ARO-PUF: An Aging-Resistant Ring Oscillator PUF Design

Md. Tauhidur Rahman[1], Domenic Forte[1], Jim Fahrny[2], and Mohammad Tehranipoor[1]

[1]ECE Dept., University of Connecticut
{tauhid, forte, tehrani}@engr.uconn.edu

[2]Comcast
jim_fahrny@comcast.com

Abstract—**Physically Unclonable Functions (PUFs) have emerged as a security block with the potential to generate chip-specific identifiers and cryptographic keys. However it has been shown that the stability of these identifiers and keys is heavily impacted by aging and environmental variations. Previous techniques have mostly focused on improving PUF robustness against supply noise and temperature but aging has been largely neglected. In this paper, we propose a new aging resistant design for the popular ring-oscillator (RO)-PUF. Simulation results demonstrate that our aging resistant RO-PUF (called ARO-PUF) can produce unique, random, and more reliable keys. Only 7.7% bits get flipped on average over 10 years operation period for an ARO-PUF due to aging where the value is 32% for a conventional RO-PUF. The ARO-PUF shows an average inter-chip HD of 49.67% (close to ideal value 50%) and better than the conventional RO-PUF ($\sim 45\%$). With lower error, ARO-PUF offers $\sim 24X$ area reduction for a 128-bit key because of reduced ECC complexity and smaller PUF footprint.**

Keywords—PUF, reliable RO-based PUF, reliable PUF, robust PUF, aging resistant PUF, PUF reliability.

I. Introduction

In the effort to design secure systems, Physical Unclonable Functions (PUFs) have emerged as a potential security block [1-4] as they can generate volatile secret keys for a system. PUF is an integrated circuit that generates secret keys by exploiting the inherent physical variations of devices. PUFs provide a high level of protection in security block. It offers strong volatile key storage to make the system tamper-resistant. Functionally, a PUF maps a challenge, input to the PUF, to responses, PUF output. A PUF exploits the physical characteristics of silicon and provides an alternative to conventional digital signature stored in non-volatile memory. It uses the physical properties of each device to generate a chip-specific fingerprint or key. Identical PUFs with the same manufacturing process provide a different set of data because of small variations between each device. PUF can be used extensively in security applications such as IC identification/authentication, hardware metering, certified execution, and key generation for encryption [4-9]. Several PUFs have been proposed over the past decade, such as Arbiter PUF [2], ring-oscillator-based PUF (RO-PUF) [4], SRAM-based PUF [13], Butterfly PUF [14], etc. Among them, the RO-PUF is considered more reliable under a wide range of temperatures and it has been more widely accepted because it is less complex and easier to fabricate [4, 17, 22].

In order to be useful in practical security applications, the fingerprint or key generated by the PUF should be reliable or stable (i.e., not change over time). For example, in cryptography, decrypting the original message will be impossible with wrong private/public keys. Authentication of devices, secure communication, etc. also suffer from complications due to PUF instability. It is relatively well known that aging and environmental variations lead to performance degradation and lower reliability in ICs [10-12, 23-24, 32]. Similarly PUFs, hence, the keys they generate will therefore also be rendered less reliable by such variations. Run-time aging effects such as negative bias temperature instability (NBTI), hot carrier injection (HCI), oxide breakdown, and electromigration (EM) are the most critical causes of continuous performance and reliability degradation [10]. Threshold voltage (V_T), channel length, timing, etc. are the critical parameters that decide the performance of a chip. NBTI can degrade V_T of a transistor by 10-15% in the first year depending on technology and workload [23], which reduces drive current and hence circuit performance. During negative bias (pMOS is ON), pMOS experiences a constant degradation. However, partially recovery occurs when the stress is removed (pMOS is OFF). HCI is a function of switching activity and can accelerate degradation even further by shifting the threshold voltage of nMOS transistors over time [12]. While HCI mostly impacts the V_T of the nMOS, it may also degrade the drain current of both nMOS and pMOS [32]. The delay degradation due to NBTI and HCI follows the same trend as the V_T degradation. The severity of the degradation due to NBTI and HCI is dependent on workload, logic function, temperature, supply voltage, threshold voltage, technology and geometry [10, 21, 23-24, 32]. In general, low V_T transistors experience more degradation over time than high V_T transistors. Similarly, higher-supply voltage, V_{DD}, and higher-operating temperature expedite the delay degradation over time. Fundamentally, aging will *permanently* shift many critical parameters the PUF uses to generate its key and therefore is a significant concern to PUF reliability. Another issue for PUF reliability is temperature variation. Operating temperature affects the delay of a device by changing its mobility and threshold voltage [12]. As temperature increases, the threshold voltage decreases which leads to an increase in the drain saturation current. At the same time, it decreases the mobility of the MOSFET, which causes a decrease in the drain saturation current. However, the mobility degradation dominates, and consequently, the delay of the device decreases. Similar to aging, these temperature-induced changes to delay will also create noise in the PUF's key. However, unlike aging, the effects can be reversed by returning the device to its nominal operating temperature. Like temperature, power supply noise also affects the delay, because of deviation from nominal V_{DD}, of logic gates and hence the reliability of an IC. The power supply delivery network and parasitic impedance of packages result in V_{DD} fluctuation and impact the IC performance. Like aging and temperature variation, V_{DD} fluctuation is also liable to impact the reliability of a PUF. Unlike aging the supply noise's impact is temporary, i.e., when V_{DD} is back to its nominal value, the PUF operates more reliably. Researchers have proposed several techniques to improve the reliability of a PUF [16-19, 21, 23, 24, 28-29]. For example, error correcting codes (ECC) have been used to fix up to a certain number of erroneous bits in the PUF key. For example, it has been reported in [15] that the index-based syndrome followed by a 3x repetition code and BCH [30] code can lower the RO-PUF error rate below 1 ppm under severe operating conditions. Unfortunately, ECC has high VLSI overheads that increase quadratically with the number of errors. To reduce these costs, several techniques have been proposed to combat environmental variations. A circuit technique has been proposed to improve the reliability and uniqueness in [16]. The authors showed that sub-threshold region of operation and forward body bias drastically improve the PUF uniqueness and reliability. They also showed to preserve better reliability; a PUF should maintain a nominal operating voltage or a well-below threshold voltage. Temperature-Aware Cooperative (TAC) was proposed in [17] to improve the reliability under different operating temperatures on RO-PUF. In [18], the authors found an operating point where temperature effects have been minimized. Aging effects on the reliability of a PUF was studied in [20]. The authors showed how changes to the intra-chip hamming distance (HD) due to aging causes error during authentication.

