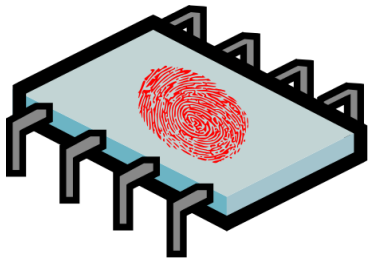
PUFSec:
Protecting Physical Unclonable Functions Using Hardware Isolation-based System Security Techniques

Mengmei Ye*, Mehrdad Zaker Shahrak**, and Sheng Wei*
*University of Nebraska-Lincoln (UNL)
**Arizona State University (ASU)

PUF for Authentications



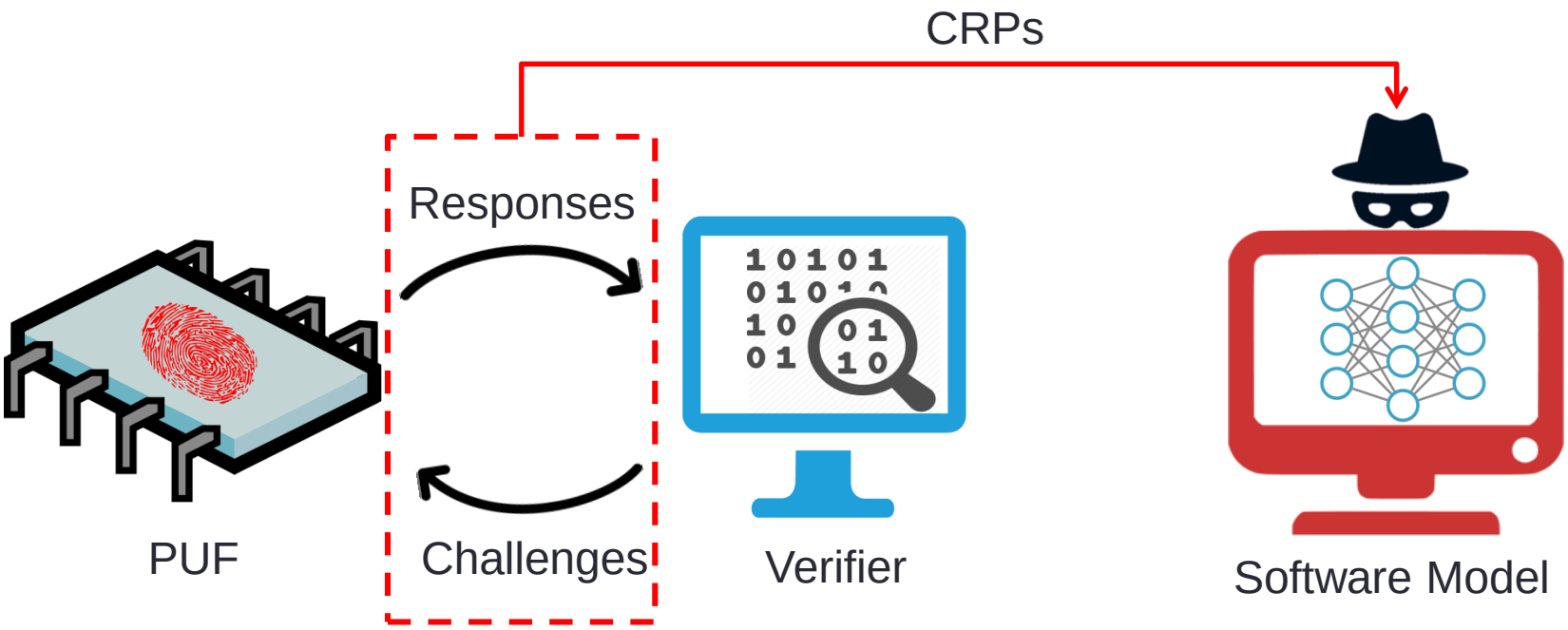
Device with PUF

Responses

Challenges

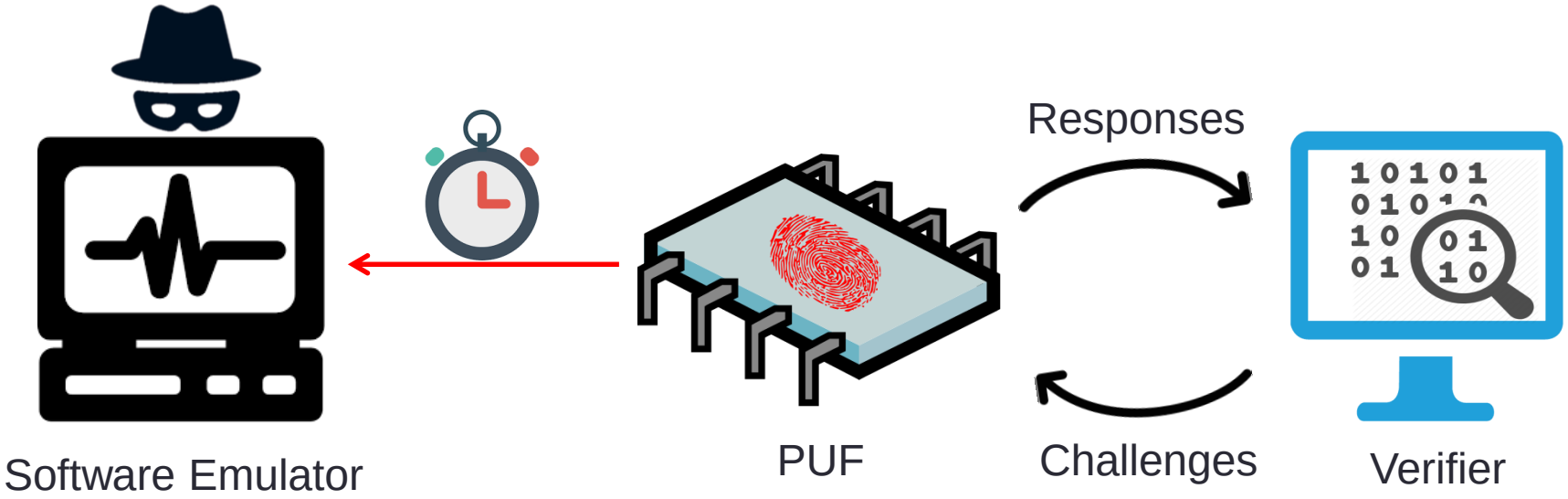
Verifier

Modeling Attacks on PUF[1][2][3]



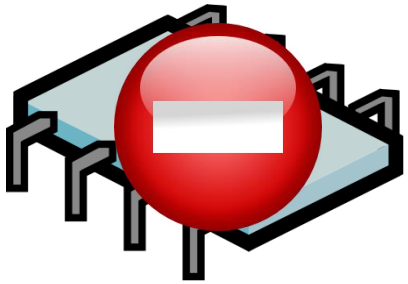
[1] C. Helfmeier, C. Boit, D. Nedospasov, and J.-P. Seifert, “Cloning physically unclonable functions,” in HOST, 2013, pp. 1–6.
[2] S. Wei, J. B. Wendt, A. Nahapetian, and M. Potkonjak, “Reverse engineering and prevention techniques for physical unclonable functions using side channels,” in DAC,2014, pp. 1–6.
