Side-Channel Analysis of the TERO PUF

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

[1] Technical University of Munich, Germany
{lars.tebelmann, m.pehl}@tum.de
[2] Fraunhofer Institute AISEC, Germany
vincent.immler@aisec.fraunhofer.de

Abstract. Physical Unclonable Functions (PUFs) have the potential to provide a higher level of security for key storage than traditional Non-Volatile Memory (NVM). However, the susceptibility of the PUF primitives to non-invasive Side-Channel Analysis (SCA) is largely unexplored. While resistance to SCA was indicated for the Transient Effect Ring Oscillator (TERO) PUF, it was not backed by an actual assessment. To investigate the physical security of the TERO PUF, we first discuss and study the conceptual behavior of the PUF primitive to identify possible weaknesses. We support our claims by conducting an EM-analysis of a TERO design on an FPGA. When measuring TERO cells with an oscilloscope in the time domain, a Short Time Fourier Transform (STFT) based approach allows to extract the relevant information in the frequency domain. By applying this method we significantly reduce the entropy of the PUF. Our analysis shows the vulnerability of not only the originally suggested TERO PUF implementation but also the impact on TERO designs in general. We discuss enhancements of the design that potentially prevent the TERO PUF from exposing the secret and point out that regarding security the TERO PUF is similar to the more area-efficient Ring Oscillator PUF.

Keywords: TERO PUF · Side-Channel Analysis · Non-Invasive · EM Side-Channel · Physical Unclonable Function

1 Introduction

Physical side-channel attacks based on power or electromagnetic (EM) analysis, such as Differential Power Analysis (DPA) [10,17], have been subject to extensive research, especially w.r.t. cryptographic algorithms. Such attacks typically require only moderate resources, e.g., a decent oscilloscope. Therefore, they create an imminent threat since an attacker is almost guaranteed to have the necessary equipment at hand to perform the attack. Correspondingly, it is of utmost importance to protect against physical side-channel attacks.

Equally important is the protection of stored secrets, such as cryptographic key material. Storing secret data permanently puts it at risk of extraction by optical

[1] The paper was accepted at COSADE 2019. The final authenticated version is available online at https://doi.org/10.1007/978-3-030-16350-1_4

analysis upon delayering the Integrated Circuit (IC) or related attacks [19]. To overcome these limitations of non-volatile storage, PUFs have been proposed [5] and are assumed to provide a higher level of security when compared to NVMs. When requested, a PUF leverages the device-inherent manufacturing variation and provides fingerprint-like data for subsequent use, e.g., for key derivation. Extracting the minuscule manufacturing dependent parameters is considered infeasible while the system is powered-off and the PUF can be protected against invasive attacks when the system is powered-on.

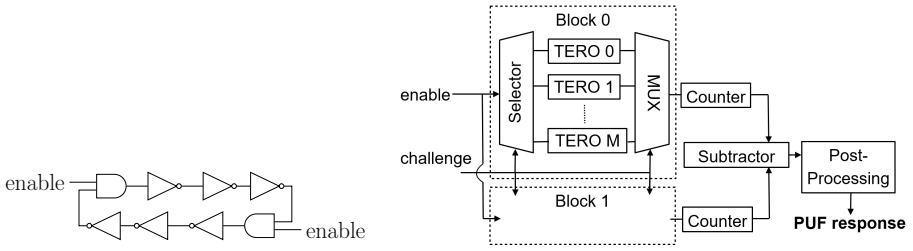
For key storage, the PUF utilizes the variations to provide the secret PUF response which is processed to a key during *enrollment*. In this process, public helper data are derived to support later *reconstruction* of the same key from noisy PUF responses. Clearly, securing the processing of secret PUF responses during reconstruction is essential to protect the key. To date, research primarily focused on risks associated with storing helper data [4], algorithmic processing of the PUF responses [20], and (semi-)invasive attacks on the PUF [7, 11]. Very few attempts have been made to attack the PUF primitives by means of an even more powerful non-invasive side-channel attack.

In this work, we address the challenge of attacking the Transient Effect Ring Oscillator (TERO) PUF, an FPGA PUF primitive that has been favored independently by several authors [2, 14, 24] over other PUFs. With regard to Side-Channel Analysis (SCA), its original authors consider the TERO PUF an improvement compared to the Ring Oscillator (RO) PUF that was already known to be vulnerable to SCA at the time. Breaking the TERO PUF by means of SCA entails specific difficulties, e.g., extracting a multi-bit response per TERO cell and measuring the otherwise hard to observe TERO oscillations.

Related Work. Similar to RO PUFs, TERO PUFs are based on observing oscillations of an inverter ring. For RO PUFs, frequencies of two oscillators are compared while for TERO PUFs the difference in settling times of bistable rings is used to derive a secret. In contrast to TERO PUFs, RO PUFs have been subject to substantial analyses regarding side-channels [15, 16]. The main observations are: (*i*) The emanated frequencies of the ROs allow for recovering the secret if the same RO is used for multiple comparisons. (*ii*) Single ROs can be distinguished by their EM emanations using on-chip surface measurements, i.e., localized EM analysis of a depackaged chip. (*iii*) Multiplexers and counters show the most significant EM leakage when the instances are spatially separated. Interleaved placement of these components was proposed as a countermeasure.

The possibility to identify and locate ROs by their EM emanations has also been studied in the context of its application in TRNGs [1] and for EM cartography in general [18]. While RO and TERO PUFs share similarities, they also show substantial differences. To the best of the author's knowledge, no work was published regarding the side-channel specifics of the TERO PUF or how its primitive can be attacked by means of a non-invasive side-channel analysis.

Contribution. We are the first to successfully perform an EM-based side-channel attack on the TERO PUF primitive *without* depackaging the chip. As part of this work, we present a new Short-Time Fourier Transform based method



(a) TERO cell (b) TERO PUF

Fig. 1: TERO cell example and TERO PUF architecture as used in [3, 13, 14]

to evaluate the oscillations of the TERO primitive. We propose a semi-automatic attack which is able to significantly reduce the entropy of the TERO PUF: While it can recover up to 25% of the response bits without any error, the overall error probability of all estimated bits is less than 18%. The estimate of the failure probability for each bit facilitates an optimal smart guessing strategy. Furthermore, assuming a PUF scenario, where up to 20% errors are corrected, the error probability is sufficiently small to consider the examined TERO PUF design with overlapping comparisons broken by the attack. We also demonstrate that the number of oscillations in TEROs, forming the secret, can be predicted accurately such that the derivation of multiple bits from a single comparison is prone to side-channel analysis. Our method is independent from the specifics of the implementation and is presumably applicable to other implementations of the TERO PUF such as [24], too.

