Current based PUF Exploiting Random Variations in SRAM Cells

Fengchao Zhang*, Shuo Yang*, Jim Plusquellic†, Swarup Bhunia*
*Department of Electrical and Computer Engineering, University of Florida, USA
fzhang67@ufl.edu, sy@ufl.edu, swarup@ece.ufl.edu
†Department of Electrical and Computer Engineering, University of New Mexico, USA
jplusq@unm.edu

***Abstract*—Physical Unclonable Function (PUF) is a security primitive that has been proven to be effective in diverse security solutions ranging from hardware authentication to on-die entropy generation. PUFs can be implemented in a design in two possible ways: (1) adding a separate dedicated circuit; and (2) reusing an existing on-chip structure for generating random signatures. A large percentage of existing PUFs falls into the first category, which suffers from the important drawback of often unacceptable hardware and design overhead. Moreover, they cannot be applied to legacy designs, which do not allow insertion of additional circuit structures. Intrinsic PUFs, that rely on pre-existing circuit structures, such as static random-access memory (SRAM), fall into the second category. They, however, typically suffer from poor entropy as well as lack of robustness. In this paper, we introduce a novel PUF implementation of the second category that exploits the effect of manufacturing process variations in SRAM read access current. In particular, we note that transistor level variations in SRAM cells cause significant variations in the read current and the variation changes with the stored content in a SRAM cell. We propose a method to transform the analog read current value for an SRAM array into robust binary signatures. The proposed PUF can be easily employed for authentication of commercial SRAM chips without any design modification. Furthermore, it can be realized, with minor hardware modification, into chips with embedded memory, e.g., a processor, for on-die entropy generation. Simulation results at 45nm CMOS process for 1000 chips as well as measurement results based on 30 commercial SRAM chips, show promising randomness, uniqueness and robustness under environmental fluctuations.**

I. Introduction

Security has emerged as an important design parameter for integrated circuits (ICs), which are vulnerable to diverse threats including counterfeiting, reverse engineering, and tampering attacks. A promising security primitive that has been investigated to deal with several hardware security issues, is Physical Unclonable Function (PUF). PUFs enable variety of security solutions for ICs - e.g., intellectual property (IP) counter-plagiarism, functional security measures, and hardware integrity validation. PUFs transform the intrinsic random variations in device parameters, e.g., threshold voltage (V_{th}), transistor length (L), width (W), and oxide thickness (T_{ox}) into circuit-level parameters, e.g., path delay or supply current to generate random digital signatures from an IC. PUFs typically lead to construction of unique and random set of challenge-response pairs (CRPs) for a chip. A random signature or key can be derived from a digital response from the PUF triggered by a digital input as challenge. The unclonability of PUFs originates from the unpredictable, random and hard-to-copy manufacturing variations in device parameters.

In this paper, we present a novel current-based strong PUF realized into an SRAM array that exploits the variations in read access current. It measures the transient current (I_{DDT}) during the read operation of SRAM array to generate large population of unique, robust and random signatures. The proposed PUF implementation exploits the effect of manufacturing process variations in SRAM word access current. In particular, we note that transistor level variations in SRAM cells can cause significant variations in the read current for a word based on the memory cells content. Simulation results on $45nm$ technology as well as experimental results on commercial off-the-shelf chips are analyzed regarding uniqueness, robustness and randomness. Integration of on-chip current sensor for on-die entropy generation has also been discussed.

II. Background

A. Related work

In the past few years, the design of silicon and non-silicon PUF has been a hot topic in hardware security that has led to many pioneering publications through nearly a decade of research. Existing PUFs can be broadly classified, based on how they are implemented, into two major categories: (1) PUFs based on separate circuit structures [1], [2]; (2) PUFs realized with common on-chip structures e.g., SRAM, flip-flops, or scan chain [3]–[5]. A majority of PUF implementations relies on independent circuit block to transform device level variations into digital signatures. These PUFs typically incur considerable hardware overhead and requires additional design/verification effort. On the contrary, the second class of PUFs, e.g., a popular SRAM PUF [6] that converts the power-on random state of SRAM cells into digital signatures is attractive in terms of virtually zero hardware or design overhead. However, such a PUF are limited with entropy density (one bit per cell) as well as poor robustness since the residual charge and minor environmental fluctuations can alter the power-up randomness of signature. Another disadvantage for such a PUF is that it requires altering the bit configuration procedure to retain the values and read it out [4]. Intrinsic SRAM PUFs that use parameter variation induced failures to generate random signatures have also been reported [7] [8].

