Securing Things: A Novel CRO Applicable in PUF and Recycled IC Detection

[1]Saswat Kumar Ram, [2]Sauvagya Ranjan Sahoo, [3]Banee Bandana Das, [4]Kamalakanta Mahapatra, [5]Saraju P Mohanty
[1]Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India
[2,4] Department of Electronics and Communication Engineering, National Institute of Technology, Rourkela, India
[3] Department of Computer Science and Engineering, SRM University, Andhra Pradesh, India
[5] Department of Computer Science and Engineering, University of North Texas, Denton, USA
E-mail: saswatram01@gmail.com

Abstract: **Ring Oscillator (RO) is widely used to address different hardware security issues. For example, using RO-based physical unclonable function (PUF) generates a secure and reliable key for the cryptographic application, RO-based aging sensor for efficient detection of recycled ICs. This paper uses a conventional CMOS inverter with two voltage control signals to design a configurable RO (CRO). With its control signal, 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 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, the proposed architecture is also area and power-efficient compared to conventional architectures.**

Keywords— **Process Variation (PV); Aging; Configurable Ring Oscillator (CRO); Challenge-Response pair (CRP); Bit Error Rate (BER); Recycled IC.**

1. Introduction

In this current era of technology, IC security and its power, performance, and area become 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 free from adversary attacks. A malfunction due to a malicious attack on any device may propagate among the group, leading to the failure of the entire system. Further, globalization and complexity in the IC supply chain led to the presence of counterfeited IC [3] by the untrusted foundry, untrusted suppliers, etc., which is also related to the security of IC. A Counterfeit IC may be a tampered, cloned, copied, overproduction, or recycled IC. The report in [4, 5, 6, 7] indicates a revenue loss of U.S. $169 billion to chipmakers due to these counterfeited ICs. Although these ICs function properly but their reliability is questionable. This scenario is quite a concern in critical applications like aerospace, defense, lifesaving appliances, etc. As reported in [7, 8, 9, 10], out of several types of counterfeited IC, a significant share is occupied by recycled ICs. So during both the design and fabrication of ICs, security issues must be addressed along with VLSI metrics like power, performance, and area. Although there are several securities-related issues are associated with IC manufacturing [11], in this research work, two major issues are being addressed i.e.

- Highly reliable crypto key generation using PUF.
- Efficient detection of recycled IC using RO sensor.

1.1 Reliable key using PUF

The conventional approach includes storing crypto-key in an external ROM. This approach is vulnerable to attack from adversaries [11], area overhead, and higher power consumption due to bulky ROM architecture. PUF [12] has emerged as a promising breakthrough in generating the secure key in the last decade as a solution. PUF explores the secret of the inherent manufacturing PV [13], which is difficult to clone or model. This manufacturing PV is a unique phenomenon that produces the difference in behavior between two identical IC fabricated by the same designer in the same foundry using the same process technology. PUF [12, 14, 15] generates the key only when powered up, unlike memory, where the security 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 like [15], uniqueness, reliability, uniformity, strict avalanche condition (SAC), etc. These metrics are measured by collecting a group of response bits (called a secure key) from PUF by applying a set of challenges. These challenges and the corresponding response are termed as CRPs. Uniqueness measures the variation among the response bit 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.

1.2 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 [3,16,17]. The aging of 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 than a fresh or unused IC. Several circuit-level techniques are proposed in the literature to accelerate this aging mechanism for the efficient detection of recycled ICs.

In literature [16, 18 -21], several circuit-level techniques are proposed to address these security issues. Different types of PUF 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 [21] to predict the amount of aging experienced by the IC under test.

From this discussion, the common problem related to PUF and sensors is; that the impact of aging on PUF must be lowered to improve its reliability. Simultaneously, the aging must be accelerated to improve the detection rate of recycled IC by a sensor. Based on these challenges, the objective of this research work includes: -

- To design a CRO that can enable both acceleration and retardation of aging depending on its application as sensor and PUF, respectively.
- The proposed PUF must be highly reliable, and the proposed sensor also improves the rate of detection of recycled IC compared to conventional architectures.
- Finally, both the proposed architecture must be area and power efficient.

The rest of this paper is organized as follows. The novel contribution of this research work is presented in Section 2.

Section 3 introduces prior research work on different types of RO-based PUF, RO sensors, and the scope for further improvement. The proposed CRO architecture and its functionality are briefed in Section 4: section 5, which briefs about applying the proposed CRO as PUF and sensor. Results and discussion are provided in Section 6, and a comparison summary is outlined in Section 7. Finally, this research work is concluded in Section 8.

2. Novel Contribution

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: -

- Reconfigurable Inverter: The core of this proposed work is to design a reconfigurable inverter. The proposed inverter 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 sets of operating voltages for the inverter.
- Area efficient CRO: The proposed cascaded inverter behaves as a CRO with its voltage control input. Hence, area-efficient due to the absence of MUX as in conventional CRO [22, 35].
- 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 the control signal in the proposed inverter. This feature makes it suitable for both applications, i.e., the design of a reliable CRO PUF and RO sensor with an improved rate of detection of recycled IC.

3. Background

In the last decade, researchers have worked on designing different types of PUF, recycled IC detection circuits, and different techniques to improve its performance are proposed in the literature. For PUF [14,15], the proposed techniques aim at improving its VLSI and security metrics. Similarly, a lightweight RO sensor [17] is used to improve the detection rate of recycled ICs. Further, it is observed, that the ring oscillator is one of the most suitable primitives found in PUF and sensor circuits. The reason to use RO is: -

- Simple architecture only cascaded inverter.
- The oscillation frequency is explored by PV, hence suitable for the 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 PUF or sensor application.

This section is segregated as follows: -

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

3.1 PUF

All the PUF architectures are divided into either Si or non-Si-based PUF [15]. The significant Si-PUF architecture includes delay-based PUF like RO PUF, arbiter PUF, CRO PUF, ARO PUF, etc., and memory-based PUF like SRAM PUF, FF PUF, etc. [18-24]. These are also validated in both FPGA and ASIC platforms. This paper's discussion is kept limited to one of the most widely used delay-based Si-PUF, i.e., RO PUF. The reason to choose RO PUF is its simple architecture for CRP collection. It can be easily embedded with other functional units to provide security primitive and generate a highly reliable response.

Different RO PUF topologies and corresponding pros and cons are briefed in Table 1. A conventional RO PUF [20] 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 a slightly different frequency. 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 as (1),

$$R = \begin{cases} 1 & \textit{if } f_1 > f_2 \\ 0 & \textit{otherwise} \end{cases} \qquad (1)$$

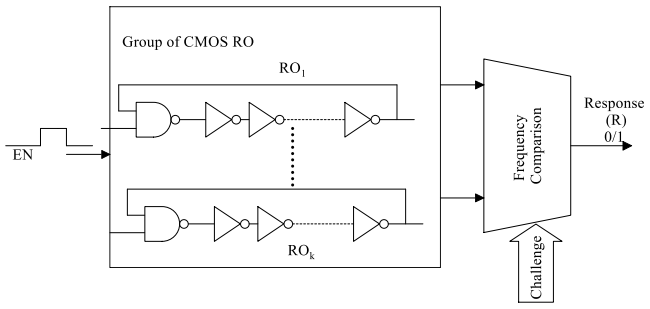


Fig. 1. Conventional RO PUF [16]

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 [22]. A conventional CRO architecture consists of either a two-row of the inverter [22] or a single row of the inverter [35] with cascaded MUX (as shown in Fig. 2). A CRO with an n-selection line (C1, C2…Cn: challenges applied to MUX) is configured as a 2n number of different RO. Hence, both the CROs [22, 35] are area efficient.

