TV-PUF : A Fast Lightweight Analog Physical Unclonable Function

Tanujay Saha* and Vikash Sehwag†
Department of Electronics and Electrical Communication Engineering
Indian Institute of Technology, Kharagpur
West Bengal, India
Email: *tanujay.saha@gmail.com,†sehwag.vikash@gmail.com,

***Abstract*—Physical Unclonable Function (PUF) is the hardware counterpart of a one-way function. It is capable of addressing hardware security issues such as device authentication, secret key generation for cryptographic protocols, producing seeds for Random Number Generators and much more. In this paper, we propose a design of an aging resistant, lightweight and low-power analog PUF which exploits the susceptibility of Threshold Voltage (V_{th}) of MOSFETs to process variations. Analyses of this *Threshold Voltage PUF (TV-PUF)* show improvements in power consumption, reliability and anti-aging properties over the contemporary PUF designs. Improvements have also been observed in security parameters like uniformity, reliability and uniqueness for 64-bit key generation over the existing PUF schemes. At 1 GHz clock input for the sense amplifier, our design consumes 0.18 μW/bit power with 50% uniqueness and 50% uniformity. Moreover, it has been seen that the performance of this PUF is independent of the technology node in which it is being used, i.e., it gives high performance in 45nm, 65nm and 90nm technology nodes. Aging analysis of the TV-PUF shows that the reliability of our PUF remains unaffected by aging of the device.**

***Index Terms*—Physical Unclonable Function (PUF) , Threshold Voltage, Hardware Security primitive, Low power VLSI circuits**

I. Introduction

Physical Unclonable Function (PUF) is a hardware primitive which utilizes the process induced variations present in a device to generate unique cryptographic keys [1]–[3]. The security of the PUF is based on the fact that a particular instance of a PUF can never be mimicked due to the uncertainty of the process variations present in different devices. While it is a major weapon against IC counterfeiting [4], it can also be used for IP protection [5].

PUFs can be broadly classified into two design categories, namely *Delay-based* PUFs (Arbiter PUF, Ring oscillator PUF, Glitch PUF, Schmitt trigger PUF) and *Memory-based* PUFs (SRAM based PUF, Butterfly PUF, Latch PUF) [6]. While each of these excels in different aspects, a less complex and low power design is always desirable for a PUF so that it does not produce any overhead and is easy to fabricate. Previously, a threshold voltage based IC identification scheme called ICID [7] was proposed. It is shown in this paper that the proposed Threshold Voltage PUF (TV-PUF) is more efficient than ICID both in terms of security parameters as well as VLSI design parameters (area and power consumption). Another important aspect in PUF characteristics is its degradation of reliability with aging of the device [8], [9]. This is an important design parameter of the PUF as it determines its longevity. Most of the previous PUF designs employ CMOS technology which incorporates both PMOS and NMOS. In MOSFETs, the major reliability issues are Bias Temperature Instability (BTI) and Hot Carrier Injection (HCI). Negative-Bias Temperature Instability (NBTI) is observed in PMOS while Positive-Bias Temperature Instability (PBTI) has its impact on NMOS. Both HCI and NBTI cause undesired increase in the threshold voltage of the transistor (V_{th}) over time whereas PBTI only plays a role when high-K gate oxide materials are used. In our design, only NMOS transistors are used. So, the core threat to the reliability of TV-PUF is the HCI effect in transistors.

We propose a Threshold voltage (V_{th}) based PUF (TV-PUF) which captures the effect of process induced variations in V_{th} of NMOS transistors. Threshold voltage has been chosen as the primary source of process variations because it is dependent on numerous factors [10]. Some of them are the oxide thickness, doping concentrations of the n and p regions of the FET and the work function of silicon. Moreover, its dependency on the doping of the channel is highly non-linear. Such irregular dependencies on so many factors make the process variations very random, thereby making it more difficult to clone a particular PUF instance.

