

Aging Resilient RO PUF with Increased Reliability in FPGA

Sreeja Chowdhury, Xiaolin Xu, Mark Tehranipoor, Domenic Forte
Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL
sreejachowdhury@ufl.edu, {xiaolinxu, tehranipoor, dforte}@ece.ufl.edu

Abstract—Several design approaches have been proposed for IP protection, attestation, etc. of FPGA hardware designs and physical unclonable function (PUF) is one of the most popular amongst them. However, different transient variations like temperature, supply voltage and environmental noise make it challenging for a PUF to produce a reliable signature. Besides the above-mentioned issues that impact the transient reliability of PUFs, aging is another factor that produces irreversible impact on the reliability of PUFs. Though an aging resistant ring oscillator (RO) PUF has been proposed previously for ASIC design, implementing the same technique in FPGA is impossible as it involves redesigning the circuit at transistor level. In this paper, we propose an aging resilient RO PUF design on FPGA that exploits the SRAM cells and multiple paths available in FPGA look up tables (LUTs). The aging of our proposed RO PUF can be slowed down by putting the oscillation path into sleep mode. Experimental measurements from Spartan 3A FPGA boards demonstrate that our proposed RO PUF is less affected by aging, the reliability of which increases by 37.4% on an average. Moreover, by comparing our design with conventional RO PUF in FPGA, the aging degradation decreases by 37%.

I. INTRODUCTION

Electronic counterfeiting is a persistent threat to the semiconductor industry, especially with increasing incorporation of third party intellectual property (3PIP) and growing complexity of supply chain. Physical unclonable functions (PUFs) have been widely researched as a vital approach to combat cloning of electronic ICs [1] [2]. Silicon manufacturing variations are intrinsic, random, unclonable and thus are used by PUFs to generate a fingerprint for an integrated circuit (IC). The main applications of PUF include authentication and key generation. Several types of PUFs have been proposed such as delay based PUF (RO, arbiter), memory based PUF (SRAM, DRAM), optical PUF, etc. The performance of a PUF is characterized by PUF metrics which include uniqueness, reliability and randomness [3]. A PUF generated identifier should be reliable across varying operating and environmental conditions which is quantified by the intra-chip hamming distance.

RO PUF is one of the most popular delay based PUFs (shown in Figure 1a). In RO PUF, a pair of ring oscillator (RO) frequencies are compared to generate a response bit. Though both the ROs have the same number of delay stages, their frequencies vary due to process variations and noise which are intrinsic properties of a chip. The difference in the frequencies (positive or negative) can be quantized as an output response bit. There is an advantage of implementing a RO PUF to other delay based PUFs (arbiter PUF) in FPGA. For the latter, routing asymmetry can cause delay changes 10% higher than that from process variations which makes

it difficult to implement in FPGA [4]. On the contrary, RO PUFs do not have a strict requirement on routing asymmetry, therefore can be easily implemented in FPGAs. However, there are also some disadvantages for RO PUFs in FPGA. The designer should minimize the systematic variations along the RO paths through careful layout to avoid the output bias and allow more randomness for the PUF responses. RO PUFs have high area and power overheads which are also limitations for incorporating it inside any IC. Reliability of a RO PUF is dependent on various parameters like transistor aging, temperature and voltage variations. All these above factors become even more challenging because the internal architecture of FPGA is a black box for the users. This makes it impossible to exploit layout/gate level design alterations to improve reliability.

In this paper, we focus on improving RO PUF reliability in FPGA due to silicon aging. Maiti et. al [3] was the first to study the impacts of aging on FPGA based PUFs and showed that aging increases the number of unreliable bits in a PUF response. The location of response bits that change due to aging was also shown as random. In [5], Parthasarathi et. al proposed to alter SRAM configuration bits and unused inputs of LUTs to leverage aging degradation in FPGA. In [6], the authors implemented techniques which provide smaller reliability reduction and anti aging effects for 65nm CMOS SRAM PUF. An aging resistant PUF was proposed in [7] which reduces NBTI significantly by pumping the input of inverters to high in non-oscillation mode. This idea, though efficient in ASIC designs, is difficult to implement in FPGA where circuit architecture cannot be altered. In [8], we see similar process of using multiple paths and SRAM bits to compensate for aging of ROs in FPGA. Other methods proposed to improve PUF reliability include error correction code (ECC) [9], modelling techniques [10], ranking methodologies [11] and majority voting [12]. However, all these methods will consume extra silicon or power resource to correct the flipped PUF responses.

Compared to [8], our analysis explains the aging degradation improvement in two types of FPGA architectures (T-gate and PT based LUTs). Our experiments focus on reliability and aging degradation improvement of an entire RO PUF and not only ROs. As shown in Figure 1a, an RO is a part of RO PUF which includes several other components like counter, multiplexer, etc. Reducing aging of ROs does not necessarily imply improving PUF reliability. Reliability of RO PUFs increase only if all the ROs in the PUF age homogeneously which is targeted by our proposed technique. Compared to [7], our method focuses on building an aging-resistant RO PUF in FPGA architecture. The method proposed in [7] requires redesigning of transistor level architecture

This work was supported in part by the National Science Foundation under Grant No. 1559772 and by the AFOSR MURI grant under award number FA9550-14-1-0351.

