Industry 4.0 Security Trust Anchors: Considering Supply Voltage Effects on SRAM-PUF Reliability

Pascal Ahr, Julian Dreyer, Marvin Reski, Christoph Lipps, Ralf Tönjes and Hans Dieter Schotten

27. ITG Fachtagung Mobilkommunikation
Osnabrück
11 Mai 2023

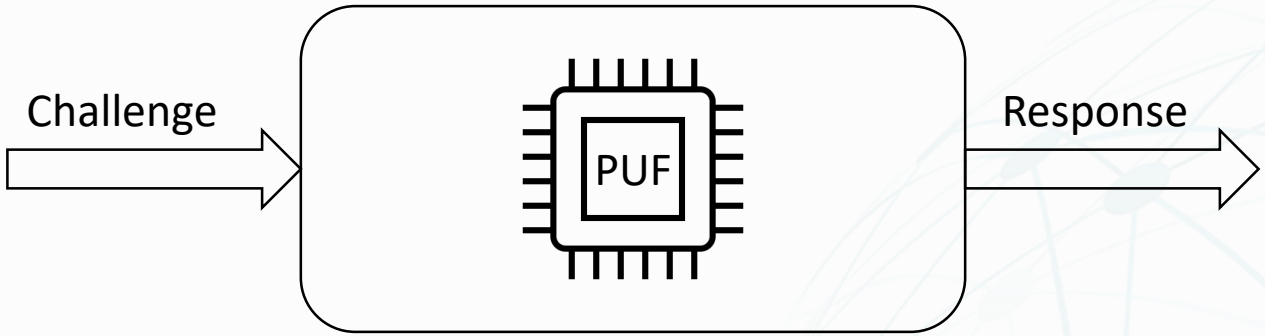
HOCHSCHULE OSNABRÜCK
UNIVERSITY OF APPLIED SCIENCES

Industrial Internet Of Things

- Intelligent networking of Machines and processes in industry
- Linking Big Data and the Internet of Things
- Internet as the core technology
- Sensible Data
- Things as small, energy-limited actors
- Industrial environment with different conditions

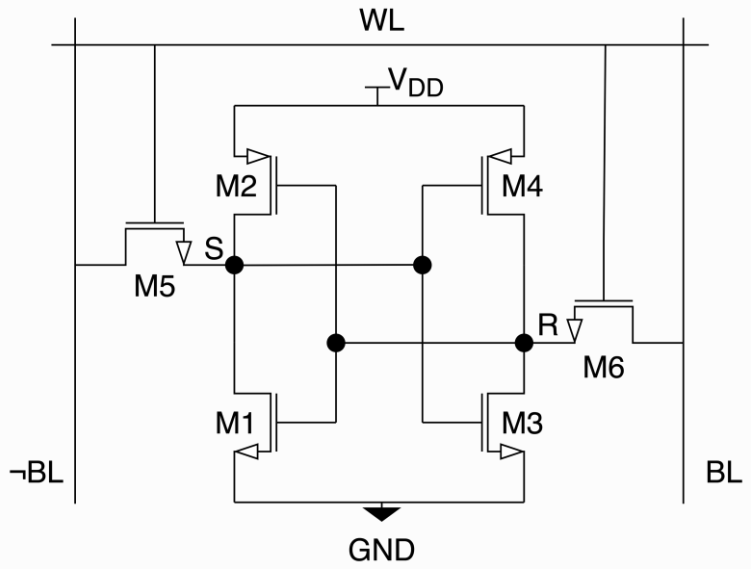
Physically Unclonable Function

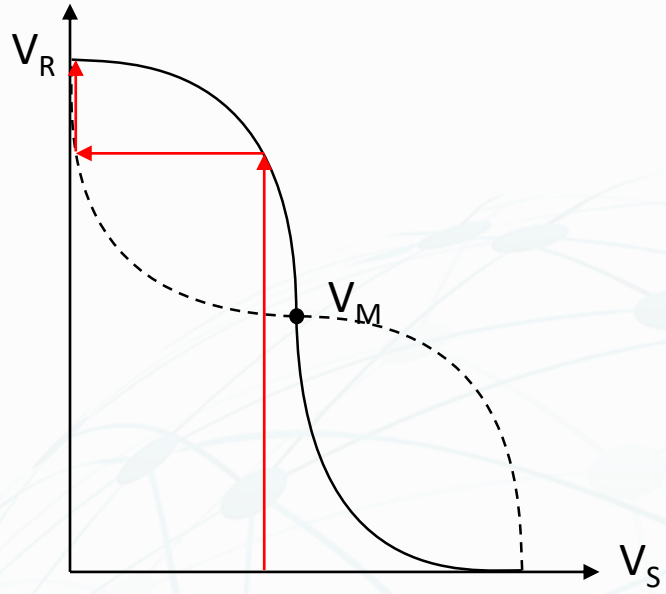
„[...] physical entity whose behaviour is a function of its structure and the intrinsic variation of its manufacturing process“
-Basel Halak-



