Reliable, Machine Learning Resistant Physically Unclonable Functions

Manoj Sachdev
Electrical and Computer Engineering Department

UNIVERSITY OF WATERLOO

Acknowledgement

Contributions and help from Kleber Hugo Stangherlin, Zhuanhao Wu, and Hiren Patel for this presentation are gratefully acknowledged.

Presentation Summary

- Motivation – What problem are we trying to solve?
- Background – What are Physical Unclonable Functions?
- Authentication with Strong PUFs
- PUF on PUF – Reliable, ML Resistant PUF

Motivation – What problem we are trying to solve?

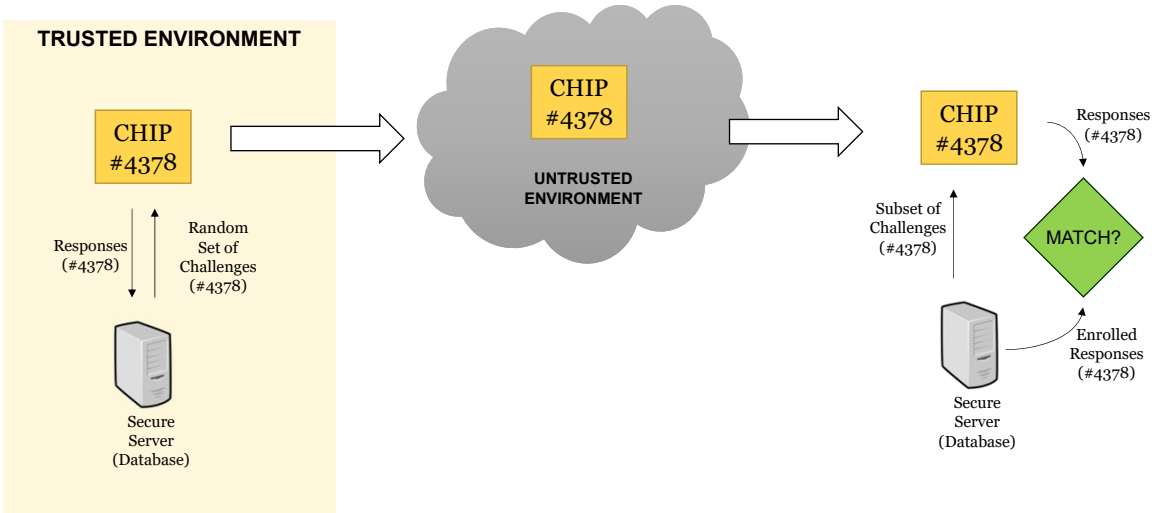
- How to identify and authenticate billions of devices?
- Traditional solution: secret IDs programmed during the test
  - Vulnerable to tampering attacks (implementation dependent)
  - "*Merely calling a bit string a "secret key" does not make it secret, but rather identifies it as an interesting target for the adversary*" [1]
- Programmed secrets don't prevent counterfeiting
  - $75 billion dollar fake semiconductor market [2]

[1] Ron Rivest, "*Illegitimi non carborundum*". Invited keynote talk, CRYPTO 2011.
[2] https://www.designnews.com/cyber-security/dangers-counterfeit-semi-chips, accessed on 1 Dec 2020

What are Physical Unclonable Functions?

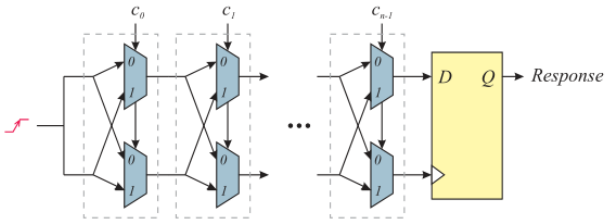
- PUFs offer low-cost entity for secret key generation or authentication
- PUFs create a unique device "fingerprint" from inherent device process variation
- Manufacturing another identical PUF is unlikely
- PUFs use a challenge-response protocol
- Weak PUFs have limited number of challenges-response pair (CRP)
  - Require extra hardware for error correction and encryption
- Strong PUFs have large number of challenges
  - Exhaustive enumeration of challenge-response pairs (CRPs) is impractical

How is authentication performed with a Strong PUF?



