Soft Response Generation and Thresholding Strategies for Linear and Feed-Forward MUX PUFs

Chen Zhou, Saroj Satapathy, Yingjie Lao, Keshab K. Parhi and Chris H. Kim

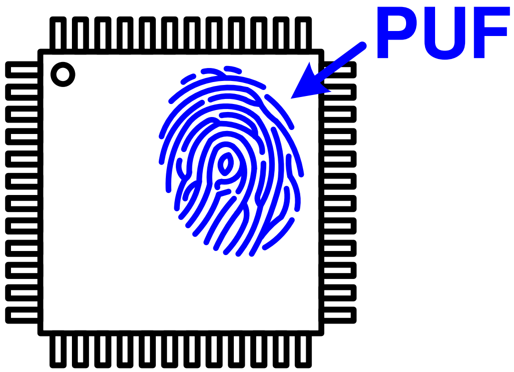
Department of ECE
University of Minnesota

Outline

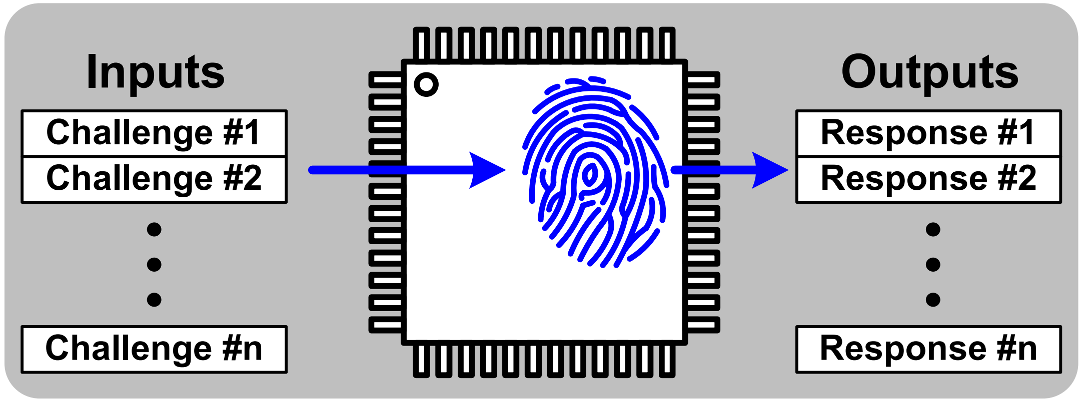
- Physical Unclonable Function (PUF)
- 32nm PUF Chip Measurements
- Soft Response Thresholding Strategies
- Linear PUF vs. Feed-forward PUF
- Conclusion

Physical Unclonable Function (PUF)

Fingerprint of chip

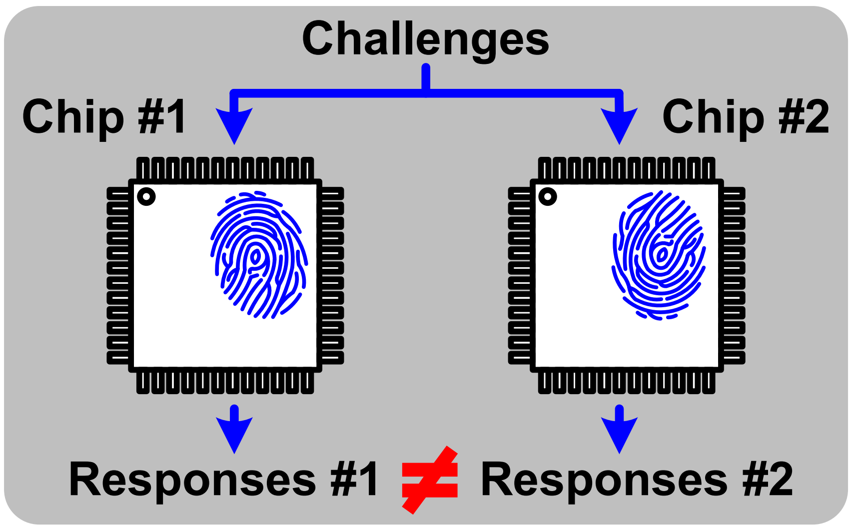


Numerous input choices

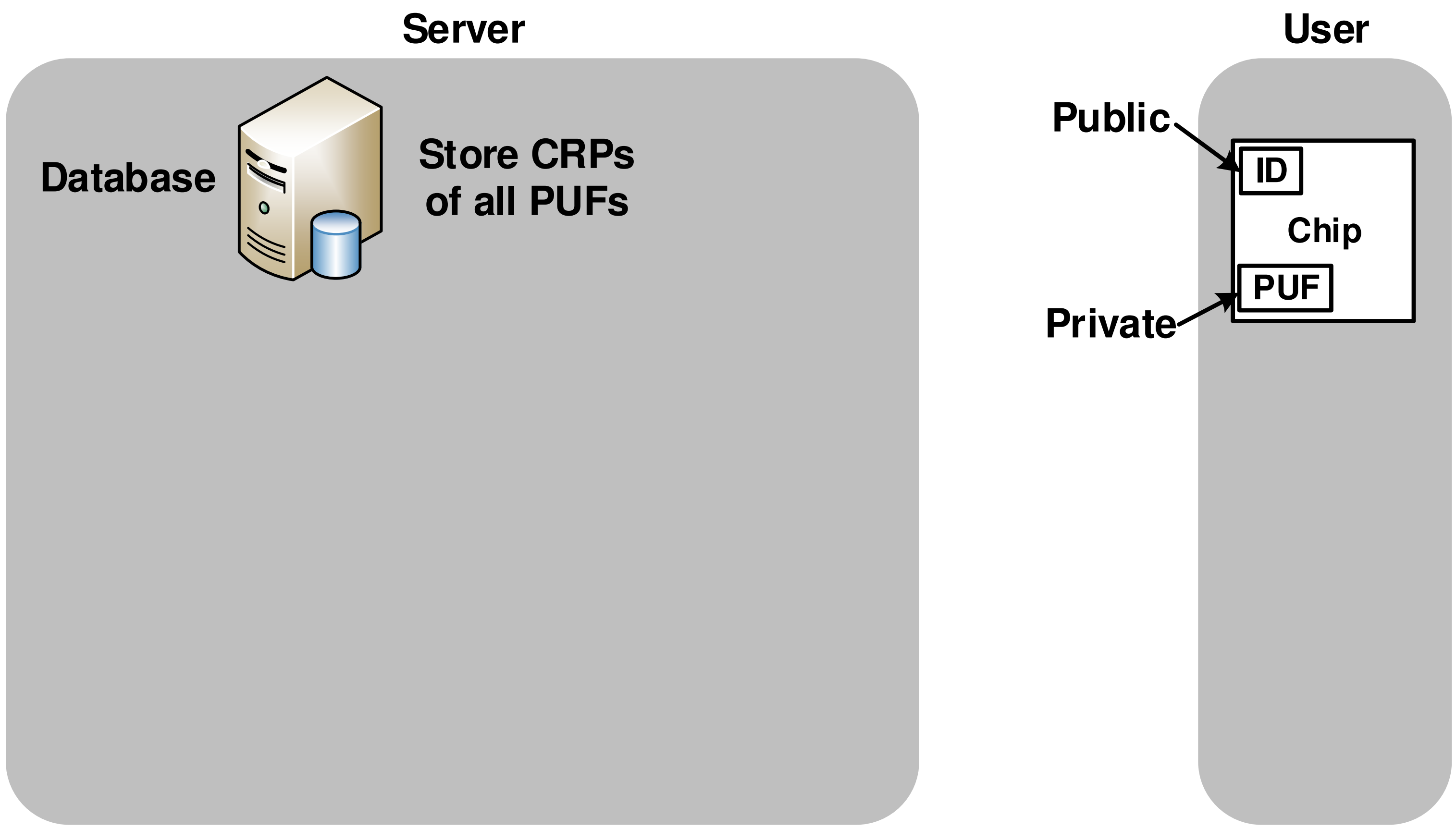


- **Unique and random: Based on inherent process variation**
- **Secure: Large # of challenge-response pairs (CRPs)**