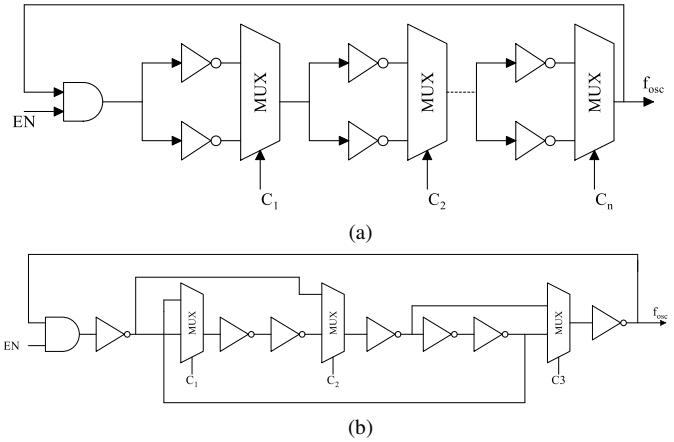


Fig. 2. Conventional CRO using (a) 2-row of cascaded inverter [18] (b) single row of cascaded inverter [31]

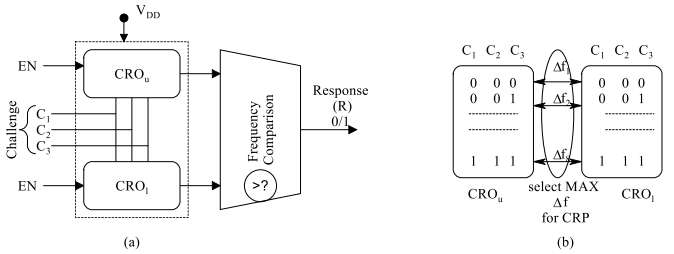


Fig. 3. (a) Conventional CRO PUF (b) CRP collection approach [18]

A conventional CRO PUF [22] with a response bit collection approach is shown in Fig. 3. Each set of applied challenge patterns (C1, C2, C3) results in a RO with a unique oscillation frequency due to PV. The frequency comparison between the RO in CROu and CROl is carried out. A pair of RO with maximum frequency separation only is considered to measure the response bit. (as shown in Fig. 3(b)).

Although, this CRO PUF results in highly reliable response bits and both power and area efficient features (due to a reduction in the number of RO). However, the vulnerability of oscillation frequency against temperature variation [20], and aging [25,26] also affect its reliability. The cause and corresponding mitigation techniques are briefed below.

3.1.1 PUF Reliability: Cause and Mitigation Technique

(a) Cause

The expression for oscillation frequency (f_{osc}) of a RO [20] is given as follows,

$$f_{osc} = \frac{1}{2mt_p} \qquad (2)$$

Where, m is the number of cascaded inverters, t_p is the delay of each inverter. Different environmental effect like temperature variation or aging affects the threshold voltage (V_{th}) of MOS led to degradation in f_{osc} ($t_p = f(V_{th})$ [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 some time (t) due to aging, as shown in Fig. 4(b). As a result, a flip in response bit (0 to 1 or 1to 0) occurs, leading to overall reliability degradation of PUF. This 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 [27-28], leading to permanent degradation in the reliability of PUF.

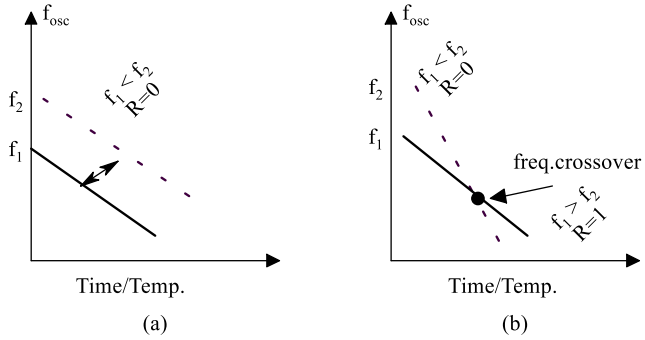


Fig. 4. Reliability degradation (a) No Crossover: Pair of RO with higher frequency separation (b) frequency cross over at higher Temp. /Time

The threshold voltage degradation due to NBTI as compared to well-known aging mechanisms like [28] 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 [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 [28], which leads to an overall degradation in the oscillation frequency of RO. Further, this degradation rate increases with an increase in aging over a while [28]. Hence, the design of NBTI resilient RO is more important, in order to restore reliability of PUF.

This discussion clarifies that a RO with lower frequency deviation against temperature variation or aging lowers the possibility of frequency crossover and improves the overall reliability of PUF.

(b) Mitigation Technique:

Several mitigation techniques 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 architecture, few NBTI tolerant RO [29-32, 35] are shown in Fig. 5 (b, c). Both this NBTI tolerant RO reduces the impact of NBTI by lowering the negative bias across PMOS in non-oscillation mode, as follows: -

- In aging tolerant RO (ARO [32]), the added NMOS (T_N) to the input of each cascaded inverter lowers the

VGS, P across all the PMOS from $-V_{DD}$ (in conventional CMOS RO) to $-V_{t,n}$.

- However, the most recent RO proposed in [33,34,35] 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, these modified ROs also lower the frequency deviation against temperature variation.

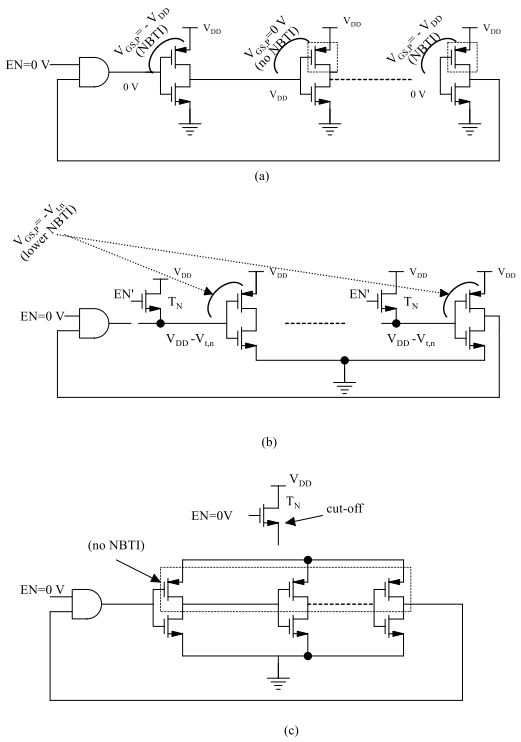


Fig. 5 NBTI stress on different types of RO (a) CMOS RO [16] (b) ARO [28] (c) RO with reduced supply voltage [31]

3.2 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 [17] is shown in Fig. 6, and its functionality is given in Table 2. It consists of two identical RO, i.e., reference RO ($(RO)_{REF}$) and stressed RO ($(RO)_{STR}$). The control module generates the necessary control signal to drive the RO into the stress or authentication phase, as described in Table 2. The registration and authentication of a recycled IC in a group of similar IC 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, F_{DIF} is slightly positive or negative due to inherent manufacturing variation, as shown in Fig. 7. The spread's mean (μ) for a fresh IC group, 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 is the magnitude of F_{DIF}, and more shift in F_{aged} towards right
- The region of overlap between the two spread 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.

