SCIENCE CHINA
Information Sciences

• LETTER •

November 2023, Vol. 66 219402:1–219402:2
https://doi.org/10.1007/s11432-022-3640-0

# 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*

Received 24 June 2022/Revised 6 September 2022/Accepted 29 November 2022/Published online 20 October 2023

**Citation** Song S Y, Huang P, Shen W S, et al. A 3.3-Mbit/s true random number generator based on resistive random access memory. Sci China Inf Sci, 2023, 66(11): 219402, https://doi.org/10.1007/s11432-022-3640-0

In the era of mobile computing and the Internet of Things, hardware security systems have become ever-increasingly crucial. Resistive random access memory (RRAM) has gained increasing interest in stochastic computing and information security applications due to easy entropy extraction and a high parallel stochastic number throughout [1]. However, the existing RRAM-based true random number generators (TRNGs) rarely reach a desirable speed and low-energy consumption [2].

In this study, we experimentally demonstrate a novel TRNG based on the high-frequency signals found in an RRAM device. In particular, we find a way to avoid the demanding requirement of a sense amplifier (SA) process error. Compared with previous TRNGs based on RRAM, our TRNG has the evident advantage of a single-cell stochastic number generation frequency that reaches 3.3 Mbit/s. In addition, because of the fast comparing speed and no redundancy voltage pulse applied on RRAM, 0.4 pJ/bit-energy efficiency is achieved. Ultimately, our TRNG schemes are supported by presenting and discussing randomness tests under a differential temperature environment.

To demonstrate the proposed TRNG, 4k-bit (64 × 64) 1T1R RRAM arrays are fabricated. Figure 1(a) displays a photograph of the experimental test board and the encapsulated 1T1R RRAM chip. An NMOS transistor fabricated in a 130-nm standard CMOS process ($W = 1$ μm, $L = 500$ nm) and an RRAM with a TiN/$TaO_x$ (45 nm)/$HfO_2$ (8 nm)/TiN structure integrated on top of the transistor drain (500 nm × 500 nm) compose the 1T1R unit in our array. The quasi-static DC current-voltage ($I$-$V$) curve measurement was repeated 1000 times, and the characteristics of RRAM turned out to be relatively stable.

Figure 1(c) shows the basic construction of the TRNG circuit, where two entropy source units (A and B) are connected with current mirrors that lead to two sides of the SA. The entropy sources are implemented using in-chip 1T1R cells, while the SA and other peripheral circuits are also embedded inside our chip. Before our TRNG work, we used a bidirectional incremental gate voltage together with the fixed SET/RESET pulse parameters to precisely adjust the expected high conductance state (HCS) state conductance value in the preconditioning stage. This process is repeated until the target conductance state is reached [3]. Figure 1(d) presents the waveform of the clock signal controlling the work phase of the SA and output signal possibility under different situations. The application of a positive voltage in the clock signal enables the supply voltage ($V_{DD}$) for powering two input cells. The current of cells A and B is duplicated into the positive and negative input ends of the SA through a current mirror, respectively. If $I_A$ is larger than $I_B$, the potential of the output nodes reaches nearly '0', which represents logical '0'; otherwise, the output node potential remains high, which represents logical '1'.

As mentioned in the previous study, electron transport can be inhibited because of the Coulomb blockade, which is caused by charge trapping at defects located near the conductive filament. The state perturbation and the state led by the capture and emission events involved in the charge may be one factor that varies the RRAM current and results in high-frequency current fluctuation [4]. Moreover, the relative fluctuation of the random difference noise current of A and B in the time domain leads to a high-frequency stochastic number throughout. As the RRAM conductance can be controlled more stably in HCS than low conductance state (LCS), HCS state high-frequency noise is used in this work. In the second procedure, with the clock rising to a low electrical level, the cross-coupling latch circuit in the SA enters the reset phase, and the output nodes further return to high potential to prepare for the next comparing operation cycle.

A certain degree of offset can be corrected to the probability of 0.5 by von Neumann post-processing, but if the mismatch is too large, almost all the generated bits are 0 or 1, failing random number generation. When the RRAM resistance values of A and B are identical, the '1' generation probability of a random number is approximately 0.5. However, it will deviate from 0.5 considering the difference in the

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

 

