A Robust Euclidean Metric Based ID Extraction Method Using RO-PUFs in FPGA

Van-Toan Tran, Quang-Kien Trinh, and Van-Phuc Hoang

***Abstract*— Main problems in FPGA-based ring oscillator (RO) PUFs are that the RO frequencies are highly sensitive to operating conditions and other types of global variations. In addition, the RO frequencies are highly correlated by local variations. Therefore, in practice, conventional RO-PUF application schemes using Hamming distance normally require complex identification (ID) extraction algorithms and/or a large number of ROs to ensure a high level of uniqueness and reliability of the extracted IDs. In this work, we proposed a novel scheme of ID extraction based on Euclidean distances. Our proposed scheme stably and reliably generates the ID using a non-selective small number of ROs. Specifically, the generated IDs are mostly non-sensitive to global variables and operating conditions such as ambient temperature. In oppose to Hamming-based extraction, the close-frequencies ROs are normally removed to avoid flipping bits, our proposed scheme takes all those in to account and simplifies the extraction process. Experiments on our available hardware have shown a very good level of reliability and uniqueness with ID collision rate is estimated less than 2×10^{-9}.**

***Index Terms*— PUF; Ring oscillator; FPGA; chip authentication; Euclidean metric; hardware security.**

I. Introduction

PHYSICALLY Unclonable Functions (PUFs) nowadays are one of the reliable techniques to extract the unique circuit identification (ID) used for device authentication, as well as instance-specific keys for popular cryptography applications. From a technology perspective, Field-Programmable Gate Arrays (FPGAs) recently is gaining popularity and along with ASIC become a mainstream integrated platform for many applications [1]. Indeed, state-of-the-art FPGA is proven to be powerful enough and are applied for a wide range of applications [3], from commercial electronics to enterprise telecommunication equipment and data center level. Compared to ASIC, developing using FPGA is not only cost-effective but is a great time-to-market solution, especially with the rapid changes in technology nowadays [4]. The extension in FPGA applications essentially comes with the demand for enhancing device security, where PUFs could offer a strong quantity for deploying security techniques at the physical level. However, there is a limited number of FPGA-based PUF, though ASIC-based PUFs are extensively and well studied and commercially applied. That limitation might be due to the stringent FPGA design flow, especially in terms of logic optimization and narrow primitive selection while the PUF in the general case is not a purely digital logic circuit[1].

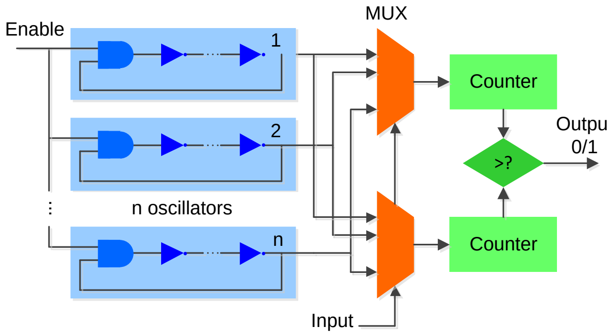


Fig. 1 Ring oscillator based PUF circuit.

In this work, we focus on FPGA-based PUF, and particularly on Ring Oscillator PUF (RO-PUF). RO-PUF is the least-technology independent PUFs since the RO evaluation circuit can read the frequency without altering the character of the ROs. Thus, RO-PUF is well-suited for FPGA though there are still special implementation techniques required.

The conventional FPGA-based RO-PUF design was proposed by Suh *et al.* in 2007 [6] (Fig. 1) which belongs to the weak PUF category, where PUF schemes are limited to a small number of challenge-response pairs. By using a pair of multiplexers with the control bits as the PUF challenges, the output frequencies f_1–f_n are selected by pairs f_i and $f_j (i \neq j)$. The respond value [8] is determined as

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

due to the difference between rings in a single die and between the same ring in different dies caused by intrinsic process variations, and different operating conditions. The signed function style of this method causes loss the information and requires a large number of ROs to extract reliable and unique

Manuscript received December xx, 2020; revised …; accepted … This research is funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.02-2020.14. *(Corresponding author: Quang-Kien Trinh.)*

Van-Toan Tran and Quang-Kien Trinh are with the Faculty of Radio-Electronic Engineering, Le Quy Don Technical University, Hanoi, Vietnam (e-mail: toantv@lqdtu.edu.vn, kien.trinh@lqdtu.edu.vn).

Van-Phuc Hoang is with the Institute of System Integration, Le Quy Don Technical University, Hanoi, Vietnam (e-mail: phuchv@lqdtu.edu.vn).

This work was published in part at 2019 IEEE International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC).

[1] PUFs circuit layout strictly needs to be regular and symmetric while they normally do not follow the common digital logic rules and can be amended or trimmed during the logic optimization stage

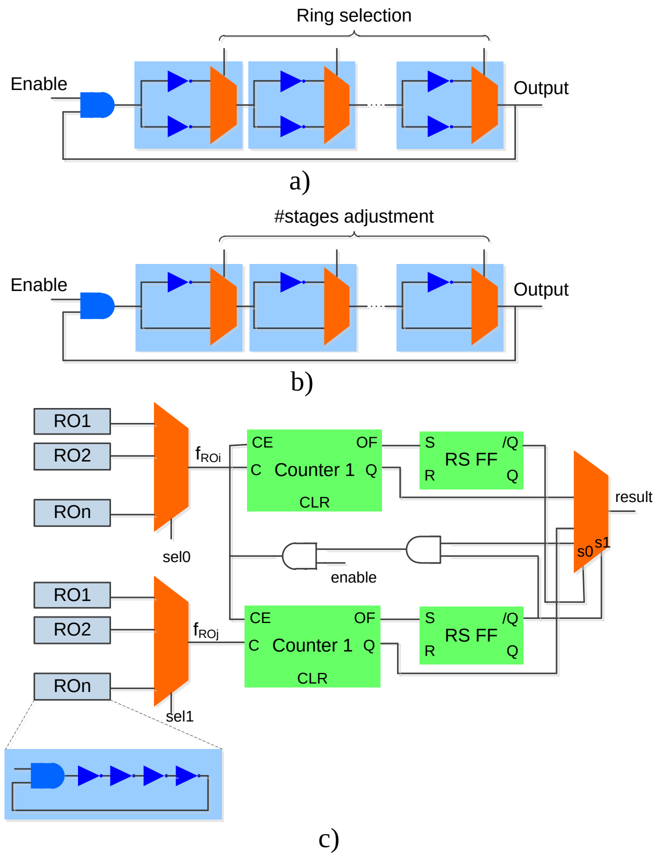


Fig. 2. Configurable RO and its modification.

chip identification. In addition, the fluctuation in absolute RO frequencies caused by operating conditions and other sources make this conventional scheme not practical. Many works have been done to improve conventional RO-PUF in two main directions. The first direction is to increase the flexibility in RO-PUF hardware configurations, so equivalent to retrieve more RO pairs, and the second, improve the data processing technique to enhance the efficiency of RO PUF data extraction.

