The Impact of Aging on an FPGA-based Physical Unclonable Function

Abhranil Maiti
Electrical and Computer Engineering
Virginia Tech
Blacksburg, Virginia 24061
Email: abhranil@vt.edu

Logan McDougall
Electrical and Computer Engineering
Virginia Tech
Blacksburg, Virginia 24061
Email: 1337@vt.edu

Patrick Schaumont
Electrical and Computer Engineering
Virginia Tech
Blacksburg, Virginia 24061
Email: schaum@vt.edu

***Abstract*—On-chip Physical Unclonable Functions (PUFs) are emerging as a powerful security primitive that can potentially solve several security problems. A PUF needs to be robust against reversible as well as irreversible temporal changes in circuits. While the effect of the reversible temporal changes on PUFs is well studied, it is equally important to analyze the effect of the irreversible temporal changes i.e. aging on PUFs. In this work, we perform an accelerated aging testing on an FPGA-based ring oscillator PUF (RO-PUF) and analyze how it affects the functionality of the PUF. Based on our experiment using a group of 90-nm Xilinx FPGAs, we observe that aging makes PUF responses unreliable. On the other hand, the randomness of PUF responses remains unaffected despite aging.**

***Keywords*-Physical Unclonable Function; aging; FPGA;**

I. Introduction

With an ever-increasing usage of computing devices, security challenges such as protecting user data and preserving user privacy are becoming significant. An on-chip PUF can solve these challenges in an efficient way. It is a die-specific, challenge-response function which maps its challenges to its responses based on complex, random variation of logic and interconnect in integrated circuits (ICs). This process variation is spatial in nature and is expected to remain static in the post-fabrication phase of a chip. Among many possible applications of PUF, it can be used as a random key generator, as a volatile key storage technique and as a challenge-response generator in an authentication mechanism [1]. Moreover, it is tamper-resistant against physically invasive attacks [2].

However, before a PUF can be successfully used in a system, we need to answer many fundamental questions. A designer needs to ensure that a PUF produces statistically unpredictable as well as chip-specific response for a given challenge. Furthermore, though a PUF is built upon spatial variation of ICs, temporal variations such as changing ambient temperature and supply voltage fluctuation negatively affect the reproducibility of PUF responses.

The effect of temporal variations in ICs can be of two types: reversible and irreversible. Varying ambient temperature, supply voltage fluctuation cause changes in ICs that disappear once the applied variation is withdrawn. For example, at a higher temperature, an IC might operate slower than its intended frequency, but it can restore its normal frequency once it is cooled down to its normal operating temperature. This type of change is fast and can be observed over a reasonably short period of time. On the other hand, aging causes irreversible changes in circuit components leading to permanent shifts in the circuit behavior. VLSI phenomena such as negative bias temperature instability (NBTI), temperature-dependent dielectric breakdown (TDDB), hot carrier injection (HCI) and electro-migration are some of the causes of aging [3]. With the continuous shrinking of silicon devices, aging is becoming more prominent [4].

There have been several PUF techniques proposed so far such as Arbiter PUF [5], SRAM-based PUF [6], ring oscillator-based PUF [1] and Butterfly PUF [7]. All these works have mainly focused on extracting random responses out of ICs and ensuring the reproducibility of the responses over reversible temporal changes in circuits. However, it is also very important to study the effect of aging on the PUF functionality. Kirkpatrik et al. proposed software-based techniques to prevent drift in PUF responses due to aging with the assumption that aging alters the PUF responses; no analysis of the aging effect on the PUF functionality was provided [8]. Though a preventive solution is necessary in case a PUF is affected by aging, it is equally important to study how aging actually affects the functionality of a PUF. In this work, we present an analysis of the aging effect on PUF based on an on-chip aging testing as well as simulation. The experimental data is based on a ring oscillator-based PUF implemented on commercially available FPGAs. We have three distinct contributions in this work.