The rest of the paper is organized in the following manner. Section II discusses the contributions of TV-PUF to the literature. Section III provides the detailed description of the design while Section IV provides the experimental evaluations of standard PUF metrics for the proposed PUF and compares them with those of the existing PUFs. In section V, reliability concerns due to aging are discussed. Section VI compares the TV-PUF with the existing PUFs in terms of power consumption and transistor count. Section VII concludes the work and sugests some future directions of research in this area.

II. Our Contributions

TV-PUF contributes to the literature of PUFs in the following dimensions:

*†***Both authors contributed equally to this paper***

- The TV-PUF has a very low circuit overhead. It comprises of six NMOS transistors and a sense amplifier for the generation of one challenge-response pair. Thus, being lightweight, it can be embedded on an IC chip with minimum overhead.
- TV-PUF can operate at very high frequencies due to its very low critical path delay. The TV-PUF has only two NMOS transistors in its critical path. This causes a delay in the order of 100 ps at 1V supply voltage in 65 nm technology node. Due to very low latency, it may be used in a wide variety of day-to-day devices like authentication of smart cards.
- Improvements in PUF quality metrics such as uniformity, uniqueness, reliability and bit aliasing have also been observed for TV-PUF. A detailed comparison with some of the most widely used PUFs have been given in Section IV. Moreover, it is shown that these properties do not alter with the change of the technology node.
- TV-PUF shows a strong aging resistant nature. In Section V, we discuss the effect of aging on its reliability over a span of 5 years.

III. Design of TV-PUF

The threshold voltage of a MOSFET, being highly susceptible to process induced variations, is being used as the basis of operation in the design of TV-PUF. For a NMOS pass transistor (Fig. 1), as V_x increases, the current-drive of the transistor ($V_{IN} - V_x$) reduces significantly. This is evident from the characteristic curve of the pass transistor, by the long tail in V_x (Fig. 1) as it approaches $V_{dd} - V_{th}$.

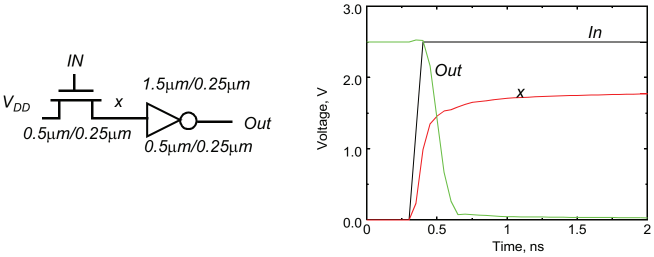
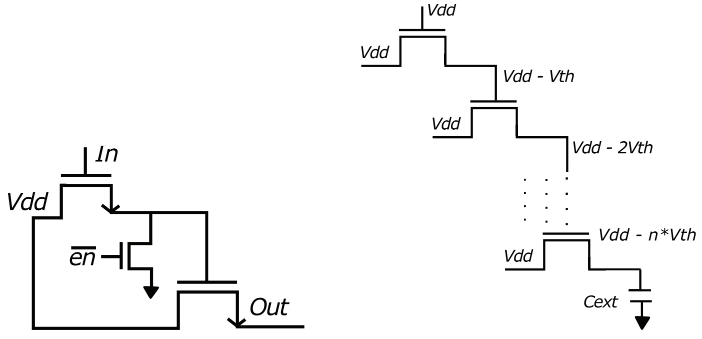


Fig. 1: NMOS Pass transistor and its Voltage transfer characteristic (VTC) [10]

A. Block Diagrams and Working of the design

If the PUF response is produced solely on the basis of the difference in V_{th} of two isolated transistors, the response will not be robust. This is because the difference in the threshold voltages of these two transistors will be very small. So they will be highly susceptible to environmental noises. However, the robustness of the TV-PUF can be increased by cascading n transistors in series and collecting the output at the source terminal of the last transistor. This causes the output voltage at the source terminal of the cascaded series of transistors to be $V_{DD} - n \times V_{th}$. In this design, two pass transistors are cascaded in series, that is $n = 2$ (Fig. 2).



