Leakage Sources of the ICLooPUF: Analysis of a Side-Channel Protected Oscillator-Based PUF

COSADE 2024

Niklas Stein
Michael Pehl

Technical University of Munich

Lehrstuhl für Sicherheit
in der Informationstechnik

Physical Unclonable Functions (PUFs)

- Fingerprinting of semiconductor devices
- Threshold voltage determines gate delay
- Random unique values but slightly noisy

Depends on the distribution of dopant atoms,
unlike NVM a direct readout is not feasible

→ Side Channel Attacks are the main threat

Interleaved Challenge Loop PUF (ICLooPUF)

Challenge selects delay path

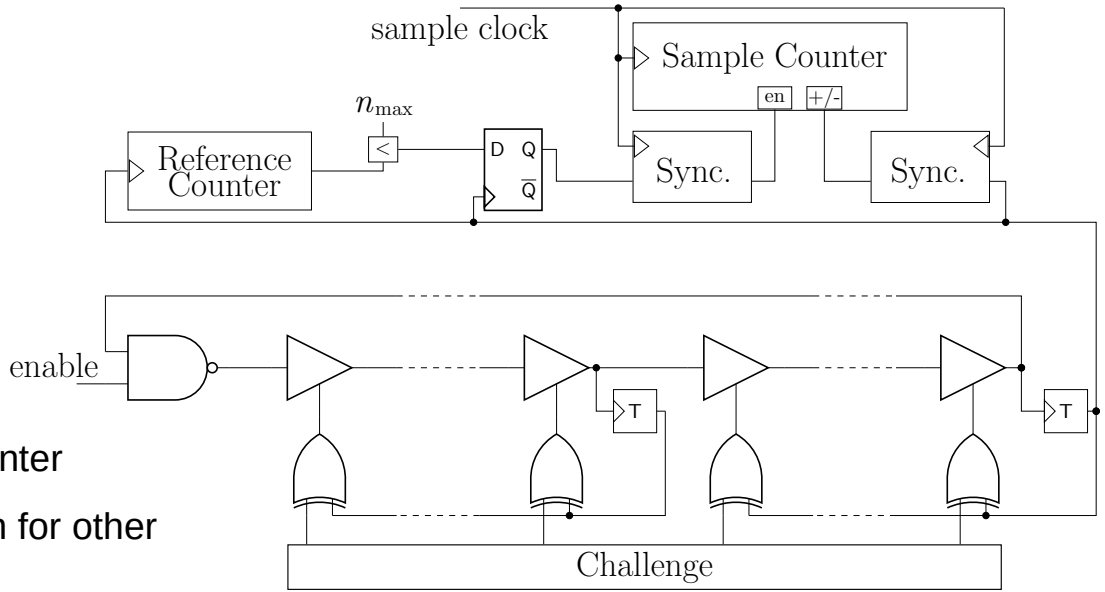
Measure delay difference of two challenges

Hot-swap challenge each oscillation

Delay difference is sampled in up/down counter

Upwards for one challenge/oscillation, down for other

→ counter difference



L. Tebelmann et al. (2022): Interleaved Challenge Loop PUF. DOI: 10.1109/TCSI.2022.3208325

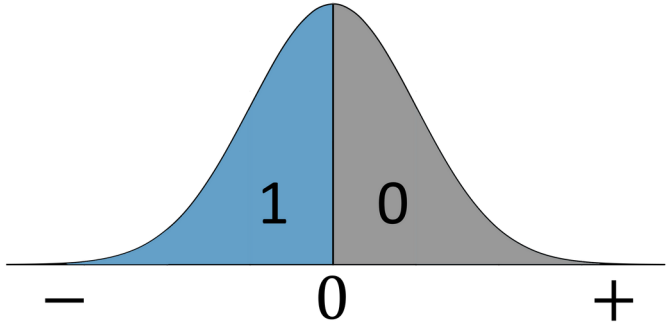
Deriving secret bits

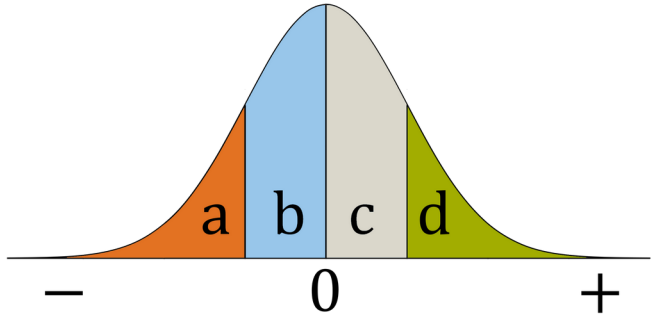
Differential counter will follow normal distribution

