# A Novel Aging Tolerant RO-PUF for Low Power Application

*Sauvagya Ranjan Sahoo, Sudeendra Kumar, Kamalakanta Mahapatra, Ayaskanta Swain*
*NIT Rourkela,Odisha*
*email:{sauvagya.nitrkl, kumar.sudeendra, kmaha2, swain.ayas}@gmail.com*

***Abstract*— Physical Unclonable Functions (PUFs) is one of the popular security primitives for IC which is mainly used for identification and cryptographic application. Although various environmental parameter affect its performance but aging causes permanent degradation in its reliability. This paper presents a modified aging tolerant architecture for ring oscillator based PUF (RO-PUF) in which the conventional CMOS based ROs are replaced by modified RO. The proposed architecture for RO shows high tolerance to aging as compared to existing RO. Further the proposed RO minimizes the overall power consumption of RO-PUF. Simulation results in 90 nm technology shows improvement in power consumption and security metrics of proposed RO-PUF as well as it is more area efficient as compared to existing aging tolerant RO-PUF.**

***Keywords*— Physical Unclonable Function (PUF); Challenge-Response pair (CRP); Aging; process variation (PV).**

## I. INTRODUCTION

In the current era of IoTs, along with power and performance, security issue [1] of IC is a key aspect because of its pervasiveness. Several primary security aspects of IC includes authentication, identification of malicious element at different level of fabrication [2], prevention from active and passive attacks [3] and detection of counterfeit IC [4]. Ignoring these security aspects will lead to major revenue losses to semiconductor industries.

In the past decade PUF has emerged as the most promising hardware security primitive for IC identification. The traditional identification method consists storing the crypto key in ROM/EPROM. The memory is vulnerable and adversaries can leak the key using various methods like side-channel analysis etc. The PUF based approach generates does not store any key. Key is generated when IC is powered up and it is difficult for the adversary to crack the system.

A PUF is a standalone or small circuit embedded inside the IC which generates response from inherent manufacturing PV, hence also called as IC/Si biometric. The biometric signifies even if the same PUF is fabricated multiple times using same fabrication process but each one will generate unique response due to manufacturing variability.

A state of art of different PUF topologies proposed can be found in the literature [5-10]. Pappu et al. is the first to coin this term and proposes a non-Si PUF i.e. optical PUF [5]. Latter on several Si based PUFs like Arbiter PUF [6], RO-PUF [7], SRAM PUF [8], and composite PUF [9], hybrid PUF [10] etc. is proposed. All these different PUF explores the randomness in the delay variation of MOSFET and interconnects to extracts the response bits. A Set of response bits obtained from PUF with respect to applied inputs (challenges) called as challenge response pair (CRP). Among the several existing PUF architecture RO-PUF is widely used because of its simple architecture, easy validation in both FPGA/ASIC and more resilient against model building attack. Despite of its several advantages further enhancement in its security metrics [11] and power consumption needs to be improved.

The quality of PUF is determined by measuring its security metrics like uniqueness, reliability and randomness. Although the same PUF architecture is replicated in different IC for identification, the response/key generated by the PUF must be unique to that IC only. The uniqueness feature is used to distinguish the IC in the large group.

The reliability determines the stability of response bit over environmental variation (Temperature & $V_{DD}$) and time (aging). Due to environmental variation any change in response bits regain its original value once the PUF returns to its normal operating environment. In the case of aging effects like Negative Bias Temperature Instability (NBTI), Hot Carrier Injection (HCI), Electromigration (EM) etc. [12, 13, 14] causes permanent change to the response bits over time. So to mitigate the permanent reliability degradation due to various aging mechanisms the PUF architectures must show high tolerance to aging. Further PUFs are the additional circuit used along with the main circuit hence the amount power consumption by the PUF adds to the total power budget. So during the design of PUF architecture higher emphasis must be given to minimize the power budget as well as to enhance the security metrics.

In this paper we proposed a modified architecture for RO-PUF which leads to following contributions:-

- The modified RO-PUF architecture is highly sensitive to PV (higher uniqueness) and less sensitive to aging (lowers the reliability degradation).
- The power consumption of RO-PUF is minimized by reducing the supply voltage of the inverters used in RO (ring oscillator) section at a voltage lower than the standard supply voltage.

