Analysis of Ring Oscillator Structures to Develop a Design Methodology for RO-PUF Circuits

Giray Kömürcü
National Research Institute of Electronics and Cryptology,
TÜBİTAK, 41470, Kocaeli, Turkey
Email: giray.komurcu@tubitak.gov.tr

Ali Emre Pusane, Günhan Dündar
Bogazici University, Dept. of Electrical and Electronics Eng.
34342 Bebek, Istanbul, Turkey
Email: {ali.pusane, dundar}@boun.edu.tr

***Abstract*—Ring Oscillators (RO) are the main primitives of Physical Unclonable Functions (PUFs) that generate chip specific signatures depending on the uncontrollable components present in the manufacturing process. RO-PUFs are one of the popular PUF types among various structures presented in the literature. However, due to the noisy nature of RO circuits, robust output generation is problematic in RO-PUFs. Maximizing the robustness of a PUF is the main design objective, and analytical solutions have not been developed yet to overcome this problem. In this work, RO structures are analyzed and the effects of RO inverter count and measurement time are examined theoretically and practically in terms of jitter and spatial variation. Next, a design methodology is presented to easily determine the measurement time and RO inverter count for best performing RO-PUFs. In addition to this, the design methodology is practically verified by comparing the jitter and spatial variation to the robustness measurements of previously built RO-PUF circuits.**

***Keywords*-Ring Oscillator, Physical Unclonable Functions, Robustness, Jitter, Spatial Variation.**

I. Introduction

PUF structures, which have the unique capability of generating chip specific signatures, were first introduced by Pappu *et al.* in 2001 [1]. Uncontrollable components, such as oxide thickness and threshold voltage, that are present in the manufacturing process maintain their unclonability property. These process variations cannot be replicated for another circuit, hence guaranteeing unique and chip specific signatures.

Optical PUFs are the first structures presented in the name of physical one-way functions [1]. Their impractical usage and integration problems prevented wide acceptance and silicon PUFs dominated the area with high integrability and less fabrication cost. Gassend *et al.* in 2002 [2], [3] presented RO based PUFs, extracting the output from delay differences of identically laid out structures. In standard RO-PUFs, frequencies of two identical ROs are compared and one bit output is generated [4]. Drawbacks of RO-PUF structures are their high power consumption and speed limitation. However, low sensitivity to environmental variations increases their strength in terms of robustness.

Although the RO-PUFs are better than the other PUF structures in terms of robustness, a 100% error-free output generation is still very hard to achieve, even without speed and resource usage considerations. There are two types of variations among RO structures that should be considered for a well-performing RO-PUF design. The first is the variation of the oscillation frequency within each RO at different time instances, which is called jitter. The second is the variation of oscillation frequency between identical ROs at different locations on the same integrated circuit and is called spatial variation. Due to the jitter phenomenon and environmental variations in ROs, some output bits generated by the circuit differ from measurement to measurement.

Jitter can be classified as short-term jitter and long-term jitter as explained in [5]–[8] in the literature. Short-term jitter is the instantaneous change on oscillations that are observed from period to period. Long-term jitter is the jitter over a time period and is also called accumulated jitter. Since the PUF operation requires measurements over a time period, accumulated jitter is subject to analysis in this work and the term jitter will refer to accumulated jitter throughout the paper. In order to generate outputs with minimum error using optimum resources and limited time, RO characterization in terms of accumulated jitter and spatial variation is required as a first step. In [7] and [9], spatial variation is presented based on measurements on FPGAs. The effect of number of stages and supply voltage on both jitter and spatial variation is presented by Johguchi *et al.* in [10] based on experimental data.

Even though ROs are well studied in the literature, the effects of number of stages and measurement time on accumulated jitter and spatial variation have not been studied in the context of PUF performance. We provide a design methodology for all types of RO-PUFs which guarantee maximizing their performance in terms of robustness, area and measurement time.

