A Metal-Via Resistance based Physically Unclonable Function with Backend Incremental ADC

Beomsoo Park, *Student Member, IEEE*, Domenic Forte, *Senior Member, IEEE,* Mark Tehranipoor, *Fellow, IEEE*, and Nima Maghari, *Senior Member, IEEE*

***Abstract*— This paper presents a novel physically unclonable function (PUF) for security authentication. Instead of using the variation of transistors or PDK provided passive components as entropy source, the parasitic resistance created between metal and via layers is used as the static entropy source. A symmetric bridge configuration consisted with the parasitic resistance creates the necessary voltage difference for comparison. An accurate backend incremental analog-to-digital converter (IADC) is implemented to convert the voltage difference into a digitized value. The operation of the IADC allows to achieve a good native instability. Two different types of layout structures are implemented to create the necessary parasitic resistance and compared. Fabricated in a 65nm process, the prototype PUF achieves a native instability and bit error rate of less than 1.45% and 0.12% with 5000 repeated evaluations. The proposed design shows 0.58%/0.1V and 0.53%/10ºC bit error across the voltage and temperature range of 0.9 to 1.4V and 0ºC to 85ºC, respectively without any stabilization techniques. The distance ratio between intra-die and inter-die Hamming Distance is above 305×.**

***Index Terms*—Parasitic resistance, hardware security, physically unclonable function (PUF), stability, temperature and voltage variation, hamming distance, stabilization techniques.**

I. Introduction

PHYSICALLY unclonable functions (PUFs) have emerged as a compact and stable chip level solution for security authentication [1]-[3]. Although previous approaches using nonvolatile memory to secure the identity of the chip have proven to be effective, such approaches are often costly, consumes large amount of power and area, and are vulnerable to invasive attacks. Instead of storing the identity in digital memory, PUFs self-generate the identity by leveraging the process and manufacturing variations. The unpredictability of the variation enables each PUF to generate its own unique and stable response to a challenge [2]. By using process and manufacturing variations, predicting or extracting the identity of the chip becomes extremely difficult and allows PUFs to provide high level of security.

Designing a PUF can typically be divided into four steps as shown in Fig. 1(a). First is to find the entropy source and convert the entropy source into a digitized value, which is fundamentally a 1bit analog-to-digital converter (ADC), using either local digitization or differential comparison. Local digitization generates the entropy source in a single-ended structure and amplifies locally to create the PUF response [10]. On the other hand, differential comparison compares two identical circuits with the same functionality using either a comparator, positive feedback, or D flip-flop (DFF) to generate the PUF response. Following digitization, most PUFs use a stabilization process such as temporal majority voting (TMV), trimming, remapping, reconfiguration, among others to improve the stability [4]-[16]. Finally, error-correcting code (ECC) is used to achieve 100% reliable PUF outputs.

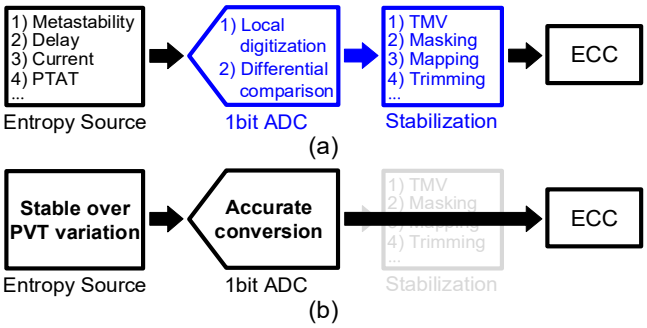

Fig. 1. Design steps of PUF. (a) Typical PUF design process and (b) skipping stabilization step by using an accurate self-programmable 1bit ADC.

Regardless of the entropy source and the type of digitization, PUF stability is determined depending on how well the PUF cells with small mismatch are handled and resolved. These either need to be precisely evaluated using a high-resolution digitization method or discarded/corrected using stabilization technique. However, many stabilization techniques improve the stability with the sacrifice of increased data processing time. Sometimes, the processing time and steps are more than the evaluation time itself [4]. In this design, we aim to leverage an entropy source that is relatively insensitive to PVT variations as well as an accurate 1bit ADC structure to achieve good native instability and bit error rate (BER) in effort to skip stabilization and simplify the PUF design as shown in Fig. 1(b).

Rather than using transistors as the main entropy source, this paper proposes a new type of weak PUF that utilizes passive components [17]. Instead of using PDK provided passive components such as poly/diffusion resistors and all metal type capacitors, the parasitic resistance created between metal and via interconnections are used as the entropy source. Two different type of layout structures, M-shape version and S-shape version, for PUF cells using multiple metal and via

Manuscript submitted March 10, 2021. This work was supported by the National Science Foundation (CCSS-1610075).
The authors are with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA (e-mail: beomsoo0927@ufl.edu).

TABLE I
CATEGORIZATION OF THE STATE-OF-THE-ART DESIGNS

	Hybrid [4], [5]	SRAM [6]	Ring Oscillator [7], [15]	NAND [8]	2TR/inverter [9], [10]	Current Mirror [11], [12]	Leakage [13]	PTAT [14]	Contact [16]
Entropy Source	Delay & metastability	Metastability	Delay	Threshold voltage	Threshold voltage	PMOS/NMOS current ratio	Leakage current	Threshold voltage	Contact formation
Digitization (1bit ADC)	Differential comparison	Differential comparison	Differential comparison	Local digitization	Local digitization	Local digitization	Differential comparison	Differential comparison	Local digitization
Stabilization	Masking, TMV, burn-in	HCI burn-in	Dynamic threshold / Calibration	Mapping, SMV	TMV, reconfiguration	Temperature compensation	TMV, Remapping	TMV, Calibration	Resistance comparison

layers of a 65nm process are implemented to build the necessary parasitic resistance for comparison.

Typically, stabilization techniques require to store an initial evaluation of the PUF array in order to detect the unstable (small mismatch) PUF cells followed by a final evaluation with the stabilization technique applied. Some even require voltage or temperature sweep that increases the post processing time. Instead of applying additional stabilization method, an input dependent self-programmable incremental ADC (IADC) is employed to perform the digitization. The implemented IADC inherently determines whether a certain PUF cell has small mismatch or not and increases its resolution accordingly to mitigate the noise from affecting the PUF output. Additional steps for data storage and comparison to find the unstable bits is unnecessary. Although the implemented IADC throughput is low and consumes large area, some system-on-a-chips (SoCs) use IADCs as high-resolution ADCs with low offset and noise to measure or calibrate voltage, current, temperature, among many others [18]-[20]. In those SoCs, the proposed PUF is a good candidate for security authentication as the existing IADC can be modified and reused to minimize the cost and area overhead. Thanks to the inherent noise averaging provided by the IADC, the prototype PUF achieves a native instability and BER of less than 1.45% and 0.12% for both versions.

This paper is organized as follows. Section II overviews the state-of-the-art PUFs based on the design steps shown in Fig. 1(a). In section III, details of the proposed metal-via resistance (MVR) based PUF and the architecture of the design is discussed. Section IV goes over the overall operation of the MVR PUF with the backend IADC. Measurement results with comparison to previous state-of-the-art designs are shown in section V and conclusions are made in section VI.

II. OVERVIEW OF THE STATE-OF-THE-ART DESIGNS

With the pursue of developing sturdy PUFs, conventional PUFs like SRAM PUFs, arbiter PUFs, and ring oscillator (RO) PUFs have become outdated [21]-[23]. These PUFs tend to consume large amount of area, have low stability, and are susceptible to modeling attacks [24]. Recently developed PUFs emphasize in utilizing entropy sources that create large mismatch or apply stabilization techniques to substantially improve the stability [4]-[16].

