TV-PUF : A Fast Lightweight Aging-Resistant Threshold Voltage PUF

Tanujay Saha[⋆] and Vikash Sehwag[⋆]

Dept. of Department of Electronics and Electrical Communication Engineering,
Indian Institute of Technology,
Kharagpur, West Bengal, INDIA-721302
tanujay.saha@gmail.com, sehwag.vikash@gmail.com

Abstract. Physical Unclonable Function (PUF) is the hardware analog of a one-way function which can address hardware security issues such as device authentication, generating secret keys, producing seeds for Random Number Generators, etc. Traditional silicon PUFs are based on delay (Ring Oscillator PUFs and Arbiter PUFs) or memory structures (e.g, SRAM PUFs). In this paper, we propose the design of an aging resistant, lightweight and low-power analog PUF that exploits the susceptibility of Threshold Voltage (V_{th}) of MOSFETs to process variations. Analysis shows improvement in power consumption, reliability over device aging along with quality metrics like uniformity, reliability and uniqueness for a 64-bit key generation. For 1 GHz clock input, this design consumes 0.18μW/bit power with 50 % uniqueness and 51% uniformity along with the independence of these metrics on technology nodes. Experimental results suggest 4% variation in reliability under temperature variation from -55°C to 125°C and 20% variation in supply voltage. Aging analysis further projects the independence of reliability over device aging.

Keywords: Hardware security, Physical unclonable function (PUF), Process variation, Aging resistant PUF, Low power embedded systems

1 Introduction

Physical Unclonable Functions (PUFs) are now widely used for generating cryptographic keys. It has the ability to create unique cryptographic keys specific to devices properties which exploit the process variation in device manufacturing [1]. Secure key generation is possible even from biased PUFs [2]. PUFs also find use in error detection methods in Finite State Machines [3]. Nowadays, Physically Unclonable Function (PUF) [4,5] is a major weapon against IC counterfeiting. The hard-coded key in the IC can be replaced with PUF circuits which take challenges as inputs and provides responses as outputs. The challenge to response mapping should strictly be a one-to-one mapping, even under changing environmental conditions like fluctuations in temperature and supply voltage.

[⋆] these authors contributed equally to this work

The responses depend on the process variations of the components involved in the circuit. The security of the PUF is based on the fact that practically any circuit cannot be mimicked exactly due to the process variations present in its components. Hence, it is almost impossible for the adversary to predict the responses. The more random the process variations in the PUF are, more difficult it is for the adversary to clone the PUF. Still adversaries have attacked many PUF designs using Machine Learning prediction techniques like Support Vector Machines [6]. In [7], it is also shown that PUF enabled cryptographic primitives are vulnerable to advanced side channel attacks like Differential Template attacks. PUFs can be broadly classified into two design categories: i). Delay based PUFs (Arbiter PUF, Ring oscillator PUF, Glitch PUF and Schmitt trigger PUF) ii). Memory based PUFs (SRAM-based PUF, butterfly PUF, Latch PUF). A technique for IC identification based on the unique resistance values in its power supply distribution system was introduced in [8]. In [9], irregular current-voltage characteristics of diodes packed in a crossbar memory are exploited to construct a PUF. Some PUFs have tried to capture the randomness in the subthreshold operating region of the FET [10]. New technologies have emerged which uses memristors as the basic building blocks of Arbiter PUFs [11]. Previously, another threshold voltage based PUF called ICID [12] had been proposed. It is shown that our Threshold Voltage PUF (TV-PUF) is more efficient than ICID in terms of both challenge-response performances (security parameters) as well as area and power consumption (VLSI design parameters). Another important aspect in PUF characteristics is its reliability degradation over aging of the device. Previous works in this field [13–15] discuss the effect and mitigation of degradation of PUF reliability due to aging. In semiconductor devices, performance degradation due to the aging of devices is a crucial factor in design consideration as it affects the reliability of device over time. Most of the previous PUF designs employs CMOS technology which incorporates both PMOS and NMOS. In MOSFETs, the key reliability issues are Bias Temperature Instability (BTI) and Hot Carrier Injection(HCI). Negative bias temperature instability (NBTI) is effective in PMOS while Positive-bias temperature instability has an impact in NMOSs. Both the effects causes an increase in Threshold voltage of the transistor (V_{th}) over time. In our model, we have used only NMOS transistors which are supported by the result that NBTI is the major reliability concern as compared to HCI [16]. Use of only NMOSs in PUF design exclude the impact of NBTI on the reliability of PUF as in NMOS, only HCI and PBTI concern the aging issue. However, PBTI only plays a role when high-k gate oxide materials are used [17, 18].

