IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 24 April 2023, accepted 9 June 2023, date of publication 28 June 2023, date of current version 7 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3290896

RESEARCH ARTICLE

True Random Number Generator Based on the Variability of the High Resistance State of RRAMs

MARYAM AKBARI[1], SATTAR MIRZAKUCHAKI[1], DANIEL ARUMÍ[2], SALVADOR MANICH[2], (Member, IEEE), ALVARO GÓMEZ-PAU[2], (Member, IEEE), FRANCESCA CAMPABADAL[3], MIREIA BARGALLÓ GONZÁLEZ[3], AND ROSA RODRÍGUEZ-MONTAÑÉS[2]

[1]Department of Electrical Engineering, Iran University of Science and Technology, Tehran 16846-13114, Iran
[2]Department of Electronics Engineering, Universitat Politècnica de Catalunya, 08034 Barcelona, Spain
[3]Centre Nacional de Microelectrònica, Institut de Microelectrònica de Barcelona (CSIC), Bellaterra, 08193 Barcelona, Spain

Corresponding authors: Sattar Mirzakuchaki (m_kuchaki@iust.ac.ir) and Rosa Rodríguez-Montañés (rosa.rodriguez@upc.edu)

This work was supported in part by the Spanish Ministry of Science, Innovation, and Universities under Grant PID2019-103869RB-C33/AEI/10.13039/501100011033; and in part by the Fondo Europeo de Desarrollo Regional (FFEDER) funds under Grant TEC2017-84321-C4-1-R.

ABSTRACT Hardware-based security primitives like True Random Number Generators (TRNG) have become a crucial part in protecting data over communication channels. With the growth of internet and cloud storage, TRNGs are required in numerous cryptographic operations. On the other hand, the inherently dense structure and low power characteristics of emerging nanoelectronic technologies such as resistive-switching memories (RRAM) make them suitable elements in designing hardware security modules integrated in CMOS ICs. In this paper, a memristor based TRNG is presented by leveraging the high stochasticity of RRAM resistance value in OFF (High Resistive) state. In the proposal, one or two devices can be used depending on whether the objective is focused on saving area or obtaining a higher random bit frequency generation. The generated bits, based on a combination of experimental measurements and SPICE simulations, passed all 15 National Institute of Standards and Technology (NIST) tests and achieved a throughput of tens of MHz.

INDEX TERMS True random number generator (TRNG), resistive random access memory (RRAM), RRAM based TRNG.

I. INTRODUCTION

Since the number of IoT devices is growing by huge amounts, the cryptographic applications of electronic devices like Random Number Generators (RNG) are becoming integral in today's life. The two main types of RNGs are the pseudo random number generator (PRNG) and the True Random Number Generator (TRNG). PRNGs mainly produce random bits using a deterministic function along with a seed. This process is similar to that followed by linear feedback shift registers (LFSR) which are based on a deterministic seed and, thus, the generated bits are emulating randomness therefore being vulnerable against modeling attacks. TRNGs can be realized by extracting any nondeterministic function like intrinsically stochastic physical characteristic of the device. These physical unpredictable phenomena can be, among others: random telegraph noise (RTN) [1], soft breakdown of gate oxides [2], thermal noise generated by resistors [3], clock jitter in ring oscillators ROs [4], [5] or metastable state [6]. Most of the state of the art TRNGs are implemented in CMOS technology and, in many cases, these designs and implementations introduce bias [7], [8], [9].

Thermal noise stands out as the most popular source of randomness among physical sources of entropy in TRNG designs due to its technology-invariance and frequency-independence [10]. A direct amplification of the thermal noise has been proposed in [11] and [12] while [8] uses a single inverter with multi-time amplification. The amplified noise is compared to a given threshold to generate the random sequences. However, the analog amplifier required for the

The associate editor coordinating the review of this manuscript and approving it for publication was Gian Domenico Licciardo.

detection of thermal noise necessitates a high-gain in a wide-band, hence resulting in large power dissipation. Moreover, the existence of an offset in the amplification eventually limits the performance and demands the need of calibration or post-processing [11], [12].

In most cases, thermal noise is indirectly harvested through jitter in ring oscillators [11], [13], [14] and metastability in latches [7], [15] or in sense-amp [7]. RO-based TRNGs are frequently designed with simplicity and exhibit noise injection attack tolerance through an automatic tuning loop [14]. However, many inverters in ROs not only occupy a large area but also consume a significant amount of power due to successive charge and discharge during operation. Metastability-based implementations can provide a fast response with excellent energy efficiency, but they also require considerable effort to calibrate and suppress device mismatches [7], [10], [19], [20]. Latch-based TRNGs offer low power consumption and small size due to the simple structure of the latch and the fact that data generation requires only a one-time voltage transition. However, a mismatch in the latch's inverter pair biases the output, resulting in low randomness. To overcome it, a capacitance-based charge pump is used in [16] and [17]. This analog method consumes space and power. The design in [10], [18], and [20] requires a complex calibration circuit and feedback control loop to compensate for mismatches. In general, the need for runtime calibration for process, voltage, and temperature (PVT) variations not only prevents the fast operation but also increases costs in power and area [21].

In order to mitigate the aforementioned problems, the use of stochastic properties like the probabilistic mechanism of transport and/or the switching characteristics of emerging nanoscale devices (spin transfer-torque, magnetic memory and memristors) have been recently proposed [22], [23], [24]. Intrinsic entropy source with high quality randomness including device-to-device (D2D) variability within a memory array or a wafer [25], [26], [27] and cycle-to-cycle (C2C) variability for the same device at each cycle [23], [28], make memristors in general, and RRAM in particular, quite suitable devices for generating true random numbers [29]. Also, they offer a large resistance window, area scalability, high endurance and low power characteristics. Metal-oxide RRAMs have been shown to feature current programming in the nA range [30], [31], sub-nanosecond switching [32], [33] and sub-10-nm scalability [34]. Additionally, these devices exhibit endurance capabilities of up to 10^{11}-10^{12} cycles [35], [36]. The proposed methods for implementing TRNGs based on memristor are cycle-to-cycle (C2C) variation [37], RTN [22], [38], device-to-device (D2D) variation [25], [26], and stochastic switching [23], [27]. It has been reported in many of these works that the generated bits from these TRNGs need post processing to be truly random [27], [38] which costs energy and area overhead. Also, they cannot achieve a bit generation rate higher than a few hundreds of kb s^{-1}. In this work we use C2C variability in RRAMs in OFF state as the main entropy source to generate multiple random bits. The generated bits pass all the 15 NIST tests therefore proving to be truly random. The generated bits pass all 15 NIST tests providing preliminary evidence of the data's randomness.

This paper is organized as follows. RRAM devices and the experimental setup used in this work are explained in Section II. The architecture for the proposed TRNG is described in Section III. In Section IV, experimental results are presented and, finally, conclusions are drawn in Section V.

II. EXPERIMENTAL SET-UP

The RRAM devices considered in this work are TiN/Ti/HfO_2/W structures [37]. The 10 nm-thick HfO_2 layer was grown by atomic layer deposition (ALD) at 225°C using TDMAH and H_2O as precursors, and the top and bottom metal electrodes were deposited by magnetron sputtering. The bottom electrode consists of a 50 nm-W layer deposited on a 20 nm-Ti adhesion layer on a highly doped n-type silicon wafer, and the top electrode is a 200 nm-TiN on a 10 nm-Ti layer acting as oxygen getter material. Electrical contact to the bottom electrode is made through the Al-metallized back of the silicon wafer. The resulting structures are square cells of different sizes, but the cells considered through out this work were of 15 × 15 μm^2. A top view optical image of one device is shown in Figure 1(a) and the corresponding schematic cross-section of the active area is given in Figure 1(b).