Authors in [8] proposed configurable FPGA-based RO-PUFs that allow the inverters to be flexibly selected by a multiplexer (Fig. 2a). Accordingly, an RO with N stages of inverter could be configured to generates 2^N different frequencies. Gao *et al.* in [9] proposed a similar structure, where the number of stages inverters can be adjusted by several multiplexers as shown in Fig. 2b. Therefore, metastable outputs can be avoided. Authors in [10] could extract longer PUF output using less ROs by latching the counter value in Gray code of the slower RO (Fig. 2c) of each pair. The disadvantage of this method lies in the complexity of data processing in choosing the significant bit string locations. In general, these designs lead to high complexity in hardware layout caused by the integration of many multiplexers, thus maintaining the layout symmetry and regularity is especially challenging. Besides, the evaluation in those works follows the conventional way as described in [6].

There are also many prior works focusing on methods to improve the data processing efficiency. In the pairwise comparison method (Fig. 1), n ROs can generate $n/2$ bits [6]. The neighbor chain approach [11] which can form $n-1$ bits have the only advantage in simplicity but do not fully exploit the information from the set of n random frequencies. To leverage the upper bound of the number of generated bits, Yin *et al.* in [12] grouped the ROs under given conditions, resulting in increasing the limit of bits generated from $O(n)$ to $O(nlog_2 n)$. The threshold R_{th} is set to guarantee the reliability so that the difference between frequencies in groups should not be smaller than R_{th}. In another approach, to reduce systematic variations and utilize the random process variations, Yin and Qu in [13] designed a variation distiller based on polynomial curves that fit the trend of the systematic variations. In [12], the authors use Kendall Syndrome Code to replace the Compact Syndrome Code 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 be excluded during the ID extraction. Also, the hardware implementation of this complex coding scheme can be costly.

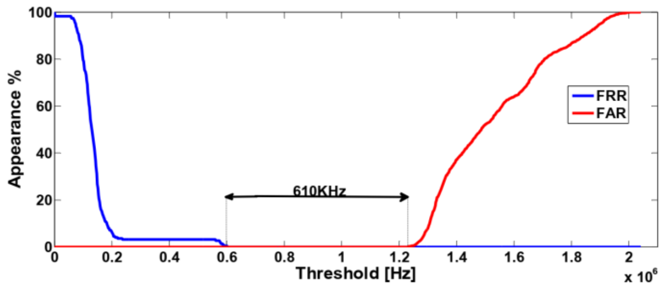


Fig. 3. FAR and FRR of the authentication process when increasing the resolution of the frequency difference measurement.

The works in [15], [17] based on the conventional scheme, proposed that the ID can be extracted by the frequency difference of each RO pair rather than just comparing their distances. This method theoretically could help to mitigate the impact of dynamic variations such as from the supply voltage and the temperature and the global process variations (i.e. die-to die process variations). In addition to this, the authors in [17] extract ID by the concatenation of differential RO frequencies and use the Manhattan distances of ID samples to evaluate the ID stability and uniqueness. Nonetheless, not only the target FPGA device is relatively outdated, the intra-ID[2] threshold has been empirically defined without considering temperature impacts in experimental.

In this paper, we proposed an approach to quantify intra- and inter- PUF distance based on the Euclidean metric and statistically define intra-ID threshold based on the worst-case deviation considering not only the RO location, device but also the temperature. By extensive experiment on both old (Spartan 3E) and new (Spartan 6) FPGA devices, we show this proposed approach fully detach the local mismatches from global variations, and eventually produces a relatively robust device ID.

[2] If the distance between two ID less than the intra-ID threshold then two ID is consider extracted from the same physical device and vice versa.

The remainder of the paper is organized as follows. In Section II, we first discuss some main features of a RO PUF by processing measurement data from the evaluation of a specific RO PUF circuit. In Section III, we point out the general expression of ID extracted from RO-PUF and the disadvantages of conventional ID extraction methods using binary Hamming distance. The proposed scheme of chip identification and authentication as well as relative discussions are presented in Section IV. Finally, Section V concludes the paper.

II. Main Features of FPGA-based RO PUFs

A. *Implementation of FPGA-Based RO PUFs*

To examine the main features of FPGA-based RO PUFs, we use the design based on the basic RO PUF circuit proposed by Suh *et al.* [6] with some modifications and targeted for Xilinx Spartan-6 and Spartan-3E series FPGA. The detailed functional schematic of the design is shown in Fig. 4 while the physical layout is shown in Fig. 5. The delay element (inverter) of the RO occupies one primitive LUT. To maintain an identical RO layout, the basic RO comprising of 2^N inverters and a NAND gate was manually routed before encapsulating as an FPGA hard macro. To ensure the symmetric layout, the RO macros are precisely placed so that the relative distances between ROs to the evaluation counter are mostly the same as presented in Fig. 5. Furthermore, we used only one counter, which evaluates the RO frequency sequentially, thereby reducing the resource usage and eliminate any possible bias caused by the counter. This theoretically may not be necessary for low-frequency ring oscillators because the difference in frequency is not dependent on the phase mismatches caused by the relative location from the counter to the ROs. 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. Specifically, we have implemented 32 ROs, each RO comprises of 16 inverter stages, evaluated by 255 samples. The samples acquired from four Spartan-6 and six Spartan-3E FPGA devices are transferred directly to the host computer for post-processing via a serial interface. With this design, we keep the ROs as simple as possible to maintain better regularity, symmetry, and compactness of the ROs, as opposed to ROs designs in [6], [9], [11].

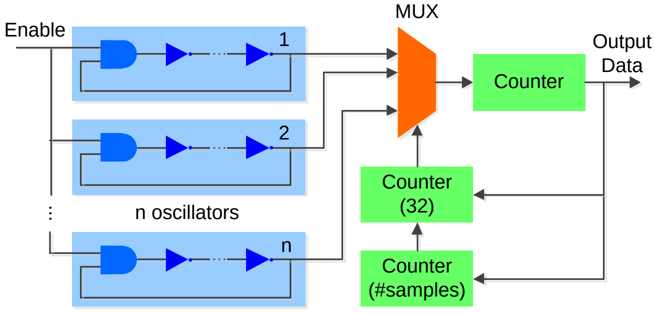


Fig. 4. Functional schematic of the proposed RO PUF circuit.

