Side-Channel Analysis of the TERO PUF

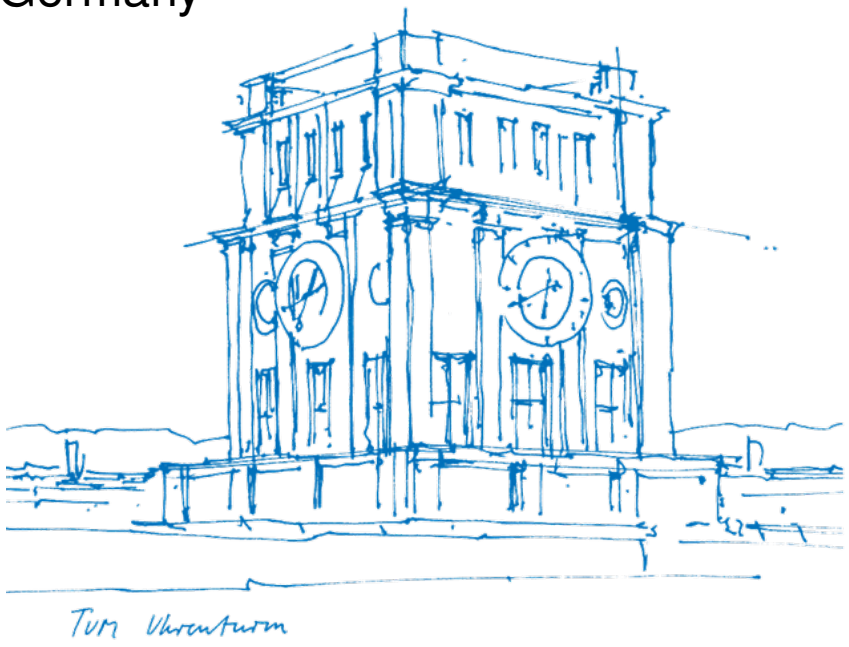
Lars Tebelmann[1] Michael Pehl[1] Vincent Immler[2]

[1]Technical University of Munich, München, Germany

[2]Fraunhofer AISEC, Garching bei München, Germany

April 4th, 2019

COSADE 2019
April 4th-5th, 2019
Darmstadt, Germany



Agenda

Physical Unclonable Functions (PUFs)

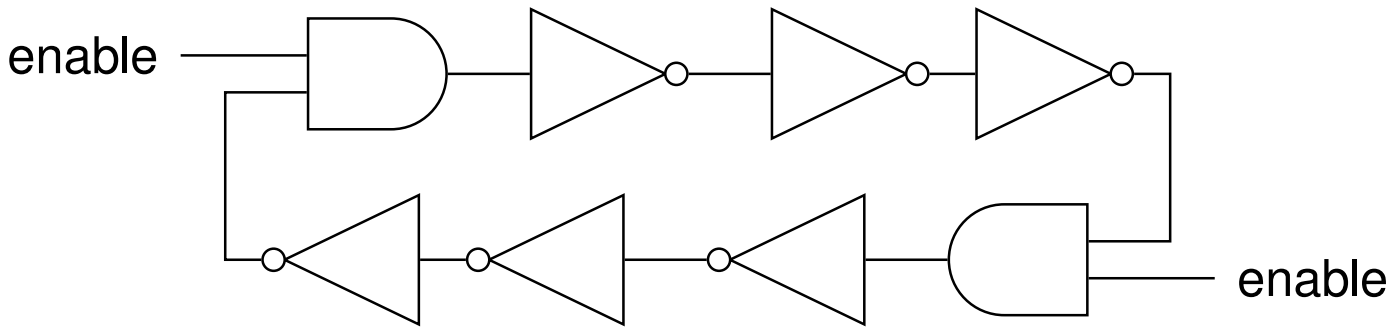
- Randomness from manufacturing variations
  - Hardware-intrinsic features
  - “Fingerprint” of a device
- Alternative for secure low-cost key storage
  - Key generation during run time
  - No key material on device after power-off

Side-Channel Analysis of PUF Primitives

- SRAM: **semi-invasive**, photon emission
  - Helfmeier et al.: *Cloning Physically Unclonable Functions*. HOST 2013
- Arbiter PUF: **semi-invasive**, photon emission
  - Tajik et al.: *Physical Characterization of Arbiter PUFs.* CHES 2014
- RO PUF: **semi-invasive**, Laser Voltage Probing
  - Lohrke et al.: *No Place to Hide: Contactless Probing of Secret Data on FPGAs*. CHES 2016
- RO PUF: **semi-invasive**, localized EM
  - Merli et al.: *Semi-invasive EM Attack on FPGA RO PUFs and Countermeasures*. WESS 2011
  - Merli et al.: *Electromagnetic Analysis of RO PUFs*. HOST 2013

In this talk: **non-invasive** attacks on TERO PUF based on EM

The Transient Effect Ring Oscillator (TERO)[1]