The hybrid delay/cross-coupled based PUF is an extension of SRAM PUFs where both the delay and metastability are used as entropy source [4], [5]. Differential comparison using positive feedback between two inverters is applied to convert the entropy source. While the native instability of 30% is quiet poor, using techniques such as TMV, burn-in hardening, and dark bit masking reduces the instability below 5% and ECC finally resolves the remainder of the unstable bits [4]. A different SRAM based PUF using hot carrier injection (HCI) burn-in as stabilization method showed that a near 0% BER can be achieved [6].

The RO based PUF using oscillation collapse unlike conventional RO designs use even number of inverters in two different paths [7]. The delay difference between the two paths eventually causes the oscillation to collapse and provide the PUF output. A dynamic thresholding technique is implemented that evaluates the number of cycles for the PUF to finish its operation. The ones with long collapse time reveal that noise rather dominates the response than mismatch and is discarded by the threshold value. Thus, a tradeoff exists between the number of discarded bits and bit instability.

The NAND based PUF and 2-TR/inverter based PUFs employ similar structures which use local digitization as its conversion method [8]-[10]. These PUFs first generate a voltage through a voltage divider configuration in its first stage. The second stage compares and amplifies the difference between the generated voltage and the switching voltage of the second stage. The rest of the stages enable the conversion to its full rail. Using static operation and local digitization allows the native instability to be superior compared to delay or metastability based PUFs. Nonetheless, additional stabilization methods are used to further reduce the instability.

The current mirror based PUF uses the difference between the PMOS and NMOS mirrored current and amplifies the current difference using the large output impedance of the cascoded transistors [11], [12]. Due to the static and monostable characteristic of the architecture, the instability of below 3% is achieved without using any stabilization methods. The leakage based PUF utilizes the delay time for the leakage current to charge a certain node from ground to the supply voltage and compares cells from two different arrays using a DFF [13]. A remapping technique along with TMV is used to stabilize the PUF. The remapping enables to select two PUF cells with sufficient delay difference to reduce the instability to below 0.1%.

The PTAT based PUF compares the voltage difference between a pair of PTAT circuits which is robust against voltage and temperature variation [14]. Differential comparison is performed using a sense amplifier. An off-chip offset calibration is applied to remove the offset of the sense amplifier which can bias the output. The contact based PUF violates the contact DRC rules to achieve a polarized resistance (open or short circuit) distribution which enables to achieve 0% BER [16]. A resistance comparison method is implemented to disregard the PUF cells that have resistive contacts.

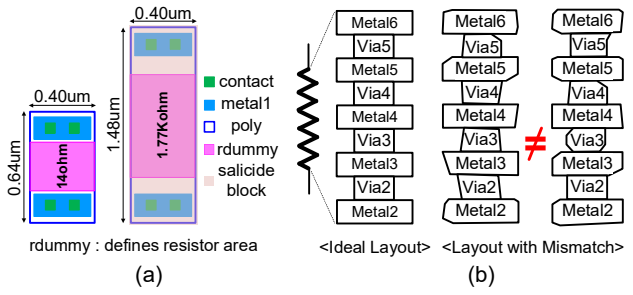

Fig. 2. (a) PDK provided poly resistors in its minimum size for the given 65nm process and (b) layout based parasitic resistance.

Summarization of the entropy source, digitization method, and stabilization technique of the state-of-the-art designs is shown in Table I. While stabilization techniques significantly help to enhance the stability of the PUF, most require extreme amount of pre/post data processing to reduce the instability.

III. Proposed MVR Based PUF

A. Parasitic Resistance as Entropy Source

Passive components such as resistors can be utilized to operate as PUF. However, the PDK provided resistors such as the poly resistors with or without silicide consume large amount of area even with its minimum size as shown in Fig. 2(a). Moreover, these resistors are often relatively well matched and also occupy the poly and metal1 layers that are necessary for transistors. Consequently, using PDK provided resistors result in large unit PUF cell size [16]. Other PDK provided resistors such as N-well resistors and diffusion resistors have similar issues and is not an optimum choice as PUF elements. In this work, the parasitic resistance between the interconnection of multiple layers of metals and vias are leveraged to create the necessary entropy source for PUF cells. Although some previous works showed the potential of using parasitic resistance as the entropy source, those require large area, large current, or an external voltage-meter and thus is not suitable for SoC application [25],[26].

In essence, via is one of the least controlled elements in a process and its shape can vary from the ideal shape significantly due to its small vertical spacing. Therefore, the via mismatch due to the process and manufacturing variation create the necessary difference that can be utilized as PUF elements as shown in Fig. 2(b). Using metal and via interconnections as entropy source can be significantly more beneficial than PDK provided resistors when built with multiple layers as it creates more deviations which is imperative in PUF designs. As poly and metal1 are used for internal routing and transistors, metals 2 through 6 which have the same design rules in the given process, are used to build the MVRs.

The basic design steps to maximize and increase the mean and the variation of the MVRs in a specified area is as follow : 1) Minimum thickness, spacing, and inclusion rules provided by the process is used. 2) A single via is used instead of using multiple vias for connections between different metals. 3) As aforementioned, metals 2 through 6 with the same design rules

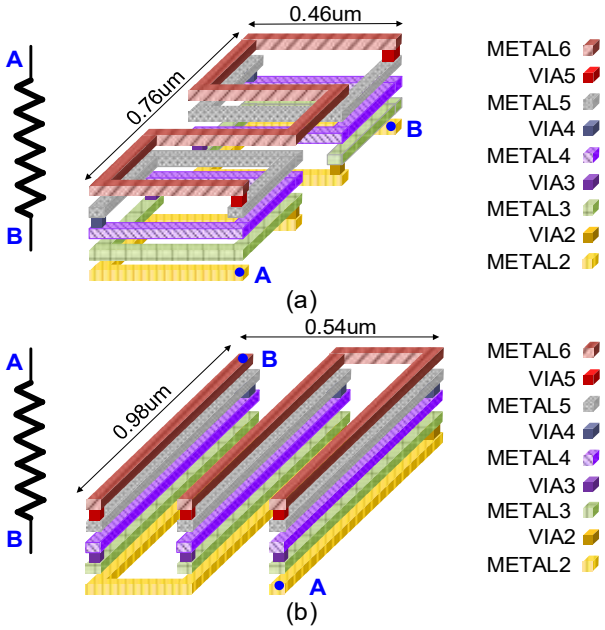

Fig. 3. Three-dimension layout view of MVR. (a) M-shape version and (b) S-shape version.

are stacked on top of poly and metal1 to build the MVRs. With these basic steps, two different versions of layout, M-shape version and S-shape version, are implemented for comparison as shown in Fig. 3. The M-shape version adopts a spiral type of layout while the S-shape version connects three of the stacked metals from metal2 to metal6 in series. A compact area of 0.46um × 0.76um and 0.54um × 0.98um is used for M-shape and S-shape, respectively. Comparing the two structures, M-shape uses 31 metal layers (every edge counted) and 8 via layers while S-shape uses 17 metal layers and 12 via layers. Post simulation result shows metal parasitic resistance of 42ohm for M-shape and 45ohm for S-shape. Considering that via parasitic resistance is not extracted through post simulation, adding the resistance value provided by the process gives a total of 54ohm and 63ohm (each via ideally equals 1.5ohm) for M-shape and S-shape, respectively. Although the mean value seems small, the variations, especially via variations, cause the MVRs to deviate from the mean value significantly.

