A Lightweight Reconfigurable RRAM-based PUF for Highly Secure Applications

Basma Hajri, Mohammad M Mansour, Ali Chehab, Hassen Aziza

A Lightweight Reconfigurable RRAM-based PUF for Highly Secure Applications

Basma Hajri, Mohammad M. Mansour and Ali Chehab
[1]Electrical and Computer Engineering department
American University of Beirut, Beirut 1107 2020, Lebanon
E-mail: {bh24, mmansour, chehab}@aub.edu.lb

Hassen Aziza
[2]IM2NP, UMR CNRS 7334, Aix-Marseille Université
38 rue Joliot Curie, F-13451, Marseille Cedex 20, France
E-mail: hassen.aziza@univ-amu.fr

***Abstract*— Recently, memristors received considerable attention in various applications. Even some of the main drawbacks of resistive memory devices (RRAM), such as variability, have become attractive features for hardware security in the form of a Physically Unclonable Function (PUF). Although several RRAM-based PUFs have appeared in the literature, they still suffer from some issues related to reliability, reconfigurability, and extensive integration cost. This paper presents a novel lightweight reconfigurable RRAM-based PUF (LRR-PUF) wherein multiple RRAM cells, connected to the same bit line and same transistor (1T4R), are used to generate a single bit response. The pulse programming method used is also innovative: 1) it allows for a power-efficient implementation, and 2) it exploits variations in the number of pulses needed to switch the RRAM cell as the primary entropy source of the PUF. The main feature of the proposed PUF is its integration with any RRAM architecture at almost no additional cost. Through extensive simulations, including the impact of temperature and voltage variations along with statistical characterization, we demonstrate that the LRR-PUF exhibits such attractive properties that are lacking or poorly achieved in other previously proposed RRAM based PUFs, including high reliability (almost 100%), which is critical for cryptographic key generation, reconfigurability, uniqueness, cost, and efficiency. Furthermore, the design successfully passes relevant NIST tests for randomness.**

Keywords*— *Physical Unclonable Function (PUF), Memristor, RRAM, Reconfigurable PUF, reliability, security.

I. Introduction

The memristor, introduced in 1971 by Chua [1], is a two-terminal nanodevice, the properties of which have attracted researchers from various domains such as physics, chemistry, electronics, computer, and neuroscience. RRAM is a practical implementation of memristors. In its primitive form, a resistive memory element relies on a Metal/Insulator/Metal (MIM) stack acting as a resistive switch with Top and Bottom electrodes, as shown in Fig. 1. An RRAM device can switch from R_{LRS} (Low Resistance State, SET mode) to R_{HRS} (High Resistance State, RESET mode) and vice versa.

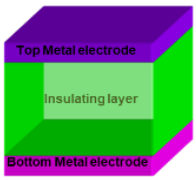

Fig. 1 Physical structure of a memristor device.

For oxide-based memristor devices, the switching process is mainly due to the formation and dissolution of Conductive Filaments (CF) [2], [3] between the metal electrodes. The geometry of the CF, which depends on the migration and recombination of oxygen vacancies in the oxide layer, strongly affects the switching characteristics of the memristor. Based on this physical mechanism, RRAM cell switching behavior is commonly modeled by the CF formation/rupture process during SET and RESET phases, as shown in Fig. 2. SET and RESET operations occur when the applied voltage V(T, B) across the Top and Bottom electrode exceeds specific thresholds referred to as V_{SET} and V_{RESET}, respectively.

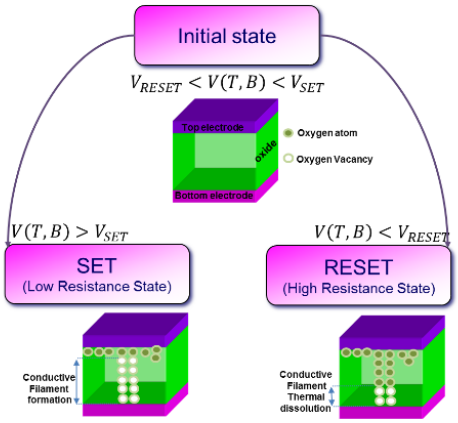

Fig. 2 Modeling of the switching behavior of a memristor device.