1) We present a detailed analysis of the effect of circuit aging on the functionality of a PUF. The analysis is done in the context of two main PUF application scenarios: device authentication and cryptographic key generation.
2) We performed an on-chip, accelerated aging testing to observe the effect of aging on PUFs. This shows how the frequencies of the ROs in an RO-PUF change with aging and how that change eventually influences the PUF functionality.
3) Finally, we extrapolated the aging effect on a large population of FPGA chips using simulation to estimate how the ability of a PUF to distinguish several chips is influenced by it.

The experimental results, based on a group of 90-nm Xilinx FPGAs, show that aging makes the responses produced by a PUF unreliable. However, the randomness

of PUF responses remains unaffected despite aging.

The rest of the paper is organized as follows. Section 2 briefly describes the aging phenomena in ICs and the related works on the aging effect on PUF. Section 3 presents an analysis of the PUF functionality and the possible implications of aging on it. The results of the on-chip experiments and the simulations are presented in Section 4. We discuss security risks of PUF due to aging in Section 5 along with the possible countermeasures. We conclude the paper in Section 6.

II. Background

In this section, we discuss an overview of circuit aging and few related works on the aging effect on PUF.

A. Circuit aging

With continuous usage of ICs, circuit components gradually undergo structural degradation, resulting in hard faults. These faults cannot be rectified and make a chip unreliable to use. Two main types of degradation are: a) oxide wear-out and b) interconnect failure [3].

a) Oxide wear-out - The gate oxide of a transistor wears out due to the following phenomena.

1) Negative Bias Temperature Instability (NBTI) - Due to the applied electric field across the gate oxide, dangling bonds are developed at the interface of the channel and the oxide layer. This affects a transistor by increasing the threshold voltage thus making switching difficult. NBTI is enhanced by high temperature and high supply voltage.

2) Hot Carrier Injection (HCI) - When carriers with high energy collide with the gate oxide layer and remain trapped there, the oxide layer is damaged, resulting in alteration of the transistor characteristics. High switching rate of a circuit as well as excess supply voltage enhance this effect.

3) Temperature-Dependent Dielectric Breakdown (TDDB) - Due to the voltage applied across the gate oxide, conduction starts through it using the trapped charges, resulting in gradual break-down of the oxide layer. A high operating voltage as well as higher temperature accelerate TDDB.

b) Interconnect failure- Besides the transistors, interconnecting wires too are prone to aging. Electro-migration causes failure in interconnects. Due to high current flow, the metal atoms in the wires shift, resulting in faulty connections. This is enhanced by high temperature.

Assessment and prevention of failures in ICs are among the major concerns for the designers. Research has been done to predict the failure of chips as well as to prevent it. Since aging is time-dependent and often takes a long period of time to introduce noticeable errors, accelerated aging testing has been one of the ways pursued by the researchers to estimate aging. Stott et al. performed accelerated aging testing to estimate how FPGA components such as LUTs, routing wires degrade with time [9]. In this work, we run accelerated aging on an FPGA-based RO-PUF to observe how a PUF is influenced by aging.

B. Previous works on the aging effect on PUFs

Kirpatrik et al. proposed software-based techniques to prevent the effect of aging on PUFs [8]. They proposed two solutions: a) detection of drift in PUF responses due to aging and updating the affected challenge-response pairs (CRPs) b) prevention of drift in PUF responses by making the lifespan of a CRP short. The proposed solutions employed protocol-level techniques such as Feige-Fiat-Shamir zero-knowledge protocol and Markel Hash tree, and did not involve any implementation results. In our work, we mainly focus on estimating the effect of aging on the PUF characteristics using on-chip experiments as well as simulations, and evaluate the possible implications.

In another work, Lim et al. briefly mentioned about aging in their work on the Arbiter-based PUF [5]. They performed a one-month-long aging testing on the Arbiter PUF under normal condition without applying increased temperature or excess supply voltage. On the contrary, in this paper, we performed an aging testing not only under normal condition but also applying elevated temperature and excess voltage on the PUF. Additionally, we analyze the effect of aging on PUF with significant elaboration.

Guajardo et al. also discussed about the robustness of SRAM PUF against aging [6]. However, the PUF robustness was evaluated against a specific case of continuous writing of ones and zeros in SRAM cells. Aging of the SRAM PUF was not done under severe operating conditions such as increased temperature and excess supply voltage. We instead evaluated the aging effect on PUFs caused by the traditional VLSI degradation factors using voltage and temperature stress on an RO-PUF.

