

A Stochastic All-Digital Weak Physically Unclonable Function for Analog/Mixed-Signal Applications

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—Physically Unclonable Functions (PUFs) are a promising security technique which utilize the random process variation in silicon fabrication in order to create unique identifiers and other security features that are impossible to recreate exactly. This paper builds upon and evaluates a weak PUF which employs dynamic latched comparators and their random input offset voltages to create a chip-specific identifier. The proposed PUF can be used in analog/mixed-signal (AMS) chips due to the analog characteristics of the comparators employed. Because comparators are a fundamental block in AMS applications, the proposed PUF can reuse comparators in an AMS chip to generate unique identifiers with minimal hardware overhead. Additionally, the comparators tested in this work can be created with digital components, making this PUF suitable for use in digital chips as well. The proposed PUF is fabricated using a 0.13 μm CMOS process. Measurements show that the PUF achieves a normalized intra-Hamming Distance (HD) of less than 0.15% and 0.96% across 0°C-80°C and 0.8V-1.4V, respectively. The normalized inter-HD is 48.5% for a 64-bit PUF output key. The power consumption of the PUF is 1.5 nJ/bit with a throughput of 4Mb/s.

Keywords—Physically Unclonable Function, Dynamic Latched Comparator, Physically Obfuscated Key, Analog PUF

I. INTRODUCTION

The Internet of Things (IoT) has ushered in a new era in which technology is advancing at an unprecedented rate. Although the idea behind the IoT is to create a connected, efficient, and safe environment, countless security challenges must be faced before this can become a reality. One such challenge is electronic counterfeiting, which can harm both industries and its consumers through cloning, recycling, repackaging, and other methods.

A widely researched approach in counterfeit detection is the physically unclonable function (PUF). These security primitives are capable of chip identification and authentication [1], as well as hardware piracy and counterfeiting prevention [2], [3]. PUFs are implemented at the chip level and generate reliable chip-specific responses based on a given challenge. The uniqueness of a PUF response is achieved by utilizing random process variations and device mismatch, making a PUF virtually impossible to recreate exactly. Furthermore, a PUF must be robust and reliable across environmental variations, including noise, voltage supply, and temperature variations, in order to produce a stable response under any

condition. Uniqueness and reliability are two unique PUF metrics that are measured by the inter-chip Hamming Distance (HD) and intra-chip HD, respectively.

An extensive amount of research involving PUFs has been carried out, resulting in a wide range of PUF implementations. Optical PUFs [4] were the first reported PUF, but generally lacked a large number of challenge-response pairs (CRPs), allowing adversaries to more easily reproduce the function through brute force attacks. Soon after, digital PUFs were introduced by utilizing inherent process variations in digital arbiters and ring oscillators [5]. As digital PUFs became more popular, research to reduce the aging effects in application specific integrated circuits (ASICs) and field programmable gate arrays (FPGAs) [6] was performed in order to increase reliability and uniqueness. Memory PUFs, such as SRAM PUFs [7], [8], D Flip-Flop PUFs, and Butterfly PUFs [9], utilize the initial startup response of memory cells, an integral part of nearly every electronic system, to produce a reliable and unpredictable response. Some recent advances in analog/mixed-signal PUFs include an extremely low power (38 μW) CMOS PUF with a bit error rate of less than 0.1% at 125°C or $\pm 10\%$ voltage supply variation [10], as well as an ultra-compact (3.07 $\mu\text{m}^2/\text{bit}$) proportional to absolute temperature PUF with a bit error rate of 3.5% and 1.004% across temperature and voltage supply variations, respectively [11].

Conventionally, all PUFs are categorized as either a strong or a weak PUF, depending on the number of CRPs that PUF contains. The number of CRPs in a strong PUF will increase exponentially as the PUF is scaled larger, while the number of CRPs in a weak PUF will only increase linearly. Weak PUFs can have as few as one CRP, in which case it is known as a physically obfuscated key (POK) [11].

This paper builds upon and evaluates the weak analog/mixed-signal PUF, first introduced in [12], which employs dynamic latched comparators in order to produce a robust and reliable chip-specific identifier. The PUF leverages each comparator's inherent input offset voltage, which is determined by random process variation and device mismatch. The digital control circuitry discussed in this work determines the strength of each comparator so that the user may easily mask unstable bits and thus, obtain a more reliable and robust response. Test chips with two different PUF implementations were fabricated using a 0.13 μm CMOS process, exhaustively tested, and the measurement results presented. The measurements show that the proposed PUF is reliable across extreme environmental variations, with an intra-HD less than 0.15% and 0.96% across 0-80°C and 0.8-1.4V, respectively.

