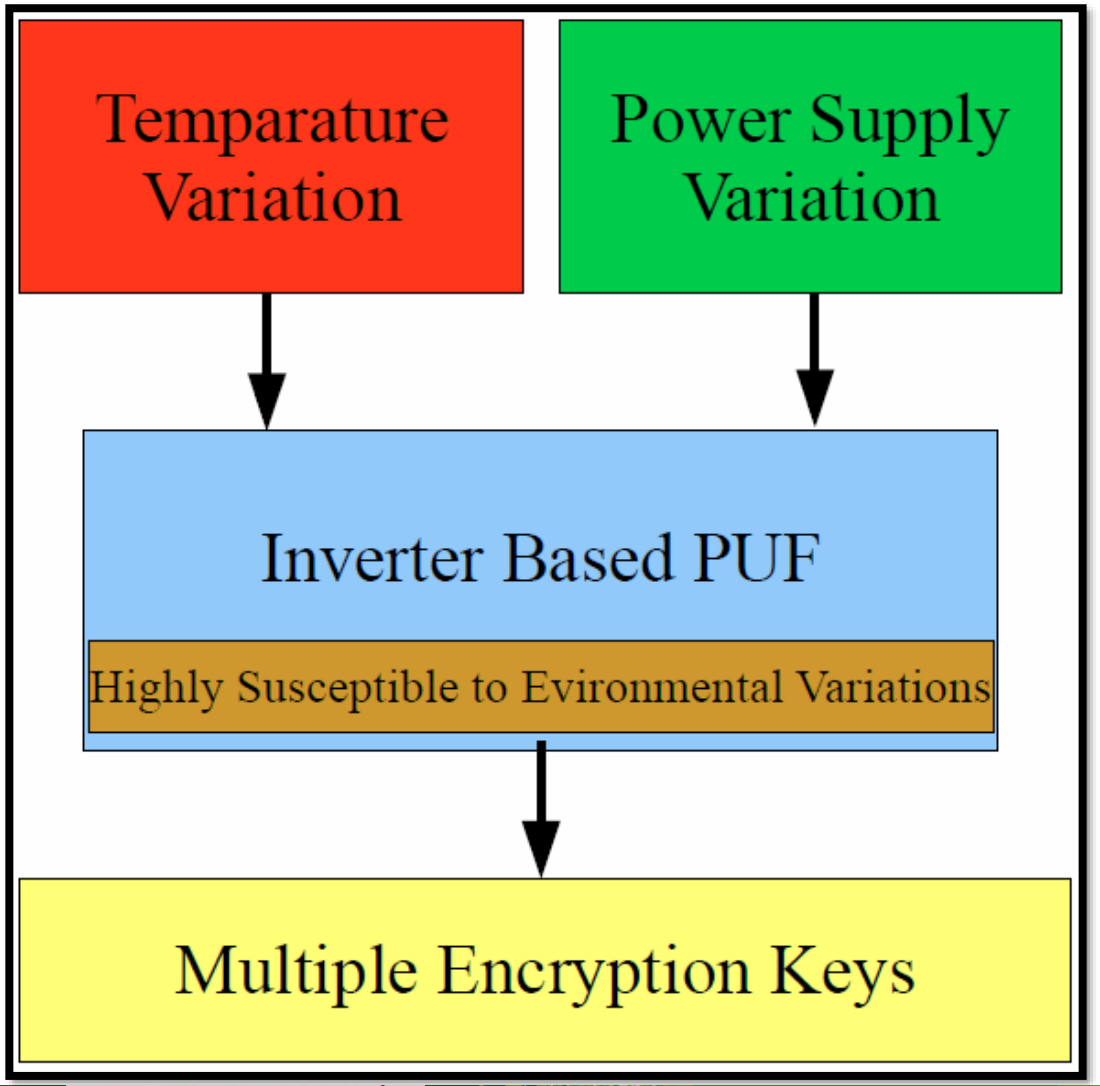
- Arbiter PUF designed using Multiplexers and Flip-flop.
- SRAM PUF designed using SRAM modules.
- RO PUF using different architectures of Ring Oscillator.
- Research shows most of the designs are not reliable.

Novel Contributions of This Paper

- Two Designs of Physical Unclonable Function are Proposed :
  - Power Optimized Multi-Key Generating PUF
  - Speed Optimized Multi-Key Generating PUF
- Each of the designs is specifically designed to be incorporated in the respective IoT application.
- For every run, a new key will be generated.