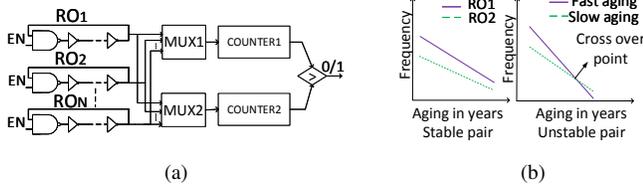


Figure 1: (a) RO PUF architecture (b) Reliability issue of RO PUF with aging: stable and unstable RO pairs.

which is not possible for users in FPGA. Our method also improves reliability thus reducing overhead due to ECC. In this paper, we address the reliability and aging degradation issues of RO PUFs in FPGA architecture through the following contributions.

- We present a detailed analysis of aging impact on conventional RO PUF in FPGA. In addition, we discuss the difference between aging conditions for pass transistor (PT) and transmission (T) gate based LUT structures in FPGA.
- We propose an aging resilient RO PUF in FPGA with increased reliability. Our method utilizes multiple paths and SRAM cell configuration of LUT to build the former. The advantage of this process is that it fully leverages the flexibility of LUTs in FPGA to implement reliable RO PUFs with negligible overhead. We also present a detailed analysis of the aging improvement due to the proposed method assuming 90nm (and above) technology nodes.
- We evaluate the proposed RO PUF with Hspice simulation and silicon implementations on Spartan 3A FPGA. Both results demonstrate that our proposed RO PUF has improved reliability against aging compared to conventional RO PUF.

The paper is organized as follows. Section II briefly describes different LUT configurations, types of aging in transistors and impact of aging on reliability of RO PUF. Section III gives a detailed analysis of aging in conventional RO. Section IV describes the proposed methodology and analysis. Simulation and measurement results are demonstrated in section V. Section VI states the future work and concludes the paper.

II. BACKGROUND

A. Look up Table (LUT) structure in FPGA

Logic functions in FPGA are mapped in configurable logic blocks (CLBs). Each CLB is composed of slices comprising of basic building blocks called look up tables (LUTs) and flip-flops. LUT consists of an array of SRAM cells connected by a multiplexer tree. SRAM cells store the user defined configuration bits and multiplexer logic implements the programmed function. Researchers have studied several types of LUT structures like transmission-gate (T-gate), pass-transistor (PT), etc. [13], [14] to explain the phenomenon of aging in FPGA. Due to structural differences, PT based LUTs and T-gate based LUTs undergo aging differently [13]. T-gate LUTs are 15% larger than PT LUTs in FPGAs. But in lower technology nodes like 22nm, T-gate implementations can be 10-25% faster than PT ones [15]. The schematic implementation of both PT and T-gate based LUTs are shown in Figure 4.

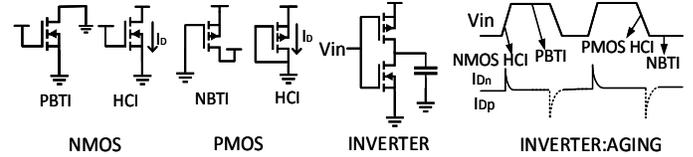


Figure 2: HCI and BTI aging in NMOS and PMOS transistors.

B. Aging in transistors and their types

Transistor aging is one of the major causes of reliability issue faced by modern ICs including FPGAs. It is the resultant of trapped charges and broken bonds at gate dielectric interfaces which results in increase of threshold voltage (V_{th}) and switching activity thus, deteriorating transistor performance in scaled modern devices.

1) Bias Temperature Instability (BTI)

BTI results in a positive shift in the absolute value of V_{th} in both PMOS as well as NMOS. BTI is the condition often referred to as DC stress when the PMOS/NMOS has already pulled up/ down but the gate is still biased in strong inversion. The drain to source voltage becomes zero signifying negligibly small lateral electric field [16] as shown in Figure 2. For PMOS, the condition is called negative BTI (NBTI) whereas for NMOS it is positive BTI or PBTI. Full recovery of transistor can occur from BTI if we can remove inversion ($V_{gs} \approx \text{low}$) and increase lateral electric field ($|V_{ds}| \approx \text{Vdd}$) [17]. NBTI is dominant and PBTI is negligible for high technology nodes. But for lower technology nodes (<65nm) with introduction of high-K metal gates PBTI effect has become a major concern for transistor aging [14].

2) Hot Carrier Injection (HCI)

During transistor switching, the accelerated carriers drift towards the drain under the influence of the lateral electric field. During this process, they generate secondary carriers through impact ionization. It occurs when the transistor is switching under strong inversion ($|V_{gs}| \approx \text{Vdd}$) and the lateral electric field is high ($|V_{ds}| \approx \text{Vdd}$) as demonstrated in Figure 2. As a result, it increases V_{th} of transistor and decreases its switching speed. HCI effect is considered negligible for higher technology nodes but its effect increases rapidly with higher scaling for lower technology nodes (<40nm) [14].