In this paper, we propose a Threshold voltage (V_{th}) based PUF (TV-PUF) which captures the effects of process variations of V_{th}. Threshold voltage has been chosen as the primary basis for the operation of the PUF as it accumulates the process variations in many factors like doping of the n and p regions, gate length, width and oxide thickness. This makes it much more difficult to clone a particular instance of the TV-PUF. TV-PUF takes a n-bit challenge and produces a 1-bit response similar to the Ring Oscillator PUF(RO-PUF). A sense amplifier is used at the end of the circuitry to convert the analog response to a digital response. TV-PUF will find use in various lightweight applications such as device authentication, countering IC counterfeiting, etc. Similar to the operation of a Ring-Oscillator PUF, a unique part of the circuit is employed to operate for a particular challenge. This avoids any dependency between the responses of any two challenges. The rest of the paper is organized as follows. Section 2 briefly discusses the contribution of this design where section 3 focuses on the design and working aspects. In Section 4 we evaluate the performance of TV-PUF based on standard puf metrics. In section 5 we discuss the effecting of device aging on the reliability of TV-PUF. In section 6 we compare our design with previous Puf design in terms of power consumption and number of transistors. Finally, we conclude the paper in section 7 with a discussion of future work in section 8.

2 Our Contributions

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

- TV-PUF requires only three NMOS transistors for the implementation of a block. Additionally, it consists of a decoder and a sense amplifier. Due to lightweight, it can be embedded on any IC chip with minimum circuit overhead.
- TV-PUF can operate at very high frequency due to the less critical path. Such reduction in critical path is caused due to only three NMOS in the critical path which provides a delay in the order of 100ps at 1V supply voltage. Due to very less latency, it can be used in a wide variety of day-to-day devices like smart cards for authentication and security processes.
- Improvement in PUF properties such as uniformity, uniqueness, reliability and bit aliasing have also been observed for TV-PUF. A detailed comparison with the most widely used PUFs, i.e., Ring Oscillator PUF and Arbiter PUF, have been given in the section-4 of this paper. Further, it is also shown that these characteristic are independent on technology node.
- TV-PUF has also employed aging resistant nature. In section-5 we have discussed the effect of aging over a span of 5-years.

3 Design of TV-PUF

The threshold voltage of a MOSFET, being highly susceptible to process variations, is being used as a differentiating factor in the design of TV-PUF. For NMOS pass transistor (fig.1), V_x is initially zeros. As V_x is increased, current-drive of the transistor(V_{gs}) reduces significantly. This reflects in the long tail in V_x as it approaches $V_{dd} - V_{th}$. We use only NMOS pass transistors (fig.1) in the design of TV-PUF. The motivation is to compare source voltages, which is output at the terminal(x) of two independent NMOSs. There will be slightly different due to the difference in the V_{th} of the two FETs caused by process

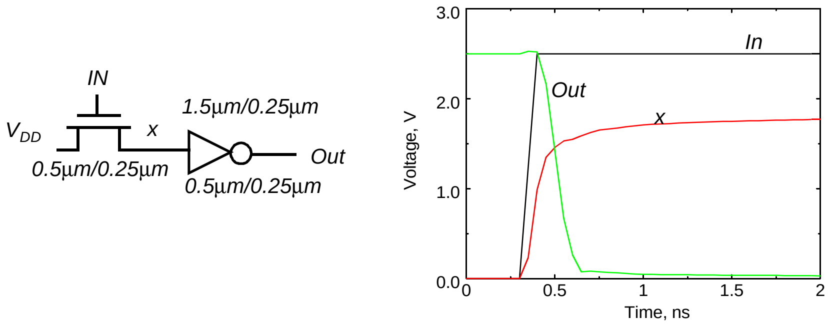

Fig. 1. Nmos Pass transistor and its Voltage transfer characteristic (VTC) [19]

variations.

