Physically Unclonable Function based on Voltage Divider Arrays in Subthreshold Region

Aishwarya Bahudhanam Venkatasubramaniyan
Department of Electrical Engineering
State University of New York at Buffalo
Buffalo, NY 14260
Email: abahudha@buffalo.edu

Arindam Sanyal
Department of Electrical Engineering
State University of New York at Buffalo
Buffalo, NY 14260
Email: arindams@buffalo.edu

***Abstract*—This paper proposes a novel architecture of a simple, low energy silicon physically unclonable function arrays depending on the large random variation of threshold voltage of MOSFETs operating in subthreshold region. The proposed structure is a strong silicon PUF with 2^{60} challenge response pairs and consumes an energy of 0.48pJ/bit. The PUF is simulated in 65nm CMOS technology and has a normalized inter-HD of 0.4982 and intra-HD of 0.0225.**

I. Introduction

Silicon physically unclonable functions (PUF) are innovative primitives to derive secrets from complex physical characteristics of integrated circuits (IC). A Si PUF exploits random mismatches in IC incurred during fabrication process to create a unique code which is extremely difficult to predict or extract. Thus, a PUF acts like a fingerprint for ICs. The lightweight hardware encryption capability provided by Si PUFs make it attractive for internet-of-things (IoT) applications where power constraints prevent heavyweight cryptographic algorithms from being used. A PUF has to satisfy two primary requirements for it to be used as an authentication mechanism a) the response of a PUF should be difficult to replicate and be unknown even to its manufacturer and b) repeated evaluation of a PUF with same challenge should yield the same response. The first condition is a measure of uniqueness of the PUF and is quantified by measuring the hamming distances (HDs) between 2 distinct PUFs issued with the same challenge. This metric is known as inter-HD and for an ideal PUF, normalized inter-HD should be 0.5. The second condition is a measure of reliability of PUF and is measured by issuing the same challenge to a PUF over time and conditions. This metric is known as intra-HD and for an ideal PUF, intra-HD should be 0. PUFs can be classified into 2 broad groups, strong PUF and weak PUF. For a strong PUF, the number of challenge-response pairs (CRPs) grows exponentially with area while for weak PUFs, the number of CRPs grows linearly with area.

The first strong Si PUF was an arbiter PUF [1] which generated a 1-bit response depending on the variation in delay between two nominally identical paths. Variants of the arbiter PUF include XOR-ing of parallel arbiter-PUFs [2] and addition of feedforward path to inject nonlinearity [1]. Another widely used PUF is SRAM PUF which is a weak PUF that generates a unique signature by exploiting the variations in threshold voltage of transistors in SRAM cell [3], [4]. However, SRAM PUFs often exhibit bias and require post-processing to improve stability. A current-mirror based PUF [5] achieves high reproducibility without requiring post-processing but at the cost of large area. [6] has presented a series-NAND gate based weak PUF which reduces area compared to the current-mirror PUF but is sensitive to supply voltage variation. [7] extends the idea of [6] by using cascaded two-transistor amplifiers biased in deep subthreshold to generate a rail-to-rail output. The most recent work [8] presents a strong analog PUF based on the subthreshold current arrays of MOSFETs. The strong nonlinear dependence of MOS current on threshold voltage in the subthreshold region is exploited to generate randomness.

We present a strong PUF based on voltage divider arrays working in subthreshold region. The proposed PUF derives its uniqueness from the wide random fluctuations in threshold voltages of transistors in subthreshold region. A majority voting technique is used to reduce noise from the comparator and results in a low bit-error rate (BER) at a good energy efficiency. The proposed work does not require any post-processing to improve reproducibility.

The rest of this paper is organized as follows: Section II presents the proposed strong PUF architecture, Section III presents simulation results and the conclusion is brought up in Section IV.

II. Proposed Architecture

The proposed PUF architecture is shown in Fig. 1. The unit cell consists of an inverter with gate and drain shorted such that it acts as voltage divider. The PUF cell is biased in weak inversion by a tail current source. A PUF array is formed by connecting the unit cells through a switch (S_1 in Fig. 1) which is controlled by the challenge input C_i. For each challenge input, outputs of 2 identical PUF arrays are compared to form the response output. The PUF cells are disconnected from the supply through switch S_2 during sleep mode. The strong-arm latch in Fig. 2 is used as the comparator. Offset in comparator leads to loss in randomness of the PUF response. Comparator offset is calibrated using two additional transistors in parallel to the input transistors [8].