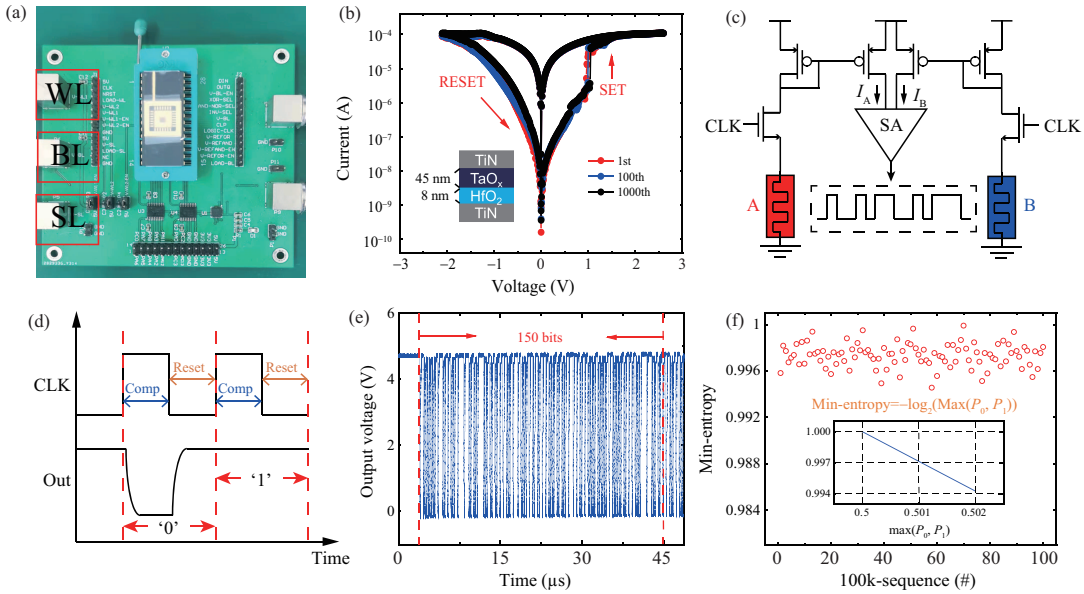


**Figure 1** (Color online) (a) Photograph of the experimental test board and encapsulated 1T1R RRAM chip; (b) structure and *I-V* curve measurement of RRAM; (c) architecture block diagram of the RRAM-based TRNG, including two entropy source devices, the current mirrors, and the SA; (d) concept waveform of the clock and output signal under different circumstances; (e) output voltage of the entropy source device through the SA; (f) distribution of min-entropy in a time-sequential and the relationship between min-entropy and 0/1 uniformity.

SA caused by fabrication [5]. To improve the circumstance of the probability of 0 and 1 deviating from the expectation, we set the average conductance of device A always higher than that of device B to balance the SA mismatch. Ultimately, the '1' generation probability of a random number is controlled between 0.4 and 0.6, which is an acceptable value in post-processing. The detailed measurement is presented in Appendix B.

A fast single-cell throughput $>$ 3.3 Mbit/s is achieved among our RRAM-based TRNGs with a clock cycle set to 300 ns. We estimate that much faster generation can be achieved ($>$ 50 Mbit/s) by exploiting an SA that can operate at a higher frequency. As shown in Figure 1(e), random number bit streams, which comprise '1's and '0's, are measured at the SA output. The von Neumann correction, a standard post-process analysis, is used here to remove the 0 and 1 probability bias from our random number sequence.

We evaluate the randomness of stochastic number bit streams in terms of 0/1 uniformity and independence through the methods of min-entropy estimation and auto-correlation tests, respectively. The maximum possible value for the min-entropy of the random variable $X$ is 1, which is attained when the random variable has a uniform probability distribution. A group of 100-kbit sequences is experimentally generated in chronological order, and min-entropy is achieved very near 1, as indicated in Figure 1(f), clearly demonstrating the uniform distribution of 0/1 by the proposed TRNG. The details of auto-correlation tests can be seen in Appendix C.

A randomness test must be used to assess the performance of any TRNG. The NIST SP 800-22 randomness tests are passed for ten groups of 1-Mb binary bit sequences obtained by our RRAM-based TRNG at room temperature. We further characterize the operations of our RRAM-based TRNG in response to two temperature effects, and it satisfactorily passes the NIST tests even at ambient temperatures ranging from 240 to 360 K.

*Conclusion.* In summary, we have successfully developed a detailed theoretical and experimental TRNG using high-frequency noise in 130-nm embedded RRAM. Binary bit sequences generated by our RRAM-based TRNG are evaluated through min-entropy and pass all the NIST SP 800-22 randomness tests. Moreover, it shows excellent temperature stability; thus, it can be applied in various harsh environments. The high-speed, low-power RRAM-based TRNG demonstrated here shows great potential for communication data security.

**Acknowledgements** This work was supported in part by National Key Research and Development Program of China (Grant No. 2019YFB2205100), National Natural Science Foundation of China (Grant Nos. 61874006, 61834001), and 111 Project Program (Grant No. B18001).

**Supporting information** Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

## References

1 Tseng P H, Lee M H, Lin Y H, et al. ReRAM-based pseudo-true random number generator with high throughput and unpredictability characteristics. IEEE Trans Electron Dev, 2021, 68: 1593–1597
2 Lin B, Gao B, Pang Y, et al. A high-speed and high-reliability TRNG based on analog RRAM for IoT security application. In: Proceedings of IEEE International Electron Devices Meeting (IEDM), San Francisco, 2019
3 Feng Y, Huang P, Zhao Y, et al. Improvement of state stability in multi-level resistive random-access memory (RRAM) array for neuromorphic computing. IEEE Electron Dev Lett, 2021, 42: 1168–1171
4 Puglisi F M, Pavan P, Larcher L, et al. Statistical analysis of random telegraph noise in HfO2-based RRAM devices in LRS. Solid-State Electron, 2015, 113: 132–137
5 Pelgrom M J M, Duinmaijer A C J, Welbers A P G. Matching properties of MOS transistors. IEEE J Solid-State Circ, 1989, 24: 1433–1439