An Alternative to Error Correction for SRAM-Like PUFs

Maximilian Hofer and Christoph Boehm

Institute of Electronics, Graz University of Technology,
maximilian.hofer@tugraz.at, christoph.boehm@tugraz.at ,
WWW home page: http://ife.tugraz.at

Abstract. We propose a new technique called stable-PUF-marking as an alternative to error correction to get reproducible (i.e. stable) outputs from physical unclonable functions (PUF). The concept is based on the influence of the mismatch on the stability of the PUF-cells' output. To use this fact, cells providing a high mismatch between their crucial transistors are selected to substantially lower the error rate. To verify the concept, a statistical view to this approach is given. Furthermore, an SRAM-like PUF implementation is suggested that puts the approach into practice.

Keywords: Physical Unclonable Functions, SRAM, Pre-Selection

1 Introduction

Due to the widespread use of Smart Cards and radio frequency identification (RFID) devices, the demand for secure identification/authentication and other cryptographic applications is continuously increasing. For this purpose a ”fingerprint” of a chip can be useful. Physical unclonable functions (PUFs) provide such an output. In 2001, Pappu et al. introduced the concept of PUFs [1]. In this approach a unique output is produced by evaluating the interference pattern of a transparent optical medium. Unfortunately, due to the way of pattern extraction, Pappu's approach turns out to be quite expensive. In [2, 3], Gassend et al. introduce physical unclonable functions in silicon. The concept utilizes manufacturing process variation to distinguish between different implementations of the same integrated circuit (IC). This is done by measuring the frequency of self-oscillating loop circuits. These frequencies differ slightly between the realizations. However, the chip area is large and the current consumption is high. Another approach is to use the initial values of SRAM cells. [4, 5] shows that there exist SRAM chips which deliver the same start-up value again and again which is the crucial property of a PUF. The best of them deliver an error rate of less than 3 %. So it seems that SRAM-like structures are feasible as dedicated PUF-cells [6].

One way to deal with errors in the PUFs' responses is to use error-correction codes (ECC) [7]. Here, redundace is added by storing parity bits during an initialization phase. These bits can be used afterwards to reconstruct the reference value. Unfortunately, efficient decoding is difficult. If the error rate is high, the runtime increases strongly [8, 9]. Other methods use statistical data of the fuzziness [10] (i.e. the degree of instability) of the PUF responses. In [10], Maes et. al. read out the response several times to collect data about the stability of the different PUF-cells. An advantage of this Soft Decision Data Helper Algorithm is that the number of PUF-cells can be reduced up to 58.4 %. A drawback is that the initialization phase needs a higher number of runs (e.g. 64 in [10]).

In this work we propose an alternative method to deal with unstable PUF-cells. The time needed for the read-out phase is reduced due to the fact that further post-processing of the PUF response becomes less complex or even needless depending on the application.

The remainder of the paper is organized as follows. Section 2 describes the idea behind the concept. In Section 3 a statistical analysis is given. Section 4 provides an approach to an implementation in silicon. Finally, section 5 concludes the paper. In the appendix some additional calculations and tables are given.

2 Idea

Figure 1 shows a CMOS SRAM-cell that can be used as a PUF-cell. A whole PUF consists of an application dependent number of such cells. We assume that the design and the layout of that PUF-cell are optimized in such a way that the PMOS transistors match and the NMOS transistors mismatch.[1] In an SRAM PUF, the output which is defined by the state of OUT after power-up, mainly depends on the threshold voltage (V_{th}) mismatch. Assuming identical initial potentials at OUT and $\overline{OUT}$, the mismatch of the NMOS transistors lead to a difference between i_1 and i_2 in the two branches of the SRAM cell. If i_2 is higher than i_1, the potential at OUT will move towards V_{SS}, the potential at $\overline{OUT}$ will move towards V_{DD}. If i_2 is lower than i_1, the cell behaves the other way round. This behavior at OUT and $\overline{OUT}$ should be an intrinsic property of the cell and should not change over time. If the mismatch is too small, the cell result will be unstable due to noise, temperature shifts, and other shifts in the working point, e.g. caused by changes in V_{DD}.

The idea is to select only the stable cells (i.e. those cells providing a high mismatch) to generate the PUF output. Before the PUF is used for the first time, during an initialization phase the stable PUF-cells are detected. These cells are marked. All the other PUF-cells are not used any longer. From now on, only stable PUF-cells generate a stable response.

This gives rise to the question of how to select the stable bits. An intuitive approach is to measure the results of a PUF-cell repeatedly and chose only those cells which always provide the same output. For various reasons this is not practicable. First of all, additional measurements must be done to get useful

[1] The mismatch's variance of the transistors can be controlled over the transistor area: Smaller area leads to higher mismatch. This means that the analog designer can influence the variance but not the individual value of the mismatch which defines the PUF-cell output.

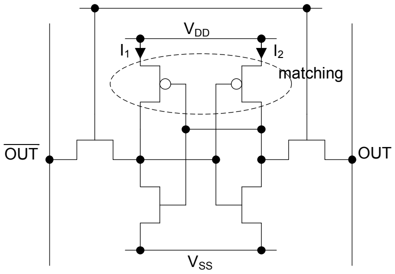


Fig. 1: Common SRAM-cell.

statistical data and thus is not feasible for an initial production test flow where measurement time has proportional impact on the product costs. Another problem is that there are cells which show temperature depending behavior. So the initial measurements would have to be done over the whole temperature range. Furthermore, the influence of aging changes the mismatch behavior [5] and could cause additional errors after some time.