Due to the stochastic nature of the oxygen vacancies creation/destruction process, wide variations in the switching parameters are observed [4]. The variations are more extensive during the RESET process (R_{HRS}) than the SET process (R_{LRS}), and that is a common feature of RRAM cells. Even though these random variations are highly inconvenient for memory applications as they degrade the overall performance [6], they offer the key feature granting the success of RRAM technology in hardware security and particularly Physical Unclonable Function (PUF). PUFs employ the physical and manufacturing process variability to generate security primitives that can serve as authenticators, key generators [7], etc. Several RRAM-based PUFs appeared in the literature, such as Write Time Memristive PUF [8], Cross Bar PUF [9], RRAM PUF [10], and EPUF [11]. However, most still suffer from some issues, mainly reliability, reconfigurability, and extensive integration cost. The motivation of this paper is to present a novel Lightweight Reconfigurable RRAM-based PUF (LRR-PUF) highly reliable and that can be integrated with any RRAM architecture with almost no additional cost. Reconfigurability, achieved by reprogramming the RRAM array, improves security protocols [12]. For the proposed architecture, we selected the RRAM memory architecture with selector because of its superior energy efficiency and perfect cell isolation (increased reliability) [13] that are crucial characteristics in PUF applications.

The rest of this paper is organized as follows. Section II details the operation of the proposed LRR-PUF. Section III presents the simulation results and the main characteristics of LRR-PUF, including validation and assessment at the circuit level. Section IV concludes the paper.

II. PROPOSED LRR-PUF ARCHITECTURE

Different PUF architectures exist in the literature; however, most of them still suffer from major limitations related to the reliability, aging effect, power consumption, and the integration cost. The novel Lightweight Reconfigurable RRAM based PUF (LRR-PUF) is proposed to overcome the limitations mentioned above.

A. One cell LRR-PUF architecture

Fig. 3 presents the general scheme of the suggested LRR-PUF operation. When a challenge is applied, the selected RRAM cells are SET progressively (1) via pulse programming until they reach a certain reference current detected by a sense amplifier (2) during a READ operation [14]. A multi-bit counter (3) is then used to count the number of pulses required to SET the selected RRAM cells, and finally, the different outputs of the counter are XORed (4) to generate a single response.

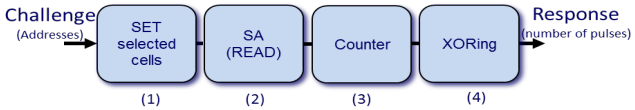

Fig. 3 Scheme of LRR-PUF operation procedure.

Fig. 4 represents the fundamental circuit of a 1-bit PUF, and Fig. 5 depicts related timing waveforms. A continuous sequence of voltage pulses (P) of fixed width is applied across the selected 1T4R RRAM cell through the Bit Line (BL) until the output of the current comparator (OC) reaches logic 1 (meaning that at least one RRAM cell is SET). At this point, the cell current I_{cell} reaches the reference current I_{ref}. When the RRAM cell is SET, BL falls back to zero (as P signal is controlled by the tri-state buffer activated by Q, which is the output of RS flip-flop). Due to the stochastic switching process, the time needed to SET the RRAM cell is random, and hence, the voltage signal BL drops to zero after a random number of pulses. BL is then sent to a counter. The counter binary bit stays at its pre-status logic 0 before the cell is turned ON, it flips rapidly (triggered by clock signals) until the pulses end and then stays at its steady-state logic 1. The rising edge of the clock signal triggers the bit flipping in the counter, and hence the frequency of this signal is half of the clock frequency. The bit on which the counter stops is random. Based on the variability of the RRAM cell, we use a 4-bit counter, and its outputs are then fed to a 4-input XOR gate to generate the response of the PUF. The novelties and contributions introduced in the proposed PUF architecture are the following:

1. A 1T4R cell is used rather than a traditional 1T1R. In this approach, 4 memristors coupled in parallel are driven by the same select transistor (used to protect the cells from current overshoot) and the same bit line. The specific number 4 of the parallel RRAM cells is selected after simulations to satisfy two constraints: 1) keeping a reasonable reference current for the sense amplifier and 2) reaching very high reliability.
2. Power-efficient implementation: pulse programming is used rather than continuous DC voltages and feedback from the sense amplifier to stop the generated pulses once the cell is SET.
3. Instead of using delays or R_{HRS}/R_{LRS} variability as PUF randomness sources, the number of pulses needed to SET a specific RRAM cell is used in the proposed architecture.
4. Enhanced unpredictability and uniqueness: a 4-bit XOR connects the outputs of the counter to generate a single bit response [15].

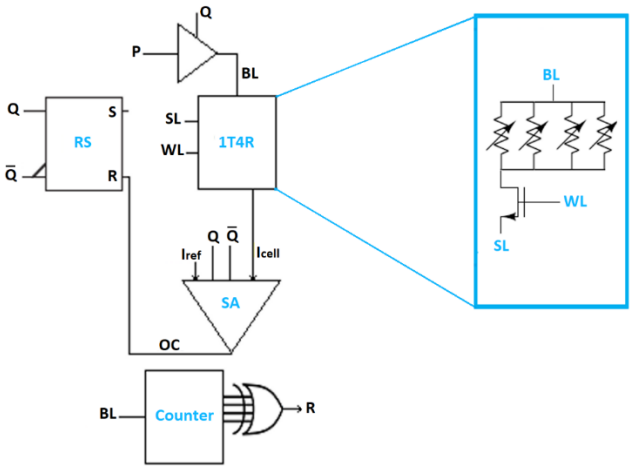

Fig. 4 Basic 1-bit LRR-PUF circuit.

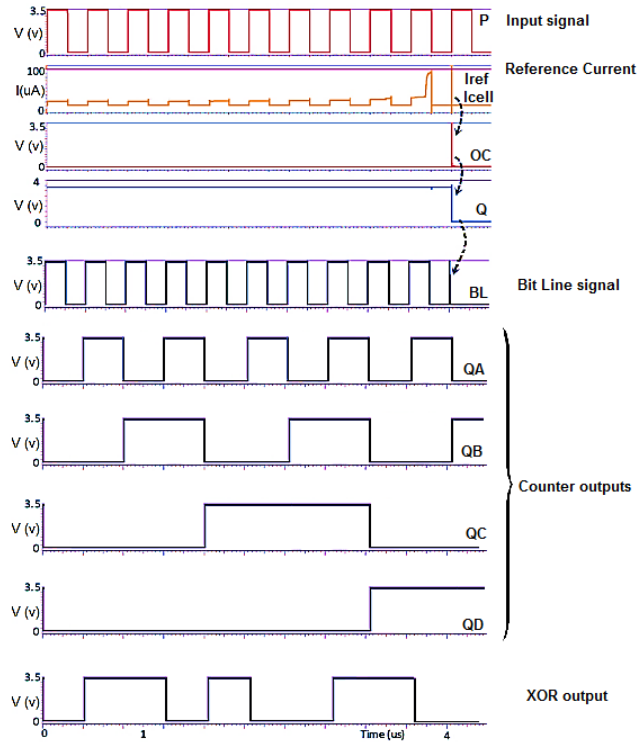

Fig. 5 Timing diagram of 1-bit LRR-PUF.

