Enhanced ID Authentication Scheme Using FPGA-Based Ring Oscillator PUF

Van-Toan Tran, Quang-Kien Trinh, and Van-Phuc Hoang
Le Quy Don Technical University
236 Hoang Quoc Viet Str., Hanoi, Vietnam
Email: trantoantbb@gmail.com, kien.trinh@lqdtu.edu.vn, phuchv@lqdtu.edu.vn

Abstract—**FPGA-based ring oscillator (RO) PUF is very popular for its unique properties and easy implementation. However, the designs are normally expensive, and the RO frequency is highly sensitive to operating condition and other types of global variations. In addition, the local variations are also highly correlated, which normally requires complex the identification (ID) extraction algorithm and/or a large number of ROs. In this work, by using statistical analysis, we have experimentally shown that the RO frequencies are very sensitive to global variation factors. Fortunately, their local process variations within a die are relatively consistent regardless of the operating condition and this can be used for unique ID extraction. Furthermore, we have proposed an ID authentication scheme using FPGA-based RO PUF. Our proposed scheme allows to fully extract the local variation characteristics by using an almost technology- and vendor-agnostic PUF circuit. In addition, the ID extraction circuit is kept simple and compact, so that the overall design is area- and energy efficient. The experimental results show a very good level of reliability (99.94 %) for a design of 32 ROs in different physical FPGAs.**

Keywords—PUF, FPGA PUF, chip authentication, hardware security, ring-oscillator

I. Introduction

Thanks to advance in technology and design, state-of-the-art Field-Programmable Gate Arrays (FPGAs) find themselves sufficient powerful for a majority of applications [1]. As FPGAs intrinsically are CMOS devices so it is feasible to implement FPGA-based Physical Unclonable Functions (PUFs). PUFs undoubtedly are the most reliable random generator for majority hardware security device and can be used to extract the unique product identification used for authentication. While designing PUF on a full-custom CMOS circuit is quite straightforward, designing FPGA-based PUF normally requires special design methodologies and techniques. This because the most PUF circuits normally do not follow the common digital logic rules, they can be amended or trimmed during the logic optimization stage. In addition, PUFs circuit layout also strictly needs to be regular and symmetry, which typically is very difficult to control if not possible on reconfigurable logic. FPGA-based PUF is one of the exceptions as its implementation on FPGA requires the least complex (among FPGA-based PUFs) and the design is almost device-, technology-, and vendor-independent.

One of the first FPGA-PUF designs was proposed by Suh and Devadas in 2007 [3]. The RO-PUF circuit is comprised of n individual identical laid-out ROs as shown in Fig. 1. The output frequencies f_1–f_n are combinatorial selected by pairs f_i and $f_j (i \neq j)$ using a pair of multiplexers with the control bits as the PUF challenges. Due to the intrinsic process variations, and different operating conditions, f_i and f_j are typically different between rings in a single chip and between the same ring in different dies. The response value r_{ij} conventionally [5] is simply determined as

$$r_{ij} = \begin{cases} 1 & if\ f_i > f_j, \\ 0 & otherwise. \end{cases} \tag{1}$$

This method is not as effective as a significant portion of the information is dismissed after the threshold comparing function in (1). Correspondingly, many ring oscillators may be needed in order to extract reliable and unique chip identification. In addition, ROs apart from being highly sensitive to operating conditions and other sources of global variations, the local variations are quite correlated [11], making the conventional evaluation scheme not practical. Many prior works have focused on either improving the PUF quality at microarchitecture or improving the effectiveness of the entropy extraction process.

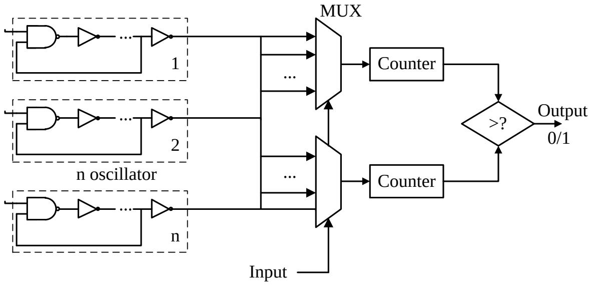

Fig. 1. Ring oscillator based PUF circuit.

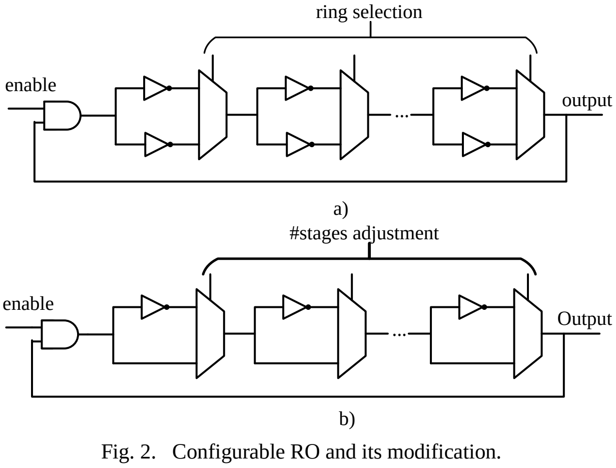

Fig. 2. Configurable RO and its modification.

Authors in [5] proposed configurable FPGA-RO PUFs that allow the inverters to be flexibly selected by a multiplexer (Fig. 2a). Accordingly, a N stage ROs could be configured generates 2^N different frequencies. Gao et. al. in [6] proposed a similar structure, where the number of stage inverters can be adjusted by multiplexer as shown in Fig. 2b. by doing so, the frequencies of each compared ROs can be chosen to be as different as possible after implementation to avoid the metastable outputs. This help increases the reliability and security for PUF design. However, these configurable methods [5, 6] lead to high complexity in hardware layout caused by the integration of multiplexers. Indeed, the multiplexer itself is more complicated than the inverters, consequently, maintaining the layout symmetry and regularity is especially challenging. In addition, the evaluation in those works follows the conventional way as described in [3].

