FRONTIERS OF PHYSICS

RESEARCH ARTICLE
Volume 19 / Issue 1 / 13202 / 2024

A high-speed true random number generator based on Ag/SiN_x/n-Si memristor

Xiaobing Yan[#,†], Zixuan Zhang[#], Zhiyuan Guan[#], Ziliang Fang, Yinxing Zhang, Jianhui Zhao, Jiameng Sun, Xu Han, Jiangzhen Niu, Lulu Wang, Xiaotong Jia, Yiduo Shao, Zhen Zhao, Zhenqiang Guo, Bing Bai

Institute of Life Science and Green Development, Key Laboratory of Brain-Like Neuromorphic Devices and Systems of Hebei Province, College of Electron and Information Engineering, Hebei University, Baoding 071002, China
[#]These authors contributed equally to the work.
Corresponding author. E-mail: [†]yanxiaobing@ime.ac.cn
Received April 1, 2023; accepted June 14, 2023

© Higher Education Press 2023

ABSTRACT

The intrinsic variability of memristor switching behavior can be used as a natural source of randomness, this variability is valuable for safe applications in hardware, such as the true random number generator (TRNG). However, the speed of TRNG is still be further improved. Here, we propose a reliable Ag/SiN_x/n-Si volatile memristor, which exhibits a typical threshold switching device with stable repeat ability and fast switching speed. This volatile-memristor-based TRNG is combined with nonlinear feedback shift register (NFSR) to form a new type of high-speed dual output TRNG. Interestingly, the bit generation rate reaches a high speed of 112 kb/s. In addition, this new TRNG passed all 15 National Institute of Standards and Technology (NIST) randomness tests without post-processing steps, proving its performance as a hardware security application. This work shows that the SiN_x-based volatile memristor can realize TRNG and has great potential in hardware network security.

Keywords volatile memristor, true random number generator (TRNG), delay time, threshold switching device

1 Introduction

The Internet of Things (IoT) is a vast network that connects the internet with other objects through information-capturing devices [1]. With the dramatic growth of the number of IoT objects and the excessive use of cyberspace by users around the world, the existing hardware infrastructure is becoming increasingly vulnerable to security threats [1, 2], but the traditional software-based data protection methods are vulnerable to attack by predictive algorithms. "True Random Number Generator (TRNG)" is a hardware component that can generate random bits based on its inherent stochastic physical process to perform the function of key generation and data encryption [3]. Researchers discovered that the memristor exerts a great attraction as a resistive switching device that changes the resistance state by applying an external bias voltage, which has attracted attention due to its low power consumption [4], operational capability, high durability [5], fast switching speed [6], simple metal-insulator-metal structure (MIM) [7], and Complementary Metal Oxide Semiconductor (CMOS) compatibility [8, 9], and it is very suitable for TRNG implement. Early

*Special Topic: Materials, Mechanisms and Applications of Memristors (Eds.: Xiaobing Yan, Bin Gao & Qi Liu).

Higher Education Press

https://doi.org/10.1007/s11467-023-1331-1

TRNGs use the switching voltage or current fluctuations of nonvolatile memristors as a random source, and these methods are feasible. However, due to the lack of true randomness, most TRNGs have difficulties in subsequent randomness testing and require subsequent processing (e.g., von Neumann correction) to pass the NIST randomness test [10–13]. Therefore, researchers turned their attention to volatile-memristor-based TRNG. Jiang *et al.* [14] used the switching delay time in the Ag:SiO_2 diffusive memristor (DM) as a random source, and designed a new circuit with a clock and counter to convert the stochasticity into randomness, and the volatile-memristor-based TRNG that can pass the NIST randomness test without post-processing was developed, and the bit generation rate was increased to 6 kb/s. Subsequently, Woo *et al.* [15] not only used an HfO_2-based volatile memristor, but also optimized the circuit by introducing nonlinear feedback shift register (NFSR), further improving the bit generation rate to 16 kb/s. Kim *et al.* [16] also proposed a self-clocking TRNG device using the oscillating behavior of Mott memristor as a random source, improving the bit generation rate to 40 kb/s. Li *et al.* [17] further increasing the operating speed to 108 kb/s. Above works all have confirmed the randomness of the TRNG through experiments and simulations. However, the operational efficiency of the mentioned TRNGs is only suit for ordinary encryption applications now and still required to be improved for wide application.

In this work, we fabricated a threshold switching (TS) device based on the simple architecture of Ag/SiN_x/n-Si (ASS) for more efficient demonstration of TRNG. It is a newly developed volatile memristor, which has a typical threshold switching characteristic with stable repeat ability, and more encouragingly, the delay time of this TS device is about 47 ns, which is already faster than most TS devices. Further, we use the delay time of this memristor as a random source for setting up TRNG units, which is the key to the successfully setting up high-speed TRNG. Compared with the traditional random number circuits, the ASS-memristor-based TRNG and multiple nonlinear feedback shift register (NFSR) functions are combined, and the rising edge and falling edge of the clock signal are effectively used, which realizes the dual output function and further improves the bit generation rate and operation speed. In addition, since the input bit is converted to a nonlinear function of the previous state, it is better able to withstand password attacks, and the bits generated by this TRNG can directly pass 15 NIST randomness tests without post-processing.

2 Experimental

2.1 Device preparation

In our experiments, SiN_x thin films were prepared on highly conductive silicon (crystal orientation ⟨100⟩, type n, electrical resistivity 0.005–0.007 Ω × cm, thickness (400 ± 15) μm) substrates by radio frequency (RF) magnetron sputtering at a pressure of 1 Pa (only Ar) and a temperature of 300 °C. Finally, the top Ag electrode was deposited by direct current (DC) sputtering with the help of a 100 μm diameter mask.

2.2 Characterizations

The film thickness and the surface morphology were observed by using transmission electron microscope (TEM) and atomic force microscopy (AFM). The I–V curves and pulse electrical measurements were measured by using a Keithley 4200 SCS source meter with 4225 PMU. The input pulse was generated by the Agilent 33250 A function/arbitrary waveform generator and the pulse waveforms were captured with a LeCroy WaveRunner 62 Xi oscilloscope.

