A Metal-Via Resistance Based Physically Unclonable Function with 1.18% Native Instability

Beomsoo Park, Mark Tehranipoor, Domenic Forte, Nima Maghari
Department of electrical and computer engineering, University of Florida, Gainesville, Florida USA, 32611
Email: beomsoo0927@ufl.edu

Abstract **A physically unclonable function (PUF) leveraging the parasitic resistance created by the metal via interconnection as entropy source is proposed in this paper. Metals 2 through 6 of a 65nm process is used to create the necessary parasitic resistance. Instead of using additional stabilization techniques, an incremental analog to digital converter is implemented to precisely measure the voltage difference between two branches consisting of the metal via interconnection based parasitic resistances. The fabricated PUF, without using any post processing algorithm, achieves a native instability of 1.18% with 1000 repeated evaluations. The worst case instability for voltage and temperature ranging from 0.8V to 1.3V and 0°C to 85°C, respectively is below 2.5%. The distance ratio between intra die and inter die Hamming Distance is above 310X.**

Keywords ***Physically unclonable function, incremental analog-to-digital converter, parasitic resistance, stability, uniqueness, Hamming Distance***

I. INTRODUCTION

Physically unclonable functions (PUFs) are volatile on-chip built primitives that have emerged as a solution for security authentication [1]. While most circuits aim to reduce the process and manufacturing variations, PUFs leverage these inherent characteristics as entropy sources. Depending on the process and manufacturing variations, each PUF generates its own unique and stable response to a set of challenges. The unpredictable and repeatable characteristic of PUFs enable a high level of security and resistance to physical/nonphysical attacks and thus is a promising alternative to digital memory [1].

Recently published PUFs [2]-[6] exploit mainly two different types of entropy sources: 1) the threshold voltage and aspect ratio variations due to transistor mismatches and 2) the delay variations from interconnection mismatches. Although the performance of these PUFs surpass the conventional SRAM, arbiter, and ring oscillator (RO) based PUFs, the current mirror [3], NAND gate [6], and cross- coupled inverter [5] based PUFs consume a rather large area. Moreover, additional stabilizing and calibration techniques such as temporal majority voting (TMV), masking, burn-in, and ECC correction are applied for most PUFs to increase stability as well as to decrease the sensitivity to voltage and temperature variations.

In this work, rather than using transistors as the source of entropy, a new type of weak PUF is presented which utilizes passive components, i.e. the parasitic resistance created between metal-via interconnections as the source of entropy. Multiple layers of metals and vias are used to increase the variation of the parasitic resistance. A backend incremental analog-to-digital converter (IADC) is implemented to precisely evaluate the PUF response and to remove any additional stabilizing techniques which tends to increase the overall testing time.

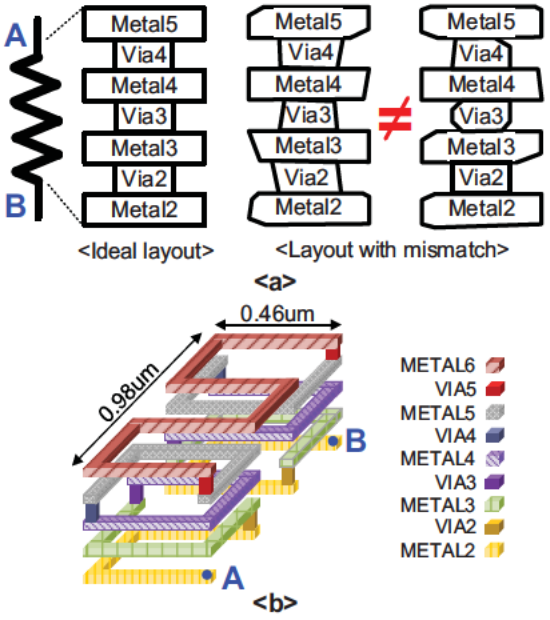

Fig. 1. (a) Conceptual parasitic resistance of metal and via layers as entropy source and (b) three dimensional version of implemented layout.