There are also many prior works focused on methods to improve data processing efficiency. Fig. 3 shows the functional schematic of the RO PUF circuit. In the pairwise comparison method, n ROs can generate $n/2$ bits [3]. The neighbor chain approach [7] can form $n-1$ bits. In fact, these approaches have the only advantage in simplicity but do not fully exploit the information and extract all the features from the set of n random frequencies. To leverage the upper bound of the number of generated bits, Yin et al. in [8] grouped the ROs under given conditions, result in increasing the limit of bits generated from $O(n)$to $O(nlog_2n)$. The threshold $R_{th}$is set to guarantee the reliability so that the difference between frequencies in groups should not smaller than R_{th}. In another approach, to reduce systematic variations and utilize the random process variations, Yin and Qu in [9] designed a variation distiller based on using a polynomial curve fitting the trend of the systematic variations. In [10], the authors use Kendall Syndrome Code to replace the Compact Syndrome Code in order to guarantee reliability. However, these works did not cover the fact that in ROs, the impact of the global variations typically is stronger than the local variations. Thus the global impact needs to exclude during the ID extraction. In addition, the hardware implementation of this complex coding scheme can be too expensive.

The works in [11, 13] proposed that the ID can be extracted by the frequency difference of each RO pairs rather than just comparing their distance. This method effectively mitigates the impact of dynamic variations from the supply voltage and the temperature and the global process variations (i.e. die-to die process variations). The changes in voltage and temperature normally result in an equal impact on all rings, e.g., increase (decrease) temperature leads to reduction (increase) of the frequency [6]. However, the scheme in [6] adopts the conventional ID authentication using the binary Hamming distance [11] or using non-standard quantization approach [13], which may not be effective and adequate.

In this work, we propose a novel scheme of ID extraction using FPGA-based ROs. At the circuit level, we adopted a simple design of ROs and their frequency evaluation circuit. The design hence is compact and is readily implemented in any FPGAs devices and vendor with only minor changes. At the ID extraction stage, we also proposed a novel scheme that can be suited for both on-chip and off-chip processing. In our scheme, we also exclude the impacts of global variations and operating conditions as in [11]. The major difference is that we quantify the ID difference, not by the binary Hamming distance but Euclid distance when authenticating the ID. This reflects well the nature of the extracted information where each ID represents an n-dimensional vector. The proposed scheme offers a more reliable authentication scheme even small number of ROs, hence, being area- and energy-efficient. The remaining of the paper is organized as follows. In Section II, some details are provided to make the design clear. In Section III, we will evaluate a number of quantitative factors from measurement data to express some main features of a PUF. The proposed scheme of chip identification and authentication is present in Section IV. Finally, Section V concludes the paper.

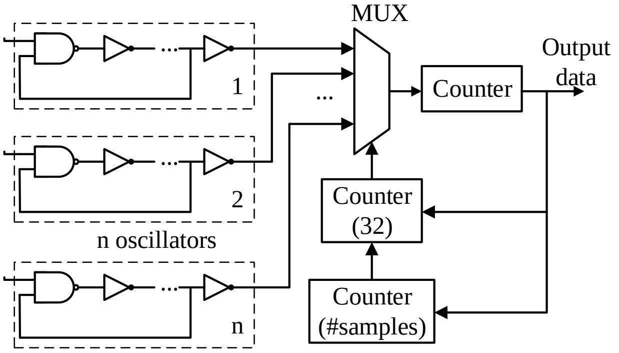

Fig. 3. Functional schematic of RO PUF circuit.

II. Implementation of FPGA-based RO PUFs

Our design is based on the basic RO PUF circuit proposed by Suh and Devadas with some modifications and targeted for Xilinx Spartan 6 Series FPGA. The delay element (inverter) of the RO occupies one primitive LUT. In order to maintain identical of ROs laid out, basic RO comprised 2^N inverters and a NAND gate manually routed by FPGA editor before encapsulating as an FPGA hard macro. Furthermore, we used only one counter, which evaluates ring frequency sequentially rather than using multiple counters in parallel because we will

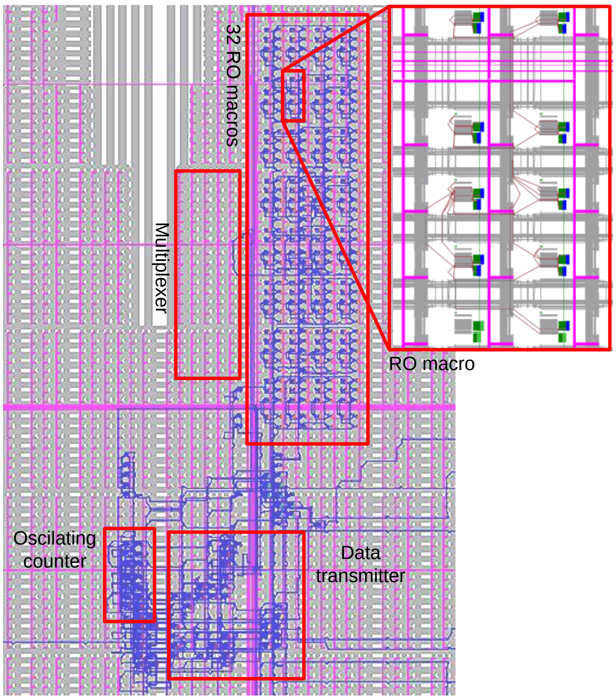

Fig. 4. RO PUF layout.

not adopt pairwise comparison here. This would help reduce the resource usage for evaluation circuitry and eliminate any possible bias caused by the counter. Furthermore, to ensure the symmetric layout, RO macros are precisely placed so that the relative distances between ROs to the evaluation counter are mostly the same as presented in Fig. 4. This theoretically maybe not necessary for low-frequency ring oscillators because the difference in frequency is eventually converted into a digital value by the counter. However, this can be important for the high-frequency ring (e.g., a few hundred MHz), where clock jitter could degrade the reliability. The generated clocks from ROs are multiplexed before feeding to the counter. The multiplexer, in turn, is controlled by a counter value to successively switch the oscillating signal from the ROs. With this design we keep the ROs as simple as possible, this would help to maintain better regularity, symmetry and the compactness of the ROs, as opposed to ROs designs in [3, 6, 7].