$$\begin{aligned} Response &= 1, \qquad if \qquad V_{x_0} > V_{x_1} \\ &= 0, \qquad if \qquad V_{x_0} < V_{x_1} \end{aligned}$$

where, x_0 and x_1 represent the source terminal of two different pass transistors.

3.1 Block Diagrams and Working of the design

If PUF response is produced solely on the basis of the differences of V_{th} of a single transistor, the response will be less robust. This is due to less voltage difference which depends on the variance of V_{th} process variations. To increase robustness 'n' NMOS pass transistors can be cascaded creating a multiplying factor such that output voltage is $V_{DD} - nV_{th}$. In this design we are cascading two pass transistors i.e. n = 2 (fig. 2).

Block level design of TV-PUF is projected in fig.3. Input which is a $n - bit$

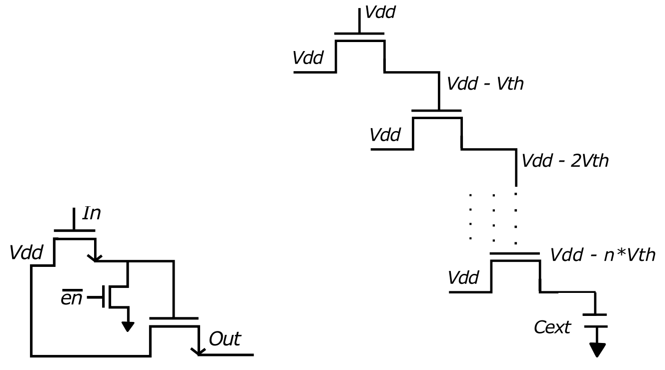

Fig. 2. a) Transistor level design of one block b) Cascading of n pass transistors

challenge passes to the $n - to - 2^n$ line decoder (Active High). This cause one of the output pins to level HIGH (V_{dd}) while all the others are LOW (0V). Each output pin of decoder acts as input to two blocks of puf. These pins are connected to the gate terminals (IN) of the first MOSFET in each block. For a particular challenge, only one of the decoder outputs is HIGH, so only two blocks out of 128 have $V_g = V_{dd}$. Rest of the blocks serves as the high-Z state as they have gate voltage = 0V implies cut-off region. As explained earlier, the output of the blocks with $V_g = V_{dd}$ approaches its limiting voltage $V_{out} = V_{dd} - 2V_{th}$. Due to process variation effects, V_1 and V_2 will be different. These two voltages further act as inputs to the sense amplifier. The response (R) of the PUF is given as:

$$\begin{aligned} R &= 1, \qquad V_1 \geq V_2 \\ &= 0, \qquad V_1 < V_2 \end{aligned}$$

All these operations do not affect the other transistors in the other blocks because they are in High Z condition, which means they are not operational.

