A Capacitive-Loaded Weak PUF Insensitive to Thermal Noise and Voltage/Temperature Changes

Griffin Prechter
EECS Department
University of California, Berkeley
griffinprechter@berkeley.edu

Antroy Roy Chowdhury
EECS Department
University of California, Berkeley
antroy@berkeley.edu

***Abstract*—PUFs are low-cost hardware primitives that exploit process variations for use in security applications like key generation and user authentication. PUF cells can be implemented drawing entropy from meta-stability resolution, delay variation, mismatch in threshold voltages, etc. For key generation applications, stability of a PUFs response is an essential characteristic. To achieve a 100% stable PUF response several techniques have been proposed including temporal-majority voting, dark-bit masking etc., but none of them can achieve a 100% stable PUF response and rely on power and area consuming error-correction mechanisms. This work addresses this issue by reinforcing the existing PUF bias through capacitive loading giving a PUF response which is 100% stable towards noise and voltage/temperature fluctuations. For demonstrating the effectiveness of our capacitive-loaded PUF (CL-PUF), and other state-of-the-art PUFs, arrays of 128 PUF cells have been simulated in GPDK 45nm technology and evaluated. The core PUF cell consumes $7.53\mu W/bit$ from a $1V$ supply with an estimated area of $0.43\mu m^2/bit$.**

***Index Terms*—physically unclonable function, key generation, BER, stability, intra and inter PUF variation**

I. Introduction

The incorporation of reliable and robust security features in electronic devices has seen growing demand for applications ranging from banking infrastructure to critical communication links. Specifically, the IoT devices that are plentiful in many households and institutions often strive for low power consumption and handle sensitive information. Physically Unclonable Functions (PUFs) are popular low-cost hardware primitives largely utilized for hardware-security applications. The operations that PUFs are capable of performing have historically required larger, more power-hungry, crypto processors and many clock cycles. PUFs are not only enticing from an efficiency standpoint, they also come with innate security advantages. PUFs leverage the manufacturing variation of integrated circuits to produce an unpredictable, yet consistent, signature (or "finger print"). This signature forms the foundation of applications such as key generation/storage, device anti-counterfeiting, user authentication, IP protection, and hardware/software binding. Traditional one time programmable (OTP) fuse-based key storage technologies are prone to invasive probing attacks where an attacker can expose internal circuit nodes to observe the stored key. The volatile nature of PUFs provides a high level of security and tamper resistance against invasive probing attacks. Moreover, they enable significant die cost reduction by eliminating additional manufacturing steps associated with fabricating fuses. A PUF's randomness is encoded as a response to some given challenge, known as a challenge-response pair (CRP). Depending on the possible number of CRPs and the type of application, PUFs are broadly classified as "weak" or "strong". A strong PUF can produce a large number of CRPs and it is typically used for device authentication [1], [2]. On the other hand, weak PUFs have only one or a few feasible CRPs and are mainly utilized for secure key generation [3], [4]. While strong PUFs, used in user-authentication, are often vulnerable to machine learning based modelling attacks, side-channel attacks, etc., weak PUFs, on the other hand, are vulnerable to several probing and power cyclic attacks. It is the role of the designer to make them resilient against these attacks. Another major issue with the PUF circuits is that raw PUF responses derived directly from the PUF circuits are not inherently 100% stable. Insufficient device mismatch, high thermal noise, and changes in operating conditions can lead to a high degree of instability in raw PUF bits. A key generation scheme must be resilient to these conditions to guarantee reliable operation of security applications. Several techniques have been demonstrated in literature to improve the stability of PUF bits including temporal-majority voting (TMV), soft dark-bit masking [3], [4], valid masking [5] etc. Nonetheless, all these techniques fail to make the PUF response 100% stable and rely on error-correction codes (2-D Hamming codes [6], BCH codes [7]) to get a 100% stable PUF response. In this paper we propose a stability enhancing technique which reinforces PUF cell bias using capacitive loading to produce a PUF cell that is resilient to transient changes in operating conditions and high thermal noise within a given power cycle.

