A Strong Physically Unclonable Function With $>2^{80}$ CRPs and $<1.4\%$ BER Using Passive ReRAM Technology

Mohammad Reza Mahmoodi, *Member, IEEE*, Zahra Fahimi, Shabnam Larimian, Hussein Nili, Hyugin Kim, *Member, IEEE*, and Dmitri B. Strukov

***Abstract*—We experimentally demonstrate a strong physically unclonable function (PUF) circuit featuring $>2^{80}$ challenge-response pair (CRP) capacity, <1.4% bit-error-rate (BER), and strong resiliency against advanced machine learning (ML) attacks. Similar to our recent work, our design takes advantage of the intrinsic variations in the nonlinear static characteristics and leakage currents of as-fabricated $F = 250$-nm half-pitch 64 × 64 ReRAM circuits. Passive crossbar circuits with $4F^2$ area per crosspoint device and reduced peripheral overhead, not requiring any circuitry for programming, result in an extremely compact design, while low-power consumption is achieved by keeping ReRAM devices in the highly resistive, virgin states. The key contributions of this letter is a novel leakage injection approach using an electrically isolated portion of the crossbar array, which boosts PUF's robustness, and a key-booking scheme, which dramatically improves reliability across a wide temperature range of operation and further increases PUF circuit density by reducing error correcting overheads. The experimental results showed near-ideal functional performance metrics, including 49.55% uniformity, 49.95% diffuseness, and 49.25% uniqueness. The measured response also passed all relevant NIST randomness tests.**

***Index Terms*—Hardware security, physical unclonable function (PUF), ReRAM, strong PUF**

I. Introduction

Secure operation is among the major challenges for the deployment of the Internet-of-Things systems and many other emerging system technologies [1], [2]. The elevated risks in establishing secure data transfer and authentication have led to the development of dedicated hardware circuits that ensure systems' security. One of the prominent examples of such circuits is physical unclonable function (PUF), which exploits unpredictable manufacturing and synthetic variations as a static entropy source to create die- and/or instant-specific responses.

The linear input–output mapping of most existing pure CMOS PUFs makes them vulnerable to machine learning (ML) attacks [3]. Emerging strong PUFs [4], [5] address such limitations by leveraging nonlinear *I–V* characteristics and sneak-path current in resistive memory crossbar circuits. However, the previous designs suffer from large BER and might be potentially vulnerable to side-channel attacks.

The motivation of this letter is to address such shortcomings. The studied baseline PUF architecture is based on the virgin-state fixed-resistance passive crossbar circuits, which do not require programming circuitry and ensure very low-power secure operation by utilizing highly resistive crosspoint junctions [5]. The major contribution of this letter is the employment of two novel techniques. First, a portion of the crossbar is isolated to ensure the consistent contribution of leakage current in the output and, hence, to eliminate possible information leakage through the comparator. Second, the new design utilizes a key-booking scheme in which the reference key is measured at several temperatures, rather than only a room temperature. A similar idea is previously suggested in the context of SRAM-based weak PUFs [6]. The main difference is that [6] work uses resource-hungry reverse fuzzy extractor and preprocessing techniques, such as majority voting and bit masking for error correction. On the other hand, our approach dramatically reduces raw BER without discarding [8] or masking CRPs [5], [7], or digital fine-tuning [9].

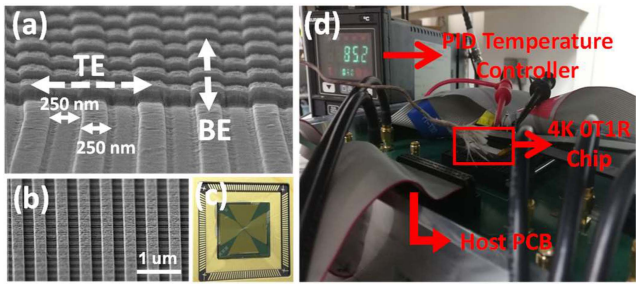

Fig. 1. Experimental setup. (a) Oblique-view and (b) top-view SEM images. The photographs of (c) wire-bonded fabricated 64 × 64 crossbar circuit with bottom electrodes (BE) and top electrodes (TE) directions highlighted, and the (d) setup with the mounted circuits during the BER measurements.

