Circuit-Level Techniques for Reliable Physically Uncloneable Functions

Vignesh Vivekraja and Leyla Nazhandali
Department of Electrical and Computer Engineering
Virginia Tech
Blacksburg, Virginia 24061
Email: (vigneshv,leyla)@vt.edu

***Abstract*—In this paper we study the effect of transistor supply voltage and body bias on the performance of ring oscillator Physically Uncloneable Functions (PUFs). The uniqueness (ability to identify a PUF) and reproducibility (ability to reproduce the same output) of PUFs increase drastically in the subthreshold region of operation. Also, the reproducibility of PUFs increase when the transistors are forward body biased. A ring oscillator PUF was tested and it achieved a uniqueness of 47.8% and reproducibility of 100% when operating at a supply voltage of 0.2 V. Compared to a base line configuration, our method improved the uniqueness by 18% and reproducibility by 7%. Therefore, apart from architectural optimizations, circuit level considerations like supply voltage and body bias can improve the reliability of PUFs.**

I. Introduction

In today's world, it is very important to establish the true identity of an object in a trustworthy manner for a wide range of applications. Examples include electronic passports, Radio-Frequency Identifiers (RFID) for secure access, anti-counterfeiting of expensive items and important documents, and authorized access to prescription medications in hospitals, to name a few. It is very important that the item used as an identifier of the object is almost impossible to clone (counterfeit). Using simple pieces of data — such as numbers — as identifiers keeps the door open for stealing the secret identifier in various ways including side-channel attacks [1].

Physically uncloneable functions (PUFs) have been proposed and successfully implemented to overcome some of the problems faced by traditional techniques [2]. PUFs employ innovative configurations of circuits to derive secrets from the inherent physical variations of ICs rather than storing a unique identifier in physical memory. Since PUFs rely on uncontrollable and unpredictable process variations during IC fabrication, the secret is extremely difficult to predict. Therefore, PUFs are ideal candidates for low cost devices like smart cards and they are less costly in terms of processing power and chip area. PUFs can also be used for protection of hardware IPs [3].

Various device-level, architectural-level and protocol-level methods have been proposed that use random variations for effective implementation of PUFs. Pappu et.al. use the speckle pattern of an optical medium focused with a laser to derive random variations [2]. Coating PUFs have been proposed, where in, random dielectric particles are deposited on top of the IC [4]. However, the more popular PUFs are based on inherent delay variations in circuits due to the process variation associated with IC manufacture.

Interchip and intrachip process variation are an undesirable factor in traditional CMOS circuit design. Various techniques like forward body biasing [5] and adaptive body biasing [6] have been proposed that make the circuits more tolerant to process variation. However, for PUFs, increasing the effect of random process variations in ICs is desirable as it can potentially make the PUFs more secure and distinguishable. It is also known that the sensitivity of circuits to random process variations changes depending on various device-level and circuit-level factors, such as transistor length (feature size) and operating voltage.

The purpose of this paper is to study the effect of two of these circuit-level decisions on ring oscillator PUFs, namely 1) the operating (supply) voltage of the circuit and 2) the body bias voltage of the transistors in the circuit. Our goal is to uncover the best combination of these two decisions that results in highest uniqueness and reproducibility of the ring oscillator PUF circuit. Uniqueness is a measure of the ability to identify a PUF and reproducibility is the ability of the PUF to reproduce the same output under varying conditions. Our study shows that we are able to increase the uniqueness by 18%

978-1-4244-4804-3/09/$25.00 © 2009 IEEE

and reproducibility by 7% compared to a base design by carefully adjusting these two variables. The broader goal of our paper is to show that within the same PUF architecture and protocol, there are lower-level knobs that can be tuned to achieve more distinguishable and stable PUFs.

The rest of this paper is organized as follows : Section 2 presents the background on ring oscillator PUFs and a brief description of related work about them; Section 3 discusses the effect of supply voltage and body bias on sensitivity of circuit delay to process variation; Section 4 provides the experimental setup and Section 5 presents the results. Finally, conclusions and future work are presented in Section 6.