- No need to store keys
- Lightweight
- Technical Fingerprint

Static Random Access Memory

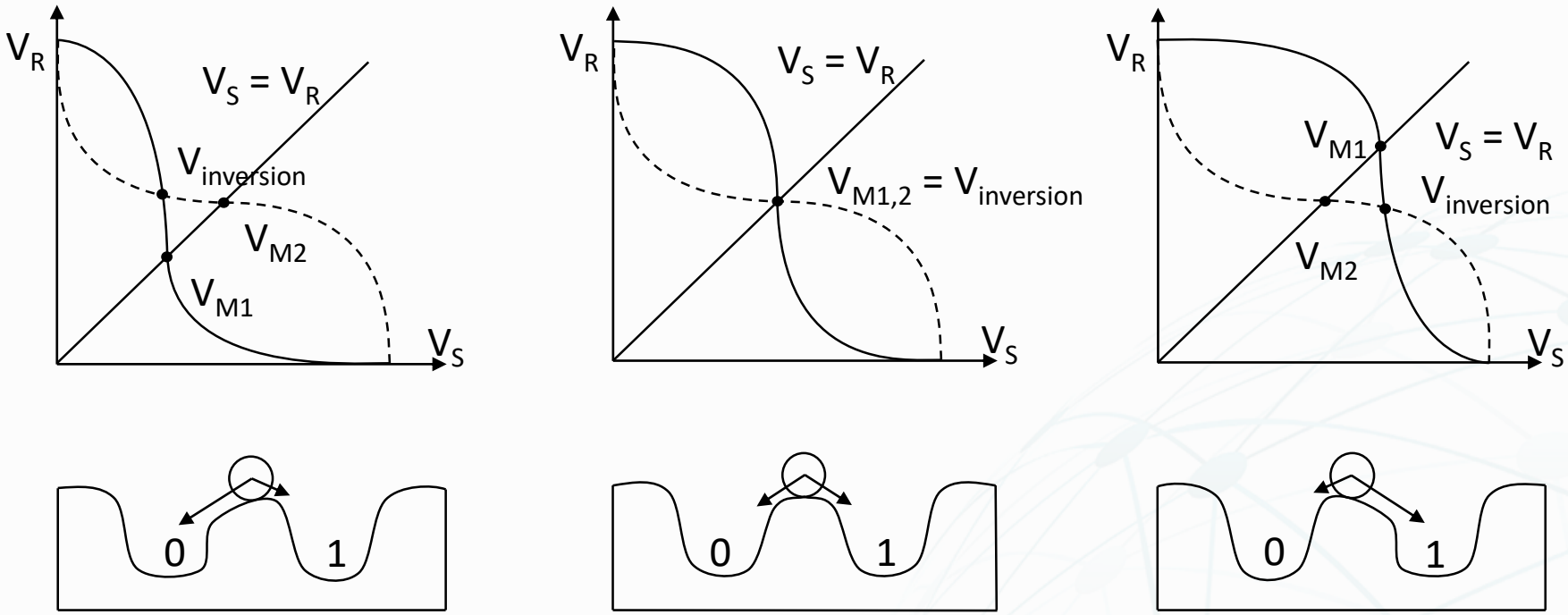




- Volatile memory
- Included in almost every µC
- CMOS Technology
  → Power loss ∝ frequency

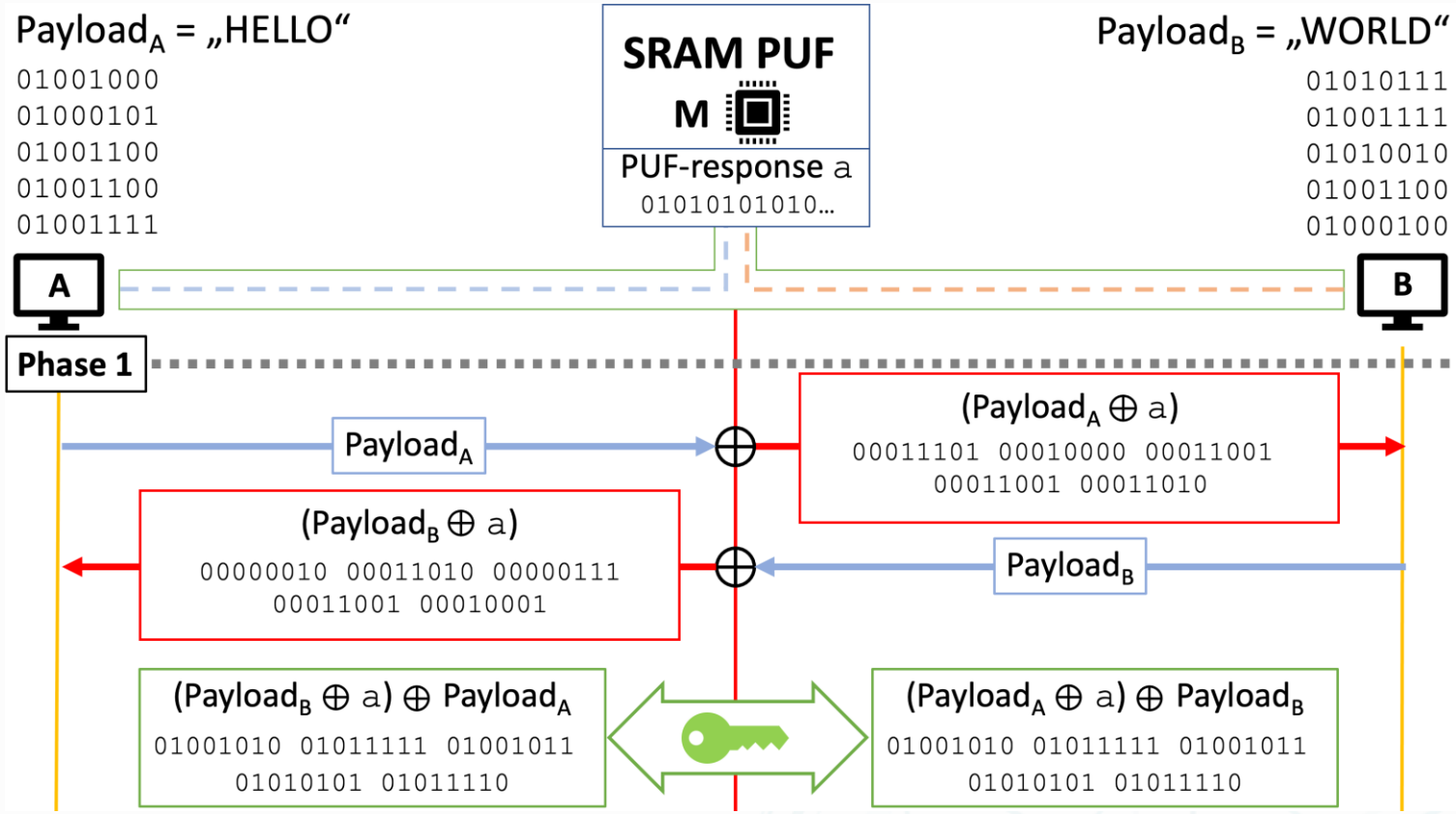
- Every cell stores one Bit
- 2 coupled inverter
- Bistable system