III. PUF Functionality and Aging

In this section, we analyze how the functionality of a PUF could possibly be affected by aging. We propose a hypothesis that is based on the functional characteristics of a PUF. We consider two primary application scenarios of a PUF and point out the implications they will have if aging occurs. The scenarios are: a) device authentication and b)cryptographic key generation. We first introduce two parameters of a PUF: Inter-chip Hamming Distance (HD_{INTER}) and Intra-chip Hamming distance(HD_{INTRA}).

Inter-chip HD - If two chips, i and j ($i \neq j$), have n-bit responses, R_i and R_j respectively for the challenge C, the average inter-chip HD among k chips is defined as :

$$HD_{INTER} = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(R_i, R_j)}{n} \times 100\% \tag{1}$$

It is an estimate of the inter-chip variation in terms of the PUF responses, and not the actual probability of the inter-chip process variation.

Intra-chip HD - To estimate the intra-chip HD, we extract an n-bit reference response (R_i) from the chip i at normal operating condition (at room temperature using the normal supply voltage). The same n-bit response

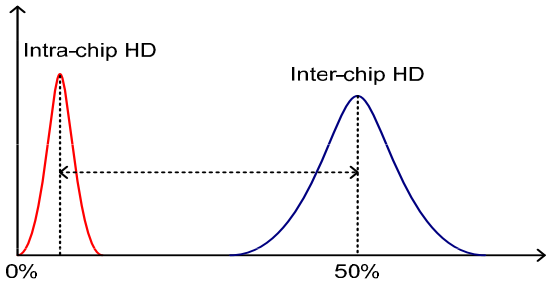

Figure 1. Basic PUF functionality

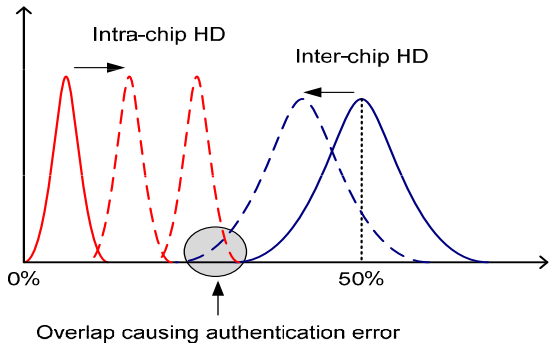

Figure 2. Possible effect of aging on the functionality of PUF

is extracted at a different operating condition (different ambient temperature or different supply voltage) with a value R'_i. m samples of R'_i are collected. For the chip i, the average intra-chip HD is estimated as follows.

$$HD_{INTRA} = \frac{1}{m}\sum_{l=1}^{m}\frac{HD(R_i, R'_{i,l})}{n} \times 100\% \quad (2)$$

where $R'_{i,l}$ is the l-th sample of R'_i. HD_{INTRA} indicates the average number of unreliable/noisy PUF response bits. In other words, the reliability of a PUF can be defined as:

$$Reliability = 100\% - HD_{INTRA} \quad (3)$$

Figure 1 shows an example of the distributions of the intra-chip HD and the inter-chip HD of a PUF [1]. Ideally, for a truly random PUF, the inter-chip HD is centered around 50%. For minimal error, the intra-chip distribution should be centered near 0%. We now discuss how the two applications, mentioned earlier, could be affected by aging.

a) Device Authentication - For an error-free authentication, the two distributions shown in Figure 1 should stay as far as possible from each other. Now, if the two distributions shift closer to each other (shown by the dashed curves in Figure 2) and eventually have an overlap, there will be errors in the authentication (Figure 2). There are two types of error:

1)False negative - If the responses of a chip deviate significantly from its reference, it might be deemed as a different chip and rejected, resulting in a false negative.

