An Overview of and Comparison Framework for High-Stability PUF Design Suitable for Key Generation

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. In this report three state-of-the-art key generation schemes are discussed and we investigate several trade-offs between the key-metrics that govern PUF performance. We distill the efficacy of individual PUF cells into three categories: stability, uniqueness and randomness, and power and area efficiency — all encompassing various metrics. The three discussed PUF designs are evaluated, and a comparison testbench for future PUF cell evaluation is described.**

***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, 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 initially an unpredictable, yet consistent, unique signature (or a device "finger print"). This signature forms the foundation for many 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 decapsulates the chip and exposes internal circuit nodes to observe the stored key. However, 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. In addition, the absence of a copy of the key with the device manufacturer also alleviates counterfeiting risks. 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 in key generation application. It is the role of the designer to make them resilient against these attacks. Another major issue with the PUF circuits is that the 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 changes in voltage, temperature, and device aging conditions to guarantee reliable operation of security oriented applications over a product's life-time. Several techniques have been demonstrated in literature to improve the stability of PUF bits including temporal-majority voting (TMV), soft dark-bits masking [3], [4], valid masking [5], use of error-correction codes (2-D Hamming codes [6], BCH codes [7]) etc.

This report focuses specifically on weak PUFs utilized in stable and secure key generation application. Section-II first summarizes different state-of-the-art PUF architectures and discusses three of them in detail. Section-III proposes a testbench and various metrics to compare the performance of different PUF cells. Section-IV summarizes the comparison results and Section-V summarizes the report.

II. State of the art PUF Design

PUFs exploit die-to-die process variation to generate static entropy with sufficient stability in the face of temporal voltage,

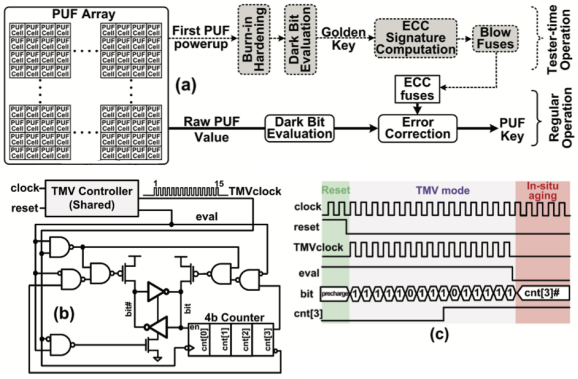

Fig. 1. PUF architecture proposed in [3]: (a) Overall system and basic PUF cell, (b) implementation of TMV and burn-in hardening to reduce the BER, (c) TMV and burn-in hardening timing diagram.

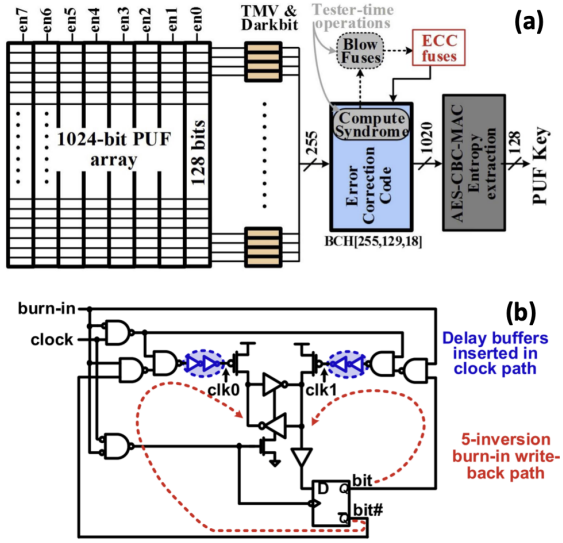

Fig. 2. PUF architecture proposed in [4]: (a) Overall system architecture, (b) basic PUF cell.

and 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.

All the above mentioned techniques for PUF cell implementation provide a promising solution for applications such as user authentication where device disambiguation can still be accomplished with minor deviations from the original PUF output by using multiple challenge-response pairs. However, 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 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 and make them suitable for secure key generation.

