Physical Unbiased Generation of Random Numbers With Coupled Resistive Switching Devices

Simone Balatti, *Student Member, IEEE*, Stefano Ambrogio, *Student Member, IEEE*, Roberto Carboni, Valerio Milo, Zhongqiang Wang, Alessandro Calderoni, Nirmal Ramaswamy, *Senior Member, IEEE*, and Daniele Ielmini, *Senior Member, IEEE*

***Abstract*— The resistive-switching memory (RRAM) is currently under consideration for fast nonvolatile memory thanks to its relatively low cost and high performance. A key concern for RRAM reliability is stochastic switching, which impacts the operation of the digital memory due to distribution broadening. On the other hand, stochastic behaviors are enabling mechanisms for some computing tasks, such as physical unclonable function (PUF) and random number generation (RNG). Here, we present new circuit blocks for physical RNG, based on the coupling of two RRAM devices. The two-resistance scheme allows to overcome the need of probability tracking, where the operation voltage must be tuned to adjust the generation probabilities of 0 and 1. Probability tests are proved successful for one of the three proposed schemes.**

***Index Terms*— Memory reliability, random number generation (RNG), resistive-switching memory (RRAM).**

I. Introduction

RANDOM number generation (RNG) is essential for generating random encryption keys for secure transmission protocols [1]. The pervasiveness of Internet-based communication and the need to protect data from eavesdropping raise the need for compact RNG circuits, capable of generating true random numbers with high entropy quality and high throughput. To generate true random numbers that do not rely on deterministic algorithms and are totally unpredictable, it is important to identify a convenient on-chip entropy source and to design the corresponding circuit for generating the random bit stream with high throughput and stability. Previous approaches to true/physical RNG include random telegraph noise (RTN) in dielectrics [2] or in resistive-switching memory (RRAM) [3]. The RTN appears as a random fluctuation of current, or resistance, between two or more levels, as a result of the random charging/discharging of the bistable defects [4]. However, the RTN is difficult to control in terms of both the amplitude and the frequency, thus raising the need for dedicated techniques for RTN initiation. In addition, the RTN has been shown to be unstable in the RRAM, where the current fluctuation at a given bias can show unpredictable onset and interruption [5]. Other schemes relying on physical fluctuation phenomena are, therefore, under scrutiny for efficient and stable RNG.

Recently, novel RNG concepts based on the switching variability in low-voltage memory technologies, such as spin-transfer-torque (STT), magnetic memory (MRAM) [6], [7], and RRAM [8], [9], have been proposed. Switching variation in RRAM was similarly applied to develop physical unclonable function (PUF) [10] and to enhance learning in neuromorphic circuits [11]. For RNG, one can take advantage of the stochastic variation of a switching parameter, such as the voltage V_{set} for the set transition from high-to-low resistance [12]. Application of a voltage close to the median value in the distribution of V_{set} statistically results in a random set transition randomly occurring only in a fraction of attempts. A key problem in this approach, however, is the need for a careful tracking of the applied voltage, which must be exactly centered in the median of the V_{set} distribution to ensure perfect balance between 0s and 1s [12]. For this purpose, real-time voltage tracking techniques must be used for compensating 0 and 1 probabilities [7].

This paper presents new solutions for the RRAM-based unbiased RNGs, overcoming the need for probability tracking. These novel approaches rely on stochastic switching in two coupled RRAM devices, driven by the same voltage pulse and having different (e.g., parallel or series) configurations. Unbiased RNG relies either on a comparison between the resistance levels after independent switching, or on alternative switching in series/parallel RRAM, similar to the operation of RRAM logic gates [13]. The new RNG schemes are finally supported by presenting and discussing randomness tests.

II. RRAM Switching Characteristics

Devices used in our RNG circuits were bipolar RRAMs, consisting of a Si-doped HfO_2 switching layer with TiN bottom electrode (BE) and Ti top electrode (TE), acting as an oxygen exchange layer for defect generation at the TE side [4], [14]. Fig. 1 shows the RRAM device stack and the corresponding I–V characteristics. One-transistor/one-resistor (1T1R) structures were used for proper control

Manuscript received November 13, 2015; revised January 28, 2016; accepted February 18, 2016. Date of publication March 22, 2016; date of current version April 20, 2016. This work was supported in part by the European Research Council Consolidator Grant ERC-2014-CoG-648635-RESCUE. The review of this paper was arranged by Editor Y.-H. Shih.

S. Balatti was with the Dipartimento di Elettronica e Informazione, Italian Universities Nanoelectronics Team, Politecnico di Milano, Milan 20133, Italy. He is now with Intermolecular, Inc., San Jose, CA 95134 USA (e-mail: simone.balatti@intermolecular.com).

S. Ambrogio, R. Carboni, V. Milo, Z. Wang, and D. Ielmini are with the Dipartimento di Elettronica, Informazione e Bioingegneria, Italian Universities Nanoelectronics Team, Politecnico di Milano, Milan 20133, Italy (e-mail: stefano.ambrogio@polimi.it; roberto.carboni@polimi.it; valerio.milo@polimi.it; zhongqiang.wang@polimi.it; daniele.ielmini@polimi.it).