Outline. The remainder of this paper is organized as follows: In Sec. 2, the TERO PUF is introduced. Sec. 3 outlines weaknesses of TERO PUFs by performing a conceptual analysis and by practically discovering the TERO oscillations to tailor the attack. A description of the experimental setup in Sec. 4 is followed by our proposed attack in Sec. 5. We conclude our work in Sec. 6.

2 Transient Effect Ring Oscillator (TERO) Preliminaries

In Sec. 2.1, we reiterate over the TERO PUF architecture. Afterwards, in Sec. 2.2, we describe this work's setting and provide some remarks on the TERO PUF architecture.

2.1 TERO PUF Architecture

The TERO was introduced in 2010 as an entropy source for TRNGs [23]. Each TERO cell comprises two identical branches, consisting of an AND gate and an odd number of inverter gates, that form a metastable ring as depicted in Fig. 1a. When setting the *enable* signal from low to high, two events start to propagate. While in theory the TERO oscillates until the *enable* signal is reset,

manufacturing variations of the underlying CMOS structures result in different delays of the two branches and a break down of the oscillation in finite time.

The manufacturing variation-dependent number of oscillations until the TERO reaches its stable state is utilized in [2] to construct the TERO PUF. The proposed architecture of the PUF in [3, 13, 14] is shown in Fig. 1b. It consists of two blocks of TERO cells and two corresponding counters. One TERO cell is selected from each block by a challenge. The two cells are activated and connected to the counters by multiplexers. Thus, only the two TERO cells that are compared oscillate at a time. The selection of pairs of cells is not restricted in [3, 13, 14]: Each of the M cells from one block is compared to all M cells from the other block resulting in M^2 challenge-response pairs.

After a fixed acquisition time T_{acq}, the activated TERO cells are stopped. T_{acq} allows for a trade-off between reliability, uniqueness, and run time. It is chosen such that most of the TERO cells are expected to be settled. Therefore, T_{acq} is in the range of several hundred nanoseconds depending on the number of inverters in a branch of the TERO cells, e.g., 600 ns for seven inverters [13, 14].

To derive the PUF response, the counter values after T_{acq} are subtracted. The Least Significant Bits (LSBs) are unstable due to noise and are ignored. The Most Significant Bits (MSBs), in particular the sign, are variation-dependent and relatively stable over time. Hence, the sign bit and specific unique and steady bits (e.g., Bit 4, Bit 5 or Bit 6 [13, 14]) serve as PUF response bits. Gray coding can be applied to the difference to ease further processing and to potentially increase robustness w.r.t. noise [3]. However, the large-scale analysis in [24] suggests that using any counter bits other than the sign drastically decreases reliability.

2.2 Remarks on the TERO PUF architecture

In the original proposals [2, 13] of the TERO PUF, the separation of the two cell blocks is deemed necessary in order to avoid dependencies of the responses. This may lead to bias in the responses though, as spatial gradients in silicon can cause cells of one part of the die to settle faster (or slower) than on other parts. Comparing adjacent cells would largely counteract such spatial effects. In addition, spatially separating the TERO blocks makes them prone to attacks by localized EM measurements. While resolving adjacent cells may not be feasible by localized EM measurements, identifying spatially separated cells is certainly within scope based on attacks on similar structures [8, 22]. Due to its architectural limits, we consider the TERO PUF only suited for PUF-based key generation and *not* challenge-response authentication.

Another important design decision is whether to compare TERO outputs among all TERO cells or not. We point out that by comparing a certain cell to multiple other cells enables a similar attack as proposed for RO-PUFs [16]. Also, inherent correlations between PUF bits occur and lower the entropy of the remaining PUF response bits, i.e., the response does not have full entropy as from the comparison of M cells at most $\log_2(M!)$ bits of entropy can be extracted [12]. But restricting the number of derived bits to at the utmost $\log_2(M!)$ changes

the evaluation of the efficiency of the TERO PUF significantly so that we take the originally proposed designs as the base for our research.

3 Exploration of the TERO PUF

As a next step, we explore the TERO PUF by identifying suitable attack vectors, discovering the TERO oscillations, estimating their oscillation duration, and briefly introducing the STFT. This corresponds to Sec. 3.1 to Sec. 3.4.

3.1 Attack Vectors

In [6], the temporary oscillations in the TERO structure were modeled. While aimed at providing a stochastic model for the TERO TRNG, the results from the physical model are also useful in the context of the TERO PUF. One key observation of [6] is that equally built TEROs on a device oscillate with constant and similar frequency. Therefore, TERO cells and their location are identifiable by an attacker based on their characteristic frequency. Another result from [6] is that the variation of the duty cycle changes monotonously over time until it reaches 0 % or 100 % and the oscillation collapses. Consequently, in the spectrum an attacker can observe a TERO cell at a constant and approximately known frequency as long as it is oscillating. The number of oscillations per TERO cell that are used to derive the secret can be estimated from the frequency as soon as an attacker observes the beginning and the end of the oscillation. Depending on the TERO implementation the observations lead to two attack vectors:

Multiple usage of TERO cells. A comparison of each cell from one TERO block to all cells of the other TERO block and taking the sign of the counter differences was suggested to increase the number of secret bits. However, an attacker that observes the approximate duration of each of the simultaneously oscillating TERO cells from the two blocks knows which cell is reused. Consequently, the assignment of the observed duration to blocks and, given the public challenge, even to cells is possible. Then, similarly to [16], the attacker knows the sign bit derived from the subtractor (i.e., the secret) from the observed oscillation times and the knowledge which time belongs to which cell.

