Exploiting Body-Driven Feedbacks in Physical Unclonable Functions for Ultra Low Voltage, Ultra Low Power Applications: A 0.3 V Weak-PUF

Riccardo Della Sala, Davide Bellizia, Francesco Centurelli, *Senior Member, IEEE*, Giuseppe Scotti, *Senior Member, IEEE*, and Alessandro Trifiletti

***Abstract*— This paper introduces an innovative approach to designing a mismatched current mirror with a fully unbalanced output, significantly reducing the minimum supply voltage requirements for Regulated Cascode Current Mirror (RCCM) Physical Unclonable Functions (PUFs). Leveraging body-driven feedback mechanisms, the proposed circuit reliably operates with supply voltages as low as 0.3V, maintaining stable power consumption through a reference bias current. The resulting PUF achieves remarkable energy efficiency, consuming only 0.3 fJ per bit, without compromising statistical performance. It exhibits a response bias of 49.42%, a reliability of 99.483%, and a uniqueness of 50.176%. Validation of this novel approach is conducted through simulations and measurements on a 130nm CMOS test-chip, considering a nominal supply voltage of 0.3V, ±10% supply voltage variations, and a temperature range from 0°C to 75°C. Rigorous experimental verification on 20 chip samples, along with detailed explanations of design methodologies, underscores the robustness and practicality of the proposed Body-PUF design. Comparative analyses against state-of-the-art literature reveal that the Body-PUF outperforms previous PUF designs in Figures of Merit (FOM), making it promising for real-world authentication scenarios. Its outstanding trade-off between performance and practicality positions it as a compelling solution for secure applications, including Internet of Things (IoT) devices and other security-critical systems.**

***Index Terms*— IoT, ultra-low voltage (ULV), physical unclonable functions (PUFs), body-driven, hardware security, key generation.**

I. Introduction

IN TODAY'S modern world, electronic devices have become an integral part of our daily lives, aiding us in various tasks such as banking, email, shopping, and reservations [1], [2], [3]. With the widespread use of these devices, ensuring their security has become paramount, leading to the development of innovative solutions to combat potential hardware-based attacks [4], [5], [6], [7]. Electronic equipments are frequently counterfeited and result vulnerable to side-channel attacks (SCAs) [8], [9], [10], which pose significant security challenges in the hardware domain. Physically Unclonable Functions (PUFs) have emerged as a promising tool for chip identification and authentication [11], [12], [13]. These cryptographic primitives exploit physical effects, such as process parameter variations and mismatches, which are unavoidable in semiconductor technologies, as entropy sources, to generate on chip unique and unclonable bits words. PUFs can replace conventional memory cells in the creation of cryptographic keys, providing a secure alternative [14], [15], and represent a valid protection against counterfeiting and SCAs [16], [17]. Their ability to harness inherent physical variations, such as mismatched frequencies in ring oscillators, to generate keys is groundbreaking. The first PUF proposed in the literature and validated in CMOS technology is reported in [18]. PUFs based on Ring Oscillator (RO) usually rely on ROs that nominally exhibit the same oscillation frequency, but due to technological mismatches, one of the frequencies is higher than the other. A single bit of the key is extracted by comparing the oscillation frequencies of these ROs [19], [20], [21]. RO-based PUFs are also popular in (Field Programmable Gate Arrays) FPGAs platforms due to their straightforward operational principle and design. However, they face limitations in terms of entropy and uniqueness, prompting the exploration of techniques to enhance their randomness as discussed in earlier literature [22], [23], [24], [25]. Furthermore, these simple architectures can be prone to high instability under process, supply voltage, and temperature (PVT) variations [26]. At this purpose it is important to note that, even if ideally the bits words generated by a PUF have to be independent from PVT variations, typically in real applications there exist certain bit cells of the PUF, for which voltage and temperature dependencies can lead to bit flips, thus degrading the reproducibility of the unique key [27], [28], [29], [30], [31]. In related works like [21], [23], and [32], various methods have been proposed to enhance the stability performance of traditional Ring Oscillator (RO) based PUFs. As an example, Current Starved (CS) inverters have been proposed in [32] to allow a calibration of the oscillation frequency of ROs through a control voltage set for optimal reliability. Arbiter PUFs (APUF) which are based on measuring the delay differences between two nominally identical timing paths have become very popular both for ASIC and FPGA implementations [33], [34], [35], [36], [37], [38], [39], [40], [41]. Metastable PUFs

Manuscript received 19 January 2024; revised 31 March 2024; accepted 28 April 2024. This article was recommended by Associate Editor Q. Liu. *(Corresponding author: Riccardo Della Sala.)*

Riccardo Della Sala, Francesco Centurelli, Giuseppe Scotti, and Alessandro Trifiletti are with the DIET Department, Sapienza University of Rome, 00184 Rome, Italy (e-mail: riccardo.dellasala@uniroma1.it; francesco.centurelli@uniroma1.it; giuseppe.scotti@uniroma1.it; alessandro.trifiletti@uniroma1.it).

Davide Bellizia is with Telsy S.p.A., 00161 Rome, Italy (e-mail: davide.bellizia@telsy.it).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCSI.2024.3396916.

Digital Object Identifier 10.1109/TCSI.2024.3396916

rely on a positive feedback loop which forces the output to either logic one or logic zero depending on mismatch variations, and several papers dealing with these kind of architectures have been recently proposed [17], [28], [29], [42], [43], [44], [45], [46], [47], [48]. Also metastable PUFs are sensitive to PVT variations, and several approaches such as the use of complementary to absolute temperature current sources, temporal majority voting circuits, or the introduction of soft dark bits, have been exploited in the literature to reduce the number of unstable bits, thus improving reliability [49], [50], [51], [52].

Fully static and monostable PUFs have been presented in the literature as robust and power-efficient solutions for on-chip key generation [26], [53], [54]. Static PUFs generate an output bit by measuring the difference between two nominally identical currents, produced by two MOS transistors affected by mismatch variations, and do not require an excitation phase, which can be susceptible to transient noise effects [26]. Contrastingly, other solutions that rely on excitation sequences may be vulnerable to transient noise, leading to a degradation of bit stability, even under nominal conditions [52]. Furthermore, unlike metastable-based PUFs, which are bistable [17], [28], [51], the keys generated by monostable PUFs remain immune to accidental flipping.

A well established approach to implement static PUFs relies on regulated cascode current mirrors (RCCMs), in which mismatch variations in both a PMOS and an NMOS current mirrors are exploited to generate a current offset, which is converted into a voltage thanks to the very high output resistance of the current mirrors [26]. This voltage, generated by complementary current mirrors, is then amplified to obtain a stable output bit. However, as previously mentioned, this architecture may lead to bit-flipping occurrences under PVT variations due to fluctuations in NMOS and PMOS threshold voltages [55]. To enhance the resiliency of RCCM PUFs against PVT variations, an improved version of the RCCM was proposed by [55], where a feedback mechanism to generate a control voltage that adjusts the body terminals of the cascode current mirrors is introduced to properly set the threshold voltage under PVT variations, the output resistance is increased by means of a gain-boosting configuration, and a C-Muller cell is added to provide a stable logic value at the bit-cell output.

Other static PUF topologies which rely on cross-coupled architectures, incorporating an additional error amplifier to better exploit mismatch variations between two nominally identical branches have been reported in [56] and [57]. A static PUF based on voltage dividers, which leverages the mismatch of threshold voltages in four stacked PMOS transistors to generate an offset voltage, which is further amplified by a cascoded stage has been recently presented in [58]. The main drawback of this circuit is in its highly variable power consumption, due to the strong dependence of the bias current on PVT variations.

A monostable PUF exploiting improved regulated cascode current mirrors to boost the native bit stability against transient noise, and improve the robustnsess with respect to environmental variations has been proposed in [59]. The minimum supply voltage allowed by this circuit is 0.6V.

This paper is an extended version of the conference paper [60], in which a novel approach to implement an highly mismatched current mirror with a fully unbalanced output is introduced. This approach involves the usage of body-driven feedbacks in order to decrease the minimum supply voltage of the circuit. The minimum supply voltage of previously presented RCCM PUFs [55], [59], [61] is in the range of 0.6V, whereas the proposed PUF cell is able to work with a supply voltages as low as 0.3V. An additional advantage of the proposed approach is that the nominal power consumption is well-defined through a reference bias current, ensuring that power consumption remains stable despite PVT variations. A testchip including 128 bit-cells has been fabricated in a 130nm CMOS process, and measurements results have shown that the proposed PUF is able to work with very low energy consumption per bit (about 0.3 fJ/bit) and with good overall statistical performance, resulting in a response with a 49.42% bias, a reliability of 99.483% (measured without the requiring any postprocessing), and a uniqueness of 50.176%.

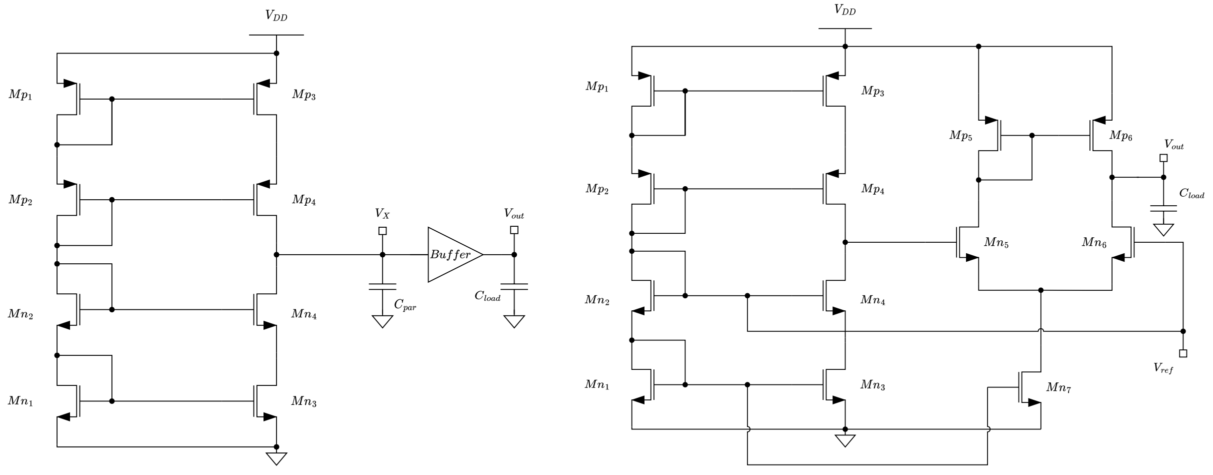
In the following Section II a background of monostable PUFs has been provided, Section III presents the circuit topology of the proposed PUF and explains its operating principle, providing a detailed analytical study of circuit's behavior, Section IV describes the design and implementation of a 128 bit PUF macro in a 130nm CMOS prototype chip. Measurement results are presented in Section V. Figures of merit and performance evaluation metrics are reported in Section VI. A comparison with the state-of-the-art is discussed in Section VII, and finally, conclusions are drawn in Section VIII.

II. Background of Monostable Physical Unclonable Functions

Static PUF bit cells produce an output bit by measuring the difference between two nominally identical currents generated by two highly mismatched MOS transistors. Unlike metastable-based PUFs, which are bistable [17], [28], [51], the keys generated by monostable PUFs are not compromised by accidental flips [52], since they do not require an excitation phase susceptible to transient noise [26]. Thanks to their working principle, fully static and monostable PUFs are considered among the most robust and power-efficient solutions for on-chip key generation both in terms of reliability and stability concerning supply voltage and temperature variations.