A. Calderoni and N. Ramaswamy are with Micron Technology, Inc., Boise, ID 83707 USA (e-mail: acaldero@micron.com; dramaswamy@micron.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TED.2016.2537792

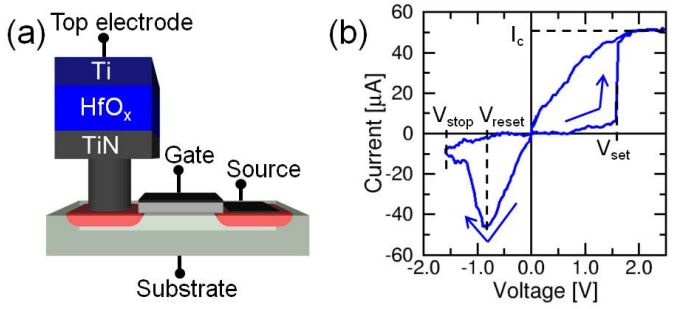


Fig. 1. (a) Schematic of the 1T1R structure used in this paper and (b) corresponding I–V curve providing definition of the set voltage V_{set}, the compliance current I_C, the reset voltage V_{reset}, and the stop voltage V_{stop}. The RRAM stack includes a Si-doped HfO_x switching layer, a Ti TE, and a TiN BE.

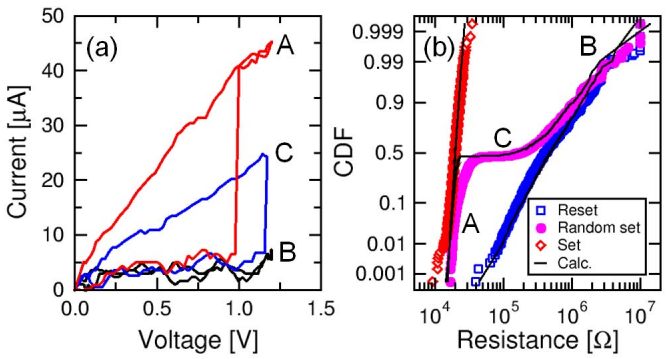


Fig. 2. (a) Measured I–V characteristics during random-set operation and (b) cumulative distributions of resistance after reset, after set, and after random set at $V_A = 1.2$ V. Random-set operation can results in either set transition (A) or no transition (B). Partial set transition (C) can also be observed.

of the resistance level by limiting the current of the integrated select transistor [15]. Application of a positive voltage causes set transition from high-resistance state (HRS) to low-resistance state (LRS) in correspondence of V_{set}, while application of a negative voltage causes the reset transition from LRS to HRS, starting at a reset voltage V_{reset}. A compliance current $I_C = 50$ μA was used during the set transition by applying a relatively small gate voltage. A maximum negative voltage V_{stop} was applied during the reset sweep. Triangular pulses of width $t_P = 1$ ms were used for set and reset in Fig. 1 and throughout this paper. The relatively long pulse was needed to overcome the parasitic capacitance inducing delays in the custom board used for experimental verification. We applied a suitably low voltage for set and reset to avoid any degradation in the device during cycling.

III. RRAM-Based RNG Circuits

The RRAM is affected by stochastic switching, where the switching parameters randomly change from cycle to cycle [16], [17]. The resistance R in both the HRS and the LRS, the set voltage V_{set}, and the reset voltage V_{reset} were shown to vary during cycling, depending on the compliance current I_C [18] and the stop voltage V_{stop} [17]. These statistical fluctuations were explained by the random formation and rupture of the conductive filament (CF) and the varying number of defects within the CF in both the HRS and the LRS [18]. While variability is a considerable concern for digital memory applications, where distinct set/reset distributions should be ensured, random variations of V_{set} were previously used to generate random bits [12]. In fact, the application of a voltage V_A close to the median value of V_{set} to the HRS results in a random set, as shown in Fig. 2(a). The device undergoes set transition if $V_A > V_{\text{set}}$ [case A in Fig. 2(a)], while no change is seen if $V_A < V_{\text{set}}$ [case B in Fig. 2(a)]. This leads to a bimodal distribution of R measured after a random set, as shown in Fig. 2(b). Between the HRS and the LRS subsets in the bimodal distribution, there is intermediate case C in Fig. 2(a), where the set transition took place only partially due to insufficient time to complete the CF formation [12]. The simulation results are provided in Fig. 2(b). The LRS distribution is modeled by a lognormal distribution of resistance with the median value 20 kΩ and a relatively small standard deviation $\sigma(\log R) = 8.64 \times 10^{-2}$. The HRS distribution is modeled as the sum of an LRS resistance and a lognormal distribution with the median 480 kΩ and the standard deviation $\sigma(\log R) = 0.82$. The series combination of the LRS and the HRS allows to better describe the low-resistance portion of the HRS distribution, where the resistance of the incompletely-dissolved filament and of the top and bottom interface resistances cannot be neglected. The random set distribution was obtained by combining the randomly selected HRS and LRS resistances with equal probabilities of 50%, resulting in the bimodal distribution in Fig. 2(b). The random-set operation on HRS can be used as an entropy source for true RNG, however, achieving an unbiased RNG with equal probabilities of 0 and 1 in Fig. 2(b) requires careful adjustment of the voltage V_A in correspondence of the median of the V_{set} distribution. This can be obtained by real-time probability tracking techniques [7], however, at the expense of a higher circuit and algorithm complexity. In addition, V_{set} might decrease during cycling due to degradation and wear out of the CF region in the RRAM device [19], which further supports the need for voltage tracking techniques. To avoid this issue, we redesign RNG blocks based on random switching in two coupled RRAM devices, with the purpose of compensating the unbalanced generation and achieve unbiased RNG. RRAM devices can be coupled in either series or parallel configurations, while the source of entropy is the variability of either set or reset transitions. As a result, three RNG schemes with coupled RRAMs are developed, as detailed in the following.

