Effects of Aging and Compensation Mechanisms in Ordering Based RO-PUFs

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

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

***Abstract*—With the increasing need for highly secure systems, Physical Unclonable Functions (PUFs) have emerged within the last decade. Ordering based Ring Oscillator (RO) PUFs are one of the best performing structures with their robustness and suitability to FPGA implementations. Even though the performance of the ordering based RO-PUFs have been analyzed in detail, effects of aging have not been studied before. In this work, we present the results of an accelerated aging test applied to analyze the effects of aging on ROs. Then, the effects of aging on ordering based RO-PUFs are examined. Finally, a compensation method to protect the 100% robustness claim of the PUF structure is proposed and its influence on the circuit performance is presented.**

***Keywords*-PUF, Physical Unclonable Functions, Aging, Reliability, Robustness, Ring Oscillator, FPGA, Challenge-Response, CRP**

I. Introduction

With the increasing need for high security in many applications, Physical Unclonable Functions (PUFs) have become a widely accepted primitive in the last decade. Cryptographic key generation, IP protection, authentication, and ID generation are the main areas that PUFs provide economic and secure solutions [1]. In addition to these, PUFs eliminate the need for a non-volatile memory for ID and key storage purposes. Optical PUFs and Coating PUFs are the first two proposed PUF structures [2]–[4]. Due to impractical use and expensive equipment requirements of both structures, Silicon PUFs, such as Ring Oscillator (RO) PUFs, Arbiter PUFs, SRAM PUFs, Butterfly PUFs, and Glitch PUFs have drawn more attention with their low cost and ease of integration [5]–[10].

Imperfect manufacturing technology of integrated circuits leads to deviation of parameters such as threshold voltage, oxide thickness, and doping concentration from nominal values. These imperfections are the basis for the main PUF properties, which are uniqueness, robustness, unclonability, and unpredictability. Since the unique intrinsic physical properties of ICs are also present in FPGAs, some PUF structures, such as RO-PUFs, are convenient for FPGA implementations as well [11]. Based on the mentioned properties, PUF responses should differ from chip to chip randomly (inter-PUF variability), but should be stable during multiple read-outs from the same circuit (intra-PUF variability). In addition to these, the outputs should be unpredictable without using the PUF itself. Finally, manufacturing another circuit with the same PUF characteristic should be impossible.

Robustness is a measure of stable bits in a PUF circuit within different measurements. It is an important performance parameter for PUF structures [12]. Since PUF outputs are generated depending on small mismatches in the IC, any temporal variability present in the system may easily effect the output and result in generating unstable signatures. Almost all PUF structures mentioned above are vulnerable to internal and external effects and generate noisy outputs. Temporal variations that lead to unstable outputs can be classified as reversible and irreversible variations. The changes in the temperature and supply voltage are reversible variations and their effect disappears when the cause is removed. Decreasing the supply voltage is an example of reversible temporal variations. Even though lowering the supply voltage may change the state of output bits, the effect will be withdrawn immediately, when the voltage is returned to the normal level. However, irreversible changes are permanent and affect the circuit through the end of its lifetime [13].

Aging is the most important contributor of irreversible temporal variations and should be considered carefully in order to guarantee the required long-term robustness performance of the PUF circuit. Negative-bias temperature instability (NBTI), hot carrier injection (HCI), temperature-dependent dielectric breakdown (TDDB), positive-bias temperature instability (PBTI), electromigration, and soft errors can be considered as the main aging mechanisms that cause permanent changes in the electrical characteristics of the IC [14]–[16]. The impact of aging on the performance and reliability of ICs is also a function of the technology scaling. It is observed that the aging mechanisms mentioned above shorten the lifetime of the CMOS devices more and more with the shrinking of the device sizes [17].

Since the working principle of PUF circuits depends on small mismatches present in the IC, the effects of aging may change the behavior drastically and prevent the correct operation of the primitive. Especially for ICs designed for a long life span, the effects of aging should be investigated and countermeasures should be taken if necessary. In this work, we focus on the effects of aging on ordering-based RO-PUFs, depending on the results of the accelerated aging test (AAT) performed in FPGA environment and we present countermeasures to

maintain the reliability of the structures during the lifetime of the IC. The main advantage of the ordering-based RO-PUFs is their 100% robustness even under variable environmental conditions, which is very hard to achieve using other PUF types. This property eliminates the need of an error correction codes (ECC) block for applications that require 100% robust PUF outputs, significantly decreasing the cost of the system.

The rest of this paper is organized as follows. Aging mechanisms and previous works on PUF aging are presented in Section II. Then, properties of PUF circuits and the expected effects of aging on conventional RO-PUFs and ordering based RO-PUFs are discussed in Section III. AAT is applied on ROs and the analysis of the test results are presented in Section IV. Effects of aging on ordering based RO-PUFs and compensation methods are discussed in Section V. Finally, Section VI concludes the paper.

