Microelectronics Journal 92 (2019) 104605

Contents lists available at ScienceDirect

Microelectronics Journal

journal homepage: www.elsevier.com/locate/mejo

An ultra-low power, reconfigurable, aging resilient RO PUF for IoT applications

Sajid Khan [a], Ambika Prasad Shah [b], Neha Gupta [a], Shailesh Singh Chouhan [c], Jai Gopal Pandey [d], Santosh Kumar Vishvakarma [a,*]

[a] *Nanoscale Devices, VLSI Circuit & System Design Lab, Discipline of Electrical Engineering, Indian Institute of Technology Indore, M.P. 453552, India*
[b] *Institute for Microelectronics, Technische Universität Wien, Vienna 1040, Austria*
[c] *EIS Lab, Department of Computer Science, Electrical and Space Engineering, Lulea University of Technology 97187, Sweden*
[d] *Integrated System Group, CSIR-CEERI, Pilani, Rajasthan 333031, India*

ARTICLE INFO

Keywords:
Lightweight
Low power architecture
Physically unclonable functions
Reliability
NBTI
IoT
Challenge-response pair
Security

ABSTRACT

Physically Unclonable Functions (PUF) have emerged as security primitives which can generate high entropy, temper resilient bits for security applications. However, the power budget of the ring oscillator (RO) PUF limits the use of RO PUF in IoT applications, in this concern a low power variant of RO PUF is much needed. In this paper, we have presented an ultra-low power, lightweight, configurable RO PUF based on the 4T XOR architecture. The proposed architecture is aging resilient; hence it produces a stable PUF output over the years. Also, it has a large number of challenge-response-pair (CRP) compared to the other architectures, which makes it suitable for chip identification as well as cryptographic key generation. The proposed PUF is implemented on 40 nm CMOS technology, and for the validation of design, we have also implemented on FPGA. The simulation results show that it has a uniqueness of 0.489 and worst-case reliability of 96.43% and 93.15% at 125 °C and 1.2 V, respectively. Compared to the conventional RO PUF it consumes 98.06% and 95.47% less dynamic and leakage power, respectively.

1. Introduction

Internet of things (IoT) is being used in a variety of emerging applications, such as smart homes, smart factories, intelligent vehicles, highways, wearable electronics, remote health care, agriculture, environmental monitoring system, personal health monitoring devices, and many more [1]. The IoT utilizes real-time analysis and machine learning methods to process data and make decisions; hence, security failure of these devices can affect billions of lives and huge financial loss with privacy invasion [2,3]. These make the security as one of the main concerns in the deployment of IoT devices on a large scale [4,5]. With the development of various hardware hacking methods, such as side-channel attacks and use of machine learning algorithms, make the key stored in non-volatile memory vulnerable to an attacker. To protect the sensitive data, Physically Unclonable Functions (PUF) have emerged as a promising security solution. PUF generates a unique, reliable, and secure key not only for cryptography but also for hardware authentication applications. It is well known that during fabrication, each chip experiences some unpredictable and uncontrollable semiconductor manufacturing process variations, which are usually undesired. These random process variations result in random changes in MOS parameters like the threshold voltage (V_{TH}), and channel length (L_{eff}). By exploiting these inherent physical variations, a PUF generates a practically unclonable, random functions. These variations are then converted into information in the form of response (output) corresponds to a challenge (input). Since manufacturing process variations are uncontrollable, unpredictable and random in nature, therefore, it is nearly impossible to have two chips with the same response for the same circuit. Hence, PUF can be considered as a unique fingerprint of the selected chip. This makes the PUF response as an active research area in the field of cryptography [6]. Broadly, PUF can be categorized into two categories: strong PUFs and weak PUFs [7]. The strong PUF has a large number of challenge-response pairs (CRPs), while CRPs of a weak PUF are limited [8]. A strong PUF is an ideal candidate for chip identification, as the chip can be identified using different challenges in each session without repeating any challenge.

[*] Corresponding author.
E-mail address: skvishvakarma@iiti.ac.in (S.K. Vishvakarma).

https://doi.org/10.1016/j.mejo.2019.104605
Received 29 April 2019; Received in revised form 4 August 2019; Accepted 6 August 2019
Available online 9 August 2019

Many PUF architectures have been introduced in the literature like, Ring Oscillator (RO) PUF [8], Arbiter PUF [9], SRAM PUF [10], DRAM PUF [11] and RS latch PUF [12]. In the studies it has been observed that RO PUF is one of the best candidates for implementations in both FPGAs [13–16] as well as ASIC in the following ways:

- It offers fabrication simplicity and high security over the others [6,8,16].
- The hard macro of RO can be instantiated multiple times. This makes all the ROs identical in terms of routing and placement. Also, the oscillation frequency of RO does not depend on routing delay.
- Delay difference due to process variations can be further amplified by allowing ROs to oscillate for a longer time.

To make a PUF useful in any of the aforementioned applications, the PUF response should be stable over time. However, due to aging, voltage and temperature variations, the performance of ASIC degrades, and the output becomes unreliable over time [17–19]. The transistor also suffers from various temporal degradations: Hot Carrier Injection (HCI), Bias Temperature Instability (BTI), Time-Dependent Dielectric Breakdown (TDDB), all of these degradations shift the threshold voltage (V_{TH}) and reduces carrier mobility and increase the delay.

BTI is a time-dependent phenomenon that is caused by dangling bond defects at Si/SiO$_2$ interface, which increases the threshold voltage of both NMOS and PMOS at elevated temperature [20]. The PMOS and NMOS both have Negative Bias Temperature Instability (NBTI) and Positive Bias Temperature Instability (PBTI). Usually, only NBTI in PMOS is considered because the effect of NBTI in PMOS is the more considerable and dominant limiting factor of device performance compared to other BTI components [21]. Depending upon the workload, the transistor threshold voltage can increase up to 15% due to BTI during one year of operation [18]. Fig. 1 shows the PMOS threshold voltage change and mobility degradation with stress time for 40 nm standard CMOS technology. The result indicates that degradation is maximum during the initial phase of stress time.

In addition to this, the delay difference caused by manufacturing variations is also sensitive to the environment and hence contributes to making the response of PUF unreliable. In Ref. [8], it is shown that every 15 °C increase in temperature roughly increases the delay of RO by 10–15%. If the frequencies generated by an RO pair are close enough, then there exists a possibility of bit flipping due to the change in temperature as shown in Fig. 2. For the proper operation of the circuit, the frequency of ROs must not flip under any operating conditions. From Fig. 2 it is also observed that the possibility of bit flipping can be avoided in two different ways. First, by increasing the difference between the frequencies of two ROs. Second, by designing a temperature-independent RO circuit.

