Device Aging-Based Physically Unclonable Functions

Saro Meguerdichian and Miodrag Potkonjak
Computer Science Department
University of California, Los Angeles
{saro, miodrag}@cs.ucla.edu

ABSTRACT

To improve resiliency against reverse engineering we propose dynamic physically unclonable functions (DPUFs) whose physical properties are subject to unpredictable changes between uses. We demonstrate this idea using device aging to alter delay characteristics according to user instructions.

Categories and Subject Descriptors

B.7 [**Hardware**]: Integrated Circuits

General Terms

Design, Security

Keywords

Device aging, hardware security, PUF, PPUF, self-trust

1. INTRODUCTION

The physically unclonable function (PUF) emerged in the last decade as the security primitive of choice due to its low power, high speed, and (most importantly) resiliency to side-channel, physical, and software attacks [1][2][3][4]. However, all PUFs proposed until now are static and hence subject to reverse engineering and emulation attacks that are often surprisingly effective [5][6]. In order to improve PUF security, we develop a dynamic PUF (DPUF) that is capable of completely changing its characteristics between uses, effectively providing the attacker with a moving and unpredictable target. Security is now placed not only within the difficulty inherent in reverse engineering a PUF, but also in how quickly it alters its physical parameters and relationship between challenges and responses, to an arbitrary extent. Therefore, in order for an attacker to be successful he must search an exponentially large design space that keeps evolving. Equally importantly, the approach removes the need that the PUF user trusts the IC manufacturer or entity that issues the card, since the PUF can be customized solely according to user specifications. Finally, the DPUF can be used either as a PUF or a public PUF (PPUF), where device characteristics are determined post-silicon and published as a public key [7][8].

DAC 2011, June 5-10, 2011, San Diego, California, USA.

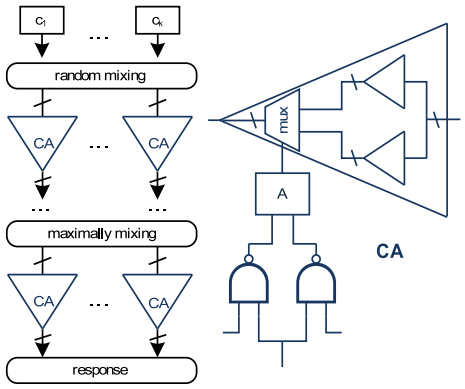

Figure 1: Example DPUF architecture (left), consisting of customization amplifier (CA) cells (right) connected using random and maximally mixing networks.

The key idea is to leverage physical phenomenon such as heating, crosstalk, or device aging in order to alter a PUF's physical properties. One of our desiderata is that the new PUF is solely composed of gates in order to enable integration of the PUF with parts of the design, thus preventing removal of the PUF from the circuitry without significantly altering or damaging the original design.

Therefore, we propose device aging PUFs. We focus on device aging because it provides rapid and low-energy customization and exhibits fast reversibility since static negative bias temperature instability (NBTI) can be easily and promptly reversed using negative bias voltage [9]. As previously stated, the user is completely in charge of customizing the security device with no need to trust the foundry or even the PUF card issuer. Other important desiderata include high speed and low power requirements, complete unpredictability and zero conditional predictability, low overhead and producibility via the standard silicon process, and arbitrarily high exponential advantages over the attacker.

2. RELATED WORK

Several research groups investigate methods for PUF reverse engineering [5][6]. The former describes numerical algebra techniques for reverse engineering several PUF classes, while the latter uses machine learning tools as a universal way to reverse engineer almost all published PUFs. One key observation is that PUFs cannot simply be made arbitrarily large to combat these types of attacks because, in general,

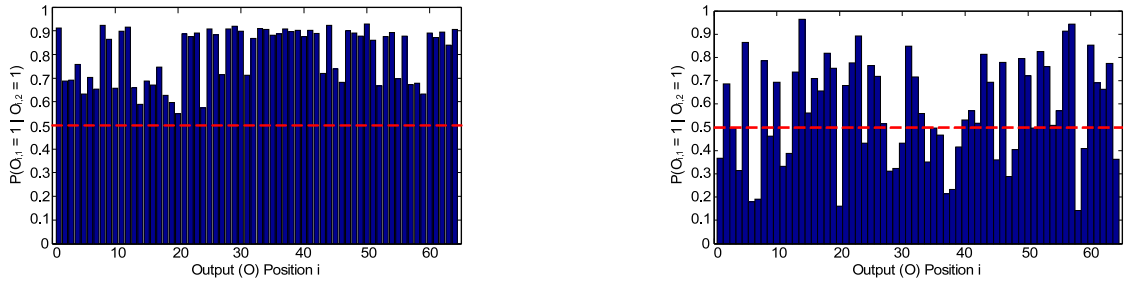

Figure 2: For a single challenge and PPUF instance, the probability that an output bit is 1 after aging given that it is 1 before aging: (a) without customization amplifiers; and (b) with customization amplifiers. The red dashed lines depict the ideal case, where $P(O_{i,1} = 1|O_{i,2} = 1) = 0.5$ for all i.

