Bias-based modeling and entropy analysis of PUFs

Robbert van den Berg
Boris Škorić
Vincent van der Leest

TU/e

INTRINSIC ID

TrustED 2013
4 November

Outline

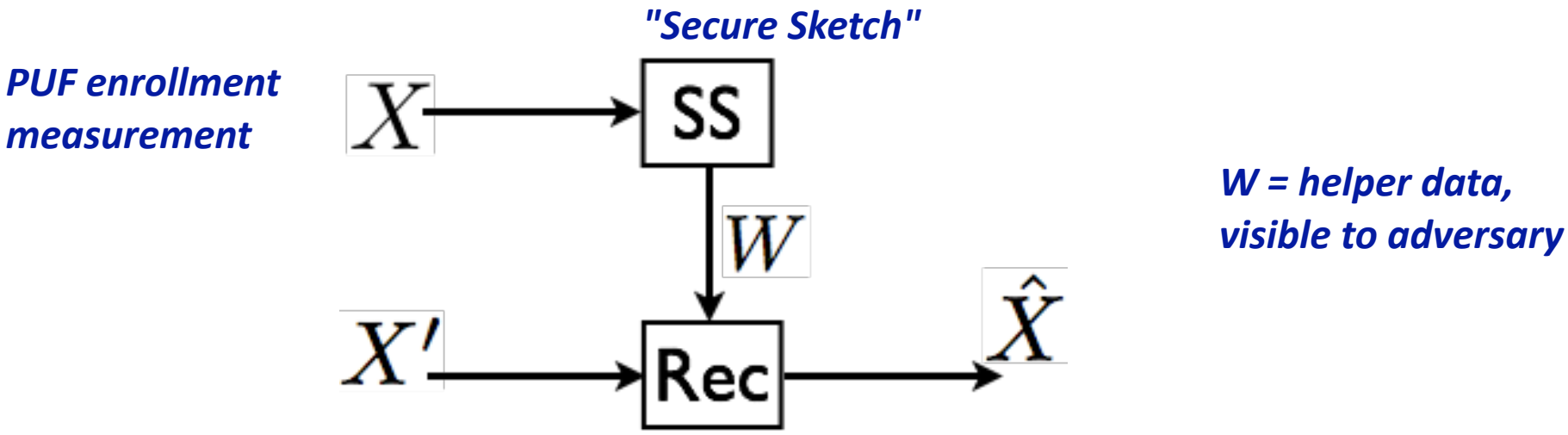
- Physical Unclonable Functions (PUFs)
- Memory-based PUFs
- How many bits can be extracted?
  - uniqueness
  - noise
- "Reconstruction capacity"
  - Model: PUF = vector of biases
  - Mutual info between enrolment and reconstruction meas.
  - captures uniqueness *and* noise
- Numerics

Physical Unclonable Functions

Memory-based PUFs

- Memory cells consisting of cross-coupled inverters that can retain 0/1 value:
  - SRAM memory
  - flipflops
  - latch
  - buskeeper
- Startup value
  - unique fingerprint
  - uncontrollable, even for manufacturer

Extraction of identifier/key from PUF



- Typically X is not uniform.
  - OK for identifier or password
- To get a uniform key, apply Universal Hash Function to X
  - UHF is wasteful, so typically take a good one-way hash

Question: How much secret info is there in X given W?

Model for memory-based PUFs

At **enrolment**, each cell has a **bias**

- Prob[cell *i* starts up in state "1"] = b_i. $b_i \in [0,1]$
- PUF fully characterized by vector **b**=(b_1, ... ,b_n)
- prob. density at manufacture: ρ(**b**)
- multiple (k) measurements of each cell: x_i= #(meas. yielding "1" in cell i)
- vector **x**/k is estimator for **b**

Reconstruction

- Noise! Biases may have changed.
- transition prob. τ(**b**'|**b**)
- multiple (ℓ) measurements: y_i= #(meas. yielding "1" in cell i)
- vector **y**/ℓ is estimator for **b**'

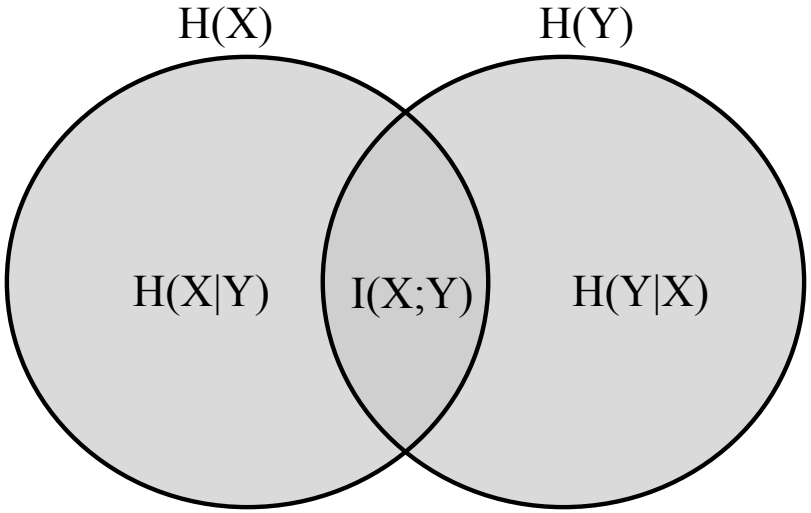
$$\Pr[\boldsymbol{X}=\boldsymbol{x},\boldsymbol{Y}=\boldsymbol{y}] \quad = \quad \int_0^1 \mathrm{d}^n b\ \rho(\boldsymbol{b}) p_{\boldsymbol{x}|\boldsymbol{b}} \int_0^1 \mathrm{d}^n b'\ \tau(\boldsymbol{b}'|\boldsymbol{b}) q_{\boldsymbol{y}|\boldsymbol{b}'}$$