[3] U. Rhrmair, F. Sehnke, J. Slter, G. Dror, S. Devadas, and J. Schmidhuber, “Modeling attacks on physical unclonable functions,” in CCS, 2010, pp. 237–249.

Modeling Attacks on PUF[1][2][3]

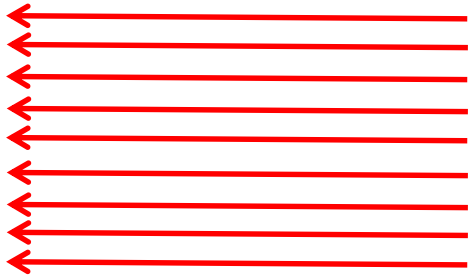


[1] C. Helfmeier, C. Boit, D. Nedospasov, and J.-P. Seifert, “Cloning physically unclonable functions,” in HOST, 2013, pp. 1–6.
[2] S. Wei, J. B. Wendt, A. Nahapetian, and M. Potkonjak, “Reverse engineering and prevention techniques for physical unclonable functions using side channels,” in DAC,2014, pp. 1–6.
[3] U. Rhrmair, F. Sehnke, J. Slter, G. Dror, S. Devadas, and J. Schmidhuber, “Modeling attacks on physical unclonable functions,” in CCS, 2010, pp. 237–249.

