A Physical Unclonable Function based on Capacitor Mismatch in a Charge-Redistribution SAR-ADC

Qianying Tang, Won Ho Choi†, Luke Everson, Keshab K. Parhi and Chris H. Kim
Dept. of Electrical and Computer Engineering, University of Minnesota, Minneapolis, MN, USA
†Western Digital Research, CA, USA
Email: {tangx280, choi0444, evers193, parhi, chriskim}@umn.edu

Abstract—**A Physical Unclonable Function (PUF) using capacitor mismatch in a standard successive approximation register analog-to-digital converter (SAR-ADC) as the entropy source is demonstrated in 65nm CMOS. SAR-ADCs are readily available in many system-on-chips, making the hardware overhead of the proposed PUF almost negligible. The inherent process variation of metal-oxide-metal (MOM) capacitors is harnessed through a charge redistribution operation which is sampled by the voltage comparator. To enhance the stability of the PUF output, soft response generation and dynamic thresholding techniques were adopted. Finally, we verify that performing the enrollment operation at a lower operating voltage can ensure that PUF responses are stable at the nominal supply voltage used during authentication.**

Keywords—Physical Unclonable Function (PUF); Successive Approximation (SAR) ADC; capacitance variation; charge redistribution;

I. INTRODUCTION

Hardware security has become an important concern for internet-of-things (IoT) devices as these systems can be the target of unauthorized access and malicious tampering attacks. Authenticating IoT systems is more challenging than authenticating computers or smart phones due to the limited hardware resources available and stringent energy constraints [1,2,3,4]. Physical Unclonable Function (PUF) is a circuit block that can generate unique and random keys based on the chip's manufacturing variation. It is an attractive solution for authenticating IoT systems due to several reasons: (1) Compared to storing a secret key in a non-volatile memory (NVM), PUF based authentication is known to be more secure [1,5]; (2) PUFs can be built in a standard logic process and therefore are less expensive than NVMs; (3) Some PUFs can be directly used for authentication without additional cipher blocks; (4) PUFs are irreversible as the entropy source comes from the physical characteristic of the chip; and (5) PUFs are immune to offline attacks.

Analog-to-digital converter (ADC) is a critical component for IoT systems that interact with the real analog world. There are three main types of ADCs used in IoT systems: Success-Approximation (SAR) ADC, sigma-delta ADC, and pipeline ADC. In particular, SAR ADC has become a popular choice as it achieves a good balance between energy-efficiency and performance. In this work, we present an *in-situ* PUF which utilizes the capacitance mismatch in a charge-redistribution SAR-ADC for generating the output response. Fig. 1 compares the proposed PUF with conventional delay based and SRAM based PUFs. The proposed PUF has unique properties such as (1) incurring almost no hardware overhead as compared to the delay-based PUF [6], (2) providing an exponentially higher number of challenge-response pairs as compared to the SRAM based PUF [7,8], and (3) better stability against voltage, temperature, and aging variation owing to the usage of passive capacitors. Process induced variation is relatively small in passive devices than active devices. Therefore, a thorough evaluation based on extensive chip measurements must be performed. Several attempts have been made to implement PUFs using passive devices. A PUF based on power grid metal wire variation has been investigated where resistance variations of each chip were used as unique signatures [9,10]. A switched capacitor structure based PUF was experimentally demonstrated in [11] utilizing capacitance variation. However, this design is not suitable for authentication of lightweight IoT systems due to the large area required to implement the dedicated stand-alone PUF. Furthermore, the design suffers from high design complexity and a power hungry Error Correcting Code (ECC) block. To our knowledge, this paper is the first to report a PUF design based on a standard charge-redistribution SAR-ADC.

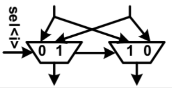
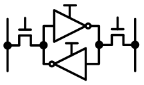
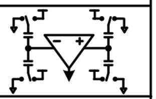
	Delay based PUF	SRAM PUF	Proposed PUF
Unit Cell Schematic			
Entropy Source	Delay difference	Power up value	Capacitance mismatch
# of CRPs per N cells	2^N	N	N choose k (k=1,2,…,N)
Pros	1. Strong PUF 2. Simple	1. Reuse existing SRAM IP	1. Reuse existing SAR-ADC IP 2. Less sensitive to V, T and aging 3. Strong PUF
Cons	1. Considerable circuit design effort 2. Area overhead	1. VDD must be turned on and off	1. Small process variation

Fig. 1. Comparison between delay based, SRAM based, and proposed SAR-ADC based PUFs.