B. Symmetric Bridge Configuration with MVRs

A symmetric bridge configuration is implemented using the MVRs to create the necessary voltage difference for comparison as shown in Fig. 4(a). The output voltage of the symmetric bridge configuration is

$$VP - VN = g_m V_B \frac{R2 \cdot R3 - R1 \cdot R4}{R1 + R2 + R3 + R4} \quad (1)$$

where gm is the transconductance of the bias transistor, MPB. Although this structure uses four MVRs, the mismatch or the noise of the bias transistor does not affect the PUF output as it is commonly shared between the two branches and is used in this design. To verify the effect of the bias transistor, noise and

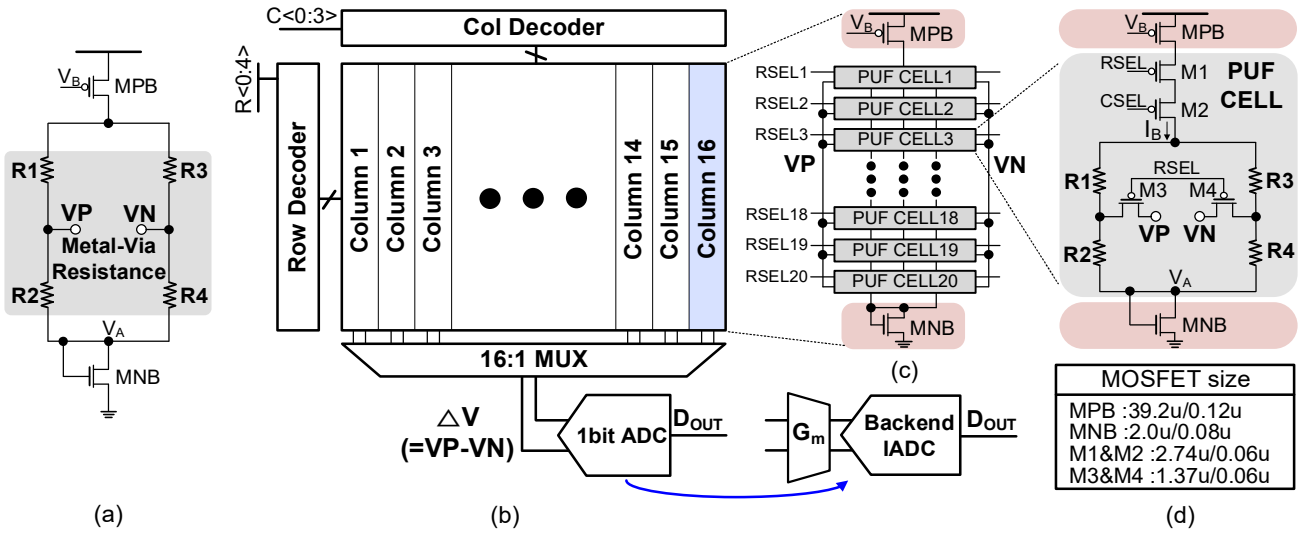

Fig. 4. (a) Symmetric bridge configuration using MVRs. (b) Overall 16 × 20 PUF array with backend IADC. (c) Column configuration of MVR PUF. (d) Unit cell of MVR PUF.

offset simulation is performed with the noise and mismatch parameters of the resistors turned off. Simulation results show little to no effect of the bias transistor on the output due to the common mode appearance of the noise (less than 0.1% of the total integrated noise) and offset. The symmetric bridge configuration enables the difference to be only dependent on the relative difference of the 4MVRs.

Further noise analysis of the differential configuration is as follow. The overall integrated noise from the symmetric bridge configuration is

$$\overline{V_{n,T}^2} = \sum_{i=1}^{4}(4kTRi \cdot BW \cdot Gi^2) + \overline{V_{n,M}^2} \approx \sum_{i=1}^{4}(4kTRi \cdot BW \cdot Gi^2) \quad (2)$$

where the first term represents the thermal noise due to the four MVRs and the second term represents noise from the bias transistor. k is the Boltzmann constant, T is the temperature in Kelvin, BW is the bandwidth of interest, and Gi is the gain factor for each resistor considering the bridge configuration. The gain factor for each resistor is as below

$$G1 = G3 = \frac{R2 + R4}{RT}, \quad G2 = G4 = \frac{R1 + R3}{RT} \quad (3)$$

$$RT = R1 + R2 + R3 + R4 \quad (4)$$

The voltage difference generated from the bridge configuration should be large than the overall noise level to show stable PUF response. The value of (2) can be effectively modeled as the noise source placed at the input of the IADC. Due to the averaging (oversampling) nature of the IADC, the noise is suppressed depending on the number of cycles it takes to reach a decision, as described in Section IV.

An advantage of the proposed PUF is its resilience to physical attacks. With the development of PUFs, diverse invasive attacks such as direct probing and focus ion beams are used to attempt and extract internal information of the PUF. Thus, protection against invasive attacks have become an important issue [27]. Adding detection methods to identify the attacks or using additional metal layers for shielding to prevent the attacks are proposed but has its limits [27]-[29]. These techniques are sensitive to voltage and temperature variation and could rather provide valuable information to attackers to apply non-invasive attacks. The proposed MVR PUF is intrinsically resilient to physical attacks as metal and via layers are used to build the resistance. The resistance value can alter due to either the decapsulation process necessary for probing attacks or the added impedance of the prob noting the centimeter scale of the probe compared to the nanometer scale of metals and vias [30]. This could eventually result in changing the PUF output. Furthermore, as the typical difference between VP and VN node is in the order of few millivolts, it is difficult to read these nodes accurately using either E-beam or backside probing noting that the MVR PUF does not provide discrete digital outputs like most PUFs. Given that the MVR PUF shape acts as a small antenna, a proper shielding by other metal layers (metals above metal 6) would help reduce electromagnetic interference as well [31].

C. *Overall Architecture of MVR based PUF*

The overall architecture of the design is shown in Fig. 4(b). A 16 × 20 PUF array along with row and column decoders, a 16:1 multiplexer (MUX), and a backend readout circuit consist the entire design. The voltage difference created by the differential structure, ΔV, is evaluated using a backend 1bit ADC that functions as a resolution programmable comparator. The global 1bit ADC with an input transconductance (G_m) and a backend IADC is used to readout the entire PUF array to minimize the overall area and power. The operation of the backend IADC provides a precise binary output allowing to remove additional stabilization.

Each column consists of a shared current source, MPB, and a shared diode-connected transistor (used to isolate the MVRs from ground), MNB, for area efficiency as shown in Fig. 4(c).