II. Aging mechanisms and PUFs

The electrical characteristics of ICs change gradually with continuous use. This may result in faulty behavior, causing reliability issues. The changes that appear due to aging are irreversible and affect the IC through the end of its lifetime. The downscaling of the physical dimensions of ICs with respectively high supply voltages makes circuits more prune to aging effects and reliability becomes a serious concern. NBTI, HCI, PBTI, TDDB, electromigration, and soft errors are the main mechanisms that lead to the aging phenomenon. Among these, NBTI and HCI are considered as the dominant ones [14].

Even though aging is an important concern for the reliability of all ICs, it becomes especially critical for PUF circuits. This is due to the fact that their working principle is based on small mismatches present in the manufacturing process. As a result of this, PUF behavior may change drastically due to small aging related drifts in the electrical characteristics of the circuit. Commonly, this change happens before the failure of other parts.

Limited amount of work is present on the aging of PUF circuits in the literature. Software based aging detection and Challenge-Response Pair (CRP) modification techniques are presented in [18]. Compared to this work, we do not propose CRP modification, but generating the CRPs according to the aging of the IC for a certain lifetime. Implementation results of the proposed protocol-level techniques are not presented in the mentioned work as well. In [5], an aging test of one month is applied to arbiter PUFs, but since the test is performed under normal operating conditions (NOC), significant changes in the behavior of the PUF circuit could not be detected. Compared to this work, we apply AAT to the IC to accelerate the aging process. Another aging test performed on SRAM PUFs under NOC is presented in [8]. In this work, it is stated that the change of initial values of SRAM cells remain under 4.5%. In [19], aging is used to develop a new kind of PUF structure, rather than detecting possible problems in previously presented PUF types. Six different PUF structures are analyzed with AAT in [20]. The results of the AAT applied to four memory based PUFs, one SRAM PUF, and one RO-PUF structure are presented. Analysis results indicate that aging decreases the robustness of PUF circuits significantly. A similar analysis of aging on RO-PUFs based on AAT is presented in [13], [21]. However, these works focus on conventional RO-PUF structures rather than ordering-based RO-PUFs and just analyze the frequency reduction of ROs. The last work we will mention here is [22], which focuses on designing an aging resistant conventional RO-PUF by changing the structure of ROs at transistor level. Reported results of the work seem successful in terms of decreasing the effects of aging. However, our work aims at removing the effects of aging completely.

Different from the works cited above, we mainly focus on the effects of aging on ordering-based RO-PUFs via real implementation results. We also propose mechanisms to compensate aging effects in ordering-based RO-PUFs. The cost of the compensation mechanism in terms of area efficiency is presented as well.

III. Ordering based RO-PUFs and Aging

A. PUF Quality Metrics

Uniqueness and robustness are the two main metrics for performance evaluation of PUF circuits. Uniqueness is also known as the inter-PUF variation and determines the unique signature generation capability of PUF structures placed on different dice. If the uniqueness of the structure is low, outputs may be similar to each other and become predictable, which is not acceptable. Uniqueness can be measured with three different metrics [12]. The most commonly used metric is the Hamming distance (HD) of outputs collected from different ICs, U_QM1, and can be defined as

$$U\_QM1 = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(R_i, R_j)}{n}, \qquad (1)$$

where, k is the total number of ICs, R_i is the response of ith circuit, HD is the Hamming distance function, and n is the total number of HD operations performed [23]. The ideal value of U_QM1 is *0.5*.

Robustness is also known as the intra-PUF variation and determines the noise level of the outputs generated by a circuit. If the consecutive outputs collected from a PUF circuit are noisy, robustness of the structure is low. Low robustness of PUF circuits increases the false-acceptance-rate and false-rejection-rate in authentication systems. If the PUF is used in cryptographic key generation that requires 100% robustness, overhead of the ECC will be higher. This is due to the fact that correcting more bits is only possible by using a higher complexity ECC block. Hamming distances of the outputs collected from the same IC, R_QM1, is the commonly used metric for robustness and can be defined as