This work was supported in part by the National Science Foundation under Grant No. 1610075. This material is also based upon work supported by the National Science Foundation Graduate Research Fellowship under Grant No. DGE-1315138.

The uniqueness of this PUF is verified with an inter-HD of 48.5% for a 64-bit output key. The fabricated design requires an energy per bit of 1.5 nJ/bit at a throughput of 4Mb/s, but, as discussed in Section III.D, an optimized design can result in an energy per bit as low as 34.5 pJ/bit at 4Mb/s.

The data provided by the Electronic Resellers Association International (ERAI) in collaboration with the Information Handling Services Inc. (IHS) shows that electronic counterfeits have quadrupled since 2009 and have, on average, increased by 25% every year since 2001[13]. One out of every four counterfeit parts reported was an analog integrated circuit (IC). Such a huge increase in analog counterfeit ICs clearly suggests the importance of security and identification primitives such as PUFs in analog ICs. The PUF presented in this paper has the following advantages:

1. **Easy identification in analog/mixed-signal (AMS) chips:** The proposed PUF is essentially analog with regards to the characteristics which can be used for identification of any AMS chip.
2. **Minimal hardware overhead:** The PUF design uses comparators and since comparators form a fundamental part in almost all AMS ICs, the proposed design can reuse comparators in any AMS chip to form a PUF with minimal hardware overhead.
3. **Utilization in digital chips:** The comparators used can be made of digital components and logic gates, making the PUF suitable for digital chips as well.

This paper is organized as follows. Section II provides a brief background on dynamic latched comparators and their input offset voltage. Section III introduces the concept of the proposed PUF as well as its implementation. Section IV presents the measurement results of the proposed PUF. Finally, Section V concludes this paper.

II. DYNAMIC LATCHED COMPARATORS

The comparator is a critical component in many analog-to-digital converters (ADCs), and has a significant impact on the overall performance of the ADC. Dynamic latched comparators are known for their high-speed, low-power, and small area, so it is not surprising that they have become widely used in ADCs. The dynamic aspect of dynamic comparators drastically reduces static power consumption, but introduces kickback noise into the system. Additionally, dynamic comparators still experience reduced accuracy due to random input offset voltage. Offset cancellation and kickback noise reduction techniques are a widely researched topic with many promising solutions. This section describes the operation of a dynamic latched comparator and briefly analyzes its input offset voltage.

A. Operation of the Dynamic Latched Comparator

The “Lewis-Gray” comparator [14], widely used in pipeline ADCs, is a variant of the conventional dynamic latched comparator and is shown in Fig. 1. It is a fully differential dynamic comparator with input transistors M_1 – M_4 . The regenerative latch is realized using cross coupled inverters, represented by transistor pairs M_5M_{10} and M_6M_{11} of Fig. 1.

The operation of the dynamic comparator begins with the reset phase when CLK goes low. In the reset phase, the

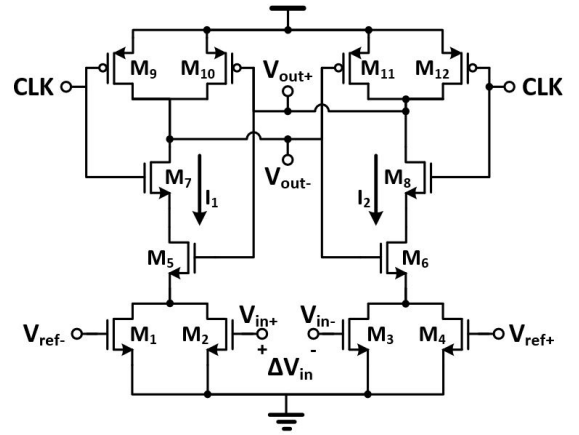


Fig. 1. “Lewis-Gray” dynamic latched comparator structure analyzed in [14]