II. Background

Figure 1 represents a typical ring oscillator PUF circuit [7]. It is comprised of 32 identical 11-stage ring oscillators[1]. Each of the oscillators oscillates at its characteristic frequency. Theoretically, all circuits would oscillate at the same frequency, but the inherent inter-chip, and intra-chip process variations, as well as the environmental conditions affect the oscillation frequency. This causes each oscillator to output a slightly different frequency. To derive digital values from these oscillators, a comparison is made between the frequency of a pair of oscillators. The output bit is set to 1 or 0 based on which of the oscillators is faster. To derive an M-bit output, M different comparison between the oscillators should be made. For a circuit with N ring oscillators, there are $N*(N-1)/2$ possible comparisons to make. The selection of the M pairs of oscillators for comparison is controlled by the MUXs based on the input challenge to the circuit. Theoretically, the maximum possible M for maximum entropy is $log_2(N!)$ bits [7]. Different PUFs have different output responses for the same challenge. This property is used to identify a given PUF based on the challenge response behavior.

Two major metrics are used to assess quality of PUFs, namely uniqueness and reproducibility.

Uniqueness is a measure of how easily a PUF can be differentiated from others. For instance, it can be measured by the hamming distance between the output of two PUFs challenged with the same input. Since there are many possible input challenges, the uniqueness is measured using the average hamming distance between the outputs for a representative set of input challenges.

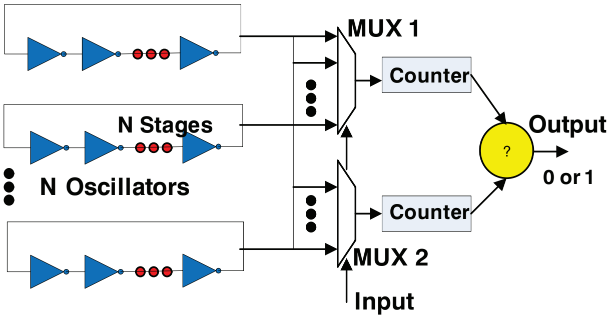

Fig. 1. Architecture of Ring Oscillator PUF

Reproducibility is the ability of the PUF to reproduce the same output response for the same input challenge at different times in the presence of environmental variations. It can be measured by the percentage of bits that remain unchanged while changing the environment variables, but keeping the input challenge the same. Again, since there are many possible input challenges, an average value of several representative input challenges can be used. Ideally, the reproducibility of a PUF must be 100%, implying it must be able to reproduce the same response even at worst case scenario.

There is a rich body of work related to designing PUFs. To name a few, [7] proposes a novel ring oscillator PUF and [9] proposes the arbiter PUF circuit. Furthermore, [10] proposes protocols and algorithms to improve PUFs. However, to the best of our knowledge, no work has been done on studying the effect of circuit-level decisions on silicon PUFs.

III. Effect of supply voltage and body bias on circuit characteristics

It is well-known that the power consumption and the frequency of a CMOS circuit are critically controlled by the supply voltage and to some extent by the body bias. The purpose of this section is to explain the impact of these two parameters, not on power and performance, but on the sensitivity of the circuit to process variation. In this regard, we define a key metric: ***Variability***. The variability of a group of 'n' ring oscillators is the ratio of the standard deviation of its characteristic frequency 'f' to the average characteristic frequency of all ring oscillators, as shown in formula-(1). Consequently, a higher value of variability indicates that the frequency of the ring oscillators in different chips are more spread apart. In other words, the design is more susceptible and less tolerant toward process variation. The motivation behind

[1] The number of oscillators and the depth of oscillators have been picked from previous work [8]. The purpose of this work is not to study the effect of changing these two parameters. We believe our results will apply to other configurations as well.