Researchers have proposed many architectures to improve the thermal and supply voltage stability of RO PUF, some of these are: 1 out of N masking scheme [8], temperature aware cooperative PUF [9], highly flexible RO PUF [10] and crossover RO PUF [22]. In most of the architectures, additional hardware is required to get a stable output from an RO PUF. For example, in 1 out of N masking scheme [8], out of N ring oscillators, only one which is thermally stable is used. On the other side, in temperature aware cooperative PUF architectures [9], each RO is designed to function over a range of temperature, and sufficient frequency distance is selected among them, which results in a sophisticated design with the temperature sensor. Similarly, highly flexible RO PUF [10] provides a way to use or skip an inverter to form a ring. All of the above architectures require a significant hardware overhead to generate a reliable cryptographic key which is not suitable in most of the IoT verticals. Also, all of the above architectures have not been evaluated for NBTI degradations, which is essential to address the reliability issues generate over time.

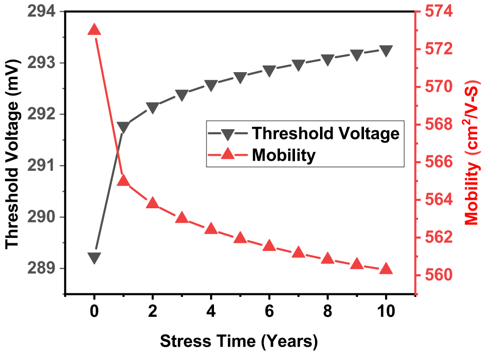


Fig. 1. PMOS threshold voltage shift and mobility degradation with stress time for 40 nm technology.

Also, most of the IoT devices are battery-powered, and the utmost priority for the IoT devices is to consume minimum power to keep the battery life as long as possible, The power budget of the conventional RO PUF limits the use of RO PUF in IoT applications. Also, RO PUF is only enabled for a brief period whenever a key is required, or an authentication takes place, the rest of the time it is in idle state. In the case of IoT, the leakage power of PUF also affects the battery lifetime. In this concern, a low dynamic as well as leakage power variant of RO PUF is much needed. In this paper, we have proposed an ultra-low power, configurable architecture of RO PUF using 4T XOR, which is NBTI resilient. Based on the input, the 4T stage can be configured either as an inverter or as a buffer. The reconfigurability results in an exponential increase in the number of CRPs with less hardware requirement. The proposed architecture is more sensitive to process variation and less sensitive to aging. The post-layout simulation results show that the proposed architecture has improved uniqueness and it is less vulnerable to aging when compared with the previously proposed architecture.

The rest of the paper is organized as follows: In Section 2, the NBTI effect is discussed. Section 3 describes our proposed RO. Proposed RO PUF architecture is discussed in Section 4 followed by FPGA and ASIC implementation in Section 5 and 6, respectively. The paper is finally concluded in Section 7.

2. Negative Bias Temperature Instability (NBTI)

As described in the literature when $V_{GS} = -V_{DD}$ for a PMOS transistor then it goes in the stress condition. During stress time few Si–H bonds get broken and trapped in the oxide layer (Stress phase). This trapping causes the change in threshold voltage of PMOS which can be expressed as [23]:

$$\Delta V_{TH\_Stress} = A_{NBTI} \times t_{ox} \times \sqrt{C_{ox}(V_{DD} - V_T)} \times e^{\frac{V_{DD}-V_T}{t_{ox}E_0} - \frac{E_a}{kT}} \times t_{stress}^{0.25} \quad (1)$$

where A_{NBTI} is the aging dependent constant, t_{ox} is the oxide thickness, C_{ox} is the gate capacitance/area, t_{stress} is the stress time, E_0, E_a are the constant that depends on device and k is the Boltzmann constant. During the operation, when $V_{GS} = 0$ i.e when transistor turns off then

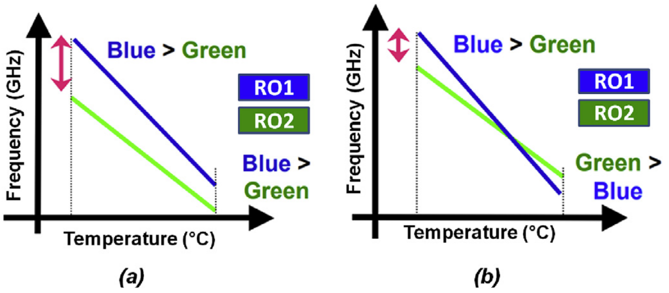


Fig. 2. Output frequencies of the RO pair result in (a) Stable output bit (b) Flipped output bit.

some of the traps are eliminated and the threshold voltage reduces. This phenomenon is called recovery phase. However, during recovery phase all the trapped charges can not be recovered and hence threshold voltage increases with time. The final change in threshold voltage can be expressed in terms of stress and recovery time as [23]:

$$\Delta V_{TH} = \Delta V_{TH\_Stress} \times \left(1 - \sqrt{\eta \times \frac{t_{Recovery}}{t_{Stress} + t_{Recovery}}}\right) \tag{2}$$

where $t_{Stress}, t_{Recovery}$ are stress time, recovery time respectively and η is a constant with value 0.35.

2.1. NBTI effect in PUF

Fig. 3 shows the conventional RO PUF. Since a PUF is only used when an authentication takes place, or a key is required which is roughly 10% of the chip lifetime. The problem with the conventional architecture is even when the PUF is disabled still approximately half of the PMOSs of RO chain are in stress condition, which reduces the PUF reliability over time. To address the aging effect, very few architectures have been proposed. In Ref. [25], to improve the reliability against aging a configurable RO is proposed in which out of 8 ROs pairs one RO pair with maximum frequency difference is used to generate the PUF response. In Ref. [24], an aging resilient RO is proposed, to mitigate NBTI effects two extra transistors are added in each RO stage as shown in Fig. 4. This architecture has two limitations — first, the presence of additional transistors that can be considered as hardware overhead. Second, the PMOSs are still experiencing some NBTI effects even when PUF is not in use because the gate-to-source voltage (V_{GS}) of PMOS transistor is not completely zero.

3. The 4T XOR cell architecture used in RO PUF

We have modified the transmission gate based XOR gate [26] by removing one inverter as shown in Fig. 5. It can be seen from Fig. 5 that two additional transistors ($M3, M4$) are added to the conventional CMOS inverter ($M1, M2$). In the architecture, the supply lines have been replaced by control signals ($C, \overline{C}$) to make the architecture data-driven.