positive feedback loop between the cross coupled inverters is broken by transistors M_7 and M_8 operating in the cutoff region. Meanwhile, transistors M_9 and M_{12} are turned on which pulls V_{out+} and V_{out-} up to V_{DD} in order to define a start condition for the comparison phase. The output of the comparator is determined during the comparison phase when CLK goes high. In the comparison phase, transistors M_9 and M_{12} turn off, leaving the node capacitances at the outputs charged to V_{DD} from the reset phase. Meanwhile, transistors M_7 and M_8 are turned on, closing the positive feedback loop of the cross coupled inverters. The input transistors M_1 – M_4 operate in the triode region and thus act as voltage controlled resistors. I_1 is the total current through transistors M_1 and M_2 , while I_2 is the total current through transistors M_3 and M_4 . The positive feedback quickly sets the outputs based on the race condition between I_1 and I_2 , which are discharging V_{out-} and V_{out+} , respectively. The larger current pulls the corresponding output low, causing the positive feedback to set the other output high. The reset phase begins again as CLK goes low, and the cycle restarts.

B. Input Offset Voltage Analysis

If no mismatch exists within the dynamic comparator, then a balanced state is reached. In the balanced state, both sides of the “Lewis-Gray” comparator are identical, so V_{out+} is equal to V_{out-} . However, a realistic circuit will experience mismatch caused by many different factors, and thus the outputs will not be equal. The input offset voltage, ΔV_{in} , is defined as the compensation voltage required at the input to set the outputs to be equal, as in the balanced state. ΔV_{in} is considered to be the static input offset voltage and is dominated by mismatches in transistor parameters μC_{ox} and V_{th} [14], where μ is the charge-carrier effective mobility, C_{ox} is the oxide capacitance, and V_{th} is the threshold voltage. An extensive analysis of the static input offset voltage of the “Lewis-Gray” comparator was carried out in [14]. It was shown that transistors M_9 and M_{12} have a negligible contribution to the static offset because they are off during the comparison stage. From the equations derived in [14] for each transistor pair mismatch, it can be seen that the random mismatch in V_{th} and μC_{ox} of each transistor M_1 – M_8 and M_{10}

– M_{11} , contribute to the overall static voltage offset of the comparator. The effects of C_{ox} were combined with μ since they are both always in the form of a product. The random mismatch in threshold voltage, $\sigma_{V_{ti}}$, and random mismatch in mobility of NMOS and PMOS transistors, $\sigma_{\mu i/\mu_{n,p}}$ can be modeled as the following.

$$\sigma_{V_t}^2 = \frac{A_{V_t}^2}{WL} + (S_{V_{T0}}^2)D^2 \quad (1)$$

$$\sigma_{\mu i/\mu_{n,p}}^2 = \frac{A_{\mu}^2}{WL} + (S_{\mu}^2)D^2 \quad (2)$$

where W and L are the width and length, respectively, of the transistor pair. A_{V_t} , A_{μ} , S_{V_t} , and S_{μ} are all process dependent parameters. The rightmost term in (1) and (2) represent the variation in mismatch due to the distance D on chip between transistor pairs. The exact distance is also process dependent, but has only a minor contribution to the overall mismatch.

Parasitic capacitance is another dominant, process dependent contributor to offset voltage, although the effects of parasitic capacitor mismatch cannot be observed when calculating the static input offset voltage. Capacitor mismatch can only contribute to the offset voltage during a transient process. Thus, the offset created by mismatch in parasitic capacitors is called the dynamic offset voltage. Similar to before, the balanced state method is used to determine the dynamic input offset voltage, $V_{OS,CL}$, which, when applied to the input, sets the output voltages to be equal and their derivatives to be equal as well. Reference [14] derives the equation for the dynamic input offset voltage:

$$V_{OS,CL} = \left(\frac{\Delta C_L}{C_L} \right) \frac{I_{ds3} + I_{ds4}}{\mu_n C_{ox} \frac{W_2}{L_2} V_{ds1}} \quad (3)$$

where ΔC_L is the mismatch between the parasitic load capacitances at the outputs. It can be seen from (3) that the process dependent parameters, μ_n and C_{ox} , also affect the dynamic input offset voltage.