Although the impact of aging on RO-PUF has been studied, little work has been done on developing PUFs that are less sensitive to aging. Unlike temperature (supply noise) analysis where high/low temperatures (supply noise) can be applied very quickly to evaluate each PUF, such luxury does not exist when analyzing aging. Aging analysis is extremely slow and expensive. Thus, there is a need to design aging-resistant PUFs such that there will be no need (and no extra cost) to aging analysis during production test of the device and the PUF. In this work, we propose an aging-resistant RO-PUF (ARO-PUF) that generates reliable volatile digital secret keys in security applications for a long time at different operating conditions. To our knowledge, the proposed ARO-PUF is the first aging resistant RO-PUF. By increasing resistance to aging, our PUF requires much lower ECC overheads, thereby making it more practical in a wider range of systems. The proposed PUF is also less sensitive to temperature variations. We analyze our structure at different operating conditions and compare with the conventional RO-PUF. Simulation results, based on a 90 *nm* technology, show that the ARO-PUF generates more stable output,$\sim 4x$ than an RO-PUF, over long term use at different operating conditions. The simulation results also show that the ARO-PUF is less sensitive to temperature than the conventional RO-PUF with similar sensitivity to V_{DD} variations. ARO-PUF is $\sim 18\%$ less sensitive to temperature than an RO-PUF. We also compare the area overhead contributed by required ROs and ECC scheme between RO-PUF and ARO-PUF. Because of less sensitivity to aging and temperature the system with ARO-PUF requires less ECC encoding and decoding complexity and less amount of bits to generate a fixed-length key. The result shows that a system with ARO-PUF requires $\sim 24X$ less area overhead than the same system with a conventional RO-PUF.

The rest of the paper is organized as follows: In Section II, we discuss the background of conventional RO-PUF, quality factors of PUFs, and RO-PUF reliability. In Section III, we discuss our proposed ARO-PUF design and how it improves PUF quality factors. The experimental results and analyses are shown in Section IV. We conclude the paper in Section V. In this paper, we use the terms conventional RO-PUF and RO-PUF equivalently.

II. Preliminaries

A. RO-PUF

Figure 1 presents a conventional RO-PUF which consists of N identically laid out ROs, two counters, a comparator, and two N-bit multiplexers. Each of the identical ROs oscillate with unique frequency because of the device's manufacturing process variations. The input to the PUF (challenge) is applied to both MUXs so that one pair of ROs is selected. The counters count the number of oscillations for a fixed time interval known as comparison time. After comparison time, the outputs of the counters are compared to generate a response. The output of the comparator is set to $'0'$ or $'1'$ based on which oscillator from the selected RO pair is faster.

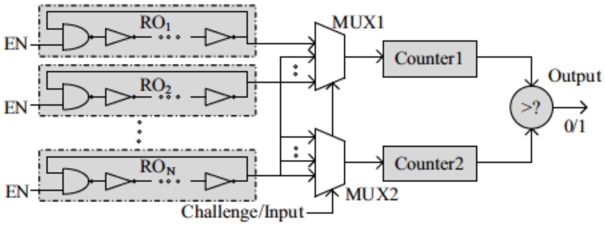


Figure 1: Conventional RO-PUF.

B. PUF Quality Metrics

Reliability, *uniqueness*, and *randomness* are three major metrics used commonly to assess the quality of a PUF. Uniqueness measures how a single PUF is differentiated from other PUFs. The average hamming distance (HD) between PUFs in different chips to the same challenges is the most popular way to measure uniqueness. Ideally, inter-chip HD should be 50%. The *Reliability* of a PUF determines how efficiently a PUF can generate the same response at different operating conditions and over time for a given challenge. Intra-chip HD is an effective metric to estimate the reliability of a PUF. For an ideal PUF, the intra-chip HD should be zero. *Randomness* measures the unpredictability of the response of a PUF and it determines whether the PUF is biased or not. One expects different responses for different challenges in a PUF. For a good PUF design, changing one bit in a challenge should alter nearly half of the response. Randomness can be measured using various practical approaches based on statistical tests, complexity, and transformations [25].