A. Parallel Reset

Fig. 3(a) shows the parallel-reset RNG circuit, where two RRAM cells (P and Q) are connected in parallel. The 1T1R structures were used for P and Q during the experimental demonstration of the RNG operation. Fig. 3(b) shows the waveforms for the TE voltage V_P of device P, the TE voltage V_Q of device Q, and the voltage V_{out} of the common node between P and Q in Fig. 3(a). The RNG cycle consists of three phases, namely, 1) application of a positive voltage across P and Q to induce set transition; 2) application of a negative voltage to induce reset transition; and 3) read,

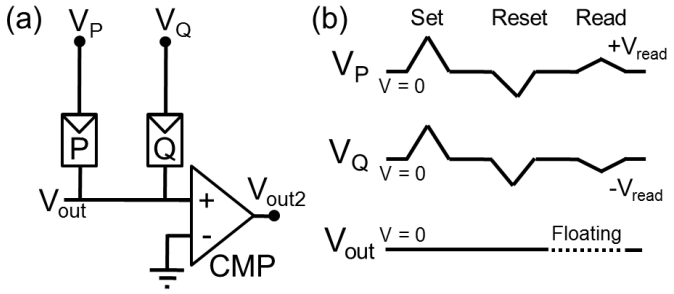


Fig. 3. (a) Parallel-reset circuit and (b) sequence of applied signals. Starting from P to Q in HRS, cells are first independent set, then reset and finally read using voltage-divider configuration. The analogical comparator (CMP) is used to digitally regenerate V_{out}.

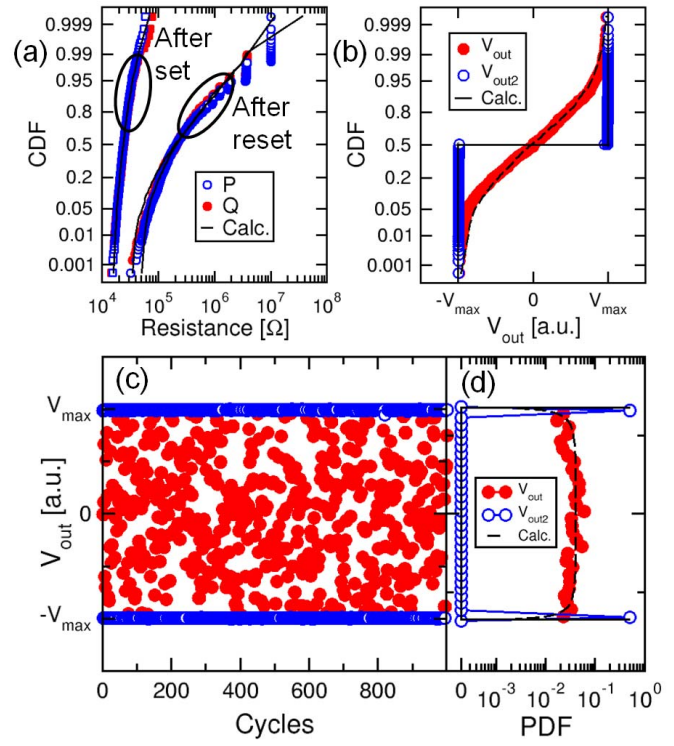


Fig. 4. (a) Cumulative distributions of resistance after set and after reset for cells P and Q. (b) Corresponding distributions of V_{out} and V_{out2} with and without comparator. (c) Measured V_{out} and V_{out2} as a function of RNG cycle and (d) PDF of measured V_{out} and V_{out2} during cycling.

where the voltage divider of P and Q is evaluated by probing the potential V_{out} with $V_P = +V_{\text{read}}$ and $V_Q = -V_{\text{read}}$. Triangular pulses with 1-ms duration were applied for set, reset, and read. Note that voltages across devices P and Q are independently applied during set and reset with no interaction between the two cells, thus both set and reset transitions occur independently in this scheme. As a result of the relatively large statistical variation of HRS resistance [14], [17], V_{out} randomly varies from cycle to cycle, thus serving as the output bit value in the RNG. HRS resistance variation serves as the entropy source in this scheme.

