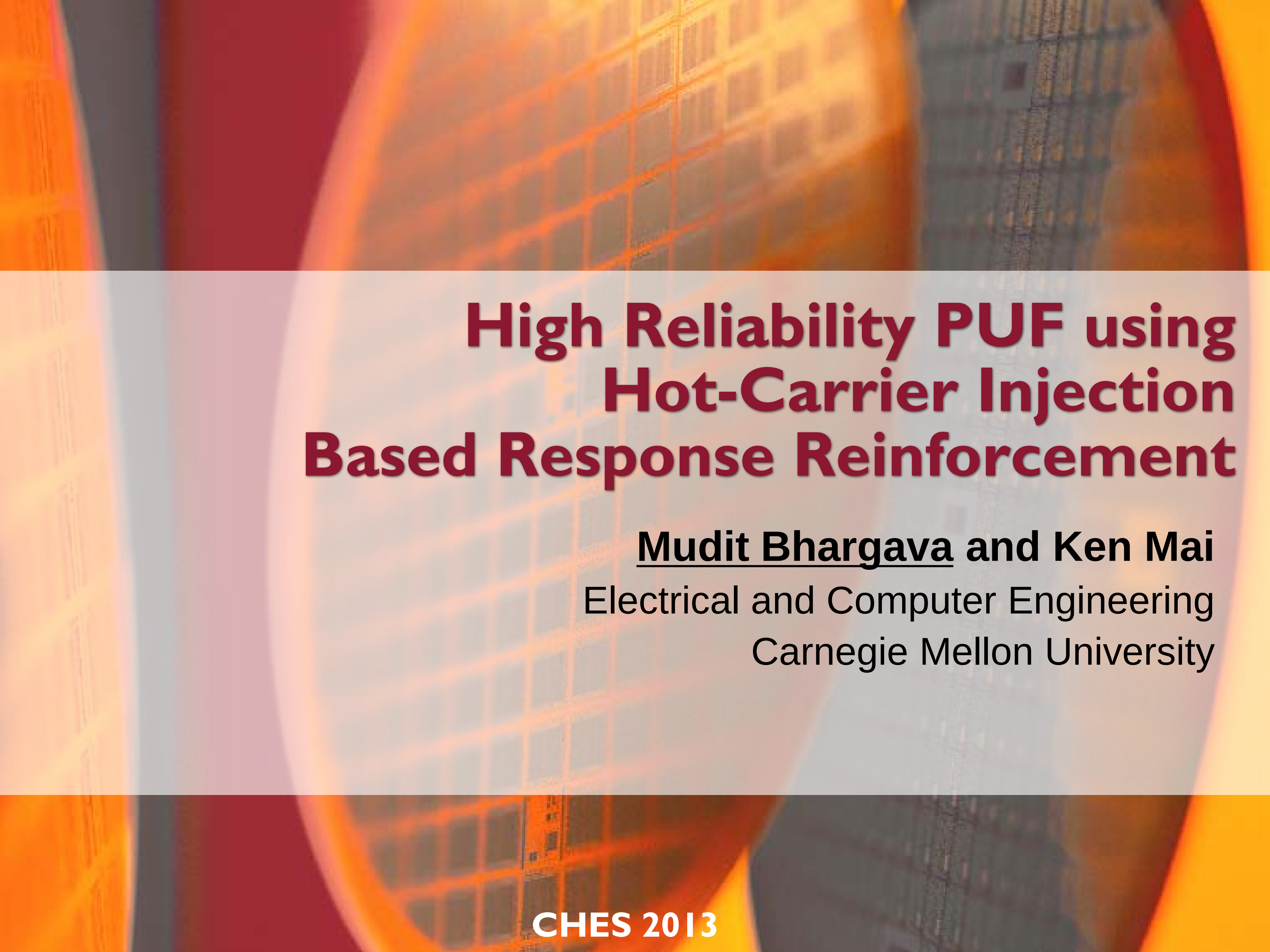


High Reliability PUF using Hot-Carrier Injection Based Response Reinforcement

Mudit Bhargava and Ken Mai

Electrical and Computer Engineering
Carnegie Mellon University

CHES 2013

Key Generation using PUFs

‘Generate’ the key instead of ‘store’ the key

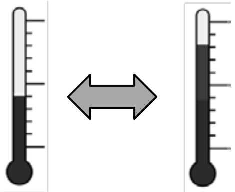
- Storage is vulnerable

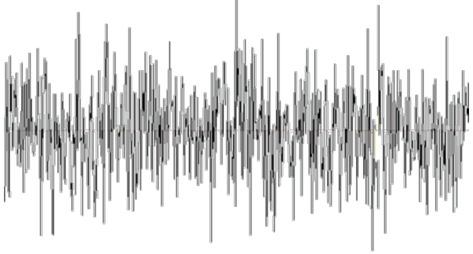
PUF response

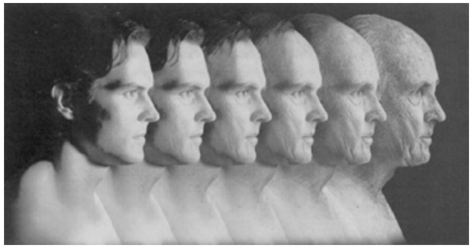
- Derived from amplification of random process variations
- Unreliability due to environmental conditions, noise, and aging

Required PUF characteristics

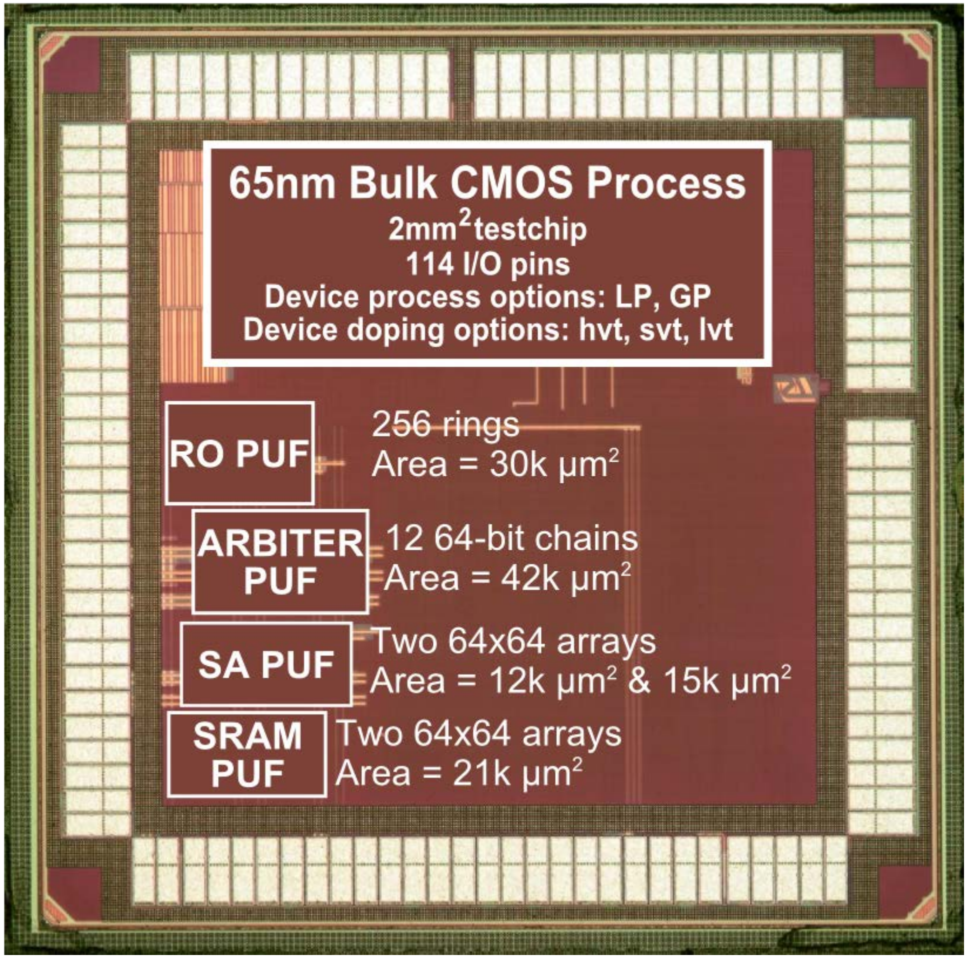
- Random
- Unique
- Reliable ← hardest to achieve





