Towards a robust and efficient EM based authentication of FPGA against counterfeiting and recycling

Mosabbah Mushir Ahmed, David Hely, Nicolas Barbot, Romain Siragusa, Etienne Perret, Maxime Bernier, Frédéric Garet

Towards a robust and efficient EM based authentication of FPGA against counterfeiting and recycling

Mosabbah Mushir Ahmed*, David Hely*, Nicolas Barbot*, Romain Siragusa*, Etienne Perret*§,
Maxime Bernier‡, Fredric Garet‡
*Univ. Grenoble Alpes, LCIS, Valence, France, §Institut Universitaire de France, Paris, France
‡University of Savoie Mont Blanc, IMEP-LAHC, Chambery, France
email: mushir-mosabbah.ahmed@lcis.grenoble-inp.fr

***Abstract*—Counterfeiting of integrated circuits (IC) has become a serious concern for semiconductor industry. It is necessary to find a robust solution which is both efficient and low cost in terms of implementation in order to detect and avoid the counterfeiting of ICs. Also, the solution must be resistant against aging and other reliability effects. In this paper we have proposed a scheme to utilize radiated Electromagnetic (EM) emission from the IC to create a fingerprint. Our proposed scheme exploits manufacturing based process variation (PV), which continues to dominate in the nanoscale technologies. We have deployed variability-aware circuit (VAC) design that generates radiated EM emission and performs realistic assessment of the PV effects. Generated EM response is treated to different encoding metrics to quantize it as a fingerprint for the IC. Latter part of the paper validates that the fingerprint is stable after the aging effects of IC. To validate our proposed scheme measurements are carried out over several FPGA boards.**

Keywords*—*authentication, aging, counterfeit, EM, FPGA, fingerprints, reliability

I. Introduction

The counterfeiting of ICs have become major concern in recent years, as it impacts the security and reliability of electronic systems especially for critical application like military, banking, health care etc [1][2]. From [1], a counterfeit electronic component can be defined as that which is not genuine, unauthorized or is an uncertified copy. They are produced by unauthorized contractors, are defective and do not conform to the specification, and hence categorized as old and recycled OCM product.

Field programmable gate array (FPGA) due to their re-programmability, flexibility, shorter time-to-market and other useful features, is an IC that has attracted a considerable interest in the semiconductor and electronics industry. With the increased use of FPGAs in critical systems, counterfeit FPGAs cause significant security as well as financial concerns for both the government and industry. Recent reports show that programmable logic is in the top 5 counterfeited electronic components with a percentage of 8.3% of reported counterfeit incidents [2]. Consequently it has become imperative to find a traceable solution which is cost-effective, easy to implement and efficient in authenticating FPGAs throughout its lifetime.

The classical techniques that involve physical and electrical inspection can be very time consuming, highly invasive and also involves the risk of damaging the IC or components under test, permanently or temporarily [3]. Second method is based on traceability approach to find fingerprint for authentication by using PV. As discussed in [3], using PV approach, physical unclonable function (PUF) is dominantly used. It exploits the inherent variability of an IC, caused due to manufacturing variations of IC itself. Each PUF contains a pair of challenge and response (c-r). For each challenge (c) sent to an IC there is a unique response(r) to that challenge [4] [5]. Apart from the IC authentication, PUFs are also used for the purpose of secret key generation for cryptographic applications. Bottleneck of the PUF approach is that it requires dedicated on-chip circuitry which may be complex to process and implement.

In this paper we propose an alternate methodology which exploits the manufacturing induced PV by utilizing the radiated EM emission from IC. With the PV from an IC, each IC has a characteristic EM signature which can be used as its fingerprint for the authentication. Using this methodology we currently target to authenticate FPGAs. In comparison to the existing methods (electrical and physical) our method requires less time, is non-intrusive and there is no risk of damaging the IC. In comparison to PUF approach, our methodology uses very less silicon area. The main point is that for PUF, the processing is done on-chip (inside the IC) whereas in this methodology it is done outside the IC. This is an advantage in terms of design cost. But the limitation of our proposed methodology is that the IC cannot use the authentication information and also requires external measurement equipments.

