Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2024.0429000

sThing: A Novel Configurable Ring Oscillator based PUF for Hardware-Assisted Security and Recycled IC Detection

SASWAT KUMAR RAM[1], (Senior Member, IEEE), SAUVAGYA RANJAN SAHOO[2], BANEE BANDANA DAS [3], (Member, IEEE), KAMALAKANTA MAHAPATRA, [4], (Senior Member, IEEE), and SARAJU P. MOHANTY, [5], (Senior Member, IEEE)

[1]Department of Electronics and Communication Engineering, SRM University, Andhra Pradesh, India (e-mail: saswatram01@gmail.com)
[2]Analog Design Engineer, Marquee Semiconductor, India. (e-mail: sauvagya.nitrkl@gmail.com)
[3]Department of Computer Science and Engineering, SRM University, Andhra Pradesh, India. (e-mail: banee.bandana@gmail.com)
[4]Department of Electronics and Communication Engineering, National Institute of Technology, Rourkela,India. (e-mail: kkm@nitrkl.ac.in)
[5]Department of Computer Science and Engineering, University of North Texas, Denton, TX. (e-mail: saraju.mohanty@unt.edu)

Corresponding author: Banee Bandana Das (e-mail: banee.bandana@gmail.com).

ABSTRACT Ring Oscillator (RO) is widely used to address different hardware security issues. For example, the RO-based physical unclonable function (PUF) generates a secure and reliable key for the cryptographic application, and the RO-based aging sensor is used for the efficient detection of recycled ICs. In this paper, a conventional CMOS inverter with two voltage control signals is used to design a configurable RO (CRO). With its control signals, the proposed CRO can perform both i.e., accelerate or lower the impact of aging on the oscillation frequency. Due to this vital feature of the proposed CRO, it can be used in PUF and RO-based sensors. The performance of both the proposed modified architecture, i.e., CRO PUF and CRO sensor, is evaluated in 90 nm CMOS technology. The aging tolerant feature of the proposed CRO enhances the reliability of CRO PUF. Similarly, the aging acceleration property of CRO improves the rate of detection of recycled ICs. Finally, both the proposed architectures are area and power-efficient compared to conventional architectures.

INDEX TERMS Aging, Bit Error Rate (BER), Challenge-Response pair (CRP), Configurable Ring Oscillator (CRO), Physically Unclonable Functions (PUFs), Process Variation (PV), Recycled IC

I. INTRODUCTION

IN this current era of technology, the security of IC along with its power, performance, and area becomes more critical due to IoT, IoE [1], [2], globalization of Semiconductor Companies, etc. So, the communication among several electronic systems in a group must be reliable and safe from the attack by adversaries. A malfunction due to a malicious attack on any device may propagate among the group and lead to the failure of the whole system. Further, globalization and complexity in the IC supply chain led to the presence of counterfeited IC [3] by the untrusted foundry, untrusted supplier, etc., which is also related to the security of IC. A Counterfeit IC may be a tampered, cloned, copied, overproduced, or recycled IC. The report in [4], [5], indicates a revenue loss of U.S. $169 billion to chip makers due to these counterfeited ICs. Although these ICs function properly their reliability is questionable. This scenario is a matter of concern in critical applications like aerospace, defense, lifesaving appliances, etc. As reported in [5], out of several types of counterfeited IC, a major share is occupied by recycled ICs. So during the design and fabrication of ICs, security issues must be addressed along with its VLSI metrics like power, performance, and area. Although there are several security-related issues associated with IC manufacturing [6], in this research work, two major issues are being addressed i.e.

1) Highly reliable crypto key generation using PUF.
2) Efficient detection of recycled IC using RO sensor.

A. RELIABLE KEY USING PUF

The conventional approach includes storing of crypto-key in an external ROM. This approach is vulnerable to attack from adversaries [7], area overhead, and higher power consumption due to bulky ROM architecture. As a solution, in the last decade, PUF [8] has emerged as a promising breakthrough in generating secure keys. PUF explores the secret of the inherent manufacturing PV [8], which is difficult to clone or model. This manufacturing PV is a unique phenomenon, which produces a difference in behavior between two identical ICs fabricated by the same designer in the same foundry using the same process technology. PUF [8]–[11], [42] gener-

ates the key only when it is powered up, in contrast to memory where the secure key is stored in ROM. Further, any attack on PUF to leak the key led to permanent damage to PUF functionality.

A PUF is characterized by different security metrics [10] like uniqueness, reliability, uniformity, strict avalanche condition (SAC), etc. These metrics are measured by collecting a group of response bits (called secure keys) from PUF after applying a set of challenges. These challenges and corresponding responses are termed challenge-response pairs (CRPs). Uniqueness is a measure of the variation among the response bits when the same challenge pattern is applied to different instances of the same PUF. It measures how two or more instances of the same PUF, differ from each other. Reliability measures, how efficiently a PUF can re-produce the secure key against temperature variation, aging, etc. In this work, the main objective is to design a PUF with higher reliability, i.e. to lower the impact of aging, and temperature variation on response bit. So, the generated key must be highly resilient against temperature variation or aging.

B. RECYCLED IC

A recycled IC is generally a removed IC from an obsolete PCB or electronics system, which undergoes cleaning, remarking, repackaging, and sold as a new one [3], [12], [13]. The aging of an IC is a slow but continuous process. It becomes severe at lower technology nodes; hence, a used or recycled IC experiences higher degradation in its aging-dependent parameter as compared to a fresh or unused IC. Several circuit-level techniques were proposed in the literature to accelerate this aging mechanism for efficient detection of recycled ICs.

In literature [8], [10]–[13], several circuit-level techniques are proposed to address both these security issues. Different types of PUFs with temperature and aging compensation circuits are proposed to generate highly reliable response bits. Similarly, the recycled IC detection approach uses lightweight aging sensors using RO [13] to predict the amount of aging experienced by the IC under test. Based on the prior research works it can be identified that the common issues related to PUF and sensors are; the impact of aging on PUF must be lowered to improve its reliability and simultaneously, the aging must be accelerated to improve the rate of detection of recycled IC by sensor. Based on these challenges, and focusing on area and power-efficient design, the objective of this research work includes:

1) To design a configurable ring oscillator (CRO), which can enable both acceleration and retardation of aging depending on its application as sensor and PUF respectively.
2) The proposed PUF must be highly reliable, and the proposed sensor also improves the rate of detection of recycled IC compared to conventional existing architectures.

The rest of this paper is organized as follows. Section II summarizes the prior research work on different types of RO-based PUF, RO sensors, and the scope for further improvement. The novel contribution of the current research work to the state of the art is presented in Section III. The proposed CRO architecture and its functionality are briefed in Section IV. Section V, presents the application of proposed CRO as PUF and sensor. The results and discussions are presented in Section VI, and a comparison summary is outlined in Section VII. Finally, this research work is concluded in Section VIII.

II. RELATED PRIOR WORKS

In the last decade, researchers have worked on the design of different types of PUF, recycled IC detection circuits, and different techniques to improve its performance are proposed in the literature. For PUF [10], [11], the proposed techniques aim at improving its VLSI and security metrics. Similarly, lightweight RO sensor [13] is used to improve the rate of detection of recycled ICs. Further, it is observed, that the ring oscillator is one of the most suitable primitives found in both PUF and sensor circuits. The reason to use RO is:

- Simple architecture, only cascaded inverter.
- Oscillation frequency is explored by PV, hence suitable for design of PUF.
- Finally, aging also affects the oscillation frequency. Hence, it is easy to design either aging tolerant or aging accelerated RO depending on its application as PUF or sensor respectively.

This section is segregated as follows:

- First, different types of RO-based PUF topology, and modified RO architecture to improve its reliability are briefed.
- Second, authentication of recycled ICs using conventional RO sensors, and aging accelerated mechanism to improve its rate of detection.
- Finally, the scope for further improvement in RO-based PUF and sensors is also briefed.

A. PUF AS A SECURITY PRIMITIVE

All the existing PUF architectures are divided into silicon or non-silicon-based PUFs [11]. The major Si-PUF architecture includes delay-based PUF like RO PUF, arbiter PUF, CRO PUF, ARO PUF, etc., and memory-based PUF like SRAM PUF, Flip Flop PUF, etc. [14]–[20], [43]. These are also validated in both FPGA and ASIC platform. In this paper, the discussion is limited to one of the most widely used delay-based Si-PUF i.e. RO PUF. The reason to choose RO PUF is because of its simple architecture for CRP collection and it can be easily embedded with other functional units to provide security primitive with a highly reliable response bit.

Different RO PUF topologies along with their advantages and constraints are briefed in TABLE 1. A conventional RO PUF [15] architecture consists of a group of RO, and a frequency comparison module, as shown in Fig. 1. All the ROs are designed with an equal number of cascaded inverters to oscillate at the same frequency. However, the manufacturing PV causes each RO to oscillate at slightly different frequencies. The frequency difference in any pair of RO is measured

by applying a set of challenges, and the corresponding logic level of response bit (R) is given by equation 1,

$$R = \begin{cases} 1, if \quad f_1 > f_2 \\ 0, otherwise \end{cases} \tag{1}$$

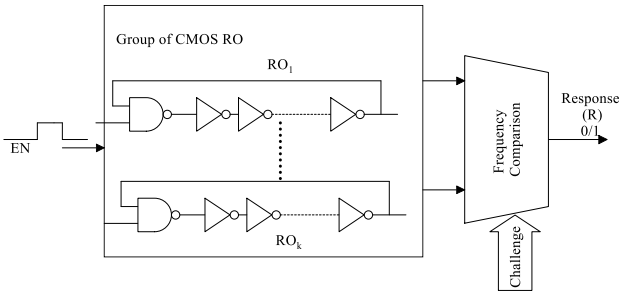
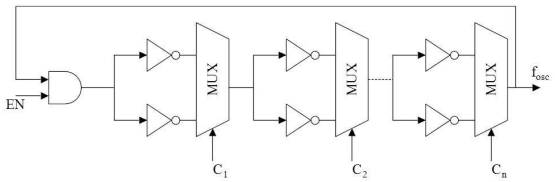
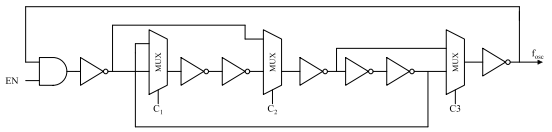


FIGURE 1: Conventional RO PUF [15].

As briefed in TABLE 1, the RO section of RO PUF is replaced by CRO, to make it both area and power-efficient. The corresponding PUF is called CRO PUF [18]. A conventional CRO architecture consists of either a two-row of inverter [18] or a single row of inverter with cascaded MUX is depicted in Fig. 2a and Fig. 2b). A CRO with n-selection line (C_1, C_2,.....C_n: challenges applied to MUX) is configured as $2n$ number of different RO. Hence, both the CRO [18] are area-efficient.