Fig. 4(a) shows the cumulative distributions of P resistance R_P and Q resistance R_Q, measured after set and reset, together with calculated results obtained as in Fig. 2(b). RNG was tested along 1000 cycles, which provides sufficient statistical

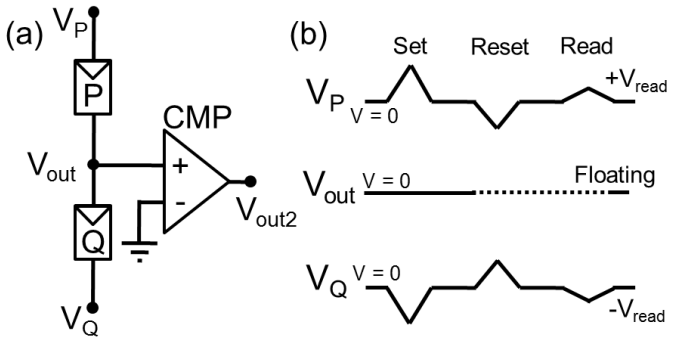


Fig. 5. (a) Series reset circuit and (b) sequence of applied signals. Starting from HRS, the cells are first independently set, then subjected to random reset where only one cell can reset, and finally read in voltage-divider configuration.

accuracy with negligible device degradation. Distributions R_P and R_Q are almost identical in both LRS and HRS, which is a key to achieve true and unbiased RNG. Fig. 4(b) shows the resulting experimental and calculated distributions of V_{out} obtained during read, indicating a bimodal shape with 50% transition probability. The bimodal distribution was improved in our experimental setup by introducing an analog comparator (CMP) in Fig. 3(a). The CMP can be replaced by one or more integrated CMOS inverters in an integrated circuit to decrease the occupied area on the chip [12]. The distribution of the CMP output voltage V_{out2} shows a bimodal distribution with abrupt transition at 50%. Fig. 4(c) shows the measured V_{out} and V_{out2} along 1000 cycles during RNG operation, while Fig. 4(d) shows the corresponding probability density function (PDF) of V_{out} and V_{out2}. Simulation results show a uniform distribution of V_{out}, in line with data. No probability tracking is needed thanks to natural matching of HRS distributions in cells P and Q [Fig. 4(a)]. This was possible because the cycle-to-cycle variability was significantly larger than the cell-to-cell variability in our devices.

B. Serial Reset

Fig. 5(a) shows the serial reset scheme for the RNG where the cells P and Q are connected in series between voltage supplies V_P and V_Q. As in the parallel-reset case, 1T1R devices were used for cells P and Q for the experimental demonstration. Fig. 5(b) shows the RNG cycle consisting of 1) independent set of P and Q; 2) conditional reset of P and Q; and 3) read of the voltage V_{out} of the common node between P and Q. During random reset, a negative voltage $V_P - V_Q < 0$ is applied across P and Q, while the intermediate node between P and Q is left floating. The total applied voltage is $|V_P - V_Q| > 2\ V_{\text{reset}}$, thus sufficient to trigger reset in at least one device. Once the reset transition is initiated in either device, the voltage across it increases because of the voltage-divider configuration, thus causing the voltage across the other cell to reduce. Fig. 6(a) shows the schematic of the I–V curve of P with Q acting as load resistance: after the onset of the reset transition in P, the voltage drop across P increases, thus accelerating reset transition in P, while the voltage drop across Q decreases, thus preventing reset transition in Q. Fig. 6(b) shows the

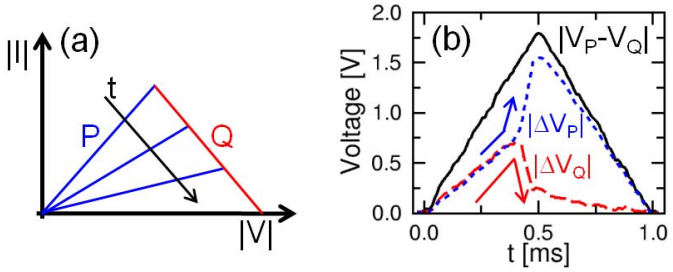


Fig. 6. (a) Schematic of time evolution of the I–V curves of cells P and Q during random reset causing the transition of P. (b) Measured voltage across P and Q.

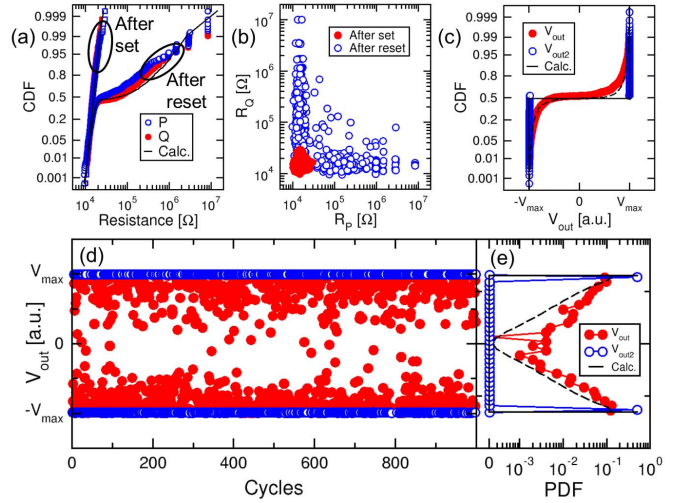


Fig. 7. (a) Cumulative distribution of R after set and after reset of cells P and Q. (b) Correlation plot of RQ as a function of RP. (c) Cumulative distribution of measured V_{out} and V_{out2}. (d) Measured V_{out} and V_{out2} as a function of RNG cycles and (e) PDF of measured V_{out} and V_{out2} during cycling.

