Statistical Analysis of Arbiter Physical Unclonable Functions using Reliable and Secure Transmission Gates

Sadulla Shaik [1], Anil Kumar Kurra [2], A. Surendar [3]

Department of Electronics and Communication Engineering
Vignan's Foundation for Science Technology & Research,
Vadlamudi-522213, Andhra Pradesh, India
[1] sadulla09@gmail.com, [2] kakumar94@gmail.com, [3] surendararavindhan@gmail.com.

***Abstract* - Physical Unclonable Functions (PUFs) are a set of emerging technologies to deal with cloning, Intellectual Property (IP) protection, and security against reverse engineering schemes to restrict the over production of semiconductor chips. Delay based PUFs represent an inviting option due to minimal space circuitry over conventional type arbiter PUF. This paper presents a novel transmission gate based arbiter PUF for authentication of the electronic hardware systems. These PUFs have been widely used as security primitives for device authentication and identification. By measuring the statistical parameters using Monte Carlo analysis we demonstrated that the proposed design significantly enhances the performance of the arbiter PUF. Our arbiter PUF produced 48.5% of uniqueness for 64 bit challenge pair, and their reliability was demonstrated across different environmental variations.**

Keywords* - *Challenge Response pairs (CRPs), Monte Carlo simulation, Physical unclonable Functions (PUFs), Reliability.

I. INTRODUCTION

Physical unclonable functions (PUFs) provide one of the promising techniques in authentification mechanism and secure key generation [1-4]. A PUF structure maps a set of challenges to a set of response pairs (CRPs) due to complex physical variations [5]. Hence it improves the degree of security of the chip. Due to its random process variations it is to hard to duplicate the similar structures and behavior of the PUF depends on electrical parameters such as delay, threshold voltage, current, and resistance value. The performance of the circuits can be evaluated by analyzing the reliability, resilience, uniqueness, uniformity etc. A low reliable PUF indicates getting same response for the different challenges and it is unacceptable for encryption [6]. The response of the PUF is continuously alters due to uncertainties in the semiconductor manufacturing process variations. Depending upon the number of challenge response pairs PUFs are divided as strong PUFs and weak PUFs [7]. Strong PUFs has different response pairs for each and every set of challenge and on the other weak PUFs are treated as getting similar kind of responses for dissimilar challenges. Based on the construction properties and operation principle PUFs can be categorized into non-electronic PUF (acoustical PUF, optical PUF), electronic PUF (coating PUF, power distribution PUF), delay based PUF (arbiter PUF, ring oscillator PUF , glitch PUF, anderson PUF), memory based PUF (SRAM PUF, butterfly PUF, flip-flop PUF). The response of the PUF is mainly depends on the delay of the successive multiplexers and the by silicon material it has common CMOS manufacturing process variations [8]. For each challenge the response of the IC are varied because the response is sensitive to circuit parameters such as process variations in transistors and wires.

II. ARBITER PUF CIRCUIT DESIGN

An arbiter based PUF consists of a set of multiplexers connected in parallel with each other and arbiter at the end. As shown in Fig.1 the multiplexer has symmetrical aspect ratios and differs with device parameters due to process variations [9-10]. A set of challenges (input pulse) is excited to an arbiter PUF. Depending upon arrival of the pulse arbiter generates response bit either 1 or 0.

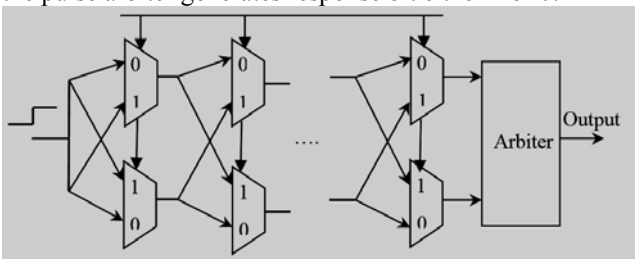


Fig. 1. Arbiter PUF structure.

Fig.2 shows multiplexers are consider being switches, it consists of the 63 switches and each switch has different configurable delay paths.

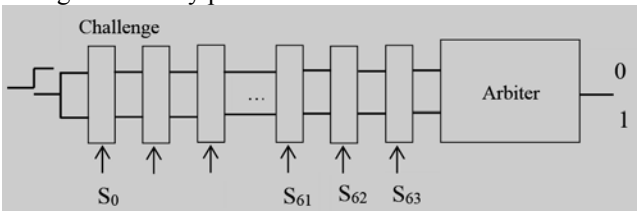


Fig. 2. Switch level Arbiter PUF.