2)False positive - If a chip's responses drift from its reference and become nearly equal to some other chip's responses, it might be accepted with the other chip's identity. This is called false positive. It is useful to mention that when multiple chips produce similar responses, bit-aliasing occurs and the entropy of the PUF goes down. This is because if a particular response bit produces the same binary value across multiple chips, it becomes deterministic and cannot be used any more as a source of randomness/entropy.

Our hypothesis is that if the circuit aging affects the functionality of a PUF, it will result in a time-dependent shift of the intra-chip as well as the inter-chip distribution. Now, for a sizable population of chips, the average inter-chip HD cannot be more than 50% [6], [1]. Therefore, the inter-chip HD distribution cannot move towards its right on the x-axis in Figure 2, and can only shift towards the left. On the other hand, the intra-chip HD distribution, being non-negative, can only move towards the right. Both the constraints lead to a possible error in authentication. With our experiments, we intend to observe whether a shift takes place or not. It is important to note that this shift due to aging is a one-way process and cannot be reverted if takes place.

b) Cryptographic Key Generation - In cryptographic applications, the keys formed by the response bits of a PUF must be completely error-free because a cryptographic algorithm generates a drastically different output if the key is altered even by a single bit. This is a strict requirement in a cryptographic application. However, PUF-generated responses are noisy by nature and cannot be reproduced exactly over multiple samplings. This is the reason why the intra-chip HD distribution in Figure 1 is always centered around a positive value. To minimize the noise, researchers have employed several error correction methods to produce error-free PUF keys. However, implementing an error-correction scheme is expensive, and the cost depends on how many bits need to be corrected by it. This is aggravated if the intra-chip HD distribution shifts towards its right (refer to Figure 2) due to aging. Therefore, estimating errors in the PUF responses due to aging is important.

As a summary, our hypothesis is that the characteristic functionality of a PUF may not remain static over time as circuit aging may introduce a time-dependent shift in its behavior. Using an accelerated aging testing, we want to validate the hypothesis and estimate how severe the effect of aging can be.

IV. Results

Here, we present the results of the on-chip experiments, the simulations and their analysis for the aging testing on the RO-PUF. An RO-PUF has n identically laid-out ROs [1]. A pair of frequencies, f_a and f_b $(a \neq b)$ out of n RO outputs, are selected as challenge to create a response. Due to random process variation, f_a and f_b tend to differ from each other. A response bit r_{ab} is produced by a simple comparison method: $r_{ab} = 1$ if $f_a > f_b, r_{ab} = 0$ otherwise.

[1]The figure represents a hypothetical case (not based on real data).