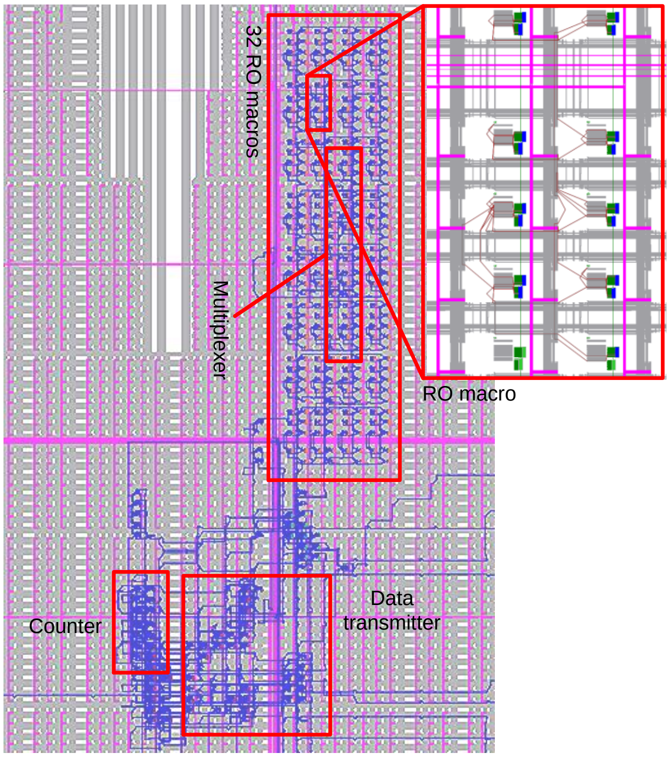


Fig. 5. RO-PUF Physical layout on Spartan-6 FPGA.

The major quality factor of the RO frequency is *reliability*, intra-die, and inter-die *uniqueness.* To quantify these performances, we used metrics based on Euclidean distance estimation.

B. *Frequency Error Caused By Measurement Windows Misalignment*

RO frequencies are derived by multiplying counter values in a time interval ΔT_{mea} by a factor k_{mea} to determine the number of clocks in one second:

$$f_{i.mea} = n_{cycle} \times k_{mea} = n_{cycle} \times \frac{1}{\Delta T_{mea}} \qquad (2)$$

As has been shown in Fig. 6, the error occurred when two oscillators have the same counter value but different by practical frequencies caused by the interval ΔT.
ΔT may have a uniform distribution in the range of 0 to T_i, with T_i is the respected period, so the maximum measured frequency error is:

$$\Delta f_{i.mea.max} = \frac{n_{cycle}+1}{\Delta T_{mea}} - \frac{n_{cycle}}{\Delta T_{mea}} = \frac{1}{\Delta T_{mea}} \qquad (3)$$
$$= k_{mea}$$

Assume that the frequency error $\Delta f_{i.mea}$ has the uniform distribution in the range of 0 to $\Delta f_{i.mea.max}$. From [2] we can evaluate the standard deviation of $\Delta f_{i.mea}$ as follows:

$$\sigma_{\Delta f_{i.mea}} = \sqrt{\frac{(\Delta f_{i.mea.max})^2}{12}} = \frac{k_{mea}}{4\sqrt{3}} \qquad (4)$$

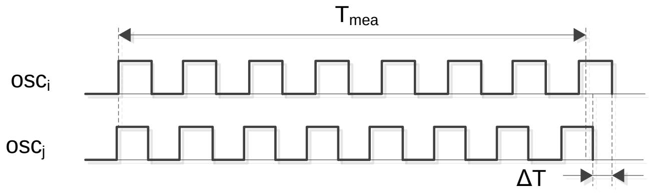


Fig. 6. The conceptual timing diagram of counter activity.

In our design, we choose $\Delta T_{mea} = 20\,ms$ and $k_{mea} = 50$, so we may evaluate $\sigma_{\Delta f_{i.mea}}$ as:

$$\sigma_{\Delta f_{i.mea}} = \frac{k_{mea}}{4\sqrt{3}} \approx 7.2\ Hz$$

For the proposed ID extraction scheme (Section IV) with the counter value proportional to differential frequencies, the standard deviation of $\delta_i = f_i - f_{i+1}$ is $\sqrt{2}\sigma_{\Delta f_{i.mea}}$. Because the Euclidean inter- and intra- distance proportional to $\sqrt{n-1}(\delta_i - \delta_j)$, so

$$\sigma_{\Delta d_{inter}} = \sigma_{\Delta d_{intra}} = \sqrt{n-1}.\sqrt{2}.\frac{\sqrt{2}\sigma_{\Delta f_{i.mea}}}{2^{k_{norm}}\sqrt{n-1}} \qquad (5)$$
$$= \frac{\sigma_{\Delta f_{i.mea}}}{2^{k_{norm}-1}}$$

approximates 6.86×10^{-6} with $k_{norm} = 21$ (Spartan-6 devices) and 1.37×10^{-5} with $k_{norm} = 20$ (Spartan-3E devices). Compared to standard deviations of intra-distances, this error may be safely ignored.

C. Statistic Model of RO Frequencies

The significant problem in using RO-PUFs for identification and authentication is that their frequencies are highly sensitive to ambient temperature and supply voltage fluctuation [6]. This leads to unstable RO-PUF responses and they should not be used directly. The total delay in an RO can be modeled as

$$f_{RO} = f_{nominal} + \Delta f_{proc,local} + \Delta f_{proc,global} + \Delta f_{OP} \qquad (6)$$

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 conditions. The remaining components in (6) 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.

D. Impact of Temporal Fluctuation

The frequency value was repeatedly measured multiple times for 4 ICs, on each of them perform measurements of 32 ROs, abbreviated as 4×32 ROs (6×32 ROs for Spartan-3E FPGAs) under a fixed operating condition (25ºC, 1.0 V voltage core). The frequencies of a particular RO varies due to the stochastic fluctuation during the operation in temperature and the supply voltage. For a single RO, this fluctuation corresponds to the Δf_{OP} variation under a fixed nominal operating condition. This impact is quantified by the *reliability factor* (of RO frequencies) which is defined as $(1 - \sigma/\mu)$ (in percentage), in which μ is the mean value of sample frequencies and σ is the standard deviation of the frequency distribution.