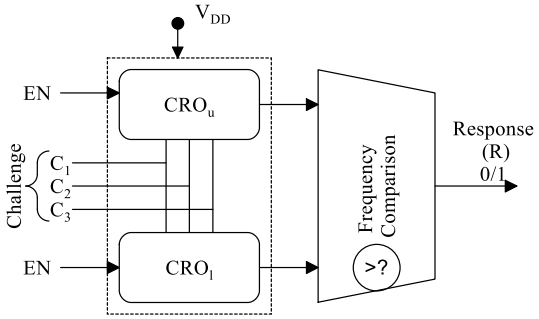
(a) Two row cascaded inverter



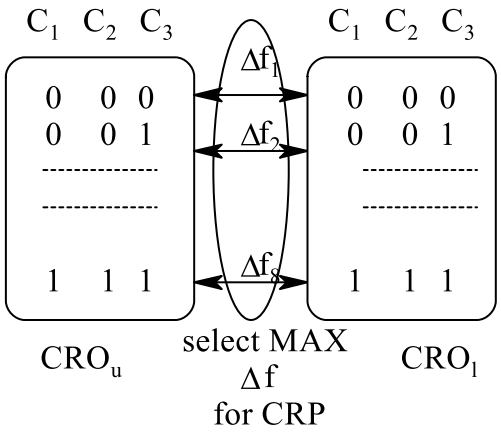
(b) Single row cascaded inverter

FIGURE 2: Conventional CRO.

A conventional CRO PUF [18] with response bit collection approach is shown in Fig. 3a and Fig. 3b. Each set of applied challenge patterns (C_1,C_2, C_3) results in an RO with a unique oscillation frequency due to PV. The frequency comparison between the RO in CRO_u and CRO_l is carried out. A pair of RO with maximum frequency separation is considered to measure response bit and is depicted in Fig. 3b). Although, this CRO PUF results in highly reliable response bits along with both power and area-efficient features (due to reduction in the number of RO), the vulnerability of oscillation frequency against temperature variation [15], and aging [21],



(a) Conventional CRO PUF



(b) CRP collection approach

FIGURE 3: Conventional CRO PUF with response collection.

[22] also affect its reliability. The cause and corresponding mitigation techniques are discussed further.

1) PUF Reliability: Cause and Mitigation Technique

The reliability of PUF is influenced by various factors and it should be mitigated. A detailed discussion on factors causing reliability degradation and proper mitigation is discussed below.

Cause:

The expression for oscillation frequency (f_{osc}) of a RO [15] is given as follows in equation 2,

$$f_{ossc} = \frac{1}{2mt_p} \tag{2}$$

Where, m is the number of the cascaded inverter, t_p is the delay of each inverter. Different environmental effects like temperature variation or aging affect the threshold voltage (V_{th}) of MOS leading to degradation in f_{ossc} (t_p=f(V_{th}) [23]), as shown in Fig. 4 (a). Hence, the possibility of frequency crossover in a pair of RO (with small frequency separation) increases either at higher temperature (T) or over a while (t) due to aging, as shown in Fig. 4 (b). As a result, a flip in response bit (0 to 1 or 1 to 0) occurs, which leads to overall reliability degradation of PUF. This type of degradation is temporary against temperature variation, and PUF can restore

its original reliability once the temperature becomes normal. However, aging causes slow but permanent degradation in the V_{th} of MOS [24], leading to permanent degradation in the reliability of PUF.

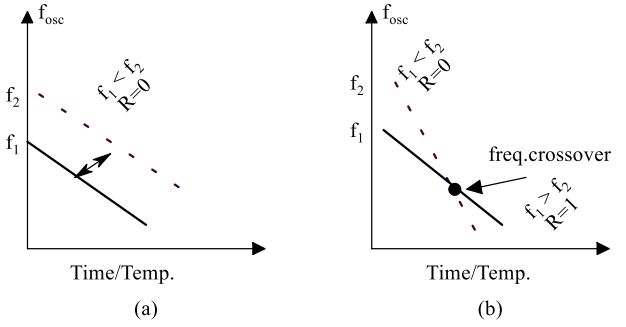


FIGURE 4: Reliability degradation (a) No Crossover: Pair of RO with higher frequency separation (b) frequency cross over at higher Temperature/Time [15].

The threshold voltage degradation due to NBTI as compared to well-known aging mechanisms like [24] bias temperature instability (BTI), hot carrier injection (HCI), electromigration, etc., is very severe in the case of RO. The RO with only powered ON (non-oscillation mode) experiences frequency degradation due to NBTI [25]–[28]. The impact of NBTI on a conventional CMOS RO is shown in Fig. 5 (a). Half of the PMOS with a negative gate-to-source bias ($V_{GS,P} = -V_{DD}$) experience NBTI. The magnitude of this negative bias determines the rate of degradation in threshold voltage of PMOS [24], which leads to an overall degradation in the oscillation frequency of RO. Further, this rate of degradation increases with an increase in aging over some time [24]. Hence, the design of NBTI resilient RO is more important, to restore the reliability of PUF.

From the above discussion, it can be summarized as, an RO with lower frequency deviation against temperature variation, or aging lowers the possibility of frequency crossover, causing improvement in the overall reliability of PUF.

Mitigation Technique:

Several mitigation techniques [28]–[31] to restore the reliability of RO PUF against both temperature variation and aging are briefed in TABLE 1. All these proposed techniques try to lower the frequency deviation. Among different architectures, a few NBTI tolerant RO [28], [31] are shown in Fig. 5b and Fig. 5c. Both these NBTI tolerant RO reduce the impact of NBTI by lowering the negative bias across PMOS in non-oscillation mode as follows:

- In Aging tolerant RO (ARO [28], [29]), the added NMOS (T_N) to the input of each cascaded inverter lowers the $V_{GS,P}$ across all the PMOS from $-V_{DD}$ (in conventional CMOS RO) to $-V_{t,n}$.
- However, the most recent RO proposed in [30], [31], uses additional NMOS to drive the RO. In this technique, the NMOS (T_N) remains in the cut-off region during the non-oscillation mode. As a result, all the PMOS remains free from negative bias. This architecture further lowers the impact of NBTI.
- Further, both these modified ROs also lower the frequency deviation against temperature variation.

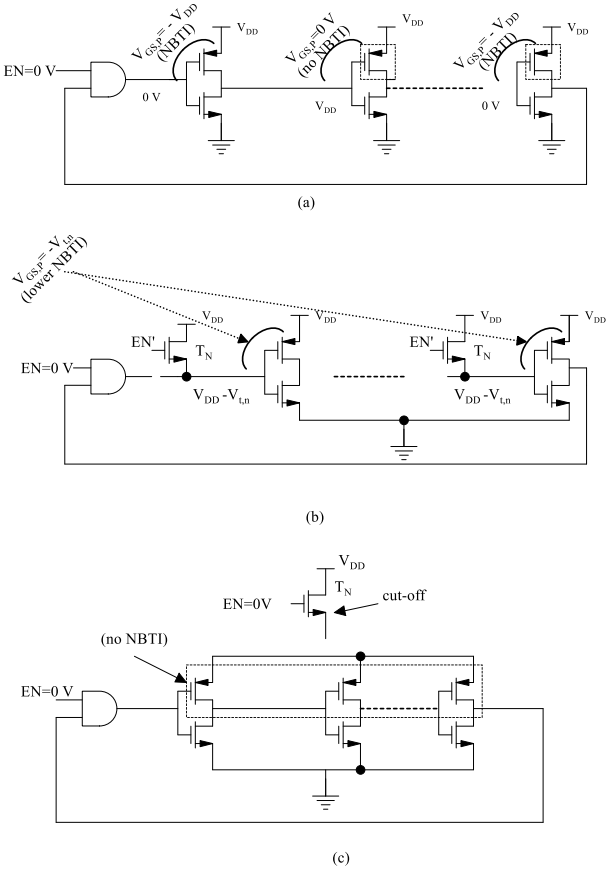


FIGURE 5: NBTI stress on different types of RO (a) CMOS RO [15] (b) ARO [28] (c) RO with reduced supply voltage [31].

B. RECYCLED IC DETECTION

Different RO sensors proposed in the literature for the detection of recycled IC are briefed in TABLE 1. A conventional RO sensor architecture [13] is shown in Fig. 6, and its functionality is given in TABLE 2. It consists two identical RO, i.e. reference RO ($(RO)_{REF}$) and stressed RO ($(RO)_{STR}$). The control module generates necessary control signals to drive both the RO either into stress or authentication phase as described in TABLE 2. The registration and authentication of a recycled IC in a group of similar ICs is briefed as follows:

- First, both the RO must be designed to oscillate at the same frequency. So, the frequency difference between both the RO, $F_{DIF} = F_{REF} - F_{STR}$ must be zero (indicates new/fresh IC).
- However, due to inherent manufacturing variation F_{DIF} is slightly positive or negative, as shown in Fig. 7. The mean (μ) of the spread for a group of fresh IC i.e. F_{fresh} is centered at zero.

- In the stress phase, the NBTI stress on $(RO)_{STR}$ is accelerated, and at the same time $(RO)_{REF}$ is made stress free. So, higher degradation in the oscillation frequency of $(RO)_{STR}$ as compared $(RO)_{REF}$ is observed. This different amount of degradation affects the magnitude of F_{DIF}. As a result, with an increase in stress duration F_{DIF} increases, and the spread of F_{DIF} for used IC (F_{aged}) is shifted towards right from its fresh value (Fig. 7). The higher the impact of NBTI on $(RO)_{STR}$, the higher the magnitude of F_{DIF}, and more shift in F_{aged} towards the right.
- The region of overlap between the two spreads indicates the percentage of misprediction (% m) i.e. in this region, it is difficult to decide whether the IC under test is a fresh or recycled one.

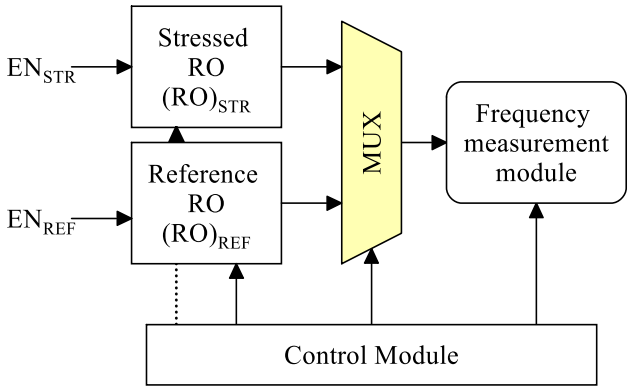


FIGURE 6: Conventional RO sensor [13].

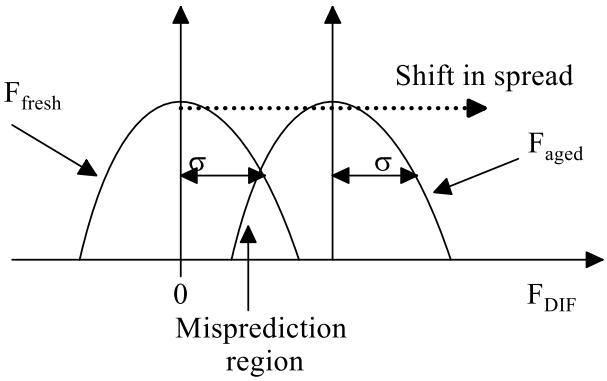


FIGURE 7: Spread of F_{DIF} [32].