The rest of this paper is organized as follows. Section II elucidates briefly about RO-PUF [7] and reliability degradation due to aging. The performance analysis proposed RO is carried out in section III. In section IV, security metrics and power budget of proposed aging tolerant RO-PUF is compared against existing aging tolerant architecture. Finally, we concluded in section V.

## II. PRELIMINARIES

### *(A) RO-PUF*

The classical RO-PUF [7] is shown in Fig. 1. It consist k-number of identical ROs. The frequency of oscillation ($f_{osc}$) of RO is given as [7],

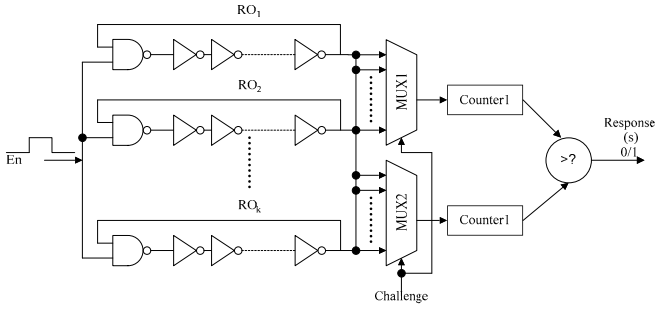



Fig. 1. RO-PUF [7]

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

Where, $t_p$: propagation delay of inverter.

$n_s$: number of inverter in a RO

Although each RO is designed by using equal number of cascaded inverter but manufacturing PV causes each RO to oscillate at slightly different frequency. Response bits are extracted from frequency comparison by selecting pair of RO through applied challenges to MUX. The logic level of response bits is as follows:

$$s = \begin{cases} 1 & if\ f_1 > f_2 \\ 0 & otherwise \end{cases} \qquad (2)$$

Where $f_1$ and $f_2$ are the frequencies of a selected pair of RO.

From the above discussion it is clear that logic level of response bits directly depends upon frequency of oscillation of RO**,** so any degradation in $f_{osc}$ impacts on the stability of the response bit.

*(B) Aging*

Aging causes continuous degradation in functioning of IC over time. Aging mechanisms includes NBTI, HCI, TDDB, EM etc. Out of several aging sources rate of degradation in $V_t$ primarily dominates by both NBTI and HCI [14]. The dependency of $V_t$ on aging is discussed as follows:-

***1) NBTI***

When the gate terminal of PMOS is subjected to a continuous DC-stress (logic-0) i.e. $V_{GS}$= -$V_{DD}$ (-ve Bias), it causes few Si-H bonds to break at the interface region between gate oxide and channel. This causes traps in the oxide layer results in increases in the $V_t$ of PMOS. The change in $V_t$ due to NBTI [14] is:-

$$\Delta V_{t,stress} = A_{NBTI} t_{ox} \sqrt{C_{ox}(V_{DD} - V_t)} e^{\left(\frac{V_{DD}-V_t}{t_{ox}E_0} - \frac{E_\alpha}{kT}\right)} t_{stress}^{0.25} \qquad (3)$$

Where $A_{NBTI}$ is a constant proportional to aging rate, $t_{ox}$ is the oxide thickness, $C_{ox}$ is gate capacitance per unit area $E_0$ and $E_\alpha$ are device dependent parameter, k is Boltzmann constant and $t_{stress}$ is the duration of stress/aging.

From (3) shift in $V_t$ depends upon the duration ($t_{stress}$) for which DC-stress being applied and the magnitude of –ve bias voltage at the gate terminal of PMOS.

***2) HCI***

Hot carriers are refers to the energetic electrons or holes which gains energy due to higher electric field in drain region. HCI effect is highly pronounced in NMOS devices as compared to PMOS and mainly at lower technology nodes. The AC-stress i.e. the logic switching at the gate of NMOS generates highly energetic electrons. These electrons generate traps in the oxide during collision. This causes shift in threshold voltage. The mathematical modelling of shift in $V_t$ [14], given as follows

$$\Delta V_{t,HCI} = A_{HCI} \alpha f e^{\frac{V_{DD}-V_t}{t_{ox}E}} t_{stress}^{0.5} \qquad (4)$$

Where $A_{HCI}$ is constant depends upon aging rate, α is activity factor, f is the frequency and E is a constant equals to 0.8 V/nm. The shift in $V_t$ mainly depends upon switching activity at the gate terminal of NMOS and the duration of applied stress.