The delay variations can be examined by differences between top and bottom paths, Generated arbiter response is vary across each integrated circuit (IC) to maintain the nominal delay differences between each PUF, has to maximize the Interchip variation of PUFs thus the response of PUFs are biased to 0 or 1.

Fig. 3 shows the switch component transmission gate based (2-to-1) multiplexer. It has two input ports A and B and a selection line S depending upon the selection line the response forwarded. As if selection line S0=0, the path move straight while S1=1 they are crossed. It can be done a set of transmission gate based Multiplexers and inverters. The cells are routed and placed uniformly and wire delay in a circuit decides response of the circuit.

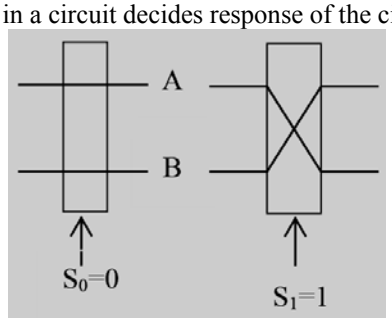


Fig. 3. Switch component level.

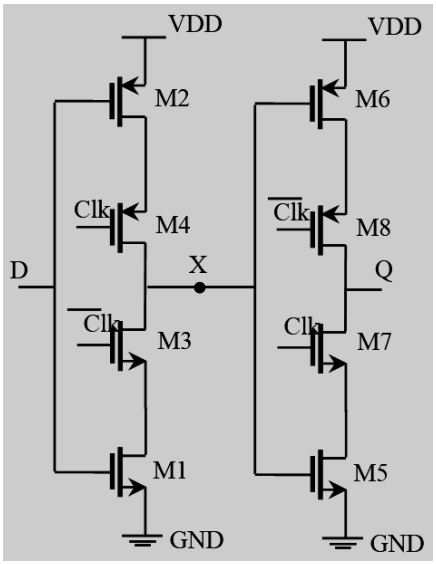


Fig. 4. Clocked CMOS Edge Triggered Register.

A. Arbiter Design

Fig. 4 shows the clocked CMOS register and it acts as data selector. It has two stages first stage acts as a master and second state acts as slave. Depending upon the CLK and applied input it can be operated in two phases. CLK=0 ($\overline{CLK}=1$) and input from the last stage of Multiplexer is D=0 as a result M2 and M4 is turn on and M1, M3 turn off, output at X becomes HIGH (VDD). It acts as input to the second stage (slave stage) when high input is applied while M6, M8 is turn off and M5, M7 is turn on condition hence Output becomes 0 at Q. CLK=1($\overline{CLK}=0$) and input from the last stage of Multiplexer is D=1 as a result M2 and M4 is turn off and M1, M3 turn on output at X becomes LOW (GND). It acts as input to the second stage (slave stage) while M6, M8 is turn on and M5, M7 is turn off condition. Output becomes 1.

B. Factors Affecting the Response of the Arbiter Pufs

To identify the characteristics of PUFs, we assign a set of challenges to the each arbiter PUF. By using variance of inter-chip variation the response of two different PUFs can be estimated. We can distinguish the response of the PUF by its probability of error [11]. Usually response of PUF affected by the factors such as noise, environmental variations, met stability and aging. In arbiter based PUF the response is mainly depends on the delay differences between the paths, process variations. Hence the effect of the environmental noise is not significantly impact on the response pair's until if much environmental variations [12-13].

III. PERFORMANCE EVALUATION AND VALIDATION OF TRANSMISSION GATE ARBITER PUF

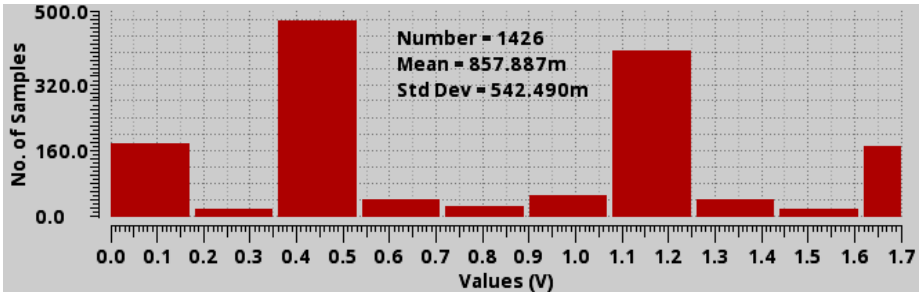
In this section we explain the statistical evaluation of the transmission gate based arbiter PUF, with respect to the security metrics of uniqueness, reliability and followed by randomness followed by their results.