This % m is used as a performance evaluation metric for RO sensors. For efficient detection of recycled IC, the corresponding sensor must possess the lower value of % m i.e. narrow region of misprediction. Hence, both the spread i.e. F_{fresh} and F_{aged} must be narrow, and far apart from each other. It can be achieved as follows:

- By accelerating NBTI stress: - With the increase in NBTI stress, more degradation in the oscillation frequency of $(RO)_{STR}$ is observed. As a result, F_{aged} shifted more towards the right from its original value (F_{fresh}), leading to a reduction of overlapped regions.
- By increasing the number of RO:- The spread (σ) of F_{DIF} depends upon the number of RO (N) [32], used as a reference and stress RO. From (3), with an increase in the number of RO, the spread (σ_N) of both F_{fresh} and F_{aged} becomes narrow. As a result, % m is reduced.

$$\sigma_N = \frac{\sigma}{N} \tag{3}$$

The light-weight AN-CDIR sensor proposed in [32] uses the above two methodologies to improve % m. The architecture, registration, and authentication flow of AN-CDIR is similar to conventional RO sensor [13] with the following modification to improve the % m as follows:

- Both reference and stressed modules consist of a group of RO rather than a pair of $(RO)_{REF}$ and $(RO)_{STR}$ [13]. With the increase in the number of RO in both the modules, the spread of F_{DIF} becomes narrow (from equation 3) leading to improvement in % m.
- Further, to accelerate the NBTI stress, the conventional CMOS RO [13] in both the module replaced by NBTI-aware RO [32]. Fig. 8 shows, how the conventional CMOS RO architecture is modified to accelerate the NBTI stress. In NBTI-aware RO, all the PMOS experience NBTI stress, as compared to half in the CMOS inverter (shown in blue color) by using a pass transistor logic (PTL) based switch and a pulldown NMOS. The PTL breaks the connection between each cascaded inverter, and NMOS is controlled externally to drive negative bias ($V_{GS,P} = -V_{DD}$) across all the PMOS during the non-oscillation mode of RO. As a result, higher degradation in oscillation frequency is observed as compared to conventional CMOS RO.

The use of a large number of NBTI-aware RO in both reference and stress modules of AN-CDIR [32] lowers the % m, i.e. it can detect the ICs used for a few days only. Although, it improves % m, but presence of a large number of RO led to area overhead.

III. NOVEL CONTRIBUTIONS OF THE CURRENT PAPER TO THE STATE OF ART

A. RESEARCH QUESTIONS AND FINDINGS

By observing all the existing research work on CRO PUF, and RO sensors, this section is summarized as follows:

- For CRO PUF, post-fabrication information on oscillation frequency is required to find out a pair of RO with maximum frequency separation.
- Underutilization of available RO: Only a pair of RO with maximum frequency separation in a group of 2n number of RO is used to generate a reliable response bit.

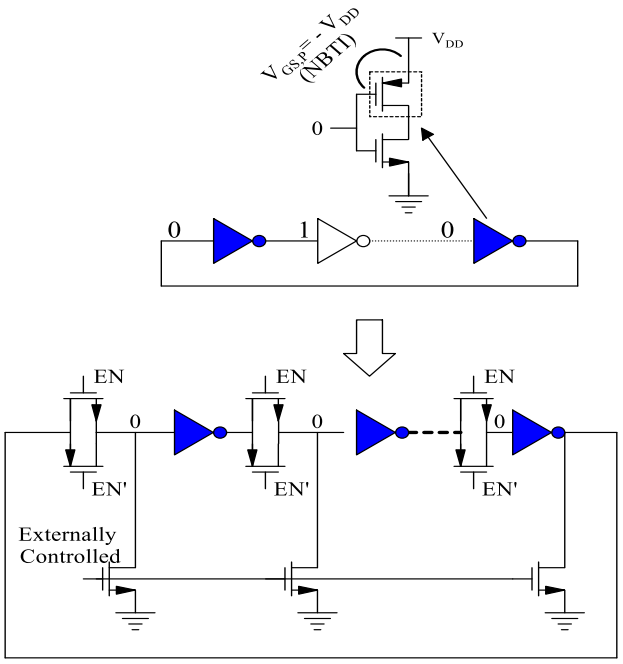


FIGURE 8: Circuit technique to accelerate NBTI stress on each inverter [32].

- Area inefficient: The number of MUX in the cascaded architecture increases [18], [31], with an increase in the number of CRO, leading to area overhead.
- All the existing RO is not suitable for both PUF and sensor applications. The existing RO can either accelerate the aging (used in the sensor) or lower the aging (used in PUF) but not both.
- Finally, the use of a large number of NBTI-aware RO in AN-CDIR [32], achieves improvement in % m at the cost of area overhead.

B. RESEARCH DIRECTIONS AND SCOPE FOR FURTHER IMPROVEMENTS

Although both the conventional CRO PUF and RO sensor are suitable to address different hardware security issues, the scope for further improvement is as follows:

- Design of RO with further reduction in frequency deviation. This eliminates the need for post-fabrication information on oscillation frequency and efficient utilization of all possible pairs of RO to generate reliable CRPs.
- Design of area-efficient CRO by eliminating MUX.
- Design of a RO with both aging acceleration and retardation properties, to make it suitable for both PUF and sensor application.
- Finally, replacing the group of RO with CRO in the AN-CDIR sensor, makes the sensor architecture much more area-efficient without affecting its recycled IC detection capability.

C. PROPOSED SOLUTION OF THE CURRENT PAPER

This research work addresses all the above issues. The key features are:

- Design of a reconfigurable inverter. The added voltage control section configures the inverter to operate at different voltages.
- The cascaded combination of the proposed inverter without MUX behaves as CRO.
- The proposed CRO possesses both aging acceleration and retardation features.
- The application of the proposed CRO as PUF to generate reliable response and sensor for detection of recycled ICs.

D. NOVELTY OF THE PROPOSED SOLUTION

In this paper, the proposed architecture for configurable RO improves the different types of shortcomings associated with existing RO-based PUF and sensors. The distinct contribution of this research work includes:

1) Reconfigurable Inverter: The core of this proposed work is to design a reconfigurable inverter, which is a conventional CMOS inverter with a voltage control section. (The voltage control section is associated with two control inputs i.e. one for supply voltage V_{DD}, and another for *GND*. These two control signal configures four different set of operating voltages for the inverter.)
2) Area-efficient CRO: The proposed cascaded inverter with its voltage control input behaves as a CRO. Hence, area efficiency is due to the absence of MUX as in conventional CRO [18], [31].
3) Finally, the proposed CRO can achieve both features i.e. it can accelerate and lower the impact of aging depending on the logic level of control signals in the proposed inverter. (This feature makes it suitable for both applications i.e. in designing a reliable CRO PUF, and RO sensor with an improved rate of detection of recycled IC.)

The architecture, functionality, and application of the proposed CRO are briefed and discussed in subsequent sections.

IV. PROPOSED CRO (SECURE THINGS)

The block diagram of CRO designed by using a proposed inverter, is shown in Fig. 9. Although this architecture is similar to conventional RO (cascaded inverter only), two control signals (C_s and C_g) of each inverter section, configure this RO architecture to behave as CRO. This section briefs:

- Design of CRO using proposed inverter.
- Performance analysis of CRO i.e. impact of PV, aging, and temperature variation on the oscillation frequency of RO.

A. PROPOSED INVERTER

As per the research work in [30], the proposed inverter is driven by two voltage control sections. As shown in Fig. 10, the proposed architecture consists of a conventional CMOS

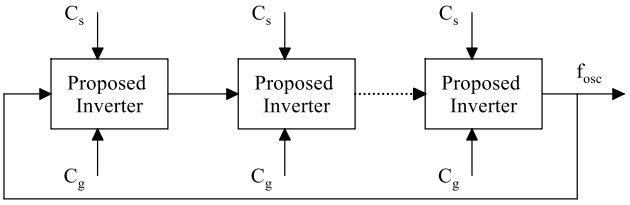


FIGURE 9: Block diagram of proposed CRO.

inverter with two voltage-control sections, one for supply voltage, and another for GND. The voltage control section consists of a transmission gate-based switch, but the gate terminal of both PMOS and NMOS is tied to the same control signal. The control signals C_s are used to limit the supply voltage into the PMOS (T_P) of the inverter, and the magnitude of *GND* voltage for the NMOS (T_N) of the inverter is controlled by C_g. Depending on the logic level at C_s and C_g, how the inverter is driven by a set of the different supply voltages (TABLE 3) is explained as follows:

- For logic-0 at C_s (T_{P1}: ON), the PMOS in the upper section (T_{P1}) drives a voltage of magnitude V_{DD} into the inverter section and for logic-1 (T_{N1}: ON), inverter operates at a reduced supply voltage determined by the threshold voltage of NMOS (T_{N1}) i.e. V_{DD} $V_{t,n}$.
- Similarly, a logic-1 at C_g (T_{N2}: ON), causes the CMOS inverter to be fully connected to *GND* (0 V) through T_{N2}, and logic-0 (T_{P2}: ON) rises the voltage at the source of T_N from 0 V to $V_{t,p}$ (threshold voltage of T_{P2}). For simplicity of analysis, it is assumed that $V_{t,p}$=$V_{t,n}$ =V_t.

As given in TABLE 3, all the possible combinations of C_s and C_g causes the inverter to operate at 4-different voltage pattern. Only the pattern [C_sC_g= 01], causes the proposed inverter to operate at a supply voltage similar to a conventional CMOS inverter. The remaining pattern reduces the rail-to-rail swing of operating voltage. This different swing of operating voltage for all 4-possible combination, affects delay (t_p), and power (P) consumption of inverter ($t_p, P = f(V_{DD})$ [23]). This feature makes the proposed inverter suitable to design CRO.

B. ARCHITECTURE OF PROPOSED CRO

The proposed CRO architecture is shown in Fig. 10. It consists of only a cascaded inverter, with C_s and C_g of the voltage control section behaving as a selection input. The different logic levels at C_s and C_g, configure the RO to oscillate at different oscillation frequencies. This is due to the different sets of operating voltage of each cascaded inverter (TABLE 3). The use of an inverter with a control signal eliminates the requirement of MUX as in conventional CRO [18]. As each inverter section consists of two selection lines, a CRO with m-cascaded inverter can be configured as 2^{2m} different RO.

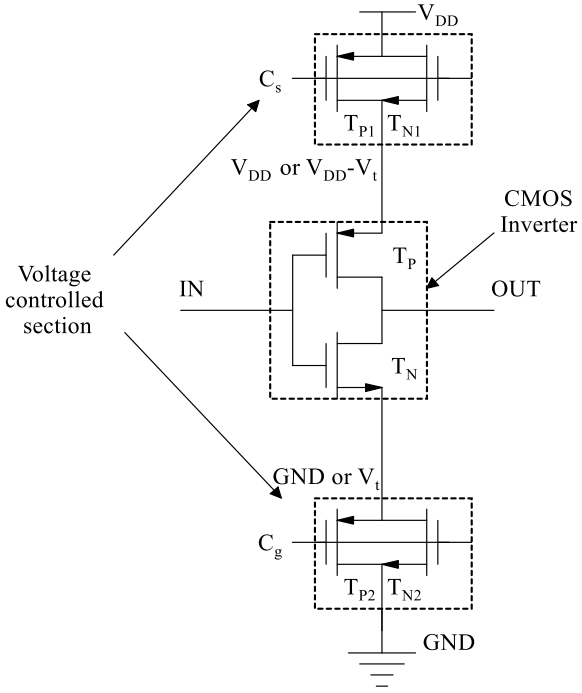


FIGURE 10: Proposed inverter.