From the above analysis aging causes:-

- Degradation in $V_t$ of both the PMOS and NMOS which is proportional to stress duration.
- Dependency of $t_p$ upon $V_t$ [15, 16], causes degradation in oscillation frequency of RO over time.

*(C) Reliability*

From our earlier discussion, reliability degradation occurs due to environmental variation as well as aging. As aging causes permanent degradation in reliability [26] hence in this section we have analyzed the effect of aging on RO-PUF and existing solutions in the literature.

The bit flip due to aging is shown in Fig. 2. Assume $f_1$ and $f_2$ are the frequency of oscillation of a selected pair of RO i.e. $RO_1$ and $RO_2$ respectively. Due to PV each one of the RO may possesses different rate of degradation. From Fig. 2(a), initially $f_1 > f_2$ but the faster aging in RO1 slower down its frequency lead to frequency crossover (response bit , s changes from 1 to 0) after certain time of aging. From Fig. 2(b) slower rate of degradation due to aging of the selected pair of RO avoids frequency cross over (no bit flip) over time and the corresponding pair is called as stable pair of RO.

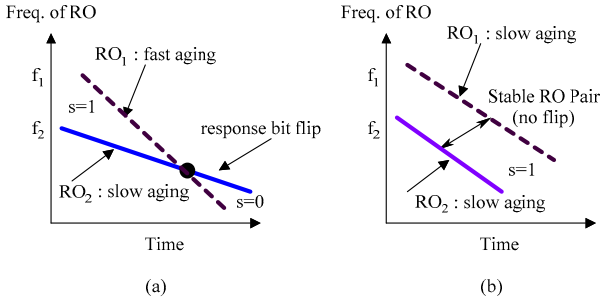



Fig. 2. Aging effect on response bit (a) frequency cross over due to faster aging (response bit flip) (b) no cross over (stable response bit)

***1) Existing techniques for reliability enhancement***

In order to improve the reliability degradation several techniques are proposed in the literature [17-23]. The primary concept behind all these techniques to select either a pair of RO [17] with highest frequency separation or multiple pair of RO [18] to avoid the bit flip over a range of operating temperature. But both these techniques require post manufacturing information about oscillation frequency. Similarly various error correcting codes (ECC) [19,20] is used to preserve the reliability but it uses response bit as hash function which is prone to attack by adversaries. These ECC increases overall area and power consumption. Furthermore, several circuit level techniques like separate body biasing [21], optimized supply voltage technique [22], additional temperature sensor along with memory [23] etc. are used to improve the overall reliability of PUF.

All these techniques discussed above enhance the reliability degradation due to variation in temperature. Although in several literature [24,25] the effect of aging on RO-PUF is discussed, but the first circuit level technique to minimize the reliability degradation due to aging is proposed in [26] called as aging tolerant RO-PUF (ARO-PUF). The Aging tolerant RO used in ARO-PUF is designed by using additional NMOS which drives the input of each inverter. Two numbers of NMOS per inverter section is used to minimize the effect of NBTI and HCI as compared to static CMOS RO. Although ARO significantly lowers the rate of degradation in $f_{osc}$ w.r.t. aging but it suffers from:-

- **Area overhead**: for a RO with n-number of cascaded inverters 2n number of additional NMOS is required.

## III. PROPOSED RO

The circuit diagram of proposed modified RO along with static CMOS based RO and ARO [26] is shown in Fig. 3. The working principle of the proposed RO architecture is same as static CMOS based RO except a NMOS ($T_N$) is used to drive supply voltage into the cascaded inverter section of RO, as shown in Fig. 3(c). Depending upon the logic level of En signal proposed RO operates as follows:-

- During the oscillating mode of RO (En=$V_{DD}$), $T_N$ turns ON and all the inverters are driven by a voltage level of $V_{DD}$-$V_{t,n}$. As the inverter section of RO operates at a voltage less than $V_{DD}$ this lead to reduction in oscillation frequency as well as improvement in total power consumption of RO as compared to CMOS RO and ARO.
- For En at 0V, the RO is in non-oscillating mode and at the same instant all the inverters are isolated from $V_{DD}$.