The objective of this paper is to use radiated EM emission from FPGA to create a fingerprint that can be used for its authentication throughout its lifetime i.e, the fingerprint should be robust and stable w.r.t aging and should be the same for both the fresh and the old (aged) FPGA. To create fingerprints, a VAC has been deployed in FPGAs and the radiated EM emission from each FPGA is measured. The purpose of implementing a VAC is to get a prudent determination of different aspects of PV as well create a radiated EM emission from FPGA. The EM response from each FPGA is treated with post-processing techniques (encoding metrics) to quantify the EM emission into a fingerprint of each FPGA. Further, the stability of the fingerprints against aging effects has been evaluated.

This paper is organized in the following way: In Section II, different types of PV, their causes and effects is briefly discussed. Section III elaborates the detail about methodology, measurements steps and initial results for EM based authentication. In Section IV, we have evaluated the effects and

challenges on the EM response due to effects of aging on FPGA. Section V discusses about multiple RO approach and using post-processing metric (encoding metrics) that is robust against the aging effects. Section VI outlines a final conclusion from the paper and gives a brief detail about the future works.

II. Process Variation in ICs

PV is an inherent variability which comes during the manufacturing process of IC [6]. PV effects can be exploited to create a fingerprint for the IC, which could be used for the purpose of the authentication. Before going in details of how PV effects can be exploited for the use of FPGA authentication, a brief understanding of PV and its effects have been given here. The authors in [6] describes the variability in a CMOS process and have divided the variabilities into two major types.

A. Temporal variability

The temporal variability comes with usage of device over period of time ranging from a few nanoseconds to a few years depending on its source and applications. From [2][6] temporal variability arises due to run-time effects caused due to negative bias thermal instability (NBTI), hot carrier injection (HCI), electromigration and time dependent gate oxide breakdown (TDDB). NBTI and HCI are of greater interest in this paper as they effect the switching speed of transistors and consequently its performance. NBTI has the most effect on the transistor aging among all other phenomena. It greatly effects the PMOS transistors. NBTI is driven by negative bias voltage, which creates interface traps that leave some permanent defects in the interface region. NBTI increases the V_{th} of the transistor which lowers the speed. HCI is another aging mechanism that effects the speed and performance of the transistors. It is particularly caused by trap accumulation in the interface which causes increase in V_{th} resulting in lowering of speed.

B. Spatial variability

It is the type of variability that occurs in an IC during its manufacturing time (t = 0*s*). This type of variation can be subdivided into intra-die and inter-die variation. Parametric variations that come due to variation among different lots (L2L), dies (D2D) or wafers (W2W) are categorized into inter-die variations. Fluctuations in device length (L), oxide thickness (t_{ox}), width (W), flat band conduction etc. are the reasons for inter-die variations. Random variations like line edge roughness (LER), random dopant fluctuations (RDF) etc. gives rise to intra-die variations. Variations in L, W, t_{ox}, flat band conduction causes inter-die V_{th} variations. The variations in V_{th} results in variation in delay, switching and speed of the circuits [6].

In this paper, the effects of both temporal and spatial variability have been evaluated. The effects of spatial variability is exploited to create fingerprints of fresh FPGAs and the effect of temporal variability is studied during the phase when aging effects on the fingerprints are evaluated.

III. EM based authentication

A. Description and Evaluation Methodology

As discussed in Section I, in this paper an EM based method has been adopted to authenticate FPGA based on EM fingerprints. As also discussed in [7], considering the CMOS circuit, the most prominent reasons for EM emission is the switching of transistors. The sudden switching changes the current in the conductor and interconnects resulting in EM emission. To create an EM emission in a FPGA, a circuit (VAC) has been deployed, whose electrical functionality causes switching of transistors to create an EM emission. Due to the effects of PV, a VAC deployed in many FPGAs of same family produces a unique response for each FPGA. The response from each FPGA is treated to post-processing techniques which quantifies the response to create a fingerprint that can be stored in a database for future reference.

A graphical illustration of the proposed evaluation methodology to create EM based fingerprints is given in Fig. 1. The methodology is divided into the selection of the VAC and DUTs (FPGAs), performing measurement steps to capture the EM emission and applying the post-processing metrics (encoding metrics). Each steps of the evaluation methodology is described in the detail in below sections.