B. SRAM Cell

SRAM is the de-facto standard of embedded memory in processor or other ICs. Fig. 1 (a) shows the schematic for a standard 6-Transistor (6T) SRAM cell. Examination of the circuit reveals the portion that will be conducting during read operation, which is shown in Fig. 1 (b) assuming that the initial value of V_Q is 0. Current flows from BL through AXL and into capacitor C_Q which is the small equivalent capacitance between Q node and ground. This current charges C_Q and thus V_Q rises and NL conducts. Equilibrium will be reached when C_Q is charged to a certain voltage at which I_{AXL} equals I_{NL}. I_{AXL} can be estimated as: $I_{AXL} = \frac{1}{2}(\mu C_{ox})(\frac{W}{L})_{AXL}(V_{DD} - V_{tn} - V_Q)^2$, where V_{tn} is the threshold voltage and I_{NL} can be written as:

978-3-9815370-6-2/DATE16/ ©2016 EDAA

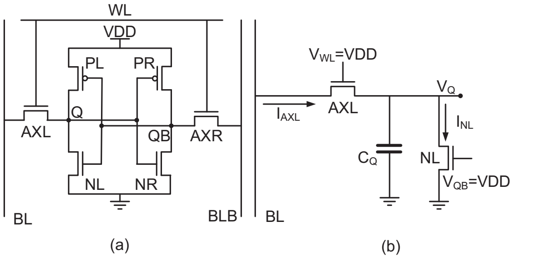

Fig. 1. (a) Structure of a typical 6T SRAM cell. (b) Relavant parts of the SRAM cell circuit during a read operation when the cell content is 0.

$I_{NL} = (\mu C_{ox})(\frac{W}{L})_{NL}[(V_{DD} - V_{tn})V_Q - \frac{1}{2}V_Q^2]$. Same current equilibrium condition happens to the BLB when V_QB is 0. More importantly, the voltage of the BL will decrease by a small amount of voltage corresponding to the voltage rising of V_Q. This is a result of the discharge of the capacitance of the BL by the current I_{NL}. When the change in BL voltage, ΔV, reaches the minimum value requirement of sense amplifier, corresponding time interval Δt is the optimal time window for I_{DDT} measurement.

III. Methodology

A. Source of Variation and Entropy

The inter- and intra-die process variations in an SRAM array are primarily caused by variations in transistor parameters, namely, L, W, Tox, and V_{th}, caused by physical phenomemnon such as line edge roughness and random doping fluctuations. A PUF typically exploits random intra-die variations, where two transistors experience purely random variations in their device parameters, in creating digital signature from a chip. Among the different sources of random intra-die variations, threshold voltage (V_{th}) variation due to the random dopant fluctuations is the most significant one for SRAM cells. In our simulations, the intra-die variation is principally contributed by V_{th} variations, while the variations on other parameters (such as L, W, Tox), are lumped as additional variation in V_{th} [7]. As shown in Fig. 1 (b), read current flows through access transistors AXL and NL and will be influenced by the V_{th} variation of AXL and NL when the cell stores logic 0. Considering the symmetric structure of SRAM cell, the read current will be influenced by the V_{th} variation of AXR and NR when the storing value is 1.

Based on the previous observation, the read current varies depending on the stored logic value. Considering a row of SRAM cells, read current in each cell flows through AXL and NL or AXR and NR. It shows that the read current (I_{DDT}) value changes depending on the stored values. $\overline{I_{DDT}}$ stands for average value of the I_{DDT} over Δt. Fig. 2 (a) shows the Hspice simulation results for $45nm$ technology of the variation of $\overline{I_{DDT}}$ based on 1000 chips with Gaussian-Distribution of V_{th} inter-die variation of $\sigma_{inter} = 15\%$, and intra-die variation of$\sigma_{intra} = 10\%$.