Service Capacity DoS Attacks for PUF



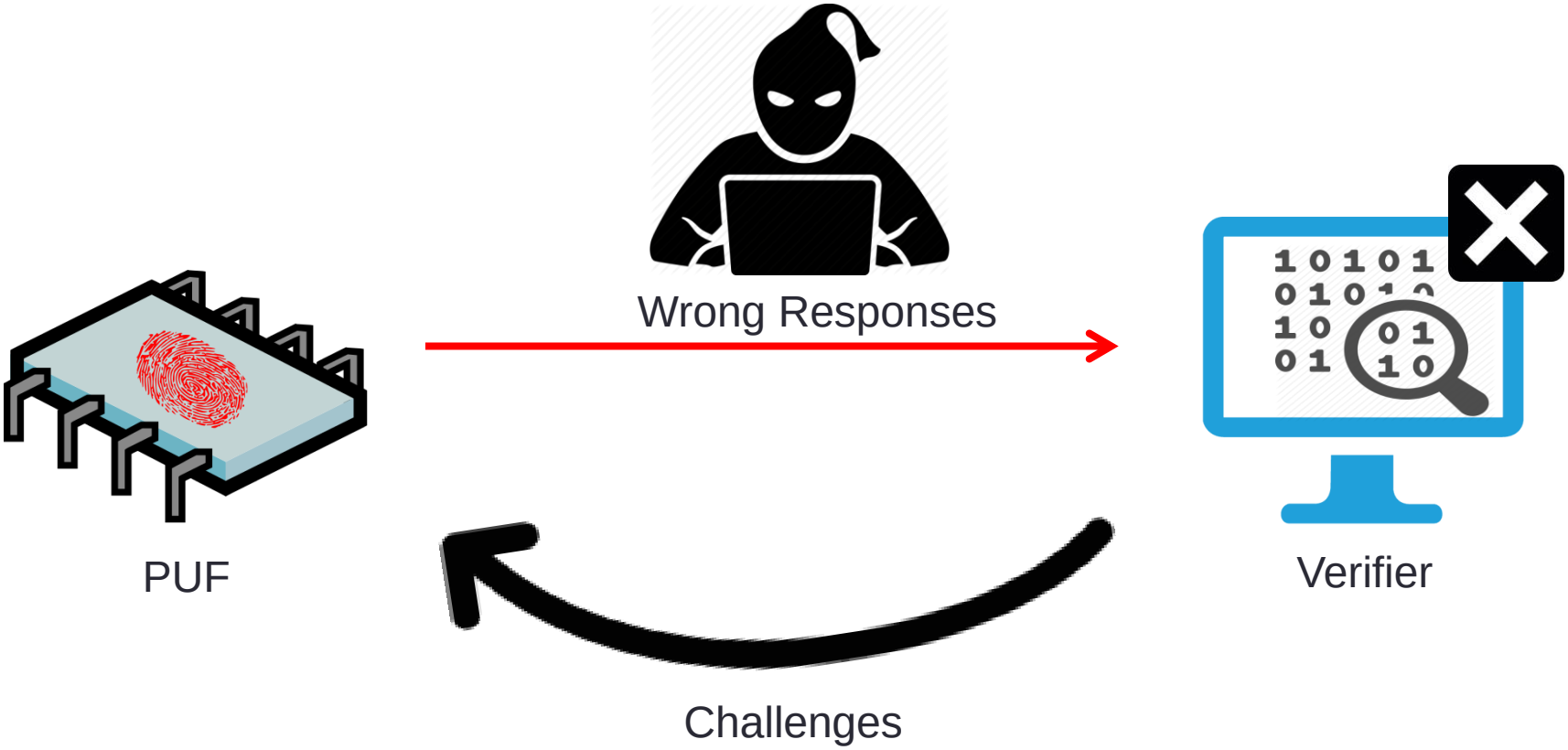
PUF



Many Challenges

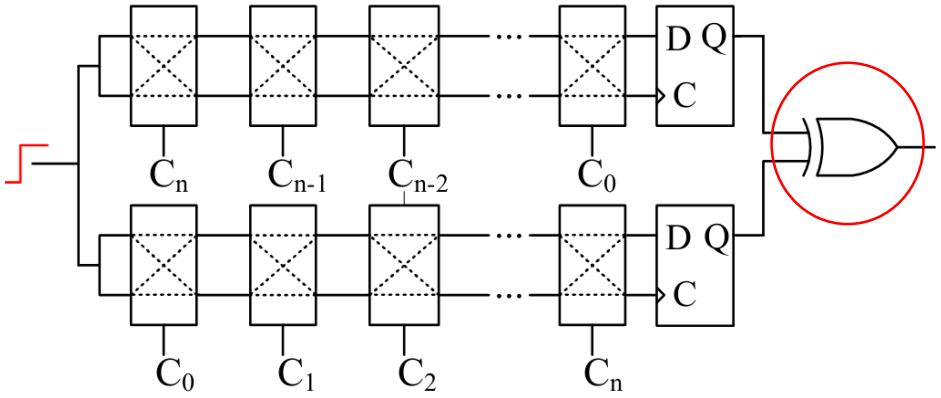
Malicious Verifier

Data Falsifying DoS Attacks for PUF



Existing Protection Schemes against Modeling Attacks

- Internal PUF improvements[4][5]
  - Maximize randomness of PUF
  - Minimize correlation between challenges and responses

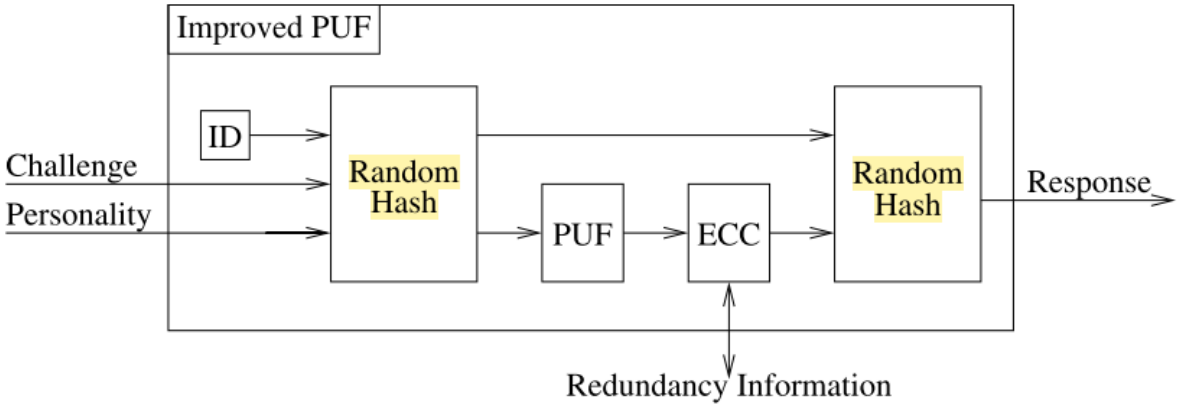


XOR PUF [Suh et al. DAC' 07]

[4] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in DAC, 2007, pp. 9–14.
[5] 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 application," in VLSI Circuits, 2004, pp. 176–179.

Existing Protection Schemes against Modeling Attacks

- External PUF protection[6][7][8]
  - Obfuscate CRPs
  - Employ security protocols

