Stable and Secure Delay-based Physical Unclonable Functions Using Device Aging

Teng Xu, and Miodrag Potkonjak
Computer Science Department
University of California, Los Angeles
{xuteng, miodrag}@cs.ucla.edu

***Abstract*—The modern secure systems are designed to require ultra-low power secure solutions due to their energy constraints. Compared to the classical cryptography approaches, the physical unclonable functions (PUFs) have emerged as a novel security primitive with the property of low power/energy, small area, and high speed. Among the family of PUFs, delay-based PUF takes advantage of the process variation on the gate delays. However, it suffers the problem of instability against operational variations. In this paper, we have proposed to use device-aging to improve the stability of the delay-based PUF which induces negligible energy and area cost. We test to compare the stability of PUFs before and after device-aging against temperature and supply voltage variations.**

I. Introduction

Security plays an essential role in many applications. The proliferation of new applications and systems such as wireless sensor networks, implantable devices have imposed new requirements for security primitives, for example, ultra-low power consumption, and resilient against side channel attacks. Classical mathematics cryptography provides elegant solutions to different domains such as privacy, integrity, and authentication in terms of both soundness and practicability. However, they are not adequate in the many newly emerged systems. For instance, wireless sensor networks require very small area and energy overhead security approach that can not be be realized by classical cryptography.

The physical unclonable functions are physical devices that have a random but deterministic mapping of inputs to outputs. On the other hand, process variation (PV) is a side effect in manufacturing. Because of PV, the physical attributes of transistors (channel length, delay, leakage) become unique when integrated circuits are fabricated. The PUFs often take advantage of the process variations so that each piece of PUF is unique and unclonable. PUFs, as security primitives, have the advantage of low power consumption and are resilient against side channel attacks. However, one significant drawback of the PUF, including the standard delay-based PUF is vulnerability against environmental variations, such as temperature and supply voltage. For example, when the temperature goes up, the delay of gates will go up, but because of process variation, the delay of different gates will increase unpredictablely. Consequently, change the functionality of the original PUF.

The primary goal of this paper is to propose a solution based on device aging (e.g. negative-bias temperature instability (NBTI)-induced transistor slowdown or wire electro-migration) to increase the stability of PUFs. The PUF we are focusing on is the delay-based PUF. It utilizes the effect of process variation on the delay components to build an unclonable structure. Meanwhile, the device aging approach, such as NBTI allows the control of threshold voltage during the post-silicon stage. Due to the fact that gate delay is influenced by threshold voltage, device aging can have a direct effect on gate delays. Based on the above observations, our key idea is to use device aging to adjust the delays of the delay-based PUF in a purpose to increase the PUF stability.

Figure 1 depicts a delay-based PUF with 3-bit challenge. An output bit is generated by assigning a challenge vector and sending a rising edge through the PUF. Each bit of challenge acts as the select signal of the two multiplexers in each segment. The two paths traverse the three delay segments, swapping positions (top and bottom) depending on the input bit at each segment, before arriving at the arbiter which determines the final output. An arbiter will set its value to 0 or 1 depending on which path (top or bottom) arrives first, effectively selecting the path that has the smaller delay.

An important observation of the delay-based PUF is that some challenge of the PUF produce relatively small delay difference between the two paths. For example, in Figure 1, 011 produce a delay difference of 2. These challenges are highly unstable challenges in a sense that when environmental condition changes, the change of gate delays can easily cause violation to the original delay relation of the two paths because the delay has been very close to each other. For example, the delay difference goes from 2 to -1, changing the output of the PUF. The motivation of device aging comes from the idea that if we internationally increase the delay difference between the upper part and the lower part within each segment, we can possibly decrease the situations where the delay of two paths are too close to each other. This is due to the fact that the delay difference of each segment is increased with device aging.