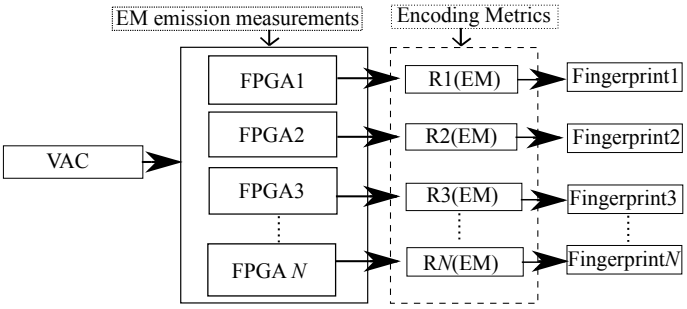

Fig. 1. Illustration of different stages to create fingerprint of FPGA.

B. EM based measurements

In the early stage, an initial measurement has been performed through which we are able to verify that each FPGA has a characteristic EM response. Below subsection determines a system overview which is used in the EM based measurement. Then the next section highlights the results from the initial measurements.

1) Variability aware circuit (VAC): Ring oscillator has been chosen as VAC circuit. Indeed RO circuit can be used as a VAC, as it is sensitive to the effect of PV. It is also a viable choice to create EM emission which is function of PV. The inter-die spatial variability as discussed in Section II, affects the V_{th} of the RO circuits, which in turn cause variations in transistor switching speed, delay etc. between two FPGAs even if they are of same family and manufacturer. The authors in [8] have used RO based EM emission technique to analyze localized EM attack on RO PUF. In this work, we extend this technique to exploit the EM emission from FPGA using RO circuits to create fingerprints for FPGAs for the purpose of authentication. In this work FPGAs have been programed with a three inverter stage RO with an AND gate and an EN (enable) pin as shown in the Fig. 2.

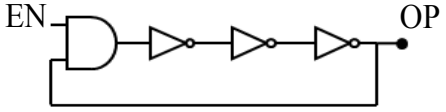

Fig. 2. Ring oscillator circuit implemented.

2) Device under test: In this work, we have selected fresh and new FPGAs as DUT. For our measurement we have used four ARTIX-7 (28nm) from Xilinx on Nexys 4 board. All the FPGAs are programmed with same RO circuits.

3) Measurement Setup and steps: For capturing the EM emission when RO is programmed in the FPGA, an EM near field (magnetic-field) probe from Langer EMV is used. Fieldfox spectrum analyzer is used for the acquisition of the EM response. The near field probe is placed horizontally and moves in the X and Y directions to capture the maximum SNR from the RO circuit. In order to get a good signal strength the probe is placed as close as possible to the FPGA. The measurement setup showing the placement and movement of probe over the FPGA, approximate spot of ROs in FPGA etc. is shown in Fig. 3.

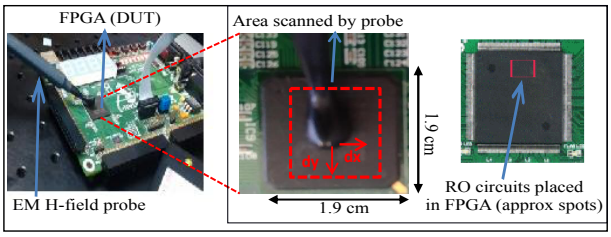

Fig. 3. (*left*) H-field probe placed horizontally over DUT. (*center*) Probe is moved horizontally over FPGA in dx=dy=1mm . (*right*) Approximate location of RO inside FPGA.

C. Measurement Results

In the initial measurement to capture EM emission from FPGAs, only one RO circuit is programmed in all the FPGAs. The RO circuit in all the FPGAs are of same configuration, number of delay elements and interconnect length. The response from a single RO on four FPGAs are depicted in Fig. 4. The spectrum analyzer is configured with the resolution bandwidth of 20 kHz and 1001 sample points.

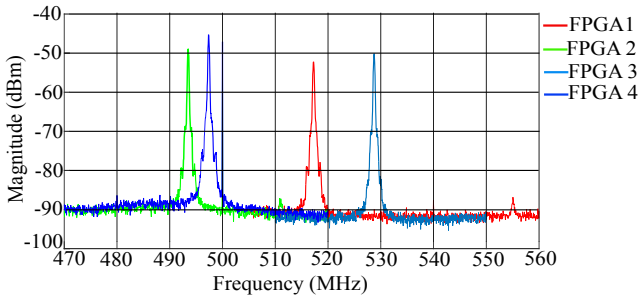

Fig. 4. EM emission from one RO circuit from four DUTs.