III. Evaluation of the Designed ROs Frequency

A. Statistic model of RO frequencies

The significant problems in using RO PUFs for identification and authentication are their sensitiveness to ambient temperature, fluctuations in supply voltage [3]. This leads to unstable RO PUF responses and they should not be used directly. The total delay in an RO can be modeled as

$$f_{RO} = f_{nominal} + \Delta f_{proc,local} + \Delta f_{proc,global} + \Delta f_{OP} \qquad (2)$$

Therein, $f_{nominal}$ is the nominal RO frequency (i.e. the frequency measured for the nominal device under the nominal condition, in this case is 25ºC, 1.0 V). This value remains constant across the rings, FPGA devices, and operating condition. The remaining components in (2) are random variables; $\Delta f_{proc,global}$ and $\Delta f_{proc,local}$ are frequency variations due to global process variation (i.e., die-to-die variation) and local process variation, respectively; Δf_{OP} is a frequency offset due to the operating condition.

In this work, we have implemented 32 ROs, comprising 16 inverter states. evaluated by 1024 samples. Those samples are transferred directly to the host computer for post-processing via a serial interface.

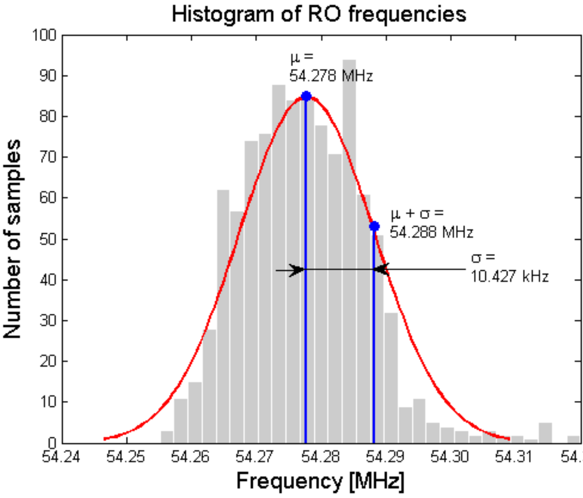

Fig. 5. Histogram of frequency samples of RO5/IC1 retrieved from 1024 repetitive measurements.

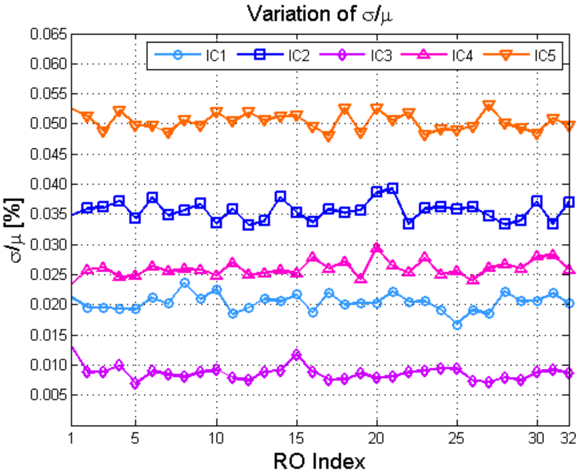

Fig. 6 σ/μ ratios of 32 ROs of 5 ICs estimated from 1024 samples in ambient temperature 25ºC

The detail functional schematic of the design is shown in Fig. 3 while the physical layout is shown in Fig. 4. This Section examines the experimental results of ROs frequencies retrieved from a design of 32 ROs for 5 different FPGA devices. The major quality factor is *reliability*, intra-die, and inter-die *uniqueness.* To quantify these performances, we used metrics based on Euclidean distance estimation.

B. Impact of the Temporal Fluctuation

The frequency value was repeatedly measured multiple times for 32x5 ROs under a fixed operating condition (25ºC, 1.0 V voltage core). The frequencies of a particular RO is hence is varies due to the stochastic fluctuation during the operation in temperature and the supply voltage. For a single RO, this fluctuation is corresponding to the Δf_{OP} variation under a fixed nominal operating condition. This impact is quantified by the *reliability factor* [15] $(1 - \sigma/\mu)$ (in percentage), in which μ is mean value of sample frequencies and σ is the standard deviation of the frequency distribution.

Fig. 5 shows a histogram from 1024 repetitive measurements for RO5 in IC5. The mean frequency is 54.28 MHz and the standard deviation is 10.43 KHz, correspondingly the temporal (σ/μ) is just ~0.02% (the expected is less than 1% according to [2]).

The measured temporal (σ/μ) of 5×32 ROs are presented in Fig. 6, which are retrieved from evaluating 32 ROs of five FPGA. From the estimation, the σ/μ ratios of ROs have the min value of 0.0069% (RO5/IC3) and the max value of 0.0532% (RO27/IC5), corresponding to the reliability of 99.99 % and 99.94 %, respectively. This result indicates that the temporal fluctuation has little impacts on the ROs measured frequencies and can be ignored in further analysis.