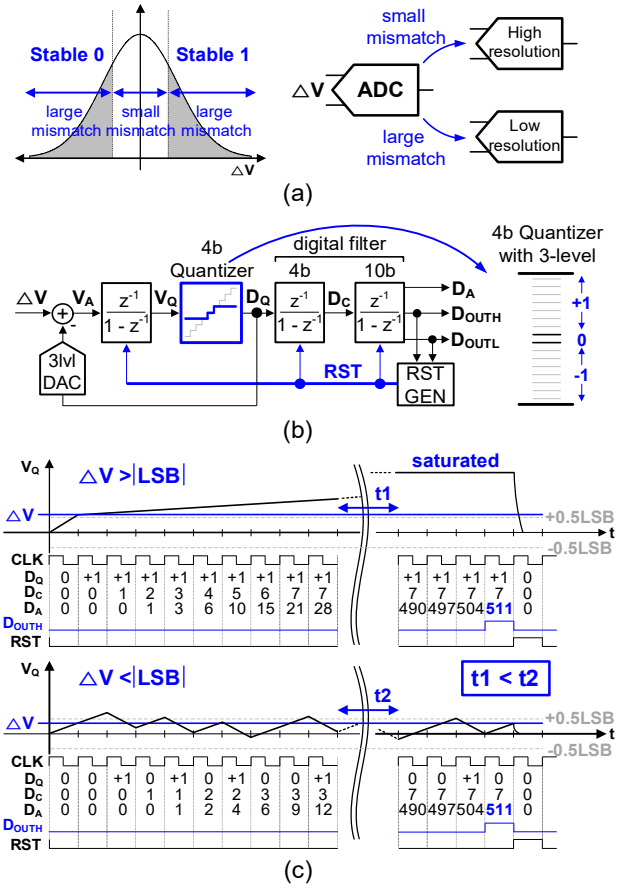

Fig. 5. (a) Distribution of ΔV and required resolution of ADC depending on ΔV. (b) Self-programmable 1st order IADC. (c) Operation of 1st order IADC depending on ΔV.

A unit PUF cell consists of column and row selection switches and 4 MVRs as shown in Fig. 4(d). The series switches of M1 and M2 enable only one of the 320 PUF cells to operate.

IV. Operation of MVR Based PUF with IADC

IADCs are widely used for DC precision measurements where high accuracy and low offset are required. To increase the signal-to-noise ratio (SNR) of the IADC, higher order loop filters, multi-bit quantizers, and large number of evaluation cycles are used [18]-[20]. The inherent averaging principle provided by the IADC enables to average out the noise and provide an accurate output. IADC thus is an optimum candidate to evaluate the voltage difference of the proposed MVR PUF. Other types of ADCs such as pipeline, successive approximation, and delta-sigma modulator with very low offset could possibly be used as the readout circuit for the proposed MVR PUF with an aid of a buffer like the Gm cell in this design between the MVR PUF output and the ADC.

A. Self-programmable IADC as Readout Circuit

Like most entropy source, the voltage difference, ΔV, of the MVR PUF follows a gaussian distribution as shown in Fig. 5(a). For a large ΔV, a low-resolution readout circuit is sufficient to evaluate ΔV into a digitized value as it typically remains stable

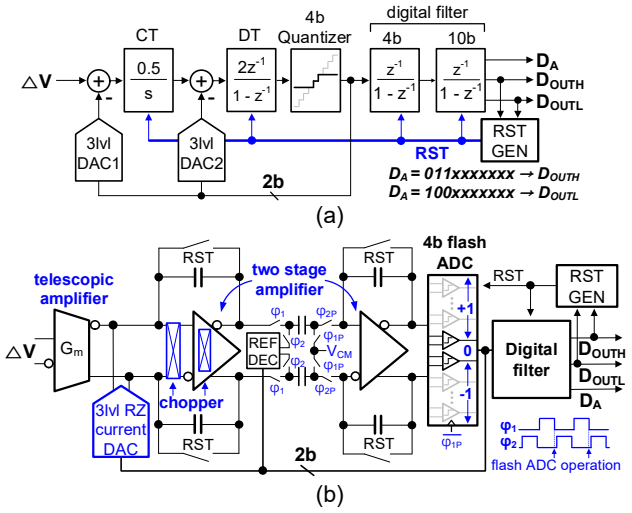

Fig. 6. Implemented self-programmable 2nd order IADC. (a) System level design and (b) schematic level design.

regardless of noise and PVT variation. However, a high-resolution readout circuit is required to precisely evaluate small ΔV values. Thus, a readout circuitry where the resolution is self-programmable depending on the ΔV highly increases the readout efficiency. In order to make the IADC self-programmable, the proposed IADC employs a backend 2nd order digital filter that resets the IADC after the digital filter reaches a defined maximum or minimum threshold value. Generating the reset signal (RST GEN of Fig. 5(b)) in such way allows for large ΔV to operate for a short time as it quickly reaches the threshold. For small ΔV, the operation cycle is naturally extended as it requires longer evaluation time to average out the noise and depict a precise output.

To illustrate the operation principle, a 1st order IADC with a 4-bit quantizer followed by a 2nd order digital filter that generates the reset signal (RST) is shown in Fig. 5(b) for simplicity noting that the real implementation employs a 2nd order IADC. Due to the limited ΔV range generated by the PUF, only the mid two levels of a 4-bit quantizer are used to create a scaled 3-level quantizer (+1/0/-1) as shown on the right of Fig. 5(b). Removing the other levels of the quantizer possibly saturates the integrator in presence of large ΔV but brings benefits to the design which is explained further in the paper. The maximum and minimum threshold value using a 10-bit digital filter considering signed number is +511/-512. Once the digital filter reaches either of these values, the flag signals D_{OUTL} or D_{OUTH} indicating a PUF output of 0 or 1, triggers to generate RST and finishes the evaluation.

The overall operation considering the two cases where ΔV is larger or smaller than the LSB of the quantizer is shown in Fig. 5(c). If ΔV is larger than the LSB, the quantizer output, D_Q, mostly outputs +1 (or -1 depending on the polarity of ΔV). As a result, the 2nd digital filter output, D_A, operating as an accumulator reaches the threshold value quickly and resets the IADC. If ΔV is smaller than the LSB, the IADC provides a stream of +1/-1s and 0s and the operation takes longer than the previous case. The extended operation time for small ΔV helps

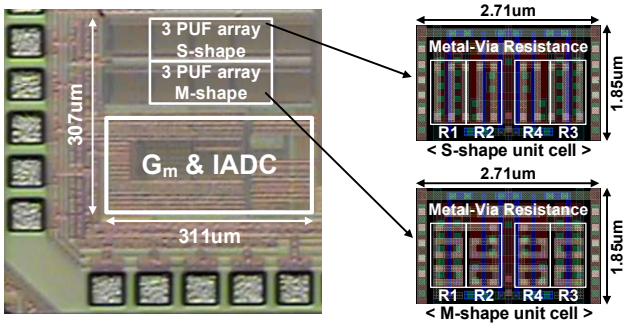

Fig. 7. Die photo and layout of the PUF unit cells.

to substantially reduce the noise through the averaging process and eventually improve the overall bit stability against noise.

B. Implemented 2nd Order IADC

A 2nd order IADC is implemented in the design to further increase the SNR as shown in Fig. 6. 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 scaled 3-level quantizer and a 2nd order digital filter as shown in Fig. 6(a). Instead of waiting for D_A to accumulate to the threshold value of +511/-512, the D_{OUTH} and D_{OUTL} flags are triggered when the three MSBs of D_A are either 011 (+384) and 100 (-385). The three MSBs are sufficient enough to show whether a certain ΔV has the tendency to be either a 1 or 0 PUF output and reduces the evaluation time. After D_{OUTH} or D_{OUTL} triggers, the IADC resets itself and the next PUF element is selected for evaluation in an asynchronous fashion.

The schematic level of the 2nd order IADC is shown in Fig. 6(b). A G_m cell is used to provide a high impedance and isolation between ΔV and the input of the IADC. The G_m converts the ΔV to current and charges the integrating capacitor of the 1st integrator. A telescopic amplifier with large PMOS input pair is used for the G_m while a two-stage amplifier with PMOS input pair is used for the 1st integrator to minimize the flicker noise and the offset. A chopper is implemented on the 1st integrator to further suppress the flicker noise and offset. It is worth noting that a chopper can be added for the G_m cell as well. However, this causes unwanted switching artifacts on the MVR PUF cell output that rather deteriorates the PUF stability.