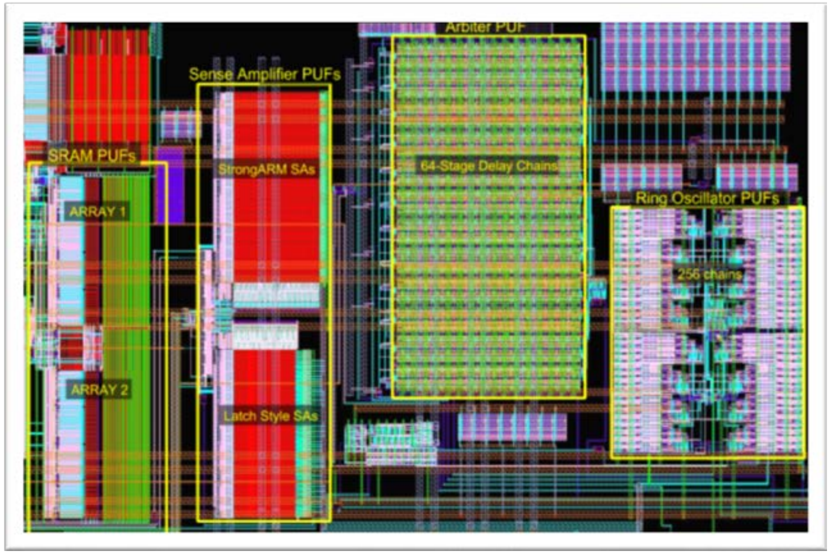


PUF Comparison Testchip



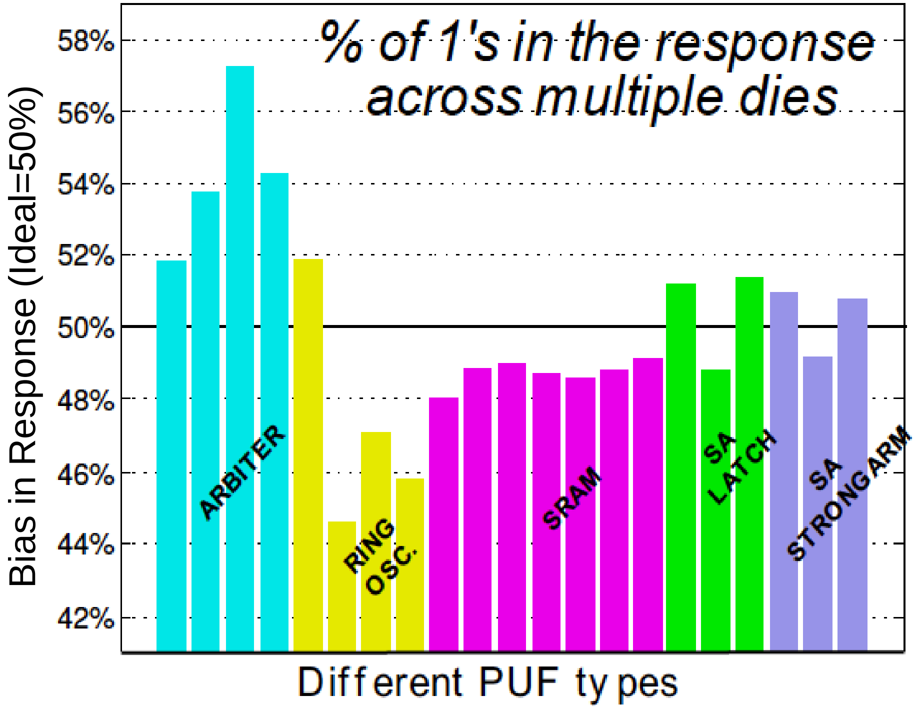
4 PUF implementations

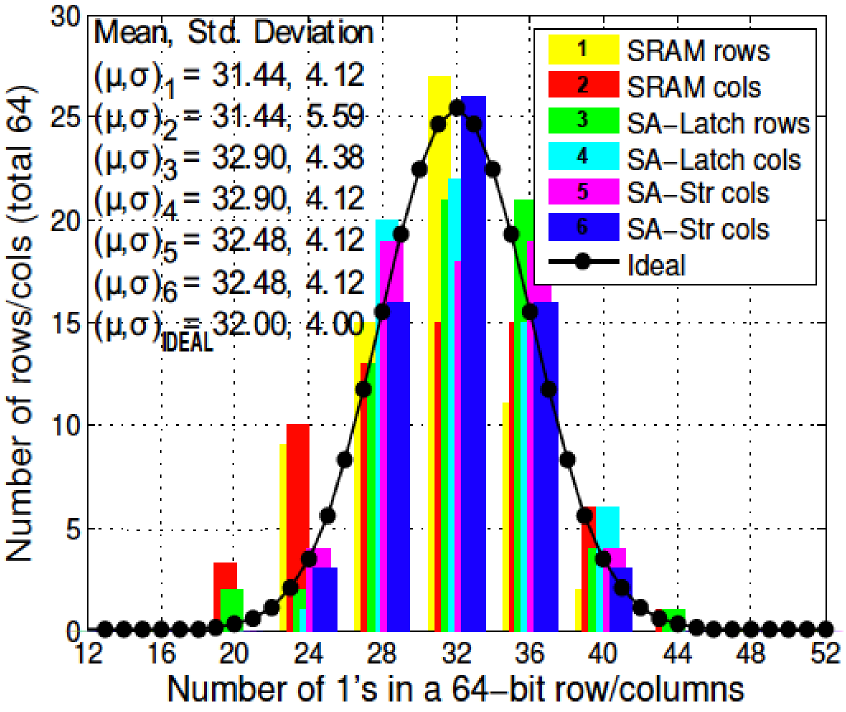
- Arbiter
- Ring oscillators
- SRAM
- Sense amplifier



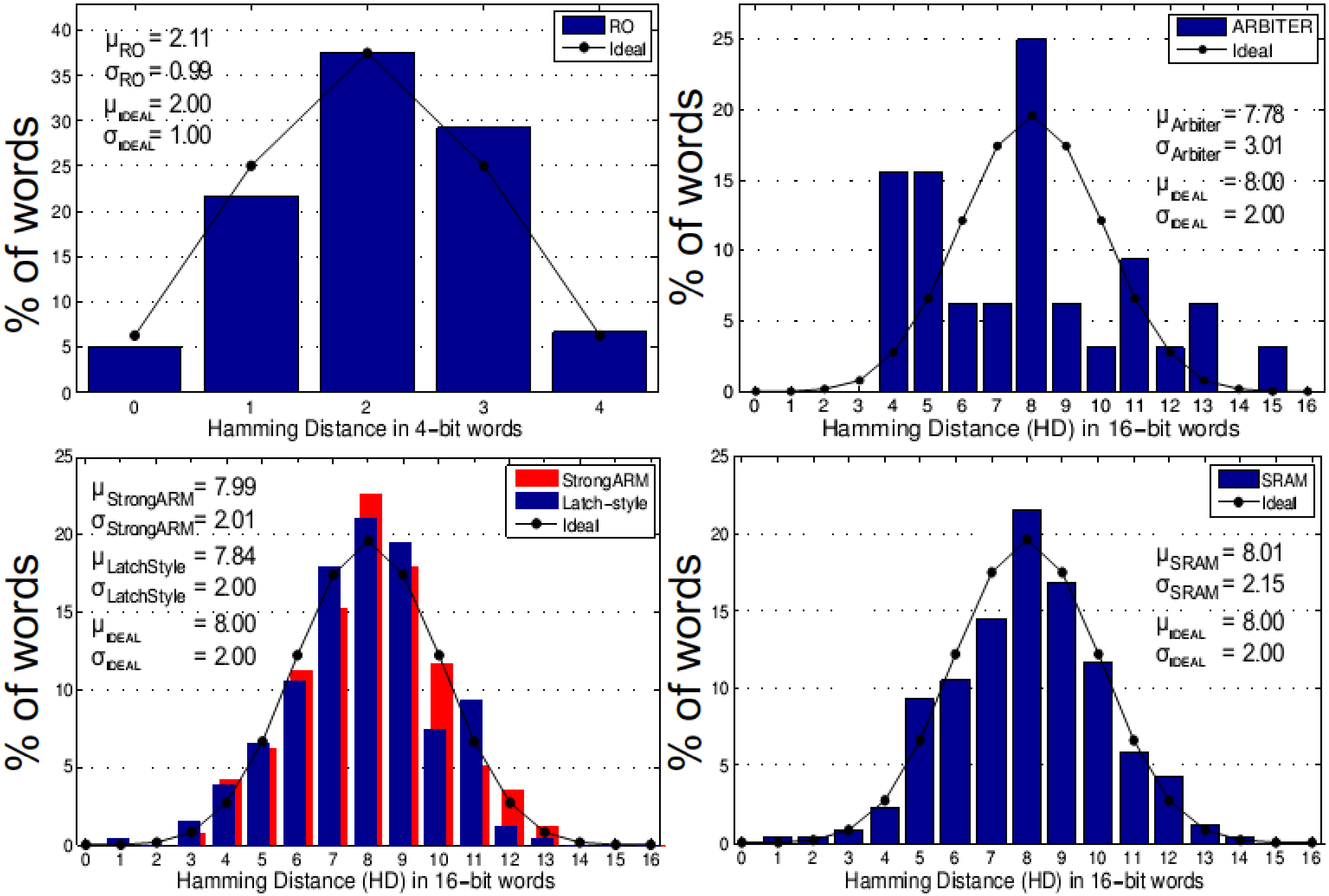
[Bhargava CICC 2012]

