TV-PUF : A Fast Lightweight Analog Physically Unclonable Function

Tanujay Saha
tanujay.saha@gmail.com

Abstract

Physical Unclonable Function (PUF) is 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 (like SRAM). In this paper, we propose a novel idea of a very fast, lightweight and robust analog PUF that exploits the susceptibility of Threshold Voltage (V_{th}) of MOSFETs to process variations. We call this the Threshold Voltage PUF (TV-PUF). Extensive implementations and simulations shows improvement in quality metrics like uniformity of the PUF, intra-die distances (reliability metric of the PUF) and inter-die distances (uniqueness metric of the PUF) for 64-bit key generation. For 1 GHz clock input for sense amplifier, our design consumes 0.18μW/bit power with 50 % uniqueness and 51% reliability. It is also shown that TV-PUF characteristics are independent on the technology node.

Keywords: VLSI , Analog PUF , Threshold Voltage

1 Introduction

Integrated Circuit (IC) counterfeiting involves duplicating the original circuit by mimicking the design and fabricating the chip so that the security of the authentic chip is breached and access to all the secret information is obtained. PUF is now widely used for generating cryptographic keys as mentioned in [1]. Secure key generation is possible even from biased PUFs as demonstrated in [Maes, secure key gen frm biased]. PUFs also find use in error detection methods in Finite State Machines [2]. Nowadays, Physically Unclonable Function (PUF) [1, 3] is a major weapon against counterfeiting. The hard-coded key in the IC is replaced with 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. 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 is, 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 [still needed citation]. In [4], it is shown that PUF enabled cryptographic primitives are vulnerable to advanced side channel attacks like Differential Template attacks.

Broadly classifying, there are two types of PUFs: i. Delay based PUFs (e.g., Arbiter PUF, Ring oscillator PUF, Glitch PUF and Schmitt trigger PUF) ii. Memory based PUFs (e.g.,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 [5]. In [6], 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 sub-threshold operating region of the FET[]. New technologies have emerged which uses memristors as the basic building blocks of Arbiter PUFs [7].Previously, another threshold voltage based PUF had been proposed which was called ICID [8]. It is shown that our Threshold Voltage PUF(TV-PUF) is more efficient than ICID in terms of both challenge-response performance (security parameters) as well as area and power consumption (VLSI design parameters).There have also been various attempts to improve the reliability and ageing of the PUF.

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 its process variations are quite large due to its dependencies on many factors like doping of the n and p regions, capacitances of the different regions of the FET, work function, etc []. Moreover, its dependency on the doping of the channel is highly non-linear. This makes it much more difficult to clone a particular instance of the TV-PUF. Dependency of threshold voltage on doping of the channel is described in detail in the following sections. The design of our TV-PUF is in 45 nm technology.

TV-PUF is an analog circuit at its core. A sense amplifier is used at the end of the circuitry to convert the analog response to a digital response. TV-PUF takes a n-bit challenge and produces a 1 bit response. This is not a delay based PUF. Hence, it cannot be attacked by machine learning techniques. 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.

2 Our Contributions

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

- TV-PUF uses analog circuitry at its core. It requires three/four NMOS transistors for the implementation of a block of the PUF,one decoder and a sense amplifier. Hence, it is lightweight and can be embedded on any IC chip with minimum overhead.

- Tvpuf can operate at very high frequency due to less critical path. Such a reduction in critical path is causes due to only three NMOS in critical path which provide delay in 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.

- TV-PUF is resistant against machine learning attacks. This is because for every challenge, a unique part of the circuit is used while the rest of it does not affect the response. So, the response for every challenge is independent of each other. - As all the units have MOSFETs as their basic elements, TV-PUF might not require any extra overhead at all. With clever connections, the existing MOSFETs of the circuit can be used to implement the TV-PUF on a chip.

- A marked improvement in the 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 following section **??** of this paper. Furthur it is also shown that these characteristic are independent on technology node.

