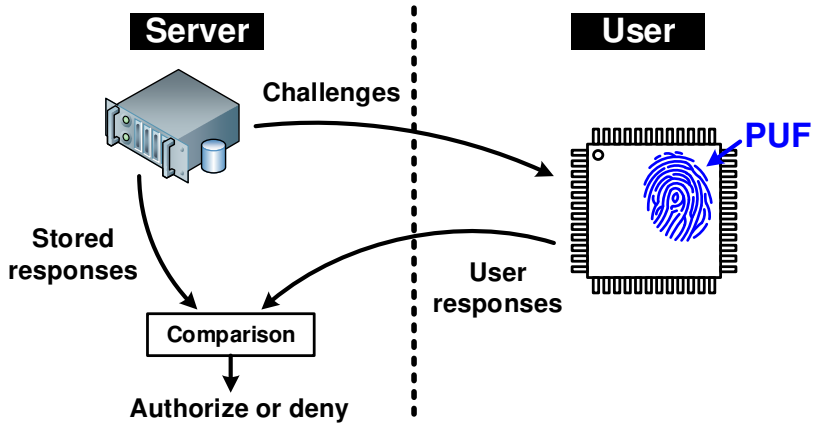
Secure and Reliable XOR Arbiter PUF Design: An Experimental Study based on 1 Trillion Challenge Response Pair Measurements

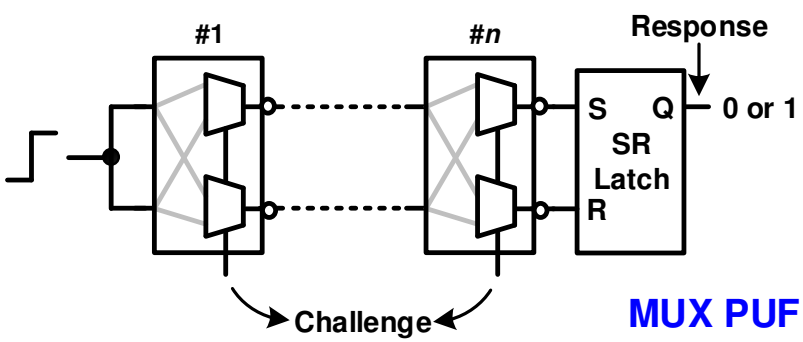
Chen Zhou, Keshab K. Parhi, Chris H. Kim

University of Minnesota, Minneapolis, MN, USA

zhoux825@umn.edu

Single MUX Physical Unclonable Function (PUF)





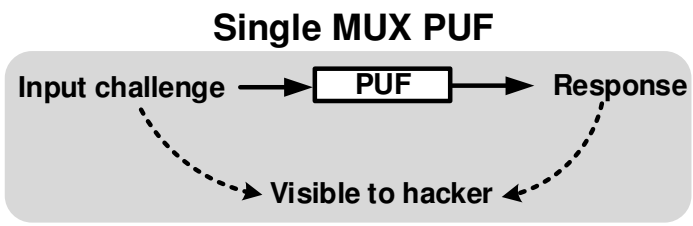
- **Advantage:**
  - **Large # of challenge response pairs (CRPs): 2^n**
- **Disadvantages:**
  - **Stability: responses sensitive to noise, VDD & temperature variation.**
  - **Security: delay parameters can be extracted easily through linear additive model**

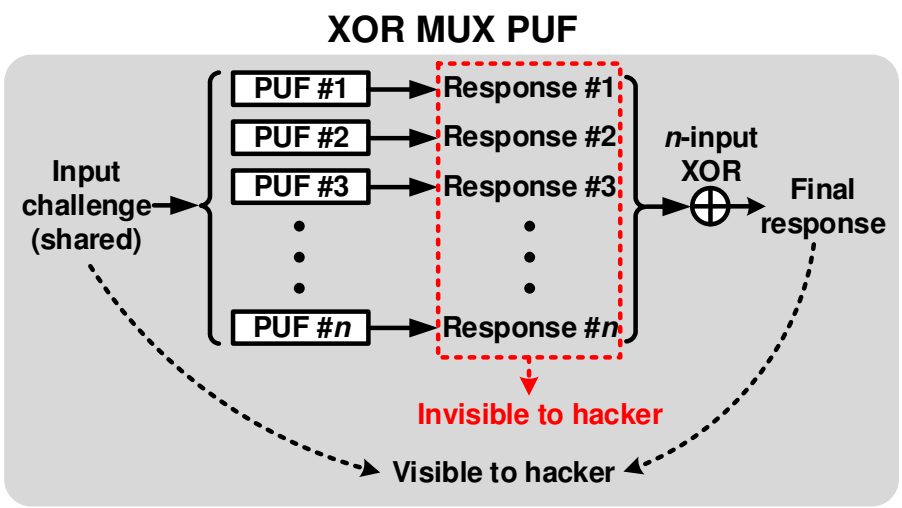
$$C = \begin{bmatrix} (2c_1-1)(2c_2-1)\cdots(2c_n-1) \\ (2c_2-1)\cdots(2c_n-1) \\ \vdots \\ (2c_n-1) \\ 1 \end{bmatrix}^T \qquad W = \frac{1}{2}\begin{bmatrix} \delta_1^0 - \delta_1^1 \\ \delta_1^0 + \delta_1^1 + \delta_2^0 - \delta_2^1 \\ \vdots \\ \delta_{n-1}^0 + \delta_{n-1}^1 + \delta_n^0 - \delta_n^1 \\ \delta_n^0 + \delta_n^1 + b \end{bmatrix}$$