Another approach to find unstable PUF-cells is to use the fact that stable cells decide faster [6]. To detect the fast flipping cells, the decision time has to be measured. In figure 2 this concept is illustrated. After a certain time t_{useful} the

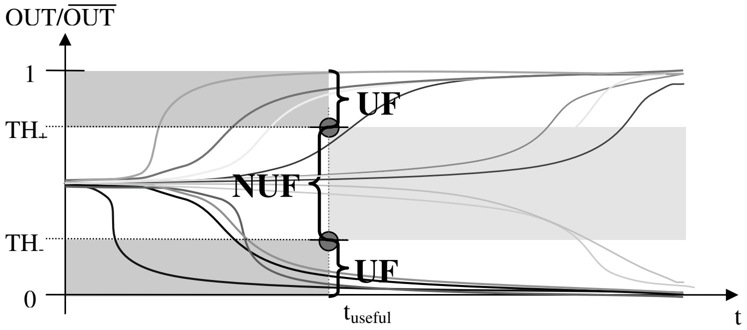


Fig. 2: Measurement of decision time (UF: useful, NUF: not useful).

cells above an upper threshold or under a lower threshold are marked as useful. All other cells which lie between the two thresholds are marked as not useful. Unfortunately, simulations show that the decision time strongly depends on the temperature. Therefore during the initialization phase a constant temperature is necessary to allow the use of an absolute time t_{useful}. Another solution to this problem could be to measure the time spans needed to reach a threshold value. The fastest cells are used. Since it may happen that the fastest cells of a chip are still not fast enough to meet the above requirements a stable behavior can not be expected in all cases.

The approach we propose in this paper is based on the selection of cells which provide a mismatch that exceeds a certain threshold. In the case of the shown SRAM-PUF, the mismatch of the NMOS transistors must be above such a threshold. In figure 3, the mismatch ΔV_{th} of two transistors is depicted schematically. Here, this distribution is assumed to be Gaussian. A positive and a negative threshold value (ΔV_{th+} and ΔV_{th-}, with $|\Delta V_{th+}| = |\Delta V_{th-}|$) are defined, which is necessary to divide the PUF-cells into three classes: the useful PUF-cells with positive mismatch (UF_+), the useful PUF-cells with negative mismatch (UF_-) and the not useful PUF-cells (NUF). In figure 3, the three sections are depicted. In the middle section, the mismatch is too small to provide a stable behavior. These bits are marked as NUF. The mismatch of the other bits is big enough to provide a stable output. Thus, the threshold value must be chosen correctly to reach an acceptable error rate. The larger the threshold value, the smaller the number of PUF-cells that are marked as stable and the smaller the error rate. Thus, to be able to provide the required number of useful cells, the number of initial PUF-cells has to be adapted to the chosen threshold value. For this reason, the threshold value is a trade-off between the ratio of the useful PUF-cells and all PUF-cells and the error rate.

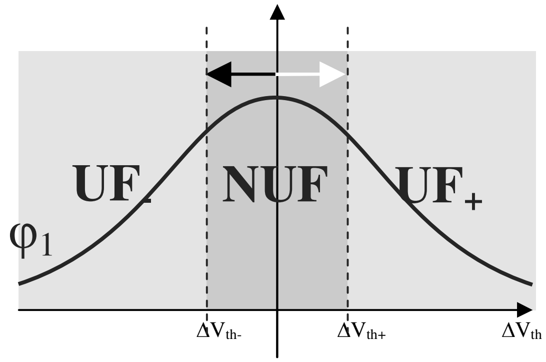


Fig. 3: The mismatch is divided in three classes: The useful PUF-cells with positive mismatch (UF_+), the useful PUF-cells with negative mismatch(UF_-) and the not useful PUFs (NUF).

One method to measure ΔV_{th} is to use a common analog to digital converter (ADC). In figure 4 a block diagram is shown. The disadvantage of this approach is the size of the ADC caused by the requirements on it. In order to get a balanced output, the ADC must have a small offset. Furthermore the ADC has to be fast and the result should not depend on the noise of the circuit.

The proposed concept to classify the cells into UF and NUF is to add a systematical V_{th} offset to the circuit (see figure 7): Two measurements per PUF-cell are needed. During the first measurement we add a negative offset. Thus the threshold is set to V_{th-}. During the second measurement we move the

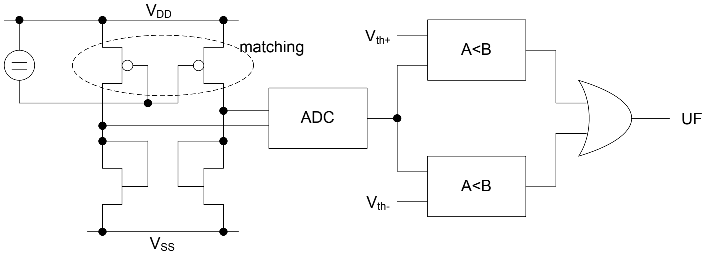


Fig. 4: Measurement of the mismatch using an ADC.

threshold to V_{th+}. This is illustrated in figure 3 denoted by the two arrows. The classification can be done as follows: If the mismatch of the transistors exceeds the threshold, the PUF-cell will provide the same output for both measurements and thus the cell is marked as useful. If the mismatch is too small, the output OUT of the cell will differ for the two measurements. The cell is marked as not useful. Problems will occur if the threshold value is chosen too big. In such a case, only a few or even no cells are marked as useful which can lead to severe problems. On the other hand, if the threshold is chosen too small, disturbances like noise will lead to output errors and make the whole pre-selection process useless.