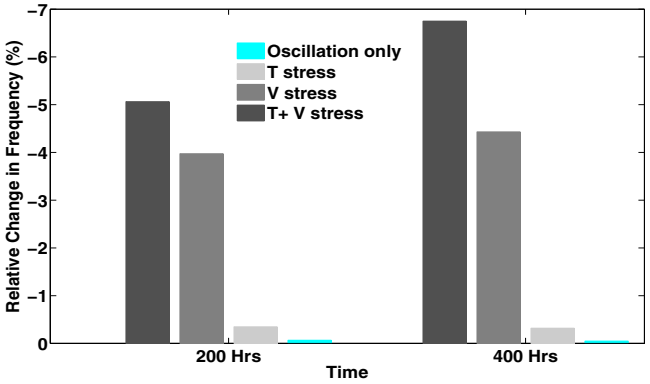

Figure 3. Change in RO Frequencies for different stresses

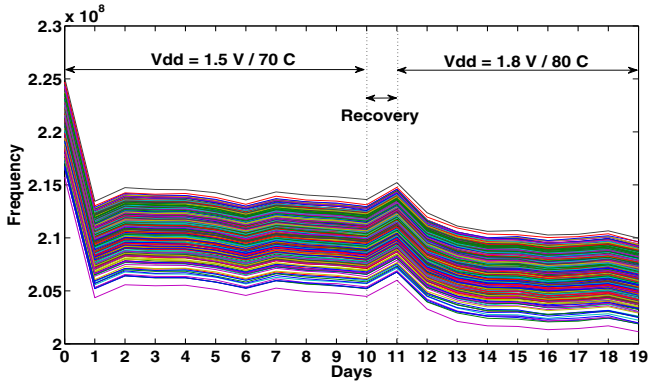

Figure 4. RO Frequency variation with aging under T+V stress

A. Experimental set up for accelerated aging

The aging experiments were done on Xilinx Spartan 3E FPGAs (XC3S500E). An RO-PUF with a group of 512 ring oscillators was implemented in a 32×16 array form on the FPGAs. We enhanced the process of aging by applying stress in terms of excess operating temperature and excess supply voltage to the core of the FPGAs. As mentioned in Section II-A, the major aging phenomena are accelerated by excess temperature and over-voltage. The FPGAs were heated using a convection-based heating oven, and the supply to the FPGA core was increased using a regulated DC power supply. We considered four different cases for the accelerated aging testing. In the first case (oscillation-only stress), all the 512 ROs were enabled simultaneously without any temperature and voltage stress. In the second case (V stress), we applied a supply voltage of 1.5V and 1.8V in two phases instead of the normal supply voltage of 1.2V to the FPGA core. In the third case (T stress), an FPGA was stressed with a temperature of 70°C and 80°C in two phases. In the fourth and the final case (T+V stress), an FPGA was stressed with 70°C temperature as well as 1.5V supply in one phase, and the stress condition was 80°C as well as 1.8V in the second phase. Four different FPGAs were used for the four cases as shown in Table I. In all of the T,V and T+V cases, 512 ROs were enabled simultaneously.

B. The effect of aging on PUF

First, we show the change in RO frequencies over the course of aging. We define the average change in the RO frequencies w.r.t to the pre-aging condition as:

$$\Delta f_{i,age} = \frac{1}{512}\sum_{j=1}^{512}\frac{f_{avg,i,j}|_{t=x} - f_{avg,i,j}|_{t=0}}{f_{avg,i,j}|_{t=0}} \times 100\% \quad (4)$$

Table I
DIFFERENT CASES OF ACCELERATED AGING

	Room temp	70°C	80°C
1.2 V	FPGA1	FPGA2	FPGA2
1.5 V	FPGA3	FPGA4	-
1.8 V	FPGA3	-	FPGA4

$f_{avg,i,j}|_{t=0}$ is the average frequency of the j-th RO of the i-th FPGA before the start of the aging experiment, and $f_{avg,i,j}|_{t=x}$ is that at time $t = x, x > 0$ and $f_{avg,i,j} = \frac{1}{100}\sum_{k=1}^{100} f_{i,j,k}$ where $f_{i,j,k}$ is the k-th sample frequency of the j-th RO of the i-th FPGA. Figure 3 shows $\Delta f_{i,age}$ for the four FPGAs stressed under different conditions at two different point of aging: 200 hours and 400 hours. We observe that the reduction (-ve y-axis) in frequency for the oscillation-only stress and the T stress are negligible compared to the other two cases. Therefore, we analyze the cases of V stress and T+V stress only. As an example, Figure 4 shows the variation in the frequencies of 512 ROs for the T+V stress. On the x-axis, the 0th day represents the condition before the accelerated aging started. We deliberately allowed the FPGAs to remain under stress-free condition for the 11th day to see if the chip recovers. An increase in frequency, though small, at the end of the recovery period implies that the V and T stress induce temporary changes besides permanent shifts. Overall, we see that there is a significant reduction in RO frequencies due to aging. All the FPGAs were found to be operational at the end of the aging testing.

Intra-chip HD of PUF due to aging - 511 response bits were created using the simple comparison method to evaluate all the PUF parameters. We calculated the intra-chip HD using Equation (2) for the V and T+V cases as shown in Figure 5. It is clear that the intra-chip HD for both the cases have increased compared to the pre-aging condition. This means aging causes more unreliable bits in PUF, resulting in the shift of the intra-chip HD distribution towards the inter-chip HD distribution. For example, under the T+V stress, the number of unreliable bits increased from ≈ 5 ($\approx 1\%$) to ≈ 35 ($\approx 7\%$). This is a significant reduction in the reliability of the PUF (from 99% to 93%, refer to Equation (3)). It can be noticed that the intra-chip HD recovers slightly on the 11th day when the chips were taken out of the stress.