SRAM PUF

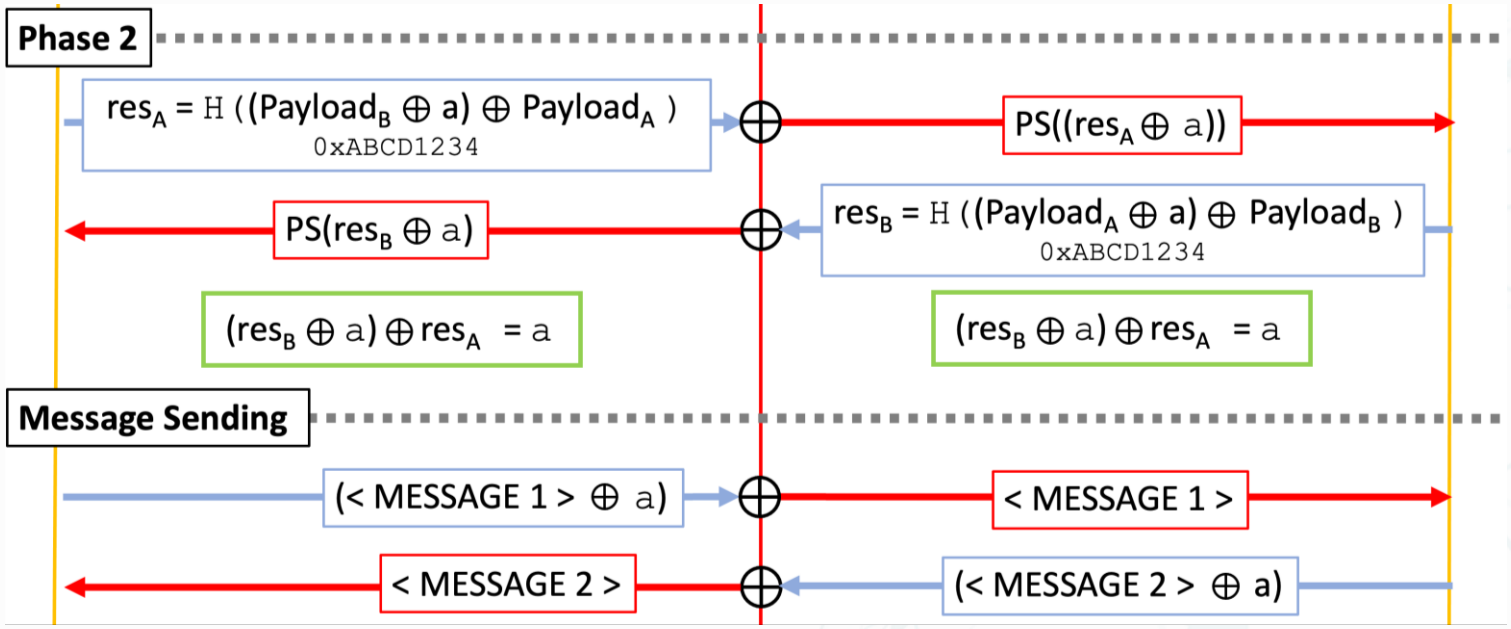


- Inverter are production related not identical
  → $V_{inversion} \neq V_M$
- Startup-Value is probabilistic
- „strongest“ inverter defines the state
- The further $V_{inversion}$ is removed form the bisecting angle the stronger the preference is