Novel Contributions

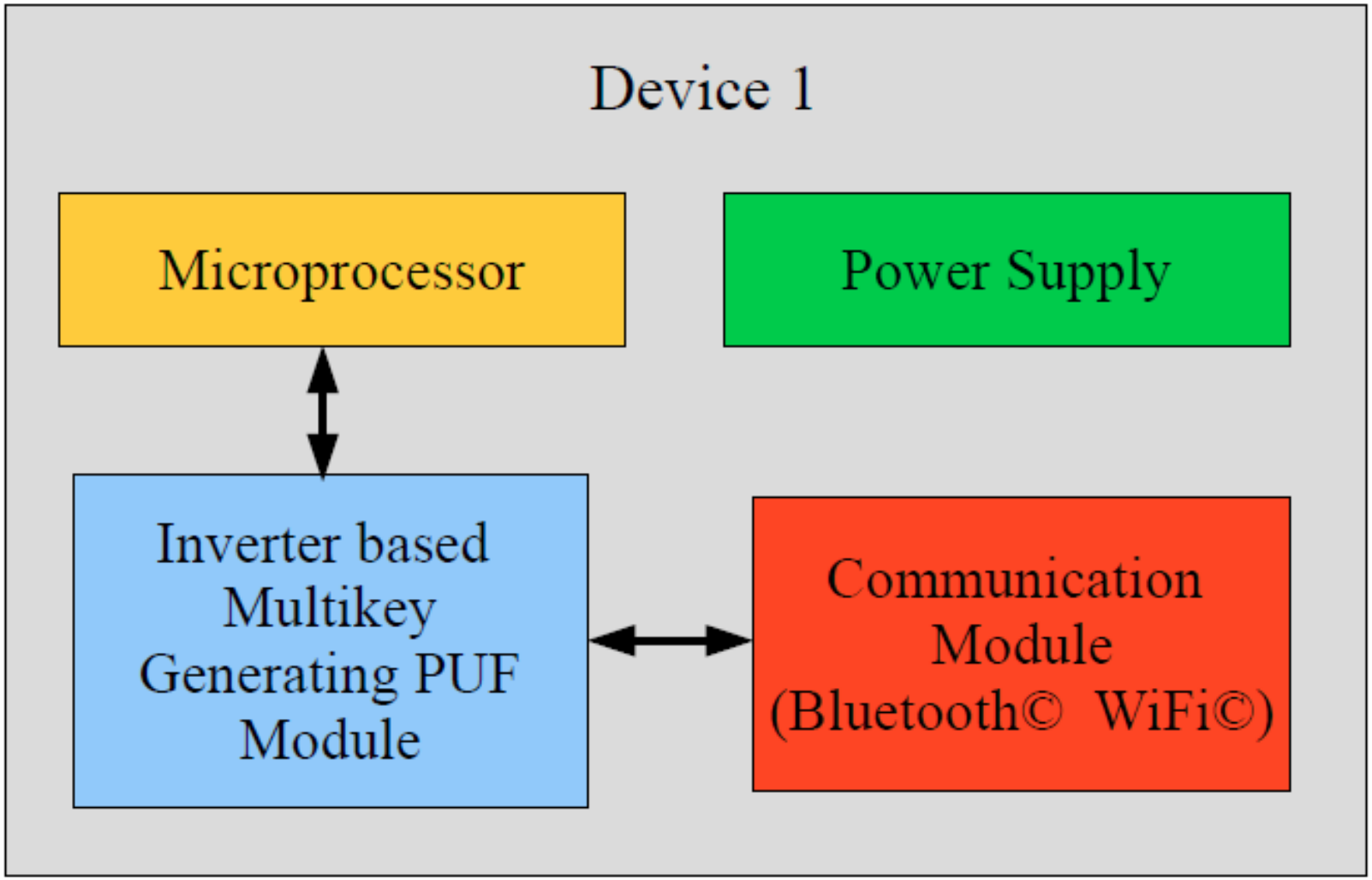
- This module works with the variations in environmental and supply voltage variations.



Multi-Key Generating PUF

- Multi-Key Generating (MKG) PUF generates a new key every time the circuit is run.
- Communication devices with MKG PUF will be much more secure.
- Different protocols have their own proprietary ways of encryption all of which can use the keys generated using this PUF.

MKG PUF Implementation



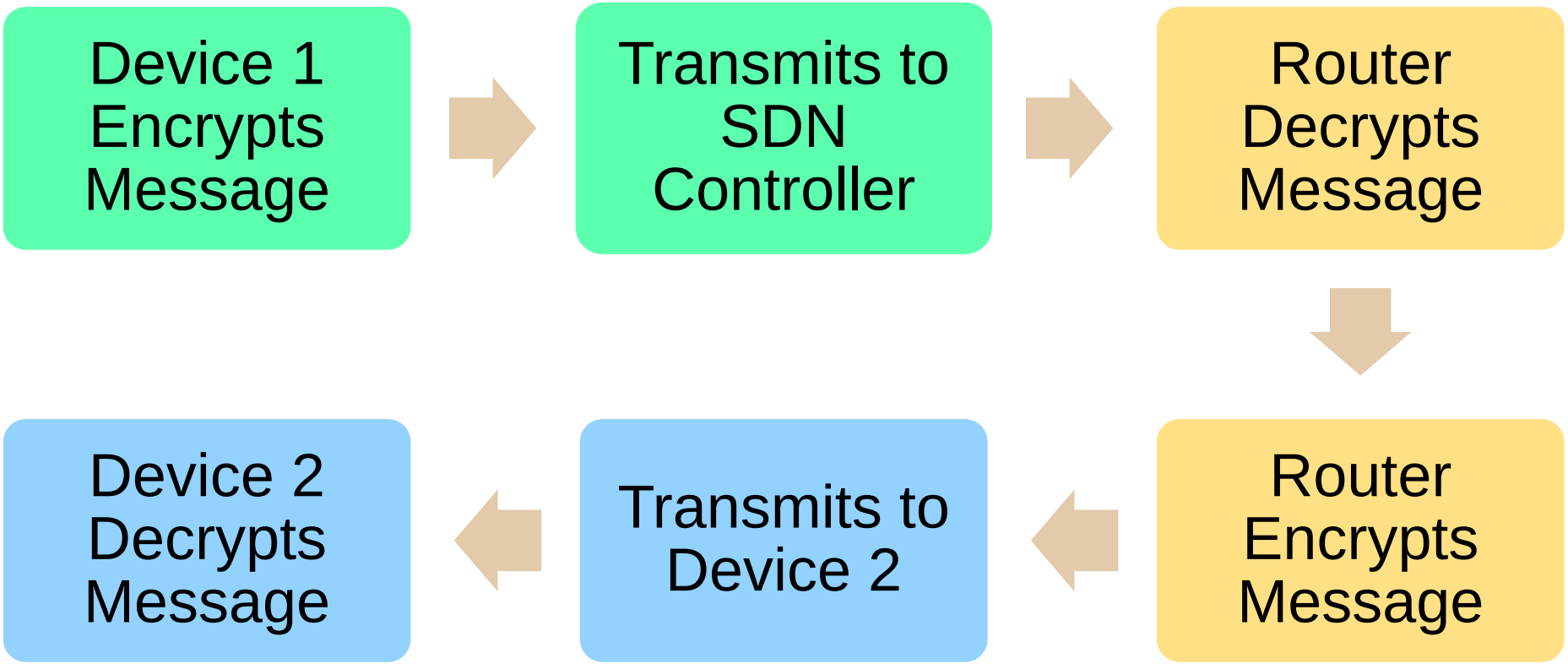
Device – to – Device Communication

- Device 1 generates data in microprocessor.
- Device 1 is connected to Device 2 using Bluetooth® or any other wireless or wired communications.
- Main idea of MKG PUF is to generate the keys for different communication modules.

Device – to – Device Communication

- Key generated and data to be transmitted will be given to the communication module.
- Communication module encrypts the data and transmits it to destination.
- Decryption will be performed at the destination using the respective protocols.