Among static PUFs, the most promising approach is based on RCCM PUFs [26]. The architecture presented in [26] is depicted in Fig. 1a. The architecture exploits differences between NMOS and PMOS currents, generated by a complementary current mirror, to produce an offset current at the high impedance output node. However, since at the node X of the architecture the voltage could not be fully saturated to either 0 or V_{DD}, a further stage has to be inserted, such as a buffer. However, as mentioned earlier, this architecture may experience bit flipping under PVT variations because the sign of the resulting offset current can change based on variations in NMOS and PMOS threshold voltages resulting from process or temperature changes. In order to improve bit flipping under PVT variations, in [26] another version of the RCCM has been proposed and is depicted in Fig. 1b.

The output buffer has been substituted with a differential pair which compares the voltage from the reference branch with respect to the one obtained at the output of the current mirror. In this way, the dependence with respect to the supply voltage and also temperature is mitigated, thus improving the reliability of the PUF and reducing the number of unstable bits and also bit error rate.



(a)

(b)

Fig. 1. PUF Cell presented in [26] and based on current mirrors, version with a buffer as output stage a) and version with a differential pair as output stage b).

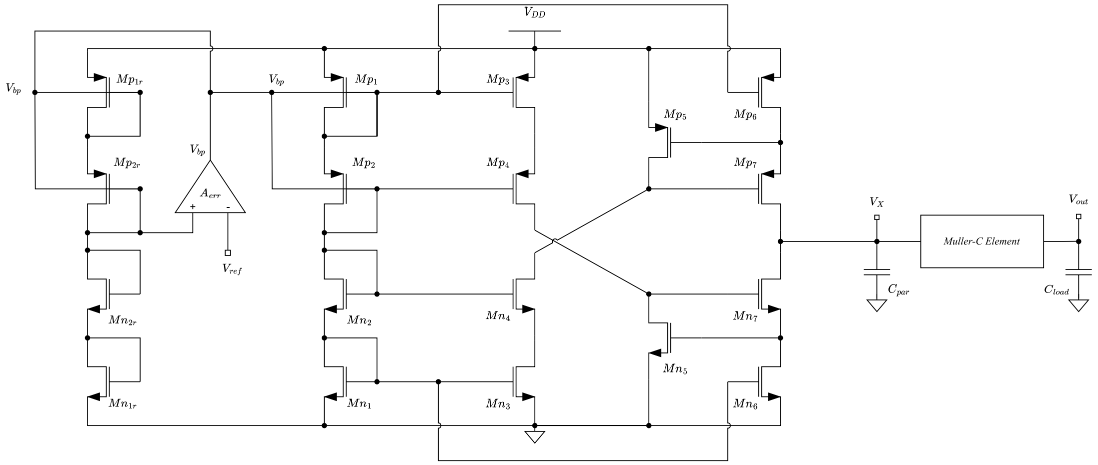


Fig. 2. PUF Cell presented in [55] and based on current mirrors.

An enhanced version of the RCCM PUF was proposed in [55]. The architecture based on the RCCM is depicted in Fig. 2. As it can be observed, a gain boosting technique to the intermediate node X has been used to enhance the output resistance in order to increase the transimpedance gain with respect to the generated offset current at the node X. In addition, an output stage composed by a Muller-C element has been inserted in order to assure that the output voltage is fully saturated to either 0 or V_{DD}. Furthermore, the gain boosting at the node X reduces also the probability of bit instability due to the noise in the start-up phase. However, in order to assure the resiliency of the PUF with respect to voltage or temperature variations, authors propose to insert a control loop based on a replica approach to control that the voltage at the middle node of the reference current branch remains in a limited range of a reference voltage. To do so, they inserted an error amplifier in the feedback loop and control the threshold voltage of both $M_{p1,2}$ through the body terminal of the latter. However, this design is not low power, since it employs many current branches and also a huge amount of area (e.g. it requires a Muller-C element, which introduces additional area and power consumption).

A recent static PUF based on voltage dividers [58] has been introduced in the literature and is depicted in Fig. 3. It utilizes threshold voltage mismatches in four stacked PMOS transistors to generate an offset voltage used as input to a cascoded inverter with high voltage gain and rail-to-rail voltage swing. Despite its promising performance, the power consumption of this architecture is not well-defined since it lacks of a current generator, resulting in potentially variable power consumption depending on the biasing of internal nodes.

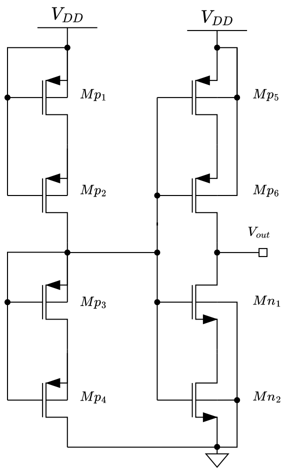


Fig. 3. PUF Cell presented in [58] and based on voltage dividers.

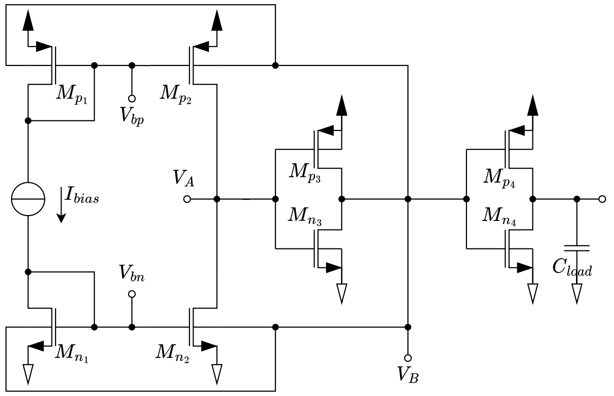


Fig. 4. Proposed PUF bit-cell topology based on body-driven feedbacks.

III. Circuit Topology of the Proposed PUF

The proposed PUF architecture is depicted in Fig.4. It is a topology derived from the Regulated Cascode Current Mirror PUF [55] in which a positive feedback through the body terminals has been exploited to reach a full-swing output at nodes A and B, as done in SRAM cells. The main current branch composed by transistors M_{n_1} and M_{p_1} mirrors a reference bias current I_{bias} through gate terminals of transistors M_{n_2} and M_{p_2}. Due to the unavoidable mismatches between M_{n_2} and M_{p_2} an offset current at node A is generated (namely I_{off}). This offset current, multiplied by the output resistance seen at node A, gives the offset voltage V_A. The offset voltage V_A is fed back to the body terminals of M_{n_1}, M_{n_2}, M_{p_1} and M_{p_2}.

A. Working Principle and Design Strategy

In order to gain insight into the behavior of the proposed circuit, it is possible to start from the analytical expression of the drain current for NMOS and PMOS devices working in the subthreshold region [62], [63]:

$$\begin{cases} I_{d_n} = I_{d0_n} e^{\frac{Vgs_n - Vth_n}{n\ Ut}} \left(1 - e^{-\frac{Vds_n}{Ut}}\right) \ \text{NMOS} \\ I_{d_p} = I_{d0_p} e^{\frac{Vsgp + Vthp}{n\ Ut}} \left(1 - e^{-\frac{Vsdp}{Ut}}\right) \ \text{PMOS} \end{cases} \tag{1}$$

where usual notation is adopted for gate-source, drain-source and threshold voltages of NMOS and PMOS transistors, Ut denotes the thermal voltage, $n = 1 + C_{depl}/C_{ox}$ and I_{d_0} can be written as:

$$I_{d0_{n,p}} = \mu_{n,p}(n-1)C_{ox}\frac{W_{n,p}}{L_{n,p}}U_t^2 \tag{2}$$

where $\mu_{n,p}$ and C_{ox} are the mobility and oxide capacitance per unit area, whereas $W_{n,p}$ and $L_{n,p}$ are gate width and gate lenght of NMOS and PMOS devices respectively.

Considering that M_{p_1} and M_{p_2} have the same Vsg_p, neglecting the effect of the drain source voltage on the drain currents, it can be derived that:

$$\ln\left(\frac{I_{d_{p1}}}{I_{d0_{p1}}}\frac{I_{d0_{p2}}}{I_{d_{p2}}}\right) = \frac{|Vth_{p_2}| - |Vth_{p_1}|}{n\ U_t} \tag{3}$$

The same considerations can be done for M_{n_1} and M_{n_2} since they have the same Vgs_n, obtaining:

$$\ln\left(\frac{I_{d_{n1}}}{I_{d0_{n1}}}\frac{I_{d0_{n2}}}{I_{d_{n2}}}\right) = \frac{Vth_{n_2} - Vth_{n_1}}{n\ U_t} \tag{4}$$

Then, considering the difference between Eq. 3 and Eq. 4 the following relation can be derived:

$$\ln\left(\frac{I_{d_{p1}}}{I_{d0_{p1}}}\frac{I_{d0_{p2}}}{I_{d_{p2}}}\frac{I_{d0_{n1}}}{I_{d_{n1}}}\frac{I_{d_{n2}}}{I_{d0_{n2}}}\right) = \\ = \frac{|Vth_{p_2}| - |Vth_{p_1}| + Vth_{n_1} - Vth_{n_2}}{n\ U_t} \tag{5}$$

The value of the output voltage of the proposed PUF can be reconduced to the value of the offset voltage at the node A (with respect to the ideal output voltage equal to $V_{DD}/2$), which is proportional to the difference between the currents $I_{d_{p2}}$ and $I_{d_{n2}}$:

$$I_{off} = I_{d_{p2}} - I_{d_{n2}} = I_{d_{p_2}}(1 - \frac{I_{d_{n2}}}{I_{d_{p2}}}) \tag{6}$$

Thus, the current offset would be 0 if $\frac{I_{d_{n2}}}{I_{d_{p2}}} = 1$ which turns in $\ln\left(\frac{I_{d_{n2}}}{I_{d_{p2}}}\right) = 0$. From Eq. 5 it can be derived that:

$$\ln\left(\frac{I_{d_{n2}}}{I_{d_{p2}}}\right) = \\ = \frac{-|Vth_{p_1}| + |Vth_{p_2}| + Vth_{n_1} - Vth_{n_2}}{n\ U_t} + \\ + \ln\left(\frac{I_{d0_{p1}} I_{d_{n1}} I_{d_{n2}}}{I_{d_{p1}} I_{d0_{p2}} I_{d0_{n1}}}\right) \tag{7}$$

Now, since the current in the first branch composed by M_{n_1} and M_{p_1} is forced to I_{bias}, $I_{d_{n1}} = I_{d_{p1}}$. Thus, Eq. 7 can be rewritten as:

$$\ln\left(\frac{I_{d_{n2}}}{I_{d_{p2}}}\right) = \\ = \frac{-|Vth_{p_1}| + |Vth_{p_2}| + Vth_{n_1} - Vth_{n_2}}{n\ U_t} + \\ + \ln\left(\frac{I_{d0_{p1}} I_{d0_{n2}}}{I_{d0_{p2}} I_{d0_{n1}}}\right) \tag{8}$$

Now, with considering Eq. 2, Eq. 8 can be further simplified as:

$$\ln\left(\frac{I_{d_{n2}}}{I_{d_{p2}}}\right) = \\ = \frac{-|Vth_{p_1}| + |Vth_{p_2}| + Vth_{n_1} - Vth_{n_2}}{n\ U_t} + \\ - \ln\left(\frac{W_{p2}W_{n1}}{W_{p1}W_{n2}}\frac{L_{p1}L_{n2}}{L_{p2}L_{n1}}\right) \tag{9}$$

Looking at Eq. 9 it is evident that, since in nominal conditions transistors M_{n_1} and M_{n_2} and transistors M_{p_1} and M_{p_2} are equal to each other, the current offset I_{off} is equal to 0. It has to be noted that, this condition is also guaranteed by the matching of the $|V_{bs_{n,p_{1,2}}}|$ which being equal to each other assure that:

$$\Delta Vth_{n(p)} = Vth_{n(p)_2} - Vth_{n(p)_1} = \\ = Vth_{0_{n(p)_2}} - Vth_{0_{n(p)_1}} + \gamma_{n(p)}(|Vbs_{n(p)_1}| - |Vbs_{n(p)_2}|) = \\ = Vth_{0_{n(p)_2}} - Vth_{0_{n(p)_1}} \tag{10}$$

where $\gamma_{n(p)}$ denotes the body-effect coefficient of the threshold voltage.

