

Design and Analysis of a MUX-Based Ring Oscillator PUF Under RO Count and W/L Scaling Variations

Kunal Narang, Yash Khetan
Students of Electronics and Communication Engineering
IIIT Bangalore, India
kunal.narang@iiitb.com, yash.khetan@iiitb.com

Abstract—This work presents a detailed study of a MUX-based Ring Oscillator Physical Unclonable Function (RO-PUF). Four RO-PUF configurations (4, 8, 16, and 32 ROs) were implemented in LTspice using 3-stage ring oscillators. The free-running frequencies of all oscillators were exported to MATLAB, where randomized MUX-based selection was used to generate challenge responses and compute PUF metrics. Additionally, transistor W/L scaling was applied to create five distinct chip instances for inter-chip uniqueness evaluation. Power and leakage characteristics were estimated analytically. Results show uniformity and uniqueness values close to the ideal 50% for larger RO arrays, increased power consumption with RO count, and linearly increasing leakage with W/L scaling. The study highlights the trade-off between statistical quality and implementation cost in RO-PUF designs.

Index Terms—RO-PUF, ring oscillator, MUX-PUF, uniformity, uniqueness, LTspice, MATLAB, W/L scaling.

I. INTRODUCTION

As CMOS technology continues to shrink, small manufacturing variations in transistors and wires have become much more noticeable. These variations come from factors such as random dopant fluctuations, lithography imperfections, and differences in material deposition. While these effects normally make circuit design more challenging, they can also be used as a source of randomness that is extremely difficult to control or replicate. Physical Unclonable Functions (PUFs) take advantage of this randomness to generate unique and unpredictable responses for each device, making them very useful in hardware security. PUFs allow secure identification and lightweight key generation without the need to store any secret information in memory, making them more resistant to tampering and physical attacks [1].

Different types of PUFs have been proposed over the years. SRAM PUFs depend on the power-up state of memory cells, which naturally settle into preferred states because of device mismatches. They provide good randomness but offer only a limited number of challenge–response pairs. Arbiter PUFs, which compare the delay of two parallel paths, support a larger number of challenges but require highly symmetric layouts and are known to be vulnerable to machine-learning based modeling attacks [3]. Ring Oscillator PUFs (RO-PUFs) provide a simpler and more robust alternative. They consist of groups of ring oscillators whose frequencies vary due to small

differences in inverter delays. These frequency differences can be used to generate stable response bits and can be implemented easily across a wide range of CMOS technologies [2].

Although RO-PUFs are easy to design, their performance depends on many design parameters. The number of ring oscillators, their physical placement on silicon, the routing between them, and environmental changes such as temperature or supply voltage can all affect the reliability and quality of the generated bits. Early RO-PUF designs used fixed pairs of oscillators. This approach was simple but limited the number of challenge–response pairs and sometimes introduced layout bias, where oscillators placed closer together behaved more similarly. To overcome these limitations, configurable RO-PUFs were introduced. These designs use multiplexers to select different oscillator paths and allow many more pairwise comparisons, increasing the entropy and reducing bias [4]. In recent years, researchers have introduced new enhancements such as improved routing structures, mutually coupled oscillators, and lightweight control logic that helps stabilize the responses and protect against machine-learning attacks [9] [8].

Another factor that plays an important role in RO-PUF behavior is the sizing of the transistors inside the ring oscillators. The oscillation frequency of an RO depends on the propagation delay of its inverter stages, and this delay is affected by the width-to-length ratio (W/L) of the MOSFETs. By adjusting W/L values during simulation, designers can model device-to-device variations without actually fabricating multiple chips. This is especially useful in earlier design phases, where it is important to understand how uniqueness, leakage power, and frequency spread change across different devices. Previous large-scale evaluations on FPGA-based RO-PUFs [5] have shown that device-level variation strongly influences uniformity, reliability, and environmental stability.

