Analytic and Simulation Results of a Gaussian Physically Unclonable Constant Based on Resistance Dispersion*

Riccardo Bernardini
http://orcid.org/0000-0001-5890-8263
DPIA — Università di Udine, 33100, Italy
riccardo.bernardini@uniud.it

April 3, 2025

Abstract

Physically Unclonable Constants (PUCs) are a special type of Physically Unclonable Constants and they can be used to embed secret bit-strings in chips. Most PUCs are an array of *cells* where each cell is a digital circuit that evolve spontaneously toward one of two states, the chosen state being function of random manufacturing process variations. In this paper we propose an Analog Physically Unclonable Constant (APUC) whose output is an analog value to be transformed in digital by a digitizer circuit. The ratio behind this proposal is that an APUC cell has the potential of providing more than one bit, reducing the required footprint. Preliminary theoretical analysis and simulation results are presented. The proposed APUC has interesting performances (e.g., it can provide up to 5 bits per cell) that grant for further investigation.

1 Introduction

A Physically Unclonable Function (PUF) [1–25] is a circuit that implements an *ill conditioned function* that maps bit-words to bit-words. The function is "ill conditioned" in the sense that the actual behavior of the circuit is very sensitive to process parameters such as the exact threshold voltage of a MOSFET [6, 17] or the reverse saturation current of a diode [18]. This makes the map implemented by a specific chip unique to that chip, a kind of *chip fingerprint*, very difficult to replicate (hence *unclonable*) and useful to authenticate the chip [2–7, 26, 27].

*Funded by EU – NextGenerationEU – PNRR M4.C2.1.1 – PRIN 2022 Codice 2022A49KR3 – CUP G53D23000360006

PUFs are divided in *strong PUF* and *weak PUF*. A PUF is strong if the cardinality of its domain grows exponentially with the PUF size [28]. Strong PUFs are very common and usually they are employed with a Challenge Response Pairs (CRP) protocol [28, 29]. A CRP protocol requires, after manufacturing, to query the PUF with many inputs (*challenges*) and storing the PUF outcomes (*responses*) for later use. Successively, to verify the chip identity, a challenge registered in the database is proposed and if the response is not too different from the recorded one, the chip identity is accepted. [28, 29]

A critical issue with the CRP protocol is that the CRP database is a single point of failure: if an opponent gets access to it, the whole protocol breaks down since the opponent can emulate all the enlisted chips. Care also must be exercised in not reusing the same query twice. Finally, PUF design is a relatively young field and many PUF schemes have not been subjected to extensive cryptanalitic scrutiny, leaving open the possibility that new attack techniques could be developed in the future. For example, machine learning is a powerful technique that can be employed against many strong PUF schemes [10, 11, 13, 30].

A possible solution to those issues is to employ the weakest type of PUFs, that is, a PUF with no input arguments whose image contains only a single value. In other words, every time the PUF is queried it always returns the same value. For this special type of PUF the names *weak PUF*, *Physically Obfuscated Key (POK)*, or *Physically Unclonable Constant (PUC)* have been proposed [17, 18, 31, 32]; we will use the latter. The ideal PUC is a *random constant* [33, 34] in the sense that at production time its value it is randomly selected (possibly uniformly among the set of possible outcomes) and returned every time the PUC is queried.

Of course, the outcome of a PUC must remain secret and cannot be used as response in a CRP protocol; nevertheless, it can provide a secret key for many cryptographic protocols, for example, encryption or authentication using asymmetric protocols [35–37] or as source of randomness in special applications [38]. If the specific application requires the CRP protocol, a PUC can used to *build a strong PUF* by using it, for example, as key in a *keyed hash* [29, 37] or as initial value in a *sponge function* [39–41]. Constructing strong PUF in this way has the advantage that the "behavior" part (e.g., the hash function) can be obtained using a well-known and well-studied, from a cryptanalitic point of view, cryptographic algorithm.

1.1 Analog PUCs

Most PUCs can be said to be inherently digital in the sense that they are digital circuits that evolve spontaneously toward one of two states [5–7, 17, 18]. In this case we will sometimes use the term Digital Physically Unclonable Constant (DPUC) to emphasize the digital nature of the PUC.

In this paper we explore a less common approach based on Analog Physically Unclonable Constants (APUCs). Similarly to a DPUC, an APUC is a circuit very sensitive to parameter variations during the

manufacturing process; the main difference is that the outcome is an analog value that is successively transformed to digital by a *digitizer* to get a digital outcome [62].

Remark 1.1

We use *digitizer* and not *quantizer* because, in principle, it can be something different by an ADC-like quantization.

The rationale behind this approach is that the analog output has the potential of producing more than one bit per cell; for example, [42] uses an APUC-based approach to get two bits per cell. Moreover, APUCs are especially suited for the *dark bit* approach which improves the reliability without requiring the complexity of error correction codes [17, 31, 43–49].

1.2 Prior works about PUCs

Digital PUCs An overwhelming fraction of the PUC schemes in the literature are DPUC and most of them belong to one of three classes.

The first class includes *Memory-based PUCs*, that is, PUCs that use "memory cells" such as latches [50,51], SRAM [9,20,52–54], DRAM [19,55] or flash memories [56]. The main advantage of these PUCs is that they are based on well-known structures that sometimes can be already present in the chip, making this a very low-cost solution. Maybe the most important drawback is that the circuit employed has two stable states by design (it is a memory) and it can happen that the PUC ends in the "wrong" state, with a probability of getting an "unstable" cell with SRAM or latches of $\approx 4\%$ [7,51] or up to 10% for a DRAM based PUC [55].

The second class includes *comparator based* PUCs which feed random voltages to comparators [23, 57]. This class can be considered as a basic version of APUC, the problem is that, depending on the statistics of the random voltage, the probability of unstable can still be relatively large [57].

The third class includes *analog comparison* PUCs and it is the smallest DPUC class. PUCs in this class compare two analog values (e.g., the saturation current of two MOSFETs in [17], the ratio of two capacitors [24] or the reverse saturation current of two Schottky diodes in [18]) using some kind of positive feedback. The advantage of this type of schemes is that every instance has only one stable state, reducing significantly the fraction of unstable cells (for example, the intra distance of the scheme in [17] is 10 to 100 times smaller than the intra distance of memory-based schemes). Another scheme in this class is proposed in where a so-called *R-diode sensor*, built from two MOSFETs and one resistor, is employed [25].

Finally, a scheme which does not fit in the categories above, but it is interesting for its stability and low power is described in [22] where, thanks to the antenna effect, a random break is caused in gate oxide. However, according to [23], the required over-voltage can cause chip degradation.

Truly Analog PUFs/PUCs Truly analog PUFs/PUCs are not commonly found in the literature. A recent contribution based on similar ideas to our proposal is [24] where a PUC based on switched capacitors is proposed. The PUC of [24] uses the ratio between to capacitances to get independence from power voltage and temperature variation and introduces transmission lines connected to the capacitors to protect the chip from invasive attacks. The PUC in [24] is used in [58] as starting point to create a strong PUF with the same robustness characteristics. Another example of APUC based on capacitances is given in [42, 59, 60], but the source of randomness is a dielectric layer added as post-processing and including particles (e.g., TiO_2 and TiN in [59]) that cause random variations in the capacitances.

Our contribution We propose and evaluate, both theoretically and via simulations, an APUC scheme. Differently from the schemes proposed in [24, 42, 58–60] the proposed scheme uses resistors as source of randomness. Similarly to [24] the proposed scheme uses the ratio of two resistors to gain temperature independence. The results show that the proposed scheme promises good performances to be confirmed in a future experimental setup, together with aging behavior.

2 Statistical model and performance metric for digital and analog PUCs

In this section we first describe a DPUCs statistical model (Section 2.1) that will be the basis for the APUC statistical model (Section 2.3). We also adapt the two quality metrics usually found in the literature, namely *inter*- and *intra*-distance, to our context (Section 2.2).

2.1 DPUC Statistical model

Many DPUCs are built as an array of smaller PUCs (often single-bit PUCs) that we will call *cell* to distinguish them from the "full PUC".

Note that in a PUC/PUF two random mechanisms are present. The first mechanism, desirable since it increases the *distance* between the behavior of different chips, is the unavoidable random variation of process parameters during manufacturing; the other source of randomness, undesirable because it can induce errors, is the measurement noise affecting the PUF/PUC behavior at query time.

We will model the behavior of a cell as a function $O : \mathbb{R}^{\nu} \times \mathbb{R}^{\kappa} \to \mathscr{A}$ where

- $\mathscr{A}$ is a finite set representing the output alphabet of the PUC (in most cases it is $\mathscr{A} = \{0, 1\}$, but this is not critical).
- The first parameter of function O is a random vector V_ℓ whose components are process parameters. For example, in an SRAM PUC [6] the components of V_ℓ can be the doping and the oxide thickness

of the two MOSFETs, in the Schottky diode PUC [18] the components of V_ℓ are the reverse saturation currents of the diodes involved. Random vectors relative to different cells will be assumed to be independent identically distributed (iid).

