RX-PUF: Low Power, Dense, Reliable, and Resilient Physically Unclonable Functions Based on Analog Passive RRAM Crossbar Arrays

Mohammad Reza Mahmoodi*, Hussein Nili*, and Dmitri. B. Strukov
Electrical and Computer Engineering Department, UC Santa Barbara, CA 93106-9560, USA

Abstract

We propose a novel architecture ("RX-PUF") for physically unclonable functions (PUF) based on analog RRAM crossbar array circuits. RX-PUF takes advantage of unique RRAM properties, such as *I-V* nonlinearity, and its device-to-device (d2d) variations and tunability. As a proof of concept, we have prototyped a 600 kb challenge response pair (CRP) PUF using 250 nm half-pitch (F) 20×20 crossbar arrays with passively integrated devices. The RX-PUF prototype features excellent physical characteristics, e.g. ~1600 F^2/bit density and up to 41 fJ/bit energy efficiency. Its functional performance, improved by utilizing hidden input, is also very promising. The measured bit error rate (BER) was 0.7% at RT and ≤ 5.3% at 100°C, even without using any error correction methods. The measured responses showed near-ideal uniformity (50.04%) and inter-HD (50.12%) and passed all relevant NIST randomness tests. The preliminary results showed also very high resilience of RX-PUF against machine learning (ML) attacks.

Introduction

PUFs are promising for identification and key generation tasks due to their potential for low-cost implementation, high-throughput and low-power operation, and resilience against counterfeiting and cloning. Various PUFs based on CMOS and emerging device technologies were proposed [1,2]. The main drawback of CMOS implementations is typically large area, which in turn leads to inferior energy and throughput. Some of the proposed RRAM-based PUFs rely on reprogramming the state for key generation, which is not practical given the severe switching endurance limitations of RRAM. Other RRAM approaches, that utilize devices in the digital mode, typically suffer from biases in the output. Correlations in the outputs reduce PUF complexity and could be easily detected by ML modeling [3]. Analog-grade RRAM enables very complex and resilient PUFs, though the main concern is device intrinsic noise which may significantly impact BER.

RX-PUF Implementation

The RX-PUF was prototyped using 20×20 crossbar arrays of passively integrated Pt/Al_2O_3/TiO_{2-x}/Pt RRAM devices [7] (**Fig. 1**). In RX-PUF (**Fig. 2**), the applied challenge uniquely determines sets of n rows and m columns, that are biased to V_{bias} and ground, accordingly, using peripheral CMOS circuitry. All remaining unselected lines are kept floating. The currents flowing into two subsets of m/2 columns are then sensed and compared against each other to generate a single output bit. Multiple response bits are grouped together to generate longer output key. The key idea of our approach is that the sensed currents on each column are sums of the currents via selected n devices and the sneak path currents that are determined by the states of all floated devices. Different selection of rows and columns results in the redistribution of sneak-path currents, which is hard to predict or model due to RRAM's *I-V* nonlinearities and their process-induced d2d variations. Furthermore, the contribution of both types of currents is carefully balanced for each column by tuning device' conductances to specifically chosen desired (Gaussian-distributed along columns and rows) values, which reduce bias in the output and increase the noise margin. Such desired values are randomly generated by solving an optimization problem and could be pre-computed. The tuning procedure is only performed once to implement specific PUF instance. The same PUF circuit can be reconfigured many times by re-tuning its devices to a new distribution. To further improve functional performance, a two-step scheme is implemented. First, the auxiliary sense amplifier (SA), hardwired to the first and last columns, generates an "AUX" bit by comparing input currents in these lines. In the next step, a second output bit is generated by main SA, that serve all but the mentioned two columns (**Fig. 2a**). This bit is then xored with AUX bit to produce the final response bit. In the implemented prototype, n = 5 (out of N = 20 total), while m = 2 (out of M = 20-2=18 total).