C. RO-PUF Reliability

An applied challenge selects a pair from a group of ROs, and the frequency of that pair is compared to generate a one-bit response. However, because of environmental and aging variations not every pair can generate a reliable bit. The temperature, supply noise, and aging have significant effects on the frequency of each set of ROs. The speed degradation of an RO depends largely on both negative-bias temperature instability (NBTI) and hot carrier injection (HCI). The frequency degradation of an RO due to NBTI and HCI has been modeled in [32]. Zero-signal probability is the reason behind NBTI and shows a wide range of variations depending on topology, operating condition, and workload. The input signal of each inverter in an RO could experience a DC stress, of which half inverters experience a constant $'0'$ and other halves receive $'1'$. NBTI degrades those gates with $'0'$ inputs by increasing the device threshold voltage and reducing the carrier mobility as a function of stress condition and time. It is preferred if all inverters on ROs receive $'1'$ so they experience minimum amount of aging. If the input of ROs' inverters are not assigned properly, the rate of frequency degradation in different pMOS transistors might be different and hence the rate of frequency increase or decrease in the ROs might be different causing the response to flip. HCI, because of switching activity, degrades the circuit with aging under normal operating conditions. Unlike NBTI, HCI depends on RO frequency. Due to different degradation rates, the RO with higher frequency can become slower than the other in a pair. This condition causes a bit flip and makes the PUF unreliable when same pair is selected by the applied challenge and their relative positions remain unchanged. To increase the robustness of a PUF under environmental variations and the

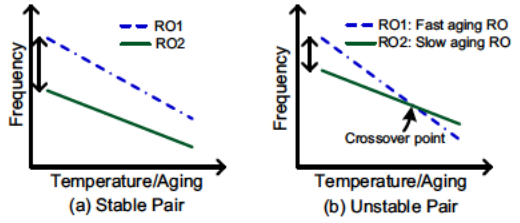


Figure 2: Reliability issue of RO-PUF.

device's aging, one can choose only the pairs with large-base frequency difference. Figure 2 illustrates how the reliability of an RO-PUF is affected by environmental variations and aging. In an RO-PUF, one can compare the frequency of ROs of a pair selected by given challenge. Suppose a pair has two ROs, RO1 and RO2, selected by MUX1 and MUX2, respectively. The pair will always generate a reliable bit if the frequency of the RO1 is always higher than the frequency of RO2, regardless of environmental variations and device aging. This pair is known as a stable or good pair (Figure 2(a)). Figure 2(b) shows how a bit could flip beyond a certain operating condition or after a certain amount of aging of the device. If the inverters of RO1 experience more logic $'0'$ than the inverters of RO2, the bit flip could occur before the target chip lifetime (i.e., time we expect to use the device containing the PUF before it fails). Before considering environmental variations and aging, RO1 is faster than RO2. But after a device reaches a certain age or experiences a different operating condition, the RO1 could become slower than the RO2 and flip the bit. We refer to this point as the crossover point. The potential crossover in frequencies makes it difficult to obtain reliable bits in an RO-PUF under different operating conditions over a long period of time. The frequency degradation of an RO due to aging is $\sim 14\%$ over 10 years period of time. The quick V_T degradation due to aging will force some bits in the PUF output to flip. So, the components in an RO-PUF should be designed in such a way that it becomes less sensitive to aging and hence the PUF generates reliable keys. The rate of decreasing/increasing frequency, i.e. the slope of the straight lines (Figure 2), is important. We consider it as the guide to design a reliable ring-oscillator-based PUF over a target chip lifetime. Note that temperature creates a temporary change in ROs' speed but aging mechanisms create a permanent change in the speed of ROs in an RO-PUF. Motivated by this, in the next section, we discuss our proposed ARO-PUF, which is less sensitive to environment variations and to a device's aging.

III. Overview of the Proposed ARO-PUF

A. Architecture and Operation

The architecture of the ARO-PUF is the same as the RO-PUF (see Figure 1), except we replace the conventional RO's with an aging resistant design. Because of its special characteristics, we call it aging-resistant RO (ARO). The digital key extraction from an ARO-PUF is same as an RO-PUF. Like the RO-PUF, a pair of AROs are selected by an applied challenge and compared to generate a digital key in the ARO-PUF. Figure 3(a) illustrates the proposed aging-resistant RO. NBTI in pMOS transistors is a critical issue for the lifetime of a device. The degradation depends on threshold voltage, the input stress (DC or AC), size, load, operating temperature, supply voltage, etc. A DC stress means that the gate receives a constant input value of $'0'$ at all times, while an AC stress indicates that the gate input changes between $'0'$ and $'1'$. When a pMOS transistor receives a $'1'$, it actually recovers parts of the NBTI-induced degradation. HCI effect, however, is due to switching between $'0'$ and $'1'$ on an nMOS transistor. Note that research and silicon data have shown that NBTI dominates HCI in terms of total degradation in the field [11-12, 21, 23, 24, 28-29, 32].