Derivation of multiple bits per TERO cell pair. Given that an attacker can estimate the oscillation duration per cell, it is evident that approximation of the counter difference is possible. Thus, when deriving multiple bits from a TERO cell as outlined in Sec. 2.1, they are revealed as soon as the attacker observes the oscillations with sufficient precision. An attacker does not have to resolve the counter differences exactly, since only relatively stable bits of the difference can be used. For the difference $\Delta_{cnt,i}$ of counter values cnt_1 and cnt_2, bit i is 1 iff

$$\Delta_{cnt,i} = (cnt_1 - cnt_2) \mod 2^{i+1} \geq 2^i. \tag{1}$$

I.e. the value of distance bit i is revealed when counter values are distinguished with a precision of 2^i. When using Bit 4 and Bit 5 (cf. [13]), an accuracy of 16 is

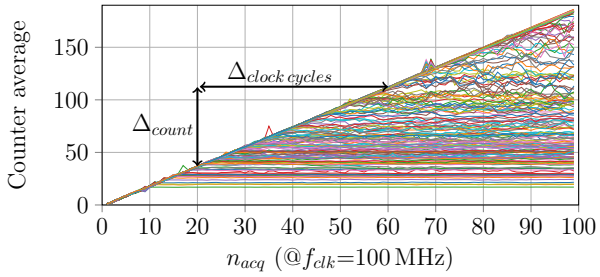


Fig. 2: Evaluation of settling time and counters for $2 \cdot 96 = 192$ TERO cells to estimate the oscillation frequency f_{TERO}, averaged over $N = 101$ measurements. Spikes exceeding the slope are due to measurement artifacts.

required to learn both bits. This corresponds to a resolution of approx. 85 ns in the time domain for a TERO frequency of 187.5 MHz as found in Sec. 3.2.

Measuring a TERO cell together with exactly one other cell, thereby avoiding the reuse in multiple pairs, improves the situation. It prevents an attacker from resolving the oscillation time to a single cell. Nevertheless, it is still possible to observe the oscillation duration's absolute value. Hence, only the sign bit of the difference remains unknown.

3.2 Discovering TERO Oscillations

An accurate estimate of the number of oscillations is required to enable the discussed attacks. The major obstacle is the very short oscillation time until a TERO cell settles. Fig. 2 depicts a practical evaluation of the settling time. The acquisition time in the experiment was varied from 1 to 99 clock cycles and the respective counter values of each TERO cell were stored. Counter values are averaged from 101 repetitions to compensate for noise at room temperature. The break point of a certain curve indicates the end of the oscillation of the corresponding TERO cell.

The results show that most of the TERO cells settle within less than 600 ns (60 clock cycles at a clock frequency of $f_{\mathrm{clk}} = 100\,\mathrm{MHz}$). This emphasizes the need for a good time resolution in order to observe the duration of the oscillation. It also motivates the acquisition time of 600 ns which we selected according to [14]. Note that a longer acquisition and oscillation time is beneficial for the attack but is deemed unrealistic for real-world implementations.

In addition to the settling time of the TERO cells, the slope in Fig. 2 confirms that TERO cells indeed oscillate with similar and constant frequency until the oscillation breaks down [6]. The expected frequency

$$f_{\mathrm{TERO}} = \frac{\Delta_{\mathrm{count}}}{\Delta_{\mathrm{acq}}} = \frac{\Delta_{\mathrm{count}}}{\Delta_{\mathrm{clock\ cycles}}} \cdot f_{\mathrm{clk}} \approx 187.5\,\mathrm{MHz} \tag{2}$$

for our design is derived from the slope of the counter values, where Δ_{count} is the difference of the counter for a given difference Δ_{acq} of the acquisition time respectively a given difference of clock cycles $\Delta_{\text{clock cycles}}$.

Note that the experiment is only carried out to validate the assumption of a constant oscillation frequency. For an attack, it is not necessary to obtain frequency counter values, as the frequency can be estimated by observing the frequency domain.

3.3 Estimating TERO Oscillation Durations

The experiment in Sec. 3.2 shows a stable oscillation of the TERO cells until the oscillation breaks down. The actual frequency of a certain TERO cell is approximated by f_{TERO} and typically lies in a small interval $f_{\text{TERO}} \pm \Delta_f$. Note that f_{TERO} is device specific and obtained by measuring the frequency domain and Δ_f is the relative deviation on the same device. Given f_{TERO}, the time T_{osc} until a TERO cell settles provides a good estimate of the number of oscillations and thus the TERO counter value n_{TERO}:

$$n_{\text{TERO}} \approx f_{\text{TERO}} \cdot T_{\text{osc}}. \tag{3}$$

All TERO cells are activated for n_{acq} clock cycles of the system clock with frequency $f_{\text{clk}} = \frac{1}{T_{\text{clk}}}$. Therefore, n_{TERO} is upper bounded by

$$n_{\text{TERO}} \leq (f_{\text{TERO}} + \Delta_f) \cdot T_{\text{clk}} \cdot n_{\text{acq}} = \frac{f_{\text{TERO}} + \Delta_f}{f_{\text{clk}}} \cdot n_{\text{acq}}, \tag{4}$$

where equality is reached iff the TERO oscillates until the acquisition time ends.

Note that for many practical cases Δ_f is negligible in Eq. (4). For a deviation Δ_f from the known nominal oscillation frequency f_{TERO}, the difference between actual and estimated counter value for $T_{\text{osc}} \leq T_{\text{acq}} = T_{\text{clk}} \cdot n_{\text{acq}}$ is at most

$$|n'_{\text{TERO}} - n_{\text{TERO}}| \approx |(f_{\text{TERO}} \pm \Delta_f) \cdot T_{\text{osc}} - f_{\text{TERO}} \cdot T_{\text{osc}}| \leq |\Delta_f| \cdot T_{\text{acq}}. \tag{5}$$

E.g., for an accurately known $T_{\text{osc}} = T_{\text{acq}} = 600\,\text{ns}$ and $|\Delta_f| \leq 1.67\,\text{MHz}$ the difference between actual and estimated counter value is 1 when Δ_f is neglected. This is below the expected variations in the measurement due to noise.

Summing up, as long as the counter frequencies lie within a narrow range around the nominal frequency f_{TERO}, the approximation in Eq. (3) holds and the counter values are indeed estimated by the oscillation time T_{osc}.

3.4 Short-Time Fourier Transform (STFT)

To estimate T_{osc}, the visibility of the TERO frequency f_{TERO} in the spectrum is analyzed. The challenge regarding the measurement is the short acquisition time of $T_{acq} = 600\,\text{ns}$ and oscillation times as short as $T_{osc} = 100\,\text{ns}$. In order to resolve time and frequency simultaneously, a Short-Time Fourier Transform (STFT) based approach is taken.