C. Effect of Aging on RO PUF reliability

As shown in Figure 1a, an RO consists of odd number of inverting delay stages which are connected in series. The output of the last stage of RO is fed back to the input of the first stage such that each RO delivers a unique frequency due to process variation. In RO PUF, a pair of ROs is selected and their output pulses are counted for a definite time interval known as the comparison time. The output of the counters is then compared to generate a high/low response bit as shown in Figure 1a. The input of a PUF is a challenge which is applied to both the multiplexers selecting RO pairs. Reliability issues occur if two ROs age differently in a RO PUF. For example, let us take two ROs, RO1 and RO2 whose frequencies get degraded due to aging. These RO pairs generate a stable bit if they age similarly with time and there is no cross over in frequencies with aging. In short, if the RO pair selected age differently like one is aging faster than the other then the bit

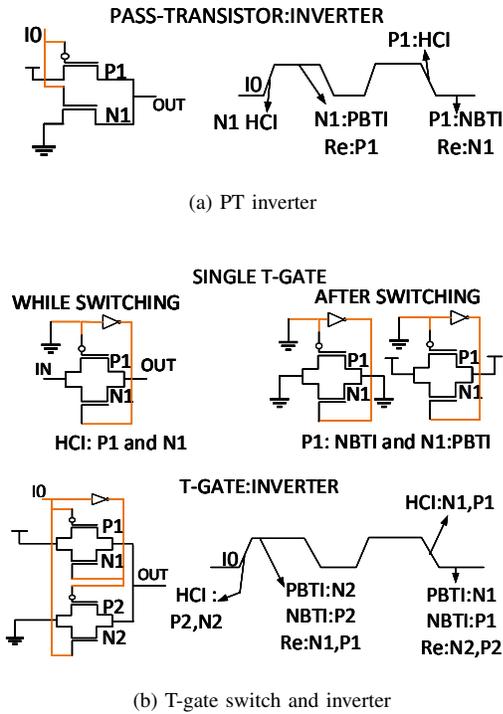


Figure 3: BTI, HCI and Recovery (Re) in PT and T-gate inverter configurations (red wires signify input).

becomes unstable with aging time. A stable RO pair and an unstable RO pair has been shown in Figure 1b.

III. AGING ANALYSIS OF CONVENTIONAL RO IN FPGA

An RO PUF has two types of operating conditions. During oscillation, there is degradation due to HCI aging. HCI is negligible for higher technology nodes ($> 40\text{nm}$) [14]. This concludes that most RO PUFs undergo negligible aging during oscillation. During most of its lifetime, a RO PUF is idle which is referred to as sleep condition. RO PUF undergoes most of its aging when idle as BTI, especially NBTI, is dominant on the transistors (for nodes $> 65\text{nm}$) increasing V_{th} . In this section, we will explain the aging in a conventional RO, where the RO is always configured in oscillation irrespective of its operating condition. As aging of LUT is entirely dependent on its internal structure, we have explained it using two types of LUT structure: the PT based and the T-gate based structure. For simplicity, we have used the 2-input LUTs, but the same analysis is applicable to other LUT structures like 4-input or 6-input.

A. Conventional RO with Pass-Transistor (PT) LUT structure

Figure 3a shows the schematic of a PT inverter structure and summarizes how it ages with the change of input (I0). Whenever the input switches from high to low it forces the PMOS (P1) to switch. During switching, PMOS experiences HCI but as soon as the PMOS output stabilizes to high, it undergoes NBTI until the input switches back to high. Similarly, NMOS (N1) undergoes HCI during low to high input transitions and PBTI when the input is stable at high. The RO implemented with a PT based LUT structure is shown in Figure 4. Every LUT has two inputs I0 and I1, I0

is the feedback input and I1 is the configurable input. The figure shows a five stage RO with four LUTs programmed as inverters and one as a NAND gate. The input enable (EN) controls the sleep and oscillation of the RO. When EN is low, the RO is in sleep mode and when EN is high, RO is in oscillation. The upper half of the RO is chosen as the oscillation path. To ensure oscillation all the LUTs are configured as inverters thus logic status of SRAM cells S0 and S1 are set to high and low respectively.

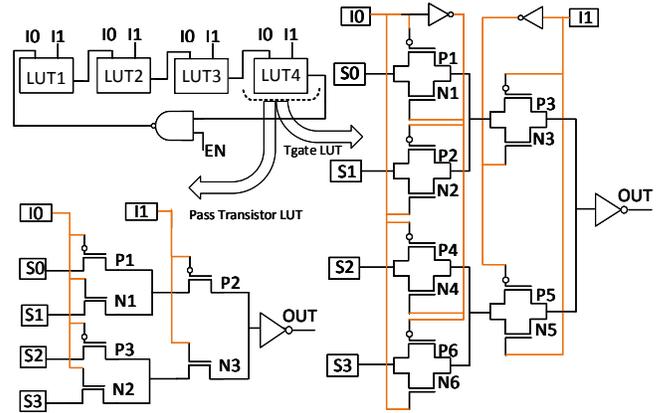


Figure 4: Conventional RO in FPGA with T-gate and PT LUT structure (red wires signify input).