Unique and random responses

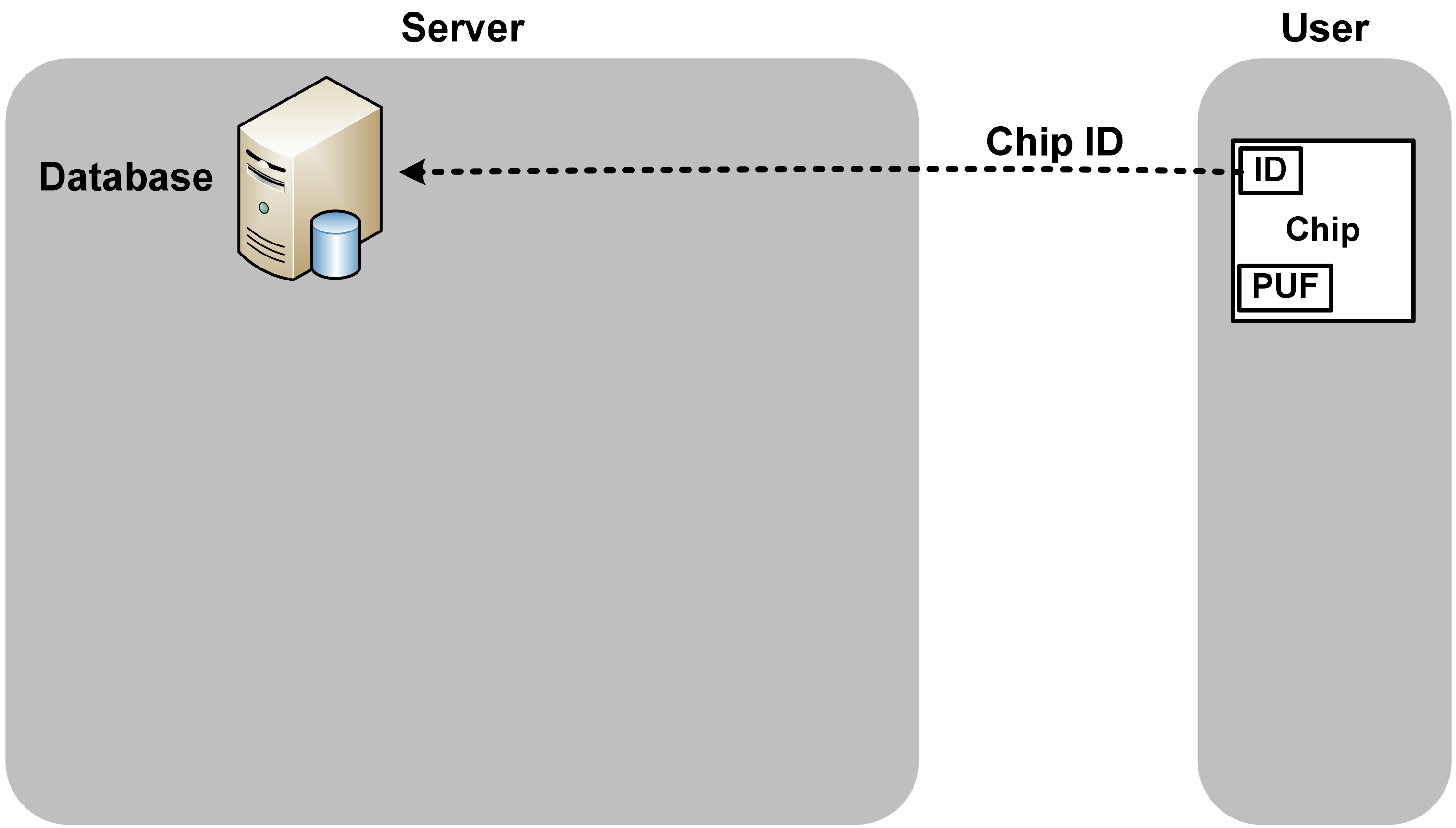


Typical Authentication Process



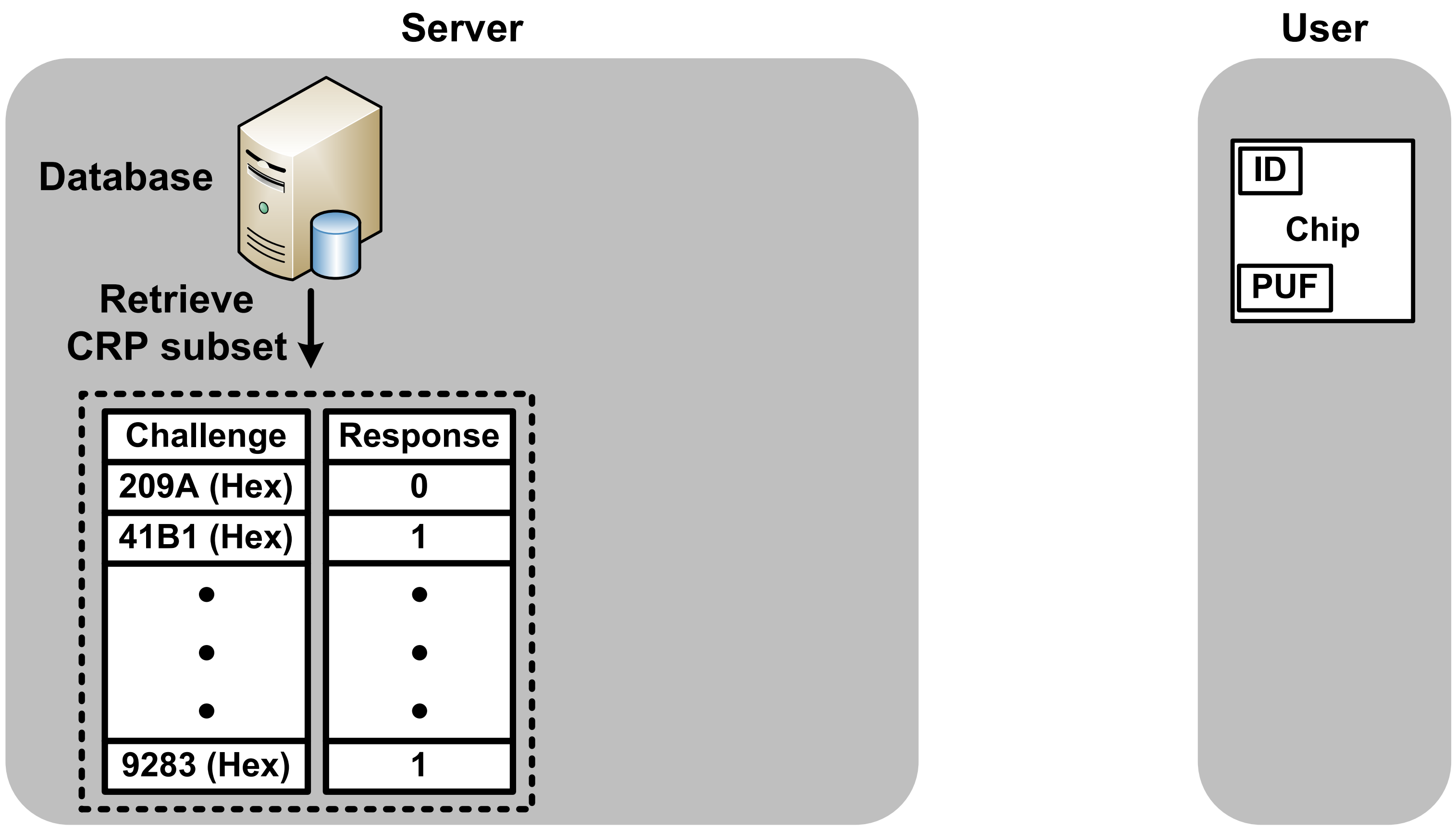
- **Server-user based authentication**
- **Challenge-response pairs tested and stored before usage**

Typical Authentication Process



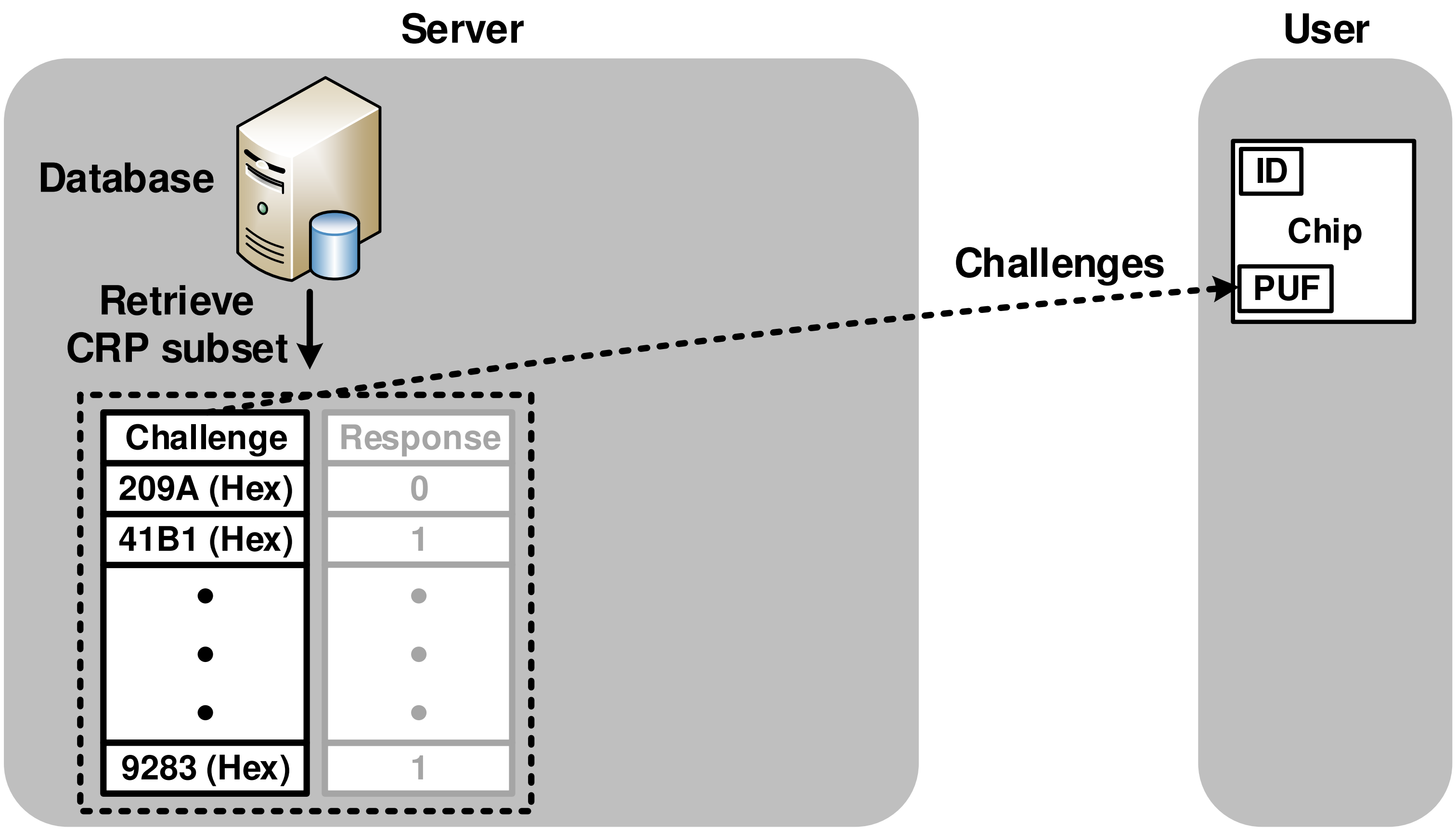
- **Public chip ID is first sent to the server**

Typical Authentication Process



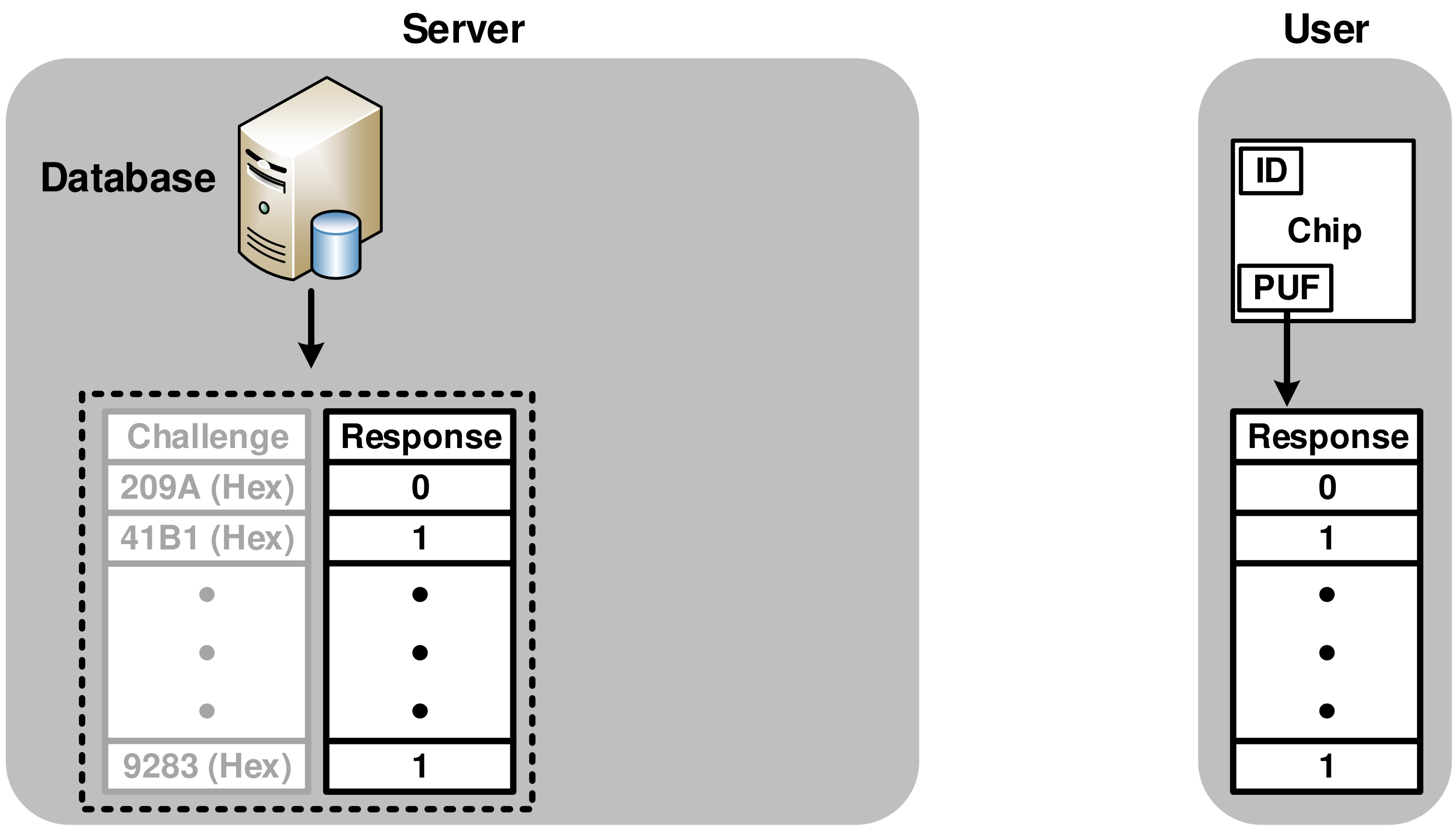
- Server retrieves CRP subset table for the given chip ID