Comparison: Randomness

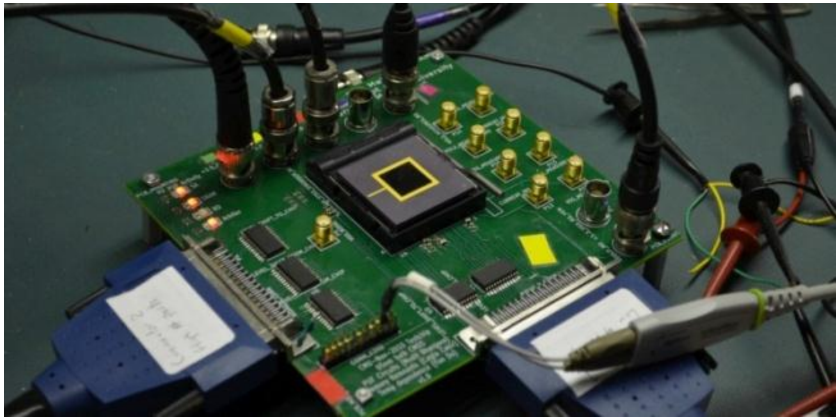




Comparison: Uniqueness

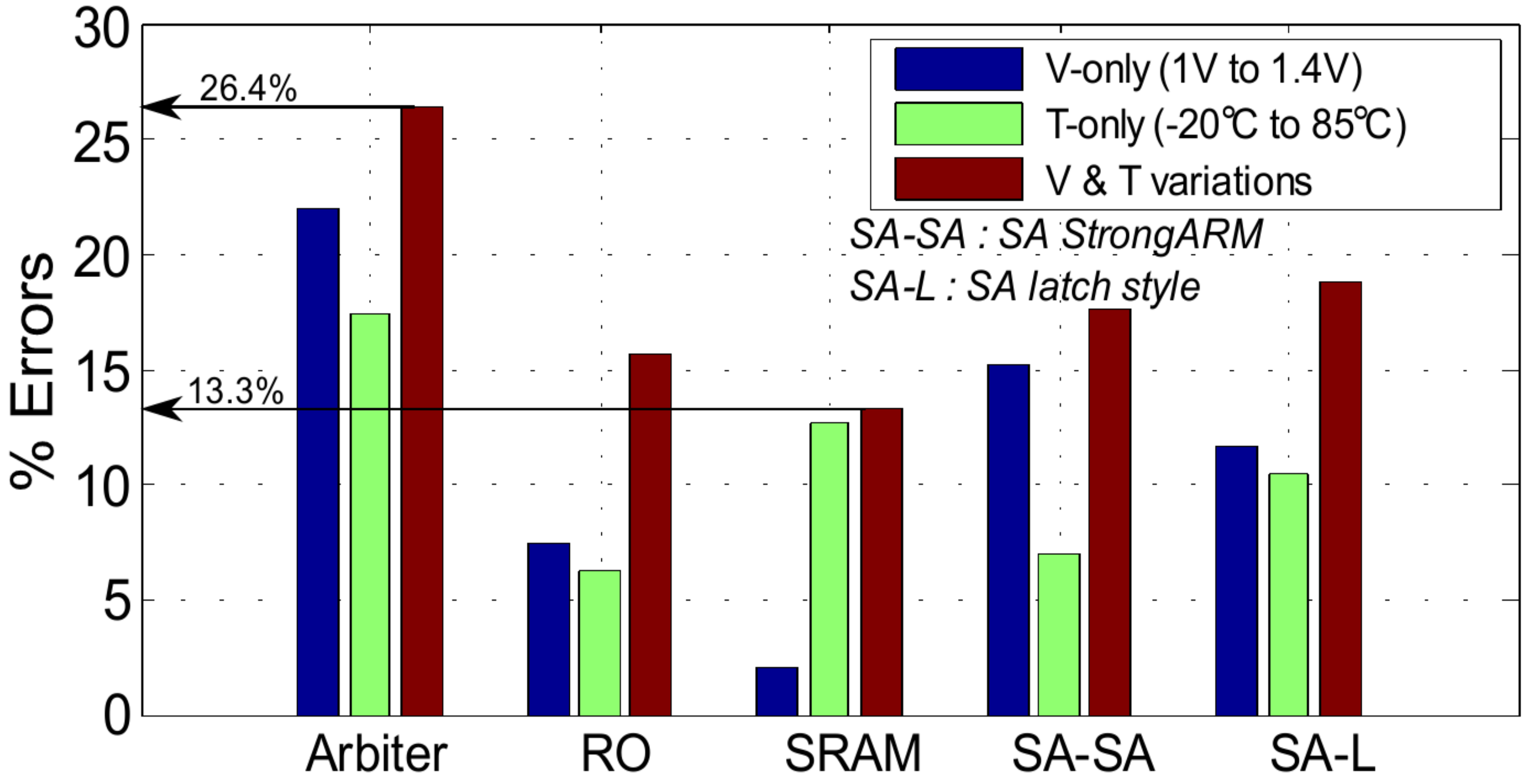


Reliability Measurement



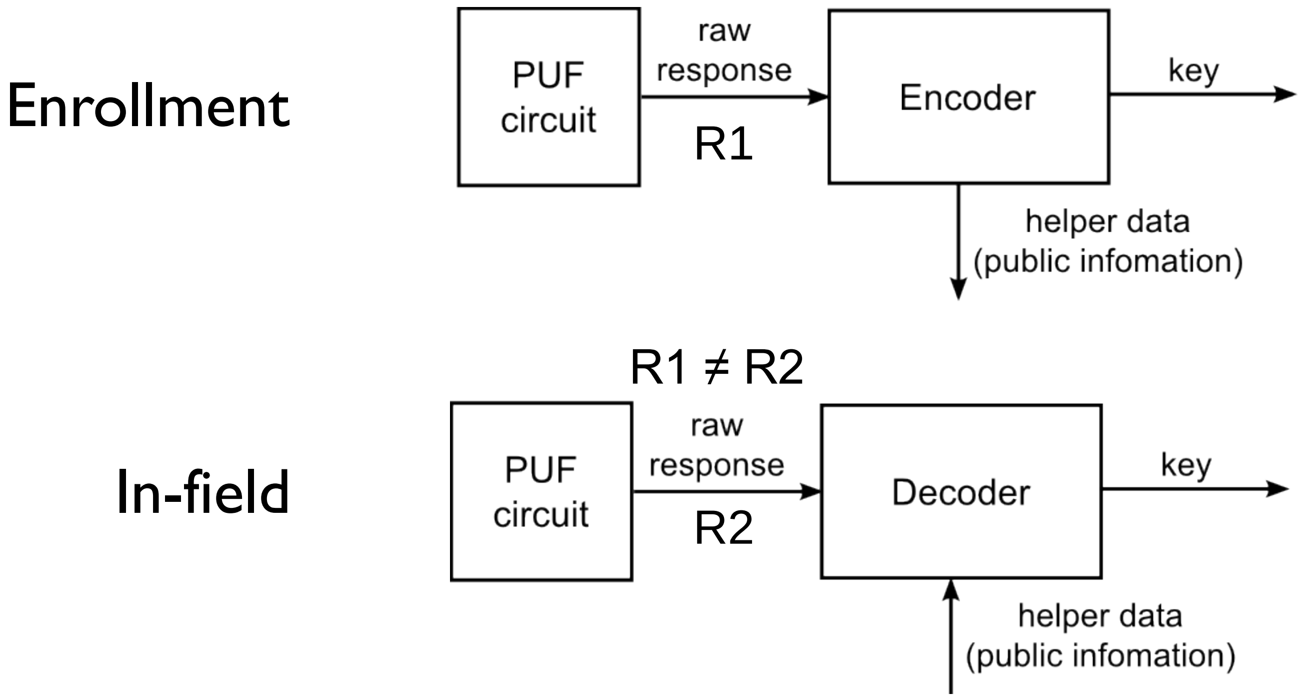
- Chips and board placed in temperature controlled chamber
- -20°C to 85°C
- 1.0V to 1.4V (1.2V nominal)
- Any response bit that flips is marked as erroneous

Comparison: Reliability



PUF reliability is insufficient for key generation

Conventional Solution: Error Correction Codes



Enrollment

PUF circuit

raw response

R1

Encoder

key

helper data (public infomation)

R1 ≠ R2

In-field

PUF circuit

raw response

R2

Decoder

key

helper data (public infomation)

- High overheads
  - Delay, power, and area
  - Complexity scale quickly with number of correctable errors
  - For BER=15%, need 20-80 response bits/key bit

- Requires helper data
  - Can leak information
- Decode is slow
  - Often thousands of cycles
  - Micro- or milli-second timescales

Proposed Solution: Response Reinforcement

Response reinforcement

- Increase the baseline reliability of the PUF core circuit
- Post-manufacturing amplification of random variations
- Minimize or eliminate the need for ECC
- No helper data

Implementation

- Measure PUF “golden” response
- Reinforce golden response by directed accelerated aging (DAA)
- DAA: Artificially induce IC aging phenomena to amplify PUF circuit random variation for increased reliability

Integrated Circuit Aging Phenomena

Many IC aging effects

- Negative Bias Temperature Instability (NBTI)
- Time Dependent Dielectric Breakdown (TDDB)
- Metal electro-migration (EM)
- Hot Carrier Injection (HCI)

Desired characteristics

- Easy to artificially induce
- Short reinforcement time
- Strong reinforcement effect
- High permanence

Integrated Circuit Aging Phenomena

Many IC aging effects

- Negative Bias Temperature Instability (NBTI) [Bhargava HOST 2012]
- Time Dependent Dielectric Breakdown (TDDB)
- Metal electro-migration (EM)
- Hot Carrier Injection (HCI)