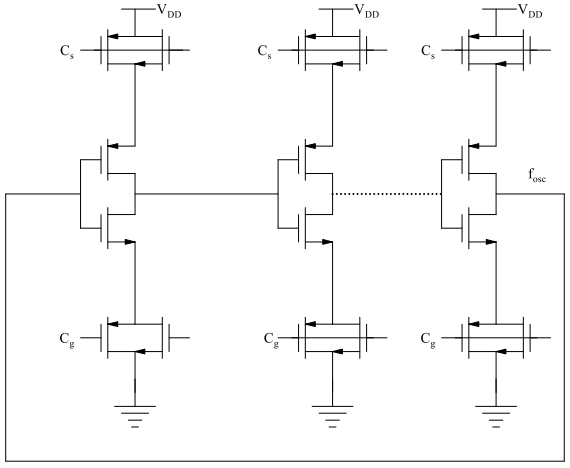


FIGURE 11: Proposed CRO.

C. PERFORMANCE ANALYSIS OF PROPOSED CRO

A CRO is characterized by its oscillation frequency. The impact of PV on oscillation frequency and frequency deviation (against temperature variation and aging) features makes the CRO appropriate for different applications like PUF, sensors, etc. This section discusses how the proposed CRO's oscillation frequency responds to temperature variation, aging, and PV, and further improvements against conventional CRO are summarized. A CRO with 3-stages of the cascaded inverter is considered in analyzing the oscillation frequency, as shown in Fig. 12. For analysis, C_s and C_g of each stage are connected. It results in a CRO, which operates at a 4-different supply

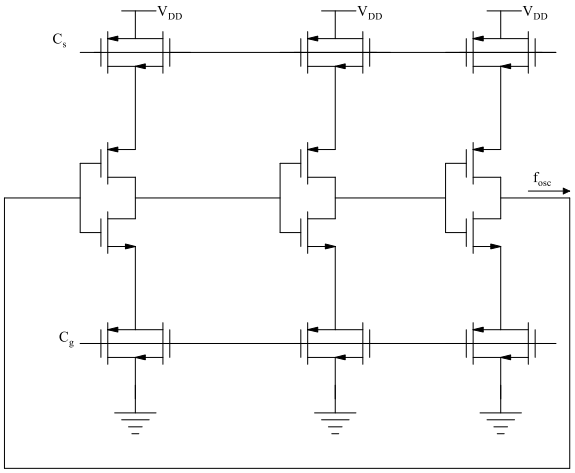


FIGURE 12: CRO with 3-stages of inverter.

voltage set (TABLE 3). The impact of temperature, aging, and PV on the oscillation frequency before fabrication is observed by using further analysis like Monte Carlo simulation, an aging model, etc.

1) Frequency deviation against temperature variation

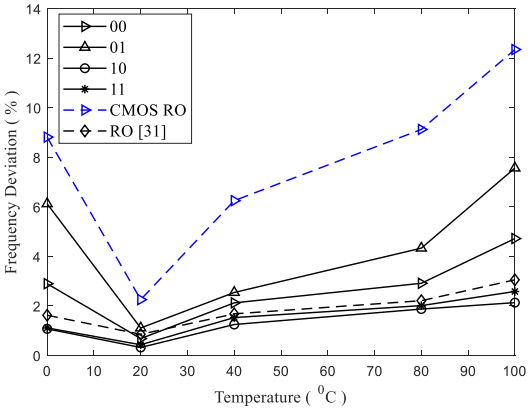
The frequency deviation is the variation in the oscillation frequency of RO from its original value i.e., measured at room temperature, given as presented in equation 4 [31],

$$\Delta f_{ossc}\,|_T = \frac{f_{ossc}\,|_{T=27^0C} - f_{ossc}\,|_{T=T}}{f_{ossc}\,|_{T=27^0C}} \tag{4}$$

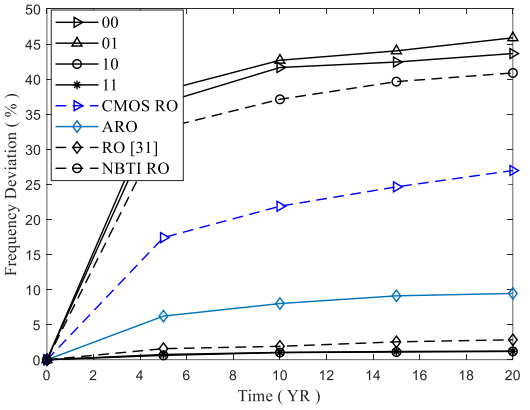
Where, $f_{ossc}\ |_{T=27^0C}$ is the original frequency of RO at room temperature, and $f_{ossc}\ |_{T=T}$ is the frequency measured at different value of temperature T.

The frequency deviation for all the possible combination of C_s and C_g i.e., 00,01,10, and 11 is observed over a variation in temperature from 0 to 100^oC, as shown in Fig. 13a. From this plot, it is observed that different logic levels of the control signal (C_s and C_g) result in different magnitudes of frequency deviation. For analysis, the frequency deviation of the proposed CRO is compared against all the existing types of RO, i.e., CRO [18], and RO with reduced supply voltage [31]. The result infers:

- All the 4-different input patterns in the proposed CRO result in different frequency deviations, but less than conventional CMOS inverter-based CRO [18].
- The input pattern for C_s at logic-1 (10,11) results in lower deviation as compared to C_s at logic-0 (00,01). This lower deviation is due to, a reduction in the operating voltage of the inverter from V_{DD} (C_s = 0) to V_{DD}– V_t (C_s = 1). Lower supply voltage reduces the oscillation frequency of RO and at the same time results in lower frequency deviation.
- The input pattern for C_s at logic-1 (10,11) results in lower deviation as compared to C_s at logic-0 (00,01). This lower deviation is due to, a reduction in the operating voltage of the inverter from V_{DD} (C_s = 0) to V_{DD}–V_t (C_s = 1). Lower supply voltage reduces the oscillation frequency of RO and at the same time results in lower frequency deviation.
- As the RO proposed in [31] operates at reduced supply voltage of V_{DD}–V_t, hence it shows less deviation from the input pattern 00 and 01.
- Finally, the maximum frequency deviation is reduced to 2 % (at 100^oC) for both the input pattern (10 and 11). As a result, the possibility of frequency crossover (Fig. 4) is minimized at higher temperatures, and the reliability of PUF against temperature variation is improved (briefed in Section VI).



(a) Frequency deviation against Temperature variation



(b) Frequency deviation against Aging

FIGURE 13: Frequency deviation against (a) Temperature variation (b) Aging.

2) Frequency deviation against aging

Similar to temperature, aging also causes continuous but permanent degradation in the oscillation frequency of RO. As discussed in Section II, NBTI is the primary aging mechanism, and the magnitude of negative bias across PMOS [24], [28] predicts the rate of degradation in the oscillation frequency of RO. The impact of NBTI on proposed RO for

two different logic levels of C_s is shown in Fig. 14a and Fig. 14b. The reason to choose C_s only is that it determines the magnitude of negative bias across all the PMOS in the 1^{st} row of the inverter. The different amounts of NBTI stress on PMOS for the different logic levels of C_s are briefed as follows:

- A logic-1 at C_s causes zero bias i.e. $V_{GS,P} = 0$ across all the PMOS in the 1^{st} row (Fig. 14a). As a result, all the PMOS experience a negligible amount of NBTI stress.
- As shown in Fig. 14b, a logic-0 at C_s cause, $V_{GS,P} = -V_{DD}$ across all the PMOS in the 1^{st} row of cascaded inverter. This higher amount of negative bias accelerates the NBTI stress.

These two different amounts of NBTI stress on the proposed CRO signify that it can achieve a different rate of degradation in oscillation frequency compared to conventional CMOS RO. The proposed CRO with C_s at logic-0 (all the PMOS experience NBTI) undergoes a higher degradation rate in oscillation frequency. The C_s at logic-1 (no PMOS experience NBTI) undergoes a lower degradation rate in oscillation frequency than conventional CMOS inverter-based RO used in [15], [18].

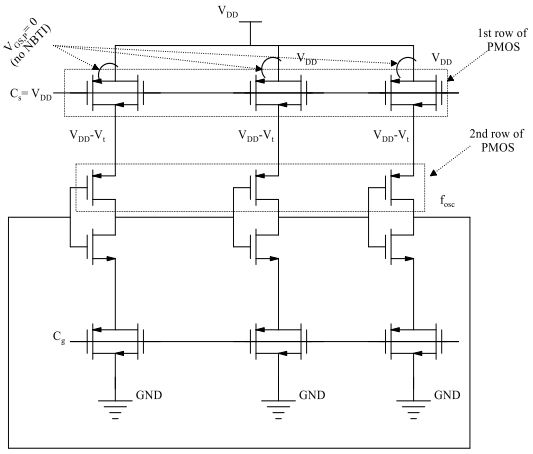
The frequency deviation in the proposed CRO due to aging is measured by using the expression in equation 5, and compared against ARO [28], RO with reduced supply voltage [31], CMOS RO [18], NBTI aware RO used in AN-CDIR [32]. The frequency deviation is the measure of degradation in oscillation frequency from time t=0 to throughout stress time (t), given as follows in equation 5:

$$\Delta f_{ossc}\,|_t = \frac{f_{ossc}\,|_{t=0} - f_{ossc}\,|_{t=t}}{f_{ossc}\,|_{T=0}} \tag{5}$$

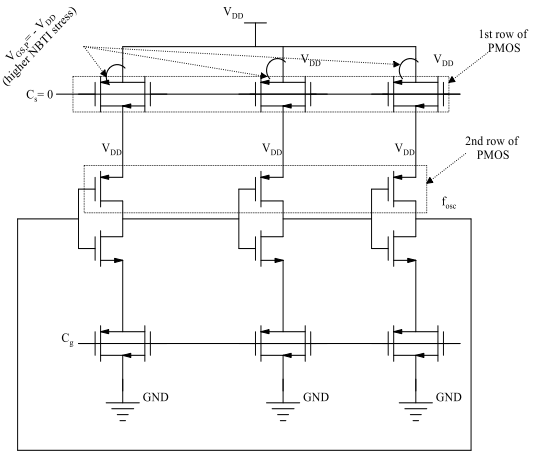
Where, $f_{ossc}\,|_{t=0}$ is the original frequency of RO, also called fresh frequency, and $f_{ossc}\,|_{t=t}$ is the frequency measured after a stress period t, called as aged frequency.

For analysis, the frequency deviation against aging is measured by applying stress continuously for 20-years (YR). The corresponding degradation in all considered RO is shown in Fig. 13b and summarized in TABLE 4. The comparison summary infers:

- Accelerated NBTI stress due to logic-0 at C_s (both 00 and 01), results in a higher rate of frequency degradation as compared to all the considered RO.
- Similarly, complete elimination of NBTI stress for logic-1 at C_s (both 10 and 11), results in a small deviation close to 1% and lower among all the considered RO.
- A larger difference in frequency deviation is observed for different logic levels of C_s (between [0X] and [1X]). However, the deviation is less dependent on the logic level of C_g ([C_s X]). This is due to the reduction in operating voltage of the inverter from V_{DD} to V_{DD}-V_t, when C_s switches from logic-0 to logic-1.



(a) NBTI stress is lowered



(b) NBTI stress is accelerated

FIGURE 14: Controlling NBTI stress through C_s (a) NBTI stress is lowered (b) NBTI stress is accelerated.