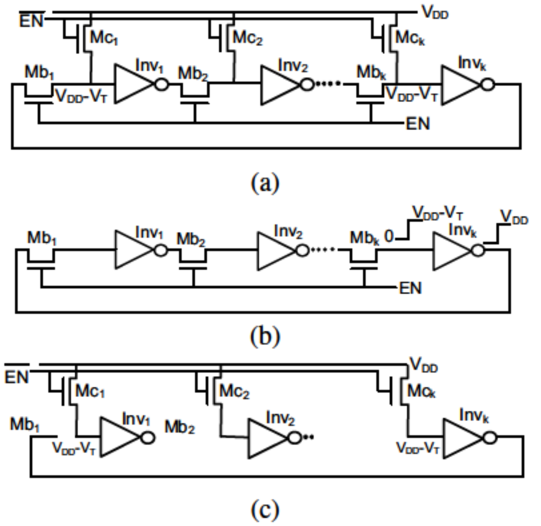
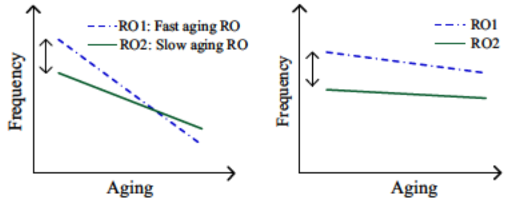


Figure 3: (a) Aging-Resistant RO (ARO), (b) Oscillatory mode, and (c) Non-oscillatory mode.

Different studies have reported that there is a strong correlation between the NBTI and zero-signal probability (DC stress) [21]. If the input of a pMOS transistor experiences $'0'$ for longer period of time, the frequency degradation becomes higher due to NBTI. One easy solution to addressing the aging problem in an RO is to use sleep transistor, however, simulation results show that the frequency degradation rate is $\sim 7\%$ when sleep transistors are used, since pMOS sleep transistor experiences static NBTI that enhances the degradation due to aging [26]. There have been a significant amount of work in literature to combat against NBTI and HCI [21, 23-24, 28-29] but none intended for RO-PUF.

In general, a PUF in a chip is used only for a short period of time; we call it *PUF activation time*. For example, if a PUF is used only for IC identification, the PUF might only be used just a few times in an IC's lifetime operation to help authenticate the IC against counterfeiting. As another example, a PUF used for on-chip key generation is only used when the system calls for a key to run a cryptography algorithm. An activation of 10% means that during chip lifetime, PUF is ON about 10% of the time. Note that, in practice, the expected PUF activation time will be much smaller than the total chip lifetime. In all cases, when the conventional RO-PUF is put in the oscillating (AC stress) or non-oscillating mode (DC stress) when it is not used, it will experience significant amount of aging, see Section IV. The ARO-PUF addresses this challenging problem by mitigating NBTI and HCI effects when PUF is not used.

The ARO, shown in Figure 3(a), significantly reduces aging in the RO inverters. In oscillatory mode, when the PUF is used, the EN signal remains active and keeps the M_bs ON and M_cs OFF. Hence the ARO acts like an RO, as shown in Figure 3(b). The frequency decreases when extra nMOS transistors are added into the ARO, as those extra nMOS transistors add additional delay and capacitive load. But it can be increased easily by reducing the number of stages (k). The frequency of each ARO remains unique because of process variations. In non-oscillating mode (see Figure 3(c)), when the PUF is not used (EN=$'0'$), the M_bs are kept OFF to stop oscillation and M_cs are turned ON to force the floating signals in each inverter's input to $V_{DD} - V_T$ to mitigate the HCI and NBTI. In an ARO, the nMOS transistors between two inverters, M_bs, could be replaced by transmission gates.



(a) ROs with different degradation rates

(b) Stable ROs with negligible degradation

Figure 4: Aging aware concept for ROs.

To eliminate the floating signal values, in input to the inverters, M_cs are used to charge the floating points. Transistor M_c forces the floating signal to $V_{DD} - V_T$ so that the pMOS transistor in inverters does not experience '0' in the non-oscillating mode. Hence the pMOS in the inverters will not age when in non-oscillating mode. An nMOS transistor has been used instead of a pMOS transistor between power supply and gate inputs to avoid NBTI effect on them. By restricting the number of oscillations and the time that a logic 0 appears at the PMOS inputs, our design can significantly mitigate the HCI and NBTI aging effects in the PUF and therefore produce more reliable outputs over time.