3 Results and disscussion

As shown in Fig. 1(a), a layer of silicon nitride about 80 nm thick can be observed in a clear cross-sectional TEM image. Figure 1(b) shows that the silicon nitride layer is a clearly amorphous film, and the film edge is clear and flat. And the AFM scan of the amorphous silicon nitride layer with an area of 10 μm × 10 μm is shown in Fig. 1(c). There is no obvious fluctuation, which means that the roughness of the silicon nitride film is very low, indicating that the amorphous silicon nitride film is relatively uniform and smooth, and can lay a foundation for achieving stable device performance. Figure 1(d) shows the electrical test structure of the memristor. In DC scanning ($I_{cc}=10^{-5}$ A), it is obvious that when the voltage is 5.2 V, the current suddenly increases from a very small current (about 10^{-9} A) to 10^{-5} A, which means that the electroforming process has taken place as shown in Fig. S1 of the Electronic Supplementary Material (ESM). And Fig. 1(e) is the 100-cycle I–V of the device, showing the reliable I–V characteristics of the TS device with 10^{-5} A current compliance, where the device suddenly reaches the low-resistance state (LRS) at about 1.7 V. While the sweep voltage is lower than 0.3 V, the device spontaneously relaxes back to high-resistance state (HRS), and exhibits typical unidirectional threshold switching behavior at a sweep voltage. In addition, the illustration in Fig. 1(e) shows the logarithmic form of I–V over 10 scan cycles, which also illustrates the good switching stability of the device. This threshold behavior is generated by the spontaneous dissipation of the conductive filament (CF) [18–21], and the corresponding mechanism details can be found in ESM. And then, we were pleasantly surprised to find that the I–V curve of the device exhibits the bipolar resistive switching characteristics when I_{cc} was applied up to 10^{-4} A, and the

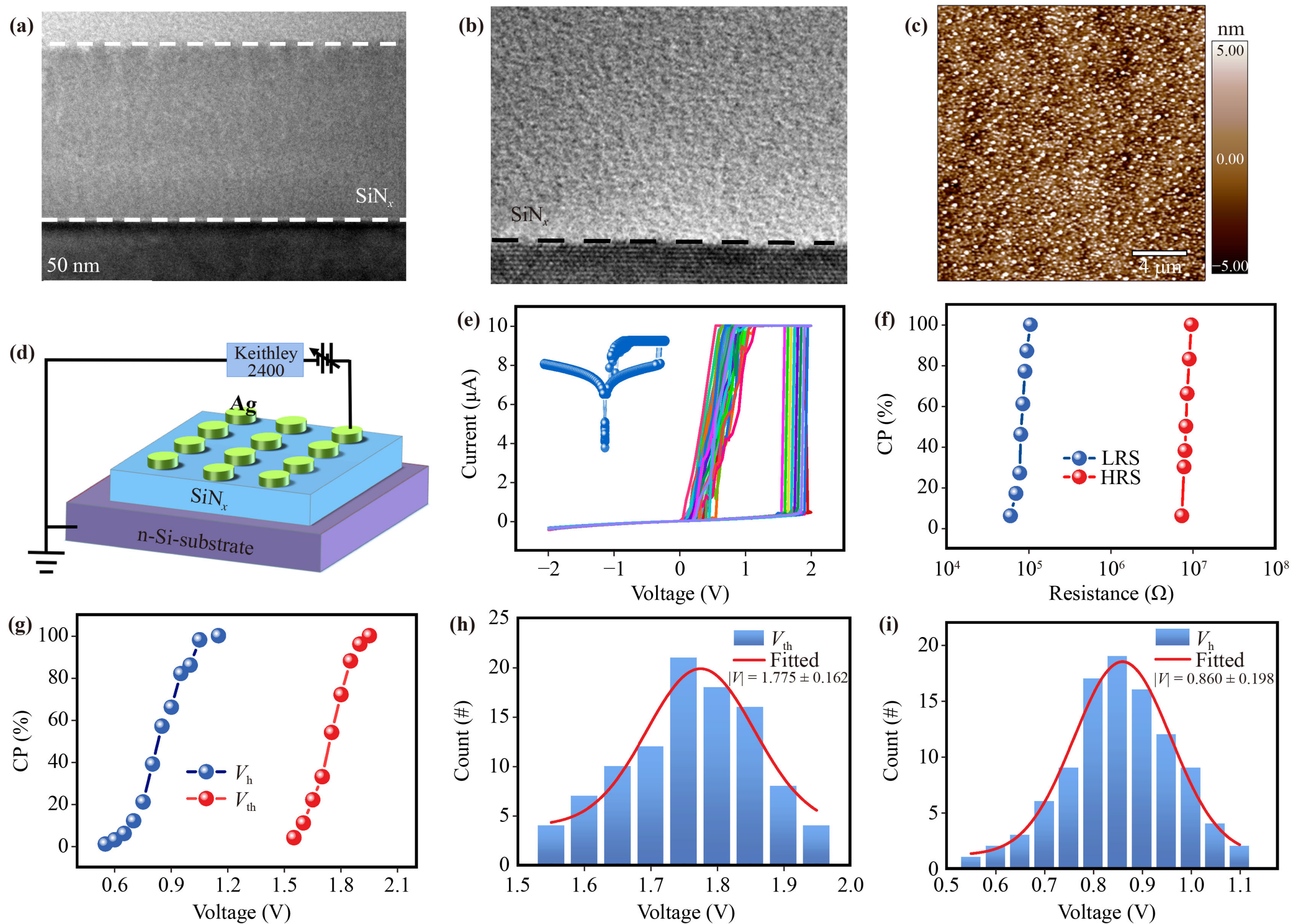


Fig. 1 Characterization of the SiN_x film and ASS device. **(a)** TEM images of a cross-section of the SiN_x film grown on n-Si substrate. **(b, c)** The top-view images of the SiN_x film surface of TEM and AFM, respectively. **(d)** Schematic of the electrical measurement setup for characterizing the ASS structure. **(e)** 100 Consecutive DC switching cycles of the volatile memristor. **(f)** The resistance states distribution from 100 I–V cycles with the I_{cc} of 10^{-5} A. **(g)** Cumulative distribution functions of threshold voltage V_{th}, V_h of the SiN_x/n-Si structure. **(h, i)** The distribution of the threshold/hold voltage with the I_{cc} of 10^{-5} A, respectively.

details of I–V curves can be observed in Fig. S1 of the ESM. To further investigate the distribution of resistance values, the high and low resistance of the device was counted for 100 sweep cycles as shown in Fig. 1(f), and it is found that the HRS is concentrated near 10^7 Ω, and the LRS is concentrated near 10^5 Ω. And the statistics of threshold voltage data under the I_{cc} of 10^{-5} A is shown in Fig. 1(g). The threshold voltage (V_{th}) and holding voltage (V_h) were calculated, and the histogram with Gaussian fit of threshold voltage was analyzed in Figs. 1(h) and (i). The distribution range of V_{th} value is 1.55 to 1.95 V, and the distribution range of V_h value is 0.55 to 1.1 V, and the standard deviations of V_{th} and V_h are (1.775 ± 0.162) V and (0.860 ± 0.198) V, respectively. The variation [$\delta = \Delta V(2\sigma)/V_{mean}$] of V_{th} and V_h of this device is about 9.1% and 23.0%, respectively, which is much lower than other threshold devices (see Table S2 of the ESM). These data are uniformly distributed, which is helpful to design the switching parameters of devices and improve the accurate control of programming voltage in device applications.

