A Capacitive-Loaded Weak PUF Insensitive to Thermal Noise and Voltage/Temperature Changes

EE241B
(Instructor- Bora Nikolic)

Griffin Prechter & Antroy Roy Chowdhury

Outline

- Introduction & Background
- PUF in Key Generation
- Proposed PUF Architecture
- Experimental Setup
- Simulation Results

PUFs: Low-Cost Crypto Hardware Primitives

Growing need for fast, low-power cryptographic primitives:

- High demand for reliable and robust security features in devices.
- Proliferation of IoT devices striving for low power and handling sensitive data.

Physically Unclonable Functions are low-cost, efficient hardware implementations of cryptographic operations.

What is a Physically Unclonable Function?

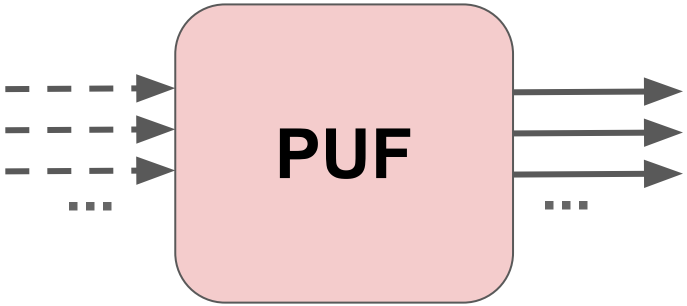
PUFs leverage IC manufacturing variations to produce a device “fingerprint”.

- Unpredictable yet consistent
- Very difficult to observe
- Cost effective

Can be applied to **key generation/storage**, device anti-counterfeiting, user authentication, IP protection, and hardware/software binding.

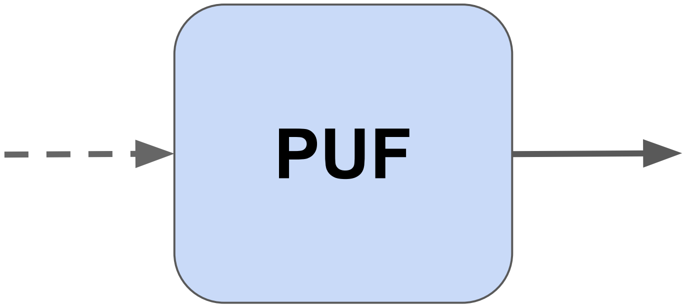
PUF Types

Strong PUF



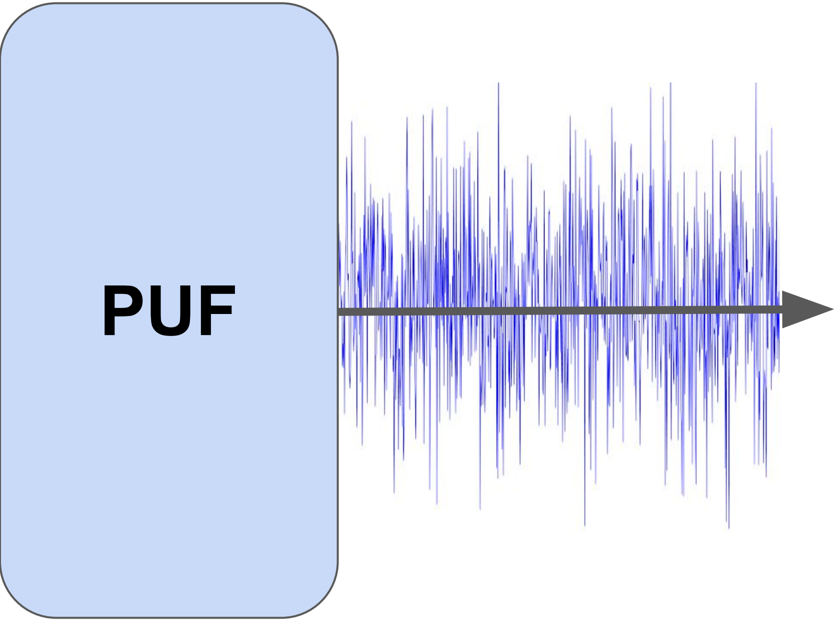
- More CRPs
- Less stable
- Used for user authentication systems

Weak PUF



- Very few CRPs
- Can achieve higher stability
- Used for **key generation**

Stability Enhancement



PUF output inherently noisy:

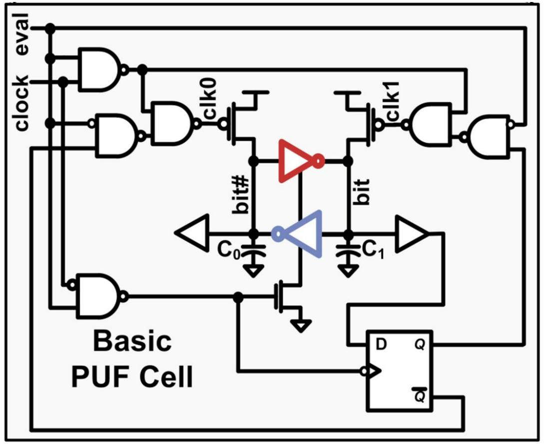
- Small device mismatch
- Thermal noise
- Changing operating conditions

Weak PUF designs employ auxiliary techniques to boost stability:

- Majority voting, soft dark-bit masking, BCH error correction codes, etc.

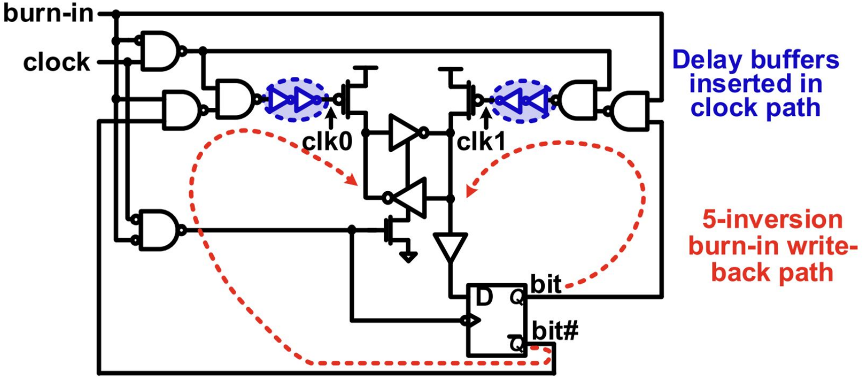
PUF in Key Generation

Hybrid PUF (Mathew, ISSCC'14)



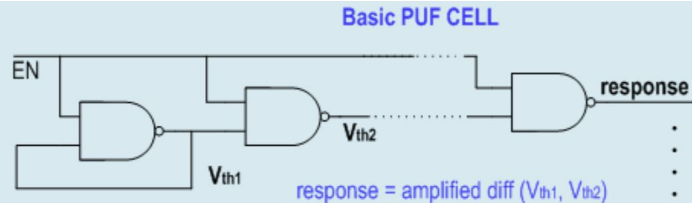
- Hybrid: metastability + Delay
- Stability improvement: TMV + Burn-in + Dark-bits
- 100% Stable: ECC (BCH)

Delay-hardened PUF (Satpathi, JSSC'17)



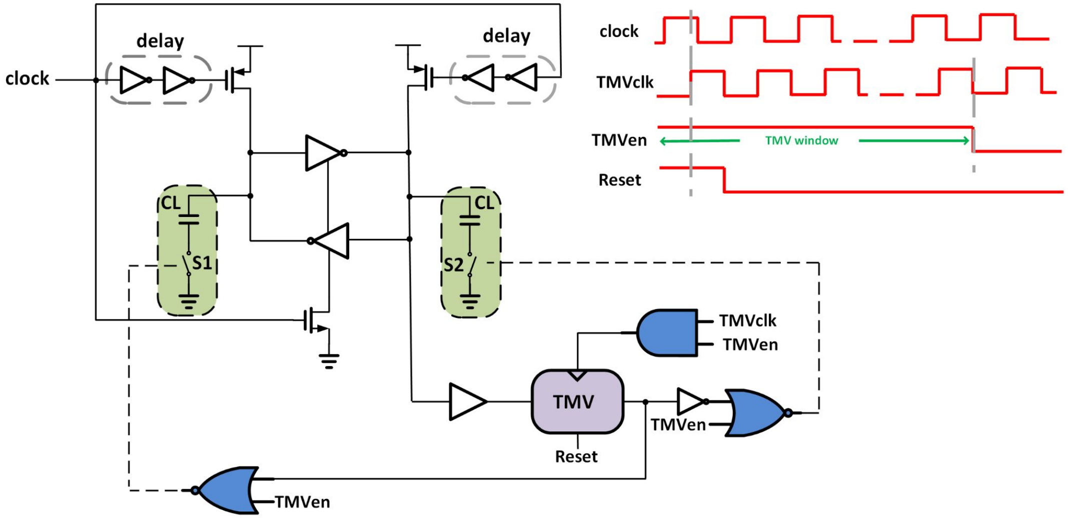
- Hybrid PUF cell
- Delay Hardening + selective-bit destabilization
- ECC + entropy extraction (AES-CBC-MAC)