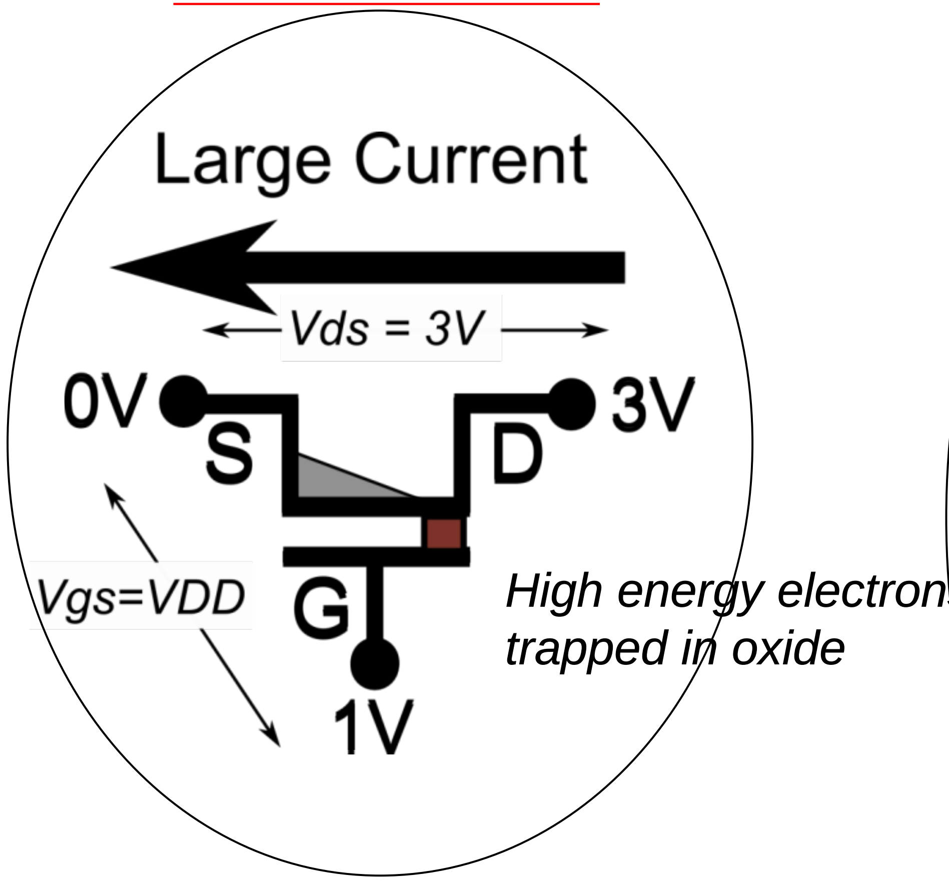
Desired characteristics

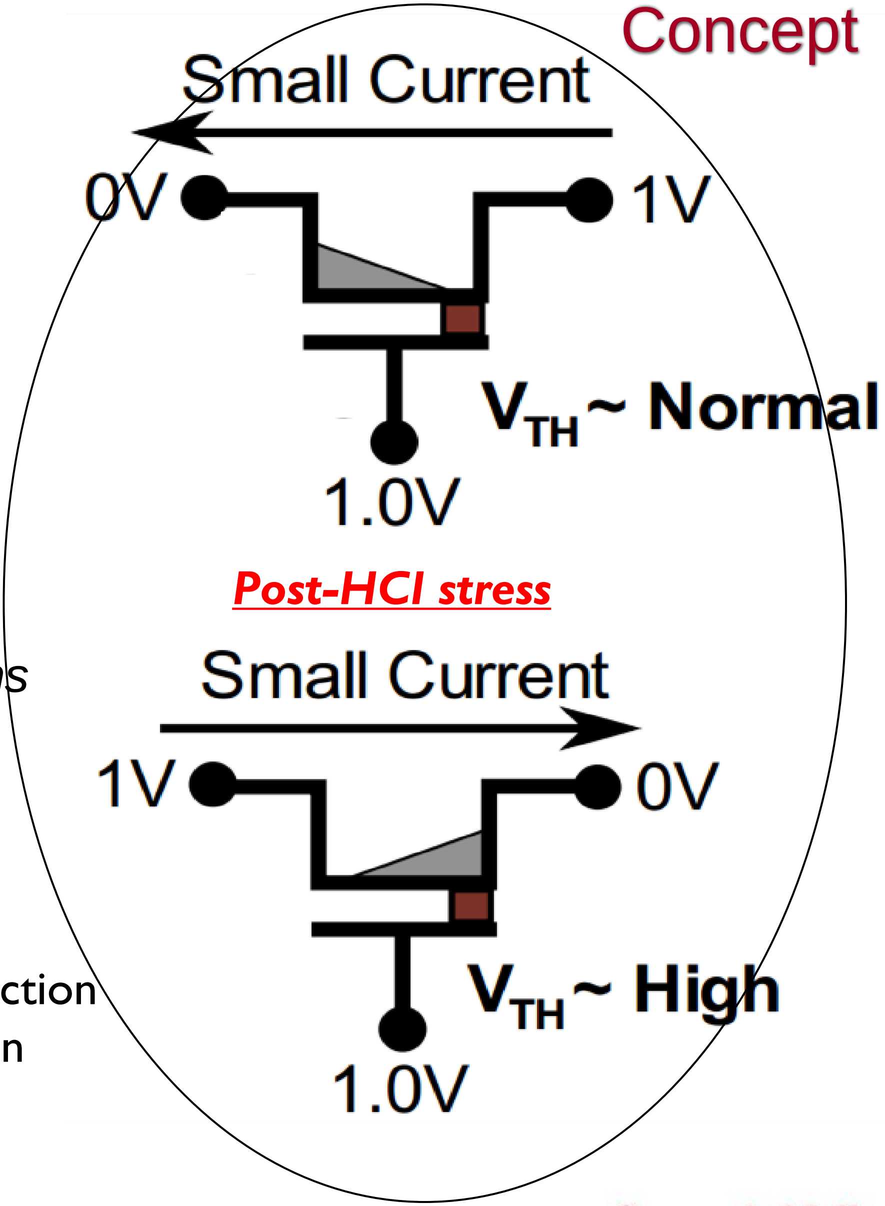
- Easy to artificially induce → Only need a raised voltage ~3V
- Short reinforcement time → ~10s reinforcement (one time)
- Strong reinforcement effect → Shifts transistor V_{TH} by >50mV
- High permanence → Effect lasts for years

Hot Carrier Injection

Concept

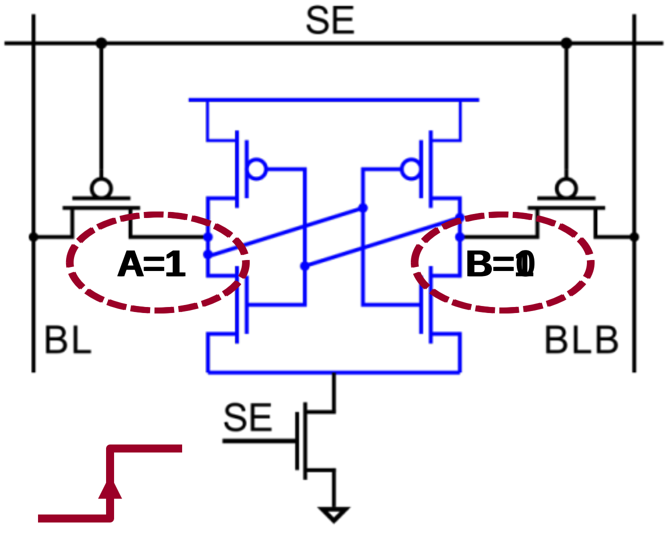
One-time HCI stress



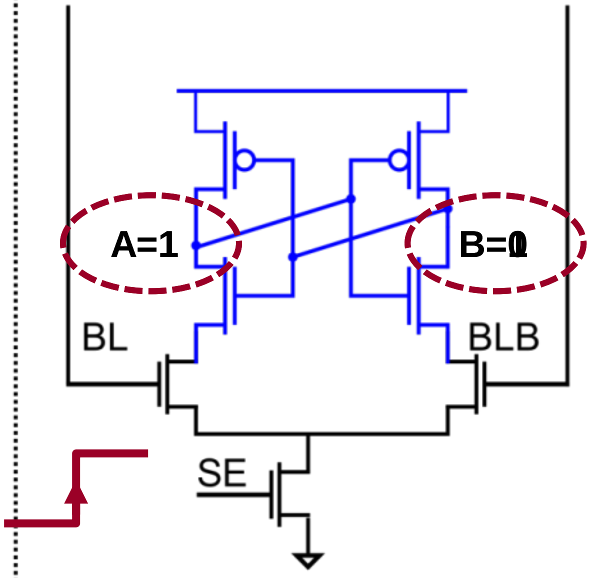


- Small increase in V_{TH} if current in same direction
- High increase in V_{TH} (~ 100 mV) if current in opposite direction

Sense Amplifier: Use as PUF



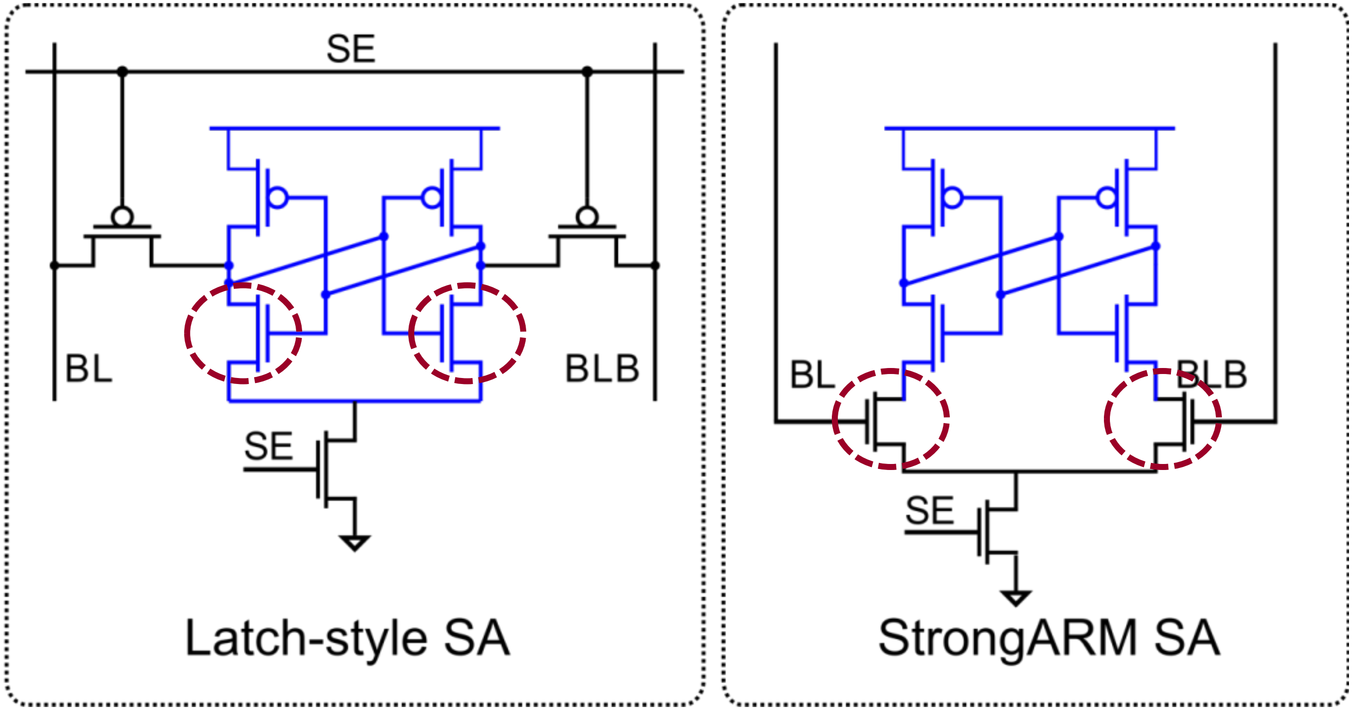
Latch-style SA



StrongARM SA

[Bhargava HOST 2010]