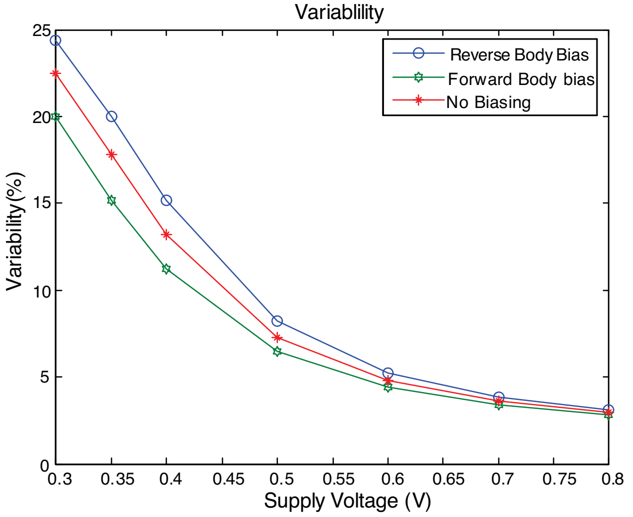

Fig. 2. Scaling of variability with supply voltage and body bias

studying variability is that we believe higher variability can result in higher uniqueness. We investigate this claim in future sections.

$$Variability = \frac{\sigma(f_1,f_2,..f_n)\,(n)}{\Sigma(f_1,f_2,..f_n)} \tag{1}$$

A. *Effect of operating voltage*

Traditionally, the reduction of supply voltage, also known as voltage scaling, has been successfully employed to reduce the power consumption of a circuit. However, lowering the supply voltage increases the sensitivity of the circuit to process variation. This has been shown in Figure 2 (the middle line with body bias of 0 V), which shows the variability of a ring oscillator with respect to operating voltage. The graph was obtained through Monte Carlo SPICE simulation of a ring oscillator using the setup explained in Section 4.

In recent years, it has been shown that the supply voltage of a CMOS circuit can be scaled even further, to voltages below the threshold voltage, which is called subthreshold operation. Various subthreshold circuits have been successfully designed, fabricated and tested to prove the effectiveness and viability of subthreshold operation [11]. However, the sensitivity of the circuit to process variation increases drastically in this region. As can be seen in Figure 2, the variability increases at a slow but steady pace as we reduce the voltage from nominal voltage to the threshold voltage, around 500 mV. However, around this point the circuit starts to show significant increase in susceptiblity towards process variation. The reason behind this is that below the threshold voltage, transistors are not switching as usual and rely heavily on leakage current for charging and discharging the load capacitance. Leakage current is more affected by process variation, which results in overall higher variability in subthreshold region. This effect is considered a drawback of subthreshold operation in general designs. However, we believe this effect can be employed to our advantage when designing a PUF circuit.

B. *Effect of body bias*

Figure 3 identifies the source, drain, gate and bulk contacts of the PMOS and NMOS transistors in a CMOS circuit. Reverse body biasing (RBB) is the process of raising the voltage of the PMOS N-wells with respect to supply voltage or lowering the voltage of the substrate relative to ground. In a forward body bias (FBB) configuration, the PMOS is biased with a voltage lower than supply voltage or the voltage of the NMOS substrate is made negative relative to ground. Traditionally, RBB [6] is employed to reduce the leakage current of the circuit, thereby reducing its leakage power. But this configuration makes the IC more susceptible to inherent process variations and decreases its performance. Forward body biasing on the other hand, has been used for increasing the frequency of operation and making the IC more tolerant towards process variation.

Figure 2 shows the effect of body bias on a ring oscillator's variability. It can be observed that RBB increases the variability of the circuit. Seemingly, RBB would be an ideal candidate for PUF circuits, as RBB increases the sensitivity of the circuit towards random process variation. In the forth coming sections of this paper we investigate this assumption and present the effect of body bias on the uniqueness and reproducibility of a PUF circuit.

IV. Methodology

All of the experiments were carried out using SPICE simulations. Monte Carlo analysis was carried out to simulate the effect of process variations. The simulations were performed on a 90-nm technology node. Industry standard transistor models and process variation models from a major foundry were used for all simulations.

