Aging Resilient Ring Oscillators for Reliable Physically Unclonable Functions (PUFs)

Aging Resilient Ring Oscillators for Reliable Physically Unclonable Functions (PUFs)

M. Omaña[1], M. Grossi[1], D. Rossi[2], C. Metra[1]

Corresponding author: martin.omana@unibo.it

[1] University of Bologna, Bologna, Italy

[2] University of Pisa, Pisa, Italy

This work was partially supported by the Italian National Resilience and Recovery Plan (PNRR) through the PE7 – SERIC (Security and Rights in the CyberSpace) Project, and by the Italian Ministry of Education and Research in the framework of the ForeLab and CrossLab projects (Departments of Excellence), Department of Information Engineering, University of Pisa, Italy.

Abstract

Physically Unclonable Functions (PUFs) are a promising low-cost solution for authentication and key generation in cryptosystems. However, it has been shown in the literature that, due to aging mechanisms such as Bias Temperature Instability (BTI), PUFs may no longer be able to generate correct outputs after a certain lifetime, thus becoming unreliable. In order to mitigate this problem, we present a novel ring oscillator (RO) based PUF design that is highly robust against BTI degradation. It will be hereinafter referred to as Highly BTI Resilient RO – HBTIRRO. In particular, we present two possible implementations for our HBTIRRO, each one corresponding to a different tradeoff among robustness against BTI, power consumption and area occupation. We compare the effectiveness and costs of the two proposed HBTIRRO implementations to those of a standard RO, and of the most recent alternative solution presented in the literature. We show that, one of our HBTIRRO implementation features the highest robustness against BTI, enabling a reduction in frequency degradation of 57.2% and 34.6% with respect to the standard RO and the recent alternate solution, respectively, while requiring a similar area and some increase in power consumption. The other implementation of our HBTIRRO features a very low cost in terms of area occupation, while featuring a robustness against BTI that is comparable to the most recent alternative solution presented in the literature. Moreover, we show that, compared to both the considered alternative solutions, our two HBTIRRO implementations present similar or higher (i.e., better) values in the three classical

PUF figures of merit (namely, uniqueness, reliability and randomness), and the highest standard deviation in the statistical distribution of the oscillation frequency resulting from process variation. Therefore, our two proposed HRTIRRO offer also a more secure implementation for RO-based PUF than the compared solutions.

Keywords: Reliability, Aging, Ring Oscillator, Bias Temperature Instability, BTI, Physically Unclonable Function, PUF.

1. Introduction

In recent years, we have assisted to a great increase in the number of applications for the Internet-of-Things technology, spanning consumer electronics, wearable sensors, smart cities, monitoring of critical infrastructures, etc. [1]. Wireless communication security is of primary concern for IoT applications, since cyberattacks may result in significant economic losses, as well as physical harm to people [2].

To prevent illegal accesses and fraudulent activities, modern electronic systems make a wide use of cryptography for data protection (integrity and privacy) [3, 4, 5] and entity authentication [6, 7, 8, 9]. Indeed, sensible data are usually protected by encrypting them using a secret key. As a result, encrypted data can be accessed only by entities knowing this secret key. However, the encryption key is often stored in non-volatile memories (NVMs) and the security system can be defeated by hacking attacks aimed at tampering the NVM [10]. For example, in [11], the feasibility of attacks in IoT devices using simple power analysis is discussed, and possible countermeasures are proposed. Additionally, a survey on security issues in public key cryptography for smart cards is presented in [12].

Similarly, entity/device authentication often relies on token-based mechanisms utilizing secret keys stored in supposedly secure NVMs [13]. Therefore, also these approaches are prone to NVM tampering attacks. In [14], a novel authentication scheme is proposed, which is based on elliptic curve cryptography for telecare medical information. However, the implementation cost of elliptic curve cryptography is high in terms of required computation and power consumption, which make it unsuitable for IoT applications.

To overcome limitations due to high implementation cost and low security, Physically Unclonable Functions (PUFs) can be used as low-cost approaches for secret key generation and device authentication [15, 16, 17]. In a PUF-based secure system, the secret key is not stored in a memory, but is generated exploiting parameter variations affecting multiple copies of the same device. Indeed, nanometer CMOS technologies are characterized by a huge dispersion in the values of manufacturing

process parameters [17]. This way, potential security threats resulting from tampering attacks can be avoided. Therefore, in comparison to conventional approaches based on storing secret keys in non-volatile memories, a PUF represents a tamper resistant approach to generate unique device fingerprints, thus guaranteeing a secure authentication process [18].

The operation of PUFs is based on applying a sequence of input signals (challenges) and monitoring the device output (response). PUFs featuring the same design, but implemented on different devices, will produce different responses to the same input challenge, due to intrinsic variations in process parameters. Therefore, the response of each PUF to a given input challenge is unique, and cannot be used to infer the response to the same input challenge of other PUFs that are implemented on different devices.

PUF devices can be designed based on different working principles. Optical PUFs, for example, exploit the random and unique speckle pattern that arises when a laser beam collides with a scattering medium [5, 19]. SRAM PUFs exploit the unique random startup values in uninitialized SRAM memory cells [20, 21]. Arbiter PUFs rely on the intrinsic delay differences of electrical signals along two symmetrical combinational paths [22]. Ring oscillator (RO) based PUFs exploit the differences in the oscillation frequency among different replicas of the circuit [23]. Different PUF technologies (SRAM, Arbiter, etc.) are characterized by different advantages and disadvantages. For instance, Arbiter PUFs can generate a large number of secret keys based on the received inputs, present a simple structure [24], but are vulnerable to machine learning attacks [25]. SRAM based PUFs feature low power consumption and area, but are very vulnerable to power side channel attacks [2]. Instead, as described in [26], RO-based PUFs are the most promising solution, since they present a good tradeoff between design simplicity and robustness [27]. However, RO-based PUFs suffer from aging effects more than other PUF technologies [28].

To ensure secure and reliable PUF operations, the device response to a challenge must be unique and repeatable. However, PUF activity during lifetime and changes in the operative conditions (i.e., temperature, humidity, power supply fluctuations, etc.) can induce unpredictive variations in the PUF response characteristics, thus degrading device reliability [18]. In particular, it is well known [18, 29, 30] that aging mechanisms can severely impact the electrical characteristics of electronic devices, permanently altering the PUF functionality and its reliability.

Among different aging mechanisms that affect electronic devices, Bias Temperature Instability (BTI) is known to be one of the most important aging mechanisms affecting the performance and the reliability of scaled-down integrated circuits [31, 32, 33, 34, 35, 36]. The BTI mechanism results in an increase of the absolute value of MOSFETs' threshold voltage with time, thus impacting the transistor electrical characteristics [31, 37]. Negative BTI (NBTI) degrades the performance of PMOS

transistors and usually has a stronger impact on the device reliability than Positive BTI (PBTI) that, instead, degrades the performance of NMOS transistors [33, 34, 35, 36].

The effects of aging on the reliability of ring oscillator (RO) based PUFs have been investigated and discussed in [18, 29, 30]. In particular, the results in [29] have shown how the aging mechanisms do not affect the device randomness, but produce a degradation (i.e., a change over time) in the oscillation frequency.

To overcome this problem, a RO based PUF that is robust against NBTI has been proposed in [18]. It has been implemented considering a 90nm CMOS technology, for which the effects of PBTI are negligible compared to those of NBTI. The RO based PUF in [18] enables a significant reduction of PUF oscillation frequency degradation compared to standard RO-based PUFs. However, as shown in [30], the solution in [18] does not enable to improve the robustness of RO based PUFs against PBTI degradation that, for technologies beyond 90nm, presents an impact on transistors' degradation similar to NBTI.

In [27], the Authors proposed a RO based PUF that is robust against both BTI and Hot Carrier Injection (HCI) degradation mechanisms. The solution is based on the use of current-starved inverters, whose bias conditions can be modified over time to compensate efficiently the effects of BTI and HCI degradation. However, the solution requires a precise transistor sizing and the inclusion of an accurate voltage reference, which may impact the overall cost and implementation complexity.

In [30], a RO based PUF that is robust against both PBTI and NBTI has been recently proposed. It enables reductions in oscillation frequency degradation compared to the standard RO and the NBTI-robust RO in [18]. However, the area occupation of this solution is not negligible, and the improvement in the oscillation frequency degradation may not be sufficient for PUFs requiring high levels of reliability.