Typical Authentication Process



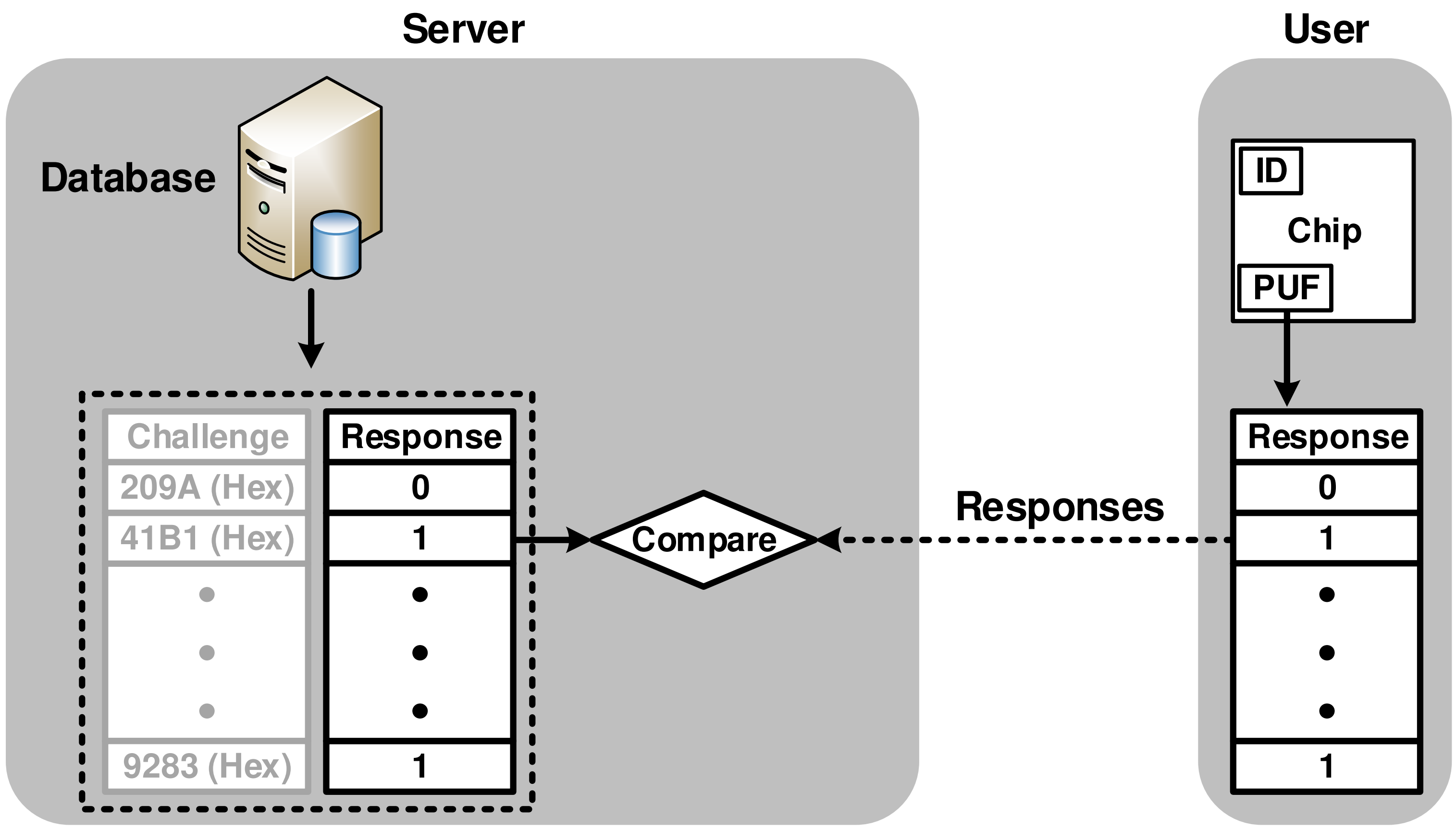
- **Challenges are sent to the user**

Typical Authentication Process



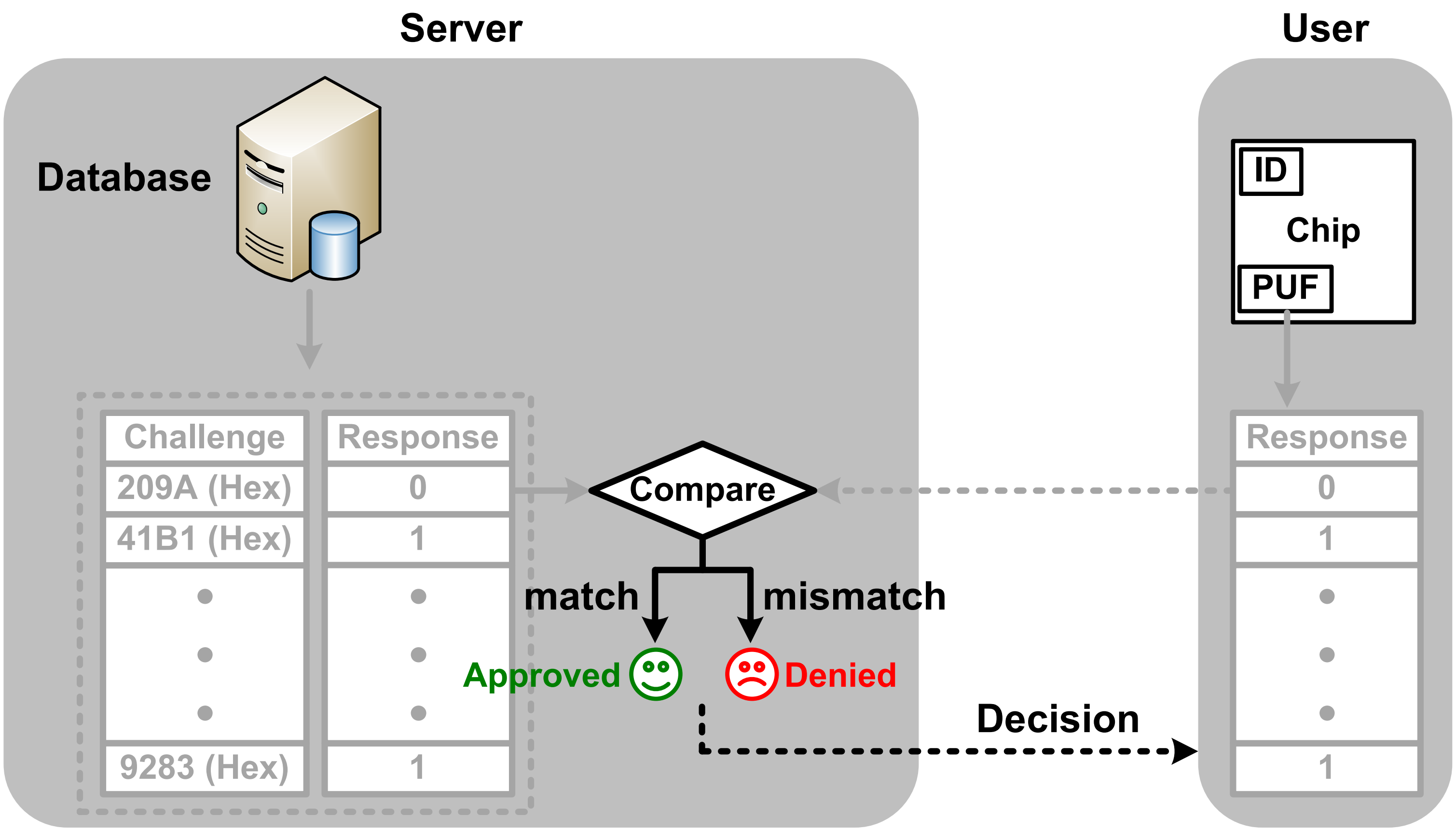
- User generates responses using PUF circuit

