INTEGRATION, the VLSI journal 52 (2016) 71–76

Contents lists available at ScienceDirect

INTEGRATION, the VLSI journal

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

Effects of aging and compensation mechanisms in ordering based RO-PUFs

Giray Kömürcü [a,*], Ali Emre Pusane [b], Günhan Dündar [b]

[a] National Research Institute of Electronics and Cryptology, TÜBİTAK, 41470 Kocaeli, Turkey
[b] Bogazici University, Department of Electrical and Electronics Engineering, 34342 Bebek, Istanbul, Turkey

ARTICLE INFO

Article history:
Received 16 December 2014
Received in revised form
7 July 2015
Accepted 30 August 2015
Available online 5 September 2015

Keywords:
PUF
Physical Unclonable Functions
Aging
Reliability
Robustness
Ring oscillator
FPGA
Challenge-response
CRP

ABSTRACT

With the increasing need for highly secure systems, Physical Unclonable Functions (PUFs) have emerged within the last decade. Ordering based Ring Oscillator (RO) PUFs are one of the best performing structures with their robustness and suitability to FPGA implementations. Even though the performance of the ordering based RO-PUFs have been analyzed in detail, effects of aging have not been studied before. In this work, we present the results of an accelerated aging test applied to analyze the effects of aging on ROs. Then, the effects of aging on ordering based RO-PUFs are examined. Finally, a compensation method to protect the 100% robustness claim of the PUF structure is proposed and its influence on the circuit performance is presented.

1. Introduction

With the increasing need for high security in many applications, Physical Unclonable Functions (PUFs) have become a widely accepted primitive in the last decade. Cryptographic key generation, IP protection, authentication, and ID generation are the main areas that PUFs provide economic and secure solutions [1]. In addition to these, PUFs eliminate the need for a non-volatile memory for ID and key storage purposes. Optical PUFs and Coating PUFs are the first two proposed PUF structures [2–4]. Due to impractical use and expensive equipment requirements of both structures, Silicon PUFs, such as Ring Oscillator (RO) PUFs, Arbiter PUFs, SRAM PUFs, Butterfly PUFs, and Glitch PUFs have drawn more attention with their low cost and ease of integration [5–10].

Imperfect manufacturing technology of integrated circuits leads to deviation of parameters such as threshold voltage, oxide thickness, and doping concentration from nominal values. These imperfections are the basis for the main PUF properties, which are uniqueness, robustness, unclonability, and unpredictability. Since the unique intrinsic physical properties of ICs are also present in FPGAs, some PUF structures, such as RO-PUFs, are convenient for FPGA implementations as well [11]. Based on the mentioned properties, PUF responses should differ from chip to chip randomly (inter-PUF variability), but should be stable during multiple read-outs from the same circuit (intra-PUF variability). In addition to these, the outputs should be unpredictable without using the PUF itself. Finally, manufacturing another circuit with the same PUF characteristic should be impossible.

Robustness is a measure of stable bits in a PUF circuit within different measurements. It is an important performance parameter for PUF structures [12]. Since PUF outputs are generated depending on small mismatches in the IC, any temporal variability present in the system may easily effect the output and result in generating unstable signatures. Almost all PUF structures mentioned above are vulnerable to internal and external effects and generate noisy outputs. Temporal variations that lead to unstable outputs can be classified as reversible and irreversible variations. The changes in the temperature and supply voltage are reversible variations and their effect disappears when the cause is removed. Decreasing the supply voltage is an example of reversible temporal variations. Even though lowering the supply voltage may change the state of output bits, the effect will be withdrawn immediately, when the voltage is returned to the normal level. However, irreversible changes are permanent and affect the circuit through the end of its lifetime [13].

* Corresponding author.
E-mail addresses: giray.komurcu@tubitak.gov.tr (G. Kömürcü), ali.pusane@boun.edu.tr (A.E. Pusane), dundar@boun.edu.tr (G. Dündar).

http://dx.doi.org/10.1016/j.vlsi.2015.08.004
0167-9260/

Aging is the most important contributor of irreversible temporal variations and should be considered carefully in order to guarantee the required long-term robustness performance of the PUF circuit. Negative-bias temperature instability (NBTI), hot carrier injection (HCI), temperature-dependent dielectric breakdown (TDDB), positive-bias temperature instability (PBTI), electromigration, and soft errors can be considered as the main aging mechanisms that cause permanent changes in the electrical characteristics of the IC [14–16]. The impact of aging on the performance and reliability of ICs is also a function of the technology scaling. It is observed that the aging mechanisms mentioned above shorten the lifetime of the CMOS devices more and more with the shrinking of the device sizes [17].

Since the working principle of PUF circuits depends on small mismatches present in the IC, the effects of aging may change the behavior drastically and prevent the correct operation of the primitive. Especially for ICs designed for a long life span, the effects of aging should be investigated and counter-measures should be taken if necessary. In this work, we focus on the effects of aging on ordering-based RO-PUFs, depending on the results of the accelerated aging test (AAT) performed in FPGA environment and we present countermeasures to maintain the reliability of the structures during the lifetime of the IC. The main advantage of the ordering-based RO-PUFs is their 100% robustness even under variable environmental conditions, which is very hard to achieve using other PUF types. This property eliminates the need of an error correction codes (ECC) block for applications that require 100% robust PUF outputs, significantly decreasing the cost of the system.