$$\Delta = C \cdot W \qquad response = (sign(\Delta) + 1)/2$$

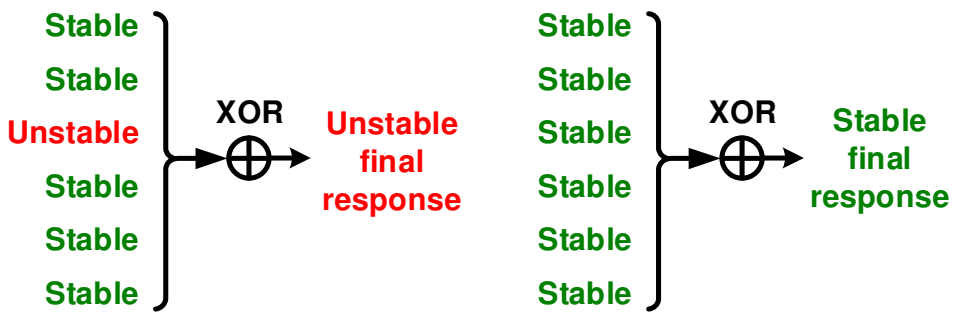
J. Delvaux, et al., HOST, 2013

XOR MUX PUF

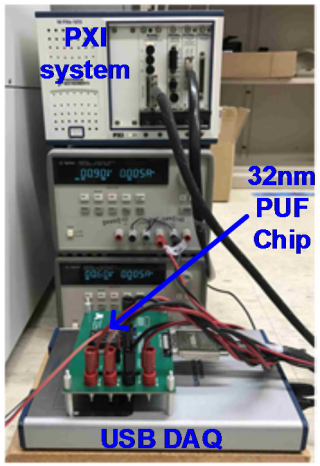


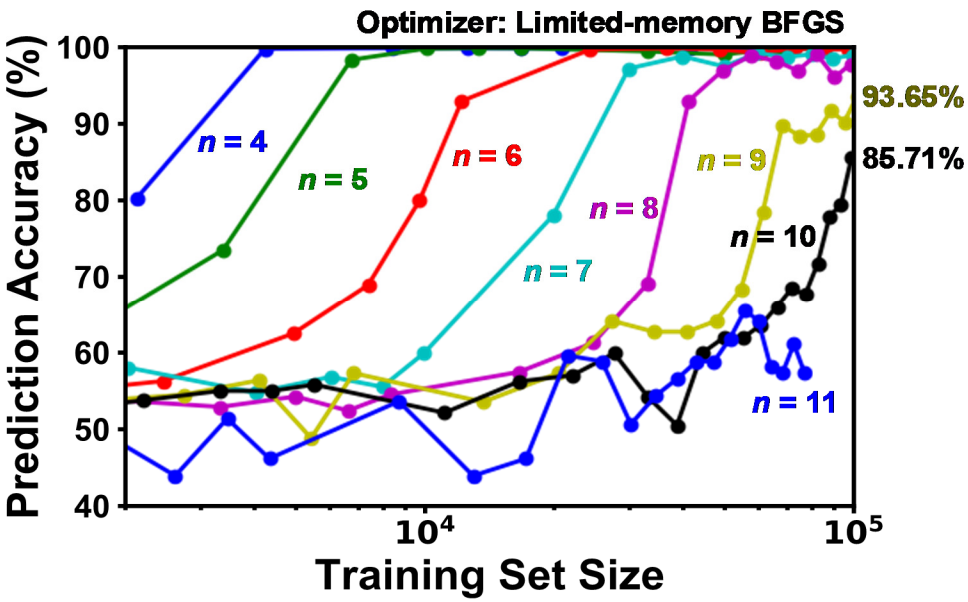


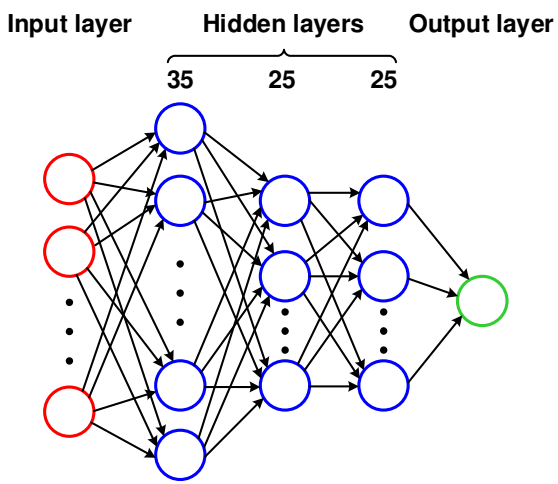
- **Advantages:**
  - Internal responses hidden
  - Linear additive model not applicable
  - Simple implementation
