PUFs: Myth, Fact or Busted?

A Security Evaluation of Physically Unclonable Functions Cast in Silicon

Christian Wachsmann

christian.wachsmann@trust.cased.de

TU Darmstadt / CASED, Germany

Joint work with:

Stefan Katzenbeisser, Ünal Kocabaş

TU Darmstadt / CASED, Germany

Ahmad-Reza Sadeghi

TU Darmstadt / CASED and Fraunhofer SIT Darmstadt, Germany

Vladimir Rožić, Ingrid Verbauwhede

KU Leuven, ESAT/COSIC, Leuven, Belgium

unique

www.unique-project.eu

System Security Lab | Fraunhofer SIT | Technische Universität Darmstadt | CASED

The Big Picture

Exchange of
security-critical data

Computing Device
generates, stores and processes
security-critical information

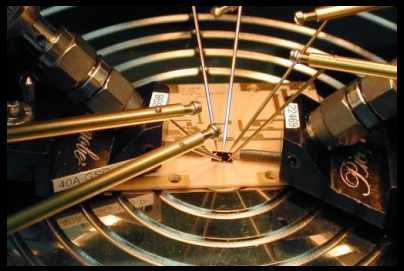
Computing Device

Cryptography can be used to protect information

Cryptography relies on secrets that must be protected on the devices

The Need for Secure Hardware

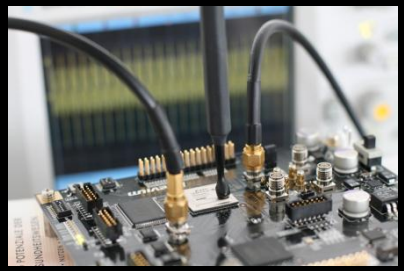
However: Cryptographic secrets can be leaked by physical attacks



Invasive Attacks

(mechanical probing, FIB, etc.)

Requires physical protection mechanisms



Side-Channel Analysis

(SPA, DPA, timing, fault injection, etc.)

Algorithmic countermeasures exist

Classic security hardware often too complex and too expensive

Promising:

Physically Unclonable Functions (PUFs)