The realization v_ℓ of V_ℓ is "drawn" and frozen at construction time.

- The second parameter is a random vector E whose components are the measurement noises that act every time the cell is queried. In the following we will assume $\kappa = 1$ and $E \sim \mathcal{N}(0, \sigma_E^2)$.

If noise E was negligible, every time cell ℓ is queried it would return the same *noiseless outcome* $O(v_\ell, 0)$. However,noise often is non negligible and errors can happen, that is, a query can return a value different from $O(v_\ell, 0)$.

2.2 DPUC Quality Measures

An ideal PUC satisfies two requirements

- The impact of noise E is minimal, in the sense that $O(v_\ell, E) = O(v_\ell, 0)$ with overwhelming probability
- The noiseless outcome $O(v_\ell, 0)$ is uniformly distributed over $\mathscr{A}$.

In literature how a PUC scheme satisfies those two requirements is measured by the *intra* and *inter distance*.

2.2.1 Reliability and intra-distance

A first measure of reliability, instrumental to the estimation of the intra-distance defined later, is the probability $\mathfrak{R}$ that cell ℓ produces the same result in two different queries, that is,

$$\mathfrak{R}(v_\ell) = P_E[O(v_\ell, E_1) = O(v_\ell, E_2)] \tag{1}$$

where E_1 and E_2 are the two independent random variables associated with the noise in the two different queries. Notation P_E in (1) emphasizes the fact that the probabilities in (1) are taken with respect to the noise E. If $\mathscr{A}$ is the output alphabet of the PUC, it is easy to prove that reliability (1) can be written as

$$\mathfrak{R}(v_\ell) = P_E[O(v_\ell, E_1) = O(v_\ell, E_2)] = \sum_{a \in \mathscr{A}} P_E^2[O(v_\ell, E_2) = a] \tag{2}$$

Remark 2.1

- In general, probabilities (1) and (2) depends on v, therefore they too are "build time random variables." This suggest that different cells will have different reliability, a fact that will become clear later.

- When $\mathfrak{R}(v_\ell) \approx 1$, it is often more convenient to consider the complementary $p_{\text{err}}(v_\ell) = 1 - \mathfrak{R}(v_\ell)$, that is the probability that two queries give different results.

As said before, in literature it is common to find the *intra-distance* μ_{intra} as a measure of reliability [61]. It can be proved that in the context of PUCs the intra-distance is the probability that a *randomly selected cell* returns two different values when queried twice [17, 18]. It is easy to prove that we can obtain μ_{intra} by averaging $p_{\text{err}} = 1 - \mathfrak{R}$ over v, that is,

$$\mu_{\text{intra}} = \int_{\mathbb{R}^v} f_V(v) p_{\text{err}}(v)\, dv = 1 - \int_{\mathbb{R}^v} f_V(v) \mathfrak{R}(v)\, dv \tag{3}$$

2.2.2 Inter distance

A commonly used measure of the uniformity of the distribution of the noiseless outcome $O(V,0)$ is *inter distance* μ_{inter} that, in the case of a PUC, can be shown to be the probability that two different cells have different noiseless outcomes [17, 18]. In other words,

$$\mu_{\text{inter}} = P_V[O(V_\ell,0) \neq O(V_m,0)] \tag{4}$$

It is easy to show that

$$\mu_{\text{inter}} = 1 - \sum_{a \in \mathscr{A}} P_V[O(V_\ell,0) = a]^2 \tag{5}$$

Another measure of uniformity, often used in cryptography, is the *min entropy* defined as

$$H_\infty = -\log_2 \max_{a \in \mathscr{A}} P_V[O(V,0) = a] \tag{6}$$

In the most common case $\mathscr{A} = \{0,1\}$ the two measures are equivalent, in the sense that from μ_{inter} one can obtain H_∞ and vice versa, as it can be seen in Fig. 1.

2.3 APUC Statistical model

The statistical model used for APUC is similar to the one described in Section 2.1, with the difference that now the value of function $O_{\mathbb{R}} : \mathbb{R}^v \times \mathbb{R}^\kappa \to \mathbb{R}$ does not belong to a finite set, but it is a real number. The digitizer will be represented by a function $Q : \mathbb{R} \to \mathscr{A}$ where $\mathscr{A}$ is a finite set. While in 1-bit PUC (a very common type) $\mathscr{A} = \{0,1\}$, in the case of an APUC we expect larger $\mathscr{A}$ sets, reflecting the multi-bit potential of APUCs [62].

In the special case where $V \sim \mathscr{N}(0, \sigma_V^2)$ and $E \sim \mathscr{N}(0, \sigma_E^2)$ are independent and the noise is additive

$$O_{\mathbb{R}}(V,E) = V + E \tag{7}$$

we will say that the APUC is a *Gaussian APUC*. Note that the theory developed in the following applies to every Gaussian APUC, therefore, it can be used even for other APUCs [24, 42, 59, 60].

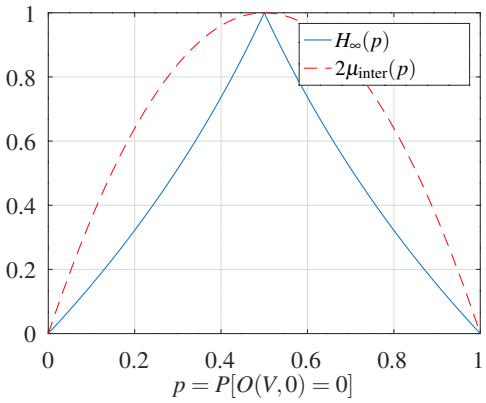


Figure 1: Comparison of the min-entropy H_∞ and the inter-distance μ_{inter} (the latter multiplied by 2 to make the comparison easier)

Remark 2.2

It will be shown in the following that the main performance indicators of a Gaussian APUC are functions of the ratio $\rho = \sigma_V / \sigma_E$, where σ_V and σ_E are the standard deviations of, respectively, V and E. Note that ratio ρ can be interpreted as a a kind of signal-to-noise ratio (SNR).

2.4 A simple digitizer

The main objective of this paper is to describe a new Gaussian APUC scheme and show preliminary simulation results. Nevertheless, in order to estimate the potential performances, it is necessary to complete the proposed APUC to a full PUC by using the simple digitizer $Q : \mathbb{R} \to \{0,1\}$ defined as

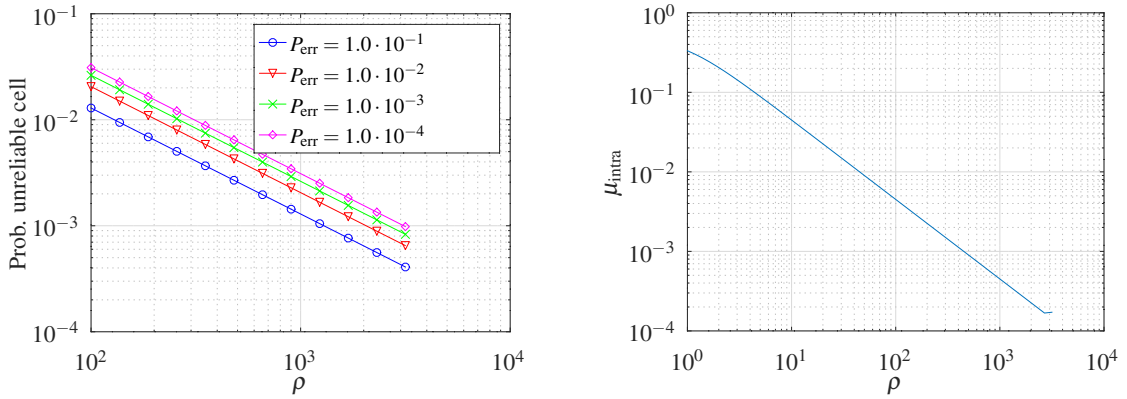
$$Q(x) = \begin{cases} 1 & x \leq 0 \\ 0 & x > 0 \end{cases} \tag{8}$$

Of course, this choice does not exploit the multi-bit potential of the APUC. The development of more powerful digitizers is part of further research activities. In order to predict the multi-bit performances of the proposed scheme, we will use the preliminary results about the multi-bit digitizer described in [62].