All the above operations occur when the *enable (en)* signal is *HIGH*. After

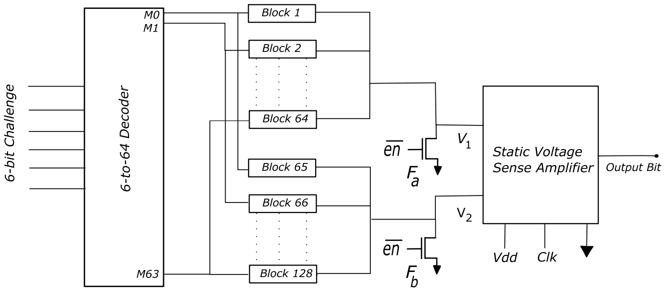

Fig. 3. Block Diagram of proposed TV-PUF with $6 - bit$ challenge

the output is obtained, the *enable* signal changes its state to LOW which activates transistors F_a and F_b thus causes $V_1 = V_2 = 0V$. Transistors F_a and F_b are named as flush transistors. These force the voltages at their drain to become zero, thus re-establishing the initial condition of the TV-PUF. Fig. 4 demonstrates the simulation of output $V_1 = V_2$ when en=low and en=high. The motivation behind using the flush transistor is to increase the reliability of PUF by keeping the system close to ideal because in long run $V_{GS} < V_{th}$ due to sub-threshold conduction. It implies that even when $V_{GS} < V_{th}$ i.e, cut-off region NMOS transistor will conduct following the exponential curve of sub-threshold conduction. To generate a 64-bit key 64 different pair of blocks are implemented. After generating one bit, enable(en) signal is used to reset the output voltages to zero using transistor $F_a and F_b$. As the time required to reset (fig. 4) the voltages $V_1 = V_2 = 0V$ is approx. $35ps$ to $40ps$ for 65nm technology node which is much less than the time of conduction. Thus, the *en* signal need not have 50% duty cycle. In contrast to the ICID [12] and [20] in which current flows through all

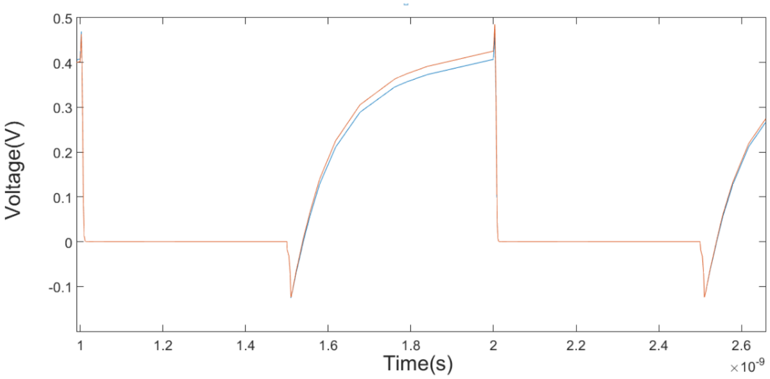

Fig. 4. Transient analysis of two different blocks output

the transistors for generation of every bit. The selective current flow mechanism reduces the power consumption of the TV-PUF in comparison to that of ICID.

4 Performance Evaluation

In this section, we evaluate our PUF by testing it for well-known performance metrics. The results are equivalent to other PUF designs close to the ideal values. The uniqueness of responses, reliability of the PUF with variations in temperature and supply voltage, uniformity, bit-aliasing and correlation values for TV-PUF are reported. We have further evaluated its performance on the basis of its frequency of operation and power consumption. We have also reported the performance metrics of TV-PUF on different silicon technology nodes, namely 45nm, 65nm and 90nm using BSIM level=54 PTM models.

4.1 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. The value of the uniqueness metric should ideally be 50%. It is measured by calculating the inter-die Hamming Distance of the different keys. 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 two chips.

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

It is desired that the response of the PUF is random, hence unpredictable. For ideal PUF response, the number of 1's and 0's should be equal. This metric of

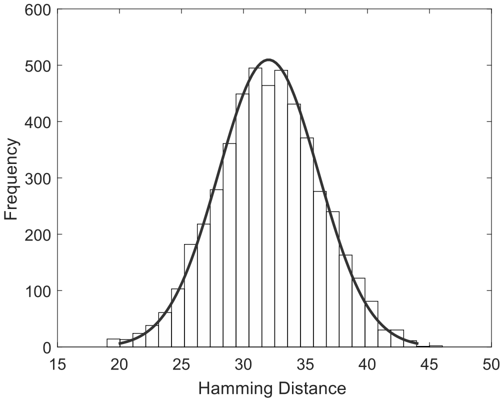

Fig. 5. Inter-chip Hamming Distances (total number of bits = 64)