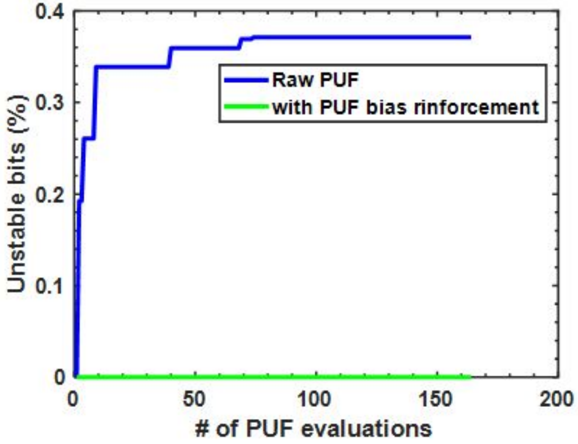
Threshold PUF (ISSCC'16)

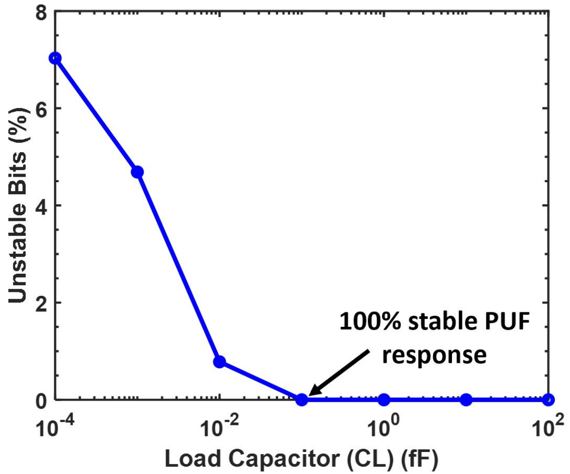


- Amplifies Voltage Threshold Mismatch
- Glitch Detection Valid Mask + TMV + SMV
- Power Gating to mitigate aging

Proposed PUF Architecture

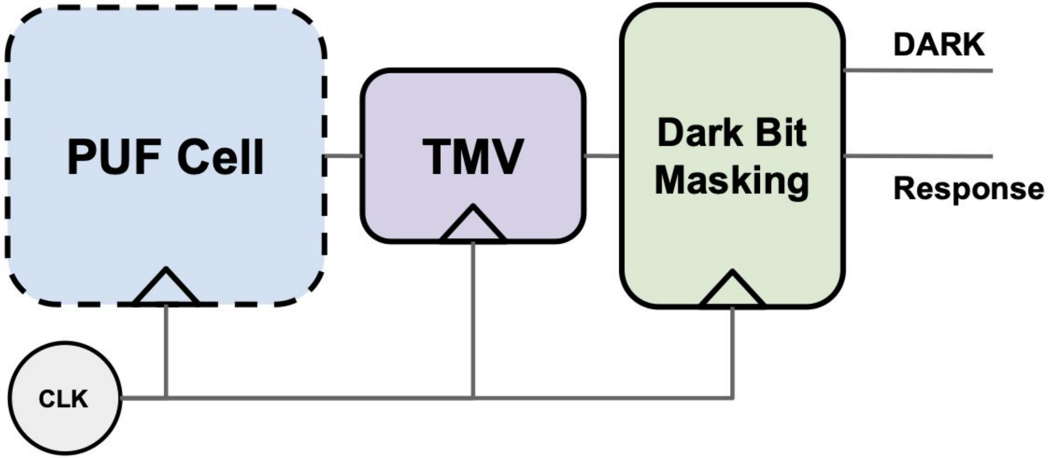






- Hybrid PUF cell
- Two stage operation:
  - Bias detection: TMV
  - Bias reinforcement: capacitive loading
- 100% stable response in a power-on cycle
- Load capacitor value > 100aF

Experimental Setup



- Implemented PUF cell schematics in GPDK 45nm process.
- Added **TMV** and **dark-bit masking** periphery using software model to reduce simulation time.
- Simulated 128bit PUF cell arrays for each of the aforementioned designs.