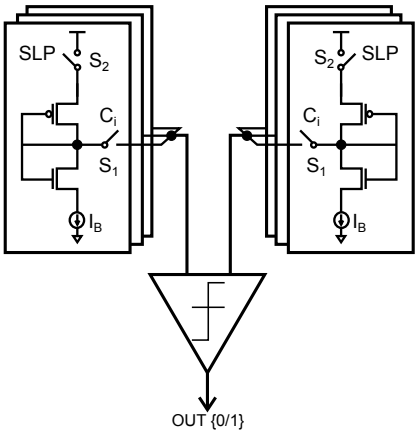

Fig. 1. Proposed PUF architecture

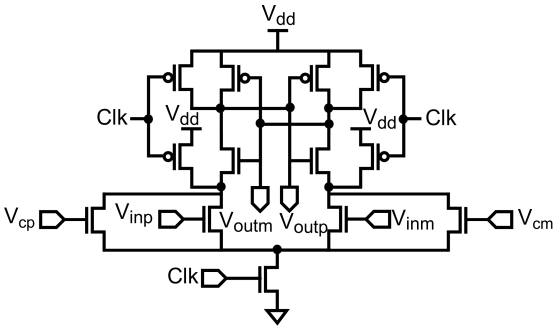

Fig. 2. Comparator schematic

Since the current through the unit PUF stack is fixed by the tail current (I_B in Fig. 1), the output voltage has similar variance as threshold voltage V_{th} of a transistor. In sub-micron devices, V_{th} exhibits large and spatially uncorrelated variation which leads to the uniqueness of the proposed PUF cell. By biasing the PUF in subthreshold, variance of V_{th} is increased even more. Fig. 3 shows the probability distribution of the differential voltage between 2 PUF cells. The standard deviation (σ) of the differential voltage between 2 PUF cells is 35mV and is calculated from 500 monte-carlo runs. For our design, we use 60 such unit PUF cells to form the complete PUF. The standard deviation of differential voltage, when all 60 PUF cells are connected to the comparator inputs, is 5mV. The comparator has to be designed such that its noise and offset does not degrade reliability of the PUF. From monte-carlo simulations, it is found that, by adjusting the voltages V_{cp} and V_{cm} between 0 to 400mV, 8mV offset can be compensated. Noise from the PUF cells can be minimized by capacitive loading of the comparator inputs which reduces bandwidth of the PUF cells. For our design, the parasitic capacitance at the comparator input was enough to significantly reduce noise from PUF cells. Hence, in subsequent noise analysis, we will only include the effect of comparator noise.

For an optimum design, we need to ensure a low bit-error rate (BER) and low power consumption. Additionally, the design also needs low systematic offset to prevent bias

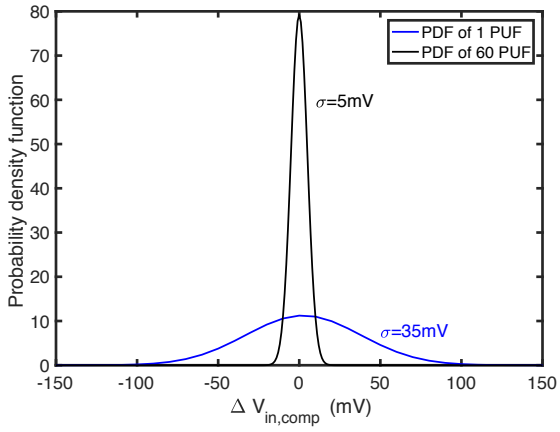

Fig. 3. PDF of differential voltage between PUF cells

in the generated output and ensure PUF uniqueness. For a PUF output to be reproducible, the comparator noise has to be low. Comparator noise depends on its power consumption and input common-mode voltage, V_{cmi}. For the same power consumption, comparator noise can be reduced by lowering V_{cmi} as shown in Fig. 4. Fig. 5 shows the variation of PUF power with comparator input common-mode voltage. The PUF power reduces with increase in V_{cmi} while noise increases with increase in V_{cmi}. Thus, there is a trade-off between PUF reliability and power and requires a judicial choice of V_{cmi}. For the present design, V_{cmi} of 475mV was chosen for a PUF power of 6μW and noise σ of 560μV.