Typical Authentication Process



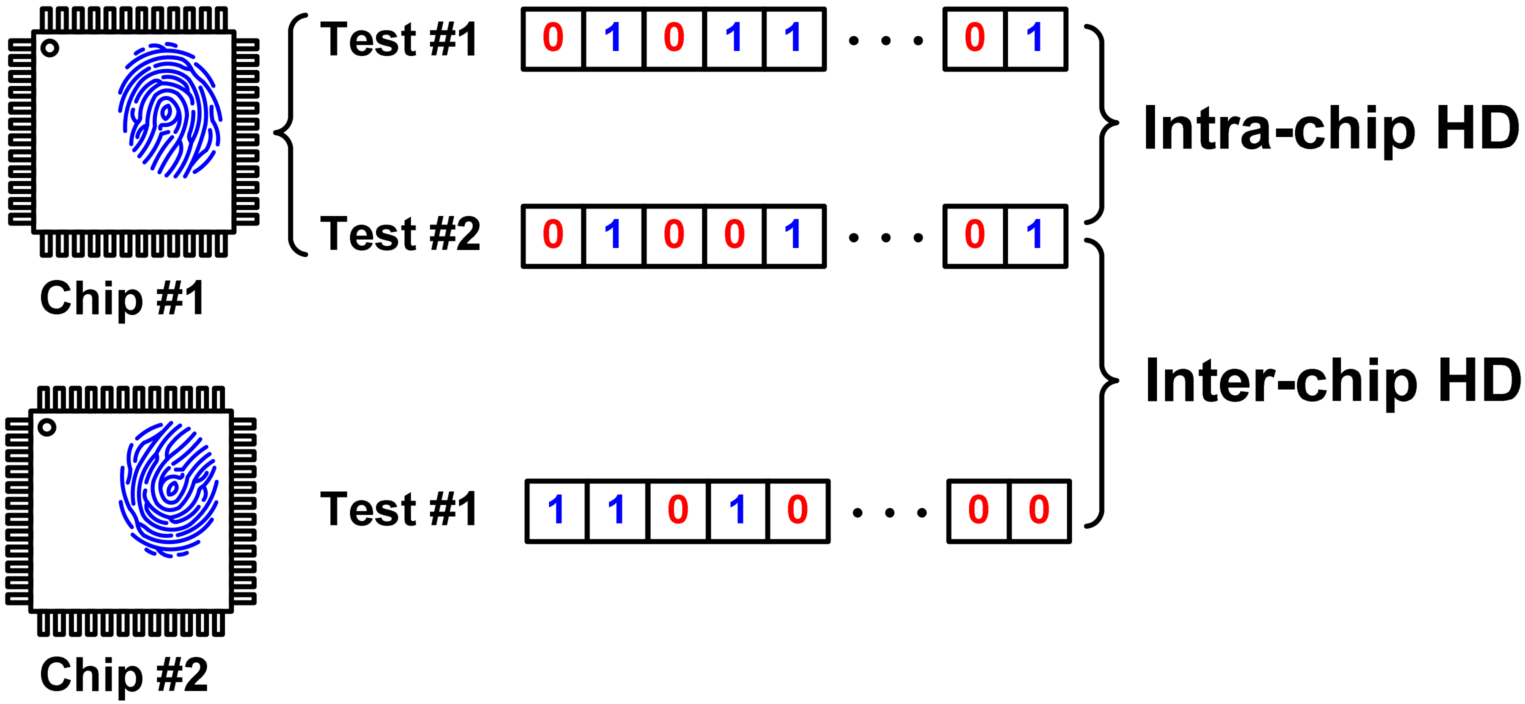
- **User responses are sent to server for comparison**

Typical Authentication Process



- Approved if responses match; denied if mismatch
- Final step: decision sent to user

Hamming Distance (HD) Calculation



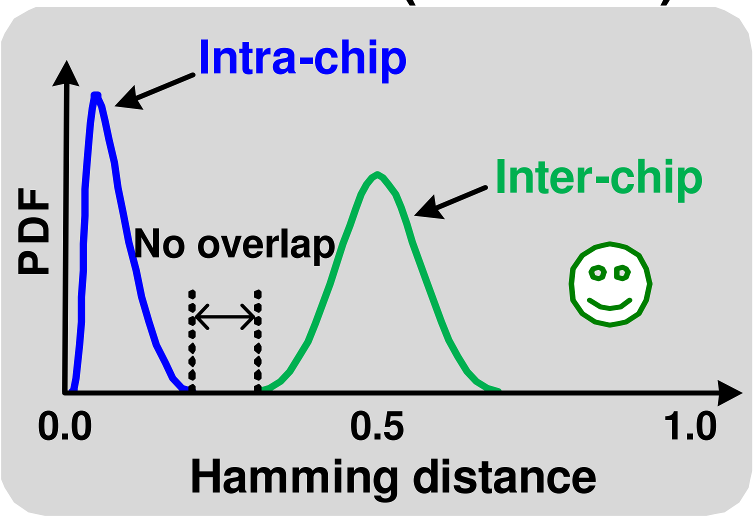
- Hamming distance can be used as matching criteria
- Intra-chip HD: Same chip, noise effects, close to 0%
- Inter-chip HD: Different chip, process variation effects, close to 50%

Outline

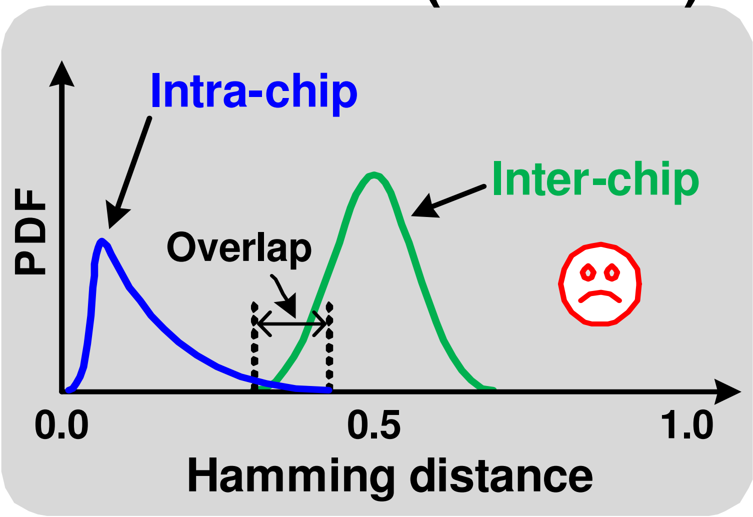
- Physical Unclonable Function (PUF)
- **32nm PUF Chip Measurements**
- Soft Response Thresholding Strategies
- Linear PUF vs. Feed-forward PUF
- Conclusion

Motivation of This Work

Ideal case (all CRPs)

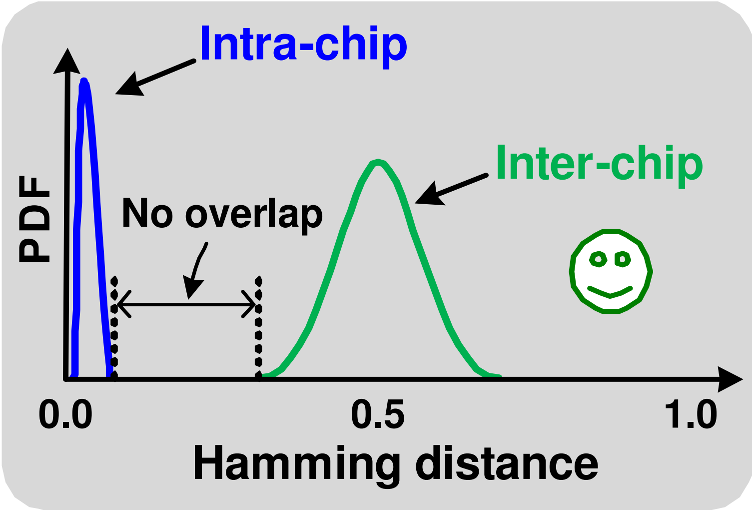


Actual case (all CRPs)



- **Stable CRPs have less intra-chip variation**
- **Measure soft response (=probability of response being ‘1’ or ‘0’) to find stable CRPs**

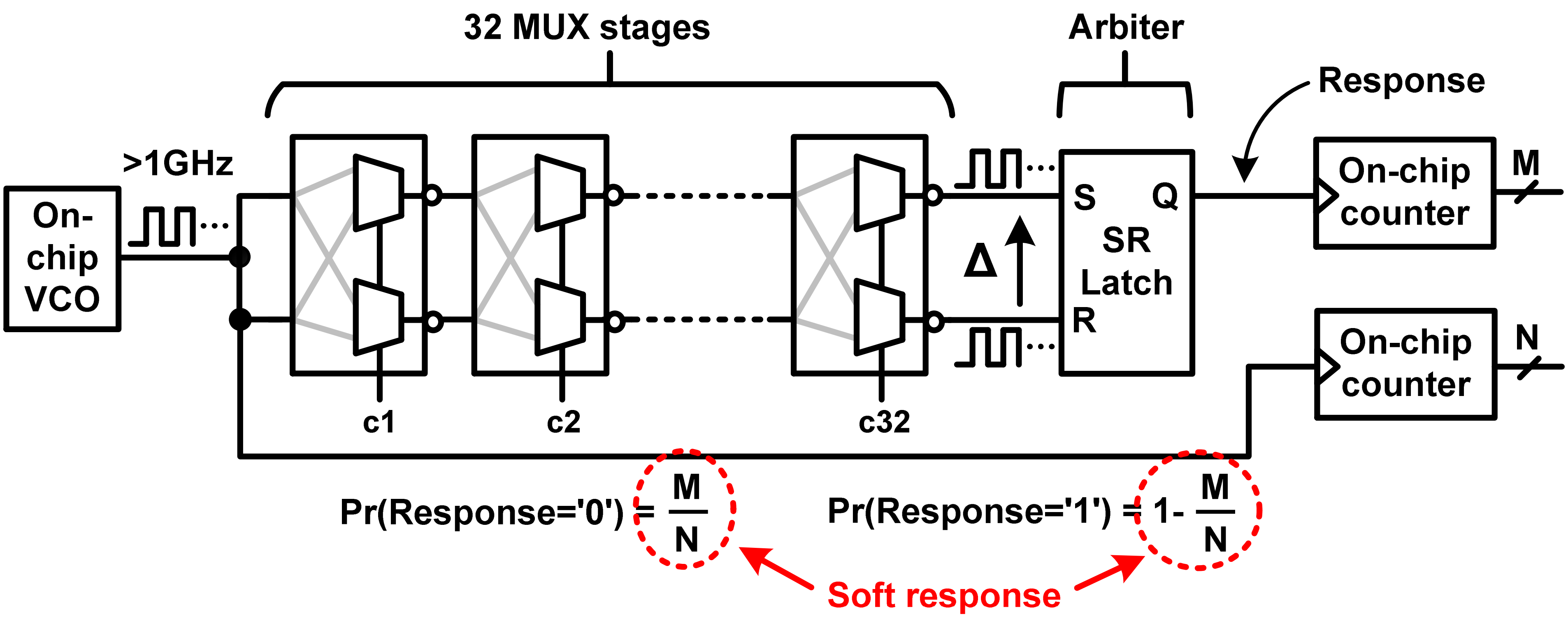
Actual case (only stable CRPs)



