INTEGRATION the VLSI journal xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

INTEGRATION, the VLSI journal

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

A very stable diode-based physically unclonable constant

Riccardo Bernardini*, Roberto Rinaldo

DPIA – University of Udine, Via delle Scienze 208, 33100 Udine, Italy

ARTICLE INFO

Keywords:
Security
Physically unclonable functions

ABSTRACT

Physically Unclonable Constants (PUC) are circuits used to embed unique secret bit-words in chips. We propose a simple PUC, employing two Schottkydiodes in reverse. The difference of the reverse currents of the two diodes is used to charge a capacitance. The charge stops when the two currents become equal. It is shown that this scheme has a single equilibrium point that depends discontinuously from the difference of the two saturation currents. The proposed scheme is studied both theoretically and by means of simulations (0.18 μm technology). It is shown that the proposed PUC is unbiased (inter distance ≈50%), very stable (intra distance from 2.8% to 1.5%) and temperature insensitive (only 0.3% of the cells changes output over a military temperature range). Energy required is predicted to be as small as 0.6 pJ/bit.

1. Introduction

The necessity of verifying the authenticity of a chip in a simple and secure way gave rise to the introduction of Physically Unclonable Functions (PUFs), circuits that implement a map from bit-words to bit-words, with the actual map randomly selected at construction time [1–6]. Such random selection is achieved by using schemes that are "ill conditioned" in the sense that their behavior changes as a consequence of small changes in process parameters (e.g., doping levels). Because of the random selection, the map implemented by a specific chip will be unique to that chip and this can be used to verify the identity of the chip [7,8]. Moreover, the ill conditioned nature of the scheme makes it very difficult to replicate the PUF of a specific chip (hence, the name). In a sense, a PUF can be considered a fingerprint of the chip.

A special type of PUF is a PUF with no input arguments, that is, a constant.[1] For this class of PUF the names *weak PUFs*, *Physically Obfuscated Keys* (POK) or Physically Unclonable Constant (PUC) are used. They are quite flexible since they can be used not only for authentication purposes, but also as source of randomness to create private keys or other special applications [9]. Used together with an hash function they can be used to emulate a strong PUF.

Ideally, a PUC is a *random constant* [10,11] in the sense that at production time a random bit-string (called in the following the *preferred outcome*) is uniformly selected and every time the PUC is queried the preferred outcome is returned with overwhelming probability. However, actual PUCs are not ideal. For example, the preferred outcome could not be uniformly distributed, that is, the PUC can be *biased*. Moreover, sometimes the preferred outcome is not returned (the PUC makes an *error*), that is, the PUC is not *reliable* (or *stable*). Reliability — a very important quality, since in many security applications a single wrong bit can make the whole system useless — can be improved by means of *stabilizers* that add some redundancy (e.g., syndrome bits [12,13,7,14], spare cells or repeated turn-ons [15,16]) with the objective of correcting errors. It is clear that less reliable PUCs require more redundancy.

1.1. Prior work

Most of the PUCs in the literature can be partitioned in two classes: memory-based PUCs and comparator-based PUCs.

Schemes based on comparators typically use a comparator fed with random voltages like in [17,18]. Their most important drawback is that the transfer function of a real comparator is continuous and this makes the probability of having cells whose output is sensitive to noises non negligible. For example, in [18] 5% unstable bits are reported.

Memory-based PUCs employ SRAM cells or similar structures like latches [19–24]. In [19] the initial state of a non-initialized SRAM is used as the PUC outcome. In [20,22] a latch-like structure is used to amplify an offset voltage. A different approach based on the measure of the data retention voltage of an SRAM is described in [23]. An approach based on Flash memory is proposed in [25]. The schemes based on uninitialized SRAM or latches [19,20,22] have the drawback that the underlying structure has two stable states and it can happen that the PUC ends in the "wrong" state. For example, according to [22], 4% of the latch-based cells are "unstable." According to [6], a similar result holds also for SRAM-based schemes. A different type of memory-

* Corresponding author.
E-mail addresses: riccardo.bernardini@uniud.it (R. Bernardini), rinaldo@uniud.it (R. Rinaldo).