Inter-chip HD of PUF based on simulated aging - The inter-chip HD is a population-based parameter and requires a group of chips for estimation. Practically, it is not an easy task to age a significant number of chips as it would require a long period of time as well as

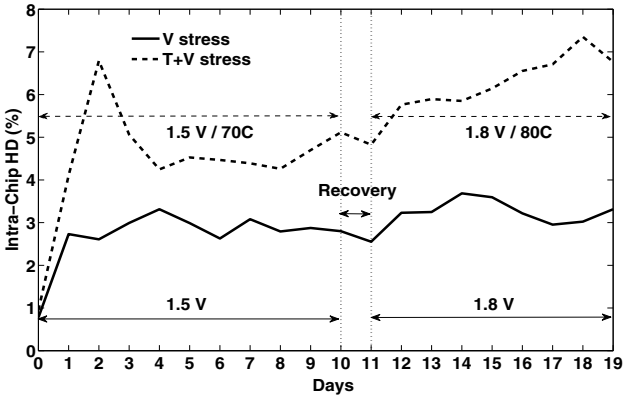

Figure 5. Change in intra-chip HD of PUF with aging

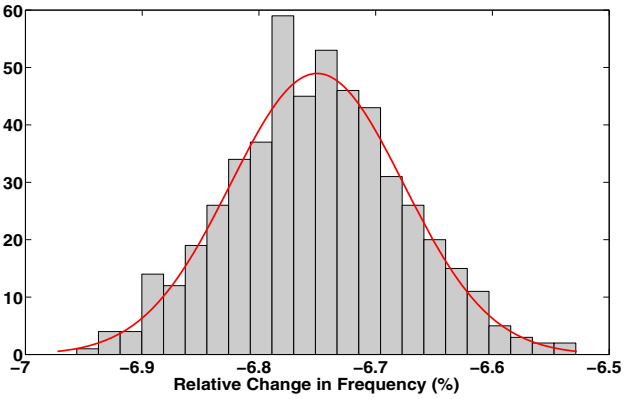

Figure 6. Aging distribution after 400 Hrs with T+V stress

money. Therefore, we employed a simulation technique to extrapolate the aging effect on a large group of FPGAs that were measured using an RO-PUF under normal condition. We decompose the RO frequency as:

$$f_{i,j} = f_{nom,i,j} + \Delta f_{PV,i,j} + \Delta f_{aging,i,j} + \Delta f_{noise,i,j} \quad (5)$$

$f_{nom,i,j}$ is the nominal characteristic frequency of the j-th RO on the i-th FPGA and does not change with aging. $\Delta f_{PV,i,j}$ is the deviation due to manufacturing process variation and also remains static over time. $\Delta f_{aging,i,j}$ is the aging factor and is time-dependent. $\Delta f_{noise,i,j}$ is the variation induced by the noise factor. Experimental data shows that this factor also changes with time.

We have measured a group of 178 ($1 \leq i \leq 178$) Xilinx Spartan3E S500 FPGA chips using an RO-PUF with 512 ROs ($1 \leq j \leq 512$) at normal condition without any stress.[2] We have collected 100 samples for each of the RO frequencies and calculated an average to remove the noise to get $f_{nom,i,j} + \Delta f_{PV,i,j}$. Now, we simulate $\Delta f_{aging,i,j}$ and $\Delta f_{noise,i,j}$ using the aging as well as the noise distribution of the FPGAs that went through aging. Here, we assume that all the chips undergo similar changes due to aging under the same stress condition.

First, at $t = x$ ($x > 0$), we calculated the parameter $\frac{f_{avg,i,j}|_{t=x} - f_{avg,i,j}|_{t=0}}{f_{avg,i,j}|_{t=0}}$ for each of the 512 ROs for the FPGA under stress. By plotting these values, we observed that they follow a normally distributed pattern. One example case for the stress condition T=80°C + V=1.8V is shown in Figure 6. We also checked that these values do not have any correlation with the location of the ROs on the FPGA. Using the mean and the standard deviation of these values, we randomly generated a set of 512 normally distributed values as Δf_{aging} for each of the 178 FPGAs using Matlab, and added them to the pre-aging average frequency values i.e. $f_{nom,i,j} + \Delta f_{PV,i,j}$, resulting in $f_{nom,i,j} + \Delta f_{PV,i,j} + \Delta f_{aging,i,j}$.