During oscillation, EN is high and the feedback input (I0) of each LUT continuously switches, thus inflicting HCI on the NMOS (N1, N2) and PMOS transistors (P1, P3) during the low to high and high to low transitions respectively. In between switching, N1 and N2 undergo PBTI if the input is stable at high whereas P1 and P3 experience NBTI if input is stable at low. The effect of BTI is not that strong as the transistors continuously switch and experience more degradation due to HCI. The other input I1 is configurable and is usually not defined in a conventional RO. For simplicity, we assume I1 as low for which P2 experience NBTI while N3 undergoes complete recovery. A detailed diagram of aging condition during oscillation has been explained in Figure 5 with changes in input conditions. All the LUTs in the RO experience similar aging condition during oscillation.

During sleep, EN is low, forcing I0 of LUT1 to be high but I1 remains low by default configuration. The LUT SRAM cells hold the same values during oscillation and sleep. The assignment of SRAM bits should be such that, the RO oscillates properly during oscillation mode as well as there is less aging during sleep mode. To ensure oscillation, SRAM cells S0 and S1 are set to high and low respectively. P1 has low $|V_{gs}|$ and high $|V_{ds}|$ thus, it undergoes complete recovery from NBTI (please refer to section II-B). P3 has low $|V_{gs}|$ and its $|V_{ds}|$ depends on logic status of SRAM cells S2 and S3 (N2 acting as a closed switch) which may not be configured for conventional RO. Thus, we may consider partial recovery from NBTI for P3. N2 has high $|V_{gs}|$ and low $|V_{ds}|$, thus undergoing complete stress due to PBTI which can be neglected for our technology node (90nm for Spartan 3A and PTM 90nm model card for Hspice simulation). For LUT2, the configuration gets entirely reversed. As LUT1 is configured as an inverter, it produces a low bit at the output and forces I0 of LUT2 to low

IV. PROPOSED METHODOLOGY AND ANALYSIS

For most modern FPGAs, LUT is commonly used; therefore, multiple paths and SRAM cells can be utilized to compensate aging in ROs and reduce the stress on oscillation path for RO PUFs. Thus, any two ROs in a RO PUF age similarly to generate a stable pair improving overall reliability against aging degradation. In our description, each LUT can be divided into two halves. The first half can be used for oscillation and the other half as sleep path. The path chosen for oscillation can be complementary to the sleep path so that the aging of the oscillation half can be relieved (i.e., receive less stress) during the sleep mode. In our design, the SRAM cells of the sleep half are configured in such a way that similar aging occurs on all the ROs to consistently formulate stable RO pairs. In this section, we analyze the proposed methodology and show how it reduces aging in FPGA LUTs to improve reliability of RO PUF.

A. Proposed RO with PT based LUT architecture:

The aging degradation of the proposed RO is similar to that of a conventional RO during oscillation mode, but it changes during the sleep mode. Referring to the PT based RO structure in Figure 4, during sleep mode we can see that: EN is low which forces the feedback input I0 of LUT1 to high. As we follow the lower half during sleep mode, we make the input I1 of LUT1 high. The SRAM cells S0 and S1 are high and low respectively as we need to configure every LUT as an inverter in oscillation mode. To ensure every LUT always outputs a high during sleep mode, SRAM cells S2 and S3 are configured as low and high respectively. For LUT1, P1 and P2 have low $|V_{gs}|$, which signifies the channel is not in inversion while the lateral electric field for P1 ($|V_{ds}|$) is approximately high. Thus, they undergo recovery from NBTI during sleep mode. For N1, $|V_{gs}|$ is high, signifying an inverted channel. The lateral electric field $|V_{ds}|$ is negligibly small thus forcing complete PBTI on N1.

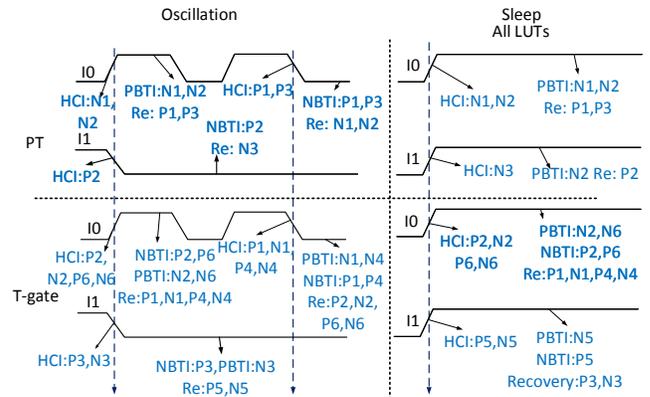


Figure 6: Comparison of BTI and HCI for proposed RO in sleep and oscillation mode (both T-gate and PT architectures) with respect to input signal transition.