Based on these considerations, in this paper we present a novel RO based PUF design that is highly robust against BTI degradation, hereinafter referred to as Highly BTI Resilient RO – HBTIRRO. The basic idea behind our proposed robust RO-PUF is to replace the NAND and all NOTs of standard RO-PUFs with a novel, modified NOT gate (referred to as NOTBTI) that presents low sensitivity to BTI degradation. In particular, our NOTBTI is designed to minimize the stress time (i.e., the conduction time) of transistors driving its output node, thus reducing the BTI degradation on such transistors. As a result, degradation of HBTIRRO oscillation frequency is also reduced during circuit lifetime. Our design strategy is based on the observation that PUFs are typically active (Enabled) only for less than the 1% of chip lifetime [18], while they are inactive for the rest of the time. Therefore, the transistors driving the output of our NOTBTI gate can be turned off in the long time intervals during which the PUFs are disabled. This allows us to reduce significantly the degradation of the

oscillation frequency of our HBTIRRO due to BTI. In particular, we propose two possible implementations of our NOTBTI. We refer to them as NOTBTI-1, and NOTBTI-2, each one corresponding to different tradeoffs among robustness against BTI, power consumption and area occupation.

The robustness against BTI and the power consumption of our HBTIRRO (for the two implementations of NOTBTI) have been verified by means of HSPICE simulations considering a 32nm CMOS technology. Particularly, robustness against BTI has been evaluated as the relative change (increase) of their oscillation frequency over chip lifetime. We then compare the effectiveness and costs of the two derived HBTIRRO implementations to those of the standard RO and the most recent alternative solution presented in [30]. We show that, our HBTIRRO implemented using NOTBTI-1 features the highest robustness against BTI. It enables a reduction in frequency degradation over time that reaches 57.2% and 34.6% with respect to the standard RO and the solution in [30], respectively, while requiring a similar area and some increase in power consumption. Instead, our HBTIRRO implemented using NOTBTI-2 features a very low cost in terms of area occupation (similar to that of the standard RO and approximately 63.5% lower than that of the solution in [30]), while presenting a robustness against BTI that is comparable to the alternate solution in [30].

In addition, we show that, compared to the standard RO and the alternative solution in [30], our two HBTIRRO implementations presents the highest standard deviation in the statistical distribution of the oscillation frequency resulting from technology parameter dispersions with respect to their nominal values. This results in a higher (average) difference among the oscillation frequency of the ROs composing the PUF, with consequent higher PUF robustness against temperature and power supply variations, as well as aging degradation. In fact, we show that, compared to the standard RO and the alternative solution in [30], our two HBTIRRO implementations present similar or higher (i.e., better) values in the three classical PUF figures of merit, namely, uniqueness, reliability and randomness.

Moreover, similarly to classical PUFs, our solution can also be adopted together with ECCs, thus further increasing the PUF reliability against temperature and voltage variations, as well as aging phenomena. For a given ECC, the adoption of such an ECC and our solution will enable to achieve a higher PUF reliability than the use of such an ECC and a standard RO-based PUF. Vice versa, for a considered targeted reliability, our solution would require the adoption of an ECC with lower correction ability (i.e., a less expensive ECC) than the standard RO-based PUF.

Therefore, our two proposed HRTIRRO solutions offer also a more secure and reliable implementation for RO-based PUF than the standard RO-based PUF and the most recent alternative solution in [30].

The rest of this paper is organized as follows. In Section 2, we recall some general concepts on RO-based PUFs and on the impact of BTI on PUF reliability. In Section 3, we present our proposed novel RO-based PUF designs that are robust against BTI. In Section 4, we evaluate the effectiveness and costs our proposed solutions, and we compared them with those of a standard RO and the most recent alternate solution in [30]. Finally, some conclusive remarks are drawn in Section 5.

2. Preliminaries on RO-Based PUF Designs and the Impact of BTI on PUF Reliability

Physically Unclonable Functions (PUFs) exploit the random variations of technological parameters that occur during fabrication to generate secure secret keys [38, 39, 18]. Silicon-based PUFs can be implemented according to different working principles, such as: Arbiter PUFs [20], SRAM-based PUFs [22], Butterfly PUFs [40], and Ring-Oscillator (RO) PUFs [23, 18]. Among these different types of PUF devices, RO-based PUFs are very promising, since they feature advantages in terms of design simplicity and security [18, 38, 39, 40].

A schematic representation of a RO-based PUF operation is shown in Fig. 1. As can be seen, the RO-based PUF receives as input (or challenge) a sequence of *m* words at times t_1, t_2, … t_m. The number of bits (*k)* of the input words is constant, and depends on the number of ROs of the considered RO-based PUF. For each input word, the PUF generates a response consisting of a single bit at its output (OUT). Therefore, the overall PUF response to the sequence of *m* input challenges is composed by the sequence of *m* PUF responses, each consisting of a single bit.

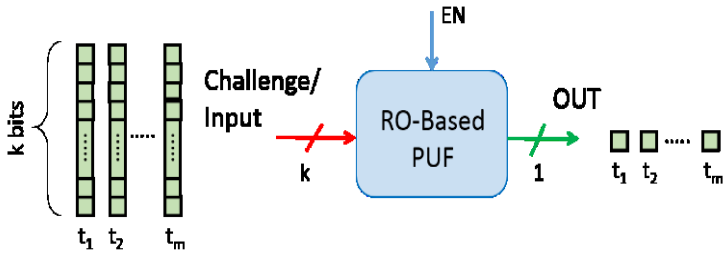

Fig. 1 Schematic representation of the operation of a typical Ring Oscillator (RO) based PUF.

Figure 2(a) shows the structure of a typical RO-based PUF [23, 30]. It presents *n* identical ROs (RO_i, $i=1, \ldots, n$), two multiplexers (MUX_1 and MUX_2), two binary counters, *Counter1* and *Counter2*, and an output comparator. The *k* bits of the PUF challenge are used as selection signals for MUX_1 and MUX_2. Therefore, the number *k* should be chosen to satisfy the condition $2^k \geq n$.

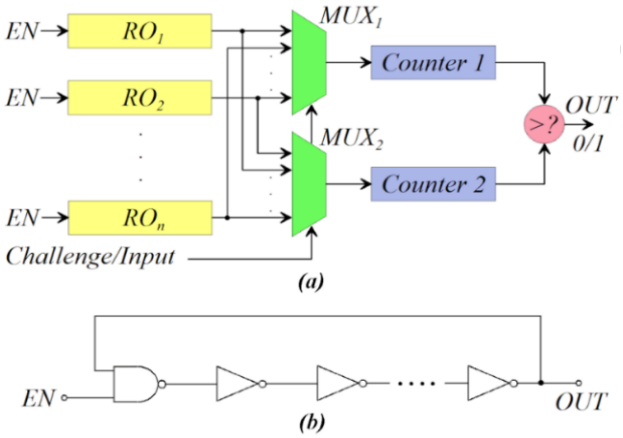

Fig. 2 (a) Schematic representation of a typical Ring Oscillator (RO) based PUF [23, 30]; (b) standard gate level implementation of each ring oscillator RO [23, 30].

The typical implementation of each RO composing the PUF is depicted in Fig. 2(b). As can be seen, each RO consists of an odd number of inverting stages, that are implemented by a NAND gate followed by an even number of NOT gates. The inputs of the NAND gate are an enable signal (EN) and the output of the last inverting stage of the RO. When EN = 1, the RO oscillates and generates at its output (OUT) a square waveform, with an oscillation frequency f_{osc} that depends on the number of inverting stages and the delay of each inverting gate. The ROs in the PUF (Fig. 2(a)) are designed with the same number of inverting stages. However, each RO features a unique value of oscillation frequency f_{osc}, because of the random variation of technological parameters occurring during fabrication [38]. Instead, when EN=0, the output of the NAND gate is always equal to 0, and the output signal of the RO (OUT) is fixed at a constant voltage value.

Moreover, the output of each RO is connected to a different input of MUX_1 and MUX_2, so that the multiplexers can select two different ROs outputs OUT_i and OUT_j, for each k-bit word received at the PUF input. The output of the RO selected by MUX_1 is used as clock signal for *Counter1*, while output of the RO selected by MUX_2 acts as clock signal for *Counter2*. Since the oscillation frequency f_{osc} of each RO is unique, the final count provided by the two counters after a predefined time interval will be different. Finally, the outputs of the counters are compared to generate the single bit response for each input challenge.