Each time domain signal $x^{\mathrm{TERO}}(t)$ during the activation of a TERO cell is processed via the STFT into the frequency domain. Instead of transforming the entire signal, segments $x^{\mathrm{TERO}}_{(l)}(t)$ of length L are taken from $x^{\mathrm{TERO}}(t)$, where (l) denotes the index of a segment. Each segment is multiplied by a Hanning window (raised cosine) function $\mathrm{w}(t)$ to reduce FFT spectral leakage effects. Windowed segments are transformed individually into the frequency domain:

$$X^{\mathrm{TERO}}_{(l)}(f) = \mathrm{FFT}\left(x^{\mathrm{TERO}}_{(l)}(t) \cdot \mathrm{w}(t)\right) = \mathrm{FFT}\left(\hat{x}^{\mathrm{TERO}}_{(l)}(t)\right). \tag{6}$$

The segments overlap for a number of samples L_{overlap}. In other words, the segments are shifted by $\Delta L = L - L_{\mathrm{overlap}}$ samples along the time axis. The stable frequencies of TERO cells allow averaging in the frequency domain for each segment over N measurements per cell to enhance the Signal-to-Noise Ratio (SNR). This is a valid approach and justified by our preliminary evaluation of the TEROs in Sec. 3.2.

In order to eliminate unwanted signals such as the system clock and other disturbances, a noise floor can be estimated to facilitate the evaluation. For the noise floor estimate, measurements $n(t)$ are taken while the TERO cells are deactivated and the same processing as in Eq. (6) is applied. Averaging over N_{noise} measurements yields the noise frequency spectrum $\bar{N}_{(l)}(f)$ for each segment (l). From the averaged signal $\bar{X}^{\mathrm{TERO}}_{(l)}(f)$ and averaged noise floor $\bar{N}_{(l)}(f)$

$$\bar{X}^{\mathrm{TERO}}_{(l)}(f) = \frac{1}{N}\sum_{i=1}^{N} \mathrm{FFT}\left(\hat{x}^{\mathrm{TERO}}_{i,(l)}(t)\right), \quad \bar{N}_{(l)}(f) = \frac{1}{N_{\mathrm{noise}}}\sum_{i=1}^{N_{\mathrm{noise}}} \mathrm{FFT}\left(\hat{n}_{i,(l)}(t)\right)$$

the frequency- and segment-dependent SNR of segment l is defined as

$$\overline{\mathrm{SNR}}_{(l)}(f) = 10\log\left(\frac{\bar{X}_{(l)}(f)}{\bar{N}_{(l)}(f)}\right) = 10\log\left(\bar{X}_{(l)}(f)\right) - 10\log\left(\bar{N}_{(l)}(f)\right). \tag{7}$$

Our attack evaluates the SNR around the expected TERO frequency f_{TERO}. During the period of activation, $\overline{\mathrm{SNR}}_{(l)}(f_{\mathrm{TERO}})$ is expected to take higher values. Estimating the time of the activation period then translates into measuring the duration of the high SNR.

Note that estimating the noise floor is not a premise for the attack, i.e., instead of evaluating the relative changes defined by the SNR in Eq. (7), absolute values of Eq. (6) could be used to carry out the attack.

Frequency resolution. For a real valued signal $x(t)$, the spectrum is symmetric and can be reduced to $N_{\mathrm{FFT}}/2 + 1$ bins ranging from DC to $f_{\max}$. Given the sampling frequency f_s, the resolution in the frequency domain is

$$\Delta_{\mathrm{FFT}} = \frac{f_{\max}}{N_{\mathrm{FFT}}/2} = \frac{f_s}{N_{\mathrm{FFT}}} \tag{8}$$

with $f_{\max}$ being the maximum frequency that can be reconstructed according to the Shannon-Nyquist theorem. In general, a narrow frequency resolution Δ_{FFT}

is desired. However, the TERO frequency f_{TERO} does not have to be resolved in detail. Instead, an attacker is mostly interested in the duration of the signal. Therefore, a trade-off towards the temporal resolution is acceptable. For the experiments in Sec. 5, $N_{\mathrm{FFT}} = 4096$ resulting in a resolution of $\Delta_{\mathrm{FFT}} \approx 4.88\,\mathrm{MHz}$ for $f_s = 20\,\mathrm{GHz}$ is chosen.

Temporal resolution. The temporal resolution also depends on N_{FFT} and f_s and behaves contrary to the frequency resolution:

$$\Delta_T = \frac{N_{\mathrm{FFT}}}{f_s} = \frac{1}{\Delta_{\mathrm{FFT}}}, \tag{9}$$

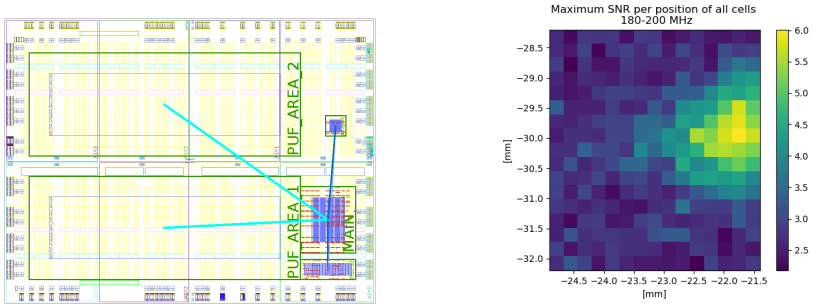
i.e., to get a good temporal resolution, high sampling rates are required. Given $N_{\mathrm{FFT}} = 4096$ and $f_s = 20\,\mathrm{GHz}$, a segment contains $\Delta_T = 204.8\,\mathrm{ns}$. Without overlapping segments, the resolution would be too coarse to analyze the TERO oscillations. As the segments overlap, a certain redundancy between segments exists, i.e., since the same samples are transformed, the resulting amplitudes are similar. Yet, as the oscillations stop after some time, all segments that contain samples during the oscillation provide information, and smaller differences than Δ_T can be resolved as shown in Sec. 5. The offset between segments is chosen as $\Delta L = 200$ as a trade-off between computational cost and temporal resolution.

4 Experimental Setup

In the following, the experimental setup is described in terms of the measurement setup, the design under attack, and a pre-evaluation by means of EM cartography.