III. PROPOSED PUF DESIGN

As can be seen from the analysis in Section II.B, the inherent offset voltage of each comparator is sensitive to process variation and device mismatch. Additionally, as the need for high-performance analog-to-digital converters has increased, dynamic latched comparators have been optimized for low power, high speed, and small chip area. Thus, dynamic latched comparators demonstrate many suitable characteristics for use in PUF applications. Fig. 2 shows the block diagram of the proposed weak PUF presented in [12], which employs a chain of N comparators to create an N -bit unique ID. As can be seen, the inputs of each comparator are all connected to a single reference voltage, V_{ref} , causing the output of the comparator to be a 1 or 0 depending on whether the inherent offset voltage, V_{OS} , is positive or negative, respectively. In this work, two different implementations of the proposed PUF were created for testing, each PUF employing a different dynamic comparator. These two comparators, the double-tail and three-latch comparators, are described in further detail in subsections III.A and III.B, respectively.

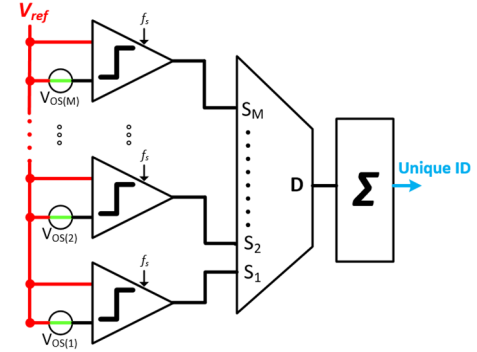


Fig. 2. Block diagram of proposed PUF circuit [12]

Because the comparator is a fundamental block among AMS applications, this PUF can reuse comparators in an AMS chip to produce a chip-specific identifier with minimal hardware overhead. The only additional hardware needed is the digital control circuitry, which consists of counters, logic gates, a MUX, and an averager (Σ in Fig. 2). The averager is a critical in combating noise and improving the reliability of the PUF response. The functions of the averager are discussed further in subsection III.C.

A. Double-Tail Comparator

One PUF was designed and fabricated using the modified double-tail dynamic comparator presented in [15] and shown in Fig. 3. This topology requires less stacking than the conventional dynamic latched comparator, allowing the double-tail comparator to operate reliably at lower supply voltages. Additionally, the intermediate stage represented by transistors M_{R1} and M_{R2} of Fig. 3 provides shielding between the input and output, thus reducing kickback noise compared to the conventional dynamic comparator. Low power is achieved through transistors M_{sw1} and M_{sw2} , which greatly reduce the static power consumption of the input stage. This low-power, low-voltage implementation would allow for an efficient PUF with a robust output across supply voltage variations. Furthermore, the reduced kickback will also increase robustness by reducing the effect of each comparator on the rest of the connected chain of comparators.

B. Three-Latch Extended Range Comparator

Comparators in most AMS systems are designed to minimize the input offset voltage, but in the proposed PUF a small input offset voltage intuitively reduces the reliability and robustness of the PUF response. If a comparator has an inherent offset voltage that is much smaller than the noise present in the circuit, then the comparator output and the corresponding unique ID bit will be dominated by noise, and thus be considered unreliable. In order to increase reliability and robustness, the second PUF was implemented using the three-latch, extended-range dynamic comparator presented in [16], and shown in Fig. 4. This comparator was designed for use in stochastic ADCs, so the standard deviation of the input offset voltage is doubled compared to the conventional NAND-based dynamic comparator. This is achieved by adding a third latch (the bottom latch in Fig. 4) to a pseudo-differential dynamic comparator in order to reduce the current through the comparator and introduce more device mismatch into the system. Furthermore, an all-digital implementation of

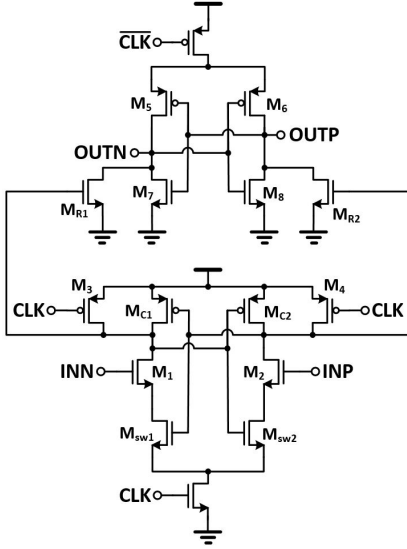


Fig. 3. Modified double-tail comparator introduced in [15]