The spectrum of RO frequency for the four FPGAs is shown in Fig. 4. The results from Fig. 4 verifies that, even if the FPGAs are of same family and configured with the same RO circuit, but due to the effects of PV, the EM response (characterized here by RO frequencies) of each FPGA is different. This determines that by utilizing the effects of PV on FPGA, all the FPGAs have characteristic and different fingerprint which can be applied for the purpose of authentication. Hence a single RO can be utilized to exploit the PV effects on FPGA and create fingerprints that can be used of the authentication purpose.

Similar measurements have also been done over several FPGAs on different family (SPARTAN 3 (90nm) from Xilinx on Nexys 2 board). The results obtained in this case are also identical as we have explained for the ARTIX-7 case.

D. Challenges due to temporal variability

The challenge here is, will the RO frequency (subsequently fingerprints of FPGAs) of the four FPGAs remain constant, after the FPGAs have been aged or been in the field where they are subjected to thermal or supply voltage stress. The temporal variability effects like NBTI, HCI etc determines the challenges posed on FPGAs fingerprints over the time. To understand the effects on fingerprints when FPGA is in stress conditions, we have performed an analysis in the next section.

IV. Effect of Aging on Fingerprints

In this section we analyze the effects of aging or thermal stress on the fingerprints. As also discussed in Section II-A, thermal stress is a part of temporal variability and results in accelerated aging of the device. Thermal stress causes ramifications such as NBTI and HCI that significantly affect the performance of CMOS transistors. To observe the effects of stress on FPGA and subsequently on the fingerprints, we have performed thermal stress on one FPGA (FPGA3 - FPGA under stress). The next subsection describes the measurement steps and the results performed for the accelerated aging of FPGA.

A. Measurements steps and results

The measurement setup to perform accelerated aging by thermal stressing of the FPGA is shown in Fig. 5. The FPGA under stress is subjected to high temperature of 85°C in a hot plate and covered with a lid to have a constant temperature stress over the board. Total duration of the aging measurement is of two weeks.

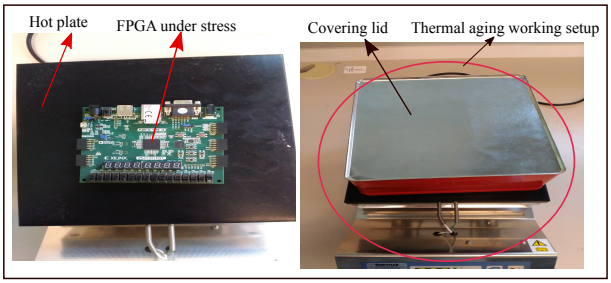

Fig. 5. Experimental setup for accelerated aging and measurement

The following points elaborates the steps implemented to do the accelerated aging of FPGA using thermal stress :

- FPGA to be stressed (aged) is selected.
- Before the aging process starts, FPGA RO frequency is measured under normal temperature.
- Put FPGA under the stress condition with the RO powered ON and running.
- Keep FPGA under the stress condition for 48 hours continuously.
- Measure the frequency of the RO; before measurement the FPGA is taken out of stress condition and is allowed to cool down to room temperature.

- Keep the FPGA back in stress condition.
- The same procedure is repeated for two week of time which is approx to 4 years aging of FPGA [10].

Applying the above steps to age/stress the FPGA, a graph showing degradation rate of frequency versus time of aging has been plotted as shown in Fig. 6. Authors in [2] have also discussed that the degradation rate of newer and fresh FPGA is more than that of old and used FPGA. From Fig. 6 and applying the aging measurement steps, a shift in the frequency of one RO when aged for two weeks is shown in Fig. 7. From Fig. 7, we can determine that the RO frequency for fresh FPGA is distinct and as the FPGA ages, the RO frequency degrades at higher rate first and then it saturates afterwards.

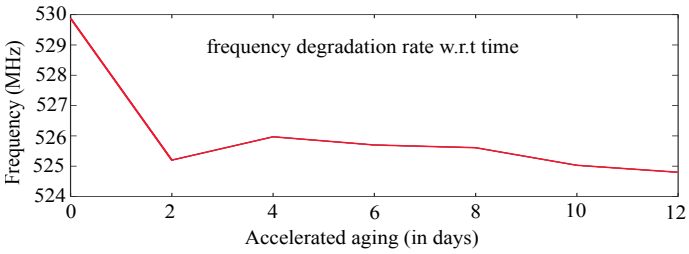

Fig. 6. Degradation curve of frequency with time.