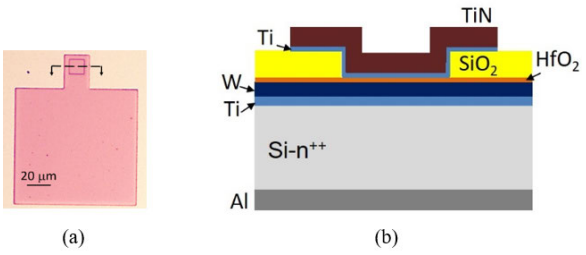

FIGURE 1. The RRAM devices used in this study (a) Top view image. (b) The cross sectional schematic.

The total resistance of the RRAM drops by applying a positive bias voltage (V+) to the top electrode during the SET operation. On the contrary, the resistance of the RRAM increases by connecting a reversed bias voltage (V+) to the top electrode resulting in a RESET operation of the device. After a SET, the device is in a Low Resistive State (LRS) and has a R_{LRS} resistance, while after a RESET, the device is in a High Resistive State (HRS) and presents a R_{HRS} resistance.

As illustrated in Figure 2, the electrical characterization in this work was achieved by using a Keysight B2912A Precision Source/Measure Unit (SMU) and a probe station. The automatic measurements were controlled and monitored by Matlab through a GPIB connection to the instruments.

In order to change and measure the resistance of the device, the aforementioned positive or negative voltage is applied to the top electrode while the bottom electrode is connected to ground.

First, as shown in Figure 3(a), the DC resistive switching behavior of the fabricated RRAM device was evaluated by applying double-sweep voltage ramps from 0 to 1.1 V for the SET operation and from 0 to -1.4 V for the RESET operation. These voltage values were extracted after previous extensive characterization of the manufacturing technology. The DC analysis of the device allows the verification of its correct behaviour. The resistive switching behavior of the RRAM was also assessed under pulse mode, as indicated in Figure 3(b), by applying a square waveform with the same voltage amplitudes as in DC mode. It can be seen from Figures 3(a) and (b) that the cycle-to-cycle variability of the device is larger in HRS than in LRS.

In order to obtain a significant number of R_{HRS}, a set of 10^6 cycles were carried out. Figure 4(a) illustrates the distribution of the measured resistances. Figure 4(b) shows the cumulative probability plot.

III. PROPOSAL FOR THE TRNG

The random numbers generated in this proposal are extracted from the variability of the high resistance state (HRS) of a RRAM device. The set of 10^6 resistances experimentally measured in our laboratory are used as the main entropy source. As depicted in Figure 3(b), it can be observed that the variability of R_{HRS} is higher than that of R_{LRS}. In order to work with magnitudes easily computed by means of digital circuits, HRS resistances are converted into time delays. In this work, this step has been done by means of electrical SPICE-based simulations where the R_{HRS} values have been extracted from the experimental measurements previously carried out. The design of the circuit is based on a STMicroelectronics 65nm CMOS process.

Figure 5 illustrates the basis of the circuit for the resistance-to-delay conversion composed of one-transistor one-memristor cell structure (1T1R), which acts as a voltage divider and controls a transmission gate that allows the charging of capacitor *cap*. The voltage of the capacitor feeds an inverter followed by an AND gate that controls the Enable input of a counter. The output of the counter is registered and the capacitor can be discharged through an nMOS transistor M_d.

In the proposed circuit, once the memristor is switched to HRS, the voltage sensed at V_{cont} during reading at the voltage divider is used to control the transmission gate. This stage needs to be done with a reading voltage low enough for not disturbing the memristor state. Furthermore, the resulting control voltage V_{cont} is not a digital signal but an intermediate analog one and, for this reason, no inverter is required between the signals controlling the gate nodes of the PMOS and NMOS transistors of the transmission gate. Depending on the resulting divider voltage, the transmission gate offers a different resistance and determines the time needed by the capacitor to achieve the threshold voltage that will stop the counter. The process of charging the capacitor (V_{cap}) begins with the input pulse V_{start} passing through the transmission gate (indicated as t_0 in Figure 6). The capacitor is connected to an inverter in such a way that when V_{cap} reaches the threshold level of the inverter, its output goes low (t_1) creating a pulse at the output of an AND gate (see Figure 6). This pulse is used as the enable signal of the counter. According to the range of R_{HRS} expected in the RRAM technology used in the work and the frequency range appropriate for the generation of random numbers, capacitor *cap* has been chosen to be 10 fF. This value is selected within an appropriate range so that its impact on area is small, while ensuring that the conversion time constant falls within the range of the processing circuit delays.

Due to the intrinsic variability of R_{HRS}, different delays are obtained in each cycle. This leads to the creation of different pulse widths which are sampled at a fixed clock frequency f_{CLK}, which is connected to the clock input of the counter (f_{CLK}=10GHz in our simulations). Figure 6 illustrates an example where the generated delay ($t_1 - t_0$) is 17.2 ns for the case of $R_{HRS} = 1.52\ k\Omega$.

The relationship between the memristance and the delay is not critical. What is important is to verify the random nature of the R_{HRS} sequence experimentally obtained. In the simulations, the real $R_{HRS}(i)$ sequence was kept (where i indicates the ith RESET cycle in the experimental characterization) as input data. Figure 4(a) illustrates the obtained distribution of R_{HRS}. The randomness of R_{HRS} was evaluated through the direct mathematical conversion of the $R_{HRS}(i)$ data into binary coded numbers $(b_n, b_{n-1}, \ldots, b_1, b_0)_i$. Since the R_{HRS} values are on the order of tens of kΩ, 14 bits were considered for this preliminary study. The randomness of these bits was assessed by the tests settled by the NIST Statistical Test Suite (STS). As a result, the least 6 significant bits passed all or failed at maximum 2 tests out of the 15 tests. In order to evaluate if the reason for not passing the complete set of 15 tests is due to some level of dependency of the conductive filament for consecutive switching transitions, the same analysis has been performed over the difference between R_{HRS} close in the sequence, namely, $R_{HRS}(i)$ and $R_{HRS}(i+j)$ for $1 \leq j \leq 5$. Thus, the subtractions $(R_{HRS}(i+j) - R_{HRS}(i))$ have been computed for $1 \leq i \leq 10^6$ and $1 \leq j \leq 5$, coded binary and assessed by NIST test. As a result, comparing R_{HRS} separated by at least 3 positions in the sequence ($j \geq 3$) is enough to make the 6 least significant bits pass all tests. Given the switching speed of RRAMs and the auxiliar circuitry needed, with these 6 bits the design of a TRNG with high throughput seems viable. These results make us assume that comparing the R_{HRS} for different cycles separated by at least 3 cycles compensates any possible dependence between cycle-to-cycle R_{HRS} resistances and results in random values. For the experimental 10^6 measures of this work, $\text{mean}(R_{HRS}) = 3069.15\ \Omega$ and $\text{mean}(abs(R_{HRS}(i+3) - R_{HRS}(i)) = 568.78\ \Omega$.

In the next section, the results of the work are presented.

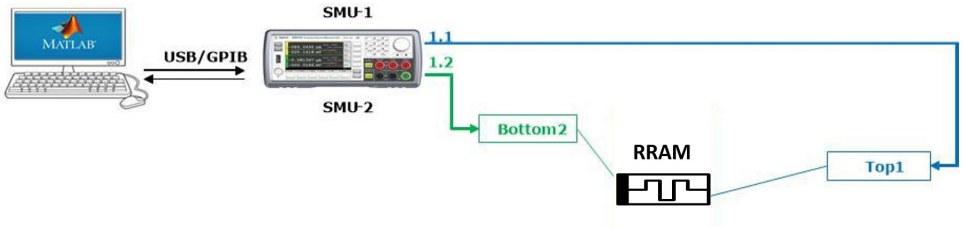

FIGURE 2. Experimental setup.