(a)

(b)

Fig. 2: a) Transistor level design of one block b) Cascading of n pass transistors

Block level design of TV-PUF is depicted in Fig. 3. The input is a $n - bit$ challenge which is passed to an active high $n - to - 2^n$ line decoder. The decoder output is such that only one of the output pins is set to level $HIGH$ (V_{dd}) while all the others are set to level LOW (0 V). These pins are connected to the gate terminals (*IN*) of the first MOSFET in the cascaded series of MOSFETs present in each block. Each output pin of the decoder is an input to two unique blocks among the 128 blocks. For a unique challenge, only one of the decoder outputs is $HIGH$, so only two blocks out of 128 blocks have $V_{IN} = V_{dd}$.

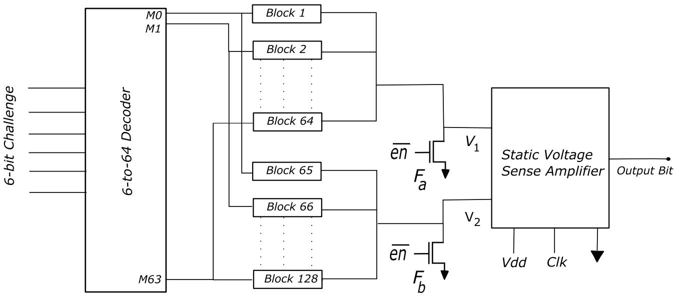


Fig. 3: Block Diagram of proposed TV-PUF with $6 - bit$ challenge

It is important to note that each decoder output is connected to two blocks where the former is one among the first 64 blocks and the latter is one among the last 64 blocks. When the TV-PUF receives an input challenge, the *enable (en)* signal is $HIGH$ in first clock cycle such that V_1 and V_2 will increase and approach the saturation voltage. Depending on the sense amplifier clock rate, it will sample the two voltages at a particular instant and compare them to generate the output bit.

After the output is obtained, the $enable$ signal changes its state to LOW which activates transistors F_a and F_b thus reinforces $V_1 = V_2 = 0V$. Transistors F_a and F_b are being referred to as flush transistors because they pull-down the voltages at the drain terminals of the cascaded series of MOSFETs to zero after the generation of one response. This re-establishes the initial condition of the TV-PUF and makes it ready for the next challenge. While producing the next output, the initial conditions need to be restored otherwise the transistors in the High-Z condition have unpredictable values which leads to erroneous responses.

Fig. 4 demonstrates the simulation of output $V_1 = V_2$ when *en=LOW* and *en=HIGH*. The flush transistors establish the accuracy of PUF by keeping the system close to ideal.

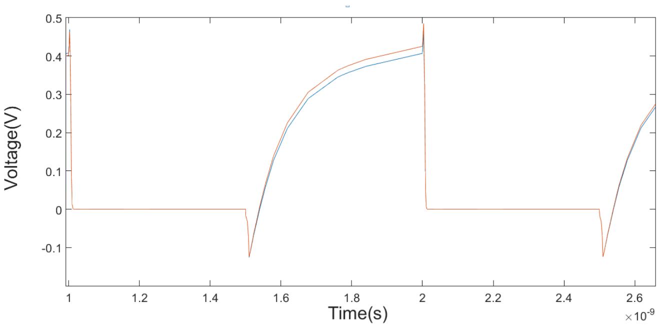


Fig. 4: Transient analysis of two different blocks output voltage

To generate a 64-bit key, 128 different pairs of blocks are constructed. For each challenge, one block from the first 64 blocks and another block from the last 64 blocks will be activated. After the generation of the one bit response, the enable (en) signal is used to reset the output voltages to zero using transistor F_a and F_b. The time required to reset (Fig. 4) the voltages $V_1 = V_2 = 0V$ is approximately $35ps$ to $40ps$ for 65nm technology node which is much less than the time of conduction. Thus, the en signal does not need to have 50% duty cycle. In contrast to [7] and [11], current does not flow through all the transistors of the TV-PUF for the generation of a one bit response. This selective current flow mechanism reduces the power consumption of the TV-PUF in comparison to that of ICID.