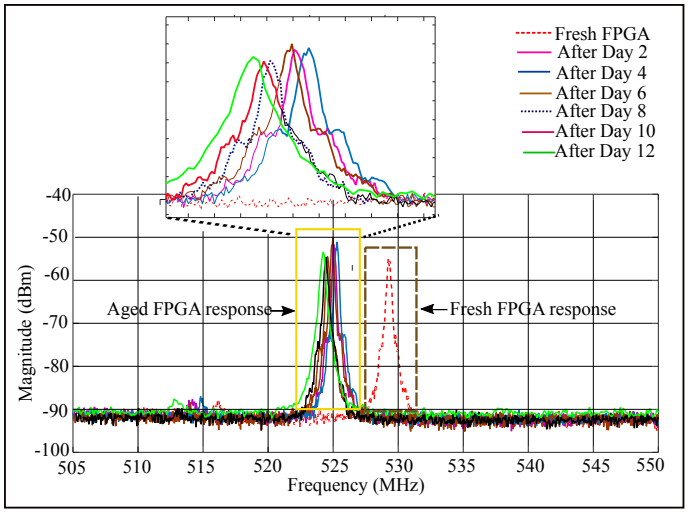

Fig. 7. Shift in RO frequency with aging. The insert zoom shows a zoom on the RO frequency after accelerated aging

From Fig. 7, we see that the RO frequency shifts with the aging of the FPGA. Due to the change in the absolute magnitude of the RO frequency with respect to time (aging), absolute magnitude of RO frequency cannot considered as a reliable metric for the purpose of authentication of the FPGA. To overcome this, we propose to use relative methods based on digital metrics which are quantifiable and do not change with time. To realize the relative method based metrics, we have extended the initial measurement of Section III. Multiple ROs are then stressed/aged by following the same measurement procedures as described in the Section IV. The obtained results from the multiple RO approach are then treated with the relative method based encoding schemes which produces a quantifiable data from the EM response from the four FPGAs.

V. Multiple RO measurements and encoding techniques

A. Multiple RO measurements

Using intra-die variations in FPGA, which leads to different characteristic frequencies on the same FPGA for different ROs, 16 ROs are employed in the same FPGA similar to as described in the initial measurement setup. Each RO is of identical length, vertically placed across the FPGA as shown in Fig. 8. Due to the intra-die variability in the FPGA, no two identical ROs in the same FPGA will give exactly the same frequency.

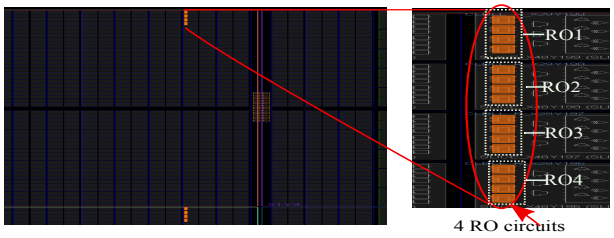

Fig. 8. ROs vertically placed in FPGA.

Similar measurement setup is used for the measurements of 16 ROs as is done in the initial measurements. To capture the EM response, at a time only one RO is enabled keeping all other ROs in OFF state. To understand the procedure of enabling one RO at a time, we can refer to Fig. 8. Suppose RO1 is enabled, then until all the measurement steps are done and results captured in spectrum analyzer for RO1, the other ROs are not enabled. This is done in order to avoid any interference or coupling effects which may arise when multiple ROs are enabled at the same time. The process is then repeated for the subsequent ROs.

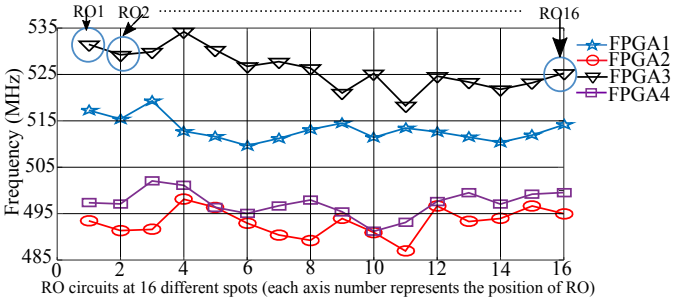

Fig. 9. Pattern of 16 RO frequencies for four FPGAs.