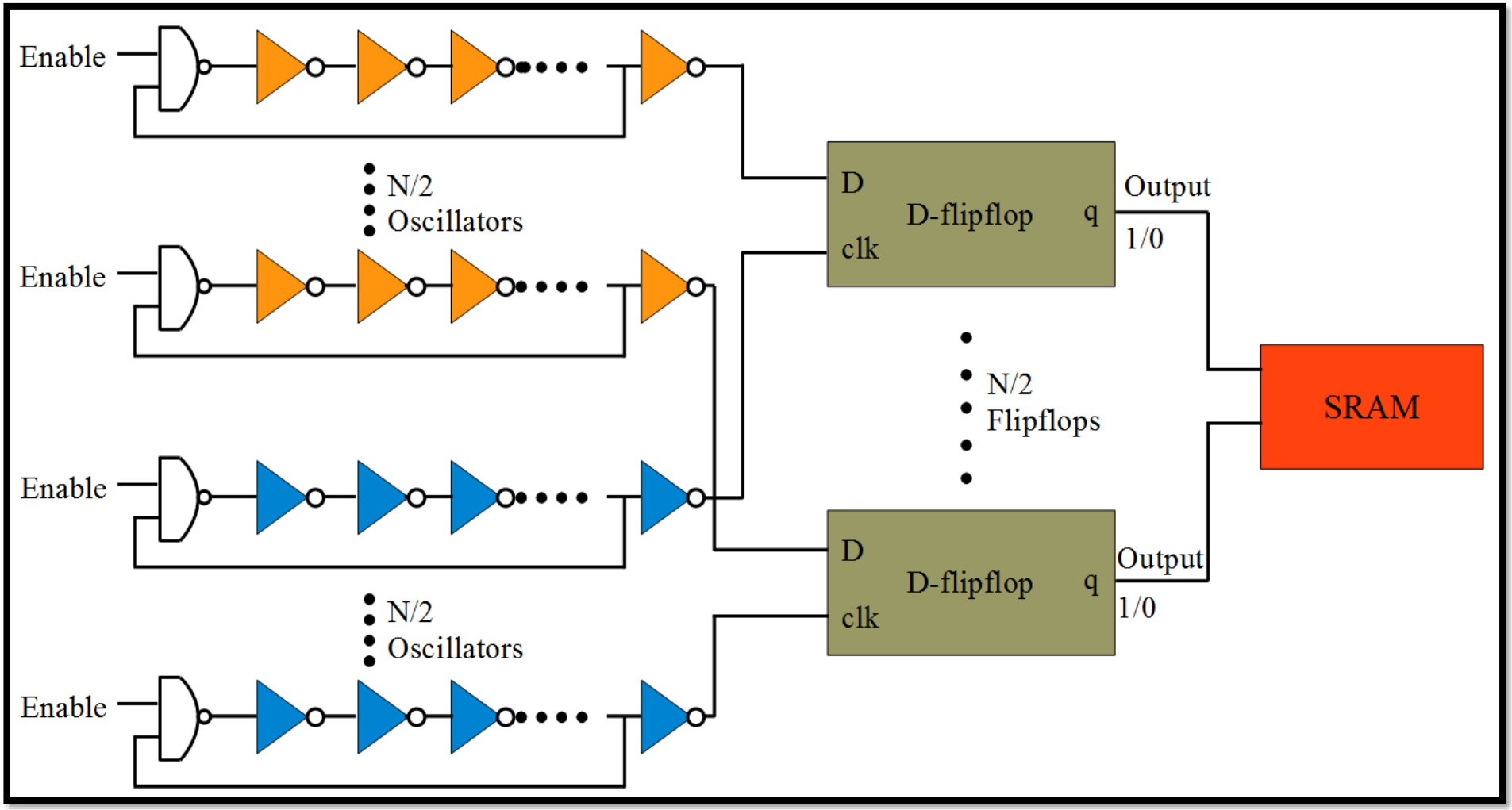
Device – to – Device Communication



Proposed Designs of MKG PUF

- Two designs are proposed.
- Speed Optimized to incorporate in devices requiring high data processing rates.
  - Network Switches, Routers, etc.,
- Power Optimized to be incorporated in devices with low power consumption.
  - Mobile phones, Smart devices, etc.,