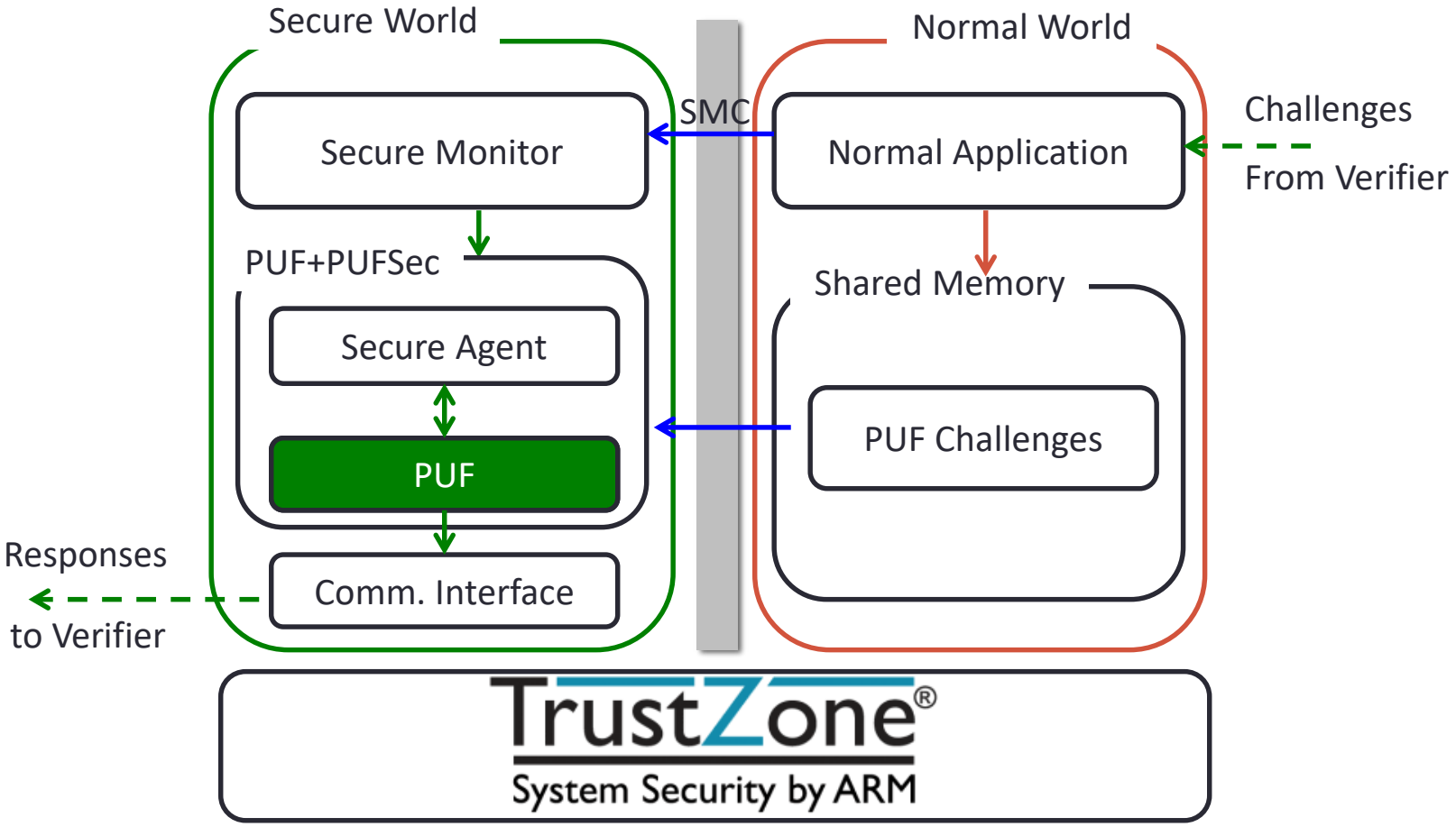


Controlled PUF [Gassend CCS'02]

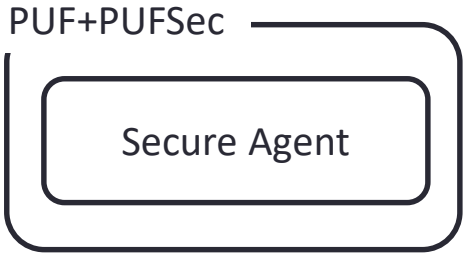
[6] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in CCS, 2002, pp. 148–160.
[7] M. Majzoobi, M. Rostami, F. Koushanfar, D. S.Wallach, and S. Devadas, "Slender PUF protocol: a lightweight, robust, and secure authentication by substring matching," in SPW, 2012, pp. 33–44.
[8] M.-D. Yu, M. Hiller, J. Delvaux, R. Sowell, S. Devadas, and I. Verbauwhede, "A lockdown technique to prevent machine learning on PUFs for lightweight authentication," IEEE Transactions on Multi-Scale Computing Systems, vol. 2, no. 3, pp. 146–159, 2016.

PUFSec: Hardware Isolation-based Secure Architecture Extension

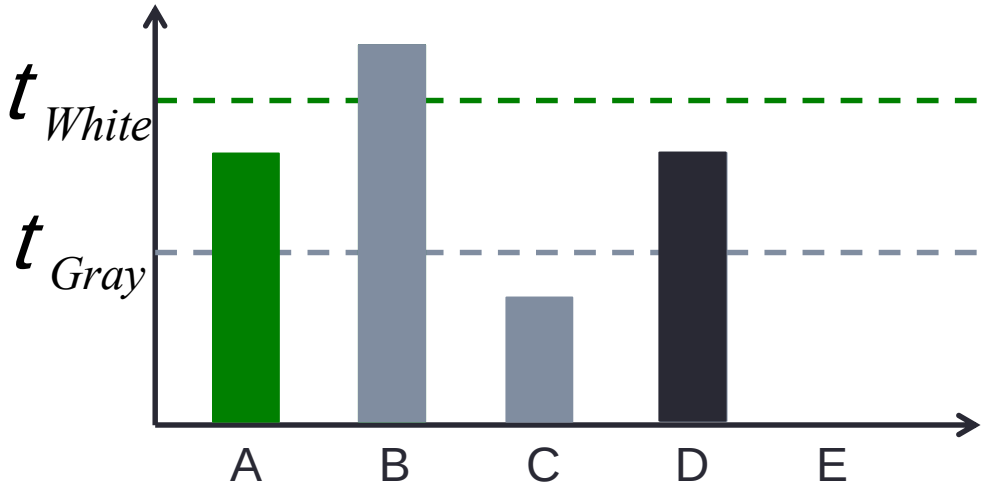
- ✓ "Divide and conquer" security paradigm
  - ✓ Extract security protection task from PUF design process
- ✓ Low performance overhead and power consumptions