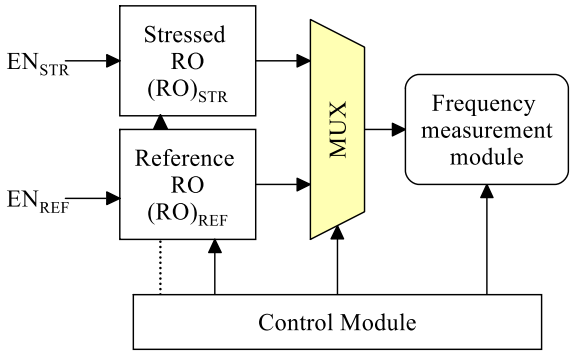


Fig. 6. Conventional RO sensor [13]

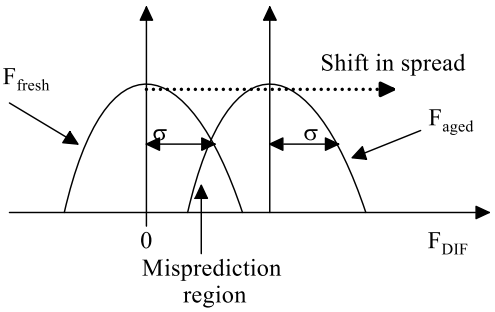


Fig. 7. Spread of F_{DIF} [32]

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

- Accelerating NBTI stress: - With an 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}), which reduced the overlapped region.
- By increasing the number of RO: - The spread (σ) of F_{DIF} depends upon the number of RO (N) [36], used as reference and stress RO. From (3), with an increase in

the number of RO, the spread (σN) of both F_{fresh} and F_{aged} becomes narrow. As a result, % m reduced.

$$\sigma_N = \sigma / N \qquad (3)$$

The lightweight AN-CDIR sensor proposed in [36] uses the above two methodologies to improve % m. The architecture, registration, and authentication flow of AN-CDIR is similar to conventional RO sensor [17] 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 $(RO)_{STR}$ [17]. With the increase in the number of RO in both modules, the spread of F_{DIF} becomes narrow (from (3)) led to improvement in % m.

- Further, to accelerate the NBTI stress, the conventional CMOS RO [17] in both modules was replaced by NBTI-aware RO [36]. 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, compared to half in the CMOS inverter (shown as blue color) by using a pass transistor logic (PTL) based switch 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 compared to conventional CMOS RO.The use of many NBTI-aware RO in both reference and stress modules of AN-CDIR [36] lowers the % m, i.e., it can detect the ICs used for a few days only. Although it improves % m, the presence of a large number of RO led to area overhead.

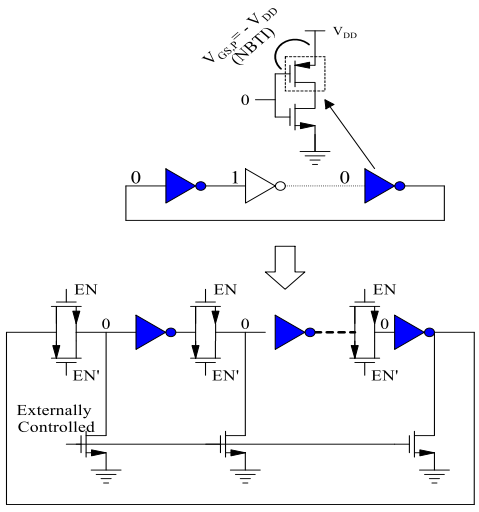


Fig. 8. Circuit technique to accelerate NBTI stress on each inverter [32]

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

- For CRO PUF, post-fabrication information on oscillation frequency is required to find 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.
- Area inefficient: The amount of MUX in the cascaded architecture increases [22,35], and an increase in the number of CRO leads 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 sensor) or lower the aging (used in PUF) but not both.
- Finally, using a large number of NBTI-aware RO in AN-CDIR [36] improves % m at the cost of area overhead.

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 a RO with both aging acceleration and retardation properties to make it suitable for 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.

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.
- Cascaded combination of proposed inverter without MUX behaves as CRO.
- The proposed CRO possess both aging acceleration and retardation feature.
- The application of proposed CRO as PUF to generate reliable responses, and sensor for detection of recycled ICs.

The proposed CRO's architecture, functionality, and application is briefed in the next section.

4. Proposed CRO

The block diagram of CRO designed using the 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 the proposed inverter.

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

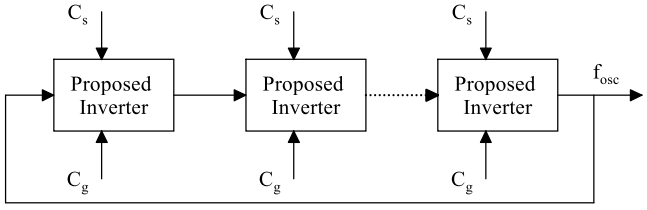


Fig. 9. Block diagram of proposed CRO

4.1 Proposed inverter

Inspired by the research work in [30], two voltage control sections drive the proposed inverter. As shown in Fig. 10, the proposed architecture consists of a conventional CMOS inverter with two voltage-control section, 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 signal C_s is 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 voltage (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 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 combination 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 conventional CMOS inverter. The remaining pattern reduce 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 ($t_p, P = f(V_{DD})$ [27]). This feature makes the proposed inverter suitable to design CRO.

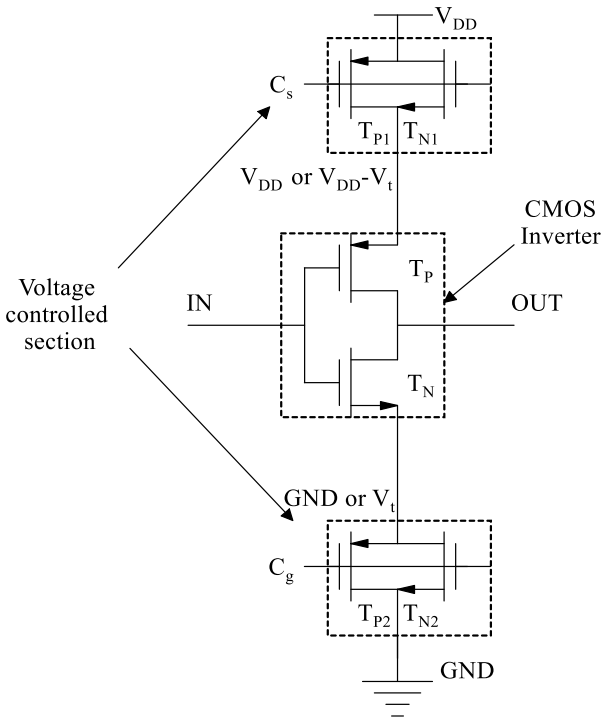


Fig. 10. Proposed inverter

4.2 Architecture of proposed CRO

The proposed CRO architecture is shown in Fig. 11. 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 frequencies. This is due to each cascaded inverter's different set of operating voltage (Table 3). The use of an inverter with a control signal eliminates the requirement of MUX as in conventional CRO [22]. Each inverter section consists of two selection lines; a CRO with an m-cascaded inverter can be configured as 22m different RO.