The main advantage of using such a configuration is that all the LUTs from LUT1 to LUT4 follow the same degradation. Thus, the aging mechanism for all the pull-up/ PMOS transistors along the oscillation path is similar ensuring a homogeneous aging for all the ROs. Again, all the PMOS

Figure 5: Comparison of BTI and HCI for conventional RO (both T-gate and PT architecture) in sleep and oscillation mode with respect to input signal transition.

and I1 remains low by default configuration. In this case, P1 and P3 undergo complete NBTI whereas N1 and N2 undergo recovery. The transition graphs in Figure 5 show the aging for LUT1 and LUT2 of conventional RO during sleep. LUT3 has same condition as LUT1 and LUT4 follows LUT2. Thus, we see that some transistors in oscillation path undergo recovery while the others undergo complete NBTI or PBTI. This kind of *heterogeneous aging* in oscillation path may be detrimental to the reliability of RO PUF. As the LUTs age heterogeneously, their degradation may override the process variation between the ROs. This produces unstable RO pairs (Figure 1a) and degrades overall reliability.

B. Conventional RO with Transmission (T-gate) LUT structure

As shown in Figure 3b, whenever a single T-gate is switching, both P1 and N1 experience HCI. After switching, P1 and N1 both undergo BTI irrespective of whether the T-gate switches from high to low or vice versa. If configured as an inverter, the upper switch comprising of P1 and N1 acts as pull-up transistor and undergoes aging like that of a PMOS transistor. It experiences BTI during stable low input and HCI during high to low input transitions. The lower switch comprising of P2 and N2 behaves like a pull-down transistor and undergoes aging like NMOS. The transition graph in Figure 3b shows the aging conditions. During oscillation of RO with T-gate LUT structure (shown in Figure 4) P2, N2, P6 and N6 comprising pull-down path experience HCI for low to high input transition. During high to low input switching P1, N1, P4, N4 which comprises the pull-up path experience HCI as shown in Figure 5. The sleep condition aging is similar to that of PT based ROs (please refer to section III-A). The only difference is that instead of two PMOS or NMOS transistors, a set of two pairs of NMOS and PMOS transistors act as pull-up/pull-down for T-gate based LUT. Thus, for LUT1, transistors N2, P2, N6 and P6 experience BTI for the entire sleep time and P1, N1, P4 and N4 undergo recovery. For LUT2, I0 gets reversed thus the aging condition is exactly opposite to that of LUT1. As I1 remains undefined and is taken as default low for the entire RO operation, P3 and N3 experience constant BTI degradation. However, P5 and N5 undergo recovery for all the LUTs irrespective of oscillation or sleep.

Table I: Comparison table of conventional and proposed RO aging with PT based structure.

Types of aging	Conventional RO (5stage)			Proposed RO (5stage)	
	Osc	Sleep		Osc	Sleep
	All LUTs	LUT1 (orLUT3)	LUT2 (orLUT4)	All LUTs	All LUTs
HCI	P1,P3, N1,N2	—	—	P1,P3, N1,N2	—
NBTI	P2	P2	P1,P2, P3	P2	—
PBTI	—	N1,N2	—	—	N1,N2, N3
recovery	N3	P1,P3, N3	N1,N2, N3	N3	P1,P2, P3
Inference	2 osc. path PMOS recover in sleep mode			8 osc. path PMOS recover in sleep mode	

transistors, in oscillation path are in complete recovery as shown in Figure 6 ensuring minimal aging of the oscillation path during sleep mode. Here, we neglect degradation due to PBTI for 90nm technology node (please refer to section II-B). So, we see minimal as well as homogeneous aging for this type of configuration. The homogeneity in aging helps to ensure that whatever changes occur in the rise and fall times of the LUTs due to aging are similar for all the ROs in the PUF.

By analyzing the sleep path aging degradation of the LUTs in sleep mode we see that P3 does not have an inverted channel. The lateral electric field or $|V_{ds}|$ is also approximately Vdd. This signifies complete recovery for P3. N2 and N3 are under inversion ($|V_{gs}|$ is high) with negligible $|V_{ds}|$ thus, undergoing complete degradation of PBTI. Neglecting PBTI for higher technology node like 90nm we conclude that the sleep path will not show much degradation in the proposed modification if the LUT structure is PT based. Detailed comparison of conventional and proposed PT structure based RO aging is shown in table I. We can see that the conventional RO has only two PMOS recovering in the oscillation path during sleep mode. On the contrary, the proposed RO has eight PMOS recovering which is four times the conventional one.

