A Stochastic Approach to Analog Physical Unclonable Function

Troy Bryant, Sreeja Chowdhury, Domenic Forte, Mark Tehranipoor, and Nima Maghari
Department of Electrical and Computer Engineering
University of Florida
Gainesville, Florida, USA
tbbryant@ufl.edu

***Abstract* — As cybersecurity becomes increasingly relevant with advancing technology, Physically Unclonable Functions (PUFs) have become a promising technique that utilize process variation and device mismatch to create unique device identifiers, secure keys, and other security features that are virtually impossible to duplicate. Many PUF circuits with diverse characteristics have been proposed, all of which exhibit a clear tradeoff between reliability, robustness, and size. This paper proposes a novel PUF which utilizes the nature of stochastic flash analog-to-digital (ADCs) to minimize hardware without sacrificing reliability or robustness against cloning. The proposed PUF creates a unique device identifier by employing the comparators used in a stochastic ADC, which are designed for maximum offset voltage due to device mismatch. The proposed PUF was modeled and simulated using a 130nm CMOS process. Simulation results show that the PUF has a normalized inter-hamming distance (uniqueness) of 48.5% and is reliable with a normalized average bit flip of 2-3% over ±10% variance in supply voltage and temperatures up to 100°C.**

Keywords — PUF, Unique Device Identifier, stochastic ADC

I. INTRODUCTION

Electronic counterfeiting is a continuous and persistent problem which has severe impacts on many sectors of the industry including military, pharmaceutical, aircraft, automotive, etc. Thus, counterfeit detection has received considerable attention from researchers in recent years. Many promising approaches in counterfeit detection for new ICs rely on Physically Unclonable Functions (PUFs). PUFs have been widely researched to provide unique unclonable chip IDs to prevent cloning, recycling, overproduction of ICs and to secure the IC supply chain [1],[2]. The main objectives of a PUF are to provide authentication, data-integrity and privacy. A PUF circuit exploits the process variations of transistors to generate a unique response corresponding to a definite challenge. There is a one-to-one relationship between a challenge and its corresponding response which cannot be reproduced by any other challenge-response pair. A PUF has a few unique metrics [3] which are essential to make the purpose of it successful and these are:

- Uniqueness: The uniqueness of a PUF is how precisely it can identify a single chip from a group of chips and can be measured by Inter-chip Hamming Distance.
- Reliability: The output of a PUF for a definite chip should be reliable and should be consistent with change in environmental and circuit conditions. This is measured by Intra-chip Hamming Distance.

Extensive research regarding PUFs has been conducted mostly in digital ICs and also in a few analog and RF ICs. The first PUFs reported were optical PUFs [4] where the number of challenge-response pairs were not enough to prevent brute force attacks. Digital PUFs soon followed and were explored with process variations in ring oscillators [5] and digital arbiters. Attempts have been made to increase reliability and uniqueness by reducing aging effects in both Application Specific Integrated Circuits (ASICs) [6],[7] and Field Programmable Gate Arrays (FPGAs) [8] implementations. The initial startup response of memory cells has been utilized to produce memory PUFs like SRAM PUFs [9],[10], D Flip-Flop PUFs, and Butterfly PUFs [11]. For analog/mixed signal applications, a few recent advances include an extremely low power (38µW) mixed signal PUF implemented in a 90nm CMOS process with a bit error rate of less than 0.1% at 125°C and 10% voltage variation [12] and monostable static PUFs implemented with cascoded current mirrors in a 65nm CMOS process with 1.9-5.8%native bit stability at 0.6-1V [13]. But all of these implementations do not talk about the hardware overheard required to implement these PUFs in digital/analog ICs for device authentication or cryptographic key generation. The amount of hardware overhead is becoming more critical in analog/mixed signal ICs, which continue to shrink in size and have an extremely limited number of input/output pins.

