# Reconfigurable physically unclonable functions based on nanoscale voltage-controlled magnetic tunnel junctions

Yixin Shao

Dept. of Electrical & Computer Engineering, Northwestern University, Evanston, IL

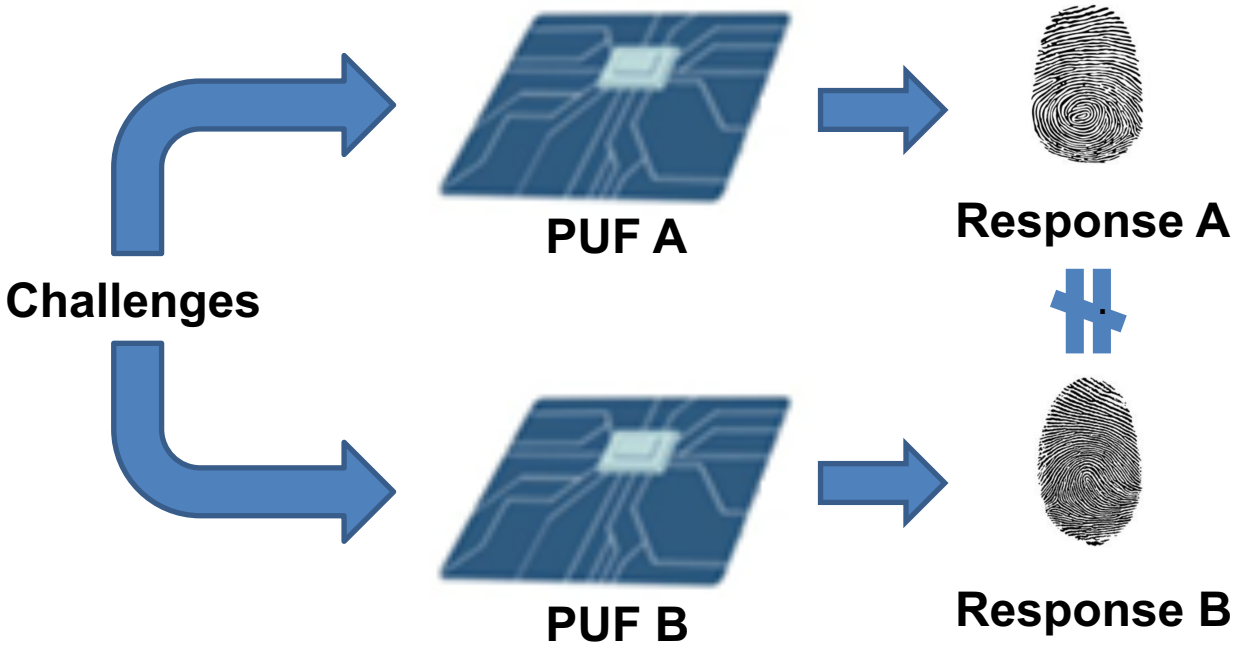
Email: yixin@u.northwestern.edu

PERL NSF

NORTHWESTERN UNIVERSITY QUAECUMQUE SUNT VERA 1851

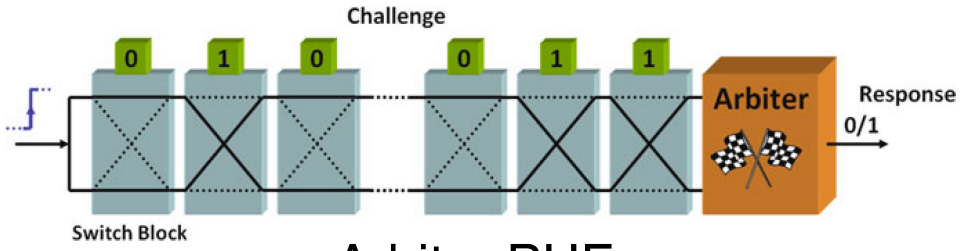
# PUF: Electrical Fingerprint

- A PUF is an “electronic fingerprint” that provides certain outputs (responses) with respect to certain inputs (challenges), where the challenge-response pairs (CRPs) are unpredictable and unique to each particular device.