Contributions of This Work

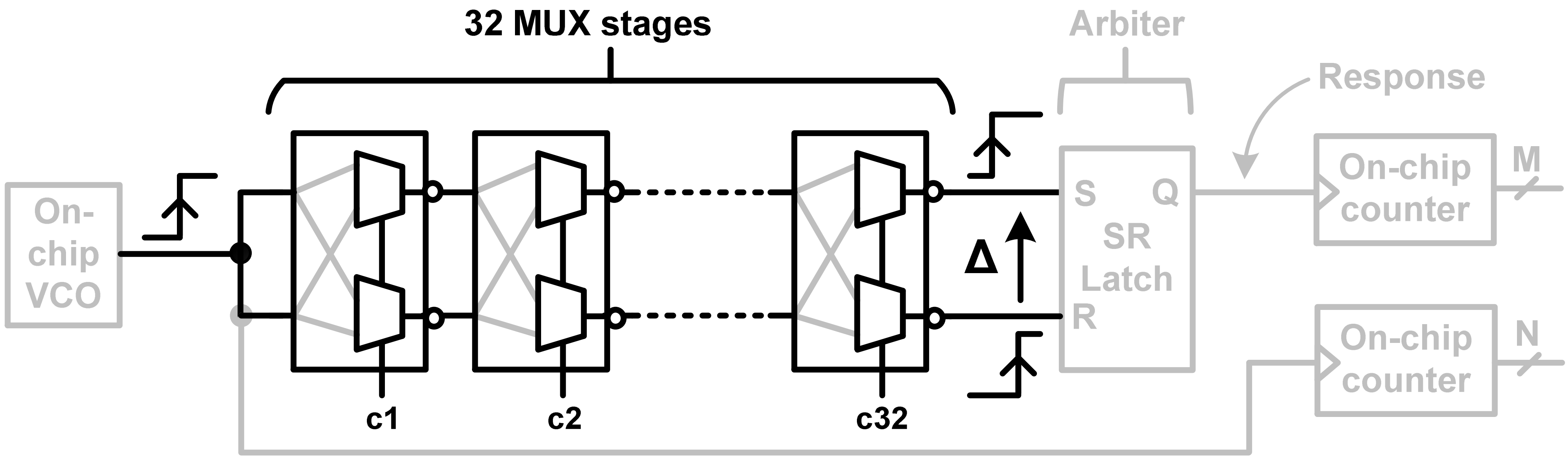
- Implemented soft response collection circuits in a 32nm test chip
- Generated MUX PUF soft response distribution based on 3.3 Gb test data
- Proposed soft response thresholding strategies to select stable challenge-response pairs
- Implemented and characterized feed-forward MUX PUF

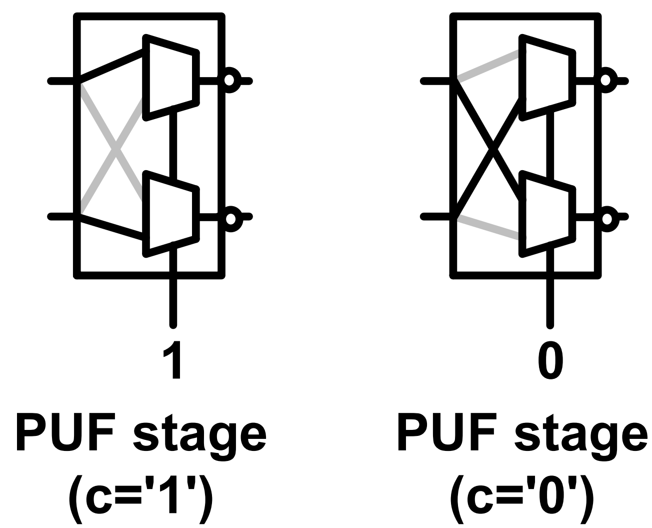
Proposed Soft Response Measurement Circuit



- Soft response = response probability information
- >GHz sampling circuits facilitate efficient soft response measurements

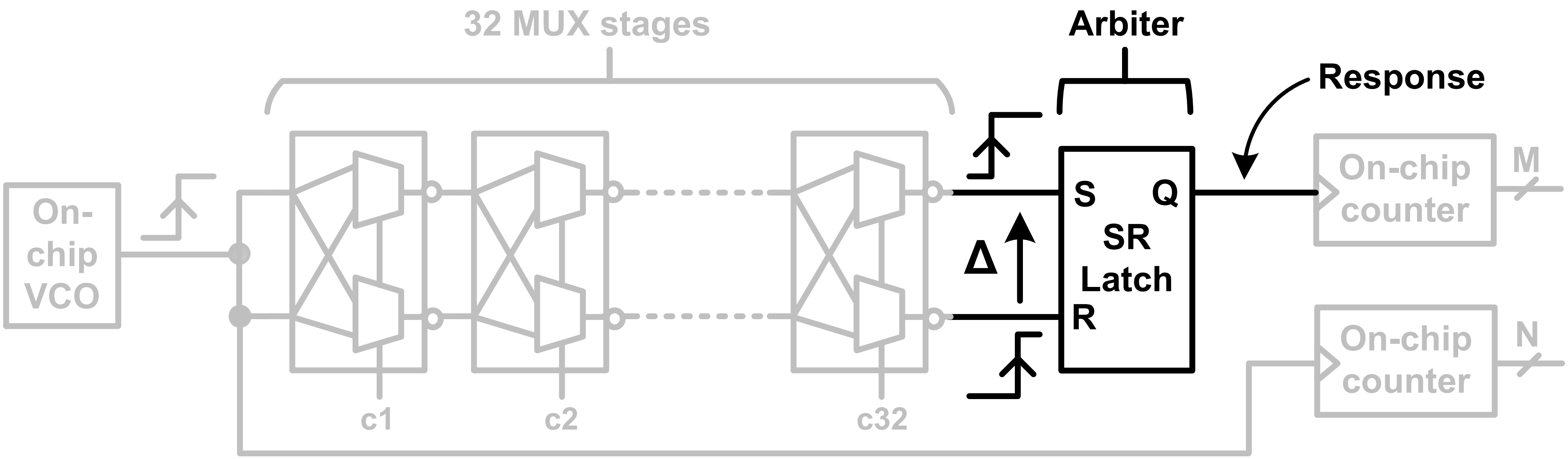
Linear MUX PUF Delay Stages

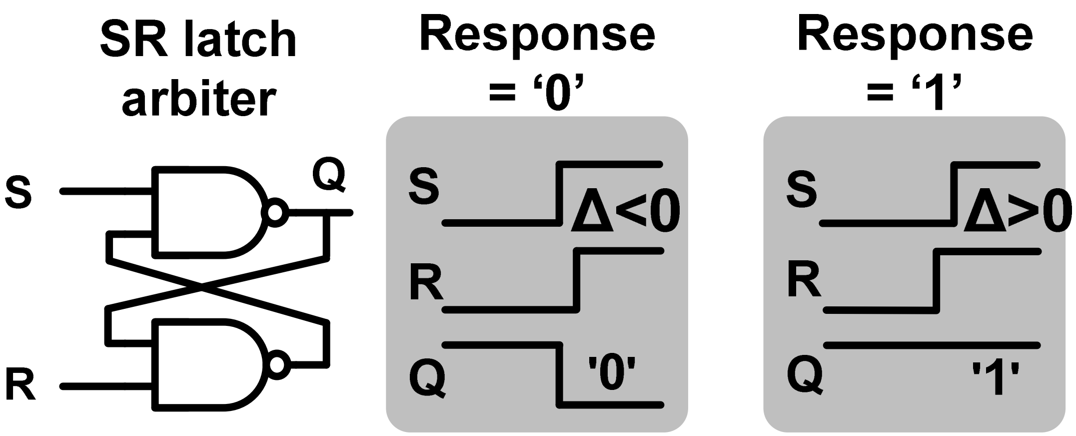




- **Parallel or crossed signal paths configured by challenge bits**
- **Delay difference determined by inherent process variation**