B. Enrollment and Data Collection

Maximum difference between 2 $\overline{I_{DDT}}$ values can be obtained if the comparison is designed to be made between two complementary word pairs. In this case, each cell will likely contribute different current value in the $\overline{I_{DDT}}$ for the word pairs. Each bit of the original word is randomly generated based on which the complementary word is produced to make up an input pair. The stored words are considered as inputs and $\overline{I_{DDTi}}$ stands for averaged current of the ith input while $\overline{I'_{DDTi}}$ represents the current value of its complementary. As illustrated in Fig. 2 (b), 384 128-bit input pairs are prepared, and $\overline{I_{DDTi}}$ and $\overline{I'_{DDTi}}$ have been collected for ith input.

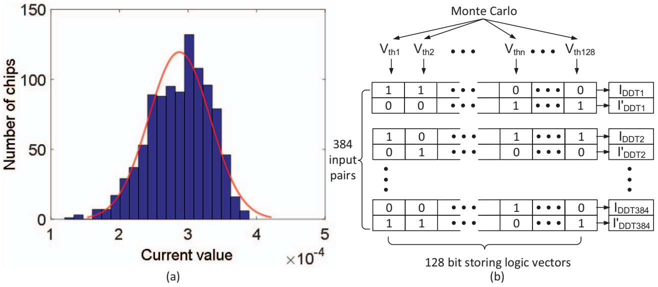

Fig. 2. (a)Histogram of $\overline{I_{DDT}}$ of 1000 chips for the same stored vector. (b) Illustration of the stored vectors and data collection.

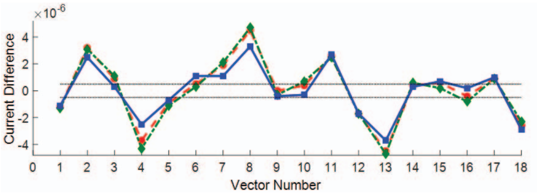

Fig. 3. $\Delta\overline{I_{DDTi}}$ @25 °C (red dash line with round marker), @10 °C (green dash-dot line with diamond marker) and @85 °C (blue solid line with square marker). The black dash lines are $\pm 0.5\mu A$ currents difference threshold @25 °C.

C. Post Process Signature Generation

The signature generation is optimized to achieve high uniqueness and robustness. Digitizing is accomplished depending on $\delta\overline{I_{DDTi}}$, the difference between $\overline{I_{DDTi}}$ and $\overline{I'_{DDTi}}$ to generate 1 bit of signature, e.g., $\Delta\overline{I_{DDTi}} \geq 0$ will result 1 at the ith bit. Both $\overline{I_{DDTi}}$ and $\overline{I'_{DDTi}}$ are influenced by the environment fluctuation and due to the different variation of transistors, the $\overline{I_{DDTi}}$ and $\overline{I'_{DDTi}}$ can change independently and will result in a flipping of the bit. Similar to the scheme proposed at [9], we apply a threshold of $\Delta\overline{I_{DDTi}}$ at normal condition to predict the range of change and discard the bits which fail to meet the threshold requirement. A threshold difference of 0.5 μA is applied and the final 128 bit signature is generated from 384 bit. This is estimated by the expectation of average Intra-HD to be acceptable with redundancy not exceeding the Triple-Module-Redundancy (TMR) scheme [10]. As shown in Fig. 3, 18 $\Delta\overline{I_{DDTi}}$ from the same chip are used to show how this threshold scheme works. Red, green and blue curve stand for the $\Delta\overline{I_{DDTi}}$ at 25 °C, 10 °C and 85°C, respectively, with dash black lines showing the threshold current difference. If the difference at 25 °C falls between the 2 threshold lines, it is very possible this bit will flip under 10 °C or 85°C. Therefore, in this diagram, bit number 6, 9, 10 and 16 are discarded but the rest are kept.

IV. Security Analysis

Monte Carlo Simulations in Hspice have been conducted using PTM $45nm$ CMOS process, with $\sigma_{inter} = 15\%$ and $\sigma_{intra} = 10\%$ based on 1×128 SRAM prototype for 1000 chips.