B. Reliability Enhancement

Based on the structure of the ARO it can be concluded that the degradation speed rate of frequency is much lower than a conventional RO, as the ARO is less sensitive to aging. The question then is how significantly the ARO improves the ARO-PUF's robustness against aging. Figure 2 depicts how a bit could be flipped because of device's aging or environmental variations. Figure 4 shows how the reliability in our technique improves significantly. Because an ARO is much less sensitive to aging, a pair in an ARO-PUF takes more time to reach the crossover point than a conventional RO-PUF as the rate of frequency degradation improves by a significant margin. As a result, the ARO-PUF eliminates the need for aging analysis and thus requires engineers to only focus on the temperature/supply noise analysis (a well investigated subject in PUF domain). The ARO-PUF generates reliable signatures for a longer period of time compared to the conventional RO-PUF. The ARO is also less sensitive to temperature variations as device experiences $V_{DD} - V_T$ in non-oscillatory mode and improves V_T degradation more than the conventional RO. Consequently the rate of changing frequency becomes slower than the conventional regular RO. As a result, ARO-PUF works reliably over different conditions and longer operating ranges. RO selection in a pair and frequency degradation rate determine the reliability of a PUF. Because of impossible zero frequency degradation, the initial frequency gap of two ROs in a pair should be as large as possible to allow some amount of frequency degradation to obtain reliable keys. The acceptable frequency degradation of an RO in a pair depends on both the initial frequency gap at normal operating temperature and the frequency degradation of each RO in that pair.

IV. Simulation Results and Analysis

Both conventional RO-PUF and ARO-PUF are implemented in HSPICE [27] with the Monte Carlo simulation for 100 chip instances in 90nm technology node. The process variation for 100 different chips are generated with 10% intra-die, 10% inter-die, and 3 sigma variations for L (channel length of transistor), V_T, and Tox (oxide thickness). A total of 64 AROs are used to implement ARO-PUF, and each ARO has 41 inverting stages, 41 M_bs, and 41 M_cs. The RO-PUF is implemented with 64 conventional ROs where each RO also has 41 inverting stages. A 32-bit response is generated from each PUF. Both NBTI and HCI have been accounted for in HSPICE MOSRA [27] to determine the reliability of each PUF after 10 years. Minimum size inverters (Wn=0.12u and Wp=2.5*Wn) are used in both PUFs. The gate sizes for M_b and M_c are 0.12u and 0.24u, respectively. Low V_T transistors are used during simulation. The frequency degradation also depends on the activation time, the time in which PUF is in oscillatory mode. Lower activation time ensures higher reliability due to less oscillation. The activation times are selected as 23%, arbitrarily. Other activation times are considered in Table I to analyze their impact on ARO-PUF. Both AC and DC stresses have been applied during simulation.

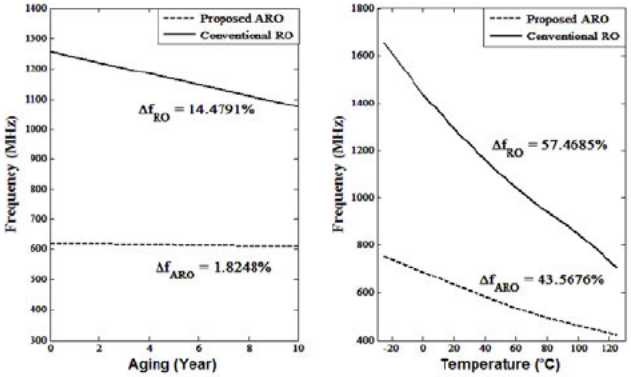


Figure 5: Frequency degradation rate (Δf$\equiv \frac{f_{initial} - f_{final}}{f_{initial}} * 100\%$) of RO and ARO under (a) Aging and (b) Temperature variation.

Impact of Aging: Figure 5(a) shows the frequency degradation rate(Δf) for both conventional RO and ARO under aging (NBTI and HCI) with the above specified simulation setup. The frequency degradation in 10 years is about 1.8% in our proposed ARO whereas it is about 14.4% for a conventional RO. The degradation rate can be further reduced by adjusting the parameters of ARO such as W_n, and gate sizes of M_b and M_c. Figure 6 shows distribution of the errors across both PUF populations after 10 years. Error measures the number of bits flipped during different measurements. The signature has been measured for the first time when the PUF is ready to be used and again 10 years later. The HD between two measurements indicates the total number of errors generated by a PUF. Reliability analysis has been done for 100 chip instances at nominal temperature and operating voltage (25°C, 1.2V). Figure 6(a) shows that the number of total bits flipped in the ARO-PUF is 2.5 on average and 3.8 maximum among

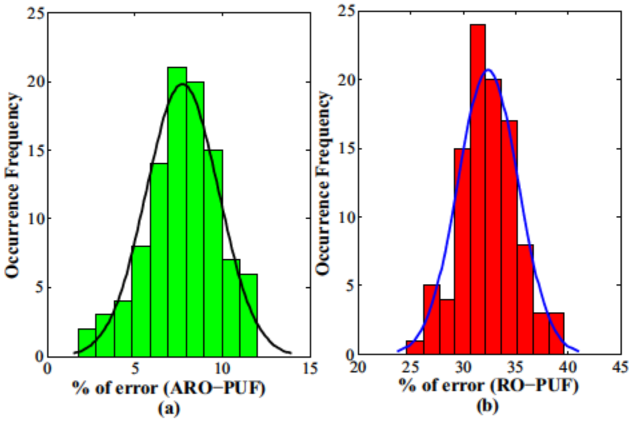


Figure 6: % of error after 10 years of operation for (a) ARO-PUF and (b) RO-PUF under same stress condition.