experimentally measured voltage V_P-V_Q applied across the two RRAM devices, the voltage ΔV_P across P, and the voltage ΔV_Q across Q, showing the reset transition after about 0.4 ms along the rising edge of the pulse. This self-accelerated random reset scheme results in the reset transition being randomly carried out in one device only, namely, the one featuring the smallest V_{reset} as a result of LRS variability [17]. The variation of V_{reset} thus serves as the entropy source in this scheme. A similar scheme was used to perform material implication in RRAM logic, where the two devices were deliberately prepared in different LRSs to avoid the unpredictable random reset in Figs. 5 and 6 [13].

After random reset, the potential of the intermediate node between P and Q is read, while a voltage 2 V_{read} is applied across the two cells. Fig. 7(a) shows the cumulative distribution of resistance R of P and Q after either set or reset in Fig. 5(b). After reset, both P and Q show equal bimodal distributions with 50% transition point, demonstrating unbiased true RNG without probability tracking. The calculated distributions after random reset were obtained by randomly moving 50% of samples from the LRS distribution to the HRS distribution. Fig. 7(b) shows the correlation plot of R_Q as a function of R_P after either set or reset. After reset, the devices show complementary state, namely, if one device shows LRS,

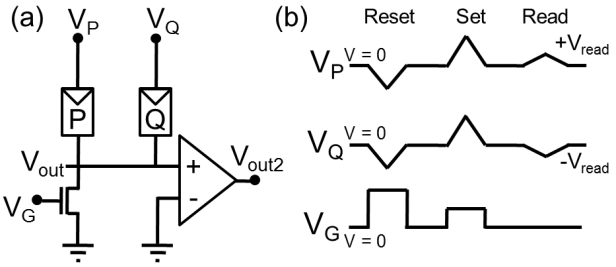


Fig. 8. (a) Parallel set circuit and (b) sequence of applied signals. Starting from LRS, the cells are first independently reset, then subjected to parallel set, and finally read with voltage-divider configuration.

then the other shows HRS, and vice versa. This is the result of the random reset process in Fig. 6, where the voltage division after the onset of the reset transition accelerates or prevents the reset process in one RRAM or the other. Fig. 7(c) shows the resulting experimental and calculated bimodal distribution of V_{out} with transition point at 50% probability. Voltage regeneration is possible by introducing a CMP (or digital inverter), resulting in the bimodal abrupt distribution of V_{out2} in Fig. 7(c). Fig. 7(d) shows the cycling evolution of V_{out} and V_{out2} during repetition of the RNG sequence in Fig. 5(b), completed by a final unconditional reset pulse, with amplitude larger than the total voltage applied during the random reset pulse $|V_P–V_Q|$, to ensure that the first set pulse is applied to equal states in P and Q. Fig. 7(e) shows the corresponding PDF of V_{out} and V_{out2} for data and calculations. These results demonstrate unbiased true RNG with no probability tracking, taking advantage of random reset in the two coupled RRAM devices. Note that this RNG scheme is particularly suited to devices with relatively low V_{reset}, since the applied voltage 2 V_{reset} is finally dropping almost totally across the HRS cell. This might cause early failure of the RRAM device, since endurance exponentially decreases with V_{stop}, i.e., the maximum voltage during reset, in RRAM [14].

C. Parallel Set

Fig. 8 shows the parallel-set scheme for RNG and the corresponding voltage pulse sequence. The two RRAM devices are connected to ground via a transistor controlled by a gate voltage V_G. The pulse sequence includes: 1) independent reset of P and Q; 2) random set of P and Q; and 3) read by application of a voltage 2 V_{read} across the two devices, while the transistor is in the off state. This RNG scheme takes advantage of the dynamic voltage divider in the 1-transistor/2-resistor structure during set: as the voltage across the two RRAM increases, set transition eventually takes place randomly in one device, while the consequent voltage decrease across P and Q inhibits the other device to undergo set transition. This finally leads to a random set transition, similar to the random reset transition in the scheme of Figs. 5–7. The variation of V_{set} serves as the entropy source in the scheme, similar to the one-RRAM scheme described in Fig. 2. Clearly, no probability tracking is needed in Fig. 8, since set transition is naturally occurring in one device only in each cycle.