Sense Amplifier: Use as PUF

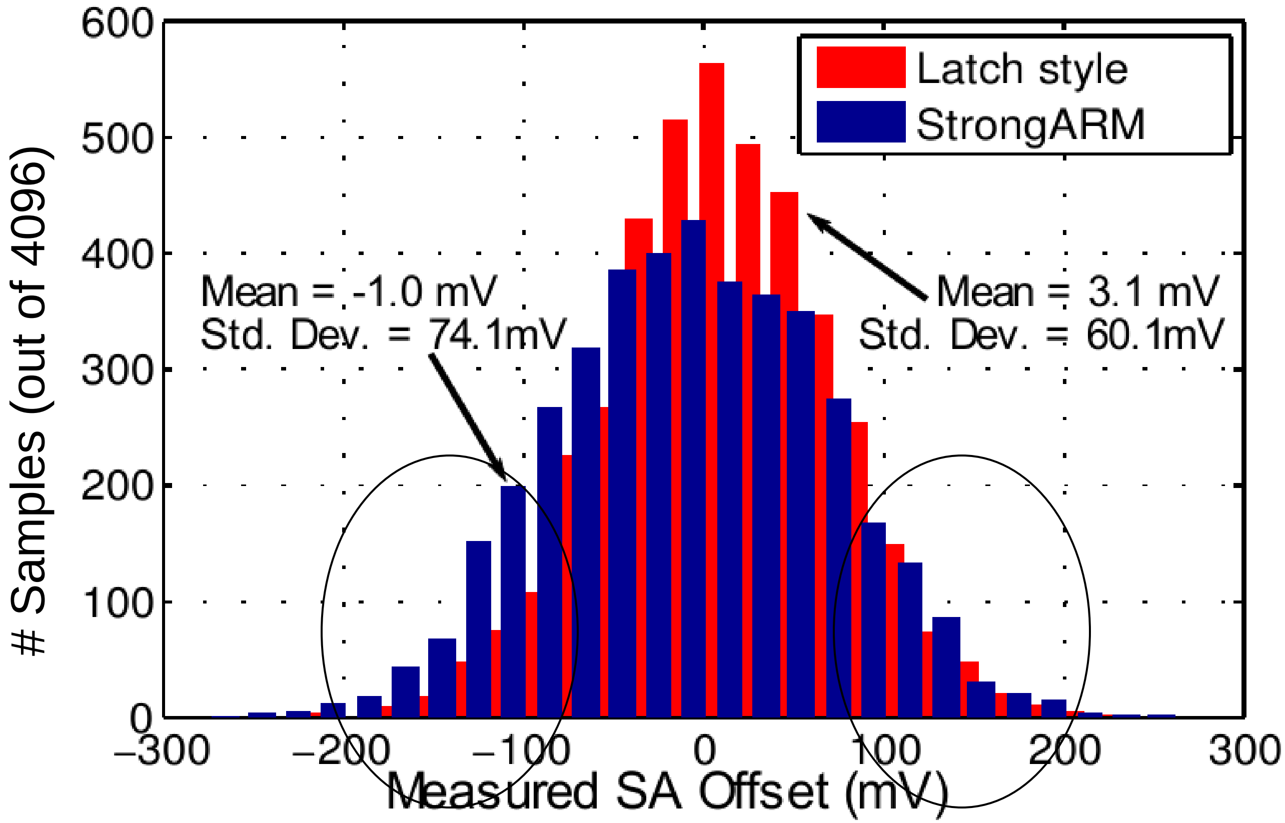


Latch-style SA

StrongARM SA

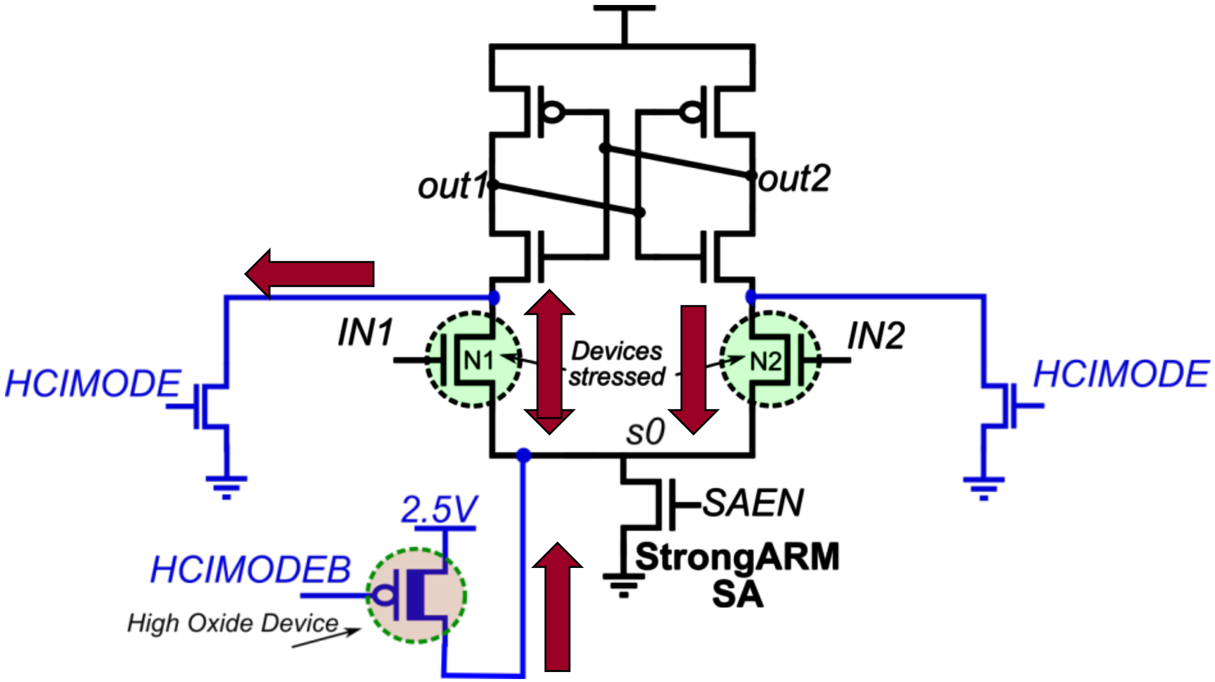
SA offset voltage strong function of difference in V_{TH} of matched devices

Sense Amplifier Offset Voltage



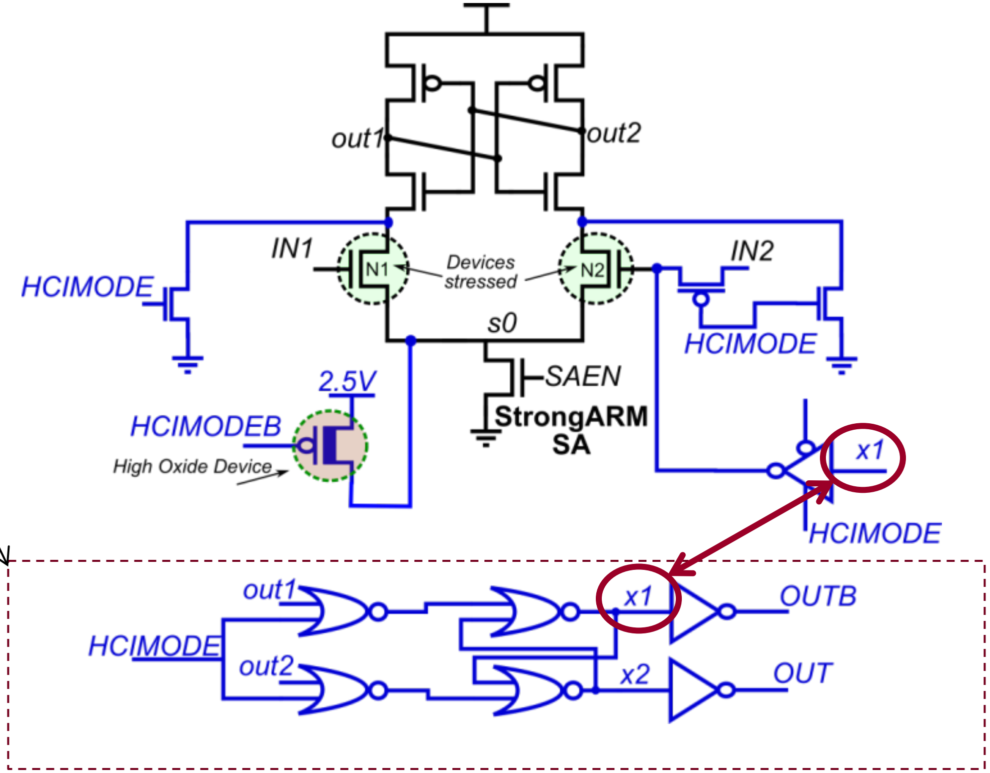
High |offset| ➔ more reliable PUF

Hot Carrier Injection Sense Amplifier (HCI-SA)