$$R\_QM1 = \frac{1}{x} \sum_{y=1}^{x} \frac{HD(R_i, R'_{i,y})}{n}, \qquad (2)$$

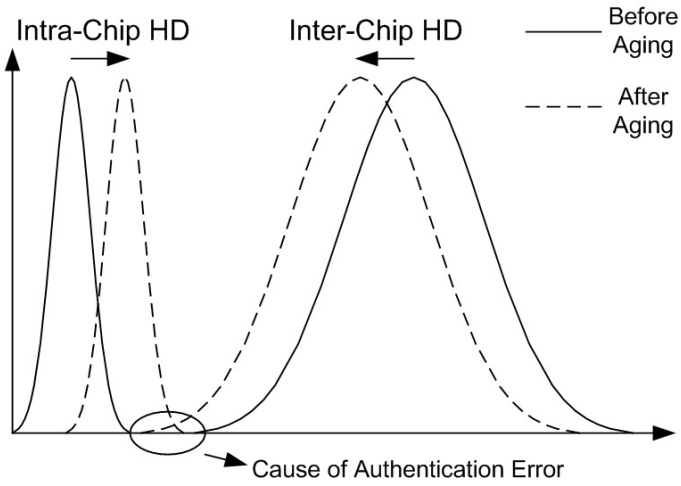

Fig. 1. Effect of Aging on Conventional PUFs

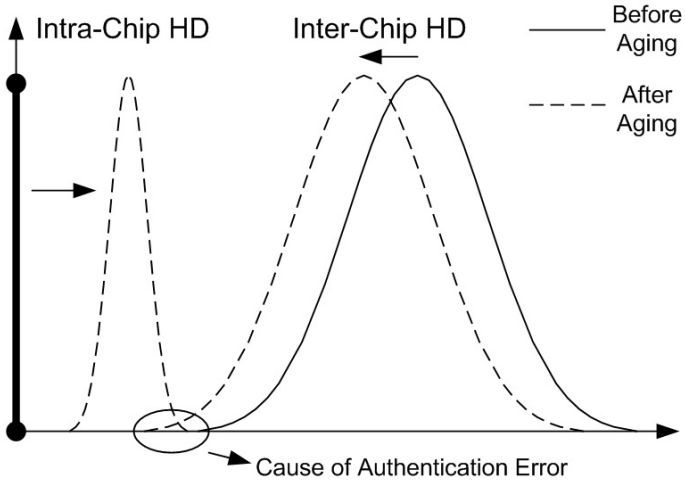

Fig. 2. Effect of Aging on Ordering Based RO-PUFs

where x is the total number of outputs collected, R_i is the first output, $R'_{i,y}$ is the yth output, and n is the total number of HD operations [23]. The ideal value of R_QM1 is *0*.

Since aging is a non-ideal process, it is expected that both uniqueness and robustness performances of the PUF structures get worse [13]. This is illustrated in Figure 1. As can be seen from the figure, intra-PUF HD distribution drifts away from *0* and inter-PUF HD uniqueness moves towards *0*. This behavior increases the authentication error probability, since the intersection of inter-PUF and intra-PUF HD distributions will get larger.

B. Ordering-Based RO-PUFs and Aging

100% robust PUF outputs were generated by adding ECC to the system [24] before the introduction of ordering based RO-PUFs in [25], [26]. Even though adding ECC is a reliable solution, it increases the area cost of the system drastically, since PUF circuits require a relatively small area. Ordering based RO-PUFs use the ordering of frequencies within a group of ROs, rather than comparing two ROs at a time as done in conventional RO-PUFs. With this method, more entropy is extracted from the system and higher area, power, and time efficiency are achieved. Ordering based RO-PUFs eliminate the need for ECC by introducing a parameter called the frequency threshold (f_{th}) [25] or the pre-determined frequency threshold (f_{thp}) [26]. The f_{thp} parameter defines the minimum frequency distance between ROs that are grouped together. It is the summation of noise in the system, $f_{th_{noise}}$, and environmental variations, $f_{th_{env}}$.

Dynamic programming (DP) is used to solve the grouping problem in ordering based RO-PUF systems with 100% reliability. With this algorithm, maximum entropy is extracted from the system by forming the largest possible RO groups with minimum computational complexity. RO frequencies measured under NOC and the f_{thp} parameter are the inputs to DP to form a list of ROs in each group. Then, the frequency ordering of ROs in these groups are used to generate the output bit stream.

As long as the noise in the system and environmental variations affect the RO frequency differences within a group by less than the f_{thp} value, reliable outputs are generated, which results in a R_QM1 of ideal value 0. Uniqeness of ordering based RO-PUFs are reported in [27]. According to these results, U_QM1 is calculated as 0.4972, which is very close to the ideal value of 0.5.

However, effects of aging on the system have not been analyzed before. Since aging is a non-ideal process, it is expected that its combination with the noise in the system and environmental variations, may cause the ordering in the groups of ROs to change erroneously and the PUF to start generating noisy outputs. For ordering based RO-PUFs, expected aging effects on intra-PUF HD and inter-PUF HD are illustrated in Figure 3. As can seen from the figure, intra-PUF HD is a Dirac delta function located at *0* before aging, exhibiting ideal PUF behavior. When the circuit is aged, changes in ordering within the groups will lead to noisy outputs and intra-PUF HD will move away from *0*. This may effect the uniqueness of the system as well.