To validate the threshold switching properties of the device, we were inspired by the fact that the triggering mechanism of biological nociceptors [22, 23] is highly dependent on total time, intensity and the number of stimuli. In this device, the threshold switching behavior is related to the energy required for the CFs to form between the electrodes [21, 23–25]. Therefore, the threshold switching device output response was simulated by applying electrical pulses with different widths and amplitudes, and when the amplitude or pulse width applied exceeds the threshold, the device was triggered [20, 26]. A series of pulses with 5 V voltage amplitude and different width (from 0.1 μs to 0.5 μs) were applied. It could be observed the device was no respond before 0.4 μs, after that, the output current suddenly increases means that the device was switched to LRS as shown in Fig. 2(a). Then, a series of different amplitudes from

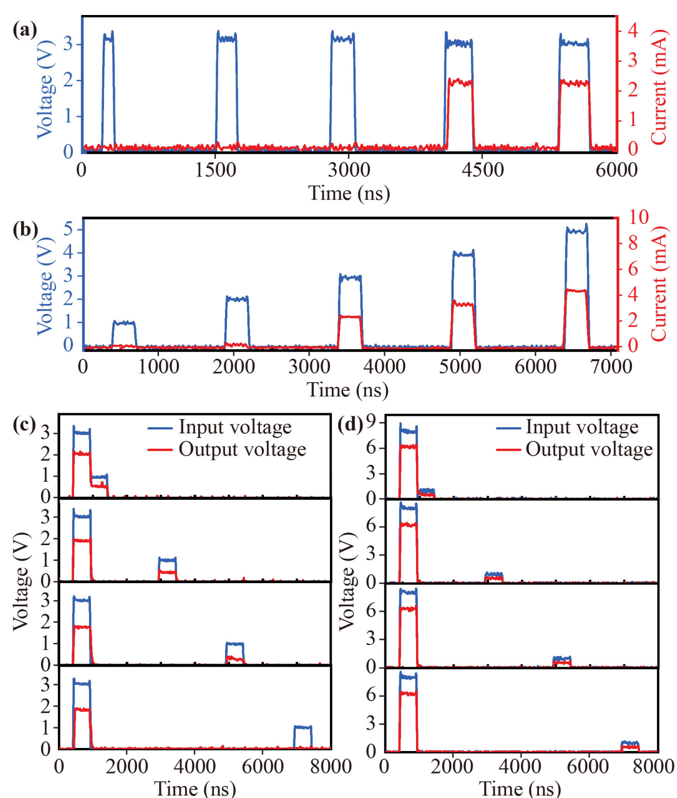


Fig. 2 The current response to the input voltage pulse of the devices. **(a)** A series of input pulses (blue line), consisting of variable width from 0.10 to 0.50 μs and the output voltage (red curve). **(b)** A series of input pulses (blue line), consisting of variable amplitude from 1.0 to 5.0 V, and the red line represents the corresponding output voltage. A higher input voltage leads to a larger output current. **(c)** The relaxation characteristic of using 3 V pulse and then using 1 V pulse, the time interval between the two pulses is 0 μs, 2.5 μs, 4.5 μs, 6.5 μs and the output voltage (red curve). **(d)** The retention characteristic of using 8 V pulse and then using a 1 V pulse, the time interval between the two pulses from 0 μs, 2.5 μs, 4.5 μs, 6.5 μs and the output voltage (red curve).

1 V to 5 V (the pulse width is 0.4 μs) were used, and it was found that when the pulse amplitude reached to 3 V, the device responded. When the amplitude increased to 4 V and 5 V, the output current would further increase, which indicates that the device needs a certain amount of energy for resistance conversion [Fig. 2(b)] [27, 28].

After being stimulated, the threshold switching device entered a "relaxed" state [29], the device output response after different amplitude voltages applied was studied. In Fig. 2(c), a first pulse (voltage: 3 V, width: 0.5 μs) was applied to the device, and then applied a second pulse (voltage: 1 V, width: 0.5 μs) at different intervals (0, 2.5 μs, 4.5 μs, 6.5 μs). It can be found that the device always responded to the first pulse, and the device gradually relaxed to HRS as the interval time increases until it relaxes completely at 6.5 μs. Then, the first pulses with different amplitudes (4 V, 5 V, 6 V, 7 V) and the same second pulses (voltage 1 V, width 0.5 μs) were applied at different intervals were applied to the device, and a similar output response was generated as shown in Fig. S3 of the ESM. However, if the first pulse amplitude was 8 V and the second pulse (voltage 1 V, width 0.5 μs) were applied at different intervals, the device always had a very clear response as shown in Fig. 2(d), which reflects an obvious bipolar resistance characteristic of this device [27], and this bipolar resistance switching characteristic is due to that higher voltage will make the Ag CFs thicker and will be difficult to break spontaneously [30, 31]. Therefore, the device has both bipolar resistance characteristic and the threshold switching phenomenon, which may have relevance to electric field strength [14]. Through these tests, it can be found that the device switching state and response can be changed by various input pulse, which provides a reliable range for selecting a suitable input pulse required by TRNG.