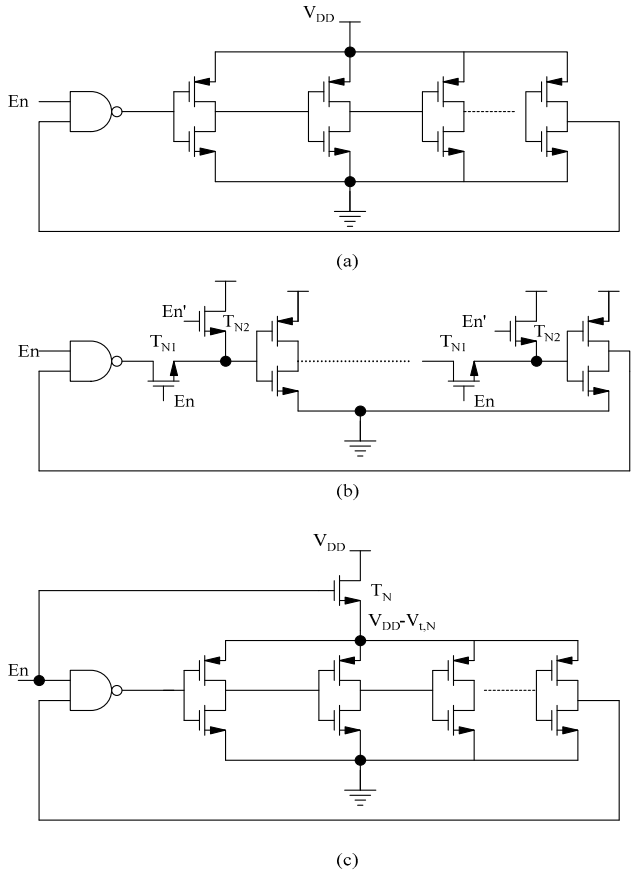



Fig. 3. Types of RO (a) CMOS RO (b) ARO [26] (c) Proposed RO

TABLE 1 POWER CONSUMPTION (IN μW) AND $f_{osc}$ COMPARISON

| Types of RO | Activation Time <in %> | | | | $f_{osc}$ <GHz> |
|---|---|---|---|---|---|
| | 20 | 40 | 80 | 100 | |
| CMOS RO | 7.486 | 14.93 | 29.73 | 36.28 | 6.259 |
| ARO | 5.732 | 11.19 | 22.09 | 26.81 | 3.640 |
| Proposed RO | 3.821 | 9.384 | 14.61 | 17.83 | 3.250 |

The performance analysis of the ROs is carried out in virtuoso environment by using 90 nm technology libraries from UMC. The $f_{osc}$ comparison for all the ROs is shown in Table 1. The cause for lower $f_{osc}$ in ARO as compared to CMOS RO is due to additional delay added by the NMOS devices which are inserted in between the cascaded chain of inverters. Whereas the proposed RO produces lower value $f_{osc}$ as compared to others due to supply voltage scaling by $T_N$. Several improvements in performance of proposed RO as compared to CMOS RO and ARO are briefed as follows:-

*(A) Sensitive to PV*

In order to observe the effect of PV on $f_{osc}$ prior to fabrication, statistical static timing analysis is being carried out using Monte Carlo simulation for 100 run. The additional NMOS transistors used in ARO and proposed RO inserts more PV as compared to static CMOS based RO as shown in Fig. 4. From the bar chart proposed RO possesses higher value of standard deviation (σ) as compared to other RO. This higher value of σ shows higher variation among the frequency components in a group of RO. As a result RO-PUF [7] designed by proposed RO is become more sensitivity to PV which lead to improvement in its security metrics. (Analyzed in next section)

