On-Line Reliability Estimation of Ring Oscillator PUF

Sergio Vinagrero Gutierrez, Giorgio Di Natale, Elena Ioana Vatajelu

On-Line Reliability Estimation of Ring Oscillator PUF

Sergio Vinagrero Gutierrez*, Giorgio Di Natale*, Elena-Ioana Vatajelu*

*TIMA (Univ. Grenoble Alpes - CNRS - Grenoble INP), Grenoble, France

***Abstract*—In this paper we propose an on-line test methodology for RO-PUF reliability which enables high accuracy in the results since it is not based on predictive simplified models of the device variability and noise, but on actual technological electrical models and high versatility since it is not based on measurements extracted from a single technology.**

***Index Terms*—device fingerprinting, ring oscillator, reliability.**

I. Introduction

Physical Unclonable Functions (PUFs) are cryptographic primitives that serve as low cost, tamper-free mechanisms for unique signature and secret key generation, and device identification. One of the most studied PUF architectures is the Ring Oscillator (RO) PUF due mainly to its simplicity. Reliability plays a big role when it comes to the wide adoption of PUFs in modern circuits. Due to reliability issues of today's PUFs, their implementation costs render them unsuitable for industrial applications, as shown in [1]. The goal of this work is to define a methodology to evaluate the reliability of the RO-PUF responses, based on the measured differences of the oscillation frequencies. This method will provide at run-time, besides the response to the challenge, the information whether the response is reliable or not.

Maes in [2] was among the first to demonstrate the the trade off between the PUF reliability and its entropy. Schaub et al. provide in [3] a generic probabilistic method for delay PUFs, where the trade off between reliability and entropy is modeled based on signal-to-noise ratio (SNR), and it is validated by real measurements. Another work, [4] of Martin et al., provides a PO-PUF reliability evaluation metric based on FPGA-extracted data. Here the trade-off between reliability and entropy is estimated from experimental data. It is also important to mention that reliability is heavily affected by aging [5], but it's effect is very difficult to study. In contrast, we propose a method that will improve the state-of-the-art as it provides a methodology to estimate reliable responses on-the-fly, based on an off-line study under different environmental conditions.

II. Preliminaries

Reliability is defined as the ability of the PUF to produce the same response for a given challenge under different operation conditions and aging. In the case of a RO-PUF, the frequencies of two ROs are compared to generate a response. By convention, if the frequency of the first RO is larger than the frequency of the second, the PUF response is 1, otherwise is 0. If the two frequencies are very similar, the response is prone to be unreliable since a small shift in the frequency in one of the ROs due to noise or environmental conditions can alter the response. Therefore, analyzing the frequency differences of all ROs in a PUF can give us a good measure of PUF reliability.

Based on the general agreement, the oscillation frequencies of all ROs in the PUF can be fitted to a normal distribution 1. Frequency differences close to 0Hz are possibly unreliable. For this case, we define a threshold T such that pairs for which $-T < f_{diff} < T$ are considered unreliable (area in yellow). Thus, reliability is calculated as $Reliability = 1 - [P(T) - P(-T)]$

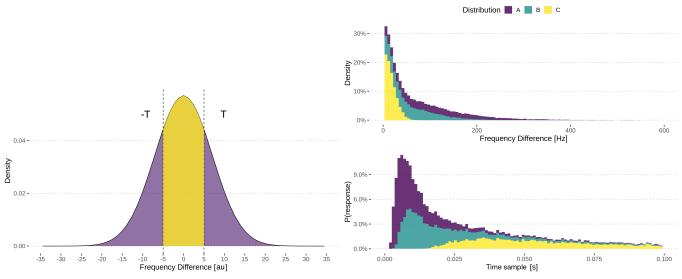

Fig. 1: On the left, distribution of frequency differences. Area in yellow marks unreliable responses. On the top right, three different distributions of absolute frequency difference. On the bottom right, the probability of obtaining a response for each distribution.

Furthermore, we can use the distribution of frequency differences to estimate the time needed to obtain a response for a certain challenge. The measurements of each RO frequency is performed resorting to a counter, which count at each rising edge of the RO, and the PUF response is obtained by comparing two counters. It has been observed that RO pairs whose frequency difference is very large can assure a meaningful counter difference early on, while pairs whose frequency difference is very small take more time to provide a meaningful counter difference since the frequency difference might be masked by the sampling effect of the counters, therefore, the two counters can register the same value, until the frequency lag becomes significant enough to counteract this effect. Our methodology is based on the observations that two RO start oscillating at the same time and any two sine waves with different frequencies will experience simultaneous zero-crossing periodically, at

intervals $T_{sync} = 1/f_{diff}$. As a result, any expected change in the counter difference must happen in a T_{sync} interval. If we observe the counter difference at certain intervals t_{sample}, we can define the *expected number of samples until the counter difference changes* as $E = T_{sync}/t_{sample} = 1/(f_{diff} \cdot t_{sample})$. By introducing the notion of frequency difference threshold for reliability (i.e., T) we can correlate the lag of meaningful counter difference with the reliability of the corresponding response.