A. Uniqueness of signature

The metric for signature uniqueness is the fractional Inter Hamming distance (Inter HD) and its average based on m chips is:

$$HD_{inter} = \frac{2}{m(m-1)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} HD_{i,j} \quad (1)$$

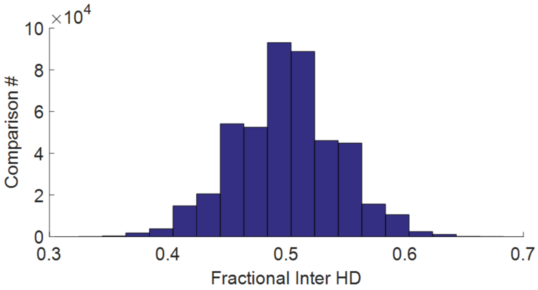

Fig. 4. Fractional Inter HD.

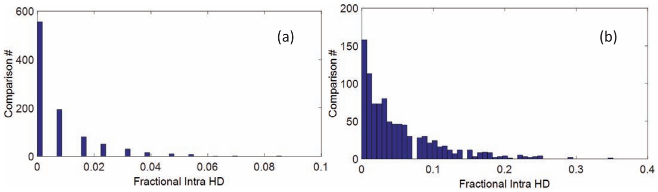

Fig. 5. Fractional Intra HD (a) @ 10 °C; and (b) @ 85 °C.

$HD_{i,j}$ is the fractional Inter HD between chips i and j and m is the number of chips. HD_{inter} is desired to be around 0.5. As shown in Fig. 4, the histogram of fractional Inter HD under normal condition (1V supply voltage and 25 °C room temperature) is distributed from 0.35 to 0.65 with the average of 49.97%.

B. Robustness of Signature

To evaluate the robustness of the signature, simulations at two different temperatures are conducted @ 10 °C and @ 85 °C. Fractional Intra Hamming distance (Intra HD) is calculated to quantify the number of different bits between the same signature @25 °C and @ 10 °C or @ 85 °C, respectively. In each case, the average of fractional Intra HD of $m = 1000$ chips is:

$$HD_{intra} = \frac{1}{m}\sum_{i=1}^{m} HD_i \tag{2}$$

HD_{intra} is desired to be 0, which means no signature bit will change due the the environmental fluctuation. In Fig. 5, histograms for Intra HD @ 10 °C and @ 85 °C are shown compared to the signature @25 °C. Average value of Intra HD are 0.72% and 5.07% for (a) and (b), respectively.

C. Randomness of Signature and Entropy

NIST randomness tests have been used to evaluate the randomness of data set [11]. Examination of the pass ratio for each test is required by NIST to evaluate the randomness. According to [11], when applied significance level $\alpha = 0.01$, the confidence interval is 98.05607%. In Fig. 6, the pass ratios are displayed which are all greater than the threshold confidence level (red dash line) which makes this method a potential candidate for on-chip entropy generation. The NIST tests that require larger input bit strings have been omitted in our study.

To analyze the unpredictability of information content, the maximum entropy of the proposed SRAM current PUF is discussed similar to [1]. The number of independent bits can be evaluated as a function of N, the number of cells in each row. There are $N!$ orderings of cells based on difference of stored content (0 or 1) in each cell and if the orderings are equally likely, the entropy will be $log_2(N!)$ bits. In this case, the 128-bit SRAM can produce 716 bits. However, each cell can only be used once to avoid any correlation and thus the 128-bit SRAM word can generate independent $128 * p$ bits, where p is entropy per cell current.

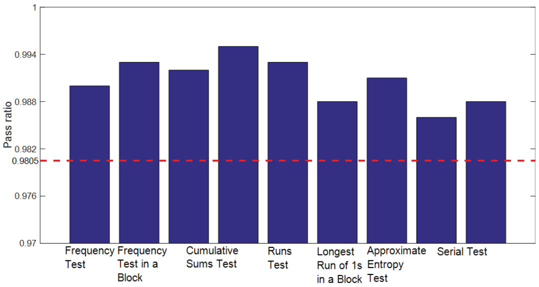

Fig. 6. Pass proportion plot with $\alpha = 0.01$.