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.

In saturation mode of operation, the drain current I_D is given by

$$I_D = \frac{\mu_n C_{ox} W}{2L} (V_{GS} - V_{th})^2 \tag{1}$$

In the steady state, the capacitor behaves as an insulator. Hence, the current

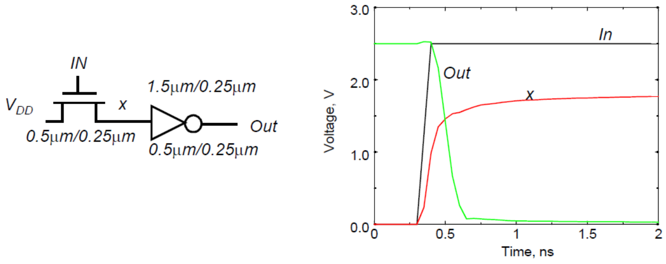

Figure 1: Pass transistor and its Voltage transfer characteristic (VTC) [?]

(I_D) flowing through the NMOS is zero.

$$\begin{aligned} I_D &= 0 \\ \frac{\mu_n C_{ox} W}{2L}(V_{GS} - V_{th})^2 &= 0 \\ V_G - V_S - V_{th} &= 0 \\ V_S = V_G - V_{th} \end{aligned}$$

We use pass transistor (fig. 1) in the design of TV-PUF. Here, the output is taken from the source of the transistor.The characteristics of a pass transistor are also shown in figure 1.

The source voltages of two independent NMOS are compared. They will be slightly different due to the difference in the V_{th} of the two FETs caused by process variations.

$$\begin{aligned} Response &= 1, \qquad if \qquad V_{S0} > V_{S1} \\ &= 0, \qquad if \qquad V_{S0} < V_{S1} \end{aligned}$$

3.1 Elementary circuit used as Block of PUF

If the PUF response is produced solely on the basis of the difference of $V_t h$ of a single transistor, the response will not be robust at all. Since the voltage difference will be very low, it will be highly susceptible to environmental noises like fluctuations in temperature and supply voltage. Moreover, to detect such small differences between voltages, a highly sensitive sense amplifier is required which is very costly and prone to environmental errors. So, a series of MOSFETs are connected in series so that the randomness is increased and the PUF is more reliable. More the number of MOSFETs, the more reliable the PUF is.

TV-PUF consists of only two MOSFETs in cascade, i.e. n = 2.(fig. **??**)
Given V_{th} follows a Gaussian distribution with mean(μ) = 0.18V and Variance(σ)=10mV

3.2 Working of the design

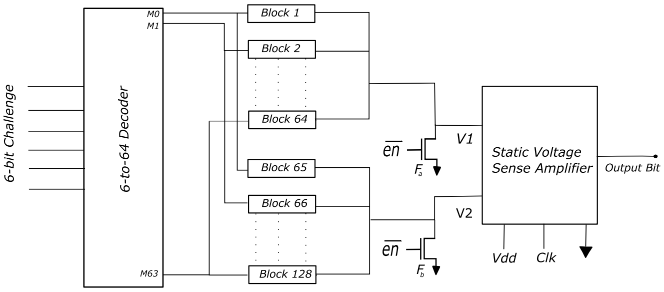

Figure 2: Block Diagram of proposed TV-PUF with 6*bit* challenge

The $n-bit$ challenge goes to the decoder as input. This is a digital $n-to-2^n$ decoder. One of the output pins is HIGH while all the others are LOW. The decoder outputs are connected to the gate terminals of the first MOSFET in each block. For a particular challenge, only one of the decoder outputs is HIGH, so only one of the MOSFETs are switched ON. Rest of the MOSFETs serve as high Z (behaviorally similar to infinite impedance) as they are in cut-off region. As explained earlier, the output of the block becomes $V_{out1} = V_{dd} - 2V_{th}$. The similar phenomenon occurs in the lower set of blocks. Its output is $V_{out2} = V_{dd} - 2V_{th}$. Due to process variation effects, V_{out1} and V_{out2} are not same. These two voltages are sent as inputs to the sense amplifier. The response (R) of the PUF is given as:

$$\begin{aligned} R &= 1, \qquad V_{out1} \geq V_{out2} \\ &= 0, \qquad V_{out1} < V_{out2} \end{aligned}$$

