Hardware Authentication through High-Capacity PUF-Based Secret Key Generation

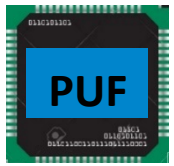
THE UNIVERSITY OF TEXAS AT AUSTIN

Challenge:

- Develop secure hardware roots of trust: physical unclonable functions (PUFs)
- Need strong PUFs immune to machine learning (ML) modeling attacks

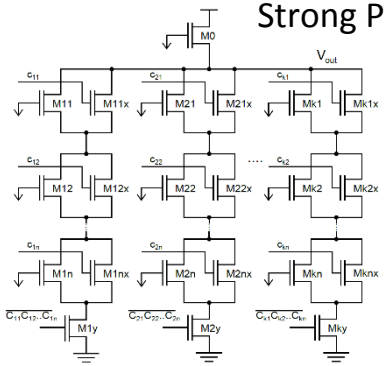
Solution:

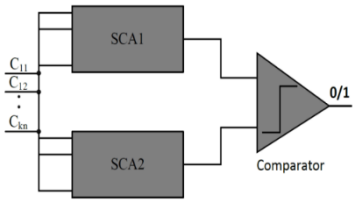
- ML-attack immunity via continuous nonlinearity
- Use subthreshold region of MOS operation
- New transistor array with exponentially large input/output space



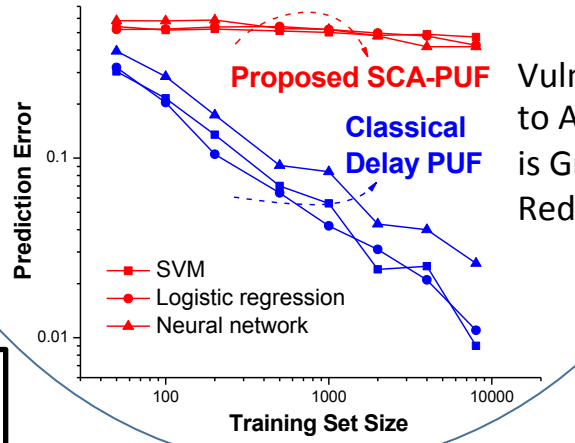
challenge	response
00111…10	0101..101
11111…11	1011..010

Strong PUF





New strong SCA-PUF



Vulnerability to Attack is Greatly Reduced

Scientific Impact:

- First silicon PUF secure against ML attacks
- Techniques for ensuring reliability of PUF outputs across a range of temperature and voltage values
- Enables lightweight PUF-based protocols

Broader Impact:

- Secure authentication on low-energy platforms
- Critical for Internet-of-Things applications
- Close interaction with industry, especially, Semiconductor Research Corporation's member companies

STARSS SaTC NSF-1441484; PIs: Michael Orshansky and Sriram Vishwanath (University of Texas at Austin);
Contact: Michael Orshansky (orshansky@utexas.edu)