IV. Performance Evaluation

In this section, we discuss the security metrics of the TV-PUF. The uniqueness of responses, reliability of the PUF with variations in temperature and supply voltage, uniformity, bit-aliasing and auto-correlation values for TV-PUF are reported. We have also reported these performance metrics on different silicon technology nodes, namely 45nm, 65nm and 90nm. All the aforementioned analyses are done using HSpice [12]. For MOSFET modelling, BSIM Level=54 model files from [13] are included.

A. Uniqueness, Uniformity, Bit Aliasing and Correlation Analysis

The response of an instance of a PUF for a particular challenge should be independent of the response of another instance of the PUF for the same challenge. This is portrayed by the $Uniqueness$ of the PUF. The value of the uniqueness metric should ideally be 50%. It is measured by calculating the inter-die Hamming Distance of the different PUF instances.

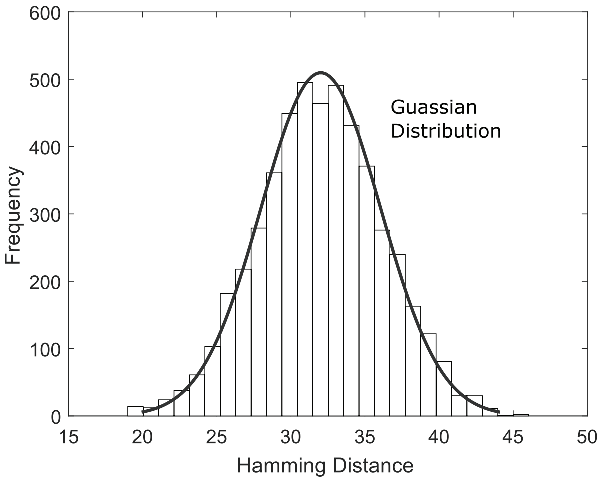


Fig. 5: Inter-chip Hamming Distances (total number of bits = 64)

The inter-die Hamming Distance follows a Normal distribution $N(\mu, \sigma)$. The ideal values of μ and σ are 50% and 0 respectively. For our experiment, Monte Carlo simulation is used to capture process variation in 100 different chips. Fig. 5 shows the simulation results for inter-die Hamming Distance for all pairs of challenges on two different instances of the TV-PUF.

Another measure of evaluating the PUF is the $Autocorrelation$ (R_{XX}) between its response bits. A higher auto-correlation implies that the responses are dependent on one another and then the PUF becomes vulnerable to Machine Learning based prediction attacks. If bit-aliasing occurs then different chips may produce nearly identical PUF responses, which is an undesirable effect. We estimate bit-aliasing of the l^{th} bit in the PUF identifier as the percentage Hamming Weight (HW) of the l^{th} bit of the identifier across k devices [14]. Table II shows the simulation results for Autocorrelation and Bit-aliasing.

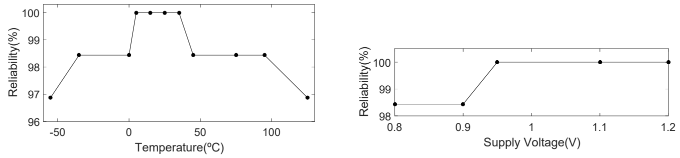
$$R_{XX}(j) = \sum_n x_n x_{n-j}$$

TABLE I: Comparison of PUF characteristics with different proposed intrinsic PUF construction [15]

PUF Construction	$\mu_{inter} \pm \sigma_{inter}$	$\mu_{intra} \pm \sigma_{intra}$
Feed-forward Arbiter PUF	38%	9.8%
Sub-threshold Arbiter PUF	≈ 50%	<5%
Ring Oscillator PUF	46.15%	0.48%
Glitch PUF	41.5%	<6.6%
SRAM PUF	49.97%± 0.3%	<12%
Latch PUF	50.55%	3.04%
Flip Flop PUF	36%± 2.9%	<13%
Butterfly PUF	≈50%	<4%
Proposed TV-PUF	≈51%	<4%