A. Uniqueness

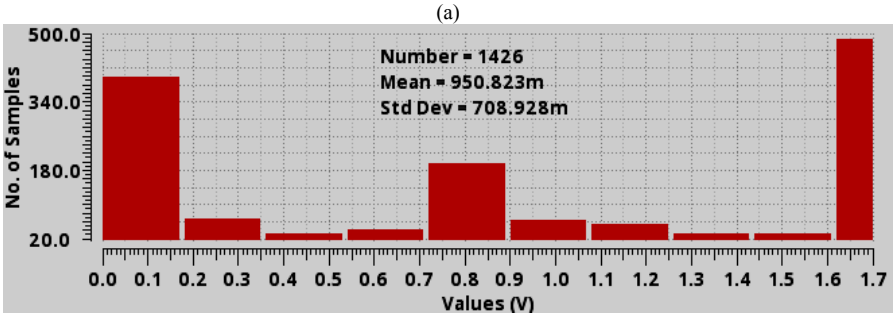
The uniqueness of the PUF is ability to maintain the response is uncorrelated for each and every instance [14]. It can be determined by evaluating the Inter die Hamming Distance (HD). It is typically the average of HD among the responses of various PUFs over multiple challenge response pairs. The interdie hamming distance among the k chips is given by 'K' represents the chips, 'Ri' and 'Rj' are n-bit responses to a challenge 'C' from chips 'i' and 'j' respectively.

$$Inter-die\,HD=\frac{2}{K(K-1)}\sum_{i=1}^{k-1}\sum_{j=i+1}^{k}\frac{HD(R_i,R_j)}{n}\times 100\% \quad (1)$$

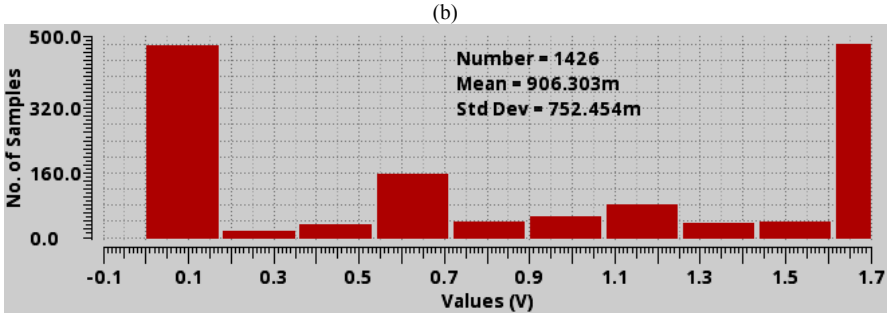
Fig. 5 shows the uniqueness is estimated From Monte Carlo Analysis by calculating Hamming Distance (HD) distribution measured over the 500 samples at 1.7V. We found that average HD(uniqueness) is 48.5% (Fig. 5 c) which is close to the ideal uniqueness (50%) and very small standard deviation of 0.0496 and mean (>3%).



(a)



(b)



(c)

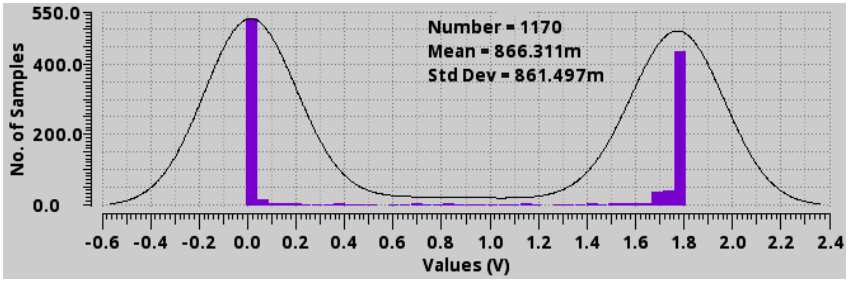
Fig. 5. (a), (b) and (c) shows the different Hamming Distance distribution for the same sampling values in transmission gate arbiter PUF.