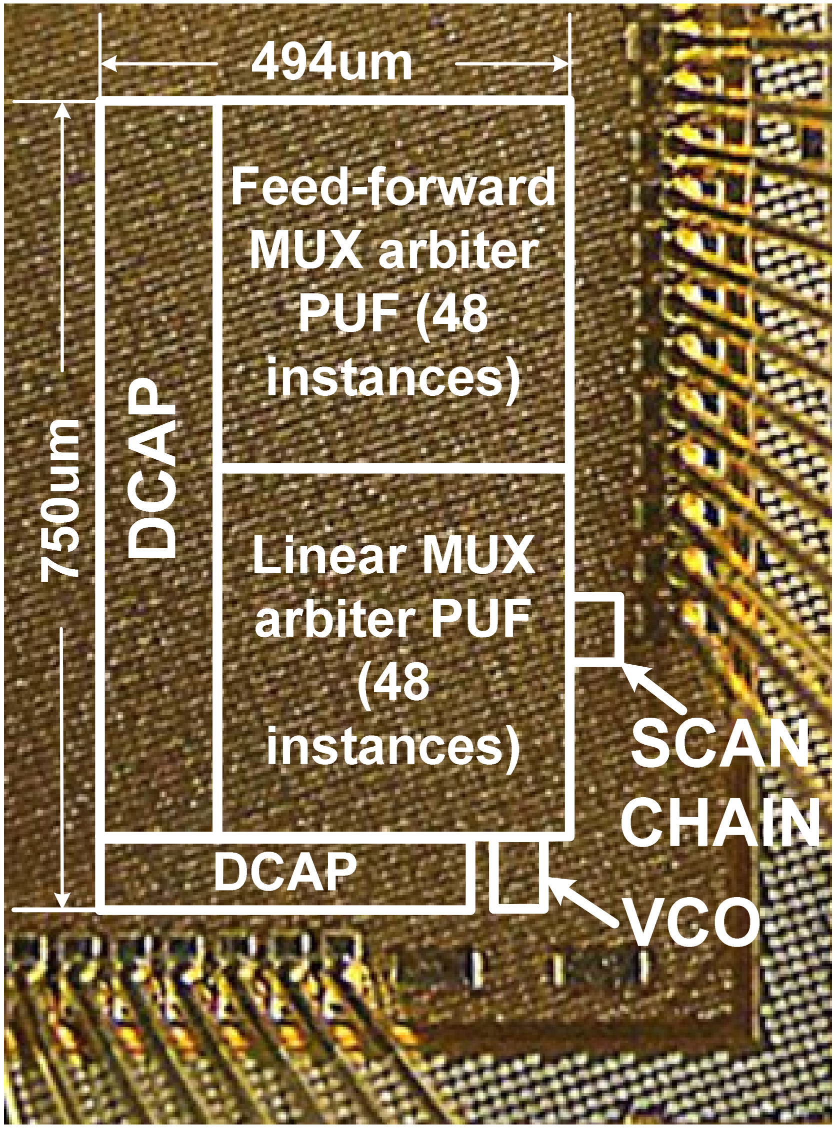
Arbiter Circuit





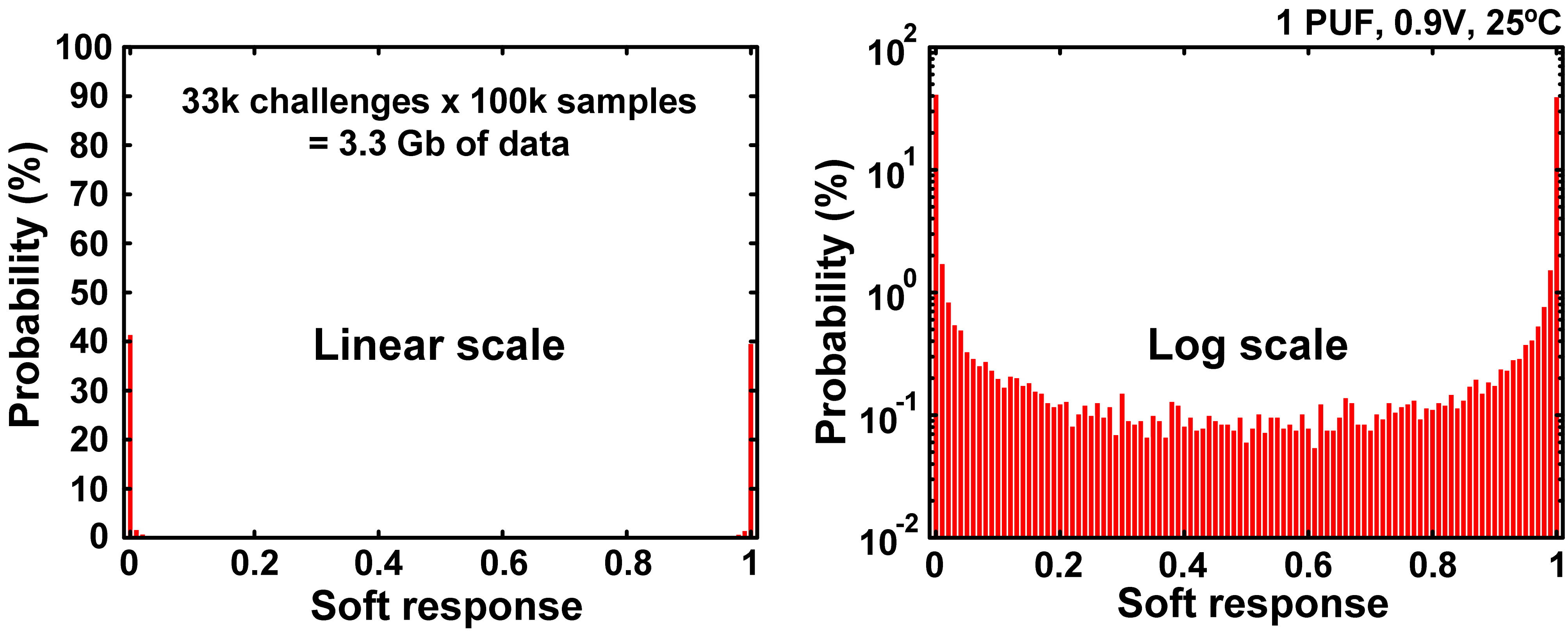
- **Arbiter generates response bit based on delay difference**

32nm PUF Test Chip



Process	32nm
VDD	0.8V, 0.9V, 1.0V (nominal: 0.9V)
Temperature	25ºC, 85ºC
Circuit area	0.37 mm^2
PUF type	Linear and Feed-forward MUX arbiter PUF
PUF stages	32
# of PUFs	48 (linear) + 48 (feed-forward)
VCO frequency	<1.4 GHz
Arbiter	SR latch

Soft Response Measurements

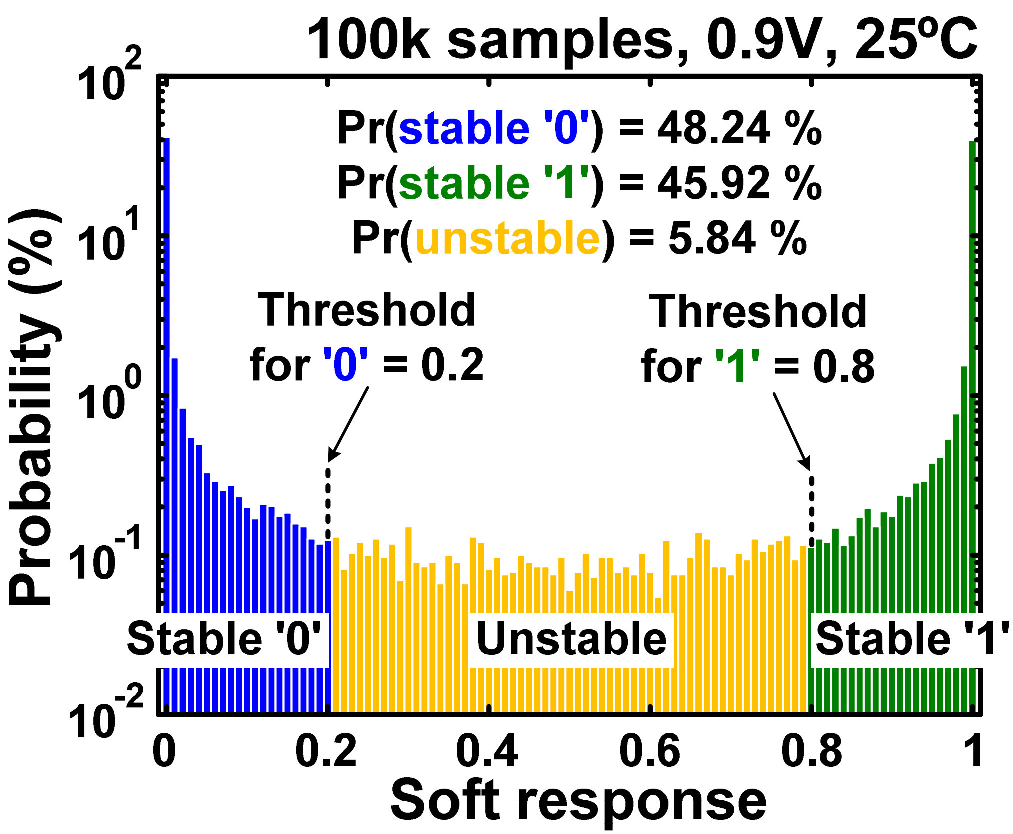


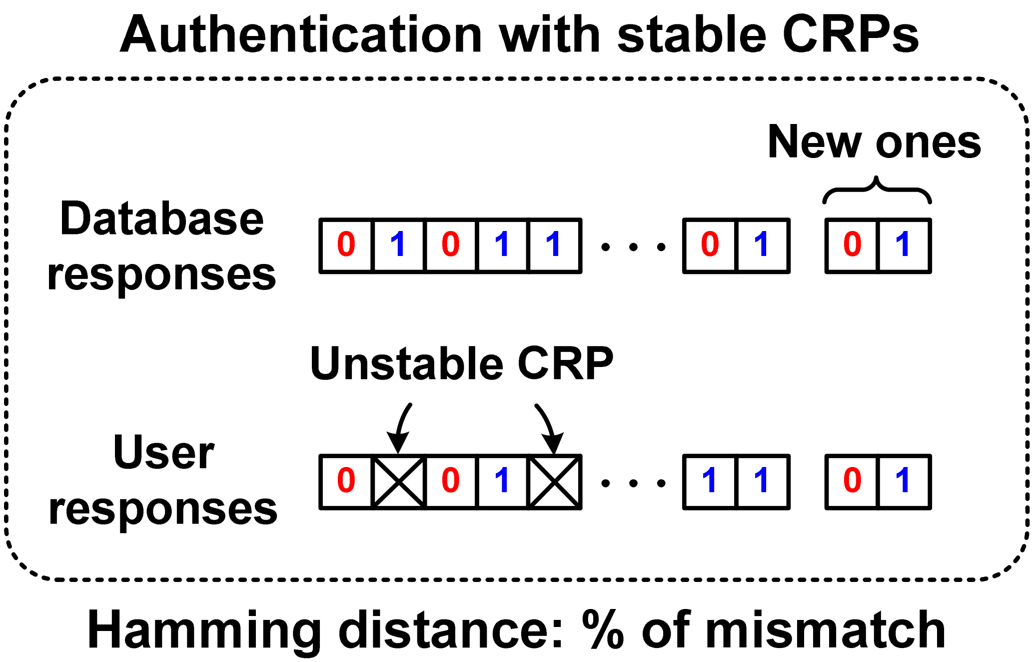
- **Soft response is a function of the actual delay difference**
- **Above distribution generated using 3.3 Gb of PUF response data**

Outline

- Physical Unclonable Function (PUF)
- 32nm PUF Chip Measurements
- **Soft Response Thresholding Strategies**
- Linear PUF vs. Feed-forward PUF
- Conclusion