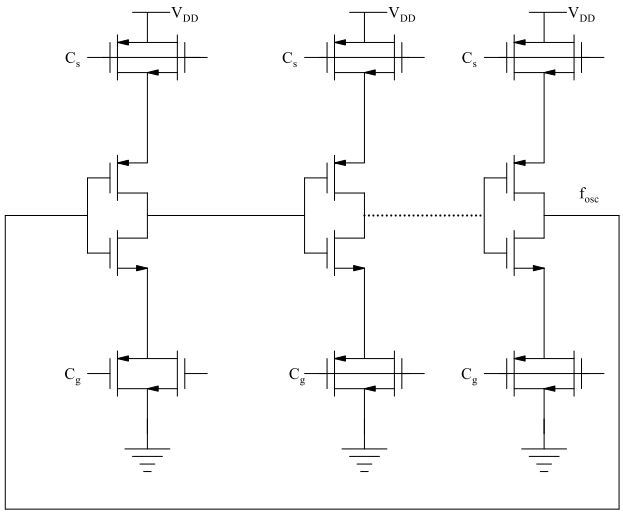


Fig. 11. Proposed CRO

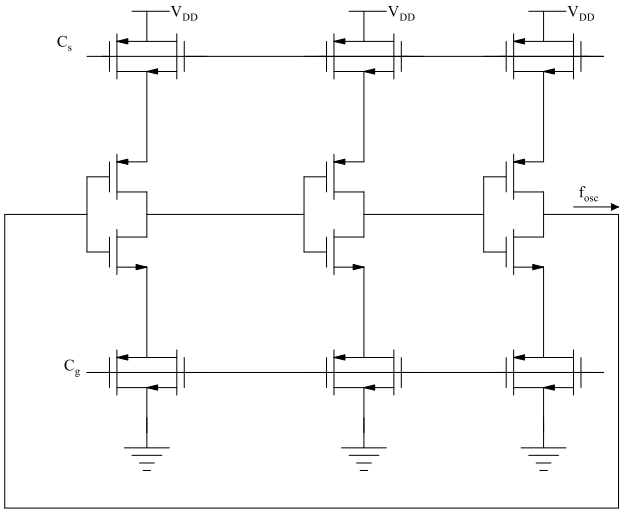


Fig. 12. CRO with 3-stages of inverter

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

4.3.1 Frequency deviation against temperature variation

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

$$\Delta f_{osc}\big|_T = \frac{f_{osc}\big|_{T=27\,^0C} - f_{osc}\big|_{T=T}}{f_{osc}\big|_{T=27\,^0C}} \qquad (4)$$

Where, $f_{osc}\big|_{T=27\,^0C}$ is the original frequency of RO at room temperature, and $f_{osc}\big|_{T=T}$ 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. 13(a). From this plot, it is observed that different logic level of control signal (C_s and C_g) results in different magnitude of frequency deviation. For analysis, the frequency deviation of proposed CRO is compared against all the existing types of RO, i.e. CRO [22], and RO with reduced supply voltage [35]. The result infers: -

- All the 4-different input pattern in the proposed CRO results in different frequency deviation, but less than conventional CMOS inverter based CRO [22].
- 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, reduction in operating voltage of 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 [35], 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, possibility of frequency crossover (Fig. 4) is minimized at higher temperature, and the reliability of PUF against temperature variation is improved (briefed in Section 6).

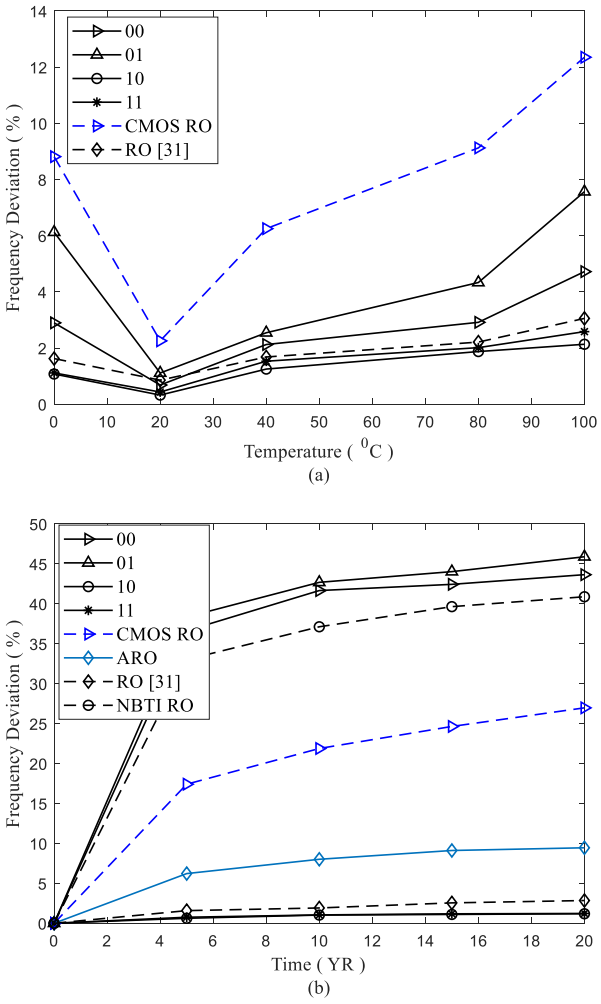


Fig. 13. Frequency deviation against (a) Temperature variation (b) Aging

4.3.2 Frequency deviation against aging

Like temperature, aging also causes continuous but permanent degradation in the oscillation frequency of RO. As discussed in Section 3, NBTI is the primary aging mechanism, and the magnitude of negative bias across PMOS [28, 32] 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. 14. The reason to choose C_s only is that it determines the magnitude of negative bias across all the PMOS in the 1st row of the inverter. The different amount of NBTI stress on PMOS for the different logic level of C_s is briefed as follows: -

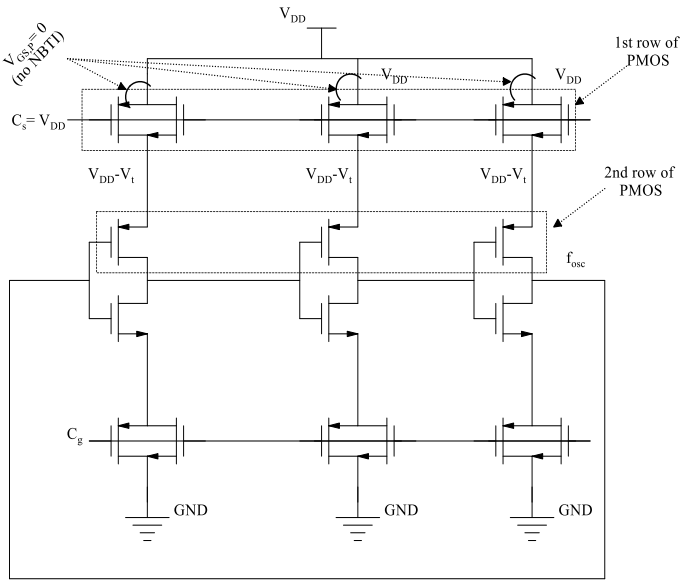
- A logic-1 at C_s causes zero bias i.e. $V_{GS,P}$=0 across all the PMOS in the 1st row (Fig. 14(a)). As a result, all the PMOS experience negligible amount of NBTI stress.
- As shown in Fig. 14(b), a logic-0 at C_s cause, $V_{GS,P} = -V_{DD}$ across all the PMOS in the 1st row of cascaded inverter.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

These two different amounts of NBTI stress on the proposed CRO signifies 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 [20,22].