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* signal is $HIGH$. After the output is obtained, the *enable* signal becomes LOW. Then all the output pins of the decoder becomeLOW and the transistors F1 and F2 are activated. These force the voltages at their drain to become zero, thus re-establishing the initial condition of the TV-PUF. Its use is described in detail in the following subsection.

In TV-PUF current flows only through two blocks while generating a single bit of Response. This is in contrast to the ICID [] in which current flows through all the transistors for generation of every bit of the ID. This selective current flow mechanism drastically reduces the power consumption of the TV-PUF in comparison to that of ICID.

3.3 Flushing transistors

The transistor $F1$ in each block and the two transistors F_a and F_b are being called flushing transistors. These flushing transistors flush the voltage at that particular node to zero when the enable pin is LOW. Hence, it causes the reset of the TV-PUF. When $en = LOW$, the transmission gate is OFF, i.e., it is in High Z(high impedance) state. But the voltage at the output of the transmission gate (same node as input to sense amplifier) remains at its previous value V_{out1}. In the next cycle, when another pair of blocks are selected, then the voltage at the input of the sense amplifier is brought to V_{out2}. This causes the same node to have two different voltages. A lot of heat is generated and consequently the circuit burns down.

To tackle this obstacle, we use the flushing transistors to bring down the voltage at the inputs of the sense amplifier to zero before each cycle of operation. When the *enable* signal is LOW, the transistor $M1$ gets switched OFF as all the decoder output bits are *zero*. The flush transistor $F1$ is switched ON which drives the potential at the gate of $M2$ to *zero*. $F2$ is also switched on at the same moment and it drives the potential at the drain of $M2$ to $zero$. Hence, the TV-PUF returns to its initial conditions before the generation of the next response bit.

3.4 Implementation details and modelling noise

The V_{th} in 65 nm NMOS has a Gaussian distribution with mean = 0.18 V and standard deviation = 10mV.

$$\sigma_{NOISE} = \sqrt{\frac{k_B T}{C}}$$

The environmental noise is modelled using the above formula[holocomb ches14] The analog voltage output of every block is shown for a few clock cycles in the next figure:

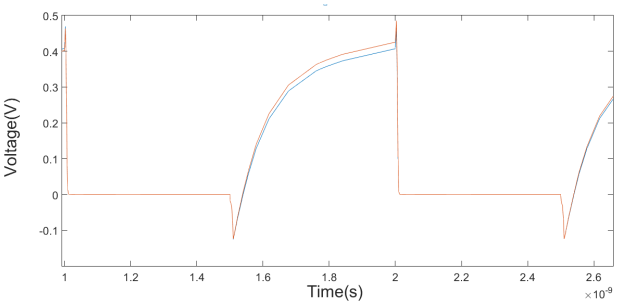

Figure 3: Transient analysis of two different blocks output

It is seen that clock is not of equal duty cycle. This is because the time required to reset the TV-PUF is much less than the time of operation.
Time required for reset = $35ps$ to $40ps$
Output of block is measured when the voltage rises to 50% of its saturation value.

The output of the elementary block varies from 1mV to 30mV with a mean value of 11mV. A Static voltage sense amplifier which operates effectively in these voltage range is selected. This prevents the operation of the TV-PUF in the metastable state. In the metastable state, the sense amplifier input will be very near to the operating voltage boundary of the device. A little fluctuation will result in the change of the output and the output will no longer remain a function of the process variations. A dynamic sense amplifier is recommended as it is effectively in this scenario. A dynamic sense amplifier uses the sample and hold technique for the interpolating process during its operation.