The rest of this paper is organized as follows. Aging mechanisms and previous works on PUF aging are presented in Section 2. Then, properties of PUF circuits and the expected effects of aging on conventional RO-PUFs and ordering based RO-PUFs are discussed in Section 3. AAT is applied on ROs and the analysis of the test results are presented in Section 4. Effects of aging on ordering based RO-PUFs and compensation methods are discussed in Section 5. Finally, Section 6 concludes the paper.

2. Aging mechanisms and PUFs

The electrical characteristics of ICs change gradually with continuous use. This may result in faulty behavior, causing reliability issues. The changes that appear due to aging are irreversible and affect the IC through the end of its lifetime. The downscaling of the physical dimensions of ICs with respectively high supply voltages makes circuits more prune to aging effects and reliability becomes a serious concern. NBTI, HCI, PBTI, TDDB, electromigration, and soft errors are the main mechanisms that lead to the aging phenomenon. Among these, NBTI and HCI are considered as the dominant ones [14].

Even though aging is an important concern for the reliability of all ICs, it becomes especially critical for PUF circuits. This is due to the fact that their working principle is based on small mismatches present in the manufacturing process. As a result of this, PUF behavior may change drastically due to small aging related drifts in the electrical characteristics of the circuit. Commonly, this change happens before the failure of other parts.

Limited amount of work is present on the aging of PUF circuits in the literature. Software based aging detection and Challenge-Response Pair (CRP) modification techniques are presented in [18]. Compared to this work, we do not propose CRP modification, but generating the CRPs according to the aging of the IC for a certain lifetime. Implementation results of the proposed protocol-level techniques are not presented in the mentioned work as well. In [5], an aging test of one month is applied to arbiter PUFs, but since the test is performed under normal operating conditions (NOC), significant changes in the behavior of the PUF circuit could not be detected. Compared to this work, we apply AAT to the IC to accelerate the aging process. Another aging test performed on SRAM PUFs under NOC is presented in [8]. In this work, it is stated that the change of initial values of SRAM cells remain under 4.5%. In [19], aging is used to develop a new kind of PUF structure, rather than detecting possible problems in previously presented PUF types. Six different PUF structures are analyzed with AAT in [20]. The results of the AAT applied to four memory based PUFs, one SRAM PUF, and one RO-PUF structure are presented. Analysis results indicate that aging decreases the robustness of PUF circuits significantly. A similar analysis of aging on RO-PUFs based on AAT is presented in [13,21]. However, these works focus on conventional RO-PUF structures rather than ordering-based RO-PUFs and just analyze the frequency reduction of ROs. The last work we will mention here is [22], which focuses on designing an aging resistant conventional RO-PUF by changing the structure of ROs at transistor level. Reported results of the work seem successful in terms of decreasing the effects of aging. However, our work aims at removing the effects of aging completely.

Different from the works cited above, we mainly focus on the effects of aging on ordering-based RO-PUFs via real implementation results. We also propose mechanisms to compensate aging effects in ordering-based RO-PUFs. The cost of the compensation mechanism in terms of area efficiency is presented as well.

3. Ordering based RO-PUFs and aging

3.1. PUF quality metrics

Uniqueness and robustness are the two main metrics for performance evaluation of PUF circuits. Uniqueness is also known as the inter-PUF variation and determines the unique signature generation capability of PUF structures placed on different dice. If the uniqueness of the structure is low, outputs may be similar to each other and become predictable, which is not acceptable. Uniqueness can be measured with three different metrics [12]. The most commonly used metric is the Hamming distance (HD) of outputs collected from different ICs, U_QM1, and can be defined as

$$U\_QM1 = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(R_i, R_j)}{n}, \quad (1)$$

where k is the total number of ICs, R_i is the response of ith circuit, HD is the Hamming distance function, and n is the total number of HD operations performed [23]. The ideal value of U_QM1 is 0.5.

Robustness is also known as the intra-PUF variation and determines the noise level of the outputs generated by a circuit. If the consecutive outputs collected from a PUF circuit are noisy, robustness of the structure is low. Low robustness of PUF circuits increases the false-acceptance-rate and false-rejection-rate in authentication systems. If the PUF is used in cryptographic key generation that requires 100% robustness, overhead of the ECC will be higher. This is due to the fact that correcting more bits is only possible by using a higher complexity ECC block. Hamming distances of the outputs collected from the same IC, R_QM1, is the commonly used metric for robustness and can be defined as

$$R\_QM1 = \frac{1}{x} \sum_{y=1}^{x} \frac{HD(R_i, R'_{i,y})}{n}, \quad (2)$$

where x is the total number of outputs collected, R_i is the first output, $R'_{i,y}$ is the yth output, and n is the total number of HD operations [23]. The ideal value of R_QM1 is 0.

Since aging is a non-ideal process, it is expected that both uniqueness and robustness performances of the PUF structures get