In order to detect the switching speed of the device, a pulse (voltage amplitude 5 V, pulse width 500 ns) ($V_{\rm in}$) was applied, and observed the voltage of series resistor ($V_{\rm out}$) through an oscilloscope. As shown in Figs. 3(a) and (b), a delay time of 47 ns was required from applying a pulse to the device until the device reached LRS, and when the applied voltage removed, the device relaxed to HRS after a relaxation time about 38 ns (See Fig. S4 of the ESM for specific calculation method), and it is faster than many traditional TS devices in Table S3 of the ESM. In order to further study the affecting factors of the delay time, we conducted different pulse amplitude and pulse frequency tests on the device, Fig. 3(c) shows the relationship between the delay time and the voltage amplitude, it can be observed the higher the voltage is, the shorter the average delay time is, and the narrower the distribution is. In addition, the delay time also depends on the pulse frequency, the higher the frequency, the shorter the delay time, as shown in Fig. 3(d). This may be owing to the local temperature increase of the device at higher pulse frequencies, which helps Ag CFs form in the SiN_x film [4, 11, 32–34]. Figure 3(e) shows the 100 cycle delay time statistics of SiN_x under the pulse with a frequency of 1 MHz and an amplitude of 5 V, which can be observed that it conforms to the Gaussian distribution. When the relationship between the average delay, the pulse amplitude and frequency are observed from a statistical point of view, it is found that the higher the voltage amplitude, the shorter the average delay time, and this phenomenon changes roughly linearly with increasing voltage, as shown in Fig. 3(f). In Fig. 3(g), the mean delay time varies significantly with the increase in frequency at the beginning. In addition, the statistical distributions of delay time under different voltages at the same frequency (100 kHz) and different frequencies at the same voltage (5 V) were also

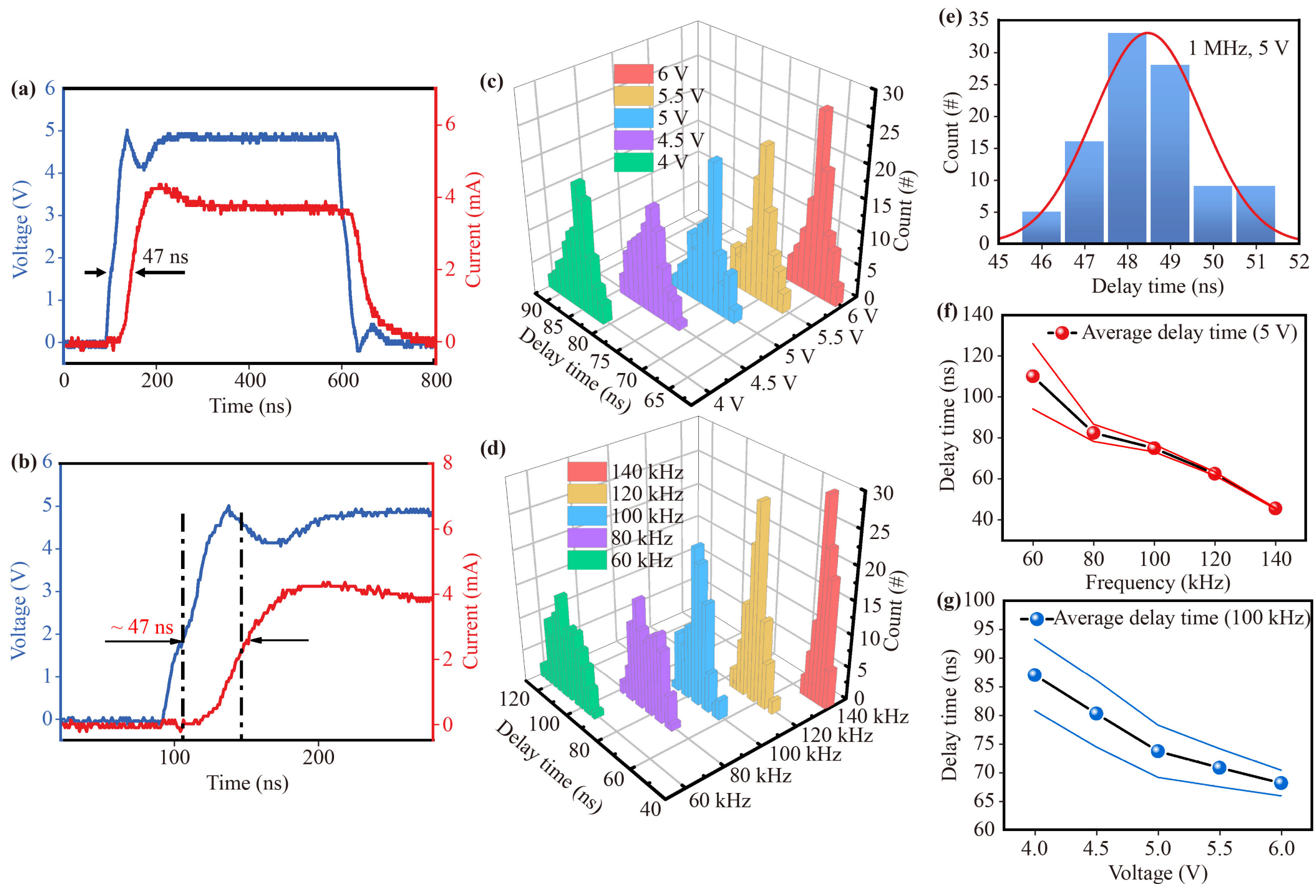


Fig. 3 The effect of voltage and frequency on delay time. **(a, b)** Switching speed of the device. **(c)** Delay time distribution for different input pulse amplitudes (4 V, 4.5 V, 5 V, 5.5 V, 6 V). **(d)** Delay time distribution for different input pulse frequencies (60 kHz, 80 kHz, 100 kHz, 120 kHz, 140 kHz). **(e)** Conduct 100 cycle delay time statistics under the pulse with amplitude of 5 V and frequency of 1 MHz. **(f)** Relationship between average delay time and input voltage. **(g)** Relationship between average delay time and input frequency.

statistically calculated as shown in Figs. S5 and S6 of the ESM.

At present, TRNG unit was constructed using the stochastic delay time generated by the electron capture process as a random source, which was different from the previous nonvolatile-memristor-based TRNG [13, 35, 36]. Traditional nonvolatile memristors need to be set and reset to switch the resistance state, while the volatile memristor exhibits a TS behavior, its random delay time can be used as a random source for a simple circuit, and random logic levels can be read to simplify circuit operation [37–39]. However, the existing volatile-memristor-based TRNG output random numbers at a low speed, that is, the bit generation rate is relatively low, which makes it only suitable for ordinary encryption [40, 41]. In order to increase the application scope of such TRNG and improve its practicality, it is necessary to improve its bit generation rate, and the Linear Feedback Shift Register (LFSR) is a method that can increase the bit generation rate, and its power consumption is also very small [38]. The feedback function of the LFSR is to simply perform a logic operation on some bits in the shift register and populate the result to the leftmost end of the LFSR, as shown in Fig. S7 of the ESM, and for each bit of data in the LFSR, we can participate in the operation or not participate in the operation, but the output of the LFSR depends heavily on the construction of the feedback function, and even if the logic gate is added to complicate the feedback function, the result of the output is also not random. In addition, when XOR gates are used for logical operations, if all initial states are in the "0" state, all D triggers in the LFSR will remain in the "0" state and all outputs will be always locked to "0". In order to solve above situations, we used a nonlinear feedback shift register (NFSR), which is slightly different from LFSR the specific working principle will be described in detail in the next paragraph. Moreover, we also used the logical structure consisted of the XOR gate and the NOT gate as a feedback function, and let the random logic level generated by the memristor participate in the operation of the feedback function, then it is output through a shift register composed of four D flip-flops. In this case, the input bits are nonlinear functions of its previous states, which effectively solves