II. CHARGE REDISTRIBUTION AND MISMATCH IN SAR-ADC

The entropy source for the proposed charge redistribution based PUF comes from the process variation induced capacitive mismatch in the MOM capacitor arrays in the SAR-ADC. To explain the basic idea of the charge-redistribution concept, we show the circuit schematic of a 3-bit single ended SAR-ADC in Fig. 2, consisting of two symmetric binary weighted capacitor arrays, a comparator, and successive approximation logic [12]. The capacitor array first samples and stores the input voltages on the selected capacitors. The charge stored on the plates must remain constant throughout the sampling phase, causing the plate voltages (V+ and V-) to change accordingly. The final goal is to bring V+ and V- voltages closer to each other in a successive manner. Fig. 3 illustrates the transfer function of a 3-bit ADC with and without capacitance mismatch. The analog input is linearly mapped to a digital code. For an ideal capacitive digital-to-analog converter (DAC) array, denoted as the dotted line, the minimum voltage steps are uniform and are equal to $V_{REF}/2^N$, where V_{REF} is the input voltage range and N is the number of bits. However, in the presence of capacitor mismatch [13], the transfer curve is distorted as indicated in the solid line. Random capacitor mismatch is generally caused by process variation or other uncontrollable layout effects. Capacitor mismatch induces variation in the DAC array bit-weight, further shifting the decision level as shown in the solid line. In this work, we utilize the inherent capacitor mismatch in a standard SAR-ADC as the PUF entropy source.

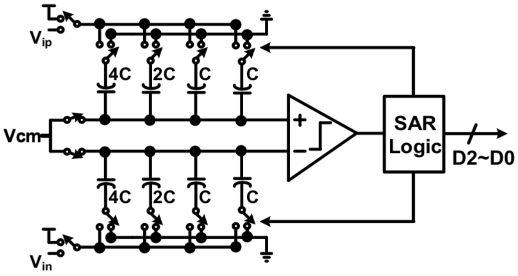


Fig. 2. 3-bit SAR ADC architecture shown as an example.

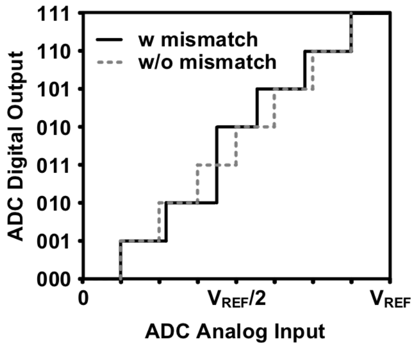


Fig. 3. Transfer curve of a 3-bit SAR ADC with and without capacitor mismatch.

III. Charge-Redistribution PUF Operation

Typically, the capacitor array in a charge-redistribution SAR-ADC is built using unit metal-insulator-metal (MIM) or metal-oxide-metal (MOM) capacitor cells as shown in Fig. 4. For example, C9 is comprised of 2^9 unit capacitors, C8 is comprised of 2^8 unit capacitors, and so on. In order to maximize the variation between capacitors selected for PUF operation, we compare the mismatch between two unit capacitors. This is because the standard deviation of a capacitor σ(C) is inversely proportional to the square root of the plate area: i.e., $\sigma(\mathrm{C}) \propto 1/\sqrt{\mathrm{A}}$. By comparing the mismatch between smaller unit capacitors, we can enhance the capacitance mismatch and obtain more stable PUF responses. In our design, only 63 unit capacitors on the same row of each capacitor array are utilized for PUF demonstration.