product of independent binomial distributions

"Reconstruction Capacity"

Mutual information between X and Y

- upper bound on Shannon entropy of robustly reproducible string
- captures "uniqueness" of **X**
- captures noise



$$I(\boldsymbol{X};\boldsymbol{Y}) = \sum_{xy} p_{xy} \log \frac{p_{xy}}{p_x p_y}$$

Extreme cases

- No noise $\Longrightarrow$ I(**X**;**Y**) = H(**X**)
- Overwhelming noise $\Longrightarrow$ I(**X**;**Y**)≈0

Curse of dimensionality

- We want to estimate Pr[**X**=**x**, **Y**=**y**] from measurements ...
- **Problem**: too few samples (PUFs) to populate the (**X**,**Y**) space
- Next best thing:
  - estimate $Pr[X_i=x_i]$ for each cell
  - estimate transition prob. $\tau(b'_i \mid b_i)$ for each cell
  - *ignore correlations between cells*

Potentially dangerous! But our data shows almost no correlation.

Simplified model

All probabilities reduce to product over cells

$$\Pr[\boldsymbol{X}=\boldsymbol{x}] \approx \prod_{i\in[n]} \int_0^1 \mathrm{d}b_i \; \rho_i(b_i) p_{x_i|b_i}$$

$$\Pr[\boldsymbol{Y}=\boldsymbol{y}] \approx \prod_{i\in[n]} \int_0^1 \mathrm{d}b'_i [\int_0^1 \mathrm{d}b_i \; \rho_i(b_i)\tau_0(b'_i|b_i)] q_{y_i|b'_i}$$

$$\Pr[\boldsymbol{X}=\boldsymbol{x},\boldsymbol{Y}=\boldsymbol{y}] \approx \prod_{i\in[n]} \int_0^1 \mathrm{d}b_i \rho_i(b_i) p_{x_i|b_i} \int_0^1 \mathrm{d}b'_i \tau_0(b'_i|b_i) q_{y_i|b'_i}$$