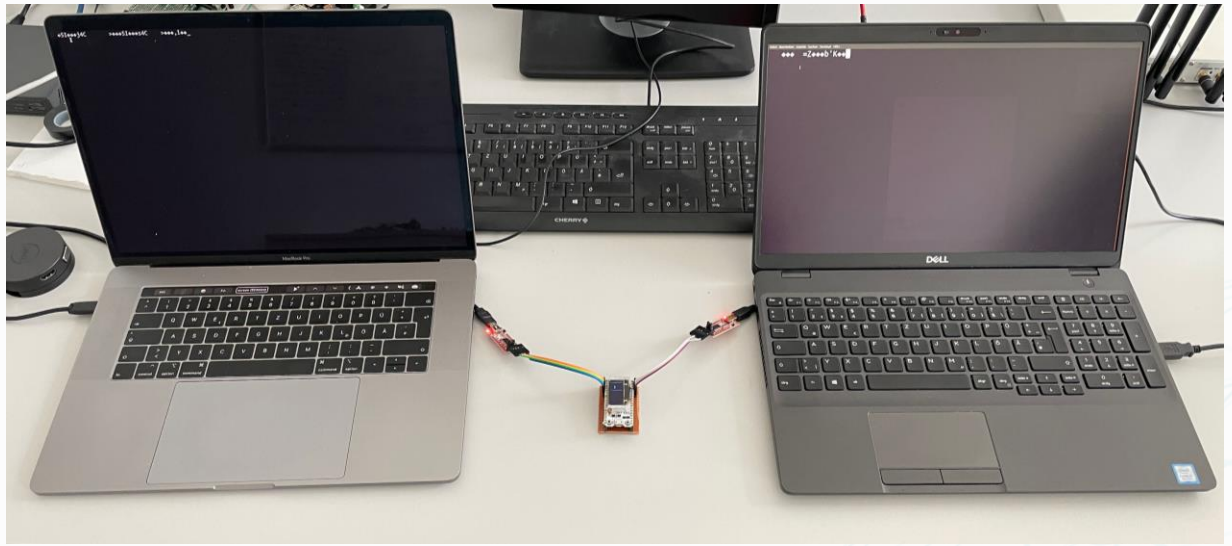
Wired Communication Scheme

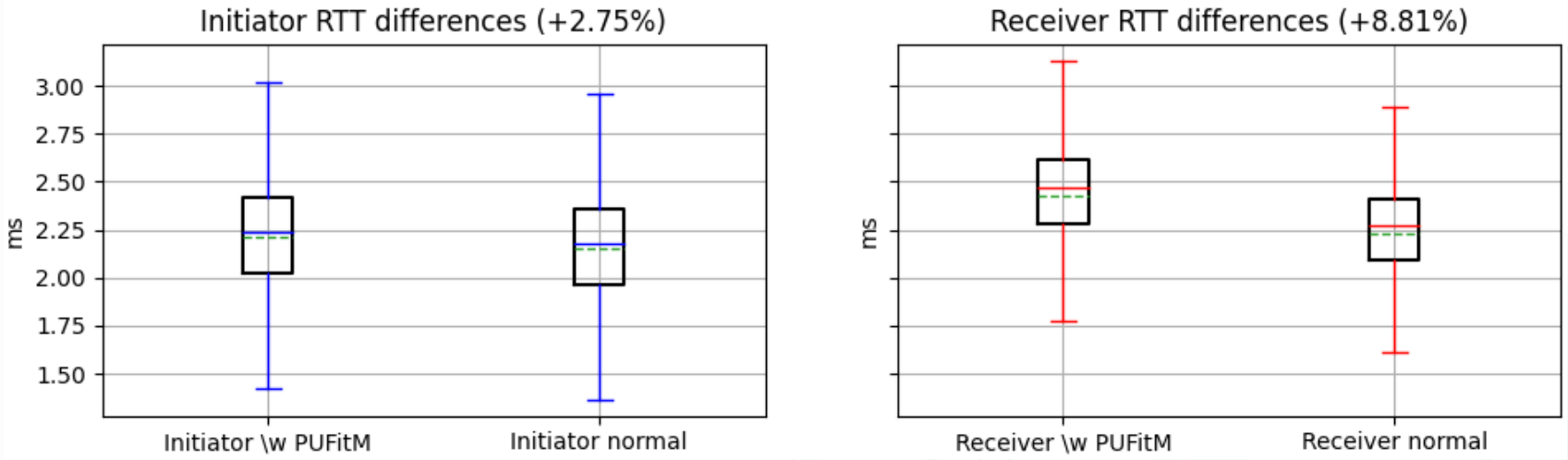


Wired Communication Scheme cont.