The G_m cell is designed with an assumption that the 1σ variation of the ΔV of the MVR PUF, $\Delta V_{1\sigma}$, is 2mV. With this initial assumption, the following equation is used to relate the $\Delta V_{1\sigma}$ to the 1LSB of the 4-bit quantizer to obtain G_m

$$G_m = \frac{V_{LSB} \times C_{\text{int}}}{\Delta V_{1\sigma} \times t} \quad (5)$$

where V_{LSB} represents the 1LSB of the 4-bit quantizer, C_{int} represents the integrating capacitor of the 1st integrator, and t represents the operation time. With V_{LSB}=0.1V, C_{int}=1.2pF, and t=20ns, the necessary G_m is 3mA/V. During measurement, the G_m was optimized around 5mA/V for better energy efficiency. As no chopper is used for the input G_m, the G_m cell is sized so that the noise and offset contribution is less than 0.01LSB and

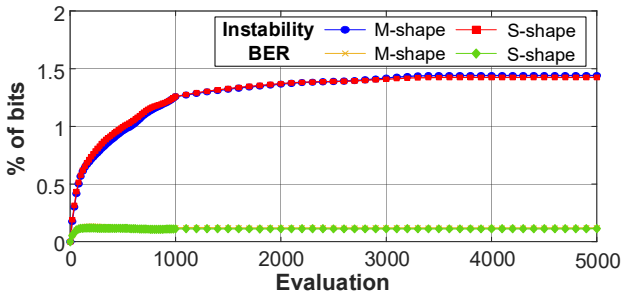

Fig. 8. Instability and BER with 5000 repeated readouts at nominal condition.

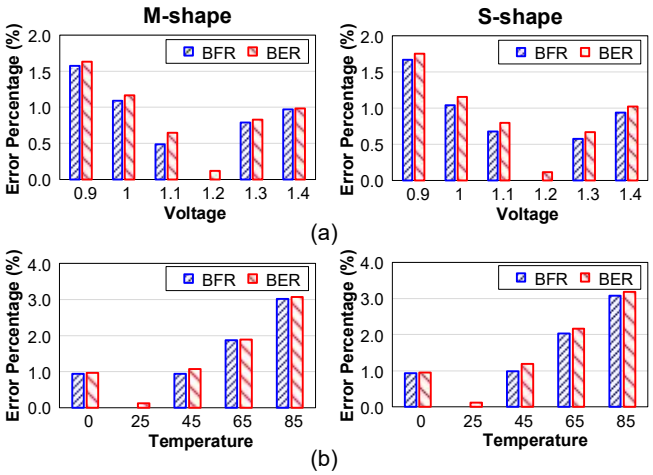

Fig. 9. (a) BFR and BER versus voltage variation and (b) BFR and BER versus temperature variation with golden data at 1.2V and 27°C.

0.075LSB, respectively which is the main source of the overall noise and offset of the readout circuit.

A flash ADC with two mid-level comparators is used as the 4-bit quantizer to create the scaled 3-levels. As previously mentioned, such approach causes the integrators to saturate for large ΔV. However, as the purpose of using IADC for PUF evaluation is to operate as a precise comparator providing a binary output, the linearity and swing requirements of the G_m and integrators are not of a concern and thus relaxes the design. In addition, removing most of the comparators simplifies the digital filter design and allows to use a single 3-level return-to-zero (RZ) current digital-to-analog converter (DAC) as the feedback DAC [32].

V. Measurement Results

The prototype chip is fabricated in a 65nm CMOS process. The die photo and layout of the PUF unit cells are shown in Fig. 7. Three arrays using the two MVR versions are implemented in a chip along with a global IADC for evaluation. The unit PUF cell size is 2.71um × 1.85um which is equivalent to 1187F². As explained above, the MVR consisted of metal 2 through 6 are stacked on top of the transistors (poly and metal1) to optimize the PUF unit area. The nominal condition stated in this section is supply voltage of 1.2V and temperature of 27°C.

A. Bias Current Optimization for Symmetric Bride Circuit

To find the optimum bias current for the symmetric bridge

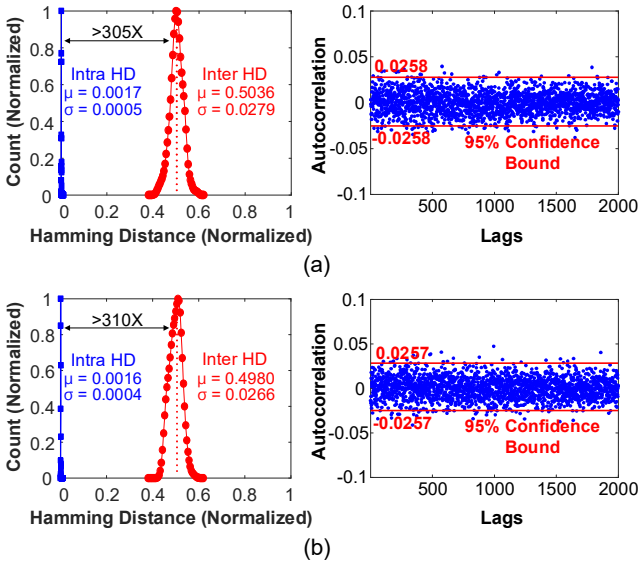

Fig. 10. Measured intra/inter hamming distance and auto-correlation function to evaluate uniqueness and randomness for (a) M-shape and (b) S-shape.

circuit considering both power consumption and performance, 6 arrays from 6 different dies (1array from each die) are tested for both layout version. The instability and BER are tested with bias current from 5uA to 100uA at the nominal condition. Each array is repetitively read out 1000 times for the evaluation. Evaluation results showed that the performance does not change much between 10uA to 100uA for both versions. For currents lower than 10uA, the instability and BER deteriorates and therefore 10uA is used as the bias current for evaluation.

B. PUF Stability

Stability against noise and voltage/temperature variations is an important parameter to evaluate PUF. To verify the impact of noise, 18 PUF arrays from 6 different dies (3 arrays per die, each containing 320 MVR PUF cells) for each version is measured at the nominal condition. The 320 MVR PUF bits are repetitively read out 5000 times for the evaluation. Fig. 8 shows the measured cumulative bit instability and BER of both versions. Regardless of the type of MVR, the accumulated instability and BER are similar for both versions. Both versions achieve raw instability of below 1.45% and BER of below 0.12% without using any stabilization techniques which is equivalent to 4.61 unstable bits per 320 bits. The similar results of the two versions reflect that the instability and BER is rather limited by the noise level of the IADC. With a higher resolution IADC, the instability and BER is expected to further decrease.

To evaluate the stability against voltage and temperature variations, the PUF array is measured across the range of 0.9V and 1.4V and 0°C and 85°C, respectively and compared with the nominal condition measurement results using bit flip rate (BFR) and BER. BFR indicates the percentage of bits measured at a certain voltage or temperature which differ from the golden key value measured at the nominal condition [14]. To compare with the golden key value, the average value after 5000 evaluation cycles is used to evaluated whether a certain bit is flipped or not. For voltage and temperature measurement, a

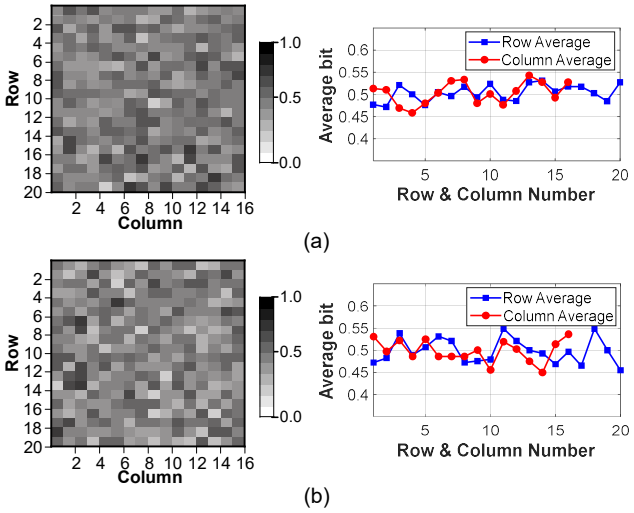

Fig. 11. Spatial distribution of 0s and 1s and row and column average bits for (a) M-shape and (b) S-shape.