The report is structured as follows. Section-II summarizes different state-of-the-art PUF architectures used in key generation and points to their drawbacks. Section-III describes the proposed CL-PUF. The experimental setup for comparing different PUF cells is shown in section-IV followed by simulation results and conclusion in section-V and section-VI respectively.

II. State-of-the-Art PUFs for Key Generation

PUFs exploit die-to-die process variation to generate static entropy with sufficient stability in the face of temporal voltage, temperature fluctuations and aging. A variety of PUF circuits based on bias generation [8], ring-oscillators [9], current mirrors [10], arbiters [11]–[13], cross-coupled inverters, oxide breakdown, and SRAMs have been proposed in recent literature.

The above mentioned PUF cell implementations provide solutions for applications such as user authentication, where minor deviations from the original PUF output are acceptable. Unlike user authentication, with secure key generation it is often crucial that the secure key is produced consistently and reliably so as to avoid potential catastrophic system failure [14]. For applications involving key generation, a PUF value has to be repeatedly created with 100% accuracy. Hybrid variants of classical designs based on arbiter/delay chains and SRAM cells have been recently used for key generation PUF implementations [1], [3], [4]. These circuits exploit metastability resolution dynamics of matching cross-coupled inverters along with delay variations in clock paths to generate static entropy in the PUF bits. Another design suitable for key generation exploits amplified threshold voltage variation [5], [14]. Several additional techniques such as TMV, burn-in hardening, dark-bit masking, BCH, etc. have been utilized atop these PUF cells to increase their stability.

A. Hybrid PUF Cell

The PUF architecture proposed in [3] achieves 100% stability and is robust against PVT variations. A "golden key", is created at first array power-up during tester-time operation and is reproduced from the inherently noisy raw PUF value during regular field operation. The golden key is used to compute an ECC signature, which is stored on-die as fuses and later used to regenerate the golden key with 100% accuracy. The basic PUF cell is based on a hybrid cross-coupled inverter circuit with a pair of precharge transistors that initialize the internal nodes to an unstable state. During the positive phase of the clock, the circuit evaluates and snaps to one of two stable states. Resolution toward a stable voltage from the initial unstable state is determined by the relative strengths of variation-impacted minimum sized inverters in the cross couple. Additionally, random variations in precharge transistors and devices along clock path produce mismatches in clock rise and arrival times introducing a transient dimension of uncertainty into PUF resolution dynamics. PUF cells that have insufficient within-die random variation generate unstable bits that resolve to "0" or "1" based on thermal noise, or voltage and temperature conditions. Such noisy bits undergo three conditioning steps to reduce overall PUF bit-error rate.

The first conditioning circuit, called temporal majority voter (TMV) computes the quantized mean of PUF responses within a voting window of size 15. Stable cells that result in count values above 8 are considered to be 1's and those with counts 7 or below are counted as 0's. [3] demonstrates a 53% reduction in total unstable bits by means of TMV-15. The next technique employed by [3] to reduce the overall BER is burn-in hardening. This technique further reduces bit errors by directed accelerated aging during tester-operation. Subsequent to first power-up and TMV evaluation, the PUF cell is subjected to high-temperature and high-voltage stress conditions while holding the complement of the golden key value. This biases transistors in a direction such that NBTI aging reinforces existing PUF bias. Although these two BER reduction techniques reduced the number of unstable bit by a large amount (55%), they fail to stabilize highly unstable bits. These highly unstable bits are identified as 'dark bits' during regular operation and a soft dark bit-mask is regenerated at the start of each power-up to eliminate these bits. After deploying these 3 different techniques, [3] achieves an overall BER of 0.97%. ECC circuits used BCH decoding to correct remnant bit errors, regenerating the golden key with 100% accuracy.