- Both the accelerated (for C_s= 0) and lower (for C_s= V_{DD}) aging feature of the proposed CRO led to 70 % higher degradation and 90 % lower degradation in oscillation frequency as compared to conventional CMOS based RO.
- Finally, the proposed CRO can lower the degradation by 60 % (for C_s= V_{DD}), and can accelerate the degradation by 12 % (for C_s=0) as compared to aging tolerant CRO [31] and aging accelerated RO [32] respectively.

From this above discussion, the unique feature of the proposed CRO is that it can perform both the task i.e., acceleration and retardation of aging for different logic levels of C_s.

3) Impact of PV on oscillation frequency

The variation in the oscillation frequency of RO against PV makes it suitable for application as PUF. A PUF explores inherent manufacturing variation to produce PV-dependent

response bits. The impact of PV on PUF quantifies its unique behavior. In conventional CRO PUF [18], the logic level of the response bit is determined from the oscillation frequency comparison. Hence, it is desired to observe how the manufacturing PV affects the oscillation frequency of the proposed CRO. Monte Carlo simulation is carried out to achieve it.

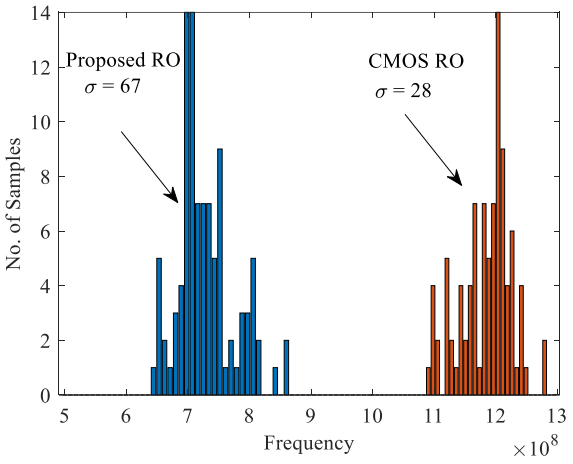


FIGURE 15: Impact of PV on f_{osc}.

For analysis, the oscillation frequency of the proposed RO is obtained for 100-iteration and compared against the conventional CMOS RO, as shown in Fig. 15. The bar chart confirms the higher impact of PV (higher value of σ) on the proposed RO's oscillation frequency compared to conventional CMOS RO. This is due to:

- CMOS RO oscillates at a supply voltage of V_{DD} resulting in lower variation (σ) across the collected frequency sample.
- However, the proposed RO oscillates at two different voltages, i.e. V_{DD} and V_{DD}-V_t (determined by C_s). This threshold voltage-dependent supply voltage i.e. V_{DD}-V_t, increases the variation among the different frequency components against PV. The average value of oscillation frequency in the proposed RO is lowered due to a reduction in supply voltage from V_{DD} to V_{DD}-V_t.

This section is summarized as follows:

- Large number of possible RO: With 3-stages of cascaded inverter, the proposed CRO can result in a maximum of 64-possible RO (2-selection lines per inverter: $2^{(2*3)}$=64 as compared to 8-possible RO (1-selection lines per inverter: $2^3 = 8$) in conventional CRO [18].
- The proposed CRO can achieve both i.e. acceleration and retardation of aging, hence suitable for both sensor and PUF applications.
- Finally, the proposed CRO is also both area and power-efficient due to the elimination of MUX and reduction in the swing of operating voltage.

V. APPLICATION OF PROPOSED CRO

As discussed above, the most crucial feature of this proposed CRO architecture is that it can perform both acceleration and retardation of aging simply by changing the logic level of the control signal (C_s and C_g). Hence, this proposed CRO architecture is suitable for the design of

- CRO PUF: Highly reliable against aging with area-efficient features.
- RO sensor: The accelerated aging property of the proposed CRO, enhances the rate of detection of recycled IC with less area overhead.

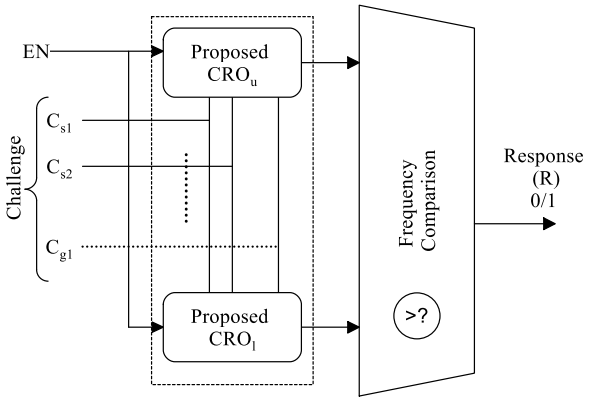


FIGURE 16: Proposed CRO PUF.

A. DESIGN OF CRO PUF

The architecture of the proposed CRO PUF is shown in Fig. 16. It consists of two CRO i.e., CRO_u and CRO_l, and a frequency comparison module to produce the response bit. Both the CRO module is designed by using the proposed CRO (Fig. 11). Further, the CRP collection approach of the proposed CRO PUF is similar to that of conventional CRO PUF.

In this PUF, different voltage control signal i.e., C_{s1}, C_{s2}, C_{g1}, C_{g2}.....etc., are treated as challenges. The logic level of the applied challenge pattern decides the operating voltage of each cascaded inverter in the proposed CRO and selects a pair of RO from CRO_u and CRO_l. The frequency comparison module produces a response bit of logic-1 or logic-0 depending on the magnitude of oscillation frequency. The important feature of this proposed architecture is that a different number of CRPs is possible depending on how C_s and C_g are configured in the cascaded inverter. The proposed CRO PUF with different configurations of C_s and C_g, behave as strong or weak PUF, briefed as follows:

- As shown in Fig. 17, C_s and C_g of corresponding cascaded inverter are tied i.e. C_{s1}=C_{s2}=....=C_{sm}=C_s, and C_{g1}=C_{g2}=....=C_{gm}=C_g. This type of configuration with two selection line (C_s and C_g) results in four different challenge patterns only i.e., 00,01,10, and 11. The total number of challenge patterns is

always limited to four and not affected by the number of stages of the cascaded inverter (m). The PUF architecture with this CRO is classified as weak CRO PUF.

- However, the control signals of each stage of the inverter are distinct in the CRO architecture shown in Fig. 18. Hence, a CRO with m-stages of cascaded inverter results in a maximum of 2^{2m} number of possible challenge patterns. As the number of possible challenge patterns increases with the increase m, the PUF with this type of CRO behaves as a strong CRO PUF.

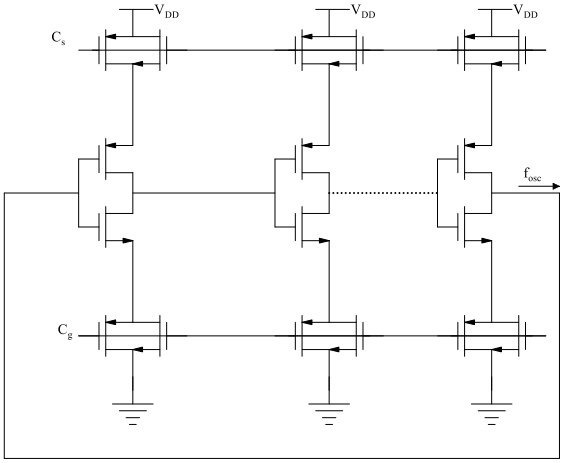


FIGURE 17: Weak CRO (number of RO=4).

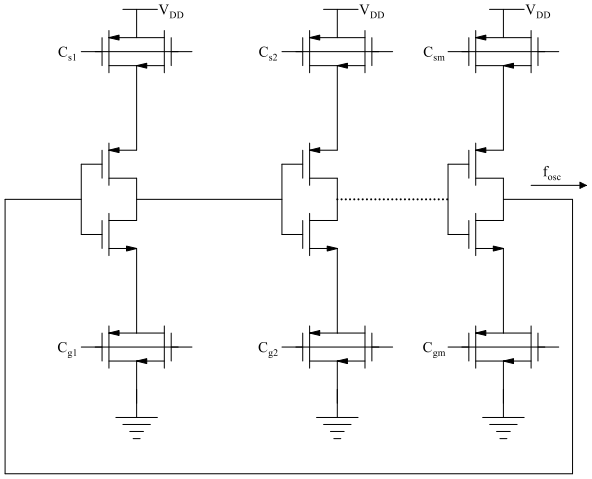


FIGURE 18: Strong CRO (maximum possible number of RO $=2^{2m}$).

The second objective of this research work is to design a lightweight RO sensor for the detection of recycled ICs. The architecture of the sensor using the proposed CRO is shown in Fig. 19. This architecture is similar to conventional RO sensor [13], but the RO section is designed using the proposed

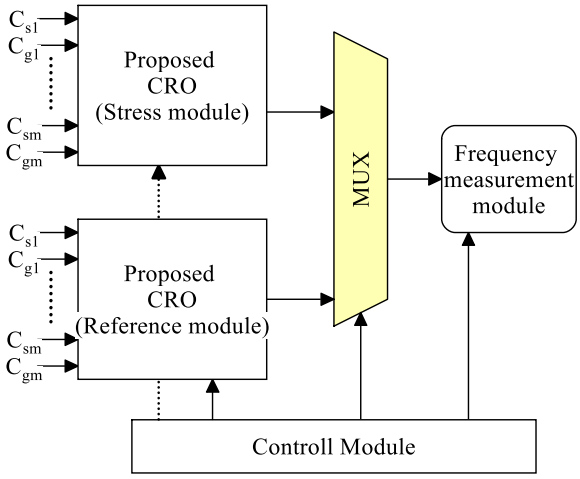


FIGURE 19: RO sensor using proposed CRO.

CRO. The number of RO in both reference and stressed block depends upon the number of available challenges i.e. C_{s1}, C_{s2}, ...C_{sm} and C_{g1}, C_{g2}....C_{gm}. As both the reference and stress module consist of a group of RO, hence the functionality of this architecture is similar to that of AN-CDIR [32]. The registration and authentication process of this proposed CRO sensor according to functional mode given in TABLE 2, briefed as follows:

- During manufacturing, the CRO in both reference and stress modules are designed using equal stages of the cascaded inverter to oscillate at the same frequency, i.e., F_{DIF}=0.
- In stress mode, all the possible CRO in the reference module remains stress-free by driving logic-1 to C_s of each stage of the inverter (C_{s1}=C_{s2}=....=C_{sm}= V_{DD}). As a result, the impact of NBTI stress is eliminated (Fig. 14a), and the RO preserves its original manufactured oscillation frequency.
- Further, in stress mode the impact of NBTI on all possible RO in the stress module is accelerated by driving logic-0 at C_s (C_{s1}=C_{s2}=....=C_{sm}= 0), as shown in Fig. 14b. This higher stress causes the degradation in the oscillation frequency. As a result, a difference in frequency (F_{DIF}) is observed between the CRO in reference and the stress module (due to degradation in oscillation frequency). Further, this difference depends upon the aging accelerating property of the proposed CRO.
- In the authentication mode, for different logic levels of C_s and C_g, a group of F_{DIF} is collected, and the average value of all the F_{DIF} is used to plot the spread (Fig. 7). The corresponding % m is measured from the spread.

This section is summarized as follows:

- The proposed CRO with its lower frequency deviation feature (Fig. 13a and Fig. 13b) enhances the

overall reliability of CRO PUF.