A reliable PUF must generate the same output for the same input challenge during its entire lifetime. However, as discussed in the Introduction, aging mechanisms, such as BTI, can seriously affect the PUF reliability by altering the RO characteristics as circuits age [17, 29]. Indeed, as shown in [18], depending on the activity of each RO in the PUF (*e.g.,* some ROs may be activated more frequently

than others) and operating conditions (*e.g.,* different temperature), which in turn depends on the input challenge, different ROs in a PUF can experience different levels of degradation during circuit lifetime, thus resulting in different variations of their oscillation frequency over time [18]. As an example, consider two ROs in the PUF in Fig. 1, hereafter referred as RO_i and RO_j, with their respective oscillation frequency f_{osc} at time 0 (fresh device). Let us also assume that at time 0 it is $f_{osci} > f_{oscj}$, with RO_i driving the clock of *counter 1* and RO_j driving the clock of *counter 2*. Thus, at the beginning of circuit lifetime, the count of *counter 1* will be higher than that of *counter 2,* and the PUF will produce at its output OUT=1. Let us now assume that during circuit lifetime RO_i experiences a faster degradation than RO_j, for instance because it operates at a higher temperature. In this case, the oscillation frequency f_{osci} will decrease faster than f_{oscj}. This way, after a certain operating time, the oscillation frequency of RO_i (f_{osci}) will become lower than that of RO_j (f_{oscj}), and the PUF will produce an incorrect output value OUT=0.

As shown in [18], NBTI can induce errors at the outputs of the PUF after only 2 years of circuit lifetime, with an average degradation of the oscillation frequency of about 12% over 10 years. The RO-PUF presented in [18] is able to mitigate the effect of NBTI degradation on the oscillation frequency of RO-based PUFs. This solution is effective for the considered 90nm CMOS technology, where NBTI was a major aging mechanism, and the impact of PBTI degradation was negligible. However, it is no longer effective for more scaled technologies, which present a PBTI impact similar to NBTI on the PUF frequency degradation.

The RO based PUF in [30], referred to as LBTIRO, is robust against BTI (*i.e.,* both PBTI and NBTI), but its area cost is not negligible. Moreover, the robustness against oscillation frequency degradation provided by LBTIRO may be not enough for circuits requiring high levels of reliability.

To overcome this limitation, in this paper, we present a novel RO-PUF that, compared to previous solutions, offers a better tradeoff among robustness with respect to BTI, power consumption and area occupation.

3. Proposed RO-Based PUFs

We present our novel ring oscillator (RO) based PUF design that is highly robust against BTI degradation (HBTIRRO). The basic idea of our proposed robust RO-PUF is to replace the NAND and NOTs of standard RO-PUFs (Fig.2 (b)) with a modified NOT gate, referred to as *NOTBTI*, that presents low sensitivity to BTI degradation. The schematic representation of our HBTIRRO is shown in Fig. 3.

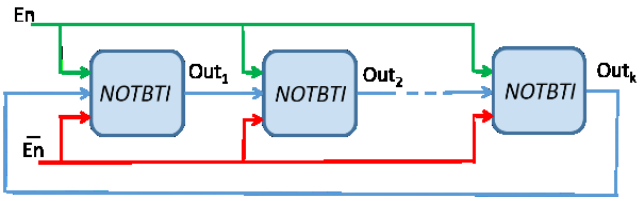

Fig. 3 Schematic representation of the proposed ROs for RO based PUFs.

Each *NOTBTI* in the chain receives as input an enable signal EN and its complemented value, as well as the output of the previous *NOTBTI* in the chain. The first *NOTBTI* is fed by Out_k of the last *NOTBTI*, which is also the output of our HBTIRRO. Similar to a standard RO-based PUF, while EN = 1, the output Out_k of our HBTIRRO oscillates with a frequency f_{osc} that is inversely proportional to the delay of the chain of *k NOTBTIs*. Instead, while EN = 0, the outputs of all gates are set to 1, and HBTIRRO is disabled.

The *NOTBTI* is designed to minimize the stress time of the transistors driving its output node, where the stress time is the portion of chip lifetime during which the considered transistors are ON. This way, the amount of BTI degradation on the transistors driving the *NOTBTI* output is reduced, and so is the impact of BTI on the HBTIRRO f_{osc} during circuit lifetime.

We propose two possible implementations of our *NOTBTI*, referred to as *NOTBTI*-1, and *NOTBTI*-2, each one offering different tradeoffs among robustness against BTI, power consumption and area occupation. The transistor level implementation of the proposed *NOTBTI*-1 is reported in Fig. 4.

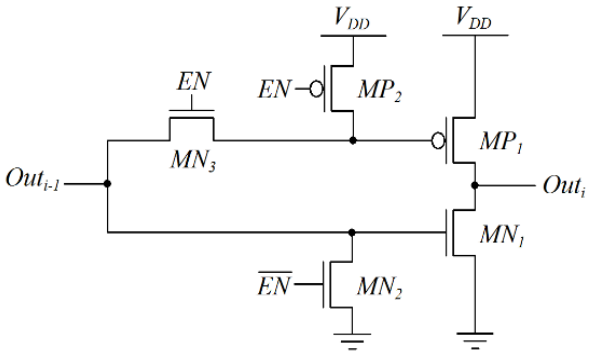

Fig. 4 Transistor level implementation of our proposed NOTBTI-1 gate, featuring low sensitivity to BTI degradation.

As can be seen, in our *NOTBTI-1* the output node Out_i is driven by transistors M_{P1}/M_{N1}. In the time intervals during which the PUF is enabled (EN=1), both transistors M_{P2} and M_{N2} are turned OFF, while the gate terminal of M_{P1} is connected to the input Out_{i-1} through the conductive pass transistor M_{N3} driven by EN=1. Therefore, while EN=1, M_{P1} and M_{N1} will alternate their ON/OFF state according to the value of Out_{i-1}: on overall, they will be ON for the 50% of the time during which EN

= 1. As a result, when EN = 1, our *NOTBTI* operates as an inverter for the output of the previous stage, as required for the correct operation of our HBTIRRO.

Instead, in the time intervals during which the PUF is disabled (EN=0), transistors M_{P2} and M_{N2} become both conductive (ON), so that the gate of M_{P1} is connected to V_{DD}, while the gate of M_{N1} is connected to ground. Therefore, transistors M_{P1} and M_{N1} are both turned OFF while EN=0. During this time interval, the pass transistor M_{N3} is OFF as well, thus preventing any electrical conflict between transistors M_{P2} and M_{N2}. Consequently, in our *NOTBTI*, transistors M_{P1} and M_{N1}driving its output Out_i are conductive only during the time intervals during which the PUF is enabled (EN=1), while they are OFF when EN=0.

As known, PUFs are typically active only for less than the 1% of the chip lifetime [17], while they are inactive for most of its lifetime. Therefore, transistors M_{P1} and M_{N1} driving the output of our *NOTBTI* are OFF most of the time, thus undergoing a very limited degradation due BTI. As a result, the propagation delay of our *NOTBTI*, and consequently the oscillation frequency of our HBTIRRO, are minimally affected by BTI degradation.

We propose a second possible implementation for *NOTBTI*, referred to as *NOTBTI*-2, whose transistor level implementation is shown in Fig. 5. The structure of our *NOTBTI-2* is very similar to that of our *NOTBTI-1* in Fig. 4. The only difference is that *NOTBTI-2* includes an additional pass transistor, M_{N4}, which connects the input node Out_i to the gate of the nMOS transistor M_{N1}. The main goal of this additional pass transistor is to equalize the rise and fall times in *NOTBTI-2*. As will be shown by the comparison analysis, the additional M_{N4} in *NOTBTI-2* enables also to achieve different tradeoffs among robustness against BTI, power consumption and area occupation when compared to our *NOTBTI-1*.

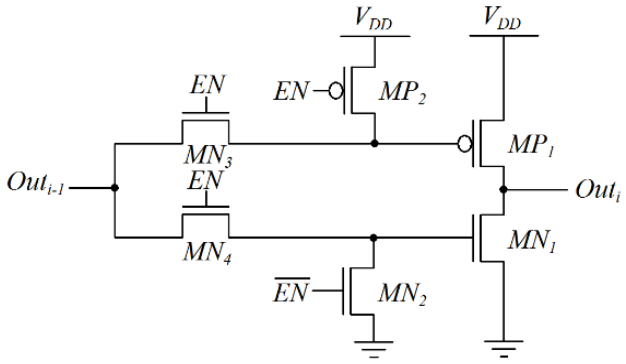

Fig. 5 Transistor level implementation of our proposed NOTBTI-2 gate, featuring low sensitivity to BTI degradation.