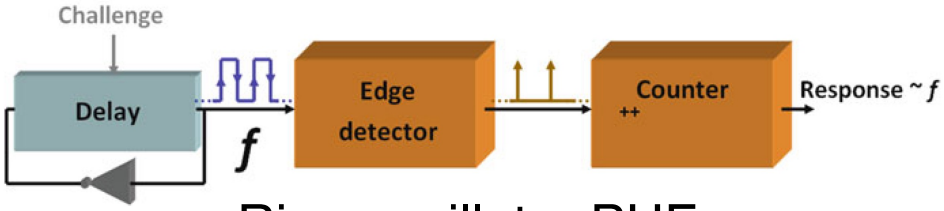


# Problems for Existing Intrinsic PUFs

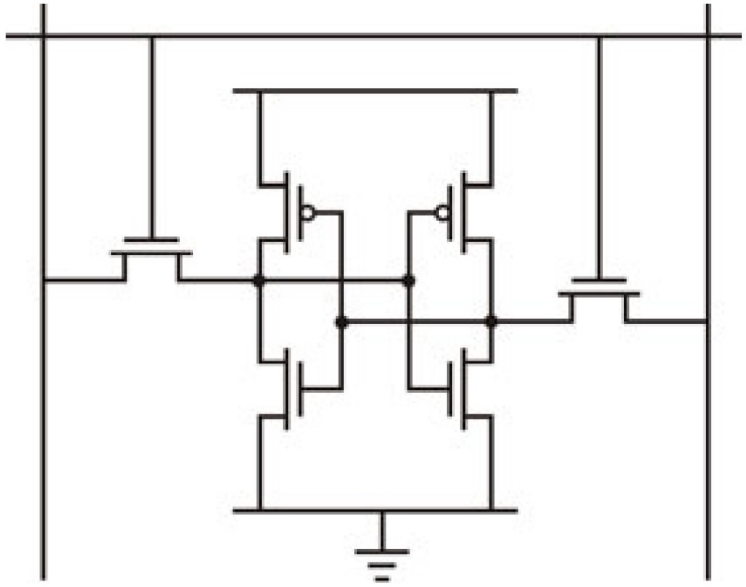
- Existing PUFs exploit manufacturing variations → static challenge-response behavior → long-term security risk




Arbiter PUF




Ring-oscillator PUF

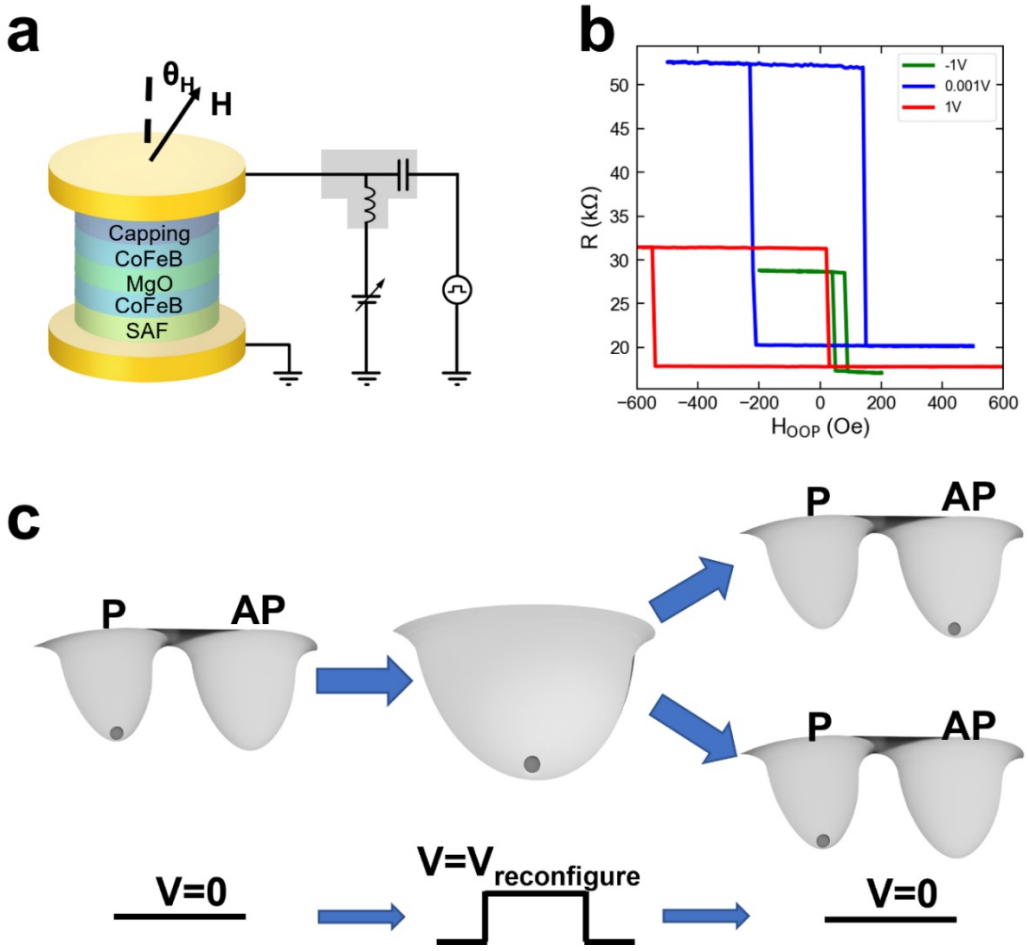


SRAM PUF

Tuyls, Pim. Towards hardware-intrinsic security: foundations and practice. Springer Science & Business Media, 2010.