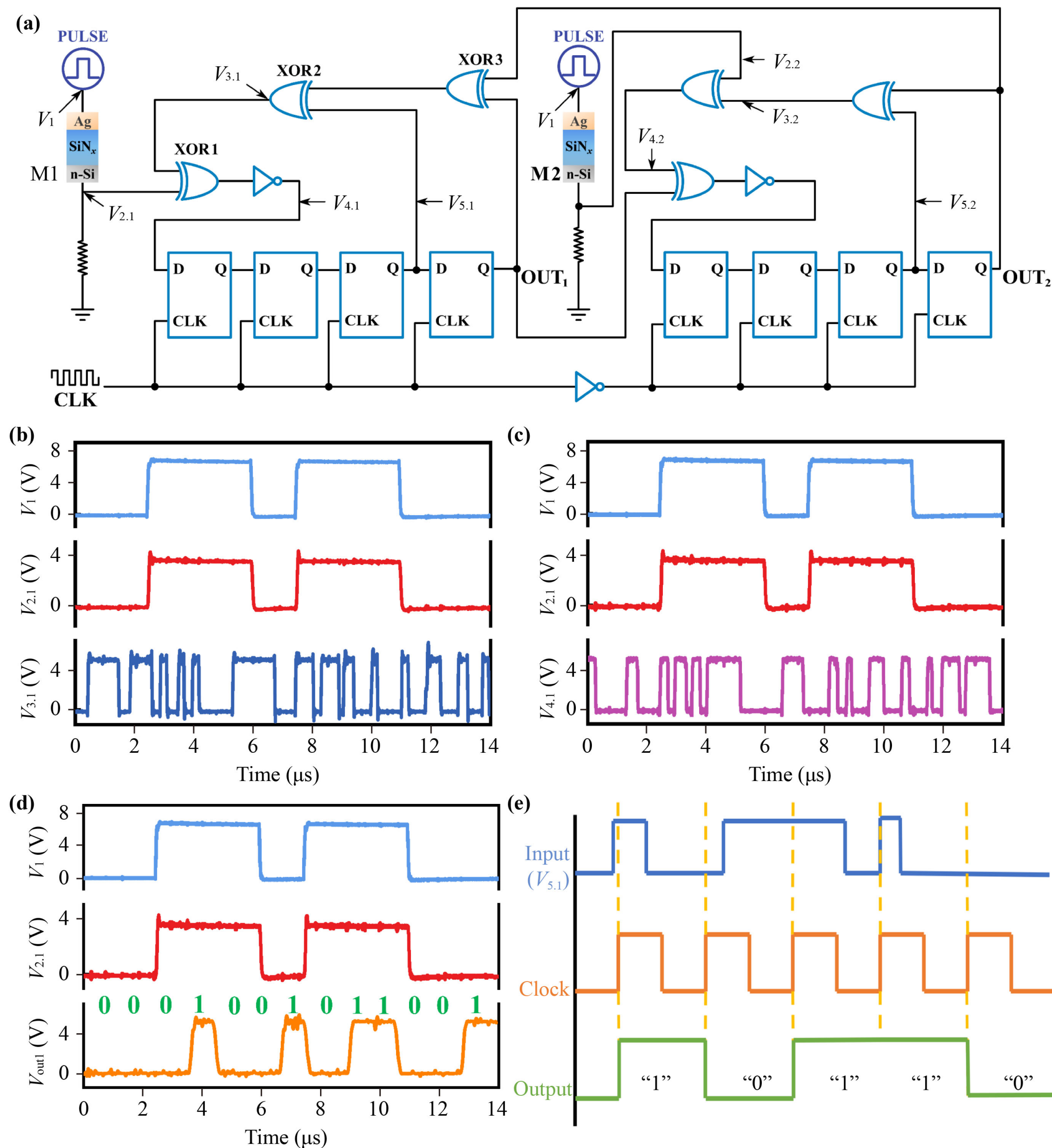


Fig. 4 Implementation of the TRNG. **(a)** Circuit schematic diagram of TRNG. **(b, c)** Voltage test results of each test node. **(d)** Measured output results of two continuous periods of TRNG. **(e)** TRNG output demonstration process.

the above-mentioned latch problem [2, 42, 43].

There are four common NFSRs have been proposed for the linear problem of LFSR, and Fig. S8 of the ESM shows several types of the NFSR. The first method is called Fibonacci NFSR, the new input of (n–1) bits are the result of bringing the last state of all output bits into the nonlinear function calculation, and the output signal strongly depends on the nonlinear function when it is transmitted. The second method is Geffe generator, which is composed of three LFSRs and a multiplexer composed of AND gates and NOT gates. And this method introduces the outputs of multiple LFSRs into nonlinear functions for operation and output results, which enhances the linear complexity too. In addition to nonlinear feedback transformation, the irregular clock signals can also be used for LFSR. And in Massey–Rueppel multispeed generator, one clock signal is the n times of the other, and the complexity of feedback is enhanced by setting two different clocks. Moreover, the Beth–Piper generator also uses an irregular clock to increase the linear complexity, and in this method, LFSR1 controls the clock of LFSR2 through the AND gate[1)] [42, 44].

In this circuit, according to the working principle of Fibonacci NFSR, multiple output bits in the shift register were introduced into the feedback function, and then

1) M. Puczko and V. Yarmolik, Presented at the Third IEEE International Workshop on Electronic Design, Test and Applications (DELTA'06), 2006

Table 1 Comparison of this work with previously reported TRNG.