PUF Construction	$\mu_{inter} \pm \sigma_{inter}$	$\mu_{intra} \pm \sigma_{intra}$
Feed-forward Arbiter PUF	38%	9.8%
Subthreshold 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

Table 1. Comparison of PUF characteristics with different proposed intrinsic PUF construction [21]

the PUF is measured by Uniformity. Similar to the inter-die distance, uniformity follows a normal distribution $N(\mu, \sigma)$ and ideal values of μ and σ are 50% and 0 respectively. If bit-aliasing happens, 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 [22]. Also, neighboring bits must not influence each other. Each bit should be independent otherwise the PUF will be threatened by modelling attacks. In order to check if correlation exists in the test chip, the autocorrelation function is used : PUF reliability captures how efficient a PUF is in reproducing the response bits. We employ intra-chip HD among several samples of PUF response bits to evaluate this metric. To estimate the intra-chip HD, a $n - bit$ reference response (R_i) is extracted from the chip i at normal operating condition (at room temperature using the normal supply

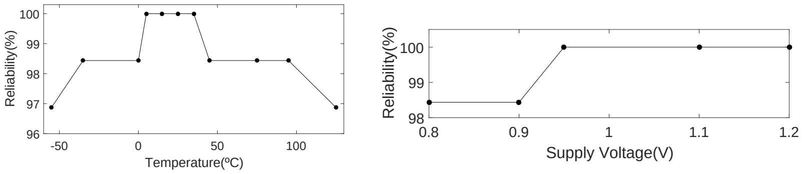

Fig. 6. a)Intra-chip Hamming Distances with Temperature variation (-55 to 125°C) b)Intra-chip Hamming Distances with Supply voltage

voltage). The same n-bit response is extracted at a different operating conditions (different ambient temperature or different supply voltage) with a value $R_i^{'}$. For our experiment table-1 contains results of uniformity and reliability with the comparison of previous designs.

4.2 Comparison of performance for various Technology Nodes

For the PUF design to be robust, it must have promising performances on all platforms and technology nodes. With the exponential growth in semiconductor device modeling, we demonstrate that TV-PUF maintains its high performance across different semiconductor technology nodes in table-2.

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%

Table 2. Comparison of PUF characteristics on different technology nodes

5 Effect of Aging on Reliability

In MOSFETs, the key reliabilty issues are Bias temperature instabilty(BTI) and Hot carrier injection(HCI). In our model we have used only NMOS transistors. Use of only NMOSs in PUF design exclude the NBTI effect in our design. In devices performance NBTI is the major reliability concern as compared to HCI [16]. So this exclude the concern over NBTI. The following analytical model [23] can

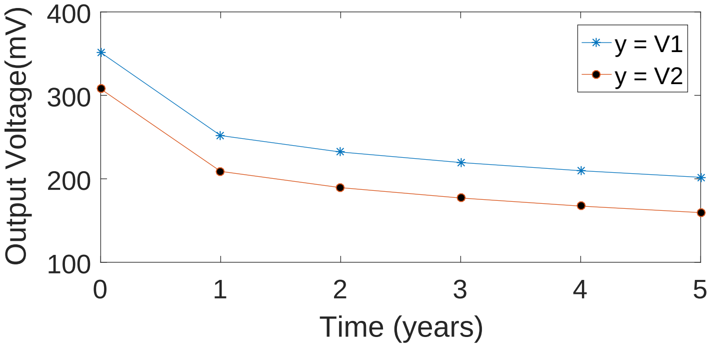

Fig. 7. Output Voltage vs. aging time duration

be used for HCI modeling.

$$\Delta V_{th} = \frac{q}{C_{ox}} K \sqrt{C_{ox}(V_{gs} - V_{th})} exp(\frac{E_{ox}}{E_0}) exp(-\frac{\phi_{it}}{q\lambda E_m}) t^n \tag{1}$$

$$where, E_m = \frac{V_{ds} - V_{dsat}}{l}, \quad V_{dsat} = \frac{(V_{gs} - V_{th} + 2V_t)L_{eff}E_{sat}}{V_{gs} - V_{th} + 2V_t + A_{bulk}L_{eff}E_{sat}}$$

$$E_{ox} = \frac{V_{gs} - V_{th}}{T_{ox}}, \quad C_{ox} = \frac{\varepsilon_o x}{T_{ox}}, \quad V_t = \frac{kT}{q}$$

