Impact of the Switching Activity on the Aging of Delay-PUFs

Naghmeh Karimi*, Jean-Luc Danger†‡, Mariem Slimani† and Sylvain Guilley†‡

*CSEE Department
University of Maryland Baltimore County
Baltimore, MD 21250
naghmeh.karimi@umbc.edu

†LTCI, CNRS, Télécom ParisTech
Université Paris-Saclay
75013 Paris, France
firstname.lastname@telecom-paristech.fr

‡Secure-IC S.A.S.
15 Rue Claude Chappe, Bât. B
35510 Cesson-Sévigné, France
firstname.lastname@secure-ic.com

***Abstract*—Physically Unclonable Functions (PUFs) are mainly used for generating unique keys to identify electronic devices. The reliability of PUFs needs to be assured under a wide variety of environmental conditions and aging mechanisms. In this paper, we evaluate the impact of NBTI and HCI aging on two types of delay-PUFs (arbiter-PUFs and loop-PUFs). The results show that the switching activity has a limited impact on delay chains and a significant impact on the arbiter (RS latch) of the arbiter-PUF.**

I. Introduction

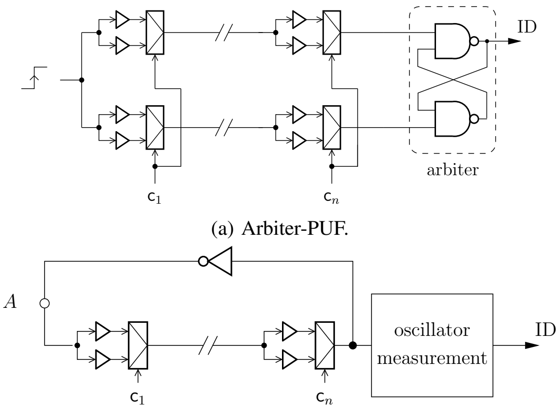
With the increasing concern about the security of integrated circuits, Physically Unclonable Functions (PUFs) are broadly deployed to provide a unique signature for each integrated circuit. A PUF signature can be used for device authentication, or for generating secret keys and random variables in cryptographic devices. To utilize a PUF in practical security applications, the key generated by the PUF should be stable over time and resilient against the aging mechanisms that affect integrated circuits [1]. However, with the advance of VLSI technology, the effect of aging mechanisms has increased. Aging-related degradation results in transistors' parameters shift during the operation time and eventually performance degradation and/or functional failures of the PUF devices. Thereby, characterizing the impact of aging degradation on PUFs and developing aging mitigation methods is crucial.

In this paper, we focus on two types of delay-PUFs: arbiter-PUFs and loop-PUFs [2] and investigate their reliability against Negative-Bias Temperature-Instability (NBTI) and Hot-Carrier Injection (HCI) aging mechanisms.

II. Preliminaries

Aging Mechanisms: NBTI and HCI are two leading factors in performance degradation of digital circuits over time [3]. Both mechanisms result in increasing switching and path delays in the circuit under stress. This leads to timing violations and finally to faster wearout of the system. NBTI mainly affects PMOS transistors and HCI targets NMOS transistors.

NBTI affects a PMOS transistor when a negative voltage is applied to its gate. A PMOS transistor experiences two phases of NBTI aging: stress and recovery phases. The former occurs when the transistor is on, and leads to an increase of the threshold voltage of the transistor. The latter occurs when the PMOS transistor is off, and partially recovers the threshold voltage drift occurred during the stress phase.



(a) Arbiter-PUF.

(b) Loop-PUF.

Fig. 1. Two Delay PUFs.

HCI occurs when hot carriers are injected into the gate dielectric during a transistor switching and remain there. HCI is a function of switching activity, and degrades a circuit by shifting the threshold voltage and drain currents of the transistors under stress.

Delay-PUFs: Delay-PUFs operate based on delay comparisons of different paths. We focus on two main types of delay PUFs named as arbiter-PUF and loop-PUF [2].

Arbiter-PUFs operate based on the race between two identical paths (top and bottom paths shown in Fig. 1a). They include a pair of delay chains and generate one response bit per challenge, in one single query.

Loop-PUFs (Fig. 1b) include a loop realized by n delay elements and one inverter. Each element $1 \leq i \leq n$ can have two delays chosen according to its challenge bit (c_i). The principle of this PUF is to measure the difference of cumulative delays for a challenge and its complementary value.

III. Aging Methodology and Evaluation

Using HSpice MOSRA [4], we first evaluate the timing parameters of single delay-element PUFs at time zero (fresh) and then evaluate the performance degradation of each PUF under both NBTI and HCI stress and with different switching activities (for the internal signals of the PUF). Then, to avoid performing thousands of time-consuming Monte-Carlo simulations for large PUFs, we conduct an *extrapolation methodology* and evaluate the impact of aging in delay-PUFs with an

978-1-5090-5457-2/17/$31.00 ©2017 IEEE

arbitrary size using the results extracted for single delay-element PUFs. Since a delay-PUF mainly relies on comparing two delay chains, the study focuses on the trend of delay change in the two considered delay paths, and in particular for the arbiter-PUFs, on the probability to have bit-flips at the arbiter stage.

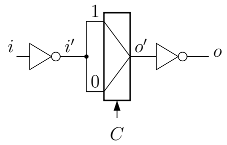


Fig. 2. Delay element considered for aging.