The circuit implementation and timing diagram for the PUF operation are shown in Fig. 5. In addition to the basic SAR-ADC blocks described earlier, we implemented a control block so that each unit capacitor can be switched independently. The area overhead of the control block is only 4% of the total SAR-ADC area. The PUF is evaluated multiple times and a counter measures the soft response value (= average response value) to determine the final PUF output. This ensures that an accidental bit flip will not result in a completely wrong PUF output. In order to minimize the comparator offset, an auto-zeroing offset cancellation technique was adopted [14]. The auto-zeroing comparator consists of three pre-amplifier stages and a latch based output sampling circuit. During the auto-zeroing phase, the inputs of each pre-amplifier are shorted to sample and store the offset of each stage on the output capacitors.

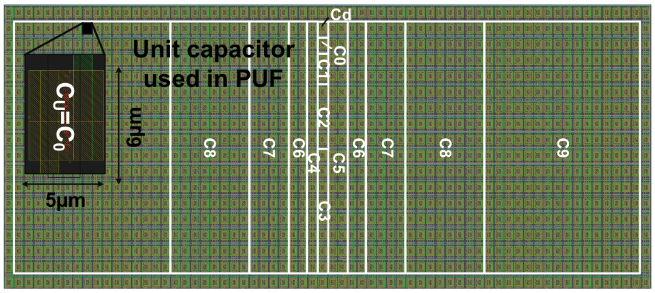


Fig. 4. Layout of a 10-bit SAR ADC capacitor array in 65nm.

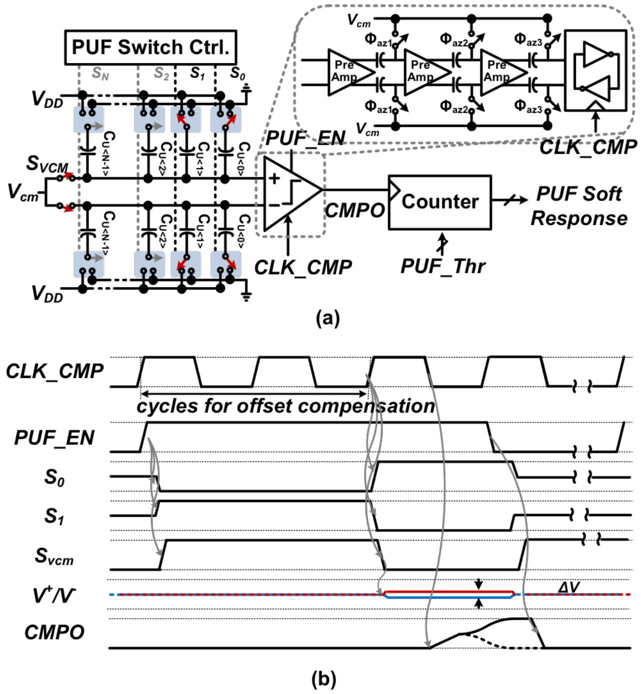


Fig. 5. (a) Schematic and (b) timing diagram of the proposed charge redistribution PUF.

Timing diagram of the charge redistribution PUF is shown in Fig. 5 (b). At the rising edge of the PUF_EN signal, V+ and V- are initialized to the common-mode voltage Vcm. The first two clock cycles are utilized for voltage sampling and auto-zeroing. During this period, two unit capacitors are enabled and connected in serial between VDD and GND, while the unselected capacitors are left floating. In the first two CLK_CMP cycles, the charge stored on top plate is:

$$Q = V_{cm} \cdot C_{U<0>} + \left(V_{cm} - V_{DD}\right) \cdot C_{U<1>}$$

At the third CLK_CMP rising edge, the bottom connections of the two capacitors are swapped, and the top plate voltage V+ is determined by the following equations.

$$Q^{+}_{clk1} = Q^{+}_{clk3} \Rightarrow V^{+} = V_{CM} - \frac{C^{+}_{U<0>} - C^{+}_{U<1>}}{C^{+}_{U<0>} + C^{+}_{U<1>}} V_{DD}$$

$$\Delta V = V^{+} - V^{-} = \left(\frac{C^{-}_{U<0>} - C^{-}_{U<1>}}{C^{-}_{U<0>} + C^{-}_{U<1>}} - \frac{C^{+}_{U<0>} - C^{+}_{U<1>}}{C^{+}_{U<0>} + C^{+}_{U<1>}} \right) \cdot V_{DD}$$

The capacitance difference between $C_{U<0>}$ and $C_{U<1>}$ results in different top plate voltages (ΔV). Depending on the polarity of ΔV, the comparator generates a logic '0' or '1'. The input to the PUF, typically referred to as "challenge" corresponds to the location of the enabled unit capacitor. The output of the PUF, referred to as "response" is the comparator output.