IV. Accelerated Aging Test and Analysis of the Results

Integrated circuits are expected to have a long life span that can be measured in years for consumer electronics and decades for military applications. It is impossible to test an IC for years in order to analyze the effects of aging. Therefore, AAT is frequently employed to emulate the aging phenomenon. As explained in Section II, contributors of aging, such as NBTI and HCI, are more effective on the IC under high temperature and/or high supply voltage. Thus, it is possible to accelerate the aging process by increasing the temperature and/or supply voltage of the IC under test.

In order to analyze the effects of aging on ordering based RO-PUFs, we have utilized an unused Xilinx 3S500 45 nm FPGA board. Actually, using multiple FPGA boards will be

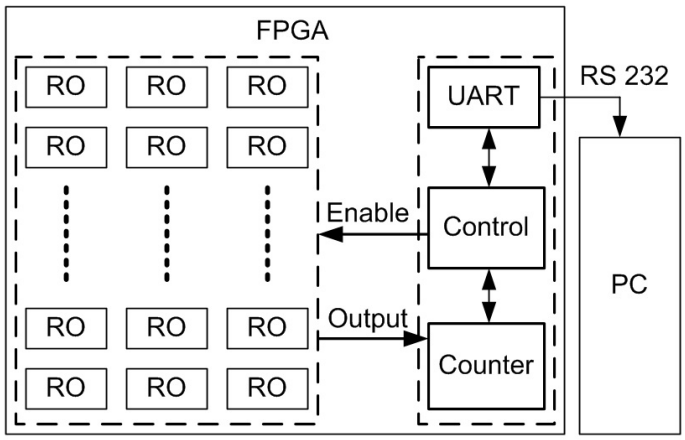

Fig. 3. Accelerated Aging Test Setup

a better practice. However, due to practical limitations in this research, we have utilized different sites on the FPGA, which will more or less simulate the different sites of the wafer. Results of this analysis is presented through the end of this section. Since it was not possible to change the operating voltage of the FPGA due to the voltage regulators present in the system, we have only used high temperature to accelerate the aging process. Acceleration factor of aging test under high temperature is called T_{factor} and can be calculated as

$$T_{factor} = e^{(E_a/k)\left(\frac{1}{T_{noc}} - \frac{1}{T_{aging}}\right)}, \quad (3)$$

where T_{noc} is the normal operating temperature of the circuit in Kelvin, T_{aging} is the temperature of the AAT in Kelvin, k is the Boltzman constant, and E_a = 0.5 eV is the activation energy [13]. In our case, the operating temperature is assumed as 25^oC and the test is applied at 100^oC to the development board, which has an industrial operation range of -40^oC to 100^oC. Under these circumstances, T_{factor} is calculated as 50.08. This means that one hour of AAT will correspond to 50.08 hours of operation under NOC for the IC.

As mentioned above, a Xilinx FPGA board is used for the AAT. For this purpose, 200 ROs composed of five inverting stages with enable inputs are implemented using the macro function. One counter is implemented to detect the number of oscillations within a certain amount of time. Universal asynchronous receiver/transmitter (UART) is used to transfer the data from the FPGA to the PC via RS-232 serial bus. In this system, the controller unit enables all ROs at the same time during the AAT phase and collects and sends the oscillation counts to the PC by enabling ROs one-by-one during the measurement phase. The AAT setup is illustrated in Figure 4. The duration of the AAT is set to 500 hours. This time is equivalent to approximately 3 years of operation under NOC. Equivalent IC working duration of the applied AAT for each 100 hours is given in Table I.

Oscillation counts of all implemented ROs are recorded before the test and after each 25 hours of AAT, one measurement at 25^oC and other at 100^oC. Each measurement is repeated

TABLE I
EQUIVALENT IC WORKING DURATION OF ACCELERATED AGING TEST

T_{Factor}	Test Duration (Hours)	Working Duration under NOC (Days)
50.08	100	208
50.08	200	417
50.08	300	626
50.08	400	834
50.08	500	1044