B. Delay-hardened Hybrid PUF Cell

In contrast to the techniques mentioned above, the delay hardened PUF proposed in [4] introduces two additional clock delay inverters into each pre-charge path (clk0 and clk1). These minimum-sized inverters introduce additional variation into PUF metastability dynamics. However, a more significant impact of the clock delay buffers on the PUF cell operation is observed during burn-in. During burn-in, the complementary value (bit#) is differentially written back into the cell, biasing the inverters in a direction such that NBTI/PBTI aging reinforces preexisting biases and improves cell stability. The clock delay inverters in the delay hardened cell are also differentially biased during burn-in such that a cell with an initial bias toward "1" self-biases and ages the appropriate clock devices. This extra bias reinforcement in the clock delay paths in addition to the directed aging of devices in the cross couple enables better post-burn-in cell stability. To increase stability a technique known as selective bit destabilization identifies cells with TMV counts ranging from 0%–10% to 90%–100% and stabilizes them by writing back the complementary PUF value into the cross couple. The remaining cells with TMV counts from 10% to 90% were destabilized by writing back the original value. This approach destabilizes 80% of all DBs, thereby increasing their probability of remaining DBs during both field and gold conditions and reducing mask mismatch induced bit error.

C. PUF Cell Exploiting Threshold Voltage Variation

The key generation PUF presented in [5], [14] further underscores the importance of reliability in PUF design by showcasing a high-reliability PUF specifically designed for incorporation in automobiles, an application domain where poor reliability could potentially lead to critical accidents. The PUF cell utilized by this paper exploits transistor threshold voltage (V_{th}) variation between two inverting logic gates — NAND gates in this case — and incorporates an enable signal [5] to trigger a response. Due to random process variation present, the threshold voltages of gates can be profiled under Gaussian distribution. Given that two gates have a high enough difference between their threshold voltages (above a certain noise margin), the threshold difference between the two gates can be amplified to output a stable to 1 or 0. A NAND gate (NAND2) with a given V_{th2} takes as its inputs an enable signal along with the output of another NAND gate (NAND1) with V_{th1}. NAND1 takes as its inputs the enable signal and its own output. While the enable signal is low, the output of the NAND1 gate is driven high to V_{DD}, as is the output of NAND2. Once the enable signal is driven high, signaling a read from the PUF cell, the output of NAND1 begins to fall until it reaches V_{th1} when the output of NAND1 will hover around that value. Based on the value of V_{th2}, the output of NAND2 will either be driven high or low, becoming the response of the PUF cell.

To mitigate the PUF cell's innate instability and reduce the bit error rate (BER) to a suitable value, the PUF cell array first undergoes an "enrollment phase" where a valid map, mask for majority voting, and BCH helper data is generated. During enrollment, the individual PUF cells are ran against a validity checker that analyzes the stability of PUF cells to mask out unstable cells from future use in key generation. To further stabilize individual PUF cells, 5b-to-1b spatial majority voting is applied. During the key extraction procedure, the output of PUF cells can be used to generate an output key bit based on majority voting. Finally, to achieve an appropriately low overall key error rate, BCH(255, 131, 18) error correction is applied twice, yielding a 256 bit key. It's also worth noting that this PUF design power-gate's the entire PUF array and only powers the cells when the key is being generated, mitigating any instabilities due to aging, like NBTI/PBTI. To satisfy safety requirements, this PUF design also incorporates detection/recovery methods for system failure.

III. Proposed CL-PUF: PUF bias reinforcement through capacitive loading

The PUF cell presented in this work utilizes the existing process dependent bias in a PUF cell and reinforces the same bias to make the PUF cell 100% stable to temporal variations within a power-on period. The proposed CL-PUF architecture is shown in Fig. 1. Similar to the previously mentioned hybrid PUF-cell and delay-hardened PUF-cell, the proposed CL-PUF uses a crossed-coupled inverter pair as the basic metastability element which makes a decision based on three major factors when the clock becomes high. The first factor is the mismatch between the inverters. Threshold voltage or other mismatch among the transistors can result in different drive strength favoring one of the output nodes for a high state. The second factor that biases the PUF cell is the delay mismatch between the inverter pairs driving the pre-charge transistors. When clock goes high, this delay mismatch causes a discrepancy between the arrival time of the clock edges at the gates of the pre-charge devices. Hence, one of the output nodes starts discharging earlier than the other. The third factor is the difference in the capacitive loading between the two nodes. The capacitive loading determines the discharge time of the nodes and can prefer one side of the PUF output for faster discharge if there is any mismatch between the capacitive loading. We utilize the last phenomenon to increase the capacitive loading of the node which is inherently biased towards high state due to process mismatch. This reinforces the existing PUF bias and avoids any temporal variation of the PUF output making the PUF cell 100% stable. The working principle of the proposed CL-PUF is delineated below.