3 Modeling and Statistical Aspects

To analyze the performance of this approach, Monte Carlo simulations are not feasible since the error rate after the pre-selection process (i.e. after the useful-PUF-marking) should be so small that the number of simulation runs to determine the error probability would exceed a tolerable number. So we prefer an analytic method to estimate the performance of the pre-selection process:

For all further analyses we assume that the distribution of the V_{th} mismatch as well as the distribution of the disturbances (noise, temperature-dependent errors, etc.) is Gaussian [11–14]. To determine the effect of the pre-selection process, we need the probability density function (PDF) $f(x)$ and its integral, the cumulative distribution function (CDF) $F(x)$ of a Gaussian:

$$f(x) = \phi_{\mu,\sigma}(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2} \tag{1}$$

$$F(x) = \Phi_{\mu,\sigma}(x) = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{x} e^{\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2} dx, \tag{2}$$

where μ is the mean and σ the variance of the Gaussian.

If there is no disturbance at the PUF-cell, the cell output will be the same whenever the PUF is read-out. In this case the output would be zero for all PUF-cells having a negative ΔV_{th} and one for all cells with positive ΔV_{th} (see figure

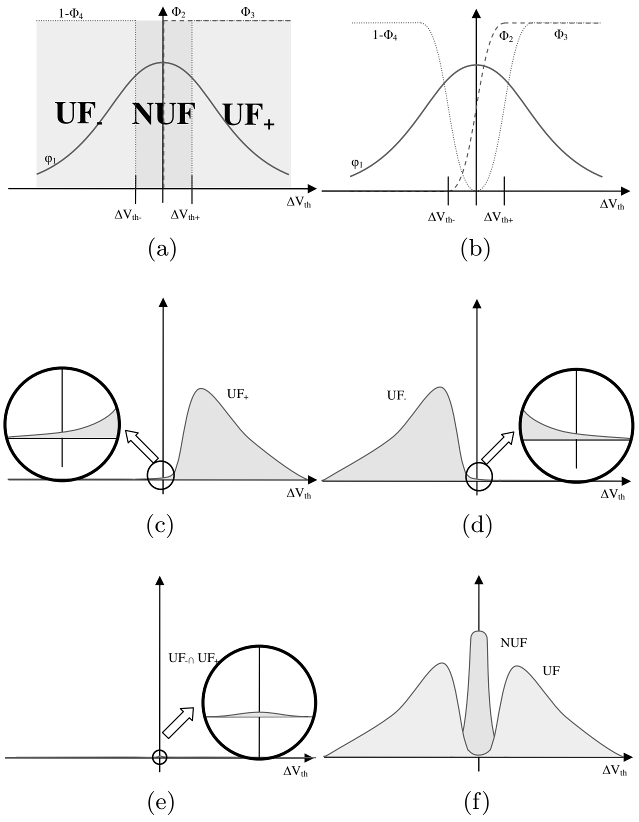


Fig. 5: (a) Ideal distributions $\Phi_1 - \Phi_4$.(b) Real distributions $\Phi_1 - \Phi_4$. (c) Useful positive PUF-cells(UF+). (d) Useful negative PUF-cells(UF-). (e) PUF-cells which occur in UF_+ and UF_-. (f) Useful PUF-cells(UF) and not-useful PUF-cells(NUF).

5a). If there are disturbances due to noise, temperature, etc., it may happen that if the mismatch is sufficiently small or the disturbance sufficiently large, the decision is defined by this disturbance. That effect can be seen in figure 5b where Φ_2 shows the mean output depending on ΔV_{th} taking the distribution of the disturbance into account. At $\Delta V_{th} = 0$ the mean output equals 0.5. The same curve but biased with the threshold ΔV_{th-} and ΔV_{th+} depict Φ_4 and Φ_3. ϕ_1 is the distribution of the mismatch. After selecting the useful PUF-cells, the error rate can be decreased significantly. Figures 5c and 5d show the product of Φ_3 and ϕ_1, and the product of $(1 - \Phi_4)$ and ϕ_1 respectively. These curves depict the distribution of being selected as useful including disturbances, the distribution of the V_{th} mismatch and a certain V_{th} offset. Hence the figures represent the number of selected PUF-cells. Figure 5e shows those cells that are selected twice, i.e. that are declared to be useful for both offsets. To get correct results these double-selections have to be compensated for in the analysis. Figure 5f shows the distributions of selected and not selected cells.

Since $\sigma_2 = \sigma_3 = \sigma_4 = \sigma$, $\mu_1 = \mu_2 = 0$, and $\mu_3 = -\mu_4$ can be assumed, we get the following equation for the number of useful PUF cells α (see appendix):

$$\begin{aligned}\alpha = 1 - \frac{1}{\sigma_1 2\pi} \int_{\infty}^{-\infty} e^{-\frac{1}{2}\left(\frac{V_{th}}{\sigma_1}\right)^2} \Bigg[\frac{1}{\sigma} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu}{\sigma}\right)^2} dV'_{th} + \\ - \frac{1}{\sigma} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu}{\sigma}\right)^2} dV'_{th} + \frac{2}{\sigma^2 \sqrt{2\pi}} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu}{\sigma}\right)^2} dV'_{th} \cdot \\ \cdot \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu}{\sigma}\right)^2} dV'_{th} \Bigg] \, dV_{th} \qquad (3)\end{aligned}$$

The error rate e at $\mathit{\Delta} V_{th}$ can be derived using the following equation (see appendix):

$$e(\mathit{\Delta} V_{th}) = \phi_1 \mathit{\Phi}_2 - \phi_1 \mathit{\Phi}_2 \mathit{\Phi}_4 - \phi_1 \mathit{\Phi}_2 \mathit{\Phi}_3 \mathit{\Phi}_4 + \phi_1 \mathit{\Phi}_3 - \phi_1 \mathit{\Phi}_3 + \phi_1 \mathit{\Phi}_3 \mathit{\Phi}_4 - \mathit{\Phi}_2 \phi_1 \mathit{\Phi}_3 \mathit{\Phi}_4, \quad (4)$$

where all ϕ_i and $\mathit{\Phi}_i$ are evaluated at $\mathit{\Delta} V_{th}$.