* the results encompass environmental fluctuations

PUF reliability captures how efficient a PUF instance is in reproducing the challenge-response pairs when subjected to



(a)

(b)

Fig. 6: a)Intra-chip Hamming Distances with Temperature variation (-55 to 125°C) b)Intra-chip Hamming Distances with Supply voltage

fluctuating environmental conditions. We analyze this property by measuring the intra-chip hamming distance among several samples of PUF response bits. To estimate the intra-chip Hamming Distance, a $n-bit$ reference response (R_i) is extracted from the chip i at normal operating condition (at room temperature using the normal supply voltage). The same $n-bit$ response is extracted at different operating conditions (different ambient temperature and/or different supply voltage) with a value $R_i^{'}$. Fig. 6 shows the reliability of TV-PUF with variations in temperature (-55 to 125°C) and supply voltage. Similarly, Table-I compares the uniformity and reliability of TV-PUF with the existing PUF designs.

B. Comparison of performance for various Technology Nodes

For the PUF to be robust, it must have promising performances in all technology nodes. Table-II demonstrates that TV-PUF maintains its high performance across different semiconductor technology nodes.

TABLE II: Comparison of PUF characteristics on different technology nodes

Technology Node	$45nm$	$65nm$	$90nm$
Uniqueness	50.02%	50.03%	50.10 %
Uniformity	49.70%	49.84%	49.06 %
Reliability	96%	96%	97%
Bit-aliasing	49.7%	49.84%	49.96 %
Autocorrelation (1,2)	15.3,15.45%	15.48,15.58%	17.31,16.9%

V. Anti-aging Properties

Due to aging of MOSFETs, the key reliability issues are Bias Temperature Instability (BTI) and Hot Carrier Injection (HCI). Use of only NMOS transistors in the PUF design excludse the undesired effects of NBTI. On the other hand, PBTI poses significant concerns only when high-K gate oxide materials are used. Considering applications like device authentication or secure key generation, a PUF circuit in a chip will be enabled for a short period of time, which is being called the *activation time*. Assuming this to be 5% of the total time of operation of the chip, it is evident that the PUF circuit on the chip is generating output key only for 5% of the chip lifetime. To avoid DC stress in the transistors, PUF circuit should be in the $'OFF'$ state for the rest of the time. In previous configurations of RO-PUF, these results are achieved using additional transistors to

