View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by idUS. Depósito de Investigación Universidad de Sevilla

Reducing bit flipping problems in SRAM physical unclonable functions for chip identification

S. Eiroa[1,2], J. Castro[1,2], M. C. Martínez-Rodríguez[1,2], E. Tena[1,2], P. Brox[2], I. Baturone[1,2]
[1]Dept. Electronics and Electromagnetism (University of Seville)
[2]Microelectronics Institute of Seville (IMSE-CNM-CSIC) Seville, Spain
{eiroa,casram,macarena,erica,brox,lumi}@imse-cnm.csic.es

***Abstract*—Physical Unclonable functions (PUFs) have appeared as a promising solution to provide security in hardware. SRAM PUFs offer the advantage, over other PUF constructions, of re-using resources (memories) that already exist in many designs. However, their intrinsic noisy nature produces the so called bit flipping effect, which is a problem in circuit identification and secret key generation. The approaches reported to reduce this effect usually resort to the use of pre- and post-processing steps (such as Fuzzy Extractor structures combined with Error Correcting Codes), which increase the complexity of the system. This paper proposes a pre-processing step that reduces bit flipping problems without increasing the hardware complexity. The proposal has been verified experimentally with 90-nm SRAMs included in digital application specific integrated circuits (ASICs).**

***Index Terms*—SRAM PUFs, hardware security, IC identification**

I. INTRODUCTION

Physical Unclonable Functions [1] have appeared as a promising solution to obtain identifiers (IDs) and cryptographic keys to be used in hardware security applications. They exploit fabrication process variability that makes each device unique and difficult to be cloned. The idea is to map a set of challenges to a set of responses that can only be evaluated with the original physical system. Different types of PUFs have been reported along last decades [2]. In SRAM-based PUFs, the challenges are the memory cells to be read and the responses are the start-up values provided by those cells. SRAM PUFs are based on cross-coupled circuits (CMOS inverters) that, once powered up, have two different stable operating points and one unstable point. If the memory cell is not driven by any input, the slight differences (threshold voltage mismatching) between the two ideally symmetrical parts (the inverters) motivate the cell to go more often to one of the stable states. Every memory cell yields one response bit that can be used to generate the bit string of an ID or a cryptographic key. The advantage of SRAM PUFs is that SRAMs already exist in most of digital designs. First implementations of SRAM PUFs were directed to be used in FPGAs [3]. Lately, their use has been reported in 65- and 90-nm integrated circuits [4][5]. The behavior of SRAM cells has been studied to generate true random numbers, identifiers, and secret keys for cryptographic algorithms [3]-[6].

In order to use PUFs for IDs or secret key generation, some statistical requirements should be met to ensure enough level of uniqueness (for security) and reproducibility (for reliability). These requirements can be established by means of the following measures:

• The inter-class Hamming Distance (HD), which represents the difference between two n-bit responses (R and R') of different PUFs to the same challenge. This distance measures the PUF uniqueness. It can be expressed as follows:

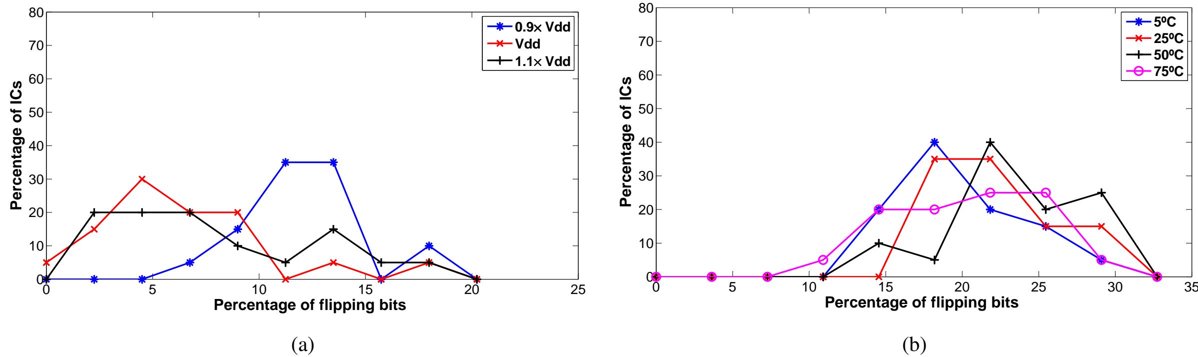
$$Fractional\ inter-class_HD = \frac{HD(R,R')}{n} \quad (1)$$

