SCIENCE CHINA
Information Sciences

• Supplementary File •

A 3.3 Mbit/s True Random Number Generator Based on Resistive Random Access Memory

Shiyue SONG[1], Peng HUANG[1,2*], Wensheng SHEN[1], Lifeng LIU[1,2*] & Jinfeng KANG[1,2]

[1]*School of Integrated Circuits, Peking University, Beijing* 100871, *China;*
[2]*Beijing Advanced Innovation Center for integrated Circuits, Beijing* 100176, *China*

Appendix A 1T1R RRAM device and array

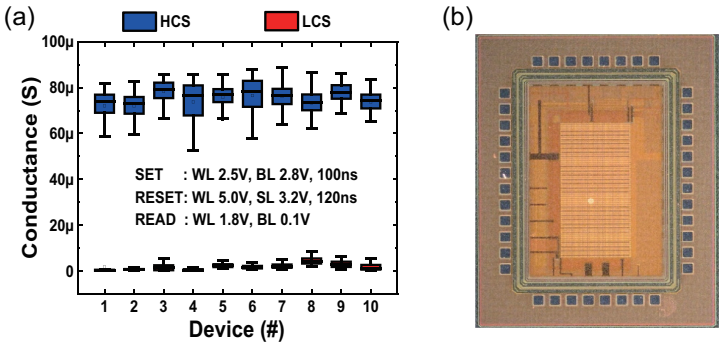

Figure A1 (a) The measured conductance distribution of 10 typical devices measured over 100 SET/RESET pulse cycles. (b) The microphotograph of fabricated 1T1R RRAM chip.

The SET operation switches a RRAM cell from low conductance state (LCS) to high conductance state (HCS), while the RESET operation switches a RRAM cell from HCS to LCS. Figure A1(a) shows the measured conductance distribution of ten typical devices measured over 100 SET/RESET pulse cycles. The microphotograph top view of fabricated 4K-bit 1T1R RRAM chip is presented in Figure A1(b).Agilent B1500A semiconductor parameter analyzer, Agilent 81160A pulse function generator, Rohde and Schwarze RTO2014 Oscilloscope, and STM32F103 Series MCUs are used in the electrical measurement.

Appendix B The mismatch in TRNG circuits

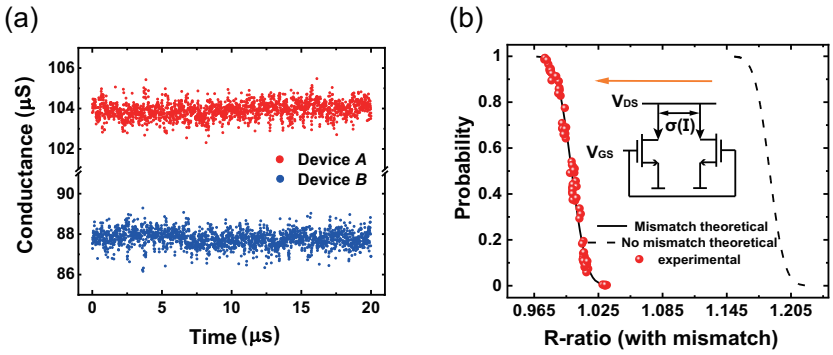

Figure B1 (a) high frequency conductance variation in device A and B. (b) The relationship of ratio of G_A/G_B and the probability of generating "1"s.

* Corresponding author (email: phwang@pku.edu.cn, lfliu@pku.edu.cn)

As shown in Figure B1(a), the HCS conductance distribution is measured in reading conditions (V_{READ} = 0.1 V) and high frequency conductance fluctuation (ΔG) as extracted from RRAM uses Keysight CX3324A device current waveform analyzer at 100 MHz operating frequency. After taking mismatch balance calibration into account, the relationship between the average conductance of the two devices tested and the probability of random number generation is indicated in Figure B2(b), without considering that the theoretical curve of the mismatch is shown as a dotted line.

Appendix C Randomness test results

Table C1 NIST SP 800-22 test results

NIST Test	P-Value	Result
Frequency	0.794838	PASS
Block Frequency	0.652542	PASS
Cumulative Sums	0.911527	PASS
Runs	0.211474	PASS
Longest Runs of ones	0.290003	PASS
FFT	0.558205	PASS
Rank	0.448299	PASS
Nonoverlapping Temp.	0.108584	PASS
Overlapping Temp.	0.614055	PASS
Universal Statistical	0.225162	PASS
Approximate Entropy	0.908113	PASS
Random Excursions	0.712463	PASS
Rand. Excursions Var.	0.450871	PASS
Serial	0.505753	PASS
Linear complexity	0.096011	PASS

Table C1 shows the NIST Special Publication 800-22 randomness all tests passed results for 10 groups of 1Mb Binary bit sequences obtained by our RRAM based TRNG under room temperature.