Table I: Activation time and vs. error

Activation Time	RO Frequency Degradation	Bits Error	
		Average	Maximum
23%	1.83%	7.81%	11.88%
10%	1.61%	7.03%	11.56%
5%	1.54%	7.03%	11.54%
1%	1.34%	7.01%	11.32%

a 32-bit response. The same values for the conventional RO-PUF are 10.35 and 13.15, respectively, as seen in Figure 6(b). After 10 years, the average error in response of the ARO-PUF is 7.73%, whereas it is 32.41% in the conventional RO-PUF. The results show a 75.84% improvement in reliability with the ARO-PUF because the ARO is less sensitive to aging. As mentioned earlier, the frequency degradation also depends on the activation time of a PUF. Practically, the activation time of a PUF in security applications should be much less than 23% used earlier. Lower activation time further reduces the error rate for the ARO-PUF, as the ARO experiences less frequency degradation. Table I shows the average frequency degradation and percent of bit error for different activation times. The results show that frequency degradation, hence error, decreases as activation time decreases. On the other hand, a conventional RO-PUF is not affected by the activation time as RO's degradation does not depend on activation time as much; with the same gate size the frequency degradation remains around 14%. These results clearly indicate that ARO provides a much reliable circuit against aging mechanisms when used for security applications in the field.

Temperature and V_{DD} Sensitivity of ARO-PUF: An RO-PUF is highly sensitive to temperature variation. The ARO is less sensitive to temperature variation because the drain current of the transistors along its oscillating path is less sensitive to temperature than the conventional RO. The reduction of V_T, because of increasing temperature, results in the increase of drain current. Because of $V_{DD} - V_T$, ARO experiences less amount of increase in current and hence reduces the rate of V_T shift with temperature. Figure 5(b) shows that the frequency degradation rate of our proposed ARO is less than a conventional RO under temperature variations. Simulation results show that the frequency degrades almost 43% if temperature is changed from $-25°$C to 150°C for our proposed ARO, whereas it is almost 57.4% for a conventional RO. The degradation rate affects the reliability under temperature variations and the device's aging. The average percentage of intra-chip HD at different temperatures is shown in Table II. The table shows the comparison in reliability between the ARO-PUF and the conventional RO-PUF under temperature variations. The response is measured at $-25°$, 0°, 25°, 50°, 75°, 100°, and 125° Celsius for both PUFs. At room temperature, the accuracy of the ARO-PUF is 1.24 times better than an RO-PUF. The average percentage of intra-chip HD at different temperatures is shown in Figure 7 for both PUFs. Our proposed ARO-PUF has a better intra-chip HD profile because it is less sensitive to temperature than the conventional RO-PUF. The average percentage of intra-chip HD for the ARO-PUF is 0.67 with a maximum of 1.5625. The average and maximum values for a conventional RO-PUF are 0.86 and 2.6042, respectively. On the other hand, Table III shows that ARO-PUF has almost similar sensitivity to V_{DD} variation as RO-PUF.

Uniqueness of ARO-PUF: Figure 8(a) shows the uniqueness of our proposed ARO-PUF at normal operating temperature. The mean normalized HD is 0.4987. The uniqueness between our proposed ARO-PUF and conventional RO-PUF under different operating temperatures is compared in Figure 8(b). The inter-chip HD for both PUFs is measured at $-25°$, 0°, 25°, 50°, 75°, 100°, and 125° Celsius. Figure 8(b) shows that the inter-chip HD of our proposed ARO-PUF is very close to 0.5 under the wide temperature variations specified above, closer than the conventional RO-PUF because of the variations imposed by M_b and M_c. At the same time, ARO-PUF shows ($\sim 50\%$) inter-chip HD at different V_{DD}s; (48.32%), (49.32%), and (47.97%) for $1.08V$, $1.20V$, and $1.32V$ respectively. ARO-PUF shows better uniqueness because of more V_T and capacitive variations induced by the special purpose nMOSs, M_bs and M_cs, used in ARO.

Table II: % Intra-chip HD comparison at different temperatures

Temperature (°C)	% Intra-chip HD		% Improvement
	ARO-PUF	RO-PUF	
–25	0.92	1.14	19.30
00	0.72	0.83	13.25
25	0.46	0.57	19.29
50	0.57	0.70	18.57
75	0.70	0.87	19.54
100	0.73	0.91	19.78
125	0.81	0.96	15.63

Table III: % of Intra-chip HD at different V_{DD}s

V_{DD}	Average		Maximum	
	ARO-PUF	RO-PUF	ARO-PUF	RO-PUF
1.08	4.92%	5.15%	10.78%	9.20%
1.14	4.72%	4.91%	9.66%	9.18%
1.26	5.09%	5.52%	10.61%	9.73%
1.32	5.57%	5.85%	10.08%	10.27%

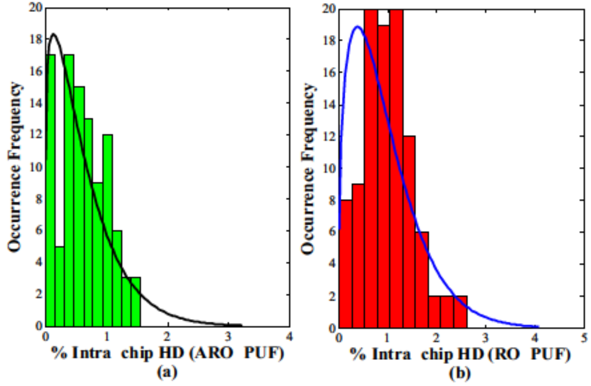


Figure 7: Improved reliability profile in ARO-PUF under temperature variations.