Background – Arbiter PUF

- Two signals race throughout identical delay paths
- Response depends on which signal arrived first at the arbiter
- Delay variability and input challenge define the response

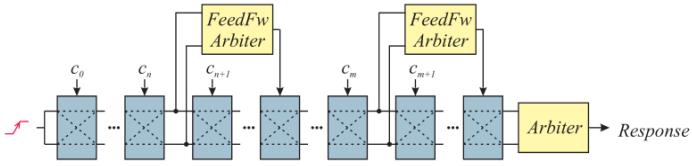


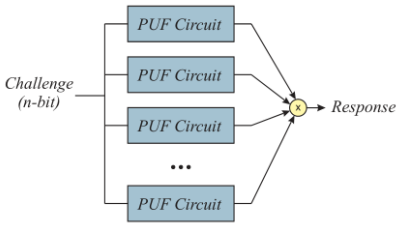
Is it secure?

640 CRPs is enough to model a 64-bit Arbiter PUF with 95% accuracy

Background – Feed-forward PUF and XOR PUF

- Additional arbiters use accumulated delay to select MUXes
- XOR combines responses of multiple Arbiter PUFs
- Additional arbiters improve learning resistance at the cost of lower reliability



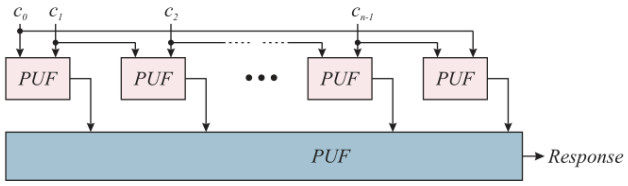


Is it secure?

Most Arbiter PUF variants can be broken!

Composite PUFs – PUF on PUF

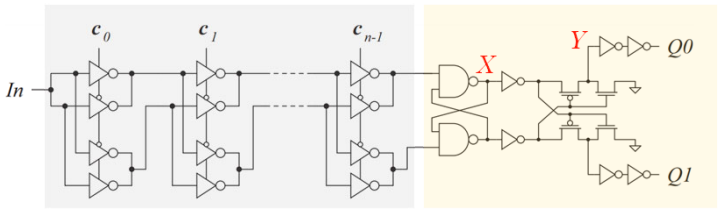
- Compositions use multiple PUF instances to act as a single strong PUF [1]
- First layer responses are used as challenge input to following layer(s)
  - Instance-specific challenge transformation



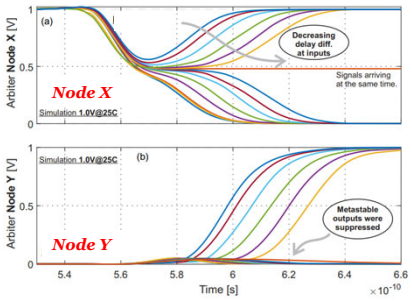
[1] Z Wu, Hiren D Patel, Manoj Sachdev, and Mahesh V Tripunitara, "Strengthening PUFs using Composition," ICCAD, pages 1 – 8, 2019.

Circuit Level Implementation – Enhancing Arbiter Reliability

- We use tristate inverters as delay cells
- Arbiter has NAND gates in positive feedback
- Glitch suppression circuit suppresses metastable outputs → enhanced reliability



MUX Path Arbiter

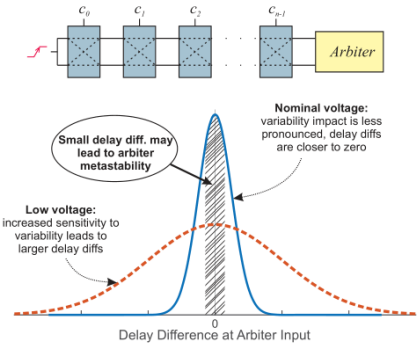


Low-Voltage Reliable PUF Operation

- At low-voltage, MOS current has increased sensitivity to process variations* → increased delay difference!
- Designed a 65 nm testchip to test this hypothesis
- Measured delay differences using dedicated outputs to IO PADs and an oscilloscope (no arbiter)**
- Lower voltages yield wider delay difference distributions
- Impact of noise is seen at 0.2V when the same set of challenges is measured a second time

*B Zhai, et al. Analysis and mitigation of variability in subthreshold design. In Int Symposium on Low Power Electronics and Design, 20–25, 2005.

**Stangherlin and Sachdev, "Reliable Strong PUF Enrollment and Operation with Temperature and Voltage Optimization," International Symposium on Quality Electronic Design, March 2021.