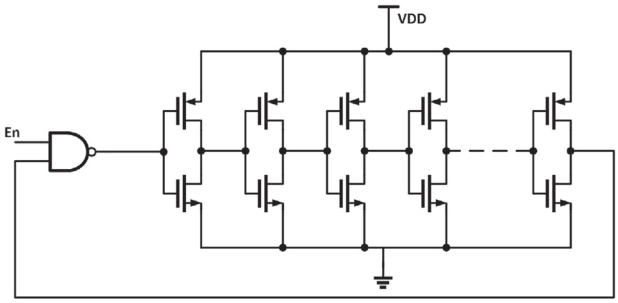


Fig. 3. Conventional RO PUF.

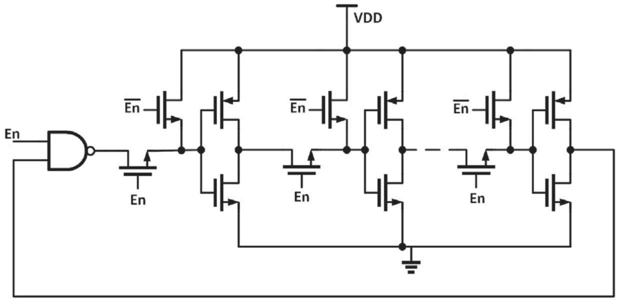


Fig. 4. Aging resilient ring oscillator (ARO) [24].

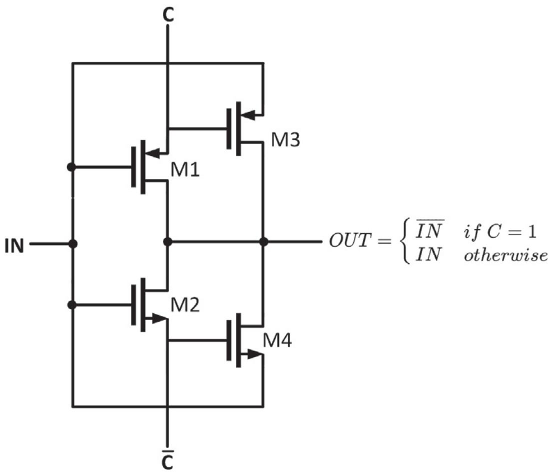

C
M3
M1
IN
$OUT = \begin{cases} \overline{IN} & if\ C = 1 \\ IN & otherwise \end{cases}$
M2
M4
$\overline{C}$

Fig. 5. Schematic of 4T XOR cell architecture used in RO PUF.

When $C =$ '1', $M1$ and $M2$ forms an inverter whereas $M3$ and $M4$ are in cut-off state. Hence, the output is an inverted version of the input. On the other hand, when $C =$ '0', $M1$ and $M2$ are in cut-off and based on input either $M3$ or $M4$ is in saturation state, this forms a transmission gate and hence without any degradation, the output is same as the input and the pass transistors ($M3$ and $M4$) may add more process variations to PUF. Based on input signals the state of transistors can be defined as follows:

Case 1: when $C = V_{DD}$ and $IN = V_{DD}$

In this case, CMOS inverter is powered through C and $\overline{C}$, Hence the V_{OUT} = '0', Now for $M3$

$$V_{GS_{M3}} = V_C - V_{IN} = 0 \tag{3}$$

Similarly for $M4$

$$V_{GS_{M4}} = V_{\overline{C}} - V_{OUT} = 0 \tag{4}$$

From (3) and (4) it is clear that $V_{GS_{M3}} > V_{TP}$ and $V_{GS_{M4}} < V_{TN}$ and both will remain in cut-off.

Case 2: when $C = V_{DD}$ and IN = '0'

Similarly to the previous stage, in this case also CMOS inverter is powered through C and $\overline{C}$, Hence the $V_{OUT} = V_{DD}$, Now for $M3$

$$V_{GS_{M3}} = V_C - V_{OUT} = 0 \tag{5}$$

Similarly for $M4$

$$V_{GS_{M4}} = V_{\overline{C}} - V_{IN} = 0 \tag{6}$$

Referring to (5) and (6) $V_{GS_{M3}} > V_{TP}$ and $V_{GS_{M4}} < V_{TN}$ and both will remain in cut-off state.

Case 3: when C = '0' and $IN = V_{DD}$

In this case, the power supply of CMOS inverter is reversed; hence it does not act as an inverter anymore. Now for $M3$

$$V_{GS_{M3}} = V_C - V_{IN} = -V_{DD} \tag{7}$$

Similarly for $M4$

$$V_{GS_{M4}} = V_{\overline{C}} - V_{OUT} = V_{DD} - V_{OUT} \tag{8}$$

(7) and (8) state that $M3$ will always remain ON while $M4$ goes to cut-off once $V_{OUT} > V_{DD} - V_{TN}$

For $M1$

$$V_{GS_{M1}} = V_{IN} - V_{OUT} \tag{9}$$

Similarly for $M2$

$$V_{GS_{M2}} = V_{IN} - V_{OUT} \tag{10}$$

Since $M3$ and $M4$ are ON, due to which $V_{OUT} = V_{IN}$, hence, $V_{GS_{M1}} ='0'$ and $V_{GS_{M2}} = $ '0'.

Case 4: when C = '0' and IN = '0'

In this case also, CMOS inverter does not work. Now for $M3$

$$V_{GS_{M3}} = V_C - V_{OUT} = -V_{OUT} \tag{11}$$

Similarly for $M4$

$$V_{GS_{M4}} = V_{\overline{C}} - V_{IN} = V_{DD} \tag{12}$$

(11) and (12) state that $M4$ will always remain ON while $M4$ goes to cut-off once $V_{OUT} < V_{TP}$ and $M1$ and $M2$ remain off as in case 3.

Both $M1$ and $M2$ remains off and current flows due to $M3$ and $M4$ only. From case 1 and case 2, we can conclude that when $C = V_{DD}$ the additional transistors $M3$ and $M4$ do not affect the state of the output. Similarly, $M1$ and $M2$ remain off when $C='0'$ and output is same as the input. These two additional transistors provide reconfigurability and may add more uniqueness to PUF.

4. The proposed PUF architecture

Fig. 6(a) shows the chain of our proposed RO, when a '1' is received as a challenge the corresponding stage is configured as an inverter, and $M3$ and $M4$ are in cut-off otherwise it acts as a buffer and $M1$ and $M2$ are in cut-off, as shown in Fig. 6(b). When RO is not in use, the feedback loop is broken by setting *Enable* = '0', and all the 4T XOR cells are configured as buffers by setting all the challenge bits to '0' as shown in Fig. 6(c). Setting *Enable* = '0' forces the output of *AND* gate to '0' since all the cells are configured as a buffer, the input and output of all the cells become '0', and there are no oscillations. Referring to (11) and (9), in this case the V_{GS} of $M1$ and $M3$ will be '0' and $-V_{OUT}$ respectively. For a buffer $V_{OUT} = V_{IN}$ and since V_{IN} ='0′, V_{GS} of $M3$ will be '0' also. Hence the proposed architecture does not experience NBTI when not in use.