Measurement results of 16 ROs frequencies from four FPGAs is depicted Fig. 9. From Fig. 9 we can clearly see that with each FPGA, due to intra-die variations, there is a pattern associated with it. Each pattern associated with a FPGA can be attained and quantified into creation of a fingerprint of each FPGA. The next step is to exploit information from the obtained pattern of Fig. 9 to create fingerprint for each FPGA using relative based methods. In the succeeding discussion we have elaborated the implementation of proposed metrics.

B. Post-processing techniques (Encoding)

The notion here is to propose post-processing or encoding techniques that is utilized in quantifying EM response from different ROs into a dataset (fingerprints). The encoding methods used in this paper takes into account the relative values of

the ROs frequencies. The measurement results from previous section and subsection have shown that due to the PV effects, each FPGA of the same family have a unique EM response when programmed with same RO circuits. The two encoding techniques proposed and used in this paper quantifies the EM responses into a binary vector. The purpose of quantification is to create a dataset to apply mathematical operations and store conveniently in a database for future uses. The other important aspect for an encoding technique is that, it should be reliable and robust. In this subsection we have first introduced the idea of two post-processing techniques we have used and then apply it on the EM response from multiple RO measurement result.

a) Mean based encoding: The first proposed encoding scheme is based on finding the mean value of all the implemented ROs frequencies and calculate the deviation of each RO frequency from that mean value. Algorithm 1, represents a pseudo-code for the mean value based encoding scheme. The employed algorithm details a finite sequence of discrete steps. Each step is an operation or instruction that can be performed by the DUT expected to carry out the procedure. Thus, the algorithm represents a set of steps for performing mean based encoding. It presents a sufficient precision and detail in an appropriate logical form, which is completely and unambiguously interpretable and executable by the particular DUT intended to perform the procedure.

Algorithm 1 mean based encoding vector

procedure BINARYVALUEUSINGMEAN(BV)
  $P_{m,i} = P_{m,i}\{R_1, R_2...R_i\}$
  $P_{m,i}$ is the *m*th FPGA and with *i* no. of ROs under test
  $R \subset \mathbb{R}$ frequency in MHz of *i* number of ROs
  compute $E(P_{m,i})$
  $E(P_{m,i})$ is the mean value of RO frequencies in *mth* FPGA
  for j=1 to i **do**
    if $P_{m,i}(R_j) > E(P_m)$ **then**
      assign $B_{mj} = 1$, where $B = \{0,1\}^n$
      else $B_{mj} = 0$
    end if
  end for
  Return B_m
end procedure

Algorithm 1 is illustrated here with an example. Consider one FPGA P_1, with i number of ROs, consider i = 16 to represent 16 ROs for the FPGA. For 16 ROs the frequency $R = \{R_1, R_2...R_{16}\}$ is calculated. Subsequently, the mean (E) value of the 16 ROs, itR_1 to R_{16} frequencies is computed for FPGA P_1. Afterwards, each single frequency $R_1, R_2...R_{16}$ is compared with the value of E, and R which are greater than that of E is assigned a binary code B as 1 and values of R less than E are assigned as binary code B of 0. Suppose that E is 100 MHz. The value say R_2 is 102 MHz, it is assigned as 1 and say R_8 is 97 MHz then it is assigned as 0. Hence, using this shift from the mean, we create a 16-bit vector, B, which is identified as a fingerprint for that FPGA.

Using our proposed encoding methodology described in Algorithm 1, the binary vector generated for the four FPGAs (DUTs) is shown in Table I.

From Table I, we can observe that for each FPGA, a binary vector has been created. The binary vectors are discriminated

TABLE I. BINARY VECTOR FOR EACH FPGA USING MEAN DEVIATION METHODOLOGY

DUT	Binary Vector
FPGA1	1 1 1 0 0 0 0 1 1 0 1 0 0 0 0 1
FPGA2	1 0 0 1 1 0 0 0 1 0 0 1 1 1 1 1
FPGA3	1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0
FPGA4	1 0 1 1 0 0 0 1 0 0 0 1 1 0 1 1

between two FPGAs using Hamming Distance (HD), which eventually computes the bitwise XOR between two binary vectors [9]. In this paper, we have computed the percentage HD, that gives by how much in percent the bits differ in two binary patterns. This metric is computed over multiple measurements on the same FPGA taking into account the repeatability errors in the measurements setup. Despite the measurement errors, percentage HD between the different measurements on same FPGA remains same ($\approx 0\%$). On the other hand, when the percentage HD is computed between the four FPGAs, the best case obtained is $\approx 62\%$ and worst case is $\approx 32\%$.