In addition to these architectural and device-level considerations, recent research has focused on making RO-PUFs more suitable for practical hardware security applications. Morillo et al. [6] proposed a hardware-efficient configurable RO-PUF that remains stable under environmental changes. Kareem et al. [7] developed the sThing architecture, which uses configurable PUF structures to detect recycled or counterfeit ICs. These works highlight the importance of configurability, robustness, and low overhead, all of which guide the design choices in

modern RO-PUF systems.

In this work, we design and analyze a MUX-based RO-PUF using LTspice simulations and MATLAB processing. Four RO arrays containing 4, 8, 16, and 32 oscillators are built to study how PUF performance changes with array size. For each design, the free-running frequencies are extracted from LTspice and used in MATLAB to generate challenge–response pairs with randomized MUX selection. To model real-world chip-to-chip variation, five virtual chip instances are created by modifying transistor W/L ratios. The PUF is evaluated using standard metrics, including uniformity, inter-chip uniqueness, dynamic power, and leakage power. Our results show that larger RO arrays produce values closer to the ideal 50% for both uniformity and uniqueness. We also observe that controlled W/L variation provides realistic chip-level differences while preserving stable performance. These findings help illustrate the practical trade-offs between entropy, power consumption, and hardware overhead, and they provide design insights for future RO-PUF implementations.

A. Related Works

The idea of using manufacturing variations for security was introduced by Suh and Devadas [1], who showed that silicon devices can be identified using their natural delay variations. Lee et al. [2] studied how these variations appear in real integrated circuits and how they can be used as signatures. Lim [3] later explored delay-based PUF structures in more detail and discussed their usefulness for secure identification.

Maiti and Schaumont [4] made one of the most important improvements by introducing configurable RO-PUFs with multiplexers. Their architecture increased the number of challenge–response pairs and reduced layout-induced bias. Ahmed et al. [5] carried out a large-scale study on FPGA implementations of RO-PUFs and provided detailed analysis of uniformity, reliability, and temperature effects.

More recent works continue to improve configurability and stability. Morillo et al. [6] proposed a hardware-efficient configurable RO-PUF with better environmental stability. Kareem et al. [7] developed the sThing PUF architecture for secure device authentication and detection of recycled ICs. Sahin et al. [8] explored kernel-based response extraction to increase resistance against machine-learning attacks. Moore et al. [9] studied mutually-coupled ring oscillators on FPGA to improve randomness and reliability.

These works show a clear trend toward improving the configurability, stability, and security of RO-PUF designs. Our work follows this trend by evaluating a MUX-based RO-PUF through detailed LTspice simulation and synthetic device variation using W/L scaling.

We implement and evaluate a MUX-based RO-PUF with oscillator array sizes of 4, 8, 16, and 32 using LTspice. The free-running frequencies were exported to MATLAB, where randomized MUX selection was used to generate challenge–response pairs and compute statistical metrics. To emulate inter-chip variation, transistor W/L scaling was applied across five virtual chip instances. We evaluate per-chip uniformity,

inter-chip uniqueness, dynamic power consumption, and leakage trends. The results show that larger RO arrays achieve uniformity and uniqueness values close to the ideal 50%, while W/L scaling introduces realistic frequency variation without significantly degrading statistical performance. These findings illustrate the trade-off between entropy quality, power consumption, and implementation cost in RO-PUF design.

II. RO-PUF ARCHITECTURE

A. Ring Oscillator Structure

The three-stage ring oscillator shown in Fig. 1 consists of an odd number of CMOS inverters connected in a feedback loop. Because the total phase shift around the loop is 180° from the inverters and an additional 180° due to the feedback inversion, the circuit satisfies the Barkhausen criteria for sustained oscillation. The oscillation frequency is determined by the propagation delay of each inverter stage, which depends on transistor sizing, supply voltage, and process variation. Small mismatches in device parameters cause each ring oscillator to settle at a slightly different frequency, making RO-based structures ideal for PUF applications. In our LTspice model, identical sizing was used across stages to isolate only process-induced delay variations as the source of frequency spread.