Figure 2 shows the the delay-based PUF after device aging. In this example, we assume that device aging can increase/decrease the delay of a gate by 8 percent based on the testing results in [1]. Our algorithm is simply to increase/decrease the gate delay in a way to maximize the delay difference of each segment. For instance, in the first segment, we use device aging to decrease the delay of the upper part from 9 to 8.28, and increase the lower part from 13 to 14.04. Consequently, the absolute value of delay difference goes up from 4 to 5.76. In Table I, we demonstrate the delay differences between two the paths given all possible challenges before and after device aging for the example in Figure 1 and Figure 2. We can conclude from the table that the delay difference generally increases significantly after device aging.

978-1-4799-8391-9/15/$31.00 ©2015 IEEE

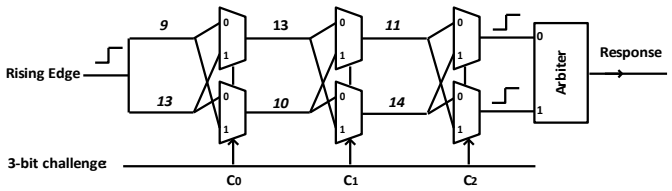

Fig. 1: A 3-bit delay-based PUF with the number indicating the upper delay and lower delay for each segment.

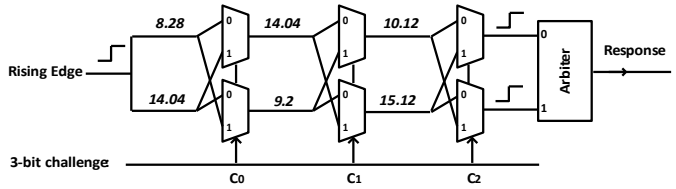

Fig. 2: A 3-bit delay-based PUF after device aging.

Challenge	Delay Difference	Diff. After Aging
000	-4	-5.92
001	4	5.92
010	-2	-4.08
011	2	4.08
100	4	5.6
101	-4	-5.6
110	-10	-15.6
111	10	15.6

TABLE I: Delay differences between two paths given all possible challenges of the delay-based PUF in Figure 1 and Figure 2.

II. Related Work

In this section, we briefly summarize the related literature on process variation, PUFs, and device aging.

A. Process Variation

The phenomenon of process variation is widely recognized in modern CMOS technologies [2]. The cause for process variation includes wafer lattice structure imperfections, non-uniform dopant distribution, mask alignment, and chemical polishing [2]. PV exists among gates or transistors when the components are designed to be identical, but due to manufacturing limitations are different and unique in terms of structural and operational properties, such as propagation delay and leakage power. Due to the fact that transistors are shrinking in size, the effect of process variation has grown. Borkar et al. indicates that identical gates may have up to 30% difference in propagation delays in the current 45 nm technology [3].

B. PUFs

The concept of PUF is first proposed by Pappu et al using mesoscopic optical systems [4]. Devadas et al developed the first silicon PUFs through the use of intrinsic process variation in deep submicron integrated circuits [5]. After that, a great variety of technologies were used for PUF creation including IC interconnect networks, thyristors, memristors, and several nanotechnologies. Consequently, a variety of PUFs are proposed including arbiter-based (APUF) [5], ring oscillator-based (RO-PUF) [6], and SRAM PUFs [7].

To solve the instability of PUF, the technology of hot carrier injection is proposed Bhargava et al. in [8] and [9]. More recently, the concept of digital PUF is proposed by Xu [10][11] and its application is demonstrated in [12] and [13]. The basic idea is to use analog PUF to initialize the randomly-connected LUT network to build unclonable digital structure. Our approach is unique in such a way that we are the first to use device aging to enhance the properties of PUFs.

C. Device Aging

NBTI is an intrinsic phenomena of deep submicron silicon technologies [14]. NBTI can shift V_{th} depending on the time for which the PMOS device is stressed. Kumar et al. has proposed an analytical model for NBTI using the framework of the Reaction-Diffusion model [1].