Measurement Setup. Measurements are recorded with an oscilloscope of 2.5 GHz analog bandwidth and a sample rate of 20 GS/s. The near-field probes `RF-B 0.3-3` and `RF-B 3-2` from Langer EMV are used, having $< 1\,\mathrm{mm}$ and $\approx 1\,\mathrm{mm}$ resolution respectively. Both probes capture emanations in vertical direction relative to the FPGA package. Two 30 dB amplifiers amplify the signals. Summarizing the results of Sec. 3.4, we set the number of FFT bins N_{FFT} to 4096, corresponding to 204.8 ns segment length and a frequency resolution of 4.88 MHz. A segment offset of $\Delta_L = 200$ samples is selected, corresponding to a full clock cycle length of the system clock with 10 ns. In all experiments in Sec. 5 the number of noise measurements to estimate the noise floor is set to $N_{\mathrm{noise}} = 9600$ and the SNR is evaluated by its maximum in the range from 180 MHz to 190 MHz, corresponding to $f_{TERO} \approx 187.5\,\mathrm{MHz}$ from Sec. 3.2.

Design Under Attack. Our evaluation target is a Xilinx Spartan-6 LX16 FPGA in a 324-pin BGA package mounted on a Nexys3 development board. The package of the FPGA remains unaltered. The design under attack contains two blocks of 96 TERO cells each. For the TERO cells a hard macro [21] for the Spartan-6 by Marchand et al. [13] is used with seven inverters per branch. The number of cells per block is slightly reduced compared to the original TERO PUF proposal in order to include serial communication and an FSM on the same chip.



(a) Floorplan (rotated) (b) EM carthography

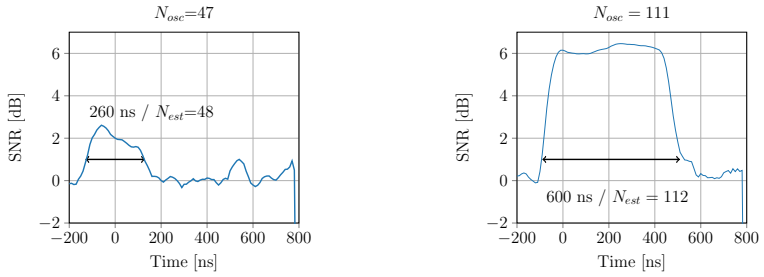
Fig. 3: a) Floorplan of TERO PUF and corresponding SNR heatmap for frequency range 180-200 MHz. b) Maximum SNR of cells during first 60 ns after the trigger.

Fig. 3a depicts the floorplan, where the TERO blocks are denoted as `PUF_AREA_1` and `PUF_AREA_2` respectively. The logic for selecting specific cells in each block and assigning their output to the counters is contained in `MAIN`, located in the lower right corner in Fig. 3a. The counters are placed separately adjacent to the second block of TERO cells. The separation allows to verify whether EM emanations stem from the TERO cells or the counters. The counters are placed side by side to prevent spatial separation of their EM emanations. This thwarts attacks targeting each counter separately.

Pre-evaluation with EM cartography. Fig. 3b depicts a heatmap generated by using the `RF-B 0.3-3` probe and an xyz-table. The SNR in the frequency range from 180 MHz to 200 MHz is shown. Measurements were taken on a grid of 0.25 mm × 0.25 mm over the part of the package where the die is located. Each point was only measured $N = 10$ times while a cell from each block was activated, same as for measuring the noise floor, i.e. $N_{noise} = 10$. The SNR according to Eq. (7) is evaluated during the first 60 ns after a trigger signal. In this period, all cells oscillate and no settling effects take place. The maximum SNR in Fig. 3b coincides with the location of the counters in the design. The area spans almost 1 mm^2, i.e., a fine-grained search over the package is not needed and we position the `RF-R 3-2` probe manually for all following experiments. Note, this is in line with previous work on EM analysis of ROs [15] showing that observed EM emanations are most likely caused by multiplexers, counters and wires in between. This is no limitation of our attack, since – similar to the attack on ROs in [16] – we mainly exploit that TERO cells are used for multiple comparisons.

5 Exploitation of the TERO Side-Channel

This section demonstrates that TERO PUFs are vulnerable to a non-invasive side-channel attack. Sec. 5.1 shows the feasibility of detecting TERO oscillations by activating cells separately. Subsequently, Sec. 5.2 practically exploits the



(a) Short oscillation (b) Long oscillation

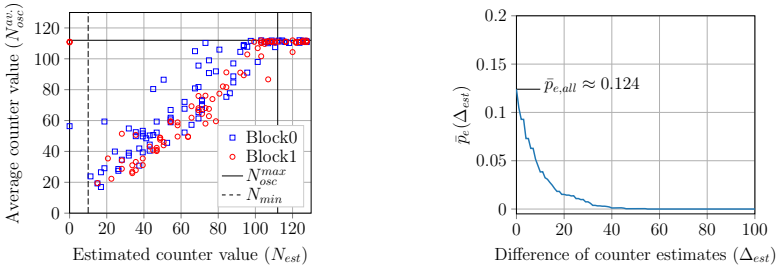
Fig. 4: Examples of the SNR according to Eq. (7) for separately activated cells. The estimated oscillation duration is depicted by double arrows.

reuse of a certain cell in the derivation of multiple response bits, i.e., two cells under comparison are activated at once. The results illustrate that the oscillation duration is well estimated by our approach. A simple countermeasure is not to reuse a certain TERO cell in multiple comparisons. The analysis in Sec. 5.3 nevertheless shows that if multiple bits are extracted from a single comparison still some counter values are leaked which renders the extraction of more than one bit per TERO cell pair insecure.

5.1 Analysis of Separately Activated Cells

In this experiment only one cell is activated at once. Fig. 4 depicts the practical application of our approach outlined in Sec. 3.4. The maximum of the STFT in the frequency range from 180 MHz to 190 MHz is plotted while shifting the segment under transformation in the time domain. The range is chosen according to f_{TERO} from Sec. 3.2. The point where the first sample of the segment in the time domain is aligned with the starting point of the oscillation corresponds to 0 ns. Note that also segments starting before 0 ns can include samples from where the TERO cell oscillates. Thus the increase in SNR starts before this point in time is reached. In addition cells with an oscillation time shorter than the FFT window can cause a maximum before 0 ns.