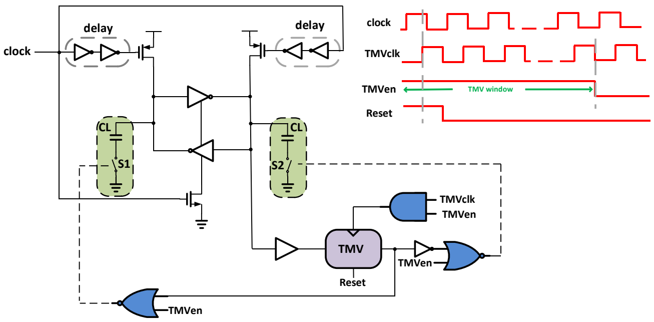

Fig. 1. Proposed capacitive-loaded PUF architecture. Switches S1 and S2 are both off during the TMV period and one of them is turned on after TMV decision loading one side of the PUF cell more than the other.

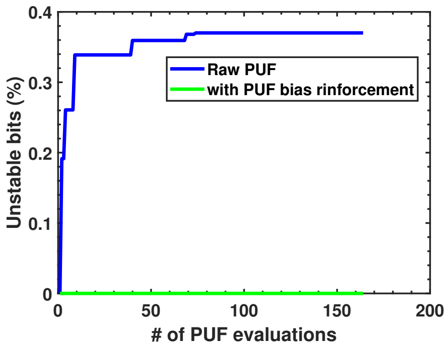

Fig. 2. Percentage of overall raw PUF bits identified as unstable as the number of PUF evaluations increases.

After power on, both switches $S1$ and $S2$ are open, hence, the capacitive loading is identical in both the output nodes. The PUF cell resolves the output bit based on its inherent process dependent mismatch and noise. This evaluated output is then averaged in time using temporal majority voting (TMV). The TMV window length indicates the number of successive PUF evaluations being averaged using TMV. If the TMV output is 'high', it turns switch $S2$ on. For the remaining time of operation switch $S2$ remains on biasing all the subsequent evaluations towards a 'high' state. Similarly, if the TMV output is 'low', switch $S1$ is turned on biasing all the subsequent evaluations towards 'low' state. Thus, this technique reinforces the existing bias. Note that, once TMV makes the decision, the 'TMVCLK' is gated using 'TMVen' signal so that there is no further change in the switch states. Fig. 2 shows how the unstable bit-count increases with number if evaluations for the raw-PUF without any bias-reinforcement. Whereas, with bias-reinforcement all the bits become fully stable.

Here it is important to analyze how the choice of load capacitance C_L affects the stability of the PUF response. Note that, as the parasitic capacitances of the PUF cell dominates the load capacitance, the effectiveness of bias reinforcement becomes very less and the PUF response can be flipped

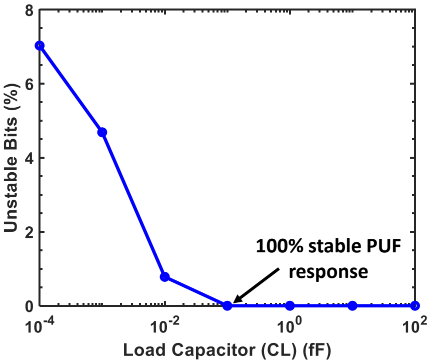

Fig. 3. Effect of the load capacitor value for bias reinforcement in the CL-PUF architecture simulated for 128 PUF cells. For $C_L > 100aF$ the bias reinforcement results in 100% stable PUF response. Below this value the parasitic capacitors of the PUF cell dominates the load capacitor.