	Random source	Bit generation rate	NIST tests
Ag:SiO_2 DM TRNG	Delay time	6 kb/s	Passed
HfO_2-based memristor TRNG	Delay and relaxation time	16 kb/s	Passed
Cu_xTe_{1-x} DM TRNG	Delay and relaxation time	32 kb/s	Passed
mott memristor TRNG	Thermal fluctuation	40 kb/s	Passed
Ag/TiN/HfO_x/HfO_y/HfO_x/Pt DM TRNG	integrate-and-firebehaviors	108 kb/s	Passed
This work	Delay time	112 kb/s	Passed

combined with the working principle of Geffe generator, so that different states of memristors would lead to different outputs of the same feedback function. So, this random behavior destroyed the pure dependence of XOR gates and avoided the predictability of pure XOR linear functions. Besides, it also combined the working principles of Massey–Rueppel multispeed generator, and separated the same clock signal into rising edge and falling edge, and reversed the falling edge as the clock of the shift register in the right circuit. In this way, the circuit can output twice in a clock cycle, which greatly improves the efficiency of random number generation. In the design process, the combined functions must be carefully selected to ensure the safety of the results [16], and Fig. 4(a) shows the circuit design of the TRNG, it includes memristor and NFSR composed of NOT gate (CD4069, Texas Instruments), XOR gate (SN74HC86, Renesas) and four D flip flops (MC14015b, Motorola).

What's more, two memristors were introduced into the circuit, which was the key to complete the nonlinear feedback characteristic. Under the pulse stimulation, the memristor completed transition from HRS to LRS after a delay time, and transformed from LRS to HRS after a relaxation time, then realize the input of random logic level [12]. In this circuit, the delay time was regarded as a random seed. The random characteristic of memristor destroys the pure dependence of XOR gate and avoids the predictable mode of output[2)]. According to its response to the input pulse, the memristor will switch to the TS-on state or TS-off state [15]. At this time, the output of the memristor can be read as logic "1" or "0" [3)] [45], and the two states can change the old feedback value (f1) to the new feedback value (f2). Its workflow is shown in Fig. S10 of the ESM. Suppose that under a certain pulse stimulation, the state of the memristor is "1" (TS on), "1", "1", "0" (TS off), "0", "0". In this hypothetical state, the output values are shown in Table S1 of the ESM. It can be observed that when the memristor is in the TS-off state, the new feedback value is opposite to the old feedback value [48]. Otherwise, the new feedback value will not change. Such a circuit structure increases the complexity of the logic operation, improves the output efficiency of data, and makes the output data more random.

Here, the circuit is divided into left and right parts. Since the functions of these two parts are similar, the workflow of the circuit on the left part is mainly introduced, and the related content of the right part is shown in Fig. S9 of the ESM. For the left circuit, the nodes of each test are marked in Fig. 4(a), and when the input pulse V_1 was applied to the memristor (M1), the output voltage value was displayed as $V_{2.1}$ ($V_{2.1}$ was the voltage value of the resistance in series with the M1), and $V_{2.1}$ continued high level after a delay time, which was input to the XOR1 gate together with the feedback signal from XOR2 gate [$V_{3.1}$ in Fig. 4(b)] for logical operation, and then the output result passed through a NOT gate, and the inverting signal would be displayed as $V_{4.1}$ in Fig. 4(c). Finally, $V_{4.1}$ entered the shift register, and was transmitted at each rising edge of the clock signal and finally output [V_{out1} in Fig. 4(d)]. At the same time, the output V_{out1} signal would also participate in the operation of its feedback function as the input of the right circuit. Similarly, the output V_{out2} of the right circuit would also participate in the operation as an input of the left XOR3. Figure 4(e) shows the sequence diagram of simulation $V_{5.1}$ through D flip-flop. Excitedly, the bit generation rate of V_{out1} was 112 kb/s, which was faster in the reported TRNG so far, as shown in Table 1. To better demonstrate the TRNG, the input square wave pulse applied to the memristor was 5 V, the frequency was 200 kHz, and the duty cycle was 70%.

The performance of TRNG is evaluated by NIST statistical test suite (SP 800-22) [35], and the suite can evaluate the randomness and unpredictability of TRNG. The whole suite includes 15 tests, each of which aims at a specific aspect of randomness and returns two statistical information each time, P-value (except for Non overlapping template and Random excursions variant) and pass rate. If the P-value is higher than 0.0001 and the minimum pass rate is reached, each test will be regarded as passed. Here, 85 sequences of 106 bit were collected, which

2) A. Poorghanad, A. Sadr, and A. Kashanipour, Presented in part at the Proceedings of the 2008 International Conference on Computational Intelligence and Security –Vol. 01, 2008

3) S. Fujita, K. Uchida, S. Yasuda, R. Ohba, H. Nozaki, and T. Tanamoto, Presented at the 2004 IEEE International Solid-State Circuits Conference (IEEE Cat. No. 04CH37519), 2004

Table 2 NIST randomness test results.

Test	*P*-value	Pass rate	Min. pass rate	Pass/fail
1. Frequency	0.676097	81/85	80/85	Pass
2. Block frequency	0.701879	84/85	80/85	Pass
3. Cumulative sums	0.624107, 0.126842	82/85, 81/85	80/85	Pass
4. Runs	0.340461	84/85	80/85	Pass
5. Longest run	0.126842	84/85	80/85	Pass
6. Rank	0.947557	85/85	80/85	Pass
7. FFT	0.284375	83/85	80/85	Pass
8. Non overlapping template	–	12447/12580	11917/12580	Pass
9. Overlapping template	0.823278	81/85	80/85	Pass
10. Universal	0.999091	85/85	80/85	Pass
11. Approximate entropy	0.624107	83/85	80/85	Pass
12. Random excursions	–	413/416	388/416	Pass
13. Random excursions variant	–	928/936	874/936	Pass
14. Serial	0.572333, 0.448892	83/85, 83/85	80/85	Pass
15. Linear complexity	0.598138	83/85	80/85	Pass

passed all 15 NIST tests without any post-processing steps, verifying the he reliability of randomness [37]. The test results are shown in Table 2.

4 Conclusion

In conclusion, we fabricated a high-performance Ag/SiN_x/n-Si volatile memristor with stable threshold switching characteristics, and the TS device has fast switch speed with the delay time of 47 ns and the relaxation time of 38 ns. In addition, we also discussed the key factors affecting the delay time of the device and provided data support. Then, the delay time of the device was used as a random source to build the TRNG and we provided a suitable choice for the input pulse of the TRNG according to the threshold characteristics. And more interestingly, the combination of volatile-memristor-based TRNG and NFSR yielded a bit generation rate of 112 kb/s, and successfully passed 15 NIST tests without any subsequent processing. With the increasing importance of hardware security in the Internet of things era, it is believed that the ASS-memristor-based TRNG has a great application potential in hardware security system.

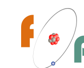
Declarations The authors declare that they have no competing interests and there are no conflicts.

Electronic supplementary materials The online version contains supplementary material available at https://doi.org/10.1007/s11467-023-1331-1 and https://journal.hep.com.cn/fop/EN/10.1007/s11467-023-1331-1.

