CycPUF: Cyclic Physical Unclonable Function

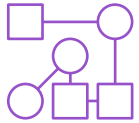
Michael Dominguez
Undergraduate Research Assistant
California State University Long Beach

Amin Rezaei
Assistant Professor
California State University Long Beach

Agenda

Introduction

Problem statement and preliminaries



CycPUF

Cyclic delay-based PUFs and their behavior

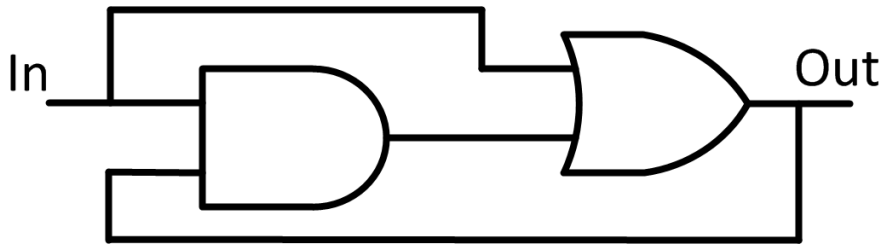
Experiments

Attack resiliency, FGPA emulation and functional metrics

Cyclic Combinational Circuits

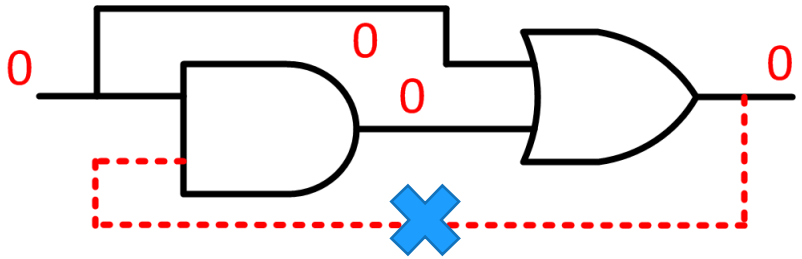
Combinational circuits with loops or feedback paths