• The intra-class Hamming Distance (HD), which represents the difference between two n-bit responses (R_i and R_j) of one PUF to the same challenge. This distance measures the PUF reliability. It can be described as follows:

$$Fractional\ intra-class_HD = \frac{HD(R_i,R_j)}{n} \quad (2)$$

Ideally, for IDs and secret key generation, fractional inter-class Hamming Distances should be 0.5 and intra-class Hamming Distances should be 0. However, the intrinsic noisy nature of PUFs causes that the bits provided by the PUF are not always the same but change under the same challenge from one use to another, which is known as bit flipping effect [4] [5]. This is a problem because it decreases both the intended reliability and uniqueness. In order to solve it, several approaches have been reported in the literature. Post-processing steps, such as the use of Fuzzy Extractor or Helper Data algorithms are employed in [3] [7], the latter work also including a pre-processing step in order to obtain and store the error probability of each bit. Such steps increase the complexity and cost of the resulting hardware. Other works, such as [8], propose the use of specific SRAM bitcells, which require full-custom schemes instead of exploiting conventional SRAMs.

This work presents the test of PUFs based on TSMC 90-nm low power dual-port SRAMs embedded into an integrated circuit designed to nonlinear control applications. Bit flipping effect is analyzed as well as the sensitivity of SRAM PUF response to temperature and power supply variations. A pre-processing step that does not require additional hardware nor specific SRAM bitcells is proposed to reduce the bit flipping problem. The paper is structured as follows. Section II is dedicated to briefly describe evaluation of SRAM PUFs in TSMC 90-nm ASICs. Section III proposes a procedure to reduce bit flipping problems in SRAM PUFs. Finally conclusions are presented in Section IV.



(a) (b)

Figure 1. Bit flipping effect measured on 168-bit responses

II. Evaluation of TSCM 90-nm SRAM PUFs in ASICs

As many other digital integrated circuits, an ASIC devoted to nonlinear control (designed by some of the authors) includes embedded SRAMs as building blocks of its architecture. In particular, the ASICs tested in this work include TSMC 90-nm low-power dual-port SRAMs to program the parameters that define the nonlinear control law provided as output. The ASIC has been designed in such a way that allows exploiting the SRAM blocks as SRAM PUFs that generate bitstrings to given challenges based on power-up values characteristics of the memory cells. Hence, different evaluations have been carried out, described in the following.

The bit flipping effect has been measured on 20 ASIC samples. The 168 bits provided by 14 words of 12 bits have been registered from the SRAM when the IC was powered up. The measurements have been performed 20 times with each sample, with different values of temperature and voltage supply. As claimed in [6], SRAM is subject to a phenomenom known as data remanence, which means that the memory retains its content during several seconds after being powered-down. In our analysis, in order to ensure the lost of any previously stored data in the SRAM, the samples were kept unpowered during time intervals that ranged from 25 to 30 seconds. Figure 1 summarizes the percentages of IC samples versus the percentages of bits that change from one measurement to another (taken the first measurement as reference). It can be seen how temperature has more influence than power supply on bit flipping. Ideally for generating identifiers and secret keys, bit flipping should be 0%. In the measurements shown in Figure 1, up to 33 % of the bits may suffer from bit flipping.

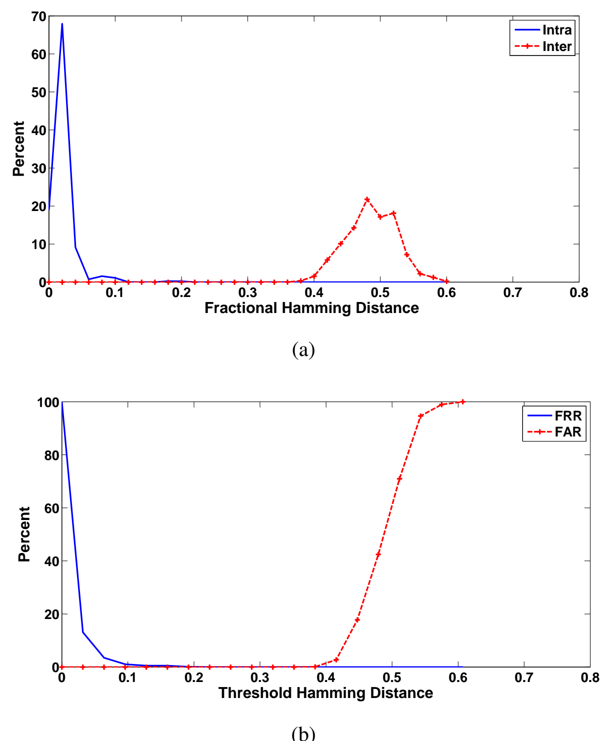
As happens in biometric identification of persons, certain level of noise is allowed in the identifiers. A commonly used metric to determine the quality of a biometric identification process is to evaluate the values of the False Acceptation Rate (FAR) and False Rejection Rate (FRR). The ideal situation is to find a threshold so that both FAR and FRR are zero. The 20 measurements of 168 bits provided by the SRAM PUFs in the 20 ICs working in the nominal case of 25°C and 1.2V of Vdd have been processed to obtain the FAR and FRR curves and the distribution of the genuine and fake populations, as shown in Figure 2.