For $\Delta f_{noise,i,j}$, we first derived the noise factor of an RO at $t = x$ as the standard deviation of the RO frequency over 100 samples: $\sqrt{\frac{1}{99}\sum_{k=1}^{100}(f_{i,j,k}|_{t=x} - f_{avg,i,j}|_{t=x})^2}$.

[2]This data is from on-chip measurements and not from simulation.

We calculated it for each of the 512 ROs of the stressed FPGA. We observed that this factor also shows normally distributed pattern when plotted. Using the mean and standard deviation of these noise factors, we generated a set of 512 normally distributed $\Delta f_{noise,i,j}$ values for each of the 178 FPGAs using Matlab. We further created 100 samples of $\Delta f_{noise,i,j}$ using $\Delta f_{noise,i,j}$ as the standard deviation for a zero-mean normally distributed variable. These simulated $\Delta f_{noise,i,j}$ values are finally added to the previously computed $f_{nom,i,j} + \Delta f_{PV,i,j} + \Delta f_{aging,i,j}$ values to complete the simulation of $f_{i,j}$ in Equation (5).

We derived response bits using the simulated frequency values and then estimated the inter-chip HD for four cases: at t=200 hours and t=400 hours of aging for each of the T and T+V cases. Table II shows the average, minimum, maximum and standard deviation values of the inter-chip HD distributions for all the cases. It is very consistent across different instances of aging. One of the possible reasons might be that the bit-flips in the PUF responses due to aging is random. In order to check it, we evaluated the Hamming Weight (HW) of the 511-bit PUF response as $\sum_{s=1}^{511} r_{i,s}$. $r_{i,s}$ is the s-th response bit from a chip $i, (1 \leq i \leq 178)$. This is an estimate of the uniformity of the PUF responses. Furthermore, to estimate the entropy loss, we evaluated bit-aliasing in PUF as the Hamming Weight for each s-th response bit position $(1 \leq s \leq 511)$ across 178 chips as $\sum_{i=1}^{178} r_{i,s}$.

Figure 7 shows the scatter plot for the uniformity for each of the four cases of aging simulation with respect to the original (pre-aging) condition. A 1:1 trend shows that aging does not cause noticeable change in uniformity. This shows that, on an average, the number of response bits

Table II
INTER-CHIP HD PARAMETERS DUE TO AGING

	Avg	Min	Max	Std
Before Aging	47.25%	36.98%	56.36%	2.43%
V:200 Hrs	47%	37.37%	56.36%	2.43%
V:400 Hrs	46.96%	36.79%	55.96%	2.4%
T+V:200 Hrs	46.96%	38.16%	56.55%	2.46%
T+V:400 Hrs	46.67%	36.2%	54.99%	2.46%

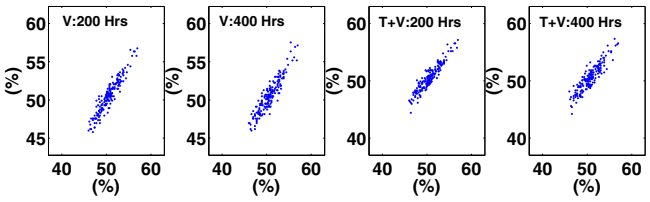

Figure 7. Uniformity of PUF due to aging (aged vs original)

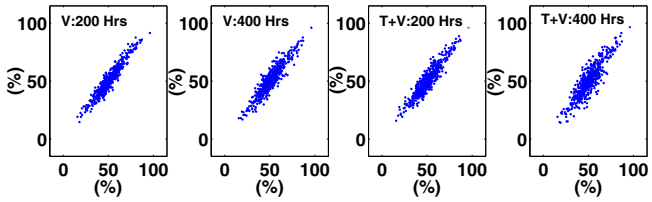

Figure 8. Bit-aliasing of PUF due to aging (aged vs original)

that flipped from '0' to '1' during aging is equal to those that flipped from '1' to '0'. In other words, the change in PUF responses due to aging is random. A similar trend in Figure 8 for the bit-aliasing factor indicates that PUF entropy is not affected by aging.