As described for our *NOTBTI-1* above, the transistors driving the output Out_i (M_{P1} and M_{N1}) of our *NOTBTI-2* are conductive only when PUF is enabled (EN=1), while they are OFF otherwise. Since the PUF is active only for less than the 1% of chip lifetime, transistors M_{P1} and M_{N1} are OFF most of

the time, and thus their BTI-induced degradation is minimized. Therefore, similar to *NOTBTI-1*, the oscillation frequency of our HBTIRRO with *NOTBTI-2* is minimally affected.

In order to determine the optimal value for transistor size ratios of our *NOTBTI-1* and *NOTBTI-2*, we have performed HSPICE simulations considering, as an example, the 32 nm High-K CMOS technology in [41], and a level 54 HSPICE model, with V_{DD} = 1.0V, and a temperature of 27 °C. The effects of BTI degradation on the transistor threshold voltage have been evaluated by utilizing the MOSRA tool from HSPICE [42]. To cover a broad number of possible PUF applications, we considered a range of PUF operating time between 0 and 7 years [18, 27],

We have implemented our HBTIRRO to achieve an oscillation frequency f_{osc} = 300MHz. To determine the optimal value for transistor size ratios of our *NOTBTI-1* and *NOTBTI-2*, we have evaluated the area of HRBTIRRO, its static power consumption (P_{static}) when EN=0, and its dynamic power consumption (P_{dyn}) when EN=1. We have also evaluated the degradation (reduction) in the oscillation frequency (Δf_{osc}) of HBTIRRO after 7 years of PUF lifetime, as:

$$\Delta fosc(\%) = 100 \cdot \frac{fosc_{0_{year}} - fosc_{7_{year}}}{fosc_{0_{year}}} \qquad (1)$$

Table I reports the obtained results for our HBTIRRO implemented by using the *NOTBTI-1* in Fig. 4 for four different size ratios of pass-transistor MN_3 (i.e., $S_{MN3} = (W/L)_{MN3}$). The size of the other four transistors (MN_1, MP_1, MN_2, and MP_2) is minimum, in order to minimize area and power, that is: $S_{MN1} = (W/L)_{MN1} = S_{MP1} = (W/L)_{MP1} = S_{MN2} = (W/L)_{MN2} = S_{MP2} = (W/L)_{MP2} = 1$.

TABLE I

CHARACTERISTICS OF OUR HBTIRRO IMPLEMENTED BY USING THE NOTBTI-1 IN FIG. 4 FOR DIFFERENT SIZES OF THE PASS-TRANSISTOR MN_3, WHILE THE OTHER TRANSISTORS ARE SET TO MINIMUM SIZE (S_{N1}=1 S_{P1}=2 S_{N2}=1 S_{P2}=2).

S_{MN3}	Δf_{osc} (%)	P_{dyn} (EN=1) (μW)	P_{static} (EN=0) (μW)	Area (μm^2)
1	6.8204	457.86	18.55	1.501
2	7.0066	331.88	28.748	1.535
3	8.4051	255.17	36.672	1.523
4	8.6675	195.4	39.515	1.467

The results in Table I show that, by increasing S_{MN3}, we obtain an increase in the f_{osc} degradation and in static power consumption when the PUF is active (EN=1), and a decrease in dynamic power when the PUF is disabled (EN=0). As for the area, it minimally changes with S_{MN3}. Since the main goal is to minimize the oscillation frequency degradation, we implemented the pass-transistor MN_3 of our *NOTBTI-1* with minimum size S_{MN3}=1.

The results obtained for our HBTIRRO implemented by using the *NOTBTI-2* in Fig. 5 are reported in Table II, for the case of three different combinations of the size ratios of pass-transistors MN_3 and MN_4 (i.e., $S_{MN3} = (W/L)_{MN3}$ and $S_{MN4} = (W/L)_{MN4}$, respectively). Again, we considered the other four transistors of *NOTBTI-2* (MN_1, MP_1, MN_2, and MP_2) as minimum sized, in order to minimize area and power.

TABLE II

CHARACTERISTICS OF OUR HBTIRRO IMPLEMENTED BY USING THE NOTBTI-2 IN FIG. 5 FOR THREE DIFFERENT COMBINATIONS OF THE SIZE OF THE PASS-TRANSISTOR MN_3 AND MN_4 WHILE THE OTHER TRANSISTORS ARE SET TO MINIMUM (S_{N1}=1 S_{P1}=2 S_{N2}=1 S_{P2}=2).

S_{MN3}	S_{MN4}	Δf_{osc} (%)	P_{dyn} (EN=1) (μW)	P_{static} (EN=0) (μW)	Area (μm^2)
1	1	10.7455	150.01	5.36	0.732
1	2	13.089	148.48	4.975	1.579
2	1	11.6994	132.12	5.37	2.629

The results in Table II show that the minimum f_{osc} degradation and area are obtained if MN_3 and MN_4 are minimum sized (i.e., S_{MN3}= S_{MN4}=1). Compared to this case, the other two cases (S_{MN3}=1, S_{MN4}=2 and S_{MN3}=2, S_{MN4}=1) present a higher f_{osc} degradation and require significantly more area, while featuring a comparable, or slightly lower, dynamic and static power consumption. Therefore, we choose minimum sized pass-transistors MN_3 and MN_4 (S_{MN3}= S_{MN4}=1).

4. Verification and Cost Comparison

We evaluate the effectiveness and costs of our proposed HBTIRRO implemented with the two proposed inverting elements *NOTBTI-1* and *NOTBTI-2*, and we compare them to those of a standard RO and the alternative BTI-robust RO (LBTIRO) recently presented in [30].

4.1 Simulation Setup and Comparison Metrics

We have simulated our HBTIRRO, the standard RO and the solution in [30], and evaluated the effects of BTI degradation considering the same setup as described in the previous section. In addition, we have evaluated frequency degradation Δf_{osc} considering a realistic PUF activation time of 1%, during which EN = 1 and the PUF is enabled. Particularly, we have implemented our HBTIRRO (with both *NOTBTI-1* and *NOTBTI-2*), the standard RO and the solution in [30] with a proper number of inverting stages that makes them feature the same f_{osc} = 300 MHz at the beginning of circuit operation (i.e., with fresh ROs).

More in detail, for the three compared solutions, we have evaluated: i) the effectiveness in reducing the impact of BTI on oscillation frequency (f_{osc}); ii) the cost in terms of energy/power consumption; iii) the cost in terms of area occupation; iv) the standard deviation of the statistical distribution of f_{osc} resulting from dispersions of technological parameters; v) the three classical PUF figures of merit: uniqueness, reliability and randomness.

As for the effectiveness of the compared solutions in reducing the impact of BTI on the RO oscillation frequency (f_{osc}), by means of HSPICE simulations, we have evaluated the degradation (reduction) in the oscillation frequency (Δf_{osc}) after 7 years of PUF lifetime, calculated as shown in (1) in Section 3.

As for the energy/power consumed by the compared ROs, we have also evaluated it by means of HSPICE simulations. More in detail, we have assessed the energy E_{OSC} consumed by the compared solutions per single oscillation period of the RO, for the time intervals during which the PUF is activated (i.e., EN=1). Its expression is:

$$E_{OSC}(W/Hz) = \left.\frac{P_{dyn}}{f_{osc}}\right|_{EN=1} \qquad (2)$$

where $P_{dyn,}$ and f_{osc} are the dynamic power and the oscillation frequency, respectively, of the compared ROs when the PUF is active (EN=1).

Instead, for the time intervals during which the PUF is disabled (i.e., EN=0), we have evaluated the static power (P_{static}) consumed by the compared ROs. It is worth noting that, since the PUF activation time is very short compared to circuit lifetime (typically less than 1% of the time), the static power represents an important contribution to the overall energy consumed by the PUF.

As for area occupation, it has been roughly estimated as the total area of the gate terminals of the transistors used to implement the compared ROs.

Next, by means of Monte Carlo simulations we have evaluated the standard deviation of the f_{osc} distribution (due to parameter dispersions) of our HBTIRRO, of the standard RO and of the solution in [30]. The standard deviation of the f_{osc} distribution indicates how well the f_{osc} of a PUF design changes from chip to chip, and is typically used as metric to assess the *uniqueness* of PUFs [18]. In particular, for this evaluation, we have performed 200 Monte Carlo simulations considering variations of transistors' oxide thickness (*tox*) and carrier mobility (*uo*), with a Gaussian distribution with: a mean μ = 1.65nm (μ = 1.75nm) and σ = 0.1705nm (σ = 0.1821nm) for the oxide thickness of nMOS (pMOS) transistors; a mean μ = 0.04172 (μ = 0.00393) σ = 0.00408 (σ = 0.000415) for the carrier mobility of nMOS (pMOS) transistors.