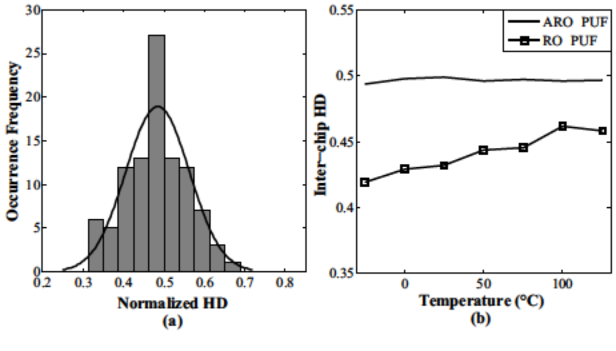


Figure 8: (a) Uniqueness in ARO-PUF at normal operating temperature and (b) Improved uniqueness in ARO-PUF at different temperatures.

Randomness of ARO-PUF: The randomness of both ARO-PUF and RO-PUF at different temperatures is reported in Table IV. The result implies that our proposed ARO-PUF shows better randomness than the conventional RO-PUF at all specified operating temperatures due to more random mismatches and better temperature profile. At normal operating temperature, the response of our proposed ARO-PUF possesses 55% '1'

Table IV: % of $'1'$ in response to all possible challenges at different temperatures

Temperature (°C)	% '1' in response		% Improvement
	ARO-PUF	RO-PUF	
−25	60	66	9.09
0	59	64	7.81
25	55	60	8.33
50	58	62	6.45
75	58	62	6.45
100	58	61	4.91
125	58	60	3.33

and 45% $'0'$ on average, which is close to the ideal value (50% $'1'$ and 50% $'0'$) and better than the conventional RO-PUF.

Table V: Area overhead comparison for 128-bit key

Blocks	ARO-PUF	RO-PUF	Reduction
Required ROs	510	16382	32x
Area for ROs	510*6.5*A_{nMOS}	16382*3.5*A_{nMOS}	17.3x
ECC Encoder	$\sim$ 3Kgates	$\sim$ 12 Kgates	$\sim 4x$
ECC Decoder	$\sim$ 20 Kgates	$\sim$ 75 Kgates	$\sim 3.75x$

A_{nMOS}: Area of nMOS with Wn=0.12u
$3.5 \equiv (Wn = 0.12u) + (Wp = 2.5 * Wn)$
$6.5 \equiv (Wn = 0.12u) + (Wp = 2.5 * Wn) + (W_{Mb} = Wn) + (W_{Mc} = 2 * Wn)$

Area Overhead: Table V shows the estimated area overhead comparison between ARO-PUF and RO-PUF for 128-bit key generation based on [30-31]. A system with the ARO-PUF requires a smaller PUF footprint. For example, to correct $\sim 7.9\%$ and $\sim 25\%$ errors for a 128-bit key generation, BCH requires 255 and 8191 bits respectively [30]. Though ARO consumes more area than a conventional RO, ARO-PUF saves $\sim 17x$ area because of smaller PUF footprint. At the same time, both BCH encoder and decoder required lower overhead (timing, power and area) since ARO-PUF has less errors than RO-PUF. Estimation shows that ARO-PUF offers $\sim 7x$ area reduction for BCH encoder and decoder. ARO-PUF offers more area efficient implementation for longer key size.

V. Conclusion

In this work, we have proposed the first aging-resistant RO-PUF design. The simulation results show that the proposed ARO-PUF ages significantly less compared to the conventional RO-PUF. The ARO-PUF provides a more stable key over long time and therefore reduces ECC complexity and offers smaller PUF footprint, resulting in a more efficient implementation. At the same time, the keys generated by the ARO-PUF are less sensitive to temperature and also possess strong security properties. In future work, we shall evaluate the proposed ARO-PUF in real ASICs and investigate complementary approaches for further reducing ECC overhead.

VI. Acknowledgment

This work was supported in part by the National Science Foundation under grant CNS-0844995 and a grant from Comcast.

References

[1] R. Pappu, "Physical one-way functions," Phd thesis, Massachusets Instutute of Tecnhology, 2001.

[2] B. Gassend et al., "Silicon physical random functions," in CCS 02: Proceedings of the 9th ACM conference on Computer and communications security. New York, NY, USA: ACM, pp. 148-160, 2002.

[3] D. Lim et al., "Extracting secret keys from integrated circuits," IEEE Trans. VLSI Syst., vol. 13, no. 10, pp. 1200-1205, 2005.