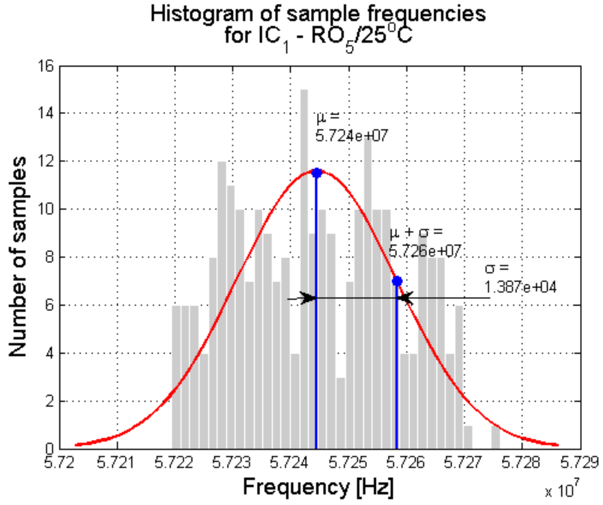


Fig. 7. Histogram of frequency samples of RO5/IC1 (Spartan-6 FPGA) retrieved from 256 repetitive measurements.

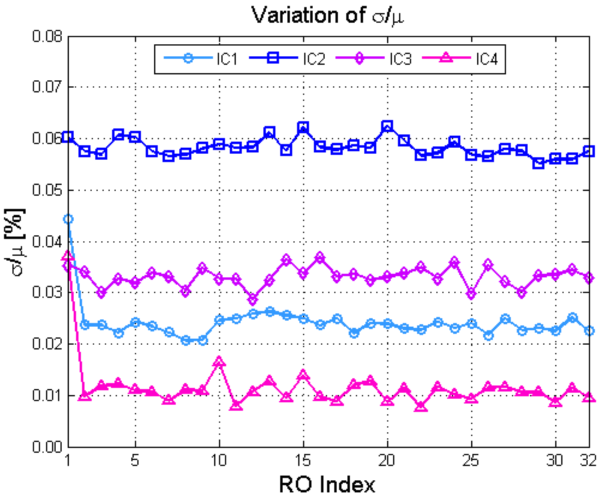


Fig. 8. σ/μ ratios of 32 ROs of 4 ICs estimated from 255 samples with the ambient temperature of 25ºC (Spartan-6 FPGA).

Fig. 7 shows a histogram from 256 repetitive measurements for RO5 in IC1. The mean frequency is 57.24 MHz and the standard deviation is 13.87 kHz, correspondingly the temporal (σ/μ) is just ~0.024% (the expected is less than 1% according to [5]). The measured temporal (σ/μ) of 4×32 ROs are presented in Fig. 8. From the estimation, the σ/μ ratios of ROs have the minimum value of 0.0077% (RO22/IC4) and the max value of 0.0624% (RO20/IC2), corresponding to the reliability of 99.99% and 99.94%, respectively. These results indicate that the temporal fluctuation has little impact on the measured RO frequencies and can be ignored.

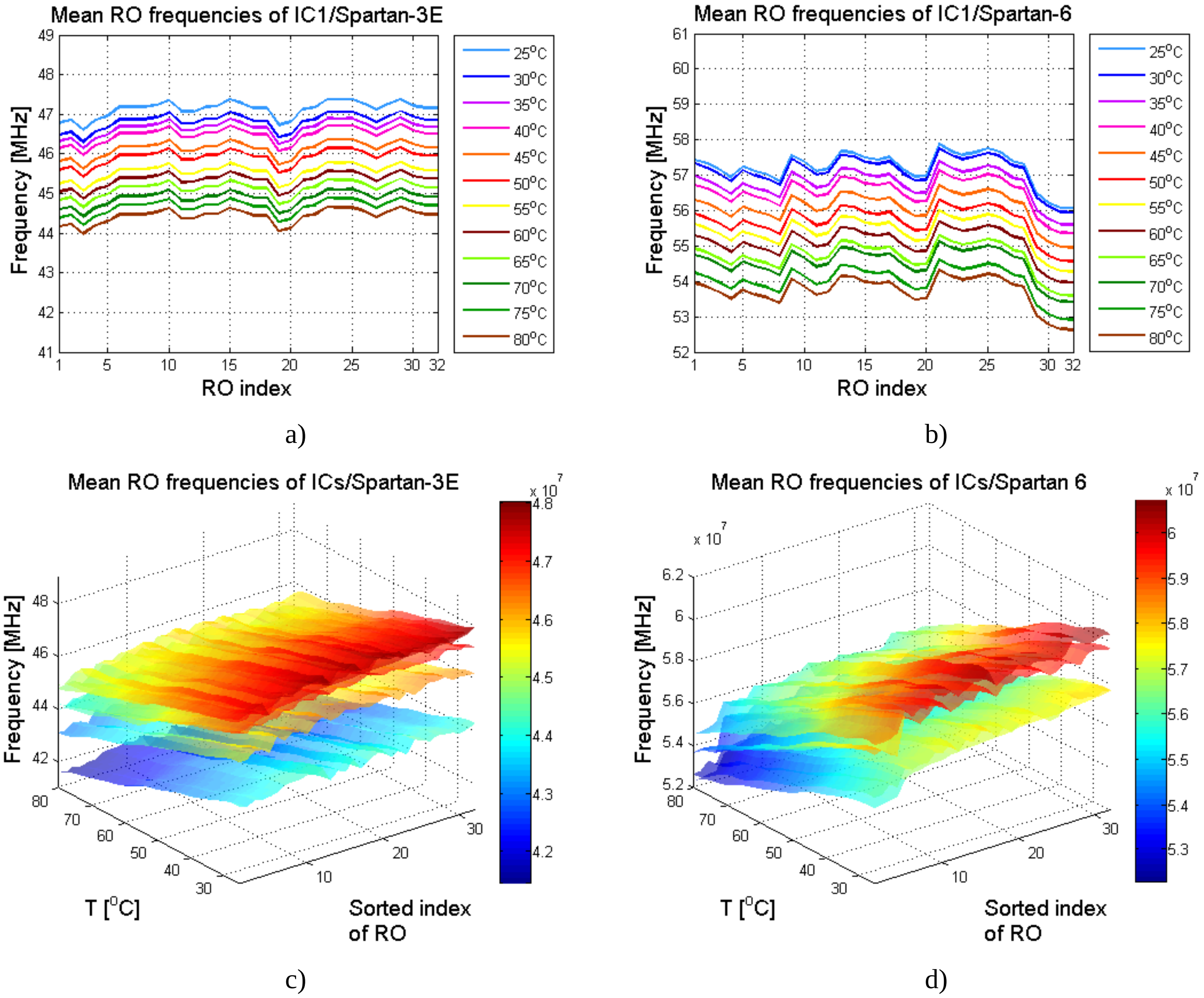
E. *Impacts of Temperature*

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–80ºC, steps by 5ºC). The measurements have been repeated 256 times for each of 4×32 rings to calculate their mean frequencies. The major results are presented in Fig. 9(a)–(b), and are consolidated in 9(c)–(d) by 3D surfaces. The RO indices are intentionally sorted by the increment of mean frequencies of IC3 to keep the 3D surface smooth and to express clearly changing the pattern. This shifting of frequencies essentially reflects the mean value of Δf_{OP} due to the operating condition in (6).