According to the above analysis, with the goal of minimizing the systematic offset (thus maximizing the entropy of the PUF cell), M_{n,p_1} and M_{n,p_2} have to be sized to obtain $V_{ds_{n,p_2}}$ equal to $V_{DD}/2$ for a bias current I_{bias}. Furthermore, transistors M_{n,p_3} and M_{n,p_4} have been sized to center the voltage transfer characteristic of the inverters at $V_{DD}/2$. In this way, the statistical performance of the bitcell are optimized and the value of its output voltage is ideally only dependent on mismatch variations.

B. Effects of Mismatch and Process Variations on the PUF Output

Given the Eq. 9 it can be derived that the ratio of $\frac{I_{d_{n2}}}{I_{d_{p2}}}$ will result in a current offset whose sign will determine the value of the output of the PUF. Indeed, if the ratio $\frac{I_{d_{n2}}}{I_{d_{p2}}}$ is greater (lower) than 1, the sign of the current offset will be minus (plus). The threshold voltages of NMOS and PMOS transistors are affected by process variations and with respect to that they follow a Normal distriubtion with mean value $\mu_{Vth_{prc}}$ and standard deviation $\sigma_{Vth_{prc}}$:

$$Vth_{n,p_{prc}} = \mathcal{N}(\mu_{Vth_{n,p_{prc}}}, \sigma^2_{Vth_{n,p_{prc}}}) \tag{11}$$

In addition, the threshold voltages are also affected by mismatch variations and follow a Normal distriubtion with mean value $\mu_{Vth_{mm}}$ and standard deviation $\sigma_{Vth_{mm}}$:

$$Vth_{n,p_{mm}} = \mathcal{N}(\mu_{Vth_{n,p_{mm}}}, \sigma^2_{Vth_{n,p_{mm}}}) \tag{12}$$

The generic threshold voltage can be thus written as:

$$Vth_{n,p} = Vth_{n,p_{prc}} + Vth_{n,p_{mm}} \tag{13}$$

which clearly follows a multivariate Normal distribution. If a single realization of the manufactoring process is considered, $Vth_{n,p_{prc}}$ is a constant whose value is here on denoted as $\nu_{n,p_{prc}}$

$$Vth_{n,p} = Vth_{n,p_{mm}} + \nu_{n,p_{prc}} \tag{14}$$

For what concerns the term $\ln\left(\frac{W_{p2}W_{n1}}{W_{p1}W_{n2}}\frac{L_{p1}L_{n2}}{L_{p2}L_{n1}}\right)$, it is also affected by mismatch and process variations, since its argument is the ratio of the channel lengths and widths of transistors that are affected by mismatch and process variations. In the following the argument of the above logarithmic term is assumed to be a multivariate random variable, similarly to the threshold voltages of NMOS and PMOS devices.

Since the ratio is given by nominally identical width and length we can write this ratio as:

$$\frac{W_{p2}W_{n1}}{W_{p1}W_{n2}}\frac{L_{p1}L_{n2}}{L_{p2}L_{n1}} = 1 + R = 1 + R_{prc} + R_{mm} \tag{15}$$

which for a given process realization results in

$$\frac{W_{p2}W_{n1}}{W_{p1}W_{n2}}\frac{L_{p1}L_{n2}}{L_{p2}L_{n1}} = 1 + R = 1 + r + R_{mm} \tag{16}$$

where $E\big[R_{mm}\big] = \mu_\rho$ and $Var\big[R_{mm}\big] = \sigma^2_\rho$. With considering a Taylor approximation of the first order [64] it follows that:

$$\begin{cases} E\big[\ln(1+r+R_{mm})\big] \approx \ln(1+r+\mu_\rho) - \dfrac{\sigma^2_\rho}{(1+r+\mu_\rho)^2} \\ = a_{mm} \\ Var\big[\ln(1+r+R_{mm})\big] \approx \dfrac{\sigma^2_\rho}{(1+r+\mu_\rho)^2} = \sigma^2_{a_{mm}} \end{cases} \tag{17}$$

Considering a process realization, by looking at Eq. 8 it can be observed that there are two threshold voltage differences. The threshold voltage difference defined as $\Delta V_{th_{n,p}} = V_{th_{n,p_2}} - V_{th_{n,p_1}}$ for a given process realization follow a normal distribution:

$$\begin{aligned} \Delta V_{th_{n,p}} &\sim \mathcal{N}\big(\mu_{Vth_{mm_{n,p2}}} - \mu_{Vth_{mm_{n,p1}}}, \\ &\quad \sigma^2_{Vth_{mm_{n,p2}}} + \sigma^2_{Vth_{mm_{n,p1}}}\big) \\ &= \mathcal{N}(\mu_{\Delta Vth_{mmn,p}}, \sigma^2_{\Delta Vth_{mmn,p}}) \end{aligned} \tag{18}$$

The Eq. 8 can be therefore written as:

$$\ln\left(\frac{I_{d_{n2}}}{I_{d_{p2}}}\right) = \frac{-\Delta V_{th_n} + \Delta V_{th_p} - \ln(1+r+R_{mm})\ nU_t}{nU_t} \tag{19}$$

Defining as ΔV_{th} the difference $\Delta V_{th_p} - \Delta V_{th_n}$, it derives that ΔV_{th} follows a normal distribution whose mean value $\mu_{\Delta Vth}$ can be written as:

$$\begin{cases} \mu_{\Delta Vth_{mm}} = \\ \qquad -\mu_{Vth_{mm_{n2}}} + \mu_{Vth_{mm_{n1}}} + \mu_{Vth_{mm_{p2}}} - \mu_{Vth_{mm_{p1}}} \\ \sigma^2_{\Delta Vth_{mm}} = \\ \qquad \sigma^2_{Vth_{mm_{n2}}} + \sigma^2_{Vth_{mm_{n1}}} + \sigma^2_{Vth_{mm_{p2}}} + \sigma^2_{Vth_{mm_{p1}}} \end{cases} \tag{20}$$

and thus:

$$\ln\left(\frac{I_{d_{n2}}}{I_{d_{p2}}}\right) = \frac{\Delta V_{th} - \ln(1+r+R_{mm})\ nU_t}{nU_t} \tag{21}$$

As a consequence, it can be derived the statistical property of the $\ln\big(\frac{I_{d_{n2}}}{I_{d_{p2}}}\big)$:

$$\begin{aligned} &E\Big[\ln\big(\frac{I_{d_{n2}}}{I_{d_{p2}}}\big)\Big] \\ &= \frac{-\mu_{Vth_{mm_{n2}}} + \mu_{Vth_{mm_{n1}}} + \mu_{Vth_{mm_{p2}}} - \mu_{Vth_{mm_{p1}}} - nU_t a_{mm}}{nU_t} \end{aligned} \tag{22}$$

and

$$\begin{aligned} Var\Big[\ln\big(\frac{I_{d_{n2}}}{I_{d_{p2}}}\big)\Big] &= \sigma^2_{\Delta Vth}/(nU_t)^2 + \sigma^2_{a_{mm}} + \\ &\quad - 2Cov\Big[\frac{\Delta Vth}{n\ U_t}, \ln(1+r+R_{mm})\Big] \end{aligned} \tag{23}$$

Normalizing the output voltage V_A of the PUF cell to the value of the supply voltage V_{DD}, we obtain the logic value of the PUF output, which results a random variable and can be expressed as follows:

$$X = \frac{1 + sign\big\{\ln\big(\frac{I_{d_{n2}}}{I_{d_{p2}}}\big)\big\}}{2} \tag{24}$$

its expected value can be derived as:

$$E\big[X\big] = \frac{1}{2} + \frac{1}{2}E\Big[sign\big\{\ln\big(\frac{I_{d_{n2}}}{I_{d_{p2}}}\big)\big\}\Big] \tag{25}$$

The expected value of the sign of $\ln\big(\frac{I_{d_{n2}}}{I_{d_{p2}}}\big)$ can be derived as:

$$\begin{aligned} &E\Big[sign\big\{\ln\big(\frac{I_{d_{n2}}}{I_{d_{p2}}}\big)\big\}\Big] \\ &= 1 \cdot P\Big(sign\big\{\ln\big(\frac{I_{d_{n2}}}{I_{d_{p2}}}\big)\big\} > 0\Big) - 1 \\ &\cdot P\Big(sign\big\{\ln\big(\frac{I_{d_{n2}}}{I_{d_{p2}}}\big)\big\} < 0\Big) \\ &= 2 \cdot P\Big(sign\big\{\ln\big(\frac{I_{d_{n2}}}{I_{d_{p2}}}\big)\big\} > 0\Big) - 1 \end{aligned} \tag{26}$$

where $P(A)$ denotes the probability of event A.

The $P\Big(sign\big\{\ln\big(\frac{I_{d_{n2}}}{I_{d_{p2}}}\big)\big\} > 0\Big)$ can be derived as:

$$\begin{aligned} &P\Big(sign\big\{\ln\big(\frac{I_{d_{n2}}}{I_{d_{p2}}}\big)\big\} > 0\Big) \\ &= \mathrm{erf}\Bigg(\frac{\mu_{\Delta V_{th}}/(nU_t) - a_{mm}}{\sqrt{2(\sigma^2_{\Delta Vth}/(nU_t)^2 + \sigma^2_{a_{mm}})}}\Bigg) \end{aligned} \tag{27}$$

and finally the expected value of the PUF output can be derived as:

$$\begin{aligned} E[X] = &\frac{1}{2} \\ &- \frac{1}{2}\mathrm{erf}\Bigg(\frac{\mu_{\Delta V_{th}}/(nU_t) - a_{mm}}{\sqrt{2(\sigma^2_{\Delta Vth}/(nU_t)^2 + \sigma^2_{a_{mm}})}}\Bigg) \end{aligned} \tag{28}$$

The above equation shows that, if ΔV_{th} which is the difference among $\Delta V_{th_n} - \Delta V_{th_p}$ (and thus is the difference of the difference of two random variables), is small enough and if the sizing is properly chosen (so that $a_{mm} = 0$), the expected value of the PUF output is equal to 0.5, and it can be associated to an ideal entropy source.

C. Effect of Supply Voltage Variations on the PUF Response

Starting from Eq. 10, and considering the dependence of the threshold voltage on the body-source voltage under mismatch variations, the difference between the threshold voltages of two nominally identical NMOS (PMOS) transistors, can be written as:

$$\begin{aligned} \Delta Vth_{n(p)} &= Vth_{n(p)_2} - Vth_{n(p)_1} = \\ &= Vth_{0_{n(p)_2}} - Vth_{0_{n(p)_1}} \\ &\quad + (\gamma_{n(p)_1} - \gamma_{n(p)_2})(|Vbs_{n(p)}|) \end{aligned} \tag{29}$$

Then, referring to Eq. 24, it can be observed that the output bit is generated according to the sign of the term $\ln\left(\frac{I_{d_{n2}}}{I_{d_{p2}}}\right)$. From Eq. 21, considering that under mismatch $\gamma_{n(p)}$ coefficients are different between each other device-per-device, the following relation can be derived:

$$\begin{aligned} \ln\left(\frac{I_{d_{n2}}}{I_{d_{p2}}}\right) = &\frac{\Delta V_{th_{0_p}} - \Delta V_{th_{0_n}} - \ln(1 + r + R_{mm})\ nU_t}{nU_t} + \\ &+ \frac{(\gamma_{p_2} - \gamma_{p_1})|Vbs_p| - (\gamma_{n_2} - \gamma_{n_1})|Vbs_n|}{nU_t} \end{aligned} \tag{30}$$

Therefore, for a given mismatch, the voltage at the internal node V_A and at the output of the PUF (node V_{Out}) are V_{DD} or GND.