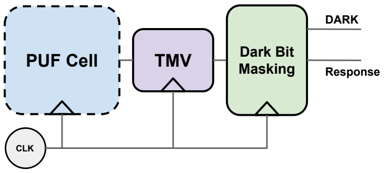

Fig. 4. Evaluation framework. PUF cells hardware simulation is placed into harness that simulates TMV and dark-bit masking in software.

by thermal noise and other temporal fluctuations resulting in instability. Fig. 3 shows the corresponding monte-carlo simulation results. It can be seen that a 100% stable PUF response can be obtained for $C_L > 100aF$. Below this value the parasitic capacitance dominates the load capacitance.

IV. Experimental Setup and PUF Cell Evaluation

A. Evaluation Framework

PUF cells in a design are typically supported by numerous extraneous circuit elements that are meant to increase the reliability. As an example, in order to satisfy automotive safety requirements, the PUF design presented by Choi et. al. [14] employs a number of peripheral techniques to achieve a cumulative Key Error Rate of as low as $1.41E-64$. These techniques included temporal majority voting, spatial majority voting, error correction with BCH, and burn-in. Another example [3] used some of these techniques along with soft dark-bit masking to reduce the bit error rate of the design to achieve 100% stability.

Since the use of extraneous techniques to increase stability varies across different designs, to set a level playing field, we chose to implement an evaluation framework that applies the same common stability-improving techniques to each individual PUF cell architecture. An overview of our evaluation framework is shown in 4. The PUF cell architecture under test produces a PUF response signal each clock cycle. For the hybrid, delay-hardened, and capacitive-loaded designs, the clock signal resets the PUF during ’low’ phase and generates the response during ’high’ phase. However, for the voltage-threshold-based PUF cell the clock simply drives a flip flop which captures the continuous response of the PUF each cycle. The use of the clock ensure that for the different PUF cell designs, a new PUF response is produced each cycle. These PUF responses are then passed through a temporal majority voting (TMV) stage increasing the stability in the face of thermal noise. After TMV, the majority response will be produced as the post-TMV PUF response. Ideally, the output of each temporal majority voting period results is the same PUF response, but this is not the case for a *highly unstable* bit with insufficient process variation. The dark bit masking stage aims to identify these highly unstable bits and exclude them from further use in PUF key evaluation. Our evaluation framework implements dark bit masking during the tester-time operation by aggregating a number of post-TMV PUF response values; if any of the post-TMV PUF responses vary, that cell is identified as a dark bit and excluded from the final *golden-key*. Any subsequent evaluations of the TMV are treated as *in-field* evaluations.

B. Implementation

In order to reduce simulation time for the PUF cells, we decided to only implement the PUF cells themselves in hardware and we simulated TMV and dark-bit masking in software using a MATLAB script. The PUF cells were all implemented using Cadence’s GPDK 45nm technology. Our experimental setup differed slightly for our proposed capacitive load PUF cell, as the switching of the load capacitors depends on feedback from an initial run of temporal majority voting. Because of this, we implemented TMV in hardware for our proposed cell, but not for our other cells due to simulation runtime concerns. Our schematic implementations of the state-of-the-art and proposed PUF cells, along with our evaluation software can be found on this project’s GitHub.

To evaluate the results from our simulations, we determined crucial metrics by which to evaluate our PUF cells. These metrics relate to three categories: **stability, randomness, and efficiency**.

C. Stability

Weak PUFs are suitable for key generation precisely because of their high stability [15], thus stability is a crucial metric. While the final reconstructed key error rate must be negligibly close to 0 (implying an 100% stable key), the PUF BER is a metric of more variation between different PUF designs. We chose to characterize the BER of each of the PUF cell designs both before and after enhancing measures (e.g. majority voting and dark-bit masking). Another metric that reflects the stability of a PUF cell array is it’s *intra*-chip hamming distance, which quantifies the number of bit differences in subsequent evaluations, and should ideally be 0. Producing meaningful data reflecting the intra-chip hamming distance would require a large number of PUF evaluations, for which we did not have the computational resources. Therefore, we only measured the bit error rate with and without different stability enhancing techniques.