After resetting the PUF, the output voltage of the block requires sometime to rise to its saturation voltage. However, it is not necessary to sample the output voltage only after it has reached its saturation value. This is because we are not considering the absolute output voltage of the block. We require the difference between the output voltages of two blocks, i.e., the relative voltages between them will suffice. It has been experimentally observed that,

$$\begin{array}{rrcll} \texttt{If} & V_{out1} & = & (V_{out1})_{sat} & \texttt{at t = } T_{sat1} \\ & V_{out2} & = & (V_{out2})_{sat} & \texttt{at t = } T_{sat2} \\ and & (V_{out1})_{sat} & > & (V_{out2})_{sat} & \\ Then & (V_{out1})_{t=t_i} & > & (V_{out2})_{t=t_i} & \forall \quad t_i > 0 \end{array}$$

Fig.9 So, we can sample the voltages as soon as their difference is above the minimum voltage difference required for the dynamic sense amplifier. Since this decreases our sampling time, it decreases our overall delay. Consequently, it decreases the latency of the circuit and increases its throughput. So TV-PUF can now operate at much higher frequencies.

4 Performance Evaluation

The details mentioned in the previous sections are used to implement the PUF. In this section, we evaluate our PUF by testing it for well-known performance metrics. The results are very close to the ideal values which make TV-PUF a promising PUF for the future.

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 practical performance on the basis of its frequency of operation and power consumption. Proceeding a step further, we have reported the performance metrics of TV-PUF on different silicon technology nodes, namely 45nm, 65nm and 90nm technology nodes.

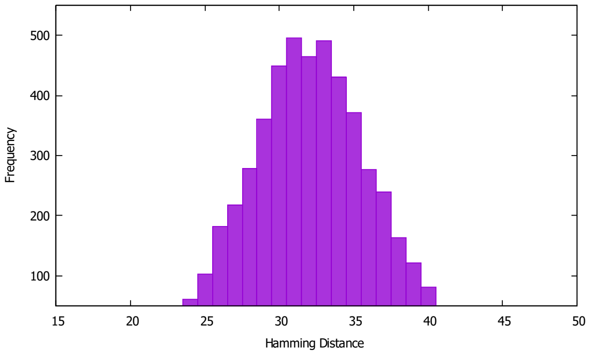

Figure 4: Inter-chip Hamming Distances (total number of bits = 64)

PUF Construction	$\mu_{inter} \pm \sigma_{inter}$	$\mu_{intra} \pm \sigma_{intra}$
Feed-forward Arbiter PUF	38%	9.8%
Subthreshold Arbiter PUF	$\approx$ 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	$\approx$50%	<6%
Proposed TV-PUF	$\approx$51%	<4%

* the results encompass environmental fluctuations

Table 1: Comparison of PUF characteristics on different proposed intrinsic PUF construction [9]

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%. The uniqueness is measured by calculating the inter-die Hamming Distance of the PUF. The inter-die Hamming Distance follows a Normal distribution $N(\mu, \sigma)$. The ideal values of μ and σ are 50% and 0 respectively.

It is desired that the response of the PUF is random, hence unpredictable. On an average the number of ones and zeroes should be equal for the PUF responses. This metric of 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 [**?**].

Also, neighbouring 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 :

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

4.2 Reliability of TV-PUF

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

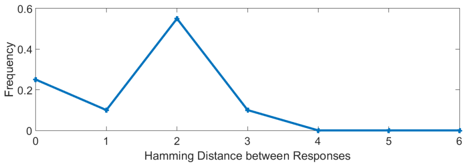

Figure 5: a)Intra-chip Hamming Distances with Temperature variation (-55 to 125 C)