The activation of the cells causes an increase of SNR in Figs. 4a and 4b. At approximately −100 ns, i.e., when the oscillation starts in the middle of the segment under transformation, the SNR reaches 0.75 dB. This value is chosen as a threshold to estimate the oscillation duration T_{osc}, i.e., T_{osc} is approximated by the time from exceeding the threshold to falling back below this value. Assuming an oscillation frequency $f_{\mathrm{TERO}} = 187.5\,\mathrm{MHz}$, the counter values are computed according to Eq. (3) as $N_{\mathrm{est}} = 48$ and $N_{\mathrm{est}} = 112$, respectively. This result fits well to the actual number of oscillations that are $N_{\mathrm{osc}} = 47$ and $N_{\mathrm{osc}} = 111$. From the experiments we conclude that both short and long oscillations of the TERO are well estimated by our approach.



(a) Counter estimation vs. real value (b) Error of estimated TERO PUF bits.

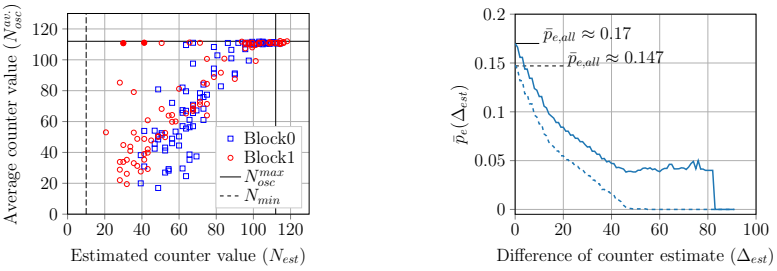
Fig. 5: a) Automatically estimated vs. actual counter values for separately activated cells. b) Probability of guessing a wrong bit using the estimates in a).

A comparison of estimated and actual counter values for all TERO cells is depicted in Fig. 5a. The actual counter values, which slightly vary due to noise, are derived from averaging among $N = 100$ measurements. Since the acquisition window is set to $T_{\text{acq}} = 600\,\text{ns}$, the maximum number of oscillations is $N_{\text{osc}}^{\max} = f_{\text{TERO}} \cdot T_{\text{acq}} \approx 112$. Thus, estimated values $N_{\text{est}} > N_{\text{osc}}^{\max}$ can be assumed to be $N_{\text{osc}}^{\max}$. Indeed, in Fig. 5a, almost all estimated values $N_{\text{est}} > N_{\text{osc}}^{\max}$ correspond to the maximum possible value, i.e., the minor overestimation of oscillations does not affect the result. Since it is known that all TERO cells have a minimum oscillation duration, certain values below $N_{\min}$ are known to be false.

Entropy reduction of the TERO PUF. Comparing each cell from one block to all cells of the respective other block and taking the sign bit as a secret results in $96 \cdot 96 = 9216$ response bits. From the $2 \cdot 96 = 192$ estimations of the oscillation durations, four results are deemed unreliable as $N_{\text{est}} < N_{\min} = 10$, i.e., for the corresponding $4 \cdot 96 = 384$ Bits no estimation can be given. For the remaining 8808 bits, the probability of guessing the PUF bit erroneously depends on the difference of the counter estimates $\Delta_{\text{est}} := \left| N_{est}^{Block\,0} - N_{est}^{Block\,1} \right|$ as depicted in Fig. 5b. The graph shows the probability of an error $\bar{p}_e$ if only difference estimates Δ_{est} greater than the value on the x-axis are considered. Clearly, the error probability decreases with an increase of the differences. This is in line with Fig. 5a: The deviation in the average counter value (ordinate) of the scatter plots is an indicator of the estimation accuracy. An inaccurate estimation has more impact if the estimated counter values are close to each other compared to when the estimated counter values are further apart.

According to Fig. 5b estimated counter differences with $\Delta_{\text{est}} \geq 55$ have an error probability of $\bar{p}_e = 0$, i.e., the 2368 bits corresponding to these estimates are revealed without any errors. Estimated counter differences with $\Delta_{est} \geq 19$ still have an error probability of only $\bar{p}_e \approx 1.5\%$, which applies to 5471 bits. The whole set of 8808 bits has an error probability of $\bar{p}_{e,all} \approx 12.4\%$.

Summing up, automatic estimation of single TERO cell oscillations and using only known error free bits, the entropy of the TERO PUF is reduced by a quarter



(a) Counter estimation vs. real value (b) Error of estimated TERO PUF bits.

Fig. 6: a) Automatically estimated vs. actual counter values for two simultaneously activated cells. b) Probability of guessing a wrong bit using the estimates in a); dashed line: result for manually discarding estimates marked in solid red in a).

from 9192 to 6848 bits. In addition, an attacker can take advantage from error probabilities for estimations. They define a confidence for each bit that allows to develop a smart guessing strategy, i.e., the remaining guessing effort is far below an exhaustive search. Also, an attacker can try to adjust the counter values for counters which contribute to unreliable differences, e.g., by visual inspection of the SNR, which provides more precise results than our automatic estimation.

5.2 Analysis of Simultaneously Activated Cells

We now analyze the scenario that each TERO cell in *Block 0* is compared to each cell in *Block 1* where the two cells under comparison are activated in parallel. In this setting, each cell i is measured 96 times, always in combination with a different cell $j \in \{1, \dots 96\}$. We assume that an attacker can figure out which cell is activated at a certain point in time, e.g., by knowledge of the design. The attacker averages over the SNR of all 96 measurements for cell i. Thus, contributions from other cells are considered noise that results in a distinguishable offset:

$$\mathrm{SNR}^{i}_{(l)}(f) \approx \mathrm{SNR}^{i}_{(l)}(f) + \frac{1}{96}\sum_{j=1}^{96} \mathrm{SNR}^{j}_{(l)}(f) \tag{10}$$

Effectively, the scenario of activating two cells at once is transformed back to the case of separately activated cells. Due to the activation of two cells and an additionally observed noise floor of approx. 1 dB, we increase the threshold in the automatic counter value estimation from 0.75 dB to 2.5 dB. Fig. 6 depicts the results for cells of both blocks. For every comparison, a single measurement is taken and the noise floor is subtracted. The $N = 96$ measurements of comparisons containing the same cell are averaged, i.e., the number of traces per cell is in the same range as in the previous experiment.

Fig. 6a compares automatically estimated counter values against averaged known counter values for this scenario. As expected, the results are slightly

degraded compared to Sec. 5.1, since not all effects caused by simultaneously activated cells cancel out. Due to few but substantial deviations of automatically estimated counter values from the actual ones, the resulting error probability for guessing TERO PUF bits in Fig. 6b increases to $\bar{p}_{e,all} \approx 17\%$ compared to $\bar{p}_{e,all} \approx 12.4\%$ in Fig. 5b. While still more than 7600 out of 9216 bits are guessed correctly, this reduces the confidence of the guess for almost all bits.