TABLE II
NIST RANDOMNESS TEST

NIST Pub 800-22	Stream Length	No. of Runs	M-shape		S-shape	
			Avg. p-value	Pass?	Avg. p-value	Pass?
Frequency	320	18	0.568	YES	0.486	YES
Block Frequency	320	18	0.634	YES	0.477	YES
Runs	320	18	0.420	YES	0.440	YES
Longest run of ones	320	18	0.411	YES	0.383	YES
Cumulative Sum-1	320	18	0.633	YES	0.541	YES
Cumulative Sum-2	320	18	0.554	YES	0.579	YES
FFT	320	18	0.666	YES	0.372	YES
Nonoverlapping template	320 (m=4)	18	0.570	YES	0.501	YES
Serial-1	320 (m=3)	18	0.467	YES	0.551	YES
Serial-2	320 (m=3)	18	0.442	YES	0.579	YES
Approximated Entropy	320 (m=3)	18	0.484	YES	0.494	YES

total of six PUF arrays are tested (1 array per each die) for each version. The measurement results at 1.2V and 27°C is used as the golden key for comparison as shown in Fig. 9. The resulting BFR and BER sensitivity to supply voltage variation for M-shape version is 0.52%/0.1V and 0.54%/0.1V and for S-shape version is 0.55%/0.1V and 0.58%/0.1V, respectively. Both versions show similar results of 1.76bit flips with an increment/decrement of 0.1V. The resulting BFR and BER sensitivity to temperature variation for M-shape version is 0.51%/10°C and 0.52%/10°C and for S-shape version is 0.51%/10°C and 0.53%/10°C, respectively. Both versions show similar results of 1.63bit flips with an increment/decrement of 10°C.

C. Uniqueness and Randomness

The uniqueness and randomness of the PUF is another important parameter for evaluation. Hamming distance (HD) is used to assess the uniqueness of the design. The intra-die and inter-die HD of the two versions are evaluated with the measured results of the 18 PUF arrays at nominal condition. As

TABLE III
PERFORMANCE COMPARISON WITH THE STATE-OF-THE-ART DESIGNS

	This Work (M-shape / S-shape)	ISSCC'14 [4]	CICC'20 [6]	ISSCC'16 [8]	JSSC'20 [10] c)	JSSC'18 [12]	ISSCC'18 [13] d)	JSSC'16 [14]	JSSC'20 [15]	JSSC'20 [16]
Technology (nm)	65	22	130	45	65	40	180	65	28	130
PUF Cell Area/Bit	5.01 um^2 1187 F^2	4.66 um^2 9628 F^2	8.40 um^2 497 F^2	5.29 um^2 2613 F^2	2.38 um^2 562 F^2	5.83 um^2 3643 F^2	28.84 um^2 890F^2	3.07 um^2 726 F^2	26 um^2 33163 F^2	42.84 um^2 2535 F^2
Native Unstable Bits (# of evaluations)	1.44% / 1.42% (5000)	30% (5000)	2.71% (1000)	--	2.95% (2000)	2.55% (500)	5.62% (1000)	6.54% (500)	--	0.0054% (--)
Native BER	0.12% / 0.11%	8.3%	0.29%	0.1%	0.3%	0.81%	0.69%	--	1.4%	<2.3x10^{-8}
Unstable Bits after Stabilization	--	< 5.0% a)	~0%	--	0.024%	--	0.08%	2.0%	--	--
BER after Stabilization	--	0.97% a)	~0%	--	0.002%	--	0.02%	--	0.078%	--
Tested Condition: Temp (°C)	0 ~ 85	25 ~ 50	-40 ~ 120	-25 ~ 85	-55 ~ 125	-40 ~ 125	0 ~ 85	0 ~ 80	-40 ~ 125	-55 ~ 260
Tested Condition: Supply (V)	0.9 ~ 1.4	0.7 ~ 0.9	0.5 ~ 0.7	--	0.7 ~ 1.4	0.8 ~ 1.0	1.2 ~ 1.8	0.6 ~ 1.2	0.4 ~ 1.3	1.35 ~ 1.65
Bit Errors per 10°C	0.52% / 0.53%	--	~0%	0.27%	0.12%	0.32%	--	0.44%	0.005%	--
Bit Errors per 0.1V	0.54% / 0.58%	0.49%	~0%	--	0.06%	0.72%	--	0.13%	0.055%	--
Normalized Mean Inter HD e)	0.5036 / 0.4980	0.49	0.4873	0.498	0.4998	0.4907	0.50	0.5001	0.4994	0.4999
Normalized Mean Intra HD e)	0.0017 / 0.0016	--	0.0041	--	0.00049	0.0049	0.00685	0.0045	0.0007	--
Inter/Intra HD Distance Ratio e)	305 / 311	19 b)	119	--	1020	102	73	110	709	--
PUF Energy/bit (pJ/bit)	18 (without IADC) 746.5 (with IADC)	0.19 (TMV15)	0.015 (0.6V)	--	0.015	0.056	3.6	6.02 (TMV11)	2.15	0.654

a) TMV15, burn-in & dark bit applied b) Supply voltage of 0.7~0.9 used c) LP mode d) Footed version
e) Stabilization applied results for the ones that use stabilization

shown in Fig. 10, the mean value of the intra-die HD for both versions is 0.0017 and 0.0016, respectively while the mean value of the inter-die HD is 0.5036 and 0.4980 which is near the ideal value of 0.5. Without any stabilization, the separation provided by M-shape and S-shape versions between intra and inter-die HD is well over 305× and 310×, respectively. The auto-correlation function is another evaluation method. The low spatial auto-correlation bound of 0.0258 and 0.0257 which is near the ideal value of 0 confirms the randomness of the MVR PUF as shown in Fig. 10. The NIST randomness test is performed for the 320bit outputs from 18 PUF arrays (5760 bits) for both versions and pass all the sub tests that suits the data size [33]. The results are summarized in Table II.

In addition, spatial distribution of the digital bits averaged across 18 PUF arrays is shown in Fig. 11 [14]. The distribution reveals that there is no systematic bias indicating that the output is independent from any type of layout patterns. Moreover, the digital bits averaged across each row and column is shown in Fig. 11. The result is around the ideal value of 0.5 which proves that the MVR PUF has no systematic pattern and no gradient effects securing independency from process variations.