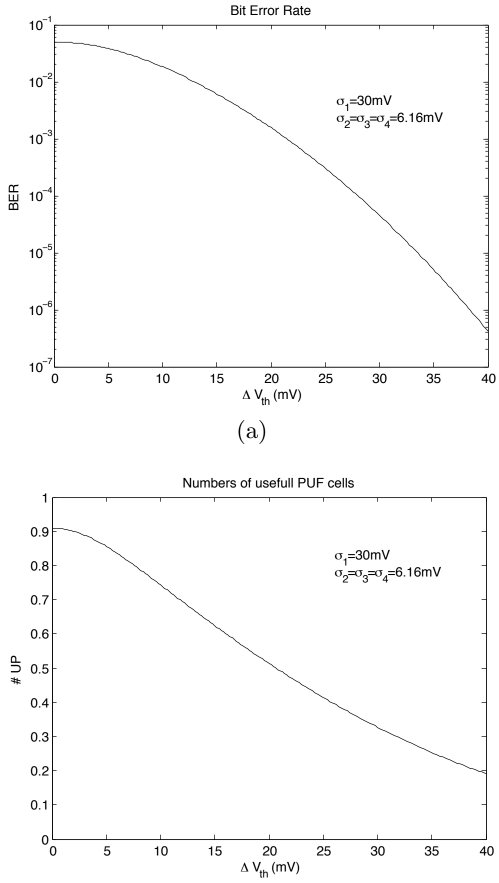
Example The standard deviation of $\mathit{\Delta} V_{th}$ is 30 mV , the standard deviation of $\phi_{2,3,4}$ equals 6.16 mV. This coresponds to an error-rate of 5%.[2] In figure 6 the error rate and the ratio of useful PUF-cells α are shown in a diagram. It can be seen that selecting for example the best 50 % can decrease the error rate significantly. A table of different examples is shown in appendix B.

4 Implementation

Different circuits are possible to implement the approach described above. One of them is presented. To understand the circuit we consider an ordinary SRAM-cell depicted in figure 7. We assume that P_1 and P_2 match. Hence, the decision depends on the mismatch of the threshold voltage of N_1 and N_2 denoted $\mathit{\Delta} V_{th}$. To mark the cells as introduced in section 2, we have to add an additional voltage source at the gate of one of the NMOS transistors to provide the bias we need for the threshold (see figure 7a). Since the implementation of such a circuit is difficult, the preferred way is to use its Norton equivalent - a current source - in parallel to one of the NMOS transistors (see figure 7b).

From figure 8, the equivalence of the two circuits can be seen. The character-

[2] We meassured an error-rate of 4% in a dedicated PUF-cell in the temperature range from $0 - 80°C$. So this is a rather pessimistic value.



(a)

(b)

Fig. 6: a) Error rate e. (b) Ratio of useful PUF-cells α against $\mu_{3,4}$.

istics of two different diode-loaded MOSFETS are shown. For the same V_{GS} and different threshold voltages, the amount of current through the transistors will be different. Thus, additional current at one of the branches of the SRAM-cell acts as a mismatch of V_{th}.

The circuit depicted in figure 9 is a practical implementation of the approach. During the first phase N_7 is switched-off. N_3, N_4 and P_1, P_2 are building a SRAM similar circuit. N_2 acts as a current limiter for this circuit. The circuit is designed, that the mismatch between P_1 and P_2 is small and should not affect the result. Due to the fact that the transistors N_3 and N_4 are diode loaded, the circuit does not flip as fast as the SRAM depicted in figure 1. During the second phase, N_7 is switched-on and the circuit flips completely to one direction. The bias transistors which are used for the PUF-cell selection (P_3 and P_4) are used

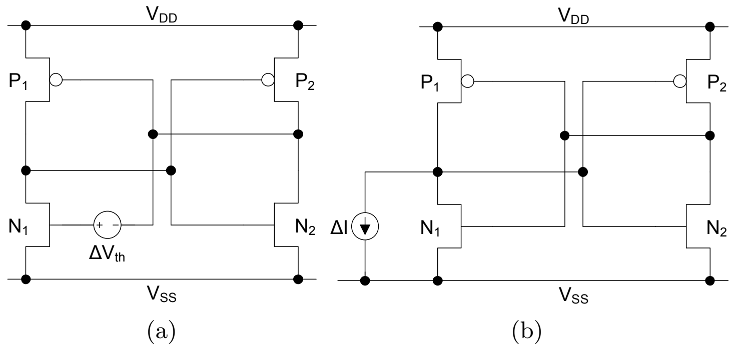


Fig. 7: (a) SRAM-cell with additional voltage source at the gate of N_1; (b) SRAM-cell with additional current source at the drain of N_1.

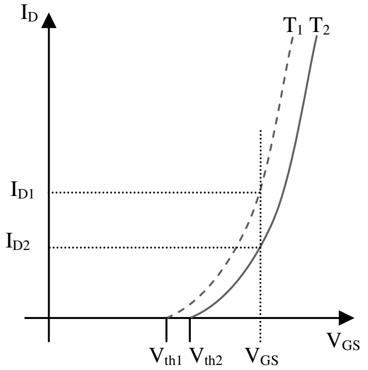


Fig. 8: Characteristics of two MOSFETS having different V_{th}.

during the first phase and switched-off during the second phase (P_7 and P_8 are switched-on; P_5 and P_6 are switched-off).