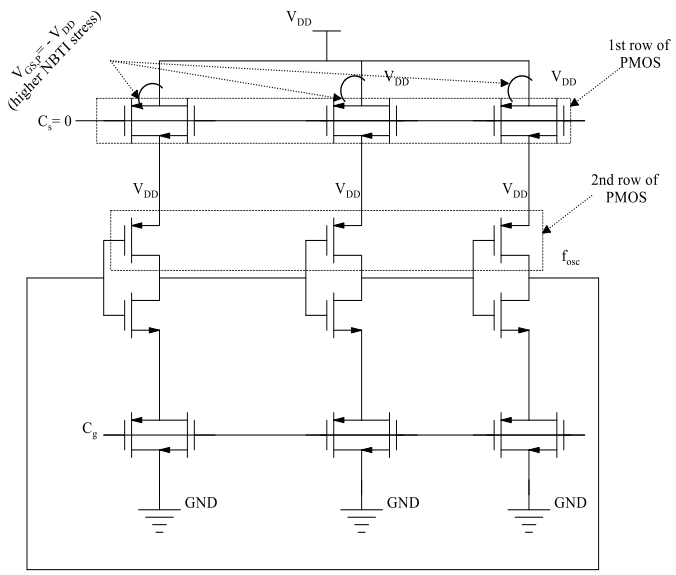
The frequency deviation in the proposed CRO due to aging is measured by using the expression (5), and compared against ARO [32], RO with reduced supply voltage [35], CMOS RO [18], NBTI aware RO used in AN-CDIR [36]. The frequency deviation is the measure of degradation in oscillation frequency from time t=0 to throughout stress time (t), given as follows: -

$$\Delta f_{osc}\big|_t = \frac{f_{osc}\big|_{t=0} - f_{osc}\big|_{t=t}}{f_{osc}\big|_{t=0}} \qquad (5)$$

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



(a)



(b)

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

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. 13(b) and summarized in Table 4. The comparison summary infers: -

- Accelerated NBTI stress due to logic-0 at C_s (both 00 and 01), result in 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 level of C_s (between [0X] and [1X]). However, deviation is less dependent on logic level of C_g ([C_s X]). This is due to reduction in operating voltage of inverter from V_{DD} to $V_{DD} - V_t$, when C_s switches from logic-0 to logic-1
- Both the accelerated (for C_s=0) and lower (for C_s=V_{DD}) aging feature of 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 [36] respectively.

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

4.3.3 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 quantizes 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.

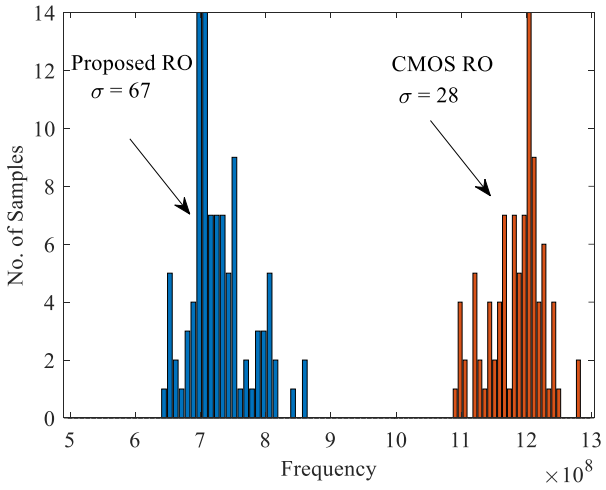


Fig. 15. Impact of PV on f_{osc}

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

- CMOS RO oscillates at a supply voltage of V_{DD} results 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 component against PV. The average value of oscillation frequency in proposed RO is lowered due to 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 results 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 [22].
- The proposed CRO can achieve both i.e. acceleration and retardation of aging, hence suitable for both sensor and PUF application.
- Finally, proposed CRO is also both area and power efficient due to elimination of MUX and reduction in swing of operating voltage.

5. 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 feature.
- **RO sensor**: Accelerated aging property of proposed CRO, enhances the rate of detection of recycled IC with less area overhead.

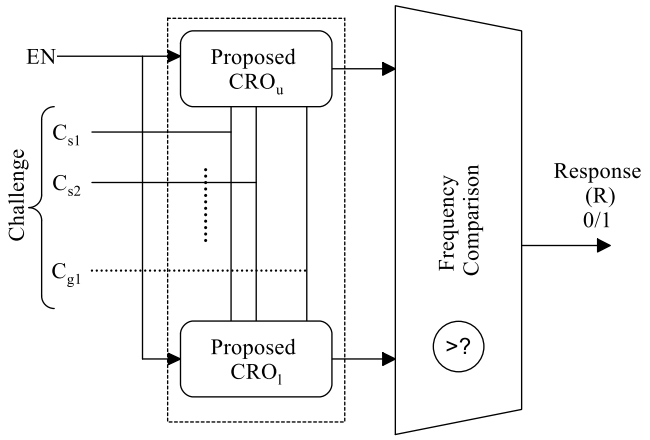


Fig. 16. Proposed CRO PUF

5.1 Design of CRO PUF

The architecture of proposed CRO PUF is shown in Fig. 16. It consists 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 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 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 different number of CRP is possible depending on the way how C_s and C_g is configured in the cascaded inverter. The proposed CRO PUF with different configuration 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 pattern is always limited to four and not affected by the number of stages of cascaded inverter (m) The PUF architecture with this type of CRO, is classified as weak CRO PUF.
- However, the control signal of each stage of 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 pattern. As the number of possible challenge pattern increases with increase m, the PUF with this type of CRO behaves as a strong CRO PUF.

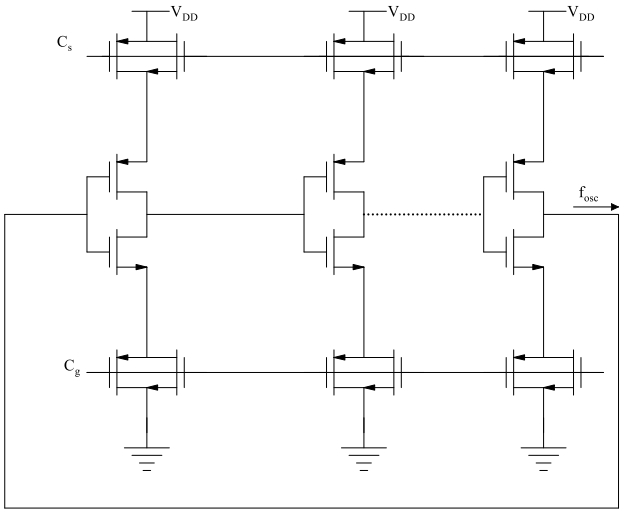


Fig. 17. Weak CRO (number of RO=4)

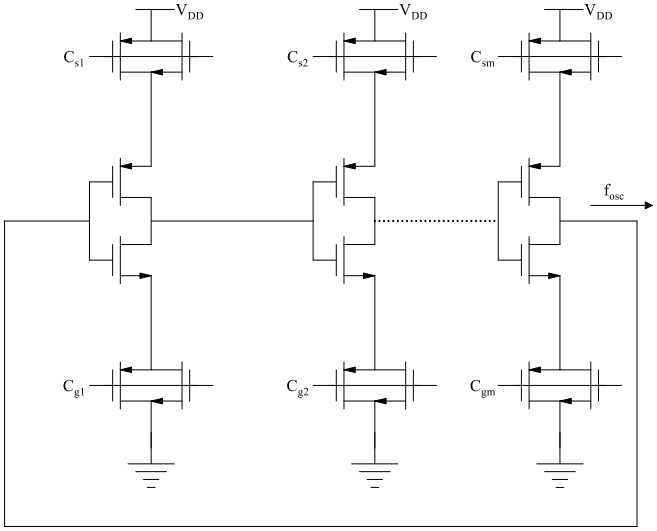


Fig. 18. Strong CRO (maximum possible number of RO =2^{2m})