# Reconfigurable PUF based on VC-MTJ

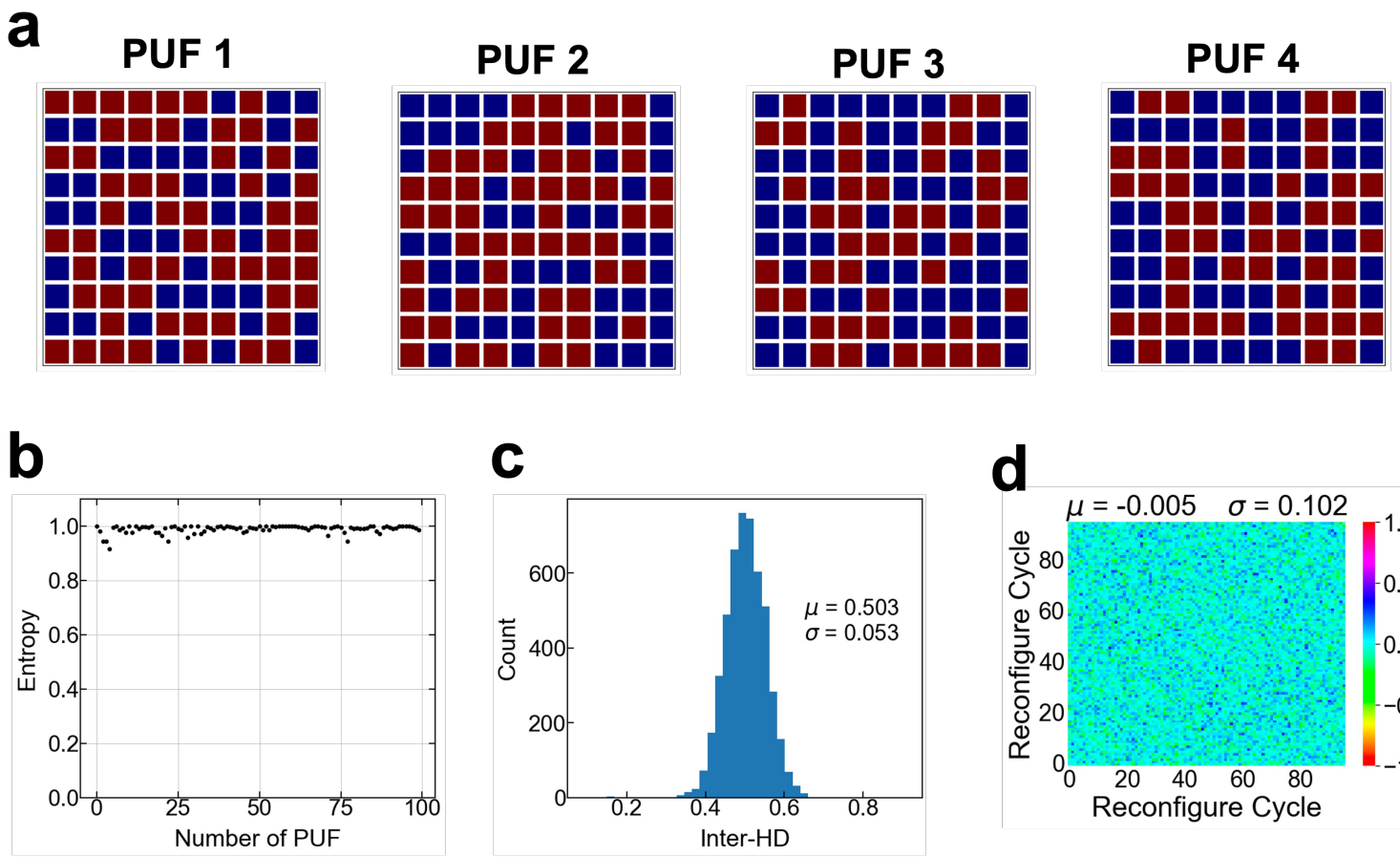
- Readout via tunneling magnetoresistance (TMR)
- Reconfigured via ns voltage pulse




Y. Shao et al., “Reconfigurable Physically Unclonable Functions Based on Nanoscale Voltage-Controlled Magnetic Tunnel Junctions. ”, Advanced Electronic Materials (2023): 2300195.