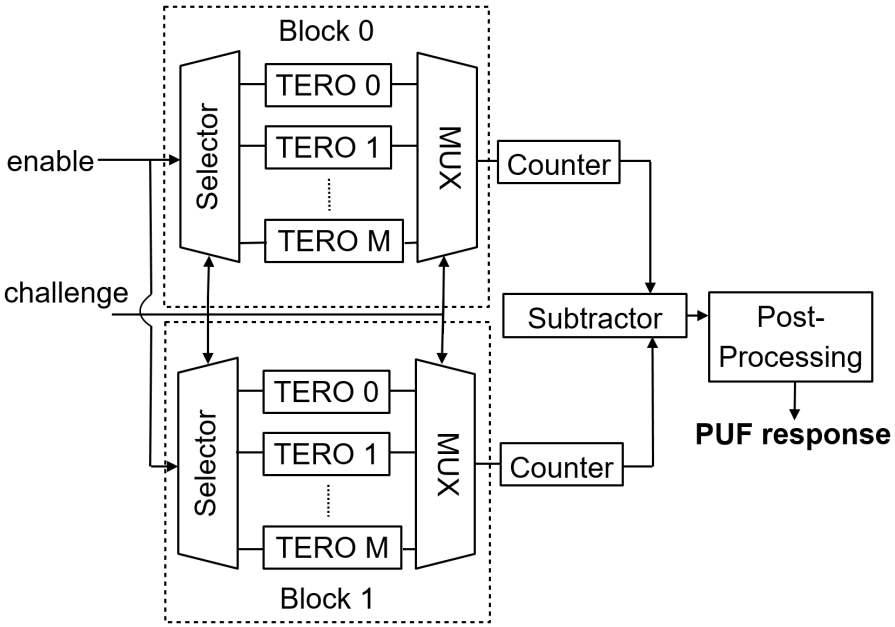


- Metastable oscillations
  - Two propagating events upon *enable*
  - Ideal: Oscillation until reset
  - Real: Oscillation stops after T_{osc}
- Applications
  - TRNGs[1]
  - Primitive for PUFs

[1] Varchola/Drutarovsky: *New High Entropy Element for FPGA Based True Random Number Generators*. Cryptographic Hardware and Embedded Systems (CHES), 2010

The TERO PUF Architecture[1]

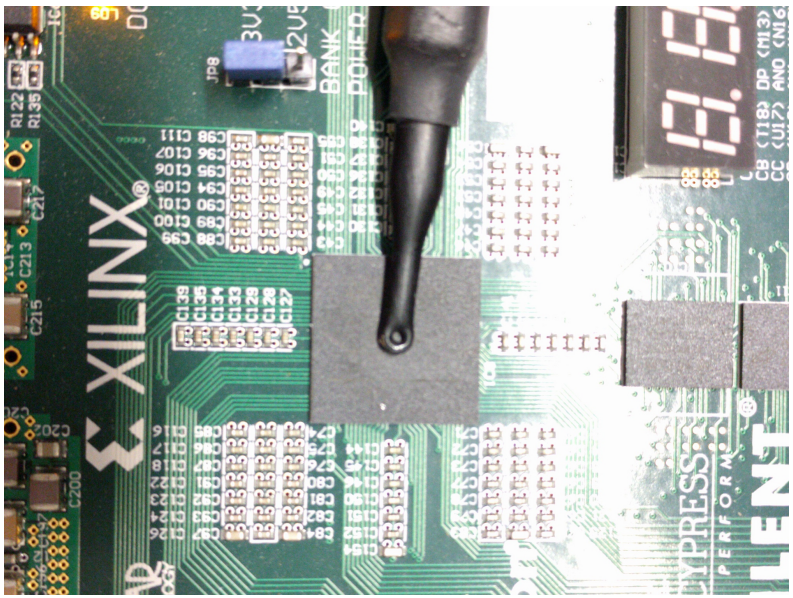
- Select one cell per block (Challenge)
- Enable cells for $T_{acq} = 600\,\text{ns}$
- Response: stable subtractor bits
  - Single-bit: MSB only
  - Multi-bit: further LSBs
- Claimed advantage[1] over RO: no side-channel weakness



[1] Marchand et al.: *Design and Characterization of the TERO-PUF on SRAM FPGAs*. IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2016

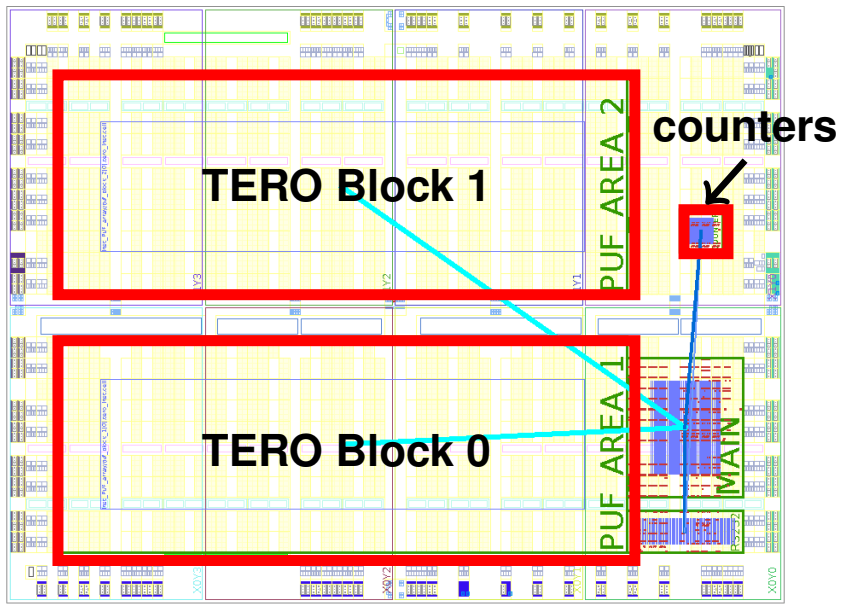
Agenda

Experimental Setup



Measurement setup

- Xilinx Spartan-6 LX16
- Near-field probe
- Sampling oscilloscope (20 GS/s)



Target floorplan

- TERO PUF: 2×96 cells
- Adjacent counters

Attack Sketch

Strategy:

1. Measure TERO oscillation with EM probe and oscilloscope
2. Observe oscillation duration in time-frequency domain
3. Derive counter values from oscillation duration
4. Reveal secret

Requirements:

1. TEROs oscillate with approx. same frequency
2. Oscillations are observable
3. Strategy to derive oscillation duration

Preliminary Experiments

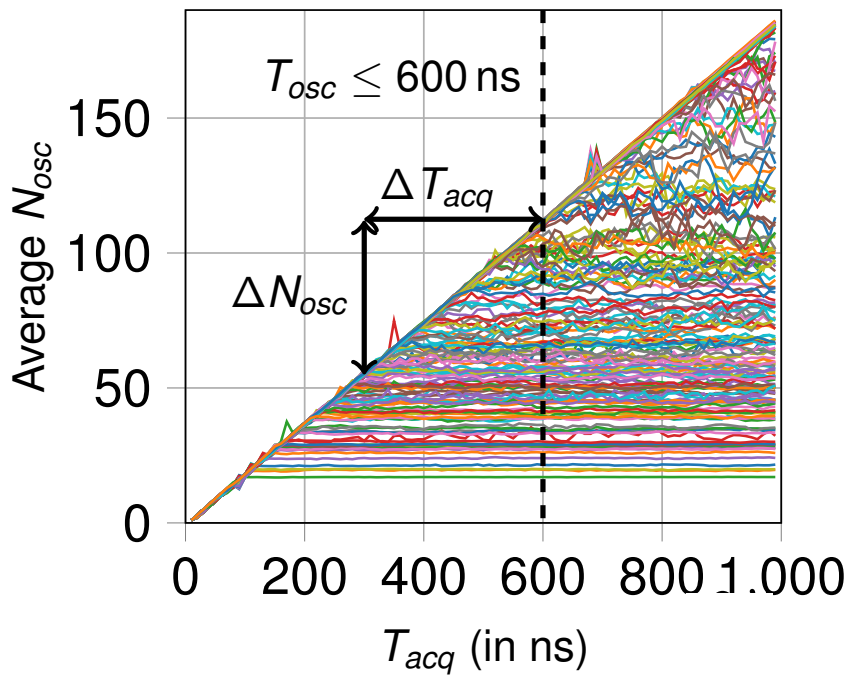
Discovering TERO Oscillations: Do TEROs oscillate with the same frequency? ✓

- Run TEROs for different T_{acq}
- Read out counter values N_{osc}
- Slope: Constant oscillation frequency

$$f_{TERO} = \frac{\Delta N_{osc}}{\Delta T_{acq}} \approx 187.5\,\text{MHz}$$

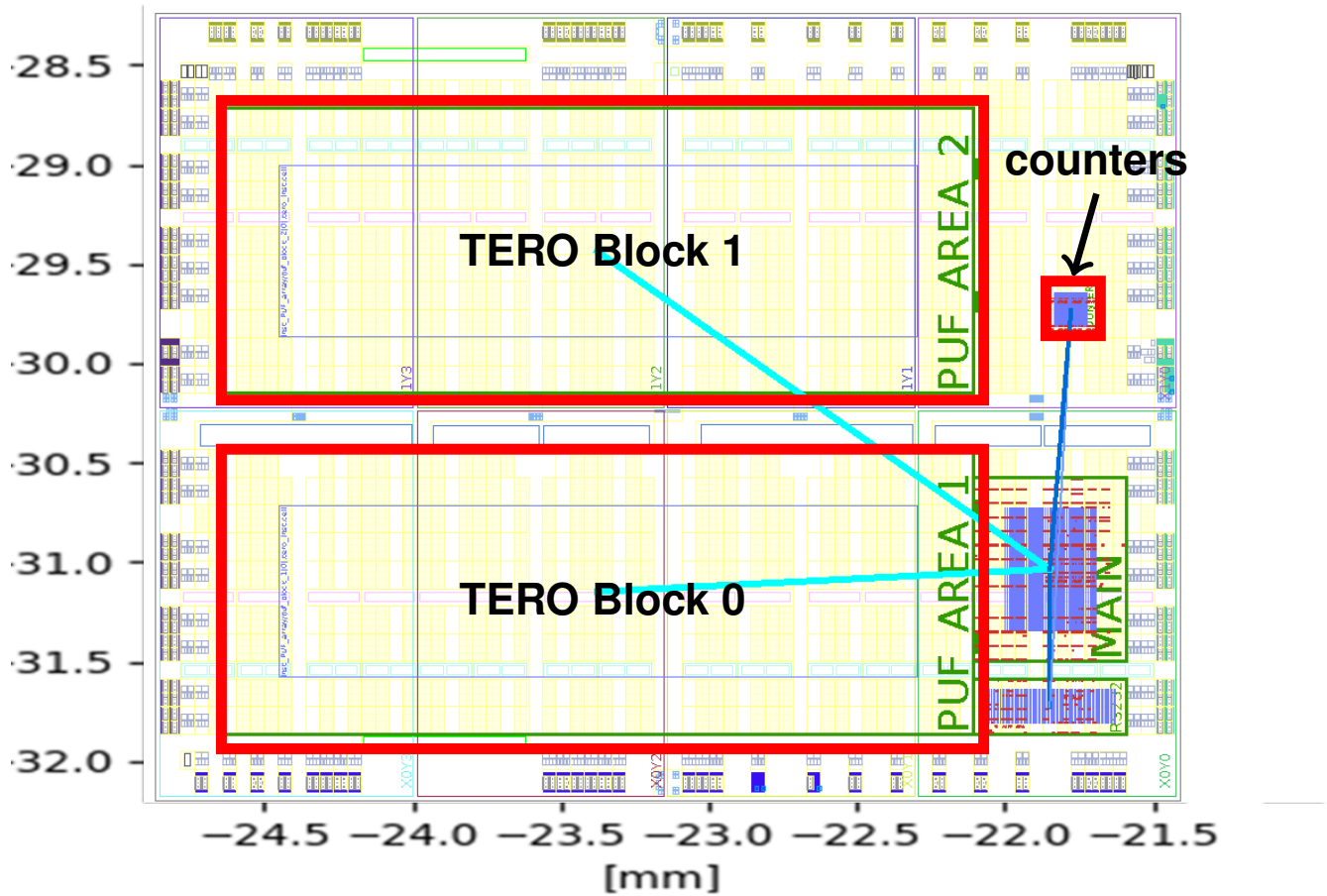
$\Rightarrow$ Estimate N_{est} of counter value by oscillation time T_{osc}