5.2 *Design of RO sensor*

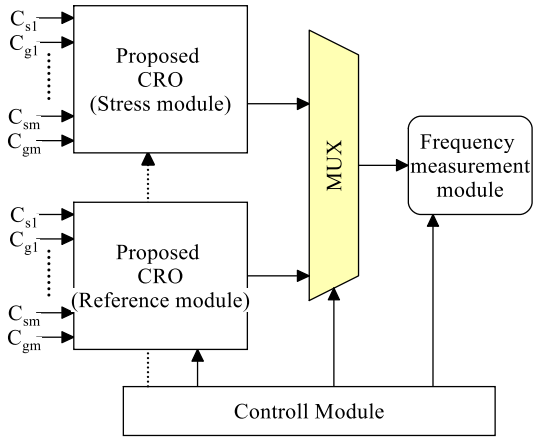


Fig. 19. RO sensor using proposed CRO

The second objective of this research work is to design a lightweight RO sensor for detection of recycled ICs. The architecture of sensor using proposed CRO is shown in Fig. 19. This architecture is similar to conventional RO sensor [17], but the RO section is designed using proposed 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 a group of RO, hence the functionality of this architecture is similar to that of AN-CDIR [36].

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 module are designed using equal stages of cascaded inverter to oscillate at 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 inverter (C_{s1}= C_{s2}=… C_{sm} = V_{DD}). As a result, the impact of NBTI stress is completely eliminated (Fig. 14(a)), and the RO preserve its original manufactured oscillation frequency.
- Further, in stress mode the impact of NBTI on all possible RO in stress module is accelerated by driving logic-0 at C_s (C_{s1}= C_{s2}=… C_{sm} = 0), as shown in Fig. 14(b). 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 stress module (due to degradation in oscillation frequency). Further, this difference depends upon the aging accelerating property of proposed CRO.
- In the authentication mode, for different logic level 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. 13) enhances the overall reliability of CRO PUF.
- The proposed CRO PUF with fewer cascaded inverter results in large number of CRPs. For e.g., a 3-stages of cascaded inverter in each CRO module (CRO_u or CRO_l) can be configured as 64-possible RO.
- Use of proposed CRO as sensor, improves the rate detection 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 right (Fig. 7) led to improvement in % m.
- Finally, use of proposed CRO architecture (Fig. 18), rather than a group of individual RO in AN-CDIR [36] led to

(a) improvement in %m: a greater number of RO causes narrow spread (as expression (3)) which led to improvement in % m.

(b) lower area overhead due to area efficient property of CRO against RO.

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

6. 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 1V and 27 ºC. Two different analysis is carried 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 fabrication process. It uses statistical transistor modelling provided by the foundry. This helps in measuring the security metrics of PUF [37], and spread of F_{DIF} [36] 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 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 sensor.

6.1 Performance analysis of proposed CRO PUF

The performance of the proposed CRO PUF is compared against the conventional CRO PUF [22], ARO-based CRO PUF [32], and CRO PUF with reduced supply voltage [35]. 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 [22, 32, 35]. 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 PUF to measure different security metrics.

6.1.1 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 voltage (Table 3). Hence, it is also required to find out the best and worst possible challenge patterns and corresponding reliability. The different security metrics are 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: -

(i) 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 as follows [37],

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

$$\text{Re}liability = 100\% - BER \quad (7)$$

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

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

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 the Fig. 20. 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 challenge.
- Then the same set of challenge is applied by varying the temperature from 0 to 100 ºC, to collect different responses. The BER obtained by using (6) is shown in the Fig. 20(a), and the corresponding reliability is reported in Table 5.

Similarly, to measure the BER against aging, all the considered CRO PUF architecture are subjected to continuous stress for a period of 20-years. The BER at different aging instance is shown in Fig. 20(b), 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 as fresh netlist.
- All the considered PUF experience aging continuously for a period of 20-years, and corresponding aged SPICE netlist is extracted at a time interval of 5,10,15, and 20-years.
- Identical challenge pattern is applied to both fresh and aged netlist, and the corresponding percentage of bit flip is observed.

As shown in Fig. 20, the proposed CRO PUF possess lower BER as compared to all the considered CRO PUF i.e., close to 5% at a higher temperature of 100 ºC, and less than 2% after a continuous stress for a period of 20-year. Although, the BER in proposed CRO PUF is slightly improved against the CRO PUF [35], but higher improvement is observed against conventional CRO PUF [22]. This improvement in reliability is due to: -

- Lower frequency deviation of 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, higher impact of PV on f_{osc} (Fig. 15) causes wider separation among frequency component in the selected pair of RO. As a result, possibility of frequency crossover is also minimized.

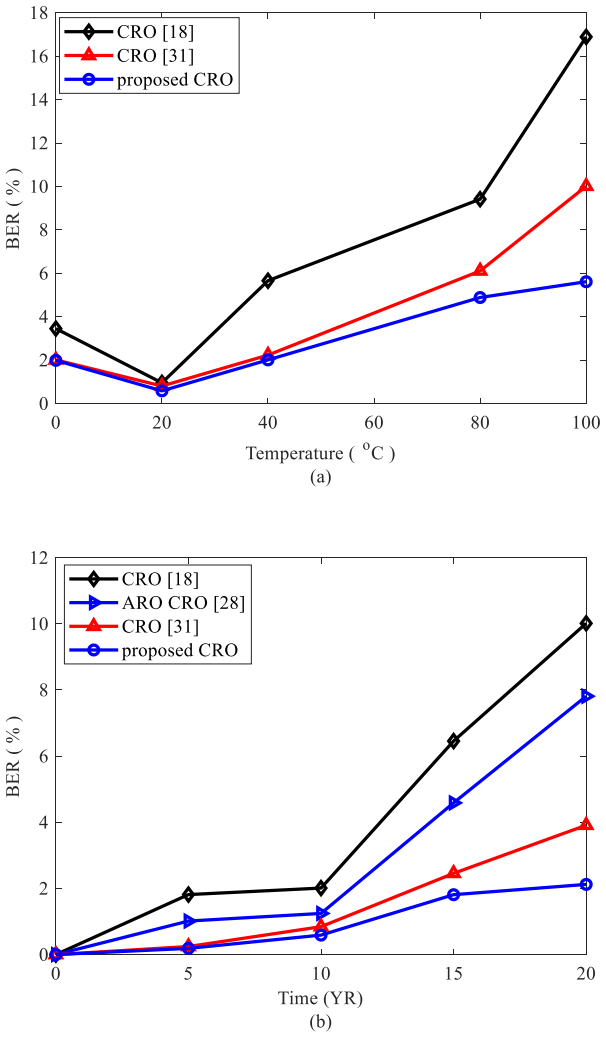


Fig. 20. BER in different types CRO PUF against (a) Temperature variation (b) Aging

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

- A group of challenge pattern 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 pattern 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 pattern cause different amount of frequency degradation (Table 4), results in different BER against temperature variation and aging. These challenge pattern led to best and worst reliability as reported in Table 6, and the corresponding BER is shown in Fig. 21. 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 ºC 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%). These set of challenge pattern led to a very low BER i.e., close to 1 % against both the variation.

Very low BER i.e., higher reliability of proposed CRO PUF implies, it can reproduce almost all response bit correctly against temperature variation and aging. As a result, the extracted response found suitable to be used as secure-key in different application [38,39,40].