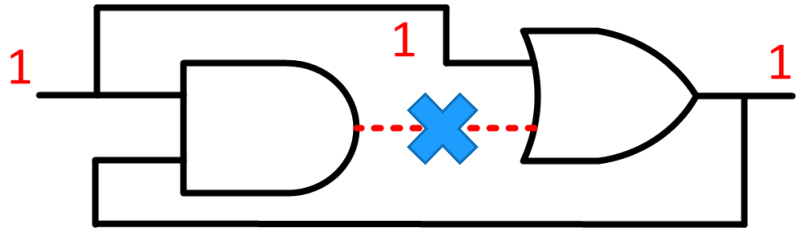
Cyclic Combinational Circuits



Combinational feedback

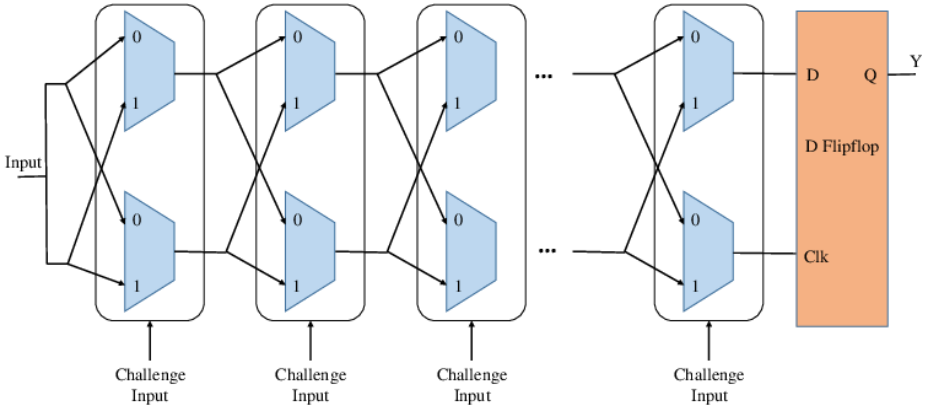
In	Out
0	0
1	1



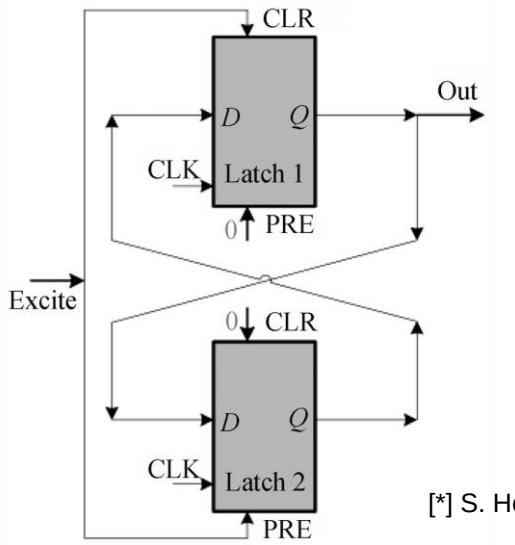


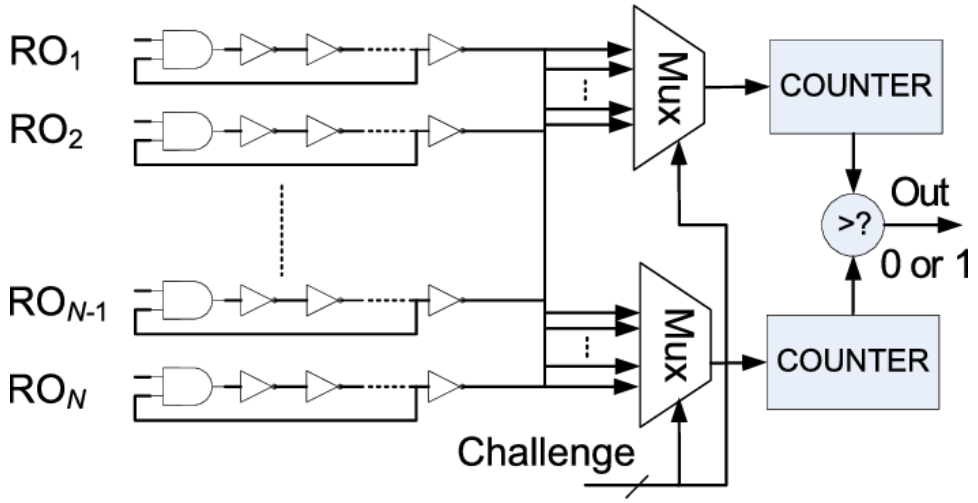
PUF Primer

(a) Arbiter PUF [*]



(b) Butterfly PUF [$]





(c) Ring Oscillator PUF [%]

- Physical Unclonable Function (PUF) produces a unique response (output) to a given challenge (input)
- PUFs have been implemented in cryptography, resource-constrained devices, and privacy protection

[*] S. Hemavathy and V. S. K. Bhaaskaran, "Arbiter PUF—A Review of Design, Composition, and Security Aspects," in IEEE Access, 2023.

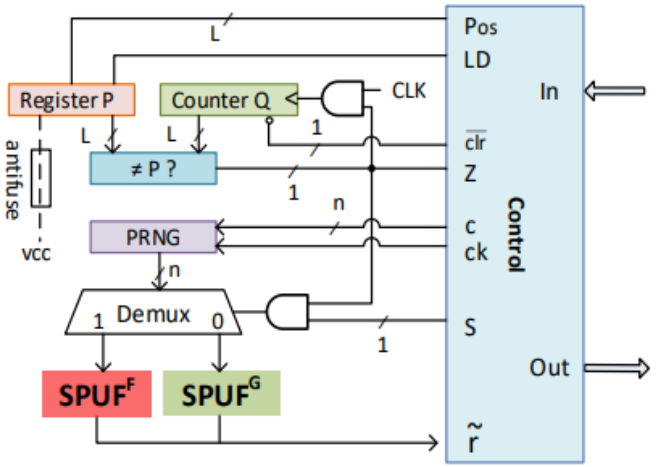
[$] S. S. Kumar, J. Guajardo, R. Maes, G. -J. Schrijen, and P. Tuyls, "The Butterfly PUF Protecting IP on Every FPGA," in HOST, 2008.