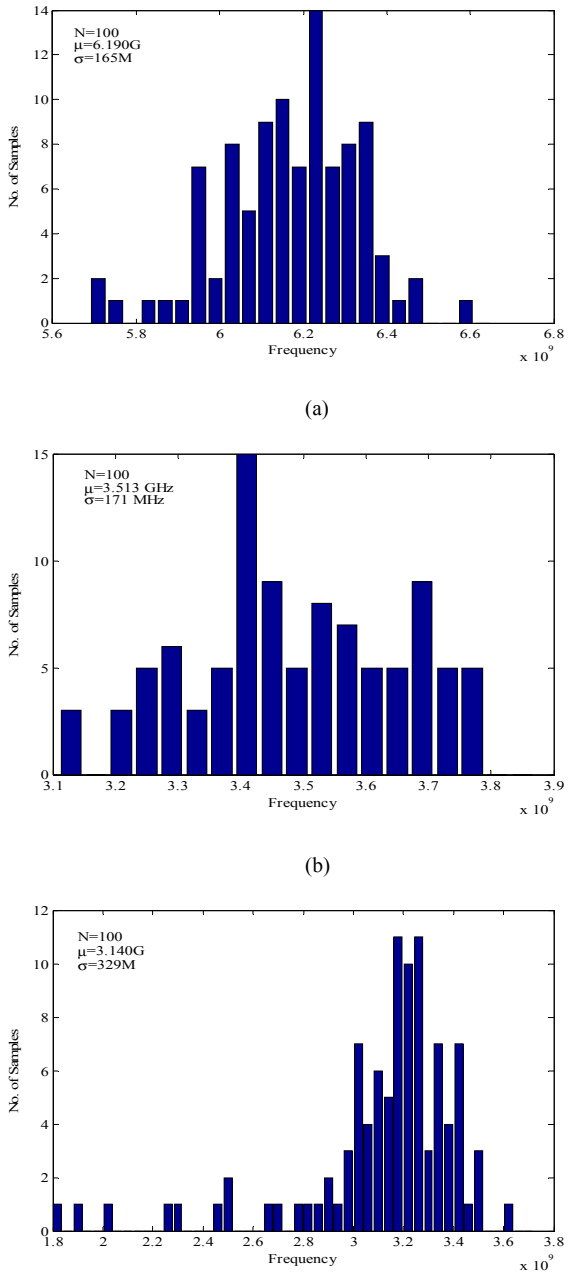


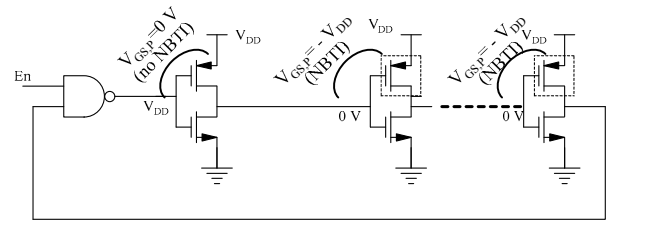

Fig. 4. Inter-die frequency variation (a) CMOS RO (b) ARO (c) Proposed RO

*(B) Degradation in $f_{osc}$ over time*

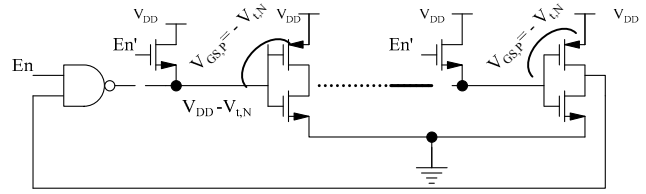
As discussed in the earlier section out of several aging mechanism the degradation occurs primarily by NBTI and HCI. In this section we have discussed the effect of both the aging mechanism during oscillating and non-oscillating mode of RO.