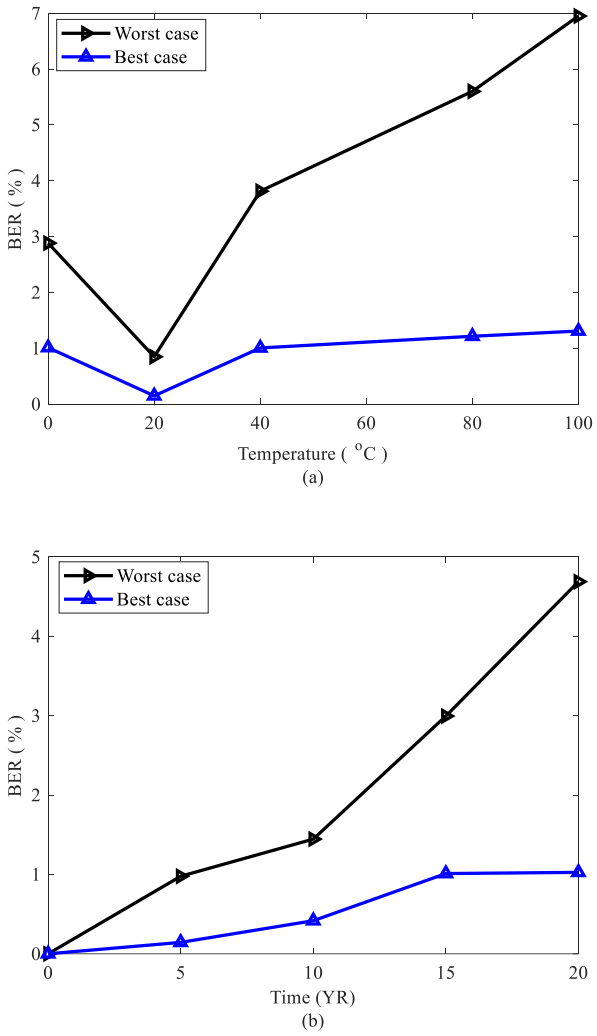


Fig. 21. Best and worst BER in the proposed CRO PUF against (a) Temperature variation (b) Aging

(ii) Uniqueness: -

To measure the uniqueness, response bit is collected by applying same challenge simultaneously to all the 100-different instances of PUF. Like this on an average 5000 CRPs are

collected. The average value of uniqueness is reported in Table 5. The result shows higher uniqueness of the proposed CRO PUF as compared to all the considered CRO PUF. This higher value is due to higher impact of PV on oscillation frequency of RO.

Similarly, other security metrics like, uniformity, SAC is also measured from the extracted response, and 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 is comparable with all the conventional CRO PUF architecture.

Further, the reliability of proposed CRO PUF is measured by increasing the number of CRO from 64 (m=3) to 1024 (m=5) and reported in Table 7. The measured reliability shows very less degradation.

6.2 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 [36] 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 module consist 64-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 module with 3-stages of cascaded inverter (Fig. 18).
- Monte Carlo simulation with 200-iteration is carried for each sensor in order to collect PV dependent frequency, which is used to observe the spread of F_{DIF} at different aging interval.
- 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 sensor is shown in Fig. 22. The reason to choose lower aging interval, because at higher aging interval a recycled IC can be easily detected. The efficiency of a sensor is measured by its ability to detect a IC which experience 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 sample lies in the overlap region between: -

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

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 $F_{DIF}|_{t=0}$, 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.
- $F_{DIF}|_{t=0}$, indicates the average of all the frequency difference obtained from each instances of a sensor. (no NBTI)
- The μ of $F_{DIF}|_{t=0}$ 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_{DIF}.
- This process repeated across the 200-different instances of both the considered RO sensor, and the overall spread of F_{DIF} at t=2D and 4D is shown in Fig. 22.
- The μ of both the spread $F_{DIF}|_{t=2D}$ and $F_{DIF}|_{t=4D}$ shifts toward right from $\mu|_{t=0}$, and the shift increases with increase in stress duration from 2D to 4D i.e. $\left[(\mu|_{t=4D} - \mu|_{t=0}) > (\mu|_{t=2D} - \mu|_{t=0})\right]_{AN-CDIR\,or\,proposedSensor}$
- As shown in Fig. 22, at higher aging interval (t=4D), the spread of $F_{DIF}|_{t=4D}$ in both the considered sensor is far apart from its original spread i.e $F_{DIF}|_{t=0}$. As there is no-overlap region between these two spreads, hence %m=0, for both the considered sensor.
- However, at lower aging interval i.e. t=2D, shift in spread of F_{DIF} is less, led to overlap between the spreads $F_{DIF}|_{t=2D}$ and $F_{DIF}|_{t=0}$ 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 proposed CRO as compared to NBTI aware RO used in AN-CDIR [32]. As given in Table 4, proposed CRO experience an accelerated degradation (for C_s=0) of 12 % higher than the RO used in AN-CDIR.
- As a result, shift in the μ value of F_{DIF} is more towards right, in proposed sensor as compared to AN-CDIR i.e. $\left[(\mu|_{t=2D} - \mu|_{t=0})\right]_{CRO} > \left[(\mu|_{t=2D} - \mu|_{t=0})\right]_{AN-CDIR}$

This above discussion clarifies, 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 interval both the RO sensor can detect all the recycled IC efficiently.

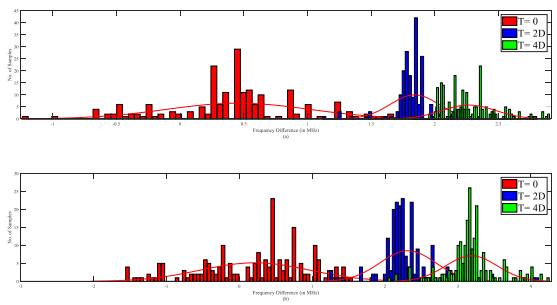


Fig. 22. Misprediction analysis from the spread of F_{DIF} in (a) AN-CDIR sensor (b) proposed CRO sensor

6.3 VLSI Metrics

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 [35] and 70 % more than the conventional CRO PUF [22]. 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 pattern 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. 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 [35] and conventional CRO PUF [22].

Finally, the proposed CRO sensor is also 80 % area-efficient compared to the AN-CDIR sensor [36]. 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 signal).

7. 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 (see Table 4), depending on the Cs' 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 [35].
- The reliability of proposed CRO PUF against both aging and temperature variation is improved. The best-case challenge pattern (see Table 6) results in 99 % reliability, which is close to the ideal value. It is due to a higher aging tolerant feature of proposed CRO.
- In the proposed CRO sensor, the % m is improved by 75 % compared to conventional AN-CDIR at a small aging interval of 2-D. It is due to aging accelerated feature of proposed CRO.
- The proposed CRO is also area efficient. This is due to difference in CRO architecture i.e., a conventional CRO [22] consist two rows of cascaded inverter with MUX, CRO in [35] 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 proposed CRO are area efficient.
- The lower power budget of proposed CRO PUF is due to reduction in 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 (see Table 4). But, this shortcoming of proposed CRO is compensated by the design of CRO without MUX and a greater number of possible RO (2^{2m}) with few stages of cascaded inverter only.

8. 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.

Data Availability Statement

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

REFERENCES

[1] I. Butun, P. Österberg and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures," in *IEEE Communications Surveys & Tutorials*.

[2] K. Yang, D. Blaauw and D. Sylvester, "Hardware Designs for Security in Ultra-Low-Power IoT Systems: An Overview and Survey," in *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," in *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1207-1228, 2014.