D. Uniqueness and Randomness

Uniqueness and Randomness are important security metrics to use when evaluating a PUF. Uniqueness is the measurement of how different PUFs are from one-another. The inter-chip hamming distance measures how different a response is for the same challenge on different PUFs. Inter-chip hamming distance requires collecting PUF responses from many *different* instances of our PUF array. Thus, due to limited compute resources and time constraints, we were unable to gather meaningful data to determine the inter-chip hamming distances of our PUF cell designs. An equally important metric of a PUF cell is its randomness, can be characterized by running the responses from a PUF cell array against a set of statistical tests outlined by the National Institute of Standards and Technology's (NIST) Special Publication 800-22 [16].

The NIST 800-22 tests accept a binary stream of data that are generated by a random or pseudo-random generator; in our case the PUF cell itself, with process variation induced mismatch, acts as the random number generator. Each bit in the binary stream passed into the NIST tests shall be a different instance of a PUF cell. The individual values in random sequences are independent and unpredictable, both properties we care about in our PUF cells. If an individual were able to infer the response of a PUF based on publicly available information or the response of other PUF cells, it would compromise the security of all PUF arrays. It is important to note that no finite set of tests for randomness could be truly complete, as there exists an infinite set of tests that could search for the presence of a specific pattern in a binary sequence. As an example, some of the NIST tests we applied to our PUF cell data inspect the total number of 1s and 0s within a sequence, or groups of all 1s or all 0s to determine if they are approximately the same that would be expected by a truly random sequence.

E. Efficiency (Power, Area)

Another important area for evaluation, particularly on mobile or IoT devices, is a PUF's power and area consumption, which we broadly categorize under the "Efficiency" of a PUF cell. We evaluate power/bit and area/bit; a bit is the output of each PUF cell.

V. Results

We implemented and evaluated the discussed state-of-the-art PUF cell architectures along with our proposed capacitive load PUF cell and measured the aforementioned metrics. For each PUF cell we generated a 128 bit PUF array. First, to evaluate the stability of each PUF design, we determined the bit error rate with and without stability enhancing techniques. For these simulations, we used a TMV value of 7, indicating that 7 PUF evaluations contribute to each post-TMV response. Dark-bit masking was applied after 10 rounds of TMV, identifying and removing highly unstable bits. It is of note that there is no BER data for our CL-PUF architecture due to it's specific biasing behavior. Since the CL-PUF biases the PUF cell immediately after the first TMV round, with an appropriate load capacitance, we observed a BER of 0% for a given transient simulation, therefore we excluded it from our results. The resulting bit error rates for our simulations are shown in Figure 5. We observed expected behavior with the application of stability improving techniques like TMV and dark-bit masking. Figure 6 demonstrates the trade off between a wider TMV period and the number of dark bits remaining. The final post-TMV+DB BER results from our simulations closely reflect the trends presented in the state-of-the-art papers [3], [4], [14] that proposed the designs.

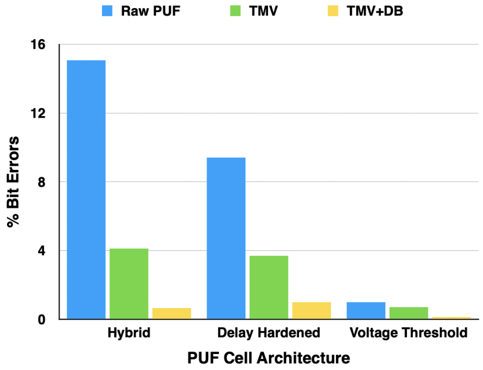

Fig. 5. Bit Error Rate of 128 bit PUF Cell array for each of the relevant PUF Cell Architectures. Includes BER for Raw PUF responses, post-TMV responses, and post-dark bit masking.