- The proposed CRO PUF with fewer cascaded inverters results in a large number of CRPs. E.g., a 3-stages of cascaded inverter in each CRO module (CRO_u or CRO_l can be configured as 64-possible RO.
- The use of the proposed CRO as a sensor, improves the rate detection of recycled ICs, due to its accelerated aging feature. The accelerated NBTI stress by the proposed CRO with C_s at logic-0 (TABLE 4), shift the spread of F_{aged} more towards the right (Fig. 7) led to improvement in % m.
- Finally, the use of the proposed CRO architecture (Fig. 18), rather than a group of individual RO in AN-CDIR [32] led to (a) improvement in $\%m$: a greater number of RO causes narrow spread (as equation 4)) which led to improvement in % m. (b) lower area overhead due to the area-efficient property of CRO against RO.

The performance analysis of the proposed architecture i.e., the CRO PUF and the CRO sensors is briefed in the next section, and improvements as compared to different existing architectures are also summarized.

VI. RESULTS AND DISCUSSION

This section is divided into two parts. First, the performance analysis of the proposed CRO PUF is carried out and compared against different types of conventional CRO PUF. Second, how efficiently the proposed CRO sensor can detect the recycled ICs? Both the proposed CRO PUF and CRO sensor circuits are implemented in Cadence Virtuoso, using 90 nm CMOS technology. The simulation environment is set at 1 V and 27^oC. Two different analyses is carried out to evaluate the performance of both the proposed architecture, i.e.:

- Monte Carlo simulation is carried out to extract the PV-dependent response bit prior to the fabrication process. It uses statistical transistor modeling provided by the foundry. This helps in measuring the security metrics of PUF [33], and the spread of F_{DIF} [32] collected across a group of similar fresh/aged IC.
- Aging analysis for both PUF and sensor is carried out by using the Relxpert simulator in the virtuoso analog design environment. It uses the aging model library provided by Foundry to measure the frequency degradation of RO over a period of time. This helps in tracking the reliability degradation against aging for CRO PUF and % m for CRO sensors.

A. PERFORMANCE ANALYSIS OF PROPOSED CRO PUF

The performance of the proposed CRO PUF is compared against the conventional CRO PUF [18], ARO-based CRO PUF [28], and CRO PUF with reduced supply voltage [31]. In order to make the comparison fair, all the different PUFs are designed to have an equal number of CROs. In this analysis, all the considered CROs possess 64-different ROs. The CRO in the proposed PUF consists of only 3-cascaded inverter (6-selection lines) compared to 6-stages of cascaded inverter in conventional CRO architectures [18], [28], [31]. Monte Carlo analysis with 100 iteration is carried out by setting both intra-die and inter-die PV, which is equivalent to the fabrication of 100-different PUF instances. On average, 5000-responses of 128-bit width are collected from all the considered PUFs to measure different security metrics.

1) Security Metrics

Among different security metrics like uniqueness, reliability, SAC, uniformity, etc., the reliability of PUF is more critical. As the response bit is generally used as a key in the cryptographic application, a PUF must produce a highly reliable response bit. Further, another important feature of this proposed PUF architecture is that different challenge pattern causes each cascaded inverter to operate at different supply voltages (TABLE 3). Hence, it is also required to find out the best and worst possible challenge patterns and corresponding reliability. The different security metrics measured from the extracted CRPs are reported in TABLE 5. The simulation results validate the improved security metrics of the proposed CRO PUF against all the considered PUF architecture, which is explained briefly as follows:

Reliability:

It measures the number of flipped bits in the extracted response against temperature variation or continuous aging, also called BER (bit error rate). It is measured by using the hamming distance (HD) variation between the reference response and other possible responses collected at different environmental conditions without altering the applied challenge pattern. The expression for BER for a p-bit width response and the corresponding reliability is given by equation 6 as follows [33],

$$BER = \%\ of\ bit\ flip = \frac{1}{x}\sum_{y=1}^{x}\frac{HD(R_i, R'_{i,y})}{p} * 100\% \quad (6)$$

$$Reliability = 100\% - BER \quad (7)$$

The expression for hamming distance (HD [33] [33]) is given as in equaion 8,

$$HD(R_i, R_j) = \sum_{t=1}^{p} R_{i,t} \oplus R_{j,t} \quad (8)$$

Where, R_i is reference sample, $R'_{i,y}$ is the y^{th} sample of R_i at different environmental condition, and x is the total number of such response. The BER against both temperature variation and aging are shown in Fig. 20a and Fig. 20b. The BER against temperature variation is measured as follows:

- First, a reference response (128-bit) is extracted at room temperature (27^oC) by applying a set of challenges.
- Then the same set of challenges is applied by varying the temperature from 0 to 100^oC, to collect

different responses. The BER obtained by using equation 6 is shown in Fig. 20a, and the corresponding reliability is reported in TABLE 5.

Similarly, to measure the BER against aging, all the considered CRO PUF architectures are subjected to continuous stress for a period of 20-years. The BER at different aging instances is shown in Fig. 20b, and the corresponding reliability is reported in TABLE 5. The BER against aging is measured as follows:

- SPICE netlist for all the considered PUF is extracted without aging (at time, t=0), called a fresh netlist.
- All the considered PUF experiences aging continuously for a period of 20-years, and the corresponding aged SPICE netlist is extracted at a time interval of 5,10,15, and 20-years.
- An identical challenge pattern is applied to both fresh and aged netlists, and the corresponding percentage of bit flip is observed.

As shown in Fig. 20a and Fig. 20b, the proposed CRO PUF possesses lower BER as compared to all the considered CRO PUF i.e., close to 5% at a higher temperature of 100^{o}C, and less than 2% after continuous stress for a period of 20-year. Although, the BER in the proposed CRO PUF is slightly improved against the CRO PUF [31], but higher improvement is observed against conventional CRO PUF [18]. This improvement in reliability is due to:

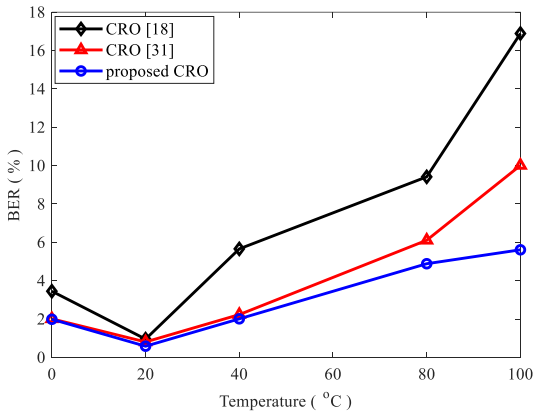
- The lower frequency deviation of the proposed CRO against both temperature variation and aging (TABLE 4) is the major cause of reliability improvement. This minimizes the possibility of bit flip due to frequency crossover within the operating temperature range or over a stress period of 20-years.
- Further, the higher impact of PV on f_{osc} (Fig. 15) causes wider separation among frequency components in the selected pair of RO. As a result, the possibility of frequency crossover is also minimized.

Further, the most significant feature of this proposed CRO PUF is, that all the possible sets of applied challenge patterns can be classified into two different categories i.e.

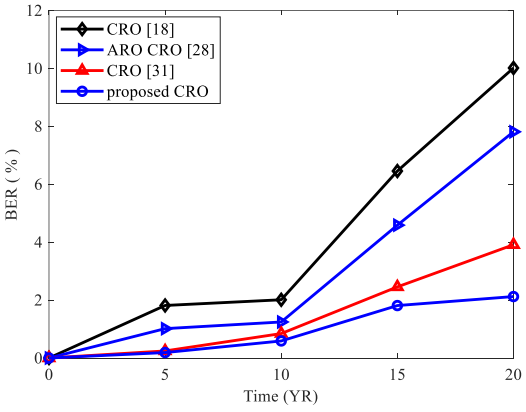
- A group of challenge patterns for which the corresponding inverter section operates at a supply voltage of V_{DD} (challenge pattern with C_s=logic-0) and another group of challenge patterns that causes corresponding inverter section to operate at a supply voltage of V_{DD}-V_t (challenge pattern with C_s= logic-1)

These two categories of applied challenge patterns cause different amounts of frequency degradation (TABLE 4), resulting in different BER against temperature variation and aging. These challenge patterns led to best and worst reliability as reported in TABLE 6, and the corresponding BER is shown in Fig. 21a and Fig. 21b. The comparison results show:

- Worst case i.e., high BER is observed for applied challenge pattern with logic-0 value of C_s (C_s=C_{s1}=C_{s2}=C_{s3}=0). A maximum BER close to 7 % at a high temperature of 100^{o}C and 5 % after a stress period of 20-years is observed.
- Best case i.e., low BER is observed when logic-1 appears at C_s, and the reliability of proposed CRO PUF approaches close to its ideal value (100%). This set of challenge patterns led to a very low BER i.e., close to 1% against both the variation.



(a) Against Temperature variation



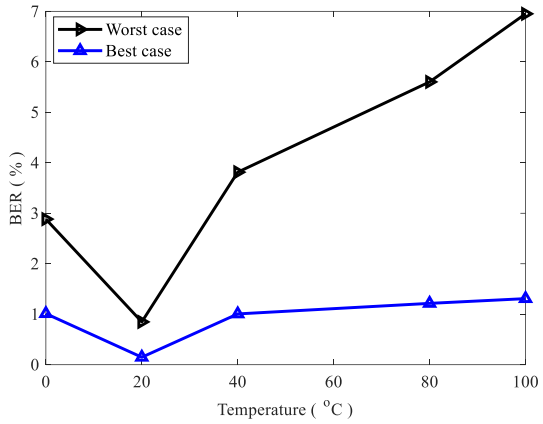
(b) Against Aging

FIGURE 20: BER in different types CRO PUF against (a) Temperature variation (b) Aging.

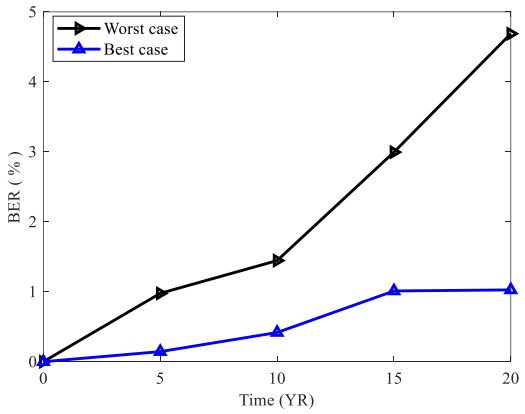
Very low BER i.e., higher reliability of proposed CRO PUF implies, it can reproduce almost all response bits correctly against temperature variation and aging. As a result, the extracted response was found suitable to be used as a secure-key in different applications [27], [34]–[41].

Uniqueness:

In order to measure uniqueness, the response bit is collected by applying the same challenge simultaneously to all the 100-different instances of PUF. Like this, on average, 5000 CRPs are collected. The average value of uniqueness is reported in TABLE 5. The result shows the higher uniqueness of the proposed CRO PUF compared to all the considered CRO PUF. This higher value is due to the higher impact of PV on the oscillation frequency of RO. Similarly, other security metrics like uniformity and SAC is also measured from the



(a) Against Temperature variation



(b) Against Aging

FIGURE 21: Best and worst BER in the proposed CRO PUF against (a) Temperature variation (b) Aging.

extracted response, and the corresponding value is reported in TABLE 5. The proposed CRO PUF shows improvement in security metrics as compared to others. The uniformity and SAC of the proposed CRO PUF are comparable with all the conventional CRO PUF architecture. Further, the reliability of the proposed CRO PUF is measured by increasing the number of CROs from 64 ($m = 3$) to 1024 ($m = 5$) and reported in TABLE 7. The measured reliability shows significantly less degradation.