A. Hybrid PUF Cell

The PUF architecture proposed in [3] and shown in Fig. 1 achieves 100% stability and is robust against PVT variations. A golden key is created at first array power-up during tester-time operation (Fig. 1(a)) and subsequently this golden value is derived 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. During regular operation, error correction circuits mix raw PUF bits with ECC fuse values to regenerate the golden key with 100% accuracy. The basic PUF cell is based off of 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 (Fig. 1(b,c)). 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 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 (Fig. 2(b)) into each pre-charge path (clk0 and clk1). These minimum-sized inverters introduce additional variation into PUF metastability dynamics, resulting in a reduction in BER over the basic hybrid cell proposed in [3]. 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#) (Fig. 2(b)) is differentially written back into the cell, biasing inverter devices 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 to push out clk1 rise delays, while pulling in clk0 rising edges relative to a nominal two inverter delay. This extra bias reinforcement in the clock delay paths in addition to the directed aging of devices in the cross couple enables better postburn-in cell stability. As a drawback of the DB masking method, it was shown in [4] that mismatches between the golden mask and the field mask increases the BER. As a solution to this, a TMV count based windowing technique that selectively hardens each cell toward higher or lower stability to improve overall BER was proposed. Also known as selective bit destabilization, in this technique all cells with TMV counts ranging from 0%–10% to 90%–100% were stabilized by writing back the complementary PUF value into the cross couple, while 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 dark at 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 [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. Built upon a PUF cell design originally showcased in [5], this paper employs various auxiliary techniques in order to increase the stability of the key generation hardware to meet necessary automotive standards.

The PUF cell utilized by this paper exploits transistor threshold voltage (V_{th}) variation between two inverting logic gates — NAND gates in this example — incorporating an enable signal [5]. 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. A schematic of this PUF cell is shown in Figure 3.

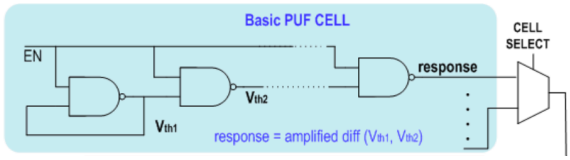

Fig. 3. A schematic view of the (paritial) PUF Hard Macro from [5] incorporated into the high-reliability design presented in [14]

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. PUF cell validity checks are repeated 8 times at 50 kHz under 5 different operating temperatures, decreasing the BER from 10.5% to just 0.97%. To further stabilize individual PUF cells, 5b-to-1b spatial majority voting is applied, allowing at most 2 bit flips out of 5 bits to be corrected. This is achieved by generating a 4-bit mask during initial operation which can be stored in non-volatile memory without revealing any key information. 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 to 255 bits of PUF output and helper data, correcting at most 18b errors and yielding a 131 bit PUF key. In this example, the design is intended to yield a 256 bit key, and thus the process is ran twice. 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. For example, the MAC of the PUF key is stored in non-volatile memory. This does not reveal the value of the key, but can detect failure in key generation. Register redundancy is incorporated into the design to protect against potential failure.

III. Comparison Framework and Testbench

Given our target application of PUF key generation, we have identified three primary areas of interest when evaluating PUF designs. We incorporate these three areas of analysis to provide holistic views of the efficacy of each of the presented state-of-the-art PUF designs.

A. Stability

Weak PUFs are suitable for key generation precisely because of their high stability [15], thus stability is a crucial metric. In our analysis, we used two measures of stability when evaluating each of the PUF implementations. Most PUF implementations for key generation present the stability of the individual PUF cells and the stability of the entire PUF-based key-generation pipeline separately. While the 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, and is characterized for the PUF cell array after some cell-specific BER enhancing measures (e.g. majority voting). Another metric that reflects the stability of a PUF cell is it's *intra*-chip hamming distance. During the enrollment phase of the PUF, when the "golden key" is generated, upon subsequent evaluations, the intra-chip hamming distance quantifies the number of bit differences in the generated key which should ideally be 0.