To significantly improve the result, the underlying SNR is evaluated to eliminate cases showing a distorted SNR over time when compared, e.g., to Fig. 4. The most obviously degraded cases in our results correspond to the two solid red dots in Fig. 6a. Eliminating these yields the dashed line for the error probability in Fig. 6b. Similar to Fig. 5b, bits that are guessed with an estimated counter difference of $\Delta_{est} \geq 62$ are regarded error free. This applies to 831 bits while smart guessing can be used to get remaining bits as suggested above.

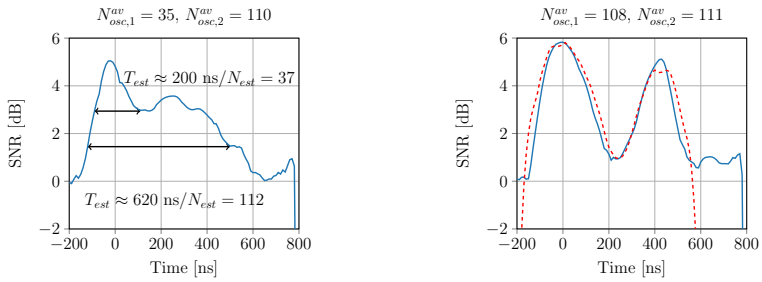
In a typical PUF setting, an error correction is applied to the PUF response to compensate variations due to e.g., environmental conditions. Hence, an bit error probability (BER) in the estimated response of up to the correction capability is tolerable for a successful attack. Please note, despite an empirical BER in the range of $5 - 10\%$ within academic settings [9, 24], it is common practice to consider a substantially larger amount of errors in a commercial setting to ensure a failure free operation throughout the whole lifetime of a product, including industrial temperature ranges from $-40°$ to $+85°$ C, leading to an anticipated BER of $15 - 20\%$. Therefore, the examined TERO PUF can be considered broken by our attack even if not all bits are known, e.g., through smart guessing.

5.3 Attack on Multi-Bit Responses

The attack in Sec. 5.2 is prevented by using every TERO cell in only one comparison. Then, an attacker cannot assign a counter value to a certain cell as long as the measurements cannot be spatially resolved to cells, which is the case for our setup. Consequently an attacker cannot reveal the secret, i.e., the sign bit of counter differences. But if multiple bits are derived from a comparison of the counters, the difference itself is of interest, since knowing its absolute value reduces the entropy to one bit, as discussed in Sec. 3.1.

While no automatic detection was implemented, visual inspection of the SNRs over time of the measurements reveals the difference of counter values in many cases as depicted in Fig. 7a. Knowing from our previous investigations that the SNR over time develops a plateau while a TERO cell is oscillating, decreases afterwards, and has a knee when no more oscillations are seen in the time segment under observation, the graph can be interpreted: The first peak corresponds to the duration of the first oscillation, while the second oscillation is present until the plateau decays and the SNR vanishes in the noise floor of approx. 1 dB. In Fig. 7a the counter values, and thus the difference, is estimated quite accurately and only the sign bit is still secret when neglecting unreliable LSBs.

In contrast, Fig. 7b shows that revealing the counter differences from the SNR over time is more difficult in other cases. Still, by modelling the behavior of the TERO, the two apparently untypical peaks are explained: (i) The two



(a) Visual estimation (b) Model-based estimation

Fig. 7: SNR over time for two simultaneously activated cells ($N = 100$). a) visually estimated oscillation duration. b) additional model given as red dashed line.

TEROs have similar oscillation durations, (*ii*) we assume in our model that the TERO with the shorter oscillation duration has a 1.5 MHz higher oscillation frequency. Property (*i*) causes that the end points of the oscillation durations can hardly be distinguished, while (*ii*) results in a cancellation of the oscillations in the spectrum due to our relatively crude resolution in the frequency domain. The result of our model is marked by the red dashed line in Fig. 7b. Therefore, we suggest one of two approaches to develop automated side-channel analysis of the multi-bit extraction from TERO PUFs: either the frequency resolution is improved, e.g., using a spectrum analyzer, to minimize the probability of cancellation or a model can be fitted to the SNR over time to estimate the counter difference.

5.4 Interpretation and Countermeasures

The results of Sec. 5.2 and Sec. 5.3 prove that current methods to derive multiple bits per pair of TERO cells are vulnerable to side-channel attacks. We emphasize that this applies also to the derivation of multi-bit responses from other oscillation-based PUF primitives.

However, TERO PUFs can be protected by similar mechanisms as RO PUFs: (*i*) Increasing the number of counters decreases the attackers SNR as more TEROs oscillate simultaneously. (*ii*) Interleaved placement of counters and multiplexers is mandatory to prevent an attacker from spatially resolving them. (*iii*) The shuffling of compared TERO cells impedes averaging of measurements with the same TERO cell as the attacker does not know to which cell pair a measurement belongs. (*iv*) Restricting the TERO PUF to non-overlapping pair-wise comparisons and using only the sign bit impedes the presented attacks entirely. However, applying (*iv*) removes the claimed advantages of TERO over RO PUFs: The number of derived bits for TERO PUFs is then equal to the RO PUF, while the latter is more area-efficient due to the lower number of inverters. Alternatively to (*iv*), if the counter values are stored, comparisons can be made of the stored value. Hence, the oscillation of a single cell can only be observed

once revealing no additional side-channel leakage. Yet, this approach can also be applied to RO PUFs, i.e., the comparison above is not altered.

6 Conclusions

In this work, we studied different TERO PUF designs and how they can be attacked. Based on our conceptual analysis and modeling of the TERO PUF, we were able to identify several weaknesses and confirm them by our experiments. Our non-invasive EM measurements and tailored attack methodology exactly recovers up to 25% of the PUF bits without errors while the overall error probability of all estimated bits is below 18%. We point out that our approach is generic and applies to all known TERO designs. Even with our coarse measurement setup, and assuming a typical PUF scenario, where up to 20% errors are corrected, the remaining error probability is sufficiently small to consider the TERO PUF design with overlapping comparisons broken by our attack. With a slightly more advanced measurement setup, e.g., a spectrum analyzer, but applying our proposed technique, we assume that the improvement in terms of measurement enables a complete break of the TERO PUF even without the need of a smart guessing strategy.