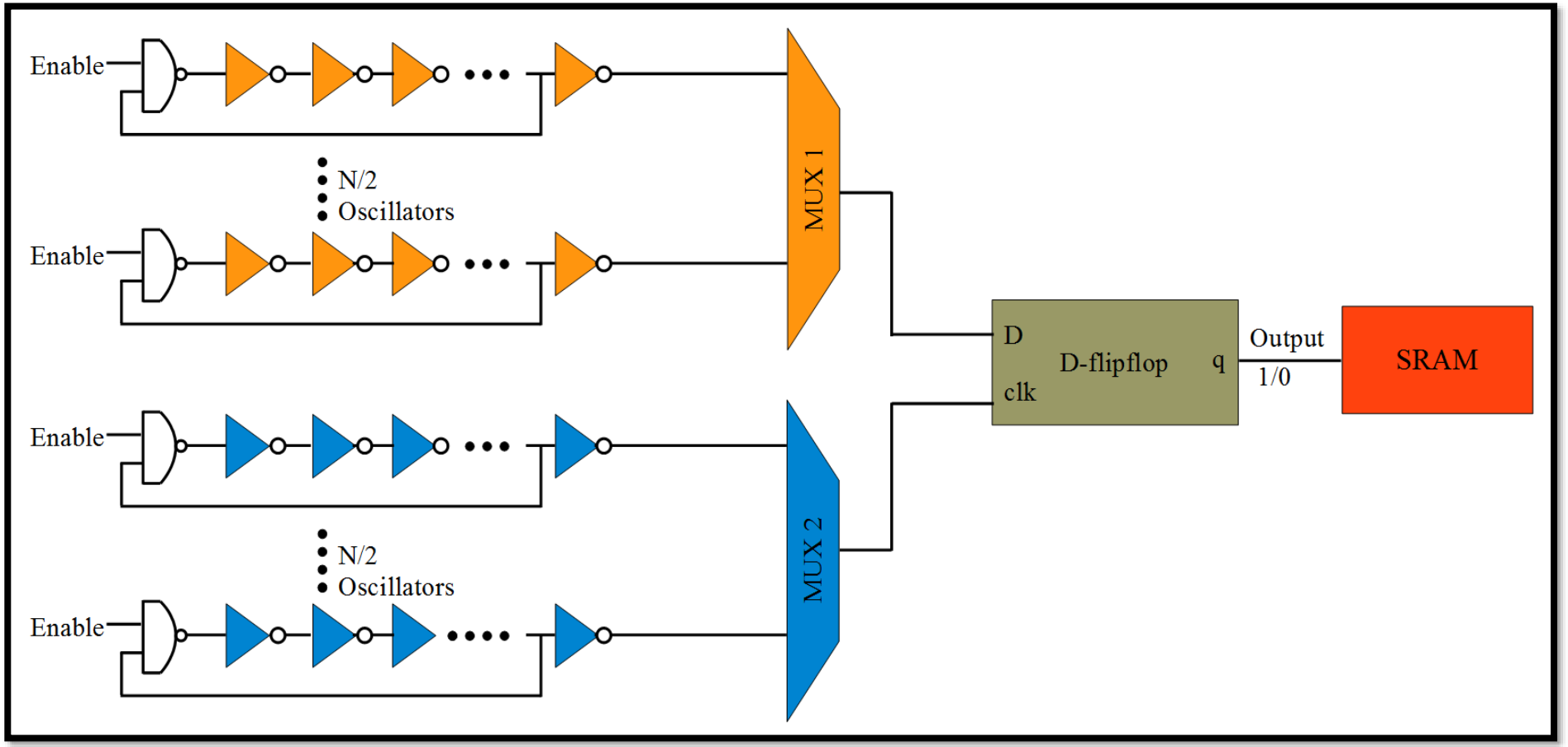
Speed Optimized MKG PUF



Speed Optimized MKG PUF

- Ring Oscillators generate the oscillations.
- Two sets of Ring Oscillators.
- ROs from set1 connected to the D-Input of Flip-Flop.
- ROs from set2 connected to clock of Flip-Flop.
- For N-ROs, N/2 Flip-Flops are needed.
- High speed and more power consumption.

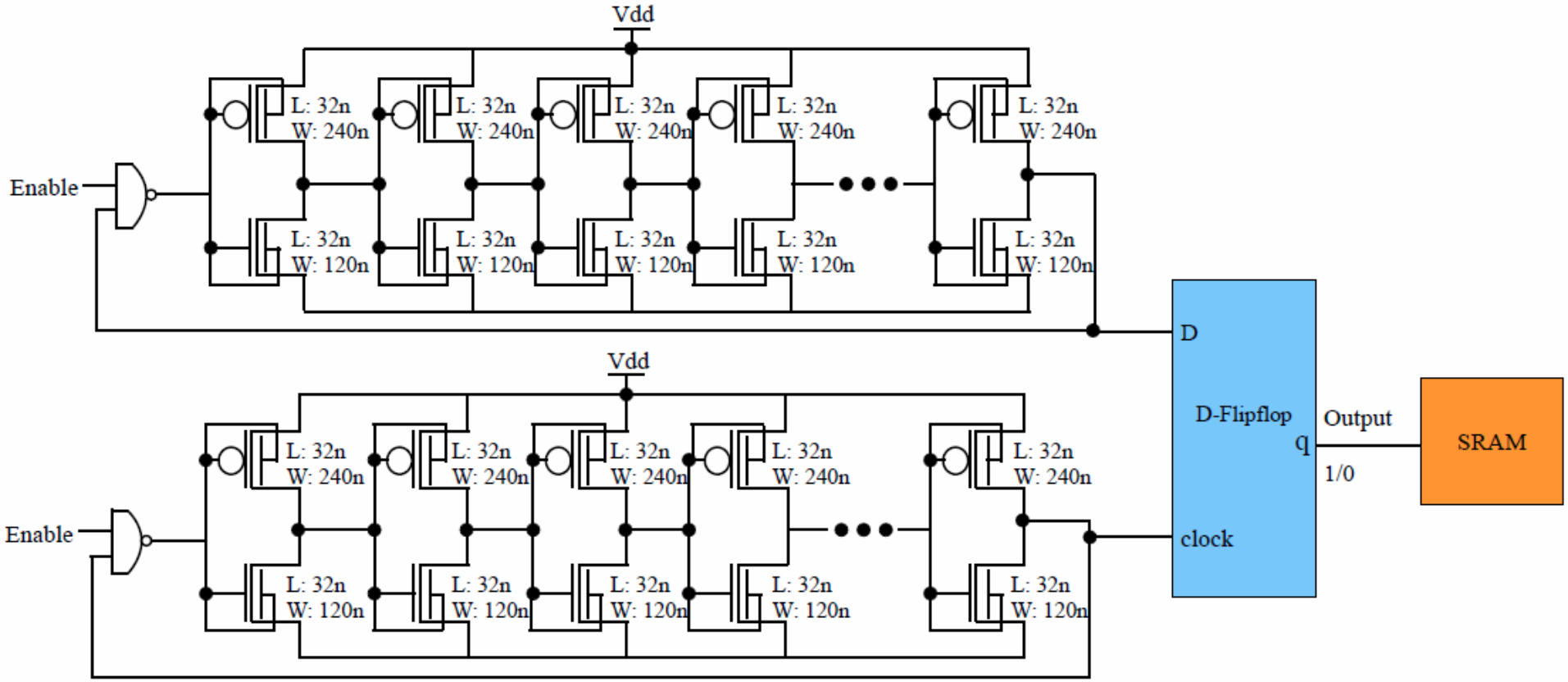
Proposed Designs of MKG PUF



Power Optimized MKG PUF

- Similar to Speed Optimized MKG PUF but with Multiplexers.
- N-ROs but only one Flip-Flop.
- Multiplexers select the Ring Oscillators to be fed to the Flip-Flop.
- Less components for low power consumption and less chip area.

Circuit Level Design of MKG PUF



Circuit Level Design of MKG PUF

- Conventional inverter is used to design MKG PUF.
- RO frequency is highly affected by environmental and power supply variations.
- Multi Vdd is used to change the power supply used to change the frequency of each of the RO.
- This changes the output frequency and thus the output key of PUF.