PUF Concept

Challenge

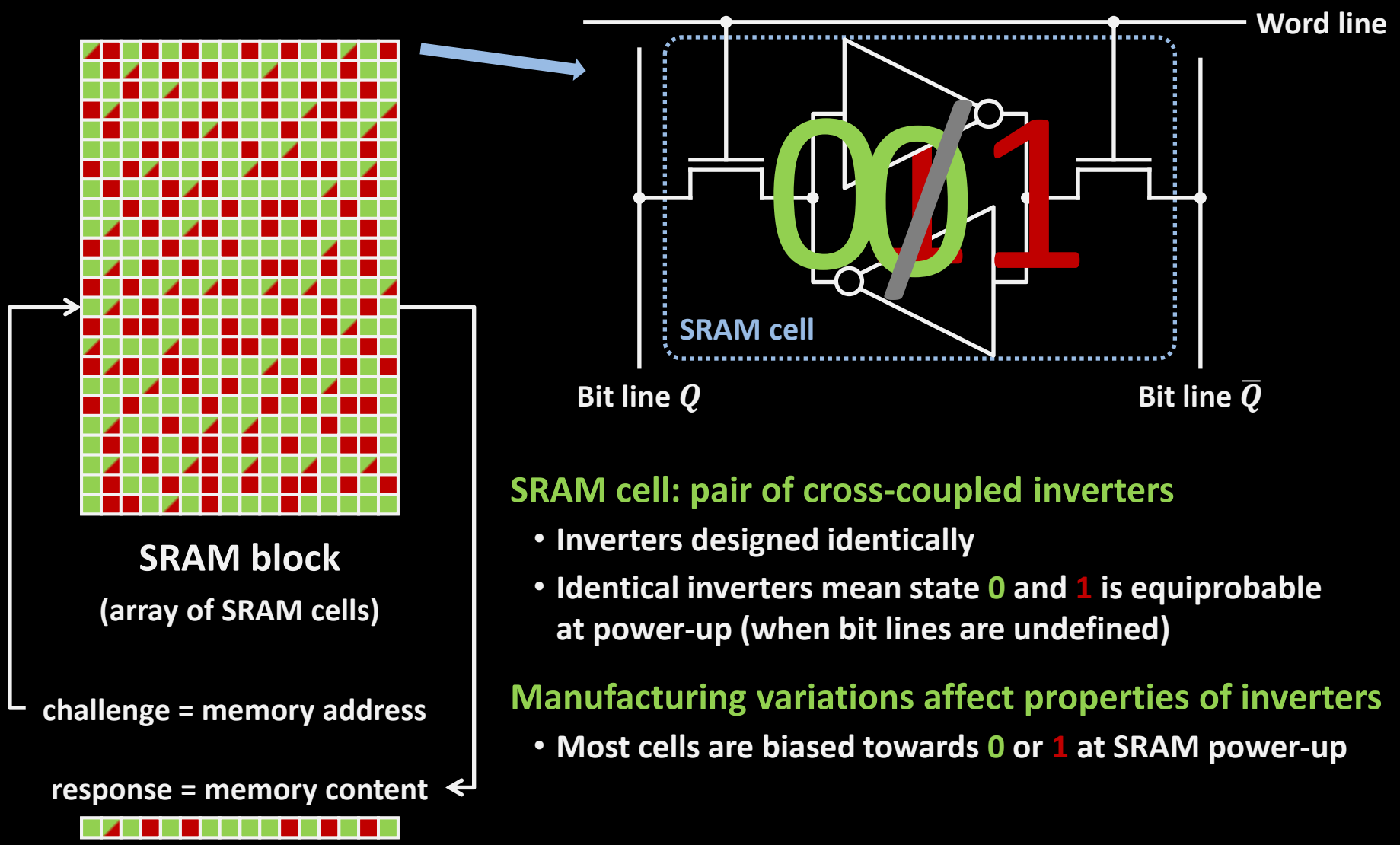
Response

Integrated circuit
(contains PUF)

Hardware Fingerprint
(unique intrinsic device identifier)

PUFs exploit random variations of manufacturing process that make each individual sample of a device unique on the physical level

Example: SRAM PUF



SRAM cell: pair of cross-coupled inverters

- Inverters designed identically
- Identical inverters mean state 0 and 1 is equiprobable at power-up (when bit lines are undefined)

Manufacturing variations affect properties of inverters

- Most cells are biased towards 0 or 1 at SRAM power-up

Common Assumptions

- **Unclonability**
  PUF is unique due to unpredictable variations of manufacturing process
- **Robustness**
  PUF always returns similar PUF responses when queried with the same challenge
- **Unpredictability**
  PUF's challenge/response behavior is pseudo-random

Fundamental for PUF-based crypto/security primitives

- **Tamper-evidence**
  Physical analysis of PUF changes its challenge/response behavior

Typical Applications

- Device identification/authentication
  (e.g., anti-counterfeiting)
- Secure key-storage
- Binding hardware and software
  (e.g., IP protection)
- Building block in cryptographic and security solutions
  (e.g., encryption/attestation)

Benefits of using PUFs

- No secure memory required

  Cryptographic secret derived from the PUF response when needed

- Intrinsic protection against invasive hardware attacks

  Physical modifications of the (PUF) circuit assumed to change device fingerprint

However:

Security properties of PUF-based solutions unclear

Gap between PUF implementations and PUF models in the literature

- Often idealized / not all properties of PUF implementations reflected
- Include security parameters that cannot be determined in practice

Existing analysis results of PUF implementations difficult to compare

- Varying test conditions (different technologies, test cases)
- Different analysis methods (theoretical, empirical, different metrics)
- Unavailability of test data sets

Our goal:

Meaningful evaluation and fair comparison of the most common PUF types in ASIC

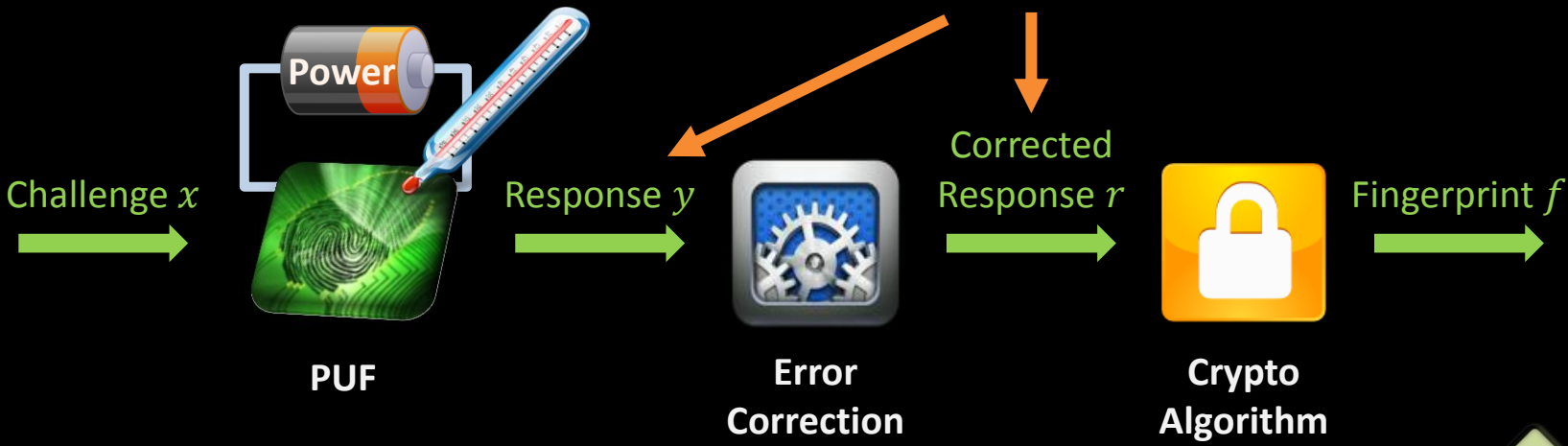
Our Contribution

- First large scale evaluation of real PUF implementations in ASIC
  96 ASICs with multiple instantiations of most common PUF types
- PUF evaluation framework for the most important PUF properties
  Empirical assessment of the robustness and unpredictability property

More Details on PUFs

Noise:
Varying operating conditions affect PUF response

Emulation Attacks:
Some PUFs can be emulated in software if large number of challenge/response pairs are known



Fundamental questions:

- How big is the impact of noise?
- How unpredictable are PUF responses when other responses are known?

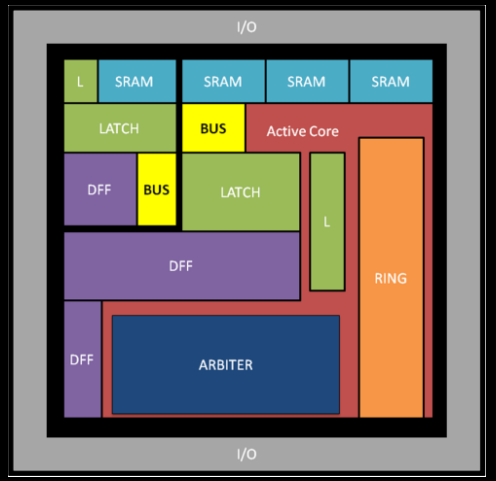
PUF ASIC and Test Setup

unique
www.unique-project.eu

UNIQUE ASIC

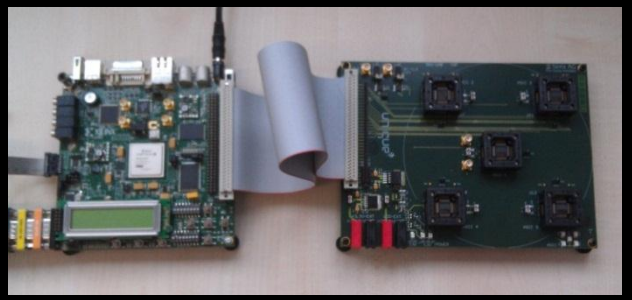
- 96 ASICs manufactured in TSMC 65 nm CMOS multi-project wafer run
- Includes 5 most common intrinsic PUFs (see table) and noise generator
- PUFs designed by our partners Intrinsic ID and KU Leuven in UNIQUE project

PUF Class	PUF Type	No. of PUF instances per ASIC
Delay-based	Arbiter	256
	Ring Oscillator	16
Memory-based	SRAM	4 (8 kB each)
	Flip-flop	4 (1 kB each)
	Latch	4 (1 kB each)