Starting from analyzing the case in which the V_A is GND (output bit 0), from Eq. 30 the V_{bs} term related to the PMOS can be simplified (because $V_{bs_p} = 0$) and it follows that the sign of $\ln\frac{I_{d_{n2}}}{I_{d_{p2}}}$ is -1, thus the following relation is satisfied:

$$\begin{aligned} &\Delta V_{th_{0_p}} - \Delta V_{th_{0_n}} - \ln(1 + r + R_{mm})\ nU_t \\ &\quad - (\gamma_{n_2} - \gamma_{n_1})V_{DD} < 0 \end{aligned} \tag{31}$$

Denoting with ΔV_{DD} the variation of the supply voltage, the bit value is flipped if and only if:

$$\begin{aligned} &\Delta V_{th_{0_p}} - \Delta V_{th_{0_n}} - \ln(1 + r + R_{mm})\ nU_t + \\ &\quad - (\gamma_{n_2} - \gamma_{n_1})V_{DD} - (\gamma_{n_2} - \gamma_{n_1})\Delta V_{DD} > 0 \end{aligned} \tag{32}$$

Referring to the above equation, two cases have to be considered. In the first case, $\Delta V_{DD} > 0$, and the output bit flips only if the condition: $\gamma_{n_2} - \gamma_{n_1} < 0$ is verified. In the second second case, the $\Delta V_{DD} < 0$, and the only possibility for which the output will flip is that $\gamma_{n_2} - \gamma_{n_1} > 0$. Thus, each cell whose nominal output is GND can be flipped with a positive or negative supply voltage variations depending on the sign of the difference of the terms γ_n. The critical value of ΔV_{DD} which results in a bit flipping can be expressed as:

$$\begin{aligned} &\Delta V_{DD} \\ &> \frac{|\Delta V_{th_{0_p}} - \Delta V_{th_{0_n}} - \ln(1+r+R_{mm})\ nU_t - (\gamma_{n_2} - \gamma_{n_1})V_{DD}|}{|\gamma_{n_2} - \gamma_{n_1}|} \end{aligned} \tag{33}$$

It has to be remarked that the denominator tends to 0 ($M_{p_{1,2}}$ are sized nominally identical) and as a consequence very large supply voltage variations have to occur to flip the bits.

Similar considerations hold for the case in which the nominal output is V_{DD}. In that case the following relation is satisfied:

$$\begin{aligned} &\Delta V_{th_{0_p}} - \Delta V_{th_{0_n}} - \ln(1 + r + R_{mm})\ nU_t \\ &\quad + (\gamma_{p_2} - \gamma_{p_1})V_{DD} > 0 \end{aligned} \tag{34}$$

The output bit flips in this condition if and only if the following relation is satisfied:

$$\begin{aligned} &\Delta V_{th_{0_p}} - \Delta V_{th_{0_n}} - \ln(1 + r + R_{mm})\ nU_t + \\ &\quad + (\gamma_{p_2} - \gamma_{p_1})V_{DD} + (\gamma_{p_2} - \gamma_{p_1})\Delta V_{DD} < 0 \end{aligned} \tag{35}$$

The ΔV_{DD} sign which can satisfy the above equation is related to the sign of $\gamma_{p_2} - \gamma_{p_1}$. Considering a positive(negative) supply voltage variation ΔV_{DD}, the output bit can be flipped only for $\gamma_{p_2} - \gamma_{p_1} < 0$ ($\gamma_{p_2} - \gamma_{p_1} > 0$) for a quantity given by the following relation:

$$\Delta V > \frac{|\Delta V_{th_{0_p}} - \Delta V_{th_{0_n}} - \ln(1+r+R_{mm})\ nU_t + (\gamma_{p_2} - \gamma_{p_1})V_{DD}|}{|\gamma_{p_2} - \gamma_{p_1}|} \tag{36}$$

Also in that case, it can be observed that the denominator tends to 0 ($M_{n_{1,2}}$ are sized nominally identical) and as a consequence very large supply voltage variations have to occur to flip the bits.

Overall, the proposed architecture is effective to reject effect of the supply voltage variations on the generated bit response, guaranteeing an high reliability if transistors $M_{p_{1,2}}$ and $M_{n_{1,2}}$ are nominally identical between each other.

D. Effect of Temperature Variations on the PUF Response

In order to understand how the temperature affects the PUF reliability, it can be taken into account that the threshold voltage under temperature variations changes according to the following relation:

$$Vth_{n(p)} = Vth_{0_{n(p)}} - \kappa_{n(p)}(T - T_0) \tag{37}$$

where $\kappa_{n(p)}$ denotes the thermal coefficient of the threshold voltage with respect to temperature variations. Considering mismatch effects, Eq. 29 can be rewritten as:

$$\begin{aligned}\Delta Vth_{n(p)}(T) &\\ = Vth_{n(p)_2}(T) - Vth_{n(p)_1}(T) &= \\ = Vth_{0_{n(p)_2}} - Vth_{0_{n(p)_1}} - (\kappa_{n(p)_2} - \kappa_{n(p)_1})(T - T_0) &\end{aligned} \tag{38}$$

Being the sign of the output bit given by relation Eq. 21, under temperature variations it can be rewritten as:

$$\begin{aligned}\ln\left(\frac{I_{d_{n2}}(T)}{I_{d_{p2}}(T)}\right) &\\ = \frac{\Delta V_{th_{0_p}} - \Delta V_{th_{0_n}} - \ln(1+r+R_{mm})\ n\ kT/q}{n\ kT/q} &+ \\ - \frac{\kappa_{p_2} - \kappa_{p_1} - \kappa_{n_2} + \kappa_{n_1}}{n\ kT/q}(T - T_0) &\end{aligned} \tag{39}$$

where the thermal voltage term has been expanded as: $nU_t = kT/q$, where q is the elementary charge, T is the temperature in Kelvin, and k is the Boltzman constant.

By looking at Eq. 39 it can be observed that in the nominal condition ($T = T_0$) the ratio has a sign which determines the value of the PUF output bit. Now, considering as an example that the output of the PUF cell is V_{DD} (GND), the sign of Eq. 39 is positive (negative) and thus:

$$\begin{aligned}\ln\left(\frac{I_{d_{n2}}(T_0)}{I_{d_{p2}}(T_0)}\right) &\\ = \frac{\Delta V_{th_{0_p}} - \Delta V_{th_{0_n}} - \ln(1+r+R_{mm})\ n\ kT_0/q}{n\ kT_0/q} &\gtrless 0\end{aligned} \tag{40}$$

However, under temperature variations it can happen that the sign of Eq. 39 changes and so:

$$\begin{aligned}\ln\left(\frac{I_{d_{n2}}(T)}{I_{d_{p2}}(T)}\right) &\\ = \frac{\Delta V_{th_{0_p}} - \Delta V_{th_{0_n}} - \ln(1+r+R_{mm})\ n\ kT/q}{n\ kT/q} &+ \\ - \frac{\kappa_{p_2} - \kappa_{p_1} - \kappa_{n_2} + \kappa_{n_1}}{n\ kT/q}(T - T_0) &\lesseqgtr 0\end{aligned} \tag{41}$$

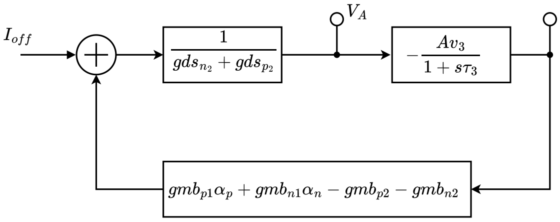

I_{off}
V_A
V_B
$\frac{1}{gds_{n_2} + gds_{p_2}}$
$-\frac{Av_3}{1 + s\tau_3}$
$gmb_{p1}\alpha_p + gmb_{n1}\alpha_n - gmb_{p2} - gmb_{n2}$

Fig. 5. Block scheme of the proposed PUF architecture.

Thus, there is the possibility that the bit flips if a temperature variations ΔT greater than a given quantity occurs, according to the following relation:

$$|\Delta T| > \frac{|\Delta V_{th_{0_p}} - \Delta V_{th_{0_n}} - \ln(1+r+R_{mm})\ n\ kT_0/q|}{|\ln(1+r+R_{mm})\ n\ k/q + \kappa_{p_2} - \kappa_{p_1} - \kappa_{n_2} + \kappa_{n_1}|} \tag{42}$$

For what concerns the sign of the ΔT, it will be determined by the sign of the denominator of Eq. 42, and by the outcome of the mismatch on the specific PUF instance. For the case in which the nominal output is V_{DD} (GND), the sign of the ΔT can be derived from Eq. 41, and is concordant (discordant) to the sign of: $\ln(1+r+R_{mm})\ n\ k/q + \kappa_{p_2} - \kappa_{p_1} - \kappa_{n_2} + \kappa_{n_1}$. It is worth noting that larger threshold mismatches lead to an increase in the numerator. Moreover, considering that the thermal coefficient varies between devices in a second-order approximation, the term $|\kappa_{p_2} - \kappa_{p_1} - \kappa_{n_2} + \kappa_{n_1}|$ approaches values close to zero. Consequently, this amplifies the minimum temperature shift necessary to alter the bits.

E. Effect of the Body-Driven Feedbacks

A crucial requirement for ensuring the functionality of the proposed PUF is the imperative need to completely saturate the output voltage V_B to either 0 or V_{DD}. However, given the very low supply voltage of only 0.3V, cascoded stages are not allowed and, as a consequence, solutions based on conventional RCCM-based PUFs such as the ones reported in [26] and [55] are not feasible. To overcome this issue, the proposed PUF exploits body-driven feedbacks to provide fully unbalance of the output voltage V_B to 0 or V_{DD}, as will be better detailed in the following.

The block scheme describing the feedback mechanism exploited in the proposed PUF is depicted in Fig. 5, where usual notation is adopted for small signal parameters of MOS transistors. The two terms α_p and α_n are defined as follows:

$$\begin{cases}\alpha_p = \dfrac{gm_{p2}}{gm_{p1} + gds_{p1}} \\ \alpha_n = \dfrac{gm_{n2}}{gm_{n1} + gds_{n1}}\end{cases} \tag{43}$$

and it can be thereafter defined:

$$gmb_{p1}\alpha_p - gmb_{n1}\alpha_n - gmb_{p2} - gmb_{n2} = -gmb_{eq} \tag{44}$$

which is a negative quantity.