For capacitor pairs with extremely small mismatch, the PUF output may not be consistent in the presence of voltage and temperature variations. To mitigate PUF stability issues, error-correction techniques are commonly used. In this work, we adopt a low-overhead soft-response based error-correction technique where the average value of the response bit is used to determine the final PUF output [15, 16]. This is accomplished by repetitively evaluating the PUF using the same challenge (i.e., asserting PUF_EN multiple times) and counting the number of times the comparator output evaluates to '1' using an on-chip counter. The ratio between the count value and the total number of evaluation cycles is defined as the *soft response*.

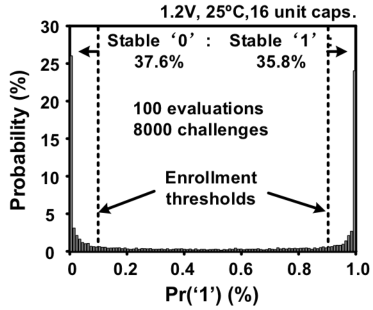


Fig. 6. Measured soft response (=probability of response being '1') distribution for the SAR-ADC PUF.

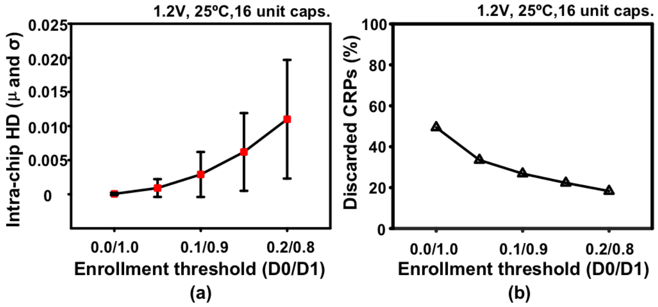


Fig. 7. Measured data from SAR-ADC PUF: (a) Intra-chip Hamming distance and (b) percentage of discarded CRPs for different enrollment thresholds.

The number of Challenge-Response Pairs (CRPs) obtainable from the proposed PUF is determined by the total number of available unit capacitors *N* and the number of enabled unit capacitors *k*. This is equivalent to randomly choosing *k* unit capacitors from an *N* unit capacitor array. The total number of different cases is C(*N*, *k*), where C(.) is the combination function. For example, in the scenario shown in Fig. 5, the total number of CRPs is C(63, 2) = 63x62/2 = 1,953. To further increase the number of CRPs, we can increase the number of enabled unit capacitors (=*k*) for each comparison. The maximum number of CRPs is obtained when 50% of the unit capacitors are enabled for comparison (i.e., *k*=*N*/2).