- **Disadvantage:**
  - Poor stability



XOR MUX PUF Security

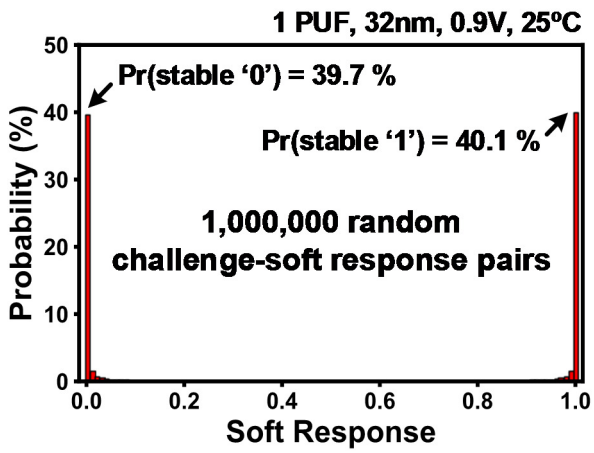


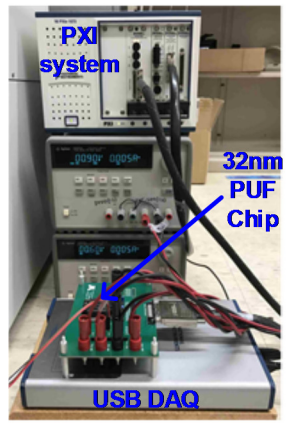


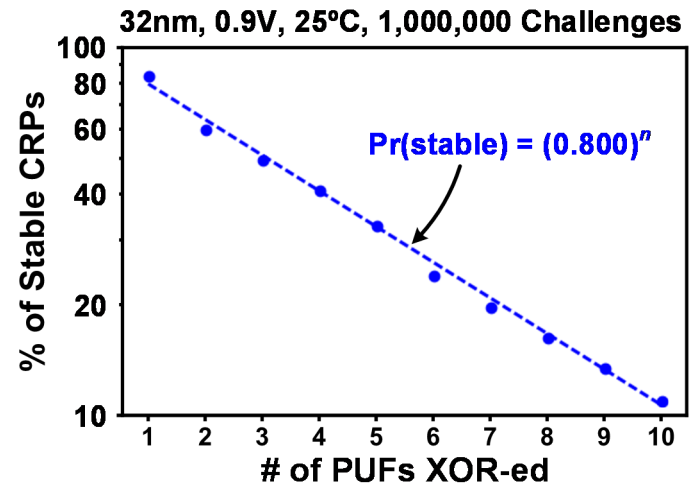


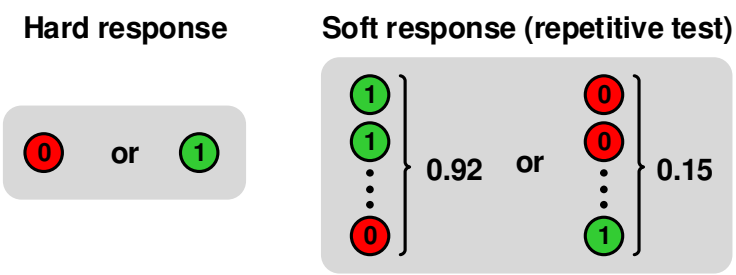
- **1,000,000 CRPs collected in 32nm chip**
- **3-layer perceptron classifier used**
- ***n>10* required for sufficient security**