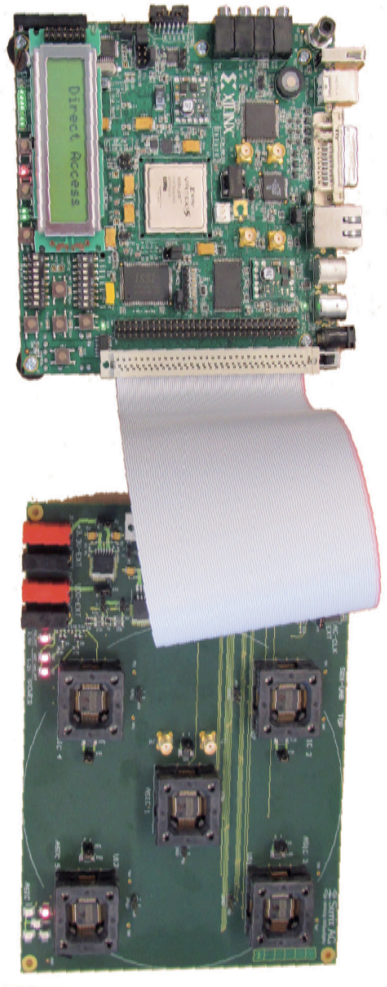
Estimate from measure-ments

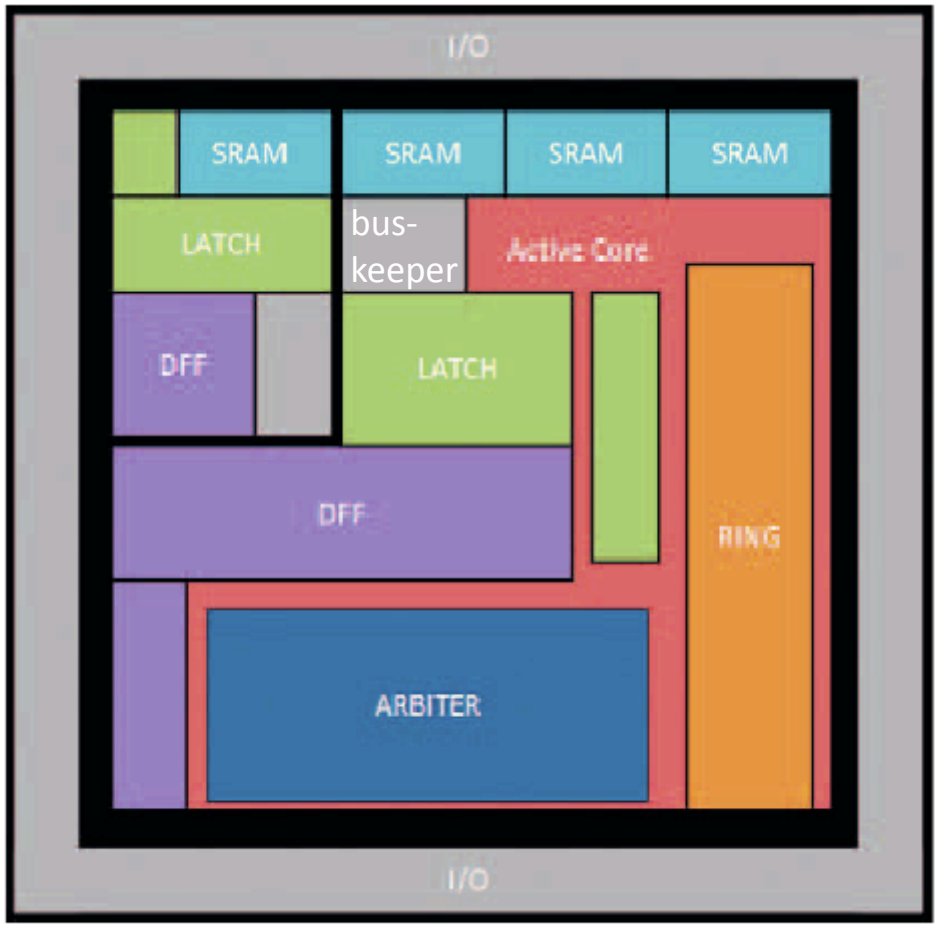
Entropy becomes sum over cells

$$\mathrm{I}(\boldsymbol{X};\boldsymbol{Y}) \approx \sum_{i\in[n]} \mathrm{I}(X_i;Y_i)$$

Data set

- UNIQUE project: ASIC containing multiple PUF types
- 192 ASICs





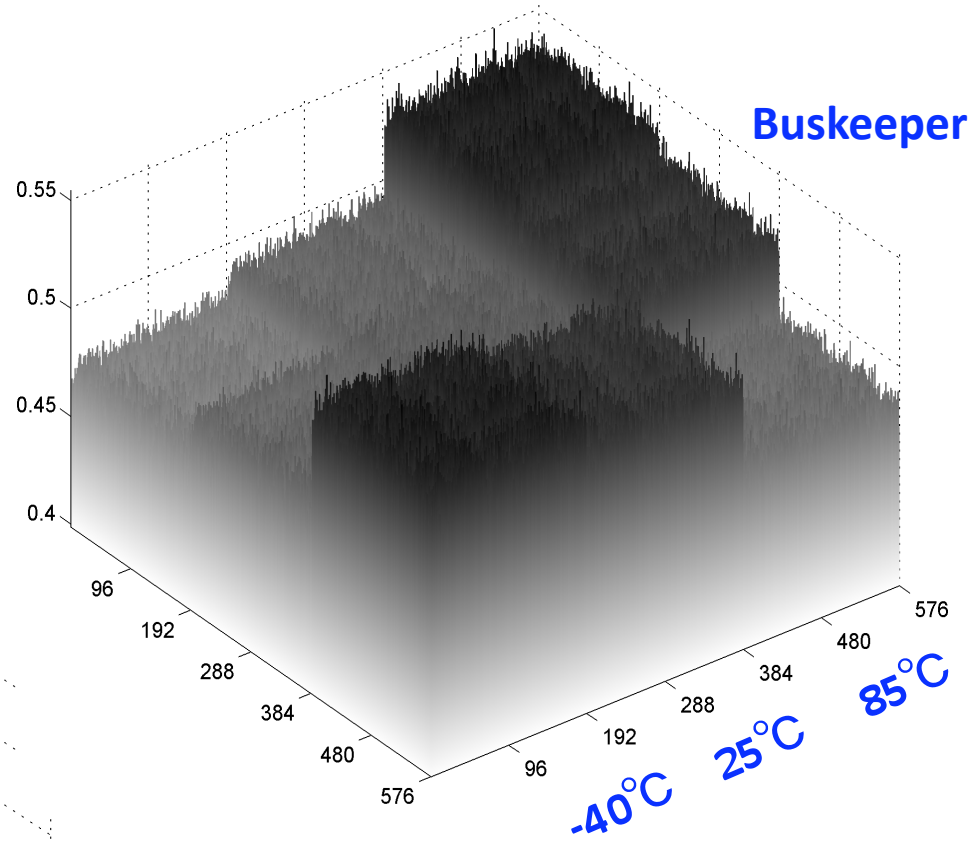
Floorplan of the UNIQUE ASIC design

Inter-device distance in terms of biases

Distance between PUFs p and p'