Fig. 7 shows the complete mechanism of our proposed PUF architecture where the shaded block is shared by all the ROs. In the conventional RO PUF, two ROs are used to generate only a single bit. However, in our proposed architecture two ROs can generate multiple bits. For the proper operation of the proposed architecture numbers of 1's in the challenge must be odd. To fulfill the above conditions, either user can be asked, or a PUF controller can be used. Fig. 8 shows the flowchart of the PUF controller with Linear Feedback Shift Register (LFSR) counter used in our design. We have generated challenges from the PUF controller in two ways: (i) challenges having all odd number of ones (between 3 and 25) and (ii) challenges having n number of ones, where n can be any odd number. Following are the steps to generate the aforementioned challenges:

i. First, a 25-bit number is generated using the seed and then the number of ones is calculated.
ii. If the total number of ones are n, where n can be either any odd number between 3 and 25 as shown in Fig. 8(a) or a user-specified odd number (15, 17, 19 or 21) as shown in Fig. 8(b) then the generated number is given to PUF as a challenge; otherwise, the next number is generated, and step (ii) is repeated.
iii. The PUF response is stored and the next challenge is generated using the step (ii). Steps (ii) and (iii) are repeated to collect a large set of challenge-response pairs.

For the effectiveness of the design, we have implemented the proposed PUF architecture in ASIC as well as in FPGA.

5. Experimental results: the functional testing

The functionality testing of the proposed PUF architecture is done on ten *Basys*3 FPGA boards using *Xilinx V ivado*. FPGA implemented architecture is shown in Fig. 9. On each FPGA we have implemented 32 instances of PUF in four different places. Challenges to PUF are given by using a 25-bit LFSR counter, and then responses are transmitted to PC using UART. In FPGA implementation of our proposed PUF 4T architecture is replaced by XOR gates and to avoid any routing effect, all

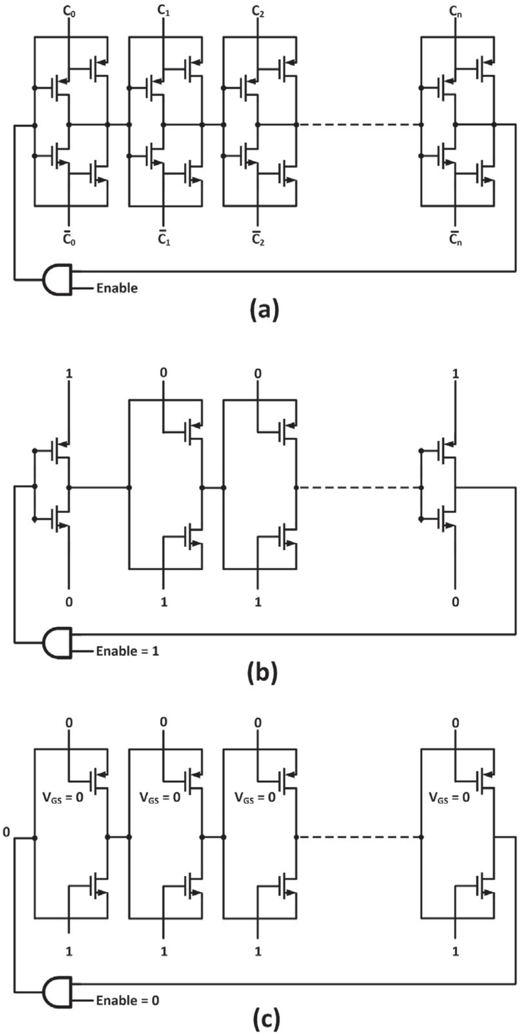


Fig. 6. (a) Chain of proposed RO, (b) Challenge dependent configuration, and (c) All buffer configuration when $Enable='0'$.

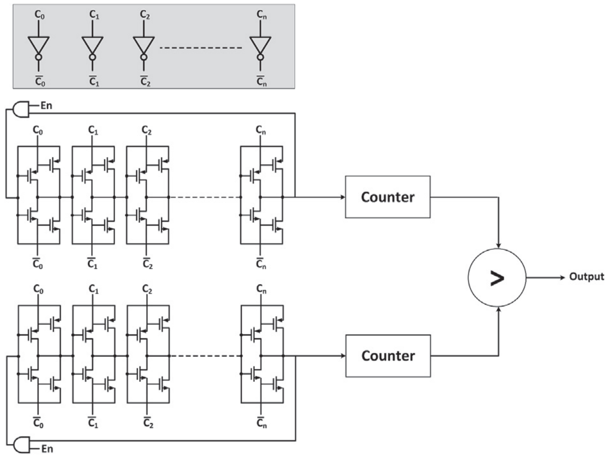


Fig. 7. Proposed RO PUF architecture.

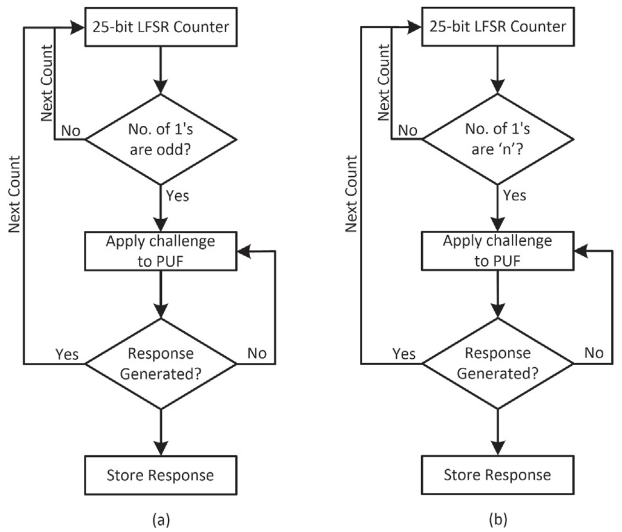


Fig. 8. Flow chart for LFSR (a) For all challenges with all odd number of ones (b) For challenge with total 'n' number of ones.

the ROs are placed manually. The resource utilization report is shown in Table 1.

5.1. Uniqueness

The uniqueness distinguishes two PUF instances. It is calculated using the inter-die Hamming distance (HD). It suggests that when imposing the same challenge to any two PUF instances then half of the response bit should be different. It has an ideal value of 50%.