In this work, our contribution is threefold. Firstly, the effect of the number of RO stages on frequency, accumulated jitter, and spatial variation is analyzed theoretically and verified experimentally. Next, the effect of the measurement time on accumulated jitter and spatial variation is also analyzed. Finally, a solid design methodology for RO-PUFs is devised based on the foundations developed. With this methodology, the design of best performing RO-PUFs in terms of speed, area, and robustness is guaranteed. Experimental validation is also presented by using the results of previously built basic RO-PUF structures.

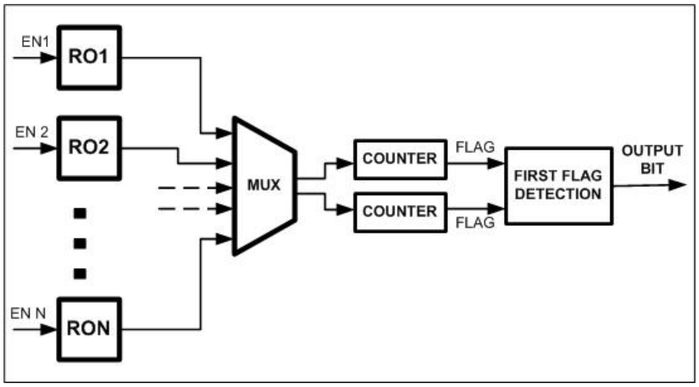

Fig. 1. PUF output bit generation.

The rest of the paper is organized as follows. Section 2 explains the bit generation mechanism of RO-PUFs and robustness. Sections 3 and 4 focus on the effect of the number of stages and measurement time on accumulated jitter and spatial variation. Section 5 presents the experimental validation of theory and Section 6 concludes the paper.

II. Output Generation Mechanism of RO-PUFs and Robustness

Before starting to characterize an RO to increase the robustness of RO-PUFs, both the output generation mechanism and the robustness should be fully understood. In regular RO PUFs, the output basically depends on the oscillation frequencies of two ROs with the same number of identical delay elements. By using two ROs, one bit response is generated. For instance, if RO1 is faster than RO2, the output is defined as 0, otherwise, the output is defined as 1. Since a PUF structure should generate more than one bit output, a number of identical ROs based on the RO-PUF structure are built in the circuit and two are selected for comparison during each bit generation. The mechanism to compare the oscillation frequencies of two ROs is to implement counters that will count the number of transitions of the RO outputs in a certain time interval, t_m, as shown in Figure 1. Finally, the system requires a comparator to determine which counter has the higher value and produce one bit output. To build the required amount of response bits, different ROs are compared and one bit data is generated for each comparison.

Due to the noisy nature of PUF circuits, stable outputs at each generation are very hard to achieve. As a result of environmental variations and internal characteristics, such as jitter, it is very likely for some bits to change their state from measurement to measurement. The number of these erroneous bits determines the robustness of an RO-PUF and should be very low or ideally zero for highly robust PUF circuits. Robustness can be measured in a number of ways as presented in [11]. The most common method is to calculate the mean error rate, defined as

$$R\_QM1 = \frac{1}{x}\sum_{y=1}^{x}\frac{HD(R_i, R'_{i,y})}{n} * 100\%, \qquad (1)$$

TABLE I
Notations and Meanings

Notation	Meaning of Notation
t_m	Measurement time
N	Number of inverters in an RO
M	Number of ROs in the design or analysis
$t_{d_{i,j,k}}$	Delay of the *j*th inverter in the *i*th RO at time instance *k*
t_{inv}	Nominal delay of an inverter gate
δs_i	Variation of mean gate delays of inverters in the *i*th RO
$\delta s_{i,j}$	Gate delay variation of the *j*th inverter in the *i*th RO
$\delta r_{i,j,k}$	Random delay component of the *j*th inverter in the *i*th RO at time instance *k*
σ_r	Standard deviation of the random delay component
$t_{r_{i,k}}$	Delay of the *i*th RO at time instance *k*
σ_{ro}	Standard deviation of the RO delay
$t_{d_{i,j}}$	Mean delay of the *j*th inverter in the *i*th RO for a number of measurements
t_{r_i}	Mean delay of the *i*th RO for a number of measurements
$t_{\Delta r_{i,i+1}}$	Delay difference of the *i*th and *i+1*th RO for one period
$t_{\Delta r_{i,i+1}}(t_m)$	Accumulated delay difference of the *i*th and *i+1*th RO after t_m
K	PUF output length
t_{PUF_K}	*K* bit PUF output generation time
$e_{PUF_{t_m}}$	Energy consumed per PUF operation

where HD(.,.) denotes the Hamming distance between two vectors, and R_i and $R_{i,y}$ represent the reference measurement and following measurements respectively.