Figure of Merits

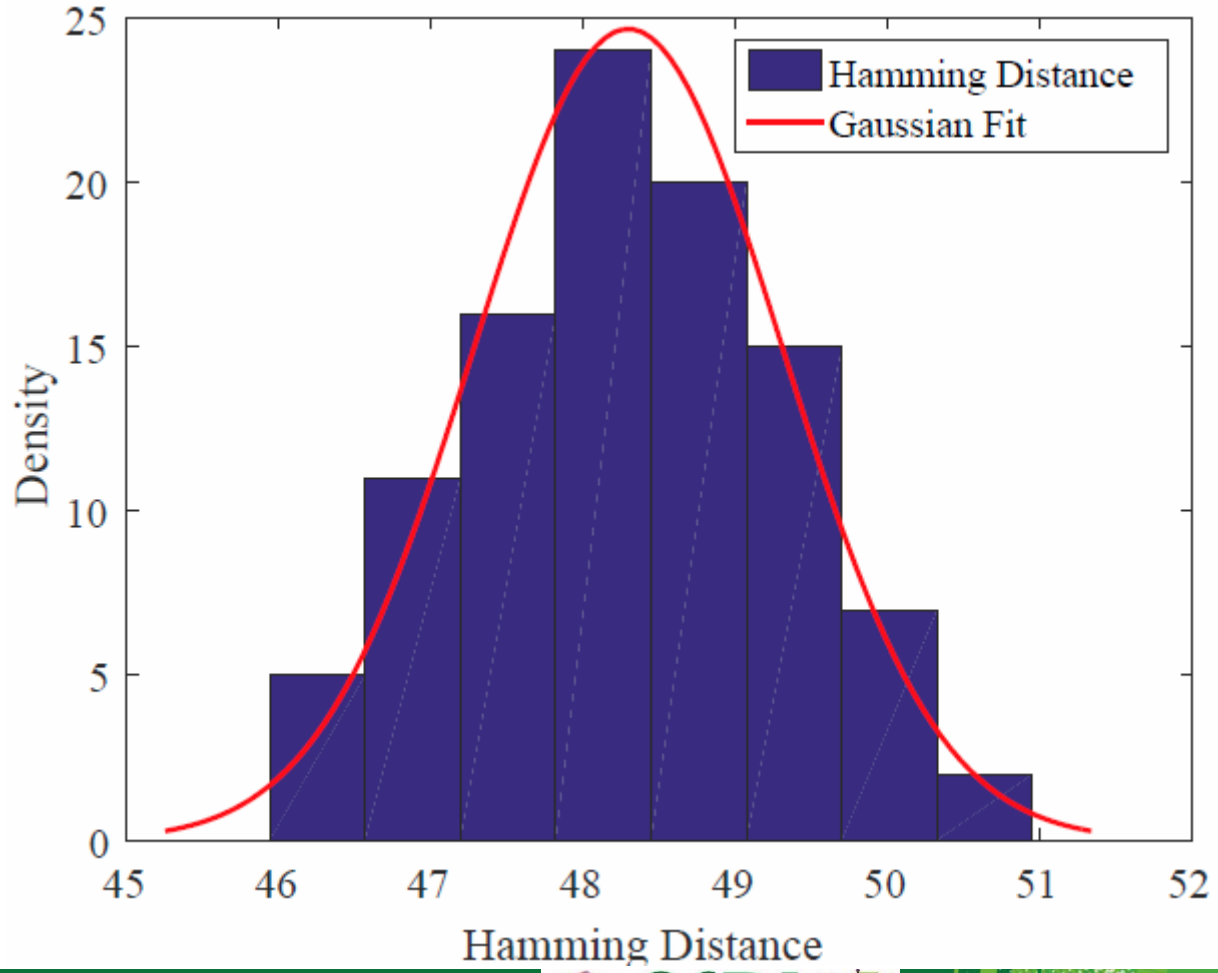
- Hamming Distance
  - Hamming distance of keys generated should be 50% under ideal conditions.
- Reliability
  - Creating same key with no change in challenge bits.
  - But in this case, same key should not be generated.

Figure of Merits

- Average Power
  - Average Power of MKG PUF is the sum of all leakage powers and the dynamic power.