This paper is organized as follows. Section II discusses in detail the proposed metal-via resistance (MVR) based PUF and the architecture of the design. In section III, the overall operation of the MVR PUF with the backend IADC is illustrated. Measurement results with comparison to previous state of art designs are shown in section IV and finally a conclusion is made in section V.

II. PROPOSED MVR PUF

The overall concept of utilizing metal-via interconnections as entropy source is shown in Fig. 1. Unlike conventional PUFs such as arbiter and RO based PUFs where the delay variation of metal-via interconnections is used as the entropy source, this work utilizes the static difference due to interconnection mismatches. Although identical metal-via interconnections ideally create equivalent parasitic resistances, the process and

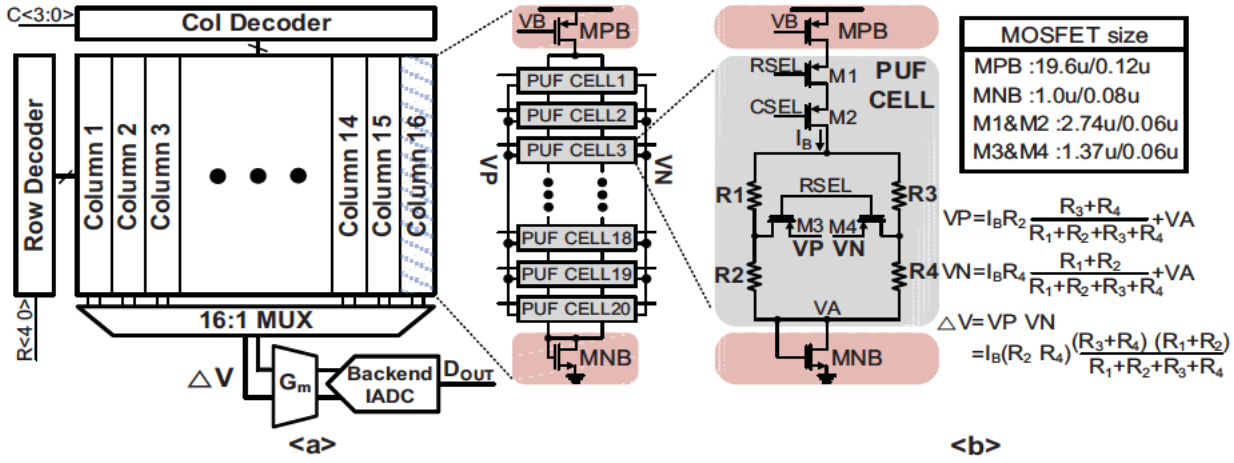

Fig. 2. (a) Overall 16X20 PUF array with backend IADC and (b) configuration of metal-via resistance (MVR) based PUF unit cell.

manufacturing variations cause these interconnections to have different patterns as shown in Fig. 1(a). These different patterns will result in the resistance values to differ from one another.

Leveraging entropy source with large variation is important in building a unique and stable PUF. The large variance enables the PUFs to have distinctive outputs consistent throughout repeated number of evaluations which reflects the repeatability of the PUF. The use of multiple metal and via layers increases the possibility of the physical dimensions to vary between equivalent layout structures creating larger deviations. Thus, metals 2 through 6 are used in this design along with a spiral type layout to increase the mean value as well as the variation of the parasitic resistance in a compact area (0.46um x 0.98um) as shown in Fig. 1(b).

Protecting the PUF from outside invasive attacks have also become an important issue for PUF designs [7]. A common solution is to add additional top-level metal layers to shield the PUF but this technique does not protect the PUF from invasive attacks such as focused ion beam (FIB). However, the proposed MVR PUF is inherently resilient to physical attacks. Any invasive attempts to the metal layers to monitor the PUF response will alter the resistance value and modify the output result. In addition, monitoring the output of the IADC which will be discussed later will give no valuable information as the accumulated output provide the PUF response. Thus, physical attacks such as probing or tampering is extremely difficult to apply to the MVR PUF and therefore allows the design to be resistant from invasive and noninvasive attacks.