B. PERFORMANCE ANALYSIS OF PROPOSED CRO SENSOR

This section discusses the detection of recycled IC by the proposed CRO sensor. Further, a comparative analysis is carried out against the conventional AN-CDIR [32] sensor. The reason to choose AN-CDIR only is that in this architecture, both reference and stress modules consist of a group of RO. So, it is fair to compare by choosing an equal number of RO in both the proposed CRO sensor and conventional AN-CDIR. In this analysis, the considered RO sensor consists of a group of 64-RO in both the reference and stressed modules. The detection capability of the RO sensor is characterized by the parameter, i.e., the percentage of misprediction (% m). The simulation setup to find % m is given as follows: -

- In AN-CDIR, both reference and stress modules consist of 64- the number of individual conventional CMOS-based RO.
- However, in the proposed CRO sensor, the same number of RO is achieved by designing both reference and stress modules with 3-stages of cascaded inverter (Fig. 18).
- Monte Carlo simulation with 200 iteration is carried out for each sensor in order to collect PV-dependent frequency, which is used to observe the spread of F_{DIF} at different aging intervals.
- A continuous NBTI stress is applied to both the RO sensor for a period of $4D$(days), and the aged netlist is extracted at a time interval of t=$2D$ and $4D$.
- This aged netlist is used to measure the spread of F_{DIF} at t=$2D$ and $4D$.
- For both the considered RO sensor, % m is measured from the spread of F_{DIF} collected at t=0 (for fresh RO), and t=$2D$ and $4D$ (for aged RO).

The spread of F_{DIF}, at t=0, $2D$, and $4D$ for both the RO sensors is shown in Fig. 22. The reason to choose a lower aging interval is that at a higher aging interval, a recycled IC can be easily detected. The efficiency of a sensor is measured by its ability to detect an IC that experiences a small amount of aging. The mean (μ) of each spread, and % m measured from Fig. 22 is summarized in TABLE 8. The % m is measured from the spread by observing how many frequencies the sample lies in the overlap region between:

- $F_{DIFF}\ |_{t=0}$ and $F_{DIFF}\ |_{t=2D}$
- $F_{DIFF}\ |_{t=0}$ and $F_{DIFF}\ |_{t=4D}$

The analysis of extracted spread, F_{DIF} at t=0, $2D$, and $4D$ is briefed below:

(a) For fresh/new IC, t=0

- The spread of $F_{DIFF}\ |_{t=0}$, across all the 200-different instances of both the RO sensor is shown in Fig. 22, and the corresponding μ is reported in TABLE 8.
- $F_{DIFF}\ |_{t=0}$, indicates the average of all the frequency differences obtained from each instance of a sensor. (No NBTI)
- The μ of $F_{DIFF}\ |_{t=0}$ ideally must be zero, but PV causes a value close to zero for both the sensor, as reported in TABLE 8.

(b) For recycled IC, t=$2D$/$4D$

- To observe the impact of aging, NBTI stress is continuously applied for a period of $2D$ and $4D$, and the frequency of both reference and stress RO is measured to calculate F_{DIFF}.
- This process repeated across the 200-different instances of both the considered RO sensor, and the overall spread of F_{DIFF} at t=$2D$ and $4D$ is shown in Fig. 22.

- The μ of both the spread $F_{DIFF}\ |_{t=2D}$ and $F_{DIFF}\ |_{t=4D}$ shifts toward right from $\mu\ |_{t=0}$, and the shift increases with increase in stress duration from $2D$ to $4D$ as in equation 9 i.e.

$$[(\mu\ |_{t=4D} - \mu\ |_{t=0}) > (\mu\ |_{t=2D} - \mu\ |_{t=0})]_{Proposed\ Sensor} \tag{9}$$

- As shown in Fig. 22, at the higher aging interval (t=4D), the spread of $F_{DIFF}\ |_{t=4D}$ in both the considered sensor is far apart from its original spread i.e $F_{DIFF}\ |_{t=0}$. As there is no overlap region between these two spreads, hence % m=0, for both the considered sensors.
- However, at lower aging interval i.e. t=2D, shift in spread of F_{DIFF} is less, led to overlap between the spreads $F_{DIFF}\ |_{t=2D}$ and $F_{DIFF}\ |_{t=0}$ of both the proposed CRO and AN-CDIR sensor.
- The % m obtained at t=2D from the spread is reported in TABLE 8. The measured result shows proposed CRO sensor improves % m as compared to AN-CDIR.

This improvement in % m is due to,

- NBTI causes more considerable degradation in f_{osc} in the proposed CRO as compared to NBTI-aware RO used in AN-CDIR [32]. As given in TABLE 4, the proposed CRO experiences an accelerated degradation (for C_s=0) of 12 % higher than the RO used in AN-CDIR.
- As a result, the shift in the μ value of F_{DIFF} is more towards the right, in the proposed sensor as compared to AN-CDIR as in equation 10 i.e.

$$[(\mu\ |_{t=2D} - \mu\ |_{t=0})]_{CRO} > [(\mu\ |_{t=2D} - \mu\ |_{t=0})]_{AN-CDIR} \tag{10}$$

This above discussion clarifies, that at a lower aging interval of 2D, the proposed CRO sensor improves the misprediction by 75 % as compared to conventional AN-CDIR. However, at higher aging intervals both the RO sensors can detect all the recycled IC efficiently.

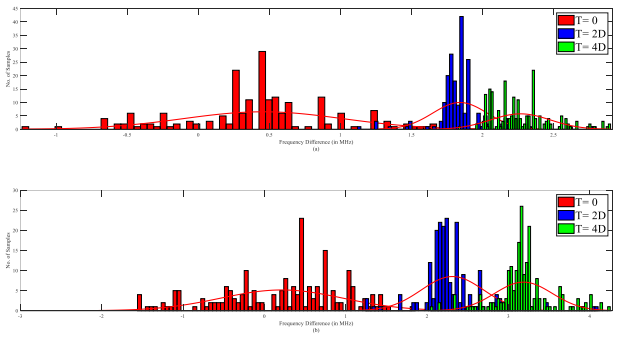


FIGURE 22: Misprediction analysis from the spread of F_{DIFF} in (a) AN-CDIR sensor (b) proposed CRO sensor.

C. VLSI METRICS

Power Consumption

The average power consumption during the CRP extraction area is measured from the layout and summarized in TABLE 5 (for PUF) and TABLE 8 (for RO sensor). The average power consumption for all the considered PUF is measured across 5000-CRPs and reported in TABLE 5. The proposed CRO PUF is 18 % more power-efficient than the CRO PUF with reduced supply voltage [31] and 70 % more than the conventional CRO PUF [18]. The lower value of power consumption is due to a reduction in supply voltage from V_{DD} to V_{DD}-V_t across CRPs for a different logic level of C_s. All the applied challenge patterns except [C_s C_g] =01 (as reported in TABLE 3) lowers each cascaded inverter's rail-to-rail operating voltage in the proposed CRO PUF.

Area

The proposed CRO PUF and sensor are also much more area-efficient due to MUX-free CRO architecture and many possible CROs using only a few stages of the cascaded inverter. The proposed CRO PUF is 25 % and 55 % area-efficient compared to the CRO PUF with reduced supply voltage [31] and conventional CRO PUF [18]. Finally, the proposed CRO sensor is also 80 % area-efficient compared to the AN-CDIR sensor [32]. This is possible by replacing a large group of individual RO with a single proposed CRO. In this analysis, a total of 128-number (64 reference + 64 stressed) of individual RO in AN-CDIR is replaced with two proposed CROs (1-reference and 1-stressed CRO), each consist a 3-cascaded inverter only (6-control signals).

VII. COMPARISON SUMMARY

From the simulation results, the improvements achieved by the proposed CRO, and its application as PUF and sensor briefed as follows:

- The proposed CRO is capable of aging acceleration and retardation (as mentioned in TABLE 4), depending on the $C_s^{'}$ logic level. The accelerated aging is 12% higher than the most recently proposed NBTI-aware RO [32]. Similarly, the aging tolerant feature is also improved by 60% compared to one of the most suitable aging tolerant RO proposed in [31] [31].
- The reliability of the proposed CRO PUF against both aging and temperature variation is improved. The best-case challenge pattern (as presented in TABLE 6) results in 99 % reliability, which is close to the ideal value. This is due to a higher aging tolerant feature of the proposed CRO.
- In the proposed CRO sensor, the % m is improved by 75 % compared to conventional AN-CDIR at a small aging interval of 2D. This is due to the aging accelerated feature of the proposed CRO.
- The proposed CRO is also area-efficient. This is due to differences in CRO architecture i.e., a conventional CRO [18] consists of two rows of cascaded inverters with MUX, CRO in [31] is designed using

a single row of cascaded inverter with MUX, and proposed CRO is designed by using only cascaded inverter. Hence, both the PUF and sensor architecture designed by using the proposed CRO are area-efficient.

- The lower power budget of the proposed CRO PUF is due to a reduction in the rail-to-rail swing of inverter operating voltage across several challenge patterns during CRP extraction.
- Finally, the proposed CRO consists of 4-additional MOS per inverter section (Fig. 11), which is more than all the existing RO architecture (as presented in TABLE 4). But, this shortcoming of the proposed CRO is compensated by the design of CRO without MUX and more number of possible RO (2^{2m}) with few stages of cascaded inverter only.

VIII. CONCLUSION

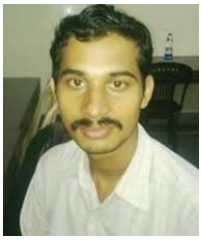
This paper presents a research work on novel CRO architecture, which is suitable for addressing security issues of ICs. With its aging acceleration and retardation property, the proposed CRO is found to be ideal in applications such as PUF and sensors. The aging acceleration feature of the proposed CRO enables the sensor to detect the ICs used for a few days only. The proposed CRO PUF also generates a highly reliable response bit. Hence, it is suitable for the generation of the crypto key. Finally, the use of the proposed CRO as a PUF and sensor lowers the footprint on IC.