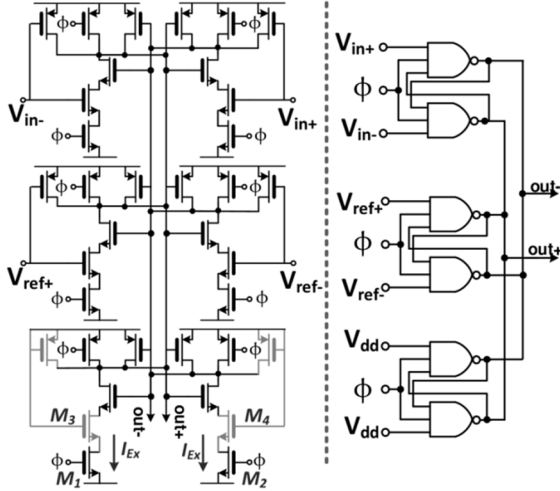


Fig. 4. Three-latch extended range comparator (left) and its digital implementation (right) introduced in [16]

this comparator can be achieved using NAND3 gates, as shown in Fig. 4.

C. Digital Averager

The digital averager, represented by Σ in Fig. 2, is implemented to reduce the effects of noise and, as a result, increase the reliability of the PUF. This is achieved by averaging each comparator output over a given number of cycles and determining the corresponding unique ID bit based on the majority output. In this work, the averaging concept is further extended to assign each unique ID bit into one of a number of bins set by user-defined thresholds. In the implemented PUF design, four bins were used to characterize each bit as a strong 1, a weak 1, a weak 0, or a strong 0. A comparator with a large input offset voltage will rarely be affected by noise, if at all. Thus, its output will be consistent and the corresponding ID bit is considered to be strong and reliable. On the other hand, a comparator with a small input offset voltage will be hindered by noise and will experience

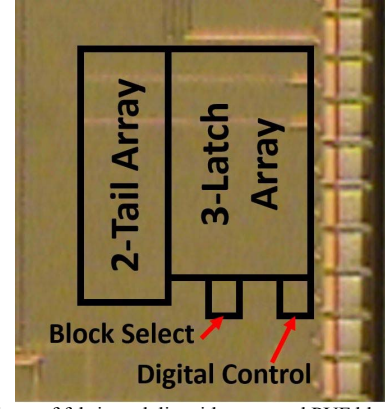


Fig. 5. Photo of fabricated die with proposed PUF blocks labeled

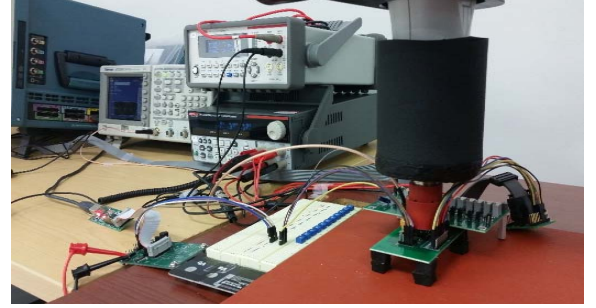


Fig. 6. Photo of test setup used during PUF measurements

occasional or frequent bit flips at its output. This corresponds to a weak and unreliable ID bit. The digital averager's built in characterization allows the user to easily mask unreliable bits, as explained in the measurement results of Section IV, in order to ensure a reliable and robust PUF output.

IV. TEST-CHIP MEASUREMENT RESULTS

The proposed PUF in Fig. 2 was fabricated using a 0.13 μm CMOS process. The die photo shown in Fig. 5 contains both implementations of the PUF mentioned in the previous section. Each die contains a double-tail array and a three-latch array (each with 448 comparators), as well as block selection and digital control circuitry. A total of 1792 bits were generated for each PUF implementation across 4 chips. Each comparator is sampled over 15 cycles and averaged to determine the corresponding unique ID bit. The strength of the ID bits are determined by the number of ones sampled from each comparator over the 15 cycles and are defined as follows:

- Strong 1: Number of 1's sampled ≥ 12
- Weak 1: $8 \leq \text{Number of 1's sampled} \leq 11$
- Weak 0: $4 \leq \text{Number of 1's sampled} \leq 7$
- Strong 0: Number of 1's sampled ≤ 3

The test setup used to measure each PUF is shown in Fig. 6. A Temptronic ATS-605 thermostream system was used to perform temperature variation measurements and a Tektronic TLA6404 Logic Analyzer was used to capture the digital PUF outputs.