II. Strong PUF Design and Fabrication

The proposed PUF is prototyped using 64 × 64 crossbar circuits based on Al (70)/TiN (45)/Al_2O_3(1.5)/TiO_{2-x}(30)/Ti (15)/Al (90)/TiN (80) passively integrated devices (layer thickness in nm). Fig. 1 shows the fabricated crossbar circuit and the experimental setup. The details of the fabrication process are discussed in [10].

Fig. 2 shows the implemented strong PUF topology. A single bit response per 128-bit challenge is generated in two cycles. Specifically, the first 64 bits of a challenge uniquely determines sets of m selected rows, that are grounded with CMOS peripheral circuits. The remaining two 32-bit sets of a challenge determine the two selected electrodes. The unselected electrodes are kept floating to circulate sneak-path current in the array, hence, complicating the mapping. In each of the two cycles, currents flowing into the selected columns are compared using the dynamic current comparator to produce a single bit. The two bits are then XORed to generate one bit of a response (similar to our previous work [11]). The total number of CRPs is $\sum \binom{64}{m}\binom{32}{2}$, which is $> 2^{80}$ for $m = 16 \div 48$.

To ensure consistent contribution of leakage current in the outputs, 32 columns are isolated from the main circuit, which further

Manuscript received May 5, 2020; revised June 27, 2020 and July 7, 2020; accepted July 15, 2020. Date of publication July 20, 2020; date of current version August 6, 2020. This article was approved by Associate Editor Stefan Rusu. This work was supported in part by a Semiconductor Research Corporation (SRC) funded JUMP CRISP center, under NSF/SRC E2CDA Grant 1740352. *(Corresponding author: Mohammad Reza Mahmoodi.)*

The authors are with the Electrical and Computer Engineering Department, University of California at Santa Barbara, Santa Barbara, CA 93106 USA (e-mail: mrmahmoodi@ucsb.edu).