From the figure, the dependence of RO frequencies on temperature is quite strong and follows a predicted pattern. Indeed, the increasing temperature would lead to reducing in the RO frequencies (as the switching rate of the transistor getting slower). It can be observed that increasing temperature from 25ºC to 80ºC results in equally shifting the mean frequencies of ROs by 3.32-4.58 MHz (Spartan-6) and 2.29-2.95 MHz (Spartan-3E).

F. *Impacts of 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 (6). For the global variation, we could observe from Fig. 9(c)-(d) 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. 9(c)-(d) are all shifted up or down from IC to IC, and this phenomenon is valid even under different temperatures. 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 characterizing the physical



a)

b)

c)

d)

Fig. 9. Variation of mean ROs frequencies changes for temperature (at 25ºC, 30ºC,…, 80ºC), measured for one FPGA devices of Spartan-3E (a) and Spartan-6 (b) families, and 3D-illustration of the ROs frequencies for multiple FPGA devices of Spartan-3E (c) and Spartan-6 (d) families.

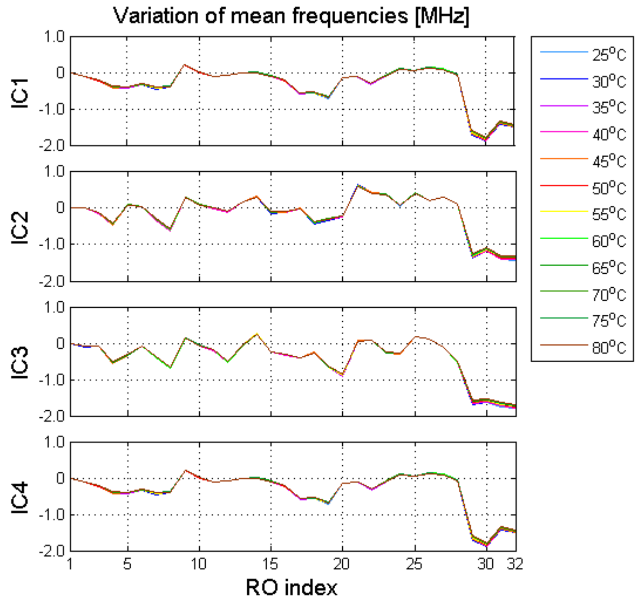


Fig. 10. Zero-centered frequency plots of the local variations for 4 ICs (Spartan-6 FPGA) under different temperatures.

devices.

Furthermore, we examine the local variation impacts, i.e., the difference in RO frequency across ROs in a single device. From the measurement, the mean values of the frequencies of 32 rings are shown in Fig. 9(a)–(b). The ripples of the surfaces in Fig. 9(c)–(d) caused by dissimilarity of ordered RO sets would represent the impacts of $\Delta f_{proc,local}$ in (6). It has been reported in many prior works that within a large number of ROs, the cases of two or more RO frequencies being closed to each other are quite common. In such a case, the pairwise method could easily result in an ambiguous response bit. So 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 [8], [12] 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 (8.05 kHz to 123.35 kHz for Spartan-6 and 1.07 kHz to 161.17 kHz for Spartan-3E). However, it is interesting that the pattern of local variation is very stable regarding the changes in the temperature. Indeed, from Figs. 9(a)–(b) that the zigzags for a single FPGA are mostly the same across temperatures. To achieve a better quantitative analysis, we remove the bias frequency caused by the temperature by subtracting the RO frequencies from the first RO frequency. Hence, all frequencies are shifted to the zero-centered range as plotted in Fig. 10. 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 123.35 kHz, which is in the same order as the temporal fluctuation. Similar results were recorded for Spartan-3E FPGAs. 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 Sections.

III. 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 conditions and, 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 can distinctively characterize the devices.

As the first step, to obtain only data on the local variation, all frequency biases due to global variations, which include global process variation, voltage, and temperature dependence, need to be excluded. From Figs. 9(c)–(d), it is predicted that we could remove the impact of global process variation and/or voltage and temperature-dependent components by taking not the actual frequencies but the differences among them. The latter represents 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

$$ID = F(\{\Delta f_{ij}\}) \qquad (7),$$

where $\Delta f_{ij} = f_i - f_j$ represents the local variations, the number of pairs (i, j) depends on the particular scheme. In the conventional ID extraction scheme using neighbor pairwise [15], F is simply the sign function.

Fig. 11 shows the frequencies difference, taken from the two consecutive frequencies $(i) - th$ and $(i + 1) - th$ plot of all ROs at 25ºC. 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 RO-20 (RO-28) tends to be the fastest (slowest) among all rings across ICs. This phenomenon has been pointed out in [6]. If we again apply the neighbor pairwise method as in [15] but taking only one bit: 1 (0) if $i - th$ RO is faster (slower) than $(i + 1) - th$