D. *Impact of Aging*

The impact of device aging is an essential factor to consider for PUF stability. The major factor for aging is hot carrier injection and bias temperature instability [12]. Accelerated aging test is performed by increasing the supply voltage to 1.38V (15% of the nominal condition) and at 125°C for both the MVR PUF and IADC [34]. The test is performed for 40 hours and measured every 4 hours to evaluate the number of bit flips compared to the initially measured data as shown in Fig. 12. Over a 40-hour period, the number of bit flips is maintained

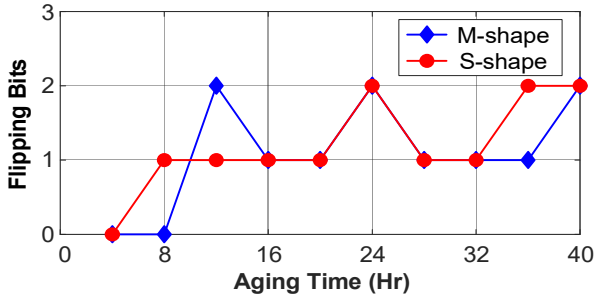

Fig. 12. Number of flipping bits during the accelerated 40-hour aging test.

below 2 bits similar to the state-of-art designs [12], [14].

E. *Energy efficiency*

The power consumption of a unit PUF cell and the IADC (including all other peripheral circuits) is 12uW/bit and 486uW, respectively. As previously mentioned, only one of the PUF cell is turned on while the rest of the 319 PUF cells are turned off during evaluation. The IADC operates at 50MHz with an average of 75cycles/bit which results as 666.7kHz/bit. Thus, the energy consumption of the MVR PUF without and with IADC is 18pJ/b (calculated with just the static power of 12uW/bit) and 746.5pJ/b (calculated with all power added), respectively. Although the energy consumption is large due to the low throughput of the IADC, security authentication is not frequently required and repeated in SoC applications and thus the concern of power overhead is less than regular IPs. Thus, the bias voltages of the PUF and the IADC are configured to reduce the static power consumption to below 10nW when security authentication is unnecessary. Moreover as mentioned

previously, in SoCs where IADC is used for various monitoring or interface application, the existing IADC can be shared and modified for the purpose of the MVR PUF digitization method to eliminate the need for dedicated IADC.

F. Comparison with State-of-the-Art Designs

Table III summarizes the measurement results and compares the results with the state-of-the-art designs. While most of the state-of-the-art designs apply stabilization techniques to minimize the instability and BER, the proposed MVR PUF achieves one of the best native instability and BER of below 1.45% and 0.12% without any stabilization. The BFR and BER change per 0.1V and 10ºC as well as the distance ratio between inter and intra-die HD is moderate compared to other designs even without using any additional stabilization methods.

VI. Conclusion

This paper presents a PUF based on the parasitic resistance formed by metal-via interconnections. Two different types of layout structures are implemented and compared to create the necessary parasitic resistance. Rather than using on-chip stabilization techniques or off-chip post processing to minimize the instability and BER which require pre/post data processing, the proposed design uses a backend IADC as the digitization method which can self-program the resolution depending on the input to minimize noise from affecting the stability. The proposed IADC is also applicable to other types of PUFs that generate voltage differences and require comparison such as the one in [14]. The native measurement results of instability, BER, distance between intra-die and inter-die HD, among others prove that good robustness can be achieved without using stabilization techniques. In addition, the proposed PUF is inherently resilient to invasive attacks due to its analog like operation and thus is a promising candidate for security authentication.

Acknowledgement

This work was supported by the National Science Foundation (CCSS-1610075).

References

[1] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, 2002, pp. 148-160.

[2] J. W. Lee, D. 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," in *Proc. IEEE Symp. VLSI Circuits*, Jun. 2004, pp. 176–179.

[3] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[4] 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," in *Proc. IEEE Int. Solid-State Circuits Conf.*, Feb. 2014, pp. 278–279.

[5] S. Satpathy *et al.*, "4-fJ/b delay-hardened physically unclonable function circuit with selective bit destabilization in 14-nm trigate CMOS", *IEEE J. Solid-State Circuits*, vol. 52, no. 4, pp. 940-949, Apr. 2017.

[6] K. Liu, H. Pu, and H. Shinohara, "A 0.5-V 2.07-fJ/b 497-F^2 EE/CMOS hybrid SRAM physically unclonable function with < 1E-7 bit error rate achieved through hot carrier injection burn-in," in *Proc. IEEE Custom Integrated Circuits Conference*, March 2020, pp. 1-4.

[7] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, "A physically unclonable function with BER <10^{-8} for robust chip authentication using oscillator collapse in 40 nm CMOS," in *Proc. IEEE Int. Solid-State Circuits Conf.*, Feb. 2015, pp. 254–255.

[8] B. Karpinskyy, Y. Lee, Y. Choi, Y. Kim, M. Noh, and S. Lee, "Physically unclonable function for secure key generation with a key error rate of 2E-38 in 45 nm smart-card chips," in *Proc. IEEE Int. Solid-State Circuits Conf.*, Jan. 2016, pp. 158–159.

[9] K. Yang, Q. Dong, D. Blauuw, and D. Sylvester, "A 553F^2 2-transistor amplifier-based physically unclonable function (PUF) with 1.67% native instability," in *Proc. IEEE Int. Solid-State Circuits Conf.*, Feb. 2017, pp. 146–147.

[10] D. Li and K. Yang, "A self-regulated and reconfigurable CMOS physically unclonable function featuring zero-overhead stabilization," *IEEE J. Solid-State Circuits*, vol. 55, no. 1, pp. 98-107, Jan. 2020.

[11] A. B. Alvarez, W. Zhao, and M. Alioto, "Static physically unclonable functions for secure chip identification with 1.9–5.8% native bit instability at 0.6–1 V and 15 fJ/bit in 65 nm," *IEEE J. Solid-State Circuits*, vol. 51, no. 3, pp. 763-775, Mar. 2016.

[12] S. Taneja, A. B. Alvarez, and M. Alioto, "Fully synthesizable PUF featuring hysteresis and temperature compensation for 3.2% native BER and 1.02 fJ/b in 40 nm," *IEEE J. Solid-State Circuits*, vol. 53, no. 10, pp. 2828–2839, Oct. 2018.

[13] J. Lee, D. Lee, Y. Lee, and Y. Lee, "A 445F^2 leakage-based physically unclonable function with lossless stabilization through remapping for IoT security," in *Proc. IEEE Int. Solid-State Circuits Conf.*, Feb. 2018, pp. 132-134.

[14] J. Li and M. Seok, "Ultra-compact and robust physically unclonable function based on voltage-compensated proportional-to-absolute-tempera ture voltage generators," *IEEE J. Solid-State Circuits*, vol. 51, no. 9, pp. 2192-2202, Sept. 2016.

[15] Z. Liang, H. Wei and T. Liu, "A wide-range variation-resilient physically unclonable function in 28 nm," *IEEE J. Solid-State Circuits*, vol. 55, no. 3, pp. 817-825, March 2020.

[16] D. Jeon, J. H. Baek, Y. Kim, J. Lee, D. K. Kim and B. Choi, "A physical unclonable function with bit error rate < 2.3 × 10^{-8} based on contact formation probability without error correction code," *IEEE J. Solid-State Circuits*, vol. 55, no. 3, pp. 805-816, Mar. 2020.

[17] B. Park, M. Tehranipoor, D. Forte, and N. Maghari, "A metal-via resistance based physically unclonable function with 1.18% native instability," in *Proc. IEEE Custom Integrated Circuits Conference (CICC)*, Apr. 2019, pp. 1-4.

[18] J. Markus, J. Silva, and G. C. Temes, "Theory and applications of incremental ΔΣ converters," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 51, no. 4, pp. 678-690, Apr. 2004.

[19] C.-H. Chen, Y. Zhang, T. He, P. Chiang, and G. C. Temes, "A micro-power two-step incremental analog-to-digital converter," *IEEE J. Solid-State Circuits*, vol. 50, no. 8, pp. 1796–1808, Aug. 2015.