Since the frequencies of ROs are determined via counters, oscillation counts within the measurement time t_m will be considered to characterize ROs in terms of spatial variation and accumulated jitter. The notation used in this paper is presented in Table 1.

III. Effect of the Number of Stages

The number of stages in an RO is one of the most important design parameters for an RO-PUF implementation. Theoretically, any odd number of inverter stages will work as an RO, and one bit PUF output can be generated by using two of these ROs. But, in practice, the number of stages has immense importance for the speed, jitter, spatial variation, and area of ROs, hence determining the performance of RO-PUFs.

Frequency of an RO is directly determined by the delay of a single inverter and the inverter count in the ring. Other factors that effect the oscillation frequency are the delay variation of inverters due to physical effects, and random variation caused by noise as explained in [12]. The total noise in the RO manifests itself as the jitter on oscillations. The following analysis is done for *M* ROs, RO_i, *i*=1,2..,*M*, which are built using *N* inverters, $INV_{i,j}$, *j*=1,2..,*N*, each. The delay of the *j*th inverter in the *i*th RO at time *k*, $t_{d_{i,j,k}}$, is given as

$$t_{d_{i,j,k}} = t_{inv} + \delta s_i + \delta s_{i,j} + \delta r_{i,j,k} \qquad (2)$$

In (2), t_{inv} is the nominal delay of the inverter, δs_i is the variation of mean gate delays of inverters in the *i*th RO, $\delta s_{i,j}$ is gate delay variation of the *j*th inverter in the *i*th RO, and

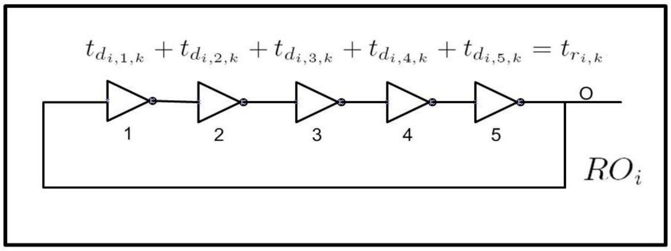
$t_{d_{i,1,k}} + t_{d_{i,2,k}} + t_{d_{i,3,k}} + t_{d_{i,4,k}} + t_{d_{i,5,k}} = t_{r_{i,k}}$
1
2
3
4
5
O
RO_i

Fig. 2. 5-stage RO schematic.

$\delta r_{i,j,k}$ is the random delay component. Here, δs_i, $\delta s_{i,j}$, and $\delta r_{i,j,k}$ can be assumed to be samples from Gaussian random variables (RV) with mean zero [13]. Therefore, $t_{d_{i,j,k}}$ is also a sample from a Gaussian RV with mean t_{inv}. The delay of an RO, hence the period $t_{r_{i,k}}$, is the total delay of inverters in the RO i as shown in (3).

$$\begin{aligned} t_{r_{i,k}} &= \sum_{j=1}^{N}(t_{inv} + \delta s_i + \delta r_{i,j,k}) \\ &= N * t_{inv} + N * \delta s_i + \sum_{j=1}^{N}(\delta r_{i,j,k}) \end{aligned} \tag{3}$$

Here, $\delta s_{i,j}$ component is discarded since the inverters of an RO are located very near each other, hence the variation within the RO is small and this variation does not effect the total RO delay significantly. Similar to the inverter case, $t_{r_{i,k}}$ is a sample from a Gaussian RV with mean $N * t_{inv}$ + $N * \delta s_i$ and t_r is a sample from a Gaussian RV with mean $N * t_{inv}$. Schematic and delay components of an RO is presented in Figure 2.