Let us consider that corresponds to a challenge C, R_a and R_b are respectively two n-bit responses from randomly selected chip a and b out of m number of available chips. The uniqueness(U) from m chips can be expressed as:

$$U = \frac{2}{m(m-1)} \sum_{a=1}^{m-1} \sum_{b=a+1}^{m} \frac{HD(R_a, R_b)}{n} \times 100\% \tag{13}$$

In the experiment, on each FPGA we have instantiated proposed PUF in four different places, extracted a thousand of 32-bit response from each of the instantiation and calculated uniqueness. We have also calculated the uniqueness between any two instantiations of proposed PUF on the same FPGA as intra-chip uniqueness. On a single FPGA, we have instantiated the proposed PUF on four different locations, hence we have total of six intra-chip CRPs for a single FPGA. Among all of the CRPs of ten FPGA boards, the maximum, minimum and mean value of intra-chip and inter-chip uniqueness for each case is reported in Table 2.

Table 1
Resource utilization on Basys3.

S.No.	Design	No. of LUTs	No. of FFs
1.	RO	26	0
2.	Counter	2	21
3.	LFSR	130	96
4.	UART	32	23

Table 2 shows that inter-chip and intra-chip uniqueness are lower when the number of inverters is 21, and it is the highest when the number of inverters is 17. Hence when the number of inverters is closed to the number of buffers the proposed PUF shows better inter-chip and intra-chip uniqueness. The distribution for inter-chip Hamming distance is shown in Fig. 10 shows the distribution of inter-chip Hamming distance for uniqueness value of 0.487, 0.469, 0.465 and 0.489 for 17, 19, 21 and all odd number of inverters (between 3 and 25), respectively.

Similarly, the distribution of intra-chip Hamming distance for uniqueness value of 0.475, 0.469, 0.458 and 0.490 for 17, 19, 21 and all odd number of inverters (between 3 and 25), respectively is shown in Fig. 11. Additionally, the average intra-chip Hamming distance for uniqueness between any two PUF response pair is 0.485, 0.488 and 0.479 for 17, 19 and 21 number of inverters, whereas, 0.501 for all odd number (between 3 and 25) of inverters. Further, we have also validated our design by performing simulation at 40 nm CMOS process as discussed in the subsequent section.

6. Simulation results

To generate a 32-bit response, 64 instances of ARO PUF, conventional RO PUF and proposed PUF are implemented using 40 nm CMOS process and each RO contains 25 inverting stages. Minimum size transistors ($W_{NMOS} = 120n$ and $W_{PMOS} = 300n$) are used for conventional RO and proposed RO and for ARO as specified in Ref. [24].

By sharing the controller block for each RO stage and using drain sharing technique, the proposed RO PUF has very less area overhead compared to the ARO PUF. Also the area overhead for aging reliability enhancement is zero. Fig. 12 shows the layout of the conventional RO pair, ARO pair and the proposed RO pair having a total area of 29.33 μm^2, 59.67 μm^2 and 53.84 μm^2, respectively. We have performed 1000 sets of Monte Carlo simulation with $\pm 3\sigma$ deviation to generate 32-bit CRPs and found that the uniqueness for the proposed PUF is 0.489, 0.478, 0.471 and 0.491 for 17, 19, 21 and all odd number (between 3 and 25) of inverters, respectively. The histogram for inter-chip Hamming distance is shown in Fig. 13. Simulation results

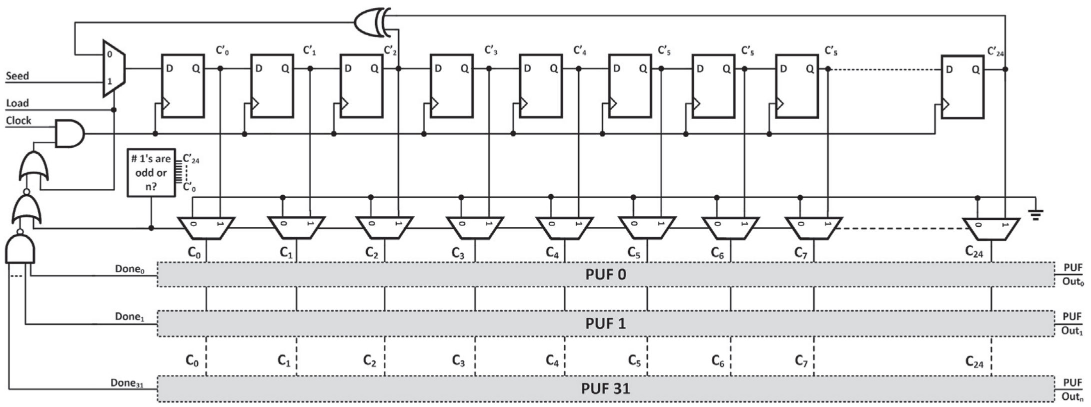


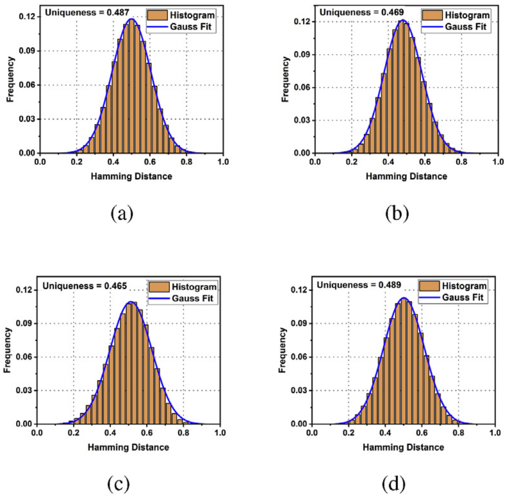
Fig. 9. Architecture of proposed PUF with LFSR counter.

Table 2
Inter-chip and intra-chip uniqueness.

#Inverters (Out of 25)	Inter-chip Uniqueness			Intra-chip Uniqueness		
	Max.	Min.	Mean	Max.	Min.	Mean
17	0.489	0.476	0.486	0.512	0.479	0.485
19	0.477	0.466	0.471	0.521	0.475	0.488
21	0.470	0.458	0.468	0.530	0.451	0.479
All odd numbers (between 3 and 25)	0.491	0.477	0.491	0.509	0.478	0.501

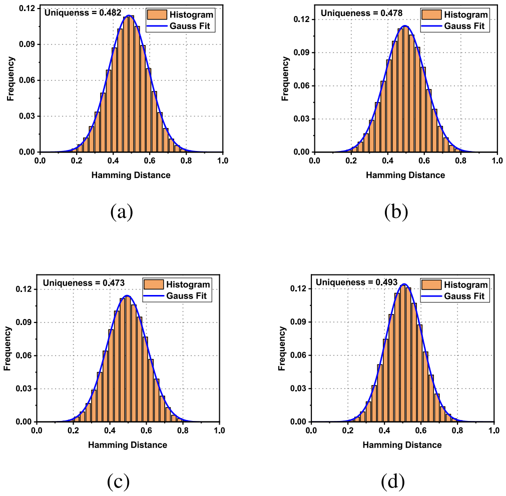
for uniqueness are approximately equal to the FPGA results; hence the simulation results are confirmed by the FPGA results.