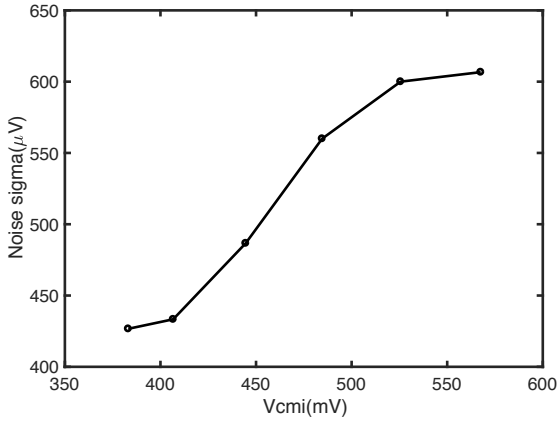

Fig. 4. Comparator noise vs V_{cmi}

If the PUF mismatch for a certain challenge input is smaller than noise level, the response for that challenge will vary with time or be temporally unstable. To minimize the number of such temporally unstable CRPs, standard deviation of noise should be much smaller than standard deviation of random mismatch in PUF cells. Since the distribution of PUF mismatch and noise are gaussian, probability of a CRP being temporally stable can be written as

$$P = 1 - erf\left(\frac{\sigma_n}{\sigma_{mis}\sqrt{2}}\right) \quad (1)$$

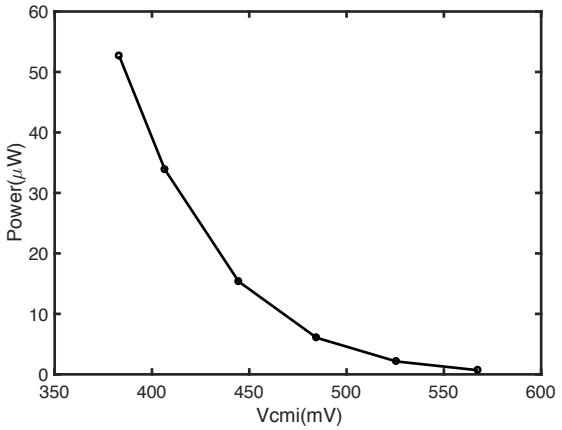

Fig. 5. PUF power vs V_{cmi}

where σ_n is the standard deviation of noise and σ_{mis} is the standard deviation of random mismatch in the PUF. The worst case σ_{mis} for our design is 5mV (when all 60 unit cells are connected to the comparator input). For $P = 0.97$, σ_n has to be less than 190μV. Since σ_n for the comparator is 560μV, we used majority voting technique to reduce the standard deviation of noise. Fig. 6 shows the probability density function of comparator noise as majority voting is applied. A majority voting of 7 reduces σ_n from 560μV to 200μV while a majority voting of 15 reduces σ_n to 168μV. A counter clocked by comparator positive output is used for implementation of majority voting. Majority voting by $2^n - 1$ (where n is an integer) is chosen to simplify the circuit implementation. The counter is reset at the start of voting and the most significant bit (MSB) of the counter output at the end of voting indicates the result of voting. For this design, majority voting of 7 was chosen.

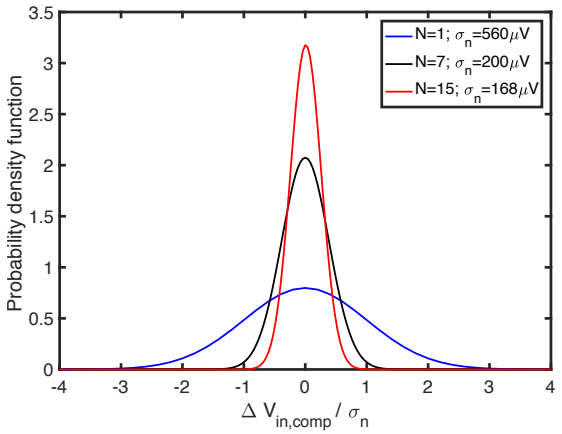

Fig. 6. Noise standard deviation versus majority voting

III. Simulation Results

Fig. 7 shows the layout of the PUF cells along with the comparator. The circuit core occupies an area of 40μm by 70μm. Working from a 0.8V supply, the proposed PUF consumes 6μW of power while running at a frequency of 12.5MHz. The leakage power of the design is 39nW. The PUF cells consume the same amount of power irrespective of the challenge issued which makes the design robust against non-invasive thermal imaging attacks or differential power analysis attacks.