PUF stability is inversely proportional to its size; thus, [6] postulates that non-linear elements must be present in the PUF design to effectively protect against feasible modeling attacks. Our proposed aging-based PUF is as such, depending on the non-linearity that stems from unpredictable, user-controlled device aging.

3. AGING-BASED PUF ARCHITECTURE

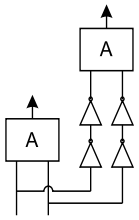

Figure 3: Arbiter network for stability.

Figure 1 shows the DPUF architecture. It consists of customization amplifier (CA) cells connected using random and maximally mixing networks. Random networks are used to increase randomness of the structure while maximally mixing networks ensure that all output signals are affected by the maximum number of input signals. CA cells operate in the following way. The user can age and slow down one of two NAND gates by applying an appropriate input vector. This will result in enabling different paths by the controlling multiplexers. The gates on these paths can be sized in such a way that they have very large differences in their delays.

Numerous CAD tasks can be identified with respect to the design and realization of the DPUF including: (i) design of a PUF structure optimized for maximal entropy or stability; (ii) optimization using gate sizing; and (iii) deriving strategies that maximize the NBTI input effect.

4. RESILIENCE TO SECURITY ATTACKS

The aging-based DPUF intrinsically protects against many types of security attacks, including guessing, simulation, emulation, and protocol attacks. Experimental results presented in Figure 2 show resilience to guessing attacks. The effect of aging on PUF responses is shown in Figure 2a, which depicts the probability of an output bit in a response vector to a particular challenge after aging being the same as that before aging. The results show that although there is some change in properties, aging alone is not sufficient to protect to maximal effect attacks which employ previous knowledge of challenge responses. Therefore, we provide the same results in Figure 2b but this time also employ our customization amplifiers. We see that there is dramatic improvement in entropy of the data, with many outputs being close to the ideal case (50%).

5. STABILITY AGAINST ENVIRONMENTAL AND OPERATIONAL CONDITIONS

Our DPUF structure exhibits stability against environmental and operational conditions, such as variations in temperature or supply voltage, by employing another set of arbiters, as shown in Figure 3. Here, we add add a series of buffers on both of the input paths of the new arbiter. We only consider the output if both arbiters agree, i.e. if the paths differ in delay by *greater than* some Δd defined by the buffers. Thus, we create resiliency to any conditions which change delay properties by *less than* Δd.

6. CONCLUSION

We have developed a new class of dynamic PUF that employs dynamic system alteration with respect to individual gate speeds, enabling each user to create his own PUF as needed. Our evaluation indicates that the DPUF has very high unpredictability and can easily be stabilized.

7. ACKNOWLEDGMENTS

This work was supported in part by the NSF under awards CNS-0958369 and CNS-1059435.

8. REFERENCES

[1] B. Gassend et al., "Silicon physical random functions," *ACM CCS*, pp. 148–160, 2002.

[2] N. Beckmann and M. Potkonjak, "Hardware-based public-key cryptography with public physically Unclonable Functions," *Info. Hiding*, pp. 206–220, 2009.

[3] M. Potkonjak et al., "Trusted sensors and remote sensing", *IEEE Sensors*, pp. 1104–1107, 2010.

[4] M. Potkonjak et al., "Differential public physically unclonable functions: architecture and applications," *ACM/IEEE DAC*, 2011.

[5] M. Majzoobi et al., "Testing techniques for hardware security," *IEEE ITC* pp. 1–10, 2008.

[6] U. Ruhrmair et al., "Modeling attacks on physical unclonable functions," *ACM CCS*, pp. 237–249, 2010

[7] S. Wei et al., "Gate-level characterization: foundations and hardware security applications," *ACM/IEEE DAC*, pp. 222–227, 2010.

[8] S. Wei et al., "Malicious Circuitry Detection Using Thermal Conditioning," *IEEE TIFS*, 2011.

[9] B. Cheng et al., 11PBTI/NBTI-related variability in TB-SOI and DG MOSFETs," *IEEE Electron Devices Letters*, vol. 31, no. 5, pp. 408–410, 2010.