B. Proposed RO with T-gate based LUT structure

In T-gate LUT structure (Figure 4), each of pull-up and pull-down paths are comprised of both NMOS and PMOS transistors. Thus, during sleep mode even if we compensate degradation of NBTI along the pull-up path (P1, P3) of oscillation half, the pull-down path (P2) undergoes NBTI (shown in Figure 6). So, with our proposed configuration PMOS transistors P2, P6 and P5 always age during sleep mode. Thus, we expect that aging degradation improvement for the T-gate structure RO PUF will be less than that of the PT structure RO PUF using our proposed design.

The next issue is whether the proposed methodology will help with improving the reliability of RO built in T-gate structure. As we have discussed before in section II-C reliability is unaffected as long as the ROs comprising the RO PUF age in a similar fashion (Figure 1a). In our proposed method for T-gate LUTs, if we compare two ROs undergoing degradation, we see that all the PMOS transistors in the pull-up (upper) oscillation path are under complete recovery while the NMOS transistors are under complete PBTI degradation. In the pull-down (lower) oscillation path, all the NMOS transistors are

Table II: Comparison table of conventional and proposed RO aging with T-gate based structure.

Types of aging	Conventional RO (5stage)			Proposed RO (5stage)	
	Osc	Sleep		Osc	Sleep
	All LUTs	LUT1 (orLUT3)	LUT2 (orLUT4)	All LUTs	All LUTs
HCI	P1,N1, P2,N2, P4,N4, P6,N6	—	—	P1,N1, P2,N2, P4,N4, P6,N6	—
NBTI	P3,N3	P2,P6, P3	P1,P4, P3	P3,N3	P2,P6, P5
PBTI	—	N2,N6, N3	N1,N4, N3	—	N2,N6, N5
recovery	P5,N5	P1,N1, P4,N4, P5,N5	P2,N2, P5,N5, P6,N6	P5,N5	P1,N1, P4,N4, P3,N3
Inference	4 osc. path PMOS recover in sleep mode			8 osc. path PMOS recover in sleep mode	

Table III: Simulation results: Reliability.

Simulation Results	Reliability		
	Conventional	Proposed	% improvement
T-gate LUT	$\mu=2.90\%$ $\sigma=.99$	$\mu=2.21\%$ $\sigma=0.83$	23.7%
PT LUT	$\mu=3\%$ $\sigma=1.12$	$\mu=2.15\%$ $\sigma=0.93$	28.3%

under complete recovery whereas the PMOS transistors get degraded due to NBTI. Though there is aging degradation, there still exists a homogeneity as all the ROs age similarly. For sleep path degradation, we see that the lower T-gate PMOS transistors P6 and P5 undergo NBTI continuously and get degraded during sleep mode. Thus, in contrary to the PT based LUT structure, the T-gate based structure should undergo substantial degradation in the sleep path for higher technology nodes like 90 nm. Note however that since the RO PUF signature is generated from the oscillation path, it should not be impacted by aging in the sleep path.

V. SIMULATION AND SILICON MEASUREMENT RESULTS

In this section, we analyze aging and RO PUF reliability through simulations and silicon demonstrations.

A. Simulation Results

A set of 50 RO PUF instances are simulated in Hspice using Monte Carlo and MOSRA aging degradation tools. PTM 90 nm model card is used as the technology node, which is analogous to the Spartan 3A FPGAs in our experiment. In Hspice, the ROs are modeled using LUT based FPGA architecture as shown in Figure 4. Both T-gate and PT based LUT structures are simulated with every RO PUF consisting of 128 ROs generating a 64-bit response (frequency of RO1 is compared with RO65 and so on). The comparison time is 10 μ s and the ROs are aged using MOSRA degradation tool for an accelerated aging time of 1 year. In practice, PUFs are used for a very small time in chips. For authentication purposes, a PUF may be used only for a few times throughout the chip lifetime. Whereas, for key generation purposes the PUF is only used when the system calls for a key to run any cryptographic algorithm. During aging, we model the RO PUF to be in oscillation for 10% of lifetime (activation time) and for the rest of the time it is kept in sleep. In real scenario, the PUF may be used for a much less amount