Accumulated jitter is the main source of erroneous bits in RO-PUFs and is composed of two noise sources, correlated and uncorrelated, as explained in [8]. Correlated noise highly depends on physical conditions such as layout and is likely to increase with growing number of delay elements [14]. The main source of uncorrelated noise is the random component in the inverter delay $\delta r_{i,j,k}$. As stated above, this random delay component can be safely assumed as Gaussian with zero mean and standard deviation σ_r. When the whole RO is considered, N delay elements are connected serially and their delays add up. In this case, N random delay components which are samples from Gaussian RVs are added. The resulting random delay component of the N-stage RO has again zero mean and N times the variance of a single inverter. Hence, the standard deviation of RO delay, σ_{ro}, is proportional to $N^{1/2}$. When the effect of correlated noise is considered, for large N, σ_{ro} may increase linearly with N as stated in [14]. But, employing a large number of stages is not very convenient for RO-PUFs due to speed and area limitations, hence this is not applicable for our discussion.

Spatial variation, which is the difference between identically laid out ROs at different locations of an integrated circuit and on different integrated circuits is the main mechanism for the RO-PUF architecture. The difference between the frequency of oscillations of ROs are used to generate chip specific signatures. In order to determine the optimum number of stages in an RO, period variation of a set of different ROs is analyzed. In this case, analysis is again done for M different ROs with N-stages. It is assumed that the measurements are repeated for a number of times and the results are averaged in order to vanish the random component. Thus, the delay of an inverter, $t_{d_{i,j}}$ can be stated as in (4).

$$t_{d_{i,j}} = t_{inv} + \delta s_i + \delta s_{i,j} \tag{4}$$

When summing the delays of inverters in an RO, the $\delta s_{i,j}$ component is discarded, since the variation within the RO is out of concern for spatial variation. Hence, the delay of the ith RO, t_{r_i}, is defined as in (5).

$$t_{r_i} = N * t_{inv} + N * \delta s_i \tag{5}$$

Here, δs_i is a sample from a Gaussian RV with mean zero and standard deviation σ_i. Since multiplying a Gaussian RV with a constant C increases the variance with C^2 and the standard deviation with C, t_{r_i} is a sample from a Gaussian RV with mean $N * t_{inv}$ and standard deviation $N * \sigma_i$.

Consequently, the standard deviation of jitter increases by $N^{1/2}$, whereas spatial variation increases by N for an N-stage RO. When the frequency of oscillations is considered, jitter decreases by $N^{1/2}$ and spatial variation decreases by N, since the frequency and period are multiplicative inverses of each other.

Since the robustness is linearly proportional to spatial variation and inversely proportional to jitter, an RO-PUF consisting of ROs with small number of stages is the optimum structure. This is also the best case for speed and area of implementation, as validated through an FPGA implementation.

IV. Effect of Measurement Time on RO

As mentioned above, RO-PUF bit generation depends on the oscillation counts of ROs within a certain time interval, t_m. Finding the optimum measurement time is a primary design objective, since it is closely related to speed and robustness of the system. In order to determine an optimum t_m, accumulated jitter and spatial variation are analyzed, since they are closely related to robustness. Accumulated jitter has two components, correlated and uncorrelated jitter, that depend on the measurement time [8]. Correlation coefficient of accumulated jitter in the system may be in the interval [0,1], depending on the components. If the noise is totally uncorrelated, the correlation coefficient is equal to zero. For a fully correlated system, the correlation coefficient becomes one. Since the correlated and uncorrelated jitter depend on time, the correlation coefficient of the system changes dynamically. As explained in [8] correlated component is proportional to t_m and hence dominates the uncorrelated jitter as t_m goes towards infinity. In addition to this, it becomes visible after a certain t_m depending on the technology and layout. In spite of this, uncorrelated component is dominant for small t_m and stabilizes within time since it is expected to be proportional to ${t_m}^{1/2}$. Therefore, when both components are considered, accumulated jitter should display less than linear increase for low t_m and a slope converging to one for large t_m. The effect of correlation is also discussed in section III in detail.