(A) Secret bit = sign of counter difference
Rather well to protect (shuffling)
But only one low-quality bit

(B) Higher order symbol ↔ signed magnitude
More bits or better bits (Two-metric scheme)
Absolute magnitude now also leaks

→ ICLooPUF should protect this





Contribution

ICLooPUF already proven resistant to conventional attacks:
Detect the individual frequencies and calculate difference [1][2]

But processes in the design are highly complex
→ search for possible attack vectors
→ estimate their practicability

Topics:

1. Attack on the counter
2. Improved leakage model for the ring

[1] D. Merli (2014): Attacking and Protecting Ring Oscillator Physical Unclonable Functions and Code-Offset Fuzzy Extractors
[2] L. Tebelmann, M. Wettermann, M. Pehl (2022): On-Chip Side-Channel Analysis of the Loop PUF

Setup

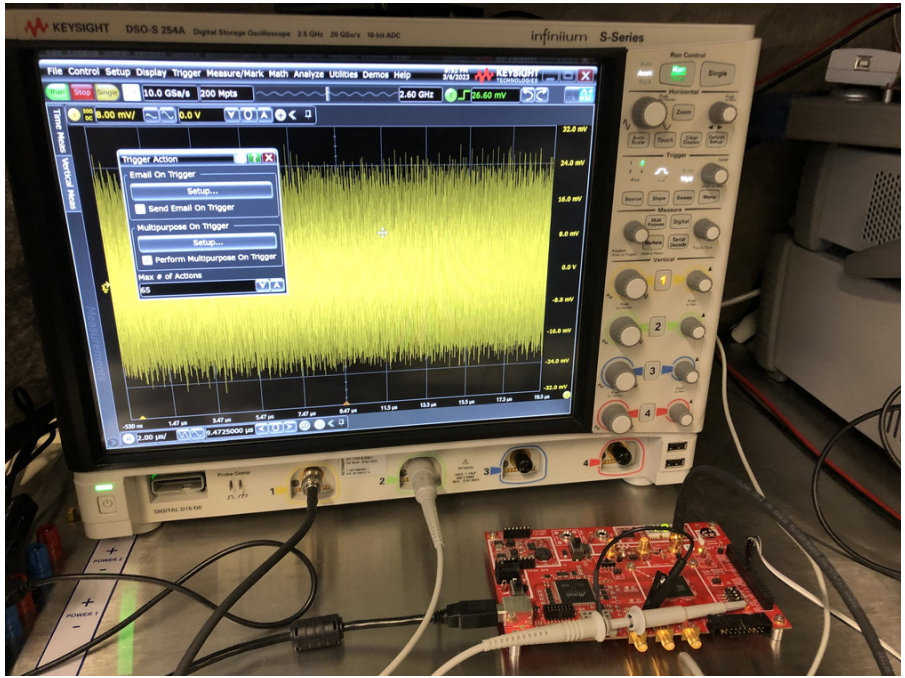
Power-SCA on FPGA target

One PUF instance with 64 bits

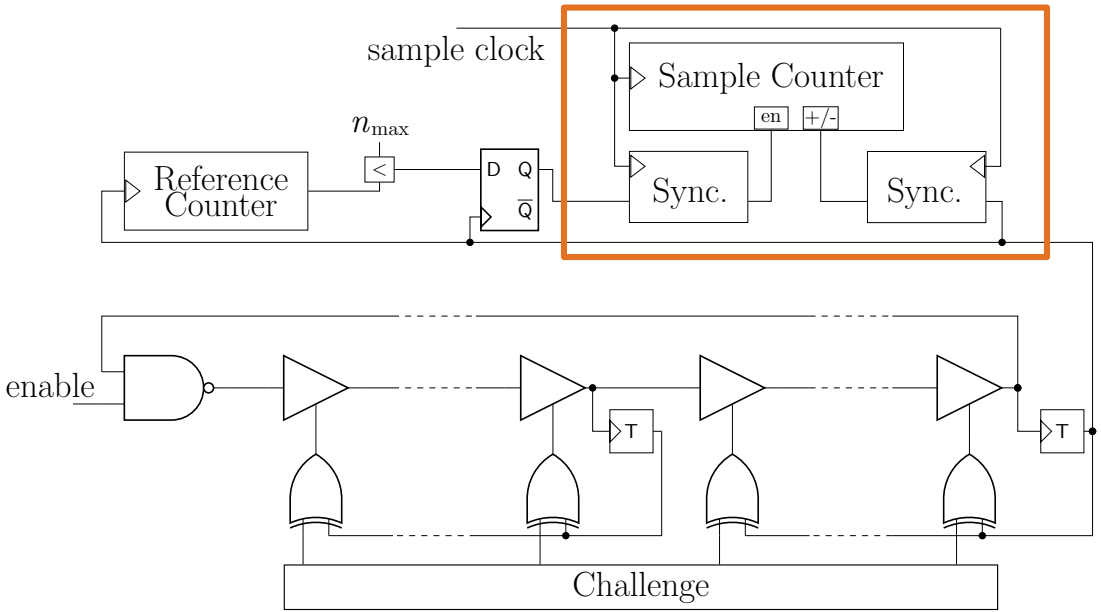
20G Samples/second, 10 bit resolution

Other functions in parallel
→ evaluation by frequency filters

Key storage scenario