XOR MUX PUF Stability



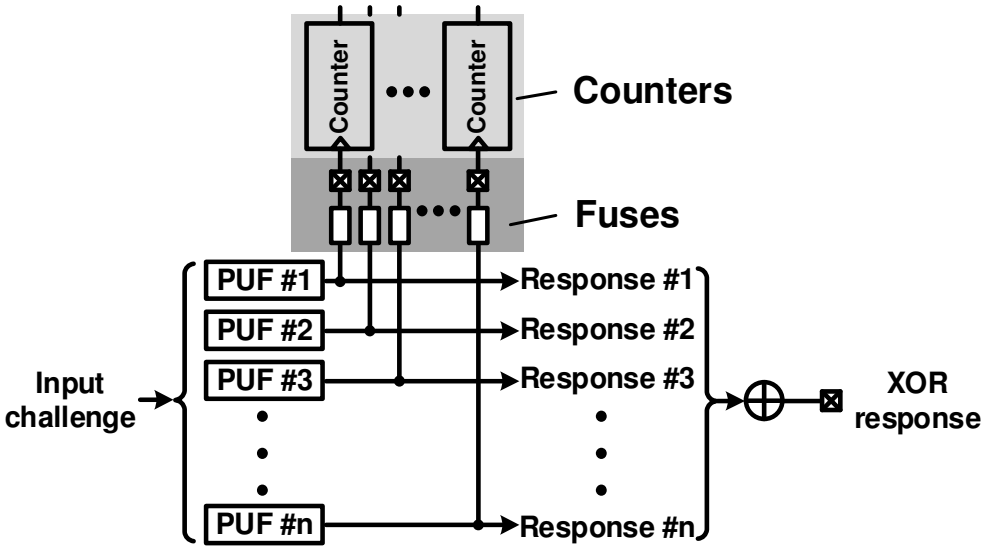


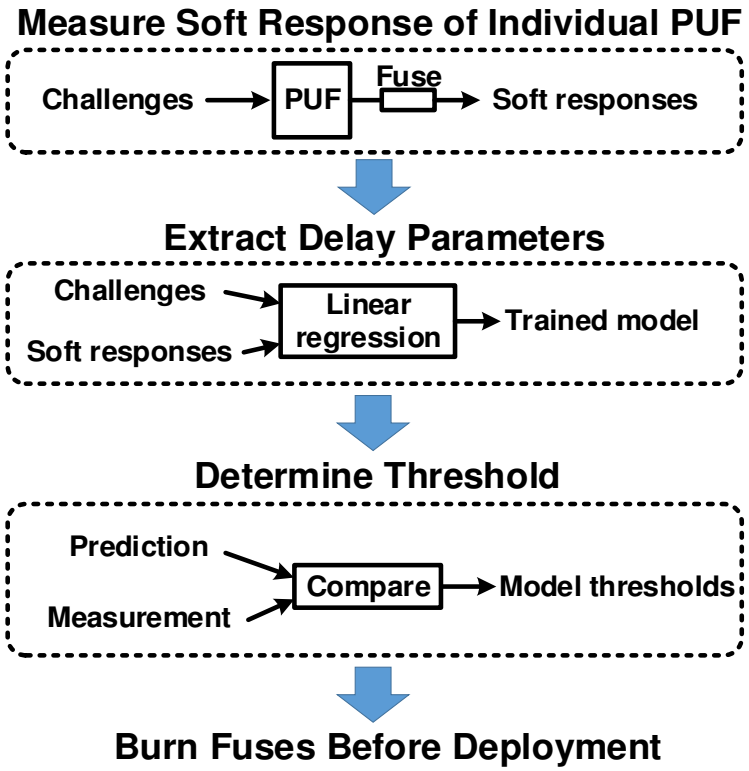




- **Single MUX PUF**
  - Soft response based on 100,000 repetitive tests
  - 79.8% of CRPs are stable (in 1 million tested CRPs)
- **XOR PUF**
  - All *n* responses must be stable
  - ~$(80\%)^n$ of CRPs yield stable final responses