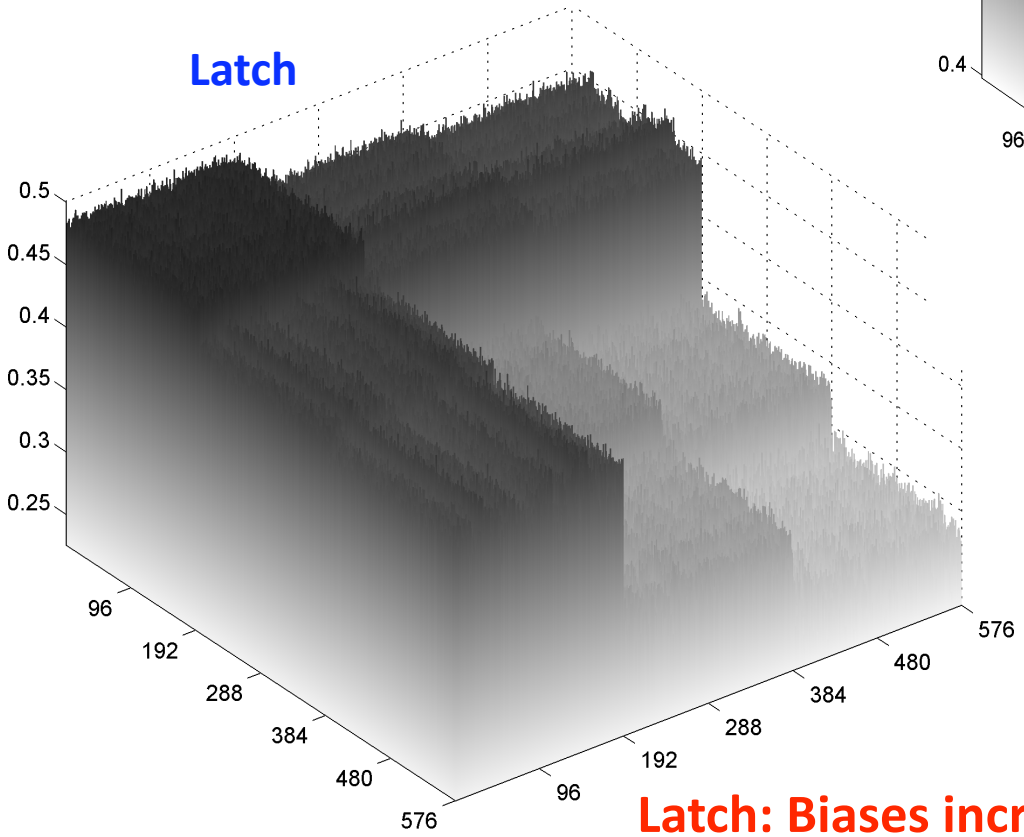
$$\frac{1}{n}\sum_{i=1}^{n}\left|\frac{x_i^{(p)}}{k}-\frac{x_i^{(p')}}{k}\right|$$