$$N_{est} = f_{TERO} \cdot T_{osc} \approx N_{osc}$$



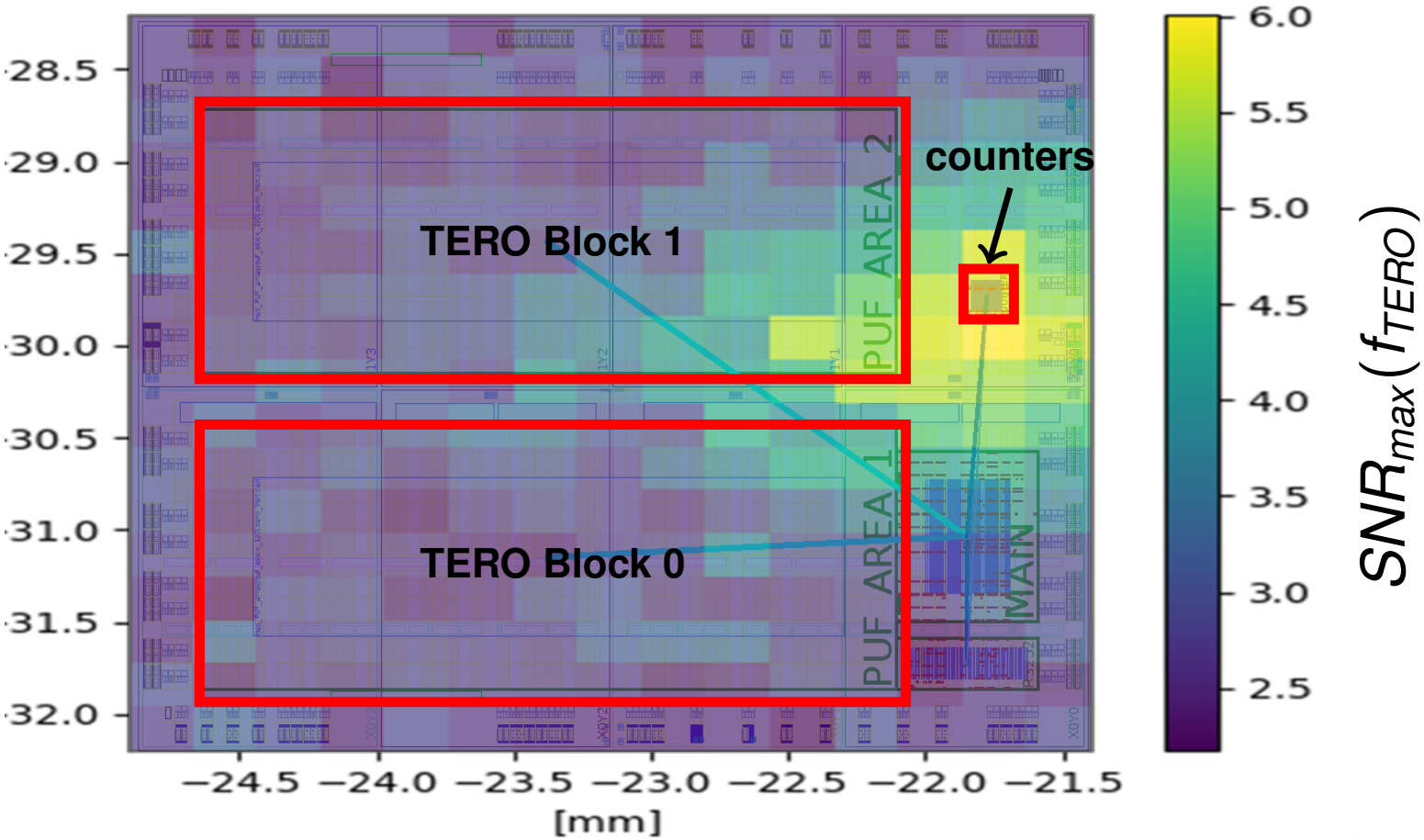
Preliminary Experiments

EM Cartography: Are TERO oscillations observable?