Hot Carrier Injection Sense Amplifier (HCI-SA)

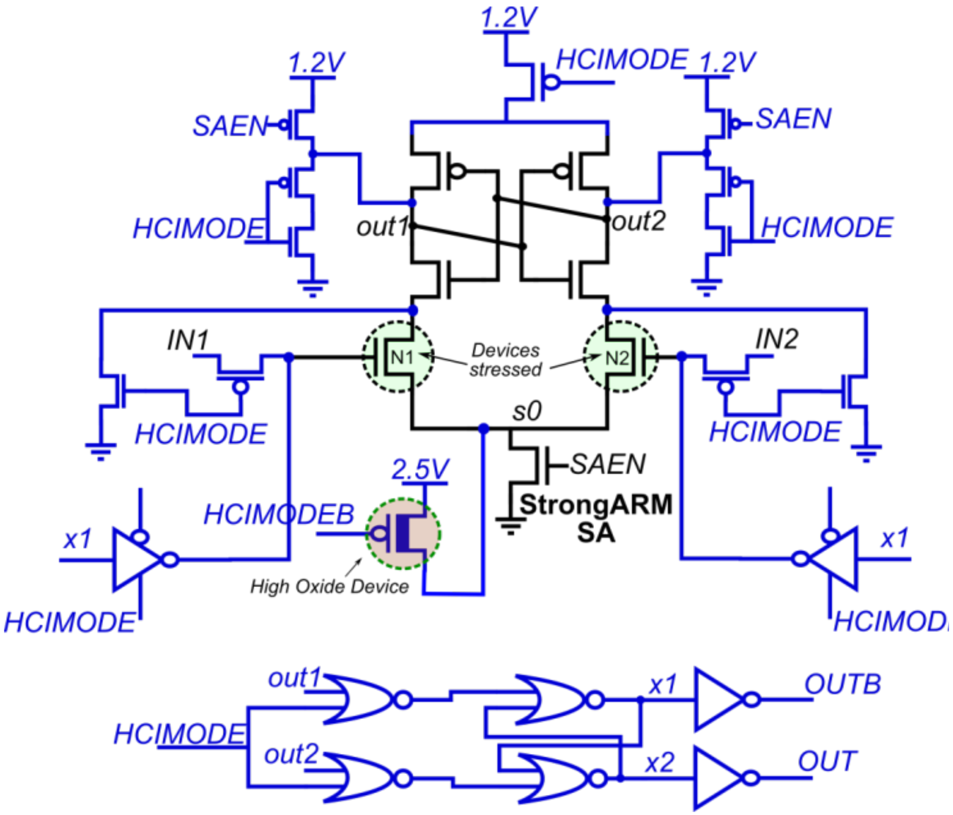
This memory structure locally stores the value x1 and x2 as copies of out1 and out2 when the HCI-SA is run like a normal SA (HCIMODE=0; HCIMODEB=1) before any HCI stress. These values are later used to provide the right biasing during HCI-stress in the stress mode (HCIMODE=1; HCIMODEB=0)



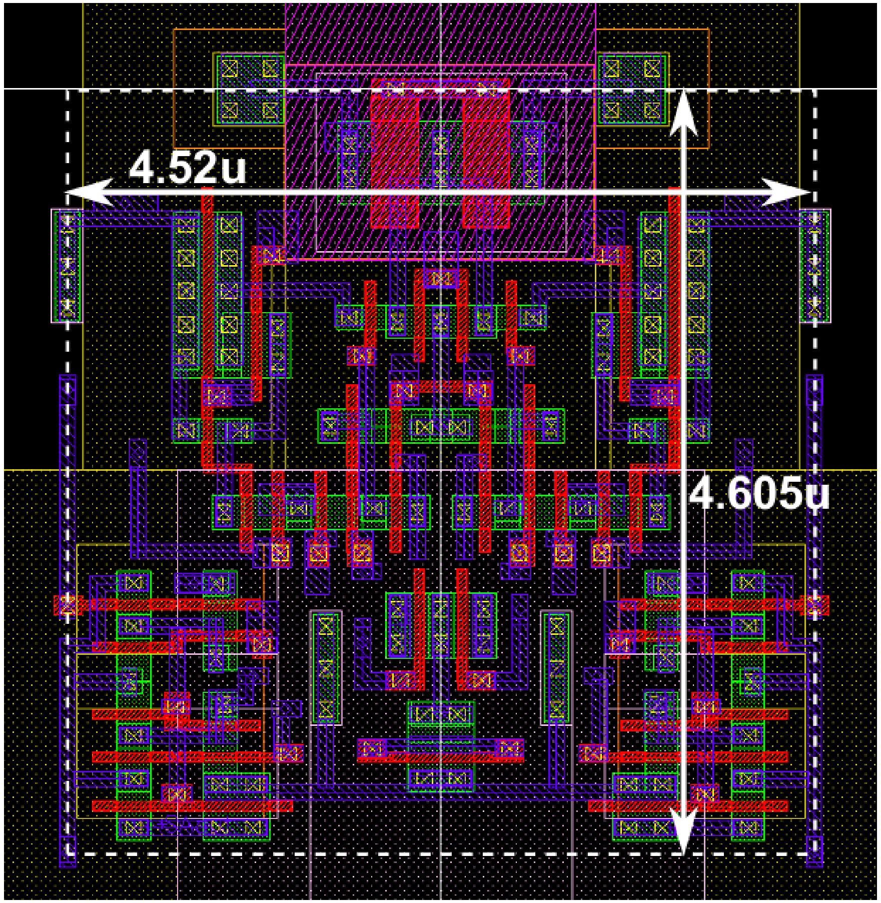
Per-cell local memory to store preferred value for burn-in

Hot Carrier Injection Sense Amplifier (HCI-SA)