Digital Object Identifier 10.1109/LSSC.2020.3010255

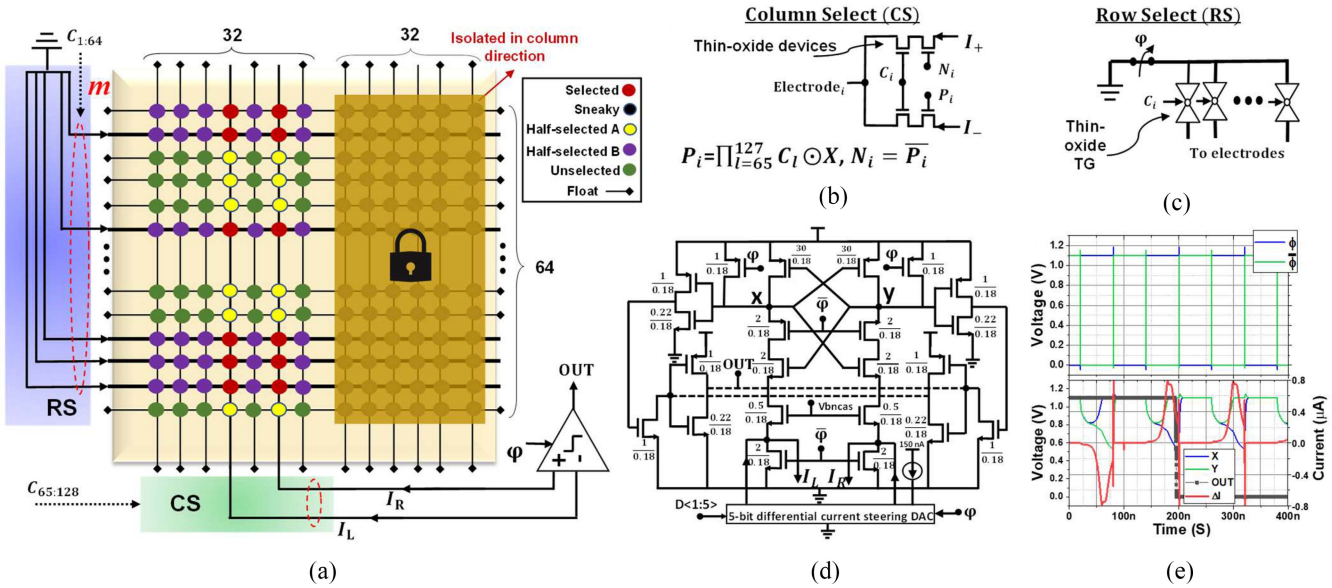

Fig. 2. Proposed PUF design. (a) Top-level diagram showing row/column selection, current comparator, and a 64 × 64 crossbar array circuit. Design of (b) row select (RS) and (c) column selection (CS) circuits [4]. Note the absence of large-area thick-oxide programming switches which are not needed in the proposed PUF design due to using virgin-state (i.e., as-fabricated) RRAM devices. (d) Current comparator and (e) its simulated timing diagram.

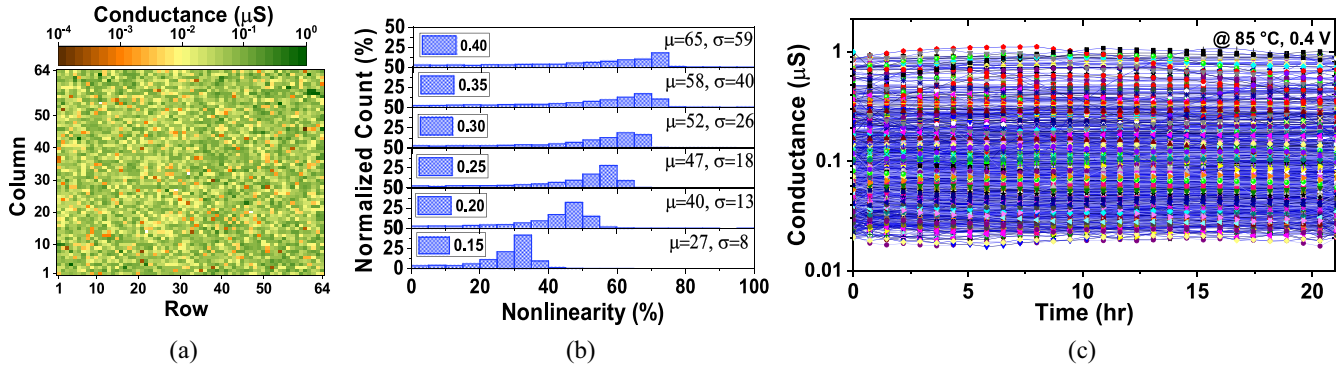

Fig. 3. ReRAM crossbar circuit characterization results. (a) Measured conductance map (at 0.4 V) of the virgin-state crossbar shown in Fig. 1(c). Median resistance is ∼ 22 MΩ. (b) Measured distributions of nonlinearity, defined as $(|G_0 - G(V_{\text{bias}})|/G_0) \times 100$, and its variations for several values of V_{bias}. G_0 is the measured conductance at 0.1 V. (c) Accelerated retention test results at 85 °C for 1000 randomly selected devices.

complicates the functional response. When a single row is selected, the readout current is $> 10\times$ larger, on average, than the expected range of values, due to the introduced leakage.

It is worth noting that the two-cycle reading scheme reduces the possible bias, which could be otherwise present, e.g., as a result of nonideal fabrication yield. It also improves the robustness against modeling attacks by adding extra-nonlinearity in the output response.

Fig. 3(a) shows the measured conductance of 4K cells in the crossbar array at 0.4 V, highlighting very resistive crosspoint devices and, subsequently, low-power operation. The uniform conductances of crosspoint devices result in a tight Gaussian distribution of differential $(I_R - I_L)$ currents and high uniformity of the response.

Due to the tunneling charge transport mechanism at the high-resistance virgin state, the devices' $I - V$ characteristics are extremely nonlinear. More importantly, Fig. 3(b) shows that the average nonlinearity and its variations increase at larger biases (more than twofold increase in average and sevenfold in standard deviation when the bias voltage is increased from 0.15 V to 0.4 V), which is an important feature for improving robustness against ML attacks [2].

