ADVANCED ELECTRONIC MATERIALS
www.advelectronicmat.de

A Combination of a Volatile-Memristor-Based True Random-Number Generator and a Nonlinear-Feedback Shift Register for High-Speed Encryption

*Kyung Seok Woo, Yongmin Wang, Yumin Kim, Jihun Kim, Woohyun Kim, and Cheol Seong Hwang**

A true random-number generator (TRNG) and a nonlinear feedback shift register (NFSR) are combined to create a new type of TRNG. This TRNG is based on the intrinsic stochasticity of threshold switching behavior in a Pt/HfO_2/TiN memristor and an NFSR circuit. Considering the transition rate of the hopping process, the stochasticity of the delay time can be attributed to the phonon-assisted hopping process. This novel TRNG passes all 15 National Institute of Standards and Technology randomness tests without post-processing steps, proving its performance as a hardware security application. By combining the TRNG with the NFSR, the bit generation rate is further improved, allowing it to be used for high-speed applications.

The memristor has received significant attention for a wide variety of applications, due to its high density, low power consumption, and high switching speed.[1–3] However, achieving switching uniformity remains an issue that must be realized for actual commercialization. The nonuniformity comes from stochastic and complicated physical phenomena during the switching process, and it is hard to overcome. However, in recent years, this randomness is being used for security applications, such as the true random number generator (TRNG) and physically unclonable function.[4–8] The TRNG is hardware security that generates random bits from its intrinsically stochastic physical process. As the global market for the Internet of Things (IoT) is growing by huge amounts, security and data privacy have become more necessary. Since the pseudorandom number generator (PRNG), a software component that relies on a pre-determined and predictable algorithm, is susceptible to cryptographic attacks, researchers have focused on the memristor-based TRNG. The most important step in implementing TRNG is to pass the National Institute of Standards and Technology (NIST) randomness tests without any post-processing step. The requirement of a post-processing step means that the device itself lacks randomness.[9] Jiang et al. introduced a TRNG that passed all the NIST tests for the first time as a memristive-switching TRNG.[10] The stochastic delay time, attributed to the ionic process of Ag particles detaching from an Ag reservoir, was utilized as a random source. This was also the first volatile-memristor-based TRNG, and it is superior to the nonvolatile-memristor-based TRNG, in that it does not need a RESET process. Another volatile-memristor-based TRNG was previously reported with a Pt/HfO_2/TiN structure.[11] Here, the TRNG was realized with two random sources: delay and relaxation times. The newly developed circuit was simple, small, and immune to memristor breakdown. However, all prior volatile-memristor-based TRNGs provide low bit generation rate, which is only suitable for low-speed encryption applications, such as car keys, identification cards, and secure session link keys.[12,13] For such TRNGs to be used more widely, the bit generation rate must be improved. A linear feedback shift register (LFSR) is a simple way to increase the bit generation rate with minimal power consumption.[10,14] This is a shift register that uses either an XOR or an XNOR gate as a linear function, so its input bit becomes a linear function of its previous state. However, it is PRNG that is not truly random. The outputs of the LFSR depend heavily on the chosen algorithm; the number of D flip-flops, or what we can term the order of the LFSR. Its inherent linearity makes it vulnerable to cryptographic attacks. Also, in the case of all "0" states when an XOR gate is used, all the D flip-flops will remain "locked-up," and the output will always be "0." The same situation goes for an XNOR gate, as all "1" states will cause the output to be "1." On the other hand, the nonlinear feedback shift register (NFSR) has been proposed as an alternative to the LFSR. It is slightly different from the LFSR, in that its input bit is now a nonlinear function of its previous state, becoming more resistant to cryptographic attacks.[15,16] There have been several NFSR designs to solve the linearity problem of the LFSR, and these can be classified into three kinds: i) a nonlinear combination of output bits from the LFSR, ii) a nonlinear combination of several LFSRs, and iii) irregular clocking in the LFSR.[17–19] Figure S1 in the Supporting Information shows the three types. Figure S1a in the Supporting Information contains *n* bits (from right

K. S. Woo, Y. Wang, Y. Kim, J. Kim, W. Kim, Prof. C. S. Hwang
Department of Materials Science and Engineering and Inter-University Semiconductor Research Center
Seoul National University
Gwanak-ro 1, Gwanak-gu, Seoul 08826, Republic of Korea
E-mail: cheolsh@snu.ac.kr

The ORCID identification number(s) for the author(s) of this article can be found under https://doi.org/10.1002/aelm.201901117.