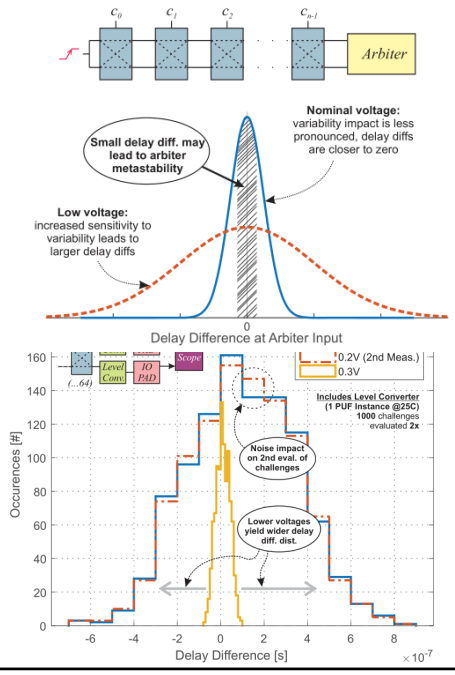


Low-Voltage Reliable PUF Operation

- At low-voltage, MOS current has increased sensitivity to process variations* → increased delay difference!
- Designed a 65 nm testchip to test this hypothesis
- Measured delay differences using dedicated outputs to IO PADs and an oscilloscope (no arbiter)**
- Lower voltages yield wider delay difference distributions
- Impact of noise is seen at 0.2V when the same set of challenges is measured a second time

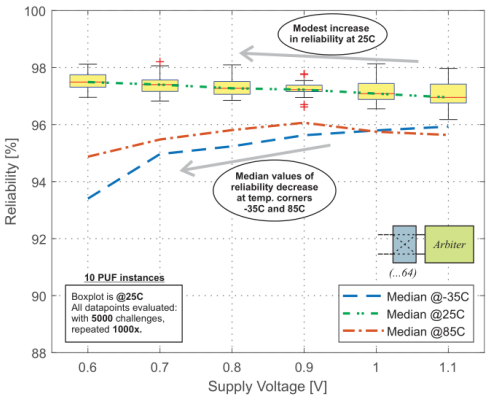
*B Zhai, et al. Analysis and mitigation of variability in subthreshold design. In Int Symposium on Low Power Electronics and Design, 20–25, 2005.

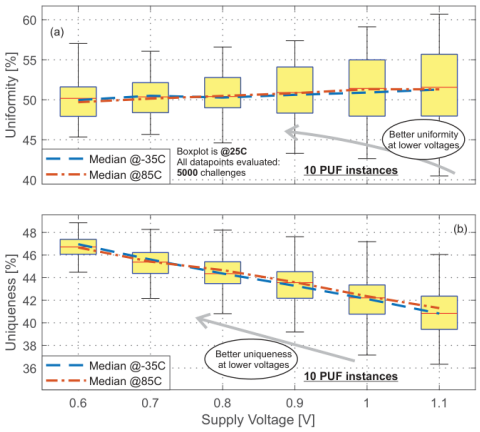
**Stangherlin and Sachdev, "Reliable Strong PUF Enrollment and Operation with Temperature and Voltage Optimization," International Symposium on Quality Electronic Design, March 2021.



Measurement Results

- Measurements on 5,000 challenges repeated 1000 times each
  - Modest increase in reliability with reduced voltage
  - Significant improvement in Uniformity and Uniqueness

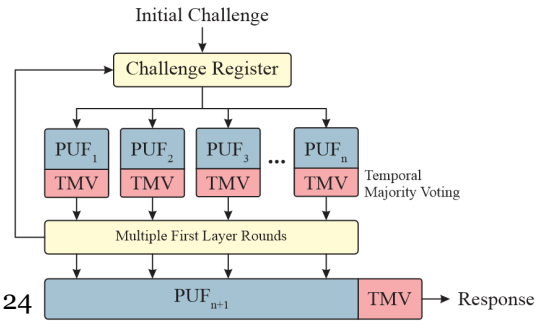




Stangherlin and Sachdev, "Reliable Strong PUF Enrollment and Operation with Temperature and Voltage Optimization," International Symposium on Quality Electronic Design, March 2021.

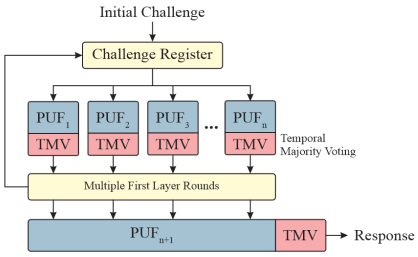
Composition to Build Learning Resistant PUFs