For better device robustness, one should expect no variation in 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 will hold. It implies that ΔV_{th} of different pass transistors should be independent of V_{th}. This argument is supported by the fig.7, which shows relation output voltage V_1 and V_2 for a particular challenge vs. time for one challenge. Fig.7 shows the independent of ΔV_{th} over initial process variation in V_{th} which is also reflect by equation 1 if $V_{gs} \approx V_{th}$. These analyses are performed using MOSRA [24] for 45nm, 65nm and 90nm technology nodes accounting HCI effect. Simulation results for 10 different chips shows that impact of HCI is negligible on reliability. Although the ΔV_{th} increases approx. 50% for each pass transistors in span of 5 years, voltage difference at output($V_1 and V_2$) hardly changes only by 0.2-0.3mV. This argument is also supported by fig.7 as it shows that due to increase in V_{th} over time, output voltages V_1 and V_2 start decreasing but the relative difference remain constant. Major hurdle in reliability concern is the sensitivity of sense amplifier. Fig.8 project the gray zone with a voltage difference in ±dV. dV will further depend on the sensitivity of sense amplifier. Voltage difference lower this level demand a design of sense amplifier with better sensitivity which again cause increase in power consumption.

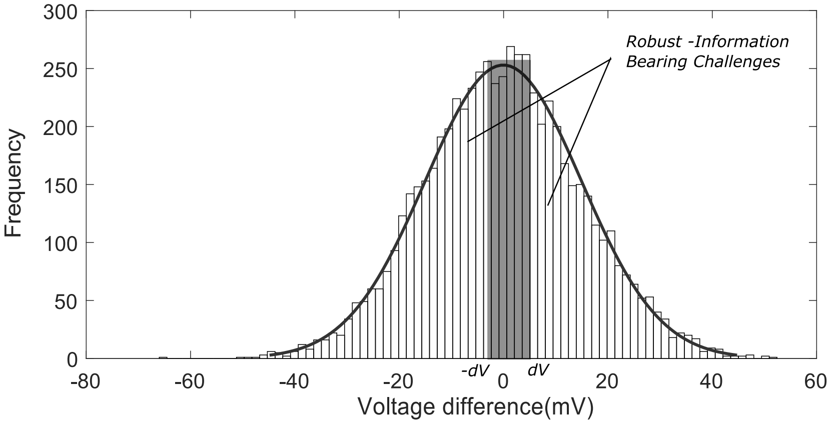

Fig. 8. Voltage difference across PUF output terminals

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

The clock frequency of the sense amplifier in this design will be affected by the delay in measuring two responses. As fig.4 demonstrates, after measuring one responses we change input of decoder and flush the output terminal of PUF using *en* signal. For next decoder input, different blocks will get selected which further result in a different output(0,1) from amplifier output terminal. The voltage difference between $V_1 and V_2$ increases with time and approaches the limiting value caused by threshold voltage mismatch. Hence the input can be sampled any time in the rising period of voltage at $V_1 and V_2$ depending on the desired voltage difference. In previous works [10], the design of a lightweight PUFs operating in the subthreshold region is proposed.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. Also, the power consumption of proposed design is comparable to previous ones due to less circuit complexity. The following table compares power consumption and clock frequency of proposed design with previous works. However stated power consumption and no. of transistors of our design doesn't include decoder and sense amplifier designs.