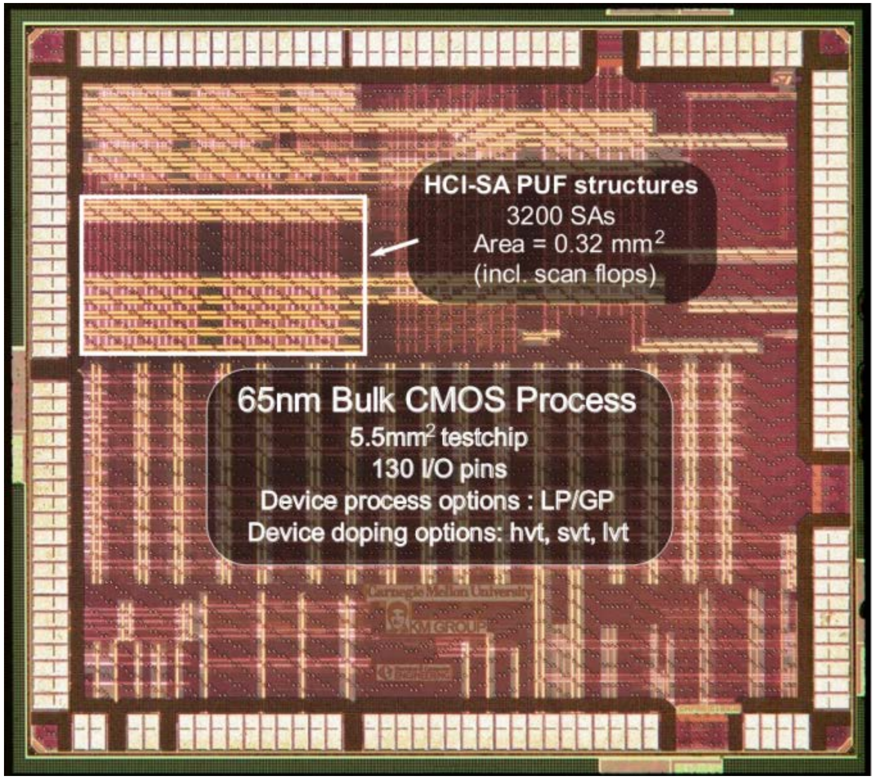
Complete Schematic



Complete Layout

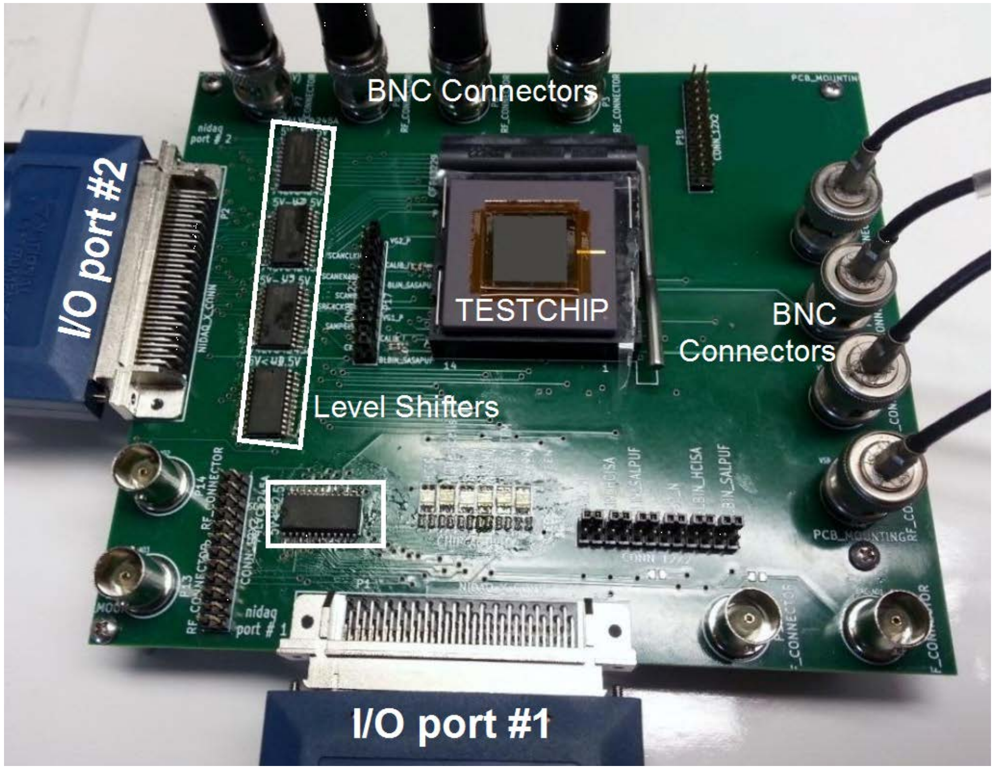


HCI-SA Testchip



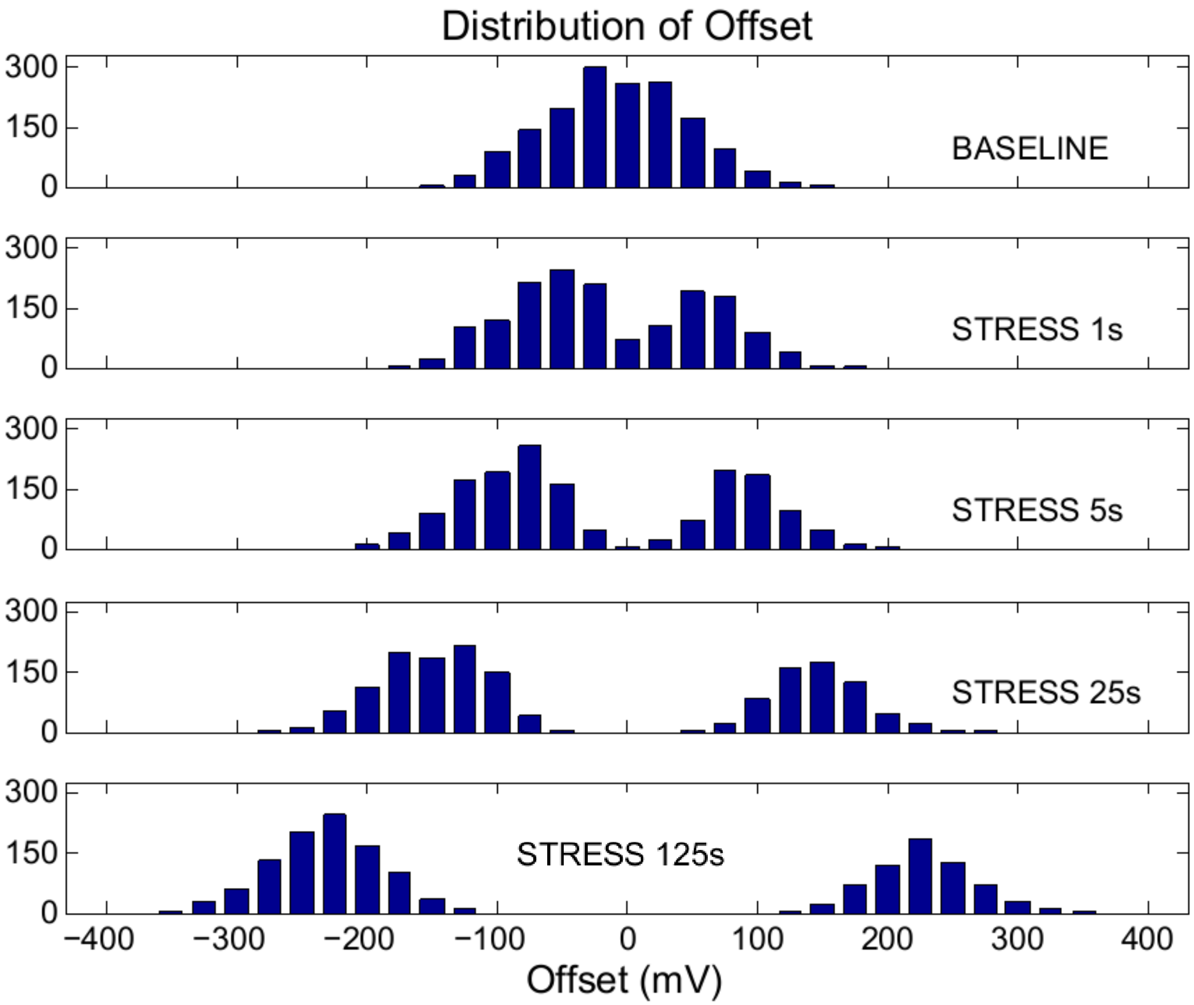
HCI-SA PUF structures
3200 SAs
Area = 0.32 mm^2
(incl. scan flops)

65nm Bulk CMOS Process
5.5mm^2 testchip
130 I/O pins
Device process options : LP/GP
Device doping options: hvt, svt, lvt

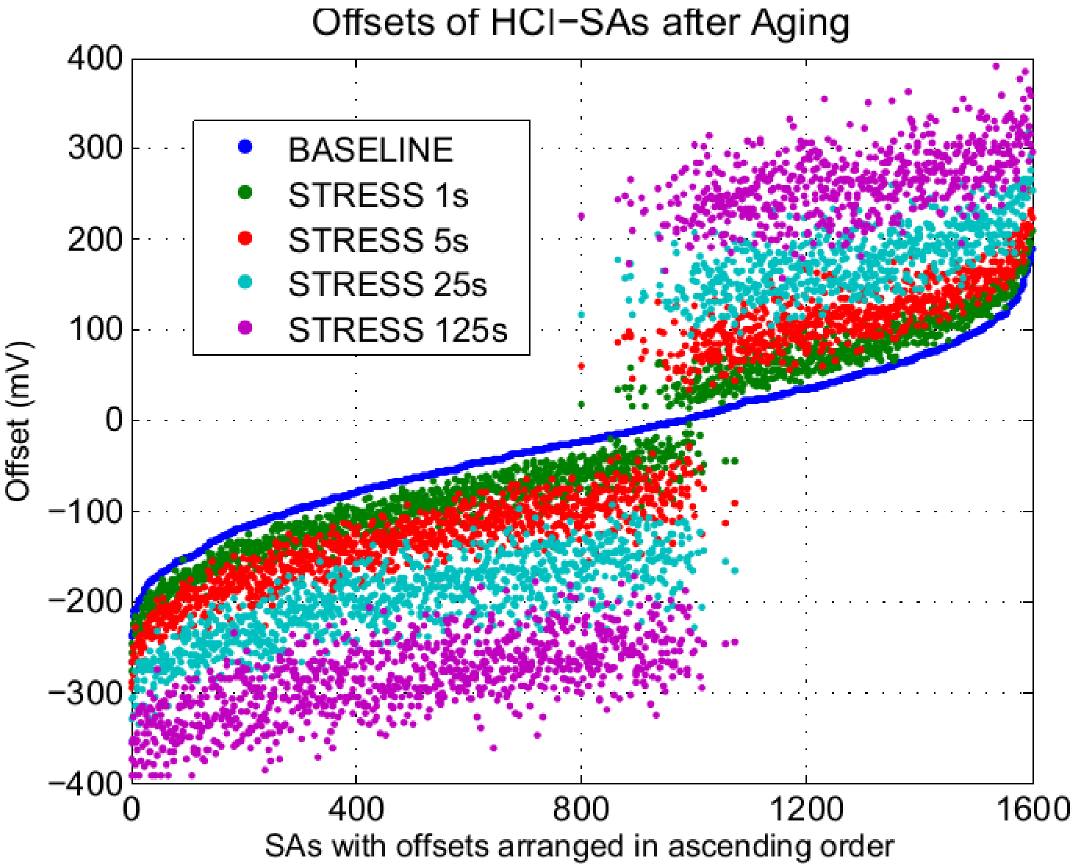


- 1600 self-reinforcing HCI-SA
- 1600 manually controlled HCI-SA
- Tested across 9 voltage/temperature corners
- HCI stress times of 1s, 5s, 25s, 125s