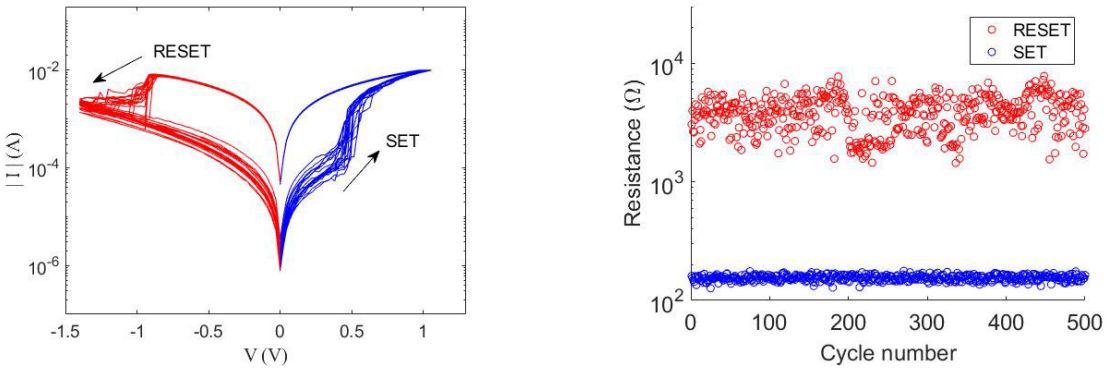

FIGURE 3. (a) Current/Voltage characteristics of the RRAM during successive SET and RESET operations in DC mode. (b) R_{LRS} and R_{HRS} resistances after SET and RESET operations in pulse mode.

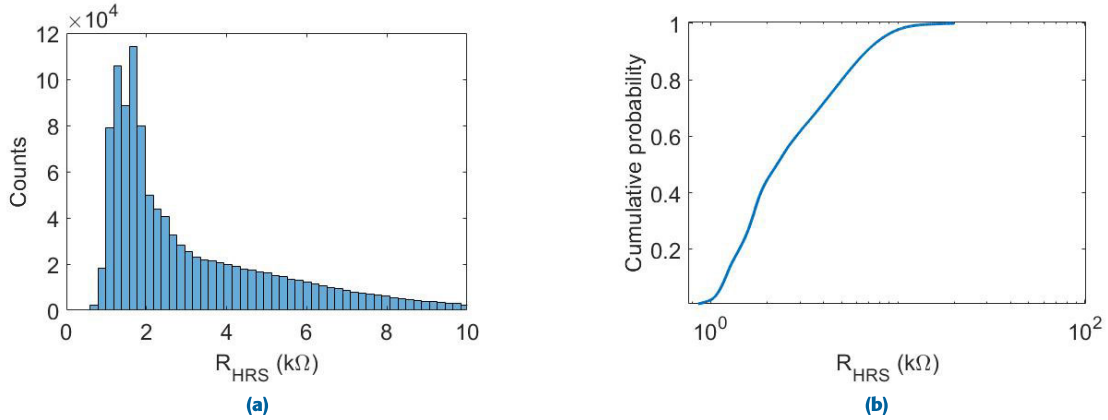

FIGURE 4. (a) Distribution of the experimental 10^6 R_{HRS} measured values from a sample RRAM under pulsing operation. The experimental data follow a lognormal distribution with μ=7.86 and σ=0.65 (b) Cumulative probability plot.

IV. RESULTS AND DISCUSSION

A. GENERATION BY MEANS OF ONE RRAM DEVICE

According to the previous section, the comparison between a pair of R_{HRS} generated at different switching cycles of a RRAM device provides the source of randomness for the TRNG. For generating the random bit, the proposal of this work consists in switching a RRAM device to HRS and computing the delay caused in the basis of the circuit of Figure 5 coded as ($count_1$). Next, the device is switched to HRS 3 more times (2 of them are dummy transitions) and the delay is computed again ($count_2$) and subtracted from the previous one, ($count_2 - count_1$). To perform the subtraction, in the particular case of 1-bit counter, it is equivalent to perform an addition. So, the 1-bit counter is only initialized before generating ($count_1$). The final ($count_1 + count_2$) yields the random generated bit.

In order to use the minimum silicon area possible, the circuit used in this work is shown in Figure 7 where the voltage of the divider (V_{cont}) has been shifted since the range of voltages generated is too low to control the gate of M_n due to that V_{read} is low enough for not disturbing HRS. The voltage shifter is made up of a pMOS transistor and a nMOS

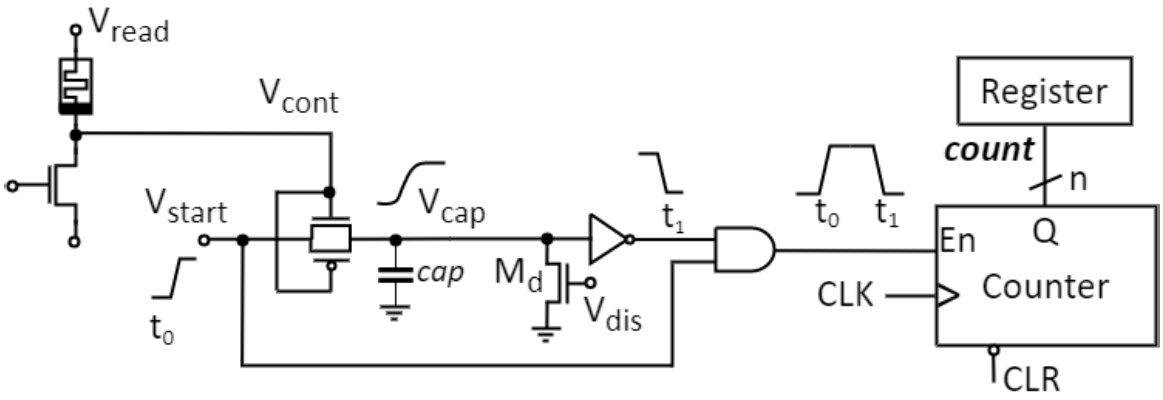

FIGURE 5. Circuit for converting the R_{HRS} value into a delay with n-bits resolution.

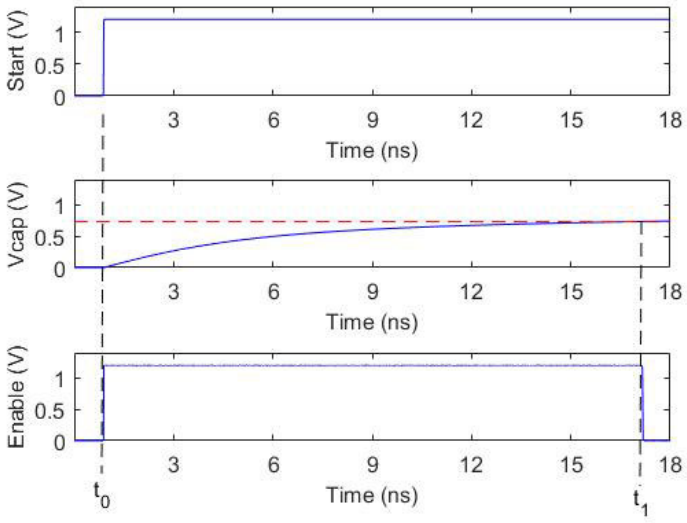

FIGURE 6. Example of operation of the circuit where the capacitor (cap=10 fF) starts charging at t_0 and V_{cap} reaches the threshold value after 17.2 ns (t_1) for $R_{HRS} = 1.52\ k\Omega$. The Enable signal of the counter is active during the (t_0, t_1) interval.

transistor acting as a resistor. The transmission gate has been replaced with an nMOS transistor. Furthermore, the counter is not active (through signal V_{activ}) during the process of discharging *cap* and switching control of the RRAM. Figure 8 illustrates the state of the reset signal (activated before generating $count_1$) and the discharge of *cap* ($V_{activ} = 0$). Also, the two dummy HRS cycles have been indicated in grey. Before each HRS transition a LRS transition is needed although not shown in the figure.

For the case of cap=10 fF, the mean delay value obtained is 16.9 ns and the maximum delay is 29.3 ns resulting in a mean time equal to 33.8 ns required to charge two times the capacitor. Figure 9(a) illustrates the delay versus R_{HRS} for different sizes of the pMOS M_p of the voltage shifter (referred to the minimum feature of the technology, $L_{min} = 0.65\mu m$) and (b) the distribution of delays obtained for the set of 10^6 samples. Table 1 indicates the area or size of the different elements of the circuit.