Finally, we have also evaluated and compared the three classical PUF figures of merit (namely, uniqueness, reliability and randomness) of the compared RO-based PUFs. As a case study, and similar to [27], we have considered PUFs with 256 ROs, an input challenge of 128 bytes, a response of 64 bits, and 10000 Challenge-Response Pairs (CRPs).

As for the Uniqueness (U) figure of merit, it is typically evaluated by the following equation [27]:

$$U = 100\frac{2}{m(m-1)}\sum_{i=1}^{m-1}\sum_{j=i+1}^{m}\frac{HD(R_i,R_j)}{n} \qquad (3)$$

where m is the number of considered different PUF implementations, n is the length of the response (number of bits), while R_i and R_j are the responses of two different devices to the same input challenge. Finally, $HD(R_i, R_j)$ is the Hamming Distance of the two responses R_i, R_j, which is defined as the number of bit positions at which the two responses differ. The ideal value for uniqueness is 50% [27].

As for the Reliability (S) figure of merit, it is typically evaluated by means of the following equation [27]:

$$S = 100\left[1 - \frac{1}{k}\sum_{j=1}^{k}\frac{HD(R_i,R_j)}{n}\right] \qquad (4)$$

where, n is again the length of the PUF response (number of bits), R_i is now the response of the PUF under nominal operating conditions (i.e., temperature and power supply voltage) at the beginning of circuit operation (*i.e.,* without BTI affecting the PUF), $R_{i,j}$ is the response of the PUF under a given operating condition j (different from the nominal one) and circuit aging time, and k is the number of considered couples of operating conditions (temperature and power supply).

Finally, the Randomness (R) figure of merit is evaluated by means of the following equation [43]:

$$R = -100log_2[\max(P, 1-p)] \qquad (5)$$

where the parameter p is defined as:

$$p = \frac{1}{m \cdot k \cdot n}\sum_{i=1}^{m}\sum_{j=1}^{k}\sum_{l=1}^{n} R_{i,j,l} \qquad (6)$$

where m is the number of considered CRPs, k is the number of times the same challenge is applied to the PUF, while n is the length of the PUF response (number of bits). The ideal value of randomness is 100% [43].

4.2 Simulation Results

We report the results obtained from the comparison analyses described in the previous subsection. In particular, Fig. 6 reports the relative degradation (reduction) of oscillation frequency Δf_{osc} of the compared solutions, as a function of circuit lifetime, for a PUF activation time of 1%.

We can see from Fig. 6 that the degradation of Δf_{osc} over time is consistent with the trend of BTI degradation observed for scaled CMOS technologies [44, 45]. Indeed, the Δf_{osc} degradation of the three compared solutions presents a fast increase during approximately the first six months of circuit lifetime, after which the degradation tends to saturate. We can also observe that our proposed HBTIRRO implemented with the *NOTBTI-1* (black line) presents the lowest Δf_{osc} during the whole circuit lifetime, thus being the most robust against BTI. Instead, our HBTIRRO implemented by the *NOTBTI-2* (blue line) presents a Δf_{osc} that is approximately the same as that of the LBTIRO in [30] (green curve). Finally, the standard RO-based PUF (blue curve) presents the highest Δf_{osc} during the whole considered circuit lifetime.

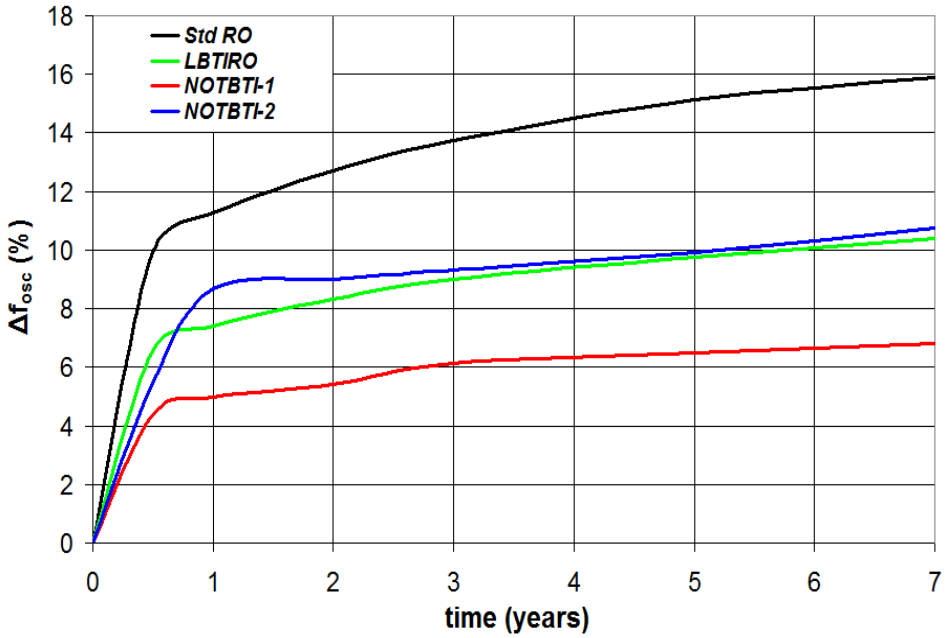

Fig. 6 Frequency degradation Δf_{osc} of the compared ROs, as a function of PUF lifetime, for the case of a PUF activation time of 1%.

More in details, Table III reports the maximum frequency degradation Δf_{osc} of the compared ROs after 7 years of circuit lifetime (second column of the table).

TABLE III

MAXIMUM FREQUENCY DEGRADATION $\Delta FOSC$ AFTER 7 YEARS OF CIRCUIT LIFETIME, ENERGY/POWER CONSUMPTION (EOSC/PSTATIC) AND AREA OF THE COMPARED ROS, FOR THE CASE OF A PUF ACTIVATION TIME OF 1%.

	Frequency degradation Δfosc (%)	Eosc (nW/MHz)	Pstatic (µW)	Area (µm2)
Standard RO	15.9 %	134.7	10.7	0.74
Solution in [30]	10.4 %	183.4	1.8	2.0
Our HRBTIRRO with NOTBTI-1	6.8 %	1541.6	18.55	1.5
Our HRBTIRRO with NOTBTI-2	10.7 %	504.4	5.3	0.73

As can be seen, after 7 years of operation, the Δf_{osc} of our HBTIRRO implemented with *NOTBTI-1* and *NOTBTI-2* is 6.8% and 10.7%, respectively. Instead, for the same lifetime interval, the Δf_{osc} of the

standard RO and the solution in [30] is 15.9% and 10.4%, respectively. Therefore, our HBTIRRO with *NOTBTI-1* enables a reduction in the maximum frequency degradation Δf_{osc} of approximately 57.2% and 34.6% with respect to the standard RO and the most recent alternative solution in [30], respectively. Instead, our HBTIRRO with *NOTBTI-2* features a maximum Δf_{osc} that is 32.7% smaller than that of the standard RO, and similar to that of the alternative solution in [30].

Table III shows also the energy E_{OSC} (Eq. (2)) and the static power (P_{static}) consumed by the compared ROs when the PUF is enabled (EN=1) and disabled (EN=0), respectively. We can observe that the standard RO presents the lowest energy consumption when EN=1, while the solution in [30] presents the lowest static power when the PUF is disabled. We can also observe that our HRBTIRRO with *NOTBTI-1*, which features the lowest BTI degradation, presents the highest energy and static power consumption. Instead, our HRBTIRRO with *NOTBTI-2* requires a static power consumption that is approximately 50% lower than that of the Standard RO and 71% lower than that of our HRBTIRRO with *NOTBTI-1*.

The increase in the energy E_{OSC} in our proposed HRBTIRRO when enabled (En=1) is inherent to the structures of the proposed NOTBTI-1 and NOTBTI-2 in Fig. 4 and Fig. 5, respectively, as they require longer commutation times than traditional NOTs and the NOTs in [30]. As known, the longer the commutation times, the longer the duration of the short circuit current flowing through the transistos of the pull-up and pull-down networks of the NOTs, and consequently the higher the energy consumption. Therefore, since the energy of all new NOTBTI-1 and NOTBTI-2 in our HRBTIRRO increase, with respect to traditional NOT design and the NOTs in [30], also the energy of our HRBTIRRO increases over the standard RO and the solution [30]. However, as clarified before, PUFs are generally enabled for a very short time (e.g., 1% of circuit lifetime according to [18]). Thus, the increase in power consumption required by our HRBTIRRO turns out to be very limited, and can be reasonably accepted, given the significantly higher robustness with respect to aging, thus the higher security, offered by our solutions.