Finally, the devices show excellent retention characteristics with no significant change in the conductance observed after baking the chip at 85 °C for >20 h and continuously measuring the conductance of the devices at 0.4 V [Fig. 3(c)]. Such features enable the design of a reliable, strong PUF.

III. Results

A. General PUF Characteristics

We prototyped more than half a million CRPs using the demonstrated crossbar with randomly applied challenges from the CRP space.

Fig. 4(a) shows the distribution of readout currents obtained by applying 1500 challenges at $V_{\text{bias}} = 0.1$ V. The symmetric distribution of differential-mode currents and relatively low common-mode response indicate high uniformity and low-power operation. The typical speckle pattern of 64-bit keys generated by the proposed PUF supports the high quality of generated bits [Fig. 4(c)]. More quantitative, statistical analysis of >500 000 generated bits shows almost no direct correlation between inputs and output. Indeed, Fig. 4(c) shows that by selecting different row and column electrodes, the average response is always close to 50%, indicating no direct bias due to the selection of specific rows or columns. The statistical properties of the

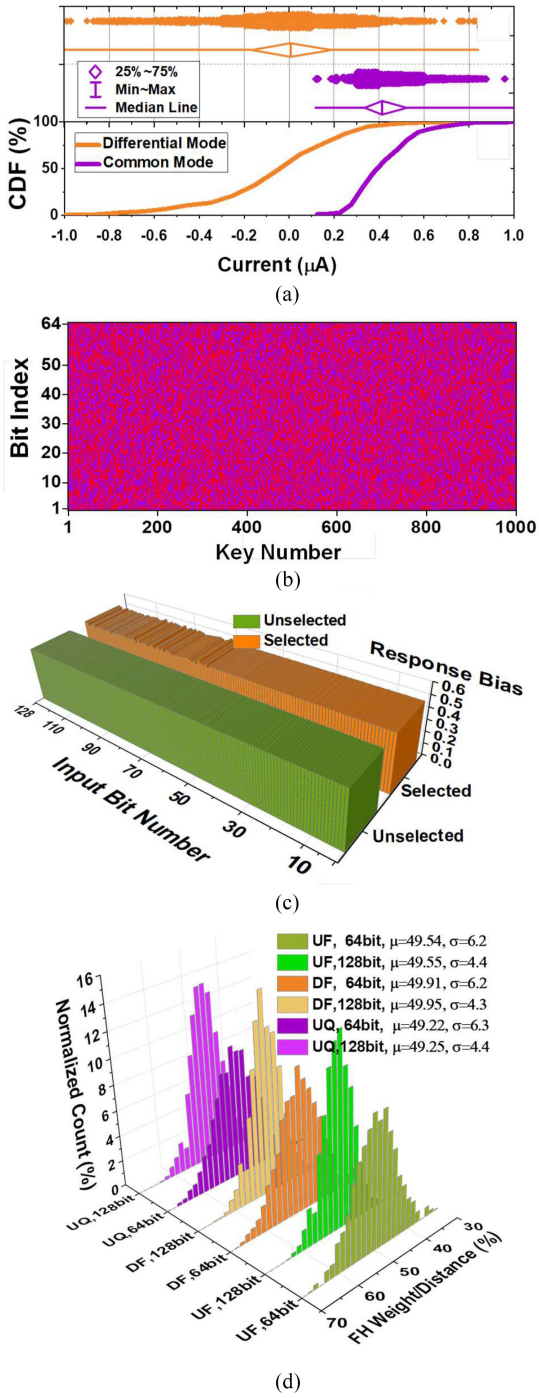

Fig. 4. General PUF characteristics. (a) Common-mode and differential distributions of output currents (top panel) and corresponding CDF (bottom panel) over 15 kb responses measured at 0.1 V and room temperature. (b) Speckle pattern for 1000 64-bit keys. Blue/red shows "1"/"0" responses. (c) Input–output correlations. Each column shows PUF output (at 0.4 V, @ 25 °C), averaged over outputs of all (500k) measured CRPs with the same fixed value of specific input bit. (d) Uniformity (UF), diffuseness (DF), and uniqueness (UQ), measured at 0.4 V and 85 °C. Fractional Hamming (FH) weight/distance distributions are computed based on 4k keys. All keys are formed by grouping generated 1-bit responses from randomly ordered challenges.

demonstrated PUF were also assessed using the common evaluation metrics in [1] and [2]. As shown in Fig. 4(d), near-ideal uniformity, diffuseness, and uniqueness for 64-bit and 128-bit keys are achieved with the proposed PUF.