The voltage gain Av_3 and the time constant τ_3 of the inverter made up of transistors M_{n,p_3} can be easily computed as:

$$\begin{cases} Av_3 = \dfrac{gm_{n3} + gm_{p3}}{gds_{p3} + gds_{n3}} \\ \tau_3 = \dfrac{C_{L3}}{gds_{p3} + gds_{n3}} \end{cases} \tag{45}$$

The variation of the voltage V_B with respect to its initial value assumed to be $V_{DD}/2$ can be derived as follows:

$$V_B(s) = \frac{i_{off}}{gmb_{eq}} \cdot \frac{1}{1 - s\tau_3 gds_2/(gmb_{eq}Av_3)} \tag{46}$$

which can be further simplified as:

$$V_B(s) = \frac{i_{off}}{gmb_{eq}} \cdot \frac{1}{1 - s\frac{gds_2 C_{L3}}{gmb_{eq}(gm_{n3}+gm_{p3})}} \tag{47}$$

which in the time domain results in:

$$v_B(t) = \frac{i_{off}}{gmb_{eq}} \cdot e^{t\frac{gmb_{eq}(gm_{n3}+gm_{p3})}{gds_2 C_{L3}}} \tag{48}$$

Assuming that at t=0 the output voltage V_A is nominally fully balanced to $V_{DD}/2$ (due to the design strategy) and as a consequence also $V_B = V_{DD}/2$, it can be derived the time required to fully unbalance V_B by imposing a $v_B(t_{gen}) = V_{DD}/2$:

$$t_{gen} = \frac{gds_2 C_{L3}}{gmb_{eq}(gm_{n3} + gm_{p3})} \ln\left(\frac{gmb_{eq}}{i_{off}}\frac{V_{DD}}{2}\right) \tag{49}$$

In order to quantify the value of gmb_{eq} we can consider that:

$$\begin{cases} 1 - \alpha_p \approx \dfrac{gds_{p1}}{gm_{p1}} = 1/Av_{p1} \\ 1 - \alpha_n \approx \dfrac{gds_{n1}}{gm_{n1}} = 1/Av_{n1} \end{cases} \tag{50}$$

and thus, if we assume that $Av_{p1} = Av_{n1} = A_v = gm_{n,p}/gds_{n,p}$ which is the intrinsic gain of the generic MOS device in the selected technology, we can further simplify Eq. 46 as:

$$gmb_{eq} = \frac{gmb_{p2} + gmb_{n2}}{A_v} \tag{51}$$

Finally, Eq. 49 can be written as:

$$t_{gen} = \frac{A_v}{gmb_{p2} + gmb_{n2}} \frac{gds_2 C_{L3}}{(gm_{n3} + gm_{p3})} \cdot \cdot \ln\left(\frac{gmb_{p2} + gmb_{n2}}{A_v \; i_{off}} \frac{V_{DD}}{2}\right) \tag{52}$$

From Eq. 52 the role and the aim of feedbacks introduced by body terminals are clear:

- they form a positive feedback which regenerates the output offset current given by mismatch variations at the node A, guaranteeing the right operation of the PUF;
- they allow to reduce the minimum supply voltage required for the proposed PUF to be able to work;
- they ensure that nodes A and B remain completely unbalanced, even in the presence of a slight current offset, thereby ensuring the absence of static power consumption;
- they reduce the time to generate the output bitstream, minimizing the Energy/bit.

TABLE I

TRANSISTORS' SIZING

	Mp_1	Mp_2	Mp_3	Mp_4
W [µm]	0.75	0.74	0.57	0.57
L [µm]	0.13	0.13	0.13	0.13

	Mn_1	Mn_2	Mn_3	Mn_4
W [µm]	0.15	0.15	0.15	0.15
L [µm]	0.47	0.47	1.35	1.35

IV. Body-PUF Implementation

The PUF-bit cell topology reported in Fig.4 has been designed in a commercial 130nm triple-well bulk CMOS process, and deep n-well NMOS devices have been used in the PUF bit cell to isolate the bulk terminals. The proposed design targets a supply voltage V_{DD} of 0.3V, and an ultra-low power consumption set through a bias current I_{ref} of only 10 nA. It has to be pointed out that, being this architecture designed for ULV and ULP applications, the possibility that the pn junction between the source and the bulk of MOS devices turns on is not a concern. However this possibility prevents the usage of this PUF topology with supply voltages higher than 0.6V. Dimensions of MOS devices are reported in Tab. I, and have been chosen to obtain a gate-source bias voltage and a drain-source bias voltage both equal to half the supply voltage $V_{DD}/2$.

In order to maximize the symmetry of the design, a floorplan based on 4 PUF-bit cells has been designed, and the full-custom, transistor level layout of a 4-bits macro has been implemented. The layout of the 4-bits macro is reported in Fig. 6b, where the layout of the single bit cell is contained within the blue rectangle, with an area footprint of 10.825 × 7.95 μm^2. Starting from the 4-bits macro we performed an automatic place and route flow as in [59], to obtain a 128-bits PUF. Fig. 6c shows the microphotograph of the prototype chip, in which the 128-bits PUF is contained in the green rectangle. A detail of the layout of the 128-bits PUF is visible in the upper right corner of the figure, and its area is 11,015 μm^2.

A conventional SPI interface which allows to set the configuration registers of the prototype chip and to receive the output bits of the PUF has been integrated for testing purposes.

V. Simulation and Measurement Results

A. Bias of the 128-Bits Keys

In the PUF context, the bias of the response is defined as the mean value of the number of logic '1's expressed as a percentage, and its ideal value is 50%. Transistor-level mismatch Monte-Carlo simulations exploiting the accurate statistical models provided by the IC manufacturer have been carried out in order to evaluate the bias of the proposed PUF, showing a bias ≈ 48.88 % for 1,000 Monte Carlo iterations.

All the 20 available packaged prototype chips have been tested to evaluate the statistical performances of the 128-bit key across several chip samples. The number of unstable bits and the bias of 20 keys are reported in Fig. 7 and Fig. 8 respectively, whereas a graphical representation of the 128-bits keys over the 20 chips is depicted in Fig. 9. It was found that, in average, the mean value μ of the bias response is about 49.42% with a standard deviation σ around 3.69%. While the maximum number of unstable cells found in typical conditions is 3.125% and it was found on just 1 chip out of the 20, the number of unstable cells in typical conditions extracted from considering all the 20 chip samples has been found to have a

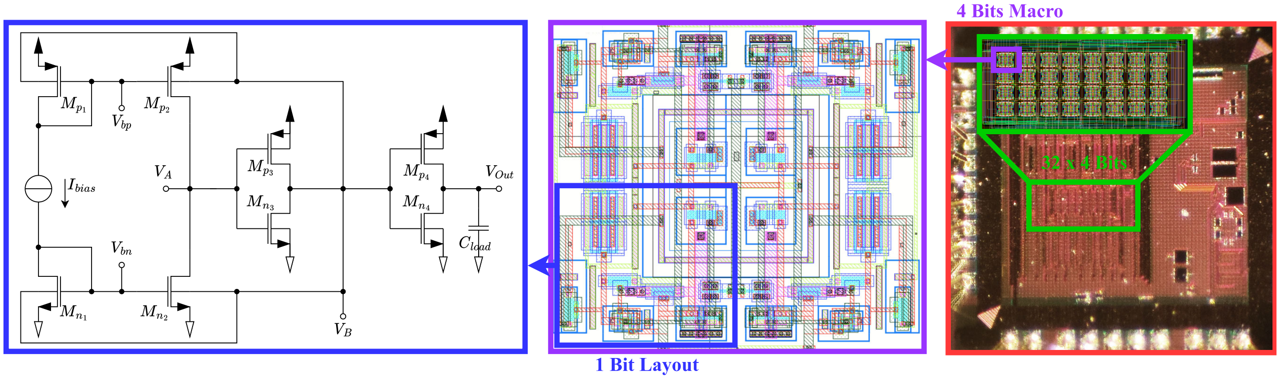


Fig. 6. Proposed PUF architecture a), the 4 bits PUF macro b) and the micro-photograph view of the Layout of a 32 × 4-bit PUF macro on a 130nm testchip: the overall area consumption is about 7836 μm^2 c).

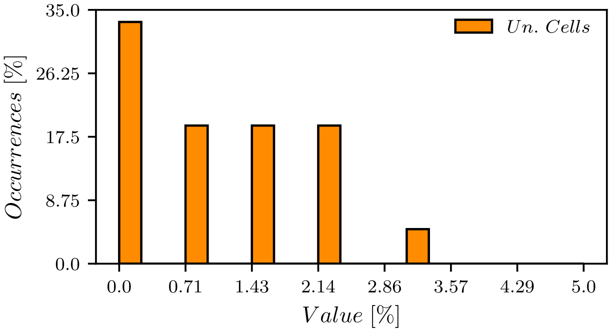


Fig. 7. Histogram of the number of unstable bits computed for the 128-bits on all the 20 chip samples.

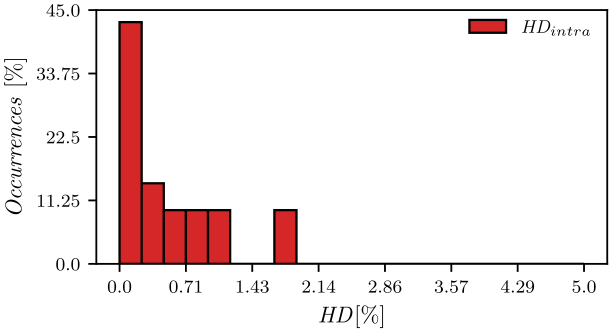


Fig. 10. Histogram of the Reliability measured as HD_{intra} on all the 20 chip samples.

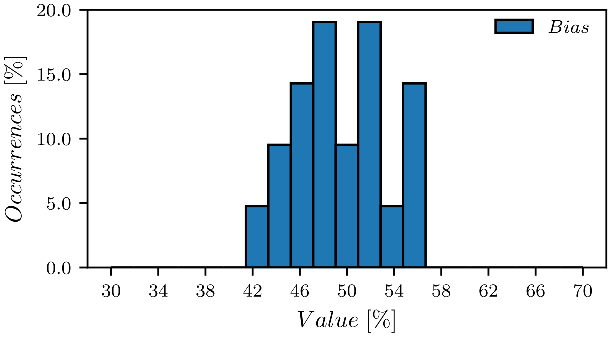


Fig. 8. Histogram of the bias for the 128-bits PUF keys on all the 20 chip samples.

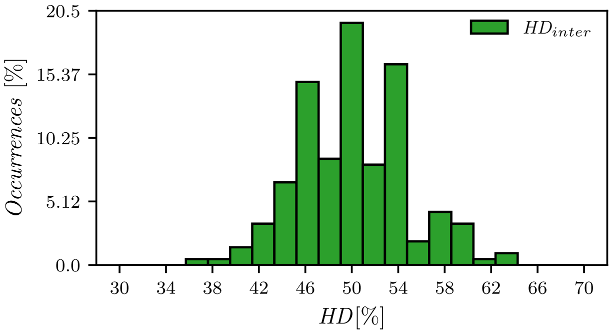


Fig. 11. Histogram of the Uniqueness measured as HD_{inter} on all the 20 chip samples.

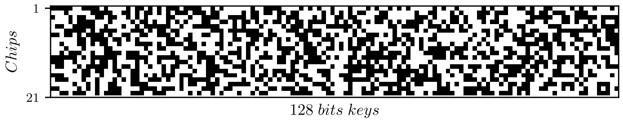


Fig. 9. Graphical representation of the 128-bits PUF keys on all the 20 chip samples.

mean value of about $\mu \approx 1.094\%$ and a standard deviation of about $\sigma \approx 1.001\%$.

B. Uniqueness and Reliability in Nominal Conditions

The intra Hamming Distance HD_{intra} and the inter Hamming Distance HD_{inter} evaluate how many bits of the response in percentage vary with respect to a nominal value over different chip realizations, and are used to quantify the Uniqueness and Reliability of PUFs [17]. Transistor-level Monte-Carlo simulations accounting for both process and mismatch variations have also been carried out. Results of the 1,000 Monte Carlo iterations have shown an inter Hamming Distance HD_{inter} of $\approx 50.12\%$, thus confirming the good Uniqueness achieved by the proposed PUF. Measurement results of HD_{intra} and HD_{inter} on all the 20 chip samples are reported in Fig. 10 and Fig. 11 respectively. The measured HD_{intra} exhibits a mean value $\mu \approx 0.517\%$ and a standard deviation $\sigma \approx 0.574\%$, whereas the HD_{inter} has a mean value $\mu \approx 50.177\%$ and a standard deviation $\sigma \approx 4.691\%$. Measured results on the proposed PUF provide Uniqueness and Reliability performances in good agreement with the simulated ones, and in line with the state of the art, despite the extremely low supply voltage.

The autocorrelation function (ACF) has been computed over all the measured PUF outputs as in [26], [49], and [55], and the results are reported in Fig. 12, showing a mean value of the ACF of $0.19 \cdot 10^{-3}$, with a boundary of 95% confidence level of 0.02548(−0.02587).