Fig. 2(a) shows the overall PUF design based on the parasitic resistance. A 16x20 array configuration similar to traditional SRAM designs is used for area and readout efficiency [4] followed by a transconductance (G_m) and a backend IADC operating as a high-resolution comparator. The G_m provides both the high input impedance and low noise that is necessary between the PUF array and the backend IADC. The current source, MPB, and the diode-connected transistor for isolation to the ground, MNB, are shared among each column for area efficiency. Considering the leakage current from PUF cells that are off, a column is limited to 20 PUF cells [4]. To minimize any noise or offset sources other than the parasitic resistance that could possibly affect the PUF response, a symmetrical bridge configuration is used to generate a voltage difference (ΔV) between the two branches as shown in Fig 2(b). Overall, the proposed MVR PUF cell consists of the shared MPB and MNB, and four parasitic resistances (R1-R4) generated from metal-via interconnections.

III. Operation of MVR PUF with Backend IADC

Previous PUF designs that detect small voltage differences using a comparator require a calibration technique to remove the

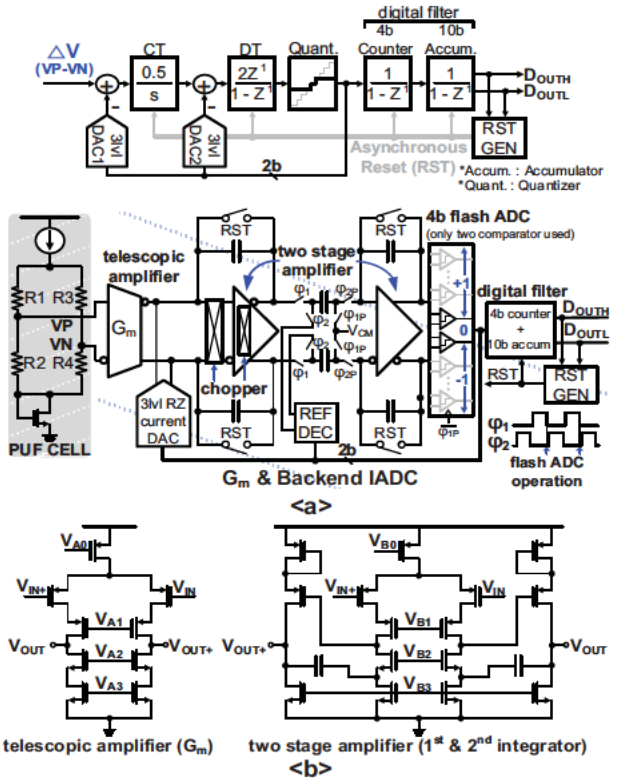

Fig. 3. (a) System (top) and circuit (bottom) level design of implemented G_m and 2nd order IADC and (b) implemented telescopic and two stage amplifier.

offset and to increase the accuracy of the comparator [4]. Instead of using any static or dynamic comparator to detect the small voltage range of the MVR PUF, an on-chip low-offset IADC is implemented in this work as shown in Fig. 3(a). The 2nd order IADC consists of a combination of continuous (CT) and discrete time (DT) integrators to form a 2nd order loop filter followed by a 4-bit quantizer and a 2nd order digital decimation filter. Due to the limited input voltage range generated by the PUF, only the two mid-level comparators are used in the quantizer to simplify both the quantizer and the backend decimation filter. In the case of large mismatch between MVR PUF elements resulting in large ΔV, the IADC may saturate due to the removal of these extra comparators. This saturation however is a merit to the overall performance as it provides more stable output bits as described below.