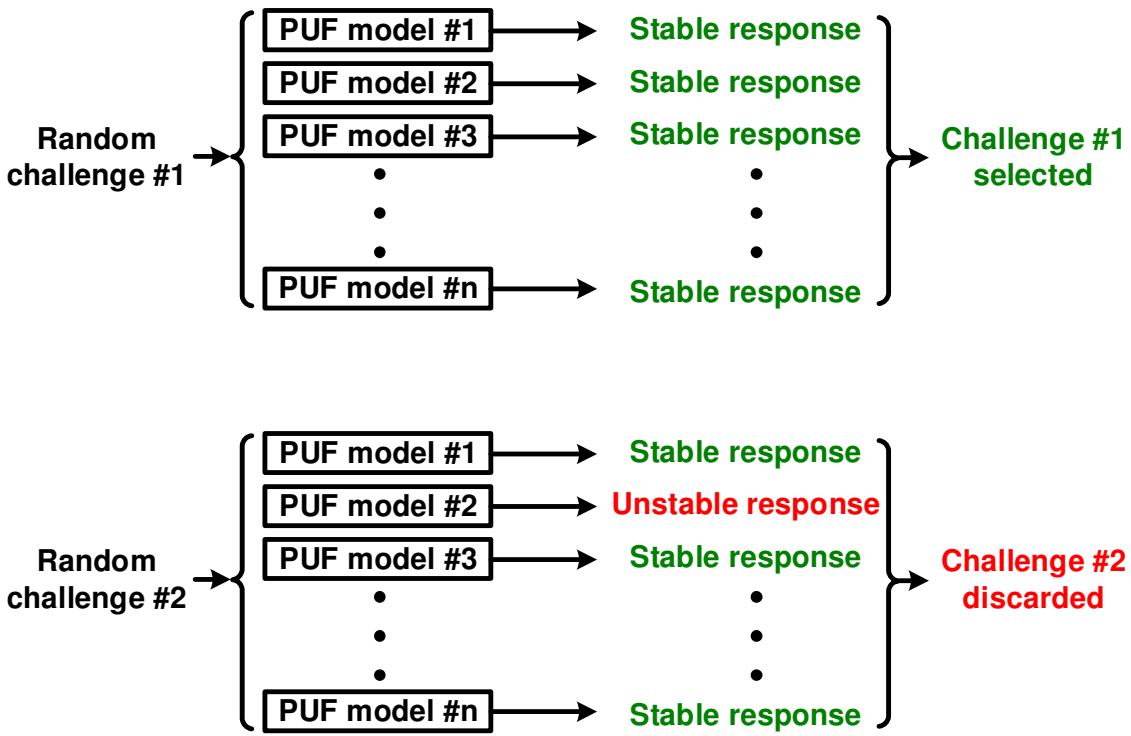
Proposed XOR PUF Enrollment Method

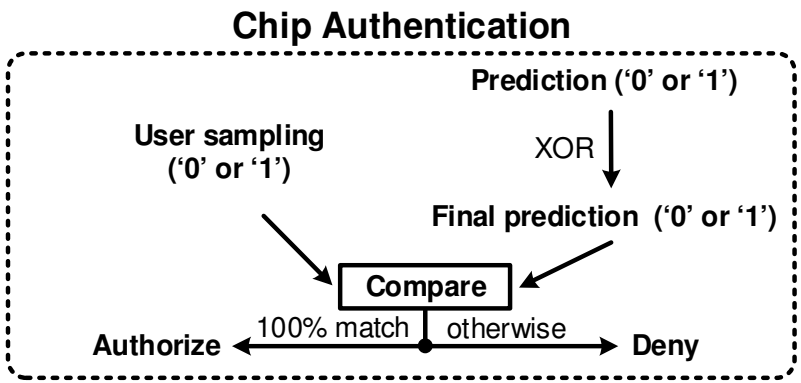




- Counters measure soft responses
- Linear model and thresholds extracted
- Fuses blown out