This paper introduces a novel PUF to be implemented in a stochastic ADC, or alternatively any circuit that employs a number of comparators. The proposed PUF utilizes some of the many comparators within a stochastic ADC to create a reliable and robust unique device identifier with minimal additional hardware. The length of the identifier and the number of challenge-response pairs can be easily increased, as it is not uncommon for accurate stochastic ADCs to contain thousands of comparators.

This paper is organized as follows. Section II briefly explains the concepts of a stochastic ADC. Section III describes the concepts of the proposed PUF. The simulation results are presented in Section IV. Finally, Section V concludes this paper.

II. TRADITIONAL STOCHASTIC FLASH ADC

In an N-bit Flash ADC, 2^{N-1} equally spaced comparators are used to quantize an input signal. The thresholds of the comparators are accurately set by a resistor ladder such that they are equally spaced by 1 LSB. In practice, the inherent random offsets add to the comparator thresholds causing the actual flash ADC transfer function to deviate from the ideal one.

A stochastic flash ADC uses a similar configuration to the flash ADC, but there is no resistor ladder. The random inherent offset voltages are used to set the comparator trip points, as shown in Fig. 1, and these trip points are used to quantize the input voltage. A large number of minimum-sized comparators are used in stochastic ADCs in order to create a Gaussian distributed input offset voltage with mean μ and variance σ^2. The comparator outputs appear to be random, but the total sum of the comparator outputs increases monotonically with increasing input voltage. The transfer function of the traditional stochastic ADC follows the cumulative distribution function (CDF) of the input offset voltage distribution. The linear range of the stochastic ADC is determined by the variance of the comparator offset, and is very limited compared to other ADCs. Different comparator topologies can be used to increase the maximum possible voltage offset caused by mismatch, thus increasing the linear range of the ADC. This will be discussed further in Section III.

The number of comparators in a stochastic ADC must be enough so that the transfer function accurately resembles the CDF of the comparator offset. In [15], the average number of comparators, *n*, necessary to achieve N effective bits in a stochastic ADC is formulated to be

$$n = 4^N - 1 + \sqrt{4^{2N} + 2^{2N+1}} \tag{1}$$

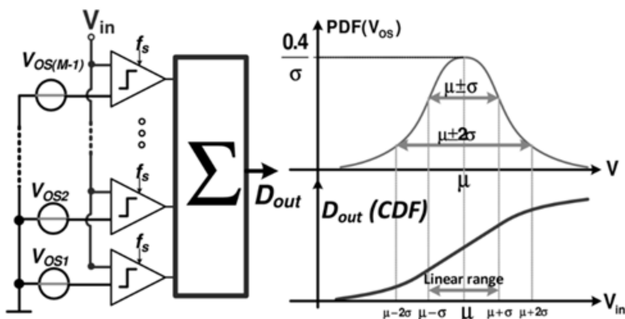

Fig. 1. Functional stochastic ADC with comparator offset PDF and CDF [14]

III. Proposed PUF Circuit

As mentioned in the previous section, the comparators used in stochastic ADCs are designed to maximize the effects of process variation and device mismatch, two characteristics that are critical to PUF implementation. The proposed PUF shares the comparators in a stochastic ADC (alternatively the PUF can be implemented in other designs that require many comparators) in order to reduce the amount of additional hardware necessary to generate a unique identifier.

A block diagram of the PUF circuit is shown in Fig. 2, it consists of an array of comparators that are shared with the stochastic ADC and digital control circuitry.

A. Comparator Array

In the proposed PUF an array of N-comparators is used to create an N-bit unique ID. Each comparator in the array is used to determine a single bit of the ID. To determine each bit, both comparator inputs are tied to the same reference voltage, V_{ref}, causing each comparator to output a 1 or a 0 depending on whether its offset voltage is positive or negative, respectively.