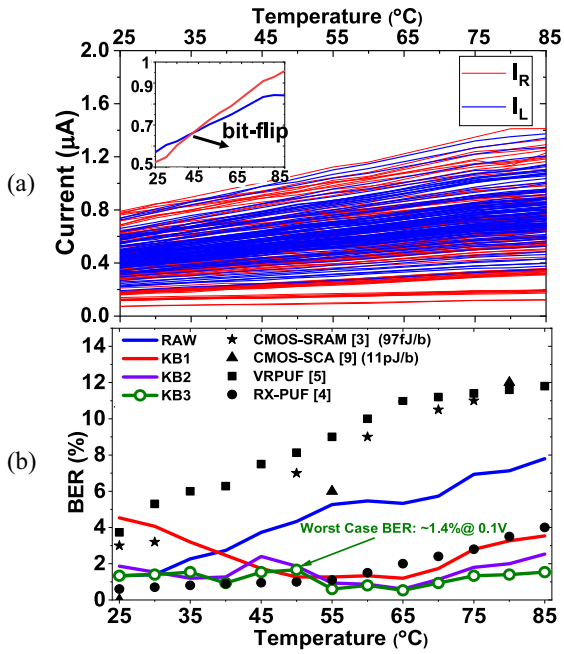

Fig. 5. PUF reliability. (a) Sensed currents as a function of temperature for 100 randomly selected CRPs. The inset shows a bit-flip at ~45 °C. (b) Reliability of the PUF (@ 0.1 V) and comparison with previous works. RAW, KB1, KB2, and KB3 are associated with defining the golden keys at 25 °C; 55 °C; 40 °C, 65 °C; and 25 °C, 45 °C, 65 °C. For the KB3 PUF @ 0.4 V, BER is estimated to be ~0.7%.

The experimental data show that the proposed PUF demonstrates similar close-to-ideal statistical properties compared to our previous works [4], [5].

B. Reliability Improvement

Unlike CMOS PUFs in which the response instability is a complex function of temperature, the output currents in the proposed PUF are semilinearly dependent on the temperature with different slopes due to device-to-device and state-dependent variations. This is illustrated in Fig. 5(a), which shows the output current as a function of temperature for 100 randomly picked CRPs. Such dependency results in a large BER at elevated temperatures, as shown in Fig. 5(a) (which is still better or comparable to native, i.e., uncorrected, BER of CMOS strong PUFs). To mitigate this issue, we propose a key-booking technique, which takes advantage of the monotonic current-temperature relationship. Specifically, an error (a bit-flip), if happens, only occurs once in the entire temperature range. By storing the golden key at three temperatures, namely, 25 °C, 45 °C, 65 °C during enrollment (case KB3), and retrieving the response at the closest to the operating temperature during authentication, we achieve intrinsic ~1.4% and ~0.7% errors for 0.1-V and 0.4-V biases across the whole temperature range [Fig. 5(b)]. (Note that such BERs are largely dominated by the noise, justifying the use of only a few reference temperatures during enrolment.) Hence, no on-chip post-processing and its significant overhead, or CRP loss, are imposed in our approach. Fig. 5(b) also provides a comparison with our previous work [4], [5] and CMOS strong PUFs [3], [8].