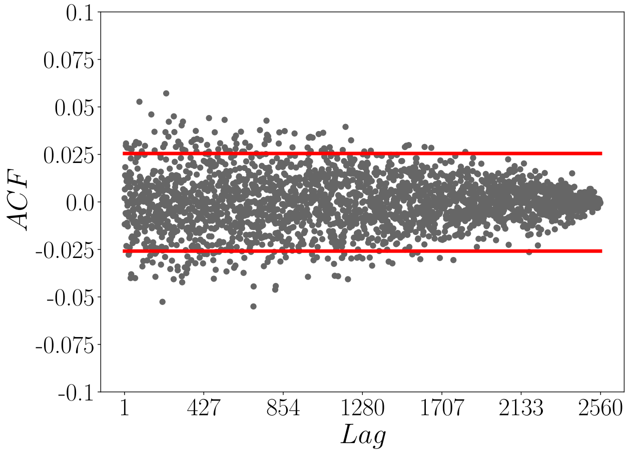


Fig. 12. ACF of all the measured outputs of the proposed PUF. The red lines are used to mark the boundary of the 95% confidence level.

C. Reliability Under Variations of Supply Voltage and Temperature

The capacity of PUFs to consistently replicate the same key under supply voltage and temperature fluctuations is a crucial attribute. The fraction of cells that can consistently reproduce a given value under different voltage and temperature conditions is known as reliability. The reliability of a PUF is defined as $(1-BER)$, where the HD_{intra} between a golden key extracted under nominal conditions and a key extracted under differing environmental conditions provides the BER, which is defined as the Bit Error Rate. Since reproducing the same key under various environmental conditions is one of PUFs primary criteria, reliability is a crucial parameter that needs to be examined and verified. Results of mismatch Monte Carlo simulations for different values of supply voltage and temperature have shown a good Reliability of the proposed PUF, resulting in a worst case intra Hamming Distance $(HD_{intra}) \approx 2.4\%$. The number of unstable cells, or cells that can't consistently replicate the same key, is another crucial PUF performance characteristic that needs to be examined under different environmental conditions. With respect to a nominal V_{DD} value of 0.3V, we have investigated the number of unstable cells and the BER in percentage over a ±10% range of supply voltage changes (from 270mV to 330mV). It should be noted that the key's reliance on voltage and temperature fluctuations is usually assessed on a single chip [26], [55]. Being the focus of these measurements the investigation of the average trend of the performances of the proposed PUF, the behavior of all the 20 available chips has been considered (20/20 of the chips have been tested) and the average trend for the selected samples has been extracted, as can be seen in Fig. 13. Based on 500 repeated measurements, it was found that the average BER under typical conditions is as low as 0.517 %. When we take into account a ±10% of voltage variation with respect to the nominal value, we can see that the worst case BER is only 3.125%, while the average worst case BER is only 1.15%. We examined a range of temperatures from 0 to 75 °C to test the response's reliability. We found that temperature changes have no effect on Body PUF, resulting in an average BER that is consistently less than 1.602%. In the worst case scenario, on three of the 20 chip samples, it results in roughly 3.125%, as can be seen in Fig. 14.

Over 500 extractions were conducted to determine the number of unstable bits, and the results are shown in Figs. 13 and 14 versus temperature and supply voltage fluctuations, respectively. It was found that, on average, there are never more unstable bits than 1.17% for variations in V_{DD} and 1.09% for variations in temperature. In the worst case conditions, 3.90% of unstable bits results from variations in the supply voltage and 3.66% from variations in temperature.

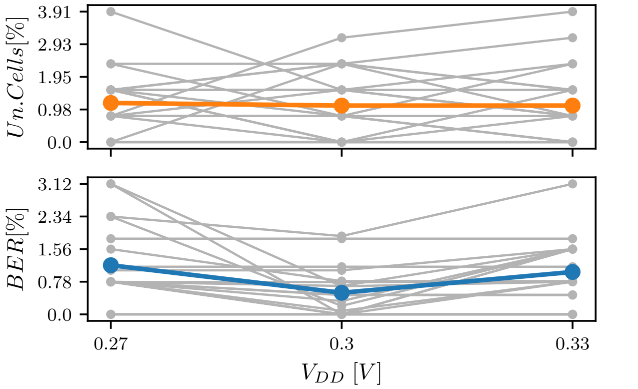


Fig. 13. Number of unstable bits and percentage BER under voltage variations across 20 chip samples, the average trend is highlighted in green and red colors respectively.

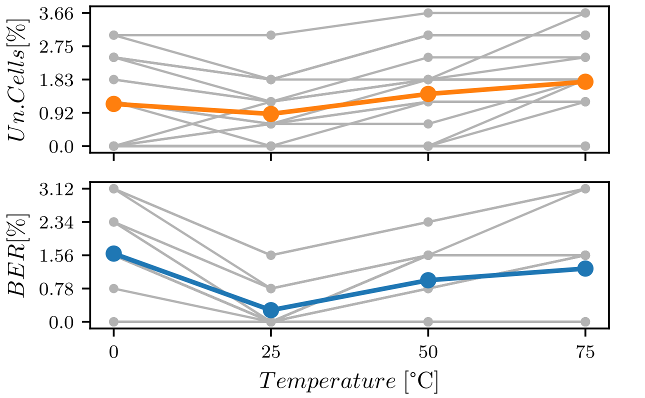


Fig. 14. Number of unstable bits and percentage BER under temperature variations over 5 chips, the average trend is highlighted in blue color.

TABLE II

RANDOMNESS ASSESSMENT THROUGH NIST TESTS

NIST Test	Stream length	p-value	Result
Frequency	2560	0.0438	✓
Frequency block	2560	0.1465	✓
Runs	2560	0.9379	✓
Longest Run	2560	0.3065	✓
DTFT	2560	0.9880	✓
Non Overlapping	2560	0.7025	✓
Serial	2560 (m=9)	0.9014	✓
Approximate Entropy	2560 (m=6)	0.8786	✓
Cumulative Sum	2560	0.0594	✓

D. Randomness Assessment

Since the sequences that are retrieved from PUFs have to meet stringent requirements for unpredictability, the bitstream quality must be assessed using an ad-hoc test suite. As in other studies, [26], [28], [55], and [59], we used NIST tests for this purpose. We took into consideration a cumulative key of 2560 bits, of which 128 bits were taken from each of the 20 measured chip samples. We then extracted the p-value for each test and reported it in Tab. II in order to assess the randomness. The test is successfully passed and the bitstream satisfies the test requirement if the p-value is higher than 0.01

TABLE III
COMPARISON TABLE

		This Work	[59]	[51]	[61]	[67]	[49]	[55]	[26]
Nominal Characterization	Technology [nm]	130	130	22	65	14	180	40	65
	Area/bit [μm^2] F[‡] @130nm	86.05	72.03	4.66	**12.91**	158.94	**13.22**	61.58	86.4
	Area/bit normalized	5092°	4262.13°	9628.10	**764**	9404.73	782.25	3643.79	5114.79
	Typ V_{DD} [V]	**0.3**	0.8	0.9	1.20	**0.65**	0.8	0.9	1
	V_{DD} range* [V]	[0.27,0.33]	[0.6-1.2]	[0.7-0.9]	[0.95,1.30]	[0.55-0.75]	[0.8-1.8]	[0.6-1.2]	[0.6-1]
	T Range [°C]	[0 , 75]	[0 , 75]	[25, 50]	[-40,120]	-	[-40 , 120]	[-40 , 125]	[25 , 85]
	Energy/bit (fj/bit)	**0.331**	5.36	13	124	4	11.3	1.02	15
	number of evaluation	500	500	5k	500	-	2000	500	400
	# Bits	128	128	256	1	128	1024	3000	256
	Entropy	0.9999029	0.99984	0.997	-	**0.99993**	-	0.9972	0.9967
	ACF @ 95% c.l.[△]	0.025	0.025	0.088	0.019	-	0.017	**0.007**	0.036
	$UB_{typ}[\%]$	1.132	**0.586**	5^{+}	1.50	-	1.70	3.48	1.88
	$\mu_{HD_{intra}}$ [%]	0.517	0.491	0.97 [τ]	16.97	3.4	**0.18**	0.49	0.861
	$\mu_{HD_{inter}}$ [%]	50.177	50.12	49.00	**49.94**	48.60	49.80	49.07	50.14
PVT	$B\hat{E}R_V[\%]$	5.88	**3.12**	-	5.62	9.75	3.36	4.34	-
	$B\hat{E}R_T[\%]$	**0.534**	0.35	-	0.46	0.95	0.62	0.94	-
	$U\hat{B}_V[\%]$	7.5	**2.08**	-	-	-	3.48	9.00	8.83
	$U\hat{B}_T[\%]$	0.755	**1.25**	-	-	-	4.20	15.75	10.75
FOM	$FOM_{UB}[\%]$	0.131	**0.40**	-	-	-	0.175	0.054	0.0712
	$FOM_{BER}[\%]$	0.169	**0.314**	-	0.056	0.096	0.292	0.224	-
	$FOM_{HD}[\%]$	1.830	1.978	0.718	0.059	0.272	**3.716**	0.951	1.146
	$FOM_{HDE}[\%/(fJ/bit)]$	**5.529**	0.369	0.055	0.5m	0.068	2.173	0.933	0.076
	$F\hat{O}M_{HDE}[\%/(fJ/bit)] \cdot 10^{-3}$	**1.086**	0.087	0.006	0.62m	0.007	0.421	0.256	0.015
	$FOM_{TOT}[(fj/bit)] \cdot 10^{-9}$	**0.0240**	0.0109	-	-	-	0.0215	0.0031	-

[*] Supply Voltage Range; [‡] Area of the PUF cell with considering the minimum feature size of a 130nm technology; [△]Confidence Level; [τ] After TMV + Burn-in + Dark bits soft mask;

(i.e., a 99% confidence level has been evaluated). The p-value measures the bitstream performance with regard to a certain test (such as the cumulative sum test). The p-value results for each test are shown in Tab. II, indicating that the bistream obtained for the proposed PUF passed the statistical tests.

VI. PUFs Metrics and FoMs Definition

We used the following FOM_{HD} to compare various PUFs implementations in terms of the tradeoff between HD_{intra} and HD_{inter}:

$$FOM_{HD} = \frac{1}{\sqrt{HD_{intra}^2 + \left(0.5 - HD_{inter}\right)^2}} \tag{53}$$

As per the definition given above, a better trade-off between HD_{inter} and HD_{intra} is attained when FOM_{HD} is bigger. It is crucial to consider the trade-off between energy consumption per bit, uniqueness, and reliability because PUF performance can be maximized by making the circuit more complex. In order to assess this trade-off, we present the subsequent FOM:

$$FOM_{HDE} = \frac{FOM_{HD}}{Energy/bit} \tag{54}$$

Lastly, we assess the area-normalized $FO\hat{M}_{HDE}$ defined as follows, because many solutions must cope with severe criteria in terms of silicon Area on ASIC [26], [49], [56] or resources usage on FPGA [17], [28], [65], [66]:

$$FO\hat{M}_{HDE} = \frac{FOM_{HDE}}{Area_{bit}} \cdot Area_{min} \tag{55}$$

in which $Area_{bit}$ is the Area/bit of the PUF bit cell and $Area_{min}$ denotes the minimum Area size allowed by the technology[1] (e.g. for a 130nm technology, the $Area_{min} \approx 0.0169\mu m^2$).

Furthermore, to evaluate the robustness of the bit-stream to supply voltage (V_{DD}) and temperature (T) variations two BER normalization metrics are used as follows:

$$B\hat{E}R_V = \frac{BER_{wcV}}{\frac{VDD_{max} - VDD_{min}}{VDD_{typ}}} \quad B\hat{E}R_T = \frac{BER_{wcT}}{\frac{T_{max} - T_{min}}{T_{typ}}} \tag{56}$$

in which $BER_{wcV(T)}$ is the worst case BER related to supply voltage (temperature) variations and $VDD_{max} - VDD_{min}$ ($T_{max} - T_{min}$) is the V_{DD} (T) range with respect to the typical value VDD_{typ} (T_{typ}) considered for the computation of the PUF BER.