TABLE 1. Area / size of the cells/devices used in circuit of Fig. 7.

Cell	Area (μm^2) or Width
M_p, pMOS	W = 8.5 L_{min}
R_A, nMOS	W = 1 L_{min}
M_n, nMOS	W = 5 L_{min}
M_d, nMOS	W = 2 L_{min}
HS65_LS_IVX2	3 μm^2
HS65_LS_AND3X4	5.4 μm^2
HS65_LS_DFPHQNX4	13 μm^2 *

* modified to include Reset

The randomness of this TRNG has been assessed by the tests settled by the NIST STS. The randomness of the

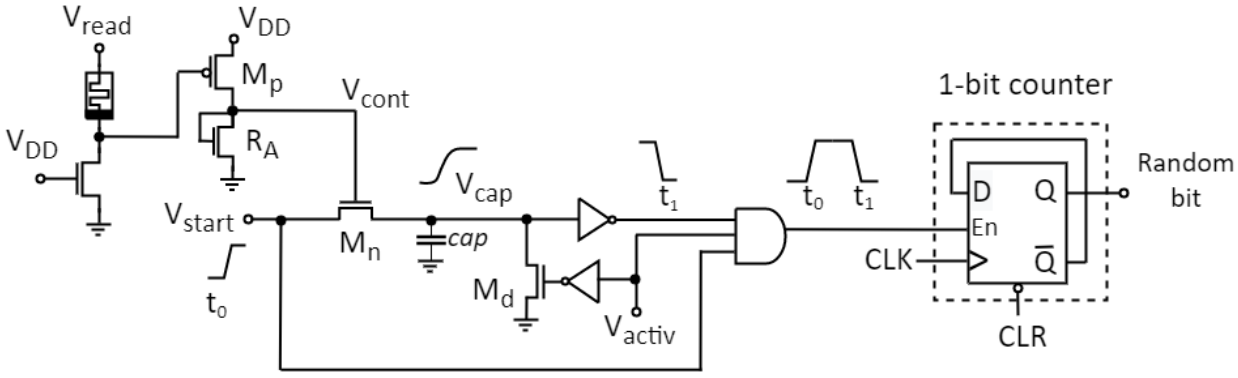

FIGURE 7. Circuit for the generation of one random bit by means of one RRAM device.

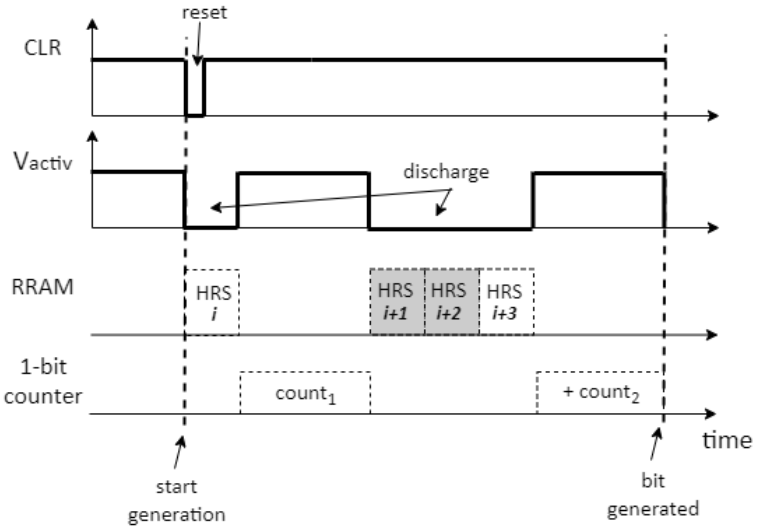

FIGURE 8. Reset and active signals during the process of generating a random bit. Note that each HRS cycle is preceded by a LRS not shown in the time diagram. Dummy HRS cycles are indicated in grey.

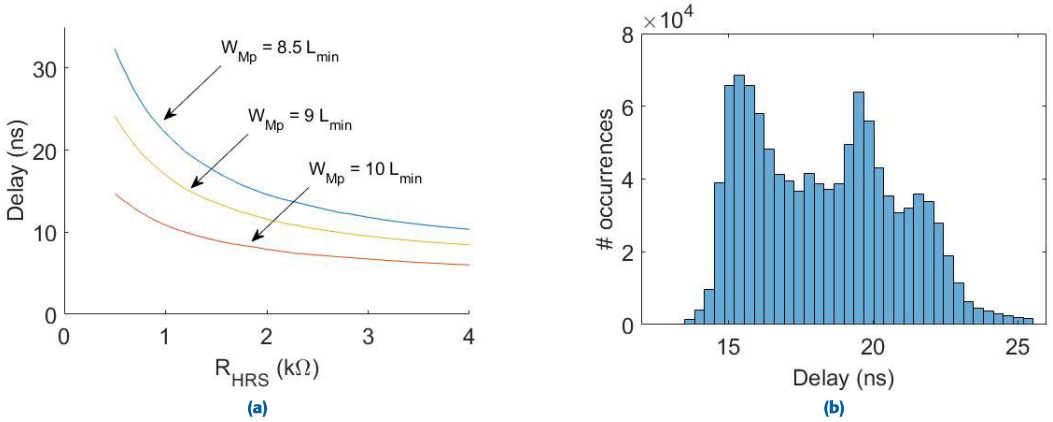

FIGURE 9. (a) Delay dependence on R_{HRS} for different widths of pMOS transistor M_P. (b) Distribution of delays.

dataset is indicated by P-value. The P-value more than 0.01 is required to pass a specific test. All 15 NIST tests have been applied on the 10^6 derived bits. Results are shown in Table 2 where the column labeled "raw bit" indicates the result of NIST test applied to the direct bit ($count_1$) extracted from the circuit. Only 5 test passed and 3 can not be applied because of

TABLE 2. NIST test results for the random bit obtained from the circuit of Figure 7. Column labeled "raw bit" indicates direct results of $count_1$. Column labeled with "added bit" is derived from comparing/adding bits from two HRS cycles separated by 2 dummy transitions, i.e., $count_1 + count_2$.

	raw bit ($count_1$)		added bit ($count_1 + count_2$)	
Test	P-value	result	P-value	result
Frequency	0.000000	FAILED	0.387067	PASSED
Block frequency	0.000000	FAILED	0.047188	PASSED
Cumulative sums (forw/rev)	0.000000	FAILED	$>$ 0.440477	PASSED
FFT	0.503539	PASSED	0.577474	PASSED
Linear complexity	0.531463	PASSED	0.910111	PASSED
Runs	-		0.068284	PASSED
Longest runs of ones test	0.000101	FAILED	0.189096	PASSED
Rank	0.801291	PASSED	0.473964	PASSED
Nonoverlap. templates	$>$ 0.000000	FAILED	$>$ 0.018899	PASSED
Overlap. template all ones	0.000000	FAILED	0.411706	PASSED
Universal statistical	0.557208	PASSED	0.948667	PASSED
Approximate entropy	0.000000	FAILED	0.196116	PASSED
Random excursions	-		$>$ 0.104005	PASSED
Random excursions variant	-		$>$ 0.058283	PASSED
Serial	$>$0.223090	PASSED	$>$ 0.734575	PASSED

TABLE 3. NIST test results.

	circuit of Fig. 10 (two RRAMs)	
Test	P-value	result
Frequency	0.231036	PASSED
Block frequency	0.301739	PASSED
Cumulative sums (forw/rev)	$>$ 0.176974	PASSED
FFT	0.712308	PASSED
Linear complexity	0.138627	PASSED
Runs	0.292252	PASSED
Longest runs of ones test	0.393486	PASSED
Rank	0.852243	PASSED
Nonoverlap. templates	$>$ 0.016186	PASSED
Overlap. template all ones	0.870248	PASSED
Universal statistical	0.883179	PASSED
Approximate entropy	0.108698	PASSED
Random excursions	0.030241	PASSED
Random excursions variant	0.302457	PASSED
Serial	$>$ 0.564126	PASSED

not enough data. Column labeled "compared bit" shows the NIST test results for the proposal of comparing (addition) bits obtained for two cycles separated by 2 dummy transitions, i.e., corresponds to count $= count_1 + count_2$. All 15 test passed in this case.