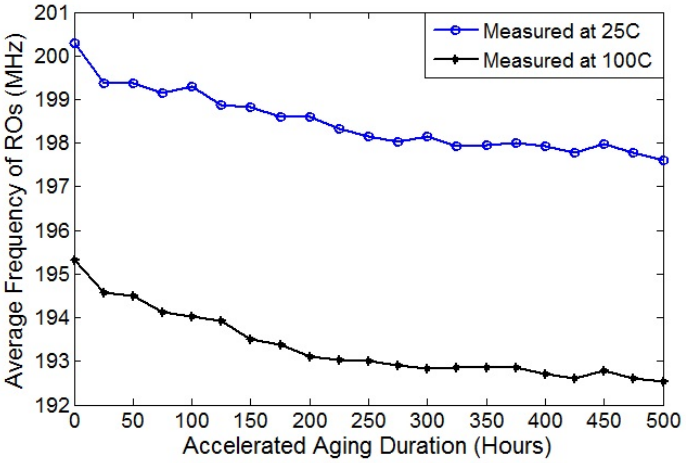

Fig. 4. Mean Frequency of ROs vs. Accelerated Aging Test Duration

50 times to determine the noise in the system and analyze the effects of aging on the noise. The average frequencies of ROs measured at 25^oC and 100^oC are presented in Figure 5. As can be seen from the figure, 500 hours of AAT decreases the average RO frequency by more than 1.3%. This result is also compatible with the results presented in [13]. In the cited work, AAT results in a frequency reduction of 9.4%. The reason behind the difference of frequency reduction is the difference of the duration and composition of the AATs, since our test is applied under high temperature for 500 hours, whereas the other test is applied under high temperature and high voltage for 1100 hours. According to our analysis results, frequency reduction rate of the ROs also decreases as the test duration increases. This is an expected behavior, since the effect of NBTI decreases due to the decreasing amount of threshold voltage shifts with aging as well.

The PUF output depends on the ordering of ROs within a group. Therefore, relative frequency reduction of independent ROs are critical, rather than the average frequency change. If all of the ROs within a group slow down at the same rate, ordering does not change and the robustness of the system is not affected. However, if the slowing rates of ROs in a group differ from each other and the frequency ordering changes, erroneous outputs are generated. In order to determine the relative frequency change of ROs, deceleration of individual ROs are calculated after each 100 hours of AAT with respect to the pre-aging frequency. The distribution of ROs depending on frequency reduction rate is presented in Figure 6. From the analysis, it is seen that different ROs slow down at different

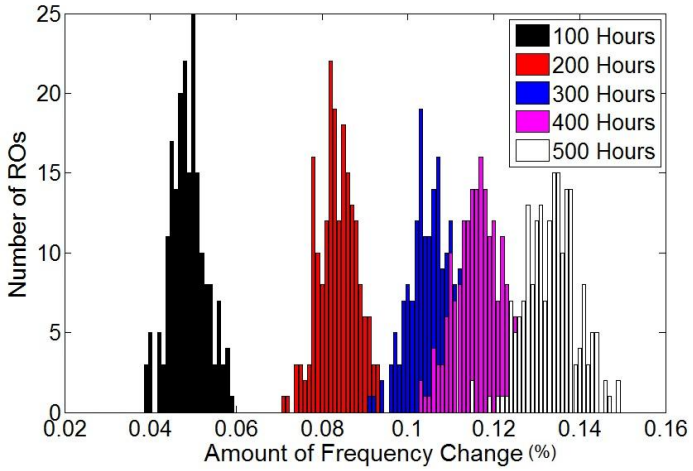

Fig. 5. Distribution of ROs depending on Frequency Reduction due to Aging

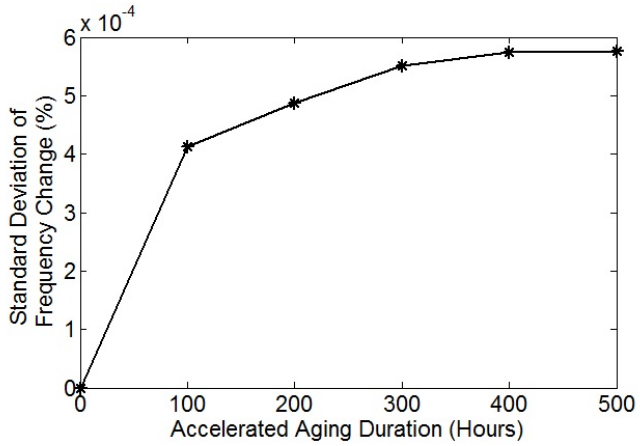

Fig. 6. Standard Deviation of Frequency Reduction due to Aging

rates. In addition to this, the distributions cover a wider range as the AAT progresses. For a more detailed analysis, the standard deviations of the distributions are calculated and presented in Figure 7. As can be seen from the figure, the increase in the standard deviations of the distributions slows down over time. This behavior indicates that the effects of aging on the relative RO frequency reduction diminishes after 300 hours of AAT and continuing the test after this point does not contribute much to the analysis. It can be concluded that, even though the measurements we have done correspond to 1044 days of aging, the robustness analysis applied based on this data will be valid for longer operation durations as well.