The power, area, and frequency of any circuit are essential parameters, which govern the effectiveness of the design. Apart from configurable and aging resilient the proposed RO is data-driven; hence, it requires very lower power and provides moderate output frequency. The dynamic power, leakage power, output frequency and area comparison among our proposed RO and other ROs, are shown in Fig. 14. For a total of 64 instances, our analysis indicates that the proposed RO consumes 95.4% and 98.06% less dynamic power, 99.93% and 99.94% less leakage power with 82.84% higher and 59.29% lower frequency, compared to the ARO and conventional RO, respectively. Also, the proposed design takes 83.56% more and 18.89% less area compared to the conventional RO and ARO, respectively.



(a) (b) (c) (d)

Fig. 10. Distribution of Inter-chip Hamming distance for proposed PUF for (a) 17 inverters and 8 buffers (b) 19 inverters and 6 buffers (c) 21 inverters and 4 buffers (d) All odd number (between 3 and 25) of inverters.



(a) (b) (c) (d)

Fig. 11. Distribution of Intra-chip Hamming distance for proposed PUF for (a) 17 inverters and 8 buffers (b) 19 inverters and 6 buffers (c) 21 inverters and 4 buffers (d) All odd number of inverters (between 3 and 25).

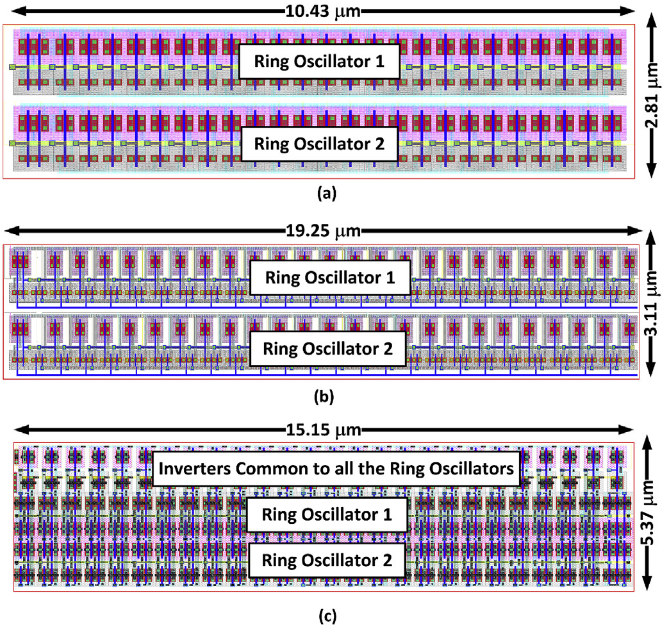
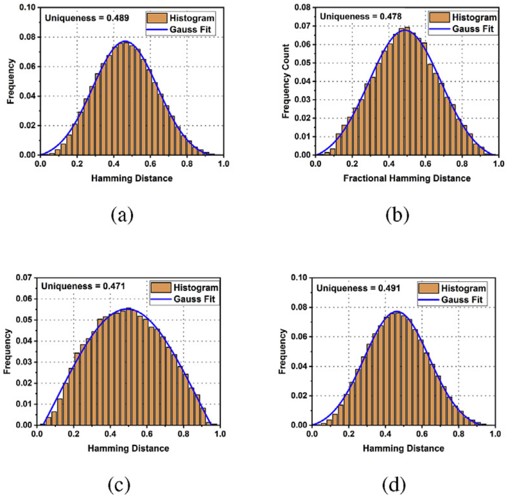


Fig. 12. Layout of (a) Conventional RO pair (b) ARO pair and (c) Proposed RO pair.



(a) (b) (c) (d)

Fig. 13. Distribution of Hamming distance for proposed PUF for (a) 17 inverters and 8 buffers (b) 19 inverters and 6 buffers (c) 21 inverters and 4 buffers (d) Any odd number of inverters.

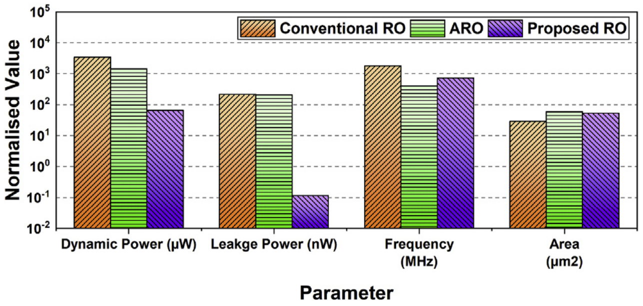


Fig. 14. Comparison of proposed RO with ARO and conventional RO.

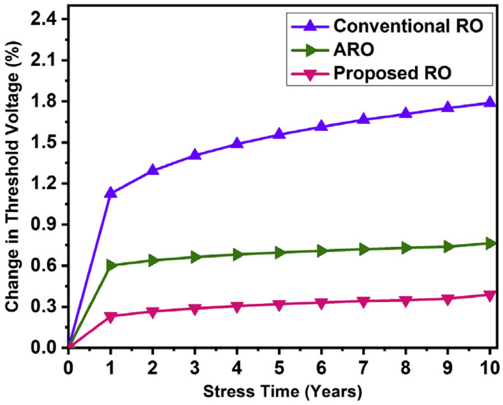


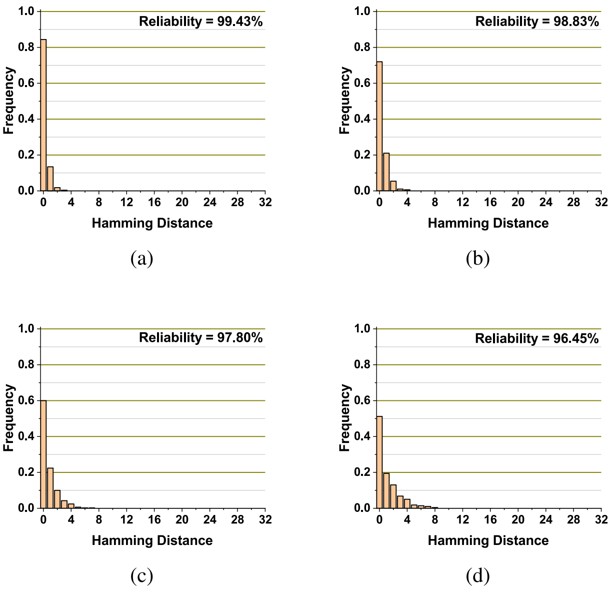
Fig. 15. Threshold voltage variation with stress time.