[%] S. R. Sahoo, S. Kumar, and K. Mahapatra, "A Novel ROPUF for Hardware Security," in VDAT, 2015.

Related Works

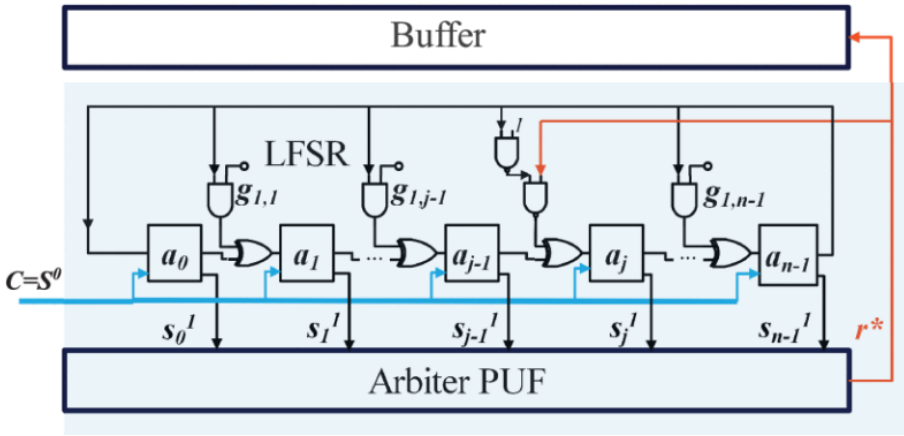
Prior Works and Challenges

- Deception Protocol PUF [*]
  - has been proposed using a Strong PUF, a fake Strong PUF, a PRNG, a *L*-bit counter, a *L*-bit register, a comparator, and a controller



(a) Deception Protocol PUF

- FLAM-PUF [$]
  - Linear-Feedback Shift Registers (LFSR) are used to obfuscate CRPs



(b) FLAM-PUF

- Challenges in PUF
  - ML susceptibility
  - Fault-vulnerability
  - High hardware overhead

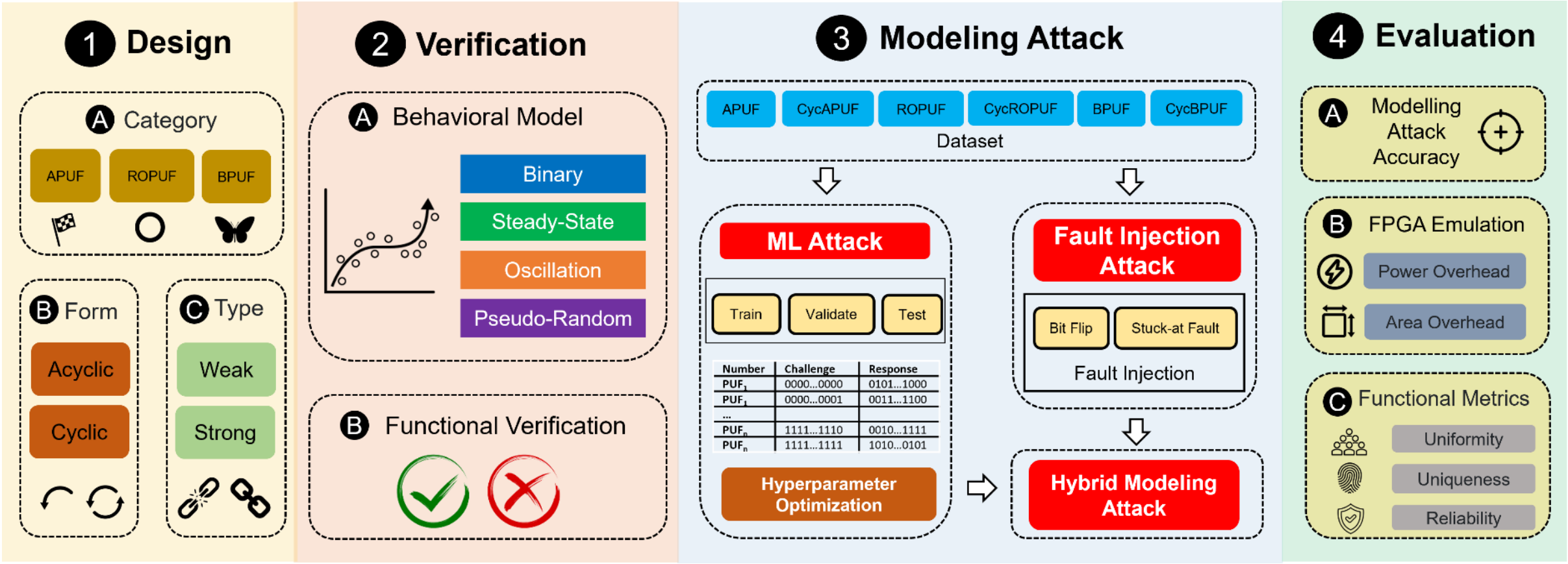
[*] C. Gu, C. -H. Chang, W. Liu, S. Yu, Y. Wang and M. O'Neill, "A Modeling Attack Resistant Deception Technique for Securing Lightweight-PUF-Based Authentication," in IEEE TCAD, 2021.