The noise in the environment is an important parameter for the robustness of PUF circuits and directly affects the determination of the f_{thp} parameter. Within the scope of this work, the effects of aging on the noise in the system is analyzed. For this purpose, each measurement collected from each RO is repeated 50 times and the standard deviation of these 50 measurements are calculated during different phases of the AAT at both 25^oC and 100^oC for each RO. Then, mean of the standard deviations of ROs is calculated during

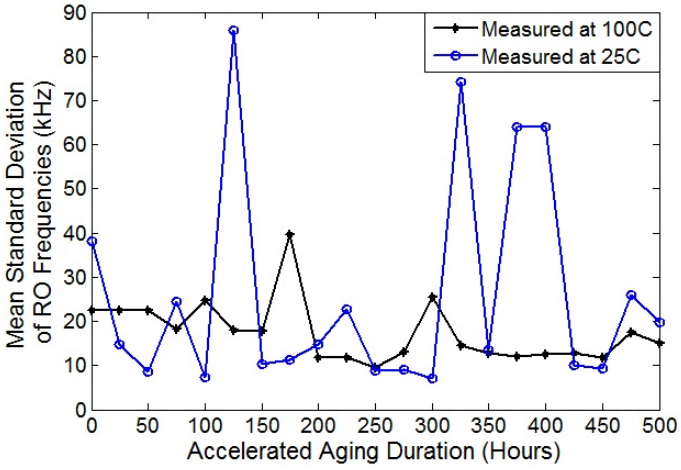

Fig. 7. Noise on RO Frequency Measurements vs. Aging

TABLE II
RO FREQUENCY REDUCTION DUE TO AGING VS. RO LOCATION

	Left	Middle	Right
Top	0.0134	0.0138	0.0125
Middle	0.0132	0.0140	0.0134
Bottom	0.0130	0.0134	0.0131

the AAT. Mean standard deviation of consecutively measured RO frequencies are presented in Figure 8. As can be seen from the figure, the noise level is not correlated with the duration of the AAT at neither 25^oC nor 100^oC and remains below 90 kHz at all times. As a result, the noise component in the f_{thp} parameter, $f_{th_{noise}}$, does not need to be updated due to aging in ordering based RO-PUF circuits.

The effect of RO locations on the aging process is also analyzed via calculating the frequency reduction rates of ROs that are located at 9 distinct sites on the FPGA from top-left to right bottom. As can be seen from Table II, a clear correlation between the frequency reduction vs. RO locations does not exist. It can be concluded that power distribution and heat dissipation of the FPGA seem balanced; hence, each site on the IC indicates a similar behavior in terms of aging. This situation, which can also be interpreted as using multiple FPGAs, is not severely critical for our research, since aging seems to be location independent on the wafer.

V. Effects of Aging on Ordering Based RO-PUFs and Compensation

According to the analysis presented based on the AAT applied, different ROs are affected differently from the irreversible changes that occur due to aging. Since the robustness of ordering based RO-PUFs depends on the f_{thp} parameter, different frequency reduction rates may cause frequency fluctuation values greater than the f_{thp} value and result in ordering changes within some groups. Each RO pair that changes ordering is called a problematic RO pair. The probability of erroneous output generation due to problematic RO pairs is discussed in [28]. An unintended change of ordering in a

TABLE III
NUMBER OF PROBLEMATIC RO PAIRS

f_{thp} **error (kHz)**	**50**	**100**	**150**
Num. of Problematic Pairs	2	5	15

group is called a symbol error and depends on three conditions. Initially, problematic RO pairs should be placed in the same group. Secondly, ordering of the RO pair should be prone to error generation, i.e., if the slower RO slows down more than the faster RO due to environmental conditions, noise, or aging effects, ordering does not change and an error is not generated. The third condition is to have the worst case environmental conditions and noise in the system to trigger the symbol error by pushing the frequency change within a pair by more than the f_{thp} value. The probability of symbol error rate is then given as

$$p = 0.5 * \sum_{s=2}^{m} k_s * (s-1)/(M*(M-1)) \tag{4}$$

in [28] where M is the total number of ROs implemented, s is the group length, k_s is the average number of groups with size s, and m is the size of the largest group. Based on this formula, the symbol error rate for a system of 160 ROs that has a single problematic RO pair is given as 2.26×10^{-3} for an f_{thp} value of 1 MHz. The number of problematic RO pairs depends on the effect of aging on the f_{thp} value, which is called $f_{th_{aging}}$. $f_{th_{aging}}$ is basically the difference between the frequency changes of the most and least slowing ROs after the AAT. If the $f_{th_{aging}}$ value is not taken into account during the calculation of the f_{thp} value, higher values of $f_{th_{aging}}$ will result in a higher number of problematic RO pairs; hence, increasing the probability of the symbol errors. The effect of a wrong f_{thp} value on the number of problematic RO pairs is discussed in [28] and presented in Table III. Based on this data, if an $f_{th_{aging}}$ value of 100 kHz is introduced during the lifetime of the system, 5 problematic RO pairs may be generated. In this case, the symbol error probability of the overall system can be calculated as $5 \times 2.26 \times 10^{-3} = 1.13 \times 10^{-2}$. This error probability can be acceptable especially in identification and authentication systems.