The purpose of the IADC is to average out the thermal noise and amplify the differential input voltage, ΔV, of the MVR in order to eventually yield an absolute binary level after decimation (cascade of two digital integrators). The inherent averaging of the thermal noise provided by the operation of the IADC plays an essential role in the bit stability of the PUF, removing the need for any post processing algorithms. The G_m which is used to isolate the ΔV generated by the MVR PUF from the input of the IADC, converts the ΔV to differential current (ΔI) and charges the integrating capacitor of the first integrator. To minimize the inherent offset and the flicker noise of the G_m as well as the 1st integrator, a telescopic amplifier with a large PMOS input pair and a two stage amplifier with a PMOS input pair is used respectively, as shown in Fig. 3(b). To further suppress the offset and flicker noise, the IADC input stage (1st integrator) is chopped at 1/16 rate of the sampling frequency as shown in Fig. 3(a). It is worth noting that an additional chopper can be added to the input of the G_m to minimize the G_m offset as well. However, this results in undesired switching artifacts on the MVR PUF cell output that reduces the PUF stability. Since the IADC essentially acts as a precision comparator with a binary decision output, linearity and swing requirements of the operating G_m and integrators are not critically important hence simplifying the overall circuit topology. As the quantizer consist of only two comparators, a single three level return-to-zero (RZ) current digital-to-analog converter (DAC) element is used as the feedback DAC [8]. This removes the linearity issue found in multi-element DACs that may affect the bit stability.

The operation principle of the G_m and IADC is as follows: if the input ΔV is large and much greater than the thermal noise, it translates to a large ΔI input to the IADC which outputs a "1" (or "0" depending on the polarity) in almost every cycle. The decimator saturates quickly and provides the final PUF decision (D_{OUTH} or D_{OUTL} of Fig. 3(b)). However, if the ΔV is small or even below the thermal noise, the IADC provides a stream of "1"s and "0"s. The operation takes longer compared to a large ΔV, but the average of the output bit sequence through decimation eventually depicts the final PUF decision. Therefore, the noise is averaged over all cycles and is substantially reduced, improving the overall bit stability. Following the final decision, the IADC resets itself and the next PUF element is selected for evaluation in an asynchronous fashion. Thus, the evaluation of all 320 PUF bits is automated. Although the IADC, unlike single-shot PUFs, requires more clock cycles to resolve a bit, it does not require any post processing used in most PUFs which demand extra testing time and therefore reduces the overall complexity and removes the need for any off-chip calibration.

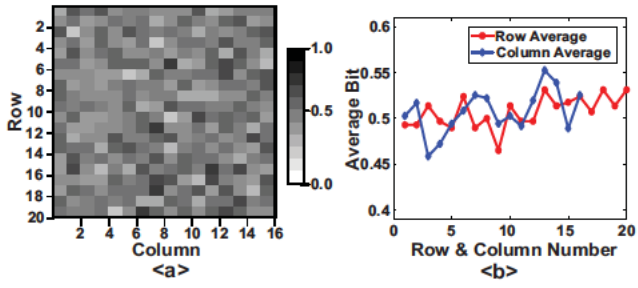

Fig. 4. (a) Spatial distribution of 0s and 1s averaged over 18 PUF arrays and (b) average value of each row and column for 18 PUF arrays.

IV. Measurement Results

The proposed MVR PUF is fabricated using a 65nm process for verification. Measurement is performed with 18 PUF arrays from 6 different dies (3 arrays per die, each 320 MVR PUF cells) at a supply voltage of 1.2V for 1000 evaluations. The spatial distribution of the digital bits averaged across 18 PUF arrays is shown in Fig. 4(a). The distribution reveals that there is no systematic bias indicating that the output is independent from the layout pattern. Moreover, Fig. 4(b) shows the digital bits averaged across each row and column which results around 0.5. This proves that the implemented MVR pattern has no systematic process variation.

Uniqueness between PUF instances as well as the reproducibility of each PUF instance are the parameters of utmost importance used to evaluate a PUF. Fig. 5(a) shows the normalized intra-die and inter-die Hamming Distance (HD) measured results of 0.0016b and 0.5027b at nominal condition using 18 PUF arrays which is close to the ideal value of 0 and 0.5. The separation provided by the intra-die and the inter-die HD is well over 310X. The value at 95% confidence of the autocorrelation function (ACF) shown in Fig. 5(b) is 0.0258 which is close to 0 showing good uniformity of the PUF.