B. Crossbar array LRR-PUF Architecture

We implemented a 32x32 array to evaluate the main characteristics of the LRR-PUF. In the literature, RRAM based PUF [8], [9], [10], [11] use exclusively R_{HRS} or R_{LRS} resistance variations as entropy source for response generation. An attractive feature of LRR-PUF is that it can be configured to use either R_{HRS} or R_{LRS} resistance variations, depending on the application. Fig. 6 shows the detailed LRR-PUF array architecture, where each cell in the array includes 4 RRAM cells connected to the same BL and a common bottom electrode connected to one select transistor. Fig. 7a, and Fig. 7b present the Source Line (SL) and BL decoders with the challenges (cell addresses) as input and SL/BL signal

as output. Pulses are generated continuously through SL and BL and delivered to the selected cell. These signals are stopped (set to zero) when the output of the sense amplifier (Fig. 7c) gets high, meaning that the cells are either SET or RESET successfully. Fig. 7d is the response stage, including a 2-1 Mux to use either BL or SL depending on the type of operation (SET or RESET). A 4-bit counter is used to count the number of pulses, and finally, the 4 outputs of the counter are XORed to generate a single bit response.

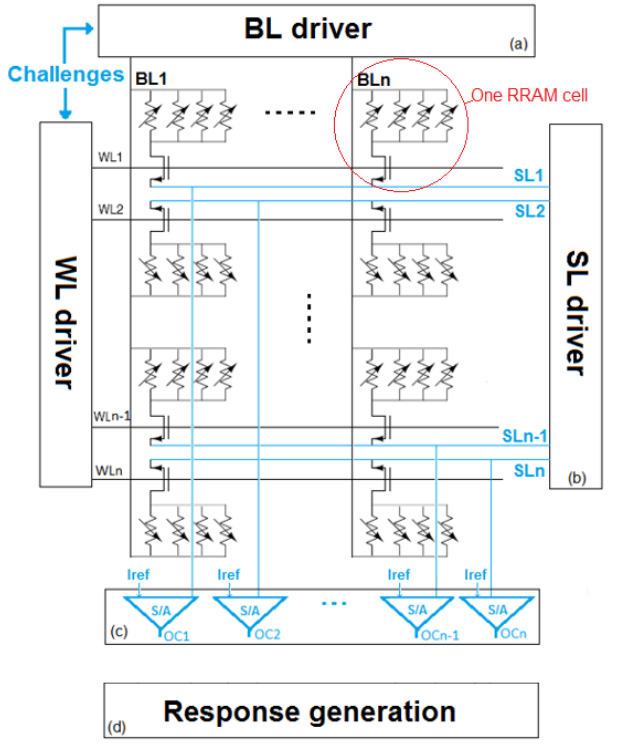

Fig. 6 Schematic of the LRR- PUF (1T4R architecture and peripheral circuitry) with n challenges, n responses.

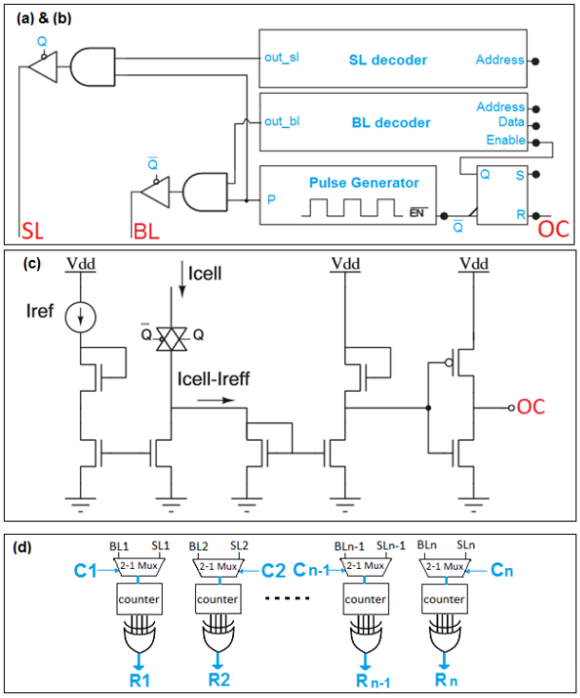

Fig. 7 LRR- PUF peripheral circuitry (a), (b) Bit line, and Source line decoders controlled by a pulse generator. (c) Sense amplifier circuit [14]. (d) Response generation stage with 2-1 mux, 4-bit counter, and XOR gate.