REFERENCES

[1] I. Butun, P. Österberg, and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 2019.
[2] K. Yang, D. Blaauw, and D. Sylvester, "Hardware designs for security in ultra-low-power iot systems: An overview and survey," *IEEE Micro*, vol. 37, no. 6, pp. 72–89, 2017.
[3] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1207–1228, 2014.
[4] J. Cassell, "Reports of counterfeit parts quadruple since 2009, challenging us defence industry and national security," 2012.
[5] L. Kessler and T. Sharpe, "Faked parts detection, circuits assembly, the journal for surface mount and electronics assembly," 2010.
[6] M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1283–1295, 2014.
[7] S. P. Skorobogatov, "Semi-invasive attacks: a new approach to hardware security analysis," 2005.
[8] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.
[9] D. Boning and S. Nassif, "Models of process variations in device and interconnect," *Design of high performance microprocessor circuits*, p. 6, 2000.
[10] C.-H. Chang, Y. Zheng, and L. Zhang, "A retrospective and a look forward: Fifteen years of physical unclonable function advancement," *IEEE Circuits and Systems Magazine*, vol. 17, no. 3, pp. 32–62, 2017.
[11] S. Joshi, S. P. Mohanty, and E. Kougianos, "Everything you wanted to know about pufs," *IEEE Potentials*, vol. 36, no. 6, pp. 38–46, 2017.
[12] Y. Zhang and U. Guin, "End-to-end traceability of ics in component supply chain for fighting against recycling," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 767–775, 2019.
[13] X. Zhang and M. Tehranipoor, "Design of on-chip lightweight sensors for effective detection of recycled ics," *IEEE transactions on very large scale integration (VLSI) systems*, vol. 22, no. 5, pp. 1016–1029, 2013.
[14] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.
[15] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 148–160.
[16] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*. IEEE, 2007, pp. 9–14.
[17] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "The butterfly puf protecting ip on every fpga," in *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*. IEEE, 2008, pp. 67–70.
[18] A. Maiti and P. Schaumont, "Improved ring oscillator puf: An fpga-friendly secure primitive," *Journal of cryptology*, vol. 24, no. 2, pp. 375–397, 2011.
[19] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "Fpga intrinsic pufs and their use for ip protection," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2007, pp. 63–80.
[20] R. Maes, P. Tuyls, and I. Verbauwhede, "Intrinsic pufs from flip-flops on reconfigurable devices," in *3rd Benelux workshop on information and system security (WISSec 2008)*, vol. 17, 2008, p. 2008.
[21] D. Ganta and L. Nazhandali, "Study of ic aging on ring oscillator physical unclonable functions," in *Fifteenth international symposium on quality electronic design*. IEEE, 2014, pp. 461–466.
[22] A. Maiti and P. Schaumont, "The impact of aging on a physical unclonable function," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 22, no. 9, pp. 1854–1864, 2013.
[23] J. M. Rabaey, A. P. Chandrakasan, and B. Nikolić, *Digital integrated circuits: a design perspective*. Pearson Education, Incorporated., 2003.
[24] A. Tiwari and J. Torrellas, "Facelift: Hiding and slowing down aging in multicores," in *2008 41st IEEE/ACM International Symposium on Microarchitecture*. IEEE, 2008, pp. 129–140.
[25] Y. Cao, L. Zhang, C.-H. Chang, and S. Chen, "A low-power hybrid ro puf with improved thermal stability for lightweight applications," *IEEE Transactions on computer-aided design of integrated circuits and systems*, vol. 34, no. 7, pp. 1143–1147, 2015.
[26] C. Q. Liu, Y. Cao, and C.-H. Chang, "Low-power, lightweight and reliability-enhanced current starved inverter based ro pufs," in *2016 IEEE Asia Pacific conference on circuits and systems (APCCAS)*. IEEE, 2016, pp. 646–649.
[27] S. R. Sahoo, S. Kumar, and K. Mahapatra, "A novel reliable and aging tolerant modified ro puf for low power application," *Analog Integrated Circuits and Signal Processing*, vol. 103, no. 3, pp. 493–509, 2020.
[28] M. T. Rahman, F. Rahman, D. Forte, and M. Tehranipoor, "An aging-resistant ro-puf for reliable key generation," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 3, pp. 335–348, 2015.
[29] C. Q. Liu, Y. Cao, and C. H. Chang, "Acro-puf: A low-power, reliable and aging-resilient current starved inverter-based ring oscillator physical unclonable function," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 12, pp. 3138–3149, 2017.
[30] S. R. Sahoo, S. Kumar, K. Mahapatra, and A. Swain, "A novel aging tolerant ro-puf for low power application," in *2016 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*. IEEE, 2016, pp. 187–192.
[31] S. R. Sahoo, S. Kumar, and K. Mahapatra, "A novel configurable ring oscillator puf with improved reliability using reduced supply voltage," *Microprocessors and Microsystems*, vol. 60, pp. 40–52, 2018.
[32] U. Guin, D. Forte, and M. Tehranipoor, "Design of accurate low-cost on-chip structures for protecting integrated circuits against recycling," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 24, no. 4, pp. 1233–1246, 2015.
[33] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," in *Embedded systems design with FPGAs*. Springer, 2013, pp. 245–267.
[34] S. K. Ram, S. R. Sahoo, B. B. Das, K. Mahapatra, and S. P. Mohanty, "Eternal-thing: A secure aging-aware solar-energy harvester thing for sustainable iot," *IEEE Transactions on Sustainable Computing*, vol. 6, no. 2, pp. 320–333, 2020.
[35] S. K. Ram, B. B. Das, K. Mahapatra, S. P. Mohanty, and U. Choppali, "Energy perspectives in iot driven smart villages and smart cities," *IEEE Consumer Electronics Magazine*, vol. 10, no. 3, pp. 19–28, 2020.

[36] P. Krishnan, K. Jain, R. Buyya, P. Vijayakumar, A. Nayyar, M. Bilal, and H. Song, "Mud-based behavioral profiling security framework for software-defined iot networks," *IEEE Internet of Things Journal*, vol. 9, no. 9, pp. 6611–6622, 2021.
[37] K. Hatti and C. Paramasivam, "Design and implementation of enhanced puf architecture onfpga," *International Journal of Electronics Letters*, vol. 10, no. 1, pp. 57–70, 2022.
[38] K. Nimmy, S. Sankaran, and K. Achuthan, "A novel lightweight puf based authentication protocol for iot without explicit crps in verifier database," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–16, 2021.
[39] N. Mohankumar, M. Jayakumar, and M. Nirmala Devi, "Lightweight logic obfuscation in combinational circuits for improved security—an analysis," in *Expert Clouds and Applications*. Springer, 2022, pp. 215–225.
[40] S. K. Ram, S. R. Sahoo, B. B. Das, K. Mahapatra, and S. P. Mohanty, "Eternal-thing 2.0: Analog-trojan resilient ripple-less solar energy harvesting system for sustainable iot in smart cities and smart villages," *arXiv preprint arXiv:2103.05615*, 2021.
[41] F. Jose, M. Priyatharishini, and M. N. Devi, "Hardware trojan detection using deep learning-generative adversarial network and stacked auto encoder neural networks," in *ICT Analysis and Applications*. Springer, 2022, pp. 203–210.
[42] Deng, D., Hou, S., Wang, Z. & Guo, Y. Configurable ring oscillator PUF using hybrid logic gates. *IEEE Access*. **8** pp. 161427-161437 (2020)
[43] Huang, Z., Bian, J., Lin, Y., Liang, H. & Ni, T. Design guidelines and feedback structure of ring oscillator PUF for performance improvement. *IEEE Transactions On Computer-Aided Design Of Integrated Circuits And Systems*. (2023)

SASWAT KUMAR RAM (SM'14) received the professional degree in Electronics and Telecommunication Engineering with Honours from Biju Patanaik University of Technology, India in 2005, the M.Tech and Ph. D. degree from NIT, Rourkela, India in 2011 and 2022 respectievly. He is currently working as an Assistant Professor in the department of Electronics and Communication Engineering, SRM University, Andhra Pradesh, India. His current research interest includes energy harvesting for IoT, low power VLSI design, Embedded Systems, Hardware security, Power System, Internet of Things, and Machine learning.



SAUVAGYA RANJAN SAHOO (S'18) received the engineering degree (ENTC) from DRIEMS, Odisha in 2006. In 2012, he obtained his M.Tech in VLSI Design Embedded Systems from National Institute of Technology, Rourkela, Odisha. In 2019, he obtained his Ph.D. in Electronics and Communication Engineering from National Institute of Technology, Rourkela. He is currently working as an Analog Design Engineer, Marquee Semiconductor, India. His main research interests include low power CMOS VLSI circuit design, Hardware security.

BANEE BANDANA DAS (S'19)) received the professional degree in Computer Science Engineering from Biju Patanaik University of Technology, India in 2010, the M.Tech degree from from Biju Patanaik University of Technology, India in 2012. She obtained her Ph.D. degree in Computer Science and Engineering from National Institute of Technology, Rourkela. She is currently working as an Assistant Professor in the epartment of Computer Science and Engineering at SRM University, Andhra Pradesh, India. Her current research interest includes Machine learning, Computer vision, Neural network and Computational intelligence, Internet-of-Things, Hardware security, and Embedded Systems

KAMALAKANTA MAHAPATRA (M'12) obtained his B. Tech degree with Honours from Regional Engineering College, Calicut in 1985, M. Tech from Regional Engineering College, Rourkela in 1989 and Ph. D. from IIT Kanpur in 2000. He is currently a Professor in Electronics and Communication Engineering Department of National Institute of Technology (NIT), Rourkela. He assumed this position since February 2004. He is a fellow of the institution of Engineers (India) in ECE Division. He has published several research papers in National and International Journals. His research interests include Embedded Computing Systems, VLSI Design, Hardware Security and Industrial Electronics.

SARAJU P. MOHANTY (SM'08) received the bachelor's degree (Honors) in electrical engineering from the Orissa University of Agriculture and Technology, Bhubaneswar, in 1995, the master's degree in Systems Science and Automation from the Indian Institute of Science, Bengaluru, in 1999, and the Ph.D. degree in Computer Science and Engineering from the University of South Florida, Tampa, in 2003. He is a Professor with the University of North Texas. His research is in "Smart Electronic Systems" which has been funded by National Science (NSF), Semiconductor Research Corporation (SRC), U.S. Air Force, IUSSTF, and Mission Innovation. He has authored 500 research articles, 5 books, and 10 granted and pending patents. His Google Scholar h-index is 57 and i10-index is 243 with 13,000 citations. He is regarded as a visionary researcher on Smart Cities technology in which his research deals with security and energy aware, and AI/MLintegrated smart components. He introduced the Secure Digital Camera (SDC) in 2004 with built-in security features designed using Hardware Assisted Security (HAS) or Security by Design (SbD) principle. He is widely credited as the designer for the first digital watermarking chip in 2004 and first the low-power digital watermarking chip in 2006. He is a recipient of 19 best paper awards, Fulbright Specialist Award in 2021, IEEE Consumer Electronics Society Outstanding Service Award in 2020, the IEEE-CS-TCVLSI Distinguished Leadership Award in 2018, and the PROSE Award for Best Textbook in Physical Sciences and Mathematics category in 2016. He has delivered 24 keynotes and served on 14 panels at various International Conferences. He has been serving on the editorial board of several peer-reviewed international transactions/journals, including IEEE Transactions on Big Data (TBD), IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), IEEE Transactions on Consumer Electronics (TCE), and ACM Journal on Emerging Technologies in Computing Systems (JETC). He has been the Editor-in-Chief (EiC) of the IEEE Consumer Electronics Magazine (MCE) during 2016-2021. He served as the Chair of Technical Committee on Very Large Scale Integration (TCVLSI), IEEE Computer Society (IEEE-CS) during 2014-2018 and on the Board of Governors of the IEEE Consumer Electronics Society during 2019-2021. He serves on the steering, organizing, and program committees of several international conferences. He is the steering committee chair/vice-chair for the IEEE International Symposium on Smart Electronic Systems (IEEE-iSES), the IEEECS Symposium on VLSI (ISVLSI), and the OITS International Conference on Information Technology (OCIT). He has mentored 3 post-doctoral researchers, and supervised 15 Ph.D. dissertations, 27 M.S. theses, and 27 undergraduate projects