***1) Non-oscillating mode:***

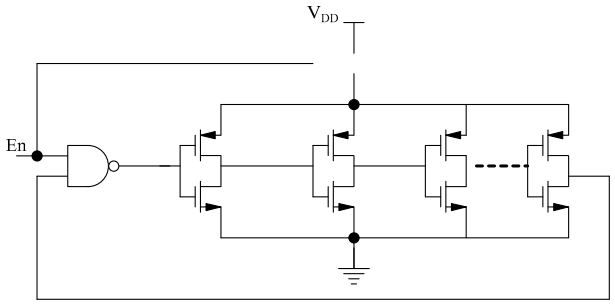
The non-oscillating mode (En=0) of all the three different RO is shown in Fig. 5. In case of static CMOS based RO 50 % of PMOS device in the cascaded chain of inverter experience constant NBTI stress due to logic 0 at their gate terminal ($V_{GS,P}$= -$V_{DD}$), as shown in Fig. 5(a). This –ve bias causes shift in threshold voltage of PMOS ($V_{t,P}$) [14], which leds to permanent degradation in $f_{osc.}$ . Whereas for ARO (Fig. 5(b).) the gate of all the PMOS devices are subjected to a constant stress of $V_{DD}$-$V_{t,N}$ (so $V_{GS,P}$=-$V_{t,N}$). Although in this architecture all the PMOS are subjected to constant DC stress but its magnitude is much less than CMOS RO. So degradation in $V_{t,P}$ is less as compared to CMOS RO. For the proposed RO, En=0 V drives $T_N$ into cut-off region as shown in Fig. 5(c). Hence, all the PMOS devices in the cascaded chain become isolated from supply voltage, as a result NBTI stress almost negligible. From this analysis, if all the ROs are subjected to NBTI for equal stress duration then proposed RO undergoes less degradation in $V_{t,P}$ as compared to others.




(a) CMOS RO




(b) ARO [26]




(c) Proposed RO

Fig. 5. NBTI effect during non-oscillating mode (En =0 V)

***2) Oscillating mode:***

In the oscillating mode (En=$V_{DD}$) continuous switching occurs at the output terminal of all the inverters. This switching causes degradation in threshold voltage of all the NMOS ($V_{t,N}$) devices due to HCI [14] effect and the rate of degradation depends upon switching activity. From Table 1 lower value of $f_{osc}$ of proposed RO as compared to other RO results in lower switching activity. Due to lower switching activity rate of degradation in $V_{t,N}$ is less for the proposed RO.

So from the above analysis the effect of both the stress is less on proposed RO as compared to other RO. As a result proposed RO shows lower degradation in $f_{osc}$. Table 2 shows the degradation in $f_{osc}$ over time by applying both NBTI and HCI stress simultaneously to all the three ROs. The rate of degradation is measured by comparing the $f_{osc}$ at initial time (t=0) with the aged value measured after time t, which is given as follows:-

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

The result confirms that proposed RO possesses lower rate of degradation in $f_{osc}$ as compared to others. Although ARO shows significantly lower rate of degradation as compared to CMOS RO, but for proposed RO negligible effect of NBTI causes lowers its rate of degradation as compared to ARO as well as CMOS RO. Further the rate of degradation in $f_{osc}$ increases with increase in stress duration.

TABLE 2 FREQUENCY DEGRADATION OF RO OVER TIME

| Time <in Yr> | Frequency Degradation ($\Delta f_{osc}$) <in %> | | |
|---|---|---|---|
| | CMOS-RO | ARO | Proposed-RO |
| 4 | 18.65 | 8.78 | 0.78 |
| 8 | 21.94 | 10.54 | 1.21 |
| 12 | 24 | 12.24 | 1.51 |
| 16 | 25.68 | 13.87 | 1.75 |
| 20 | 27.02 | 14.12 | 2.09 |

*(C) Low power consumption*

All the ROs are designed with equal number of cascaded inverter for comparing total power consumption. The total power of RO depends upon rate of switching activity at the output terminal of each inverter. The comparison result for different RO with different activation time (time duration for which RO is in oscillating mode) is given in Table 1. The proposed RO consumes around 50% less power as compared to its counterpart because of its lower switching activity due to lower $f_{osc}$. Further with increase in activation time power consumption by all the RO increases.

*(D) Area efficient*

From Fig. 3(b) and (c) the proposed RO requires only one NMOS ($T_N$) per RO section, whereas in ARO two NMOS ($T_{N1}$ and $T_{N2}$) per inverter section is used to minimize the effect of aging. So for designing RO with n-number of cascaded inverter, the proposed architecture requires only one additional NMOS as compared to 2n number of NMOS in ARO. Hence, the proposed architecture of RO is more area efficient than ARO.

## IV. RESULTS & DISCUSSION

The RO section of RO-PUF [7] as shown in Fig. 1 is replaced using different types of ROs as discussed in the earlier section like CMOS RO, ARO and proposed RO for various performance metrics comparison. For our analysis all the three RO-PUFs are designed in Cadence Virtuoso Environment using 90 nm CMOS technology libraries from UMC foundry. The performance summary is shown in Table 4.