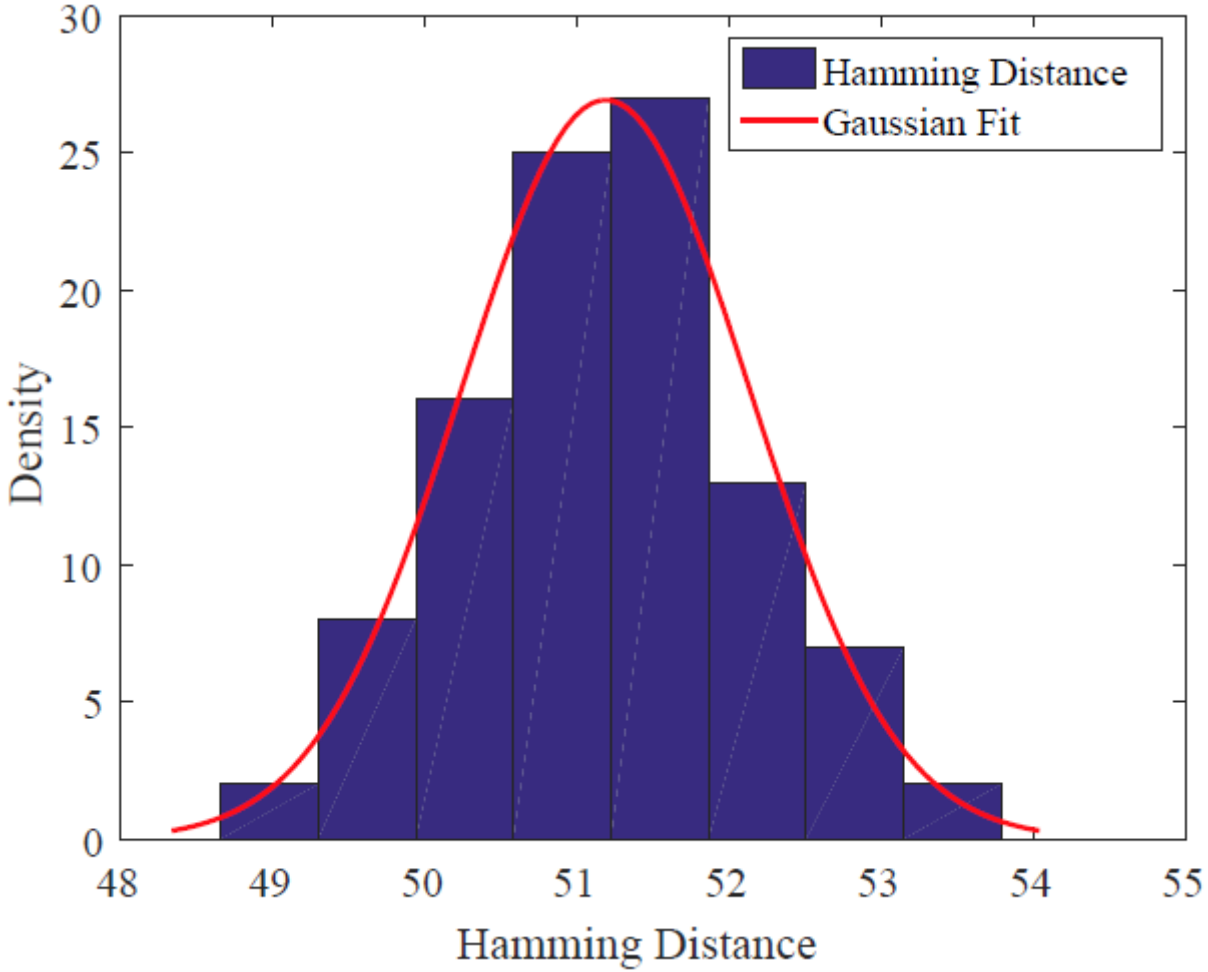
Results – Hamming Distance

- Speed Optimized PUF Hamming Distance.



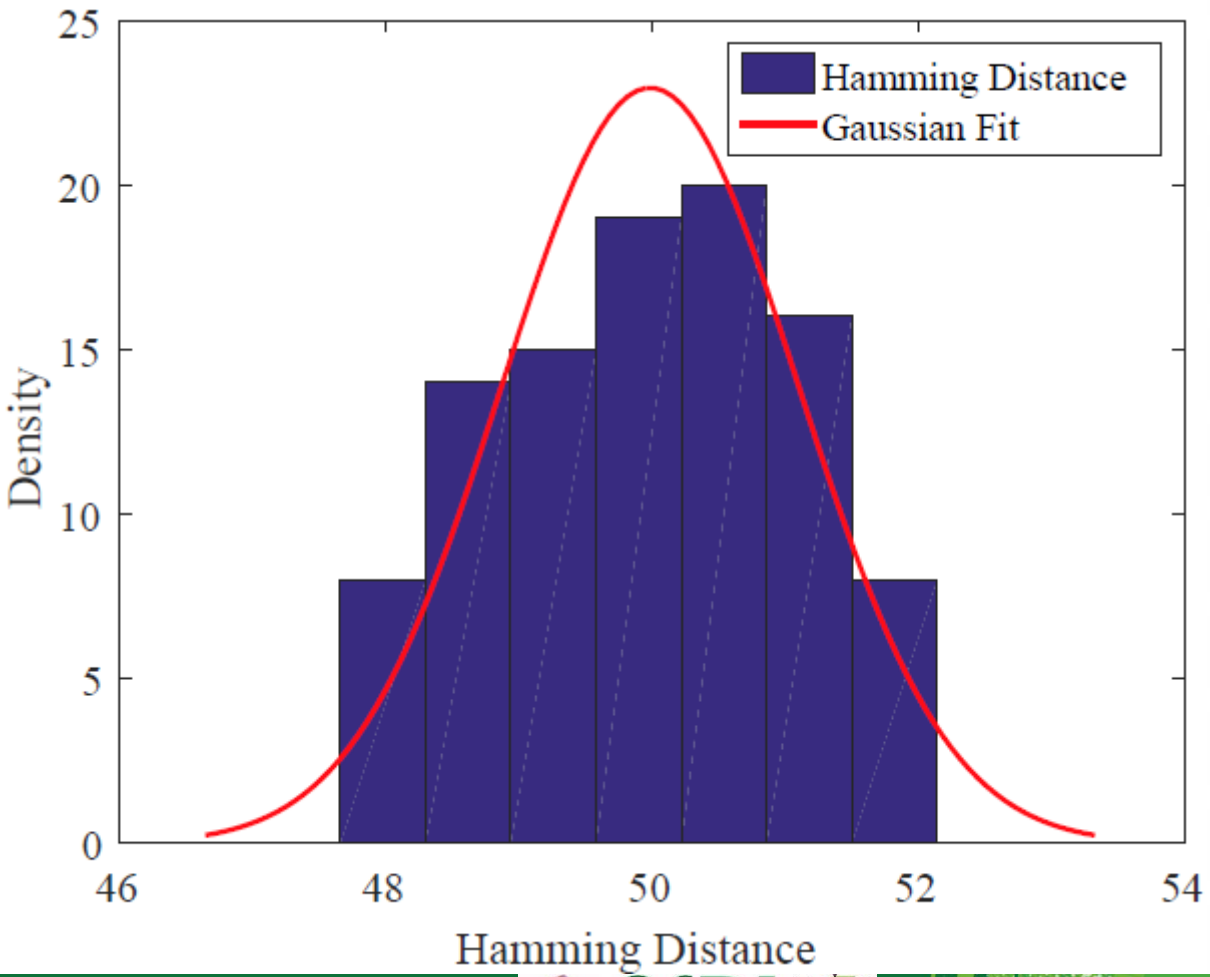
Results – Hamming Distance

- Power Optimized PUF Hamming Distance.