Acknowledgements This work was financially supported by the National Key R&D Plan "Nano Frontier" Key Special Project (Grant No. 2021YFA1200502), Cultivation Projects of National Major R&D Project (Grant No. 92164109), the National Natural Science Foundation of China (Grant Nos. 61874158, 62004056, and 62104058), the Special Project of Strategic Leading Science and Technology of Chinese Academy of Sciences (Grant No. XDB44000000-7), Key R&D Plan Projects in Hebei Province (Grant No. 22311101D), Hebei Basic Research Special Key Project (Grant No. F2021201045), the Support Program for the Top Young Talents of Hebei Province (Grant No. 70280011807), the Supporting Plan for 100 Excellent Innovative Talents in Colleges and Universities of Hebei Province (Grant No. SLRC2019018), the Interdisciplinary Research Program of Natural Science of Hebei University (No. DXK202101), the Institute of Life Sciences and Green Development (No. 521100311), the Natural Science Foundation of Hebei Province (Nos. F2022201054 and F2021201022), the Outstanding Young Scientific Research and Innovation Team of Hebei University (Grant No. 605020521001), the Special Support Funds for National High Level Talents (Grant No. 041500120001), the Advanced Talents Incubation Program of the Hebei University (Grant Nos. 521000981426, 521100221071, and 521000981363), and the Science and Technology Project of Hebei Education Department (Grant Nos. QN2020178 and QN2021026).

References

1. R. H. Weber and R. Weber, Internet of Things, Springer, 2010
2. V. d. Leest, R. Maes, G. J. Schrijen, and P. Tuyls, in: ISSE 2014 Securing Electronic Business Processes, Springer, 2014, pp 188–198
3. C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, Secure integration of IoT and cloud computing, *Future Gener. Comput. Syst.* 78, 964 (2018)
4. M. D. Pickett and R. Stanly Williams, Sub-100 fJ and sub-nanosecond thermally driven threshold switching in niobium oxide crosspoint nanodevices, *Nanotechnology* 23(21), 215202 (2012)
5. 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, *Nat. Mater.* 10(8), 625 (2011)
6. A. C. Torrezan, J. P. Strachan, G. Medeiros-Ribeiro, and R. S. Williams, Sub-nanosecond switching of a tantalum oxide memristor, *Nanotechnology* 22(48), 485203 (2011)
7. S. Kvatinsky, E. G. Friedman, A. Kolodny, and U. C. Weiser, TEAM: Threshold adaptive memristor model, *IEEE Trans. Circuits Syst. I Regul. Pap.* 60(1), 211 (2013)
8. Q. Xia, W. Robinett, M. W. Cumbie, N. Banerjee, T. J. Cardinali, J. J. Yang, W. Wu, X. Li, W. M. Tong, D. B. Strukov, G. S. Snider, G. Medeiros-Ribeiro, and R. S. Williams, Memristor–CMOS hybrid integrated circuits for reconfigurable logic, *Nano Lett.* 9(10), 3640 (2009)
9. Z. K. Dong, D. L. Qi, Y. F. He, Z. Xu, X. F. Hu, and S. K. Duan, Easily cascaded memristor-CMOS hybrid circuit for high-efficiency boolean logic implementation, *Int. J. Bifurcat. Chaos* 28(12), 1850149 (2018)
10. 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* 28(45), 455202 (2017)
11. 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, *Nat. Commun.* 8(1), 882 (2017)
12. L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, S. D. Leigh, M. Levenson, M. Vangel, N. A. Heckert and D. L. Banks, A statistical test suite for random and pseudorandom number generators for cryptographic applications, National Institute of Standards & Technology, 2010
13. 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 Dev.* 63(5), 2029 (2016)
14. J. H. Yoon, Z. Wang, K. M. Kim, H. Wu, V. Ravichandran, Q. Xia, C. S. Hwang, and J. J. Yang, An artificial nociceptor based on a diffusive memristor, *Nat. Commun.* 9(1), 417 (2018)
15. K. S. Woo, Y. M. Wang, J. Kim, Y. Kim, Y. J. Kwon, J. H. Yoon, W. Kim, and C. S. Hwang, A true random number generator using threshold-switching-based memristors in an efficient circuit design, *Adv. Electron. Mater.* 5(2), 1800543 (2019)
16. G. Kim, J. H. In, Y. S. Kim, H. Rhee, W. Park, H. Song, J. Park, and K. M. Kim, Self-clocking fast and variation tolerant true random number generator based on a stochastic Mott memristor, *Nat. Commun.* 12(1), 2906 (2021)
17. Y. F. Lu, H. Y. Li, Y. Li, L. H. Li, T. Q. Wan, L. Yang, W. B. Zuo, K. H. Xue, and X. S. Miao, A high-performance $Ag/TiN/HfO_x/HfO_y/HfO_x/Pt$ diffusive memristor for calibration-free true random number generator, *Adv. Electron. Mater.* 8(9), 2200202 (2022)
18. H. He, Y. Pei, J. Wang, Z. Zhang, J. Liu, L. Yan, Y. Zhao, X. Li, Y. Wei, and J. Chen, A hamming weight calculation of binary string in one nMOS transistor–one Ag/HfO_2/black phosphorus/Pt memristor, *IEEE Trans. Electron Devices* 69(9), 22008490 (2022)
19. L. Yan, Y. F. Pei, J. J. Wang, H. He, Y. Zhao, X. Y. Li, Y. X. Wei, and X. B. Yan, High-speed Si films based threshold switching device and its artificial neuron application, *Appl. Phys. Lett.* 119(15), 153507 (2021)
20. Y. X. Zhang, Z. L. Fang, and X. B. Yan, HfO_2-based memristor-CMOS hybrid implementation of artificial neuron model, *Appl. Phys. Lett.* 120(21), 213502 (2022)
21. Z. R. Wang, S. Joshi, S. E. Savel'ev, H. Jiang, R. Midya, P. Lin, M. Hu, N. Ge, J. P. Strachan, Z. Y. Li, Q. Wu, M. Barnell, G. L. Li, H. L. Xin, R. S. Williams, Q. F. Xia, and J. J. Yang, Memristors with diffusive dynamics as synaptic emulators for neuromorphic computing, *Nat. Mater.* 16(1), 101 (2017)
22. X. Xu, E. J. Cho, L. Bekker, A. A. Talin, E. Lee, A. J. Pascall, M. A. Worsley, J. Zhou, C. C. Cook, J. D. Kuntz, S. Cho, and C. A. Orme, A bioinspired artificial injury response system based on a robust polymer memristor to mimic a sense of pain, sign of injury, and healing, *Adv. Sci. (Weinh.)* 9(15), 2200629 (2022)
23. R. Midya, Z. Wang, J. Zhang, S. E. Savel'ev, C. Li, M. Rao, M. H. Jang, S. Joshi, H. Jiang, P. Lin, K. Norris, N. Ge, Q. Wu, M. Barnell, Z. Li, H. L. Xin, R. S. Williams, Q. Xia, and J. J. Yang, Anatomy of Ag/Hafnia-based selectors with 10^{10} nonlinearity, *Adv. Mater.* 29(12), 1604457 (2017)
24. X. Yan, H. Li, L. Zhang, C. Lu, J. Zhao, Z. Zhou, H. Wang, J. Wang, X. Li, Y. Pei, C. Qin, G. Wang, Z. Xiao, Q. Zhao, K. Wang, D. Ren, and S. Zheng, Density effects of graphene oxide quantum dots on characteristics of $Zr_{0.5}Hf_{0.5}O_2$ film memristors, *Appl. Phys. Lett.* 114(16), 162906 (2019)
25. Y. Wang, Q. Wang, J. Zhao, T. Niermann, Y. Liu, L. Dai, K. Zheng, Y. Sun, Y. Zhang, J. Schwarzkopf, T. Schroeder, Z. Jiang, W. Ren, and G. Niu, A robust high-performance electronic synapse based on epitaxial ferroelectric $Hf_{0.5}Zr_{0.5}O_2$ films with uniform polarization and high Curie temperature, *Appl. Mater. Today* 29, 101587 (2022)
26. D. Q. Liu, H. F. Cheng, G. Wang, X. Zhu, and N. N. Wang, Diode-like volatile resistive switching properties in amorphous Sr-doped $LaMnO_3$ thin films under lower current compliance, *J. Appl. Phys.* 114(15), 154906 (2013)
27. L. A. Liu, J. H. Zhao, G. Cao, S. K. Zheng, and X. B. Yan, A memristor-based silicon carbide for artificial nociceptor and neuromorphic computing, *Adv. Mater. Technol.* 6(12), 2100373 (2021)
28. S. A. Chekol, S. Menzel, R. Waser, and S. Hoffmann-Eifert, Strategies to control the relaxation kinetics of Ag -based diffusive memristors and implications for device operation, *Adv. Electron. Mater.* 8(11), 2200549 (2022)
29. Y. H. Chen, Y. Wang, Y. H. Luo, X. W. Liu, Y. Q. Wang, F. Gao, J. G. Xu, E. T. Hu, S. Samanta, X. Wan, X. J. Lian, J. Xiao, and Y. Tong, Realization of artificial neuron using MXene Bi-directional threshold switching memristors, *IEEE Electron Device Lett.* 40(10), 1686 (2019)