*(A) Power consumption*

The RO section of PUF envisages the overall power budget of PUF because during CRP collection all the ROs are in oscillating mode and consumes significant power. Table 4 shows the power consumption per response bit collection. The proposed RO consume less power/response bit because of its lower oscillation frequency as compared other ROs.

*(B) Security metrics evaluation*

For our analysis Monte Carlo Simulation is carried out for three different types of RO-PUF with 100 iterations to extract the response bits. This is equivalent to collecting response bits from 100 different PUF IC. The RO-PUF architecture as shown in Fig. 1 is replicated 32-times to extract 32-bit response for a particular challenge. We have collected 100 CRPs per PUF to analyze different security metrics of PUF.

*1) Reliability:*

It is also called as intra-IC variation. The reliability degradation due to aging is measured as follows:-

- Spice netlist of all the RO-PUFs are extracted.
- A 32-bit (m) reference response ($S_i$) is collected by applying the challenges to the extracted netlist at nominal operating condition i.e. $V_{DD}$=1V and T=27$^0$C.
- The aged netlist of all the RO-PUFs are extracted by applying both NBTI and HCI stress. For each RO-PUF we have collected the aged netlist after 4, 8, 12, 16 and 20 years.
- Then at the same operating environment ($V_{DD}$=1V and T=27$^0$C), same set of challenge is applied to the extracted aged netlist for collecting the response bits ($S_j$). The degradation in $f_{osc}$ due to aging (discussed in section III) causes few response bits to flip. The percentage of bit flip is measured by using hamming distance (HD), expressed as:-

$$HD_{\text{int}ra} = \frac{1}{x}\sum_{y=1}^{x}\frac{HD(S_i, S_{j,y})}{m}\times 100\% \qquad (6)$$

Where, $S_{j,y}$ is the y$^{th}$ sample of $S_j$ and the HD between two responses are measured as follows:-

$$HD(S_i, S_j) = \sum_{t=1}^{32} S_{i,t} \oplus S_{j,t} \qquad (7)$$

Where, $S_{i,t}$ is the t$^{th}$ response bit of the 32-bit response string $S_i$.

- Table 2 shows percentage bit flip due to aging. The result shows that with increase in time (year) larger percentage of bit flip occurs due to higher rate of degradation in $f_{osc.}$ Since the proposed RO-PUF is more aging tolerant as compared to other RO-PUF, it suffers less percentage of response bit flip. As a result the reliability degradation of proposed RO-PUF is lowered as compared to other RO-PUF as shown in table 4
- Likewise 100 samples of response bit/PUF are collected to measure the overall reliability. The expression for reliability is given as [11],

$$\text{Reliability} = 100\% - HD_{\text{int}ra} \qquad (8)$$

TABLE 3 AVERAGE BIT FLIP ( %) DUE TO AGING

| Time <in Yr> | CMOS-RO | ARO | Proposed-RO |
|---|---|---|---|
| 4 | 3.254 | 0.132 | 0.054 |
| 8 | 4.213 | 0.557 | 0.171 |
| 12 | 5.387 | 1.654 | 0.451 |
| 16 | 7.652 | 2.458 | 0.971 |
| 20 | 9.812 | 4.654 | 1.435 |

*2) Uniqueness:*

It is also called as inter-IC variation. In order to measure the uniqueness, the same set of challenge is applied to 100 different instances (C) of RO-PUF created by Monte Carlo simulation. Although all the instances of RO-PUF consists same architecture but due to PV each instances generates different response bits. The variation among the response bits are measured using HD. The expression for uniqueness [11] is as follows,

$$\frac{2}{C(C-1)}\sum_{i=1}^{C-1}\sum_{j=i+1}^{C}\frac{HD(S_i, S_j)}{m}\times 100\% \quad (9)$$

The uniqueness comparison among different PUF is shown in Table 4. Since the proposed RO shows higher sensitive to PV (high value of σ in Fig. 4) it adds more variation among the response bit collected across different instances. As a result the overall uniqueness of proposed RO-PUF is higher as compared to other RO-PUF.