Notice that, for the sake of utilizing the entire available dataset of 10^6 samples to apply the 15 NIST tests, the first bit is generated using the values of $R_{HRS}(1)$ and $R_{HRS}(4)$, while the second bit is generated using the values of $R_{HRS}(2)$ and $R_{HRS}(5)$, and so on. This approach involves using sequences of six consecutive $R_{HRS}(i)$ values, namely $[R_{HRS}(6k), \ldots, R_{HRS}(6k+5)]$, to generate three bits, i.e., $[bit(k), bit(k+1), bit(k+2)]$. Specifically, the proposed scheme requires the utilization of three 1-bit counters to store $count_1(k)$ for $R_{HRS}(6k)$, $count_1(k+1)$ for $R_{HRS}(6k+1)$, and $count_1(k+2)$ for $R_{HRS}(6k+2)$, respectively. To generate the first bit of the three-bit output sequence, $count_2(k)$ is activated when the value of $R_{HRS}(6k+3)$ is obtained. Similarly, $count_2(k+1)$ and $count_2(k+2)$ are activated when the values of $R_{HRS}(6k+4)$ and $R_{HRS}(6k+5)$ are obtained, respectively, to generate bit(k+1) and bit(k+2). Notice that this counter interleave strategy used for the experiments could be applied to any similar TRNG to maximize throughput, regardless of the RRAM cycle distance used.

To verify that the random behavior of the proposal is due to the stochastic nature of the RRAM device and not to the experimental setup or instrumentation, we conducted the same experiment but substituted the RRAM with a plain resistor. The resulting behavior was proven not to be random, with the percentage of zeros and ones significantly biased from 50%.

As far as the throughput of the proposal is concerned, the time required to apply a number of SET and RESET operations to the RRAM has to be considered in addition to the delay generated to charge the capacitor. In this context, the presented implementation provides a throughput higher than Mbps, which is sufficient for some encryption applications [22]. RRAM devices have been proved to switch at faster speed even in the sub-nanoseconds range (<5ns has been assumed in this paper) [39], [40]. In this implementation, the RRAM have to be switched 8 times (<40ns) and the delay have to be measured twice (<2 × 29.3ns) resulting in a throughput higher than 10Mbps.

B. GENERATION BY MEANS OF TWO RRAM DEVICES

With the goal of increasing the rate of the generated random bit, the comparison of the delay caused by two RRAMs has been considered with the circuit shown in Figure 10 (discharge transistor and reset are not included for simplicity). We experimentally characterized a second RRAM device to obtain an additional set of 10^6 HRS measurements, which

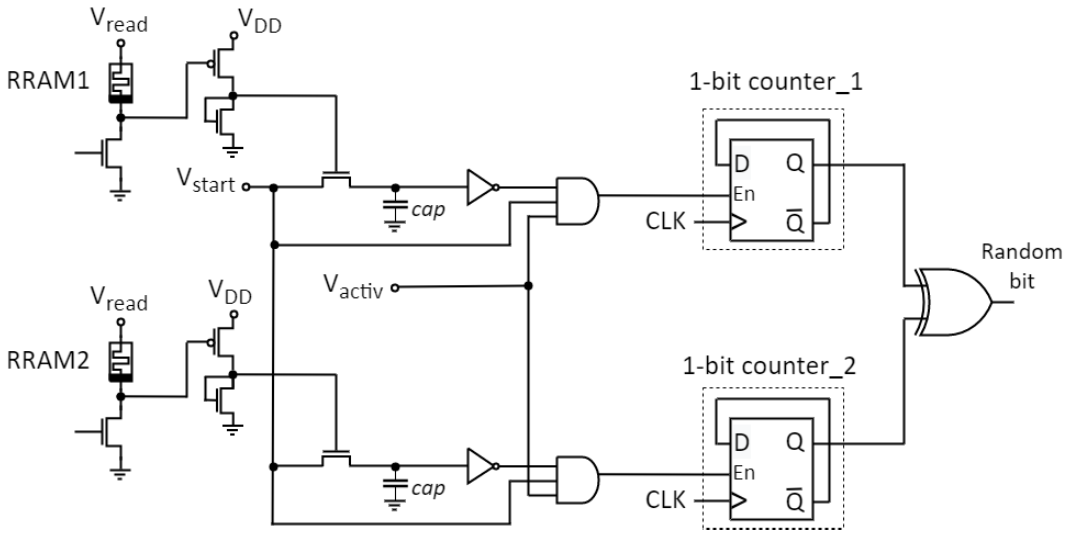

FIGURE 10. Circuit for the generation of one random bit by means of two RRAM devices.

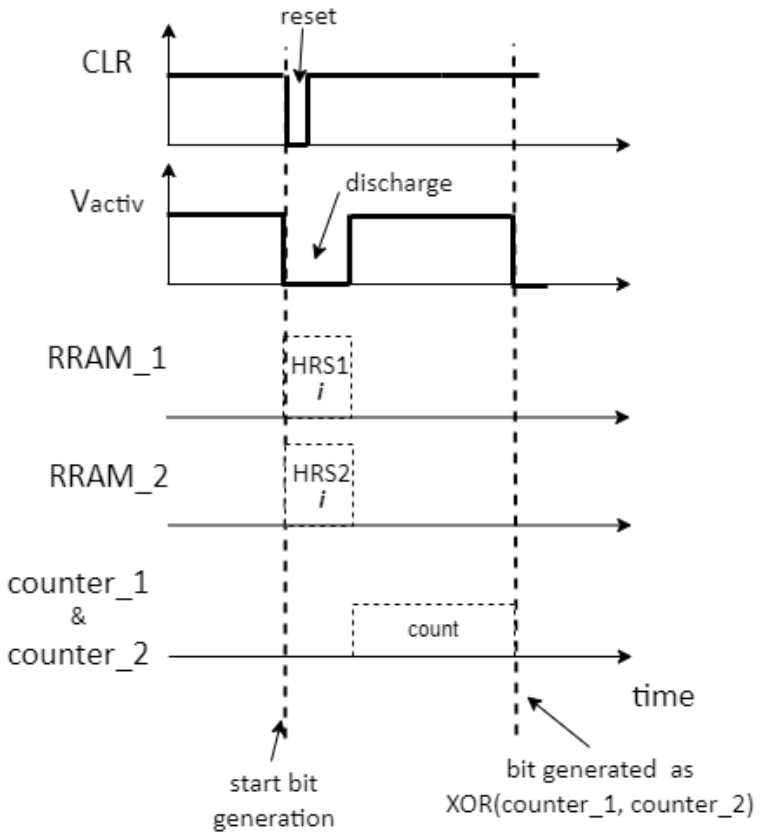

FIGURE 11. Reset and active signals during the process of generating a random bit by means of two RRAMs. Each HRS cycle is preceded by a LRS not shown in the time diagram.

enabled us to validate this proposal. Figure 11 illustrated the timing evolution of the main signals. The results of applying the NIST tests on the results are shown in Table 2 where all tests passed. The area required for this solution doubles the previous one with the addition of an XOR gate implemented with cell $HS65\_LS\_XOR2 \times 3$ that occupies 6 μm^2. However, the time needed to generate the random bit requires a single transition to HRS of both RRAMs (<10ns) and the

TABLE 4. Performance benchmarking with recent works on RRAM-based TRNGS.