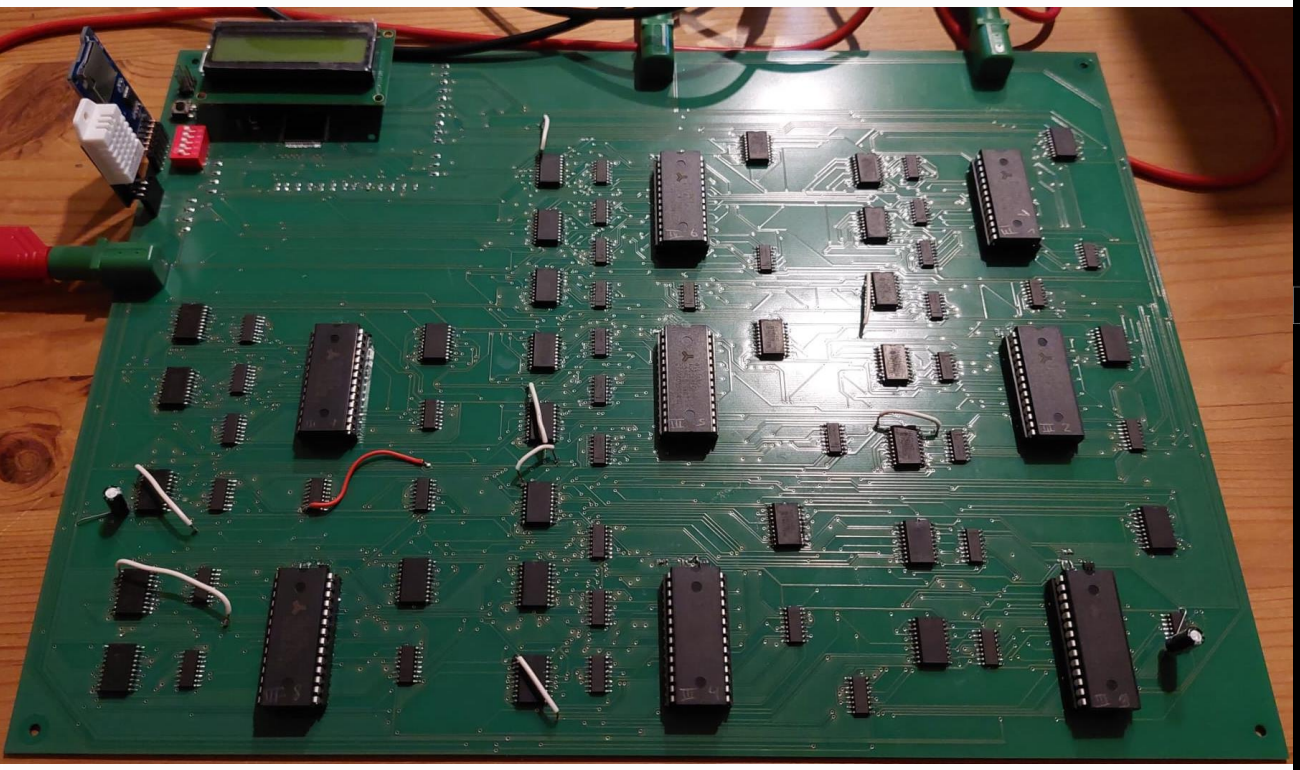


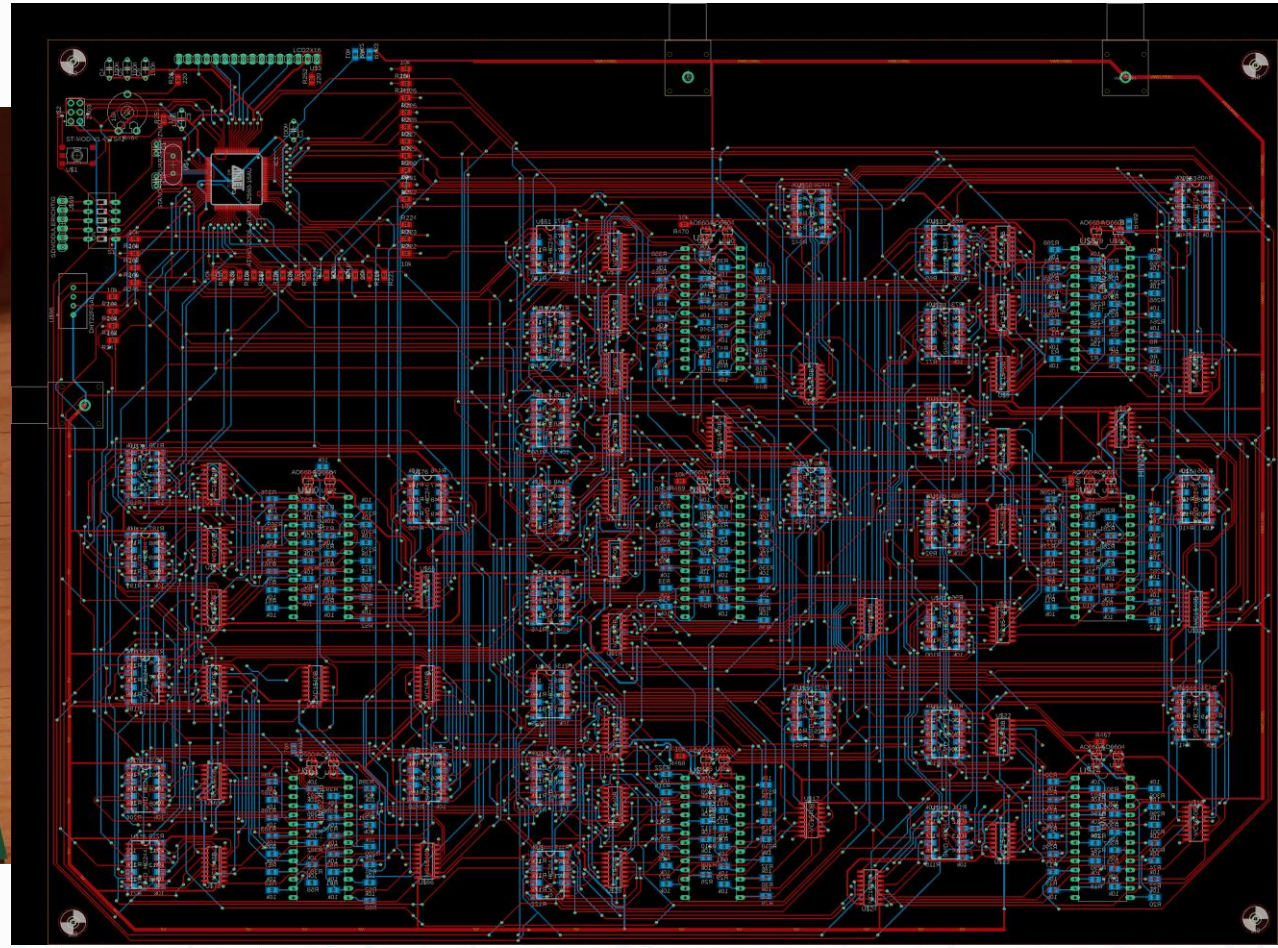
Experimental Setup





Supply Voltage Evaluation Platform



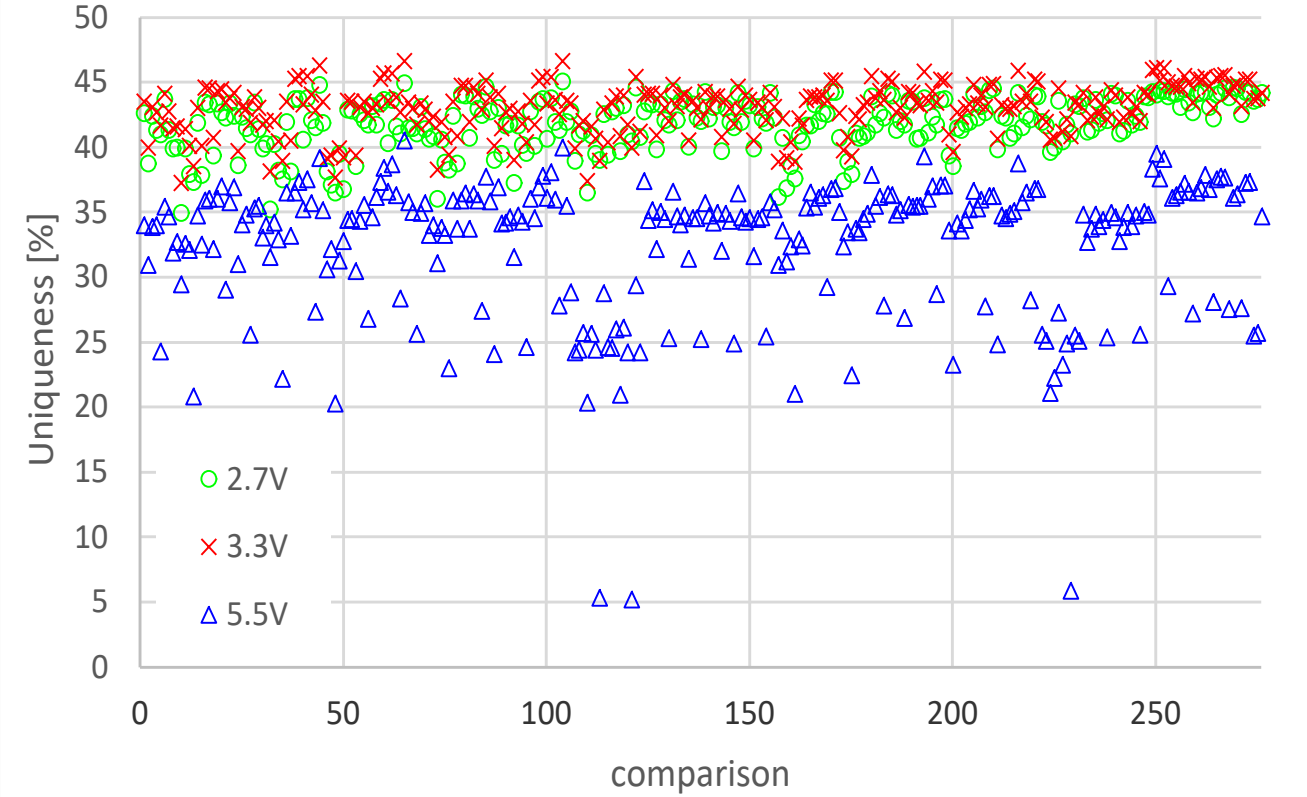


Uniqueness

$$\mathrm{HD}_{\mathrm{inter}} = \frac{2}{k \cdot (k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{\mathrm{HD}\left(R_i(n), R_j(n)\right)}{n} \cdot 100\%$$