C. Impacts of the Temperature

To quantify the dependence of the RO frequencies on the ambient temperature, we have conducted the measurement for all FPGA devices under different temperatures (25ºC, 40ºC, 55ºC, and 70ºC). The measurements have been repeated for 256 times for each of 5×32 rings in order to calculate their mean frequencies. The major results are presented in Fig. 7(a)-(e), and are consolidated in 7(f) by a 3D surface. The RO indices are intentionally sorted by

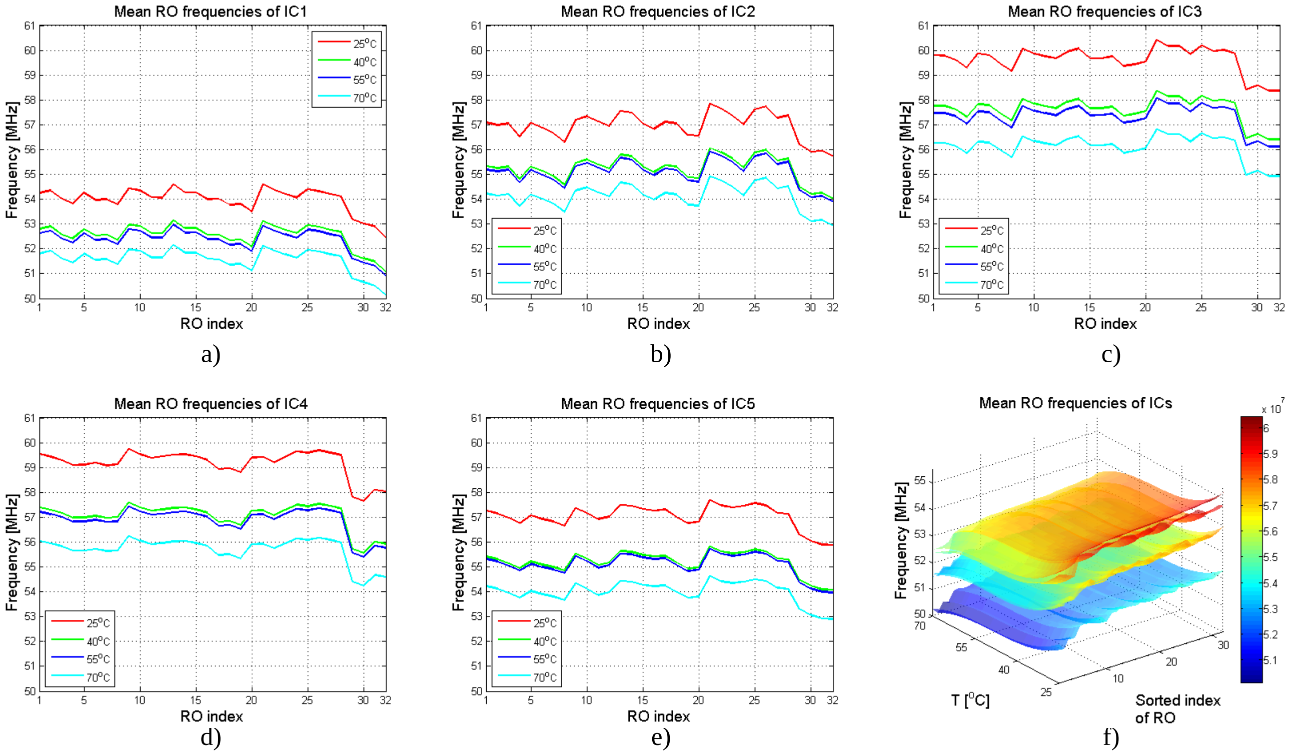

Fig. 7. (a)–(e) Variation of mean ROs frequencies and (f) 3D-illustration of the ROs frequencies change with respect to temperature (at 25ºC, 40ºC, 55ºC, and 70ºC), measured for 5 physical FPGA devices.

the increment of mean frequencies of IC3 in order to keep the 3D surface smooth and to express clearly changing the pattern. This shifting of frequencies essentially reflects the mean value of the Δf_{OP} due to operating condition in (2).

From the figure, the dependence of RO frequencies on temperature are quite strong and follow a predicted pattern. Specifically, the increasing temperature would lead to reducing in the RO frequencies (as the switching of the transistor getting slower). It can be observed that increasing temperature from 25ºC to 70ºC results in equally shifting the mean frequencies of ROs by 2.34-3.59 MHz.

Furthermore, the ROs frequencies do not necessary to be linear because of the non-linear dependence of the transistor current on the temperature at advanced technology node [14]. Changing temperature from 40-55ºC leads to decrease only 0.09-0.29 MHz. Nonetheless, these differences are much greater than the temporal fluctuations (by approximately 10-30 times of sigma values) reported in the last section. This confirms the fact that absolute frequencies values are not suited for unique ID extraction as they may vary in a wide range.

D. *Impacts of the Global And Local Process Variations*

The process variations are the combination of the local (within-die) and global (die-to-die) variations, which are represented respectively by $\Delta f_{proc,local}$ and $\Delta f_{proc,global}$ in equation (2). For the global variation, we could observe from Fig. 7(f) that for a dedicated ROs, its frequency could vary significantly from die-to-die. For example, for RO5 the frequency shifted up to 5.61 MHz from IC1 to IC3 at 25ºC.

Interestingly the frequency surfaces in Fig. 7(f) are all shifted up or down from IC to IC, and this phenomenon is valid even under different temperatures. For examples, from Fig. 7 and 8, all ROs frequencies increase by about +1.73 MHz to +3.41 MHz from IC1 to IC2 regardless of the temperature. In a broad sense, the impact of the temperature can be a global factor as it equally affects the ROs as the global process variation. These impacts, unfortunately, are quite significant so that the solely ROs frequency have very weak uniqueness, hence, the frequency values cannot be directly used for characterized the physical devices.

Furthermore, we examine the local variation impacts, i.e., the difference in RO frequency across ROs in a single device. From the measurement mean values of the frequencies of 32 rings are populated in Fig. 7(a)-(f). The ripples of the surfaces caused by dissimilarity of ordered RO sets would represent the impacts of $\Delta f_{proc,local}$ in (2).