Evaluation Metrics

Stability:

- Bit Error Rate, Intra-PUF Hamming Distance

Randomness:

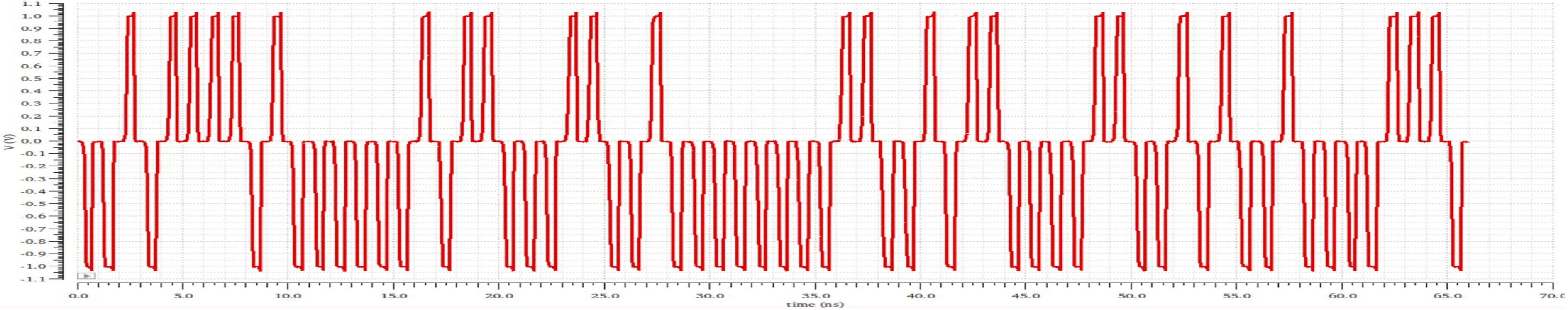
- NIST 800-22 Test Results, Inter-PUF Hamming Distance

Efficiency:

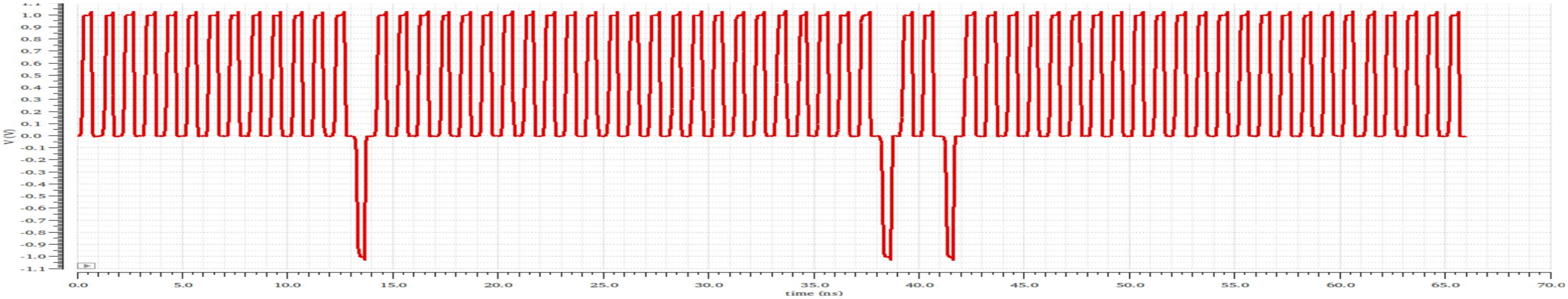
- Power/bit, Area/bit

Raw PUF Simulation Results

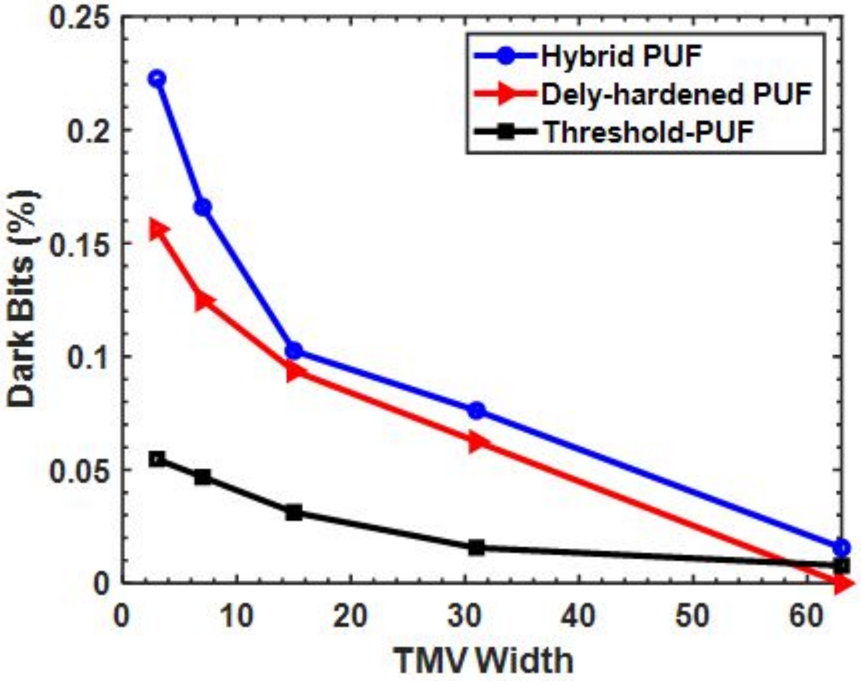
Highly unstable

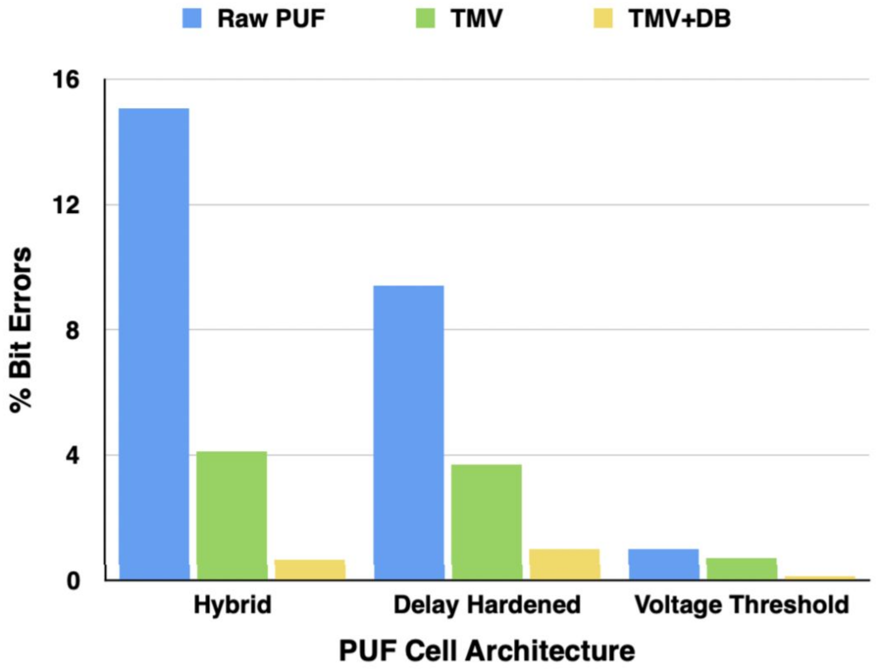


Moderately unstable



Stability Results





Randomness Results

NIST 800-22 Randomness Test Results

Test	Hybrid		DH		V_{TH}		C Loaded	
	P	*Pass*	*P*	*Pass*	*P*	*Pass*	*P*	*Pass*
Freq.	0.48	✓	0.11	✓	0.48	✓	0.15	✓
Runs	0.14	✓	0.89	✓	0.35	✓	0.2	✓
Longest	0.5	✓	0.53	✓	0.22	✓	0.5	✓
Cum-Sum	0.65	✓	0.17	✓	0.77	✓	0.25	✓
Serial	0.49	✓	0.49	✓	0.49	✓	0.49	✓
Block F.	0.48	✓	0.11	✓	0.48	✓	0.15	✓
Entropy	0.36	✓	0.49	✓	0.26	✓	0.43	✓

* Important to note limited input stream length.

Efficiency Results

Evaluation Results Summary

Metric	**Hybrid [3]**	**DH [4]**	V_{TH} **[14]**	**This Work**
Tech.y	45nm	45nm	45nm	45nm
BER	0.65%	0.99%	0.12%	-
NIST	PASS	PASS	PASS	PASS
Power/Bit	$4.26\mu W/b$	$8.53\mu W/b$	$2.66\mu W/b$	$7.53\mu W/b$
Area/Bit	$0.146\mu m^2/b$	$0.21\mu m^2/b$	$0.13\mu m^2/b$	$0.43\mu m^2/b$

*PUF cells simulated with 1V supply voltage.

Thank you!

Questions?