Consider the delay element shown in Fig. 2 (C is the challenge bit). We first perform MonteCarlo simulations for a set of instances with one delay-element and extract the propagation time to send a rising/falling signal between the input i' and the output o' of each element. Time ① (Time ②) shows the rising (falling) propagation time when challenge is 1. Similarly, Time ③ (Time ④) shows the rising (falling) propagation time when challenge is 0. Then, we use the following equations to find the delay of each PUF with one delay element (C is the challenge bit for the considered PUF). In the following equations, T_{LPUF} and T_{APUF} denote to the delay of the loop-PUF and the arbiter-PUF, respectively. Note that in an arbiter-PUF (as shown in Fig. 1a), two elements are in parallel per challenge bit C. Accordingly, to evaluate T_{APUF}, in the following equation we use $\textcircled{1}_1$ and $\textcircled{3}_1$ to refer to the timing parameters of the first element, and $\textcircled{1}_2$ and $\textcircled{3}_2$ to consider the timing parameters of the second element.

$$T_{LPUF} = C((\textcircled{1} + \textcircled{2}) - (\textcircled{3} + \textcircled{4})) + \overline{C}((\textcircled{3} + \textcircled{4}) - (\textcircled{1} + \textcircled{2}))$$
$$T_{APUF} = C(\textcircled{1}_1 - \textcircled{2}_2) + \overline{C}(\textcircled{3}_1 - \textcircled{3}_2)$$

In the next step, for loop-PUFs with n elements (arbiter-PUFs with $2n$ elements), we add the T_{LPUF} (T_{APUF}) of all elements extracted using the above equations. Here, for each element, the delay is computed based on its own challenge bit.

IV. Experimental Results And Analysis

We used a 45-nm technology from the NANGATE library [5]. We utilized HSpice MOSRA model for the aging evaluations. We considered 0% and 100% PUF activities. We ran Monte Carlo simulations for 8192 instances of delay elements (with Gaussian distribution: L: $3\sigma = 10\%$; V_{TH}: $3\sigma = 30\%$, and t_{OX}: $3\sigma = 3\%$), and extracted the aging results to extrapolate the effect of aging on 512 PUFs, each with 16 delay elements. We considered 45°C and 80°C operating temperatures and 20 months of operation.

We estimated the aging-related bit error rate (BER) for each PUF under different operating conditions. For loop-PUFs, we evaluated the ratio between the BER at time i (i: aging time) and at time 0 for M challenges. Fig. 3 represents the impact of HCI and NBTI aging on the delay chain of a loop-PUF with 16 elements during 20 months of usage. The results are shown for a PUF with no activity and a PUF with 100% activity.

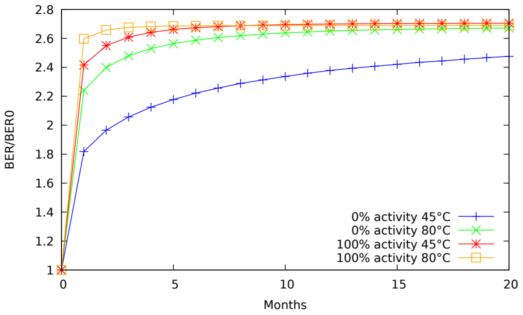


Fig. 3. BER/BER^0 change for different activity rates and temperatures.

Degradation under 100% of switching activity is more significant than 0% activity. In fact, under dynamic conditions, the BER degradation is due to the combined effect of NBTI and HCI. While, under static conditions just NBTI degradation is observed. The degradation increases with the temperature.

The delay chain behavior with regards to aging is the same for the arbiter and loop-PUF. However the reliability of the arbiter-PUF is greatly impacted by the aging of the arbiter. As shown in Fig. 4, the number of relative bit-flips (BER) for the PUF with high switching activity can be 20 times worse than the case without activity after 20 months. A potential cause is the imbalance of the states between the NAND gates.

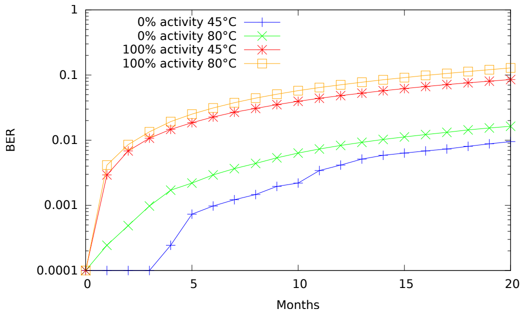


Fig. 4. BER change of the arbiter-PUF for different conditions.

V. Conclusions

This paper investigates the impact of aging on two types of delay-PUFs. The results show that the loop-PUF, and more generally the PUFs with only combinatorial logic are less sensitive to aging. Sequential PUFs such as arbiter-PUFs are much more impacted by aging, and particularly are more sensitive to the switching activity and the temperature.

References

[1] M. T. Rahman et al., "ARO-PUF: An aging-resistant ring oscillator PUF design," in *Design, Automation Test in Europe (DATE)*, 2014, pp. 1–6.

[2] N. Karimi et al., "Predictive aging of reliability of two delay PUFs," in *Security, Privacy, and Applied Cryptography Engineering (SPACE)*. 2016, pp. 213–232, Springer, LNCS 10076.

[3] F. Oboril et al., "Extratime: Modeling and analysis of wearout due to transistor aging at microarchitecture-level," in *Dependable Systems and Networks (DSN)*, 2012, pp. 1–12.

[4] Synopsys, "HSPICE user guide: basic simulation and analysis," 2016.

[5] "Nangate 45nm open cell library," "http://www.nangate.com".