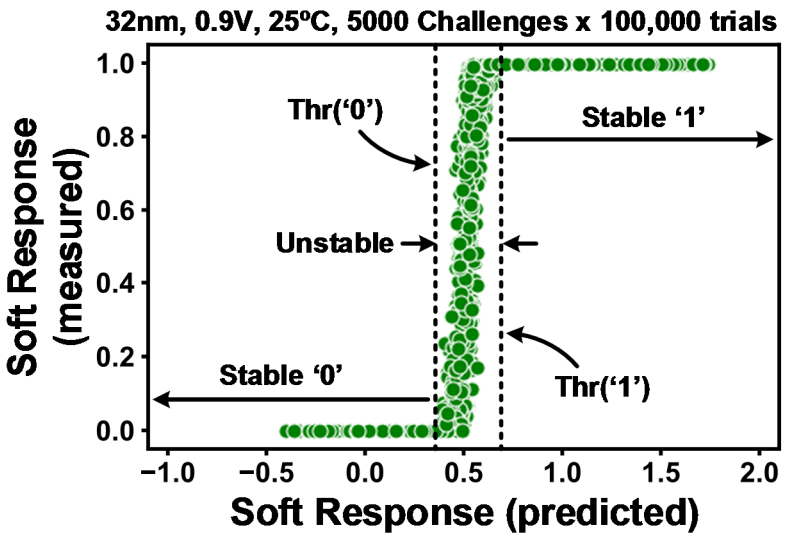
Proposed XOR PUF Authentication

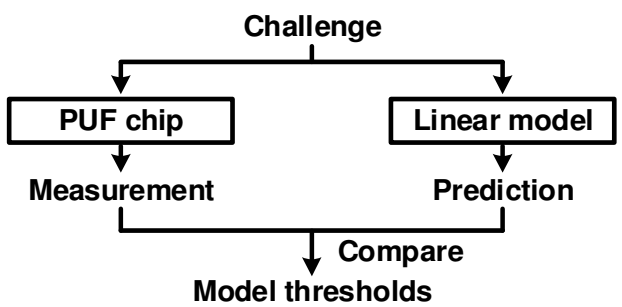


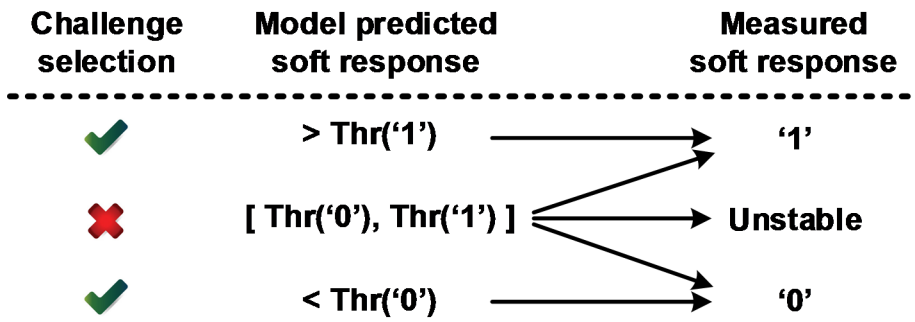


- Challenges selected by models
- 100% match required to authorize access

Model Threshold Determination