Buskeeper



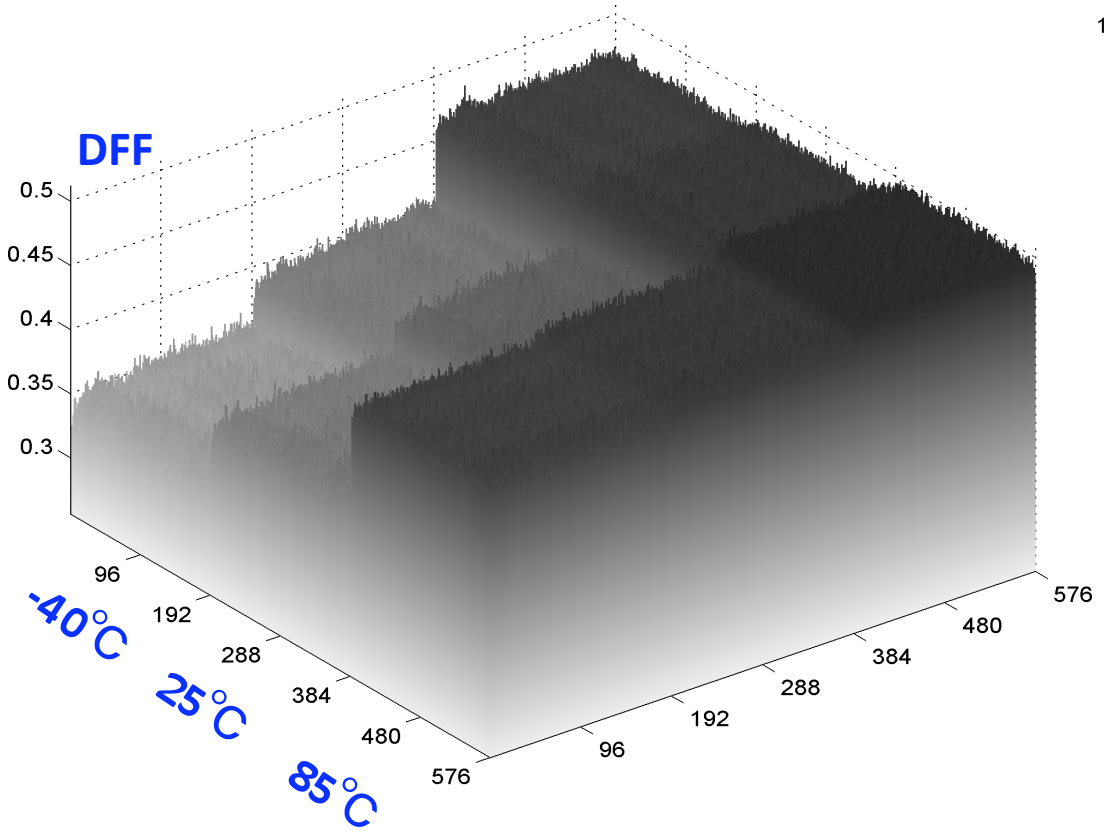
Buskeeper:
Higher bias at 85°C

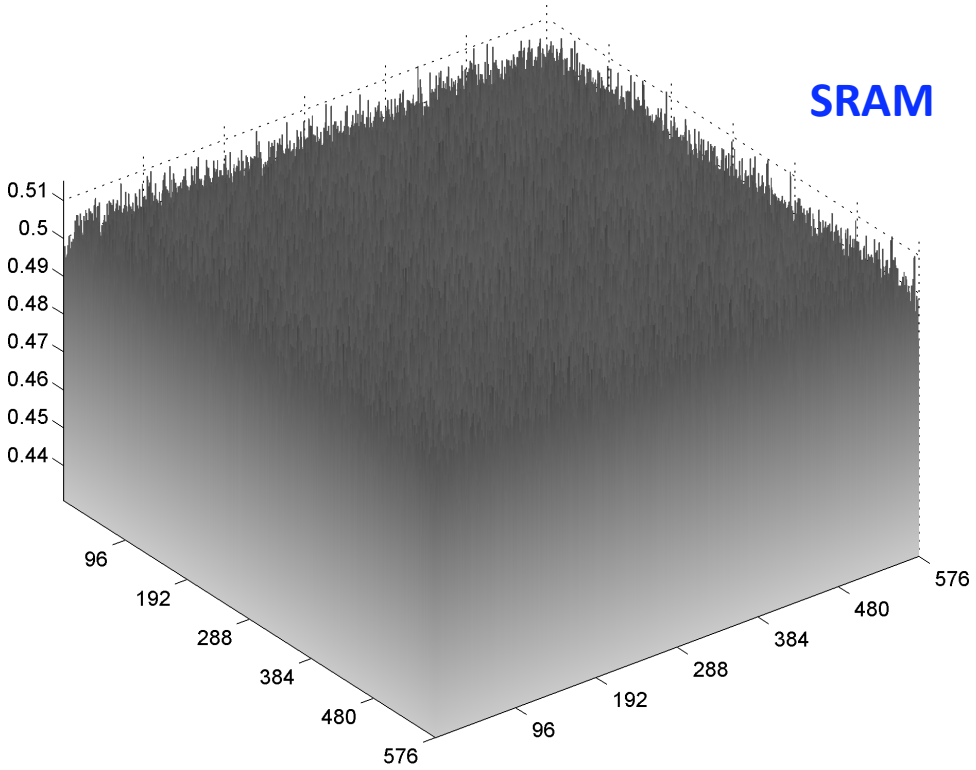
Latch



Latch: Biases increase at high temp.