[$] L. Wu, Y. Hu, K. Zhang, W. Li, X. Xu and W. Chang, "FLAM-PUF: A Response–Feedback-Based Lightweight Anti-Machine-Learning-Attack PUF," in IEEE TCAD, 2022.

CycPUF

Cyclic Physical Unclonable Function

Proposed Solution



CycPUF Framework

CycPUF Behaviour

- By feeding response back into challenge, we create a cyclic PUF that shows *PUF modes*:
  - **Binary**: fixed challenges produce fixed responses like normal
  - **Steady-State:** fixed challenges produce fixed responses; however, it takes time to stabilize
  - **Oscillating**: response vector bounces between two or more different responses, making a discernible pattern
  - **Pseudo-Random**: response vector changes at unpredictable times and has no noticeable pattern

Results

Functional Metrics

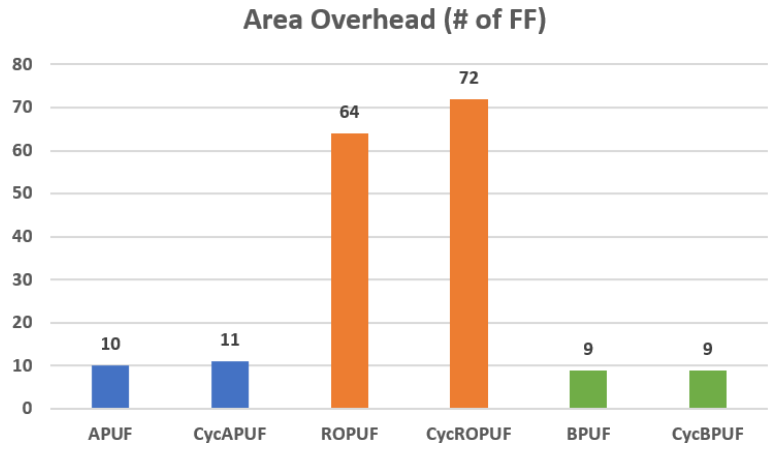
- Avg Bit Value
  - Allows us to apply the acyclic PUF functional metrics to CycPUF