[4] Krishnan P, Jain K, Buyya R, Vijayakumar P, Nayyar A, Bilal M, Song H. MUD-based Behavioral Profiling Security Framework for Software-defined IoT Networks. IEEE Internet of Things Journal. 2021 Sep 17.

[5] Hatti K, Paramasivam C. Design and Implementation of Enhanced PUF Architecture onFPGA. International Journal of Electronics Letters, Jan 2;10(1):57-70, 2022.

[6] Rajan A, Sankaran S. Lightweight and Attack-resilient PUF for Internet of Things. In2020 IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS) pp. 139-142.2020.

[7] Nimmy K, Sankaran S, Achuthan K. A novel lightweight PUF based authentication protocol for IoT without explicit CRPs in verifier database. Journal of Ambient Intelligence and Humanized Computing. pp. 1-6, 2021.

[8] J. Cassell, Reports of Counterfeit Parts Quadruple Since 2009, Challenging US Defense Industry and National Security, 2012.

[9] L. Kessler, T. Sharpe, Faked Parts Detection, Circuits Assembly, the Journal for Surface Mount and Electronics Assembly, 2010.

[10] M. Rostami, F. Koushanfar and R. Karri, "A Primer on Hardware Security: Models, Methods, and Metrics," in *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1283-1295, 2014.

[11] S. P. Skorobogatov, "Semi-invasive attacks- a new approach to hardware security analysis, " *in Technical report UCAM-CL-TR-630*, university of cambridge computer laboratory, 2005.

[12] C. Herder, M. Yu, F. Koushanfar, and S. Devadas, "Physical unclonablefunctions and applications: A tutorial," *Proc.of IEEE*, vol. 102, no. 8, pp.1126-1141, 2014.

[13] D. S. Boning and S. Nassif , 'Models of Process Variations in Device and Interconnect,' *Design of High Performance Microprocessor Circuits*, chapter 6.

[14] C. Chang, Y. Zheng and L. Zhang, "A Retrospective and a Look Forward: Fifteen Years of Physical Unclonable Function Advancement," in *IEEE Circuits and Systems Magazine*, vol. 17, no. 3, pp. 32-62, thirdquarter 2017.

[15] S. Joshi, S. P. Mohanty and E. Kougianos, "Everything You Wanted to Know About PUFs," *in IEEE Potentials*, vol. 36, no. 6, pp. 38-46, 2017.

[16] Y. Zhang and U. Guin, "End-to-End Traceability of ICs in Component Supply Chain for Fighting Against Recycling," in *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 767-775, 2020, doi: 10.1109/TIFS.2019.2928493

[17] X. Zhang and M. Tehranipoor, "Design of On-Chip Lightweight Sensors for Effective Detection of Recycled ICs," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 22, no. 5, pp. 1016-1029, 2014.

[18] R. S. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-Way functions," *Science,* vol. 297, pp. 2026-2030, 2002.

[19] B. Gassend, D. Clarke, M. van Dijk, and S. Devdas, "Silicon physical random functions," in Proc. 9th ACM. Conf. Computer Communication security, pp. 148-160, 2002.

[20] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," *In Proc. of ACM/IEEE Design Automation Conference*, pp. 9-14, 2007.

[21] S. S. Kumar, J. Guajardo, R. Maes, G. J. Schrijen, P. Tulys, "The Butterfly PUF: Protecting IP on every FPGA," *in proc. IEEE Int. workshop. on HOST.*, pp. 67-70, 2008.

[22] A. Maiti, and P. Schaumont, "Improved Ring oscillator PUF: An FPGA-friendly secure primitive," *J. Cryptology*, pp. 375–397, 2010.

[23] J. Guajardo, S. S. Kumar, G. J. Schrijen and P. Tuyls, "FPGA intrinsic PUF and their use for IP protection," *in proc. of Int. workshop on Cryptographic Hardware & Embedded Systems. LNCS,* vol. 4727, pp. 63-80, 2007.

[24] 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.

[25] D. Ganta and L. Nazhandali, "Study of IC aging on ring oscillator physical unclonable functions, " in *Fifteenth International Symposium on Quality Electronic Design*, pp. 461-466, 2014.

[26] A. Maiti and P. Schaumont, "The impact of aging on a physical unclonable function, " *in IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, pp. 1854-1864, 2014.

[27] J.M. Rabaey, A. Chandrakasan, B. Nikolic, '*Digital Integrated Circuits: A Design perspective*' 2e Prentice-Hall, Upper saddle River, NJ, 2002.

[28] A. Tiwari and J. Torrellas, "Facelift: Hiding and slowing down aging in multicores," *in Microarchitecture, 41st IEEE/ACM International Symposium*, pp. 129-140, 2008.

[29] Y. Cao, L. Zhang, C. H. Chang, and S. Chen, "A Low-Power Hybrid RO PUF With Improved Thermal Stability for Lightweight Applications," *IEEE Trans. On CAD of Integ. Ckt. And Syst.,* vol. 34, no.7, pp. 1143-1147, 2015.

[30] C. Q. Liu, Y. Cao and C. H. Chang, "Low-power, lightweight and reliability-enhanced current starved inverter based RO PUFs," *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, pp. 646-649, 2016.

[31] S. R. Sahoo, S. Kumar and K. Mahapatra, "A Novel Reliable and Aging Tolerant Modified RO PUF for Low Power Application," *in Analog Integrated Circuits and Signal Processing, Springer*, 103, pp. 493-509, 2020.https://doi.org/10.1007/s10470-018-1317-z.

[32] M. T. Rahman, F. Rahman, D. Forte and M. Tehranipoor, "An Aging-Resistant RO-PUF for Reliable Key Generation,*" in IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 3, pp. 335-348, 2016.

[33] 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," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 12, pp. 3138-3149, Dec. 2017.

[34] S. R. Sahoo, S. Kumar, K. Mahapatra and A. Swain, "A Novel Aging Tolerant RO-PUF for Low Power Application," *IEEE International Symposium on Nanoelectronic and Information Systems (iNIS),* pp. 187-192, 2016.

[35] S. R. Sahoo, S. Kumar and K. Mahapatra, "A novel configurable ring oscillator PUF with improved reliability using reduced supply voltage," *Microprocessors and Microsystems*, *60*, pp.40-52, 2018.

[36] U. Guin, D. Forte and M. Tehranipoor, "Design of Accurate Low-Cost On-Chip Structures for Protecting Integrated Circuits Against Recycling," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 24, no. 4, pp. 1233-1246, 2016.

[37] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of PUF," *Embedded systems design with FPGAs*, pp. 245-267, 2013.

[38] S. R. Sahoo, S. K, A. Mahapatra, A. K. Swain and K. K. Mahapatra, "On-chip RO-Sensor for Recycled IC Detection," *IEEE International Symposium on Nanoelectronic and Information Systems (iNIS),* pp. 252-256, 2017.

[39] S. K. Ram, S. R. Sahoo, B. B. Das, K. mahapatra and S. Mohanty, "Eternal-Thing: A Secure Aging-Aware Solar-Energy Harvester Thing for Sustainable IoT," in *IEEE Transactions on Sustainable Computing*, vol. 6, no. 2, pp. 320-333, 2020.

[40] Saswat K. Ram, Banee B. Das, Kamalakanta Mahapatra, Saraju P. Mohanty, and Uma Choppali. 2021. Energy Perspectives in IoT Driven Smart Villages and Smart Cities. IEEE Consumer Electronics Magazine vol. 10, no. 3, pp, 19–28, 2021.