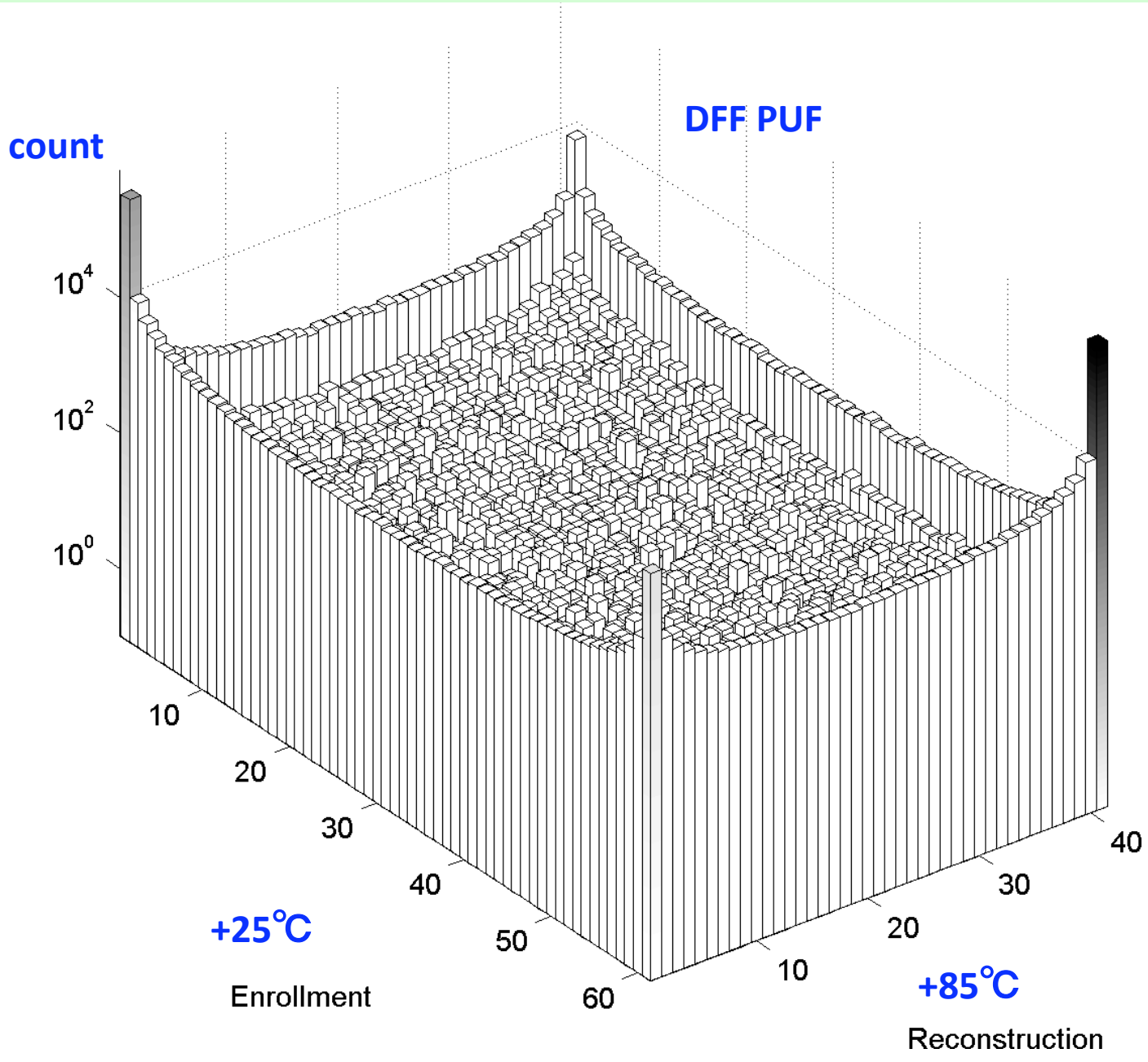
DFF:
biases go up at low temp.





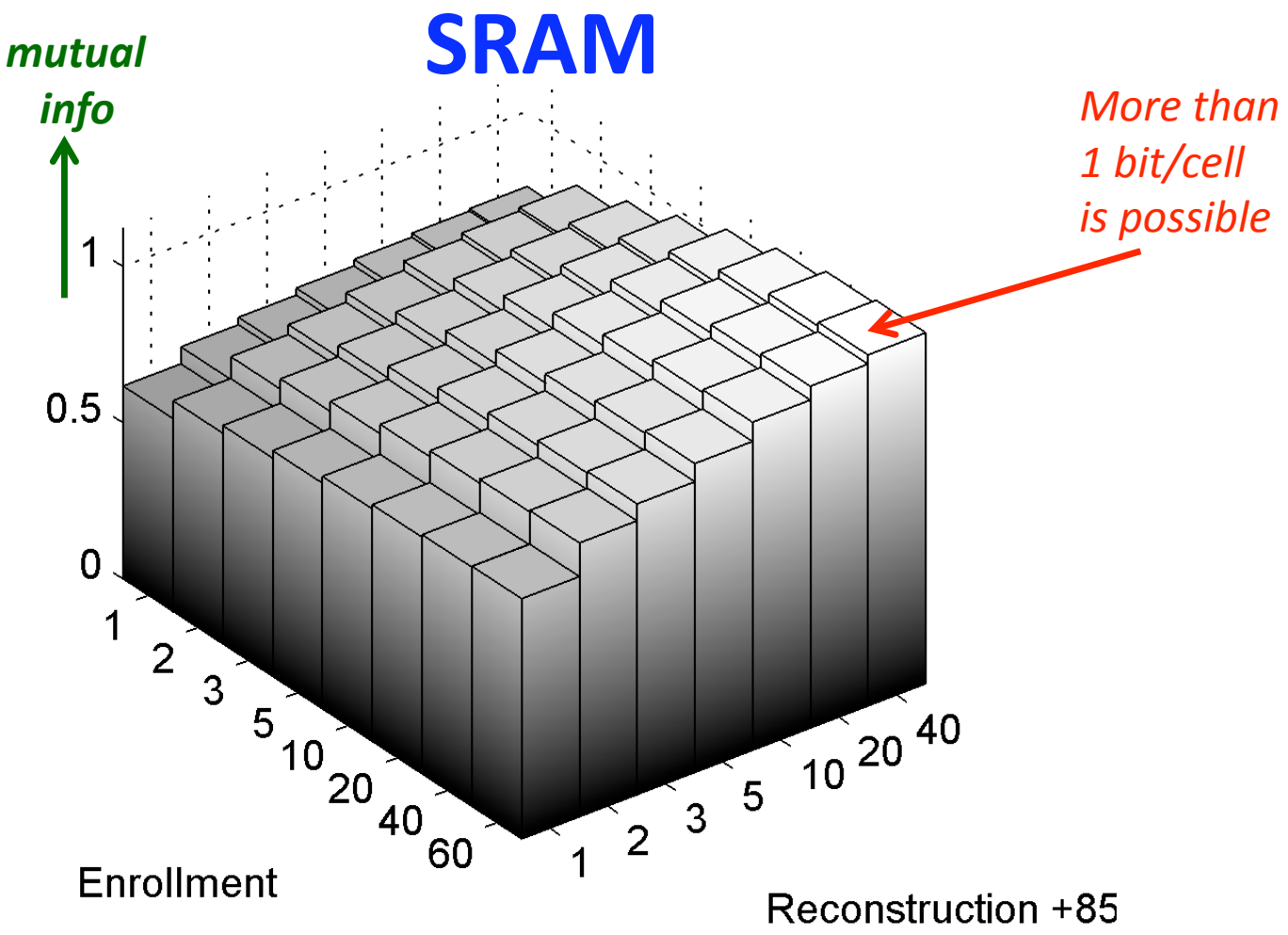
SRAM:
Temp. has little effect.