It is easy to show that with these hypotheses that (i) cell reliability $\mathfrak{R}(v)$ can be written as (see A.1)

$$\mathfrak{R}(v) = \Phi^2\left(-\frac{v}{\sigma_E}\right) + \Phi^2\left(\frac{v}{\sigma_E}\right) \tag{9}$$

(ii) $\mathfrak{R}(v)$ is even (that is, $\mathfrak{R}(v) = \mathfrak{R}(-v)$) and (iii) it has a single minimum in $v = 0$ (which makes sense since if v is near to zero, even a small noise can cause a sign change.) If a maximum error probability P_{err} is chosen, we will say that a cell is *reliable* if $\mathfrak{R}(v) > 1 - P_{\text{err}}$. It is easy to prove that a cell is reliable if and



(a) (b)

Figure 2: Performances of a Gaussian APUC as function of $\rho = \sigma_V/\sigma_E$. (a) Probability of an unreliable cell vs SNR $\rho = \sigma_V/\sigma_E$. (b) μ_{intra} vs ρ

only if

$$\left|\frac{v}{\sigma_E}\right| > T_{P_{\text{err}}} := \Phi^{-1}\left(\frac{1}{2} + \frac{\sqrt{1-2P_{\text{err}}}}{2}\right) \approx \Phi^{-1}\left(1 - \frac{P_{\text{err}}}{2}\right) \tag{10}$$

where the approximation is obtained by truncating the Taylor series of $x \mapsto \sqrt{1-x}$ around $x = 0$. Finally, the probability of getting an unreliable cell is (see A.2)

$$P\left[\left|\frac{V}{\sigma_E}\right| \leq T_{P_{\text{err}}}\right] = 1 - 2\Phi\left(-\frac{T_{P_{\text{err}}}}{\sigma_V/\sigma_E}\right) = 1 - 2\Phi\left(-\frac{T_{P_{\text{err}}}}{\rho}\right) \tag{11}$$

Note that, as soon as P_{err} is fixed, $T_{P_{\text{err}}}$ is determined via (10) and probability (11) depends only on signal-to-noise ratio $\rho = \sigma_V/\sigma_E$. This allows to plot curves like the ones in Fig. 2.a that shows the probability of having a unreliable cell as function of SNR ρ for different values of P_{err}.

2.5 Intra-distance

The intra-distance μ_{intra} can be written as (see **??**)

$$\mu_{\text{intra}} = 1 - 2\int_{\mathbb{R}} \phi(u)\Phi^2(\rho u)\, dx \tag{12}$$

Since μ_{intra} depends only on ρ, plots like the one in Fig. 2.b are possible. It is easy to verify numerically that the curve Fig. 2.b can be well approximated as $\mu_{\text{intra}} \approx 0.45/\rho$ with a relative error $\leq 0.05\%$ as soon as $\rho \geq 22$.

2.6 Inter distance

If both V and E have zero mean, the inter distance is maximum, $\mu_{\text{inter}} = 1/2$, since 0 and 1 have the same probability. If the mean of V is not zero, that is, $V \sim \mathcal{N}(m_V, \sigma_V^2)$, 0 and 1 are unbalanced and the intra

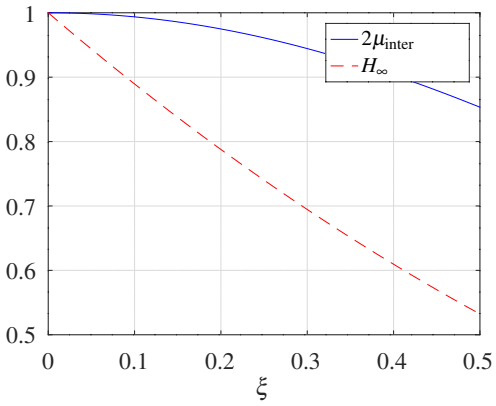


Figure 3: $2\mu_{\text{inter}}$ and H_∞ as function of $\xi = m_V/\sigma_V$

distance gets smaller.

It is easy to prove that the probability of getting 1 and 0 can be written as

$$\begin{aligned} P[Q(V)=1] &= P[V<0] = \Phi\left(\frac{m_V}{\sigma_V}\right) = \Phi(\xi) \\ P[Q(V)=0] &= P[V>0] = \Phi(-\xi) \end{aligned} \tag{13}$$

where we introduced the notation $\xi = m_V/\sigma_V$. From (13) it follows

$$\begin{aligned} \mu_{\text{intra}} &= 2\Phi(\xi)\Phi(-\xi) \\ H_\infty &= -\log_2 \max(\Phi(\xi), \Phi(-\xi)) \end{aligned} \tag{14}$$

From (14) it is clear that both measures depends only on ξ. It is also clear that measures (14) do not depend on the sign of ξ. See also Fig. 3 that shows $2\mu_{\text{inter}}$ and H_∞ as function of ξ.

Observe that these results and the plots of Fig. 2 and Fig. 3 have been obtained using only the hypothesis of having a Gaussian APUC; therefore, they can be applicable even to APUCs different from the one proposed in this paper [24, 42, 59, 60].

3 Resistor based APUC

We propose to use as random variable V the resistance of a slab of n-doped semiconductor with nominal dopant concentration n and dimensions $W \times L \times d$. In this section we discuss the expected statistic, the impact of temperature variations and how to reduce them.

3.1 Statistical dispersion of the conductance

Because of manufacturing variations, the actual conductance of the slab at temperature T can be modeled as a Gaussian random variable g_T, more precisely

$$g_T \sim \mathcal{N}\left(G_T, \Gamma^2 \frac{G_T^2}{WL}\right) = \mathcal{N}\left(G_T, (\sigma_{\%} G_T)^2\right) \tag{15}$$

where

$$G_T = \frac{n_0}{N_\square} \frac{q\mu(T)}{d} \tag{16}$$

is the nominal conductance with $N_\square = L/W$ and $\mu(T)$ the electron mobility at temperature T [63], Γ is a constant that depends on the production process (for example, in SKY130, $\Gamma = 3.47\%/\mu\text{m}$) and

$$\sigma_{\%} = \frac{\Gamma}{\sqrt{WL}} = \frac{\Gamma}{W\sqrt{N_\square}} \tag{17}$$

is the relative standard deviation (ratio of the standard deviation to the mean) and it is inversely proportional to the square root of the area, as well known. See A.3 for details.

Note that Since g_T is Gaussian, the proposed APUC is a Gaussian APUC and the theory of Section 2.4 is applicable.

3.2 Impact of temperature

A drawback of using the conductance of a semiconductor slab as the analog variable is the sensitivity to temperature variations. If g_{T_1} is the conductivity at temperature T_1, it is easy to see that

$$g_{T_1} = \overline{\mu}(T_1) g_{T_0} \tag{18}$$

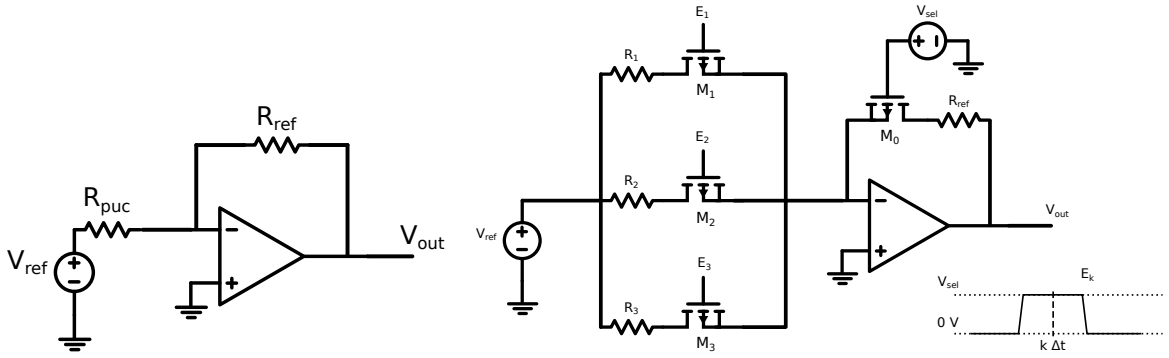
where

$$\overline{\mu}(T) := \frac{\mu(T)}{\mu(T_0)} \approx \left(\frac{T}{T_0}\right)^{-3/2} \tag{19}$$

In (19) we used the approximation $\mu(T) \propto T^{-3/2}$, valid for $T > 100$ K [63]. Using $T_0 = 300$ K, $\overline{\mu}(T)$ ranges between 0.65 and 1.61 when T ranges between -55 °C and 125 °C. This suggests that temperature changes can alter the resistance value up to $\pm$50–60%.