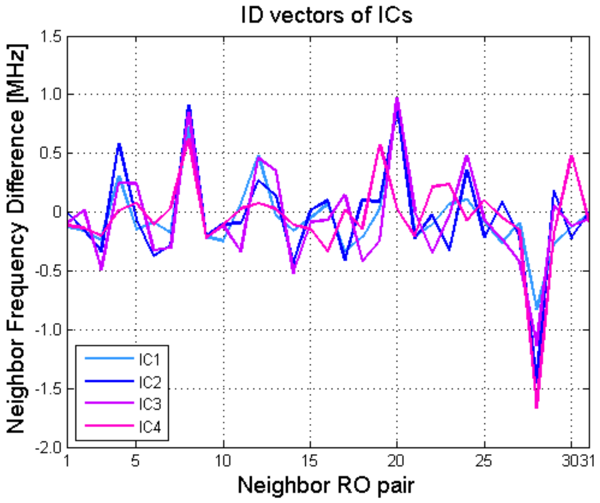
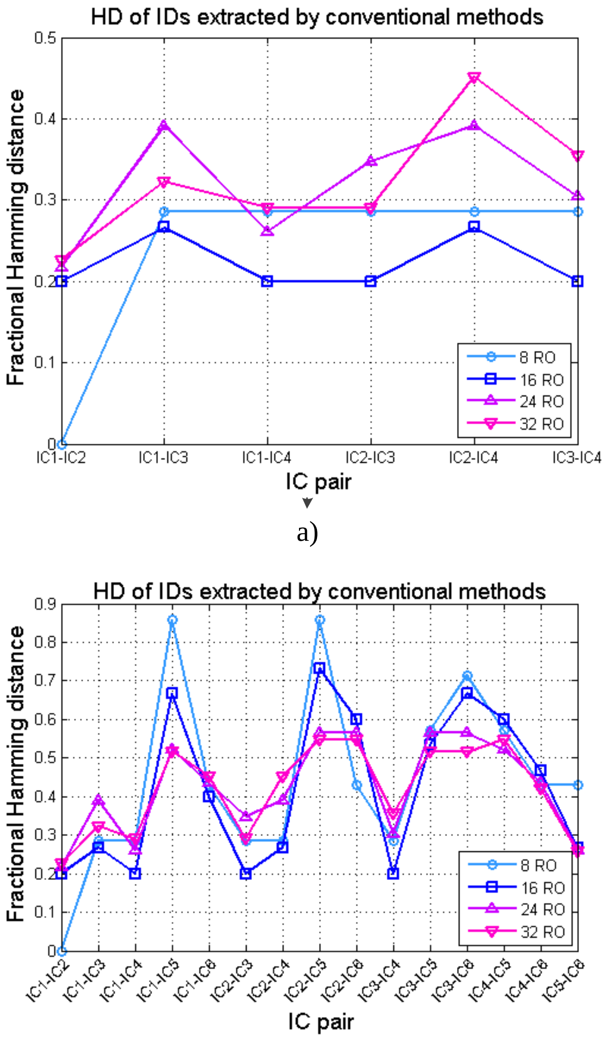


Fig. 11. Zero-centered frequencies plot of local variation for 4 ICs (Spartan-6 FPGA) at 25ºC.



a)

b)

Fig. 12. Fractional Hamming distances of ID extracted by the conventional neighbor-pairing method: (a) Spartan-6 FPGA; (b): Spartan-3E FPGA.

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} as in Fig. 12.

As can be seen with a large number of rings, for Spartan-6, when n_{RO} = 32 (24), the minimum Hamming distance between IDs are 7-bit, 23% (5-bit, 22%). However, when n_{RO} = 16 the IC pairs IC1-IC2, IC1-IC4, IC2-IC3, and IC3-IC4 are different by just 2 bits (12.5%). For n_{RO} = 8 IC1 and IC2 are even not distinguishable. The correlation phenomenon is more explicit for the case of a larger number of physical devices. 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.

IV. Proposed ID Extraction Scheme

A. Determination of Euclidean Distance

Results from the last section 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. 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 a sense, we do not need to exclude similar ROs, as their level of similarity can be treated as one of the unique features. A similar approach has been proposed in [17] although the root cause of the ID instability was not systematically studied and experimentally proven.

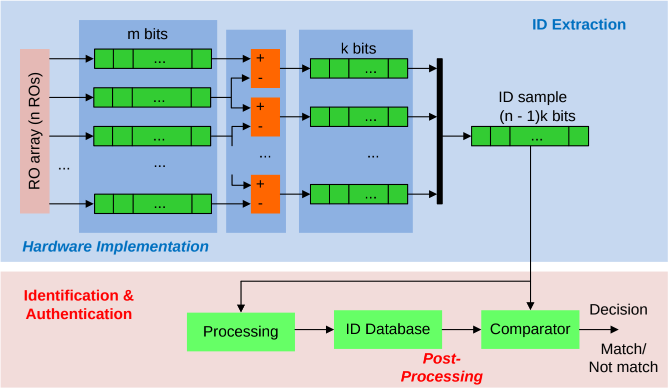


Fig. 13. Proposed ID extraction and authentication scheme.

The proposed ID extraction and authentication scheme is shown in Fig. 13 that could enhance ID extraction by fully quantifying the characteristics of the local variation. This would help to exploit 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 (Fig. 4), each consecutive neighbor frequency pair produces a $k - bit$ response by a comparator. The value of k can be much smaller than m because it represents only the magnitude local difference between frequencies (in this particular design $n = 32, m = 24,\ k = 24$). 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 of just one counter and one comparator for the whole process and the circuit is very compact. At this phase, our scheme is very similar to the proposed method in [17]. The major difference is in the evaluation and authentication phase and the way we process the ID.

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

$$\delta_i = f_i - f_{i+1} \tag{8}$$

is the magnitude of the *i-th* neighbor frequency difference.

The vector $\boldsymbol{R}$ for each IC essentially characterizes the unique zigzag pattern in Fig. 11, 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 $\boldsymbol{R_i}$ and $\boldsymbol{R_j}$ 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[3]

$$d_{intra} = \frac{d(\boldsymbol{R_l},\boldsymbol{R})}{2^k\sqrt{n-1})} \tag{9}$$

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

$$d_{inter} = 1 - \sum_{i,j}\frac{2d(\boldsymbol{R_i},\boldsymbol{R_j})}{N(N-1)2^k\sqrt{n-1})} \tag{10}$$

For a good IDs set, the value of d_{inter} is close to 0.5 (50%), however, this essentially requires a significantly large number of IDs for evaluation.

The equations (9) and (10) are actually generalized of the proposed metric in [8], where the binary Hamming distance is replaced by the Euclidean distance, which would be more appropriate to quantify the magnitude of vector components.

B. *Evaluation of ID Stability*

Using the proposed scheme, we first evaluated the reliability of the design. Fig. 14 presents the standard deviations of differential frequencies, which are much smaller than standard deviations of absolute frequencies. So the reliability of differential frequencies is higher than in the case of absolute frequencies in Section II.D. The histogram of differential frequencies for a RO pair of a specific IC (ROp2/IC1) is presented in Fig. 15.