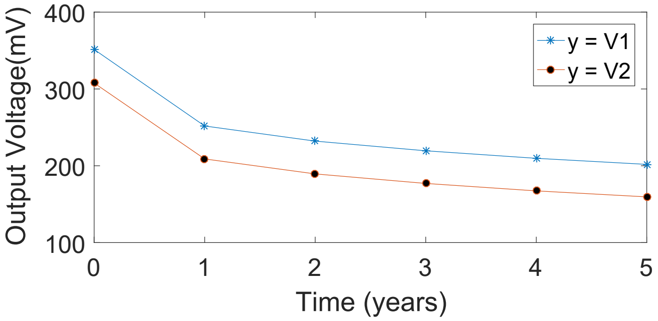


Fig. 7: Output Voltage vs. aging time duration

break the feedback loop of the inverter. But in this design no additional circuitry is needed to mitigate the device aging-effect. Whenever circuit is idle, each bit of the input challenge can be set to 0 V. However, if the PUF circuit is operating for a significant amount of time then HCI can degrade the circuit performance even under normal operating conditions due to switching activity. For better device robustness, one should expect no variation in the output bit for a particular challenge. Suppose for a challenge, initially $V_1 > V_2$. Over the device aging, one should expect that the same relation holds true. This implies that ΔV_{th} of different pass transistors should be independent of V_{th} of the individual transistors. To evaluate the reliability of PUF over device aging, simulations are performed using MOSRA in HSPICE [12] for 45nm, 65nm and 90nm technology nodes accounting HCI effect. These simulation results for 20 different chips show that the impact of HCI is negligible on the reliability of TV-PUF. Although the ΔV_{th} increases approximately by 50% for each pass transistor in a span of 5 years, yet the voltage difference at the output (between V_1 and V_2) changes by only 0.2-0.3 mV. This argument is further supported by the Fig. 7, which shows the relation between the output voltages V_1 and V_2 with time for a particular challenge. It demonstrates that due to the increase in V_{th} with time, the output voltages V_1 and V_2 start decreasing but the relative difference between them remains constant. For these simulations, we excluded the design of the sense amplifier assuming it to be a different design block which can be optimized separately depending on the specifications of power consumption, aging-resistance, sensitivity and input offset voltage.

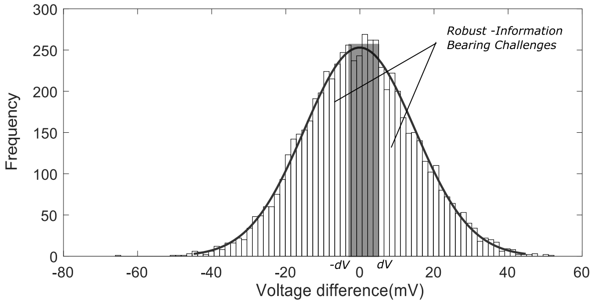


Fig. 8: Voltage difference across PUF output terminals

VI. Comparison of TV-PUF with Sub-threshold PUF, Super-threshold PUF and other existing PUF schemes

Design of low power security application is always encouraged [16]. Previously, the design of a lightweight PUF operating in the sub-threshold region is also proposed [17]. The operation of devices in the sub-threshold or super-threshold region invokes huge delay and consequently it works at a much lower clock frequency. Moreover, the power consumption of TV-PUF is comparable to the previous ones due to less circuit complexity. Hence, TV-PUF can operate at a higher clock frequency while having the same power consumption as the sub-threshold and super-threshold PUFs. Table-III compares the power consumption and clock frequency of TV-PUF with the existing PUF designs.

The major factor affecting both reliability and power consumption of the TV-PUF is the sensitivity of sense amplifier. Fig. 8 denotes a gray zone with a voltage difference $\pm dV$. For difference of output voltages V_1 and V_2 less than dV, output of sense amplifier will be unpredictable. To minimize the gray zone, the sensitivity of the sense amplifier should be very high. This optimized design specification will cause a additional increase in power consumption of TV-PUF.

TABLE III: Comparison with Sub-threshold and Super-threshold PUF (for 1-bit generation)

PUF model	Power	Energy/cycle	No. of Transistors
$Sub\text{-}threshold$	0.047μW @ 1 MHz	0.047 pJ	1672
$Super\text{-}threshold$	136.4μW @ 1 GHz	0.136 pJ	1672
$TV-PUF$	0.181μW @ 1 GHz	1.81×10^{-3} pJ	586
$ICID$	250μW @ 0.5 MHz	500 pJ	NA
$Thermal$	32.3 μW @ 230 MHz	0.14 pJ	NA

VII. Conclusion

The TV-PUF requires voltage comparison. This has certain advantages over delay based PUFs. Delay based PUFs either have a large critical path (Arbiter PUF) or they have to wait for many cycles of operation before producing a response bit (RO-PUF), which makes the effective path quite long. These result in a very low throughput. Unlike these, TV-PUF has a very low critical path delay which makes its bandwidth much higher than the delay based PUFs. It is shown in [18] that a RO-PUF cannot be mimicked therefore it is resistant to modelling attacks. The design of TV-PUF is quite similar to that of a RO-PUF, except the fact that the RO-PUF compares the frequencies of two ring oscillators whereas the TV-PUF compares the cumulative threshold voltages of two cascaded MOSFETs. Hence, TV-PUF is also resistant against modelling attacks. Since TV-PUF has a lightweight circuit, it is easy to fabricate it and the overhead to embed it on a chip is negligible. Furthermore, it consumes very low power and its reliability is independent of the chip aging.