→ repetition possible



Attack on the sample counter



Attack on the counter

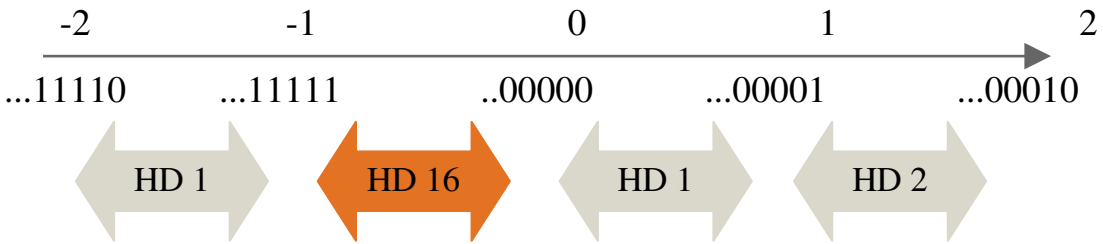
Binary up/down counter

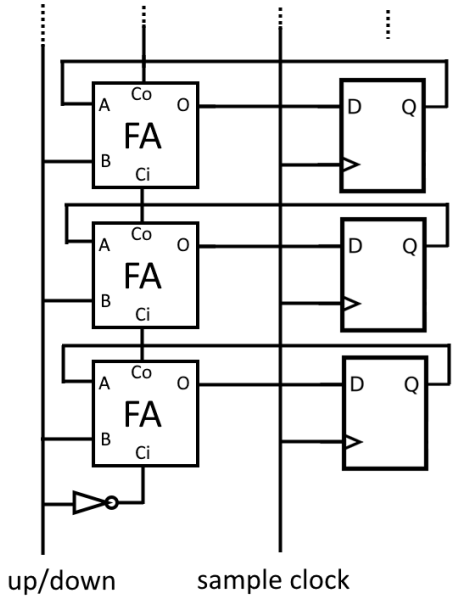
High sample frequency required

Synchronous adder with fast carry chain

Counting on 2‘s complement

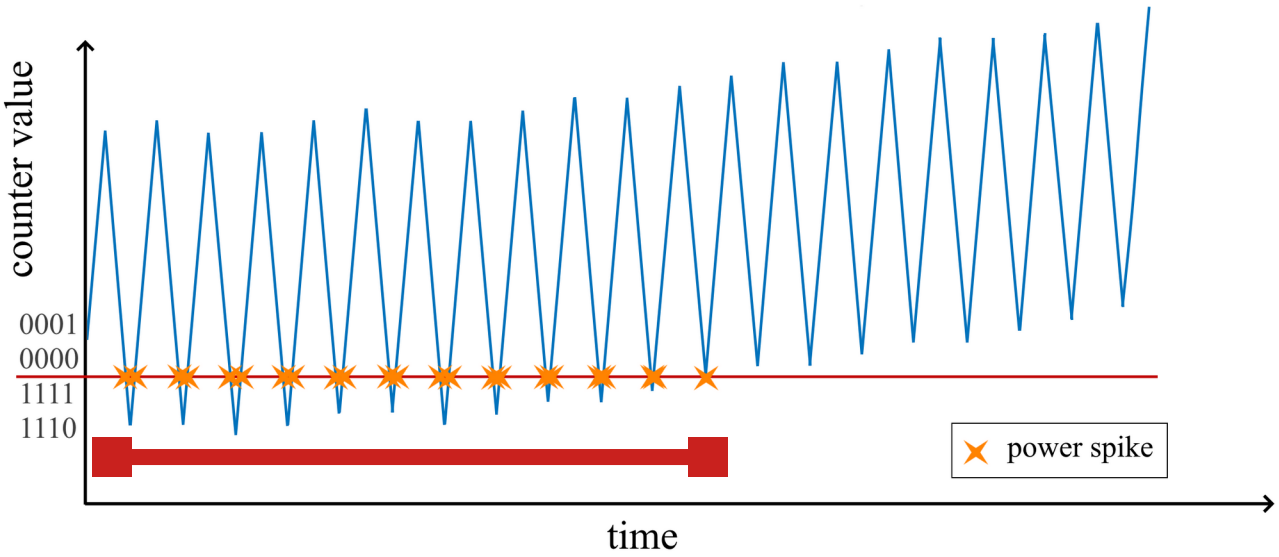
→ Hamming Distance at MSB carry-over is large





Attack on the counter

Counter Side Channel



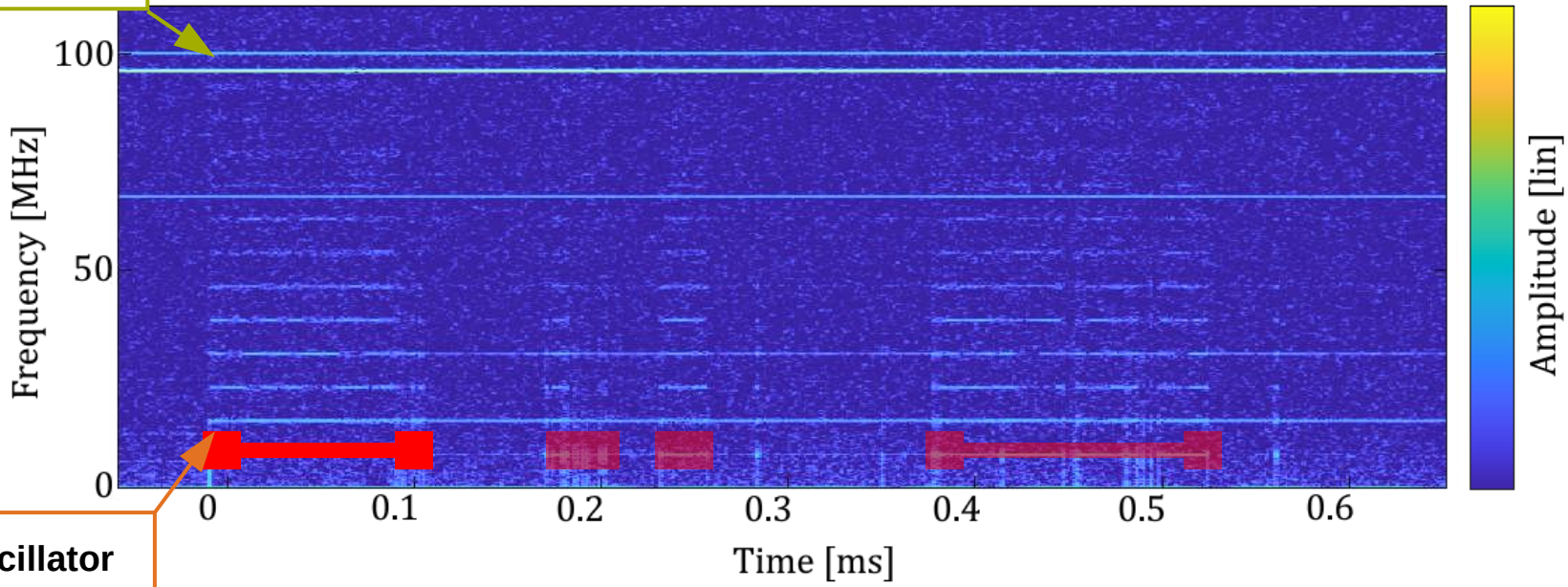
→ **Duration of this state correlates with the secret amplitude**