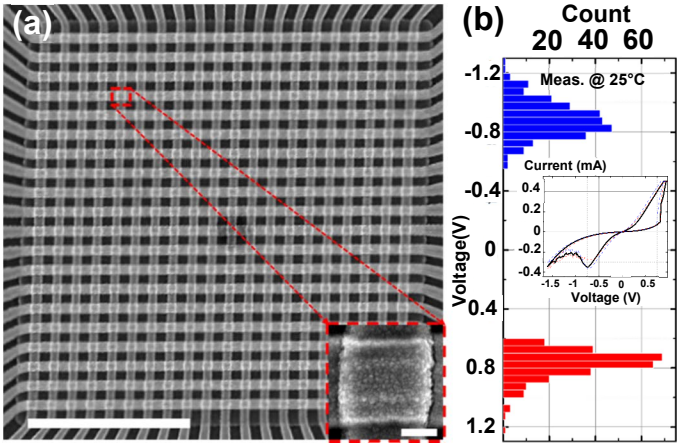
Results and Discussion

Fig. 3 shows the programmed conductances for the studied PUF instance. The implemented tuning was very crude (with conductances of ~ 20% devices significantly lower than the desired values) to emulate various device non-idealities, e.g. crossbar arrays with large variations in switching thresholds (**Fig. 1b**). We then collected output currents (**Fig. 4**) and the corresponding responses (**Fig. 5**) on all 600 kb CRPs, and BER on the worst-case 10 kb responses under wide ambient temperature range (**Fig. 6**). The measured data clearly shows the benefit of AUX approach, which allowed to reduce output bias due to imperfect tuning (**Fig. 5**), and successfully pass NIST randomness test (**Fig. 7**). The inter-HD for 64 and 128 keys (**Fig. 8**) showed near-ideal values, while the detailed analysis of such keys showed almost no correlations for the AUX approach (**Fig. 9**). The resilience against machine learning attacks was assessed with 40×500×500×1 multi-layer perceptron classifier. The classifier was trained on a subset of specific size of the observed CRPs and then tested on another mutually exclusive observed set (**Fig. 10**). Even with large fraction of the training data, the classifier predicted output with close to ideal 50% accuracy for the PUF with AUX approach. The circuit consumes on average 212 fJ per response bit for V_{bias}= 0.3 V, with ~20% of the energy dissipated in RRAM array. The energy efficiency can be further improved to 41 fJ/bit by using V_{bias}= 0.1 V without significantly degrading other metrics. **Table** 1 summarizes the results and shows that proposed approach compares very favorably with the state-of-the-art. We expect that a moderate increase in crossbar array size may exponentially improve resilience even against modelling with very deep classifiers, while scaling-down device feature sizes would lead to sub-fJ operation.

References

[1] S.Jeloka *et al.* VLSI'17; [2] Y.Pang *et al.* VLSI'17; [3] X.Xi *et al.* VLSI'17; [4] K.Yang *et al.* ISSCC'15; [5] A.Alvarez *et al.* ISSCC'15; [6] S.Mathew *et al*. ISSCC'14; [7] G.Adam *et al.* TED, 2017.

*These authors contributed equally to this work.



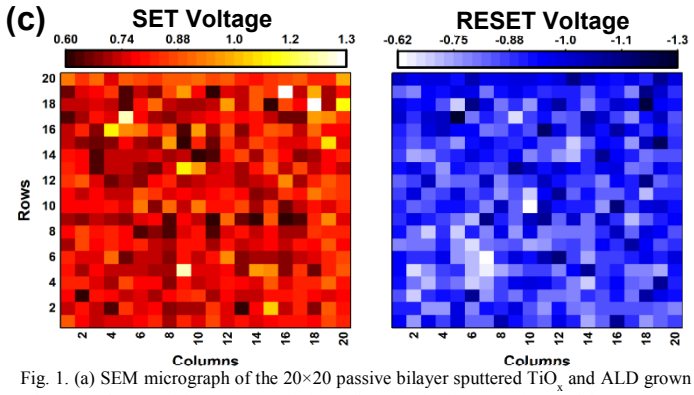


Fig. 1. (a) SEM micrograph of the 20×20 passive bilayer sputtered TiO_x and ALD grown Al_2O_3 crossbar, (scalebar: 5 µm). The inset shows a single crosspoint (scalebar: 100 nm). (b),(c) histogram and spatial maps of SET and RESET switching voltage threshold distributions for crosspoint devices.