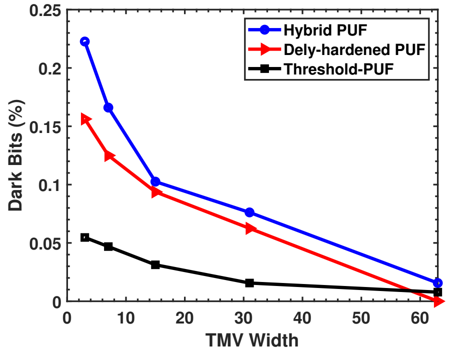

Fig. 6. Percentage of overall PUF cells identified as dark bits as the number of TMV cycles increases for the state-of-the-art PUF cell designs.

TABLE I
NIST 800-22 Randomness Test Results

Test	Hybrid		DH		V_{TH}		C Loaded	
	P	*Pass*	*P*	*Pass*	*P*	*Pass*	*P*	*Pass*
Freq.	0.48	✓	0.11	✓	0.48	✓	0.15	✓
Runs	0.14	✓	0.89	✓	0.35	✓	0.2	✓
Longest	0.5	✓	0.53	✓	0.22	✓	0.5	✓
Cum-Sum	0.65	✓	0.17	✓	0.77	✓	0.25	✓
Serial	0.49	✓	0.49	✓	0.49	✓	0.49	✓
Block F.	0.48	✓	0.11	✓	0.48	✓	0.15	✓
Entropy	0.36	✓	0.49	✓	0.26	✓	0.43	✓

We also ran select tests from the NIST 800-22 test suite to determine the cell's randomness. For all tests we used an input

TABLE II
EVALUATION RESULTS SUMMARY

Metric	**Hybrid [3]**	**DH [4]**	V_{TH} **[14]**	**This Work**
Tech.y	45nm	45nm	45nm	45nm
BER	0.65%	0.99%	0.12%	-
NIST	PASS	PASS	PASS	PASS
Power/Bit	$4.26\mu W/b$	$8.53\mu W/b$	$2.66\mu W/b$	$7.53\mu W/b$
Area/Bit	$0.146\mu m^2/b$	$0.21\mu m^2/b$	$0.13\mu m^2/b$	$0.43\mu m^2/b$

*PUF cells simulated with 1V supply voltage.

sequence length of 128, where the recommended minimum is 100. These tests are: Frequency, Runs, Longest Runs, Cumulative Sum, Serial, Block Frequency, and Approximate Entropy. Additional tests [3] like the FFT and Ranks tests, both require much higher minimum stream lengths and due to compute resource limitations we were unable to generate the necessary input length. The results from the NIST tests is shown in Table I. For each PUF design, all NIST tests passed.

Finally, we calculated approximate values for PUF cell efficiency metrics: power/bit, energy/bit, and area/bit. These results are shown in Table II. It is important to note that each our approximations do *not* reflect the inclusion of TMV in the PUF cell. We separately calculated the metrics for TMV, with power consumption of $22.55\mu W/b$, and an area of $3.82\mu m^2$. For power, the voltage threshold showcased the lowest power consumption. Our proposed PUF had power nearing that of the delay hardened PUF cell. The voltage threshold PUF design was the smallest of the PUF cells, due to it's use of less logic gates. Our proposed capacitive loaded PUF design had the highest area consumption due to the use of 2 capacitors as well. These $1fF$-value capacitors are implemented using MOSFETs to minimize the area-overhead.

A. Simulation Constraints

Due to computational resource and time constraints we were unable to simulate and evaluate a large number of individual PUF cells and PUF arrays leading us to be unable to compute some metrics. Given more PUF evaluations results like the BER, and NIST randomness tests would be more reliable and accurate. There exist techniques that have been shown to decrease the simulation burden such as importance sampling [17], but exploration of this technique has been left to future work.

VI. CONCLUSION

PUFs are a prominent area of research due to their potential applications and strong security properties. In this paper we implemented and evaluated three state-of-the-art PUF cell designs for secure key generation, along with our own proposed PUF cell design. Our proposed PUF cell design demonstrated a resilience to noise and changes in operating conditions and high thermal noise, through the use of dynamically adding capacitive loads to bias PUF cell responses. We implemented a software evaluation tool to perform stability enhancing techniques like TMV and dark-bit masking. Finally, we evaluated the PUF architectures with concern for their stability, randomness, and efficiency.