III. SIMULATION RESULTS AND BENCHMARKS

A. RRAM modeling

To evaluate the LRR-PUF performance accurately, we selected the Stanford model [16]. This physics-based model is calibrated with HfOx RRAM experimental data and takes into consideration the variability of the memory cell, the temperature, and SET/RESET time (effect of the duration of the applied voltage pulse). The main equations of the model are the following:

$$I = I_0 * \exp\left(-\frac{g}{g_0}\right) * \sinh\left(\frac{V}{V_0}\right) \quad (1)$$

$$\frac{d\langle g\rangle}{dt} = -v_0 \times exp\left(-\frac{E_A}{kT}\right) \times sinh\left(\gamma \times \frac{a_0}{t_{ox}} \times \frac{qV}{kT}\right) \quad (2)$$

The growth of the gap distance g is calculated, taking into account the electric field, temperature-enhanced oxygen ion migration (2), and the local temperature due to Joule heating. The parameter V is the applied voltage across the cell. E_A is the activation energy, a_0 is the atomic spacing, and t_{ox} is the oxide thickness. The prefactor I_0, the gap coefficient g_0, and the voltage coefficient V_0 are fitting parameters. The model fitting parameter variations considered in the simulations, along with their default values, are listed in Table I. These percentages of variation are rigorously selected so that the obtained LRS/HRS resistances stay compliant with the experimental data ranges [13].

TABLE. IV PARAMETER VARIATION

	Parameter	Default value	Variation (%)
Model parameters	v_0	400m/s	5
	g_0	0.4n	5
	I_0	1e13	5
	V_0	0.4V	5
CMOS parameters	V_{th}	400 mV	5
	L	100 nm	5
	W	240 nm	5

B. Simulation Setup

Monte-Carlo (MC) simulations are performed to get significant analytical results while considering the process and mismatch variations. However, to include also the effect of the parameters listed in Table I, corners are added to the MC simulation. We performed all the simulations using Cadence IC6.16 and HCMOS9 ST-microelectronics technology. A 400ns period pulse is used to program the RRAM cells.

C. Main characteristics of LRR-PUF

In this section, we introduce the relevant characteristics of the LRR-PUF, and we discuss the results.

1) Reconfigurability

By resetting all the RRAM cells after the response generation, it is possble to reconfigure the LRR-PUF to an entirely new state. The advantages of the proposed architecture are:

(1) No additional circuitry is required to make the LRR-PUF act as a reconfigurable PUF (and hence lower cost compared to other PUFs).

(2) Nearly unlimited possible configurations (i.e., the number of times that RRAM cells can be RESET then SET again to a new state).

(3) The prediction of the LRR-PUF new state is almost improbable due to the stochastic nature of the memristor switching behavior caused by the arbitrary conductive filament formation/rupture, as shown in Fig. 8.

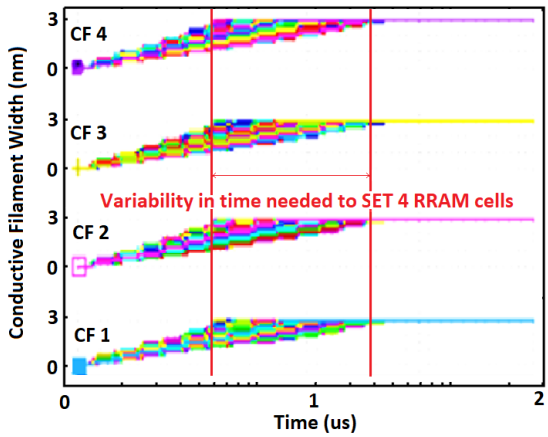

Fig. 8 Conductive Filament variability measurements in SET time for the 4 RRAM cells under cycle-to-cycle variations.