- k: number of chips
- $R(n)$: n bit response
- HD: Hamming distance

- Best Value 50%



2.7V	3.3V	5.5V
41.81%	42.96%	32.56%

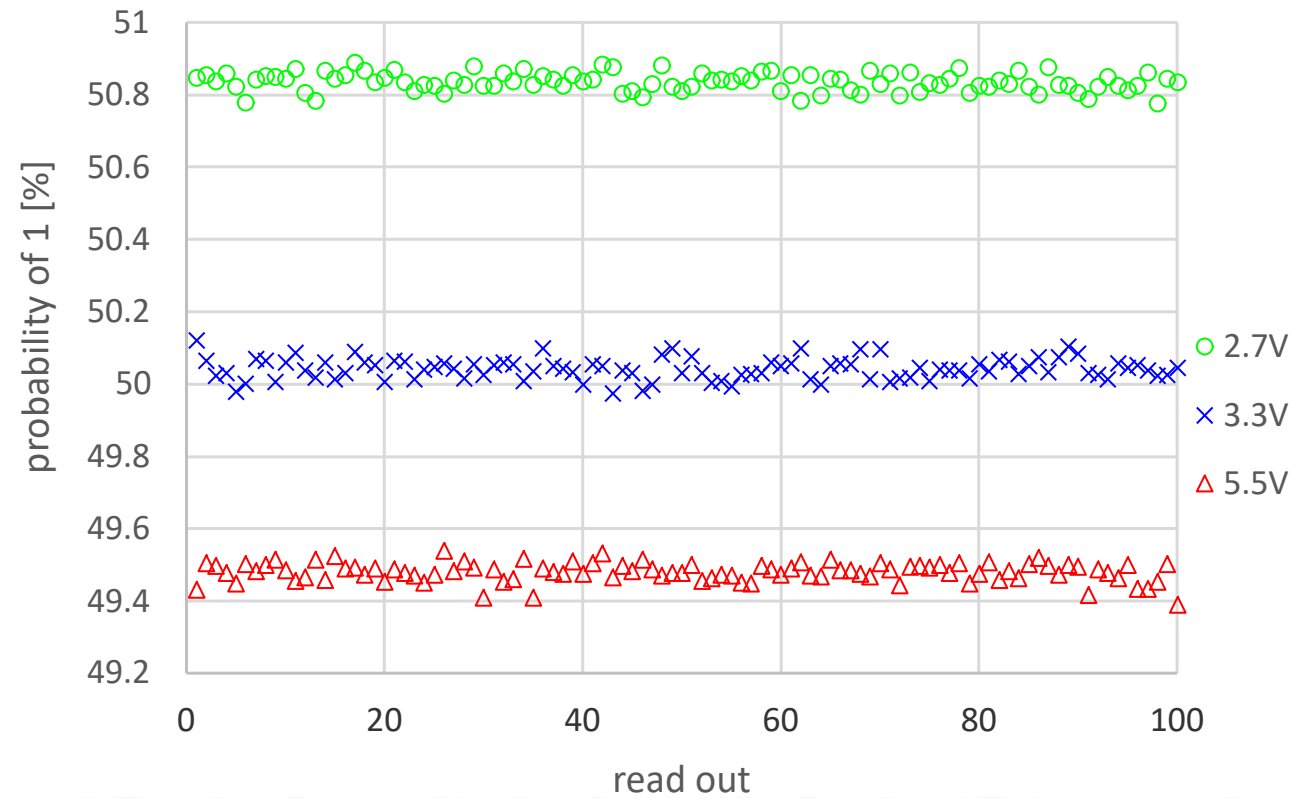
Uniformity

$$\text{Uniformity} = \frac{1}{k}\sum_{i=1}^{k} r_i \cdot 100\%$$

- k: number of responses of same chip
- r_i: Hamming Weight of response

- Best Value 50%

2.7V	3.3V	5.5V
49.95%	49.3%	48.84%



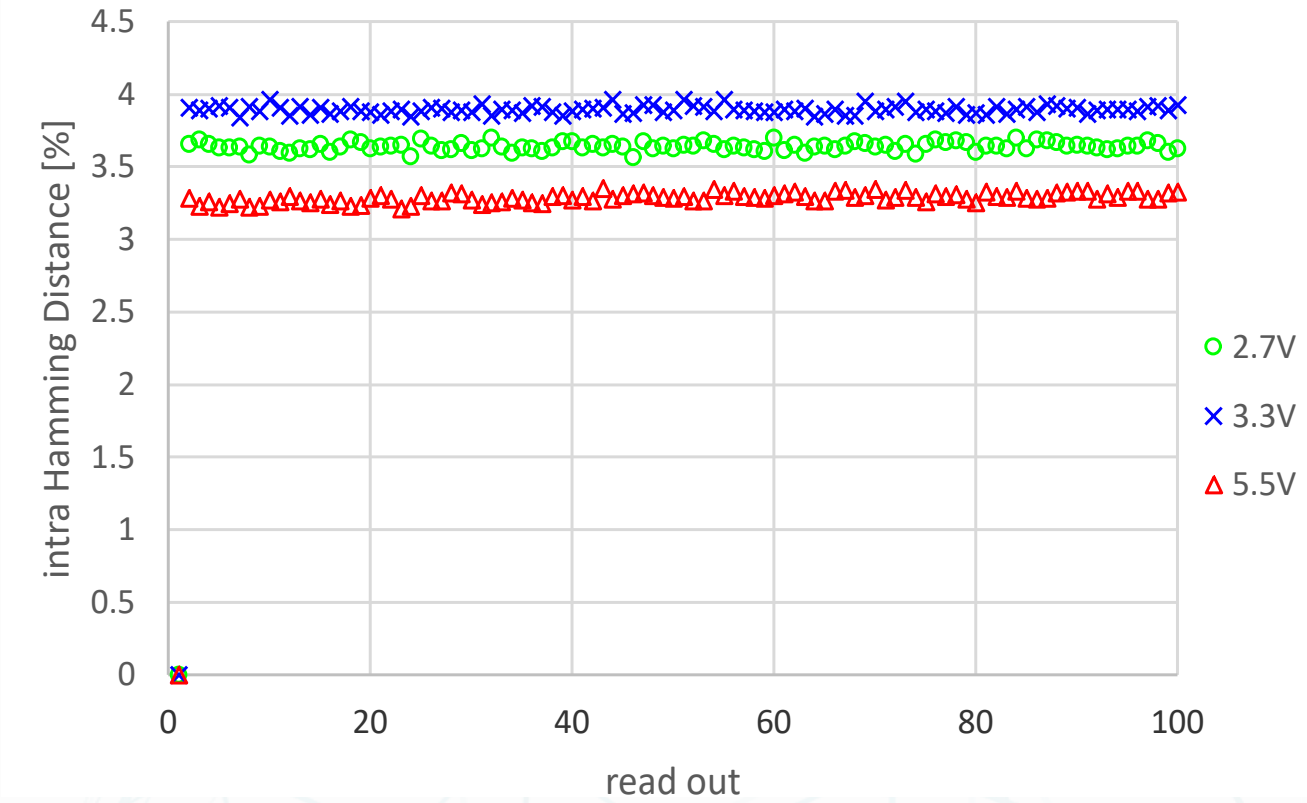
Reliability

$$100\% - \mathrm{HD}_{\mathrm{intra}} = \frac{1}{k}\sum_{i=1}^{k}\frac{\mathrm{HD}\left(R_i(n), R_i'(n)\right)}{n} \cdot 100\%$$