In case the server has accurate information on the ambient temperature of the chip containing the PUF circuit, the overhead of the proposed technique is negligible—just an increase of the stored CRP table size on the server. Otherwise, the additional minor overhead is the addition of an on-chip temperature sensor, e.g., low-cost sensors available in IoT devices [12]. Such a sensor would be used for

TABLE I
COMPARISON WITH PREVIOUS WORKS (LL = LIBLINEAR PACKAGE, LS = LIBSVM PACKAGE, * AT 0.1-V/ 0.4-V BIAS)

	ISSCC'15 [7]	ISSCC'15 [14]	VLSI'17 [3]	VLSI'17 [8]	VLSI'18 [4]	IEDM'19 [5]	DAC'19 [12]	This work
Technology	22 nm CMOS	65 nm CMOS	28 nm CMOS	130 nm CMOS	250 nm ReRAM	250 nm ReRAM	55 nm eFlash	250 nm ReRAM
Demo Complexity	Crosscouple $9581F^2$	SA PUF $12000F^2$	64×64 SRAM $\sim 194F^2$	SCA PUF	20×20 $\sim 4 \times 4F^2$ 0T1R	64×64 $4F^2$ 0T1R	5× 10×10 $\sim 120F^2$	64×64 $4F^2$ 0T1R
Pre-configuration	Intrinsic	Intrinsic	Intrinsic	Intrinsic	Preprogramming	Intrinsic	Preprogramming	Intrinsic
Capacity	-	$\sim 2 \times 10^{12}$	$\sim 2^{36}$	$\sim 2^{65}$	$\sim 2^{25}$	$\sim 2^{86}$	$\sim 2^{700}$	$\sim 2^{82}$
BER @ 85 °C	~4.5 %	5 %	~ 12.5 %	~ 9 %	4.2 %	~ 11.5 %	~ 5 %	1.4% / 0.7% *
NIST Test	Fail	Pass	Not Tested	Not Tested	Pass	Pass	Pass	Pass
ML Attack	Weak PUF	Weak PUF	LL, LS 10k bits	LL, LS, NN,10k bits	MLP, 128k bits	MLP, LL, LS, LSTM, 80k bits	MLP, LL, LS, LSTM, 100k bits	MLP, LL, LS, 500k bits
Prediction Acc.	-	-	~ 40%	~ 40%	~50%	~50%	~50%	~50%

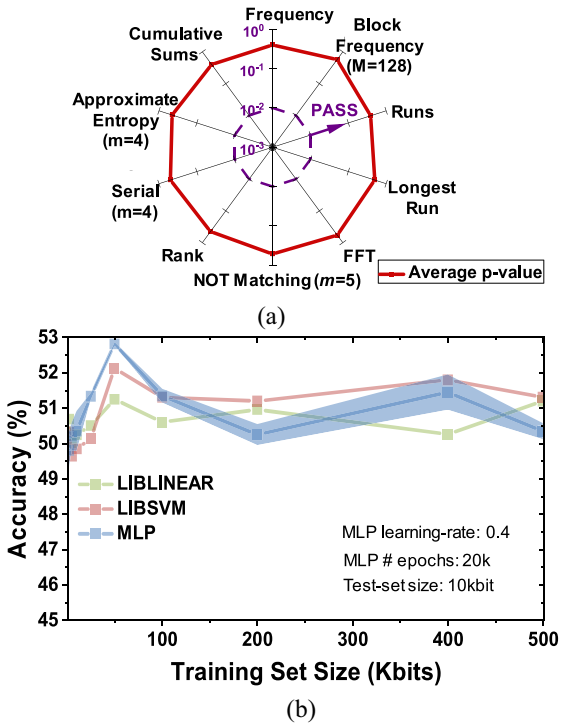

Fig. 6. Randomness and resilience. (a) Results of applying NIST test based on 23 25k-bit-long bitstreams generated at 0.4 V bias and room temperature. (b) Prediction accuracy for three considered ML models as a function of the number of CRPs data used in training. The training and test set sizes are expressed in the number of response bits.

informing the server about the chip temperature in both enrollment and authentication stages.

C. Randomness Evaluation and Machine Learning Modeling

The statistical properties of >500k generated response bits are tested using the NIST test suite [13]. The average p-value on all tests is well above the minimum pass value [Fig. 6(a)].