	$Sub - threshold$	$Super - threshold$	$TV - PUF$	$ICID$	Thermal [25]
Power	0.047μW @ 1 MHz	136.4μW @ 1 GHz	0.181μW @ 1 GHz	250μW @ 0.5 MHz	32.3 μW @ 230 MHz
Energy/cycle	0.047 pJ	0.136 pJ	1.81×10^{-3} pJ	500 pJ	0.14 pJ
No. of Transistors	1672	1672	586	NA	NA

Table 3. Comparison with Sub-threshold and Super-threshold PUF(for 1-bit generation)

7 Conclusion

The TV-PUF requires voltage comparison. This has certain advantages over delay based PUFs. In delay-based PUFs, the delay has to be substantial for the delays between the two blocks/paths to be detectable by the sensor (for both RO-PUF and Arbiter PUF). On one side arbiter, PUF suffers from the requirement of the symmetric path in the circuit and hold time of arbiter. Similarly, at the inverters in Ring Oscillator PUFs, PMOS is used which is susceptible to NBTI which causes degradation in reliability with time. Delay PUFs have a large path (e.g., Arbiter PUF) or it has to wait for many cycles of operation before producing the response (for RO-PUF) which makes the effective path quite long for RO-PUFs. This causes the time of operation to be huge and throughput is very low. TV-PUF, on the other hand, has a very low critical path delay which makes its clock frequency much larger than the delay based PUFs. The design of TV-PUF is quite similar to that of a Ring Oscillator PUF (RO-PUF), except the fact that the Ring Oscillator PUF compares the frequencies of two blocks whereas the TV-PUF compares the cumulative threshold voltages of two cascaded MOSFETs in a block. It is shown that the RO-PUF is impossible to be modeled [26] and is safe from modeling attacks.

Similar to the RO-PUF, the TV-PUF also requires an exponential number of blocks, that is, for a n-bit challenge the number of blocks required is 2^n. If it is required to generate more responses from the TV-PUF to strengthen the security of a system, it becomes an obstacle. Increasing the number of challenge bits by one doubles the hardware requirement of the TV-PUF. This causes a disruption in the environment it is placed in. A future direction of research may be to investigate various combinations of the blocks to reduce the exponential dependency of hardware requirement on the size of the response.

8 Future Work

A significant improvement will be to reduce the exponential hardware requirement of the TV-PUF. As its key generation mechanism correlate with RO-PUF, those techniques can be employed in this design. Reliability of this design can be further increased by using a control circuit which neglects the inputs challenges which generate output voltage difference less than a specified threshold depending on the sensitivity of sense amplifier. Attempts can be made to bring about a better optimization between the sensitivity of the sense amplifier and reliability.

References

1. 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

2. R. Maes, V. van der Leest, E. van der Sluis, and F. Willems, "Secure key generation from biased pufs," in *Cryptographic Hardware and Embedded Systems - CHES 2015 - 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings*, 2015, pp. 517–534. [Online]. Available: http://dx.doi.org/10.1007/978-3-662-48324-4_26
3. G. Hammouri, K. D. Akdemir, and B. Sunar, "Novel puf-based error detection methods in finite state machines," in *Information Security and Cryptology - ICISC 2008, 11th International Conference, Seoul, Korea, December 3-5, 2008, Revised Selected Papers*, 2008, pp. 235–252. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-00730-9_15
4. D. E. Holcomb and K. Fu, "Bitline PUF: building native challenge-response PUF capability into any SRAM," in *Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings*, 2014, pp. 510–526. [Online]. Available: http://dx.doi.org/10.1007/978-3-662-44709-3_28
5. C. W. Lin and S. Ghosh, "A family of schmitt-trigger-based arbiter-pufs and selective challenge-pruning for robustness and quality," in *IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2015, Washington, DC, USA, 5-7 May, 2015.* IEEE, 2015, pp. 32–37. [Online]. Available: http://dx.doi.org/10.1109/HST.2015.7140232
6. 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, CCS 2010, Chicago, Illinois, USA, October 4-8, 2010*, 2010, pp. 237–249. [Online]. Available: http://doi.acm.org/10.1145/1866307.1866335
7. D. Karakoyunlu and B. Sunar, "Differential template attacks on PUF enabled cryptographic devices," in *2010 IEEE International Workshop on Information Forensics and Security, WIFS 2010, Seattle, WA, USA, December 12-15, 2010*, 2010, pp. 1–6. [Online]. Available: http://dx.doi.org/10.1109/WIFS.2010.5711445
8. R. Helinski, D. Acharyya, and J. Plusquellic, "A physical unclonable function defined using power distribution system equivalent resistance variations," in *Proceedings of the 46th Design Automation Conference, DAC 2009, San Francisco, CA, USA, July 26-31, 2009*, 2009, pp. 676–681. [Online]. Available: http://doi.acm.org/10.1145/1629911.1630089
9. U. Rührmair, C. Jaeger, C. Hilgers, M. Algasinger, G. Csaba, and M. Stutzmann, "Security applications of diodes with unique current-voltage characteristics," in *Financial Cryptography and Data Security, 14th International Conference, FC 2010, Tenerife, Canary Islands, January 25-28, 2010, Revised Selected Papers*, 2010, pp. 328–335. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-14577-3_26
10. L. Lin, D. E. Holcomb, D. K. Krishnappa, P. Shabadi, and W. Burleson, "Low-power sub-threshold design of secure physical unclonable functions," in *Proceedings of the 2010 International Symposium on Low Power Electronics and Design, 2010, Austin, Texas, USA, August 18-20, 2010*, V. G. Oklobdzija, B. Pangle, N. Chang, N. R. Shanbhag, and C. H. Kim, Eds. ACM, 2010, pp. 43–48. [Online]. Available: http://doi.acm.org/10.1145/1840845.1840855
11. U. Chatterjee, R. S. Chakraborty, J. Mathew, and D. K. Pradhan, "Memristor based arbiter PUF: cryptanalysis threat and its mitigation," in *29th International Conference on VLSI Design and 15th International Conference on Embedded*