Work	[41]	[37]	[25]	[42]	[43]	[44]	This work 1 x RRAM	This work 2 x RRAM
simulated / experim.	simul.	exper.	exper.	exper.	exper.	exper.	exper.	exper.
Random source	Intra-device + Inter-device switching variability	Intra-device RESET switching variability	Inter-device switching variability	RRAM switching current	Switching-time variability	Intra-device resistance variability	Intra-device resistance variability	Inter-device resistance variability
RRAM cell	RRAM+R	RRAM+R	kbit array	8x8 array	array	kbit array	1T1R	2x1T1R
Additional circuit	SR Latch	Comparator + counter	Comparator	Comparator	FPGA	Counter + DFF	4T + 2inv + AND + DFF	8T + 4inv + 2AND + 2DFF + XOR
NIST passed	15	9/9	12/12	12/15	15	15	15	15
Post-processing	No	No	XOR	XOR	XOR	No	No	XOR
Energy	-	-	-	138 pJ/bit *	-	3.51 pJ/bit **	3.28 pJ/bit ***	1.3 pJ/bit ***
Area / technology	1.4 μm^2 (65nm)	-	-	1297 μm^2 (130nm)	-	-	21.5 μm^2 (65nm)	43 μm^2 (65nm)
Sequence	10^7 bits	$20{\cdot}10^3$ bits	10^7 bits	$49{\cdot}10^3$ bits	10^7 bits	-	10^6 bits	10^6 bits
Throughput	10 Mbit/s	-	10 kbit/s	-	0.25 kbit/s	1.1 Mbit/s	10 Mbit/s	25 Mbit/s

* during global SET with $V_{BL} = 1.2$ V, $I_{TOT} = 1150$ µA, $t_{SET} = 100$ ns.
** RRAM array only.
***RRAM cell(s) during generation

consequent delay for charging the two capacitors cap in parallel (<29.3ns) resulting in a throughput higher than 25Mbps.

We have evaluated the performance of the proposed TRNG implementations against recent RRAM-based TRNGs, as shown in Table 4. Our proposals offer a high range of throughput while maintaining a quite compact area. Furthermore, the 10^6 output bitstreams generated by our TRNG implementations have successfully passed all the NIST tests. In terms of energy per bit, our proposal consumes less than previous state-of-the-art TRNGs, as shown in row "energy" where, for the sake of comparison with [42] and [44], the energy of the RRAM cell is measured only. However, in a final implementation, the consumption of the extraction circuitry beyond the RRAM cells should be considered for the total energy budget. In our proposal, it corresponds to 9,49 pJ/bit and 3.79 pJ/bit, respectively, for one/two RRAM cells. This should be compared to the equivalent circuitry of other works (e.g. comparator / counter / DFF) if available. Our proposal using two RRAM cells (Figure 10) is the most competitive in terms of energy per random bit.

As far as the reliability of the proposed TRNG is concerned in front of temperature variations, it is worth noting that Ti/HfO_2-based devices are known for their high thermal stability [44], [45], allowing them to withstand significant temperature changes without affecting their performance or reliability. Therefore, temperature is not expected to be a reliability issue in the resistance states of Ti/HfO_2based technology, which serves as the foundation for the presented random number generation. Furthermore, the switching behavior of RRAMs has been shown to depend on the width and amplitude of SET/RESET pulses [46], [47], [48]. Therefore, prior characterization of the RRAM technology is essential for ensuring reliable generation of random bits. This characterization should include determination of the optimal range of pulse duration and amplitude to achieve the correct circuit behavior. As demonstrated in [47], reducing the pulse width (i.e., increasing the frequency) can be a powerful technique for saving energy.

There are many causes that may affect the correct operation of TRNGs, from design, manufacturing or to in-field

operation. Therefore, to assure the randomness of the generated bits, TRNGs have to undergo extensive testing, not only after manufacturing but also during operation. On-the-fly tests of TRNGs implemented in hardware aim to detect failures or statistical weaknesses of the entropy source. These real-time circuits enable prompt identification of any instances where the generator fails to exhibit the intended properties, providing a mechanism to mitigate potential issues.

V. CONCLUSION

In this paper, a circuit capable of generating random bits has been proposed by expoiting the high stochasticity of the OFF state (HRS) of one or two RRAMs through its conversion to time delays. In the case of one RRAM, the delays generated for two different switching cycles of the device are compared through a 1-bit counter. In the case of two RRAMs, the delays are compared through an XOR gate after being evaluated by two 1-bit counters. The randomness of experimentally generated bit has been assessed by the NIST randomness tests. The proposed TRNG designs could be applicable for security purposes like cryptographic operations, stochastic computing and others, with low power consumption and throughput higher than 10Mbps.

REFERENCES

[1] A. Mohanty, K. B. Sutaria, H. Awano, T. Sato, and Y. Cao, "RTN in scaled transistors for on-chip random seed generation," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 25, no. 8, pp. 2248–2257, Aug. 2017, doi: 10.1109/TVLSI.2017.2687762.

[2] N. Liu, N. Pinckney, S. Hanson, D. Sylvester, and D. Blaauw, "A true random number generator using time-dependent dielectric breakdown," in *Symp. VLSI Circuits Dig. Tech. Papers*, Kyoto, Japan, Jun. 2011, pp. 216–217.

[3] B. Jun and P. C. Kocher, "The Intel random number generator," Cryptogr. Res., San Francisco, CA, USA, White Paper 27, 1999, pp. 1–8.

[4] L. Ning, J. Ding, B. Chuang, and Z. Xuecheng, "Design and validation of high speed true random number generators based on prime-length ring oscillators," *J. China Univ. Posts Telecommun.*, vol. 22, no. 4, pp. 1–6, 2015, doi: 10.1016/S1005-8885(15)60661-6.

[5] B. Sunar, W. Martin, and D. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," *IEEE Trans. Comput.*, vol. 56, no. 1, pp. 109–119, Jan. 2007, doi: 10.1109/TC.2007.250627.

[6] V. B. Suresh and W. P. Burleson, "Entropy and energy bounds for metastability based TRNG with lightweight post-processing," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 7, pp. 1785–1793, Jul. 2015, doi: 10.1109/TCSI.2015.2441966.

[7] V. R. Pamula, X. Sun, S. M. Kim, F. U. Rahman, B. Zhang, and V. S. Sathe, "A 65-nm CMOS 3.2-to-86 Mb/s 2.58 pJ/bit highly digital true-random-number generator with integrated de-correlation and bias correction," *IEEE Solid-State Circuits Lett.*, vol. 1, no. 12, pp. 237–240, Dec. 2018.

[8] X. Wang, H. Liu, R. Zhang, K. Liu, and H. Shinohara, "An inverter-based true random number generator with 4-bit von-Neumann post-processing circuit," in *Proc. IEEE 63rd Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Springfield, MA, USA, Aug. 2020, pp. 285–288.

[9] R. Zhang, X. Wang, K. Liu, and H. Shinohara, "A 0.186-pJ per bit latch-based true random number generator featuring mismatch compensation and random noise enhancement," *IEEE J. Solid-State Circuits*, vol. 57, no. 8, pp. 2498–2508, Aug. 2022, doi: 10.1109/JSSC.2021.3137312.

[10] S. K. Mathew, D. Johnston, S. Satpathy, V. Suresh, P. Newman, M. A. Anders, H. Kaul, A. Agarwal, S. K. Hsu, G. Chen, and R. K. Krishnamurthy, "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.

[11] C. S. Petrie and J. A. Connelly, "A noise-based IC random number generator for applications in cryptography," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 47, no. 5, pp. 615–621, May 2000.

[12] R. Brederlow, R. Prakash, C. Paulus, and R. Thewes, "A low-power true random number generator using random telegraph noise of single oxide-traps," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2006, pp. 1666–1675.

[13] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "A high-speed oscillator-based truly random number source for cryptographic applications on a smartcard IC," *IEEE Trans. Comput.*, vol. 52, no. 4, pp. 403–409, Apr. 2003.

[14] K. Yang, D. Blaauw, and D. Sylvester, "An all-digital edge racing true random number generator robust against PVT variations," *IEEE J. Solid-State Circuits*, vol. 51, no. 4, pp. 1022–1031, Apr. 2016.

[15] N. Torii, H. Kokubo, D. Yamamoto, K. Itoh, M. Takenaka, and T. Matsumoto, "ASIC implementation of random number generators using SR latches and its evaluation," *EURASIP J. Inf. Secur.*, vol. 2016, no. 1, pp. 1–12, May 2016.