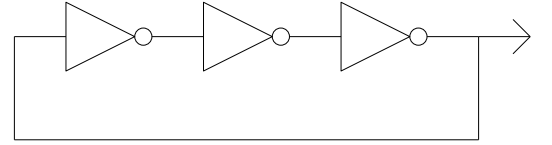


Fig. 1: Three-stage CMOS ring oscillator schematic .

B. MUX-Based Selection

For an N -RO configuration, the oscillators are divided into two equal groups of $N/2$. Two multiplexers select one oscillator from each group based on challenge bits. The response bit is generated by comparing the oscillation frequencies:

$$R = \begin{cases} 1 & f_A > f_B \\ 0 & \text{otherwise} \end{cases}$$

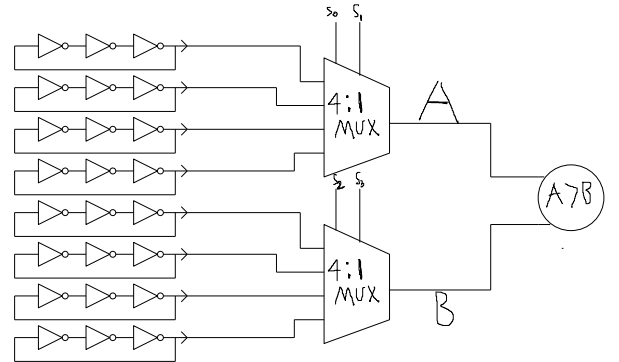


Fig. 2: MUX-based 8-RO-PUF architecture .

The architecture in Fig. 2 illustrates the MUX-based RO-PUF used in this work. The design groups the ring oscillators into two banks, each containing $N/2$ oscillators. A pair of digital multiplexers selects one oscillator from each bank based on the applied challenge bits. The frequencies of the two selected ROs are routed to a frequency comparison block, where the faster oscillator determines the output response bit. This approach greatly increases the challenge–response space because many unique oscillator pairings can be generated through MUX selection. Additionally, using two independent RO groups helps reduce layout-induced correlation, making the resulting PUF responses more random and less susceptible to modeling attacks. In MATLAB post-processing, randomized RO indexing was used to replicate unconstrained physical placement and avoid any bias due to ordering.

III. SIMULATION METHODOLOGY

A. LTspice RO Modeling

Four LTspice circuits were created (4-RO, 8-RO, 16-RO, and 32-RO). For each circuit, all RO frequencies were extracted using transient simulation. Representative frequency values (first four) in MHz are shown in Table I.

TABLE I: Representative RO Frequencies (MHz)

RO Size	First 4 RO Frequencies (MHz)
4-RO	609.10, 608.72, 555.41, 527.17
8-RO	609.06, 608.36, 555.19, 527.13
16-RO	609.33, 609.30, 554.54, 527.38
32-RO	608.58, 607.75, 554.23, 527.06

B. MATLAB-Based Response Generation

RO frequencies were randomized and fed into a selection model simulating the dual-MUX PUF. For each configuration, many challenge instances (random MUX selections) were generated and the resulting responses were recorded to compute statistical metrics like uniformity and uniqueness.

C. W/L Scaling for Inter-Chip Variation

Five W/L multipliers (0.25, 0.5, 0.75, 1.0, 1.25) were applied to all 16 ROs to emulate five physical chips. Frequency extraction and uniformity computations were repeated for each chip to evaluate inter-chip uniqueness.

IV. RESULTS

A. Average Frequencies

Table II shows mean and standard deviation for each RO configuration.