The reconfiguration of the LRR-PUF is straightforward. A new state of the PUF is possible after all RRAM cells are RESET. After that, addressed cells are switched back from high to low resistance state by applying a positive voltage to the selected column using the programming logic shown in Fig. 7.

Given the intrinsic randomness of the switching behavior and the use of 4 cells in parallel instead of one in the other RRAM based PUF, the reversibility is unattainable, which makes the LRR-PUF stronger against any attack and mainly modeling attacks and reverse engineering [17].

2) Reliability

Fig. 9 shows the cell current obtained after 6500 Monte Carlo runs under variability during the SET process. A failure is associated with a current value bellow the sense amplifier reference current, which is in our case is set to 100uA. For a single bit LRR-PUF cell (1T4R), we detected only one current failure over 6,500 simulation runs, which represents an error rate of 0.0153% (i.e., almost 100% reliability).

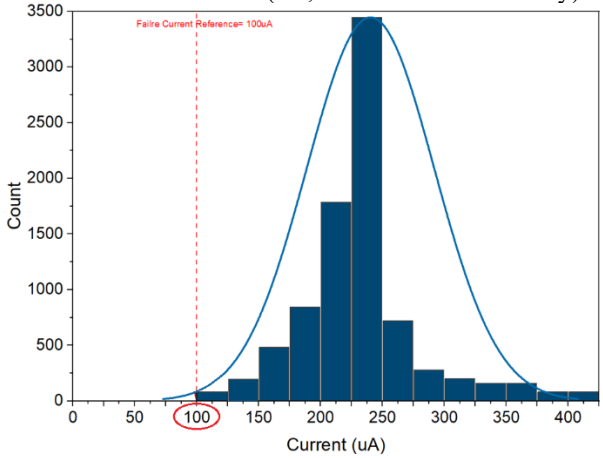

Fig. 9 Current of a single bit RRAM cell in the LRR-PUF array under variation of parameters listed in Table I.

Since the Stanford model [16] used to simulate the LRR-PUF includes temperature dependency, we performed the same simulation under different temperatures: room temperature, 40°C and 85°C. Table II indicates the results.

TABLE. V RELIABILITY UNDER DIFFERENT TEMPERATURES

	Room Temp	40°C	85°C
Number of current failure	1	179	319
Reliability (%)	≈ 100	97.24	95.09

3) Uniformity

Over 6,000 arbitrary distinct challenge sets are applied to the same LRR-PUF to test and validate the uniformity and diffuseness of the LRR-PUF. We evaluated the responses collected at the output of the XOR gates.

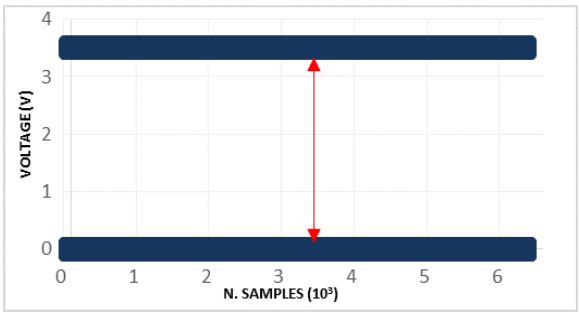

Fig. 10 Output voltage distribution of the LRR-PUF.

Fig. 10 shows the 0/V_{DD} voltage distribution and Fig. 11 depicts the 0/1 distribution of the obtained responses. The near-ideal uniformity shown in both figures derives from the stochastic RRAM resistance switching variability and is critical for the randomness of the PUF.

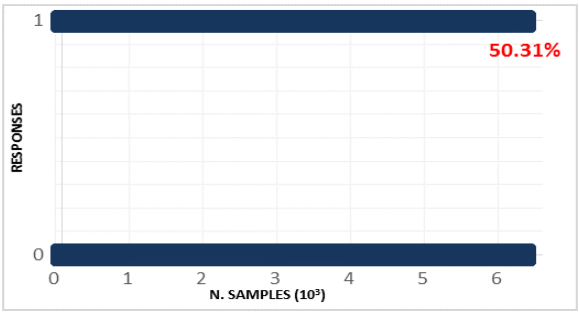

Fig. 11 Binary response distribution of the LRR-PUF.