A. Masking Unstable Bits

To maximize the reliability of the proposed PUF, the digital averager discussed in section III is used to characterize the strength of each unique ID bit, allowing the user to determine which bits are unreliable. In this work, each PUF is

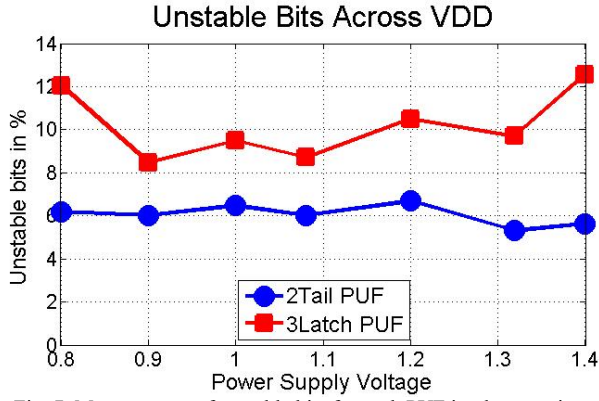


Fig. 7. Measurement of unstable bits for each PUF implementation across voltage supply variations

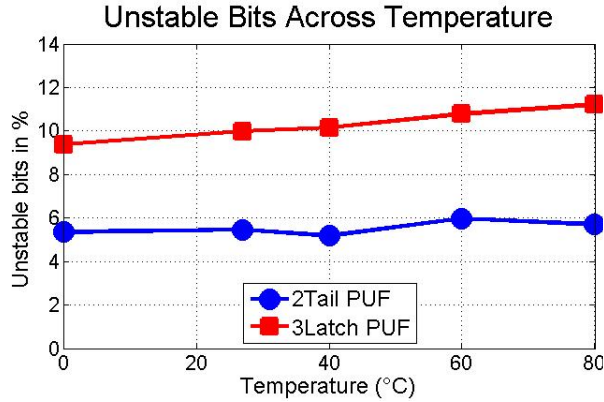


Fig. 8. Measurement of unstable bits for each PUF implementation across temperature variations

evaluated 100 times at nominal conditions (64 times at variable conditions) and each ID bit is categorized by strength. A bit is defined as unstable if it is categorized as weak at least once among the samples taken. Fig. 7 shows the percentage of unstable bits across 0.8V-1.4V voltage supplies for both the double-tail implementation and the three-latch PUF implementation. The total percentages of stable bits across 0.8V-1.4V for the double-tail and three-latch implementations are 81.9% and 69.9%, respectively. Fig. 8 shows the percentage of unstable bits across the temperature range 0°C-80°C for each PUF implementation. The total percentages of stable bits across 0°C-80°C for the double-tail and three-latch implementations are 91.2% and 83.0%, respectively.

In this work, the unreliable bits are masked so that only the bits that are stable across all voltage supply variations will be used to create 64-bit PUF outputs. Unfortunately, this functionality was not implemented into our fabricated device, so the masking was performed during the post-processing phase of the PUF measurements.

B. Intra-Hamming Distance (Reliability)

The reliability of each PUF implementation is represented by the intra-HD of each PUF response. The masking technique from Section IV.A is implemented in order to include only the strong bits across voltage supply variations. As seen in Fig. 9, the normalized intra-HDs for the double-tail and three-latch implementations across 0.8V-1.4V voltage supplies are less than 0.89% and 0.96%, respectively. Fig. 10 shows the intra-HDs for the double-tail and three-latch implementations to be

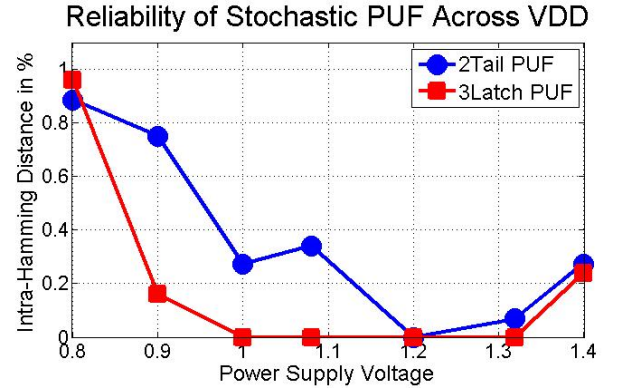


Fig. 9. Measurement of Normalized intra-Hamming Distance for each PUF implementation across voltage supply variations