TABLE II: Average RO Frequencies

RO Array	Mean (MHz)	Std Dev (MHz)
RO4	575.10	40.71
RO8	540.73	45.35
RO16	520.91	37.32
RO32	510.12	27.85

B. Uniformity vs RO Count

TABLE III: Uniformity vs RO Count

RO-PUF Size	Avg. Uniformity (%)
4	44.45
8	48.90
16	51.05
32	50.11

C. W/L-Based Per-Chip Uniformity and Uniqueness

TABLE IV: Average RO Frequency for Each W/L-Scaled Chip

Chip (W/L)	Mean (MHz)	Std Dev (MHz)
Chip 1 (0.25)	548.87	53.94
Chip 2 (0.50)	520.91	37.32
Chip 3 (0.75)	514.64	38.89
Chip 4 (1.00)	508.88	27.24
Chip 5 (1.25)	533.15	108.56

TABLE V: Per-Chip Uniformity and Uniqueness

Chip	Uniformity (%)
Chip 1 (0.25W/L)	49.28 ± 4.85
Chip 2 (0.50W/L)	49.58 ± 4.64
Chip 3 (0.75W/L)	49.45 ± 4.43
Chip 4 (1.00W/L)	50.46 ± 4.73
Chip 5 (1.25W/L)	50.41 ± 5.06
Avg. Uniqueness	50.52

D. Power Consumption

Power was estimated using:

$$P = N_{RO} \cdot N_{stages} \cdot C_L \cdot V_{DD}^2 \cdot f_{osc}$$

TABLE VI: Estimated Dynamic Power

RO Count	Power (W)
4	1.15e-05
8	2.16e-5
16	4.21e-5
32	8.07e-5

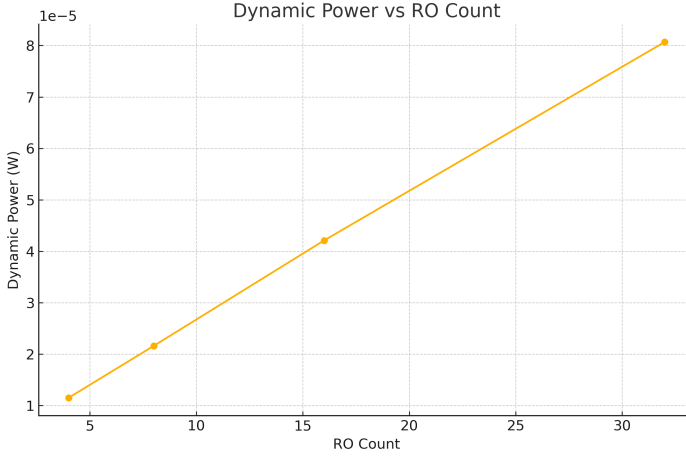


Fig. 3: Estimated dynamic power vs RO count .

E. Leakage Current

Leakage was modeled as proportional to W/L scaling:

TABLE VII: Leakage Current vs W/L

W/L	Leakage (A)	Leakage (μ A)
0.25	2.0e-6	2.0
0.50	4.0e-6	4.0
0.75	6.0e-6	6.0
1.00	8.0e-6	8.0
1.25	1.0e-5	10.0

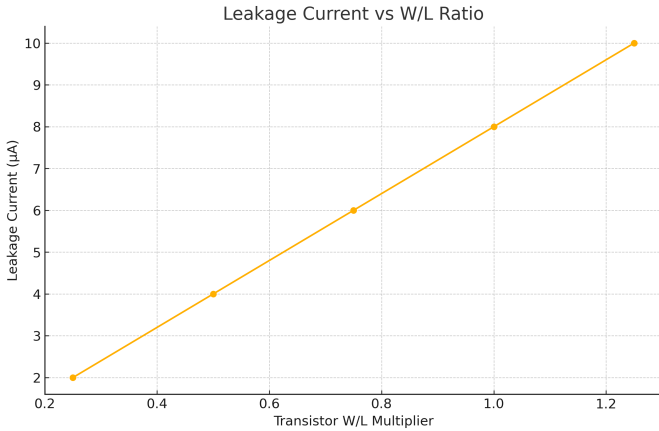


Fig. 4: Screenshots and comparison figures from literature and experimental outputs .