III. Preliminaries

A. Gate Delay, Power, and Process Variation

We use the gate-level delay and power models from Markovic et al. [15]. The delay model is reproduced in Equation (1), where k_{tp} is the delay-fitting parameter, C_L is load capacitance, V_{dd} is supply voltage, n is substreshold slope, μ is mobility, C_{ox} is oxide capacitance, W is gate width, L is effective channel length, $\phi_t = kT/q$ is thermal voltage, k_{fit} is a model-fitting parameter, σ is the drain induced barrier lowering (DIBL) factor, and V_{th} is threshold voltage.

Among the factors, device aging has a influence on V_{th}. In this paper, we consider environmental variations of changing T and V_{dd} and test the corresponding delay.

$$D = \frac{k_{tp} \cdot C_L \cdot V_{dd}}{2 \cdot n \cdot \mu \cdot C_{ox} \cdot \frac{W}{L} \cdot (\frac{kT}{q})^2} \cdot \frac{k_{fit}}{(\ln(e^{\frac{(1+\sigma)V_{dd}-V_{th}}{2 \cdot n \ \ cdot(kT/q)}}))^2} \quad (1)$$

B. Device Aging

We use the aging model proposed by Chakravarthi et al. [16] and shown in Equation (2) for the effect of device aging due to NBTI on V_{th} shift, where A and β are constants, V_G is the applied gate voltage, E_α is the measured activation energy of the NBTI process, T is the temperature, and t is time.

$$\Delta V_{th} = A \cdot e^{\beta V_G} \cdot e^{-E_\alpha / kT} \cdot t^{0.25} \quad (2)$$

In this paper, we leverage the potential positive effect of aging on gate delays in delay-based PUFs.

IV. Stability vs. Randomness

There exists a trade off between the stability of a PUF and the randomness of a PUF. A stable PUF requires the delay difference of two paths as large as possible, meanwhile this has an effect on the randomness because the predictability of

PUF outputs can be increased. For an extreme case, if one segment of PUF has extraordinarily large delay difference, the PUF will be ultra stable in a sense that whichever path has the slower part of delay for that segment, the path will be slower. However, this directly results the PUF output to be highly predictable due to the reason that attackers can easily observe the correlation between the challenge bit for the segment and the final output.

As for our situation, we want to use device aging in such a way to increase stability while not comprising security. In other words, we want to at least maintain the randomness of original PUF while increase the stability. To be more specific, as shown in the motivational example, our key idea is to use device aging to increase the path delay difference. However, the create of ultra-large delay difference is dangerous because that segment will dominate the output of the PUF. Therefore, instead of device aging for all the segments, we only choose some segments with relatively small delay difference for aging. For the segment with already large delay difference, we do not use aging to further increase delay difference. So based on this proposal, we are at least not compromising randomness of the original PUF.

V. Algorithm

In this section, we explain our algorithm for device aging as shown in Algorithm 1. The key idea is to only device aging the segment with no larger than η delay difference. We want to age the upper part delay and the lower part delay separately to increase the delay difference, hence enhance stability. Assume that the delay difference for each segment follows a gaussian distribution $D_{up} - D_{down} \sim \mathcal{N}(0, \sigma^2)$. In our further test, we assume $\eta = \sigma$.

Algorithm 1 Device Aging Delay-based PUF

Input: Delay profile for a n-bit delay-based PUF,
$D_{up}[1...n]$: Upper part delay from segment 1 to n,
$D_{down}[1...n]$: Lower part delay from segment 1 to n,
η: threshold delay difference.
Output: Delay-based PUF after device aging,

```
For i from 1 to n
    If abs(D_up[i] − D_down[i]) ≤ η
        If D_up[i] ≥ D_down[i]
            Aging to increase D_up[i]
            Aging to decrease D_down[i]
        Else
            Aging to increase D_down[i]
            Aging to decrease D_up[i]
Return D_up, D_down after aging
```

VI. Results

In this section, we demonstrate our simulation results. We first show the delay difference between two paths before and after device aging. Then we test to compare the PUF stability in variation of different temperature and supply voltage.

A. Delay Difference

Figure 3 shows the cumulative distribution function (CDF) of the delay difference between two paths before and after device aging. The test is on a 64-bit PUF and the cumulative distribution is based on 1,000,000 random challenges. In the figure, α is the standard deviation of gate delays in each segment caused by process variation. We can obviously see that the curve after device aging has much larger delay difference compared to original PUF given a same CDF.