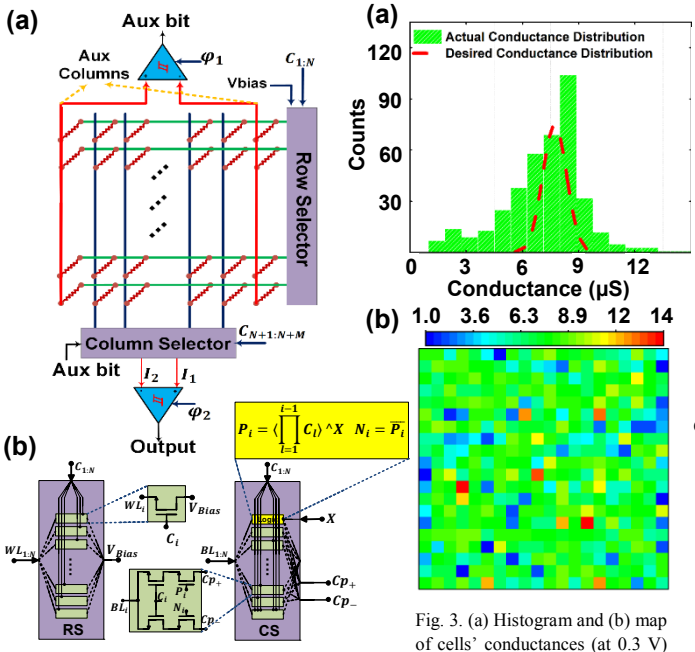


Fig. 2. (a) PUF architecture and (b) design of column/row selectors. The input is encoded by *N+M* bits, with 1s for to the selected rows/columns.

Fig. 3. (a) Histogram and (b) map of cells' conductances (at 0.3 V) for the demonstrated PUF.

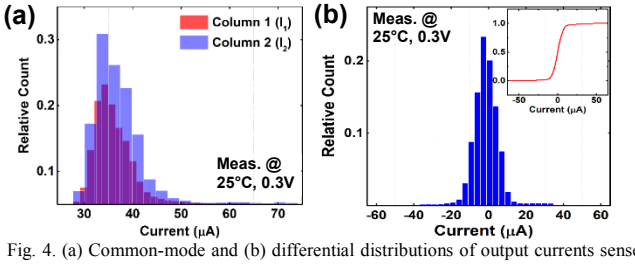


Fig. 4. (a) Common-mode and (b) differential distributions of output currents sensed by main SA over 600 kb responses. The inset shows ecdf.

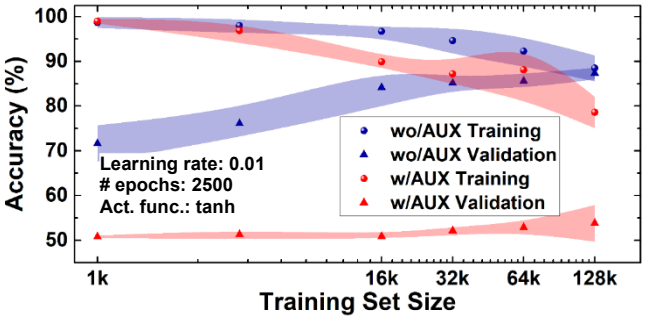


Fig. 10. Modeling attack by MLP network, tested on 5k validation set, as a function of training set size (in bits). The training was performed using a gradient descent method with momentum. Symbols show average prediction accuracy, while the line thicknesses are drawn according to the max and min values obtained over 5 runs.