A future direction of research may be to investigate various combinations of the blocks to reduce the exponential hardware requirement of the TV-PUF. The reliability of this design can be further increased by using a control circuit which neglects the input challenges generating an output voltage difference less than a fixed value. This fixed value should depend on the sensitivity of sense amplifier being used.

References

[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," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, no. 10, pp. 1200–1205, 2005.

[3] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, 2002, pp. 148–160.

[4] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of puf-based" unclonable" rfid ics for anti-counterfeiting and security applications," in *2008 IEEE International Conference on RFID*. IEEE, 2008, pp. 58–64.

[5] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "The butterfly puf protecting ip on every fpga," in *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*. IEEE, 2008, pp. 67–70.

[6] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security - Foundations and Practice*, 2010, pp. 3–37. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-14452-3_1

[7] O. U. . W. R. D. . D. T. K. Lofstrom ; SiidTech., Beaverton, "Ic identification circuit using device mismatch," *Solid-State Circuits Conference, 2000. Digest of Technical Papers. ISSCC. 2000 IEEE International , pp. 372 -373 , 2000*, 2000.

[8] T. Rahman, D. Forte, J. Fahrny, and M. Tehranipoor, "Aro-puf: An aging-resistant ring oscillator puf design," in *Proceedings of the Conference on Design, Automation & Test in Europe*, ser. DATE '14. 3001 Leuven, Belgium, Belgium: European Design and Automation Association, 2014, pp. 69:1–69:6. [Online]. Available: http://dl.acm.org/citation.cfm?id=2616606.2616692

[9] A. Maiti, L. McDougall, and P. Schaumont, "The impact of aging on an fpga-based physical unclonable function," in *International Conference on Field Programmable Logic and Applications, FPL 2011, September 5-7, Chania, Crete, Greece*, 2011, pp. 151–156. [Online]. Available: http://dx.doi.org/10.1109/FPL.2011.35

[10] B. N. Jan M. Rabaey, Anantha Chandrakasan, *Digital integrated circuits: a design perspective*. Pearson, 2003.

[11] M. Majzoobi, G. Ghiaasi, F. Koushanfar, and S. R. Nassif, "Ultra-low power current-based PUF," in *International Symposium on Circuits and Systems (ISCAS 2011), May 15-19 2011, Rio de Janeiro, Brazil*, 2011, pp. 2071–2074. [Online]. Available: http://dx.doi.org/10.1109/ISCAS.2011.5938005

[12] "Synopsys, http://www.synopsys.com/."

[13] "Reliability : ptm.asu.edu."

[14] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," *IACR Cryptology ePrint Archive*, vol. 2011, p. 657, 2011. [Online]. Available: http://eprint.iacr.org/2011/657

[15] I. Verbauwhede and R. Maes, "Physically unclonable functions: manufacturing variability as an unclonable device identifier," in *Proceedings of the 21st ACM Great Lakes Symposium on VLSI 2010, Lausanne, Switzerland, May 2-6, 2011*, 2011, pp. 455–460. [Online]. Available: http://doi.acm.org/10.1145/1973009.1973111

[16] N. Sklavos, A. Papakonstantinou, S. Theoharis, and O. Koufopavlou, "Low-power implementation of an encryption/decryption system with asynchronous techniques," *VLSI Design*, vol. 15, no. 1, pp. 455–468, 2002.

[17] L. Lin, D. Holcomb, D. K. Krishnappa, P. Shabadi, and W. Burleson, "Low-power sub-threshold design of secure physical unclonable functions," in *Low-Power Electronics and Design (ISLPED), 2010 ACM/IEEE International Symposium on*. IEEE, 2010, pp. 43–48.

[18] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security - Foundations and Practice*, 2010, pp. 3–37. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-14452-3_1