6.1. NBTI resiliency

Reliability analysis is carried out on *Cadence RelXpert* available in Cadence environment using 40 nm standard CMOS technology. Threshold variation due to NBTI under various stress time is shown in Fig. 15. Simulations results show that the proposed RO has 79.46% and 51.89% less degradation in PMOS threshold voltage compared to the conventional RO and ARO, respectively. The reason for improved threshold value is that even when disabled, instead of 0, the V_{GS} of PMOS in ARO and conventional RO are $-V_{TN}$ and $-V_{DD}$, respectively. The mobility of the charge carrier is also affected by NBTI.

6.2. Reliability

Reliability is used to measure the stability of a PUF in various environmental conditions. Ideally, the difference between any two responses of the same challenge under different environmental conditions should be zero. Temperature variation and supply voltage fluctuations are the factors which affect circuit delay in practice, and due to these factors, the PUF response may become unstable. Reliability has been measured by comparing the two responses taken at different time instances. The reliability R of a chip can be measured by:



(a)

(b)

(c)

(d)

Fig. 16. Hamming distance for proposed PUF output bits with temperature (a) 50 °C, (b) 70 °C, (c) 100 °C, (d) 125 °C, at $V_{DC} = 1.1$ V.

$$R = 1 - \frac{1}{k}\sum_{m=1}^{k}\frac{HD(R_m, R'_m)}{n} \times 100\% \tag{14}$$

where k is the number of samples, n is the number of generated bits, and $HD(R_m, R'_m)$ is the hamming distance between R_m and R'_m.

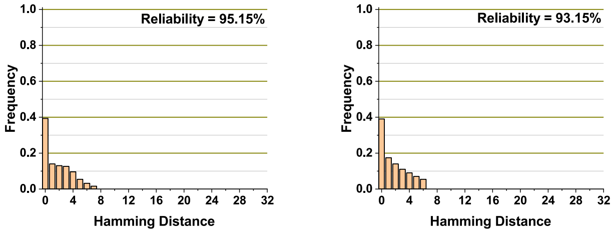
Since temperature and supply voltage are two effective factors to affect circuit delay, we have checked the reliability of proposed PUF under varying temperature and supply voltage. Table 3 shows the reliability of proposed PUF under various operating temperatures and Fig. 16 shows Hamming distance for proposed PUF output bits with varying temperature.

From Table 3, it can be seen that the proposed PUF has better thermal stability, it has a bit-error-rate (BER) of 0.57%, 0.64%, and 0.78% for 17, 19 and 21 number of inverters at 50 °C, respectively. Out of the four transistors in Fig. 5, two transistors forming the inverters are more affected by the temperature as compared to the rest two transistors. The BER also increases slightly with the increased number of inverters. The BER for proposed design is increased by 3.55%, 3.87% and 4.88% for 17, 19 and 21 number of inverters, respectively, at 125 °C.

Similarly, for the analysis of power supply variation on the proposed PUF, the supply voltage is varied with ±10% as shown in Table 3. Out of the four transistors of Fig. 5, $M3$ and $M4$ are the pass transistors, and they are less affected by the supply voltage variations as compared to

Table 3
Simulation Result for Uniqueness, Reliability and Output frequency of various PUF designs.

			Reliability						
			Temperature (in °C)				Supply Voltage		
Design	No. of Inverters (out of 25)	Uniqueness	50	75	100	125	1 V	1.2 V	Frequency (MHz)
Conventional RO PUF	25	0.486	0.9973	0.9912	0.9815	0.9784	0.9654	0.9473	1810
ARO PUF	25	0.490	0.9903	0.9871	0.9783	0.9681	0.9537	0.9389	402.9
Proposed RO PUF	17	0.489	0.9943	0.9869	0.9780	0.9645	0.9515	0.9315	669.3
	19	0.478	0.9936	0.9843	0.9760	0.9613	0.9426	0.9285	671.4
	21	0.471	0.9922	0.9831	0.9749	0.9512	0.9341	0.9214	746.4
	All odd numbers (between 3 and 25)	0.491	0.9951	0.9601	0.9609	0.9443	0.9508	0.9265	724.2 (Average)



(a) (b)

Fig. 17. Hamming distance for proposed PUF output bits with supply voltage (a) 1 V, (b) 1.2 V at 27 °C.

$M1$ and $M2$. Hence, as the number of inverter increases, the BER also increases.

Hamming distance for proposed PUF output bits with varying supply voltage is shown in Fig. 17. From Table 3 it can be shown that at 1.2 V the BER is maximum, which is 6.85%, 7.15% and 7.86% for 17, 19 and 21 number of inverters, respectively.

6.3. Randomness

Apart from being unique and reliable, the PUF output must be random. This means that from a set of PUFs, the responses of a specific PUF are unpredictable. To evaluate the randomness of the proposed PUF we have used the PUF responses as input to the NIST randomness test suite [27]. Table 4 shows that the proposed PUF passes all the NIST randomness tests that we are able to perform. Due to the limited number of the dataset, the NIST randomness tests that require large dataset have been omitted.

Fig. 18 shows the PMOS mobility degradation due to aging in conventional RO, ARO and proposed RO. After ten years of operation, the mobility degradation for conventional RO, ARO, and proposed RO are 2.23%, 0.76%, and 0.21%, respectively, from its initial value. Hence, our proposed RO PUF has better aging resiliency compared to both conventional RO and ARO PUF.

Table 4
NIST randomness test suite result.

NIST Test	P-Value	Proportion	Status
Frequency	0.0884	328/330	Pass
Block Frequency	0.4628	326/330	Pass
Cumulative Sums (Forward)	0.0404	328/330	Pass
Cumulative Sums (Reverse)	0.1023	329/330	Pass
Runs	0.0151	329/330	Pass
Serial	0.0145	326/330	Pass

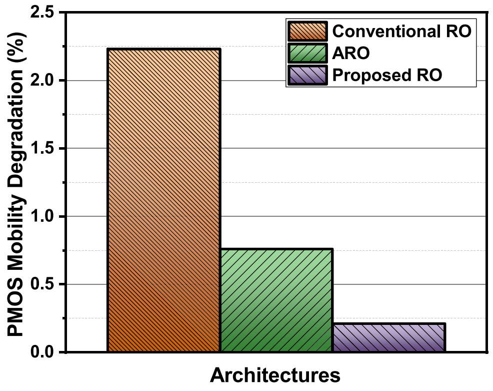


Fig. 18. Effective mobility degradation with 10 years of stress for different RO circuits.