In a similar way the normalized FoM for the unstable bits (UB), $U\hat{B}_{V,T}$, can be defined as:

$$U\hat{B}_V = \frac{UB_{wcV}}{\frac{VDD_{max} - VDD_{min}}{VDD_{typ}}} \quad U\hat{B}_T = \frac{UB_{wcT}}{\frac{T_{max} - T_{min}}{T_{typ}}} \tag{57}$$

[1] It is the minimum transistor size allowed from a given technology without considering interconnections.

in which $UB_{wcV(T)}$ is the worst case UB related to supply voltage (temperature) variations and $V_{DD_{max}} - V_{DD_{min}}$ ($T_{max} - T_{min}$) is the V_{DD} (T) range with respect to the typical value $V_{DD_{typ}}$ (T_{typ}) considered for the evaluation of UB.

To quantify the robustness of a PUF to both supply voltage and temperature variations two further FOMs defined as follows have been introduced:

$$FOM_{BER} = \frac{1}{\sqrt{BER_{typ}^2 + \widehat{BER}_V{}^2 + \widehat{BER}_T{}^2}} \tag{58}$$

$$FOM_{UB} = \frac{1}{\sqrt{UB_{typ}^2 + \widehat{UB}_V{}^2 + \widehat{UB}_T{}^2}} \tag{59}$$

The above FoMs allow to quantify BER and UB performance in different operating conditions, while considering also the typical values.

Finally, to quantify the overall performance tradeoff of a PUF, a comprehensive FOM defined as folllows can be exploited:

$$FOM_{TOT} = FOM_{UB} \cdot FOM_{BER} \cdot \widehat{FOM}_{HDE} \tag{60}$$

Clearly, the higher is FOM_{TOT}, the better is the trade-off achieved by a PUF.

VII. Comparison With the State-of-the-Art Literature

A comparison against state-of-the-art literature is depicted in Table III. As it can be observed, there are several parameters which have been taken into account in order to evaluate in the fairest way the trade-offs which characterize PUF design. The comparison table has been divided in three sections, a nominal characterization, a PVT characterization to evaluate the resilience of the PUF and finally the FOM section, in which trade-offs have been evaluated and compared. As it can be observed, the PUF presented in this work is able to operate with the minimum supply voltage ever reported in the literature. As a consequence, it results also in the minimum Energy/bit when compared with other works, which, in the best case, uses three times the Energy/bit. The number of unstable cells in typical condition is comparable to the state-of-the-art literature and is second only to [59]. Given the design choice and the bit-cell architecture, the proposed PUF is also able to reach an high entropy, which results comparable to the one of [67]. For what concerns the characterization under voltage and temperature variations it is clear that [59] has the best resiliency. This is confirmed also by the FOM_{UB} and FOM_{BER} of [59]. However, with respect to the FOM_{HDE} and $\widehat{FOM}_{HDE}$ the proposed PUF reaches the best trade-off, due to the very low energy consumption and good statistical performance. Finally, considering the FOM_{TOT}, which takes into account all the performance of the PUF, it can be observed how the proposed PUF achieves the best trade-off in the literature. It has to be remarked that this is an outstanding result, also if considering that no post-processing techniques have been used during the PUF characterization.

VIII. Conclusion

In summary, this study has introduced an innovative method for creating a mismatched current mirror with a fully unbalanced output, substantially reducing the minimum supply voltage requirements compared to previous RCCM PUFs. The integration of body-driven feedback mechanisms has enabled the circuit to operate effectively with supply voltages as low as 0.3V. Additionally, the incorporation of a reference bias current has ensured a consistent power consumption profile, even in the face of mismatch and process variations.

The outcome is a PUF that exhibits outstanding energy efficiency, with an impressively low energy consumption of 0.3 fJ/bit, while maintaining robust statistical performance. This yields a response bias of 49.42%, a reliability of 99.483%, and a uniqueness of 50.176%, all achieved without the need for post-processing techniques such as TMV or burn-in, or the introduction of soft dark bits.

The efficacy of this novel approach has been rigorously validated through a combination of simulations and measurements conducted on a 130nm CMOS test-chip. These assessments encompassed challenging conditions, including nominal power supply voltages of 0.3V, voltage variations within the range of ±10%, and temperatures spanning from 0°C to 75°C.

The comprehensive experimental verification, along with an in-depth elucidation of the techniques employed, and the meticulous measurements carried out on 20 available chip samples, affirm the resilience and applicability of the Body-PUF approach.

Furthermore, comparative analyses against state-of-the-art literature have underscored the potential of this PUF, surpassing previous works in terms of figures of merit such as FOM_{HDE}, $\widehat{FOM}_{HDE}$, and FOM_{TOT}. This positions the Body-PUF as an ideal choice for real authentication scenarios, offering an exceptional trade-off between performance and practicality.

References

[1] Y. Vishwanath, R. S. Upendra, and M. R. Ahmed, "A review on advent of IoT, cloud, and machine learning in agriculture," in *Proc. Int. Conf. Mobile Comput. Sustain. Informat.* Cham, Switzerland: Springer, Dec. 2020, pp. 595–603.

[2] A. Kalla, P. Prombage, and M. Liyanage, "Introduction to IoT," in *IoT Security*. Chichester, U.K.: Wiley, Feb. 2020, pp. 1–25.

[3] N. Sharma, M. Shamkuwar, and I. Singh, "The history, present and future with IoT," in *Internet of Things and Big Data Analytics for Smart Generation*. Cham, Switzerland: Springer, Dec. 2018, pp. 27–51.

[4] S. Sidhu, B. J. Mohd, and T. Hayajneh, "Hardware security in IoT devices with emphasis on hardware Trojans," *J. Sensor Actuator Netw.*, vol. 8, no. 3, p. 42, Aug. 2019.

[5] J. Dofe, J. Frey, and Q. Yu, "Hardware security assurance in emerging IoT applications," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2016, pp. 2050–2053.

[6] I. Tudosa, F. Picariello, E. Balestrieri, L. De Vito, and F. Lamonaca, "Hardware security in IoT era: The role of measurements and instrumentation," in *Proc. II Workshop Metrology Ind. 4.0 IoT*, Jun. 2019, pp. 285–290.

[7] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2014, pp. 417–423.

[8] F.-X. Standaert, "Introduction to side-channel attacks," in *Secure Integrated Circuits and Systems*. Boston, MA, USA: Springer, Dec. 2009, pp. 27–42.

[9] R. Spreitzer, V. Moonsamy, T. Korak, and S. Mangard, "Systematic classification of side-channel attacks: A case study for mobile devices," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 465–488, 1st Quart., 2017.

[10] M. Randolph and W. Diehl, "Power side-channel attack analysis: A review of 20 years of study for the layman," *Cryptography*, vol. 4, no. 2, p. 15, May 2020.

[11] P. Gope and B. Sikdar, "A comparative study of design paradigms for PUF-based security protocols for IoT devices: Current progress, challenges, and future expectation," *Computer*, vol. 54, no. 11, pp. 36–46, Nov. 2021.

[12] J. Obermaier and V. Immler, "The past, present, and future of physical security enclosures: From battery-backed monitoring to PUF-based inherent security and beyond," *J. Hardw. Syst. Secur.*, vol. 2, no. 4, pp. 289–296, Dec. 2018.

[13] M. Barbareschi, A. De Benedictis, E. La Montagna, A. Mazzeo, and N. Mazzocca, "A PUF-based mutual authentication scheme for cloud-edges IoT systems," *Future Gener. Comput. Syst.*, vol. 101, pp. 246–261, Dec. 2019.

[14] H. Kang, Y. Hori, T. Katashita, M. Hagiwara, and K. Iwamura, "Cryptographie key generation from PUF data using efficient fuzzy extractors," in *Proc. 16th Int. Conf. Adv. Commun. Technol.*, Feb. 2014, pp. 23–26.

[15] L. Kusters and F. M. J. Willems, "Secret-key capacity regions for multiple enrollments with an SRAM-PUF," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 9, pp. 2276–2287, Sep. 2019.

[16] W. Yu and J. Chen, "Masked AES PUF: A new PUF against hybrid SCA/MLAs," *Electron. Lett.*, vol. 54, no. 10, pp. 618–620, May 2018.

[17] R. D. Sala, D. Bellizia, and G. Scotti, "A lightweight FPGA compatible weak-PUF primitive based on XOR gates," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 6, pp. 2972–2976, Jun. 2022.

[18] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Secur.*, New York, NY, USA, Nov. 2002, pp. 148–160.

[19] A. Maiti and P. Schaumont, "Improved ring oscillator PUF: An FPGA-friendly secure primitive," *J. Cryptol.*, vol. 24, no. 2, pp. 375–397, 2011.

[20] M. Gao, K. Lai, and G. Qu, "A highly flexible ring oscillator PUF," in *Proc. 51st ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, New York, NY, USA, May 2014, pp. 1–6.

[21] M. T. Rahman, D. Forte, J. Fahrny, and M. Tehranipoor, "ARO-PUF: An aging-resistant ring oscillator PUF design," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2014, pp. 1–6.

[22] S. R. Sahoo, S. Kumar, and K. Mahapatra, "A modified configurable RO PUF with improved security metrics," in *Proc. IEEE Int. Symp. Nanoelectron. Inf. Syst.*, Dec. 2015, pp. 320–324.

[23] 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. Comput.-Aided Design Integr. Circuits Syst.*, vol. 34, no. 7, pp. 1143–1147, Jul. 2015.

[24] W. Liu, Y. Yu, C. Wang, Y. Cui, and M. O'Neill, "RO PUF design in FPGAs with new comparison strategies," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2015, pp. 77–80.

[25] X. Xin, J.-P. Kaps, and K. Gaj, "A configurable ring-oscillator-based PUF for Xilinx FPGAs," in *Proc. 14th Euromicro Conf. Digit. Syst. Design*, Aug. 2011, pp. 651–657.

[26] A. B. Alvarez, W. Zhao, and M. Alioto, "Static physically unclonable functions for secure chip identification with 1.9–5.8% native bit instability at 0.6–1 V and 15 fJ/bit in 65 nm," *IEEE J. Solid-State Circuits*, vol. 51, no. 3, pp. 763–775, Mar. 2016.

[27] A. Garg and T. T. Kim, "Design of SRAM PUF with improved uniformity and reliability utilizing device aging effect," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Jun. 2014, pp. 1941–1944.

[28] R. D. Sala, D. Bellizia, and G. Scotti, "A novel ultra-compact FPGA PUF: The DD-PUF," *Cryptography*, vol. 5, no. 3, p. 23, Sep. 2021.

[29] R. D. Sala and G. Scotti, "The DD-cell: A double side entropic source exploitable as PUF and TRNG," in *Proc. 17th Conf. Ph.D Res. Microelectron. Electron. (PRIME)*, Jun. 2022, pp. 353–356.

[30] M. Bhargava and K. Mai, "A high reliability PUF using hot carrier injection based response reinforcement," in *Cryptographic Hardware and Embedded Systems—CHES 2013*. Berlin, Germany: Springer, 2013, pp. 90–106.

[31] X. Xu et al., "A highly reliable butterfly PUF in SRAM-based FPGAs," *IEICE Electron. Exp.*, vol. 14, no. 14, 2017, Art. no. 20170551.

[32] C. Q. Liu, Y. Cao, and C. H. Chang, "ACRO-PUF: A low-power, reliable and aging-resilient current starved inverter-based ring oscillator physical unclonable function," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 64, no. 12, pp. 3138–3149, Dec. 2017.

[33] T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama, "A new mode of operation for arbiter PUF to improve uniqueness on FPGA," in *Proc. Federated Conf. Comput. Sci. Inf. Syst.*, Sep. 2014, pp. 871–878.

[34] J. W. Lee et al., "A technique to build a secret key in integrated circuits for identification and authentication applications," in *Proc. IEEE Symp. VLSI Circuits*, Jun. 2004, pp. 176–179.