If we want to add a fictive negative offset voltage at the transistor N_4, P_8 is opened and P_6 is closed. Thus, the transistor P_4 is in parallel with transistor P_2. A higher current passes N_4. The same can be done on the right branch (P_7, P_5, P_3 and N_3). The truth table for the control of the transistors P_5, P_6, P_7, and P_8 is shown in table 1.

A further improvement of this circuit can be achieved by separating the mismatching transistors N_3 and N_4 from the evaluation circuit consisting of the transistors N_5 to N_7 and P_1 to P_8. Additionally, two transistors are required to connect each cell to the evaluation circuit. So, one PUF-cell consists of only five transistors as depicted in figure 10. The cells can be selected sequentially and evaluated using the same evaluation circuit (i.e. sense amplifier). Thus, the area of one PUF-cell is scaled-down to about the size of a common SRAM-cell. For the particular topology that is about 100F^2 ('minimum featured size').

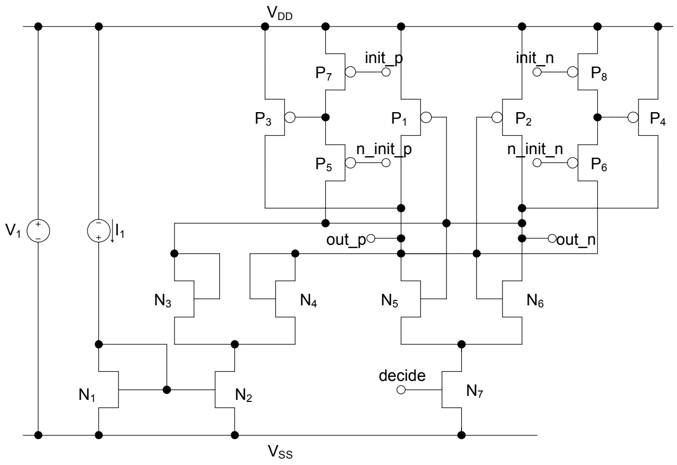


Fig. 9: Implementation example of an SRAM-like PUF with pre-selection transistors P_3 and P_4.

function	n_{th}	p_{th}	$init_p$	$ninit_p$	$init_n$	$ninit_n$
no threshold	0	0	0	1	0	1
p threshold	0	1	1	0	0	1
n threshold	1	0	0	1	1	0

Table 1: Control of the transistors P_5, P_6, P_7, P_8 for adding the current bias to the circuit.

In such a circuit it could happen that the mismatch of the evaluation circuit influences the decision. Due to this fact, cells using the same evaluation circuit could tend to output the same value. To reduce the influence of an asymmetric sense amplifier, the number of PUF-cells which use the same evaluation logic should be chosen carefully.

The whole structure diagram of the system is depicted in figure 11. There are two modes: One for the initialization phase and another one for the nominal operation. The addresses of the useful cells are stored in a non-volatile memory (NVM). During the initialization phase this memory is filled with data: The outputs of the single PUF-cells after adding both bias currents are compared. If the output stays constant for both bias values, the address of the PUF-cell is written into the NVM. The address of the NVM is incremented and the next PUF-cell is tested. This is done until the necessary number of outputs is reached. If not enough useful cells are provided an error occurs and the PUF must be considered to be defect. This indicates that the mismatch between the transistors is too small or that the ratio of required PUF-cells and available PUF-cells is too high. Possible solutions to this problem are to increase the number of PUF-cells

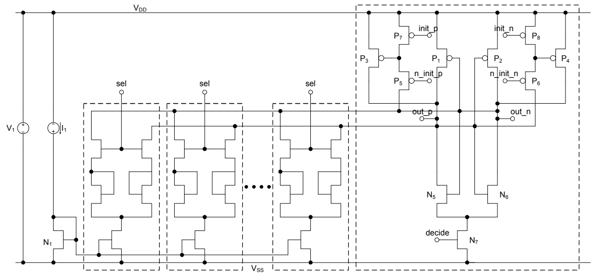


Fig. 10: PUF-cells with shared sense amplifier.

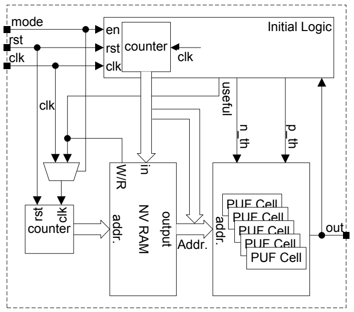


Fig. 11: Structure diagram with initialization logic.

or to reduce the upper and lower threshold values $\varDelta V_{th-}$ and $\varDelta V_{th+}$. During the nominal mode, the PUF-cells stored in the NVM are read-out.

5 Conclusion

In this paper we introduced a pre-selection process for SRAM-like PUFs which can be implemented with little effort. We demonstrated that error-rates of 10E-6 are achievable. Due to the smaller error rate, using the marking procedure makes post-processing less complex or even unnecessary depending on the application. Hence, the area of the digital part of the circuit can be reduced. Furthermore, the smaller error rate leads to less power consumption and faster read-out. The additional effort caused by the initialization phase is small since the whole process can be done at one temperature and only two read-out cycles are necessary to separate the stable and the unstable PUF-cells.