D. Attacks Analysis

Machine learning attacks can potentially happen when adversary have the information about part of the CRPs. A machine learning model can be built based on the already known CRPs and can be trained to predict the remaining CRPs. It is reported that the increase in entropy [12] and decrease in training set [13] can decline the success rate, i.e., machine learning attacks can be prevented if the number of enrolled CRPs can be significantly increased. It means large entropy source is the best protection against modeling attacks [14]. In the proposed PUF, the application of different inputs to a single row of the SRAM combines the entropy sources from the individual SRAM cells in a potentially exponential behavior. As discussed, the entropy of the proposed SRAM PUF can be evaluated as $log_2(N!)$. For SRAM chips with multiple banks or sub-arrays, multiple rows can be combined together for signature generation thus increasing the total number of SRAM cells that contribute in the PUF signature. The proposed PUF, unlike conventional SRAM PUF, also facilitates signature extraction during normal operation of an SRAM array by implementing the current-based SRAM PUF into the idle rows.

V. Experiment

A. Setup and Result

To further evaluate the effectiveness of the proposed PUF, we performed current measurements with commercial off-the-shelf SRAM chips. Experiments are conducted by measuring I_{DDT} of 30 SRAM chips – IS62C256AL 32K × 8 LOW POWER CMOS SRAM chips from ISSI. The Schematic for the experimental setup is shown in Fig. 7 (a). At the negative edge of the chip enable (CE) and output enable (OE), the SRAM performs a read operation and after a small access time, the data will be read out validly to the I/O, i.e., the read process in the SRAM cell is finished and this interval is regarded as the time window. Agilent Technology MSO6012A mixed signal oscilloscope with sample rate of 2Ga/s is used to measure the voltage difference (and hence current) across a 10Ω precision sense resistor. The digital probe of the oscilloscope is connected to the SRAM chips to determine time window. Terasic DE0 FPGA board is used to provide control signals, addresses and storing input vectors to the SRAM chips. The sequence for the control signals is shown in Fig. 7 (b). The averaging time window is selected to be 40 samples (about 2ns) and normalization is done to minimize the setup fluctuation during multiple measurements. Total of 16 different vector pairs are used to measure currents and 16 bit of signature from each chip is

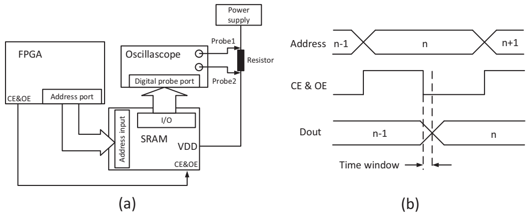

Fig. 7. (a) Schematic of the experimental setup. (b) Operation signal sequence.

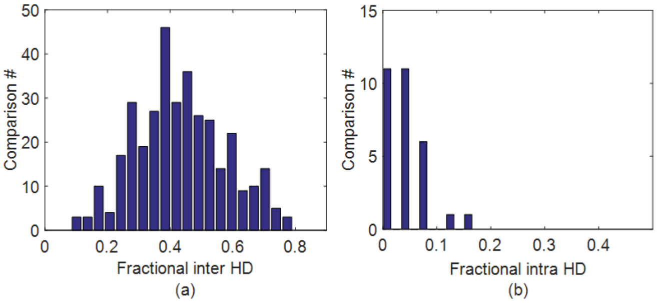

Fig. 8. (a) Fractional Inter HD; (b) Fractional Intra HD in the experimental results.

generated. The histogram of fractional Inter HD of 30 chips is displayed in Fig. 8 (a) with average Inter HD of 43.65%.

B. Repeatability and Improvement Discussion

Robustness is primarily based on the results of multiple time measurements. The measurement process discussed in the above section is applied at three different times to evaluate the stability of signatures under environmental fluctuation, e.g., voltage and temperature fluctuation. Following the same signature generation process, robustness of the signatures is evaluated by fractional Intra HD with the result shown in Fig. 8 (b) with average Intra HD of 4.61% without any bit selection process. Comparison between the proposed PUF and other SRAM PUFs is provided in Table I. It compares the entropy per cell, Inter HD, Intra HD (comparison of measured results at different time and high-temperature reliability study for simulation results) and run-time signature generation ability.