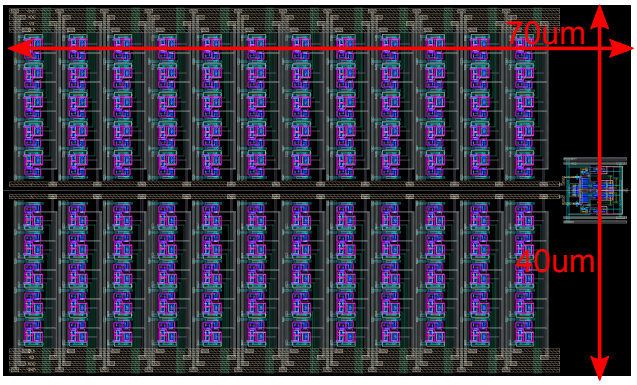

Fig. 7. PUF layout

Fig. 8 shows the results of intra and inter HD simulations. For intra-HD simulations, the supply voltage was varied from 750mV to 900mV (-6.25% to 12.5%) and the temperature was varied from -20C to 85C. The intra-HD was averaged across 5 different monte-carlo runs performed for each voltage and temperature point for 600 challenges. The normalized intra-HD has a mean of 0.0225 and standard deviation of 0.0096. Inter-HD simulation was performed for 60 monte-carlo runs of 600 challenges at a power supply of 800mV and temperature of 27C. The normalized inter-HD has a mean of 0.4982 and standard deviation of 0.0492.

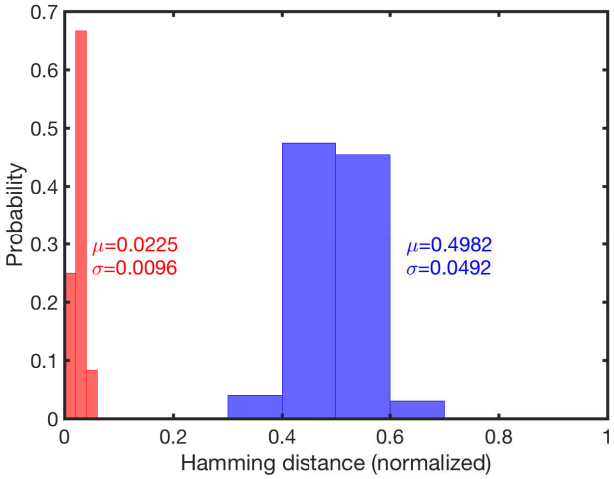

Fig. 8. Inter and intra HD plot

Fig. 9 shows the bit-error rate for 5 different monte-carlo runs of 600 challenges each for different voltage $\{0.75V, 0.8V, 0.85V, 0.9V\}$ and temperature $\{-20C, 27C, 80C\}$ points. The worst-case BER is 7% while the average BER is 2.25%.

TABLE I
COMPARISON WITH STATE-OF-THE-ART PUFS

	This work	[8]	[9]	[7]	[1]	[3]	[10]
Technology(nm)	65	130	90	40	180	22	28nm
Type of PUF	Strong	Strong	Strong	Strong	Strong	Weak	Strong
Number of CRPs	1.15×10^{18}	$\approx 3.7 \times 10^{19}$	3-6 bits	$\approx 5.5 \times 10^{28}$	$\approx 1.4 \times 10^{20}$	1	1.17×10^{11}
Worst-case BER	7%	9%	14.13%	$< 10^{-8}$	4.8%	4.6%	3.17%
Energy/bit (pJ/bit)	0.48	11	–	17.75	–	0.19	0.097
Voltage range (V)	$0.75 - 0.9$	$1.08 - 1.32$	1	$0.7 - 1.2$	$1.75 - 1.85$	$0.7 - 0.9$	$0.5 - 0.9$
Temperature range (C)	-20 to 85	-20 to 80	20 to 100	-25 to 125	20 to 70	25 to 50	0 to 80
Intra-HD	0.0225	0.058	0.0644	0.0101	0.0357	0.0097	0.0317
Inter-HD	0.4982	0.499	0.4375	0.5007	0.4	0.49	0.481-0.495
Inter-HD/intra-HD	22.1	8.6	6.8	49.5	11.2	50.5	15.6