References

1. Pappu, R., Recht, R., Taylor, J., Gershenfeld, N.: Physical one-way function. SCIENCE, 297(5589), 2026–2030 (2002)

2. Gassend, B., Clarke, D., Marten van Dijk, Devadas, S.: Silicon physical random functions CCS '02: Proceedings of the 9th ACM conference on Computer and communications. security, 148-160, (2002)
3. Blaise, G., Daihyun, L., Dwaine, C., Marten van Dijk, and Srinivas, D.: Identification and a2thentication of integrated circuits. Concurrency Computation: Pract. Exper., 16:1077-1098, (2004)
4. Guajardo, J., Kumar, S.S., Schrijen, G.-J.,Tuyls, P.: FPGA Intrinsic PUFs and Their Use for IP Protection. Cryptographic Hardware and Embedded Systems - CHES 200: 63–80, (2007)
5. Boehm, C., Hofer, M.: Using SRAMs as Physical Unclonable Functions. Proceedings of the 17th Austrian Workshop on Microelectronics - Austrochip: 117–122, (2009)
6. Ying S., Holleman, J., Otis, B.P.: A Digital 1.6 pJ/bit Chip Identification Circuit Using Process Variations. IEEE Journal of Solid-State Circuits 43(1): 69–77, (2008)
7. Dodis, Y.: Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. Proceedings of Eurocrypt 2007: 523–540, (2007)
8. Hong, J., Vitterli, M.: Simple Algorithms for BCH Decoding. IEEE Transactions of Communications, vol.43: 2324-233, (1995)
9. Boesch C., Guajardo, J., Sadeghi, A.R., Shokrollahi, J., Tuyls, P.: Efficient Helper Data Key Extractor on FPGAs. Cryptographic Hardware and Embedded Systems CHES 2008: 181–197, (2008)
10. Maes, R. ,Tuyls, P., Verbauwhede, I.: Low-Overhead Implementation of a Soft Decision Helper Data Algorithm for SRAM PUFs. Proceedings of the 11th International Workshop on Chryptographic Hardware and Embedded Systems - CHES 2009: 332–347, (2009)
11. Pelgrom, M., Duinmaijer, A., Welbers, A.: Matching Properties of MOS-Transistors. IEEE Journal of Solid-State Circuits, vol.24: 1433-1440, (1989)
12. Pelgrom, M.J.M. ,Tuinhout, H.P., Vertregt, M.: Transistor matching in analog CMOS applications. Electron Devices Meeting, 1998. IEDM '98 Technical Digest., International: 915-918, (1998)
13. Mizuno, T., Okumtura, J., Toriumi, A.: Experimental study of threshold voltage fluctuation due to statistical variation of channel dopant number in MOSFET's IEEE Transactions on Electron Devices, vol.41: 2216–2221, (1994)
14. Tsividis, Y.: The MOS Transistor New York: Oxford University Pres, (1999)

A Calculations

Ratio of Useful PUF-Cells α: Partial probability of occurrence of selected PUF cells depending on $\mathit{\Delta} V_{th}$ (see figure 7(c) and 7(d)):[3]

$$UF_{+} = \phi_1 \mathit{\Phi}_3 \tag{5}$$

$$UF_{-} = \phi_1 (1 - \mathit{\Phi}_4) \tag{6}$$

Probability of occurrence PUF-cells being selected twice depending on $\mathit{\Delta} V_{th}$ (see figure 7(e)):

$$UF_{+} \cap UF_{-} = \phi_1 \mathit{\Phi}_3 (1 - \mathit{\Phi}_4) \tag{7}$$

[3] The results of this section depend on the threshold values V_{th+} andV_{th-}.

Total probability of occurrence depending on $\mathit{\Delta} V_{th}$:

$$\begin{aligned} UF &= UF_{+} + UF_{-} - 2(UF_{+} \cap UF_{-}) = \\ &= \phi_1[\mathit{\Phi}_3 + (1 - \mathit{\Phi}_4) - 2\mathit{\Phi}_3(1 - \mathit{\Phi}_4)] = \\ &= \phi_1[1 - \mathit{\Phi}_4 - \mathit{\Phi}_3 + 2\mathit{\Phi}_3\mathit{\Phi}_4] \end{aligned} \tag{8}$$

From UF the ratio of useful PUF-cells α can be determined:

$$\begin{aligned} \alpha &= \int_{\infty}^{-\infty} UF \, dV_{th} = \\ &= \int_{\infty}^{-\infty} \frac{1}{\sigma_1\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{V_{th}-\mu_1}{\sigma_1}\right)^2} \Bigg[1 - \frac{1}{\sigma_4\sqrt{2\pi}} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu_4}{\sigma_4}\right)^2} dV'_{th} + \\ &\quad - \frac{1}{\sigma_3\sqrt{2\pi}} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu_3}{\sigma_3}\right)^2} dV'_{th} + \frac{2}{\sigma_3\sqrt{2\pi}} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu_3}{\sigma_3}\right)^2} dV'_{th} \cdot \\ &\quad \cdot \frac{1}{\sigma_4\sqrt{2\pi}} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu_4}{\sigma_4}\right)^2} dV'_{th} \Bigg] \, dV_{th} = \\ &= 1 - \frac{1}{\sigma_1 2\pi} \int_{\infty}^{-\infty} e^{-\frac{1}{2}\left(\frac{V_{th}-\mu_1}{\sigma_1}\right)^2} \Bigg[\frac{1}{\sigma_4} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu_4}{\sigma_4}\right)^2} dV'_{th} + \\ &\quad - \frac{1}{\sigma_3} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu_3}{\sigma_3}\right)^2} dV'_{th} + \frac{2}{\sigma_3\sigma_4\sqrt{2\pi}} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu_3}{\sigma_3}\right)^2} dV'_{th} \cdot \\ &\quad \cdot \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu_4}{\sigma_4}\right)^2} dV'_{th} \Bigg] \, dV_{th} \end{aligned} \tag{9}$$