Next, we have calculated the IDs of IC1 for repetitive 256 measurements. The graphically illustrated IDs are represented in Fig. 16, and one of the distributions of the normalized intra-distance is plotted in Fig. 17. From these figures, it can be seen that the IDs of IC1 retain mostly the same from sample to sample. The distribution of the distance between the IDs with respect to the nominal ID in Fig. 17. Here the nominal ID is $\boldsymbol{R} = \{mean(\delta_i), i = \overline{1,n-1}\}$. The maximum normalized distance is 0.0143. The maximum standard deviation of the normalized intra-distance is just $\sigma_{d_{intra}} = 26 \times 10^{-4}$ at 25ºC and 29×10^{-4} for all temperature values. Correspondingly, the probability that one ID measurements located outside the hypersphere with center $\boldsymbol{R}$ and radius $6\sigma_{d_{intra}}$ is 2×10^{-9} (one per billion). These results are well in line with our analysis before in Section II.D that the impact of temporal fluctuations

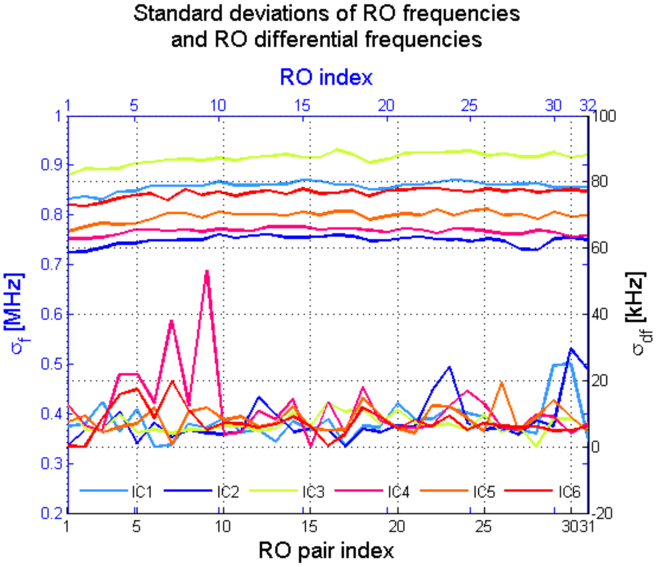


Fig. 14. Standard deviations of RO frequencies and differential RO frequencies for ambient temperature in the range of 25ºC to 80ºC.

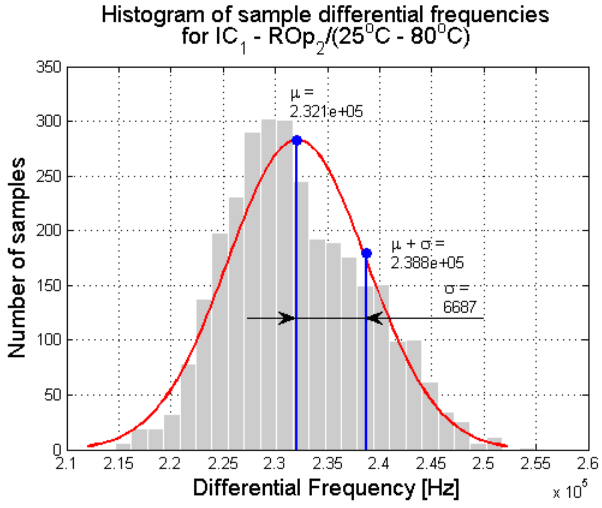


Fig. 15. Histogram of sample differential frequencies for a RO pair of an IC with respect to changing of ambient temperature.

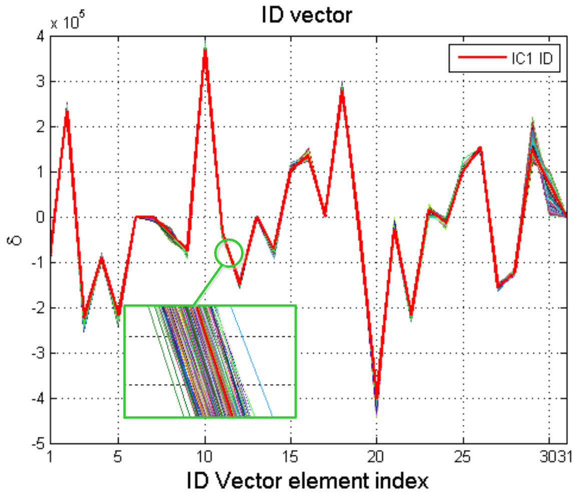


Fig. 16. Reliability of the Extracted ID (Spartan-3E FPGA) against temporal variation impacts.

[3] The maximum distance between two (n–1) dimensions vectors of k-bit value is $2^k\sqrt{n-1}$, hence the intra distance is normalized to the value of the range 0 to 1.

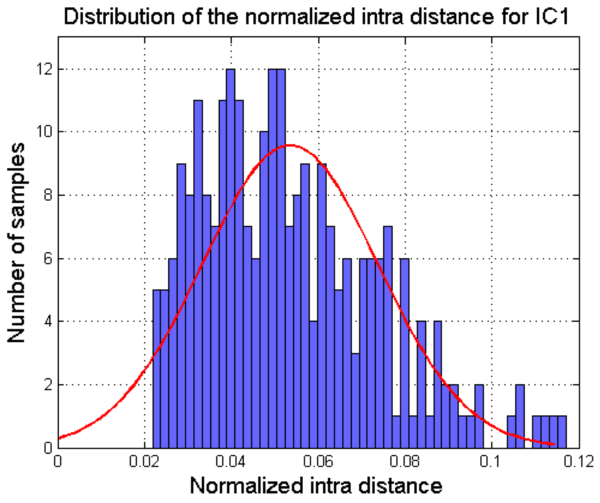


Fig. 17. Histogram of the normalized intra-distance for IC1 (Spartan-3E FPGA) for 255 measurements.

are insignificant and the measured IDs are relatively stable with respect to the temporal fluctuation.

Furthermore, the nominal ID vectors for all 6 ICs at different temperatures 25ºC to 80ºC with the step of 5ºC are shown in Fig. 18. Those IDs are visibly the same and the detailed analysis shows that the maximum normalized distance between the nominal IDs, measured for an IC across temperatures is 0.0192. 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 as 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, for example, with IC1 in 25ºC, $d_{threshold} = 0.0159$ being $\sigma_{d_{intra}} = 26 \times 10^{-4}$. This threshold distance would increase if sampling is conducted under different temperature conditions. In our particular experiment, the normalized threshold becomes $d_{threshold} = 0.0181$, being $\sigma_{d_{intra}} = 30 \times 10^{-4}$. For all samples of all the devices under different temperatures, the maximum standard deviation is $\sigma_{d_{intra}} = 36 \times 10^{-4}$, so the threshold may be chosen as $d_{threshold} = 0.0215$.