In order to reduce the impact of the temperature, we propose to measure the conductance g_{T_0} by comparing it with a reference resistor using the scheme of Fig. 4a. Resistor R_{puc} is the resistor whose value is used to generate the secret, its area must be as small as possible in order to increase σ_V; resistor R_{ref} acts as reference and it has the same $N_\square$ of R_{puc}. Assuming an ideal operational amplifier, the output is

$$V_{\text{out}} = -V_{\text{ref}} \frac{R_{\text{ref}}}{R_{\text{puc}}} = -V_{\text{ref}} \frac{\frac{q\mu(T)}{N_\square d} n_{\text{puc}}}{\frac{q\mu(T)}{N_\square d} n_0} = -V_{\text{ref}} \mathcal{N}\left(1, \sigma_{\%}^2\right) \tag{20}$$



(a) (b)

Figure 4: (a) Single cell. (b) Multi-cell scheme with three cells and cell selection. MOSFETs M_1, M_2 and M_3 are used to select the resistors R_1, R_2 and R_3 one at time; MOSFET M_0 is always on. The inset shows the signal used to select the k-th resistor at time $k\Delta t$.

where $n_{\text{puc}} \sim \mathcal{N}(n_0, n_0^2\sigma_{\%}^2)$ is the actual dopant concentration in R_{puc}. Taking the ratio between R_{ref} and R_{puc} factors out the temperature dependency.

Remark 3.1

Fig. 4b shows the circuit used in the simulations. MOSFETs M_1, M_2, ... are used to select resistors R_1, R_2, ... one at time, while the reference resistor remains the same. The inset shows the signal E_k used to select the k-th resistor at time $k\Delta t$. MOSFET M_0 in Fig. 4b seems redundant since it is always on; nevertheless its presence is necessary in order to make the scheme more "symmetrical" in order to reduce the temperature dependency, as the simulation results in Section 4 show.

3.2.1 A more faithful temperature model

By simulating the schemes in Fig. 4 at different temperatures one observes a residual temperature dependence, in contrast with (20).

A reason for this discrepancy is that in Section 3.2 we assumed that the resistor is just a slab of semiconducting material, ignoring any additional contribution such as the contact pads or the MOSFETs in Fig. 4b.

In order to get some guidelines that can help us to reduce the impact of temperature, a more faithful model is needed. We approximate the behavior of R_{ref} with the temperature as as the series of two resistors with two different temperature sensitivities, more precisely

$$R_{\text{ref}}(T) = r_{\text{ref}}\alpha(T) + \hat{r}_{\text{ref}}\beta(T) \tag{21}$$

where the first term $r_{\text{ref}}\alpha(T)$ is the resistance of the slab at temperature T, while the second term $\hat{r}_{\text{ref}}\beta(T)$ is the value of a parasitic resistor that models (approximately) the effect of contact pads, MOSFETs and so

on. In (21) α and β are two suitable (different) functions that we do not need to specify further. In an ideal case, $\hat{r}_{\text{ref}} = 0$.

Similarly, for R_{puc}

$$R_{\text{puc}}(T) = r_{\text{puc}}\alpha(T) + \hat{r}_{\text{puc}}\beta(T) \tag{22}$$

With this model the output of the operational amplifier at temperature T is

$$-V_{\text{ref}}\frac{r_{\text{ref}}\alpha(T) + \hat{r}_{\text{ref}}\beta(T)}{r_{\text{puc}}\alpha(T) + \hat{r}_{\text{puc}}\beta(T)} = \underbrace{-V_{\text{ref}}\frac{r_{\text{ref}}}{r_{\text{puc}}}}_{\text{ideal}}\ \underbrace{\frac{1 + \frac{\hat{r}_{\text{ref}}}{r_{\text{ref}}}\gamma(T)}{1 + \frac{\hat{r}_{\text{puc}}}{r_{\text{puc}}}\gamma(T)}}_{\text{Temp. dep.}} \tag{23}$$

where $\gamma(T) = \frac{\beta(T)}{\alpha(T)}$.

According to (23), the impact of the temperature can be minimized by having ratios $\hat{r}_{\text{ref}}/r_{\text{ref}}$ and $\hat{r}_{\text{puc}}/r_{\text{puc}}$ small. This suggests

- Make the nominal value of R_{puc} (and R_{ref}) large and this means using long and thin slabs. Therefore, W is chosen as the minimum possible width, while L is chosen large, but keeping in mind that a small product WL increases the dispersion $\sigma_{\%} = \Gamma/\sqrt{WL}$.
- Make the MOSFETs with a large W_{M} and short L_{M} and use a large V_{sel}.

The utility of these guidelines will be confirmed by simulations in Section 4.

4 Simulation results

We simulated the proposed scheme using the open PDK SKYWATER SKY130. We choose this PDK since it is open and this makes it easier to replicate the results. The goal of the simulations was to get data about (i) temperature dependence, (ii) noise impact and (iii) resistor dispersion. By using these data we will be able to predict the performances of the proposed scheme in terms of bit/cell.

4.1 Temperature dependence

We run few simulation to verify the effect of the temperature on the APUC output and to verify the guidelines derived above, that is, if the temperature dependency is reduced when (i) R_{ref} is large, (ii) the ratio $W_{\text{M}}/L_{\text{M}}$ is large and (iii) V_{sel} is large.

In order to increase the dispersion, the area of R_{puc} must be as small as possible and because of this we fixed the width $W_{\text{puc}} = W_{\text{ref}}$ to the smallest value possible, that is, 0.65 μm and adjusted R_{ref} by changing the length L_{ref}. In order to take into account the imbalance between R_{ref} and R_{puc}, we changed the length

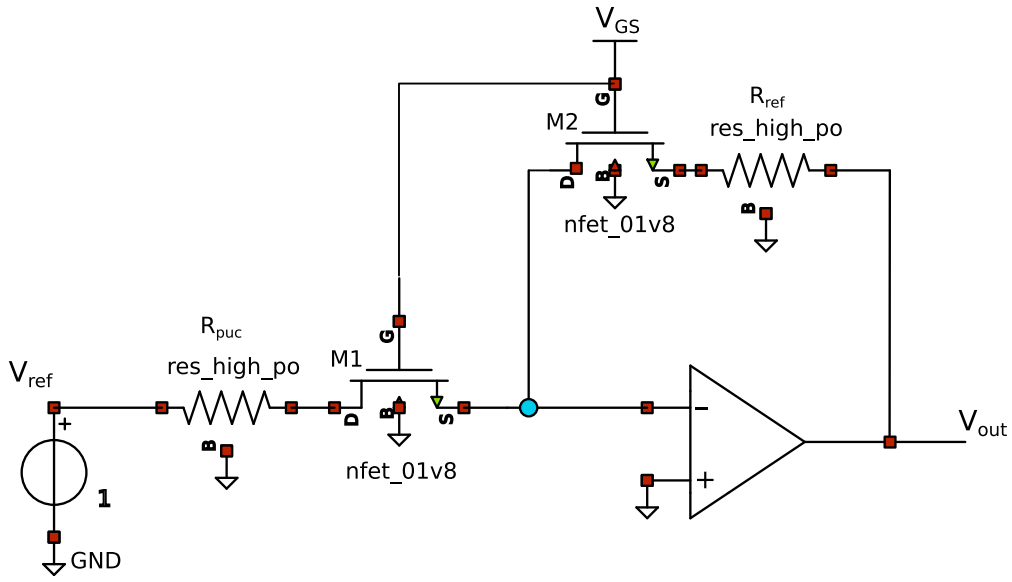


Figure 5: Circuit used in temperature sensitivity simulations.

L_{puc} of R_{puc} by choosing $L_{\text{puc}} = \theta L_{\text{ref}}$, with $\theta \in [0.7, 1.4]$ (see Remark 4.1 for a further discussion). In the MOSFETs we fixed the length to $L_{\text{M}} = 1.5\ \mu$m and changed only the width W_{M}. The temperature T ranges from $T_{\min} = -55°$C to $T_{\max} = 125°$C, with nominal temperature $T_0 = 26.85°\text{C} = 300$K.

Remark 4.1

The approach used to simulate the imbalance does not take into account the statistic of the dispersion of the resistance of R_{puc}, but since our goal here is to check the impact of the imbalance on the temperature sensitivity, we are not interested in the statistical distribution of R_{puc}. The statistical distribution of R_{puc} will be of interest later in Section 4.2, where we will use the Montecarlo approach to simulate the actual dispersion.

We simulated the circuit shown in Fig. 5 for different values of W_{M}, L_{ref}, V_{sel}, V_{ref}, θ, and T. Collect, for notation convenience, the first four parameters in a vector $\mathscr{P} = [L_{\text{ref}}, W_{\text{M}}, V_{\text{sel}}, V_{\text{ref}}]$. Let $\mathscr{O}_T(\theta, \mathscr{P})$ be the output at temperature T for a given choice of $\mathscr{P}$ and θ.