4) Randomness

We apply 32 different challenges to the 1-Kbit LRR-PUF array, we collect 32 response sequences, and then we perform 3 relevant NIST [18] tests to validate the randomness-unpredictability of the proposed architecture. Table III depicts the NIST test results.

TABLE. VI RANDOMNESS: THE NIST TEST RESULTS

	P-value	Pass Rate	Success/ Failure
1. Test Input Frequencies	0.7815	31/32	Success
2. Test Input Blocks	0.9978	31/32	Success
3. Test Input Runs	0.0057	30/32	Success

Test 1 evaluates the frequencies of 0s and 1s in the sequence. Test 2 analyzes each sequence by dividing it into 4 blocks of 8-bit length. Test 3 checks the sequence for runs. A run is a sub-sequence where all the bits are identical.

Under the above-listed variability parameters and for the given sequence length, the 3 NIST tests are successful. However, higher sequence lengths and additional NIST tests such as Approximate-Entropy, Cumulative-Sums, etc. should be considered for future work to validate the randomness of the LRR-PUF in critical cryptographic applications.

5) Uniqueness

We performed a Monte Carlo simulation by applying identical challenges on 100 LRR-PUF instances, and then we collected the corresponding responses. The average HD of the LRR-PUF is 49.69%.

D. *Comparison with previously published PUFs*

We deduced the previously presented results of LRR-PUF from simulations similar to the other RRAM-based PUF architectures [8], [9], and [11]. Hence, it is reasonable to propose a comparison. Table IV summarizes the comparison results with the PUF architectures mentioned earlier. The proposed LRR-PUF is a good compromise with high reliability, high uniqueness, reconfigurability, and no sneak current at the same time.

IV. CONCLUSION

This paper provides a novel Lightweight Reconfigurable RRAM based PUF (LRR-PUF) that overcomes the major weaknesses of previously suggested architectures. Through extensive SPICE simulations, we demonstrated that the LRR-PUF is a robust (almost 100% reliability), and low-cost security primitive. The LRR-PUF shows high uniqueness validated by Monte Carlo simulations over more than 1,000 PUF instances, in addition to the high randomness evaluated through relevant NSIT tests. The simulated RRAM cell resistances match very well the experimental data, which is an additional validity proof of the proposed LRR-PUF evaluation process. Nevertheless, additional experimental assessment is still needed in future work.

TABLE. IV COMPARISON OF LRR-PUF WITH OTHER RRAM BASED PUFS.

	WTM-PUF [11]	XBAR-PUF [13]	RRAM-PUF [15]	EPUF [16]	LRR-PUF
Uniqueness	≈ 50%	49.9%	48.83%	N/A	49.69
Reliability	N/A	85.2%	≈ 80%*	≈ 100%	≈ 100%
Reconfigurable PUF	X	✓	✓	✓	✓
Architecture used	Memristors	RRAM Crossbar (1cell/bit)	RRAM 1T1R	RRAM crossbar (8 cell/bit)	RRAM 1T4R
Main advantages	Simple implementation	1. High density 2. Easy scalability	1. Easily reconfigured 2. No sneak currents	1. High reliability 2. High density	1. High reliability 2. No sneak currents
Main disadvantages	1. Limited CRPs 2. High sensitivity to external variations	1. Low robustness against modeling attacks 2. Requires ECC	1. Limited reliability 2. Requires ECC	1. Sneak currents 2. High ref current needed	Accurate ref current needed (**)

(*) under 10% voltage fluctuation and T=325K

(**) easily extracted from experimental data of an RRAM array

REFERENCES

[1] L. O. Chua. "Memristor—The missing circuit element." *IEEE Transaction on Circuit Theory*, vol. 18, no. 5, pp. 507-519, Sep. 1971.