DOI: 10.1002/aelm.201901117

to left) and state feedback, which comes from every bit, and goes into $(n-1)$ bit. With the clock signal, the new input of $(n-1)$ bit is calculated by the nonlinear function of previous states of output bits. This measure is strongly dependent on the nonlinear function. The second way to strengthen the linear complexity is to combine several LFSRs by feeding their outputs into a nonlinear function. Figure S1b in the Supporting Information shows the Geffe generator that consists of three LFSRs and a two-to-one multiplexer, whose output is presented as $b(t) = a_1(t)a_3(t) \oplus \overline{a_1(t)}a_2(t)$. Besides the nonlinear feedback transformation, another solution is to use the irregular clocking in the LFSR. Figure S1c in the Supporting Information shows that the Massey–Rueppel's generator enhances the complexity of feedback by setting the LFSRs at two different clocks. This multispeed system leads to the output of $c(t) = \sum_{i=0}^{l-1} a(t+i)b(dt+i)$. Here, d is a secret variable, which decides the clock of LFSR-2 (d times the clock of LFSR-1). Figure S1d in the Supporting Information shows that in the Beth-Piper stop-and-go generator, the clock of the LFSR-2 is subject to the output of LFSR-1 through an AND gate. The LFSR-2 state can change at time t only when $a_1(t-1) = 1$. This situation leads to different clock frequencies for these two LFSRs, increasing the linear complexity.

In this work, the volatile-memristor-based TRNG and the NFSR were combined. The random seed produced from a Pt/HfO_2/TiN (PHT) memristor and the extra XNOR gate allowed the circuit to become unpredictable, solving the linearity problem. The XNOR gate also prevented the locked-up state. The PHT memristor is an electronic-switching-based device, which is known to have high switching speed, low power consumption, and high reliability.[3,20–23] Moreover, the stochasticity of the PHT memristor was analyzed for deeper understanding of its electron trapping/detrapping mechanism. The use of the NFSR further improved the bit generation rate. This novel TRNG overcame all the drawbacks that existed in the previous memristor-based TRNG and LFSR designs, such as bit generation rate, linearity, and locked-up state.

Figure 1 shows the threshold switching (TS) behavior of the PHT memristor. An 8 μm × 8 μm electrode area of the PHT memristor was fabricated in a crosspoint structure, as shown in the scanning electron microscopy (SEM) image (Figure 1a). The transmission electron microscopy (TEM) and the Auger electron spectroscopy (AES) images shown in Figure S2 in the Supporting Information confirm the structure of the PHT memristor. This device has an electron trapping/detrapping mechanism that can be understood by the shallow trap level with trap energy of ≈0.7 eV in the HfO_2 layer and an internal electric field caused by the work function mismatch between Pt and TiN electrodes.[24] Figure 1b shows that the TS behavior can be explained with band diagrams. Initially, the device is in OFF state (TS-off state), where the trap site is empty. A positive bias is applied to the Pt top electrode (TE) to pull the trap level down to a level below the Fermi level of the TiN bottom electrode (BE), so that the trap site can be filled with electrons injected from the TiN BE. Then, the device switches to an ON