III. Simulation Setup and Results

We base our study on 200 identically designed ROs with three CMOS inverters in 65nm technology provided by ST Microelectronics. We assume all ROs are affected by process variability. The output of a RO is connected to a counter (implemented in VerilogA) which increments its value at every rising edge of the oscillation. In this study, there is a total of 10.000 possible CPRs. The state of the counter has been sampled at each 1ns. To evaluate the PUF reliability, all ROs have been simulated under nominal conditions and environmental perturbations.

The results show that the effect of temperature variation is negligible as compared to supply voltage variation. Additionally, we can consider that there is no gradient of temperature inside the region of the circuit for the ROs, so we can consider that the working temperature is practically uniform. The distribution of frequency differences widens with increasing the supply voltages. This, according to the analytical analysis presented in section II means that at lower supply voltage the expected times to obtain a response are longer than for nominal supply voltage, which, in turn, can translate to lower reliability.

IV. Proposed Method

By convention, if the frequency of the first RO is larger than the frequency of the second, the PUF response is 1, otherwise is 0. If the two frequencies are very similar, the response is prone to be unreliable since a small shift in the frequency in one of the ROs due to noise or environmental conditions can alter the response.

Based on our observations from simulations and the general agreement on the variability distribution, the oscillation frequencies of all ROs in the PUF can be fitted to a normal distribution. RO pairs for which the frequency difference is very small are possibly unreliable and take more time to provide a meaningful counter difference. For this reason, when simulating the RO, we do not only retain the counter value at the end of the simulation time, but we also record intermediary counter values at a fixed time-step. In this way, when applying a challenge to the RO-PUF, we are able to calculate its response and also determine how fast this response can be obtained. The method can be described in the pseudo-code in figure 2. Using this method, the reliability of the RO PUF can be computed at every counter sample. More over, we can calculate the minimum counter difference required to achieve 100% reliability for every sample. This correlation is show in figure 2. A challenge whose counter difference is under the green line for any given time is considered unreliable and since the frequency difference of a pair will not change through time. This allows us to know early on if a challenge is going to be reliable.

The results after applying the proposed methodology to our simulations of the RO PUF are displayed in figure 3. It is shown the relationship between the reliability of the RO PUF, the minimum count different and the valid number of CRPs after filtering the responses that do not fall higher than the green line from figure 2. We can see that in our case, if we filter responses with a count difference lower than 4 at 80ns, we obtain while maintaining 79% of the CRPs.

```
N = numTemps * numVDDs * (nRO/2)^2
for i ← 1 to (nRO / 2) do
    for j ← 1 to (nRO / 2) do
        for c ← 1 to nSamples do
            # Calculation of nominal response
            R_nom[i][j][c] ← sign(Diff(i, j, c, V_n, T_n))
            # Calculation of reliability of each responses
            foreach T in Temperatures do
                foreach V in Voltages do
                    R ← sign(Diff(i, j, c, V, T))
                    if R = R_nom then
                        Rel[i][j][c] ← Rel[i][j][c] + 1
                    end
                end
            end
            # Calculation of PUF reliability
            Rel_puf[c] ← Rel_puf[c] + Rel[i][j][c]/N
        end
    end
end
```

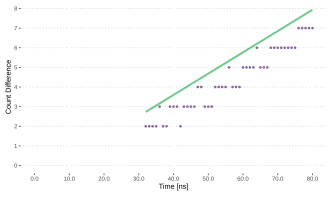

Fig. 2: On the left, the pseudo-code for our estimation method. On the right, correlation between minimum counter for reliable response and time of measurement.

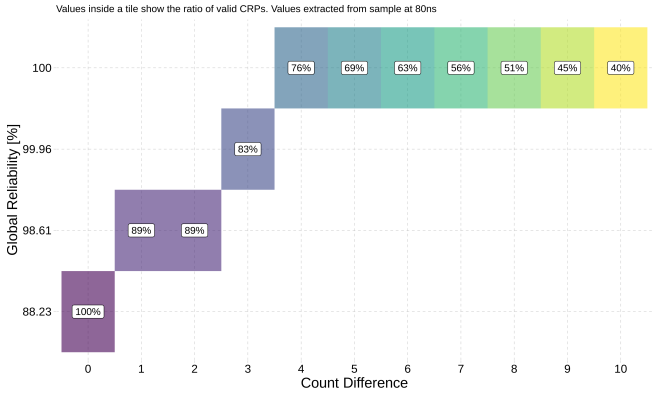

Fig. 3: Correlation between RO PUF reliability, count difference and number of valid CRPs.

References

[1] J.-L. et al, "Puf enrollment and life cycle management: Solutions and perspectives for the test community," in *2020 IEEE European Test Symposium (ETS)*, 2020, pp. 1–10.

[2] R. Maes, "An accurate probabilistic reliability model for silicon pufs," in *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 2013, pp. 73–89.

[3] J.-L. et al, "An improved analysis of reliability and entropy for delay pufs," in *2018 21st Euromicro Conference on Digital System Design (DSD)*, 2018, pp. 553–560.

[4] H. e. a. Martin, "On the reliability of the ring oscillator physically unclonable functions," in *2019 IEEE 4th International Verification and Security Workshop (IVSW)*. IEEE, 2019, pp. 25–30.

[5] G. D. N. et al, "A ring oscillator-based identification mechanism immune to aging and external working conditions," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. PP, pp. 1–23, 08 2017.