b) Frequency pair encoding: The second encoding scheme that we have used in this work is based on exploiting the frequency pair difference. In this scheme, frequencies of two adjacent ROs is compared and if the succeeding RO has higher frequency than the preceding one then a value of 1 is assigned else 0 is assigned. Similar to the previous encoding scheme, to give a logical and unambiguous understanding of this encoding scheme an algorithm, Algorithm 2, has been implemented.

Algorithm 2 frequency pair difference

procedure PAIRWISECOMPARISION(PC)
  $P_{m,i} = P_{m,i}\{R_1, R_2...R_i\}$
  $P_{m,i}$ is the *m*th FPGA and with *i* no. of oscillators under test
  $R \subset \mathbb{R}$ frequency in MHz of *i* number of ROs
  for j=1 to i **do**
    compute $[R_{j+1} - R_j]$
    if $R_{j+1} > R_j$ **then**
      assign $B_{mj} = 1$, where $B = \{0,1\}^{n-1}$
      else $B_{mj} = 0$
    end if
  end for
  Return B_m
end procedure

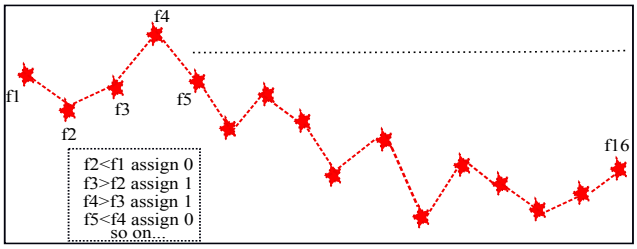

Fig. 10. A graphical illustration of frequency pair comparison metric.

A simple illustration of Algorithm 2 can be seen in Fig. 10. Using the procedure from Algorithm 2 and illustration shown

in Fig. 10, it is clear that for n number of ROs used in the FPGA, we get n-1 number of bits. For the four FPGAs used as DUT in this work, the binary vector obtained using frequency pair encoding scheme is given in Table II.

TABLE II. BINARY VECTOR FOR EACH FPGA USING FREQUENCY PAIR DIFFERENCE

DUT	Binary Vector
FPGA1	0 1 0 0 0 1 1 1 0 1 0 0 0 1 1
FPGA2	0 1 1 0 0 0 0 1 0 0 1 0 1 1 0
FPGA3	0 1 1 0 0 1 0 0 1 0 1 0 0 1 1
FPGA4	0 1 0 0 0 1 1 0 0 1 1 1 0 1 1

To find the weight of difference in the binary vectors, we apply the same percentage HD as differentiator, as is done with the previous metric. For this metric, the best case percent HD obtained is $\approx 53\%$ and worst case is $\approx 20\%$. Using the above proposed metrics and applying percent HD as differentiator, we can clearly see that each FPGA has a unique signature associated with it. This unique fingerprint can be used for authenticating the FPGAs. The next step is to evaluate the proposed relative method based encoding schemes against aging effects. This is done in order to determine the robustness and stability of the metrics and thus the fingerprints against aging effects on FPGA. The next subsection describes in detail the results obtained on the multiple RO after accelerated aging.

C. Effects of aging on encoding metrics

In this subsection we evaluate the effects of aging on the proposed post-processing (encoding) metrics. Similar measurement steps as described in Section IV is used on 16 ROs in four FPGAs. The pattern of ROs frequencies after two weeks of accelerated aging (measurements taken every 48 hours) is shown in Fig. 11.

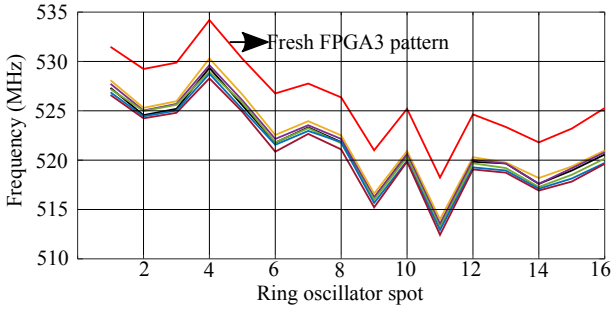

Fig. 11. Shift in the pattern of RO frequencies due aging effects.