In order to simplify the presentation of the results, we do not show $\mathscr{O}_T(\theta, \mathscr{P})$ for every temperature, but summarizes its variation in value

$$\mathfrak{D}(\theta, \mathscr{P}) = \max_{T \in [T_{\min}, T_{\max}]} \frac{|\mathscr{O}_T(\theta, \mathscr{P}) - \mathscr{O}_{T_0}(\theta, \mathscr{P})|}{\mathscr{O}_{T_0}(\theta, \mathscr{P})} \tag{24}$$

which represents the maximum relative deviation from the nominal output $\mathscr{O}_{T_0}(\mathscr{P})$.

Fig. 6 shows the maximum relative deviation (24) vs $\theta = R_{\text{puc}}/R_{\text{ref}}$ for different choices of parameters. Clearly, the guidelines deduced above are effective and by choosing W_{M} large, L_{ref} large and V_{sel} large the temperature dependency can be reduced.

Fig. 7 shows the impact of the "dummy" MOSFET M2. It is clear that the more symmetric scheme (with the dummy MOSFET included) is much less sensitive to temperature variations.

4.2 Output distribution

We simulated the circuit of Fig. 8 with $N = 5120$ copies in parallel of the basic cell. The Montecarlo model provided by SKY130 was used for the resistors, in order to simulate the dispersion of the resistance values. The resistors have been activated in sequence using a suitably timed pulse (not shown in the figure to reduce the clutter). The output values have been collected, their average computed and subtracted from the acquired values, in order to force them to be zero mean.

Fig. 9 shows the histograms of the output values, compared with the fitting Gaussian (dashed line). We simulated the circuit for different choices of the circuit parameters (L_{M}, W_{M}, L_{ref}, ...) and the results are consistent with those shown in Fig. 9 with a typical $0.04\ \mathrm{V} \leq \sigma_V \leq 0.05\ \mathrm{V}$. The Pearson chi-squared test for Gaussian distribution gives p-values of the order of 10^{-3} or even smaller.

4.3 Noise

As described in Section 2.4, the quality figure for an APUC is the signal-to-noise ratio $\rho = \sigma_V/\sigma_E$, where σ_E^2 is the noise variance. The results are plotted in Fig. 10 that shows the noise RMS vs L_{ref} for different values of W_{M}. Since $\sigma_V \approx 4 \cdot 10^{-2}$ V, we deduce that ρ can range from 10^3 up to 10^4. Using the theory of Section 2.4 we deduce that the probability of an unreliable cell is 10^{-3} or smaller. According to Fig. 2b, the expected intra distance μ_{intra} is of the order of 10^{-3} or smaller. This suggests that with the proposed APUC it could be possible to build very reliable PUCs that need no error correction. Of course, this prediction must be verified experimentally in future research activities.

Preliminary results with a multi-bit digitizer To the best of our knowledge, the only multi-bit digitizer for Gaussian APUCs in the literature is described in reprint [62]. The digitizer in [62] uses the fact that the quantization noise of a sufficiently fine quantizer is approximately uniform; therefore, it convert the outcome of the APUC using an Analog to Digital Converter (ADC) and takes only the least significant bits. Of course, by using ADCs with a large number of bits one can extract as many bits as desired; the problem is that if the resolution gets too fine, the least bits are unstable because of noise. In [62] it is derived the trade-off between the reliability of the whole PUC (APUC and digitizer) and the number of extracted bits. The key value, once again, is the SNR $\rho\sigma_V/\sigma_E$.

According to the results in [62], for a 1024-bit PUC with probability of bad turn-on between 10^{-3} and 10^{-2}, we can expect to extract **5–6 uniformly distributed bits/cell** (or more). Although this is just a

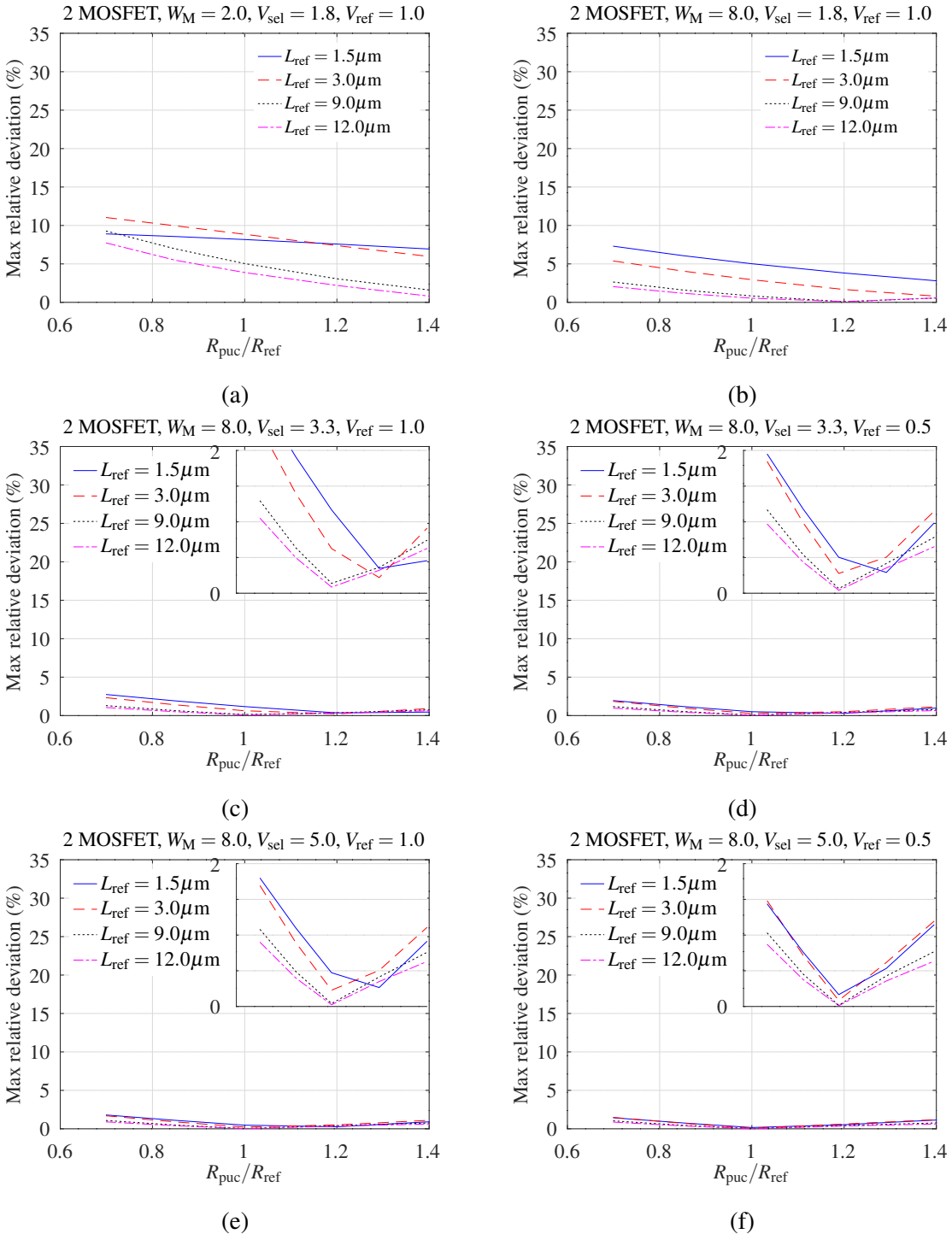


Figure 6: Maximum relative deviation vs $\theta = R_{puc}/R_{ref}$ for different choices of parameters. Different lines are relative to different values of L_{ref}. The vertical axis have the same scale to make comparison easier, when needed an inset was added. (a) Case with $W_M = 2$, $L_M = 1.5$, $V_{sel} = 1.8$ V, $V_{ref} = 1$ V. (b) Like (a), but with a wider MOSFET $W_M = 8$. (c) Like (b) but with a larger $V_{sel} = 3.3$ V. (d) Like (c), but with a smaller $V_{ref} = 0.5$ V. (e) and (f) Like (b) and (c), but with a larger $V_{sel} = 5$ V.