The architecture of the PUF circuit is similar to the one specified in Section 2. The PUF consists of 32 ring oscillators, each containing 11 stages of NAND gates. One input of NAND gate is set to 1 to make it function

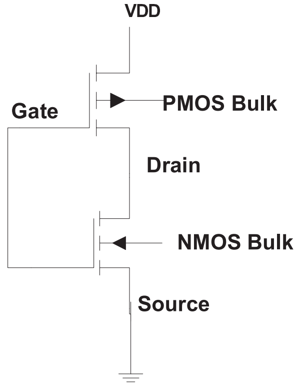

Fig. 3. Inverter with Substrate nodes Identified

effectively as an inverter. Such a circuit was simulated in SPICE over 20 different Monte Carlo runs. Both the intra-die and inter-die process variation flags were set during the simulation. This setup is analogous to the simulation of 20 different PUF ICs. The simulations were carried out using the highest possibile accuracy settings. Since it is a common practice in the design industry to rely on statistical transistor level simulations before actual implementation and since we used statistical models provided by a commercial foundry, we strongly believe that the results of the simulation, are very close to that of actual implementation.

Extracting the digital signature of each IC: As it is a common practice in the PUF design community, we derived a digital signature for each PUF IC instance by comparing adjacent oscillators. In other words, the frequency of the first oscillator was compared with that of the second, the frequency of the second was compared with that of the third, and so on. Therefore, except for the first and last oscillator, each oscillator was compared to two other oscillators. In our experiment, the comparison was done in an ideal fashion and no actual circuitry is implemented. In order to account for non-ideal comparison mechanisms and the effect of local noise, which may change the frequency of one oscillator but not the other[2], we randomly changed the frequencies of the oscillators by a maximum of 3%. The result of each comparison was reflected in a single bit. Consequently, we obtained a 31-bit signature for each PUF.

Measuring uniqueness: The uniqueness was determined by comparing the digital signature of each IC to each other and calculating the percentage of bits that are different in the two signatures. Since we had 20 chip instances, we had $20 * 19/2$, i.e. 190 possible IC comparisons. We provide the average of these numbers as the uniqueness.

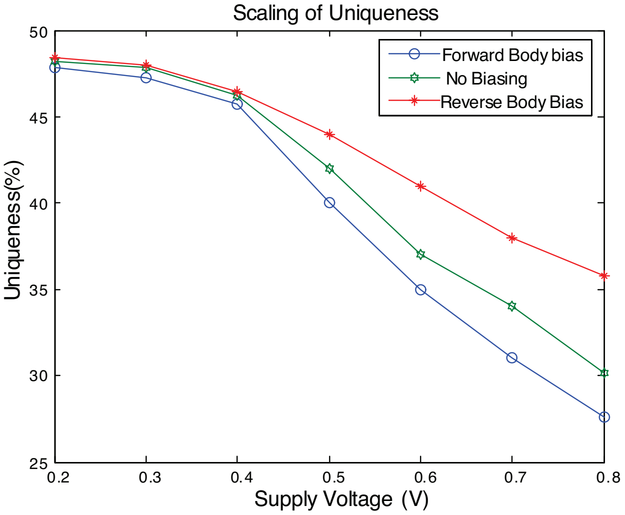

Fig. 4. Scaling of Uniqueness with Supply Voltage and Body Bias

Measuring reproducibility: The reproducibility was determined by comparing the digital signature of the same IC under different environmental variables, in our case, temperature. A single IC instance was subjected to temperatures ranging from $-15\,^{\circ}$C to $65\,^{\circ}$C degree centigrade, at intervals of $10\,^{\circ}$C. The digital signature of the PUF at each of these temperatures was obtained using the method specified above. The reproducibility of each IC instance was determined as the ratio of average number of bits that are reproduced to the total number of bits.The overall reproducibility was calculated as the average of reproducibilities for all of the ICs.

Scope of the experiments: Both the uniqueness and reproducibility are calculated for the same PUF architecture operating at supply voltages ranging from 0.2 V to 1 V and substrate bias voltage ranging from -0.2 V to +0.2 V at each of these supply voltages.