As has been reported in many prior works that within a large number of ROs, the cases of two or more RO frequencies being close to each other are quite common. Our design is not an exception. As shown in Fig. 7(f) respected to IC1 in 25ºC, the RO14 and RO15 are the difference by only 1.88 KHz. With the temporal standard deviation of 11.16 KHz, the probability of getting the same frequencies is 0.91. In such a case, the pairwise method could easily result in an ambiguous response bit. Particularly, between RO8 and RO18, RO23 and RO27, RO21 and RO13, the probability of the flipping response bit is close to 1.0. That for RO1 and RO5 is 0.55. Those high probability values indicate that we may need to exclude some of the rings from the list if we use the traditional pairwise bit extraction. However, this may be not necessary if the other methods [5, 8] are used because the level of similarity in ROs can be used as a distinctive feature of a specific IC as discussed later.

Furthermore, the local differences are typically small (17 Hz to 65.27 KHz). However, it is interesting that the pattern of local variation is very stable with respect to the

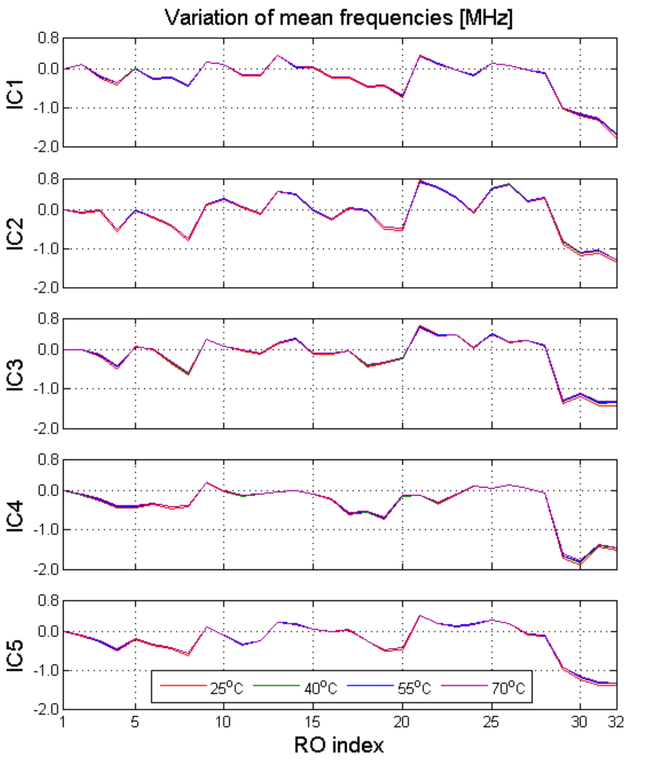

Fig. 8. Zero-centered frequency plots of the local variations for 5 ICs under different temperatures.

temperature. This can be already observed in Fig. 7(a)-(e) that the zig-zag curves for a single FPGA are mostly the same across temperatures. To have a better quantitative analysis, we remove the bias frequency caused by the temperature by subtracting the first ROs frequency. This shifted all frequencies to the zero-centered range as plotted in Fig. 9. It can be seen that the local variation impacts are mostly identical so that they are not visibly distinguishable in the figure. The maximum point-to-point frequency drift for obtained data is just about 65.27 KHz, which is at the same order of the temporal fluctuation. The similar results were recorded for other devices (hence, being omitted here). The excellent stability in local variation with respect to the operating condition could be the key characteristic of FPGA PUFs, which eventually can be exploited to extract the IC distinctive features. This will be discussed in the following section.

IV. IC Identification Extraction and Authentication Scheme

A. Conventional ID Extraction Scheme

The previous Section gives insights into the impacts of different variation sources. The results confirm that the ROs frequencies are highly sensitive to global variations and operating condition, thus, cannot be used directly for unique feature extraction. Fortunately, within a die, the local variations are quite consistent regardless of the operating condition (in this case the temperature) and this can be exploited for ID extraction.

As the first step, to obtain only data the local variation, all frequency biases due to global variations, that include global process variation and temperature dependence, need to be excluded. From Fig.7(f), it is predicted that we could remove the impact of global process variation and/or voltage and temperature dependent component by taking not the actual frequencies but the differences among them. The latter represents essentially the only local variations within the individual chip. Therefore, in a generic form, the ID is the function of the local variation information and can be expressed as

$$ID = F(\{\Delta f_{ij}\}) \qquad (3),$$

where $\Delta f_{ij} = f_i - f_j$ represent the local variations, the number of pairs (i, j) depended on the particular scheme. In the conventional ID extraction using neighbor pairwise [11], F is simply the sign function.

Fig. 9 shows the frequencies difference, taken from the two consecutive frequencies $(i)th$ and $(i+1)-th$ plot of all ROs at 25°C. As can be seen, each IC now is represented by only the local variations curves and they apparently are different from each other. However, the close analysis shows that there is a strong correlation between the local variations and hence, the response bits. Specifically, the RO20 tends to be the fastest among all rings across ICs, and RO28 tends to be the slowest. This phenomenon has been pointed out in [3]. If we again apply the neighbor pairwise method as in [11] but taking only one bit: 1 (0) if $(i+1)-th$ RO is faster (slower) than $(i)th$ RO, i.e., $F = sign\,(f_i, f_{i+1})$. Results of this method are shown for cases of different number of rings n_{RO} is shown in Fig. 10.

As can be seen with a large number of rings, when n_{RO} = 32 (24), the minimum hamming distance between IDs are 7 (20%) 6-bit (22%). However, when n_{RO} = 16 the IC2 and IC5 are different by just 3 bit (0.2%). For n_{RO} = 8 IC3 and IC5 are even not distinguishable. Note that variations of Hamming distance for cases are quite large (0.57, 0.27, 0.30, 0.23 for 31, 23, 15, 7 ID bit-length, respectively), so the reliability of the current method is not high. This data is calculated for only small populations, so with a larger number of physical devices, this conventional method will not be applicable. This could be another serious drawback of the RO PUF, for reliable ID authentication we would need a larger number of ROs, hence the design is highly area-inefficient.