Attack on the counter

Counter Side Channel

System clocks

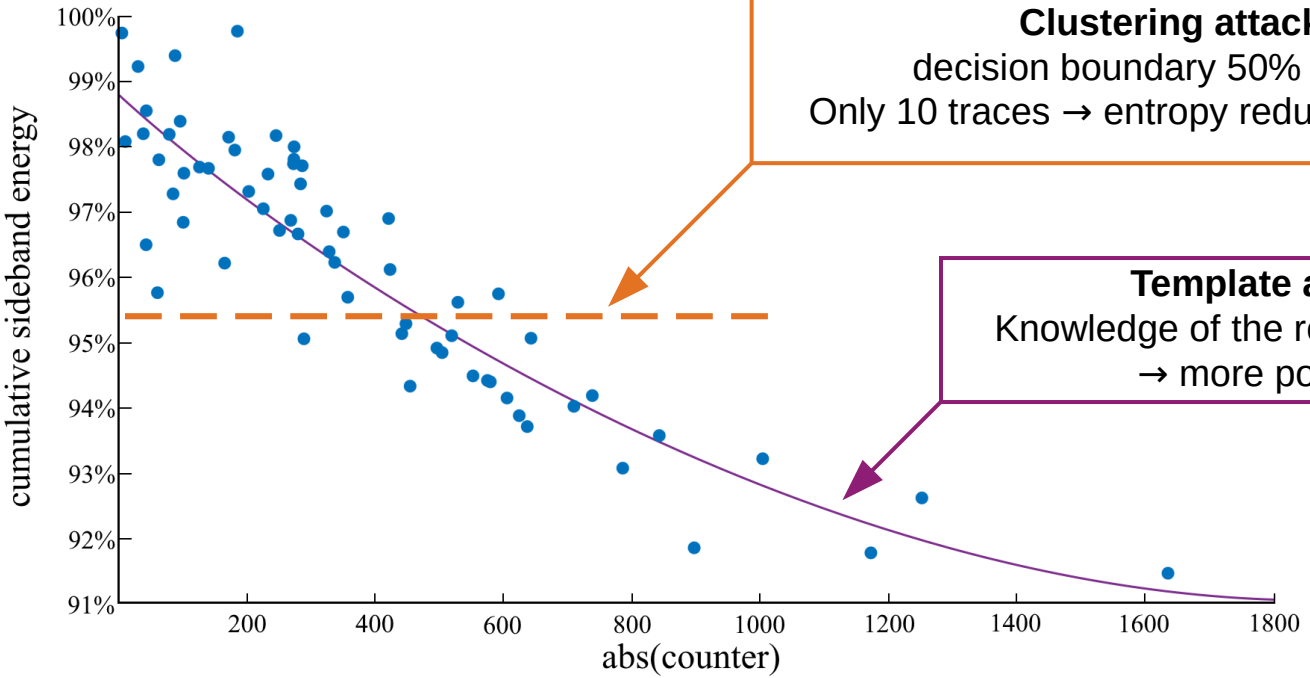
Waterfall plot (STFT) of a single trace



PUF oscillator

Attack on the counter

Counter leakage



Clustering attack:
decision boundary 50% samples
Only 10 traces → entropy reduced by 1/3 bits