Fig. 9(a) schematically shows the I–V characteristics of P and Q during the set pulse: as set transition takes place

TABLE I

RANDOMNESS TEST RESULTS FOR A SEQUENCE OF MORE THAN 2 Mb GENERATED BY THE PARALLEL-RESET SCHEME OF FIG. 3(a) DIVIDED IN 55 SEGMENTS BEFORE AND AFTER VON NEUMANN CORRECTION. TESTS ARE PASSED IF P-VALUE$_T(X^2) > 0.0001$ AND PROPORTION > 0.945454. THE RRAM SCHEME PASSES ALL TESTS AFTER VON NEUMANN CORRECTION, EXCEPT FOR THE NONOVERLAPPING TEMPLATE MATCHING TEST, WHICH WAS PASSED IN 143 SEQUENCES OVER 148, NAMELY ABOUT 96.6%

	Output		After Von Neumann correction	
Test	P-value$_T$ (X^2)	Proportion	P-value$_T$ (X^2)	Proportion
Frequency	0.000000	0.109091	0.514124	1.000000
Block Frequency	0.000000	0.000000	0.637119	1.000000
Cumulative Sums (forward)	0.000000	0.036364	0.595549	1.000000
Cumulative Sums (reverse)	0.000000	0.072727	0.401199	1.000000
Runs	0.000000	0.018182	0.437274	1.000000
Longest Run of Ones	0.000000	0.145455	0.275709	1.000000
FFT	0.000000	0.545455	0.000184	0.981818
Non Overlapping Template Matching	55/148 test passed	1/148 test passed	All test passed	143/148 test passed
Serial (P-value$_1$)	0.000000	0.018182	0.595549	0.981818
Serial (P-value$_2$)	0.000000	0.290909	0.129620	0.981818
Approximate Entropy	0.000000	0.036364	0.798139	0.981818

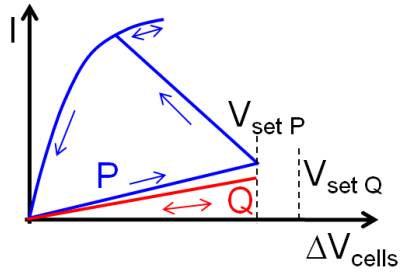


Fig. 9. Schematic of the I–V curves of P and Q during a parallel-set operation in the circuit in Fig. 8(a). As the set transition starts to occur in the cell with smaller V_{set} (P in the figure), the voltage across both cells drops, thus inhibiting set transition in the other cell (Q in the figure).

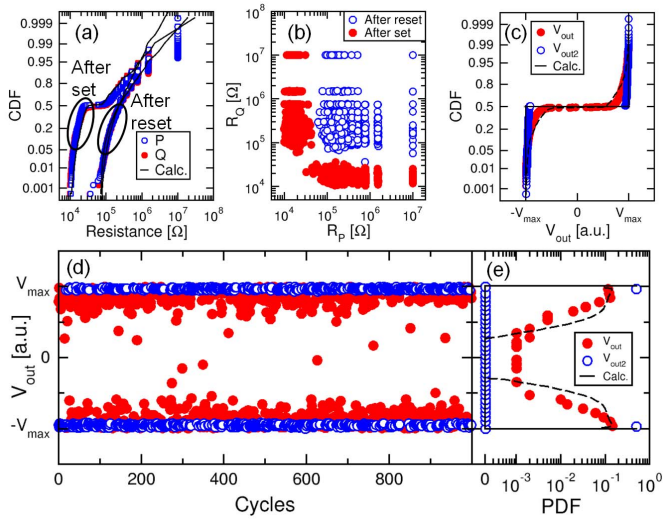


Fig. 10. (a) Cumulative distributions of R after reset and after set for P and Q. (b) Correlation plot of RQ as a function of RP after set and reset. (c) Cumulative distributions of V_{out} and V_{out2}. (d) Measured V_{out} and V_{out2} as a function of RNG cycles and (e) PDF of measured V_{out} and V_{out2} during cycling.

in P because of $V_{\text{set},P} < V_{\text{set},Q}$, the voltage across both devices drops, thus preventing any set transition in Q. Fig. 10(a) shows the resulting bimodal distribution of R for P and Q, showing a bimodal distribution with an HRS/LRS transition at 50%. Calculations were performed by randomly moving 50% samples from the HRS distribution to the LRS distribution. Fig. 10(b) shows the correlation plot of R_Q as a function of R_P, indicating complementary states, namely, P is always in HRS, if Q is in LRS, and vice versa. Fig. 10(c) shows the cumulative distributions of V_{out} and V_{out2}, and the latter shows the output of the regenerative CMP. Nice bimodal distributions with smooth and abrupt transitions are shown by V_{out} and V_{out2}, respectively. Fig. 10(d) and (e) shows V_{out} and V_{out2} as a function of the RNG cycle and the corresponding PDF. Calculations are provided for Fig. 10(c) and (e), showing good agreement with data.

Note that the parallel-set RNG shows a better performance based on the bimodal distributions of R [Fig. 10(a)] and V_{out} [Fig. 10(c) and (e)] compared with the parallel reset in Fig. 7(a). This can be understood by the abrupt set transition in the parallel-set approach as opposed to the more gradual reset transition in the parallel-reset scheme, as also visible from the I–V characteristics of the individual RRAM device in Fig. 1(b) and explained by the different microscopic processes of filament growth and gap depletion during set and reset, respectively [20].