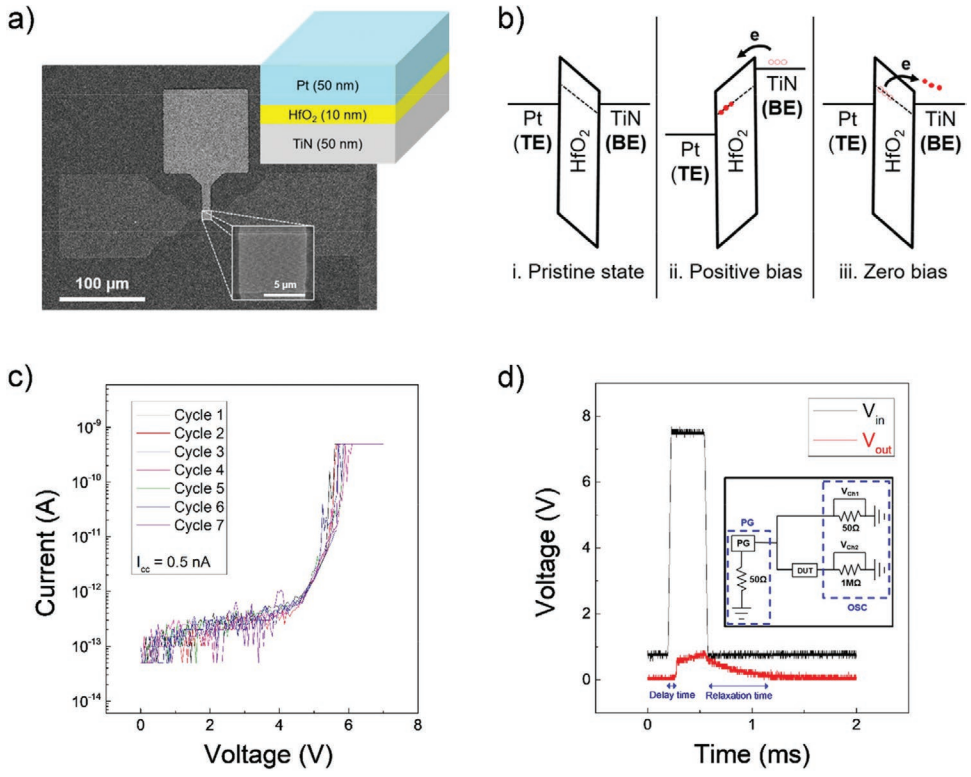


Figure 1. Pt/HfO_2/TiN (PHT) Memristor. a) SEM image of the 8 μm × 8 μm crosspoint structure. The inset shows a schematic of the PHT memristor. b) Schematic band diagram of the threshold switching behavior. c) *I–V* curves of the PHT memristor. d) Pulse switching behavior of the PHT memristor. The inset shows the circuit configuration of the pulse measurement system.

state (TS-on state) due to the trap-assisted tunneling conduction. Depending on the level of the compliance current (I_{cc}), which controls the number of trapped electrons, the device can possess either TS behavior (at low I_{cc}) or resistance switching (RS) behavior (at high I_{cc}). The RS behavior is the conventional nonvolatile-memristor behavior that requires SET and RESET processes to switch the device into the low resistance state and high resistance state, respectively. At low I_{cc}, the traps are partially filled near the Pt TE, where the Fermi level is relatively low. When the voltage is removed, the trapped electrons near the Pt TE can be detrapped easily. On the other hand, all the traps in the HfO_2 layer would be filled with electrons at high I_{cc}. During the detrapping process, the trapped electrons near the TiN bottom electrode require much more time to be detrapped. In this case, a negative voltage is required for the complete electron detrapping. This can be regarded as the RESET process. The current–voltage (I–V) curves in Figure 1c show that the memristor is electroforming-free and has TS behavior at I_{cc} of 0.5 nA, with seven consecutive sweeps being overlapped. In the pulse measurement (Figure 1d), the memristor after a certain delay time reached the TS-on state, and when the voltage was removed, relaxed back to the TS-off state. A relaxation time was also observed when the hold voltage of 600 mV was given. The inset of Figure 1d shows the circuit configuration of the pulse measurement. An input pulse was applied from a pulse generator (PG), and an oscilloscope (OSC) was used to monitor two channels: the input voltage (V_{in}) through Channel 1 (V_{Ch1}), and the output voltage (V_{out}) through Channel 2 (V_{Ch2}).