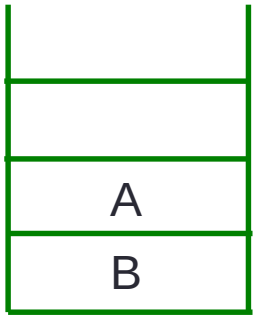


PUFSec - Access Control



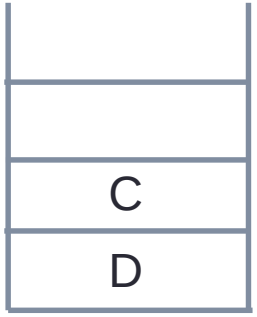
$$GrowthRate = \frac{\#CurrentCRPs}{\#TotalCRPs}$$





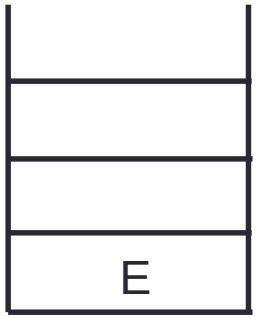
White List

Benign Verifiers



Gray List

Suspicious Verifiers



Black List

Malicious Verifiers

PUFSec Implementation

Xilinx ZC702

Secure World

Normal World

Secure Monitor

Normal Application

Secure Agent with Access Control

Zynq Processing System (PS)

AXI Interconnect

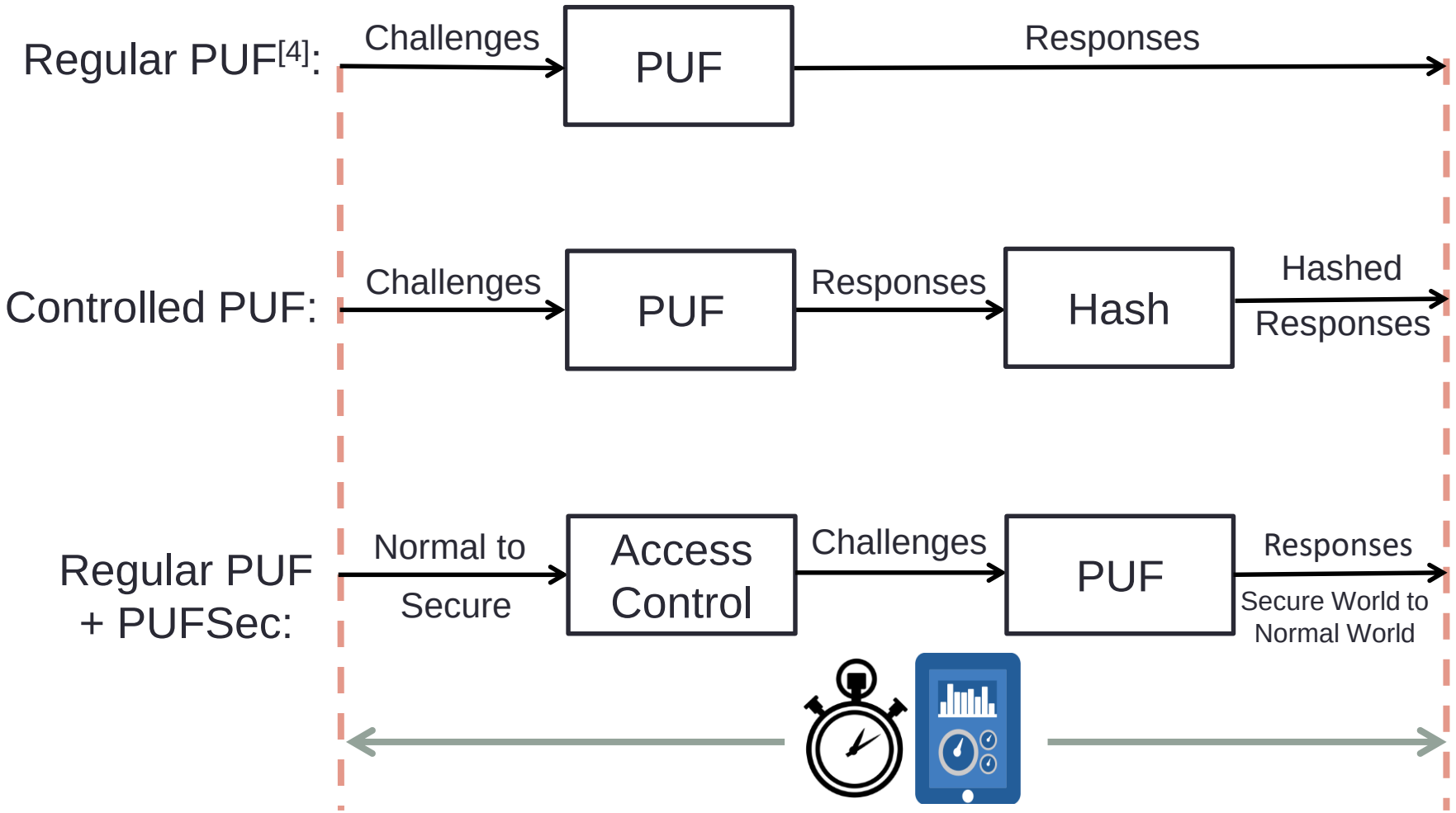
Programmable Logic (PL)