# Demonstration of 10 × 10 PUF array using VC-MTJ

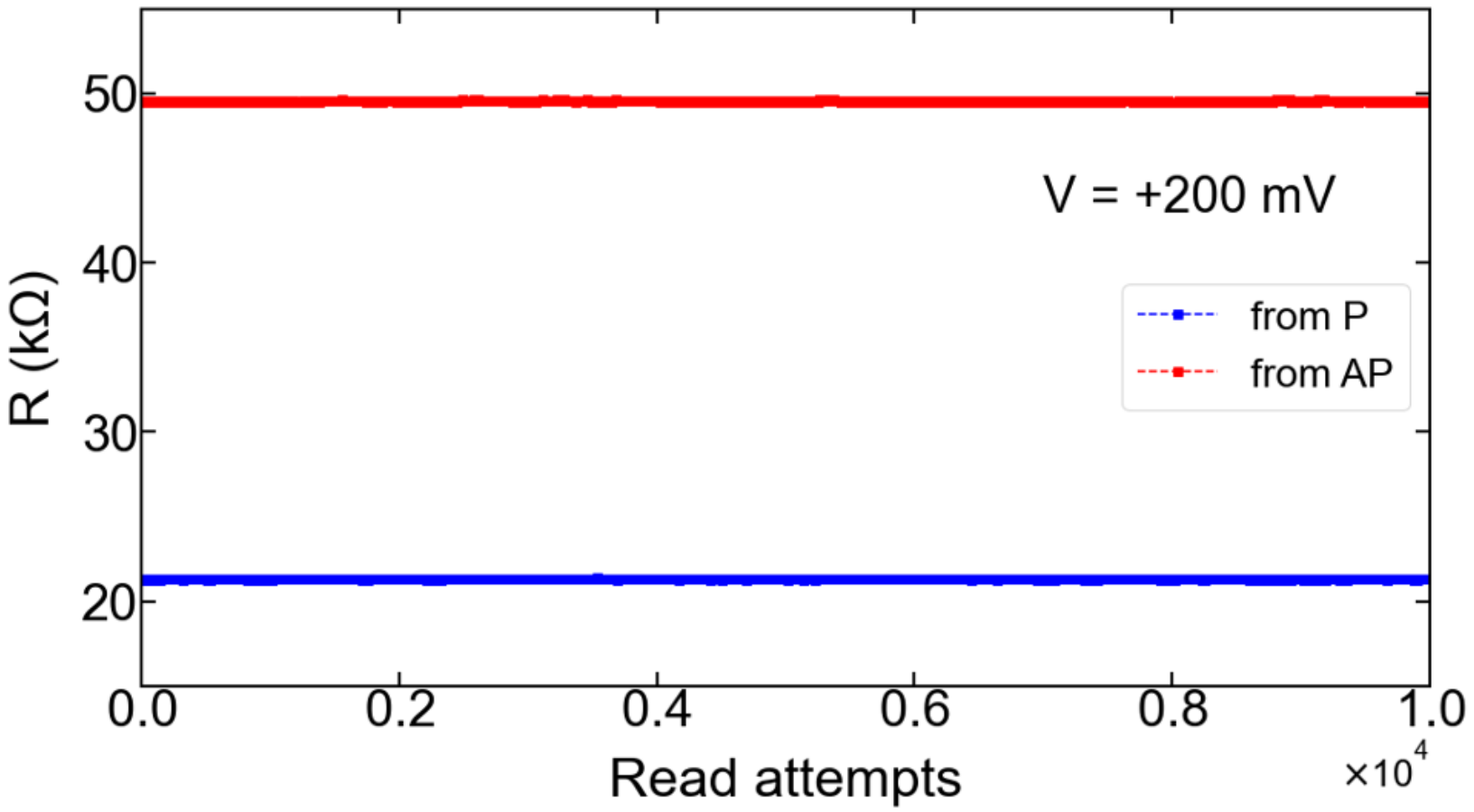
- PUF instances reconfigured with voltage pulses of 2.2 V, 10 ns
- Entropy ~ 1, inter-Hamming distance ~ 50%, correlation coefficient ~ 0




Y. Shao et al., "Reconfigurable Physically Unclonable Functions Based on Nanoscale Voltage-Controlled Magnetic Tunnel Junctions. ", Advanced Electronic Materials (2023): 2300195.

# VCMA enhanced reliability

- No bit error in $10^4$ readouts




Y. Shao et al., "Reconfigurable Physically Unclonable Functions Based on Nanoscale Voltage-Controlled Magnetic Tunnel Junctions. ", Advanced Electronic Materials (2023): 2300195.

# Conclusions

- MTJ-based reconfigurable PUF with effective metrics has been demonstrated
- Reconfiguration realized by voltage pulses as short as 10 ns using VCMA
- PUF constructed with a 10 × 10 perpendicular MTJ array with high TMR
- Entropy of ~1, inter-HD of ~ 50%, correlation coefficient of ~ 0, and zero bit-errors in $10^4$ repeated readout
- Reliable and compact solution for hardware authentication in CMOS + spintronics integrated systems.