A critical property of a PUF is to provide a very reliable and repeatable response. The comparators used in the proposed PUF are designed to be minimum sized in order to maximize the offset voltage. Due to the fact that each comparator offset is random, it is a possibility that the offset voltage could be smaller than the input noise of the comparator, which has been increased due to the minimum device sizes used. This adversely affects reliability of the PUF, as the bit now depends on noise instead of the offset voltage. One way to combat this is to increase the σ of the comparator offset without minimizing devices, thereby decreasing the probability that a very small offset voltage will occur without increasing noise. This paper uses two comparator topologies to demonstrate the effects of offset voltage variability in the proposed PUF. Fig. 3(a) shows a traditional NAND-based comparator [15]. Fig. 3(b) shows a 3-Latch NAND-based comparator that increases the input offset voltage by increasing inherent mismatch [14]. Both comparators in Fig. 3 are fully digital and can be easily implemented using digital standard cells.

The comparator array of the proposed PUF can be easily modified to meet the level of security needed for a given device. According to (1), a stochastic ADC will employ, at least, hundreds of comparators. Thus, with almost no additional circuitry required on-chip it is possible to increase the number of comparators in an array to lengthen the ID. It is also possible to increase the number of challenge-response pairs by employing multiple comparator arrays in each PUF.

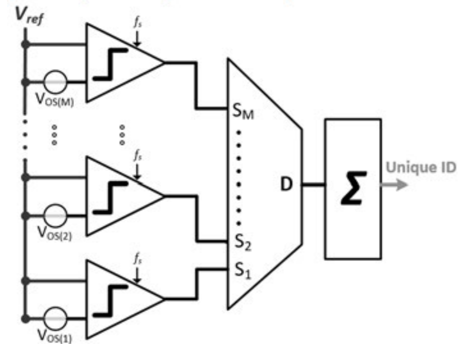

Fig. 2. Block diagram of proposed PUF circuit implemented in stochastic ADC

B. Digital Control Circuitry

The digital control circuitry is the only additional hardware the proposed PUF requires in order to generate a unique ID. The main functions of the digital circuitry are to perform an averaging function for each comparator, and to properly decode any challenge inputs.

A simple averaging function is implemented digitally in order to help combat the effects of noise. The averaging block, denoted by Σ in Fig. 2, samples each comparator and uses a running sum to determine whether the ID bit is a 0 or a 1 based on a determined threshold. For the purposes of this paper, the threshold was set to be half of the number of samples. Therefore, if a sampled comparator produced more 1's than 0's the ID output would be a 1. It would be possible to add more thresholds to determine the strength of an ID bit. For example, if a sampled comparator produced all 1's or all 0's, the corresponding ID bit would be considered a strong 1 or strong 0, respectively.

Conversely, a weak 1 or weak 0 may correspond to a comparator with a smaller offset voltage whose output occasionally switches due to noise.

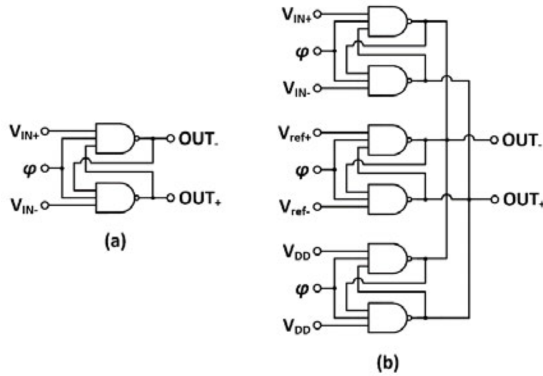

Fig. 3. (a)Traditional NAND-based comparator and (b)3-Latch extended range comparator with increased offset

As discussed in Section III.A, it would be possible to employ multiple comparator arrays in order to increase the number of challenge-response pairs in the PUF. This is implemented by using a digital decoder which is not shown in Fig. 2. In this case, the challenge input will be the address of the desired comparator array.