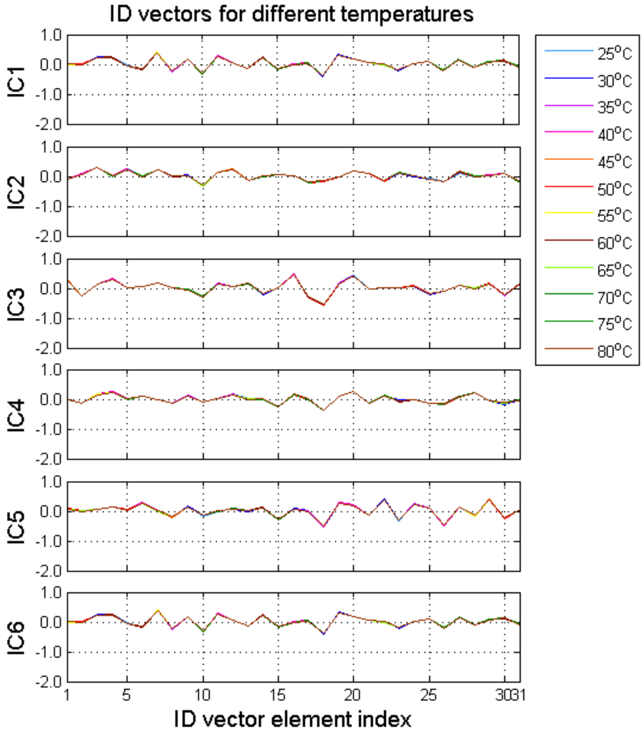


Fig. 18. Reliability of the extracted ID for 6 ICs (Spartan-3E FPGA) with respect to the change of ambient temperature.

At the authentication phase, if the intra-distance of two ID samples is greater than $d_{threshold}$, these ID samples are considered physically different. In contrast, the two ID samples are matched if they have the normalized intra-distance that does not exceed the value of $d_{threshold}$. Correspondingly, the main functionality of the authentication unit is to calculate the normalized distance to give the decision. This phase is typically done off-chip, e.g., by a computer.

C. *ID Uniqueness*

In these experiments, the number of physical devices is limited to 6 (for Spartan-3E), 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 for Spartan-3E FPGAs. From the table, it can be observed that the minimum distance between them is 0.1068 found between IC1 and IC2. This minimum distance is ~6.7 and ~5.9 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 (SPARTAN-3E).

IC2	IC3	IC4	IC5	IC6	
0.1068	0.1877	0.1788	0.1911	0.1617	IC1
	0.1673	0.1706	0.1653	0.1628	IC2
		0.1957	0.2079	0.2166	IC3
			0.2442	0.2242	IC4
				0.1901	IC5

D. *ID Authentication Experiment*

The authentication test is conducted as below. The RO PUF design in Fig.13 is implemented in several FPGA devices. In the evaluation phase, normalized inter-distances between ID vectors are calculated as shown in Table I. The maximum standard deviations of ID samples equals 0.0036. The threshold is chosen by 0.0181, approximately 6 times smaller than the minimum normalized inter-distance in Table I. In the authentication phase, 255 ID samples are archived for each device and transmitted to the PC for the next processing. ID

TABLE II. EUCLIDEAN DISTANCES BETWEEN ID VECTORS OF TEST ICS AND RECOGNIZED ICS.

	IC1	IC2	IC3	IC4	IC5	IC6
b1	0.0119	0.1134	0.1931	0.1785	0.2012	0.1676
b2	0.1874	0.1687	0.1954	0.2135	0.2603	0.2293
b3	0.1949	0.1721	0.0079	0.1895	0.2145	0.2207
b4	0.1106	0.0082	0.1671	0.1699	0.1690	0.1680
b5	0.2000	0.1744	0.2175	0.2477	0.0095	0.1962
b6	0.1695	0.1728	0.2209	0.2329	0.1948	0.0102

samples of test ICs (b_1, b_2,…, b_6) (which include recognized ICs and unknown ICs, in this case, is b_2) are converted to digital frequencies and equalized to extract respected ID vectors. These vectors are combined with nominal ID vectors to form normalized Euclidean distances (Table II). These quantities are compared with the threshold to point out the relative devices. As shown in Table II, b_1, b_3, b_4, b_5, $b_6$were recognized as IC1, IC3, IC2, IC5, IC6, respectively, and b_2 was not recognized. This is because b_2 has never been registered and the ID database do not include it's nominal ID. The experiment results showed that these devices are authenticated correctly and with a high level of reliability.

V. CONCLUSIONS

In this work, we have systematically studied the impact of variations on RO-PUFs. From the experimental results, the pattern of the local process variations within a single die is observed to be very consistent and that can be used for the 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 available experimental results show a high 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] Weste, Neil HE, and David Harris. CMOS VLSI design: a circuits and systems perspective. Pearson Education India, 2015.

[2] Gubner, John A. Probability and random processes for electrical and computer engineers. Cambridge University Press, 2006., pp. 138–183.

[3] 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.

[4] Mencer, Oskar, et al. "The History, Status, and Future of FPGAs: Hitting a nerve with field-programmable gate arrays." Queue 18.3 (2020): 71-82.

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

[6] 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.

[7] 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.

[8] Maiti, Abhranil, and Patrick Schaumont. "Improved ring oscillator PUF: An FPGA-friendly secure primitive." Journal of cryptology24.2 (2011): 375-397.

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

[10] Kodýtek, Filip, Róbert Lórencz, and Jiří Buček. "Improved ring oscillator PUF on FPGA and its properties." Microprocessors and Microsystems 47 (2016): 55-63.

[11] 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.

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

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

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

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

[16] 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.

[17] 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.

[18] Garcia-Bosque, Miguel, et al. "Proposal and Analysis of a Novel Class of PUFs Based on Galois Ring Oscillators." IEEE Access 8 (2020): 157830-157839.

[19] Cui, Yijun, et al. "Programmable Ring Oscillator PUF based on Switch Matrix." 2020 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, 2020.

Van-Toan Tran received the bachelor's and master's degrees in cybernetics and automation engineering from Le Quy Don Technical University, Hanoi, Vietnam in 2004 and 2014, respectively. He is currently pursuing a Ph.D. degree in electronic engineering with Le Quy Don Technical University. His research interest includes integrated circuit design and hardware security.

Quang-Kien Trinh (Member, IEEE) received PhD degree in computer engineering from the National University of Singapore, Singapore in 2018. He is working as the Deputy Head of The Department of Microprocessor Engineering, Le Quy Don Technical University, Hanoi, Vietnam. His research interest includes low-power integrated circuit design, emerging memory technologies, and hardware security.

Van-Phuc Hoang (Member, IEEE) received PhD degree in Electronic Engineering from The University of Electro-Communications, Tokyo, Japan in 2012. He has worked as postdoc researcher, visiting scholar at The University of Electro-Communications, Tokyo, Japan, Telecom Paris, France and

University of Strathclyde, Glasgow, UK during the period of 2012-2018. He is working as an Associate Professor, Vice Director at Institute of System Integration, Le Quy Don Technical University, Hanoi, Vietnam. His research interests include digital circuits and systems, hardware security, embedded systems for Internet of Things, and VLSI architecture for digital signal processing.