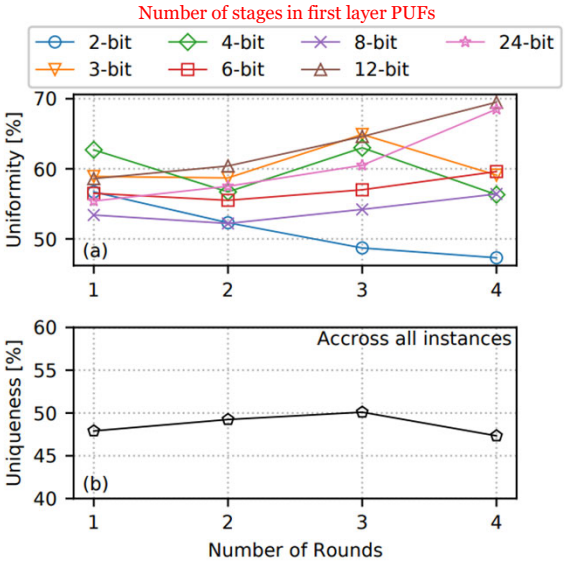
- Multiple instances of Arbiter PUFs to achieve higher learning resistance
- First layer PUFs can have multiple evaluation rounds
  - More layers for the same Silicon area
- Second layer PUF is has 64 stages
- First layer uses 64 PUF instances
  - We experiment with different sizes: 2, 3, 4, 6, 8, 12, 24
- Temporal Majority Voting (TMV) is used to enhance reliability



Uniformity and Uniqueness of Composite PUFs - Measurement

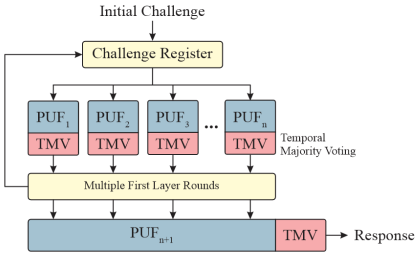
- Uniformity for single round is presents acceptable values
- Additional rounds increase uniformity bias
- Uniqueness is acceptable throughout all assessed rounds

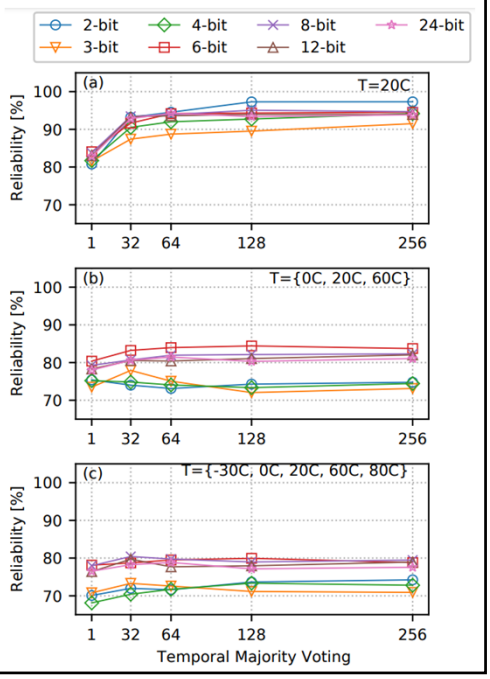




Reliability using TMV - Measurement

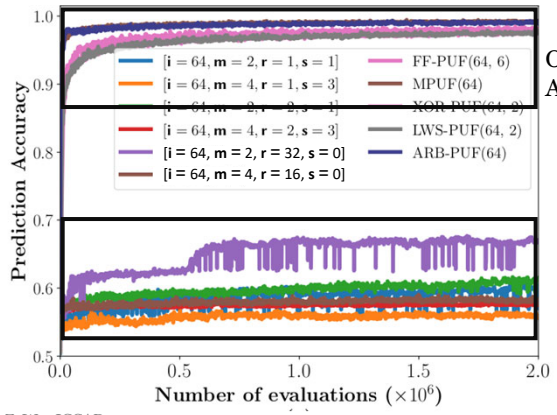
- At temperature of enrollment (20 C) TMV significantly improves reliability
- TMV improvement in reliability is significantly reduced when the PUF is evaluated at other temperatures





Comparing against other PUFs

- Evolutionary strategies using 64-bit PUFs



Other Architectures

P ∘ P

Other architectures successfully modeled at ~95% PA

P ∘ P withstand ES with PA ~70%

Z. Wu, ICCAD 2019

Learning Resistance of Composite PUFs

- Learning resistance in Composite PUFs require larger than minimal PUFs in the 1st layer
- For the 24-bit PUFs in first layer, model accuracy decreases as the number of rounds increase

Model Accuracy using Deep Neural Networks:

Bits 1st Stage	1 Round	2 Rounds	3 Rounds	4 Rounds
2-bits	81%	91%	93%	96%
24-bits	66%	60%	59%	55%


UNIVERSITY OF
WATERLOO