The modification on the SRAM structure is an option in further improving the PUF quality and usuability. The current value can be more precisely measured if SRAM arrays are designed with separate power supply for the core since the peripheral circuits can provide unpredictable contribution to the I_{DDT}. A common power supply for both core and peripheral circuits may decrease both the variation and stability of the measured current. Finally, for on-chip entropy generation, embedded current measurement circuit, e.g., a current interator and an analog-to-digital converter with appropriate sampling frequency [16] can be utilized which can also reduce the variation of the loop filter coefficient over voltage and temperature fluctuations.

TABLE I
COMPARISON AMONG SRAM PUFS

	Entropy/cell	Inter HD	Intra HD	Run-time
Power-up [15]	1	49.97%	4%	No
Experiment	5	43.65%	4.61%	Yes
MECCA [8]	1	49.9%	0.85%	No
RESP [7]	6	49.2%	2.88%	No
Simulation	5	49.97%	5.07%	Yes

VI. CONCLUSION

We have presented a novel PUF implementation in SRAM array that transforms the analog read current value for a codeword into binary signature. It shows good uniqueness, robustness and randomness while providing significantly higher entropy than common SRAM based PUFs. Since the proposed PUF does not require any design modification, it can be easily employed to authenticate stand-alone SRAM chips as well as wide array of chips with embedded memory, e.g., a processor, FPGA, and micro-controller. Due to the high entropy space, they are also promising for on-die entropy generation. While external current measurement can be effective for authentication, one needs to integrate low-overhead current sensors in a chip for on-die signature generation. The quality of the PUF is evaluated through both simulation and experiments with commercial SRAM chips, which show high quality and reproducibility of the signatures. Future work will focus on integrating on-chip current sensors and extending the approach to other kinds of memory, e.g., DRAM and flash.

REFERENCE

[1] 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.

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

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

[4] R. Maes, P. Tuyls, and I. Verbauwhede, "Intrinsic PUFs from flip-flops on reconfigurable devices," in *3rd Benelux workshop on information and system security (WISSec 2008)*, vol. 17, 2008.

[5] J. Aarestad, P. Ortiz, D. Acharyya, and J. Plusquellic, "HELP: A hardware-embedded delay PUF," *IEEE Design & Test*, vol. 30, no. 2, pp. 17–25, 2013.

[6] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up SRAM state as an identifying fingerprint and source of true random numbers," *Computers, IEEE Transactions on*, vol. 58, no. 9, pp. 1198–1210, 2009.

[7] Y. Zheng, M. S. Hashemian, and S. Bhunia, "RESP: a robust physical unclonable function retrofitted into embedded SRAM array," in *Design Automation Conference (DAC), 2013 50th ACM/EDAC/IEEE*. IEEE, 2013, pp. 1–9.

[8] A. R. Krishna, S. Narasimhan, X. Wang, and S. Bhunia, "MECCA: a robust low-overhead PUF using embedded memory array," in *Cryptographic Hardware and Embedded Systems–CHES 2011*. Springer, 2011, pp. 407–420.

[9] M. Hofer and C. Boehm, "An alternative to error correction for sram-like pufs," in *Cryptographic Hardware and Embedded Systems, CHES 2010*. Springer, 2010, pp. 335–350.

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

[11] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," DTIC Document, Tech. Rep., 2001.

[12] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, 2010, pp. 237–249.

[13] G. Hospodar, R. Maes, and I. Verbauwhede, "Machine learning attacks on 65nm arbiter pufs: Accurate modeling poses strict bounds on usability," in *Information Forensics and Security (WIFS), 2012 IEEE International Workshop on*. IEEE, 2012, pp. 37–42.

[14] J. Delvaux, D. Gu, R. Peeters, and I. Verbauwhede, "A survey on lightweight entity authentication with strong PUFs."

[15] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, *FPGA intrinsic PUFs and their use for IP protection*. Springer, 2007.

[16] M. Bolatkale, L. J. Breems, R. Rutten, and K. A. Makinwa, "A 4 ghz continuous-time adc with 70 db DR and 74 dBFS THD in 125 mhz BW," *Solid-State Circuits, IEEE Journal of*, vol. 46, no. 12, pp. 2857–2868, 2011.