30. O. Kwon, J. Shin, D. Chung, and S. Kim, Energy efficient short-term memory characteristics in Ag/SnO_x/TiN RRAM for neuromorphic system, *Ceram. Int.* 48(20), 30482 (2022)
31. O. Kwon, Y. Lee, M. Kang, and S. Kim, Synaptic plasticity features and neuromorphic system simulation in AlN-based memristor devices, *J. Alloys Compd.* 911, 164870 (2022)
32. S. Saitoh and K. Kinoshita, Oxide-based selector with trap-filling-controlled threshold switching, *Appl. Phys. Lett.* 116(11), 112101 (2020)
33. D. Dev, A. Krishnaprasad, M. S. Shawkat, Z. He, S. Das, D. Fan, H. S. Chung, Y. Jung, and T. Roy, 2D MoS_2-based threshold switching memristor for artificial neuron, *IEEE Electron Device Lett.* 41(6), 936 (2020)
34. W. Wang, W. Song, P. Yao, Y. Li, J. Van Nostrand, Q. Qiu, D. Ielmini, and J. J. Yang, Integration and Co-design of memristive devices and algorithms for artificial intelligence, *iScience* 23(12), 101809 (2020)
35. S. Balatti, S. Ambrogio, Z. Q. Wang, and D. Ielmini, True random number generation by variability of resistive switching in oxide-based devices, *IEEE J. Emerg. Sel. Top. Circuits Syst.* 5(2), 214 (2015)
36. B. Wei and C. Lu, Exploring device-circuit co-design in LC VCO circuits using monolayer transition metal dischalcogenide MoS_2 field-effect transistors, *AEU Int. J. Electron. Commun.* 138, 153867 (2021)
37. K. S. Woo, J. Kim, J. Han, J. M. Choi, W. Kim, and C. S. Hwang, A high-speed true random number generator based on a Cu_xTe_{1-x} diffusive memristor, *Adv. Intell. Syst.* 3(7), 2100062 (2021)
38. K. S. Woo, Y. Wang, Y. Kim, J. Kim, W. Kim, and C. S. Hwang, A combination of a volatile-memristor-based true random-number generator and a nonlinear-feedback shift register for high-speed encryption, *Adv. Electron. Mater.* 6(5), 1901117 (2020)
39. Y. F. Lu, H. Y. Li, Y. Li, L. H. Li, T. Q. Wan, L. Yang, W. B. Zuo, K. H. Xue, and X. S. Miao, A high-performance Ag/TiN/HfO_x/HfO_y/HfO_x/Pt diffusive memristor for calibration-free True Random Number Generator, *Adv. Electron. Mater.* 8(9), 2200202 (2022)
40. S. W. Ke, L. Jiang, Y. F. Zhao, Y. Y. Xiao, B. Jiang, G. Cheng, F. C. Wu, G. S. Cao, Z. H. Peng, M. Zhu, and C. Ye, Brain-like synaptic memristor based on lithium-doped silicate for neuromorphic computing, *Front. Phys.* 17(5), 53508 (2022)
41. L. G. Gao, F. Alibart, and D. B. Strukov, Programmable CMOS/memristor threshold logic, *IEEE Trans. NanoTechnol.* 12(2), 115 (2013)
42. R. R. Dube, Hardware-Based Computer Security Techniques to Defeat Hackers: From Biometrics to Quantum Cryptography, John Wiley & Sons, 2008
43. K. Zeng, C. H. Yang, D. Y. Wei, and T. Rao, Pseudorandom bit generators in stream-cipher cryptography, *Computer* 24(2), 8 (1991)
44. E. Dubrova, A transformation from the fibonacci to the galois NLFSRs, *IEEE Trans. Inf. Theory* 55(11), 5263 (2009)
45. W. H. Wang and G. D. Zhou, Moisture influence in emerging neuromorphic device, *Front. Phys.* 18(5), 53601 (2022)