Systems, VLSID 2016, Kolkata, India, January 4-8, 2016, 2016, pp. 535–540. [Online]. Available: http://dx.doi.org/10.1109/VLSID.2016.57

12. 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.
13. A. Maiti and P. Schaumont, "The impact of aging on a physical unclonable function," *IEEE Trans. VLSI Syst.*, vol. 22, no. 9, pp. 1854–1864, 2014. [Online]. Available: http://dx.doi.org/10.1109/TVLSI.2013.2279875
14. M. T. Rahman, D. Forte, J. Fahrny, and M. Tehranipoor, "ARO-PUF: an aging-resistant ring oscillator PUF design," in *Design, Automation & Test in Europe Conference & Exhibition, DATE 2014, Dresden, Germany, March 24-28, 2014*, 2014, pp. 1–6. [Online]. Available: http://dx.doi.org/10.7873/DATE.2014.082
15. 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
16. W. Wang, V. Reddy, A. T. Krishnan, R. Vattikonda, S. Krishnan, and Y. Cao, "Compact modeling and simulation of circuit reliability for 65-nm cmos technology," *Device and Materials Reliability, IEEE Transactions on*, vol. 7, no. 4, pp. 509–517, 2007.
17. J. Zhang and W. Eccleston, "Positive bias temperature instability in mosfets," *Electron Devices, IEEE Transactions on*, vol. 45, no. 1, pp. 116–124, 1998.
18. R. Shangqing, T. Bo, X. Hao, L. Weichun, T. Zhaoyun, X. Yefeng, X. Jing, W. Dahai, L. Junfeng, Y. Jiang *et al.*, "Characterization of positive bias temperature instability of nmosfet with high-k/metal gate last process," *Journal of Semiconductors*, vol. 36, no. 1, p. 014007, 2015.
19. B. N. Jan M. Rabaey, Anantha Chandrakasan, *Digital integrated circuits: a design perspective.* Pearson, 2003.
20. 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
21. 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
22. 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
23. "Reliabilty : ptm.asu.edu."
24. "Synopsys, http://www.synopsys.com/."
25. Y. Cao, L. Zhang, C.-H. Chang, and S. Chen, "A low-power hybrid ro puf with improved thermal stability for lightweight applications," *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, vol. 34, no. 7, pp. 1143–1147, 2015.
26. 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.* Springer Berlin Heidelberg, 2010, pp. 3–37.