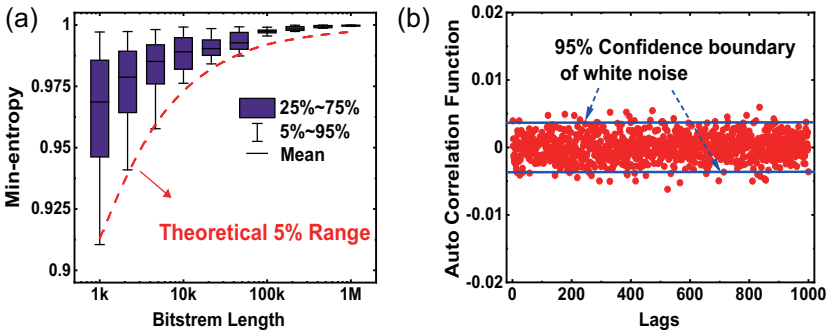

Figure C1 (a) Min-entropy distribution with diverse bitstream lengths from 1k to 1M. (b) Auto-correlation test results of consecutively generated 300 kbits sequence.

As presented in Figure C1(a), we further calculate min-entropy of different segment lengths from experimental data, which agrees well with the theoretical prediction, confirming that randomness of 0 and 1 in different length sequences is achieved. To examine the independence of the output bits, auto-correlation test of each bit relative to the following from 1 to 1000 bits are applied to the experimentally generated 300 kbits, which shows similar behavior as white noise that has the ideal randomness in Figure C2(b).

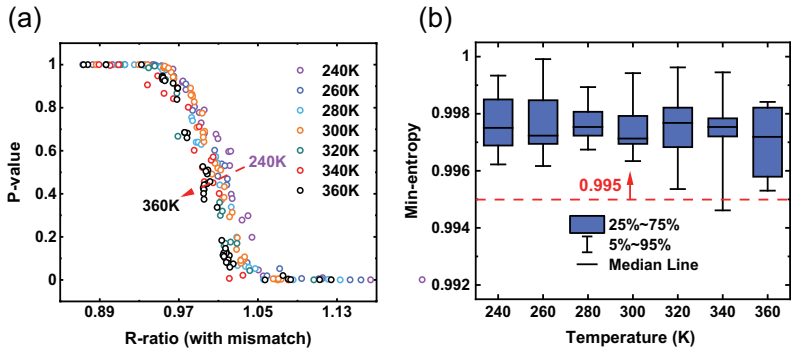

Figure C2 (a) Min-entropy distribution with diverse bitstream lengths from 1k to 1M. (b) Auto-correlation test results of consecutively generated 300 kbits sequence.

Both the threshold turn-on voltage (V_{th}) of transistor [1] and switching voltage during set process (V_{set}) of RRAM that shown in Figure 1(b) [2,3] decrease as the temperature increases, which is consistent with the previous report. As illustrated in Figure C2(a), under the same control voltage conditions, the probability of '1's generation decreased due to the decrease in V_{th} of transistor and V_{set} of RRAM with increasing ambient temperature, resulting in requisite adjustment of conductivity value of RRAM at different temperature. Figure C2(b) shows the estimated min-entropy of the generated bits at different temperatures. The minimum value of the most generated 100 kbits sequence is higher than 0.995, which suggests that excellent unbiased output can still be gained even at extreme temperatures.

References

1 Wang R, Dunkley J, DeMassa T A, et al. Threshold voltage variations with temperature in MOS transistors. IEEE transactions on Electron Devices, 1971, 18: 386-388.

2 Fang Z, Yu H Y, Liu W J, et al. Temperature Instability of Resistive Switching on HfO_x-Based RRAM Devices. IEEE Electron Device Letters, 2010, 31: 476-478.

3 Walczyk C, Walczyk D, Schroeder T, et al. Impact of temperature on the resistive switching behavior of embedded HfO_2-Based RRAM devices. IEEE transactions on electron devices, 2011, 58: 3124-3131.