Template attack:
Knowledge of the relation function
→ more powerful

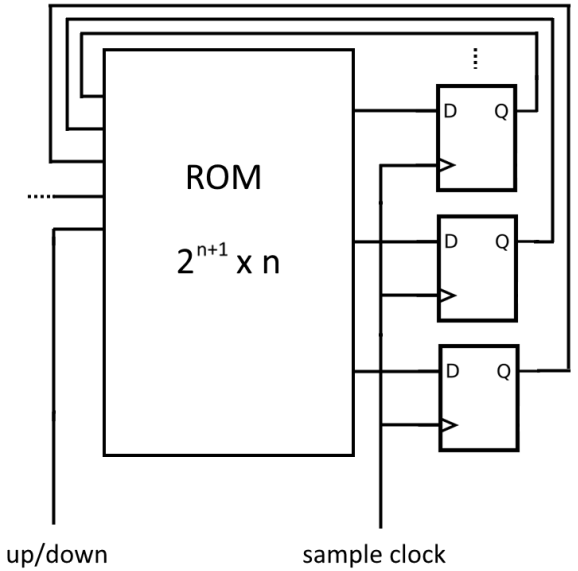
Attack on the counter

Resilient counters?

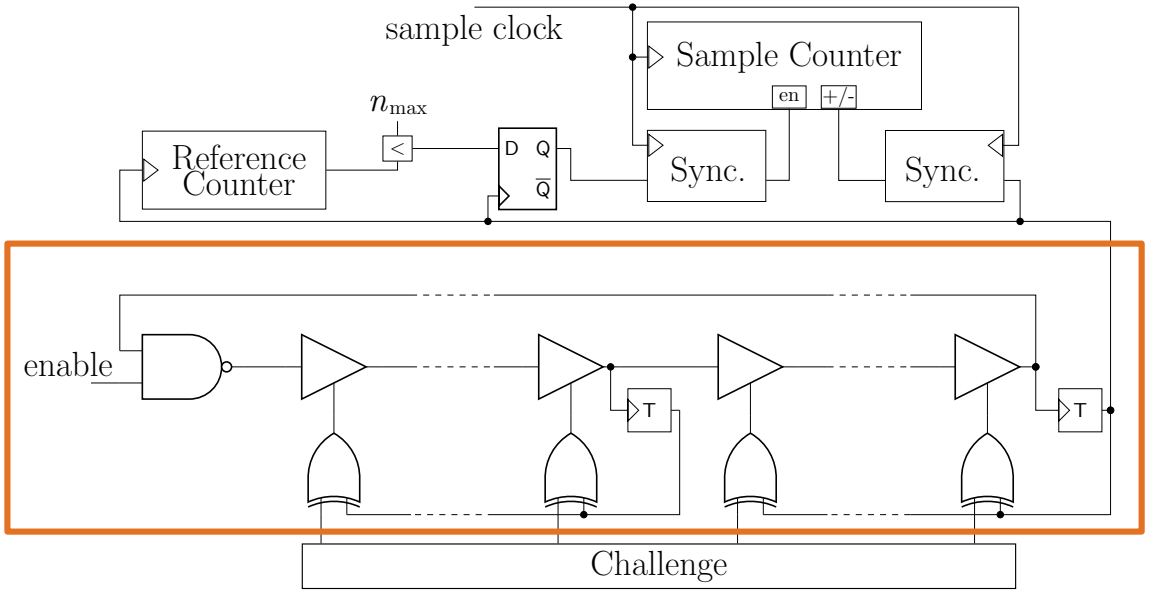
Separate counters
→ no advantage over classical PUF

Randomized starting point
→ no influence on duration

Equidistant and Gray codes
→ no (global) leakage on any transition
→ long combinatorial path or wide words
→ exponential area cost as FSM