Preliminary Experiments

EM Cartography: Are TERO oscillations observable? ✓

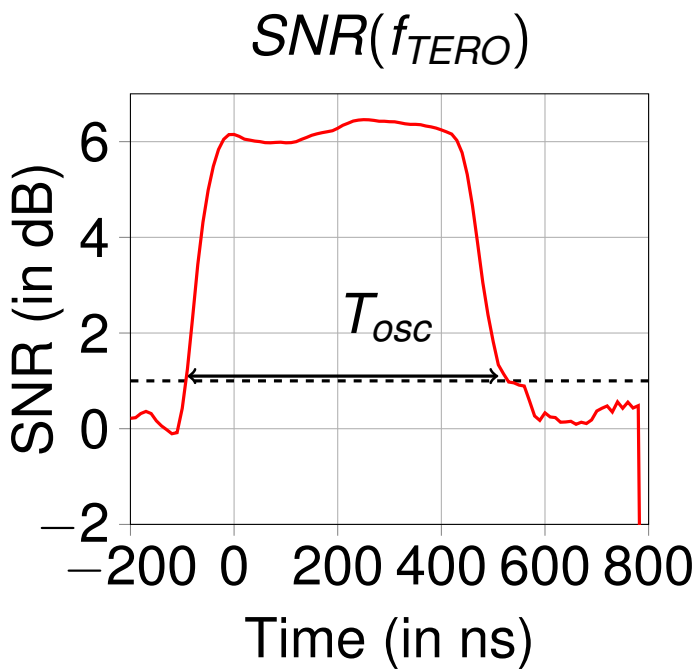


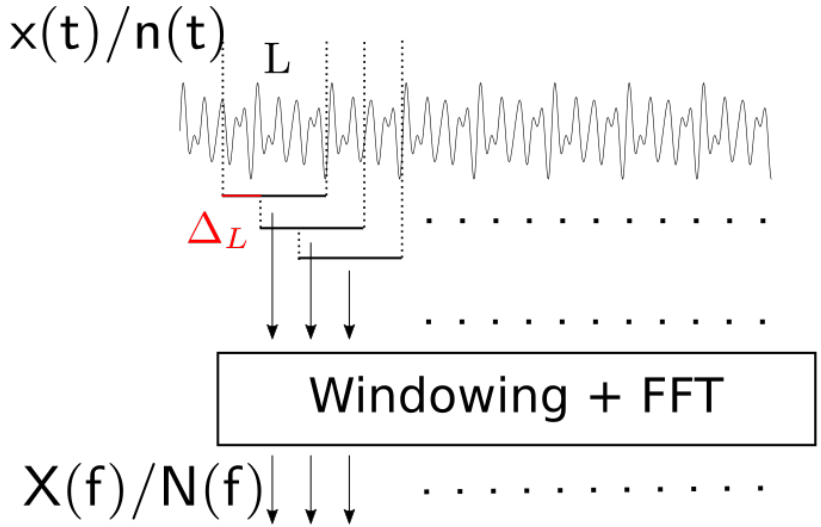
⇒ TEROs observed by the leakage of counters

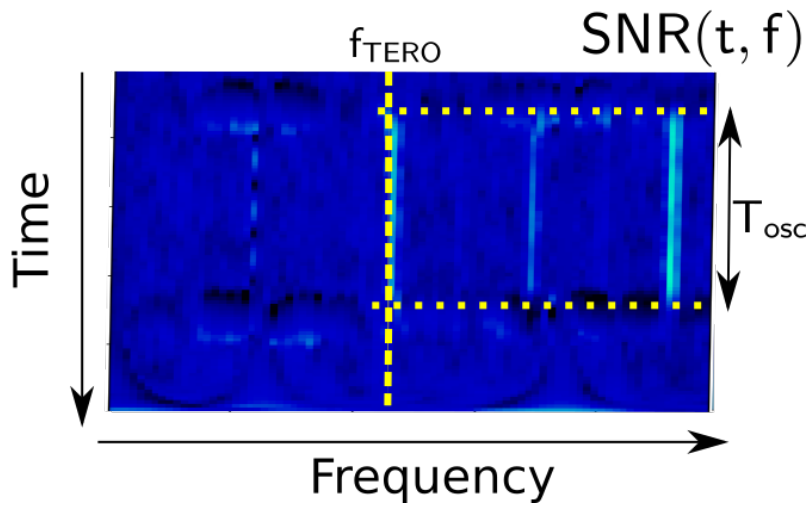
Short Time Fourier Transform (STFT) Approach

Strategy to derive oscillation duration ✓

- STFT spectrogram from time domain signals
  - Alternative: spectrum analyzer
- Estimate: $N_{est} \approx f_{TERO} \cdot T_{osc}$