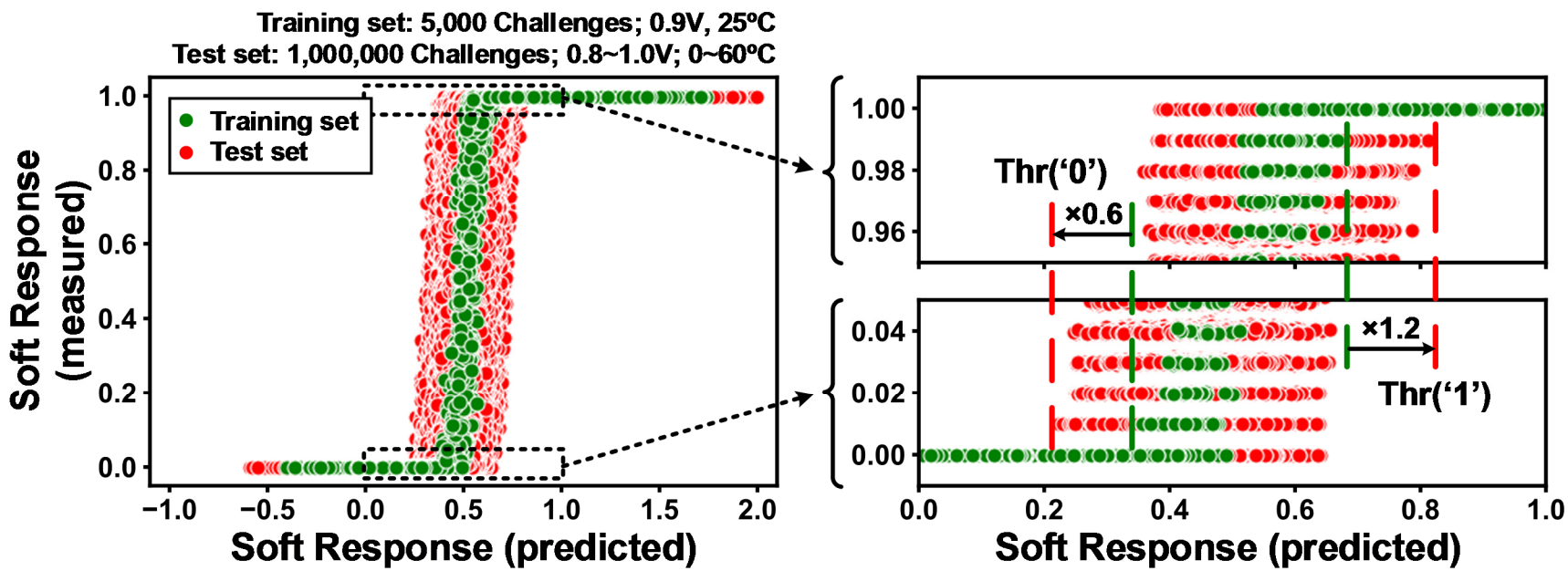






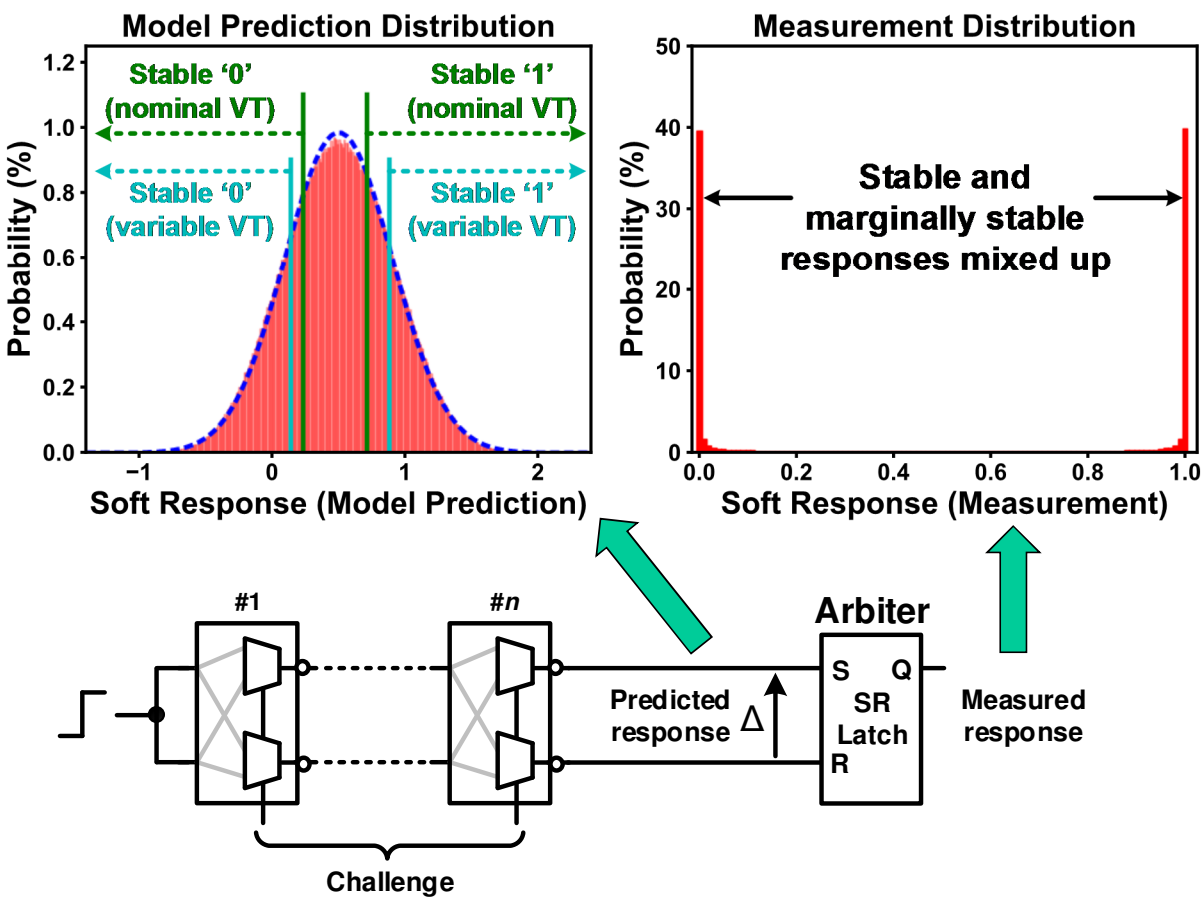
- **Thresholds help find stable CRPs**
- **Measurement vs. model prediction:**
  - **Both responses centered at 0.5**
  - **Strong correlation**
  - **Threshold levels optimized**