REFERENCES

[1] V. Suresh, R. Kumar, M. Anders, H. Kaul, V. De and S. Mathew, "A 0.26% BER, 1028 Challenge-Response Machine-Learning Resistant Strong-PUF in 14nm CMOS Featuring Stability-Aware Adversarial Challenge Selection," 2020 IEEE Symposium on VLSI Circuits, Honolulu, HI, USA, 2020.

[2] S. Jeloka, K. Yang, M. Orshansky, D. Sylvester and D. Blaauw, "A sequence dependent challenge-response PUF using 28nm SRAM 6T bit cell," 2017 Symposium on VLSI Circuits, Kyoto, 2017.

[3] S. K. Mathew et al., "16.2 A 0.19pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS," 2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC), San Francisco, CA, USA, 2014.

[4] S. Satpathy et al., "A 4-fJ/b Delay-Hardened Physically Unclonable Function Circuit With Selective Bit Destabilization in 14-nm Trigate CMOS," in IEEE Journal of Solid-State Circuits, vol. 52, no. 4, pp. 940-949.

[5] B. Karpinskyy, Y. Lee, Y. Choi, Y. Kim, M. Noh and S. Lee, "8.7 Physically unclonable function for secure key generation with a key error rate of 2E-38 in 45nm smart-card chips," *2016 IEEE International Solid-State Circuits Conference (ISSCC)*, San Francisco, CA, USA, 2016, pp. 158-160.

[6] B. Gassend, "Physical random functions," M.S. thesis, Dept. Electr. Eng. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, Jan. 2003.

[7] G. E. Suh, "AEGIS: A single-chip secure processor," Ph.D. dissertation, Dept. Electr. Eng. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, Aug. 2005.

[8] J. Li and M. Seok, "A 3.07μm^2/bitcell physically unclonable function with 3.5% and 1% bit-instability across 0 to 80°C and 0.6 to 1.2V in a 65nm CMOS," in Symp. VLSI Circuits Dig. Tech. Papers, Jun. 2015, pp. C250–C251.

[9] K. Yang, Q. Dong, D. Blaauw and D. Sylvester, "14.2 A physically unclonable function with BER $< 10^{-8}$ for robust chip authentication using oscillator collapse in 40nm CMOS," 2015 IEEE International Solid-State Circuits Conference (ISSCC) Digest of Technical Papers, San Francisco, CA, USA, 2015.

[10] A. Alvarez, W. Zhao, and M. Alioto, "15fJ/b static physically unclonable functions for secure chip identification with < 2% native bit instability and 140× Inter/Intra PUF Hamming distance separation in 65nm," in ISSCC Dig. Tech. Papers, Feb. 2015, pp. 1–3.

[11] J. W. Lee, Daihyun Lim, B. Gassend, G. E. Suh, M. van Dijk and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," 2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525), Honolulu, HI, USA, 2004.

[12] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Lightweight secure PUFs," in Proc. ACM/IEEE Int. Conf. Comput.-Aided Design, 2008, pp. 670–673.

[13] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in Proc. ACM/IEEE Design Autom. Conf., 2007, pp. 9–14.

[14] Y. Choi et al., "Physically unclonable function in 28nm fdsoi technology achieving high reliability for aec-q 100 grade 1 and iso 26262 asil-b," *2020 IEEE International Solid- State Circuits Conference - (ISSCC)*, San Francisco, CA, USA, 2020, pp. 426-428, doi: 10.1109/ISSCC19947.2020.9063075.

[15] C. Herder, M. Yu, F. Koushanfar and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," in *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126-1141, Aug. 2014.

[16] Bassham, Lawrence E. et al. "SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications" *National Institute of Standards Technology*, Gaithersburg, MD, USA, 2010

[17] T. S. Doorn et al., "Importance sampling Monte Carlo simulations for accurate estimation of SRAM yield," *ESSCIRC 2008 - 34th European Solid-State Circuits Conference*, 2008, pp. 230-233