To better characterize the use of SRAM PUFs for chip identification, the influence of different power supply and temperature conditions has been analyzed.

A. *Power supply variations influence*

The effect of the power supply variations over the SRAM start-up values was measured in the 20 ICs organized in three groups. The 168 bits of each SRAM PUF were measured 20 times for each Vdd value (the temperature was fixed to the nominal value). Groups and Vdd values defined were the following:

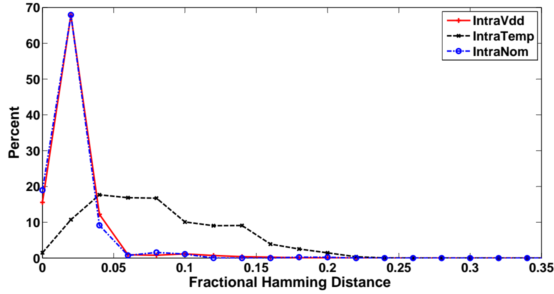
- First group (8 ICs): ICs at seven Vdd values between 1.1*Vdd and 0.9*Vdd: 1.32V, 1.28V, 1.24V, 1.2V, 1.16V, 1.12V, and 1.08V.



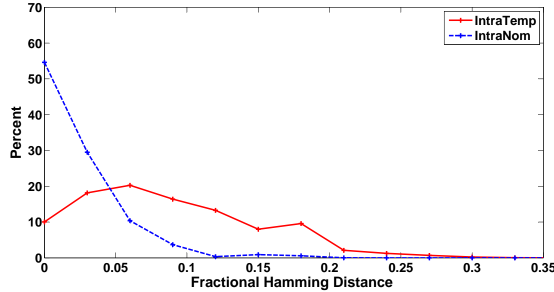
(a)

(b)

Figure 2. For IDs of 168 bits and nominal situation: (a) Genuine and fake populations. (b) False Acceptation Rate (FAR) and False Rejection Rate (FRR)

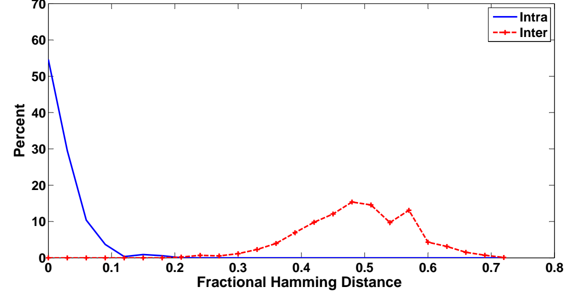


(a)

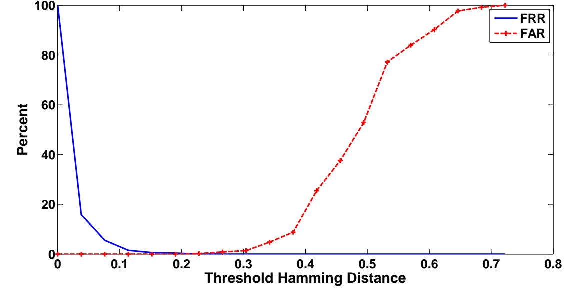


(b)

Figure 3. Influence of power supply and temperature variations in the identification reliability for IDs of: (a) 168 bits, and (b) 36 bits



(a)



(b)

Figure 4. For IDs of 36 bits and nominal situation: (a) Genuine and fake populations. (b) False Acceptation Rate (FAR) and False Rejection Rate (FRR)

- Second group (7 ICs): ICs at five Vdd values between 1.1*Vdd and 0.9*Vdd: 1.32V, 1.26V, 1.2V, 1.14V, and 1.08V.
- Third group (5 ICs): ICs at three Vdd values between 1.1*Vdd and 0.9*Vdd: 1.32V, 1.2V, and 1.08V.