Cost in terms of area of the compared ROs is also reported in Table III. We can observe that our HRBTIRRO with *NOTBTI-2* requires the lowest area, which is comparable to the area of the standard RO, while the solution in [30] presents the highest area among the compared approaches. In particular, the area of the solution in [30] is more than twice (273% higher than) the area of our HRBTIRRO with *NOTBTI-2*, and approximately 33% higher than the area required by our HRBTIRRO with *NOTBTI-1*. The lower area of our HRBTIRRO with *NOTBTI-2* with respect to the the standard RO is due to is higher propagation delay compared to a traditional NOT design. Therefore, the number cascaded *NOTBTI-2* required by our HRBTIRRO will be lower than the number of of NOTs in the standard RO, to obtain the same oscillation frequency (i.e., of 300 MHz).

As a result, despite the higher number of transistors in our *NOTBTI-2* compared to a traditional NOT, the overall area of our HRBTIRRO with *NOTBTI-2* is lower than that of the standard RO.

Therefore, our HBTIRRO with *NOTBTI*-1 features the highest robustness against BTI among the compared solutions. This is achieved at the cost of a limited increase of energy/power and area compared to the standard RO and our HBTIRRO with *NOTBTI*-2, but with a lower area cost than the alternative solution in [30].

Instead, our HBTIRRO with *NOTBTI*-2 features the lowest area occupation among the compared solutions, while presenting a robustness against BTI that is higher than that of the standard RO, comparable to that of the alternative solution in [30], and lower than that our HBTIRRO with *NOTBTI*-1.

Next, in Fig. 7 we depict the results of the Monte Carlo simulations that we have performed to evaluate the statistical distribution, thus the standard deviation (σ), of the oscillation frequency (f_{osc}) of the compared ROs, caused by process parameters variations occurring during fabrication.

As can be seen from Fig. 7, our HRBTIRRO with *NOTBTI-2* presents the highest standard deviation ($\sigma = 68.26$) of f_{osc}, followed by our HRBTIRRO with *NOTBTI-1* ($\sigma = 19.63$). More in detail, the standard deviation of f_{osc} in our HRBTIRRO with *NOTBTI-2* is approx. 3.5 times higher than that of our HRBTIRRO with *NOTBTI-1*, and more than 4.5 times higher than that of the standard RO and of the alternative solution in [30]. Instead, the standard deviation of f_{osc} in our our HRBTIRRO with *NOTBTI-1* is 49.3% and 35% higher than that of the standard RO and the solution in [30], respectively. The larger standard deviation of f_{osc} in our HRBTIRRO (with both *NOTBTI-1* and *NOTBTI-2*) over the alternative solutions can be attributed to the higher number of transistors of *NOTBTI-1* and *NOTBTI-2*, which makes them more vulnerable to process parameter variations.

Consequently, our proposed HRTIRRO (with both *NOTBTI-1* and *NOTBTI-2*) offers a more secure implementation for RO-based PUF, than the standard RO-based PUF and the most recent alternative solution in [30]. Indeed, one the most significant metrics adopted to assess PUF security is uniqueness in Eq. (3), which depends on the capability of two PUFs to generate different responses to the same input challenge. Therefore, the larger the variability of f_{osc} of diverse ROs (which corresponds to a high sigma of f_{osc} distribution), the higher the difference between the PUFs' responses and the Hamming distance between them, resulting in a higher uniqueness, and therefore a higher security.

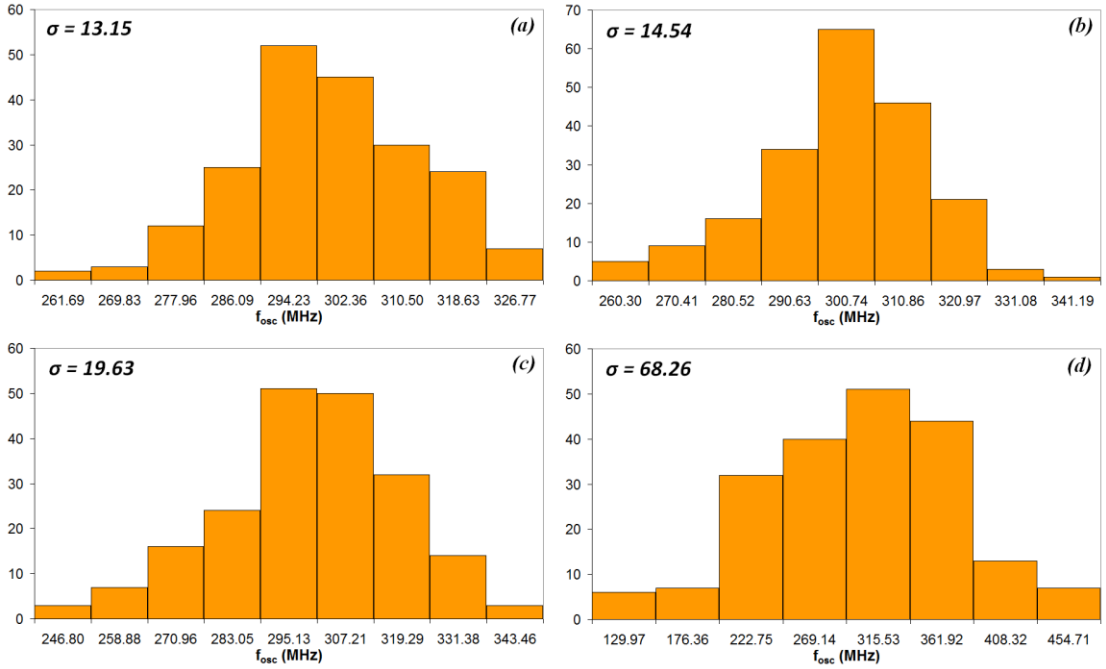

Fig. 7 Results of Monte Carlo simulations showing the statistical distribution of *fosc* due to process parameters variations of: (a) the standard RO; (b) the robust RO in [30]; (c) our HRBTIRRO implemented by NOTBTI-1; (d) our HRBTIRRO implemented by NOTBTI-2.

Finally, we have evaluated the PUF figures of merit defined by Eqs. (3), (4), (5) and (6), considering the PUF implementation described in Section 4.1.

As for uniqueness (U), our evaluations have shown that all compared solutions present a uniqueness value very close to 50%, which is the ideal value for this metric. In particular, the standard RO-based PUF presents a U=49.99%, the solution in [30] presents a U=49.97%, and our HRBTIRRO, with both *NOTBTI-1* and *NOTBTI-2,* present a U=50.00%.

As for reliability (S), we have considered an operating temperature range of 0 – 60 °C, a V_{DD} range of 0.8V – 1.2V, and a PUF aging time up to 7 years. We considered a T = 27°C and a V_{DD} = 1V as nominal operating conditions. The obtained results for reliability are depicted in Fig. 8. In particular, Fig. 8(a) reports the reliability of the compared solutions as a function of the operating temperatures, Fig. 8(b) shows the reliability of the compared solutions as a function of the power supply voltage variations, and Fig. 8(c) depicts the reliability of the compared solutions as a function of device aging time. As can be seen, the proposed HRBTIRRO implemented with the *NOTBTI-2* presents the highest reliability in the full range of considered temperature and voltage variations, as well as over the whole range of considered device aging time (0-7 years). From Figs. 8(a) and (b), we can also observe that our HRBTIRRO implemented with the *NOTBTI-1* features a reliability that is similar, or slightly higher, than that of the recent solution in [30] and, as expected, of the standard RO-based PUF, which

556 presents the lowest reliability in the full range of considered temperature and voltage variations.
557 Finally, from Fig. 8(c) we can observe that the reliability of all compared solutions diminishes with
558 the aging time. However, we can observe that the reliability reduction in our HRBTIRRO
559 (implemented with both the *NOTBTI-1* and the *NOTBTI-2*) is significantly lower than that of the
560 standard RO-based PUF. The higher reliability over lifetime offered by our proposed HRBTIRRO
561 over alternate solutions is due to its higher robustness with respect to BTI, compared to the standard
562 RO-based PUF and the alternate solution in [30].
563 As for randomness, our evaluations have shown that all compared solutions present a randomness value
564 close to 99%, thus approximating very well the randomness ideal value of 100%. In particular, the
565 standard RO-based PUF presents a randomness of 99.86%, the solution in [30] presents a randomness
566 of 99.67%, while our HRBTIRRO implemented with *NOTBTI-1* and *NOTBTI-2,* presents a randomness
567 of 99.76% and 99.88%, respectively.
568 Therefore, compared to the the standard RO-based PUF and the alternative solution in [30], our
569 HRBTIRRO presents a higher robustness with respect to BTI, and consequently higher reliability, at
570 comparable costs in terms of power consumption and area overhead. Moreover, the higher robustness
571 with respect to BTI offered by our solution, which reflects in a higher reliability, does not come at
572 the expense of uniqueness and randomness, which remain comparable to, if not better than those of
573 alternate approaches.
574 Additionally, it is worth noting that if a PUF is combined with an ECC to improve its reliability,
575 the adoption of our solution will enable to achieve a PUF reliability that is higher than or equal to that
576 of the classical solution, if an ECC with the same error correction capability is adopted in both
577 solutions. Alternately, our solution could also allow for the adoption of an ECC with lower correction
578 capability (less expensive) than the classical PUF to achieve the same PUF reliability.
579
580