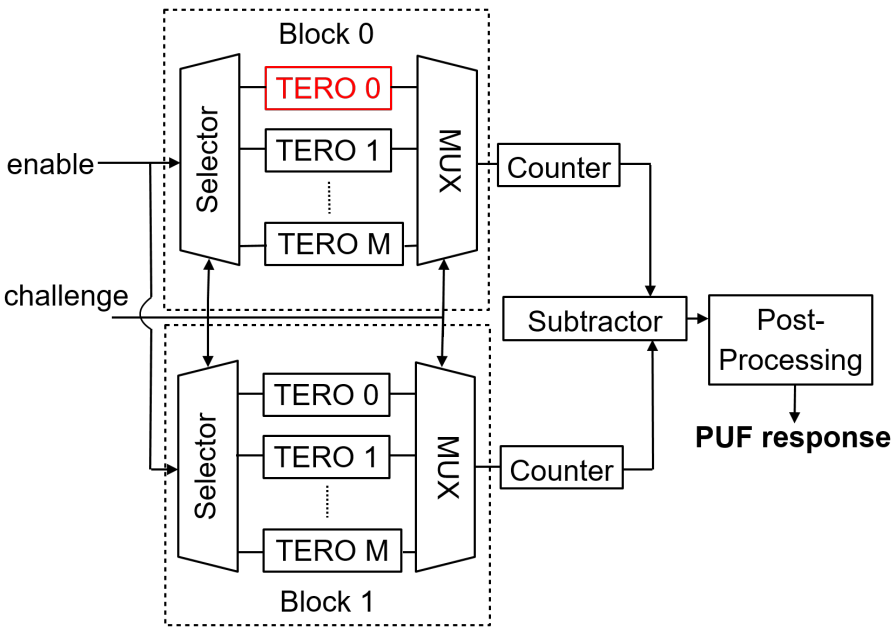


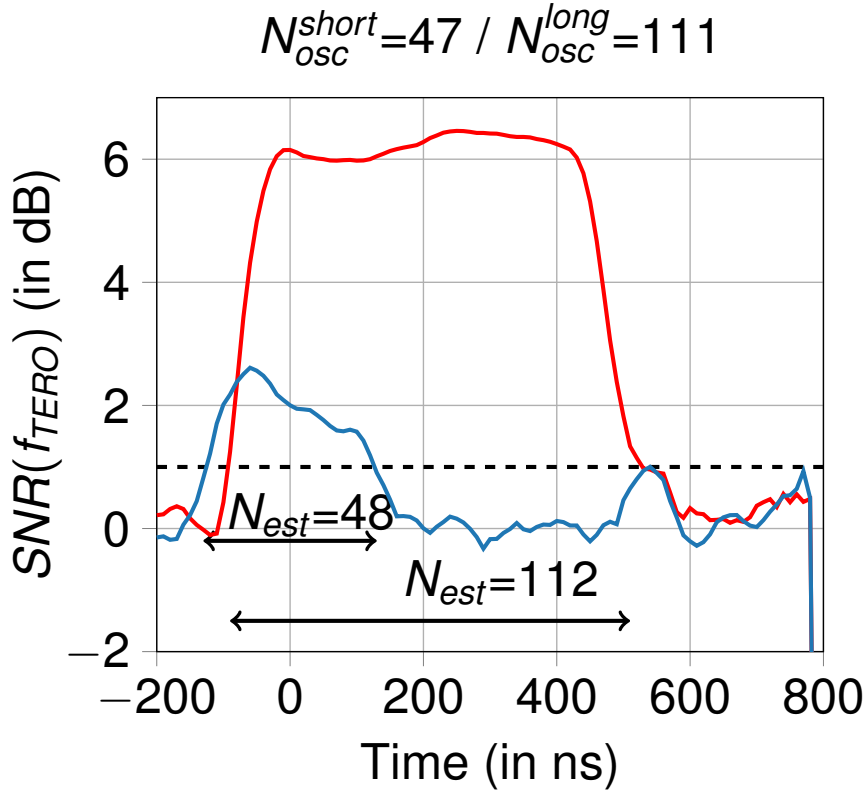


Agenda

Proof of Concept: Single Cells

Spectral Analysis



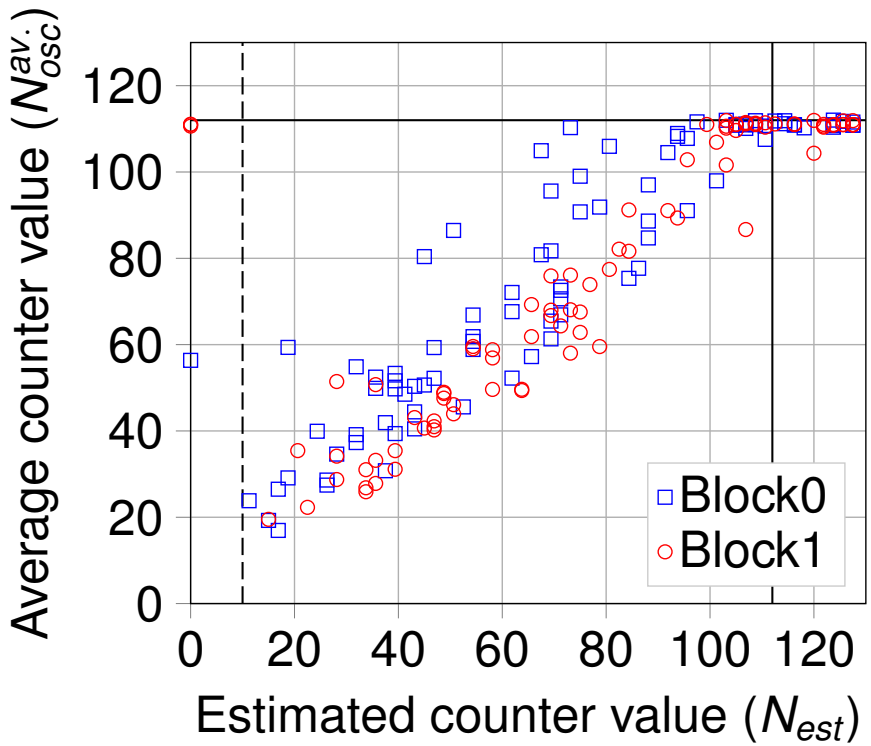


Accurate estimate for short and long oscillations

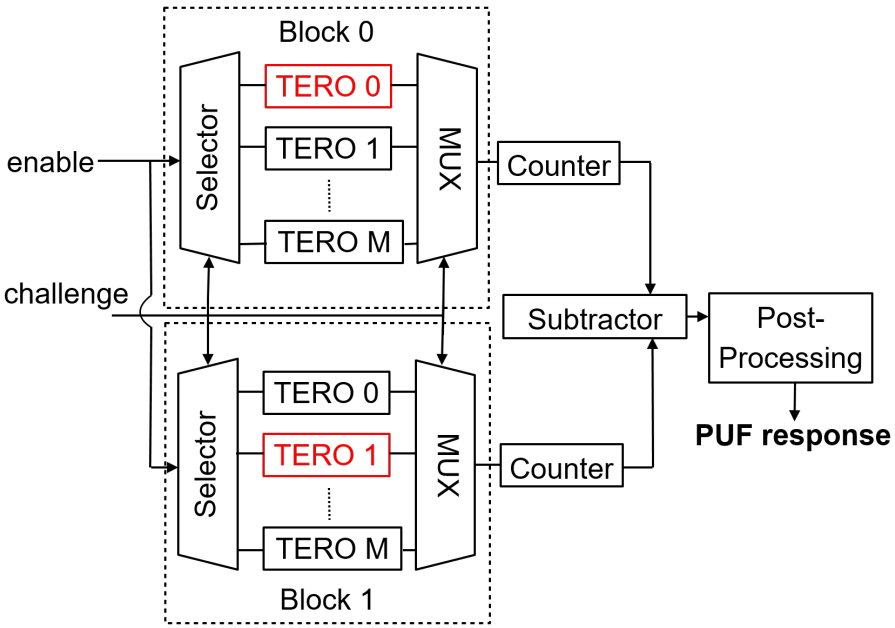
Proof of Concept: Single Cells

Estimated vs. Real Counter Values

- Automatic detection of counter values by SNR threshold
- Estimate and actual counter value match
- Realistic values:
  $10 \leq N_{est} \leq f_{TERO} \cdot T_{acq} \approx 112$
- TERO oscillations approximated by STFT method