B. Proposed ID Extraction Scheme

Results from the last subsection indicate that using only one-bit extraction by sign function is not enough due to the strong local variation correlation. Specifically, taking only “faster” and “slower” property would be not enough.

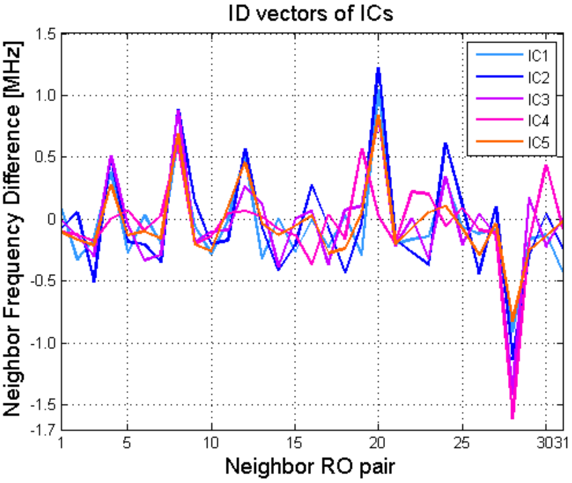

Fig. 9. Zero-centered frequencies plot of local variation for 5 chips at 25°C.

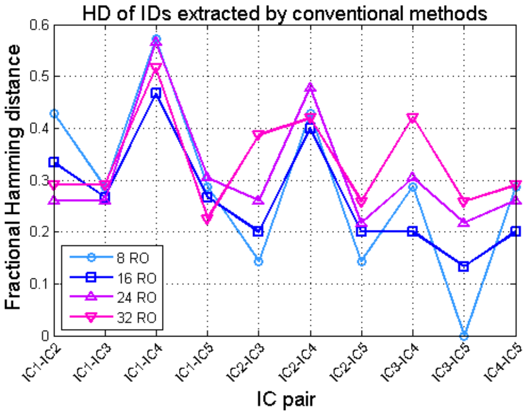

Fig. 10. Fractional Hamming distances of ID extracted by the conventional neighbor-pairing method.

This suggested that we would need to take more detailed information or entropy from the local variations. Specifically, the magnitude of the changing pattern of the RO frequencies. In such sense, we do not need to exclude similar ROs, as their level of similarity can be treated as one of the unique features. The similar approach has been proposed in [13] although the root cause of the ID instability was not systematically studied.

The proposed ID extraction and authentication scheme is shown in Fig. 11 that could enhance ID extraction by fully quantifying the characteristics of the local variation. This would help gain additional information and reduce authentication failure possibility effects of ROs.

For the ID extraction, from the $n \times m$ bit raw ROs frequencies, which are sequentially latched by the counter (see. Fig. 3), each consecutive neighbor frequency pair produces a $k - bit$ response by a comparator. k can be much smaller than m because it represents only the magnitude local difference between frequency (in this particular design $m = 32,\ k = 21$). The final ID is a $(n-1) \times k$-bit vector, i.e., much longer than the ID retrieved from the conventional method. Because timing is not critical in this phase, so the ID can be read out sequentially. This would require a minimum just one counter and one comparator for the whole process and the circuit is very compact.

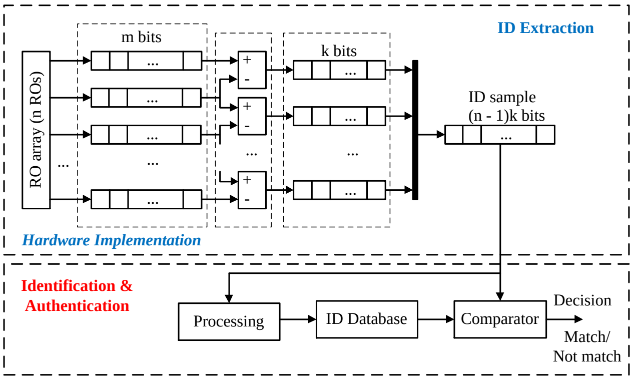

Fig. 11. Proposed ID extraction and authentication scheme.

At this phase, our scheme is very similar to the proposed method in [13]. The major difference is in the evaluation and authentication phase and the way we treat the ID.

From the mathematical point of view, the ID is characterized by a $(n-1)$ dimension vector $\boldsymbol{R}(\{\delta_i | i = \overline{1, n-1}\})$, where

$$\delta_i = f_{i+1} - f_i \tag{4}$$

is the magnitude of the *i-th* neighbor frequency difference. The vector $\boldsymbol{R}$ for each IC essentially characterizes the unique zig-zag pattern in Fig. 9, which are experimentally verified to be quite stable with respect to the global variation factors. The final form of the ID will be digitally represented by $(n-1)$-dimensional vector $\boldsymbol{R} = \{\delta_i, i = \overline{1, n-1}\}$, with each element δ_i is the k-bit value in 2's complement format.

Furthermore, we use the Euclidean distance rather than the binary Hamming to quantify all of the ID metrics. The Euclidean distance between vectors R_i and R_j is conventionally defined as $d(\boldsymbol{R_i}, \boldsymbol{R_j}) = \sqrt{\sum_{k=1}^{n-1}(\delta_{ik} - \delta_{jk})^2}$. The normalized intra-distance hence is defined as follows[1]

$$d_{intra} = \frac{d(\boldsymbol{R_l}, \boldsymbol{R})}{2^k\sqrt{n-1})} \tag{5}$$

Therein, $\boldsymbol{R_l}$ is the ID of $l - th$ measurement, $\boldsymbol{R}$ is the nominal magnitude of the ID vector, $d(\boldsymbol{R_l} - \boldsymbol{R})$ is the Euclidean distance between $\boldsymbol{R_l}$ and. Note that the nominal value of ID R is statistically calculated from sufficient large repetitive measurement samples ID. This d_{intra} value reflects the variation of $d(i)$ under various ambiance temperatures and or the fluctuations of the supply voltage, d_{intra} is expected to close to zero.