To analyze the effect of t_m on spatial variation, delay differences of identically laid out ROs are considered. By using (5), the delay difference for one period between two N-stage ROs, $t_{\Delta r_{i,i+1}}$, is calculated as in (6). Since $t_{\Delta r_{i,i+1}}$ is stable for all periods, it is directly proportional to the number of periods after t_m. The number of periods after t_m can be calculated as t_m/t_{r_i}. As a result, the total delay difference between two ROs after t_m is given in (7).

$$t_{\Delta r_{i,i+1}} = N * \delta s_i - N * \delta s_{i+1} \qquad (6)$$

$$t_{\Delta r_{i,i+1}}(t_m) = (t_m/t_{r_i}) * (N * \delta s_i - N * \delta s_{i+1}) \qquad (7)$$

In order to find the optimum t_m, accumulated jitter and spatial variation should be measured for various values of t_m and the point where the difference is the largest in favor to spatial variation should be chosen as the optimum t_m. At this optimum point, the effect of noise will be minimum, hence maximizing the robustness of the system. If there are more than one optimum points, the one with the lower t_m will be a better choice, due to speed and power considerations of the system. Selecting the optimum t_m has immense importance for the RO-PUF operation. Firstly, due to coupling problems, each output bit is generated one by one rather than activating all ROs and generating the entire output at the same time. This takes an important amount of time, $t_{PUF_K} = K * t_m$, that is proportional to the number of bits required and the time per bit. Even though one bit generation can be achieved within tens of microseconds, the total time required for a multibit key will be on the order of milliseconds, which slows down the system at each PUF output generation. Therefore, minimizing t_m without decreasing robustness is crucial. Secondly, t_m is directly proportional to the energy used by the PUF circuit. The energy used by a single inverter for one oscillation can be defined as $C_L * {V_{DD}}^2$ where the C_L is the load capacitance of the inverter and V_{DD} is the supply voltage. The energy used by an RO during one period is N times the energy of a single inverter. Since the RO continues to oscillate during the interval t_m, the energy consumed is t_m/t_r times the energy of an RO for one period. For K bit PUF output generation $2 * K$ ROs are used and the total energy consumed is stated as in (8).

$$e_{PUF_{t_m}} = 2 * K * (t_m/t_r) * N * C_L * {V_{DD}}^2 \qquad (8)$$

Therefore, optimizing t_m also optimizes the energy used and prevents unnecessary heating of the circuit.

V. Experimental Validation

ROs with 5, 7, 9, 11, 15, and 21 stages are built as hard macros on an FPGA to achieve identical layout, including the interconnects. 180 ROs are implemented on a Xilinx 3S5000 FPGA with frequency measurement circuitry based on counters and a serial port system. Since the oscillation frequency of 1 and 3-stage ROs are very high, we were not able to collect reliable data for them. In addition to this, due to area and speed concerns of PUF implementations, we did not measure beyond the 21-stage ROs. In this setup, each RO is activated one by one to minimize coupling and measured for 50 times consecutively to calculate the jitter. Each measurement result is then sent to a PC via the RS-232 interface and analyzed in MATLAB environment. Firstly, it is observed that the frequency of oscillations is inversely proportional to the number of stages as shown in Figure 3. To determine the accumulated jitter, standard deviation of 50 measurements from each RO is calculated and these values are averaged over 180 ROs, whose results are presented as the accumulated jitter in Figure 4. As seen from the graph, accumulated jitter of frequency decreases by $N^{1/2}$ as predicted via theoretical calculations. Spatial variation is measured by calculating the standard deviation of 180 distinct RO frequencies. In order to minimize the random component, mean of 13 measurements from each RO is taken to represent the frequency of that RO. The results shown in Figure 5 again validate the theoretical calculations since the spatial variation of frequency decreases as the number of stages increases.