[1] "*Constant*" in this context means that the *digital* output of the circuit does not change as long as the circuit works within admissible ranges of, e.g., power supply or temperature.

http://dx.doi.org/10.1016/j.vlsi.2017.06.010
Received 7 February 2017; Received in revised form 4 May 2017; Accepted 24 June 2017

based PUC is [26] where a DRAM instead of an SRAM is used. Given the reported poor stability of DRAM cells (e.g., 18 cells out of 100 change the outcome at least once every 10 readings) and sensitivity to temperature and voltage variations, a preliminary enrollment phase is necessary [26].

The scheme in [27] solves the problem of multiple stable states of SRAM-like schemes and the noise sensitivity of comparator-based schemes by proposing a circuit with a single stable state that depends discontinuously on the difference of the saturation currents of two MOSFETs. The intra distance of the scheme in [27] is 10–100 times smaller than the intra distance of other schemes, but it has the drawback of large consumption and possible local bias (See [28] for a discussion about the impact of local bias and how to counteract it).

To our knowledge, the only scheme that, like ours, uses diodes is described [29]. The scheme described in [29] is however very different from our proposal. First, [29] uses a so-called *R-diode sensor* which is actually built from two MOSFETs and one resistor, while our scheme uses actual diodes. Moreover, the scheme in [29] is quite complex, and uses differential amplifiers, comparators and voting circuits to determine the output bits. Our scheme is much simpler and requires only two diodes, a capacitance and an inverter. Moreover, our scheme uses the difference of saturation currents and not bias difference. Finally, [29] requires both PMOS and NMOS devices, while our proposal can be used even with semiconductors (e.g., GaAs) not especially suited to the production of complementary transistors.

Finally, we cite the scheme of [30] that exploits the antenna effect in order to randomly break the gate oxide. This scheme is interesting because of its stability and low power consumption. However, in [17] it is noted that the over-voltage used to break the oxide could cause chip degradation.

1.2. Our contribution

In [27] the authors propose a PUC based on two complementary MOSFETs and having good intra distance 10–100 times smaller than other schemes). These performances are achieved by employing a scheme that has *one and only one* equilibrium point that is a *discontinuous function* of the saturation currents of the MOSFETs.

The scheme proposed in [27], however, has some drawbacks. First, the use of CMOS makes it difficult to "export" the PUC to non-silicon technologies like GaAs or organic semiconductors. Moreover, the intrinsic asymmetry of the scheme, due to the usage of complementary MOSFETs, makes the scheme of [27] sensitive to *local biasing* [28], that is, a local preference toward a given preferred outcome (PO), since the characteristics of the two MOSFETs depend on different process steps (e.g., *n*- and *p*-doping). Another consequence of the asymmetry is the finite *crossover temperature* [27] due to the different speed of variation of NMOS and PMOS characteristics with the temperature [27]. Finally, since at steady state both MOSFETs are in conduction, the consumption of the scheme is fairly large, although some countermeasures can be taken to partially solve this problem [27].

In this paper we propose a different scheme which preserves the main characteristic of the solution of [27] (namely, a single equilibrium point very sensitive to build-time variations), while solving the drawbacks. More precisely, the proposed scheme uses two inversely polarized diodes instead of two complementary MOSFETs. This has the following important consequences (i) the scheme requires less energy than [27] since it uses two diodes in reverse, (ii) it can be easily implemented in non-silicon technologies since it does not require complementary MOSFETs, (iii) it is intrinsically symmetric and this reduces the possibility of local bias.