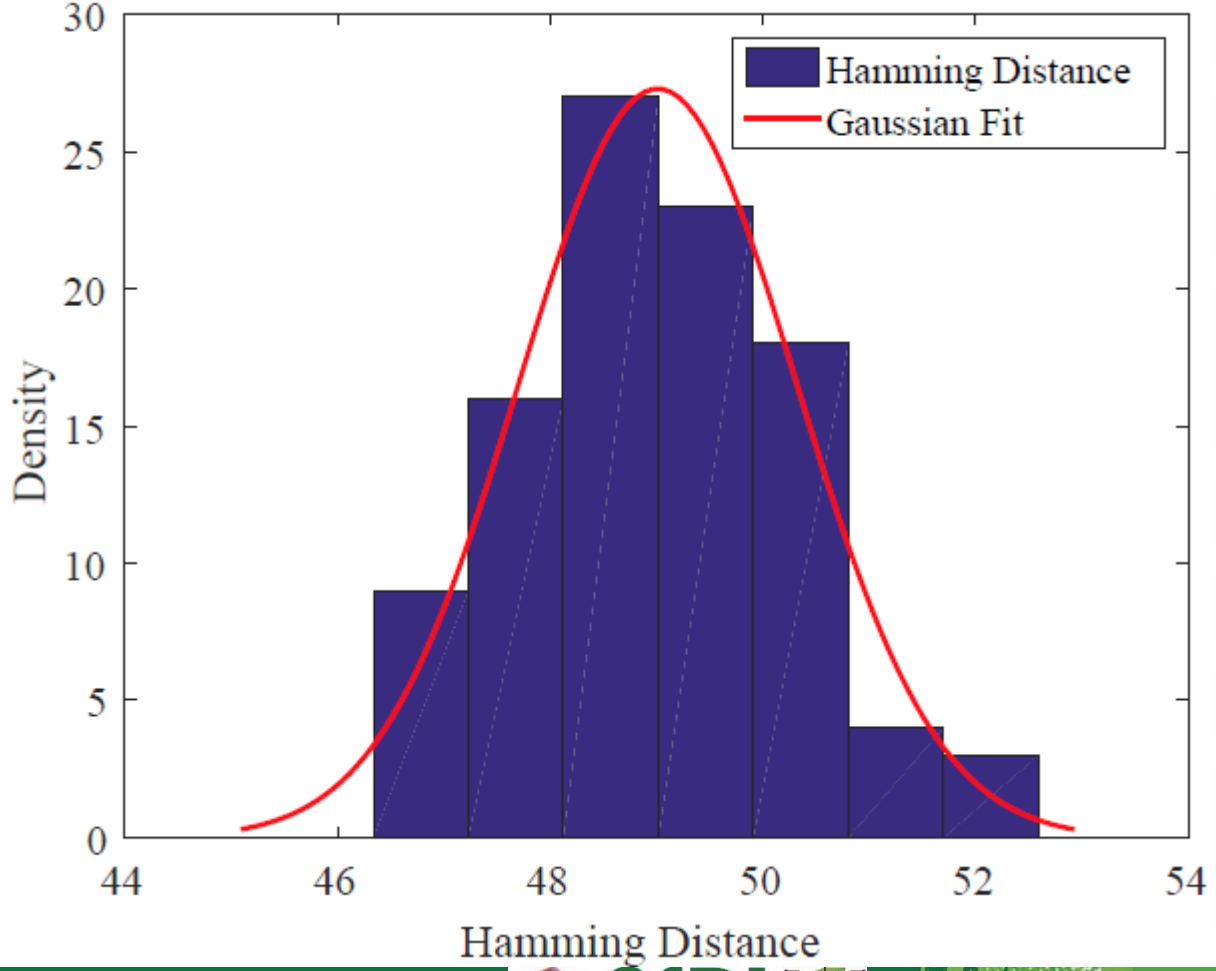
Results – Reliability

- Speed Optimized PUF Reliability.