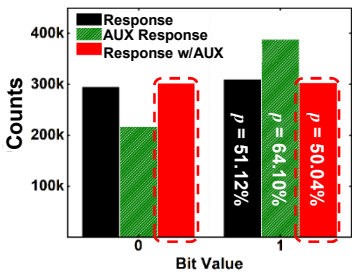


Fig. 5. Distribution of PUF response (at 0.3 V @ 25°C) with and without AUX approach.

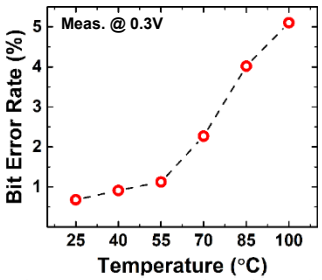


Fig. 6. BER of AUX-enhanced PUF for 10k worst-case CRPs.

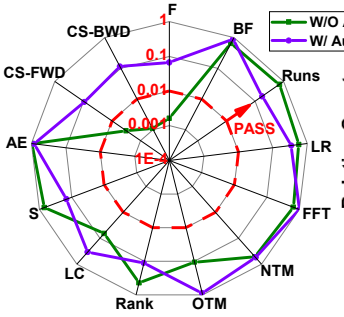


Fig. 7. Results of NIST randomness tests using measured 600kb responses for the PUF implementation with and w/o AUX.

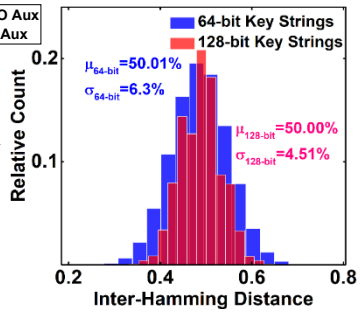


Fig. 8. Inter-hamming distance (at 0.3 V @ 25°C) for 64 and 128-bit keys formed by grouping sequentially generated 1-bit responses.

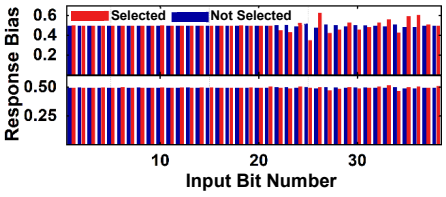


Fig. 9. Input-output correlations: Each column shows PUF output (at 0.3 V @ 25°C), averaged over all CRPs with the same fixed value of specific input bit. The bottom / top panel shows implementation with / w.o. AUX approach.

Table I. Comparison with previous works (* w/o applying correction methods)

		VLSI'17 [1]	VLSI'17 [3]	ISSCC'15 [4]	ISSCC'15 [5]	ISSCC'14 [6]	This work
Technology		FDSOI (28nm)	CMOS (130nm)	CMOS (40nm)	CMOS (65nm)-SA	CMOS (22nm)	ReRAM/CMOS (200nm/55nm)
Number of CRPs		1.17×10^{11}	3.7×10^{19}	5.5×10^{28}	NA	250K	~2.37M
Worst-case BER*		~11%	9%	9%	~21%	~30%	5%
Area Efficiency (F^2/b)		970	-	-	12K	9.6K	1.4K
Energy Efficiency		97fJ/b	11pJ/b	17.7pJ/b	163fJ/b	190fJ/b	41-213fJ/b (0.1V-0.3V)
Temperature Range (°C)		0~80	-20~80	-25~125	25~85	25~50	25~100
NIST Randomness Test		NA	NA	NA	PASS	FAIL	PASS
ML Attack	Prediction Error	15%	40%	Not Tested	Not Tested	Not Tested	53%
	Training Size	$\sim 10^{-4}$%	$\sim 10^{-13}$%	-	-	-	~5%