Thresholds Adjustment



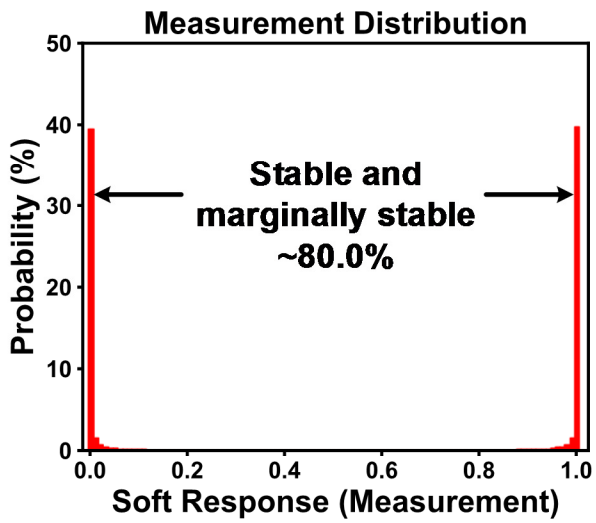
- **Response variation expanded:**
  - Test set CRPs not trained
  - VDD and temperature variation

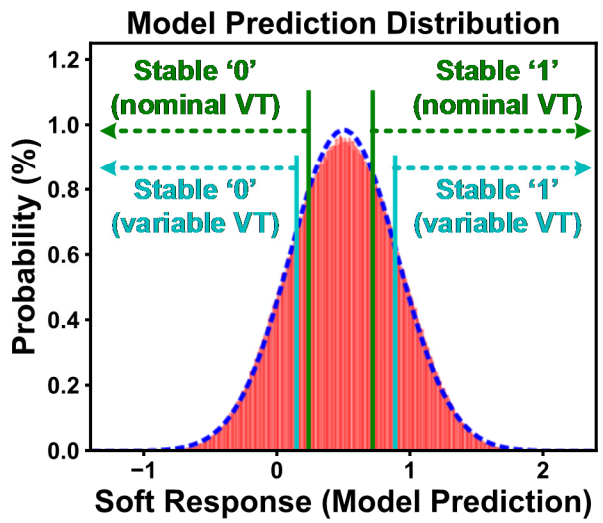
Advantage of Model based CRP Selection

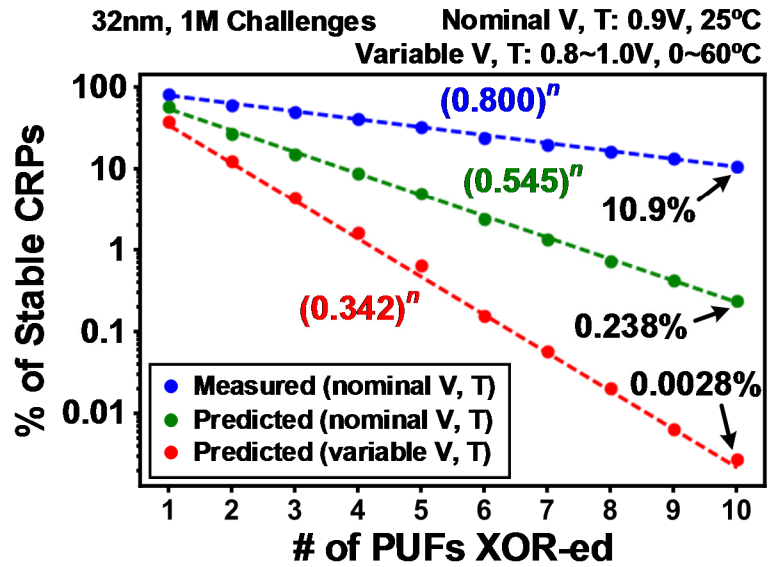


- **Measurement based CRPs selection:**
  - Stable and marginally stable CRPs indistinguishable
  - Large enrollment set size
- **Model based CRPs selection:**
  - Linearly related to delay difference
  - Captures detailed stability information
  - Modest enrollment set size: ~5,000 CRPs

of Stable CRPs







- **Percentage of stable CRPs:**
  - **80.0%: measured under *nominal* VDD and temperature**
  - **54.5%: model predicted under *nominal* VDD and temperature**
  - **34.2%: model predicted under *variable* VDD and temperature**
- **Stable CRPs in *10*-input XOR PUF (0.8V~1.0V, 0~60ºC): 0.0028%**

Summary

- **Security and stability of XOR PUF evaluated using 1 trillion CRP data measured from 32nm test chips**
- **Secure XOR PUF should have *n*>10**
- **A linear regression model helps select stable CRPs**
- **Stringent thresholds used to compensate for V and T variation**

Acknowledgements

- **National Science Foundation and Semiconductor Research Corporation for funding**