IV. Simulation Results

The proposed PUF circuit in Fig. 2 was designed and simulated in a 130nm CMOS process. To demonstrate the offset voltage variance between the traditional NAND-based comparator and the 3-latch extended range comparator a Monte Carlo simulation was run for each comparator and the offset voltage was plotted for 1000 sampled comparators, as shown in Fig. 4. It can be seen that the input offset voltage of both comparator topologies is also approximately Gaussian, as expected. The traditional NAND-based comparator showed a standard deviation, $\sigma_{Voffset}$, of approximately 65mV and the 3-latch comparator showed an increased $\sigma_{Voffset}$ of 135mV. This increased offset voltage effectively reduces the probability of weak 1's and weak 0's as will be seen in the following simulations.

To demonstrate the effects of noise on the two comparator topologies, a single comparator is sampled 63 times and these samples are summed as part of the digital averaging block, thus displaying how many of the 63 samples were 1's. In a noiseless system, the comparator outputs would not change and this simulation would return either a 63 or 0 if the offset voltage was positive or negative, respectively. When noise is introduced, the outputs of those comparators with offset voltages near 0V will be affected by noise. A Monte Carlo simulation is run for both comparator topologies and 63 samples of a single comparator are summed 512 times. The results of the traditional NAND-based comparator and the 3-latch comparator are displayed as histograms in Fig. 5. As expected, the majority of both comparator topologies provide strong outputs. Due to the smaller offset voltage variation in the traditional NAND-based comparator, it has more weak outputs than the 3-latch comparator. Additionally, the traditional topology resulted in some comparators on the midpoint threshold (a sum of about 31 in this case), meaning that the ID bit controlled by those comparators can easily be flipped, even with averaging. This condition is remedied by using the 3-latch comparator topology with increased offset voltage, which shows no weak ones/zeros at the midpoint.

To demonstrate the effects of the digital averaging block on noise, the previous simulation is repeated, but fewer samples are taken by the averaging block. Fig. 6 shows the results of 512 3-latch comparators that were only sampled 15 times before summing the outputs, instead of the 63 times shown in Fig. 5. It can be seen that there are still very few comparators with offset voltages small enough to be affected by noise, but those that are affected are much closer to the midpoint (for 15 samples, the midpoint is 7) with fewer samples. Furthermore, if no averaging at all were performed, those comparators with weak outputs would drastically degrade the reliability of the PUF since the corresponding ID bits would be unpredictable and unrepeatable.

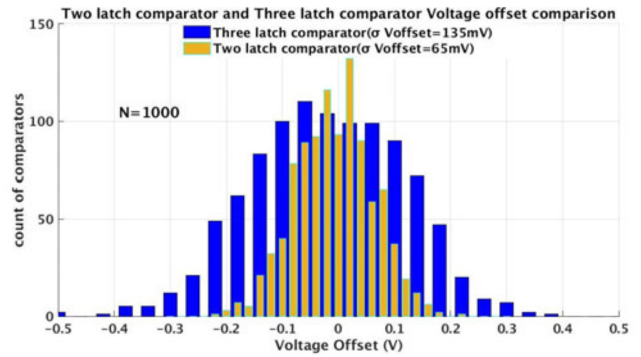

Fig. 4. Gaussian distribution of traditional NAND-based comparator and 3-Latch extended range comparator

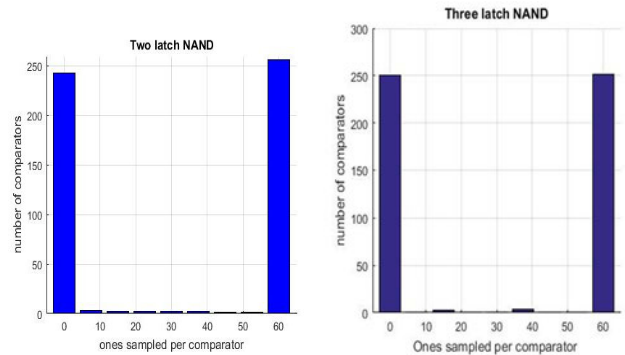

Fig. 5. 63 samples of traditional NAND-based comparator (left) and 3-latch NAND-based comparator (right) summed 512 times each