IV. PUF Measurement Results

The soft response values obtained from the proposed PUF are shown in Fig. 6. The PUF was evaluated 100 times for each challenge and 8,000 different challenges were applied. Consequently, the total number of PUF response bits plotted in Fig. 6 is 100 x 8,000 = 0.8M bits. A soft response equal to 0 or 1 means that the comparator produces a '0' or '1' for the entire 100 evaluation cycles. This implies that a large voltage difference is produced by the two capacitor arrays. On the other hand, challenges with soft response close to 0.5 indicates a relatively small voltage difference generated by the capacitor mismatch which is susceptible to random noise. Generally, the soft response is converted to a digital bit by thresholding at 0.5. That is, a soft response value greater than 0.5 will be taken as a '1' and vice versa. However, a response recognized as a '1' during the enrollment may flip to '0' during the authentication (e.g., soft response change from 0.51 to 0.49). In order to prevent such unstable responses, a dynamic thresholding scheme is applied which utilizes different decision thresholds for the enrollment and authentication. The basic idea is to set a more stringent decision threshold during the enrollment, e.g., discard soft response values that fall between 0.1 and 0.9. A relaxed decision threshold, e.g., 0.5, is applied during authentication. This method improves the PUF stability by minimizing inadvertent '1'-to-'0' and '0'-to-'1' flips. The PUF stability with different enrollment threshold is verified by checking the intra-chip Hamming distance (HD) as shown in Fig. 7 (a). Both the mean and standard deviation of the intra-chip HD decreases with a more stringent enrollment threshold. Utilizing a more stringent enrollment threshold can improve the PUF stability at the expense of fewer CRPs. The percentage of discarded CRPs for different enrollment thresholds is shown in Figure 7(b). The percentage of stable CRPs increases from 50.6% to 81.7% as the enrollment threshold for data '0'/'1' are relaxed from 0.0/1.0 to 0.2/0.8. In our experiments, we picked an enrollment threshold of 0.1/0.9 which seems to provide a good balance between PUF stability and the number of available CRPs. The percentage of discarded CRPs also depends on the number of enabled unit capacitors. As shown in Fig. 8, the percentage of discarded CRPs first decreases and then remains flat as the number of enabled unit capacitors is increased. For enhancing security, at least 16 unit capacitors should be enabled which increases the total number of CRPs to more than 3.6×10^{14}. For the rest of the measurements presented in this paper, 16 unit capacitors were selected from each array. In other words, we are comparing the mismatch between the sum of 16 randomly selected unit capacitances from two separate arrays.

PUFs must be designed with some resilience against voltage and temperature drifts, and device aging. Furthermore, invasive attacks such as side channel attacks can skew the PUF responses [17]. Therefore, maintaining stability across a wide supply voltage range is important. One benefit of using passive capacitors as the entropy source is that the change in the random signature (i.e., ΔV between the two capacitor arrays) is proportional to the supply voltage. This linear relationship implies that a response that is stable at a low supply voltage will become even more stable at higher supply voltages due to the increased ΔV. Hence, by performing the enrollment at the lowest possible supply voltage, we can ensure a stable authentication for the entire operating voltage range. To verify our hypothesis, we evaluated the PUF's intra-chip Hamming distance with different enrollment voltages using following steps;

Step 1: Apply a randomly selected challenge set C

Step 2: Determine the stable CRPs $<C_K, R_K>$ at each voltage based on a 0.1/0.9 threshold. Here, C_K is a sub-set of C corresponding to stable responses R_K

Step 3: Apply the same challenge set C again and collect new responses R' at supply voltages ranging from 0.8V to 1.2V. In this step, response bits are determined based on a relaxed 0.5 authentication threshold

Step 4: Calculate the intra-chip Hamming distances by comparing responses R_K and R_K' obtained from steps 2 and 3, respectively.

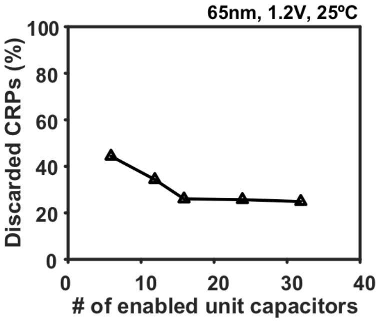


Fig. 8. Percentage of discarded CRPs for different # of enabled unit capacitors.

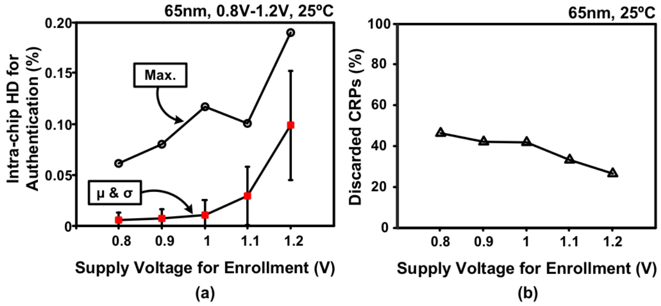
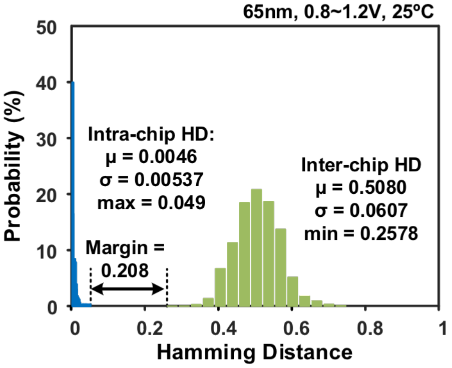


Fig. 9. (a) Intra-chip Hamming distance and (b) percentage of discarded CRPs for different supply voltages.