In general we can assume that $\sigma_2 = \sigma_3 = \sigma_4 = \sigma$, $\mu_1 = \mu 2 = 0$, and $\mu_3 = -\mu_4$. Then α becomes:

$$\begin{aligned} \alpha = 1 &- \frac{1}{\sigma_1 2\pi} \int_{\infty}^{-\infty} e^{-\frac{1}{2}\left(\frac{V_{th}}{\sigma_1}\right)^2} \Bigg[\frac{1}{\sigma} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu}{\sigma}\right)^2} dV'_{th} \; + \\ &- \frac{1}{\sigma} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu}{\sigma}\right)^2} dV'_{th} + \frac{2}{\sigma^2\sqrt{2\pi}} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu}{\sigma}\right)^2} dV'_{th} \cdot \\ &\cdot \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu}{\sigma}\right)^2} dV'_{th} \Bigg] \, dV_{th} \end{aligned} \tag{10}$$

Ratio of Not-Useful PUF-Cells β: To verify the result of α, the ratio β of not selected PUF-cells is determined as well:

$$\beta = \int_{\infty}^{-\infty} NUF \; dV_{th} \tag{11}$$

$$\begin{aligned} NUF &= \phi_1[(1-\Phi_3)(1-(1-\Phi_4)+\Phi_3(1-\Phi_4))] \\ &= \phi_1[(1-\Phi_3)(\Phi_4)+\Phi_3(1-\Phi_4))] \\ &= \phi_1[\Phi_4-\Phi_4\Phi_3+\Phi_3-\Phi_4\Phi_3))] \\ &= \phi_1[\Phi_4+\Phi_3-2\Phi_4\Phi_3))] \end{aligned} \tag{12}$$

$$\begin{aligned} \beta = &\int_{\infty}^{-\infty} \frac{1}{\sigma_1\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{V_{th}-\mu_1}{\sigma_1}\right)^2} \left[\frac{1}{\sigma_3\sqrt{2\pi}} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu_3}{\sigma_3}\right)^2} dV'_{th} + \right. \\ &+ \frac{1}{\sigma_4\sqrt{2\pi}} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu_4}{\sigma_4}\right)^2} dV'_{th} - \frac{2}{\sigma_3\sqrt{2\pi}} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu_3}{\sigma_3}\right)^2} dV'_{th} \cdot \\ &\left. \cdot \frac{1}{\sigma_4\sqrt{2\pi}} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu_4}{\sigma_4}\right)^2} dV'_{th} \right] dV_{th} = \\ = &\frac{1}{\sigma_1 2\pi} \int_{\infty}^{-\infty} e^{-\frac{1}{2}\left(\frac{V_{th}-\mu_1}{\sigma_1}\right)^2} \left[\frac{1}{\sigma_3} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu_3}{\sigma_3}\right)^2} dV'_{th} + \right. \\ &+ \frac{1}{\sigma_4} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu_4}{\sigma_4}\right)^2} dV'_{th} - \frac{2}{\sigma_3\sigma_4\sqrt{2\pi}} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu_3}{\sigma_3}\right)^2} dV'_{th} \cdot \\ &\left. \cdot \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu_4}{\sigma_4}\right)^2} dV'_{th} \right] dV_{th} \end{aligned} \tag{13}$$

In general we can assume that $\sigma_2 = \sigma_3 = \sigma_4 = \sigma$, $\mu_1 = \mu 2 = 0$, and $\mu_3 = -\mu_4$. Thus, β becomes:

$$\begin{aligned} \beta = &\frac{1}{\sigma_1\sigma 2\pi} \int_{\infty}^{-\infty} e^{-\frac{1}{2}\left(\frac{V_{th}}{\sigma_1}\right)^2} \left[\int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu}{\sigma}\right)^2} dV'_{th} + \right. \\ &+ \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu_4}{\sigma_4}\right)^2} dV'_{th} - \frac{2}{\sigma} \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu}{\sigma}\right)^2} dV'_{th} \cdot \\ &\left. \cdot \int_{-\infty}^{V_{th}} e^{-\frac{1}{2}\left(\frac{V'_{th}-\mu}{\sigma}\right)^2} dV'_{th} \right] dV_{th} \end{aligned} \tag{14}$$

Check: $1 = \alpha + \beta$

Estimation of the Error Rate e: An error occurs, if one of the PUF-cells which were marked useful provides the wrong output. Like the total ratio of selected PUFs, the total error $e(\varDelta V_{th})$ is the sum of the two partial errors $e_-(\varDelta V_{th})$ and $e_+(\varDelta V_{th})$. The following errors are evaluated at a certain $e(\varDelta V_{th})$:

$$\begin{aligned} e_-(\varDelta V_{th}) &= \frac{1}{\alpha}\varPhi_2[UF_- - (UF_+ \cap UF_-)] = \\ &= \frac{1}{\alpha}\varPhi_2[\phi_1(1-\varPhi_4) - \phi_1\varPhi_3(1-\varPhi_4)] \end{aligned} \tag{15}$$

$$\begin{aligned} e_+(\varDelta V_{th}) &= \frac{1}{\alpha}(1-\varPhi_2)[UF_+ - (UF_+ \cap UF_-)] = \\ &= \frac{1}{\alpha}(1-\varPhi_2)[\phi_1\varPhi_3 - \phi_1\varPhi_3(1-\varPhi_4)], \end{aligned} \tag{16}$$

where $\frac{1}{\alpha}$ is a normalization factor.