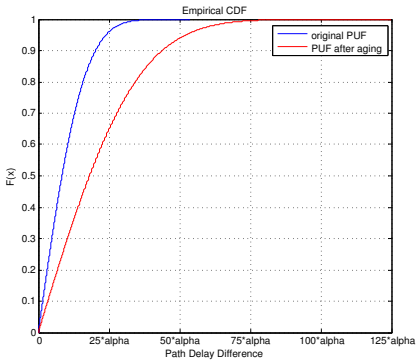

Fig. 3: CDF of path delay difference before and after device aging. Tested on 1,000,000 random challenges.

B. Stability

We test the stability of PUF against two factors, one is temperature, and the other is supply voltage. For both test, we apply 1,000,000 random challenges on a 64-bit PUF. We define the stability of a PUF as the percentage of challenges that will produce the same output when operational condition (temperature, supply voltage) changes.

Figure 4 shows the test result of PUF stability against different temperatures. Assume that the original temperature is 300K, we change the temperature ranging from 300K to 400K and test the stability. It can be concluded that when temperature changes, the PUF with device aging shows approximately 6-7 percent better stability compared to original PUF. Correspondingly, Figure 5 shows the test result of PUF stability against different supply voltages. Assume that the original supply voltage is 1V, we change it from 1V to 1.5V and test the stability. Similar to the case of temperature, when supply changes, the PUF with device aging shows approximately 5-6 percent better stability compared to original PUF.

We design another two tests by looking into the relation between stability and delay ratio. The definition of delay ratio is shown in Equation 3. It represents the relative delay difference between two paths. An important observation is that some challenges that cause larger delay ratio can have outputs with better stability. For example, in our motivational example in Section I, 110 is such challenge that creates a larger delay ratio. In this test, we compare the stability of the PUF given only challenges with a delay ratio greater than some value.

Figure 6 shows the result tested under the situation when changing temperature from 300K to 400K, but only using a subset of challenge with a delay ratio greater than the x-axis value. Still we can conclude that PUFs with device aging shows a much better stability than the original PUF. And when the delay ratio reaches 0.4%, the stability of PUFs after device aging can reach as much as 99%. Figure 7 shows the results tested when changing supply voltage from 1V to

1.5V. Similarly, the stability of PUF increases when delay ratio increases, and finally is close to 99%.

$$Delay\ Ratio = \frac{Delay_{p1} - Delay_{p2}}{min(Delay_{p1}, Delay_{p2})} \quad (3)$$

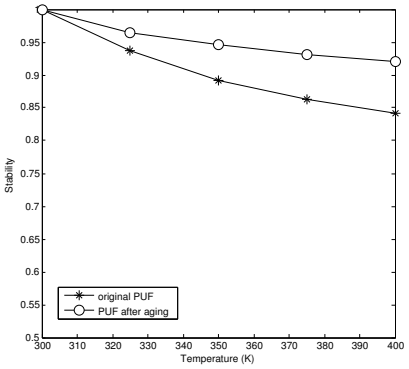

Fig. 4: Stability against temperatures from 300K-400K. Tested on 1,000,000 random challenges.

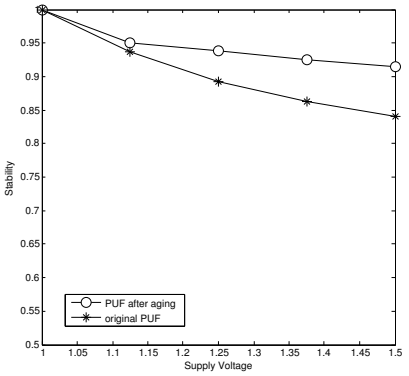

Fig. 5: Stability against supply voltage from 1V-1.5V. Tested on 1,000,000 random challenges.