Given a set of N IDs, the inter-distance, which represents the level spatial distribution (uniqueness) of the IDs across ICs can be represented as

$$d_{inter} = 1 - \sum_{i,j} \frac{2d(\boldsymbol{R_i}, \boldsymbol{R_j})}{N(N-1)2^k\sqrt{n-1})} \tag{6}$$

For a good IDs set the *d_inter* is close to 0.5 (50%), however, this essentially requires a significantly large number of IDs for evaluation.

The equations in (5) and (6) are actually generalized of the proposed metric in [15], where the binary Hamming distance is replaced by the Euclidian distance, which would be more appropriate to quantify the magnitude of vector components.

C. Evaluation of the ID Stability

Using the proposed scheme, we have calculated the IDs for IC1 first for repetitive 256 measurements, the graphically illustrated of IDs are represented in Fig. 12. And the distributions of the normalized intra-distance is plotted in Fig. 13.

From Fig. 12, it can be seen that the IDs of IC1 retain mostly the same from sample to sample. This can be quantified by the distributions of the distance between the IDs with respect to the nominal ID in Fig. 13. Here the nominal ID

[1] The maximum distance between 2 (n–1)-dimensional vector of k-bits value is $2^k\sqrt{n-1}$

is $\boldsymbol{R} = \{mean(\delta_i), i = \overline{1, n-1}\}$. The maximum normalized distance is 4×10^{-3}. The maximum standard deviation of the normalized intra-distance is just $\sigma_{d_{intra}}$ = 4.2 $\times10^{-4}$. Correspondingly, the probability that one ID measurements located outside the hypersphere with center R and radius $6\sigma_{d_{intra}}$ is 10^{-9} (one per billion). This results are well in line with our analysis before in Section III.B that the impact of temporal fluctuations are insignificant and the measured IDs are relatively stable with respect to the temporal fluctuation.

Furthermore, the nominal ID vectors for all 5 ICs at different temperatures (25°C, 40°C, 55°C, and 70°C) are shown in Fig. 14. Those IDs are visibly the same and the close analysis shows that the maximum normalized distance between the nominal IDs, measured for an IC across temperatures is 23×10^{-3}. The quantitative results presented above prove our observation before that the local variations are very consistent regardless of the operating condition and temporal fluctuation.

Practically, we would take the upper-bound of the intra-distance for determining the threshold of the ID authentication process. Specifically, if we take the threshold distance is the maximum value of $6\sigma_{d_{intra}}$ (standard deviation of the temporal normalized intra-distance) from a large set of sample IDs. If the sampling is all done at a fixed temperature, then the threshold is small (i.e. $d_{threshold}$ = 22.2 × 10^{-3}, being $\sigma_{d_{intra}}$ = 3.7 × 10^{-3}). This threshold distance would increase if sampling is conducted under different temperature conditions. In our particular experiment, the normalized threshold becomes $d_{threshold}$ = 28.8×10^{-3} (being $\sigma_{d_{intra}}$= 4.8×10^{-3}).

At the authentication phase, if two ID samples having the intra-distance less than $d_{threshold}$ are considered physically different, in contrast, the two ID sample are matched if they have the normalized intra-distance does not exceed $d_{threshold}$. Correspondingly, the main functionality of the authentication unit is to calculate the normalized distance to give the decision. This would eventually involve the square and square root. Fortunately, this phase is typically done off-chip by the computer, the calculation complexity hence is not a problem.

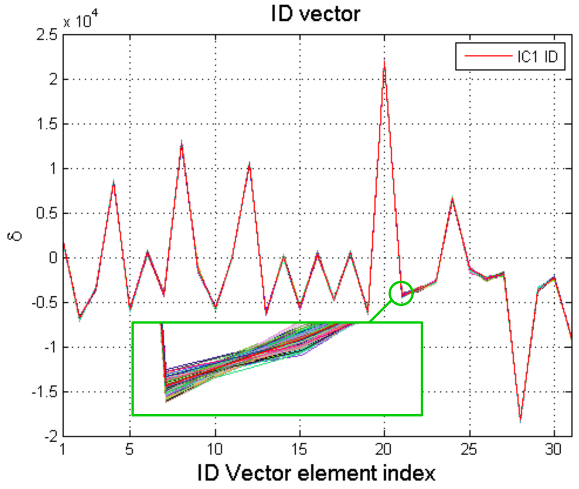

Fig. 12. Reliability of the Extracted ID again temporal variation impacts.

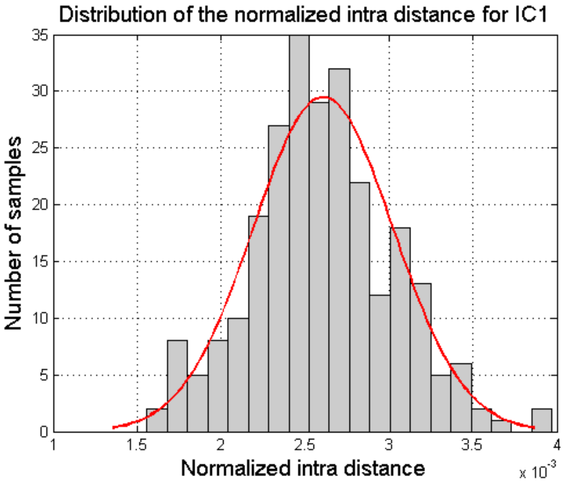

Fig. 13. Histogram of the normalized intra-distance for IC1 for 256 measurements.