B. Reliability

Reliability indicates the ability to produce the same kind of response for a particular challenge across various environmental variations like temperature. Which is one of the important parameter it describes quality of the manufactured PUF circuitry [15-16]. In this we measured the PUF response by applying random set of challenges at different temperatures. By using the linear trade line curve we estimated the maximum process variations of data and from the measured samples found the number of bits flipped for each challenge.

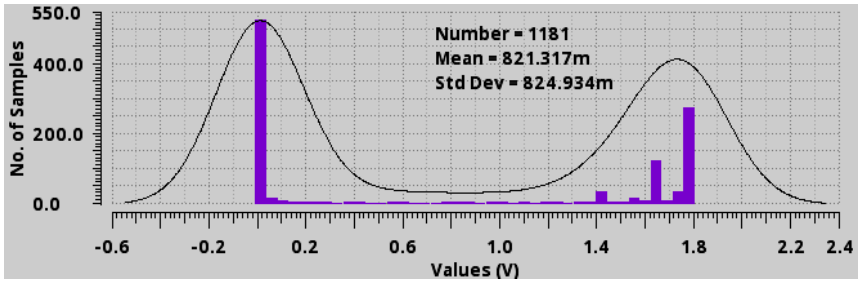
To estimate the reliability of the PUF metric it can be done by using the Intradie-Hamming distance and it is calculated by using T samples can be collected from chip i at different operating conditions at n bit response (Ri). The average reliability metric (r).

$$r_i = \frac{1}{T}\sum_{t=1}^{T}\frac{HD\left(R_i, R_{i,t}\right)}{n}\times 100\% \tag{2}$$

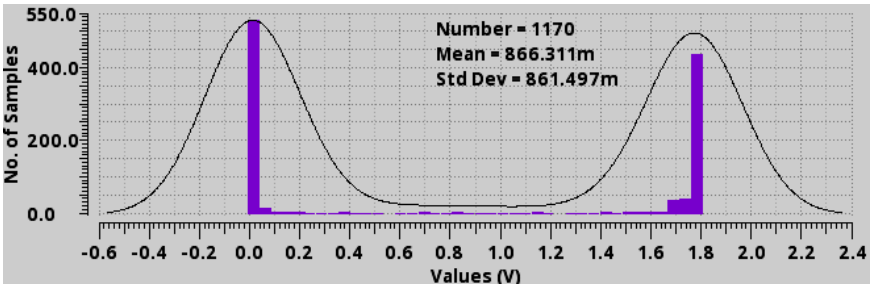


-a

Fig. 6-a. Bits flipped in PUF at different temperatures (a) -50c



-b



-c

Fig. 6-b and -c. Bits flipped in PUF at different temperatures (b) 25c (c) 750c.

For measuring intradie-Hamming distance we consider the 24 set of IDs and measured at the different operating conditions. During the challenge 1 Fig. 6 (a) 3% of samples were changed in contrast a small variation of the mean and standard deviation of the PUF. Similar to the Fig.6 (b), 4.5% and for Fig. 6 (c) 7% of variation of responses for corresponding challenge. From that analysis we concluded that most of the bits are not flipped under different conditions hence reliability of PUF close to the 90%.

C. Randomness Evaluation

Randomness evaluation of the data PUF is one of the important attribute in PUF circuit. It eliminates the prediction of the response of the cells. The silicon PUFs has wide variety of intrinsic properties and manufacturing process variations, it generates the unique ID responses and we proved it reaches to nearly 95%. To estimate the randomness of the PUF it can be evaluated by techniques such as min entropy and Shannon entropy [17]. From our analysis we used min-entropy method to estimates the number of bits is uniformly random. Min-entropy is estimated as:

$$P_{MAX} = MAX\{Hwt(i), 1 - Hwt(i)\} \tag{3}$$

$$Min - entropy = \frac{1}{128}\sum_{i=1}^{128}\left(-\log_2\left(P_{MAX}(i)\right)\right) \tag{4}$$

From the above expression 'i' represent number of ID bits, Hwt (i) defines number of hamming weights of non-zero bits. Here we calculated the randomness of PUF for 8 cases we got the entropy by 0.924, it nearly equal to min entropy of 1. Table I shows the performance of the transmission gate based arbiter PUF.

TABLE I. THE PERFORMANCE OF THE TRANSMISSION GATE BASED ARBITER PUF.