V. Results and Discussion

Figure 4 (middle line at 0 V bias) presents the scaling of uniqueness with a varying supply voltage. Firstly, it can be observed that the uniqueness of the PUF circuit increases with a decreasing supply voltage. This is because CMOS is more sensitive to process variation at lower supply voltages. Comparing Figure 2 and Figure 4, it can be seen that there is a direct relationship between variability and uniqueness of the PUF circuit. Also, in the subthreshold region the value of uniqueness tends to reach the theoretical maximum of 50%.

[2] This has a different effect from general environmental variables such as temperature that affect all oscillators.

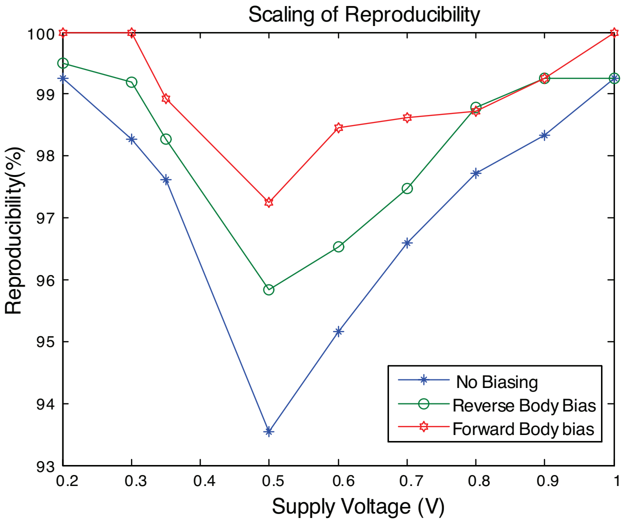

Fig. 5. Scaling of Reproducibility with Supply Voltage and Body Bias

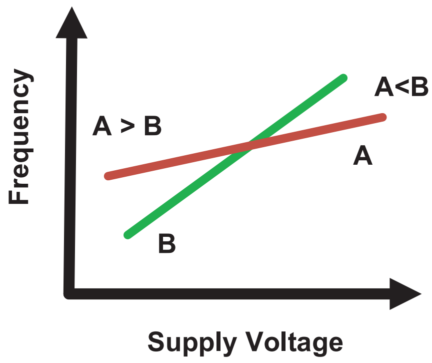

Fig. 6. Representation of Scaling of frequencies of Ring Osciallators

Secondly, it is observed from Figure 4 that reverse body bias increases the uniqueness metric. Forward body bias on the other hand, increases the circuit's stability towards process variation and therefore leads to worse uniqueness. Thirdly, the effect of body bias on the uniqueness of the PUF decreases with a decreasing supply voltage. This is because the high sensitivity of the PUF to process variation at lower voltages mitigates any effect due to body bias.

Figure 5 (bottom line) presents the results of the second experiment. It indicates the relationship between reproducibility and supply voltage. It is observed that at no bias condition, the reproducibility is around 98% percent, at a supply voltage of 0.2V and 99% at a supply voltage of 1V. However, the reproducibility is around 93% at a supply voltage of 0.5V. The PUF is more stable (higher reproducibility) when the supply voltage is around the nominal voltage or well below the threshold voltage. In the intermediate regions, the reproducibility degrades. This phenomenon is related to the way the frequencies of different ring oscillators scale with supply voltage. A fictional representation of the scaling of frequency of two different ring oscillators in the same IC is shown in Figure 6. The slopes of the oscillator A and B are different because of process variation. They converge at an intermediate supply voltage between the nominal voltage and subthreshold voltages. At nominal voltage, Oscillator B is faster than A and at subthreshold voltages Oscillator A is faster than B. In the intermediate voltages, the difference between the frequencies of the two oscillators is small, and even small disturbances introduced due to changes in temperature, noise etc. tend to flip the bits used for signature generation of PUFs. Therefore, for achieving better reproducibility, the supply voltage of PUF circuit must be maintained at either nominal voltage or well below threshold voltage.

Figure 5 also shows the effect of body bias on the reproducibility of the PUF. It is observed that, the effect of body bias is negligable except around the threshold voltage, which is an undesirable region. Therefore, we pick our optimum bias based on uniqueness only.