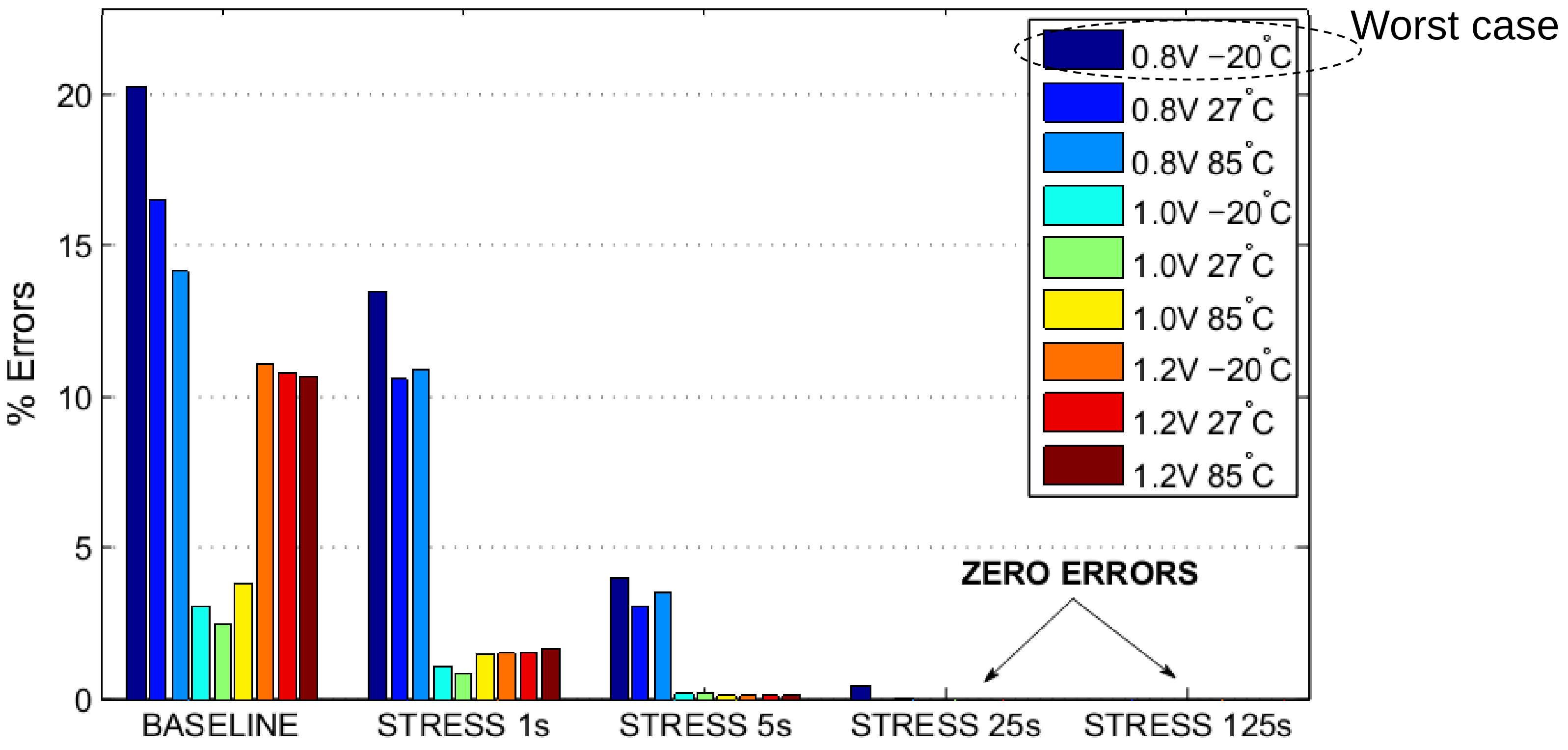
HCI-SA Offset Shift



HCI-SA Offset Shift



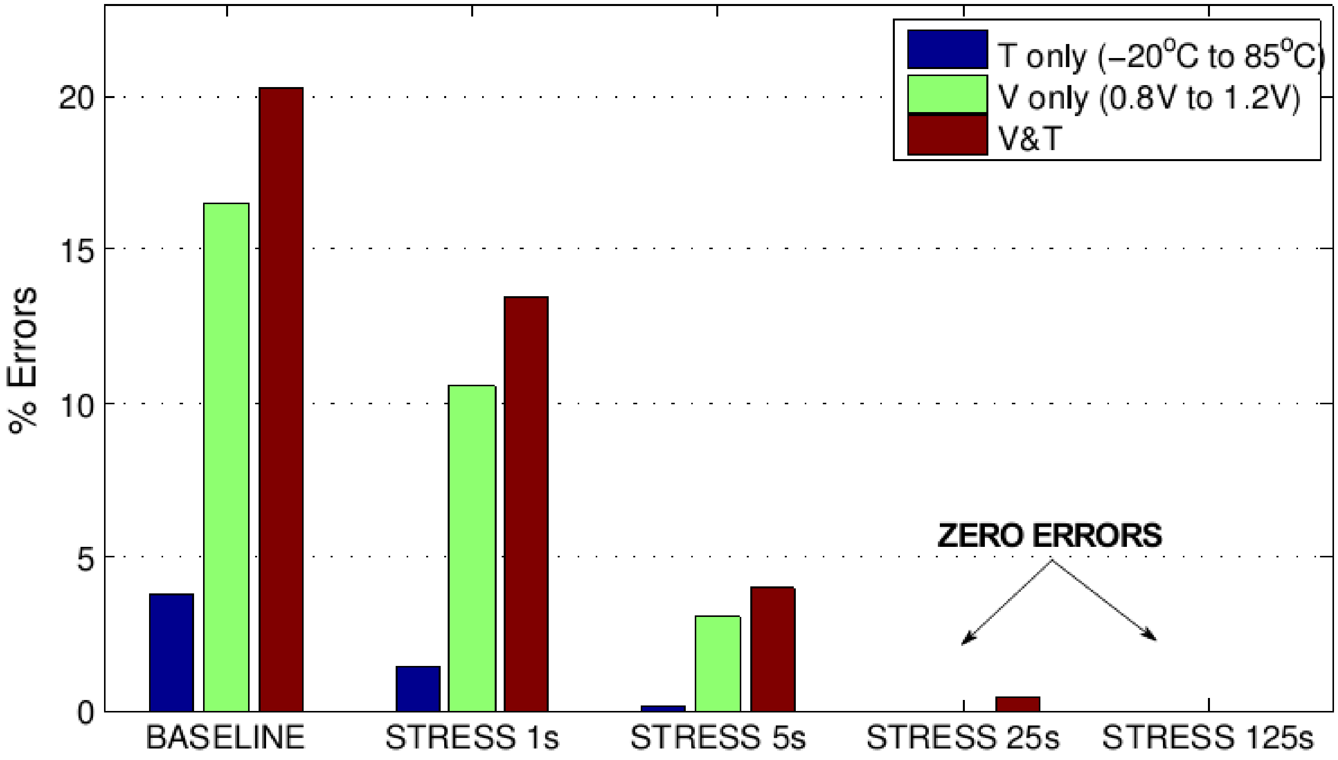
HCI-SA Reliability Measurements



100 runs at all 9 voltage/temperature corners

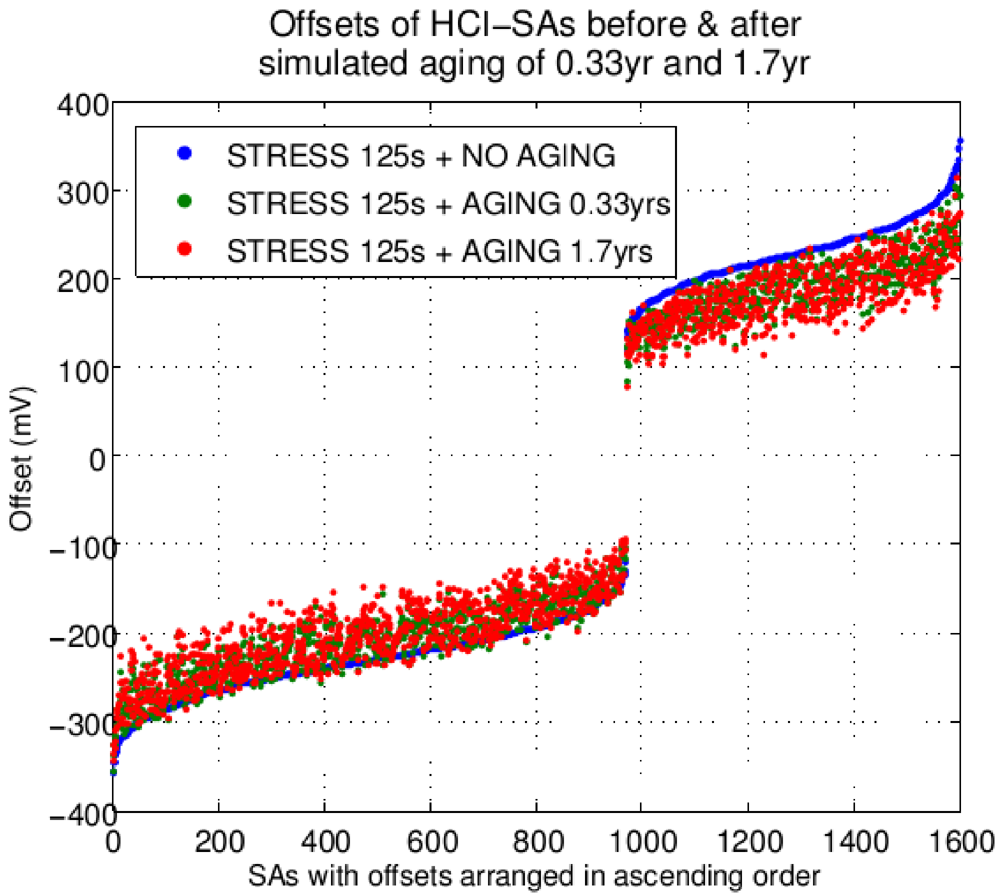
→ No errors found after stress of 125 seconds

HCI-SA Reliability Measurements



100 runs at all 9 voltage/temperature corners
→ No errors found after stress of 125 seconds

HCI-SA: Permanence of Offset Shift



Baked chips at 1.5V and 100^{0}C

- 18 hours ➔ 0.33 years
- 93 hours ➔ 1.7 years

Large-Scale Reliability Measurements

Measured 125k evaluations (125s HCI stress)

- At nominal corner (1.2V 27^{0}C)
- At worst case corner (1.0V -20^{0}C)
- No errors observed in any of the 1600 HCI-SAs

⬇

- Bit error rate BER $< 5 * 10^{-9}$
- Key error rate KER $< 0.6 * 10^{-6}$ (128-bit)
- KER target $< 10^{-6}$ for reliable key generation

Summary

HCI-SA PUF

- Reliable – BER < 5 * 10^{-9} without ECC
- Secure – No helper data
- Fast – Response generation in 1 cycle (~1ns)
- Simple – One-time short reinforcement step (125s)
- High Permanence – Small change after ~2yr simulated aging

Thank You