Scenario 1: Simultaneous Cells



- Realistic scenario[1]: activate cell from each block simultaneosly
- Challenge selects cells for activation
- Overlapping comparison of cells results in up to $M \cdot M = 96 \cdot 96 = 9216$ PUF bits

[1] Marchand et al.: *Design and Characterization of the TERO-PUF on SRAM FPGAs*. IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2016

Scenario 1: Simultaneous Cells

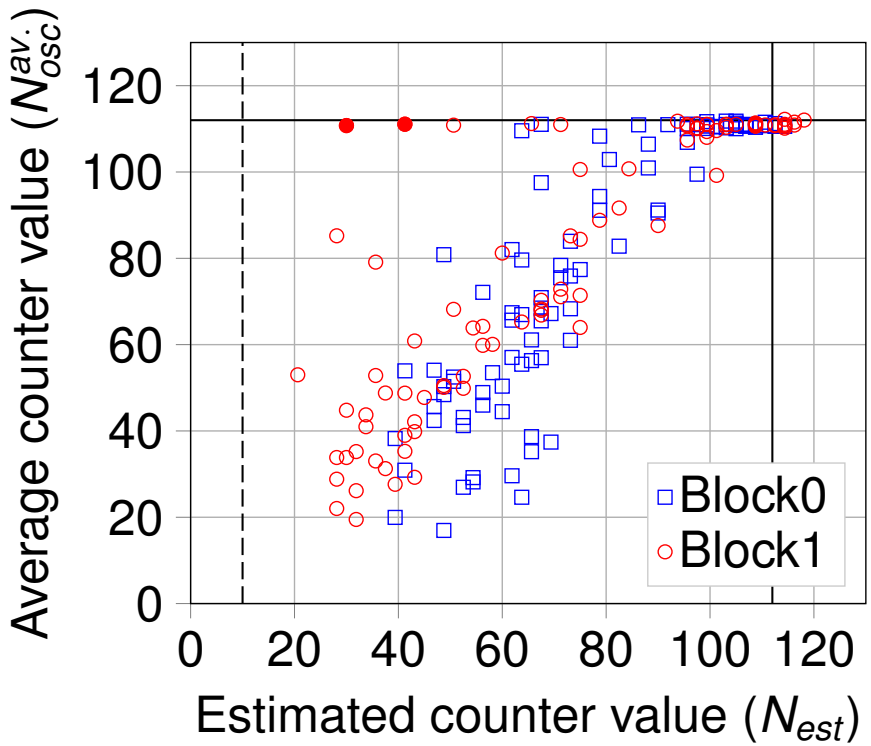
Estimated vs. Real Counter Values

Attack Strategy:

- Average over all SNRs for a cell
- SNR from other cells cancel out

⇒ Results similar to Proof of Concept

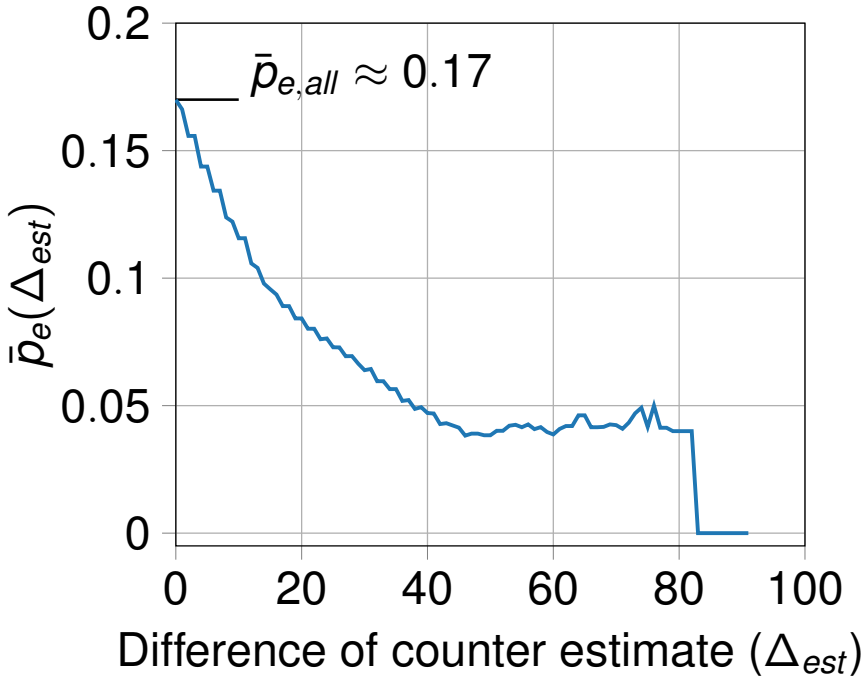
- Manual inspection of SNR can reveal unreliable estimates