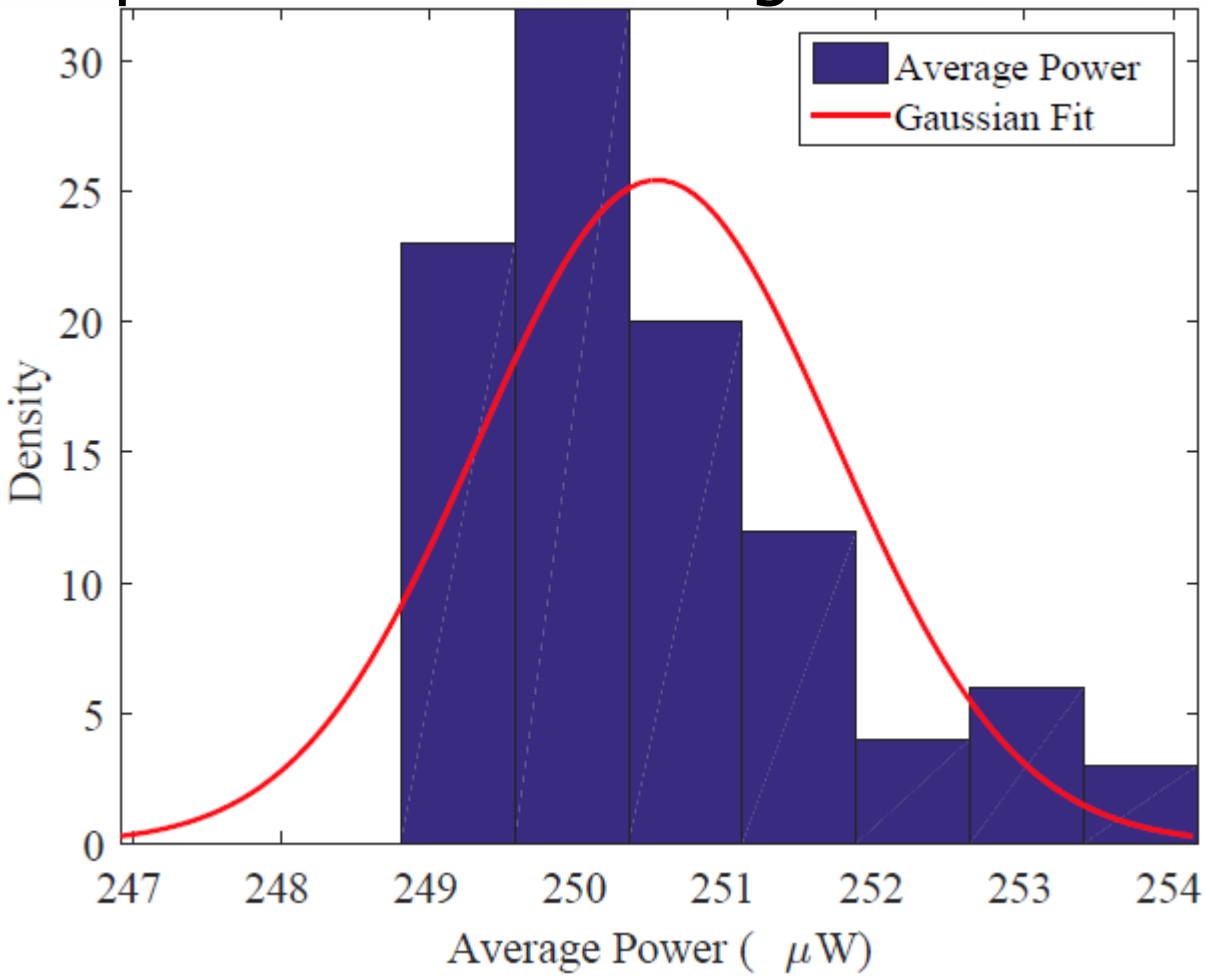
Results – Reliability

- Power Optimized PUF Reliability.



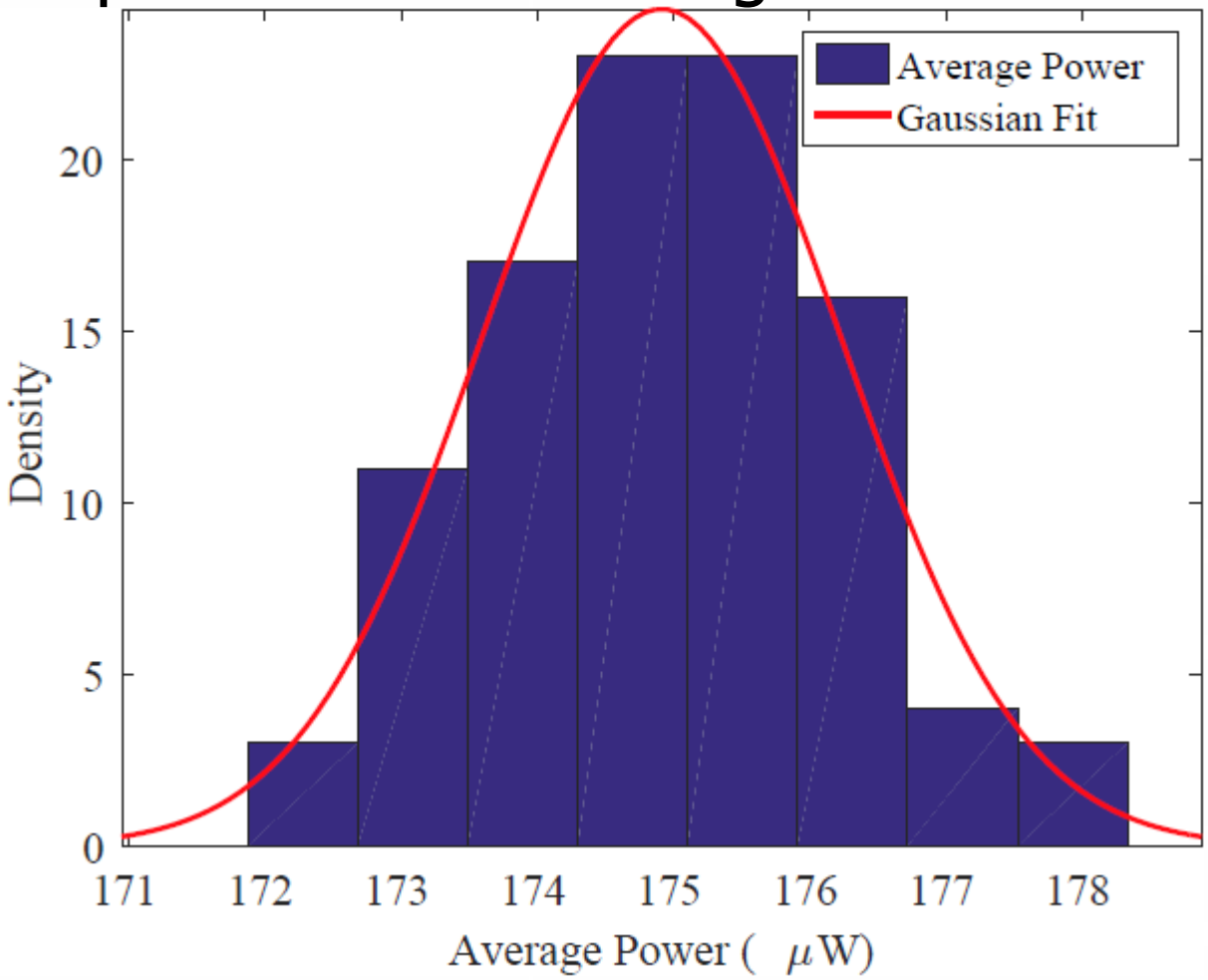
Results – Average Power

- Speed Optimized PUF Average Power.



Results – Power Consumption

- Power Optimized PUF Average Power.



Results – Characterization Table

Power Optimized Inverter MKG PUF		
Parameter	Value	
Transistor sizes	p-Type (W:L)	n-Type(W:L)
	120n : 32n	240n : 32n
Average Power	175.5 μW	
Hamming Distance	50.1 %	

Speed Optimized Inverter MKG PUF		
Parameter	Value	
Transistor sizes	p-Type (W:L)	n-Type(W:L)
	120n : 32n	240n : 32n
Average Power	251.5 μW	
Hamming Distance	48.3 %	

Results – Characterization Table

- Results comparison with other publications.

Research Works	Technology	Architecture Used	Average Power Consumed	Hamming Distance (%)
Rahman et al. [19]	90 nm		-	50
Maiti [15]	180 nm	Traditional Ring Oscillator	-	50.72
Suh [7]	-		-	46.15
Maiti et al. [13]	-	-	-	47.31
Yanambaka et al. [9]	32 nm	Current Starved Oscillator	320 μW	50.9
This paper (Speed Optimized)	32 nm	Traditional Ring Oscillator	251.5 μW	48.3
This Paper (Power Optimized)	32 nm	Traditional Ring Oscillator	175.5 μW	50.1

THANK YOU