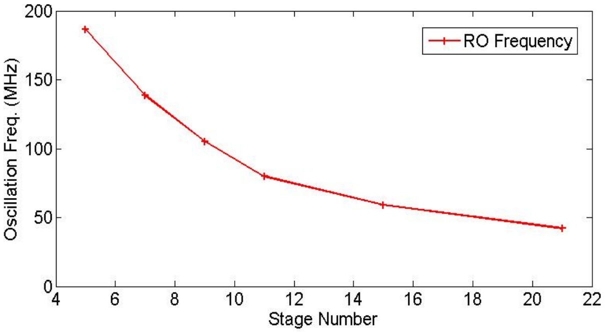

Fig. 3. Frequency of ROs vs. Stage Number.

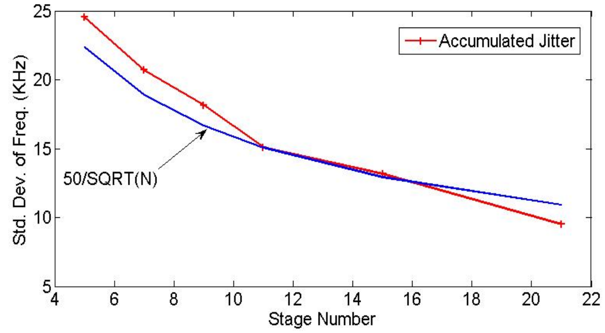

Fig. 4. Accumulated Jitter vs. Stage Number.

Optimum measurement time is analyzed experimentally via implementing 180 5-stage ROs and collecting data for 16 t_m values ranging exponentially from 0.16 μs to 5.2 ms. Each RO is measured for 50 times for each different t_m value. Based on

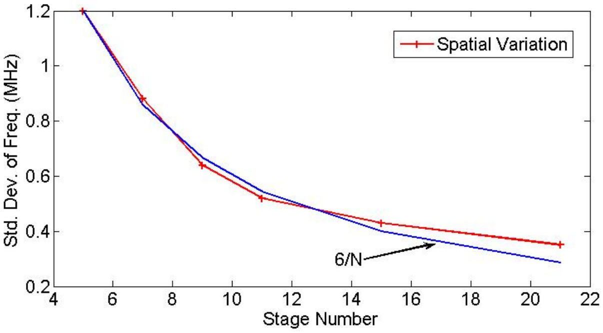

Fig. 5. Spatial Variation vs. Stage Number.

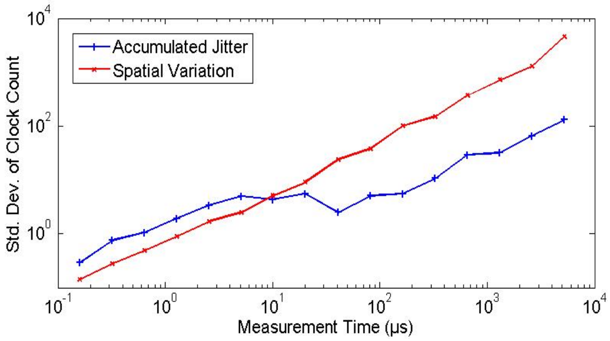

Fig. 6. Accumulated Jitter and Spatial Variation.

the measurements, accumulated jitter and spatial variation are calculated. As shown in Figure 6, which is plotted logarithmically in both axes, spatial variation is directly proportional to t_m and accumulated jitter settles down after a certain time and starts to increase linearly as the correlated jitter dominates the system. In the time domain until 10 μs, accumulated jitter is more than the spatial variation, preventing PUF operation. Between 10 μs and 0.2 ms, accumulated jitter does not change significantly, whereas spatial variation continues to increase monotonically, which we call the critical region. After 0.2 ms, both accumulated jitter and spatial variation increase linearly, hence their difference does not change significantly. Since the robustness of the system is closely related to the difference between these data, t_m=0.2 ms seems to be the optimal point for this particular technology and RO structure.

The method of determining the optimum t_m is verified using the robustness results of previously built RO-PUF structures presented in [11]. In this work, two different RO-PUF structures are built and their robustness and uniqueness are analyzed experimentally based on a set of quality metrics. This analysis is repeated for four different t_m values, which are exactly the same 4 t_m values that are in the critical region. This helps to verify the theory for determining the optimum t_m value. As shown in Figure 7, error rate percentage decreases until 0.2 ms, where the error rate settles or starts to increase slightly for four different metrics. These four metrics are mean and maximum error rate under normal operating conditions (NOC) before and after the application of majority voting (MV). This t_m value is also the optimum point for best robustness performance as explained in the previous paragraph verifying the proposed technique.