The resilience against the ML attacks is first studied by modeling PUF with a $128 \times 500 \times 100 \times 20 \times 1$ multilayer perceptron classifier [Fig. 6(b)]. Specifically, the input challenge is applied as a binary 128-bit vector to the input layer of the perceptron, while a predicted single-bit response is produced by the network's output layer. The network is trained on a specific subset of measured CRPs [Fig. 6(b)] using gradient descent with momentum and with a manually found quasi-optimal learning rate of 0.4. The testing is conducted on another CRP subset, which is mutually exclusive with the training subset. Fig. 6(b) shows that the test accuracy for all the cases is close to the ideal 50% predication accuracy, even when increasing the training set size to $\sim 5 \times 10^5$ CRPs. This means that the network, i.e., the attacker's model of the PUF circuit, always fails to make a meaningful prediction. The other ML approaches—LIBSVM and LIBLINEAR—from [3] also resulted in unsuccessful attacks with ~50% prediction accuracy, which corroborates the resiliency of the demonstrated PUF toward the ML attacks.

Table I summarizes the measurement results and compares our design with the previously reported PUFs based on CMOS and emerging technologies.

REFERENCES

[1] H. Nili *et al.*, "Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors," *Nat. Electron.*, vol. 1, pp. 197–202, Mar. 2018.
[2] M. R. Mahmoodi, D. B. Strukov, and O. Kavehei, "Experimental demonstrations of security primitives with nonvolatile memories," *IEEE Trans. Electron Devices*, vol. 66, no. 12, pp. 5050–5059, Dec. 2019.
[3] S. Jeloka, K. Yang, M. Orshansky, D. Sylvester, and D. Blaauw, "A sequence dependent challenge-response PUF using 28nm SRAM 6T bit cell," in *Proc. Symp. VLSI Circuits*, Kyoto, Japan, Feb. 2017, pp. C270–C271.
[4] M. R. Mahmoodi, H. Nili, and D. B. Strukov, "RX-PUF: Low power, dense, reliable, and resilient physically unclonable functions based on analog passive RRAM crossbar arrays," in *Proc. Symp. VLSI Technol.*, Honolulu, HI, USA, Feb. 2018, pp. 99–100.
[5] M. R. Mahmoodi, H. Nili, Z. Fahimi, S. Larimian, H. Kim, and D. Strukov, "Ultra-low power physical unclonable function with nonlinear fixed-resistance crossbar circuits," in *Proc. Int. Electron Devices Meeting (IEDM)*, San Francisco, CA, USA, Dec. 2019, pp. 1–4.
[6] Y. Gao, Y. Su, L. Xu, and D. C. Ranasinghe, "Lightweight (reverse) fuzzy extractor with multiple reference PUF responses," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1887–1901, Jul. 2018.
[7] S. K. Mathew *et al.*, "μRNG: A 300–950 mV, 323 Gbps/W all-digital full-entropy true random number generator in 14 nm FinFET CMOS," *IEEE J. Solid-State Circuits*, vol. 51, no. 7, pp. 1695–1704, Jul. 2016.
[8] X. Xi, H. Zhuang, N. Sun, and M. Orshansky, "Strong subthreshold current array PUF with 2^{65} challenge-response pairs resilient to machine learning attacks in 130nm CMOS," in *Proc. Symp. VLSI Circuits*, Kyoto, Japan, Feb. 2017, pp. C268–C269.
[9] W. Che, F. Saqib, and J. Plusquellic, "Novel offset techniques for improving bitstring quality of a hardware-embedded delay PUF," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 4, pp. 733–743, Apr. 2018.
[10] H. Kim, H. Nili, M. R. Mahmoodi, and D. B. Strukov, "4K-memristor analog-grade passive crossbar circuit," 2019. [Online]. Available: arXiv:1906.12045.
[11] M. Mahmoodi, H. Nili, S. Larimian, X. Guo, and D. Strukov, "ChipSecure: A reconfigurable analog eFlash-based PUF with machine learning attack resiliency in 55nm CMOS," in *Proc. 56th ACM/IEEE Design Autom. Conf. (DAC)*, Las Vegas, NV, USA, Jun. 2019, pp. 1–6.
[12] J. Yin *et al.*, "A system-on-chip EPC gen-2 passive UHF RFID tag with embedded temperature sensor," *IEEE J. Solid-State Circuits*, vol. 45, no. 11, pp. 2404–2420, Nov. 2010.
[13] L. E. Bassham *et al.*, *Sp 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, 2010.
[14] 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 *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, San Francisco, CA, USA, Feb. 2015, pp. 1–3.