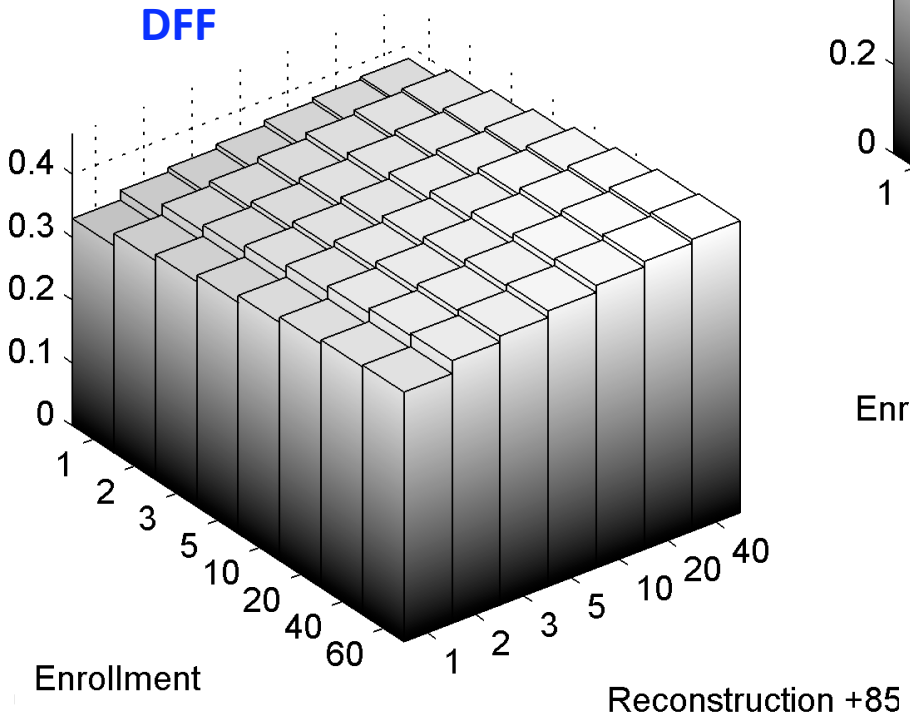
Single-cell transition probability

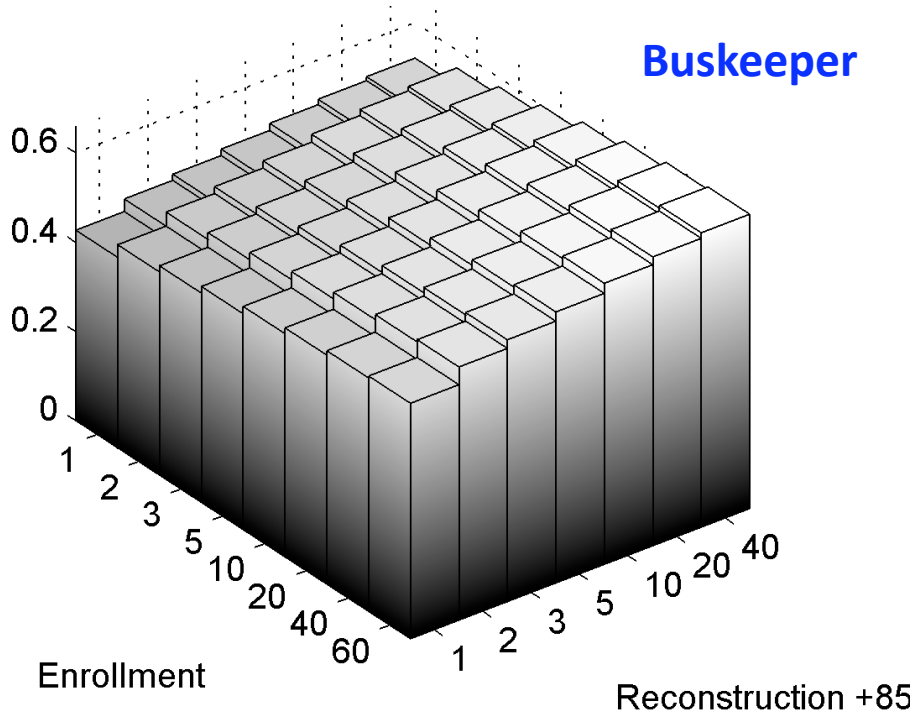


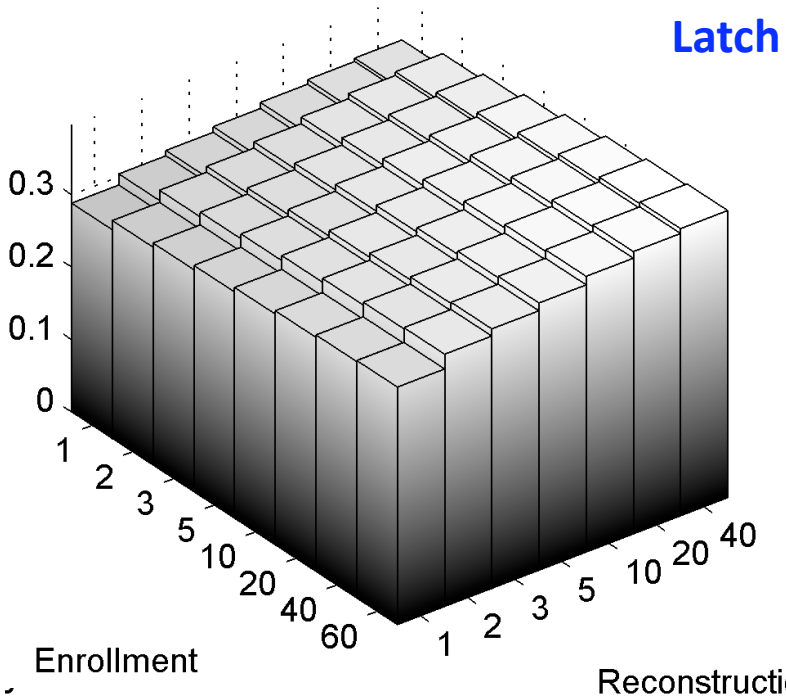
Mutual information per cell

Increasing function of k and ℓ.




DFF
0.4
0.3
0.2
0.1
0
1
2
3
5
10
20
40
60
Enrollment
1
2
3
5
10
20
40
Reconstruction +85


Buskeeper
0.6
0.4
0.2
0
1
2
3
5
10
20
40
60
Enrollment
1
2
3
5
10
20
40
Reconstruction +85


Latch
0.3
0.2
0.1
0
1
2
3
5
10
20
40
60
Enrollment
1
2
3
5
10
20
40
Reconstruction +85

Usable entropy per mm^2

PUF type	Area (mm^2)	Cells/ mm^2	Minimum #bits/mm^2		
			k=1, ℓ=1	k=60, ℓ=1	k=60, ℓ=40
SRAM	0.213	$\approx$ 1.2M	0.75M	0.95M	1.3M
DFF	0.392	$\approx$ 84k	28k	32k	37k
Latch	0.272	$\approx$ 0.12M	22k	25k	29k
Buskeeper	0.076	$\approx$ 0.22M	91k	0.11M	0.14M

Discussion

- Model for mem-like PUFs:
  "PUF = bias vector"
- Mutual information $\mathrm{I}(\mathbf{X};\mathbf{Y})$
  - uniqueness
  - noise
  - upper bound on #(robust&unique bits)
- Numerics
  - curse of dimensionality
  - we ignored correlations ← *Future work*
  - data from UNIQUE project
  - (k>1, ℓ>1) yields improvement even for small k,ℓ
  - SRAM PUF has best results

Dagstuhl 2009 correspondence

Boris:

None of this is rocket science, and the results are far from spectacular ... so I will not complain if you don't put any of this in the schedule.

Ahmad:

(...) And we do not need rocket science.
By the way, rocket science is very easy, this is a fairy-tale that rocket science is difficult. You buy some explosive powder and some metal container and you put them together.