Fig. 9(a) shows that the average and sigma values of the intra-chip Hamming distances are only 0.56% and 0.6% when the PUF is enrolled at 0.8V while these numbers increase to 9.8% and 5.3%, respectively, when the PUF is enrolled at 1.2V. It is worth noting that the intra-chip HD significantly improves with a lower enrollment voltage, while the percentage of discarded CRPs increases slightly as shown in Fig. 9(b). A helper data to the discard CRPs is required in order to generate the valid challenges during the authentication phase.

The inter-chip Hamming distance distribution measured from 10 chips is shown in Fig. 10. Measurements show that 47.8% of the 80,000 CRPs are unstable which are hence discarded during enrollment phase. Consequently, we applied 40,000 stable challenges to the 10 different chips with a supply voltage ranging from 0.8V to 1.2V. To tolerate attacks such as random guessing, it has been suggested that each authentication generate at least 128 response bit [18]. Following this suggestion, we group the 40,000 CRPs into 312×128-bit responses in further analysis. The inter-chip Hamming distance distribution has an average value of 50.6% which is very close to the ideal case (i.e., 50%) indicating that responses from different PUFs are sufficiently uncorrelated. The margin between the minimum inter-chip Hamming distance and maximum intra-chip Hamming distance is 20.8% indicating that a secure authentication can be achieved without complex ECC schemes. The 65nm test chip die photo is shown in Fig. 11.



	Intra-chip	Inter-chip
Threshold	Pr('1')<0.1 or Pr('1')>0.9	
# of challenges	8k	80k
Discarded responses	47.8%	
Enrollment range	0.8~1.2V	
# of cycles for eval.	990×10	10
# chips	1	10

Fig. 10. Measured inter-chip and intra-chip Hamming distance distributions and evaluation conditions.

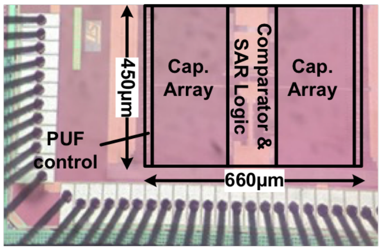


Fig. 11. 65nm charge-redistribution SAR-ADC PUF chip.

V. Conclusions

This paper has presented a PUF employing capacitance mismatch in the charge-redistribution SAR-ADC PUF. Measurement data collected from test chip fabricated in a 65nm process shows an average intra-chip HD of 0.0046 and an average inter-chip HD of 0.508 with a supply voltage ranging from 0.8V to 1.2V. The margin between the maximum inter-chip HD and the minimum intra-chip HD is 0.208 implying a good uniqueness for secure authentication. Future work will be directed towards investigation of machine learning attacks for SAR-ADC PUFs, evaluation of reliability, randomness and uniqueness of the SAR-ADC PUFs under different voltage, temperature, and environmental noise conditions. Effect of aging for MUX PUFs has been studied in [19]. Future research could also be directed towards studying effect of aging on SAR-ADC PUFs.

Acknowledgements

This research was supported in part by the National Science Foundation under grant number CNS-1441639 and the Semiconductor Research Corporation under contract number 2014- TS-2560.

REFERENCES

[1] R. H. Weber, "Internet of Things – New security and privacy challenges," *Computer Law & Security Review*, Vol. 26, No. 1, pp. 23-30, Jan. 2010.

[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] A. Ukil, J. Sen and S. Koilakonda, "Embedded security for Internet of Things," *Emerging Trends and Applications in Computer Science*, pp. 1-6, 2011.