Shared Memory

Secure Memory

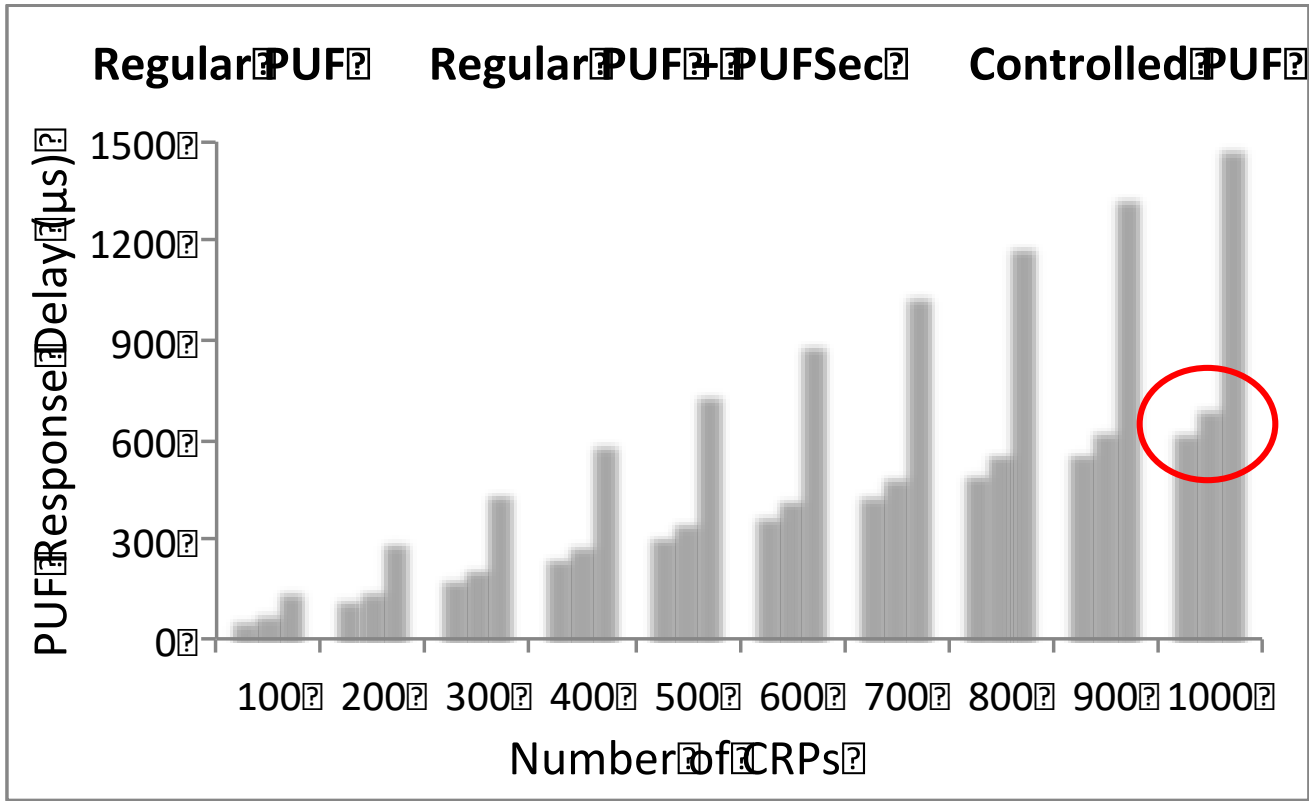
PUF IP
(Secure World)

Experimental Setup



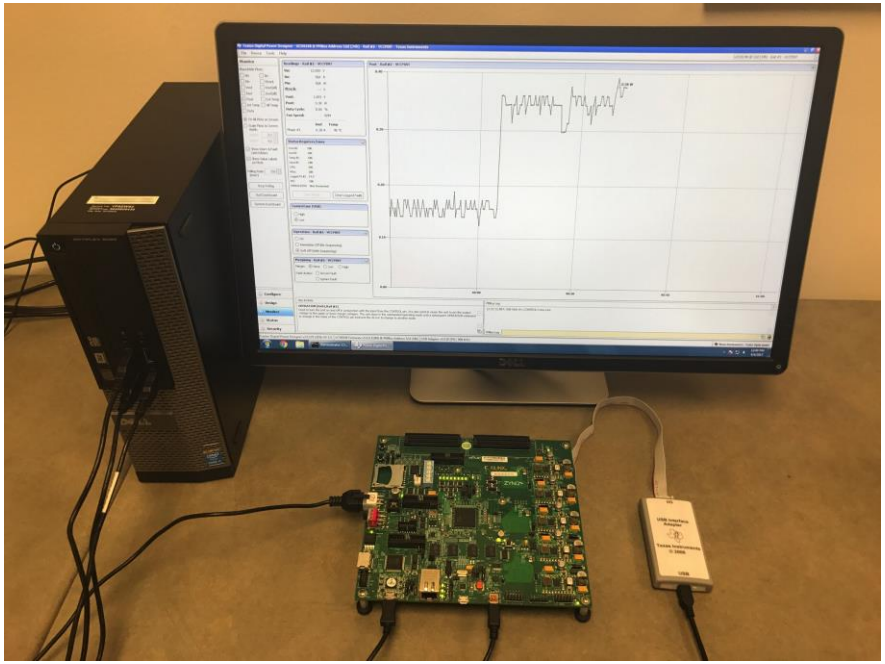
[4] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in DAC, 2007, pp. 9–14.