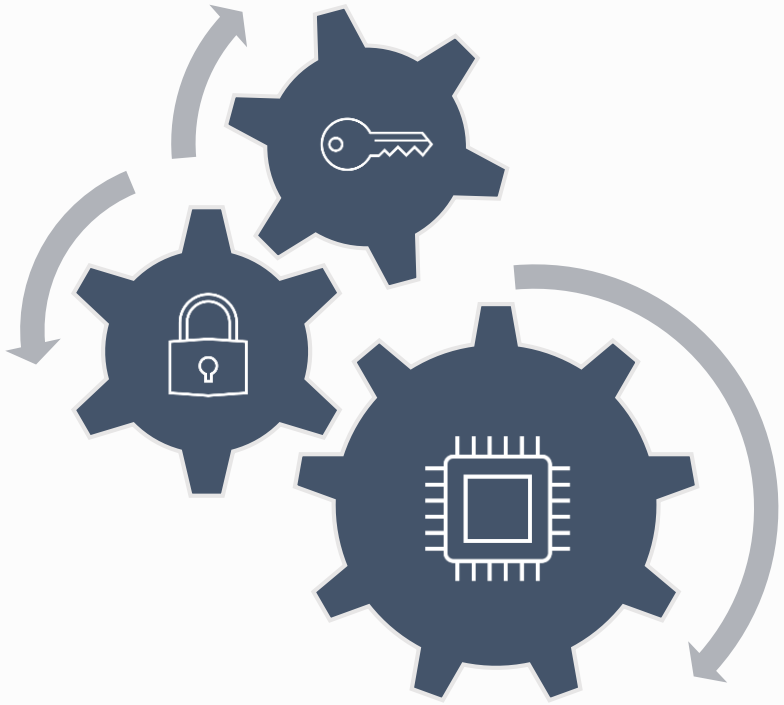
- k: number of chips
- $R(n)$: n bit response
- $R'(n)$: response at different condition
- HD: Hamming distance

- Best Value 100%

2.7V	3.3V	5.5V
96.15	96.03%	97.02%



Conclusion



- A new SRAM PUF based secure wired communication scheme
  - ➢ SRAM PUF as a source of entropy
- Successful real world implementation
  - ➢ Low overhead
- SRAM PUF is influenced by supply voltage variations
  - ➢ But still sound properties

THANK YOU

Pascal.Ahr@dfki.de

HOCHSCHULE
OSNABRÜCK
UNIVERSITY OF APPLIED SCIENCES

German
Research Center
for Artificial
Intelligence