	Case							
	1	2	3	4	5	3	4	5
Uniqueness	41%	44%	38%	46%	48%	47%	43%	45%
Reliability	72%	78%	82%	79%	83%	91%	84%	86%
Randomness	62%	82%	72%	79%	72%	81%	95%	69%

D. Effect of Temperature on Stability of Arbiter Puf

Temperature plays a significant role on the performance arbiter PUF and it affects the power leakage at the transistor level. It also much impact on the stability of the device. Here we analyze the samples of the PUF in different temperature levels (350c to -400c). It gives the variation of samples at different conditions from low temperature, high temperature and normal conditions.

TABLE II. POWER LEAKAGES DUE TO VARIATION OF TEMPERATURE.

Case	Temperature (oC)	VDD Bias (%)	3σ	Power Leakage (%)
1	35	0	0	3
2	40	-10	25	5
3	75	-10	5	8
4	-25	+10	20	4
5	-40	+5	5	6

Change in temperature may lead to change the variance of no. of samples the PUF. Considering above data we calculated the stability of the device. During the low temperatures the number of bits flipped to be 25% and at high temperature 32% of bits (from 0 to 1) are flipped. The amount of power dissipated during change in temperature is given by Table II.

E. Effect of the Voltage Variations

The challenge response of the PUF is also depends on the on the voltage variations across the PUF. To find the consistency need to estimate the PUF under different voltages. If vary the supply voltage from 15% to 25% and taken the 20 sample at low voltage condition (1.8v) and high voltage conditions 3.6v and 4.2v (Fig. 7) and the percentage of the bits are varied can be estimated as shown in below Fig. 7 represents the variation of samples under different conditions.

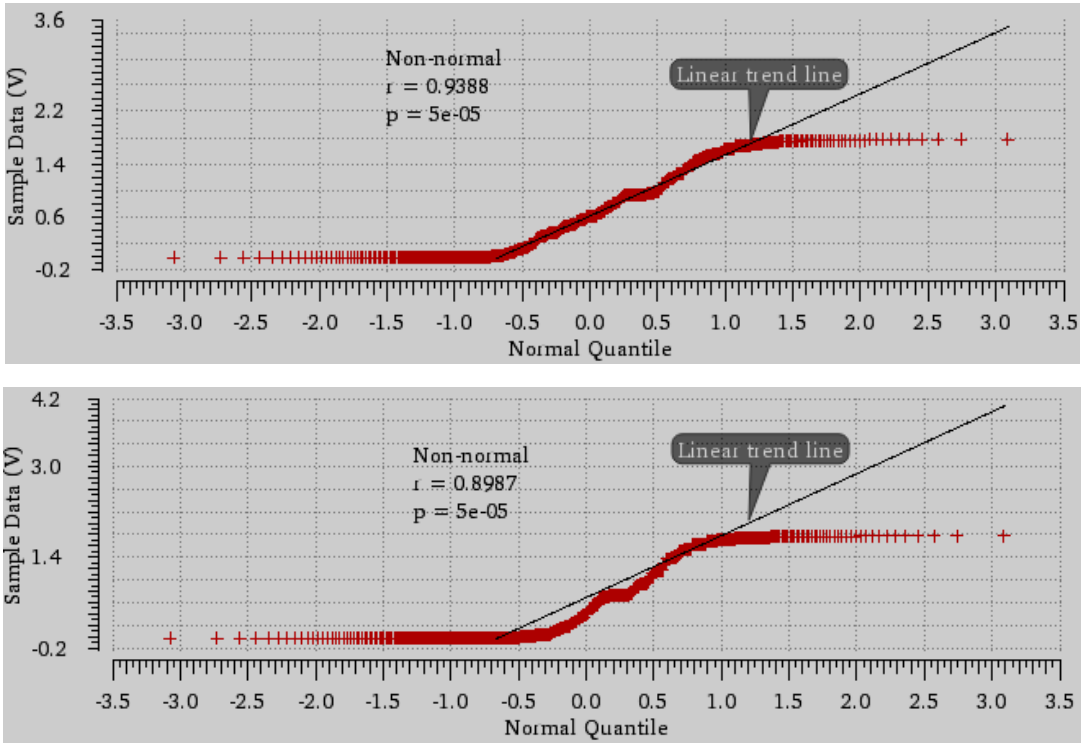


Fig. 7. Effect on Voltage variation on stability.