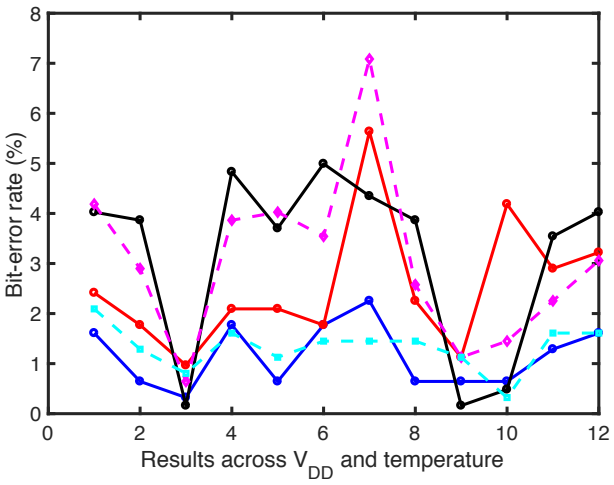

Fig. 9. BER across V_{DD} and temperature

Table I compares the proposed work with state-of-the-art PUFs. The proposed PUF compares favorably with state-of-the-art designs in terms of energy efficiency and reliability. The proposed PUF has a high inter-HD to intra-HD ratio which shows that one instance of the PUF is highly distinguishable from another instance. Randomness of PUF can also be visually seen from the speckle diagram of Fig. 10. An output of '1' is represented by a dark box and '0' by white box in Fig. 10. The output distribution has a random pattern as can be seen from Fig. 10. Probability of 1 for the outputs in Fig. 10 is 0.487.

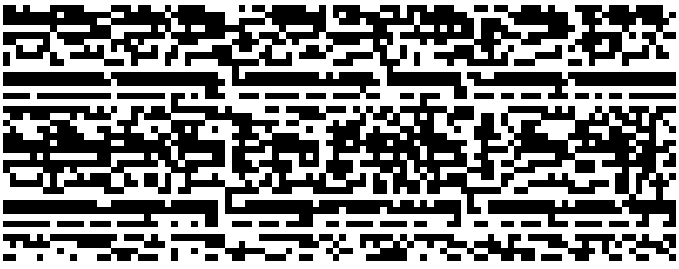

Fig. 10. PUF speckle diagram

IV. CONCLUSION

A novel strong PUF, based on voltage divider arrays, is presented in this paper. The proposed PUF exploits random variation in transistor threshold voltage in the subthreshold region and energy/bit and reliability of the PUF are expected to improve with technology scaling. The proposed PUF has a low energy consumption of 0.48pJ/bit which makes it a good candidate for secure IoT devices. The proposed PUF has a current consumption independent of challenge pattern which makes it robust against differential power and thermal imaging attacks.

REFERENCES

[1] J. W. Lee, D. 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," in *IEEE Symposium on VLSI Circuits*, 2004, pp. 176–179.

[2] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proceedings of the 44th annual design automation conference*. ACM, 2007, pp. 9–14.

[3] S. K. Mathew, S. K. Satpathy, M. A. Anders, H. Kaul, S. K. Hsu, A. Agarwal, G. K. Chen, R. J. Parker, R. K. Krishnamurthy, and V. De, " A 0.19 pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS," in *IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*, 2014, pp. 278–279.

[4] Y. Su, J. Holleman, and B. P. Otis, "A digital 1.6 pJ/bit chip identification circuit using process variations," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 1, pp. 69–77, 2008.

[5] A. B. Alvarez, W. Zhao, and M. Alioto, "Static physically unclonable functions for secure chip identification with 1.9–5.8% native bit instability at 0.6–1 V and 15 fJ/bit in 65 nm," *IEEE Journal of Solid-State Circuits*, vol. 51, no. 3, pp. 763–775, 2016.

[6] B. Karpinskyy, Y. Lee, Y. Choi, Y. Kim, M. Noh, and S. Lee, "Physically unclonable function for secure key generation with a key error rate of 2E-38 in 45nm smart-card chips," in *IEEE International Solid-State Circuits Conference (ISSCC)*, 2016, pp. 158–160.

[7] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, "A physically unclonable function with BER¡ 10- 8 for robust chip authentication using oscillator collapse in 40nm CMOS," in *IEEE International Solid-State Circuits Conference-(ISSCC)*, 2015, pp. 1–3.

[8] X. Xi, H. Zhuang, N. Sun, and M. Orshansky, "Strong subthreshold current array PUF with 2^{65} challenge-response pairs resilient to machine learning attacks in 130nm CMOS," in *IEEE Symposium on VLSI Circuits*. IEEE, 2017, pp. C268–C269.

[9] S. R. Sahoo, K. S. Kumar, and K. Mahapatra, "A novel current controlled configurable RO PUF with improved security metrics," *Integration, the VLSI Journal*, vol. 58, pp. 401–410, 2017.

[10] S. Jeloka, K. Yang, M. Orshansky, D. Sylvester, and D. Blaauw, "A sequence dependent challenge-response PUF using 28nm SRAM 6T bit cell," in *IEEE Symposium on VLSI Circuits*, 2017, pp. C270–C271.