*3) Uniformity*

Uniformity of a PUF estimates how uniform the proportion of 0's and 1's is in the response bits of a PUF.
Uniformity Comparison is shown in Table 4.

$$\left(uniformity\right)_i = \frac{1}{m}\sum_{t=1}^{m} S_{i,t} \times 100\% \qquad (10)$$

TABLE 4 PERFORMANCE COMPARISONS FOR DIFFERENT RO-PUF

| Type of RO-PUF | Security Metrics [11] <in %> | | | Power consumption/ CRP <in µW> |
|---|---|---|---|---|
| | Uniqueness | Reliability | Uniformity | |
| RO-PUF [7] | 41.15 | 84.71 | 45.23 | 79.67 |
| ARO PUF [26] | 44.31 | 91.65 | 46.47 | 64.13 |
| Proposed RO-PUF | 46.22 | 95.89 | 45.12 | 42.75 |

## V. CONCLUSION

The proposed RO enhances the security metrics of RO-PUF because of its highly aging tolerance architecture. Further the lower oscillation frequency of RO improves the power consumption of PUF during CRP collection. This feature makes the PUF suitable for low power application with improved security. Finally, the proposed architecture is more area efficient as compared to existing aging tolerant architecture for RO-PUF.

## REFERENCES


[1] DARPA, "TRUST in Integrity Circuits (TIC)," http://www.darpa.mil/MTO/solicitations/baa, 07-24, 2007.

[2] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 10–25, 2010.

[3] 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.

[4] F. Koushanfar and G. Qu, "Hardware metering," *in proc. ACM/IEEE Des. Autom. Conf.,* pp. 490-493, 2001.

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

[6] 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.

[7] 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.

[8] D. Holcomb, W. Burleson, and K. Fu, "Initial SRAM state as a fingerprint and source of true random numbers for RFID tags," *presented at Conf. RFID Security.,* Malaga, Spain, pp. 11-13, Jul. 2007.

[9] D. P. Sahoo, S. Saha, D. Mukhopadhyay, R. S. Chakraborty, and H. Kapoor, "Composite PUF: A new design paradigm for Physically Unclonable Functions on FPGA," in *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST),* , pp. 50-55. IEEE, 2014

[10] 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.

[11] 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.

[12] R. Vattikonda, W. Wenping, and Y. Cao. "Modeling and minimization of PMOS NBTI effect for robust nanometer design," In*Proceedings of the 43rd annual Design Automation Conference*, pp. 1047-1052. ACM, 2006.

[13] E. Takeda, C. Y. Yang, and A. Miura-Hamada, "Hot-Carrier Effects in MOS Devices". Academic Press, 1995.

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

[15] S. M. Kang, Y. Leblebici, '*CMOS Digital Integrated Circuits: Analysis & Design'*, TATA McGraw- Hill Publication, 3e, 2003.

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

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

[18] Yin, Chi-En, and Gang Qu, "Temperature-aware cooperative ring oscillator PUF, " *in IEEE International Workshop on Hardware-Oriented Security and Trust*, pp. 36-42, 2009.

[19] 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.

[20] C. Bosch, J. Guajardo, A. Sadeghi, J. Shokrollahi and P. Tuyls, "Efficient helper data key extractor on FPGAs," i*n proc. of Int. workshop on Cryptographic Hardware & Embedded Systems. LNCS,* vol. 5154, pp. 181-197,2008.

[21] I. Kim, A. Maiti, L. Nazhandali, P. Schaumont, V. Vivekraja, and H. Zhang, "From statistics to circuits: Foundation for future PUF," in towards Hardware-intrinsic security, information security and cryptography,springer-verlag, pp. 55–78, 2010.

[22] R. Kumar, V. C. Patil and S. Kundu, "On Design of Temperature Invariant PUF based on Ring oscillator," *in proc. of IEEE comp. society annual symp*. On VLSI, pp. 165-170, 2012.

[23] V. Vivekraja and L. Nazhandali, "Feedback Based Supply Voltage Controll for Temperature Variation Tolerant PUFs," *in proc. of VLSI Design*, pp. 214-219, 2011.

[24] 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. IEEE, 2014.

[25] 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.

[26] T. Rahman, F. Rahman, D. Forte and M. Tehranipoor, "An Aging-Resistant RO-PUF for Reliable Key Generation," *in IEEE Tran. On Emerging Topicsin computing,* vol.4, no.3, pp.335-348, 2016.