$$\begin{aligned} e(\varDelta V_{th}) &= e_+(\varDelta V_{th}) + e_-(\varDelta V_{th}) = \\ &= \frac{1}{\alpha}(1-\varPhi_2)[\phi_1\varPhi_3 - \phi_1\varPhi_3(1-\varPhi_4)] + \\ &\quad + \frac{1}{\alpha}\varPhi_2[\phi_1(1-\varPhi_4) - \phi_1\varPhi_3(1-\varPhi_4)] = \\ &= \frac{1}{\alpha}\left\{[\phi_1\varPhi_2 - \phi_1\varPhi_2\varPhi_4 - \phi_1\varPhi_2\varPhi_3 + \phi_1\varPhi_2\varPhi_3\varPhi_4] + \right. \\ &\quad \left. + [\phi_1\varPhi_3 - \phi_1\varPhi_3(1-\varPhi_4)] - \varPhi_2\phi_1\varPhi_3 + \varPhi_2\phi_1\varPhi_3(1-\varPhi_4)\right\} = \\ &= \frac{1}{\alpha}\left\{\phi_1\varPhi_2 - \phi_1\varPhi_2\varPhi_4 - \phi_1\varPhi_2\varPhi_3\varPhi_4 + \phi_1\varPhi_3 - \phi_1\varPhi_3 + \phi_1\varPhi_3\varPhi_4 - \right. \\ &\quad \left. - \varPhi_2\phi_1\varPhi_3 + \varPhi_2\phi_1\varPhi_3 - \varPhi_2\phi_1\varPhi_3\varPhi_4\right\} \end{aligned} \tag{17}$$

To get the error e over all $e(\varDelta V_{th})$, $e(\varDelta V_{th})$ has to be integrated over all $\varDelta V_{th}$:

$$e = \int_{\infty}^{-\infty} e(\varDelta V_{th})\, d\varDelta V_{th} \tag{18}$$

B Numerical Examples

Table 2 shows some numeric examples for α and e. The number of useful PUF-cells depends mainly on the ratio $\frac{\sigma_1}{\mu_{3,4}}$. The main factors for the error are $\sigma_{2,3,4}$ and $\mu_{3,4}$. $\sigma_1$influences the error rate only marginally. Table 3 shows e in dependence of $\mu_{3,4}$.

num	σ_1	$\sigma_2, \sigma_3, \sigma_4$	$\mu_3 = \mu_4$	α	e
1	30 mV	1 mV (≈ 0.7%*)	5 mV	0.8677	2.19E-06
2	30 mV	1 mV (≈ 0.7%*)	10 mV	0.7390	¡1e-12
3	30 mV	2 mV (≈ 1.5%*)	10 mV	0.7394	5.09E-6
4	30 mV	2 mV (≈ 1.5%*)	20 mV	0.5059	¡1e-12
5	30 mV	5 mV (≈ 4%*)	10 mV	0.7422	0.0087
6	30 mV	5 mV (≈ 4%*)	20 mV	0.5108	2.39E-4
7	30 mV	5 mV (≈ 4%*)	40 mV	0.1884	1.03E-9

Table 2: Examples for the error rate e and the ratio of useful PUF-cells α. *The number in the brackets shows the BER without any pre-selection.

$\mu_{3,4}$(mV)	e	α	$\mu_{3,4}$(mV)	e	α
0	4.9965E-2	0.909	26	2.1295E-4	0.396
1	4.9435E-2	0.907	27	1.4701E-4	0.378
2	4.7882E-2	0.9	28	1.0037E-4	0.361
3	4.5412E-2	0.889	29	6.7765E-5	0.344
4	4.2189E-2	0.874	30	4.5242E-5	0.327
5	3.8415E-2	0.856	31	2.9867E-5	0.311
6	3.4307E-2	0.836	32	1.9495E-5	0.296
7	3.0078E-2	0.814	33	1.2581E-5	0.281
8	2.5917E-2	0.791	34	8.027E-6	0.267
9	2.1971E-2	0.767	35	5.0631E-6	0.253
10	1.8347E-2	0.743	36	3.1571E-6	0.24
11	1.5109E-2	0.719	37	1.9460E-6	0.227
12	1.2282E-2	0.695	38	1.1858E-6	0.215
13	9.8629E-3	0.671	39	7.1416E-7	0.203
14	7.8298E-3	0.648	40	4.2516E-7	0.192
15	6.1474E-3	0.624	41	2.5017E-7	0.181
16	4.7749E-3	0.601	42	1.4549E-7	0.17
17	3.6698E-3	0.579	43	8.363E-8	0.16
18	2.7909E-3	0.557	44	4.7509E-8	0.151
19	2.1004E-3	0.535	45	2.6674E-8	0.142
20	1.5641E-3	0.514	46	1.4800E-8	0.133
21	1.1525E-3	0.493	47	8.1156E-9	0.125
22	8.4015E-4	0.473	48	4.3978E-9	0.117
23	6.0592E-4	0.453	49	2.3550E-9	0.11
24	4.3229E-4	0.433	50	1.2462E-9	0.103
25	3.0507E-4	0.414			

Table 3: Numeric examples of the error rate e and the ratio of useful PUF-cells α in dependence of $\mu_{3,4}(\sigma_1 = 30\,\mathrm{mV}, \sigma_{2,3,4} = 6, 16$ mV). Without any pre-selection ($\mu_{3,4} = 0$mV) we get an error-rate of about 5%.