PUF Functional Metrics Results

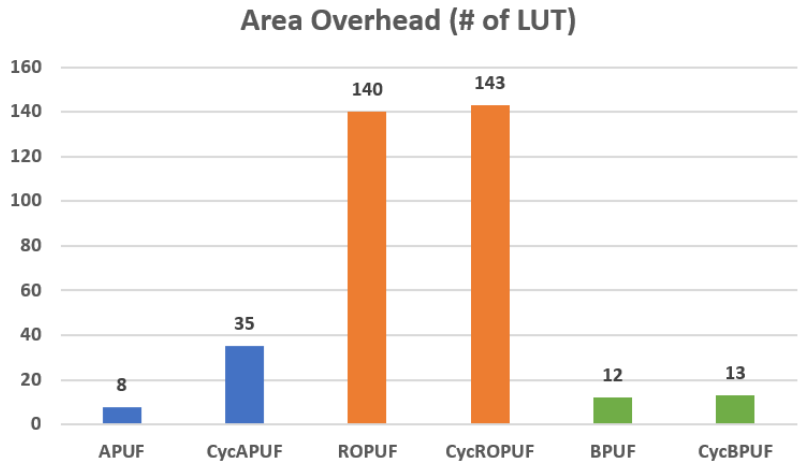
PUF Design	Uniqueness	Uniformity	Reliability
APUF	7.55%	55.42%	99.77%
CycAPUF	47.10%	47.30%	98.34%
ROPUF	44.26%	53.81%	99.05%
CycROPUF	50.68%	52.12%	95.18%
BPUF	11.48%	55.04%	97.45%
CycBPUF	53.05%	46.67%	98.62%

Avg Bit Value = $\frac{1}{m}\sum_{i=1}^{m} r_i[n]$

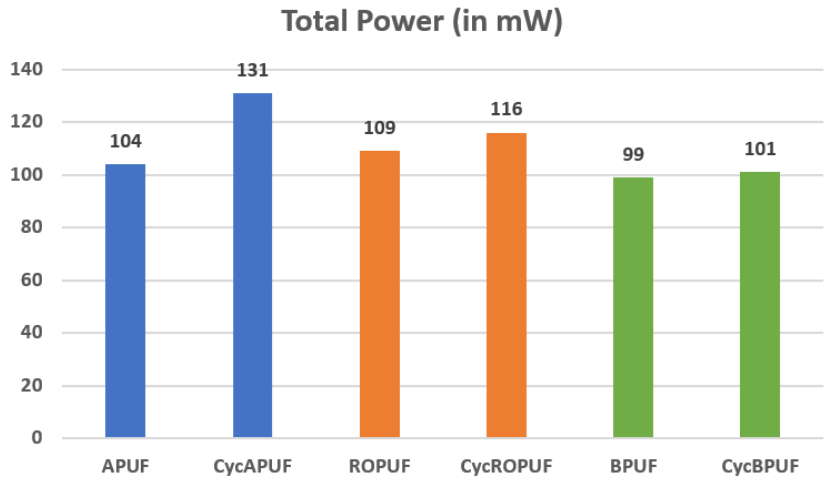
Performance Metrics



(a) Number of FFs



(b) Number of LUTs



(c) Total power consumption

Modeling & Fault-Resiliency

- **DNN-Based ML attack [*]:** fed CRPs into ML model and allowed it to guess CRPs
- **Fault-Injected ML attack [$]:** injected faults to disrupt CycPUF behavior and aid ML model

Modeling Attacks Results

PUF Design	Challenge Size	# of Training CRPs	Model Accuracy
APUF	64	500,000	99.38%
CycAPUF	64	703,340	59.49%
Faulty CycAPUF	64	500,000	76.27%
ROPUF	64	500,000	78.00%
CycROPUF	64	1,048,576	48.74%
Faulty CycROPUF	64	642,603	50.02%
BPUF	64	500,000	83.32%
CycBPUF	64	938,420	54.76%
Faulty CycBPUF	64	582,645	61.44%

[*] P. Santikellur, A. Bhattacharyay, and R. S. Chakraborty, “Deep Learning based Model Building Attacks on Arbiter PUF Compositions,” in Cryptology ePrint Archive, 2019.

[$] S. Tajik, H. Lohrke, F. Ganji, J. -P. Seifert, and C. Boit, "Laser Fault Attack on Physically Unclonable Functions," in FDTC 2015.

Conclusion

Key Takeaways

- Proposed CycPUF & PUF modes
- Close to optimal functional metrics
- High ML resiliency & fault-tolerant

Michael Dominguez

Amin Rezaei

Computer Architecture, Reliability, and Security Laboratory (CARS-Lab)

California State University, Long Beach