Soft Response Thresholding Strategy

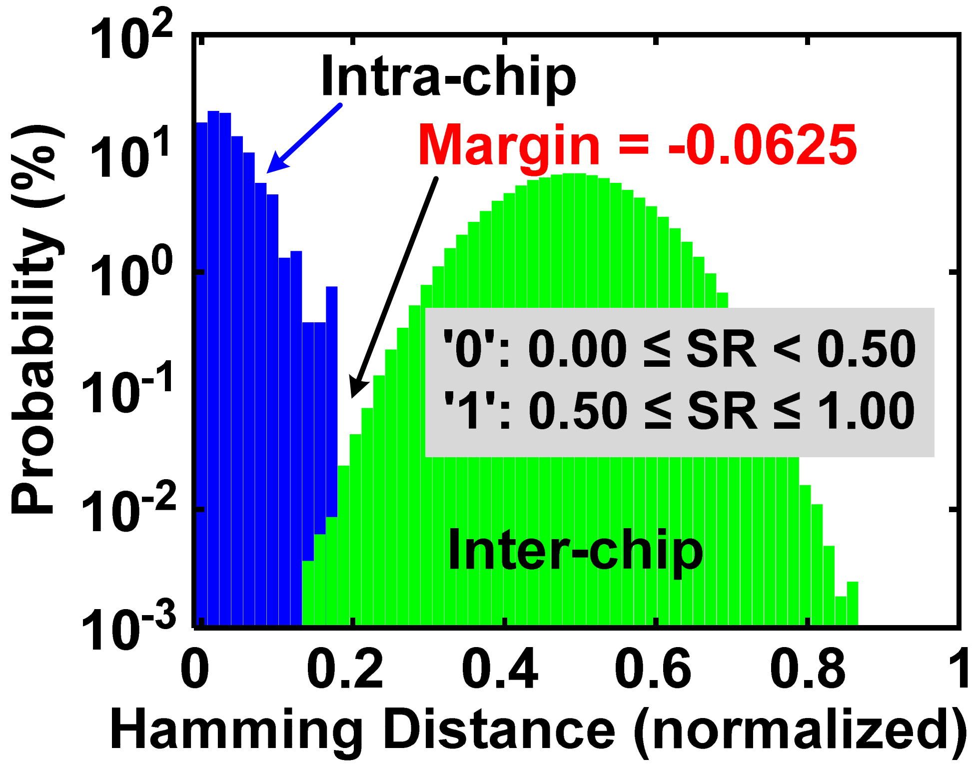


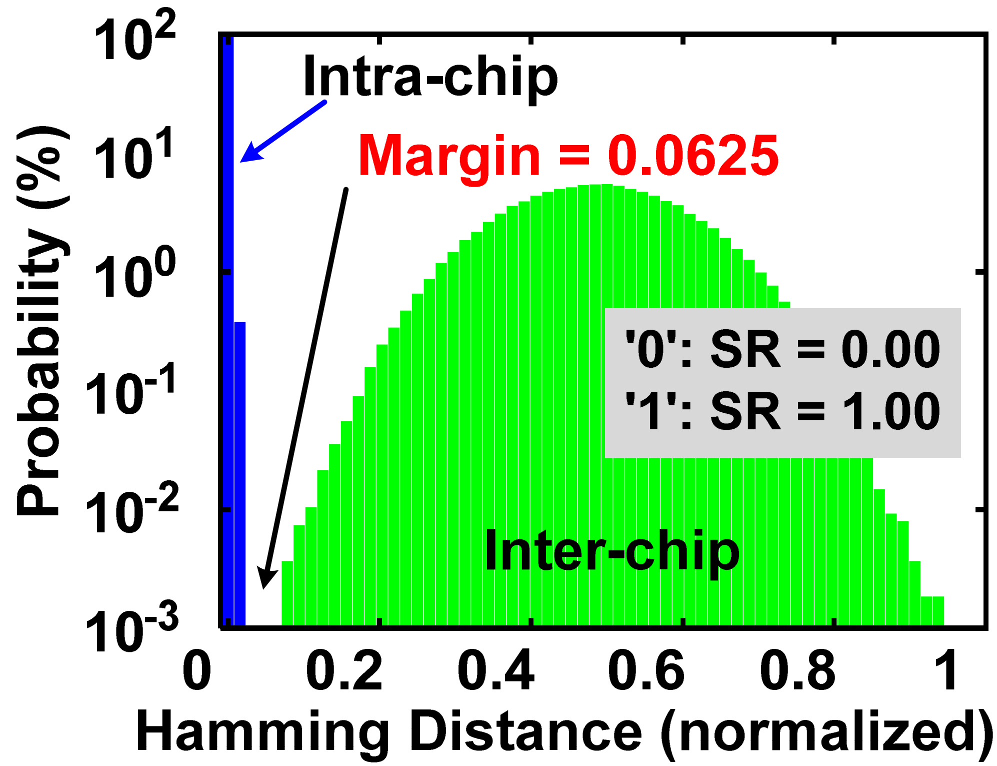


- Symmetric thresholds used to define stable and unstable CRPs
- Unstable CRPs not used for authentication

Impact of Soft Response (SR) Threshold

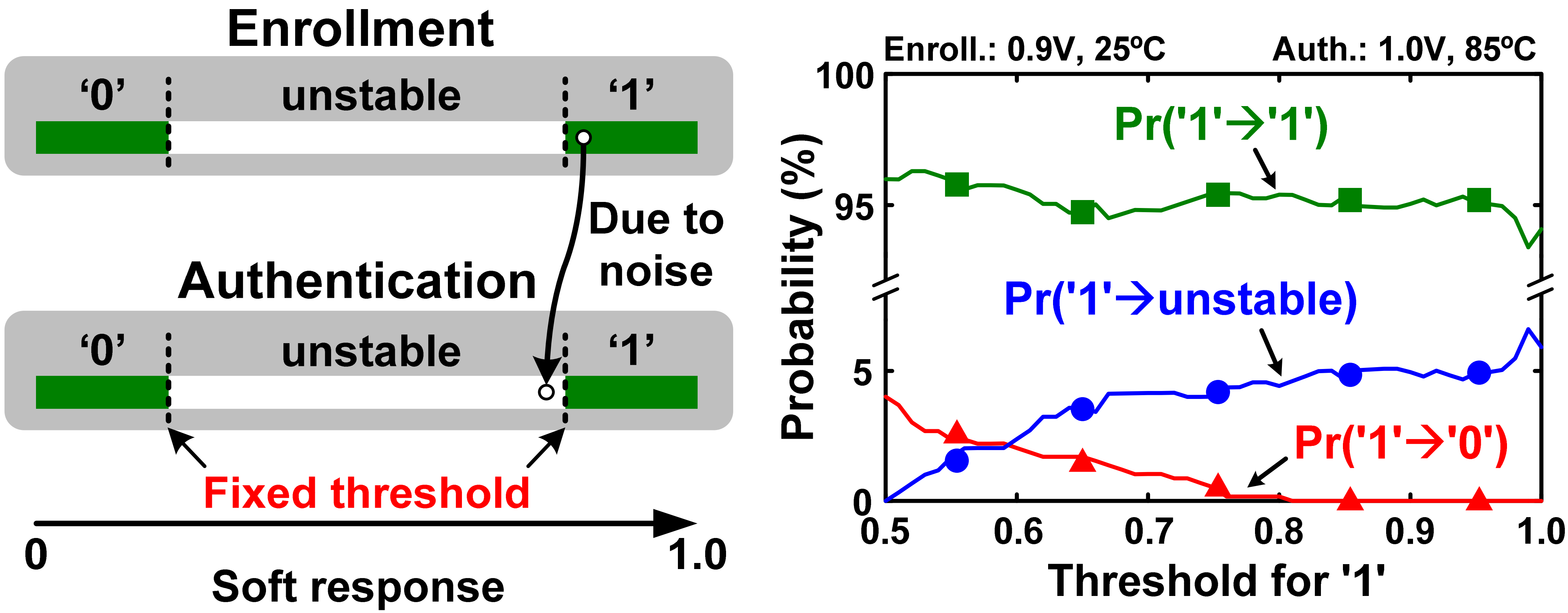
VDD: 0.8, 0.9, 1.0V   Temperature: 25, 85ºC   64 stable CRPs   32nm data





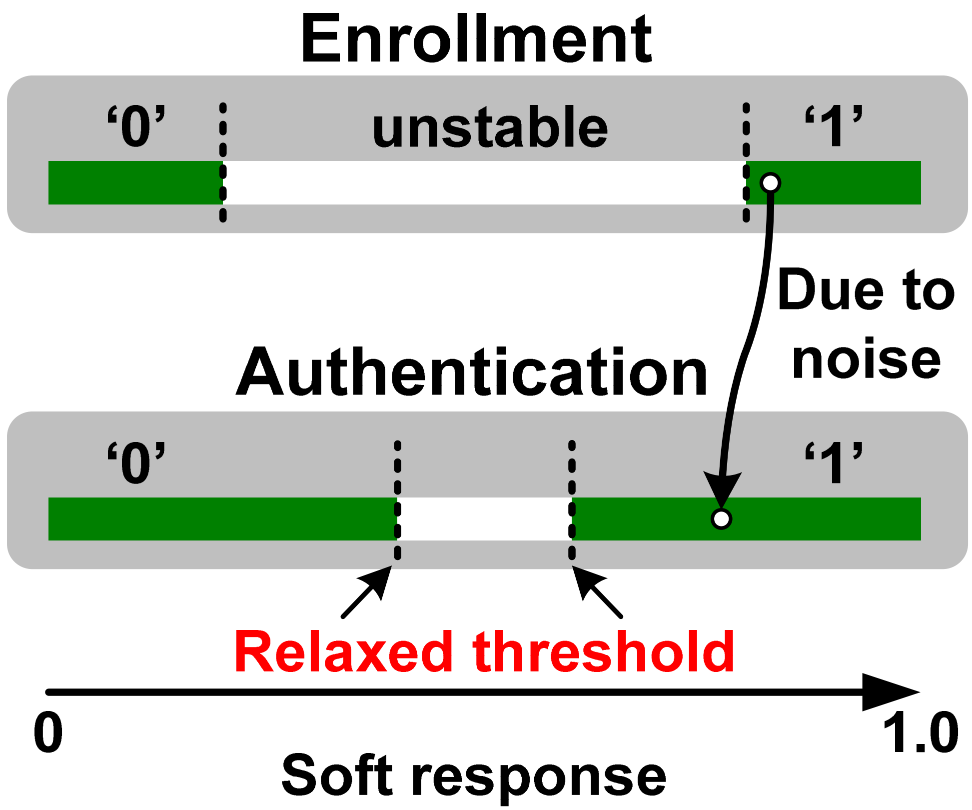
- Left: HD distributions overlap when threshold=0.5
- Right: No overlap when threshold=0 and 1 (i.e. only stable responses are used)

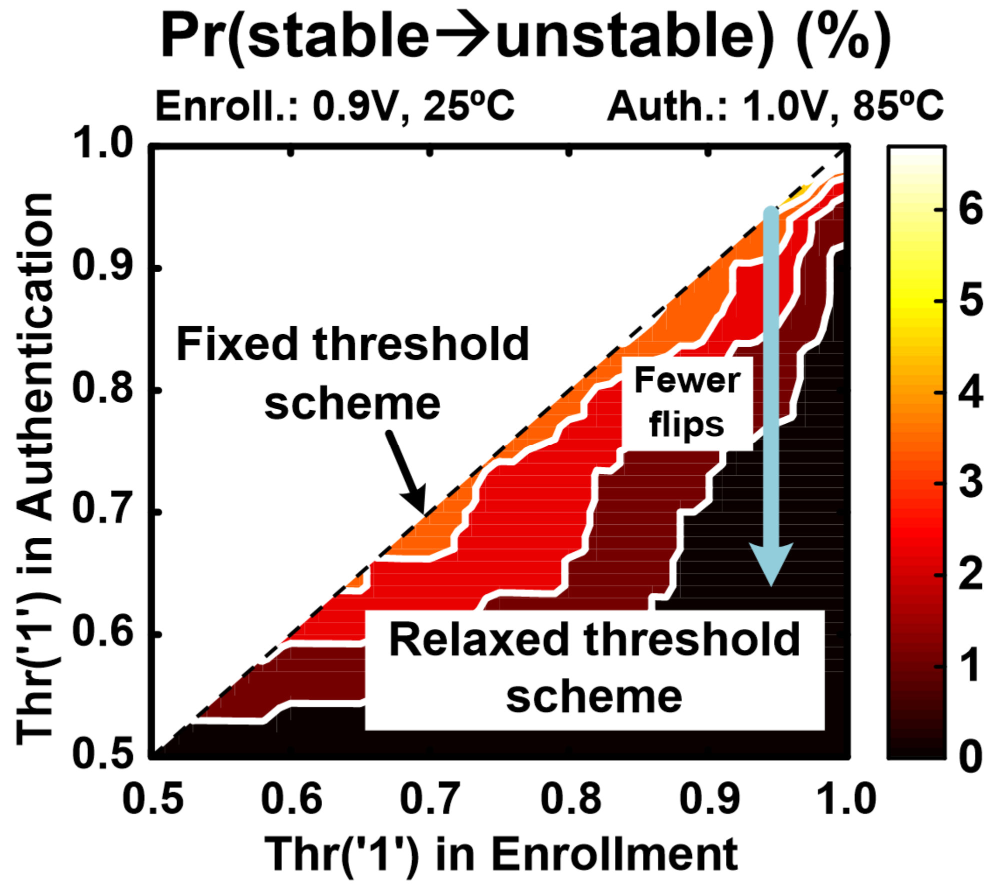
Fixed Threshold Scheme



- No stable '1' to stable '0' flips when threshold > 0.81
- Stable '1' to 'unstable' flips always exist, necessitating more tests to find stable CRPs