Performance Overhead



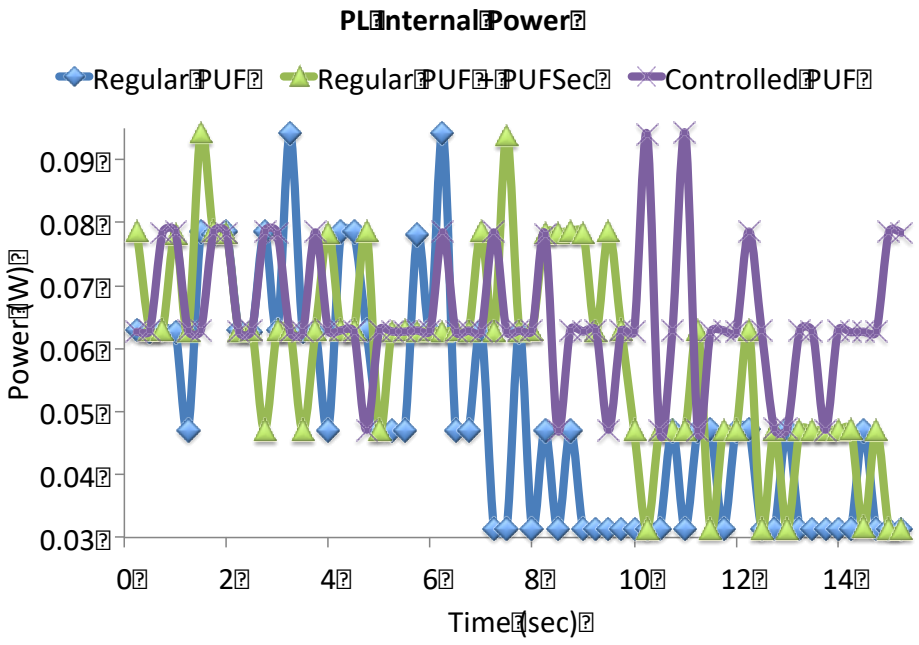
Power Experimental Setup

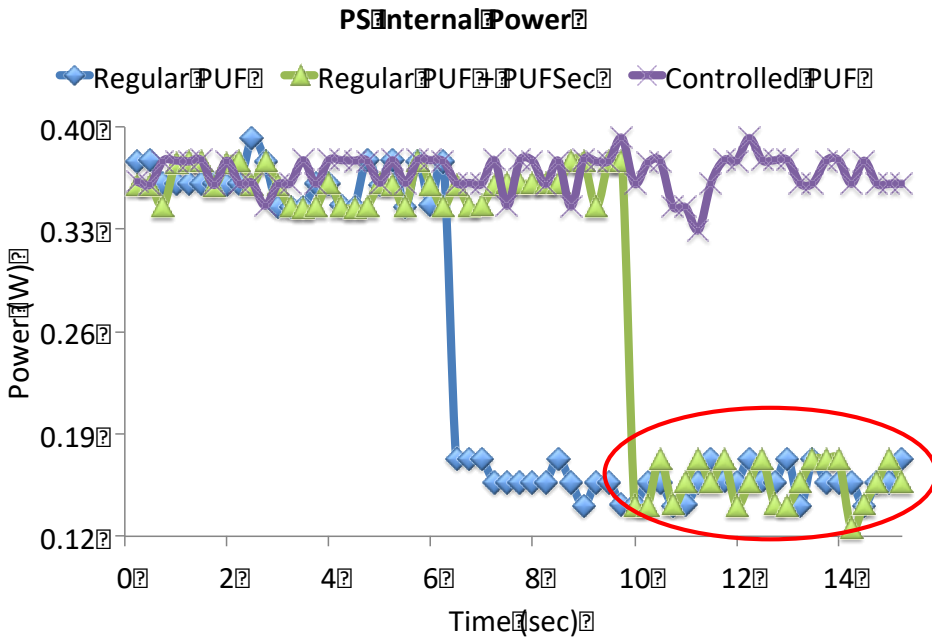
- Use TI Fusion tools for PL and PS internal power measurement[9]
- Invoke PUF with 10 million CRPs to ensure measurement accuracy



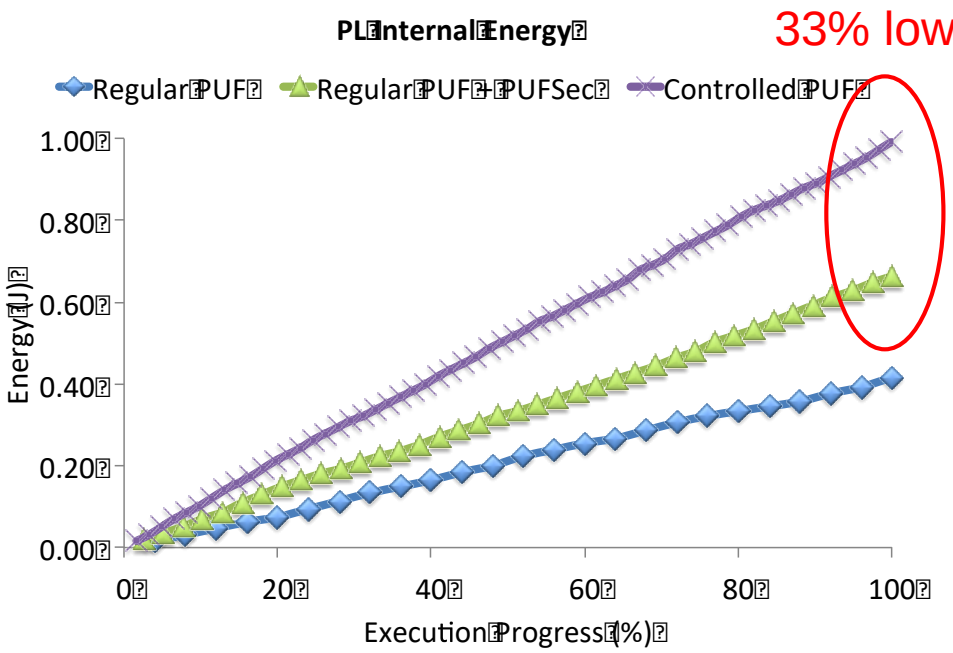
[9] E. Srikanth, “Zynq-7000 AP SoC low power techniques part 2 - measuring ZC702 power using TI Fusion Power Designer,” Xilinx, 2014.