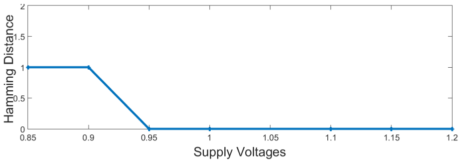

Figure 6: Intra-chip Hamming Distances with Supply voltage

Technology Node	$45nm$	$65nm$	$90nm$
Uniqueness	50.02%	50.03%	50.10 %
Uniformity	49.70%	49.84%	49.06 %
Reliability	6%	5%	4 %
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 proposed intrinsic PUF construction [9]

to evaluate this metric. To estimate the intra-chip HD, we extract a $n - bit$ reference response (R_i) from the chip i at normal operating condition (at room temperature using the normal supply voltage). The same n-bit response is extracted at a different operating conditions (different ambient temperature or different supply voltage) with a value $R_i^{'}$

4.3 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 modelling, we demonstrate that TV-PUF maintains its high performance across various semiconductor technology nodes in Table 2.

5 Detailed comparison with existing Threshold voltage based PUF

An existing implementation of threshold voltage based PUF is ICID [8].TV-PUF proves to be more advantageous than ICID in certain conditions. The ICID compares the threshold voltages of two MOSFETs for generating each bit of the ID as shown in the fig. 7. These two voltages differ by a very small amplitude. Such minute voltage differences might not be detected by the comparator because the comparator has process variations defects of its own. Practically, the comparator works correctly only if the difference between the two inputs is higher than a certain value. To reduce this practical implementation problem, TV-PUF employs two transistors in a single block. The outputs of any two blocks differ by a much larger amount since the randomness of the outputs is four times larger than that of ICID. The probability of getting a very low difference between the outputs of two blocks of TV-PUF is practically negligible. This makes the practical performance of TV-PUF much better than that of ICID.

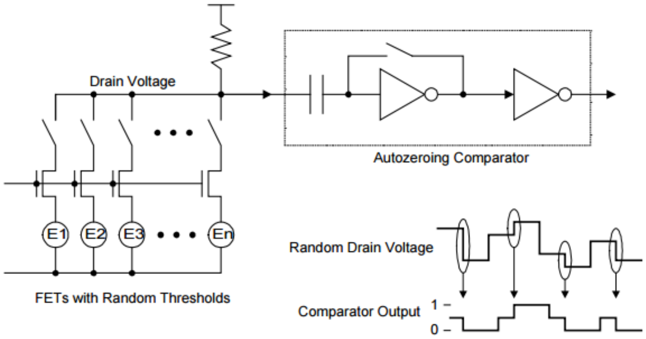

Figure 7: The working circuit of ICID []

-ICID is only used to generate a n-bit ID for a particular chip. TV-PUF is the first challenge response pair generating threshold voltage based PUF. Hence TV-PUF can be used for many processes other than just IC authentication, for example, secret key generation and pseudo random number generation. This makes TV-PUF a general purpose PUF. In ICID, all the transistors conduct current throughout the generation of all the n bits. This causes a steep increase in the static power consumption. It also causes ageing of the NMOS transistors used in the chip. To overcome this drawback, TV-PUF is designed in such a way that only two blocks are conducting current for the generation of a single bit response. This reduces both the static power consumption as well as the ageing effect. *Note: The power consumption analysis given above considers the similar operations of TV-PUF and ICID. If TV-PUF was to generate only IDs* *like ICID, the combinational decoder circuitry for decodeing the inputs would not be required. Consequently, power consumption would have diminished. For TV-PUF to operate like ICID, a random seed is fed to it as the only input while fabrication and the decoder circuit will be absent.*

-TV-PUF is claimed to be much more reliable than ICID. This is also due to the fact that ICID employs only a single NMOS transistor in a block. So, the outputs of the blocks differ minutely and will easily fluctuate with environmental noises like temperature and supply voltage fluctuations. In TV-PUF, since two transistors are used in a single block the outputs of the blocks differ by a much larger amount than that of ICID. Environmental noises will definitely change the outputs of the individual blocks but the change will not be enough to change the PUF response as the difference between the block outputs is much larger than that of ICID. This makes the TV-PUF much more reliable and robust than the ICID. The high reliability is demonstrated in the results in the previous section. ICID employs resistors in its circuit. Resistors are passive elements which consume a lot of area. This has been replaced with active loads in TV-PUF which require much less area than resistors. The decoder circuit would not be required for only ID generation of ICs, thus reducing the area overhead of TV-PUF. Hence, TV-PUF requires less area to only perform the same task as ICID.