Relaxed Threshold Scheme



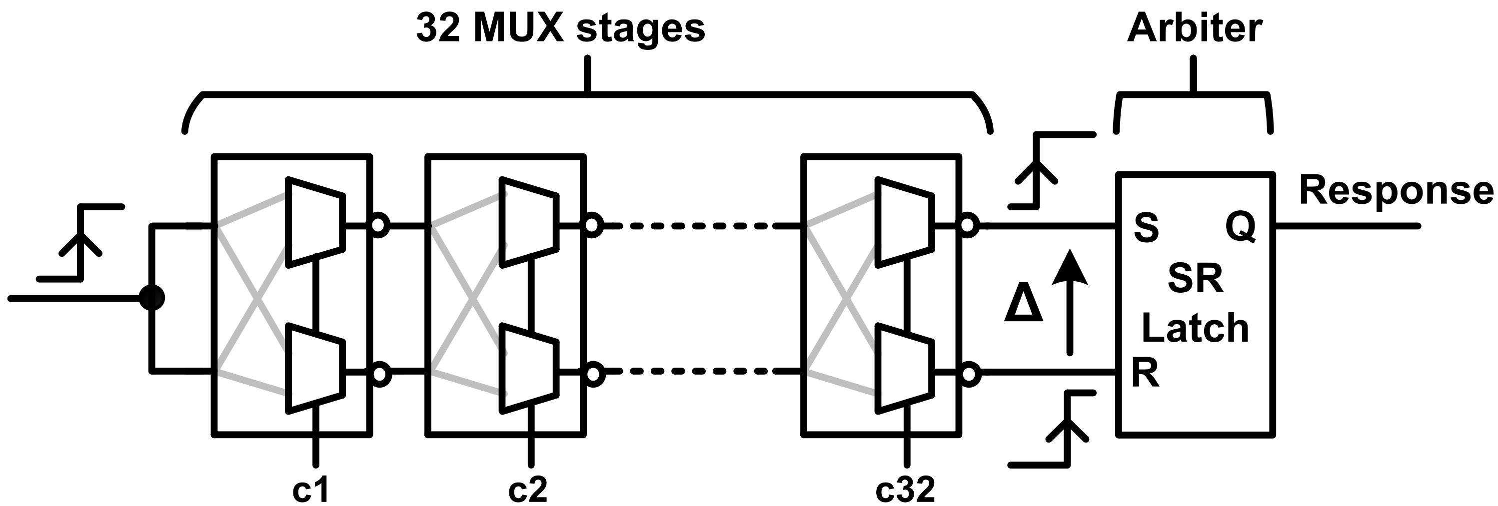


- Stringent threshold during enrollment phase and relaxed threshold during authentication
- Results in fewer '1'→'unstable' and '0'→'unstable' flips

Outline

- Physical Unclonable Function (PUF)
- 32nm PUF Chip Measurements
- Soft Response Thresholding Strategies
- **Linear PUF vs. Feed-forward PUF**
- Conclusion

Linear MUX PUF Vulnerability

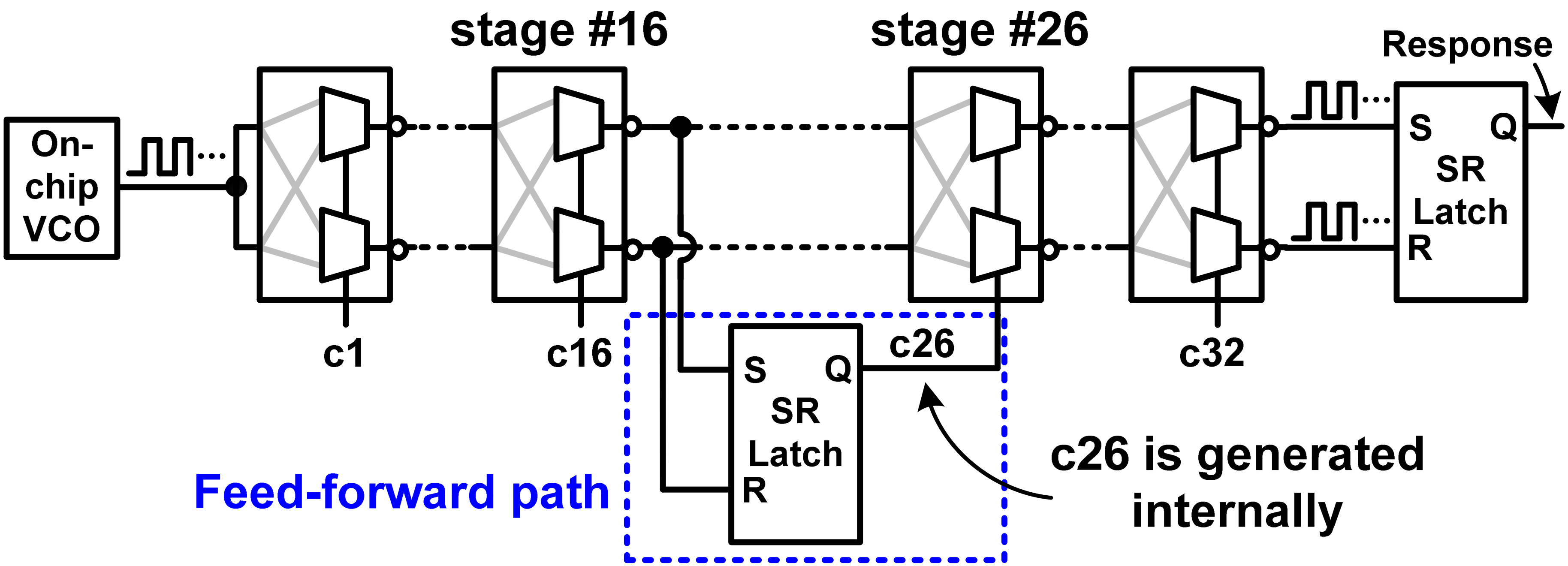


$$C = \begin{bmatrix} (2c_1 - 1)(2c_2 - 1)\cdots(2c_{32} - 1) \\ (2c_2 - 1)\cdots(2c_{32} - 1) \\ \vdots \\ (2c_{32} - 1) \\ 1 \end{bmatrix}^T \qquad W = \frac{1}{2}\begin{bmatrix} \delta_1^0 - \delta_1^1 \\ \delta_1^0 + \delta_1^1 + \delta_2^0 - \delta_2^1 \\ \vdots \\ \delta_{31}^0 + \delta_{31}^1 + \delta_{32}^0 - \delta_{32}^1 \\ \delta_{32}^0 + \delta_{32}^1 + b \end{bmatrix}$$

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

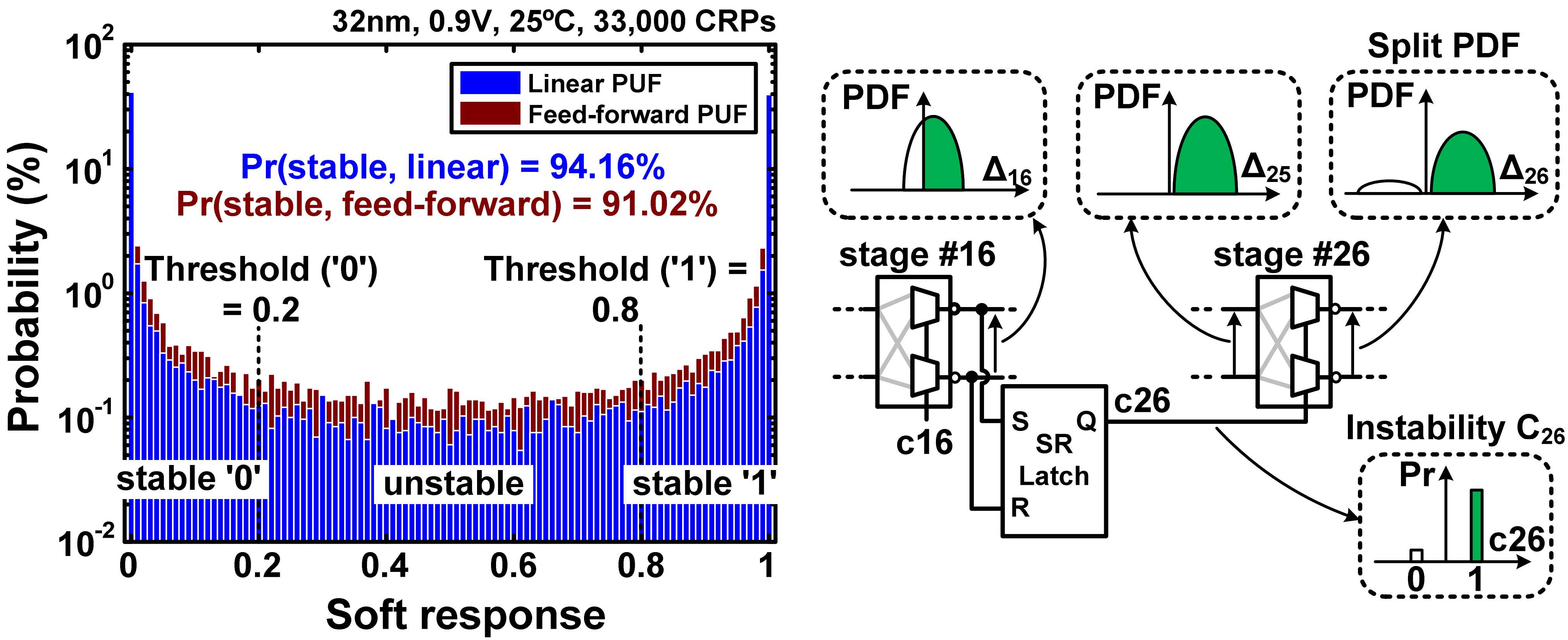
- **Linear PUFs are susceptible to modelling attack**
- **That is, attacker can predict correct response with very high probability using past CRP data**

Feed-forward MUX PUF for Improved Security



- Use intermediate response for some challenge bits
- Non-linear relationship between delay and response
  → harder for attacker to predict correct response
- No experimental data reported on feed-forward PUF

32nm Test Chip Data: Linear vs. Feed-forward MUX PUF



- % of stable CRPs decreases from 94.16% to 91.02% due to instability of internal challenge bit

Conclusion

- Soft response measurement circuit demonstrated in a 32nm test chip
  - On-chip VCO and counters enable fast measurement
- Different thresholding strategies evaluated
  - Enables robust authentication across wider voltage and temperature range
- Feed-forward MUX measured for the first time
  - % of stable CRPs decreases slightly due to instability of internal challenge bit

Acknowledgements

- National Science Foundation and Semiconductor Research Corporation for funding