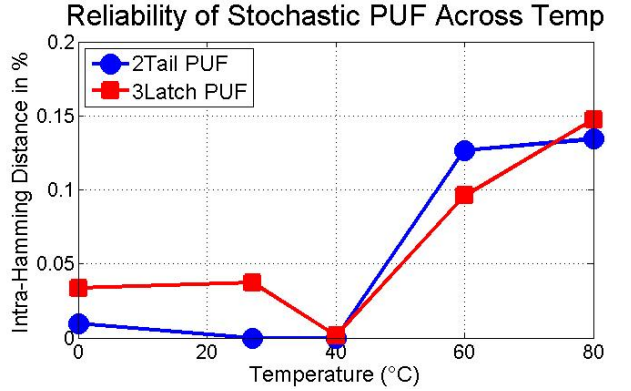


Fig. 10. Measurement of Normalized intra-Hamming Distance for each PUF implementation across temperature variations

less than 0.14% and 0.15%, respectively, for temperatures up to 80°C.

C. Inter-Hamming Distance (Uniqueness)

The uniqueness of the PUF is measured by the inter-HD. The masking technique mentioned in section IV.A is used to create 64-bit PUFs to measure the inter-HD at nominal conditions (1.20V at 27°C). 22 64-bit PUF codes were utilized for the double-tail implementation and 19 64-bit PUF codes were utilized for the three-latch implementation. The normalized inter-HD is displayed in Fig. 11 for each PUF implementation. It can be seen that the double-tail implementation has a normalized inter-HD of 47.9% with a standard deviation, σ , of approximately 1.9, while the three-latch implementation has a normalized inter-HD of 48.5% and a σ of approximately 1.6. Fig. 11 shows that both PUF implementations produce chip-specific identifiers with nearly ideal uniqueness, represented by an inter-HD of 50%.

D. Power Consumption

The power consumption of the proposed PUF was measured for the three-latch implementation at a throughput of 4Mb/s. No masking technique was used during this measurement. Unfortunately, the fabricated design operates with all 64 comparators of a PUF active, when only one needs to be active at one time to produce an ID bit. Because of this design flaw, a large amount of dynamic power is wasted on the unused, but active, 63 comparators. This design is measured to require an energy per bit of 1.5 nJ/bit at 4Mb/s. Fortunately, the power consumed by only the 64 comparators

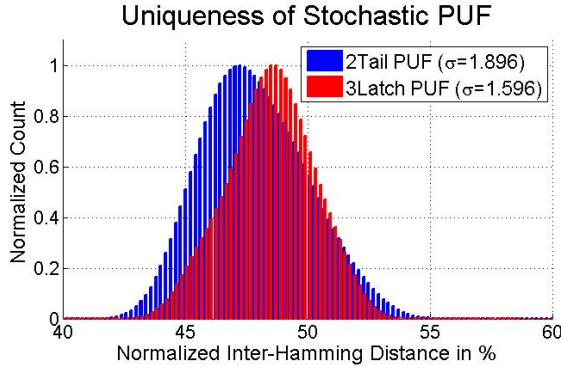


Fig. 11. Measurement of Normalized inter-Hamming Distance for each PUF implementation at nominal conditions

can be determined through manipulation of the block select circuitry in the fabricated design. Thus it is possible to estimate the power consumed by a single comparator. Using this estimation, we can then calculate the theoretical power consumption of an optimized design of the proposed PUF, which only has one active comparator at a time. The optimized energy per bit was calculated to be 34.5 pJ/bit at 4Mb/s.

E. Comparison with State of the Art

Table I compares the proposed PUF with state-of-the-art designs. Compared to previous works, the PUF proposed in this paper has a unique advantage of having all-digital components with analog capabilities. Thus, the proposed PUF can be used in analog, AMS, and digital applications. Finally, the proposed design uses simple comparators which are a fundamental block in almost all AMS chips, allowing for comparator sharing and reduction in hardware overhead.