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

In [**?**], lightweight PUFs operating in subthreshold region are demonstrated. We compare our TV-PUF to the sub-threshold and super-threshold PUFs. Here, we demonstrate that while our TV-PUF's power consumption is comparable to the afforementioned PUFs but it operates at a much higher clock frequency than those. The operation of devices in the subthreshold region invokes huge delay and consequently, it works at a much lower clock frequency. Thus, combining the above two factors, TV-PUF seems to produce a better performance.

	$Sub-threshold$	$Super-threshold$	$TV-PUF$
Power	0.047μW @ 1 MHz	136.4μW @ 1 GHz	0.181μW @ 1 GHz
Energy/cycle	0.047 pJ	0.136 pJ	1.81×10^{-3} pJ
No. of Transistors	1672	1672	586

Table 3: Comparison with Subthreshold and Super-threshold PUF(for 1 bit generation

7 Advantages of TV-PUF over existing PUF schemes

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 suffer from the requirement of symmetric path in circuit and hold time of arbiter. Similarly, at the inverters in Ring Oscillator PUFs, PMOS is used which is susceptible to NBTI which cause degradation in reliability with time[citation]. Delay PUFs have a large path (in case of 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 time of operation which makes its throughput much larger than the delay based PUFs. Due to the high throughput of the TV-PUF, it can operate at very high frequencies in comparison to most existing PUFs. The frequency of operation of TV-PUF is in the range of 1GHz.

The TV-PUF has an operation 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 modelled [Physically Unclonable Functions: a Study on the State of the Art and Future Research Directions by Roel Maes, Ingrid Verbauwhede] and is safe from modelling attacks.

Similar to the RO-PUF, the TV-PUF also requires exponential number of blocks, that is, for a n-bit challenge the number of blocks required is 2^n. According to Moores Law, the overall processing power doubles every two years. So, 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

TV-PUF is a new PUF and a lot of research can be devoted to improving it. A significant improvement will be to reduce the exponential hardware requirement of the TV-PUF. Many other combinations of comparing the block outputs can be tried and a provable security would be very much desirable. Thus, an important requirement is the extraction of maximum entropy from the TV-PUF. The power consumption may be reduced by some device engineering like operation in the subthreshold region of the MOSFET. This is an interesting direction of research. Attempts can be made to bring about a better optimization between the sensitivity of the sense amplifier and the number of MOSFETs required in cascade to prevent the shift of the TV-PUF into the metastable mode of operation. Methods more efficient than Hot Carrier Injection can be employed to increase the reliability of TV-PUF.

9 Conclusion

We proposed a new design of PUF in this paper. TV-PUF ventures into designing a PUF in the analog domain. It is the first challenge-response generating PUF employing the Hot Carrier Injection scheme to increase reliability. Better performance measures have been shown for the TV-PUF. Uniformity, intra-die and inter-die hamming distances are very near to the ideal values. Moreover, this PUF has a very high throughput which makes it a very fast PUF and it can operate even at much higher frequencies. Extensive simulations and detailed comparisons show that the many advantages of TV-PUF over the existing schemes dominate over a few disadvantages. These disadvantages can be eliminated with deeper study of this PUF. Concluding, the TV-PUF opens new dimensions in the area of PUF design.

References

[1] 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

[2] 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

[3] 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

[4] 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

[5] 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

[6] 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

[7] 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

[8] 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.

[9] 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