[20] Y. Zhang, C. Chen, T. He and G. C. Temes, "A 16 b multi-step incremental analog-to-digital converter with single-opamp multi-slope extended counting," *IEEE J. Solid-State Circuits*, vol. 52, no. 4, pp. 1066-1076, Apr. 2017.

[21] G.-J. Schrijen and V. Van Der Leest, "Comparative analysis of SRAM memories used as PUF primitives," in *Proc. Des. Autom. Test Eur. Conf. Exhib. (DATE)*, 2012, pp. 1319–1324.

[22] R. Maes, V. Rozic, I. Verbauwhede, P. Koeberl, E. van der Sluis, and V. van der Leest, "Experimental evaluation of physically unclonable functions in 65 nm CMOS," in *Proc. IEEE ESSCIRC*, Sep. 2012, pp. 486–489.

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

[24] U. Ruhrmair *et al.*, "PUF modeling attacks on simulated and silicon data," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1876–1891, Nov. 2013.

[25] R. Helinski, D. Acharyya, and J. Plusquellic, "A physical unclonable function defined using power distribution system equivalent resistance variations," in *Proc. ACM/IEEE Des. Autom. Conf.*, 2009, pp. 676–681.

[26] J. Ju, R. Chakraborty, C. Lamech, and J. Plusquellic, "Stability analysis of a physical unclonable function based on metal resistance variations," in *Proc. IEEE Int. Symp. Hardware-Oriented Security Trust (HOST)*, 2013, pp.143-150.

[27] M. Wan, Z. He, S. Han, K. Dai and X. Zou, "An invasive-attack-resistant PUF based on switched-capacitor circuit," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 8, pp. 2024–2034, Aug. 2015.
[28] R. W. Melton, "Security method for data protection," U.S. Patent 8099783B2, Jan. 17, 2012.
[29] S. Manich, M .S. Wamser, and G. Sigl, "Detection of probing attempts in secure ICs," in *Proc. IEEE Int. Symp. Hardware-Oriented Security Trust (HOST)*, Jun. 2012, pp. 134–139.
[30] H. Wang, Q. Shi, A. Nahiyan, D. Forte, and M. M. Tehranipoor, "A physical design flow against front-side probing attacks by internal shielding," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 10, pp. 2152-2165, Oct. 2020.
[31] T. Sudo, H. Sasaki, N. Masuda, and J. L. Drewniak, "Electromagnetic interference (EMI) of system-on-package (SOP)," *IEEE Transactions on Advanced Packaging*, vol. 27, no. 2, pp. 304-314, May 2004.
[32] 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, Apr. 2008.
[33] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *Nat. Inst. Stand. Technol.*, vol. 800-22, no. Rev 1a, 2010.
[34] T. Yang, D. Kim, P. Kinget, and M. Seok, "In-situ techniques for in-field sensing of NBTI degradation in an SRAM register file," in *Proc. IEEE Int. Solid-State Circuits Conf.*, Feb. 2015, pp. 264–265.

Beomsoo Park (S'16) received the B.E. and M.S. degree in electronic engineering from Sogang University, Seoul, South Korea in 2008 and 2010, respectively. From 2010 to 2016, he joined in Samsung Electronics to develop CMOS image sensor readout circuits. Since 2016, he has been working towards the Ph.D. degree in Electrical and Computer Engineering at University of Florida.

In the fall of 2019, he was with Qualcomm Inc., as an intern, where he was involved with wideband delta-sigma analog-to-digital converter. His current research interests include high performance oversampling analog-to-digital converters and hardware security. Mr. Park was a recipient of the IEEE ISSCC Student Travel Grant Award in 2019.

Domenic Forte (S'09-M'13-SM'18) received the B.S. degree in Electrical Engineering from Manhattan College, Riverdale, NY, USA, in 2006, and the M.S. and Ph.D. degrees in Electrical Engineering from the University of Maryland, College Park, MD, USA, in 2010 and 2013, respectively.

He is currently an Associate Professor with the Electrical and Computer Engineering Department, University of Florida, Gainesville, FL, USA. His research covers the entire domain of hardware security from nano devices to printed circuit boards (PCBs) on topics such as hardware security primitives, hardware Trojan detection and prevention, security of the electronics supply chain, security-aware computer-aided design automation tools, reverse engineering, and anti-reverse engineering.

Dr. Forte is a recipient of the Presidential Early Career Award for Scientists and Engineers (PECASE), the NSF Faculty Early Career Development Program (CAREER) Award, and the Army Research Office (ARO) Young Investigator Award. His research has been also recognized through nine best paper awards and nominations. He serves as an Associate Editor of the ACM Journal on Emerging Technologies in Computing Systems (JETC) and of the Journal of Hardware and Systems Security (HaSS), on the organizing committees of top conferences in hardware security such as IEEE Symposium on Hardware Oriented Security and Trust (HOST) and AsianHOST, and on the technical program committees in the areas of electronic design automation, VLSI design and test, and cybersecurity.

Mark M. Tehranipoor (F'18) is currently the Intel Charles E. Young Preeminence Endowed Chair Professor in Cybersecurity at the University of Florida. His current research projects include: hardware security and trust, supply chain security, IoT security, VLSI design, test and reliability.

Dr. Tehranipoor has published over 400 journal articles and refereed conference papers and has delivered about 200 invited talks and keynote addresses. He has published 11 books and more than 20 book chapters. He is a recipient of a dozen best paper awards and nominations, as well as the 2008 IEEE Computer Society (CS) Meritorious Service Award, the 2012 IEEE CS Outstanding Contribution, the 2009 NSF CAREER Award, and the 2014 AFOSR MURI award. He serves on the program committee of more than a dozen leading conferences and workshops. He has also served as Program Chair of a number of IEEE and ACM sponsored conferences and workshops (HOST, ITC, DFT, D3T, DBT, NATW, and more). He co-founded the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) and served as HOST-2008 and HOST-2009 General Chair. He is currently serving as a founding EIC for Journal on Hardware and Systems Security (HaSS) and Associate Editor for JETTA, JOLPE, IEEE TVLSI and ACM TODAES. Prior to joining UF, Dr. Tehranipoor served as the founding director for CHASE and CSI centers at the University of Connecticut. He is currently serving as a founding director for Florida Institute for Cybersecurity Research (FICS). Dr. Tehranipoor is a Fellow of the IEEE, a Golden Core Member of IEEE CS, and Member of ACM and ACM SIGDA.

Nima Maghari (SM'17) received the B.S. degree in electrical engineering from the University of Tehran, Iran, in 2004 and the Ph.D. degree in electrical engineering from Oregon State University in 2010.

He is currently an associate professor at the school of electrical and computer engineering, University of Florida, Gainesville. From 2004 to 2006, he was with IC-LAB, University of Tehran, where he was involved with audio delta-sigma converters and low-voltage bandgap references. In 2008 he was recipient of CICC-AMD outstanding student paper award. He has served as an Associated Editor of IEEE Transactions on Circuits and Systems-I, IET Electronics Letters and the technical program committee of IEEE CICC as Data Converter Sub-Committee Chair. He is on the editorial board of Journal of Solid-State Circuit Letters. He has published more than 60 conference and journals papers in IEEE and IEE.

His research interests include high performance analog-to-digital converters, delta-sigma modulators, synthesizable analog circuits, time-assisted data conversion techniques, low-power low-voltage regulators, and analog mixed-signal on-chip security.