2. Qualitative analysis

Fig. 1 shows the scheme proposed in this paper. Diodes D1 and D2 are *nominally* matched in the sense that they have the same inverse

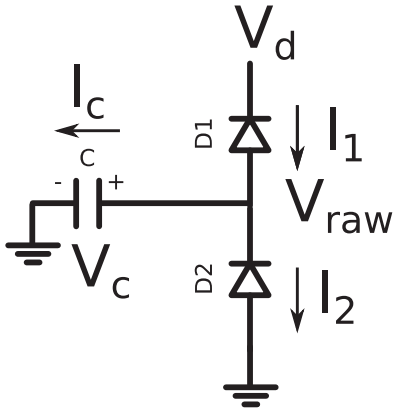

Fig. 1. The PUC proposed here.

saturation current $I_{s,1} = I_{s,2} = I_s$. Both diodes are inversely polarized, so that their currents are equal to the saturation currents. If, for example, $I_{s,1} > I_{s,2}$ the "mismatch current" $I_0 = I_{s,1} = I_{s,2}$ goes through the capacitor charging it, increasing the value of v_C and reducing the potential difference across D1. This process will continue until V_{D1} is small enough to make $I_{D1} = I_{D2}$. A similar reasoning holds for the case $I_{s,2} > I_{s,1}$.

A more precise, but still qualitative explanation of the behavior of the circuit of Fig. 1 can be given with the help of Fig. 2. Fig. 2a shows the IV characteristic of a diode with the convention shown in the top right angle (this convention is exactly the opposite of the usual one, but it is more convenient for us). By just basic algebra, it is easy to see that the curve I_C-V_C has the shape shown in Fig. 2b and it moves up and down according to the value of $I_0 = I_{s,1} - I_{s,2}$. It is clear that there is a single equilibrium point (corresponding to $i_C = 0$) which is stable since the derivative there is negative. Moreover, since the middle part is horizontal, the equilibrium position changes in a discontinuous way when I_0 moves across 0. This suggests that the scheme of Fig. 1 preserves the most interesting characteristic of the scheme of [27]: a single equilibrium point that is a discontinuous function of I_0. Therefore, the proposed PUC can be used in the same way as the PUC of [27]: the PUC is turned on and after a time $t_{\max}$ (sufficient to reach the steady state) the value of v_C is acquired and mapped to 0 or 1 depending on the fact that v_C is larger or smaller than $V_{DD}/2$. Note that the consumption of this PUC is very low since the two diodes are inversely polarized. Because of this, it is not necessary to turn off the PUC in order to reduce the consumption, unless we have a very limited power budget. This is different from what happened in [27] where the two MOSFETs were both in conduction and it was necessary to turn off the cell after reading.

3. Notation

We will denote with $I_{s,i}$ the actual reverse bias saturation current of Di, i = 1,2, with I_s their *nominal* value and with $I_0 = I_{s,1} - I_{s,2}$ their difference. If $|I_0|$ is small, we will informally say that the cell is *almost balanced*. It will turn out that $|I_0|$ can be considered as a "quality measure" of the cell, with more reliable cells having a larger value of $|I_0|$.

We will model currents $I_{s,i}$, i=1,2, as iid random variables with mean equal to the nominal value I_s and standard deviation σ_{I_s}. If a finer characterization is needed we will suppose $I_{s,i}$ Gaussian, that is, $I_{s,i} \sim \mathcal{N}(I_s, \sigma^2_{I_s})$. We will denote with $\bar{\sigma}_{I_s} \stackrel{\text{def}}{=} \sigma_{I_s}/I_s$ the coefficient of variation. It will be seen in the following that is preferable to have a large dispersion of Is, i (large σ_{I_s}).

It is more convenient to use adimensional units obtained by dividing physical values by suitable reference values. In this paper we will use the supply voltage V_{DD} as the reference for voltages, the nominal saturation current I_s as the reference for currents and C as the capacitance reference. We will also use resistance reference $\rho \stackrel{\text{def}}{=} V_{DD}/I_s$