VI. Conclusions

We have developed a design methodology, for RO-PUF structures via analyzing the effect of the number of stages and measurement time on ROs in terms of jitter and spatial variation. According to this design methodology, lowest possible number of stages should be chosen for a robust, low area and power RO-PUF circuit. Measurement time should be chosen after analyzing the spatial variation and jitter in the real system. With this analysis, the minimum measurement time should be chosen to maintain the largest difference between the spatial variation and jitter in favor of the spatial variation, which will guarantee a robust, low area, and performance effective PUF operation.

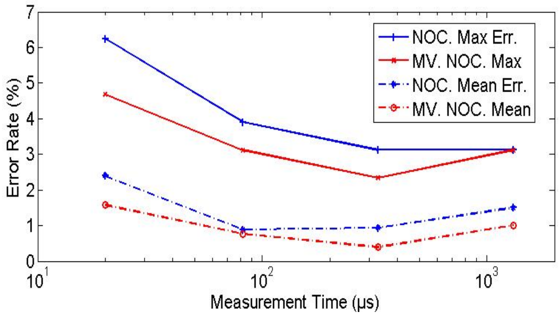

Fig. 7. Error Rate vs. Meas. Time for RO-PUF structure.

References

[1] R. S. Pappu, "Physical one-way functions." Ph.D. dissertation, Massachusetts Institute of Technology, 2001.

[2] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon pysical random functions," in *ACM Conference on Computer and Communications Security (CCS)*, 2002, pp. 148–160.

[3] B. Gassend, D. Clarke, M. Dijk, and S. Devadas, "Controlled physical random functions," in *18th Annual Computer Security Applications Conference (ACSAC)*, 2002.

[4] A. Maiti and P. Schaumont, "Improved ring oscillator PUF: An FPGA-friendly secure primitive," *Journal of Cryptology*, vol. 24, no. 2, pp. 375–397, 2011.

[5] V. Fischer, F. Bernard, N. Bochard, and M. Varchola, "Enhancing security of ring oscillator-based TRNG implemented in FPGA," *International Conference on Field Programmable Logic and Applications (FPL)*, pp. 245–250, 2008.

[6] V. Fischer, F. Bernard, N. Bochard, A. Aubert, and J. Danger, "True random number generators in configurable logic devices," *Project ANR - ICTeR*, pp. 23–28, 2009.

[7] S.Yoo, D. Karakoyunlu, B. Birand, and B. Sunar, "Improving the robustness of ring oscillator TRNGs," *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, vol. 3, 2010.

[8] C. Liu, "Jitter in oscillators with 1/f noise sources and application to true rng for cryptography," 2006, ph.D. dissertation, Worchester Polytechnic Institute.

[9] A. Cherkaoui, V. Fischer, A. Aubert, and L. Fesquet, "Comparison of self-timed ring and inverter ring oscillators as entropy sources in FPGAs," *Design Automation and Test in Europe*, pp. 1325–1330, 2012.

[10] K. Johguchi, A. Kaya, H. Mattausch, and T. Koide, "Measurement-based ring oscillator variation analysis," *Design and Test of Computers, IEEE*, vol. 27, 2010.

[11] G. Komurcu and G. Dundar, “Determining the quality metrics for PUFs and performance evaluation of two RO-PUFs,” *IEEE 10th International New Circuits and Systems Conference, NEWCAS*, 2012.

[12] S. Eiroa and I. Baturone, “Circuit authentication based on ring-oscillator pufs,” in *18th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, 2011, pp. 691–694.

[13] K. Wold, “Security properties of a class of true random number generators in programmable logic,” *Ph.D Thesis, Gjovik University College*, 2011.

[14] B. Valtchanov, V. Fischer, A. Aubert, and F. Bernard, “Characterization of randomness sources in ring oscillator-based true random number generators in FPGAs,” *13th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)*, 2010.