Even though the symbol error probability introduced due to aging in ordering based RO-PUFs is low, 100% robustness is mandatory for systems that utilize PUF circuits as cryptographic key generators. For this purpose, we propose a compensation method based on updating the f_{thp} value according to the expected effects of aging. In this method, the f_{thp} value is updated by adding $f_{th_{aging}}$ value as

$$f_{thp} = f_{th_{noise}} + f_{th_{env}} + f_{th_{aging}}. \tag{5}$$

Since DP will use a larger f_{thp} value due to aging compensation, frequency difference between the ROs in a group will be larger. This will prevent the system from unintended ordering changes that may be result of aging and maintain the robustness of outputs.

TABLE IV
EFFECT OF AGING ON f_{thp} PARAMETER AND CORRESPONDING AREA OVER

Acc. Aging Duration (Hours)	0	100	200	300	400	500
Max. Freq Diff. Ratio (%)	0	0.002	0.0027	0.003	0.0028	0.0034
Corresponding $f_{thp_{aging}}$ effect	0 kHz	400 kHz	540 kHz	600 kHz	560 kHz	680 kHz
Required Number of RO's	88	110	119	119	119	126
Area Overhead (%)	0	25	35	35	35	43

Maximum frequency reduction difference ratio based on the duration of AAT is presented in Table IV. The frequency difference between the most and least slowing ROs is calculated as 0.2% after 100 hours and 0.34% after 500 hours of AAT. Corresponding $f_{th_{aging}}$ value is also calculated and presented based on the average oscillation frequency, 200 MHz. According to the presented data, if the system designer wants to secure the system up to 3 years of fulltime working duration, an $f_{th_{aging}}$ value of 680 kHz should be added to the f_{thp} value. Since increasing the f_{thp} value requires increasing the number of ROs implemented to maintain the generation of similar length outputs, area efficiency of the system is degraded. Using the frequencies collected from the FPGA under NOC prior to AAT, the number of ROs required for an ordering based RO-PUF that generates 128 bit length outputs is calculated for an $f_{th_{noise}} + f_{th_{env}}$ value of 1 MHz and different $f_{th_{aging}}$ values ranging from 0 to 680 kHz. As can be seen from Table IV, the minimum required number of ROs varies from 88 to 126, depending on the expected working duration. Depending on these values, an area overhead of up to 43% arises for guaranteed reliability. The proposed compensation mechanism also protects the system from any uniqueness degredation due to aging, since the outputs remain the same before and after aging. Even though an area overhead is introduced due to aging, an easily applicable aging compensation mechanism is an advantage of the ordering based RO-PUF structures, which will sustain their widespread use in security systems. Robustness of the system without the compensation mechanism is analyzed in [28]. It is reported that an f_{thp} shift of 150kHz resulted in a bit error rate of 0.2, which means that 20% of the output bits became erroneous in this case. In this work, $f_{th_{aging}}$ is calculated as 680kHz for three years of reliable operation, which will degrade the robustness of the system to an unacceptable point without any compensation.

VI. CONCLUSION

Aging is an important phenomenon for the reliability of all ICs and can be even more severe for PUFs that rely on small mismatches in the electrical characteristics of the circuits. In this work, we have analyzed the effects of aging on ordering based RO-PUFs via an AAT applied on ROs that are implemented in an FPGA environment. According to

the analysis results, aging emerges as an unreliability source for ordering based RO-PUFs and threatens the robustness of the structure. In order to protect the robustness of the ordering based RO-PUFs, an efficient compensation method is proposed based on updating the f_{thp} parameter of the system. The performance of the proposed method in terms of area efficiency is presented as well.

REFERENCES

[1] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Design Automation Conference (DAC)*, 2007, pp. 9–14.

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

[3] R. S. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 6, pp. 2026–2030, 2002.

[4] P. Tuyls, G. J. Shrijen, B. Skoric, J. V. Geloven, N. Verhaegh, and R. Walters, "Read proof hardware from protective coatings," in *18th Annual Computer Security Applications Conference (CHES)*, vol. 4249, 2006, pp. 369–383.

[5] D. Lim, J. Lee, B. Gasend, G.E.Suh, M. V. Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Transactions on VLSI Systems*, vol. 13, no. 10, pp. 1200–1205, 2005.

[6] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas, "Delay-based circuit authentication and applications," in *ACM Symposium on Applied Computing*, 2003, pp. 294–301.