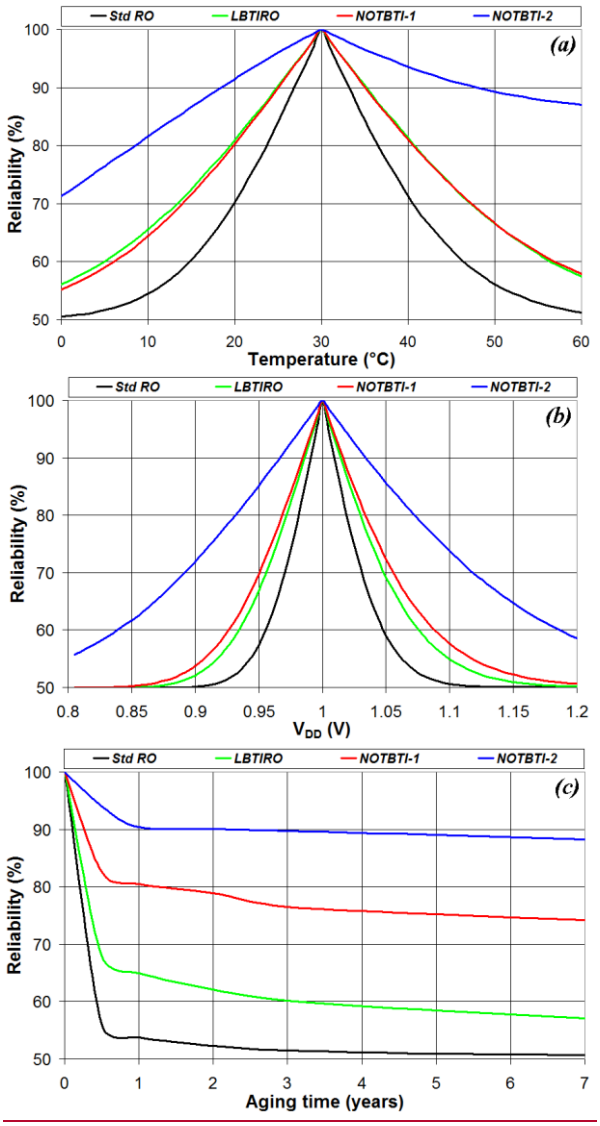

Fig. 8 Reliability figure of merit of the compared PUF solutions as a function of (a) temperature variations, (b) power supply variations, (c) PUF aging time.

4. Conclusions

We proposed a novel ring oscillator (RO) based PUF design, that is highly robust against BTI degradation, referred to as Highly BTI Resilient RO – HBTIRRO. We have presented two HBTIRRO implementations, each one featuring a different tradeoff among robustness with respect to BTI, power consumption and area occupation. The proposed HBTIRRO implementations are based on two modified versions of NOT gates (referred to as *NOTBTI-1* and *NOTBTI-2*) that present low sensitivity to BTI degradation. We have compared the effectiveness and costs of the two derived HBTIRRO implementations to those of the standard RO and the most recent alternative solution presented in [30]. The results of the performed analyses have shown that, our HBTIRRO implemented with *NOTBTI*-1 features the highest robustness against BTI, which reaches the 57.2% and 34.6% with respect to the

596 standard RO and the recent solution in [30], respectively, while requiring a similar area and some
597 increase in power consumption. Instead, our HBTIRRO implemented with *NOTBTI*-2 offers a very low
598 cost in terms of area occupation, which is similar to that of the standard RO and approximately 63.5%
599 lower than that of the solution in [30], while presenting a robustness against BTI that is comparable to
600 that of the alternate solution in [30]. Finally, we have shown that the two implementations of our
601 HBTIRRO present similar or higher (i.e., better) values in the three classical PUF figures of merit
602 (namely, uniqueness, reliability and randomness), and also feature the highest standard deviation in the
603 statistical distribution of the oscillation frequency resulting from technology parameter dispersions with
604 respect to their nominal values. Therefore, our two versions of the proposed HBTIRRO offer a more
605 reliable and secure implementation for RO-based PUF than the standard RO-based PUF and the most
606 recent alternative solution in [30].
607
608
609 **References**

610 [1] L. Atzori, A. Iera, G. Morabito, “The Internet of Things: A survey”, *Computer Networks*,
611 Volume 54, Issue 15, 2010, pp. 2787-2805.

612 [2] A. Shamsoshoara, A. Korenda, F. Afghah, S. Zeadally, “A survey on physical unclonable
613 function (PUF)-based security solutions for Internet of Things”, *Computer Networks*, *183*,
614 2020, pp. 107593.

615 [3] D. Rossi, M. Omaña, D. Giaffreda and C. Metra, "Secure communication protocol for wireless
616 sensor networks," *2010 East-West Design & Test Symposium* (EWDTS), 2010, pp. 17-20.

617 [4] Y. Cherdantseva, J. Hilton, "A Reference Model of Information Assurance & Security," *2013*
618 *International Conference on Availability, Reliability and Security*, 2013, pp. 546-555.

619 [5] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE*
620 *Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586-602, 1 Oct.-Dec. 2017.

621 [6] W. -C. Wang, Y. Yona, Y. Wu, S. N. Diggavi and P. Gupta, "SLATE: A Secure Lightweight
622 Entity Authentication Hardware Primitive," *IEEE Transactions on Information Forensics and*
623 *Security*, vol. 15, pp. 276-285, 2020.

624 [7] Y. Wang, C. Wang, C. Gu, Y. Cui, M. O'Neill and W. Liu, "A Dynamically Configurable PUF
625 and Dynamic Matching Authentication Protocol," *IEEE Transactions on Emerging Topics in*
626 *Computing* (Early Access).

[8] F. Farha, H. Ning, K. Ali, L. Chen and C. Nugent, "SRAM-PUF-Based Entities Authentication Scheme for Resource-Constrained IoT Devices," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5904-5913, 1 April1, 2021.

[9] Grossi, M., Alfonsi, F., Prandini, M., & Gabrielli, A. (2023). A Highly Configurable Packet Sniffer Based on Field-Programmable Gate Arrays for Network Security Applications. *Electronics*, *12*(21), 4412.

[9] S. Ghosh, "Spintronics and Security: Prospects, Vulnerabilities, Attack Models, and Preventions", in *Proc. of the IEEE*, Vol. 104, No. 10, October 2016, pp. 1864-1893.

[11] J. Moon, I. Y. Jung, J. H. Park, "IoT application protection against power analysis attack", *Computers & Electrical Engineering*, *67*, 2018, pp. 566-578.

[12] Y. Tian, Q. Li, J. Hu, H. Lin, "Secure limitation analysis of public-key cryptography for smart card settings", *World Wide Web*, *23*(2), 2020, pp. 1423-1440.

[13] J. Delvaux, R. Peeters, D. Gu, I. Verbauwhede, "A Survey on Lightweight Entity Authentication with Strong PUFs", *ACM Computing Surveys*, Volume 48, Issue 2November 2015, pp. 1-42.

[14] S. Qiu, G. Xu, H. Ahmad, L. Wang, "A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems", *IEEE Access*, *6*, 2017, pp. 7452-7463.

[15] R. Maes, "Physically unclonable functions: constructions, properties and applications", Springer, Berlin, 2013.

[16] T. Xu, J. B. Wendt, M. Potkonjak, in Security of IoT systems: design challenges and opportunities. *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2014, pp. 417–423.

[17] B. Halak, "Physically Unclonable Functions: From Basic Design Principles to Advanced Hardware Security Applications", Springer, Cham, 2018.

[18] M. T. Rahman, F. Rahman, D. Forte, M. Tehranipoor, "An aging-resistant RO-PUF for reliable key generation", *IEEE Transactions on Emerging Topics in Computing*, *4* (3), September 2016, pp. 335-348.