The influence over the intra-class Hamming Distance can be seen in the curve labelled as 'IntraVdd' in Figure 3a. Comparing the results with those obtained at nominal Vdd (curve labelled as 'IntrNom in Figure 3a), it can be observed that the power supply variations have almost no effect over the reliability of the identification system . This is quite interesting because in other types of PUFs, such as Ring Oscillator-based elements, the influence of power supply variations is determinant (they even mask the variation process effect, as reported in [9]).

B. Temperature variations influence

Temperature effects over the start-up values were measured at five different temperatures: 5°C, 25°C, 50°C, and 75°C (fixing the power supply to the nominal value). As in the previous case, 20 measurements of 168 bits of the 20 ICs were recorded at each temperature. The curve labelled as 'IntraTemp' in Figure 3a shows how temperature variation has a higher impact over the reliability than Vdd variation. Lower temperatures are preferred to higher ones to make the identification process more reliable.

C. Influence of the ID length

Reducing the ID length has several advantages. First of all, as the ID is formed by the consecutive reading of different memory addresses, if the length is reduced then the time required for generating the ID is shorter (reading each address requires at least two clock cycles). Secondly, the addresses employed for identification should remain uninitialized until the ID is generated, and cannot be employed for other purposes, as claimed in [6]. In the other hand, if the length of the ID decreases, the reliability of the identification process decreases also. This is illustrated in Fig. 3b and Figure 4. Comparing Figure 4 and Figure 2, it can be seen how reducing the ID length translates into genuine and fake populations that are closer. illustrates this effect when 36 instead of 168 bits are employed.

III. Proposal to reduce bit flipping

In the searching for an effective way to reduce the bit flipping present in our system, the start-up values provided for each SRAM cell were analyzed in detail considering the different operating conditions. In a first study, the bit-string outputs of the SRAM PUFs were considered as the grouping of 14 words read from the memory. A media of 2 out of the 14 words (total of 24 out of the 168 bits) has been observed to have all their bits stable (they do not flip) for different measurements, for a range of temperatures between 5 and 50°C and allowing Vdd variations of +/-10%. This means that by selecting properly the words used to form the identifier, the bit flipping can be decreased considerable or even being removed.

In order to illustrate the importance of a good selection of the memory words to read, three IDs of 36 bits have been analyzed. In the best case (these results are labelled as 'BC' in Figure 5), the ID is formed with the 3 "best" (most stable) memory words. In the worst case (these results are labelled as 'BC' in Figure 5), the ID is formed with the 3 "worst" (least

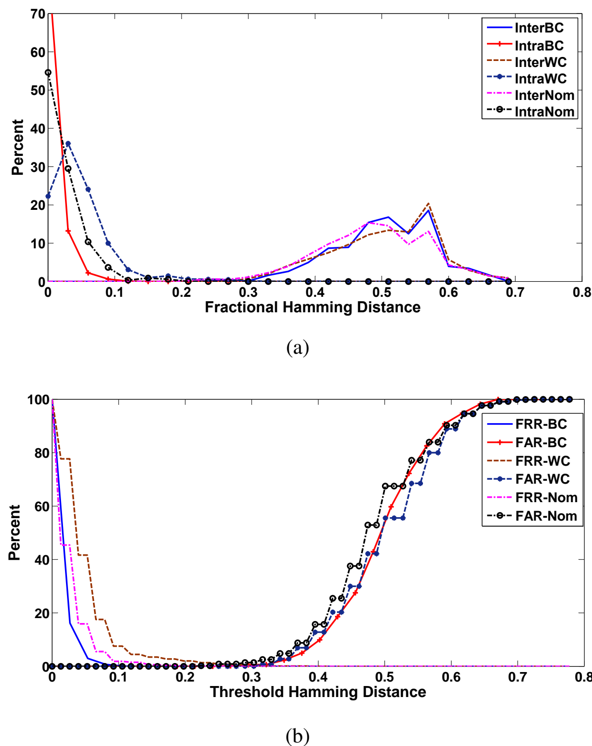


Figure 5. Fake_Genuine and FAR_FRR curves for different selections of the 36 bits for the ID

stable) memory words. In a random case, the ID is formed with 3 randomly selected memory words (these results are labelled as 'Nom' in Figure 5. The FAR and FRR curves as well as the fake and genuine populations for the three selections can be compared in Figure 5. It can be seen how the bit flipping reduction obtained by selecting the best words improves the reliability of the identification process because a bigger interval of fractional Hamming Distances can be used as threshold that ensures a zero FAR and FRR. On the contrary, if the worst case is selected, the fake and genuine populations are closer and the probability of error in the chip identification increases.