[2] H.-S. P. Wong et al. "Metal-oxide RRAM." *Proceedings of the IEEE*, vol. 100, no 6, pp. 1951-1970, 2012.

[3] P. Huang, X. Y. Liu, B. Chen, et al. "A physics-based compact model of metal-oxide-based RRAM DC and AC operation." *IEEE Transaction on Electron Devices*, vol. 60, no. 12, pp. 4090–4097, Dec. 2013.

[4] Li, Haitong, et al. "Statistical assessment methodology for the design and optimization of cross-point RRAM arrays, " in *Proc. IEEE Memory Workshop (IMW)*, 2014, pp. 1-4.

[5] Grossi, Alessandro, et al. "Fundamental variability limits of filament-based RRAM, " in *Proc. IEEE Electron Devices Meeting*, 2016, pp. 4-7.

[6] S. Ambrogio, S. Balatti, A. Cubeta, A. Calderoni, N. Ramaswamy, D. Ielmini. "Understanding switching variability and random telegraph noise in resistive RAM, " in *Proc. IEEE International Electron Devices Meeting*, 2013. p. 31.5. 1-31.5. 4.

[7] G. E. Suh, and S. Devadas. "Physical unclonable functions for device authentication and secret key generation, " in *Proc. ACM DAC*, 2007, pp. 9-14.

[8] G. S. Rose, N. McDonald, L. Yan, and B. Wysocki. "A write-time based memristive puf for hardware security applications, " in *Proc. IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2013, pp. 830–833.

[9] G. S. Rose, C. A. Meade. "Performance Analysis of a Memristive Crossbar PUF Design, " in *Proc. of the 52nd Annual Design Automation Conference (DAC)*, 2015, pp. 1-6.

[10] A. Chen. "Utilizing the variability of resistive random access memory to implement reconfigurable physical unclonable functions. " *IEEE Electron Device Letter*, vol. 36, no. 2, pp. 138140, Feb. 2015.

[11] A. Shrivastava, P. Chen, Y. Cao, S. Yu, and C. Chakrabarti. "Design of a reliable RRAM-based PUF for compact hardware security primitives," in *Proc. IEEE International Symposium on Circuits and Systems (ISCAS)*, Montreal, 2016, pp. 2326-2329.

[12] K. Kursawe, A. R. Sadeghi, D. Schellekens, B. Skoric, and P. Tuyls. "Reconfigurable physical unclonable functions—Enabling technology for tamper-resistant storage, " in *Proc. IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2009, pp. 22-29.

[13] M.-C. Wu, Y.-W. Lin, W.-Y. Jang, C.-H. Lin and T.-Y. Tseng. "Low-power and highly reliable multilevel operation in ZrO2 1T1R RRAM." *IEEE Electron Device Lett*., vol. 32, no. 8, pp. 1026–1028, Aug. 2011.

[14] H. Aziza, B. Hajri, M. M. Mansour, A. Chehab, and A. Perez. "A lightweight write-assist scheme for reduced RRAM variability and power." *Microelectronics Reliability*, vol. 88, pp. 6-10, 2018.

[15] G. E. Suh, S. Devadas. "Physical Unclonable Functions for Device Authentication and Secret Key Generation," in P*roc. ACM/IEEE Design Automation Conference (DAC)*, 2007, pp. 9.

[16] Z. Jiang and H. P. Wong. "Resistive-switching random access memory (RRAM) Verilog-A model." Internet: https://nanohub.org/publications/19/1, Oct. 2014.

[17] M. Majzoobi, F. Koushanfar, and M. Potkonjak. "Techniques for design and implementation of secure reconfigurable PUFs." *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, vol. 2, no. 1, p. 5, 2009.

[18] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker. "A statistical test suite for random and pseudorandom number generators for cryptographic applications," in *NIST, Special Publication*, 2010, pp. 800–822.