IV. RANDOMNESS ANALYSIS

To assess the performance of any true RNG, randomness test is mandatory. For this purpose, we evaluated randomness on one of our schemes, using the standard set of statistical tests developed by the National Institute of Standards and Technology (NIST) [21]. The serial reset and the parallel-set schemes showed less excellent performance against the NIST test, which we attribute to the stronger impact of cell–cell variability of V_{reset} and V_{set}, respectively. Therefore, we focused on the parallel-reset scheme in the following NIST test.

Each random bit was generated in 6 ms, including set, reset, and read pulses of 1-ms width, each followed by a 1-ms wait time. The generation rate is, therefore, ~0.16 kHz, although we estimate that much faster generation can be achieved (e.g., around 1 GHz) by taking advantage of the sub-1-ns

switching time of HfO_x RRAM [22]. The RNG output was taken at V_{out2} in the scheme of Fig. 3(a).

Randomness was tested on a generated sequence of about 2 280 000 random bits. According to the NIST guidelines, we divided the entire sequence in 55 segments and we applied nine different tests reported in Table I. Each test returned two parameters, $P\text{-value}_T(X^2)$, and proportion. If $P\text{-value}_T(X^2) \geq 0.0001$, then the sequence can be considered to be uniformly distributed, while, for the proportion, the minimum pass rate for each statistical test is 0.945454.

Table I shows the pass/fail results for both the raw bit data, and that obtained after von Neumann correction, namely, a standard postprocess analysis, which removes all the 0 and 1 bias from a pseudorandom sequence [7]. Results indicate that all tests applied to raw bits failed, while the application of the von Neumann correction allows our scheme to pass all tests except one, namely, the nonoverlapping template matching test, where the pass rate was 143 over 148. Note that von Neumann is a standard tool to improve the randomness of RNG, although it introduces additional complexity in terms of controller logic of the RNG circuit. These results appear promising for hardware-based, true unbiased RNG using RRAM technology.

V. Conclusion

We presented three new concepts for unbiased RNG relying on switching variability in RRAM. All concepts adopt two coupled RRAM devices to provide 50% probability of 0s and 1s by self-compensation schemes, as opposed to complicated probability tracking proposed before. The concepts include: 1) a parallel-reset configuration based on HRS resistance variation; 2) a serial reset configuration based on V_{reset} variation; and 3) a parallel-set configuration based on V_{set} variation. In all the cases, bimodal distributions of high/low voltage were obtained with low-to-high transition at 50%. RNG was improved by adding digital regeneration. The results of the randomness tests for the parallel-reset scheme with/without the von Neumann correction support the two-RRAM scheme for future on-chip RNG, thus enlarging the pool of potential application for the RRAM technology.

References

[1] S. K. Mathew *et al.*, "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.

[2] 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 *ISSCC Tech. Dig.*, 2006, pp. 1666–1675.

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

[4] S. Ambrogio, S. Balatti, A. Cubeta, A. Calderoni, N. Ramaswamy, and D. Ielmini, "Statistical fluctuations in HfO_x resistive-switching memory: Part II—Random telegraph noise," *IEEE Trans. Electron Devices*, vol. 61, no. 8, pp. 2920–2927, Aug. 2014.

[5] S. Ambrogio, S. Balatti, V. McCaffrey, D. C. Wang, and D. Ielmini, "Noise-induced resistance broadening in resistive switching memory—Part II: Array statistics," *IEEE Trans. Electron Devices*, vol. 62, no. 11, pp. 3812–3819, Nov. 2015.

[6] A. Fukushima *et al.*, "Spin dice: A scalable truly random number generator based on spintronics," *Appl. Phys. Exp.*, vol. 7, no. 8, p. 083001, 2014.

[7] W. H. Choi *et al.*, "A magnetic tunnel junction based true random number generator with conditional perturb and real-time output probability tracking," in *Proc. IEEE Int. Electron Devices Meeting (IEDM)*, Dec. 2014, pp. 12.5.1–12.5.4.

[8] S. Gaba, P. Sheridan, J. Zhou, S. Choi, and W. Lu, "Stochastic memristive devices for computing and neuromorphic applications," *Nanoscale*, vol. 5, no. 13, pp. 5872–5878, 2013.

[9] Y. Wang, W. Wen, M. Hu, and H. Li, "A novel true random number generator design leveraging emerging memristor technology," in *Proc. 25th Great Lakes Symp. VLSI*, 2015, pp. 271–276.

[10] A. Chen, "Utilizing the variability of resistive random access memory to implement reconfigurable physical unclonable functions," *IEEE Electron Device Lett.*, vol. 36, no. 2, pp. 138–140, Feb. 2015.

[11] S. Yu, "Orientation classification by a winner-take-all network with oxide RRAM based synaptic devices," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Jun. 2014, pp. 1058–1061.

[12] S. Balatti, S. Ambrogio, Z. Wang, and D. Ielmini, "True random number generation by variability of resistive switching in oxide-based devices," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 5, no. 2, pp. 214–221, Jun. 2015.

[13] S. Balatti, S. Ambrogio, and D. Ielmini, "Normally-off logic based on resistive switches—Part I: Logic gates," *IEEE Trans. Electron Devices*, vol. 62, no. 6, pp. 1831–1838, Jun. 2015.