[16] D. J. Kinniment and E. G. Chester, "Design of an on-chip random number generator using metastability," in *Proc. IEEE ESSCIRC*, Sep. 2002, pp. 595–598.

[17] C. Tokunaga, D. Blaauw, and T. Mudge, "True random number generator with a metastability-based quality control," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2007, pp. 78–85.

[18] S. K. Mathew, S. Srinivasan, M. A. Anders, H. Kaul, S. K. Hsu, F. Sheikh, A. Agarwal, S. Satpathy, and R. K. Krishnamurthy, "2.4 Gbps, 7 mW all-digital PVT-variation tolerant true random number generator for 45 nm CMOS high-performance microprocessors," *IEEE J. Solid-State Circuits*, vol. 47, no. 11, pp. 2807–2821, Nov. 2012.

[19] R. Zhang, X. Wang, L. Wang, X. Chen, F. Yang, K. Liu, and H. Shinohara, "A 0.186-pJ per bit latch-based true random number generator with mismatch compensation and random noise enhancement," in *Proc. Symp. VLSI Circuits*, Jun. 2021, pp. 1–2.

[20] S. K. Satpathy, S. K. Mathew, R. Kumar, V. Suresh, M. A. Anders, H. Kaul, A. Agarwal, S. Hsu, R. K. Krishnamurthy, and V. De, "An all-digital unified physically unclonable function and true random number generator featuring self-calibrating hierarchical von Neumann extraction in 14-nm tri-gate CMOS," *IEEE J. Solid-State Circuits*, vol. 54, no. 4, pp. 1074–1085, Apr. 2019.

[21] J. Park, B. Kim, and J. Sim, "A PVT-tolerant oscillation-collapse-based true random number generator with an odd number of inverter stages," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 10, pp. 4058–4062, Oct. 2022, doi: 10.1109/TCSII.2022.3184950.

[22] C. Huang, W. C. Shen, Y. Tseng, Y. King, and C. Lin, "A contact-resistive random-access-memory-based true random number generator," *IEEE Electron Device Lett.*, vol. 33, no. 8, pp. 1108–1110, Aug. 2012, doi: 10.1109/LED.2012.2199734.

[23] H. Jiang, D. Belkin, S. E. Savel'ev, S. Lin, Z. Wang, Y. Li, S. Joshi, R. Midya, C. Li, M. Rao, M. Barnell, Q. Wu, J. J. Yang, and Q. Xia, "A novel true random number generator based on a stochastic diffusive memristor," *Nature Commun.*, vol. 8, no. 1,, p. 882, Oct. 2017, doi: 10.1038/s41467-017-00869-x.

[24] T. Tanamoto, N. Shimomura, S. Ikegawa, M. Matsumoto, S. Fujita, and H. Yoda, "High-speed magnetoresistive random-access memory random number generator using error-correcting code," *Jpn. J. Appl. Phys.*, vol. 50, no. 4S, Apr. 2011, Art. no. 04DM01.

[25] B. Cambou, D. Telesca, S. Assiri, M. Garrett, S. Jain, and M. Partridge, "TRNGs from pre-formed ReRAM arrays," *Cryptography*, vol. 5, no. 1, p. 8, Feb. 2021, doi: 10.3390/cryptography5010008.

[26] T. Zhang, M. Yin, C. Xu, X. Lu, X. Sun, Y. Yang, and R. Huang, "High-speed true random number generation based on paired memristors for security electronics," *Nanotechnology*, vol. 28, no. 45, Nov. 2017, Art. no. 455202, doi: 10.1088/1361-6528/aa8b3a.

[27] S. Balatti, S. Ambrogio, R. Carboni, V. Milo, Z. Wang, A. Calderoni, N. Ramaswamy, and D. Ielmini, "Physical unbiased generation of random numbers with coupled resistive switching devices," *IEEE Trans. Electron Devices*, vol. 63, no. 5, pp. 2029–2035, May 2016, doi: 10.1109/TED.2016.2537792.

[28] J. Postel-Pellerin, H. Bazzi, H. Aziza, P. Canet, M. Moreau, V. D. Marca, and A. Harb, "True random number generation exploiting SET voltage variability in resistive RAM memory arrays," in *Proc. 19th Non-Volatile Memory Technol. Symp. (NVMTS)*, Oct. 2019, pp. 1–5, doi: 10.1109/NVMTS47818.2019.9043369.