In applications related to ASIC identification, certain amount of bit flipping can be allowed, but in the case of key generation systems, zero bit flipping is required. In our analysis, zero bit flipping is achieved by considering only 1 out of the 14 words considered. In any case, there are two possibilities to obtain a very low bit flipping: to analyze more memory words until obtaining more zero bit-flipping addresses or to study the bits of the SRAM words independently. The latter analysis has been done in two steps: firstly, the most stable addresses have been found, and from them, only the stable bits have been selected. The result has been that a media of 10 out of the 12 bits in the most stable addresses do not flip in any situation. Hence, bit strings with even zero bit flipping can be obtained.

In both cases (selecting stable words or selecting stable bits), the selecting process determine adequate challenges for the SRAM PUFs and nothing has to be stored in the ASIC, which differs from the proposal in [7]. Selecting process is done as a pre-processing step during the enrollment phase and previously to use the ASIC (with its SRAM PUF) in its application field. This analysis, which can be easily automated, could be done by the ASIC manufacturers together with other testing proofs that are carried out to evaluate the performance of the ASIC.

IV. Conclusions

This work shows how it is possible to reduce bit flipping in SRAM PUFs even to the point of obtaining zero bit flipping by carrying out a characterization of the SRAM words (and even bits) that are read to form the output bit strings. The characterization is performed as a pre-processing step previously to use the circuit in its application field, without the need of extra hardware to be included in the ASIC. The advantages of this proposal are illustrated in the case of integrated circuit identification with experimental results of TSMC 90-nm SRAMs embedded into ASICs devoted to nonlinear control applications.

V. Acknowledgment

This work was partially supported by Junta de Andalucía under the Project P08-TIC-03674 and by Spanish Ministerio de Economía y Competitividad under the Project TEC2011-24319 (both with support from FEDER), and by the European Community through the MOBY-DIC Project FP7-INFSO-ICT-248858 (www.mobydic-project.eu).

References

[1] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[2] S. Eiroa, I. Baturone, A. Acosta, and J. Davila, "Using physical unclonable functions for hardware authentication: A survey," in *XXV Conference on Design of Circuits and Integrated Systems (DCIS)*, 2010.

[3] J. Guajardo, S. Kumar, G. Schrijen, and P. Tuyls, "Fpga intrinsic pufs and their use for ip protection," *Cryptographic Hardware and Embedded Systems (CHES), LNCS*, vol. 4727, pp. 63–80, 2007.

[4] M. Claes, V. van der Leest, and A. Braeken, "Comparison of sram and ff puf in 65nm technology," *Information Security Technology for Applications*, pp. 47–64, 2012.

[5] G. Selimis, M. Konijnenburg, M. Ashouei, J. Huisken, H. de Groot, V. van der Leest, G. Schrijen, M. van Hulst, and P. Tuyls, "Evaluation of 90nm 6t-sram as physical unclonable function for secure key generation in wireless sensor nodes," in *2011 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2011, pp. 567–570.

[6] N. Saxena and J. Voris, "We can remember it for you wholesale: implications of data remanence on the use of ram for true random number generation on rfid tags," in *5th Workshop on RFID Security (RFIDSec)*, 2009, pp. 1–13.

[7] R. Maes, P. Tuyls, and I. Verbauwhede, "Low overhead implementation of a soft decision helper data algorithm for sram pufs," *Cryptographic Hardware and Embedded Systems (CHES), LNCS*, vol. 5747, pp. 332–347, 2009.

[8] S. Okumura, S. Yoshimoto, H. Kawaguchi, and M. Yoshimoto, "A 128-bit chip identification generating scheme exploiting sram bitcells with failure rate of 4.45x10-19," in *European Solid-State Circuits Conference (ESSCIRC)*, 2011, pp. 527–530.

[9] S. Eiroa and I. Baturone, "An analysis of ring oscillator puf behavior on fpgas," in *2011 International Conference on Field-Programmable Technology (FPT)*, 2011, pp. 1–4.

[10] D. Holcomb, W. Burleson, and K. Fu, "Power-up sram state as an identifying fingerprint and source of true random numbers," *IEEE Transactions on Computers*, vol. 58, no. 9, pp. 1198–1210, 2009.

[11] V. van der Leest, B. Preneel, and E. van der Sluis, "Soft decision error correction for compact memory-based pufs using a single enrollment," *Cryptographic Hardware and Embedded Systems (CHES), LNCS*, vol. 7428, pp. 268–282, 2012.