[35] S. Hemavathy and V. S. K. Bhaaskaran, "Arbiter PUF—A review of design, composition, and security aspects," *IEEE Access*, vol. 11, pp. 33979–34004, 2023.

[36] D. P. Sahoo, D. Mukhopadhyay, R. S. Chakraborty, and P. H. Nguyen, "A multiplexer-based arbiter PUF composition with enhanced reliability and security," *IEEE Trans. Comput.*, vol. 67, no. 3, pp. 403–417, Mar. 2018.

[37] T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama, "A new arbiter PUF for enhancing unpredictability on FPGA," *Sci. World J.*, vol. 2015, pp. 1–13, Sep. 2015.

[38] Z. He, W. Chen, L. Zhang, G. Chi, Q. Gao, and L. Harn, "A highly reliable arbiter PUF with improved uniqueness in FPGA implementation using bit-self-test," *IEEE Access*, vol. 8, pp. 181751–181762, 2020.

[39] J. Wen, M. Huang, Z. Chen, L. Zhu, S. Chen, and B. Li, "A multi-line arbiter PUF with improved reliability and uniqueness," in *Proc. IEEE 4th Int. Conf. Signal Image Process. (ICSIP)*, Jul. 2019, pp. 641–648.

[40] K. Fruhashi, M. Shiozaki, A. Fukushima, T. Murayama, and T. Fujino, "The arbiter-PUF with high uniqueness utilizing novel arbiter circuit with delay-time measurement," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2011, pp. 2325–2328.

[41] Z. Paral and S. Devadas, "Reliable and efficient PUF-based key generation using pattern matching," in *Proc. IEEE Int. Symp. Hardware-Oriented Secur. Trust*, Jun. 2011, pp. 128–133.

[42] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, "14.2 a physically unclonable function with BER $<10^{-8}$ for robust chip authentication using oscillator collapse in 40 nm CMOS," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2015, pp. 1–3.

[43] R. Serrano, C. Duran, M. Sarmiento, T.-K. Dang, T.-T. Hoang, and C.-K. Pham, "A unified PUF and crypto core exploiting the metastability in latches," *Future Internet*, vol. 14, no. 10, p. 298, Oct. 2022.

[44] L. Bossuet, X. T. Ngo, Z. Cherif, and V. Fischer, "A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon," *IEEE Trans. Emerg. Topics Comput.*, vol. 2, no. 1, pp. 30–36, Mar. 2014.

[45] B. Habib, J.-P. Kaps, and K. Gaj, "Efficient SR-latch PUF," in *Applied Reconfigurable Computing* Cham, Switzerland: Springer, Mar. 2015, pp. 205–216.

[46] D. Yamamoto et al., "Uniqueness enhancement of PUF responses based on the locations of random outputting RS latches," in *Cryptographic Hardware and Embedded Systems—CHES 2011*. Berlin, Germany: Springer, 2011, pp. 390–406.

[47] R. D. Sala and G. Scotti, "Exploiting the DD-cell as an ultra-compact entropy source for an FPGA-based re-configurable PUF-TRNG architecture," *IEEE Access*, vol. 11, pp. 86178–86195, 2023.

[48] R. Della Sala and G. Scotti, "A novel FPGA implementation of the NAND-PUF with minimal resource usage and high reliability," *Cryptography*, vol. 7, no. 2, p. 18, Apr. 2023.

[49] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, "8.3 a 553F^2 2-transistor amplifier-based physically unclonable function (PUF) with 1.67% native instability," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2017, pp. 146–147.

[50] M.-Y. Wu et al., "A PUF scheme using competing oxide rupture with bit error rate approaching zero," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2018, pp. 130–132.

[51] S. K. Mathew et al., "16.2 a 0.19 pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22 nm CMOS," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2014, pp. 278–279.

[52] Y. Shifman, A. Miller, O. Keren, Y. Weizmann, and J. Shor, "A method to improve reliability in a 65-nm SRAM PUF array," *IEEE Solid-State Circuits Lett.*, vol. 1, no. 6, pp. 138–141, Jun. 2018.

[53] Y. Cao, C. Q. Liu, and C. H. Chang, "A low power diode-clamped inverter-based strong physical unclonable function for robust and lightweight authentication," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 11, pp. 3864–3873, Nov. 2018.

[54] D. Li and K. Yang, "A self-regulated and reconfigurable CMOS physically unclonable function featuring zero-overhead stabilization," *IEEE J. Solid-State Circuits*, vol. 55, no. 1, pp. 98–107, Jan. 2020.

[55] S. Taneja, A. B. Alvarez, and M. Alioto, "Fully synthesizable PUF featuring hysteresis and temperature compensation for 3.2% native BER and 1.02 fJ/b in 40 nm," *IEEE J. Solid-State Circuits*, vol. 53, no. 10, pp. 2828–2839, Oct. 2018.

[56] Q. Zhao, Y. Wu, X. Zhao, Y. Cao, and C.-H. Chang, "A 1036-F^2/bit high reliability temperature compensated cross-coupled comparator-based PUF," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 6, pp. 1449–1460, Jun. 2020.

[57] M. Asghari, M. Guzman, and N. Maghari, "Cross-coupled impedance-based physically unclonable function (PUF) with 1.06% native instability," *IEEE Solid-State Circuits Lett.*, vol. 3, pp. 282–285, 2020.

[58] M. Vatalaro, R. De Rose, M. Lanuzza, and F. Crupi, "Static CMOS physically unclonable function based on 4T voltage divider with 0.6%–1.5% bit instability at 0.4–1.8 V operation in 180 nm," *IEEE J. Solid-State Circuits*, vol. 57, no. 8, pp. 2509–2520, Aug. 2022.

[59] R. Della Sala, D. Bellizia, F. Centurelli, and G. Scotti, "A monostable physically unclonable function based on improved RCCMs with 0–1.56% native bit instability at 0.6–1.2 V and 0–75 °C," *Electronics*, vol. 12, no. 3, p. 755, Feb. 2023.

[60] R. Della Sala, D. Bellizia, F. Centurelli, G. Scotti, and A. Trifiletti, "An ultra low voltage physical unclonable function exploiting body-driven," in *Proc. SIE*, C. Ciofi and E. Limiti, Eds. Cham, Switzerland: Springer, 2024, pp. 36–42.

[61] X. Zhao et al., "A 124 fJ/bit cascode current mirror array based PUF with 1.50% native unstable bit ratio," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 66, no. 9, pp. 3494–3503, Sep. 2019.

[62] R. D. Sala, F. Centurelli, P. Monsurrò, G. Scotti, and A. Trifiletti, "A 0.3 V rail-to-rail three-stage OTA with high DC gain and improved robustness to PVT variations," *IEEE Access*, vol. 11, pp. 19635–19644, 2023.

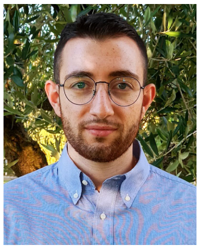
[63] F. Centurelli, R. Della Sala, P. Monsurrò, G. Scotti, and A. Trifiletti, "A novel OTA architecture exploiting current gain stages to boost bandwidth and slew-rate," *Electronics*, vol. 10, no. 14, p. 1638, Jul. 2021.

[64] H. Benaroya, S. Mi Han, S. M. Han, and M. Nagurka, *Probability Models in Engineering and Science*. Boca Raton, FL, USA: CRC Press, Oct. 2023.

[65] R. Della Sala, D. Bellizia, and G. Scotti, "A novel ultra-compact FPGA-compatible TRNG architecture exploiting latched ring oscillators," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 3, pp. 1672–1676, Mar. 2022.

[66] R. Della Sala, D. Bellizia, and G. Scotti, "High-throughput FPGA-compatible TRNG architecture exploiting multistimuli metastable cells," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 12, pp. 4886–4897, Dec. 2022.

[67] S. Satpathy et al., "A 4-fJ/b delay-hardened physically unclonable function circuit with selective bit destabilization in 14-nm trigate CMOS," *IEEE J. Solid-State Circuits*, vol. 52, no. 4, pp. 940–949, Apr. 2017.



Riccardo Della Sala was born in Naples in 1996. He received the bachelor's and M.S. degrees (summa cum laude) in electronics engineering and the Ph.D. degree from the University of Rome "La Sapienza," Italy, in 2018 and 2020, respectively. In November 2023, he holds the position of a Research Fellow with the Sapienza University of Rome. His primary research interests include designing and developing PUFs and TRNGs for hardware security both on ASIC and FPGA. Additionally, he focuses on ultra-low voltage, ultra-low power topologies for IoT, and biomedical applications within the context of analog design. This involves standard-cell-based architectures for fully synthesizable designs, including OTAs, comparators, filters, and ADCs. He has coauthored more than 30 publications in international journals and conference proceedings.

Davide Bellizia was born in June 1989. He received the M.S. (summa cum laude) and Ph.D. degrees in electronics engineering from the University La Sapienza of Rome, Italy, in 2014 and 2018, respectively. In 2017, he joined the Crypto Group, Université Catholique de Louvain (UCLouvain), Ottignies-Louvain-la-Neuve, Belgium, as a Post-Doctoral Researcher, working on several topics in hardware security, such as side-channel analysis and countermeasures, PUFs and TRNGs. In 2021, he joined the Crypto Engineering Department, Telsy S.p.A. In 2014, he received the Laureato Eccellente Award for the best graduate student of the year.

Francesco Centurelli (Senior Member, IEEE) was born in Rome in 1971. He received the Laurea (cum laude) and Ph.D. degrees in electronic engineering from Sapienza Universitã di Roma, Rome, Italy, in 1995 and 2000, respectively. In 2006, he became an Assistant Professor with the DIET Department, Sapienza Universitã di Roma. He has published more than 140 papers on international journals and refereed conferences. He has been also involved in research and development activities held in collaboration between Sapienza Universitã di Roma and some industrial partners. His research interests include system-level analysis and the design of clock recovery circuits and high-speed analog integrated circuits, now concern the design of analog-to-digital converters, and very low-voltage circuits for analog and RF applications.

Giuseppe Scotti (Senior Member, IEEE) received the M.S. and Ph.D. degrees in electronic engineering from the University of Rome "La Sapienza," Italy, in 1999 and 2003, respectively. In 2010, he became a Researcher (Assistant Professor) with the DIET Department, University of Rome "La Sapienza." In 2015, he was appointed an Associate Professor with the DIET Department. His research activity was mainly concerned with integrated circuits design and focused on design methodologies able to guarantee robustness with respect to parameter variations in both analog circuits and digital VLSI circuits. In the context of cryptographic hardware his focus has been on novel PAAs methodologies and countermeasures. He has coauthored more than 60 publications in international journals, about 70 contributions in conference proceedings, and is the co-inventor of two international patents.

Alessandro Trifiletti was born in Rome, Italy, in 1959. In 1991, he joined the Electronic Engineering Department, University of Rome "La Sapienza," as a Research Assistant, where he was involved in research activities dealing with analogue, RF, and microwave IC's design. In 2001, he joined the Faculty of Engineering, University of Rome "La Sapienza," as an Assistant Professor and became an Associate Professor in 2005 and a Full Professor in 2019. He has worked in the field of microelectronics, both from the point of view of design methodologies and circuit topologies. On these subjects, he has coauthored more than 210 publications, of which about 80 published on international journals, and the others published on the proceedings of major international conferences (a large part of these sponsored by the IEEE). In last 20 years, he has been engaged in the coordination of research teams from DIET (previously DIE) in the framework of national and international programs, involving both industrial and academic partners. From an industrial perspective, his expertise covers topics about analogue and RF microelectronics, radar and ESM systems, high-speed communication systems, security issues in cryptographic algorithms implementation, and embedded systems design.

Open Access funding provided by 'Università degli Studi di Roma "La Sapienza" 2' within the CRUI CARE Agreement