[14] S. Balatti *et al.*, "Voltage-controlled cycling endurance of HfO_x-based resistive-switching memory," *IEEE Trans. Electron Devices*, vol. 62, no. 10, pp. 3365–3372, Oct. 2015.

[15] D. Ielmini, "Modeling the universal set/reset characteristics of bipolar RRAM by field- and temperature-driven filament growth," *IEEE Trans. Electron Devices*, vol. 58, no. 12, pp. 4309–4317, Dec. 2011.

[16] S. Yu, X. Guan, and H.-S. P. Wong, "On the stochastic nature of resistive switching in metal oxide RRAM: Physical modeling, Monte Carlo simulation, and experimental characterization," in *IEDM Tech. Dig.*, 2011, pp. 17.3.1–17.3.4.

[17] S. Ambrogio, S. Balatti, A. Cubeta, A. Calderoni, N. Ramaswamy, and D. Ielmini, "Statistical fluctuations in HfO_x resistive-switching memory: Part I—Set/reset variability," *IEEE Trans. Electron Devices*, vol. 61, no. 8, pp. 2912–2919, Aug. 2014.

[18] A. Fantini *et al.*, "Intrinsic switching variability in HfO_2 RRAM," in *Proc. 5th IEEE Int. Memory Workshop (IMW)*, May 2013, pp. 30–33.

[19] Z.-Q. Wang *et al.*, "Cycling-induced degradation of metal-oxide resistive switching memory (RRAM)," in *IEDM Tech. Dig.*, 2015, pp. 7.6.1–7.6.4.

[20] S. Larentis, F. Nardi, S. Balatti, D. C. Gilmer, and D. Ielmini, "Resistive switching by voltage-driven ion migration in bipolar RRAM—Part II: Modeling," *IEEE Trans. Electron Devices*, vol. 59, no. 9, pp. 2468–2475, Sep. 2012.

[21] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST, Gaithersburg, MD, USA, Special Publication 800-22, 2010.

[22] H. Y. Lee *et al.*, "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.*, 2010, pp. 19.7.1–19.7.4.

Simone Balatti (S'12) received the B.S., M.S., and Ph.D. degrees from the Politecnico di Milano, Milan, Italy, in 2009, 2011, and 2015, respectively, all in electrical engineering.

He is currently a Device Engineer with Intermolecular, Inc., San Jose, CA, USA. His current research interests include the study of novel devices for memory applications.

Stefano Ambrogio (S'14) received the M.S. (*cum laude*) degree and the Ph.D. degree in electrical engineering from the Politecnico di Milano, Milan, Italy, in 2012 and 2016, respectively.

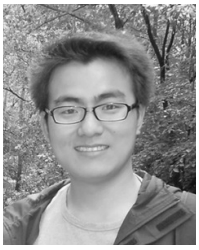
His current research interests include electrical characterization, modeling, and neuromorphic applications of resistive switching devices.

Roberto Carboni received the B.S. degree in electrical engineering from the Politecnico di Milano, Milan, Italy, in 2013, where he is currently pursuing the M.S. degree in electrical engineering.

His current research interests include the characterization and modeling of resistive switching and magnetoresistive memories.

Valerio Milo received the B.S. and M.S. degrees in electrical engineering from the Politecnico di Milano, Milan, Italy, in 2012 and 2015, respectively, where he is currently pursuing the Ph.D. degree in electrical engineering.

His current research interests include the modeling and neuromorphic applications of resistive switching and phase change memories.



Zhongqiang Wang was born in Hebei, China, in 1984. He received the B.S. and Ph.D. degrees in condensed matter physics from Northeast Normal University, Changchun, China, in 2008 and 2013, respectively.

He is currently a Post-Doctoral Researcher with the Department of Electronics, Information and Bioengineering, Politecnico di Milano, Milan, Italy.

Alessandro Calderoni received the Laurea (*cum laude*) degree in electrical engineering from the Politecnico di Milano, Milan, Italy, in 2006.

He is currently a Senior Device Engineer with the Emerging Memory Cell Technology Team, Micron Technology, Inc., Boise, ID, USA. His current research interests include the characterization of various emerging memory devices and selectors for high-density applications.

Nirmal Ramaswamy (M'07–SM'09) received the bachelor's degree in metallurgical engineering from IIT Madras, Chennai, India, and the M.S. and Ph.D. degrees in material science and engineering from Arizona State University, Phoenix, AZ, USA.

He has been with Micron Technology, Inc., Boise, ID, USA, since 2002, where he is currently the Manager of the Emerging Memory Cell Technology Team. His current research interests include various emerging memory technologies for high-density applications.

Daniele Ielmini (M'04–SM'09) received the Ph.D. degree from the Politecnico di Milano, Milan, Italy, in 2000.

He joined the Dipartimento di Elettronica, Informazione, e Bioingegneria, Politecnico di Milano, as an Assistant Professor in 2002 and an Associate Professor in 2010. He conducts research on emerging nanoelectronic devices, such as phase change memory and resistive switching memory.

Prof. Ielmini received the Intel Outstanding Researcher Award in 2013 and the ERC Consolidator Grant in 2014.