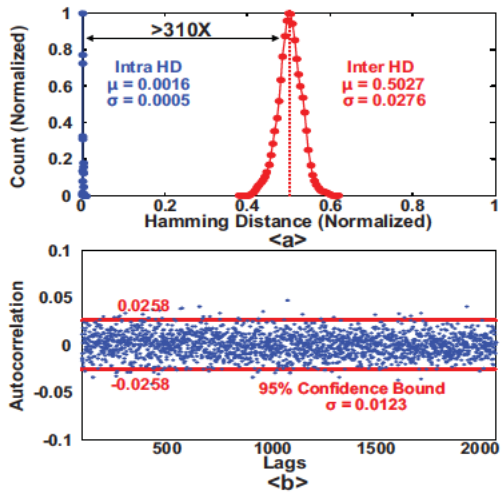

Fig. 5. (a) Measured intra-die/inter-die HD and (b) autocorrelation function.

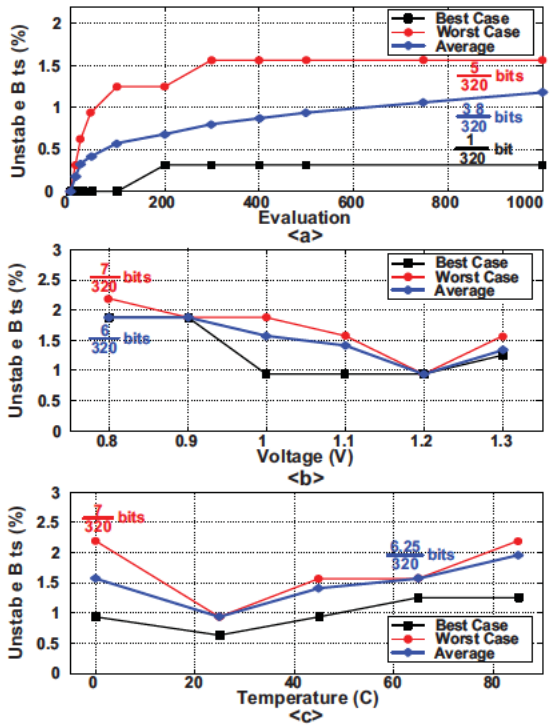

Fig. 6. Stability measurement (a) at nominal condition using 18 PUF arrays and (b) voltage and (c) temperature sweep using 6 PUF arrays.

The stability of the PUF performance over numerous evaluations as well as across different supply voltage and temperature is another major metric for PUF. The percentage of native unstable bits [5] at nominal condition of 1.2V and 27°C is 1.18% (3.8bits out of 320bits) as shown in Fig. 6(a) without using any additional calibration or post data processing techniques. The performance across supply voltages of 0.8V and 1.3V as well as temperatures of 0°C and 85°C is shown in Fig. 6(b) and Fig. 6(c), respectively. Six PUF arrays from three different dies are used for the measurement and the worst case unstable bits is below 2.5% (8bits out of 320bits) indicating strong insensitivity to supply voltage and temperature compared to previously reported values of 3.81% (at 0.7V) and 4.56% (at 85°C) [3].

The average energy consumption is measured as 0.22pJ/bit without the IADC and 17pJ/bit with IADC (20MS/s operating speed for the IADC with an average of 100cycles/bit). The die photo and PUF unit cell layout are shown in Fig. 7 and a comparison with previous works is shown in Table I.

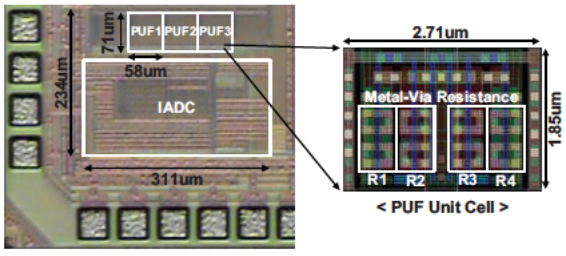

Fig. 7. Die micrograph of PUF test chip and PUF unit cell layout.