V. CONCLUSION

This paper builds upon and evaluates a novel weak PUF which utilizes the random input offset voltages of dynamic latched comparators in order to create a chip-specific identifier. The analog characteristics of the implemented dynamic latched comparators allow for the proposed PUF to be used in AMS applications. In this case, because comparators are a fundamental block in AMS circuits, comparator sharing can be employed to implement the PUF with minimal hardware overhead. It is also possible to design dynamic latched comparators using only standard digital gates. Thus, it is possible to implement the proposed PUF in all-digital applications as well. Two implementations of the proposed PUF, each using a different comparator, were designed and fabricated using a 0.13 μm CMOS process. The functionality, reliability, and uniqueness of the PUF were then

verified through experimental measurements. The PUF demonstrated excellent reliability with an intra-HD of less than 0.96% across 0.8V-1.4V voltage supply and less than 0.15% for temperatures up to 80°C. The inter-HD of the 64-bit PUF outputs was measured to be 48.5% with a σ of 1.60. Finally, based on measurements of our power inefficient design, it is calculated that an optimized design will only require 34.5 pJ/bit at a throughput of 4Mb/s. Future work will investigate the impact of aging on the proposed PUF.

REFERENCES

- [1] S. Rosenblatt *et al.*, "Field Tolerant Dynamic Intrinsic Chip ID Using 32 nm High-K/Metal Gate SOI Embedded DRAM," *IEEE J. Solid State Circuits*, vol. 48, no. 4, pp. 940-947, 2013.
- [2] C. Herder, M. D. Yu, F. Koushanfar and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126-1141, Aug. 2014.
- [3] B. Gassend, D. Clarke, M. van Dijk, S. Devadas, "Silicon Physical Random Functions," *Proceedings of the Computer and Communications Security Conference*, pp. 148-160, 2002.
- [4] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical One-Way Functions," Ph.D. Thesis, MIT, 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. 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.
- [7] 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.
- [8] 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.
- [9] 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.
- [10] S. Stanzione, D. Puntin and G. Iannaccone, "CMOS Silicon Physical Unclonable Functions Based on Intrinsic Process Variability," *IEEE Journal of Solid-State Circuits*, vol. 46, no. 6, pp. 1456-1463, June 2011.
- [11] J. Li and M. Seok, "Ultra-Compact and robust Physically Unclonable Function Based on Voltage-Compensated Proportional-to-Absolute-Temperature Voltage Generators," *IEEE Journal of Solid-State Circuits*, vol. 51, no. 9, pp. 2192-2202, Sept. 2016.
- [12] T. Bryant, S. Chowdhury, D. Forte, M. Tehranipoor, and N. Maghari, "A Stochastic Approach to Analog Physical Unclonable Function," *IEEE Midwest Symposium on Circuits and Systems (MWSCAS)*, 2016.
- [13] "Top 5 counterfeited semiconductors: Analog ICs top the list | Solid State Technology," 2015[Online]. Available: <http://electroiq.com/blog/2012/04/top-5-counterfeited-semiconductors-analog-ics-top-the-list/>
- [14] J. He, S. Zhan, D. Chen, R. J. Geiger, "Analyses of Static and Dynamic Random Offset Voltages in Dynamic Comparators," *IEEE Transactions on Circuits and Systems I Reg. Papers*, vol. 56, no. 5, pp. 911-919, May 2009.
- [15] S. Babayan-Mashhadi and R. Lotfi, "Analysis and Design of a Low-Voltage Low-Power Double-Tail Comparator," *IEEE Transactions on Very Large Scale Integration Systems*, vol. 22, no. 2, pp. 343-352, Feb. 2014.
- [16] 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.
- [17] A. Alvarez, W. Zhao, and M. Alioto, "15 fJ/b static physically unclonable functions for secure chip identification with <2% native bit instability and 140 $\times$ inter/intra PUF hamming distance separation in 65 nm," in *Proc. IEEE Int. Solid-State Circuits Conf.*, Feb. 2015, pp. 256-257.

TABLE I
COMPARISONS WITH STATE OF THE ART PUFs

	[10]	[11]	[17]	Proposed
Technology	90nm	65nm	65nm	130nm
Area/Bit (F^2) (F = min. feat. size)	2.2x10 ⁶	727	6000	6500
VDD Range (V)	0.54-0.66	0.6-1.2	0.7-1	0.8-1.4
Temp Range (°C)	25-125	0-80	25-85	0-80
Bit Instability	<0.01%	<3.5%	<5%	<0.97%
Inter-HD	-	0.5001	0.5014	0.4850
Energy/Bit (pJ)	-	0.548	0.015	34.5*

*Calculated power for optimized design