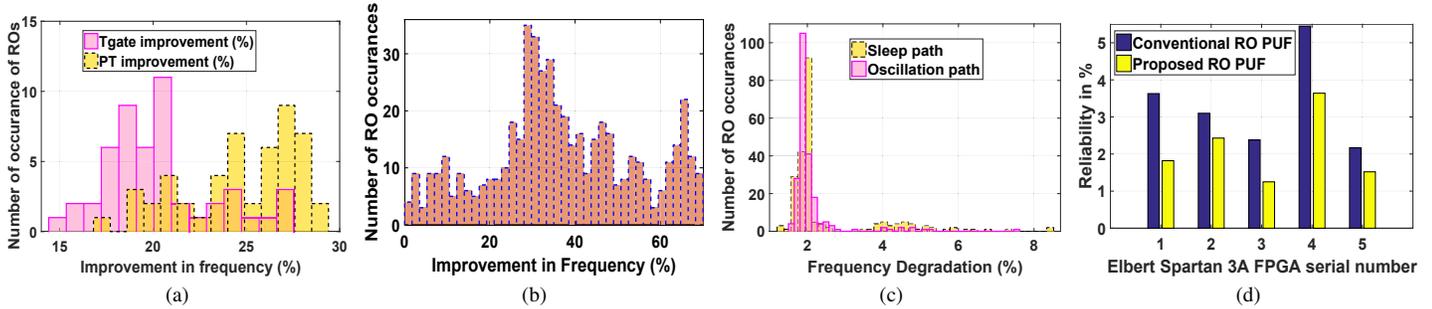


Figure 7: (a) Simulation results showing % improvement in frequency degradation $[(deg_{unmod}-deg_{mod})*100/deg_{unmod}]$ of proposed RO PUF over conventional design for T-gate and PT LUT architecture. The aging time period is 1 year with 10% activity of the PUF (b) Silicon results showing percentage improvement in frequency degradation for proposed FPGA RO PUF compared to conventional one. The aging time period is approximately 3 months of in-field aging with a PUF activity of 10% (c) Silicon results of the frequency degradation (%) along sleep and oscillation path for proposed FPGA RO PUF with 3 months of in-field aging and 10% PUF activity (d) Silicon results of Intra-Hamming Distance (reliability in %) of conventional RO PUF and proposed RO PUF with 3 months of in-field aging and 10% PUF activity

of time. Figure 7a shows an average frequency degradation improvement of 20.34% and 24.7% (comparing conventional RO PUF to proposed implementation) for T-gate structure and PT based structure respectively. As expected, the proposed implementation (PT version) experiences larger improvement since it has four times as many PMOS recovering as its conventional counterpart. In contrast, the T-gate version only has twice as many PMOS recovering (see tables I in section IV). The reliability for the RO PUF is also calculated by comparing PUF responses before and after aging. An average improvement of 23.7% and 28.3% in reliability are observed for T-gate and PT structure respectively. The reliability improvement figures are also provided in table III.

B. Measurement Results

Silicon measurement results are calculated with twelve Elbert V2 Spartan 3A FPGA boards [18]. Xilinx Spartan 3A boards belong to 90nm technology nodes [19]. The experiment was divided into two parts.

1) Experiment 1

In our first experiment, two FPGA boards are programmed with the proposed modified RO PUF program. Both the boards are aged with an applied voltage of 1.45 V (nominal operating voltage is 1.25V) at a temperature of 100°C with a thermostream [20] for 24 hours. An accelerated aging in the above-mentioned conditions corresponds to approximately 3 months of in-field aging as discussed in [21]. All measurements of both initial data as well as data after aging are taken at nominal operating voltage of 1.25 V and room temperature (around 27°C). Percentage degradation in frequency of sleep and oscillation path is shown in Figure 7c which indicates that the sleep path undergoes similar degradation as that of the oscillation path. Referring to section IV-A we can conclude that the design architecture of the specific Spartan 3A FPGA board is probably analogous to PT based LUTs. We have previously discussed that PT LUT structure will have negligible degradation along sleep path since PBTI is negligible for 90 nm technology node.

2) Experiment 2

In the second part of experiment, a set of five Elbert V2 Spartan 3A FPGA boards are prepared with the conventional

RO PUF design. After taking initial data, the boards are aged each for 24 hours using same aging conditions as in prior experiment. After aging, the frequency measurements are repeated and PUF response is obtained. The degradation of frequency is calculated and the reliability of all the boards before and after aging is computed using simple Matlab scripts. For each board, a total of 110 ROs are laid out. We randomly choose two ROs from these to formulate a 55-bit response. All the measurements are taken at nominal operating voltage of 1.25 V and 27°C. Similar to our simulation assumption, we have kept the RO PUF idle for 90% of aging time and oscillating for the rest of the time.

In the next phase of experiment, we programmed another set of five Spartan 3A FPGA boards with the modified RO PUF as explained in section IV. The boards are aged similarly as described previously for conventional RO PUFs. The initial and aged measurement data are also taken in similar conditions. The frequency degradation data from conventional and modified RO PUFs are compared to calculate the improvement in frequency degradation of the latter compared to the former. The improvement across all the 5 set of FPGAs has been shown in Figure 7b which presents a wide improvement range from 0 to 70% in frequency degradation with a mean of approximately 37%. A comparison between the reliability of the conventional RO PUF and the modified RO PUF is shown in Figure 7d. On average, there is an improvement of 37.4% in reliability with aging in the modified RO PUF. The measurement results confirm the reliability improvement in simulation results shown previously. Such improvements can dramatically lower the costs associated with PUF error correction, which exponentially grows with number of unreliable bit flips. For example, considering the heterogeneous error rate model proposed in [9], our proposed RO PUF will need much fewer response bits than conventional RO PUFs to generate a key of the same length. Moreover, an ECC block of smaller size will also enhance the security of PUF based encryption schemes, since ECC could be manipulated by attackers to compromise PUF constructions [22].