Overall, it is observed that operating the PUF circuit at 0.2V yields the best uniqueness. Also, there is just a small gain in reproducibility when FBB is applied as compared to RBB. Therefore, it would be best to operate the PUF at sub threshold voltages with RBB to achieve good balance between uniqueness and reproducibility. Compared to a baseline configuration of no bias and nominal voltage, operating the PUF at 0.2 V with FBB increases its uniqueness by 18% and reproducibility by 7%.

VI. Conclusion

Circuit level techniques provide key tuning knobs for improving the performance of physically uncloneable functions (PUFs). We have shown that operating the PUF at subthreshold voltages increases the uniqueness of the PUF. Also, it is best to operate PUFs with a forward body bias to increase their stability. Compared to a base line configuration, our method improved the uniqueness by 18% and reproducibility by 7%. Therefore, apart from architectural optimization, circuit level considerations like supply voltage and body bias can improve the reliability of PUFs.

Future Work

Apart from uniqueness and reproducibility, we intend to study the effect of supply voltage and body bias on the power dissipation and the access time of the PUF. Also, we would investigate the effect of power supply noise, inductive coupling and other noise sources on the performance of PUFs. We are presently working on implementing an ASIC to prove the effectiveness of our methodology.

References

[1] B. Yang, K. Wu, and R. Karri, “Scan based side channel attack on dedicated hardware implementations of data encryption standard,” in *Test Conference, 2004. Proceedings. ITC 2004. International*, Oct. 2004, pp. 339–344.

[2] R. Pappu, “Physical one-way functions,” *PhD thesis,Massachusetts Institute of Technology*, 2001.

[3] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, “FPGA intrinsic PUFs and their use for IP protection,” ser. Lecture Notes in Computer Science, vol. 4727. Springer Berlin / Heidelberg, 2007, pp. 63–80. [Online]. Available: http://www.springerlink.com/content/u64160h472125824/

[4] B. Skoric, G.-J. Schrijen, P. Tuyls, T. Ignatenko, and F. Willems, “Secure key storage with PUFs.” Springer London, 2008, pp. 269–292. [Online]. Available: http://www.springerlink.com/content/g282216g34w26821/

[5] C. Neau and K. Roy, “Optimal body bias selection for leakage improvement and process compensation over different technology generations,” in *ISLPED ’03: Proceedings of the 2003 international symposium on Low power electronics and design*. New York, NY, USA: ACM, 2003, pp. 116–121.

[6] J. Tschanz, J. Kao, S. Narendra, R. Nair, D. Antoniadis, A. Chandrakasan, and V. De, “Adaptive body bias for reducing impacts of die-to-die andwithin-die parameter variations on microprocessor frequency and leakage,” in *Solid-State Circuits Conference, 2002. Digest of Technical Papers. ISSCC. 2002 IEEE International*, vol. 1, San Francisco, CA, USA, 2002, pp. 422–478.

[7] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in *DAC ’07: Proceedings of the 44th annual conference on Design automation*. New York, NY, USA: ACM, 2007, pp. 9–14.

[8] A. Maiti and P. Schaumont, “Impact and compensation of correlated process variation on ring oscillator based puf,” in *FPGA ’09: Proceeding of the ACM/SIGDA international symposium on Field programmable gate arrays*. New York, NY, USA: ACM, 2009, pp. 285–285.

[9] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, “Design and implementation of PUF-based ”unclonable” RFID ICs for anti-counterfeiting and security applications,” in *RFID, 2008 IEEE International Conference on*, Apr. 2008, pp. 58–64.

[10] G. Hammouri and B. Sunar, “PUF-HB: A tamper-resilient HB based authentication protocol,” ser. Lecture Notes in Computer Science, vol. 5037. Springer Berlin / Heidelberg, 2008, pp. 346–365. [Online]. Available: http://www.springerlink.com/content/196791v64p37n130/

[11] M. B. Henry and L. Nazhandali, “Hybrid super/subthreshold design of a low power scalable-throughput FFT architecture,” ser. Lecture Notes in Computer Science, vol. 5409. Springer Berlin / Heidelberg, 2009, pp. 278–292. [Online]. Available: http://www.springerlink.com/content/p77l06h473786177/