7. Conclusion

In this paper, we have presented an ultra-low power, lightweight, NBTI resilience reconfigurable PUF for IoT applications which consume very less power as compared to the other architectures. We validated our design by implementing on the FPGA as well as simulations. Results show that the proposed design has better uniqueness with less hardware as compared to the other considered circuits. We also found that proposed architecture is less sensitive to temperature variations compared to the supply voltage variations. The effect of NBTI on proposed design is very less; hence, the design is resilient to temporal degradations. From the above discussion we can conclude that the proposed design is ultra-low power, lightweight, aging resilient and reconfigurable; hence it is best suited for the low power, high performance, and reliable IoT applications.

Acknowledgment

The authors would like to thank the UGC, Government of India under the JRF Scheme for providing financial support (Ref. No. 3548/NET-DEC. 2015). We also extend our sincere gratitude to SMDP-C2SD programme Government of India.

References

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, M. Zorzi, Internet of things for smart cities, IEEE Int. Things J. 1 (1) (2014) 22–32.
[2] A.-R. Sadeghi, C. Wachsmann, M. Waidner, Security and privacy challenges in industrial internet of things, in: Proceedings of the 52nd Annual Design Automation Conference, ACM, 2015, p. 54.
[3] B. Halak, J. Murphy, A. Yakovlev, Power balanced circuits for leakage-power-attacks resilient design, in: Science and Information Conference (SAI), IEEE, 2015, pp. 1178–1183.
[4] T. Xu, J.B. Wendt, M. Potkonjak, Security of IoT systems: design challenges and opportunities, in: Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design, IEEE Press, 2014, pp. 417–423.
[5] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, Security, privacy and trust in Internet of Things: the road ahead, Comput. Network. 76 (2015) 146–164.
[6] C. Herder, M.-D. Yu, F. Koushanfar, S. Devadas, Physical unclonable functions and applications: a tutorial, Proc. IEEE 102 (8) (2014) 1126–1141.
[7] C.-H. Chang, Y. Zheng, L. Zhang, A retrospective and a look forward: fifteen years of physical unclonable function advancement, IEEE Circ. Syst. Mag. 17 (3) (2017) 32–62.
[8] G.E. Suh, S. Devadas, Physical unclonable functions for device authentication and secret key generation, in: Proceedings of the 44th Annual Design Automation Conference, ACM, 2007, pp. 9–14.
[9] D. Lim, J.W. Lee, B. Gassend, G.E. Suh, M. Van Dijk, S. Devadas, Extracting secret keys from integrated circuits, IEEE Trans. Very Large Scale Integr. Syst. 13 (10) (2005) 1200–1205.
[10] D.E. Holcomb, W.P. Burleson, K. Fu, Power-up SRAM state as an identifying fingerprint and source of true random numbers, IEEE Trans. Comput. 58 (9) (2009) 1198–1210.
[11] F. Tehranipoor, N. Karimian, W. Yan, J.A. Chandy, DRAM-based intrinsic physically unclonable functions for system-level security and authentication, IEEE Trans. Very Large Scale Integr. Syst. 25 (3) (2017) 1085–1097.
[12] B. Habib, J.-P. Kaps, K. Gaj, Efficient sr-latch PUF, in: International Symposium on Applied Reconfigurable Computing, Springer, 2015, pp. 205–216.
[13] S. Morozov, A. Maiti, P. Schaumont, An analysis of delay based PUF implementations on FPGA, in: International Symposium on Applied Reconfigurable Computing, Springer, 2010, pp. 382–387.
[14] A. Maiti, J. Casarona, L. McHale, P. Schaumont, A large scale characterization of RO-PUF, in: 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), IEEE, 2010, pp. 94–99.
[15] L. Feiten, A. Spilla, M. Sauer, T. Schubert, B. Becker, Analysis of ring oscillator pufs on 60nm fpgas, Eur. Cooperation Sci. Technol. (2013).
[16] C.-E. Yin, G. Qu, Temperature-aware cooperative ring oscillator PUF, in: IEEE International Workshop on Hardware-Oriented Security and Trust, 2009. HOST'09, IEEE, 2009, pp. 36–42.
[17] T. Nigam, B. Parameshwaran, G. Krause, Accurate product lifetime predictions based on device-level measurements, in: Reliability Physics Symposium, 2009 IEEE International, IEEE, 2009, pp. 634–639.
[18] M. Agarwal, V. Balakrishnan, A. Bhuyan, K. Kim, B.C. Paul, W. Wang, B. Yang, Y. Cao, S. Mitra, Optimized circuit failure prediction for aging: practicality and promise, in: Test Conference, 2008. ITC 2008. IEEE International, IEEE, 2008, pp. 1–10.
[19] Y. Lu, L. Shang, H. Zhou, H. Zhu, F. Yang, X. Zeng, Statistical reliability analysis under process variation and aging effects, in: Design Automation Conference, 2009. DAC'09. 46th ACM/IEEE, IEEE, 2009, pp. 514–519.

[20] G.D. Panagopoulos, K. Roy, A three-dimensional physical model for V th variations considering the combined effect of NBTI and RDF, IEEE Trans. Electron Dev. 58 (8) (2011) 2337–2346.

[21] A.P. Shah, N. Yadav, A. Beohar, S.K. Vishvakarma, Process variation and NBTI resilient schmitt trigger for stable and reliable circuits, IEEE Trans. Device Mater. Reliab. 18 (4) (2018) 546–554.

[22] Z. Pang, J. Zhang, Q. Zhou, S. Gong, X. Qian, B. Tang, Crossover ring oscillator PUF, in: 2017 18th International Symposium on Quality Electronic Design (ISQED), IEEE, 2017, pp. 237–243.

[23] A. Tiwari, J. Torrellas, Facelift: hiding and slowing down aging in multicores, in: Proceedings of the 41st Annual IEEE/ACM International Symposium on Microarchitecture, IEEE Computer Society, 2008, pp. 129–140.

[24] M.T. Rahman, F. Rahman, D. Forte, M. Tehranipoor, An aging-resistant RO-PUF for reliable key generation, IEEE Trans. Emerg. Top. Comput. 4 (3) (2016) 335–348.

[25] A. Maiti, P. Schaumont, The impact of aging on a physical unclonable function, IEEE Trans. Very Large Scale Integr. Syst. 22 (9) (2014) 1854–1864.

[26] J.-M. Wang, S.-C. Fang, W.-S. Feng, New efficient designs for XOR and XNOR functions on the transistor level, IEEE J. Solid State Circ. 29 (7) (1994) 780–786.

[27] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Tech. rep, Booz-Allen and Hamilton Inc Mclean Va, 2001.