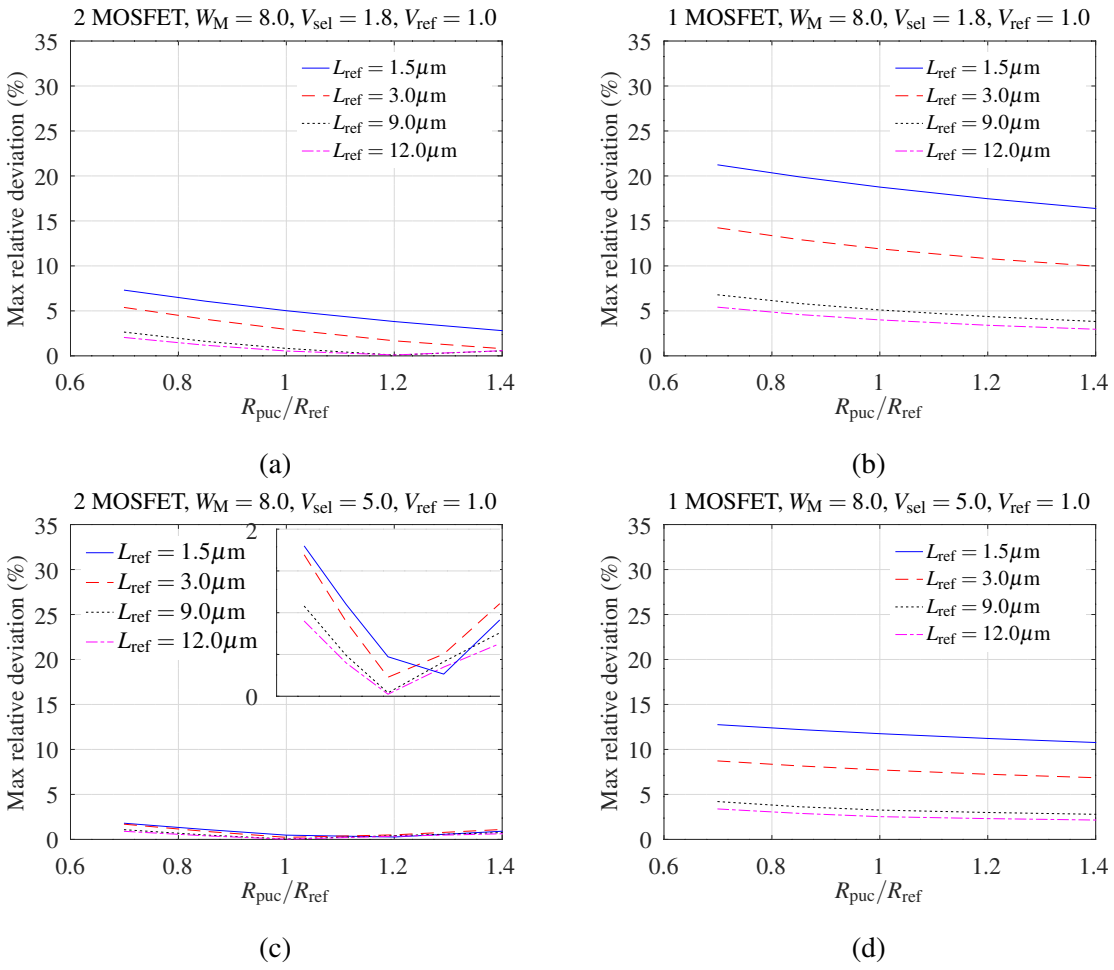


Figure 7: Impact of the dummy MOSFET on temperature sensitivity. (a) and (c) Maximum relative variation vs. $\theta = R_{puc}/R_{ref}$ for the scheme of Fig. 5 with the dummy MOSFET M2. (b) and (d) The same as (a) and (c), but without the dummy MOSFET

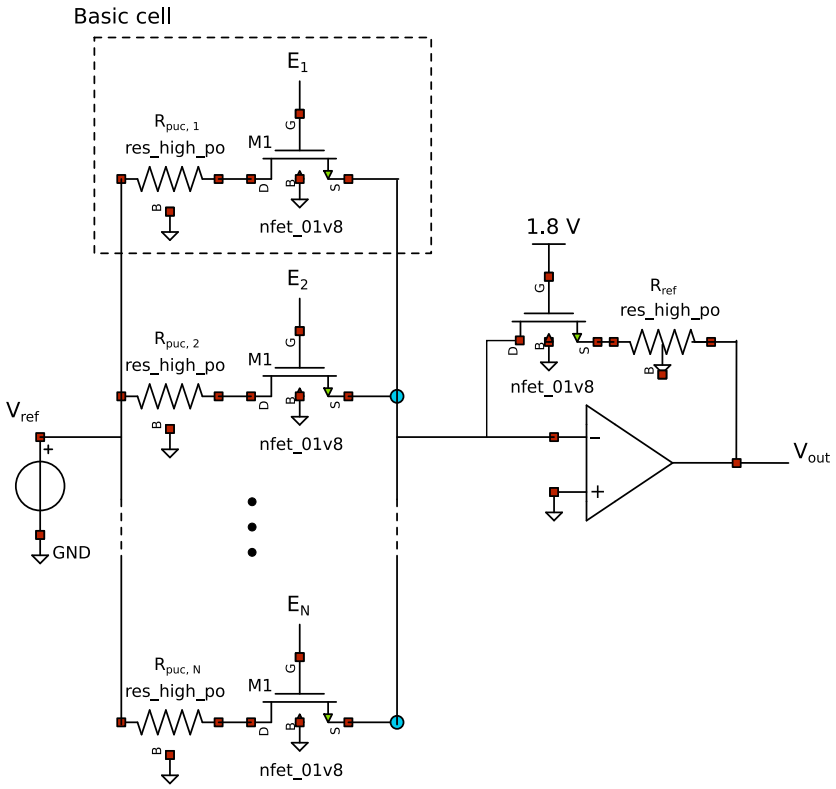
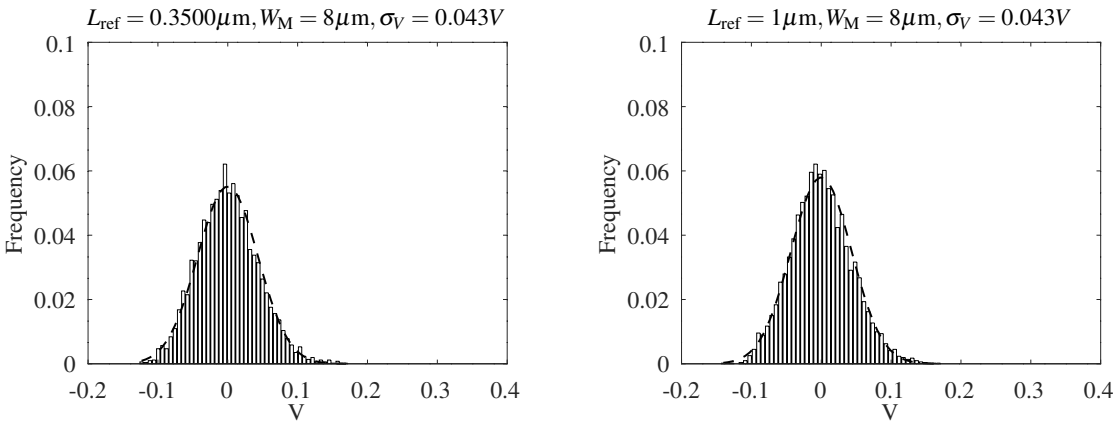
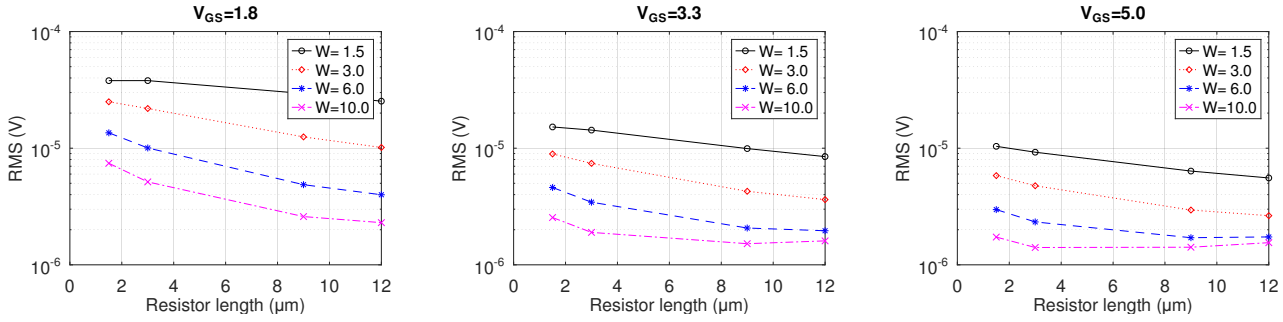


Figure 8: Circuit used to simulate the output distribution



(a) (b)

Figure 9: Distributions of the output values of the circuit of Fig. 8



(a) (b) (c)

Figure 10: Simulated noise RMS

preliminary result that needs to be confirmed experimentally, it suggests that the a Gaussian APUC followed by a suitable digitizer can be a viable solution.

5 Conclusion

We presented a simple Gaussian APUC based on the dispersion of the resistance value of a P+ polysilicon resistor. The SNR ρ derived by simulations with the open PDK SKYWATER SKY130 suggests interesting performances that predict intra distances smaller than 10^{-3} and at least 5–6 bit/cell. Possible future lines of research are the implementation of a prototype to verify experimentally the prediction described her and the development of new digitizers that exploits the multi-bit capability of the proposed APUC.