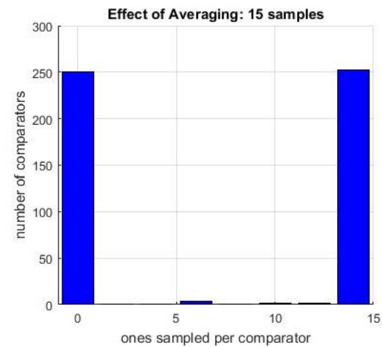

Fig. 6: 15 samples of 3-Latch extended range comparator summed 512 times

To characterize the uniqueness and reliability of the proposed PUF circuit, a comparator array was simulated to produce a 64-bit identifier output. The uniqueness of a PUF is measured by the inter-Hamming Distance (HD), which is ideally 50%. It can be seen from Fig. 7 that the traditional and 3-latch comparators gave a normalized inter-HD of approximately 47.7% and 48.5%, respectively. The reliability of the proposed 3-latch comparator based PUF was determined by measuring the intra-HD (ideally 0%) over varying temperature and supply voltage. It can be seen from Fig. 8 that the PUF circuit is reliable up to 100°C as the normalized intra-HD is on average, less than 2%. The normalized average intra-HD over the range of 27°C to 100°C is 1.27%. Similarly, Fig. 9 shows that the proposed circuit is reliable over ±10% variation in voltage supply as the normalized inter-HD is, at most, approximately 3%, with the average being 2.7%.

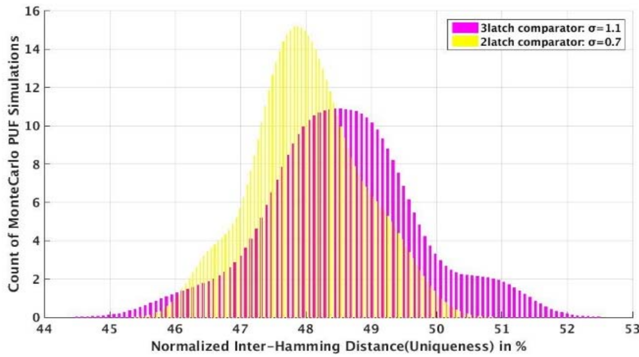

Fig. 7: Uniqueness of Traditional and 3-Latch Comparator Based PUF

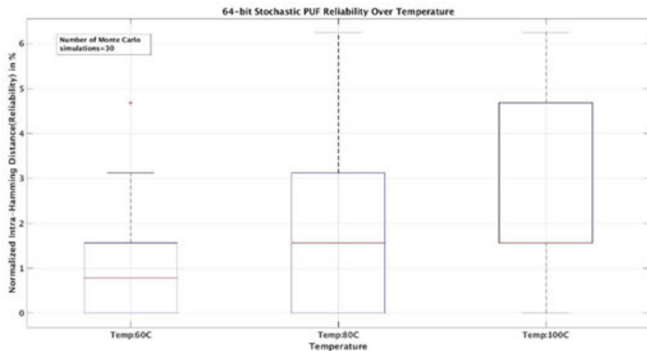

Fig. 8: Reliability of Stochastic PUF Over Temperature

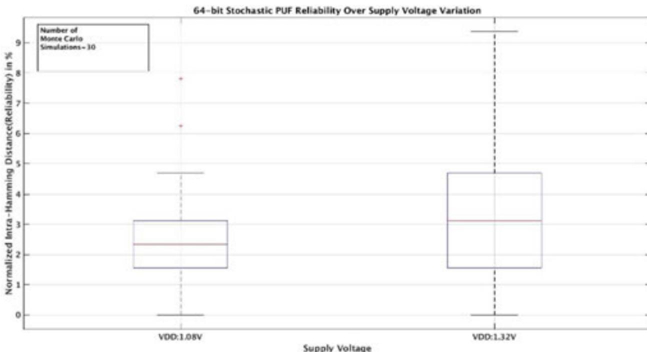

Fig. 9: Reliability of Stochastic PUF Over ±10% VDD

V. Conclusion

This paper proposed a novel PUF which can be easily implemented, with minimal hardware overhead, in stochastic ADCs or other structures that employ a large number of comparators. The increased voltage offset and minimum device sizes of the stochastic ADC comparators is shown to be advantageous for the proposed circuit. Furthermore, different comparator topologies and digital averaging are presented as solutions to combat the negative effects of stochastic ADC comparators, increased noise. Finally, the reliability and uniqueness of the proposed PUF are verified through simulations in a 130nm CMOS process. The proposed PUF has a normalized inter-HD of 48.5% and is reliable with a normalized average intra-HD of 2-3% over 10% voltage variations and at temperatures of up to 100°C.