IV. CONCLUSION

We have proposed a new transmission gate arbiter based PUF in 180nm technology and investigate its statistical parameters such as - reliability, uniqueness, and randomness at various conditions. From the simulation results shows that CMOS technology has unique manufacturing property variations which lead to maintain the more authenticity. our proposed circuit is more reliable compared to existing circuits. And we intend to fabricate our PUF circuit in future.

REFERENCES

[1] Herder, Charles, Meng-Day Yu, Farinaz Koushanfar, and Srinivas Devadas. "Physical unclonable functions and applications: A tutorial," Proceedings of the IEEE, vol. 102, no. 8, 2014, pp.1126-1141.

[2] Beckmann, Nathan, and Miodrag Potkonjak, "Hardware-based public-key cryptography with public physically unclonable functions," In International Workshop on Information Hiding, Jun 8 ,pp. 206-220. Springer Berlin Heidelberg, 2009.

[3] Guajardo, Jorge, Sandeep S. Kumar, Geert-Jan Schrijen, and Pim Tuyls, "Physical unclonable functions and public-key crypto for FPGA IP protection," In Field Programmable Logic and Applications, 2007. FPL 2007. International Conference on, pp. 189-195. IEEE, 2007.

[4] Roel MA. Physically unclonable functions: Constructions, properties and applications. Dissertation, University of KU Leuven. 2012 Aug.

[5] Rührmair, Ulrich, Jan Sölter, and Frank Sehnke, "On the Foundations of Physical Unclonable Functions," IACR Cryptology ePrint Archive 2009 (2009): 277.

[6] Guajardo, Jorge, Sandeep S. Kumar, Geert-Jan Schrijen, and Pim Tuyls, "Brand and IP protection with physical unclonable functions," In Circuits and Systems, 2008. ISCAS 2008. IEEE International Symposium on, pp. 3186-3189. IEEE, 2008.

[7] Tuyls, Pim, and Boris Škorić, "Strong authentication with physical unclonable functions," In Security, Privacy, and Trust in Modern Data Management, pp. 133-148. Springer Berlin Heidelberg, 2007.

[8] Puntin, Daniele, Stefano Stanzione, and Giuseppe Iannaccone, "CMOS unclonable system for secure authentication based on device variability," In Solid-State Circuits Conference, 2008. ESSCIRC 2008. 34th European, pp. 130-133. IEEE, 2008.

[9] Bhargava, Mudit, Cagla Cakir, and Ken Mai, "Reliability enhancement of bi-stable PUFs in 65nm bulk CMOS," In Hardware-Oriented Security and Trust (HOST), 2012 IEEE International Symposium on, pp. 25-30. IEEE, 2012.

[10] Shaik, Sadulla, and Prathiba Jonnala, "Performance evaluation of different SRAM topologies using 180, 90 and 45 nm technology," Renewable Energy and Sustainable Energy (ICRESE), 2013 International Conference on. IEEE, 2013, pp.15-20.

[11] Yu, Meng-Day Mandel, and Srinivas Devadas, "Secure and robust error correction for physical unclonable functions," IEEE Design & Test of Computers 27, no. 1 (2010): 48-65.

[12] J. Aarestad, J. Plusquellic, D. Acharyya, "Error-tolerant bit generation techniques for use with a hardware-embedded path delay PUF," Hardware-Oriented Security and Trust (HOST) 2013 IEEE International Symposium on, pp. 151-158, 2013.

[13] Gurugubelli Srirama Murthy, Darvinder Singh and Sadulla Shaik, "An Area Efficient Built-In Redundancy Analysis for Embedded Memory with Selectable 1-D Redundancy," Advances in

Intelligent Systems and Computing, Springer International Publishing AG, 2016.

[14] H. Busch, S. Katzenbeisser, P. Baecher, "PUF-based authentication protocols - Revisited," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5932, pp. 296-308, Dec 2009.

[15] Vivekraja, Vignesh, and Leyla Nazhandali, "Circuit-level techniques for reliable physically uncloneable functions," In Hardware-Oriented Security and Trust, 2009. HOST'09. IEEE International Workshop on, pp. 30-35. IEEE, 2009.

[16] Chen, An, "Utilizing the variability of resistive random access memory to implement reconfigurable physical unclonable functions," IEEE Electron Device Letters 36, no. 2 (2015): 138-140.