[4] S. L. Keoh, S. S. Kumar and H. Tschofenig, "Securing the Internet of Things: A Standardization Perspective," *Internet of Things Journal*, vol. 1, no. 3, pp. 265-275, June 2014.

[5] B. Gassend, D.E. Clarke, van Dijk, et al., "Silicon physical random functions". *Computer and Communications Security*, pp. 148~160, Nov. 2002.

[6] S. Avvaru, C. Zhou, S. Satapathy, Y. Lao, C.H. Kim, and K. Parhi, "Estimating Delay Differences of Arbiter PUFs Using Silicon Data", *Design Automation and Test in Europe*, Mar. 2016.

[7] S. K. Mathew, Sudhir K. Satpathy; Mark A. Anders; Himanshu Kaul; Steven K. Hsu; Amit Agarwal; Gregory K. Chen; Rachael J. Parker; Ram K. Krishnamurthy; Vivek De, "16.2 A 0.19pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS," *International Solid-State Circuits Conference*, pp. 278-279, 2014.

[8] Sami Rosenblatt, Daniel Fainstein, Alberto Cestero, John Safran, Norman Robson, Toshiaki Kirihata, and Subramanian S. Iyer, "Field Tolerant Dynamic Intrinsic Chip ID Using 32 nm High-K/Metal Gate SOI Embedded DRAM," *Journal of Solid-State Circuits*, vol. 48, no. 4, pp. 940-947, Apr. 2013.

[9] J. Ju, R. Chakraborty, C. Lamech and J. Plusquellic, "Stability analysis of a physical unclonable function based on metal resistance variations," *Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust*, pp.143-150, 2013.

[10] R. Helinski, D. Acharyya and J. Plusquellic, "A physical unclonable function defined using power distribution system equivalent resistance variations," *ACM/IEEE Design Automation Conference*, pp. 676-681, 2009.

[11] M. Wan, Z. He, S. Han, K. Dai and X. Zou, "An Invasive-Attack-Resistant PUF Based On Switched-Capacitor Circuit," *IEEE Transactions on Circuits and Systems I*, vol. 62, no. 8, pp. 2024-2034, Aug. 2015.

[12] C. Liu, "Design of High-Speed Energy-Efficient Successive-Approximation Analog-to-Digital Converters," *PhD Thesis, National Cheng Kung University*, June. 2010.

[13] W. Choi, H. Kim, and C.H. Kim, "Circuit Techniques for Mitigating Short-Term Vth Instability Issues in Successive Approximation Register (SAR) ADCs", *Custom Integrated Circuits Conference*, Sep. 2015

[14] R. Xu, "High-Speed Highly Sensitive CMOS Image Sensors," *PhD Thesis, Hong Kong University of Science and Technology*, Aug. 2013.

[15] C. Zhou, S. Satapathy, Y. Lao, K. K. Parhi and C. H. Kim, "Soft Response Generation and Thresholding Strategies for Linear and Feedforward MUX based PUFs," *IEEE International Symposium on Low Power Electronics and Design*, pp. 124-129, Aug. 2016

[16] S. Avvuru, C. Zhou, C.H. Kim, and K. Parhi, "Predicting Hard and Soft-Responses and Identifying Stable Challenges of MUX PUFs using ANNs", *IEEE Midwest Sympoisum on Circuits and Systems*, Aug. 2017

[17] F. Rahman, D. Forte and M. M. Tehranipoor, "Reliability vs. security: Challenges and opportunities for developing reliable and secure integrated circuits," *International Reliability Physics Symposium*, pp. 4C.6.1-4C.6.10, 2016.

[18] J. Delvaux, D. Gu and D. Schellekens, "Secure Lightweight Entity Authentication with Strong PUFs: Mission Impossible?" *International Workshop on Cryptographic Hardware and Embedded Systems*, pp.451-475, 2014.

[19] A. Koyily, S.V.S. Avvaru, C. Zhou, C.H. Kim and K. K. Parhi, "Effect of Aging on Linear and Nonlinear MUX PUFs by Statistical Modeling," Proc. of 23rd Asia and South Pacific Design Automation Conference, pp. 76-83, Jeju Island, Korea, Jan. 2018.