[29] J. Rajendran, R. Karri, J. B. Wendt, M. Potkonjak, N. McDonald, G. S. Rose, and B. Wysocki, "Nano meets security: Exploring nanoelectronic devices for security applications," *Proc. IEEE*, vol. 103, no. 5, pp. 829–849, May 2015, doi: 10.1109/JPROC.2014.2387353.
[30] W. Kim, S. I. Park, Z. Zhang, Y. Yang-Liauw, D. Sekar, H.-S. P. Wong, and S. S. Wong, "Forming-free nitrogen-doped AlO_X RRAM with sub-μA programming current," in *Symp. VLSI Technol. Dig. Tech. Papers*, Jun. 2011, pp. 22–23.
[31] Q. Luo, X. Xu, H. Liu, H. Lv, T. Gong, S. Long, Q. Liu, H. Sun, W. Banerjee, L. Li, J. Gao, N. Lu, S. S. Chung, J. Li, and M. Liu, "Demonstration of 3D vertical RRAM with ultra low-leakage, high-selectivity and self-compliance memory cells," in *IEDM Tech. Dig.*, Dec. 2015, pp. 10.2.1–10.2.4, doi: 10.1109/IEDM.2015.7409667.
[32] H. Y. Lee, Y. S. Chen, P. S. Chen, P. Y. Gu, Y. Y. Hsu, S. M. Wang, W. H. Liu, C. H. Tsai, S. S. Sheu, P. C. Chiang, W. P. Lin, C. H. Lin, W. S. Chen, F. T. Chen, C. H. Lien, and M.-J. Tsai, "Evidence and solution of over-RESET problem for HfO_X based resistive memory with sub-ns switching speed and high endurance," in *IEDM Tech. Dig.*, Dec. 2010, pp. 19.7.1–19.7.4, doi: 10.1109/IEDM.2010.5703395.
[33] C. Wang, H. Wu, B. Gao, W. Wu, L. Dai, X. Li, and H. Qian, "Ultrafast RESET analysis of HfO_x-based RRAM by sub-nanosecond pulses," *Adv. Electron. Mater.*, vol. 3, no. 12, Dec. 2017, Art. no. 1700263, doi: 10.1002/aelm.201700263.
[34] B. Govoreanu et al., "10×10 nm^2 Hf/HfO_x crossbar resistive RAM with excellent performance, reliability and low-energy operation," in *IEDM Tech. Dig.*, Dec. 2011, pp. 31.6.1–31.6.4, doi: 10.1109/IEDM.2011.6131652.
[35] M.-J. Lee, C. B. Lee, D. Lee, S. R. Lee, M. Chang, J. H. Hur, Y.-B. Kim, C.-J. Kim, D. H. Seo, S. Seo, U.-I. Chung, I.-K. Yoo, and K. Kim, "A fast, high-endurance and scalable non-volatile memory device made from asymmetric Ta_2O_{5-x}/TaO_{2-x} bilayer structures," *Nature Mater.*, vol. 10, no. 8, pp. 625–630, Aug. 2011, doi: 10.1038/nmat3070.
[36] Y. Kim, S. R. Lee, D. Lee, C. B. Lee, M. Chang, J. H. Hur, M. Lee, G. Park, C. J. Kim, U. Chung, I. Yoo, and K. Kim, "Bi-layered RRAM with unlimited endurance and extremely uniform switching," in *Proc. Symp. VLSI Technol.*, Jun. 2011, pp. 52–53.
[37] B. Yang, D. Arumí, S. Manich, Á. Gómez-Pau, R. Rodríguez-Montañés, M. B. González, F. Campabadal, and L. Fang, "RRAM random number generator based on train of pulses," *Electronics*, vol. 10, no. 15, p. 1831, Jul. 2021, doi: 10.3390/electronics10151831.
[38] J. Kim, H. Nili, N. D. Truong, T. Ahmed, J. Yang, D. S. Jeong, S. Sriram, D. C. Ranasinghe, S. Ippolito, H. Chun, and O. Kavehei, "Nano-intrinsic true random number generation: A device to data study," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 66, no. 7, pp. 2615–2626, Jul. 2019, doi: 10.1109/TCSI.2019.2895045.
[39] S. Yu and P. Chen, "Emerging memory technologies: Recent trends and prospects," *IEEE Solid-State Circuits Mag.*, vol. 8, no. 2, pp. 43–56, Spring 2016, doi: 10.1109/MSSC.2016.2546199.
[40] F. Jebali, E. Muhr, M. Alayan, M. C. Faye, D. Querlioz, F. Andrieu, E. Vianello, G. Molas, M. Bocquet, and J. M. Portal, "Embedded measurement of the SET switching time of RRAM memory cells," in *Proc. IEEE 34th Int. Conf. Microelectron. Test Struct. (ICMTS)*, Cleveland, OH, USA, Mar. 2022, pp. 1–5, doi: 10.1109/ICMTS50340.2022.9898162.
[41] M. S. Equbal, T. Ketkar, and S. Sahay, "Hybrid CMOS-RRAM true random number generator exploiting coupled entropy sources," *IEEE Trans. Electron Devices*, vol. 70, no. 3, pp. 1061–1066, Mar. 2023, doi: 10.1109/TED.2023.3241122.
[42] H. Aziza, J. Postel-Pellerin, H. Bazzi, P. Canet, M. Moreau, V. D. Marca, and A. Harb, "True random number generator integration in a resistive RAM memory array using input current limitation," *IEEE Trans. Nanotechnol.*, vol. 19, pp. 214–222, 2020, doi: 10.1109/TNANO.2020.2976735.
[43] S. Chakraborty, A. Garg, and M. Suri, "True random number generation from commodity NVM chips," *IEEE Trans. Electron Devices*, vol. 67, no. 3, pp. 888–894, Mar. 2020, doi: 10.1109/TED.2019.2963203.
[44] B. Lin, B. Gao, Y. Pang, P. Yao, D. Wu, H. He, J. Tang, H. Qian, and H. Wu, "A high-speed and high-reliability TRNG based on analog RRAM for IoT security application," in *IEDM Tech. Dig.*, Dec. 2019, pp. 14.8.1–14.8.4, doi: 10.1109/IEDM19573.2019.8993486.
[45] C. Walczyk, D. Walczyk, T. Schroeder, T. Bertaud, M. Sowinska, M. Lukosius, M. Fraschke, D. Wolansky, B. Tillack, E. Miranda, and C. Wenger, "Impact of temperature on the resistive switching behavior of embedded HfO_2-based RRAM devices," *IEEE Trans. Electron Devices*, vol. 58, no. 9, pp. 3124–3131, Sep. 2011, doi: 10.1109/TED.2011.2160265.
[46] S. Yu, Y. Wu, and H.-S.-P. Wong, "Investigating the switching dynamics and multilevel capability of bipolar metal oxide resistive switching memory," *Appl. Phys. Lett.*, vol. 98, no. 10, Mar. 2011, Art. no. 103514, doi: 10.1063/1.3564883.
[47] M. B. Gonzalez, M. Maestro-Izquierdo, F. Jiménez-Molinos, J. B. Roldán, and F. Campabadal, "Current transient response and role of the internal resistance in HfO_x-based memristors," *Appl. Phys. Lett.*, vol. 117, no. 26, Dec. 2020, Art. no. 262902, doi: 10.1063/5.0031575.
[48] M. Maestro-Izquierdo, M. B. Gonzalez, F. Campabadal, J. Suñé, and E. Miranda, "A new perspective towards the understanding of the frequency-dependent behavior of memristive devices," *IEEE Electron Device Lett.*, vol. 42, no. 4, pp. 565–568, Apr. 2021, doi: 10.1109/LED.2021.3063239.

MARYAM AKBARI was born in Kermanshah, Iran, in 1993. She received the B.Sc. and M.Sc. degrees from Razi University, Iran, in 2015 and 2017, respectively. She is currently pursuing the Ph.D. degree with the Iran University of Science and Technology (IUST), Iran. Her research interests include microstrip filters, high-frequency circuit design, physical unclonable functions (PUFs), true random number generators, and emerging technologies.

SATTAR MIRZAKUCHAKI received the B.Sc. degree in electrical engineering from the University of Mississippi, in 1989, and the M.Sc. and Ph.D. degrees in electrical engineering from the University of Missouri, Columbia, in 1991 and 1996, respectively. He has been a Faculty Member of the School of Electrical Engineering, Iran University of Science and Technology, Tehran, since 1996. His current research interests include digital systems and design of VLSI circuits.

DANIEL ARUMÍ received the M.S. degree in industrial engineering and the Ph.D. degree in electronic engineering from Universitat Politècnica de Catalunya (UPC), Barcelona, Spain, in 2003 and 2008, respectively. He is currently an Associate Professor with the Department of Electronic Engineering, UPC. His current research interests include hardware security in ICs, defect-based testing, fault modeling, defect diagnosis, and emerging technologies.

SALVADOR MANICH (Member, IEEE) received the M.Sc. and Ph.D. degrees in industrial engineering from UPC, in 1992 and 1998, respectively. He has been an Associate Professor with the School of Industrial Engineering, since 2001, and a member of the Electronic Engineering Department. He has developed a research activity with the Quality in Electronics Group (QinE). He is also a member of the Center for Research in Nanoengineering (CRNE). He was an Invited Researcher with IST, Portugal; and TUM, Germany. His main research interests include low-power design, test of digital systems, and security in hardware structures.

ALVARO GÓMEZ-PAU (Member, IEEE) received the M.Sc. degree in engineering and the Ph.D. degree in electronics engineering from Universitat Politècnica de Catalunya [BarcelonaTech (UPC)], in 2010 and 2017, respectively. He is a Researcher and an Assistant Professor with the Electronics Engineering Department, UPC. He was a Visiting Scholar with the Georgia Institute of Technology, Atlanta, GA, USA; and the University of Eindhoven, Eindhoven, The Netherlands. His research interest includes the design and test of integrated nanodevices for security primitives applications.

FRANCESCA CAMPABADAL received the Ph.D. degree in physics from Universitat Autònoma de Barcelona, Bellaterra, Spain, in 1986. She joined Consejo Superior de Investigaciones Científicas, Institut de Microelectrònica de Barcelona, Barcelona, Spain, in 1987, where she is currently a Research Professor. Her research interests include the deposition of high-k dielectric layers, their electrical characteristics, and resistive switching phenomena in RRAM devices.

MIREIA BARGALLÓ GONZÁLEZ received the degree in physics from Universitat de Barcelona, Barcelona, Spain, and the Ph.D. degree in stress analysis and defect characterization techniques of semiconductor materials and devices from Katholieke Universiteit Leuven, Leuven, Belgium, in 2011. She has completed the Ph.D. thesis with the Interuniversity Microelectronics Center (imec), Leuven, Belgium. In 2011, she joined Institut de Microelectrònica de Barcelona (IMB-CNM, CSIC). Her current research interests include fabrication, electrical characterization, and modeling of resistive switching devices.

ROSA RODRÍGUEZ-MONTAÑÉS received the M.S. degree from Universitat de Barcelona, in 1988, and the Ph.D. degree in physical science from Universitat Politècnica de Catalunya (UPC), Barcelona, Spain, in 1992. Since 1994, she has been an Associate Professor with the Department of Electronic Engineering, UPC. She was an Invited Researcher with the Test Group, Philips Research, Eindhoven, The Netherlands; and the Advanced Thin Dielectric Films Group, Centro Nacional de Microelectrónica–CSIC, Bellaterra, Spain. She is currently working on hardware security of ICs, fault models, defect characterization, defect diagnosis of digital nanometric CMOS technologies, and emerging technologies.