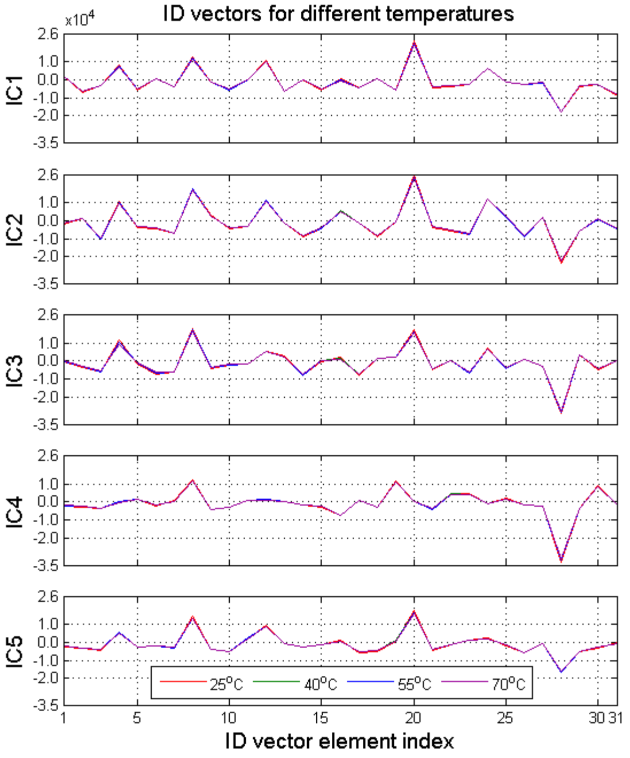

Fig. 14. Reliability of the extracted ID for 5 ICs with respect to changing of ambient temperature.

A. The ID Uniqueness

In these experiments, the number of physical devices is limited to 5 so, it would be not sufficient to have reliable statistical results about the randomness and uniqueness of the ID set. Table I shows the normalized distance between the IDs. From the Table, it can be observed that the minimum distance between them is 100.5×10^{-3} found between IC2 and IC5. This minimum distance is ~4.5 and ~3.5 times greater than the thresholds when the authentication is conducted at the same temperature and when there is no restriction in operating temperature, respectively. This would eventually create a sufficiently large margin for distinguishing the physical devices. So, the proposed scheme exhibits a very strong level of reliability.

TABLE I. NORMALIZED DISTANCE BETWEEN THE IDS.

IC2	IC3	IC4	IC5	
141×10^{-3}	146.4×10^{-3}	224.7×10^{-3}	100.5×10^{-3}	IC1
	154.4×10^{-3}	249.2×10^{-3}	140.2×10^{-3}	IC2
		194.5×10^{-3}	128.3×10^{-3}	IC3
			181.2×10^{-3}	IC4

V. CONCLUSIONS

In this work, we have systematically studied the impact of variations on RO PUFs. From the experimental results, we found that the actual RO frequencies are very sensitive to global variation factors such as operating condition and global process variations. Fortunately, the pattern of the local process variations within a single die is observed to be very consistent and that can be used for unique ID extraction. We have proposed an ID extraction and authentication scheme using FPGA-based RO PUF. In our scheme, the vector ID comprises of the neighbor pair frequency difference that self-exclude the bias due to global variations, and hence, characterizes only the local variation. The experimental results show a very good level of reliability. In addition, the circuit designs for both ROs array and ID extraction are kept simple and generic, thus, can be readily ported to other FPGAs with minimum modifications.

REFERENCES

[1] Joost, Ralf, and Ralf Salomon. "Advantages of FPGA-based multiprocessor systems in industrial applications." *31st Annual Conference of IEEE Industrial Electronics Society, 2005. IECON 2005.*. IEEE, 2005.

[2] Roel, M. A. E. S. "Physically unclonable functions: Constructions, properties and applications." Katholieke Universiteit Leuven, Belgium (2012).

[3] Suh, G. Edward, and Srinivas Devadas. "Physical unclonable functions for device authentication and secret key generation." *2007 44th ACM/IEEE Design Automation Conference*. IEEE, 2007.

[4] Vivekraja, Vignesh, and Leyla Nazhandali. "Circuit-level techniques for reliable physically uncloneable functions." *2009 IEEE International* Workshop *on Hardware-Oriented Security and Trust*. IEEE, 2009.

[5] Maiti, Abhranil, and Patrick Schaumont. "Improved ring oscillator PUF: An FPGA-friendly secure primitive." *Journal of cryptology*24.2 (2011): 375-397.

[6] Gao, Mingze, Khai Lai, and Gang Qu. "A highly flexible ring oscillator PUF." *Proceedings of the 51st Annual Design Automation Conference*. ACM, 2014.

[7] Yu, Meng-Day, and Srinivas Devadas. "Secure and robust error correction for physical unclonable functions." *IEEE Design & Test of Computers* 27.1 (2010): 48-65.

[8] Yin, Chi-En. Kendall Syndrome Coding (KSC) for Group-Based Ring-Oscillator Physical Unclonable Functions. 2011.

[9] Yin, Chi-En, and Gang Qu. "Improving PUF security with regression-based distiller." *Proceedings of the 50th Annual Design Automation Conference*. ACM, 2013.

[10] Yin, Chi-En, and Gang Qu. "Temperature-aware cooperative ring oscillator PUF." *2009 IEEE International Workshop on Hardware-Oriented Security and Trust*. IEEE, 2009.

[11] Kim, Inyoung, et al. "From statistics to circuits: Foundations for future physical unclonable functions." *Towards Hardware-Intrinsic Security*. Springer, Berlin, Heidelberg, 2010. 55-78.

[12] Yin, Chi-En Daniel, and Gang Qu. "LISA: Maximizing RO PUF's secret extraction." *2010 IEEE International Symposium on* Hardware-*Oriented Security and Trust (HOST)*. IEEE, 2010.

[13] S. Eiroa and I. Baturone, "Circuit authentication based on Ring-Oscillator PUFs," 2011 *18th IEEE International Conference on Electronics, Circuits, and Systems*, Beirut, 2011, pp. 691-694.

[14] N. Weste, and D. Harris, *CMOS VLSI Design: A Circuits and Systems Perspective (4th ed.)*. Addison-Wesley Publishing Company, USA, 2010.

[15] R. Maes, *Physically Unclonable Functions*. Springer, 2013.