Test setup

- ASIC test board of Sirrix AG
- Xilinx Virtex 5 FPGA
- PC / Matlab (not shown)



System Security Lab | Fraunhofer SIT | Technische Universität Darmstadt | CASED

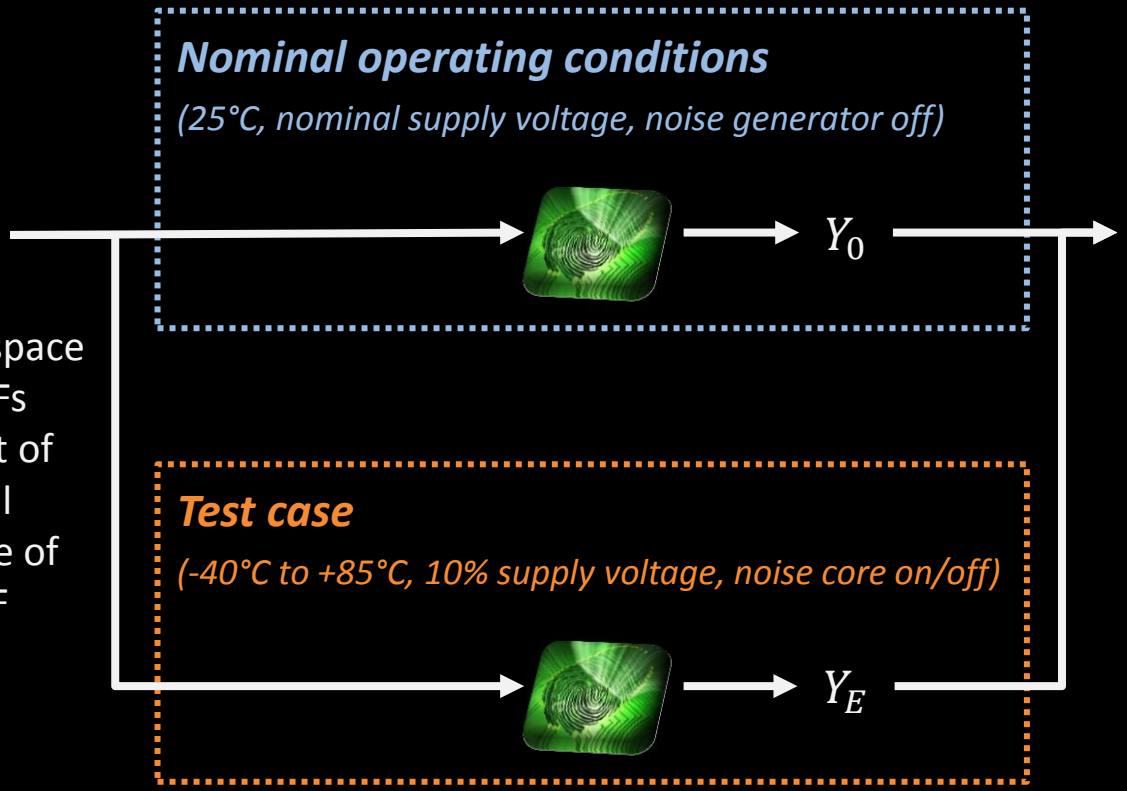
How big is the impact of noise?

Myth:

PUFs are robust to varying operating conditions.

Evaluation Strategy: Robustness

Common metric for robustness: bit error rate (BER)



- Full challenge space of memory PUFs
- Random subset of the exponential challenge space of the Arbiter PUF