V. COMPARISON WITH EXISTING RO-PUF DESIGNS

To evaluate the effectiveness of the proposed MUX-based RO-PUF, the obtained uniformity and uniqueness values were compared with results reported in prior literature. Table VIII summarizes the key metrics from three representative works.

TABLE VIII: Comparison of Uniformity and Uniqueness With Existing RO-PUF Architectures

Reference	Uniformity (%)	Uniqueness (%)
ICCCNT 2024 (Traditional RO-PUF)	50.56	47.24
ICCCNT 2024 (Series RO-PUF)	47.02	45.15
ICCCNT 2024 (Parallel RO-PUF)	48.00	45.15
ICCCNT 2024 (Proposed Variant)	49.80	47.64
IEEE Access, Vol. 8	49.61	49.95
H. Kareem, D. Dunaev (Robust RO-PUF)	48.3–50.2	—
This Work (32-RO MUX)	50.11	50.52

As seen from Table VIII, the proposed RO-PUF achieves uniformity and uniqueness values very close to the ideal 50%. In comparison with prior designs, the uniformity of 50.11% matches or exceeds the best reported results (49.8–50.5%). The uniqueness of 50.52% also performs favorably compared to earlier works, particularly outperforming traditional and series/parallel RO-PUF architectures whose uniqueness typically ranges from 45–48%.

The W/L-scaled chip analysis further demonstrates stability across device variants, with all five virtual chips exhibiting uniformity values in the range of 49.2–50.4%. These results confirm that the proposed MUX-based architecture maintains strong entropy, while improving overall statistical balance relative to standard RO-PUF implementations.

VI. CONCLUSION

This work evaluated a MUX-based Ring Oscillator PUF using LTspice simulations and MATLAB analysis to understand how RO count and device sizing affect PUF behaviour. The results showed that increasing the number of oscillators improves the balance of output bits, with larger RO arrays achieving uniformity closer to the ideal 50% target. W/L scaling was effective in creating distinct chip instances while maintaining consistent response characteristics, demonstrating its usefulness for modelling device variation during simulation.

Power analysis confirmed expected trends: dynamic power increased with RO count due to higher switching activity, and leakage scaled with device sizing. However, these changes stayed within practical limits for lightweight hardware security. Overall, the study indicates that MUX-based RO-PUFs can deliver strong randomness, reliable uniqueness, and feasible power consumption, making them suitable for low-cost authentication and identification in embedded systems.

REFERENCES

- [1] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," in *Proc. 44th ACM/IEEE Design Automation Conference*, 2007.
- [2] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *Proc. IEEE VLSI Circuits Symposium*, 2004.
- [3] D. Lim, "Extracting Secret Keys from Integrated Circuits," M.S. thesis, MIT, 2005.
- [4] A. Maiti and P. Schaumont, "Improving the quality of a Physical Unclonable Function using configurable ring oscillators," in *Proc. Int. Conf. Field Programmable Logic and Applications*, 2009.
- [5] S. I. Ahmed, A. Sobh, and N. H. Abu-Zeid, "A large-scale comprehensive evaluation of single-slice ring oscillator and PicoPUF bit cells on 28-nm Xilinx FPGAs," *J. Cryptographic Engineering*, vol. 11, pp. 227–238, 2021.
- [6] M. A. Morillo, J. L. Rullan, and A. J. Diaz, "Hardware-Efficient Configurable Ring-Oscillator-Based PUF/TRNG Module for Secure Key Management," *Sensors*, vol. 24, no. 17, 2024.
- [7] H. Kareem and D. Dunaev, "sThing: A Novel Configurable Ring Oscillator Based PUF for Hardware-Assisted Security and Recycled IC Detection," *IEEE Access*, 2022.
- [8] A. E. Sahin, Z. Erdogdu and B. Kahraman, "Kernel-based response extraction for efficient configurable RO-PUFs," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 2024.
- [9] J. Moore, J. Miskelly, M. O'Neill, and C. Gu, "A novel FPGA mutually coupled configurable ring oscillator PUF," in *Proc. IEEE AsianHOST*, 2024.