V. Security Risks and Countermeasures

We observed that by stressing a PUF using excess voltage and temperature, a significant change in the intra-chip HD can be made. This gives the adversaries an opportunity to attack a PUF using temperature and voltage stress. Suppose, in an application, a chip collects critical data from the field and sends them to a server. Now if the chip is authenticated using a PUF, an adversary might attempt to permanently change the property of the PUF by applying heat or excess supply voltage. This way the chip may fail to authenticate itself preventing the critical data to be supplied to the server. Moreover, replacing a damaged chip may not be straightforward and may incur significant cost depending on the nature of the application.

In fact, the use of excess temperature and voltage as an active means of attack against embedded systems has been discussed previously [10]. This type of attack against the RO-PUF can be thwarted with two types of countermeasures: a) active and b)passive. As an active method, a detection mechanism needs to be implemented and necessary preventive actions need to be taken as proposed in [8]. As a passive countermeasure, if we use a simple comparison method to create a response bit, the redundancy technique (proposed by Suh et al.[1]) that selects an RO-pair with maximal frequency difference is a possible solution. Another passive technique could be to employ a different quantization method to produce a PUF response instead of the simple comparison method to break the dependency of a PUF response on the frequency difference between a pair of ROs.

VI. Conclusion

In this paper, we studied the effect of aging on PUFs based on an accelerated aging testing on an FPGA-based RO-PUF implementation. Experimental results show that the intra-chip HD of PUF goes down with aging making it unreliable. We extrapolated the aging effect on a large group FPGA chip using simulation to estimate how inter-chip HD of PUF behaves. Results based on a group of 90-nm FPGAs show that inter-chip HD of PUF remains unaffected by aging. Moreover, aging does not cause loss in entropy of PUF. As a part of future work, we consider exploring techniques to prevent the aging effect on PUF as well as studying the security risks on PUFs due to aging. We also intend to observe the aging effect on PUF on smaller technology nodes.

Acknowledgment

This work was supported by the National Science Foundation by grant no. 0964680 and grant no. 0855095.

References

[1] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proceedings of the 44th annual Design Automation Conference*, ser. DAC '07, 2007, pp. 9–14.

[2] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM conference on Computer and communications security*, ser. CCS, 2002, pp. 148–160.

[3] N. Weste and D. Harris, *CMOS VLSI Design: A Circuits and Systems Perspective, (4th edition)*.

[4] D. Lorenz, G. Georgakos, and U. Schlichtmann, "Aging analysis of circuit timing considering nbti and hci," in *On-Line Testing Symposium, (IOLTS). 15th IEEE International*, 2009, pp. 3 –8.

[5] D. Lim, J. Lee, B. Gassend, G. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, vol. 13, no. 10, pp. 1200 – 1205, 2005.

[6] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "Fpga intrinsic pufs and their use for ip protection," in *Proceedings of the 9th international workshop on Cryptographic Hardware and Embedded Systems*, ser. CHES '07, 2007, pp. 63–80.

[7] S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "Extended abstract: The butterfly puf protecting ip on every fpga," in *Hardware-Oriented Security and Trust. HOST, 2008. IEEE International Workshop on*, pp. 67 –70.

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

[9] E. A. Stott, J. S. Wong, P. Sedcole, and P. Y. Cheung, "Degradation in fpgas: measurement and modelling," in *Proceedings of the 18th annual ACM/SIGDA international symposium on Field programmable gate arrays*, 2010, pp. 229–238.

[10] G. Gogniat, T. Wolf, W. Burleson, J.-P. Diguet, L. Bossuet, and R. Vaslin, "Reconfigurable hardware for high-security/high-performance embedded systems: The safes perspective," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, vol. 16, no. 2, pp. 144 –155, 2008.