Bit error rate (BER): Number of bits that are different in Y_0 and Y_E

Evaluation Results: Robustness

Test Cases

- Temperature: -40°C to +85°C
- Supply Voltage: ±10% VDD
- Noise core: On/Off

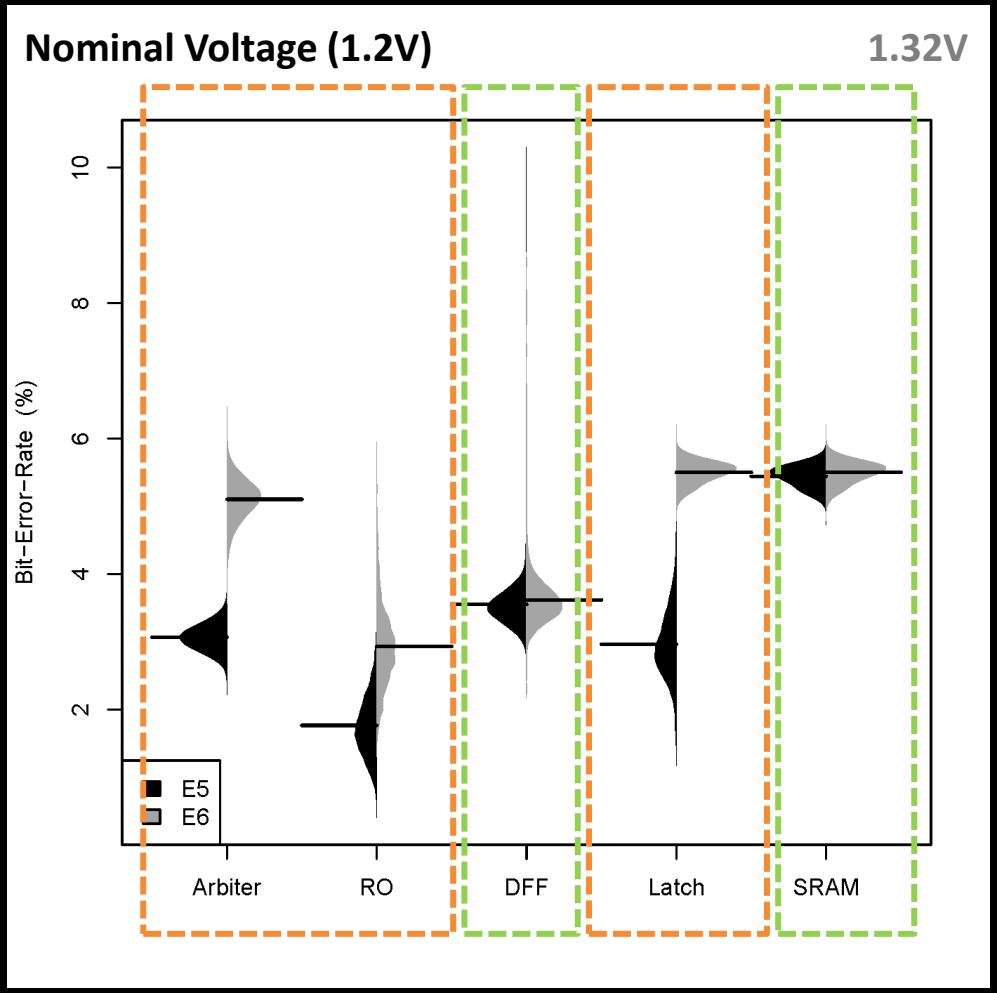
PUF-Type	Average Bit Error Rate (over all test cases)
SRAM	< 7%
Ring oscillator	< 6%
Arbiter	< 6%
Flip-Flop and Latch	< 15% BER (impractical in some applications)

Can be compensated by existing error correction schemes

Example: Voltage Variation

Arbiter PUF, Ring Oscillator (RO) and Latch PUF sensitive to supply voltage variations

Flip-Flop (DFF) and SRAM PUF not affected by supply voltage variations



See paper for graphs of other test cases.

How unpredictable are PUF responses?

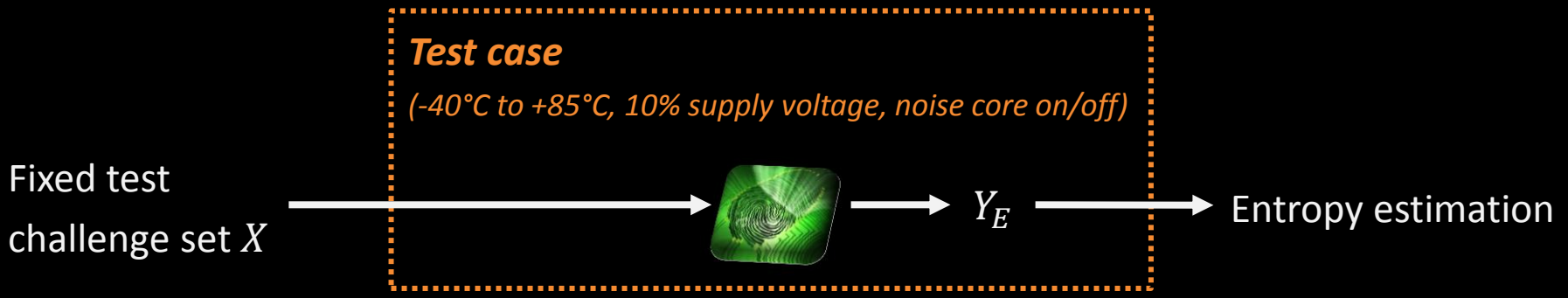
Myth:

PUFs responses can be predicted if other challenge/response pairs are known.

Depends on the PUF type.

Evaluation Strategy: Unpredictability

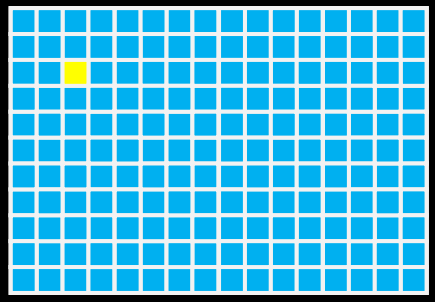
We use Shannon entropy as metric for unpredictability



We are interested in the average uncertainty in a response $Y(x)$ in case all other responses W_x are known.

That is, we are interested in the conditional entropy:

$$\boldsymbol{H}(Y|W) = -\sum_{x \in X} Pr[Y(x), W_x] \cdot \log_2 Pr[Y(x)|W_x]$$



SRAM-PUF

Computationally infeasible to determine the underlying probability distributions

Our Approach to Entropy Estimation

Observation:

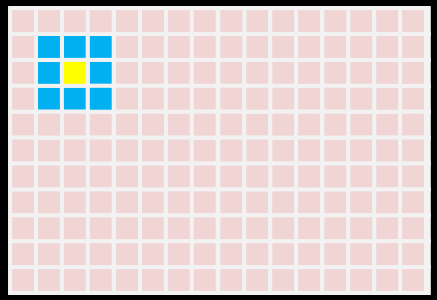
- **Typical electronic PUF structure: Array of electronic components**
  (memory cells, ring oscillators, switch blocks)
- **Common assumption: Distant components do not significantly affect each other**
  ⇒ Entropy estimation only considers responses from neighboring components

Hence, we estimate $\boldsymbol{H}(Y|W)$ with:

$$\boldsymbol{H}(Y|W') = -\sum_{x \in X} Pr[Y(x), W_x'] \cdot \log_2 Pr[Y(x)|W_x']$$

Further, we estimate the corresponding conditional min-entropy:

$$\boldsymbol{H}_\infty(Y|W') = -\log_2 \max_{x \in X}\{Pr[Y(x)|W_x']\}$$



SRAM-PUF

Similar assumptions hold for Flip-Flop, Latch, Ring Oscillator and Arbiter PUFs

Evaluation Results: Unpredictability

Test Cases

- Temperature: -40°C to +85°C
- Supply Voltage: ±10% VDD
- Noise core: On/Off

PUF-Type	Unpredictability
SRAM	Entropy and min-entropy > 80% (almost ideal)
Ring oscillator	Entropy ≈75%; min-entropy < 2% (too low for some applications)
Arbiter	Entropy and min-entropy < 1% (far too low; model building possible)
Flip-Flop and Latch	Strongly dependent on temperature (may enable attacks)

PUF must be carefully chosen
depending on the requirements of the underlying use case

Conclusion and Future Work

We presented

- First large-scale evaluation of real PUF implementations in ASIC
- PUF evaluation framework for the robustness and unpredictability properties

Current and future work

- Extension of the evaluation framework
  - More test cases (e.g., aging tests)
  - Other PUF properties (e.g., tamper-evidence, unclonability)
- Analysis of other PUF types

unique
www.unique-project.eu

Thank you!

Christian Wachsmann

christian.wachsmann@trust.cased.de

unique

www.unique-project.eu

System Security Lab

Fraunhofer SIT

TECHNISCHE UNIVERSITÄT DARMSTADT

CASED