[19] P. Saraza-Canflanca, H. Carrasco-Lopez, A. Santana-Andreo, P. Brox, R. Castro-Lopez, E. Roca, F. V. Fernandez, "Improving the reliability of SRAM-based PUFs under varying operation conditions and aging degradation", Microelectronics Reliability, Elsevier, Volume 118, 2021.

[20] L. Kusters, F. M. Willems, “Secret-key capacity regions for multiple enrollments with an SRAM-PUF”, *IEEE Transactions on Information Forensics and Security*, *14* (9), 2019, pp. 2276-2287.

[21] S. Khan, A. P. Shah, S. S. Chouhan, N. Gupta, J. G. Pandey, S. K. Vishvakarma, “A symmetric D flip-flop based PUF with improved uniqueness”, Microelectronics Reliability, Elsevier, Volume 106, 2020, 113595.

[22] Z. He, W. Chen, L. Zhang, G. Chi, Q. Gao, L. Harn, “A highly reliable arbiter PUF with improved uniqueness in FPGA implementation using Bit-Self-Test”, *IEEE Access*, *8*, 2020, pp. 181751-181762.

[23] D. Deng, S. Hou, Z. Wang, Y. Guo, “Configurable ring oscillator PUF using hybrid logic gates”, *IEEE Access*, *8*, 2020, pp. 161427-161437.

[24] S. Hemavathy, S., V.K. Bhaaskaran, “Arbiter PUF-A Review of Design, Composition, and Security Aspects”, *IEEE Access*, 2023, 33979-34004.

[25] J.W. Lee, D. Lim, B. Gassend, G.E. Suh, M. Van Dijk, S. Devadas, “A technique to build a secret key in integrated circuits for identification and authentication applications”, *IEEE Symposium on VLSI Circuits. Digest of Technical Papers*, 2004, 176-179.

[26] F. Kodýtek, R. Lórencz, “A design of ring oscillator based PUF on FPGA”, *IEEE 18th International Symposium on Design and Diagnostics of Electronic Circuits & Systems*, 2015, 37-42.

[27] C. Liu, Y. Cao, C. Chang, “ACRO-PUF: A Low, Reliable and Aging-Resilient Current Starved Inverter-Based Ring Oscillator Physical Unclonable Function”, IEEE Trans. On Circuits and Systems-I, Vol. 64, No. 12, Dec. 2017, pp. 3138 – 3149.

[28] M.S. Mispan, B. Halak, M. Zwolinski, “NBTI Aging Evaluation of PUF-based Differential Architectures”, *IEEE 22nd International Symposium on On-Line Testing and Robust System Design (IOLTS),* 2016, 103-108.

[29] A. Maiti, P. Schaumont, “The Impact of Aging on a Physical Unclonable Function”, *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *22 (7)*, 2014, pp. 1854-1854.

[30] M. Grossi, M. Omaña, D. Rossi, B. Marzulli, C. Metra, “Novel BTI Robust Ring-Oscillator-Based Physically Unclonable Function”, *IEEE 28th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, 2022, pp. 1-7.

[31] M. Omaña, D. Rossi, T. Edara, C. Metra, “Impact of aging phenomena on latches’ robustness”, *IEEE Transactions on Nanotechnology*, *15* (2), 2016, pp. 129-136.

[32] M. Grossi, M. Omaña, “Impact of Bias Temperature Instability (BTI) Aging Phenomenon on Clock Deskew Buffers”, *Journal of Electronic Testing*, *35* (2), 2019, pp. 261-267.

[33] K. Joshi, S. Mukhopadhyay, N. Goel, S. Mahapatra, “A consistent physical framework for N and P BTI in HKMG MOSFETs”, *IEEE international reliability physics symposium (IRPS)*, 2012, pp. 5A-3.

[34] M. Grossi, M. Omaña, “Investigation of the Impact of BTI Aging Phenomenon on Analog Amplifiers”, *Journal of Electronic Testing*, 37 (4), 2021, pp. 533-544.

[35] H. I. Yang, W. Hwang, C. T. Chuang, “Impacts of NBTI/PBTI and contact resistance on power-gated SRAM with high-k metal-gate devices”, *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *19* (7), 2010, pp. 1192-1204.

[36] S. M. Ramey, C. Prasad, A. Rahman, “Technology scaling implications for BTI reliability”, *Microelectronics Reliability*, *82*, 2018, pp. 42-50.

[37] D. Rossi, M. Omaña, C. Metra, A. Paccagnella, “Impact of Bias Temperature Instability on Soft Error Susceptibility”, *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* Vol. 23, Issue 4, April 2015, pp. 743 – 751.

[38] G. E. Suh and S. Devadas, ``Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Design Autom. Conf. (DAC)*, Jun. 2007, pp. 9_14.

[39] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, ``Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126_1141, Aug. 2014.

[40] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, ``Extended abstract: The butter_y PUF protecting IP on every FPGA," in *Proc. IEEE Int. Workshop Hardw.-Oriented Secur. Trust*, Jun. 2008, pp. 67_70.

[41] Predictive Technology Model (PTM). Available online: http://ptm.asu.edu (accessed on 10 February 2022).

[42] B. Tudor, J. Wang, W. Liu, H. Elhak, “MOS Device Aging Analysis with HSPICE and CustomSim”, Synopsys, 2011.

[43] Y. Hori, T. Yoshida, T. Katashita, A. Satoh, “Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs”, in Proc. of IEEE Int. conf. on reconfigurable computing and FPGAs, 2010, pp. 298-303.

[44] M. Omaña, D. Rossi, N. Bosio, C. Metra, "Self-Checking Monitor for NBTI Due Degradation", in *Proc. of the 2010 IEEE 16th International Mixed-Signals, Sensors and Systems Test Workshop, IMS3TW*, 2010.

[45] M. A. Alam, H. Kufluoglu, D. Varghese, S. Mahapatra, "A comprehensive model for PMOS NBTI degradation: Recent progress", *Microelectronics Reliability*, 47 (6), 2007, pp. 853-862.

MARTIN OMAŃA is a Contract Professor at the University of Bologna, Italy, He received the Degree in electronic engineering from the University of Buenos Aires in 2000 and the Ph.D. in electronic engineering and computer science from the University of Bologna, Italy, in 2005. His research interests are in the field of the design of approaches oriented to the on-line test, robust design, fault-tolerance and hardware security of digital circuits and systems, as well as on the design of efficient and reliable power systems.

MARCO GROSSI received the Laurea degree in electronic engineering from the University of Bologna, in 2000 and the Ph. D. degree in 2004. He is currently a post-doctoral fellow at the Department of Electronics, University of Bologna. He is involved in projects of innovative sensors for bacterial detection, characterization of food samples by electrical impedance spectroscopy and development of microcontroller based embedded sensor systems. He is co-author of more than 50 publications, most of which on internationally indexed peer-reviewed journals.

DANIELE ROSSI (Senior Member, IEEE) received the MSc degree in electronic engineering and the Ph.D. degree in electronics and computer engineering from the University of Bologna, Bologna, Italy, in 2001 and 2005, respectively. He is currently an Associate Professor in Electronics with the Department of Information Engineering, University of Pisa, Italy. His current research interests include hardware security, energy efficient and reliable digital design, and robust design for soft error and aging resiliency. Dr. Rossi has co-authored over 100 papers published in international journals and conference proceedings, has served as Technical Program Committee member for numerous international conferences in the field of electronic design and test, and is a member of the Editorial Board of several international journals.

CECILIA METRA (Fellow, IEEE) is a Full Professor in Electronics at the University of Bologna, Italy, where she received the Ph.D. in Electronic Engineering and Computer Science, and where she is Deputy President of the Engineering School. In 2002, she was a Visiting Faculty Consultant for Intel Corporation in the USA. She is 2022-2023 IEEE Director, Division V. She was the 2019 IEEE Computer Society President. She was the Editor in Chief of the "IEEE Transactions on Emerging Topics in Computing" (2018, 2020) and "Computing Now" (2012-2016), and she is a member of the Editorial Board of several international Journals. She has been involved in the organization of several IEEE sponsored Symposia/Workshops. Her research interests are in the field of test and design for test of electronic circuits/systems, reliable, safe, secure and resilient electronic circuits/systems, trustworthy AI circuits/systems, fault tolerance, error correcting codes, secure communication protocols, photovoltaic systems, emerging technologies. She is an IEEE Fellow, an IEEE Computer Society Golden Core member, and a member of the IEEE honor society Eta Kappa Nu.