References

[1] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way function," *Science*, 2002.

[2] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM conference on Computer and communications security*, CCS '02, (New York, NY, USA), pp. 148–160, ACM, 2002.

[3] D. Lim, J. Lee, B. Gassend, G. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, vol. 13, no. 10, pp. 1200–1205, 2005.

[4] D. Lim, "Extracting secret keys from integrated circuits," Master's thesis, MIT, May 2004.

[5] G. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Design Automation Conference, 2007. DAC '07. 44th ACM/IEEE*, pp. 9–14, 2007.

[6] D. E. Holcomb, W. P. Burleson, and K. Fu, "Initial SRAM state as a fingerprint and source of true random numbers for rfid tags," in *In Proceedings of the Conference on RFID Security*, 2007.

[7] R. Maes, P. Tuyls, and I. Verbauwhede, "A soft decision helper data algorithm for SRAM PUFs," in *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, pp. 2101–2105, 2009.

[8] S. K. Ram, S. R. Sahoo, B. B. Das, K. Mahapatra, and S. P. Mohanty, "sthing: A novel configurable ring oscillator based puf for hardware-assisted security and recycled ic detection," *IEEE Access*, vol. 13, pp. 2994–3013, 2025.

[9] J.-W. Nam, J.-H. Ahn, and J.-P. Hong, "Compact sram-based puf chip employing body voltage control technique," *IEEE Access*, vol. 10, pp. 22311–22319, 2022.

[10] S. V. S. Avvaru and K. K. Parhi, "Feed-forward xor pufs: Reliability and attack-resistance analysis," in *Proceedings of the 2019 Great Lakes Symposium on VLSI*, GLSVLSI '19, (New York, NY, USA), p. 287–290, Association for Computing Machinery, 2019.

[11] S. V. S. Avvaru, Z. Zeng, and K. K. Parhi, "Homogeneous and heterogeneous feed-forward xor physical unclonable functions," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2485–2498, 2020.

[12] M. C. Martínez-Rodríguez, L. F. Rojas-Muñoz, E. Camacho-Ruiz, S. Sánchez-Solano, and P. Brox, "Efficient ro-puf for generation of identifiers and keys in resource-constrained embedded systems," *Cryptography*, vol. 6, no. 4, 2022.

[13] S. Hou, Y. Ma, D. Deng, Z. Wang, and G. Ren, "Modeling and physical attack resistant authentication protocol with double pufs," *Journal of Information Security and Applications*, vol. 76, p. 103543, 2023.

[14] S. K. Ram, S. R. Sahoo, B. B. Das, K. Mahapatra, and S. P. Mohanty, "sthing: A novel configurable ring oscillator based puf for hardware-assisted security and recycled ic detection," *IEEE Access*, vol. 13, pp. 2994–3013, 2025.

[15] R. Tian and L. Dai, "A strong physical unclonable function based on sar adc," in *2024 4th International Conference on Electronics, Circuits and Information Engineering (ECIE)*, pp. 471–474, 2024.

[16] Q. Tang, W. H. Choi, L. R. Everson, K. K. Parhi, and C. H.-I. Kim, "A physical unclonable function based on capacitor mismatch in a charge-redistribution sar-adc," *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–5, 2018.

[17] R. Bernardini and R. Rinaldo, "Analytic and simulation results about a compact, reliable, and unbiased 1-bit physically unclonable constant," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 2804–2817, Dec. 2016.

[18] R. Bernardini and R. Rinaldo, "A very stable diode-based physically unclonable constant," *Integr. VLSI J.*, vol. 59, pp. 179–189, Sept. 2017.

[19] M. Yoo, S. B. Kim, H. Son, K. Kim, J. Wi, G. Nam, M. Son, M. Choi, I. Yu, D. K. Kim, and H. Ko, "Dram physically unclonable function (puf) using dual word-line activated twin-cells," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 72, no. 3, pp. 514–518, 2025.

[20] J. Trujillo, C. Merino, and P. Zarkesh-Ha, "Sram physically unclonable functions implemented on silicon germanium," in *2019 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–4, 2019.

[21] A. A. Zayed, H. H. Issa, and K. A. Shehata, "Finfet based low power ring oscillator physical unclonable functions," in *2019 31st International Conference on Microelectronics (ICM)*, pp. 227–230, 2019.

[22] F. Tang, D. Chen, B. Wang, A. Bermak, A. Amira, and S. Mohamad, "CMOS on-chip stable true-random ID generation using antenna effect," *Electron Device Letters, IEEE*, vol. 35, pp. 54–56, Jan 2014.

[23] K. Matsunaga, S. Oshima, T. Minotani, T. Kondo, and H. Morimura, "Automatic identification number generation circuit using NMOS pair current mismatch," *Japanese Journal of Applied Physics*, vol. 54, no. 4S, p. 04DE12, 2015.

[24] M. Wan, Z. He, S. Han, K. Dai, and X. Zou, "An invasive-attack-resistant puf based on switched-capacitor circuit," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 8, pp. 2024–2034, 2015.

[25] C. Bai, X. Zou, and K. Dai, "A highly stable R-Diode-based physical unclonable function," in *ICINS 2014 - 2014 International Conference on Information and Network Security*, pp. 22–27, Nov 2014.

[26] Z. Paral and S. Devadas, "Reliable and efficient PUF-based key generation using pattern matching," in *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on*, pp. 128–133, 2011.

[27] J. Delvaux and I. Verbauwhede, "Fault injection modeling attacks on 65nm arbiter and ro sum PUFs via environmental changes." Cryptology ePrint Archive, Report 2013/619, 2013. http://eprint.iacr.org/.

[28] S. Joshi, S. P. Mohanty, and E. Kougianos, "Everything you wanted to know about pufs," *IEEE Potentials*, vol. 36, no. 6, pp. 38–46, 2017.

[29] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[30] J. Miskelly, C. Gu, Q. Ma, Y. Cui, W. Liu, and M. O'Neill, "Modelling attack analysis of configurable ring oscillator (cro) puf designs," in *2018 IEEE 23rd International Conference on Digital Signal Processing (DSP)*, pp. 1–5, 2018.

[31] R. Bernardini and R. Rinaldo, "Theoretical limits of helper-less stabilizers for physically unclonable constants," *Emerging Topics in Computing, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2014. doi : 10.1109/TETC.2014.2386137.

[32] C. Herder, L. Ren, M. van Dijk, M. Yu, and S. Devadas, "Trapdoor computational fuzzy extractors and stateless cryptographically-secure physical unclonable functions," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, pp. 65–82, Jan 2017.

[33] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proceedings of the 1st ACM Conference on Computer and Communications Security*, CCS '93, (New York, NY, USA), pp. 62–73, ACM, 1993.

[34] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," *J. ACM*, vol. 33, pp. 792–807, Aug. 1986.

[35] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[36] B. Diffie, M. Hellman, and R. Merkle, "Cryptographic apparatus and method." PatentUS US 4200770 A, Apr. 1980.

[37] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley and Sons, 1994.

[38] R. Bernardini and R. Rinaldo, "Physically unclonable random permutations," in *Recent Advances in Electrical and Electronic Engineering*, (Florence, Italy), pp. 148–154, Nov. 2014.

[39] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, "RadioGatun, a belt-and-mill hash function," in *Second Cryptographic Hash Workshop*, (Santa Barbara), Aug. 2006.

[40] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, "Sponge functions," in *Ecrypt Hash Workshop*, May 2007.

[41] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, *CHES*, vol. 6225 of *Lecture Notes in Computer Science*, ch. Sponge-based pseudo-random number generators. Springer, 2010.

[42] J. Biba, S. Boche, U. Goßner, and W. Hansch, "Fabrication and characterization of 2-bit per capacitor as functional structures for physical unclonable function circuits," *IEEE Journal of the Electron Devices Society*, vol. 10, pp. 157–168, 2022.

[43] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, *FPGA Intrinsic PUFs and Their Use for IP Protection*, pp. 63–80. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007.

[44] S. K. Mathew, S. K. Satpathy, M. A. Anders, H. Kaul, S. K. Hsu, A. Agarwal, G. K. Chen, R. J. Parker, R. K. Krishnamurthy, and V. De, "16.2 A 0.19pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS," in *2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*, pp. 278–279, Feb 2014.

[45] S. Satpathy, S. Mathew, J. Li, P. Koeberl, M. Anders, H. Kaul, G. K. Chen, A. Agarwal, S. Hsu, and R. Krishnamurthy, "13fj/bit probing-resilient 250k PUF array with soft darkbit masking for 1.94% bit-error in 22nm tri-gate CMOS," in *ESSCIRC 2014 - 40th European Solid State Circuits Conference, Venice Lido, Italy, September 22-26, 2014*, pp. 239–242, 2014.