References

[1] C. Herder, M. D. Yu, F. Koushanfar and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," in Proceedings of the IEEE, vol. 102, no. 8, pp. 1126-1141, Aug. 2014.

[2] Blaise Gassend, Dwaine Clarke, Marten van Dijk, and Srinivas Devadas. 2002. Silicon physical random functions.in Proceedings of the 9th ACM conference on Computer and communications security (CCS '02), Vijay Atluri (Ed.). ACM, New York, NY, USA, 148-160.

[3] A. Maiti and P. Schaumont, "The Impact of Aging on a Physical Unclonable Function," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 22, no. 9, pp. 1854-1864, Sept. 2014.

[4] JPappu, R. Physical One-way functions Massachusetts Institute of Technology,MA, Massachusetts Institute of Technology,MA, 2001.

[5] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," 2007 44th ACM/IEEE Design Automation Conference, San Diego, CA, 2007, pp. 9-14.

[6] J. W. Lee, Daihyun Lim, B. Gassend, G. E. Suh, M. van Dijk and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," VLSI Circuits, 2004. Digest of Technical Papers. 2004 Symposium on, 2004, pp. 176-179.

[7] Daihyun Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk and S. Devadas, "Extracting secret keys from integrated circuits," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 13, no. 10, pp. 1200-1205, Oct. 2005.

[8] J. Guajardo, S. S. Kumar, G. J. Schrijen and P. Tuyls, "Physical Unclonable Functions and Public-Key Crypto for FPGA IP Protection," 2007 International Conference on Field Programmable Logic and Applications, Amsterdam, 2007, pp. 189-195.

[9] A. Hosey, M. T. Rahman, K. Xiao, D. Forte, and M. Tehranipoor, "Advanced Analysis of Cell Stability for Reliable SRAM PUFs," 2014 IEEE 23rd Asian Test Symposium, 2014.

[10] K. Xiao, M. T. Rahman, D. Forte, Y. Huang, M. Su, and M. Tehranipoor, "Bit Selection Algorithm Suitable for High-Volume Production of SRAM-PUF," Hardware-Oriented Security and Trust (HOST), 2014.

[11] S. S. Kumar, J. Guajardo, R. Maes, G. J. Schrijen and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on, Anaheim, CA, 2008, pp. 67-70.

[12] S. Stanzione, D. Puntin and G. Iannaccone, "CMOS Silicon Physical Unclonable Functions Based on Intrinsic Process Variability," inIEEE Journal of Solid-State Circuits, vol. 46, no. 6, pp. 1456-1463, June 2011.

[13] A. B. Alvarez, W. Zhao and M. Alioto, "Static Physically Unclonable Functions for Secure Chip Identification With 1.95.8% Native Bit Instability at 0.61 V and 15 fJ/bit in 65 nm," in IEEE Journal of Solid-State Circuits, vol. 51, no. 3, pp. 763-775, March 2016.

[14] A. Fahmy, J. Liu, T. Kim and N. Maghari, "An All-Digital Scalable and Reconfigurable Wide-Input Range Stochastic ADC Using Only Standard Cells," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 62, no. 8, pp. 731-735, Aug. 2015.

[15] S. Weaver, B. Hershberg, P. Kurahashi, D. Knierim and U. K. Moon, "Stochastic Flash Analog-to-Digital Conversion," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 57, no. 11, pp. 2825-2833, Nov. 2010.