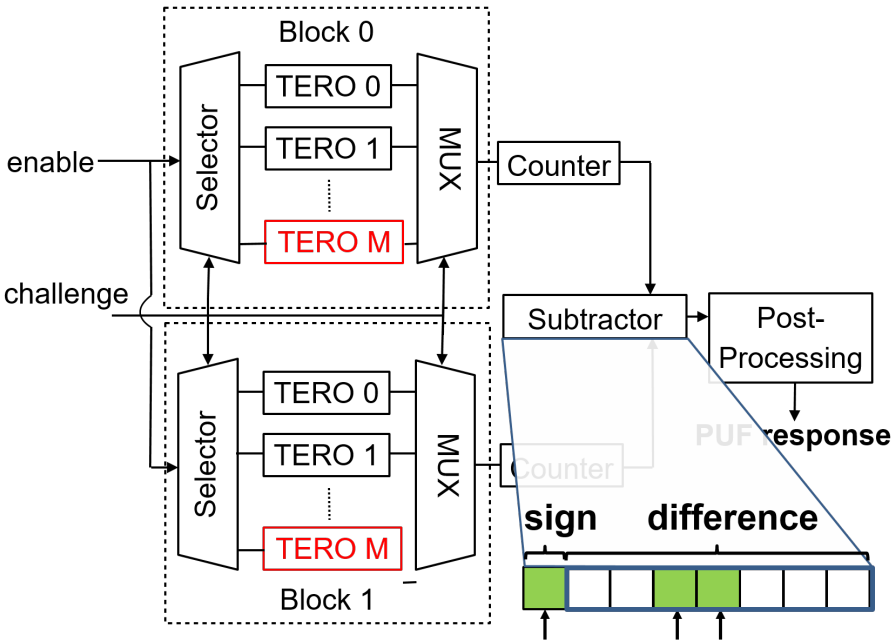
Scenario 1: Simultaneous Cells

Reducing the Entropy of the TERO PUF

- Predict PUF bits from comparison of different N_{est}
- Difference of counter estimates $\Delta_{est} = N^i_{est,0} - N^j_{est,1}$ indicates reliability of PUF bit estimate
  - Smart guessing: sorting by Δ_{est}
- Overall error of 17%
  - manually improved to 14.7%
- Design under attack with overlapping comparison broken considering PUF error correction.



Scenario 2: Multi-bit Responses



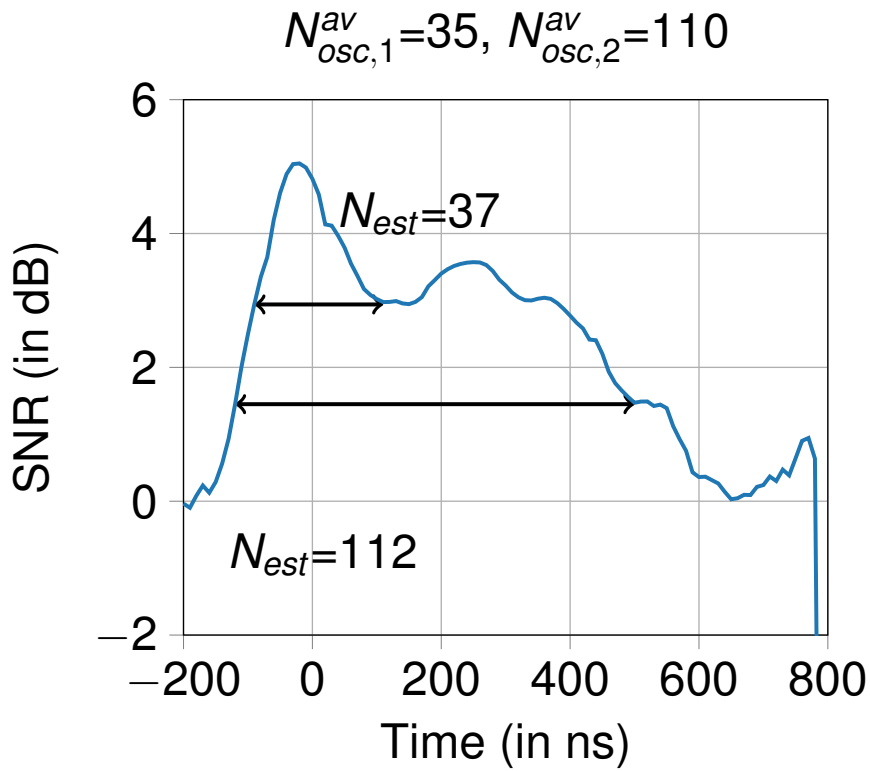
- Countermeasure: only pairwise comparison
  - (+) One measurement per cell: No averaging possible
  - (+) Sign bit cannot be attacked
  - (–) Less PUF bits
- Extension[1]: Derivation of multiple bits, i.e., difference of counters
  - (+) More PUF bits per comparison

New attack: retrieve difference

[1] Marchand et al.: *Design and Characterization of the TERO-PUF on SRAM FPGAs*. IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2016

Scenario 2: Multi-bit Responses

- Attack succeeds in many cases
  - Two oscillation durations can be observed
  - Resolution accurate enough to distinguish differences
- Deviating SNR behaviour can be modelled (c.f. paper)
- Entropy reduced to sign bit



Agenda

Summary and Future Work

- TERO PUF prone to side-channel analysis

- PoC: Oscillations of TEROs approximated by STFT methods
- Scenario 1: TERO PUF with overlapping comparisons broken
  - Overall error in the range of error correction for PUFs
  - Confidence of PUF bits based on estimate differences: smart guessing
- Scenario 2: Multi-bit responses reduced to sign bit
  - Only pairwise comparison impedes attack, but reduces PUF bits
  - Derivation of multiple bits prone to side-channel attack

- Future work
  - Further attack potential: spectrum analyzer, advanced evaluation method, semi-invasive attack, ...
  - Possible counter measures

Thank You!

Lars Tebelmann

lars.tebelmann@tum.de
https://www.sec.ei.tum.de/