B. 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. This is ideally 50%, or a normalized hamming distance of 0.5. Entropy is another valuable metric, encompassing the randomness of PUF cell. A typical measurement is entropy per bit, with the ideal value being 1. The randomness of a PUF can also be characterized by running the given implementation against the National Institute of Standards and Technology's (NIST) Special Publication 800-22, which outlines a set of statistical tests used to evaluate randomness.

C. Efficiency (Power, Area)

Another important area for evaluation is a PUF's power and area consumption, which we categorize under the "Efficiency" of the PUF cell. Power and area are important metrics, particularly on mobile or IoT devices. We use 3 metrics to quantify the cell's efficiency: power/bit, energy/bit, and area/bit; a bit is the output of each PUF cell.

To compare different PUF cells mentioned in the previous section based on the above metrics, we plan to make use of the testbench in Fig. 2(a) from [4] where a PUF cell can be substituted by the three different PUF topologies we discussed in the previous section. The PUF design's we've evaluated in the paper typically employ unique techniques, intimately tied to the PUF cell topology to increase stability before applying BCH. Our testbench aims to divide PUF-cell dependent techniques from those that are more general in enhancing stability, like BCH. With this, we should be able to easily exchange PUF architectures without hampering stability or randomness due to the removal of PUF-specific techniques. Considering this detailed comparison to be a future work, the next section compares the results that are already reported in the previously mentioned papers.

IV. Comparison Results

Utilizing our aforementioned metrics, we evaluated the three presented state-of-the-art PUF designs for secure key generation. Shown in Table I, each of the designs is evaluated for their **stability**: BER and intra-chip hamming distance; their **uniqueness and randomness**: inter-chip hamming distance, entropy/bit, and NIST 800-22 compliance; and finally their **efficiency**: power/bit, energy/bit, and area/bit. While some of the papers did not provide some of our metrics, we plan to use our testbench to evaluate those at a later date. For stability, the threshold voltage design had the lowest BER, followed by the initial hybrid cell design which also has the lowest provided intra-chip hamming distance. For uniqueness and randomness, the threshold voltage design demonstrates the best inter-chip hamming distance, highest entropy/bit and passes the NIST 800-22 test suite. The lowest power/bit and area/bit is also achieved by the threshold voltage design.

Through our evaluation we identified a trade-off between the initial hybrid cell and D-H hybrid cell. Although the delay hardened cell has lower energy/bit and lower area consumption, it scores worse in all measurements of stability, uniqueness, and randomness. This indicates that there is indeed a trade-off between efficiency and stability. One potential reason for this trade-off is the necessity of auxiliary hardware to increase stability, eating up energy and area.

TABLE I
Comparison Results

Metric	ISSCC 2014 [3]	JSSC 2017 [4]	ISSCC 2020 [14]
Technology	22nm TG CMOS	14nm TG CMOS	28nm FDSOI
PUF topology	Hybrid cell	D-H hybrid cell	Threshold voltage
BER	0.97%	1.46%	0.89%
Intra-Chip HD	0.0257	0.034	-
Inter-Chip HD	0.49	0.486	0.4978
Entropy / Bit	0.9997	0.99993	0.9999999
NIST 800-22	PASS	-	PASS
Power / Bit	$25\mu W/b$	-	$0.09\mu W/b$
Energy / Bit	13fJ/b	4fJ/b	-
Area / Bit	$4.66\mu m^2/b$	$1.84\mu m^2/b$	$2.90\mu m^2/b$

V. Conclusion

PUFs are a prominent area of research due to their potential applications and strong security properties. In this paper we went through an overview of three state-of-the-art PUF cell designs for secure key generation. We formulated a holistic comparison framework consisting of three main areas of interest, marked by various metrics: **stability**, **uniqueness and randomness**, and **power and area efficiency**. In the coming weeks we plan to implement the reviewed PUF cell designs and incorporate them into our proposed test bench to take further measurements and validate our initial comparison results. We also plan to explore our own ideas for PUF topology and use our laid out comparison framework to evaluate our design's efficacy.

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.