Acknowledgement. This work was partly funded by the German Ministry of Education and Research in the project ALESSIO under grant number 16KIS0632.

References

1. Bayon, P., Bossuet, L., Aubert, A., Fischer, V.: Electromagnetic Analysis on Ring Oscillator-Based True Random Number Generators. In: 2013 IEEE International Symposium on Circuits and Systems (ISCAS2013). pp. 1954–1957 (May 2013)
2. Bossuet, L., Ngo, X.T., Cherif, Z., Fischer, V.: A PUF Based on a Transient Effect Ring Oscillator and Insensitive to Locking Phenomenon. IEEE Transactions on Emerging Topics in Computing **2**(1), 30–36 (March 2014)
3. Cherkaoui, A., Bossuet, L., Marchand, C.: Design, Evaluation, and Optimization of Physical Unclonable Functions Based on Transient Effect Ring Oscillators. IEEE Transactions on Information Forensics and Security **11**(6), 1291–1305 (June 2016)
4. Delvaux, J., Gu, D., Schellekens, D., Verbauwhede, I.: Helper data algorithms for PUF-based key generation: Overview and analysis. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **34**(6), 889–902 (June 2015)
5. Gassend, B., Clarke, D., Dijk, M.v., Devadas, S.: Silicon Physical Random Functions. In: ACM CCS (2002)
6. Haddad, P., Fischer, V., Bernard, F., Nicolai, J.: A physical approach for stochastic modeling of TERO-based TRNG. In: Güneysu, T., Handschuh, H. (eds.) Cryptographic Hardware and Embedded Systems – CHES 2015. pp. 357–372. Springer Berlin Heidelberg, Berlin, Heidelberg (2015)
7. Helfmeier, C., Boit, C., Nedospasov, D., Seifert, J.: Cloning physically unclonable functions. In: 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). pp. 1–6 (June 2013)
8. Immler, V., Specht, R., Unterstein, F.: Your rails cannot hide from localized EM: how dual-rail logic fails on FPGAs. In: Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings. pp. 403–424 (2017)
9. Katzenbeisser, S., Kocabaş, Ü., Rožić, V., Sadeghi, A.R., Verbauwhede, I., Wachsmann, C.: PUFs: Myth, fact or busted? a security evaluation of physically unclonable functions (PUFs) cast in silicon. In: International Workshop on Cryptographic Hardware and Embedded Systems. pp. 283–301. Springer (2012)
10. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. In: Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings. pp. 388–397 (1999)
11. Lohrke, H., Tajik, S., Boit, C., Seifert, J.P.: No place to hide: Contactless probing of secret data on FPGAs. In: Gierlichs, B., Poschmann, A.Y. (eds.) Cryptographic Hardware and Embedded Systems – CHES 2016. pp. 147–167. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
12. Maes, R., Van Herrewege, A., Verbauwhede, I.: PUFKY: A fully functional PUF-based cryptographic key generator. In: Prouff, E., Schaumont, P. (eds.) Cryptographic Hardware and Embedded Systems - CHES 2012. Lecture Notes in Computer Science, vol. 7428, pp. 302–319 (2012)
13. Marchand, C., Bossuet, L., Cherkaoui, A.: Design and Characterization of the TERO-PUF on SRAM FPGAs. In: 2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). pp. 134–139 (July 2016)
14. Marchand, C., Bossuet, L., Mureddu, U., Bochard, N., Cherkaoui, A., Fischer, V.: Implementation and Characterization of a Physical Unclonable Function for IoT: A Case Study With the TERO-PUF. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **37**(1), 97–109 (Jan 2018)

15. Merli, D., Heyszl, J., Heinz, B., Schuster, D., Stumpf, F., Sigl, G.: Localized electromagnetic analysis of RO PUFs. In: 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). pp. 19–24 (June 2013)
16. Merli, D., Schuster, D., Stumpf, F., Sigl, G.: Semi-invasive EM Attack on FPGA RO PUFs and Countermeasures. In: 6th Workshop on Embedded Systems Security (WESS'2011). ACM (Mar 2011)
17. Quisquater, J.J., Samyde, D.: ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards. In: Attali, I., Jensen, T. (eds.) Smart Card Programming and Security. Lecture Notes in Computer Science, vol. 2140, pp. 200–210. Springer Berlin / Heidelberg (2001)
18. Sauvage, L., Guilley, S., Mathieu, Y.: Electromagnetic radiations of FPGAs: High spatial resolution cartography and attack on a cryptographic module. ACM Trans. Reconfigurable Technol. Syst. **2**(1), 4:1–4:24 (Mar 2009)
19. Sigl, G., Gross, M., Pehl, M.: Where technology meets security: Key storage and data separation for system-on-chips. In: ESSCIRC 2018 - IEEE 44th European Solid State Circuits Conference (ESSCIRC). pp. 12–17 (Sept 2018)
20. Tebelmann, L., Pehl, M., Sigl, G.: EM Side-Channel Analysis of BCH-based Error Correction for PUF-based Key Generation. In: Proceedings of the 2017 Workshop on Attacks and Solutions in Hardware Security, ASHES@CCS 2017, Dallas, TX, USA, November 3, 2017. pp. 43–52 (2017)
21. The SALWARE Project: Source code of the TERO-PUF implementation on SRAM FPGA (2016), `https://perso.univ-st-etienne.fr/bl16388h/salware/tero_puf.htm`, retrieved on 11.02.2019
22. Unterstein, F., Heyszl, J., Santis, F.D., Specht, R.: Dissecting leakage resilient PRFs with multivariate localized EM attacks - A practical security evaluation on FPGA. In: Constructive Side-Channel Analysis and Secure Design - 8th International Workshop, COSADE 2017, Paris, France, April 13-14, 2017, Revised Selected Papers. pp. 34–49 (2017)
23. Varchola, M., Drutarovsky, M.: New High Entropy Element for FPGA Based True Random Number Generators. In: Mangard, S., Standaert, F.X. (eds.) Cryptographic Hardware and Embedded Systems, CHES 2010. pp. 351–365. Springer Berlin Heidelberg, Berlin, Heidelberg (2010)
24. Wild, A., Becker, G.T., Güneysu, T.: A fair and comprehensive large-scale analysis of oscillation-based PUFs for FPGAs. In: 2017 27th International Conference on Field Programmable Logic and Applications (FPL). pp. 1–7 (Sept 2017)