[46] S. Satpathy, S. Mathew, V. Suresh, and R. Krishnamurthy, "Ultra-low energy security circuits for IoT applications," in *2016 IEEE 34th International Conference on Computer Design (ICCD)*, pp. 682–685, Oct 2016.

[47] S. Satpathy, S. K. Mathew, V. Suresh, M. A. Anders, H. Kaul, A. Agarwal, S. K. Hsu, G. Chen, R. K. Krishnamurthy, and V. K. De, "A 4-fJ/b Delay-Hardened Physically Unclonable Function Circuit With Selective Bit Destabilization in 14-nm Trigate CMOS," *IEEE Journal of Solid-State Circuits*, vol. 52, pp. 940–949, April 2017.

[48] S. Mathew, S. Satpathy, V. Suresh, and R. K. Krishnamurthy, "Energy efficient and ultra low voltage security circuits for nanoscale CMOS technologies," in *2017 IEEE Custom Integrated Circuits Conference (CICC)*, pp. 1–4, April 2017.

[49] R. Bernardini and R. Rinaldo, "Analysis of some simple stabilizers for physically obfuscated keys," *International Journal of Information Security*, Oct. 2019.

[50] Y. Su, J. Holleman, and B. P. Otis, "A 1.6pj/bit 96% stable chip-id generating circuit using process variations," in *2007 IEEE International Solid-State Circuits Conference, ISSCC 2007, Digest of Technical Papers, San Francisco, CA, USA, February 11-15, 2007*, pp. 406–611, 2007.

[51] Y. Su, J. Holleman, and B. Otis, "A digital 1.6 pJ/bit chip identification circuit using process variations," *Solid-State Circuits, IEEE Journal of*, vol. 43, pp. 69–77, Jan 2008.

[52] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up SRAM state as an identifying fingerprint and source of true random numbers," *IEEE Transactions on Computers*, 2009.

[53] X. Xu, A. Rahmati, D. Holcomb, K. Fu, and W. Burleson, "Reliable physical unclonable functions using data retention voltage of SRAM cells," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2015. doi: 10.1109/TCAD.2015.2418288.

[54] V. Kohli, M. Aman, and B. Sikdar, "An intelligent fingerprinting technique for low-power embedded iot devices," *IEEE Transactions on Artificial Intelligence*, vol. PP, 04 2024.

[55] F. Tehranipoor, N. Karimian, W. Yan, and J. A. Chandy, "DRAM-based intrinsic physically unclonable functions for system-level security and authentication," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. PP, no. 99, pp. 1–13, 2016.

[56] P. Prabhu, A. Akel, L. Grupp, W.-K. Yu, G. Suh, E. Kan, and S. Swanson, "Extracting device fingerprints from flash memory by exploiting physical variations," in *Trust and Trustworthy Computing* (J. McCune, B. Balacheff, A. Perrig, A.-R. Sadeghi, A. Sasse, and Y. Beres, eds.), vol. 6740 of *Lecture Notes in Computer Science*, pp. 188–201, Springer Berlin Heidelberg, 2011.

[57] K. Lofstrom, W. Daasch, and D. Taylor, "IC identification circuit using device mismatch," in *Solid-State Circuits Conference, 2000. Digest of Technical Papers. ISSCC. 2000 IEEE International*, pp. 372–373, Feb 2000.

[58] Z. He, M. Wan, J. Deng, C. Bai, and K. Dai, "A reliable strong puf based on switched-capacitor circuit," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 26, no. 6, pp. 1073–1083, 2018.

[59] D. Roy, J. H. Klootwijk, N. A. M. Verhaegh, H. H. A. J. Roosen, and R. A. M. Wolters, "Comb capacitor structures for on-chip physical uncloneable function," *IEEE Transactions on Semiconductor Manufacturing*, vol. 22, no. 1, pp. 96–102, 2009.

[60] J. Biba, S. Boche, N.-H. Sadek, and W. Hansch, "Measurement setup for physical unclonable functions," in *2021 6th International Conference on Integrated Circuits and Microsystems (ICICM)*, pp. 155–159, 2021.

[61] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security - Foundations and Practice*, pp. 3–37, Springer, 2010.

[62] R. Bernardini, "An Efficient Digitizer for Gaussian Physically Unclonable Functions," *TechRXiv*, Mar. 2025. https://doi.org/10.36227/techrxiv.174320040.05185107/v1.

[63] S. Sze and K. Ng, *Physics of Semiconductor Devices*. Wiley, 2006.

A Proofs

A.1 Proof of (9)

Let

$$p_{v_\ell}(a) = P[O(v_\ell, E_2) = a] \tag{25}$$

Observe that

$$\begin{aligned} p_v(1) &= P[Q(v+E) = 1] \\ &= P[v+E < 0] \\ &= P[E < -v] = \Phi\left(-\frac{v}{\sigma_E}\right) \end{aligned} \tag{26}$$

and that

$$p_v(0) = 1 - \Phi\left(-\frac{v}{\sigma_E}\right) = \Phi\left(\frac{v}{\sigma_E}\right) \tag{27}$$

Now (9) follows at once.

A.2 Proof of (11)

It is easy to prove that a cell is unreliable if and only if

$$\tau \leq \Phi\left(-\frac{v}{\sigma_E}\right) \leq 1-\tau \tag{28}$$

where

$$\tau = \frac{1}{2} - \frac{\sqrt{1-2P_{\text{err}}}}{2} \approx \frac{P_{\text{err}}}{2} \tag{29}$$

In (29) the approximation is obtained by truncating the Taylor series and holds for P_{err} small. Since Φ is monotone increasing, (28) is equivalent to

$$\Phi^{-1}(\tau) \leq -\frac{v}{\sigma_E} \leq \Phi^{-1}(1-Q) = -\Phi^{-1}(\tau) \tag{30}$$

that is,

$$\left|\frac{v}{\sigma_E}\right| \leq T_{P_{\text{err}}} := \Phi^{-1}(1-\tau) \tag{31}$$

Finally, the probability of getting an unreliable cell is

$$P\left[\left|\frac{V}{\sigma_E}\right| \leq T_{P_{\text{err}}}\right] = 1 - 2\Phi\left(-\frac{T_{P_{\text{err}}}}{\rho}\right) \tag{32}$$

A.3 Derivation of (??)

Using (3)

$$\begin{aligned}
\mu_{\text{intra}} &= 1 - \int_{\mathbb{R}} f_V(x)\mathfrak{R}(x)\,dx \\
&= 1 - \int_{\mathbb{R}} \frac{1}{\sigma_V}\phi(x/\sigma_V)\mathfrak{R}(x)\,dx \\
&= 1 - \int_{\mathbb{R}} \frac{1}{\sigma_V}\phi\left(\frac{x}{\sigma_V}\right)\left[\Phi^2\left(\frac{x}{\sigma_E}\right) + \Phi^2\left(-\frac{x}{\sigma_E}\right)\right]dx \quad \text{From (9)} \\
&= 1 - 2\int_{\mathbb{R}} \frac{1}{\sigma_V}\phi\left(\frac{x}{\sigma_V}\right)\Phi^2\left(\frac{x}{\sigma_E}\right)dx \\
&= 1 - 2\int_{\mathbb{R}} \phi(u)\Phi^2\left(u\frac{\sigma_V}{\sigma_E}\right)dx \qquad \text{Substitution } u = x/\sigma_V \\
&= 1 - 2\int_{\mathbb{R}} \phi(u)\Phi^2(\rho u)\,dx
\end{aligned} \tag{33}$$

A.4 Derivation of (15)

If n is large enough, the conductivity g_T at temperature T is approximately equal to $q\mu(T)n$, where $\mu(T)$ is the electron mobility at temperature T [63]. Therefore, the conductance g_{T_0} of the slab at the nominal temperature T_0 is

$$g_{T_0} = \frac{Wd}{L}\sigma = \frac{W}{L}\frac{q\mu(T_0)}{d}n = \frac{1}{N_\square}\frac{q\mu(T_0)}{d}n \tag{34}$$

where $N_\square = L/W$.

By modeling the doping process as two-dimensional Poisson random process (a physically reasonable assumption), the number of doping atoms in the slab turns out to be a Poisson random variable that in this context can be approximated with a Gaussian random variable. It follows that the dopant concentration is Gaussian too and

$$n \sim \mathscr{N}\left(n_0, \Gamma^2 \frac{n_0^2}{WL}\right) \tag{35}$$

where n_0 is the nominal dopant concentration and Γ is a constant that depends on the production process; for example, in SKY130, $\Gamma = 3.47\%/\mu\text{m}$. By using (34) in (33) one obtains (15).