Attack on the ring oscillator

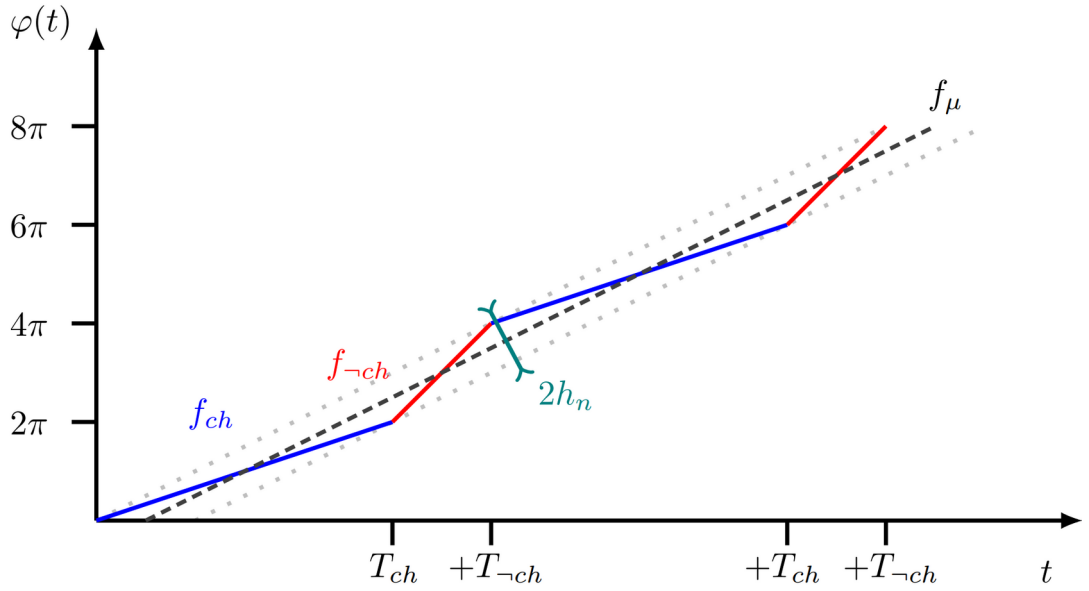


Attack on the ring

Oscillator Side Channel

Interleaving is a frequency modulation

Challenge and inverse correspond to different instantaneous frequencies



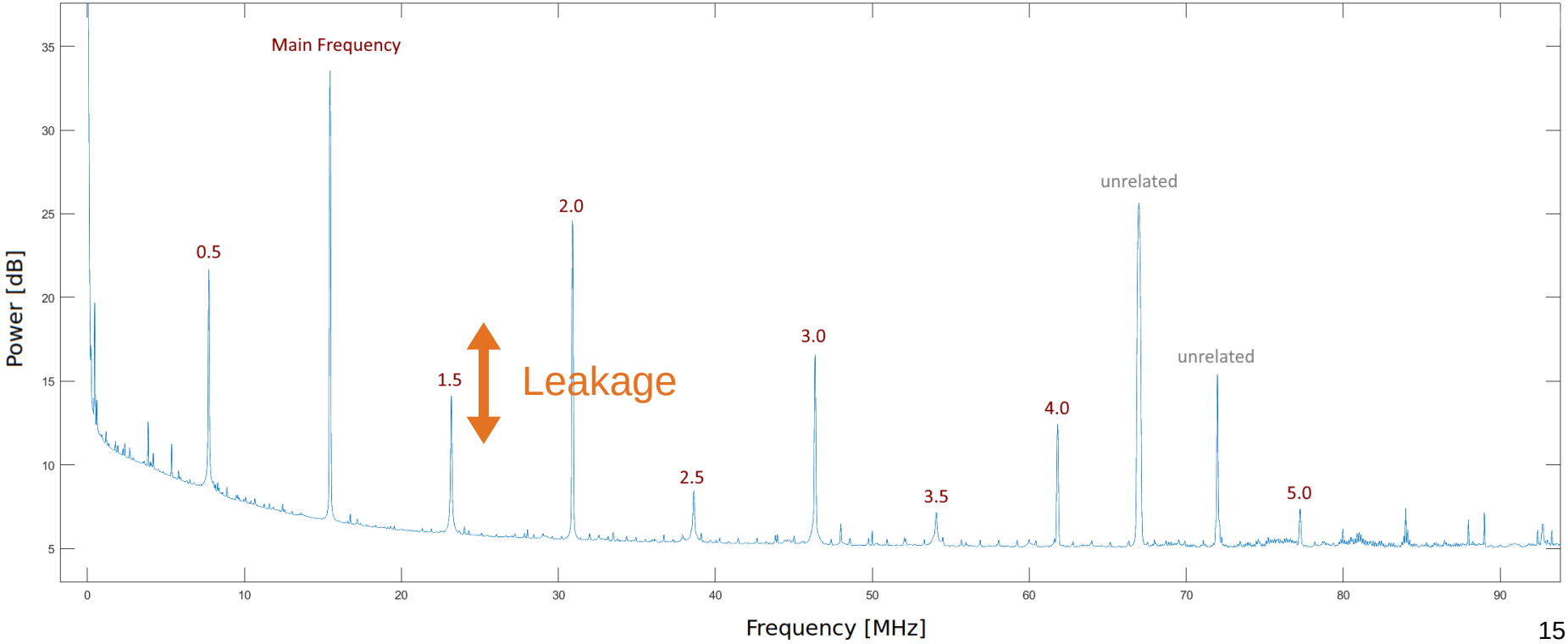
Causes side-bands in the spectrum:

Modulation coefficient ↔ power in first kind Bessel function

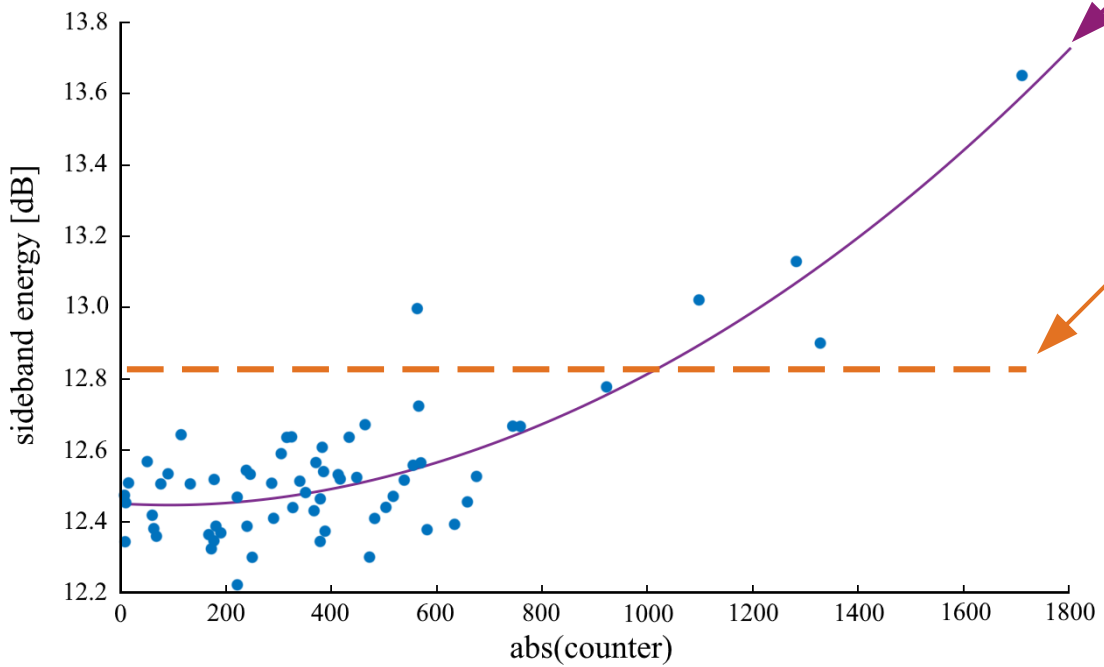
Attack on the ring

Oscillator Side Channel

Welch power spectral density estimate



Attack on the oscillator



Template attack:
Pearson correlation (lin.): **78%**
Variance too large for attack

Clustering attack:
Only few bits gained

Summary

Side-Channel resilient up/down counter for correlated data are challenging
Countermeasure has high area cost but strictly required

Oscillator also leaks amplitude directly
But extraction requires trillions of samples and high compute

→ Still orders of magnitude better than original Loop-PUF

Thank You