[4] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," in Proc. 44th ACM/IEEE Design Automation Conf. DAC 07, pp. 9-14, June 2007.

[5] F. Koushanfar and M. Potkonjak, "CAD-based Security, Cryptography, and Digital Rights Management," Design Automation Conference, 44th ACM/IEEE, pp. 268-269, June 2007.

[6] J. Guajardo et al., " Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable functions", *Information Systems Frontiers*, vol. 11, no. 1, pp. 19-41, 2009.

[7] M. Areno, and J. Plusquellic, "Securing Trusted Execution Environments with PUF Generated Secret Keys," in Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 1188-1193, June 2012.

[8] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of puf-based "unclonable" rfid ics for anti-counterfeiting and security applications," in RFID, pp. 58-64, April 2008.

[9] G. E. Suh, C.W. O"Donnell, and S. Devadas, "Aegis: A Single-Chip Secure Processor," Design & Test of Computers, IEEE , vol.24, no.6, pp. 570-580, Nov.-Dec. 2007.

[10] 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, pp. 3-8, 2009.

[11] F. Catthoor, P.Raghavan, H. Kukner, S. Khan, and S. Hamdioui, "Incorporating parameter variations in BTI impact on nano-scale logical gates analysis," IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), pp. 158-163, 2012.

[12] I.M. Filanovsky and A. Allam, "Mutual Compensation of Mobility and Threshold Voltage Temperature Effects with Applications in CMOS Circuits," IEEE Transactions on Circuits and Systems - 1: Fundamental Theory and Applications, vol. 48, no. 7, pp. 876-884, Jul. 2001.

[13] J. Guajardo, S.S. Kumar, GJ. Schrijen, and P. Tuyls, "FPGA Intrinsic Pills and Their Use for IP Protection," Workshop on Cryptographic Hardware and Embedded Systems (CHES), Sep. 2007.

[14] S. Kumar, J. Guajardo, R. Maes, GJ. Schrijen and P. Tuyls, "The Buttefly PUF: Protecting IP on every FPGA," In IEEE International Workshop on Hardware Oriented Security and Trust, 2008.

[15] M. Yu, and S. Devadas, "Secure and Robust Error Correction for Physical Unclonable Functions," Design & Test of Computers, IEEE , vol.27, no.1, pp. 48-65, 2010.

[16] V. Vivekraja, and L. Nazhandali, "Circuit-level techniques for reliable Physically Uncloneable Functions," IEEE International Workshop on Hardware-Oriented Security and Trust, pp. 30-35, July 2009.

[17] C. Yin and G. Qu, "Temperature-aware cooperative ring oscillator PUF," Hardware-Oriented Security and Trust, 2009. HOST '09. IEEE International Workshop on, pp. 36-42, July 2009.

[18] R. Kumar, H.K. Chandrikakutty, and S. Kundu, "On improving reliability of delay based Physically Unclonable Functions under temperature variations," IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 142-147, June 2011.

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

[20] A. Maiti, L. McDougall, P. Schaumont, "The Impact of Aging on an FPGA-Based Physical Unclonable Function," in Field Programmable Logic and Applications (FPL), pp. 151-156, Sept. 2011.

[21] J. Abella , X. Vera and A. Gonzalez, "Penelope: The NBTI-aware processor", Proc. Int. Symp. Microarchitect., pp. 85-96, 2007.

[22] A. Maiti et al., "A large scale characterization of RO-PUF," in Proc. IEEE Int. Hardware-Oriented Security and Trust (HOST) Symp, pp. 94-99, 2010.

[23] A. Calimera, E. Macii, and M. Poncino, "NBTI-aware power gating for concurrent leakage and aging optimization," In Proceedings of the 14th ACM/IEEE international symposium on Low power electronics and design (ISLPED '09), pp. 127-132, 2009.

[24] S. Krishnappa, H. Singh, and H. Mahmoodi, "Incorporating Effects of Process, Voltage, and Temperature Variation in BTI Model for Circuit Design," IEEE Latin American Symposium on Circuits and Systems, pp. 236-239, 2010.

[25] T. Ritter, Randomness tests: a literature survey.[Online]. Available: http://www.ciphersbyritter.com/RES/RANDTEST.HTM

[26] A. Calimera, E. Macii, and M. Poncino, "NBTI-aware sleep transistor design for reliable power-gating," in Proc. of GLSVLSI, pp. 333-338, 2009.

[27] Synopsys, http://www.synopsys.com/

[28] Z. Qi and M.R. Stan, "NBTI resilient circuits using adaptive body biasing," In Proc. GLSVLSI, ACM, pp. 285-290, 2008.

[29] L. Zhang and R.P. Dick, "Scheduled voltage scaling for increasing lifetime in the presence of NBTI," In Proc. of ASP-DAC, pp. 492-497, 2009.

[30] J.H. van Lint. Introduction to Coding Theory. Springer-Verlag, 1992.

[31] http://www.caimicro.com/web_cn/upload/caimicro_bch_intro_en_v1.2.pdf

[32] T. Nigam, B. Parameshwaran, and G. Krause, " Accurate product lifetime predictions based on device-level measurements," In Proc. IRPS, pp. $634-639$, 2009.