VI. CONCLUSION AND FUTURE WORK

In this paper, we propose an aging resilient PUF design for FPGA which can compensate for reliability issues caused by aging. Our results show an average improvement of 37.4% in reliability and 37% in frequency degradation in Spartan 3A FPGAs. The results are substantiated with proper aging analysis for both PT and T-gate based LUTs. It will be interesting to observe the aging effects on the PUF for smaller activation time with varied aging duration. Due to lack of time and available resources, we were unable to pursue the former. Nevertheless, we list them as a major objective in our future work. Our experiments of sleep and oscillation path aging degradation show characteristics of PT based LUT architecture in 90nm FPGAs. Due to lack of proprietary information of FPGA architecture, we were unable to completely confirm this. Thus, we plan to reverse engineer FPGA boards in future to deduce this missing information. In addition, this paper focused on reliability and degradation improvement of 90nm technology nodes and above. In future, we plan to extend our analysis and proposed approach for sub 90nm technology nodes where effect of HCI and PBTI are more dominant.

REFERENCES

- [1] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*.
- [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*.
- [3] A. Maiti and P. Schaumont, "The impact of aging on a physical unclonable function," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*.
- [4] S. Morozov, A. Maiti, and P. Schaumont, *An Analysis of Delay Based PUF Implementations on FPGA*, 2010, pp. 382–387.
- [5] P. M. B. Rao, A. Amouri, S. Kiamehr, and M. B. Tahoori, "Altering lut configuration for wear-out mitigation of fpga-mapped designs," in *2013 23rd International Conference on Field programmable Logic and Applications*.
- [6] R. Maes and V. van der Leest, "Countering the effects of silicon aging on sram pufs," in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, May 2014, pp. 148–153.
- [7] M. T. Rahman, F. Rahman, D. Forte, and M. Tehranipoor, "An aging-resistant ro-puf for reliable key generation," *IEEE Transactions on Emerging Topics in Computing*.
- [8] Y. Sato, M. Monden, Y. Miyake, and S. Kajihara, "Reduction of nbt-induced degradation on ring oscillators in fpga," in *2014 IEEE 20th Pacific Rim International Symposium on Dependable Computing*, 2014.
- [9] R. Maes, *An Accurate Probabilistic Reliability Model for Silicon PUFs*, 2013.
- [10] X. Xu, W. Burleson, and D. E. Holcomb, "Using statistical models to improve the reliability of delay-based pufs," in *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, July 2016, pp. 547–552.
- [11] X. Xu, A. Rahmati, D. E. Holcomb, K. Fu, and W. Burleson, "Reliable physical unclonable functions using data retention voltage of sram cells," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 6, pp. 903–914, June 2015.
- [12] X. Xu and D. Holcomb, "A clockless sequential puf with autonomous majority voting," in *Proceedings of the 26th Edition on Great Lakes Symposium on VLSI*, ser. GLSVLSI '16.
- [13] S. Kiamehr, A. Amouri, and M. B. Tahoori, "Investigation of nbt and pbt induced aging in different lut implementations," in *2011 International Conference on Field-Programmable Technology*.
- [14] S. Kiamehr, F. Firouzi, and M. B. Tahoori, "Aging-aware timing analysis considering combined effects of nbt and pbt," in *International Symposium on Quality Electronic Design (ISQED)*.
- [15] C. Chiasson and V. Betz, "Should fpgas abandon the pass-gate?" in *2013 23rd International Conference on Field programmable Logic and Applications*.
- [16] J. Keane, W. Zhang, and C. H. Kim, "An array-based odometer system for statistically significant circuit aging characterization," *IEEE Journal of Solid-State Circuits*.
- [17] X. Wang, S. hwan Song, A. Paul, and C. H. Kim, "Fast characterization of pbt and nbt induced frequency shifts under a realistic recovery bias using a ring oscillator based circuit," in *2014 IEEE International Reliability Physics Symposium*, 2014.
- [18] [Online]. Available: <https://numato.com/elbert-v2-spartan-3a-fpga-development-board/>
- [19] Xilinx, "Spartan-3a fpga family: Data sheet." [Online]. Available: https://www.xilinx.com/support/documentation/data_sheets/ds529.pdf
- [20] [Online]. Available: http://www.axiomtest.com/Temperature-and-Humidity/Temperature-and-Humidity-Chambers-_and_Systems/Tempronic/ATS_605/ThermoStream-Thermal-Inducing-System,-_20-to-+225C/
- [21] R. Maes, V. Rozic, I. Verbauwhe, P. Koeberl, E. van der Sluis, and V. van der Leest, "Experimental evaluation of physically unclonable functions in 65 nm cmos," in *2012 Proceedings of the ESSCIRC (ESSCIRC)*.
- [22] J. Delvaux and I. Verbauwhe, "Key-recovery attacks on various ro puf constructions via helper data manipulation," in *2014 Design, Automation Test in Europe Conference Exhibition (DATE)*.