[7] B. Gassend, "Physical random functions," M.S. Thesis, Massachusetts Institute of Technology, Massachusetts, 2003.

[8] J. Guajardo, S. Kumar, G. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *18th Annual Computer Security Applications Conference (CHES)*, vol. 4727, 2007, pp. 63–80.

[9] J. Guajardo, S. Kumar, R. Maes, G. Schrijen, and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," in *Hardware-Oriented Security and Trust (HOST)*, 2008, pp. 67–70.

[10] D. Suzuki and K. Shimizu, "The glitch PUF: A new delay-PUF architecture exploiting glitch shapes," in *Cryptographic Hardware and Embedded Systems (CHES)*, 2010, pp. 366–382.

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

[12] G. Komurcu and G. Dundar, "Determining the quality metrics for PUFs and performance evaluation of two RO-PUFs," in *IEEE 10th International New Circuits and Systems Conference, (NEWCAS)*, 2012, pp. 73–76.

[13] A. Maiti, L. McDougall, and P. Schaumont, "The impact of aging on an FPGA-based physical unclonable function," in *International Conference on Field Programmable Logic and Applications (FPL)*, 2011, pp. 151–156.

[14] Z. Kufluoglu and M. A. Alam, "A computational model of NBTI and hot carrier injection time-exponents for MOSFET reliability," *Journal of Computational Electronics*, vol. 3, no. 3-4, pp. 165–169, 2004.

[15] S. Zafar, Y.-H. Kim, V. Narayanan, C. Cabral, V. Paruchuri, B. Doris, J. Stathis, A. Callegari, and M. Chudzik, "A comparative study of NBTI and PBTI (charge trapping) in SiO2/HfO2 stacks with FUSI, TiN, Re gates," in *Symposium on VLSI Technology. Digest of Technical Papers.*, 2006, pp. 23–25.

[16] A. Boyer and S. Ben Dhia, "Effect of aging on power integrity of digital integrated circuits," in *14th Latin American Test Workshop (LATW)*, 2013, pp. 1–5.

[17] J. Srinivasan, S. Adve, P. Bose, and J. Rivers, "The impact of technology scaling on lifetime reliability," in *International Conference on Dependable Systems and Networks*, 2004, pp. 177–186.

[18] M. Kirkpatrick and E. Bertino, "Software techniques to combat drift in PUF-based authentication systems," in *Secure Component and System Identification (SECSI)*, 2010.

[19] S. Meguerdichian and M. Potkonjak, "Device aging-based physically unclonable functions," in *48th ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2011, pp. 288–289.

[20] R. Maes, V. Rozic, I. Verbauwhede, P. Koeberl, E. van der Sluis, and V. van der Leest, "Experimental evaluation of physically unclonable functions in 65 nm CMOS," in *Proceedings of the ESSCIRC*, 2012, pp. 486–489.

[21] A. Maiti and P. Schaumont, "The impact of aging on a physical unclonable function," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2013.

[22] T. Rahman, D. Forte, J. Fahrny, and M. Tehranipoor, "Aro-puf: An aging-resistant ring oscillator puf design," in *Proceedings of the Conference on Design, Automation & Test in Europe*, ser. DATE '14. 3001 Leuven, Belgium, Belgium: European Design and Automation Association, 2014, pp. 69:1–69:6. [Online]. Available: http://dl.acm.org/citation.cfm?id=2616606.2616692

[23] A. Maiti, J. Casarona, L. Mchale, and P. Schaumont, "P.: A large scale characterization of ro-puf," in *In: IEEE Symposium on Hardware-Oriented Security and Trust (HOST*, 2010, pp. 94–99.

[24] M.-D. Yu and S. Devadas, "Secure and robust error correction for physical unclonable functions," *IEEE Design Test of Computers*, vol. 27, no. 1, pp. 48–65, Jan 2010.

[25] C. Yin and G. Qu, "LISA: Maximizing RO-PUF's secret extraction," in *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2010, pp. 100–105.

[26] G. Komurcu, A. E. Pusane, and G. Dundar, "Dynamic programming based grouping method for RO-PUFs," in *9th Conference on Ph. D. Research in Microelectronics and Electronics (PRIME)*, 2013, pp. 329–332.

[27] G. Komurcu, A. Pusane, and G. Dundar, "Enhanced challenge-response set and secure usage scenarios for ordering-based ring oscillator-physical unclonable functions," *Circuits, Devices Systems, IET*, vol. 9, no. 2, pp. 87–95, 2015.

[28] G. Komurcu, A. E. Pusane, and G. Dundar, "An efficient grouping method and error probability analysis for RO-PUFs," *Computers & Security*, 2014, doi:10.1016/j.cose.2014.11.009.