TABLE I. PERFORMANCE SUMMARY AND COMPARISON TO PRIOR ARTS

		This Work	[2]	[3]	[4]	[5]
Technology (nm) Feature size (nm)		65 (60)	180 (180)	65 (60)	65 (60)	22 (22)
PUF Cell Area/Bit [a]		5.01 um² 1392 F²	17.9 um² 553 F²	21.6 um² 6000 F²	3.07 um² 853 F²	4.66 um² 9628 F²
Native Unstable Bits (# of evaluations)		1.18% (1000)	1.67% (2000)	1.73% (400)	7.10% (500)	30% (5000)
Additional Stabilizing Technique	TMV	X	O (TMV11)	X	O (TMV11)	O (TMV15)
	Dark bit mask Burn in	X	X	X	X	O
Unstable Bits after stabilizing technique		--	0.50%	--	2.00%	3.00% [b]
Normalized Mean Inter HD		0.5027	0.4989	0.5014	0.5001	0.49
Normalized Mean Intra HD		0.0016	0.0007	0.0036	0.0057	--
Inter/Intra HD Distance Ratio		314.1	712.7	139.9	87.7	19
PUF Energy/bit (pJ/bit)		0.22 (w/o IADC) 17.0 (with IADC)	0.0113 (@1.2V	0.015	1.1	0.013

[2] :DNW version, [3] :INV PUF version used for comparison
a) feature size on 1st row used for calculation b) 2-bit glitch detection

V. CONCLUSION

A PUF based on the parasitic resistance formed by metal-via interconnection is proposed in this paper. Rather than using on-chip stabilizing techniques or off-chip post-processing to improve stability and to suppress voltage and temperature variations, an integrated backend IADC is implemented to accurately readout the PUF responses. The proposed PUF is inherently resilient to invasive attacks due to its analog like operation. The detailed measurement results prove the stability of the proposed solution.

ACKNOWLEDGMENT

This work was supported by the National Science Foundation under Grant No. CCSS-1610075.

REFERENCES

[1] C. Herder, et al., "Physical Unclonable Functions and Applications: A Tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126-1141, Aug. 2014.

[2] K. Yang, et al., "A 553F² 2-Transistor Amplifier-Based Physically Unclonable Function (PUF) with 1.67% Native Instability," *IEEE ISSCC Dig. Tech. Papers*, pp. 146 147, Feb. 2017.

[3] A. Alvarez, et al., "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," *IEEE ISSCC Dig. Tech. Papers*, pp. 256 257, Feb. 2015.

[4] J. Li and M. Seok, "A 3.07 μm²/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," *IEEE Symp. VLSI Circuits*, pp. 250 251, June 2015.

[5] S. Mathew, et al., "A 0.19pJ/b PVT-Variation-Tolerant Hybrid Physically Unclonable Function Circuit for 100% Stable Secure Key Generation in 22nm CMOS," *IEEE ISSCC Dig. Tech. Papers*, pp. 278-279, Feb. 2014.

[6] B. Karpinskyy, et al., "Physically Unclonable Function for Secure Key Generation with a Key Error Rate Of 2E-38 in 45nm Smart-Card Chips," *IEEE ISSCC Dig. Tech. Papers*, pp. 158 160, Feb. 2016.

[7] M. Wan, et al., "An Invasive-Attack-Resistant PUF Based On Switched-Capacitor Circuit," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 8, pp. 2024 2034, Aug. 2015.

[8] M. Z. Straayer and M. H. Perrott, "A 12-bit, 10-MHz bandwidth, continuous-time ΔΣ ADC with a 5-bit, 950-MS/s VCO-based quantizer," IEEE J. Solid-State Circuits, vol. 43, no. 4, pp. 805-814, April 2008.