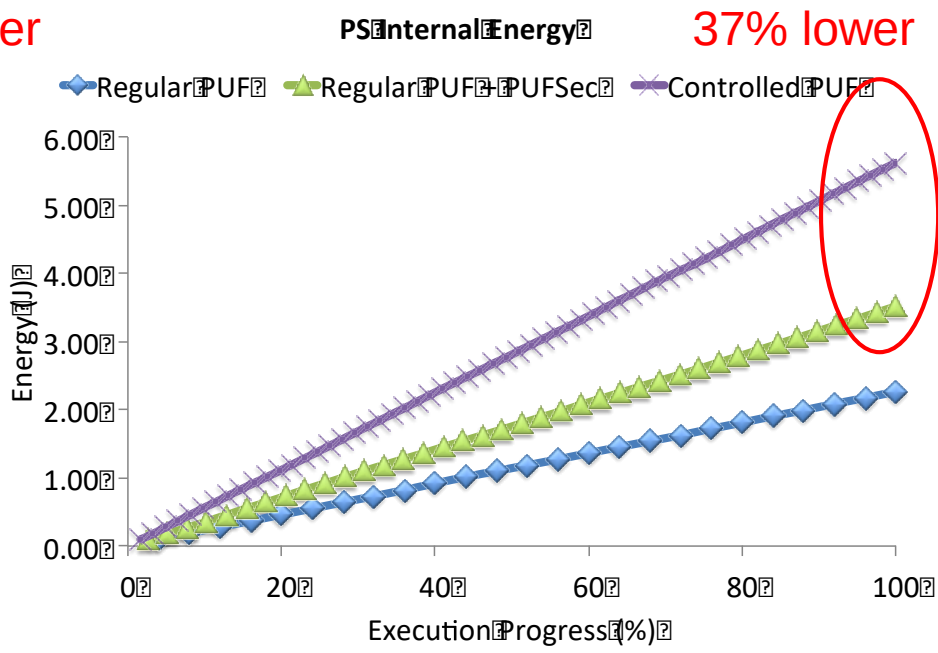
Power Consumption





Energy Consumption



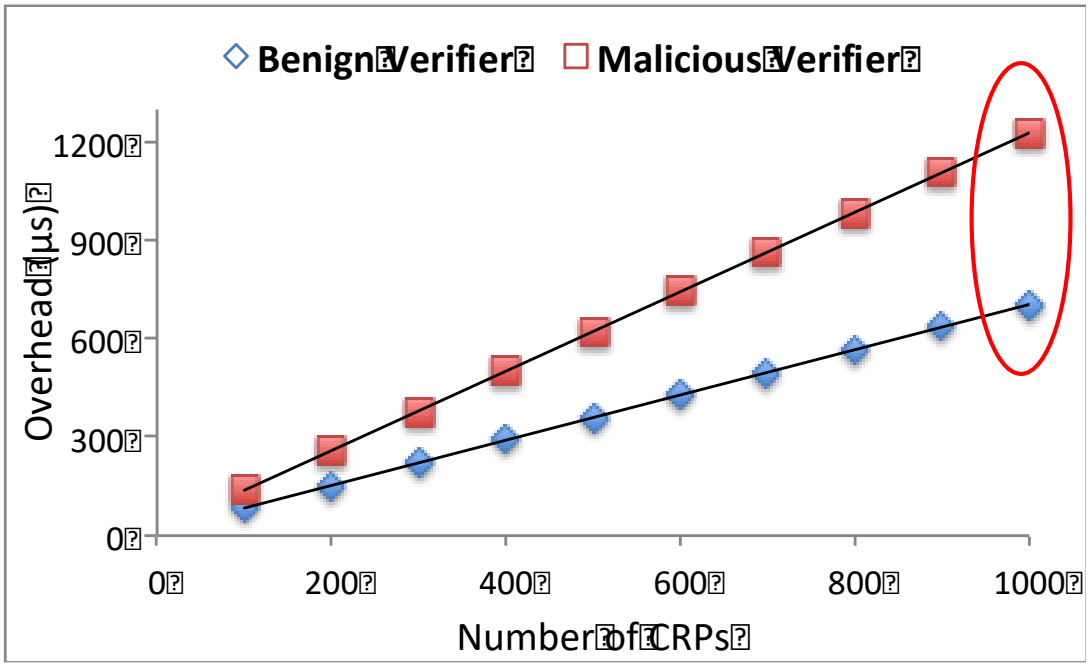


Security Analysis

PUFs	Protection Approaches	Modeling	DoS	
			Service Capacity	Data Falsifying
Regular PUF	/	NS	NS	NS
XOR PUF	Internal	S	NS	NS
Controlled PUF	External	S	NS	NS
Lockdown PUF	External	S	S	NS
Regular PUF + PUFSec	Security Extension	S	S	S

S – Secure; NS – Non-secure

Security Evaluation
- Service Capacity DoS Attacks



74% slower

Conclusion

- PUFSec: hardware isolation-based PUF protection mechanism
  - Extracted security protection task from PUF design process
  - Defended against modeling and DoS attacks
  - Achieved low performance and power overhead