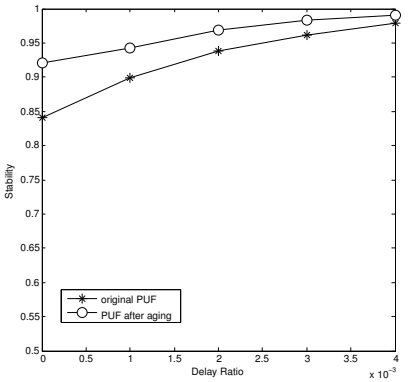

Fig. 6: Change temperature from 300K to 400K, test the stability of PUFs using challenges with different delay ratios. Tested on 1,000,000 random challenges.

VII. Conclusion

In this paper, we have demonstrated a novel approach to increase the stability of delay-based PUF using device-aging. The key idea of our algorithm is to increase the delay difference between the two paths without comprising security.

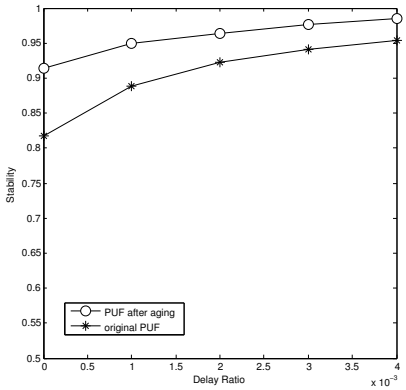

Fig. 7: Change supply voltage from 1V to 1.5V, test the stability of PUFs using challenges with different delay ratios. Tested on 1,000,000 random challenges.

Our test results indicate that by using our approach, the stability of the PUF can increase averagely by 6-7 percent when temperature changes and 5-6 percentage when supply voltage changes. Furthermore, by carefully selecting challenges, our method guarantee a PUF stability of 99% or higher.

References

[1] Kumar, Sanjay V., Chris H. Kim, and Sachin S. Sapatnekar, "An analytical model for negative bias temperature instability," *Computer-Aided Design*, 2006.

[2] K. Bernstein et al., "High-performance CMOS variability in the 65-nm regime and beyond," *IBM Research and Development*, vol. 50, nos. 45, pp. 433-450, 2006.

[3] S. Borkar et al., "Parameter variations and impact on circuits and microarchitecture," *DAC*, pp. 338-342, 2003.

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

[5] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," *ACM Conference on Computer and Communications Security*, pp. 148-160, 2002.

[6] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *DAC*, pp. 9-14, 2007.

[7] J. Guajardo, S. Kumar, G. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *CHES*, pp. 63-80, 2007.

[8] M. Bhargava, K. Mai, "A High Reliability PUF Using Hot Carrier Injection Based Response Reinforcement," in *CHES*, pp. 90-106, 2013.

[9] M. Bhargava, C. Cakir, K. Mai, "Reliability enhancement of bi-stable PUFs in 65nm bulk CMOS," in *HOST*, pp. 25-30, 2012.

[10] T. Xu, J. B. Wendt, and M. Potkonjak, "Digital Bimodal Function: An Ultra-Low Energy Security Primitive," *ISLPED*, pp. 292-297, 2013

[11] T. Xu, M. Potkonjak, "Robust and Flexible FPGA-based Digital PUF," *International Conference on Field Programmable Logic and Applications (FPL)*, pp. 1-6, 2014.

[12] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT Systems: Design Challenges and Opportunities," *ICCAD*, pp. 417-423, 2014.

[13] T. Xu, J. B. Wendt and M. Potkonjak, "Secure Remote Sensing and Communication using Digital PUFs," *ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS)*, pp. 173-184, 2014.

[14] M. A. Alam and S. Mahapatra, "A comprehensive model of PMOS NBTI degradation," *Microelectronics Reliability*, vol. 45, pp. 71-81, 2005.

[15] D. Markovic et al., "Ultralow-power design in near-threshold region," *Proceedings of the IEEE*, vol. 98, no. 2, pp. 237-252, 2010.

[16] S. Chakravarthi et al., "A comprehensive framework for predictive modeling of negative bias temperature instability," *IRPS*, pp. 273-282, 2004.