From Fig. 11 it is clear that all the ROs, the frequencies shift in the same coherent order after thermal stress. Comparing the initial pattern of FPGA3 in Fig. 9 with Fig. 11, it is seen that the pattern has remained constant even after the degradation due to the thermal stress. Subsequently in order to find the effects of aging on the fingerprints, the metrics proposed in Section IV-B are applied. Applying both the proposed encoding metrics and their respective algorithms, the binary vectors for all the patterns obtained after the accelerated aging are computed. Table III, shows that even after two weeks of thermal stress, ($\approx$ 4 years old FPGA), the binary vectors have remained constant for both the metrics used. This is significant in realizing a stable and reliable fingerprint that remains constant with aging. Therefore, it can be concluded

TABLE III. BINARY VECTORS USING BOTH METRICS AFTER ACCELERATED AGING OF FPGA3

FPGA3	Binary Vector (Fresh FPGA)	Binary Vector (accelerated aged FPGA)
Mean Based Metric	111111111000000	111111111000000
Frequency Pair Comparision	011001001010011	011001001010011

that by using the two proposed metrics, constant, reliable and stable fingerprint for each FPGA can be achieved, which can be effectively applied for the purpose of authentication.

VI. CONCLUSION AND FUTURE WORK

In this case-study we have exploited PV to create EM based fingerprint for FPGAs. Aging analysis on FPGA have been performed to evaluate the stability and robustness of the fingerprints. Using the two proposed encoding metrics, our results show encoding metrics the results show that a stable and aging resistant fingerprint for FPGAs is obtained by using EM based measurement. In comparison to classic RO PUF, this method uses very less chip area as we did not require any on-chip post-processing technique, hence it is cost effective and easy to implement. This methodology can be extended to authenticate ASICs as part of future work.

REFERENCES

[1] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor and Y. Makris, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain," in *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1207-1228, Aug. 2014.

[2] H. Dogan, D. Forte and M. M. Tehranipoor, "Aging analysis for recycled FPGA detection," *2014 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, Amsterdam, 2014, pp. 171-176.

[3] Kai He, Xin Huang and Sheldon X.-D Tan,"EM Based on-Chip Aging Sensor for Detection and Prevention of Counterfeit and Recycled ICs" *015 IEEE/ACM Int. Conf. on Computer-Aided Design (ICCAD)*, Austin, TX, 2015, pp. 146-151.

[4] Charles Herder, Meng-Day (Mandel) Yu, Farinaz Koushanfar, and Srinivas Devadas, "Physical Unclonable Functions and Applications: A Tutorial" in *Proceedings of IEEE*, vol. 102, no. 8, pp. 1126-1141, Aug. 2014

[5] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," *2007 44th ACM/IEEE Design Automation Conference*, San Diego, CA, 2007, pp. 9-14.

[6] Swaroop Ghosh and Kaushik Roy, "Parameter Variation Tolerance and Error Resiliency: New Design Paradigm for the Nanoscale Era", *in Proceedings of the IEEE*, vol. 98, no. 10, pp. 1718-1751, Oct. 2010.

[7] E. de Mulder, S. B. Ors, B. Preneel and I. Verbauwhede, "Differential Electromagnetic Attack on an FPGA Implementation of Elliptic Curve Cryptosystems," *2006 World Automation Congress,* Budapest, 2006, pp. 1-6.

[8] D. Merli, J. Heyszl, B. Heinz, D. Schuster, F. Stumpf and G. Sigl, "Localized electromagnetic analysis of RO PUFs," *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST),* Austin, TX, 2013, pp. 19-24.

[9] A. Sadr and M. Zolfaghari-Nejad, "Weighted Hamming distance for PUF performance evaluation," in *Electronics Letters*, vol. 49, no. 22, pp. 1376-1378, Oct. 24 2013.

[10] S. y. Wang, B. Neubig, J. h. Wu, T. f. Ma, J. k. Du and J. Wang, "Extension of the frequency aging model of crystal resonators and oscillators by the Arrhenius factor," 2016 Symposium on Piezoelectricity, Acoustic Waves, and Device Applications (SPAWDA), Xi'an, 2016, pp. 269-272.