Figure 2 demonstrates the new concept of the TRNG. Figure 2a shows the circuit diagram with a memristor, and an NFSR consisting of one XNOR gate (Texas Instruments, SN74LS266), one XOR gate (Renesas, HD74HC86) and four D flip-flops (ON Semiconductor, MC14015B), which are used as shift registers. In the previous TRNG research, a counter, which produces final output bits, was made of T flip-flops.[10,11] In this experiment, D flip-flops are used instead. They are superior to T flip-flops in terms of the bit generation rate. Figure S3 in the Supporting Information shows that the D flip-flop produces more bits than the T flip-flop in the same period with the same clock frequency. The reason for the bit generation rate difference lies in their operational principles. The T flip-flop generates the output bits through bit flipping, and its shortest bit flipping frequency is half of the clock frequency. The output bit is finalized at the trailing edge of the input signal. On the other hand, the output bit of the D flip-flop is produced at every leading edge of the clock signal, and the input signal level at that point becomes the final output bit. Since the clock frequency is shorter than the input frequency, the clock-dependent D flip-flop operates faster than the T flip-flop. Figure 2b shows the proof of concept with pulse sequences at each state of the circuit as labeled in Figure 2a. When a pulse voltage (V_1) is applied to a memristor, M (panel 1), the output voltage (V_2) increases after a certain delay time (panel 2). This peak goes to an XNOR gate with V_3 from the feedback (panel 3), and the output voltage (V_4 of panel 4) is sent to a shift register (SR) (panel 5). The initial state of the NFSR is termed a seed, and the SR position that is connected to the XOR gate is termed a tap. The seed is

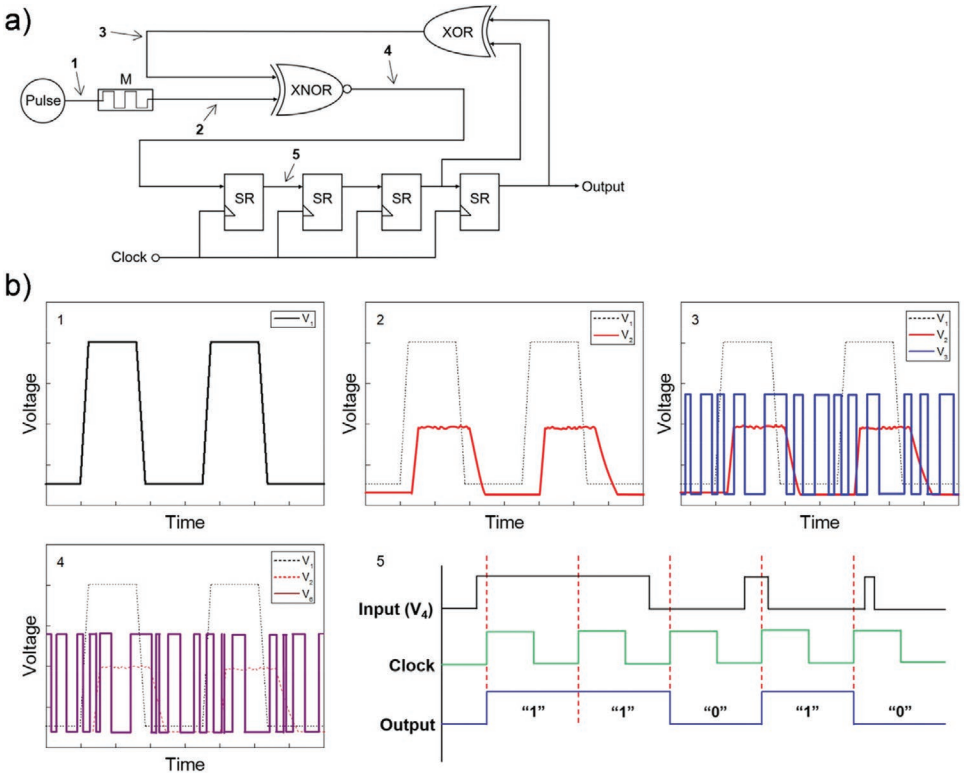


Figure 2. New concept of the TRNG with NFSR. a) Circuit diagram of the new concept consisting of a memristor, an XNOR gate, an XOR gate and four D flip-flops. b) Schematic of the pulse sequences at each step as labeled in (a). No coordinate axes are given since it is the proof of concept.

truly random as it is based on the memristor's stochastic delay and relaxation times, producing random width of V_2. The XOR gate from the tap bits gives feedback (V_3), becoming the input of the next XNOR operation. With the implementation of the XNOR gate, the feedback function is nonlinear. The nonlinear feedback function solves the linear connection problem existing in the LFSR, meeting the demand of unpredictability for secure applications. In addition, Figure S4 in the Supporting Information compares the working principles of LFSR and NFSR. For the pure cycling shift register connection (panel i in Figure S4a, Supporting Information), the output of each shift register is passed to the next one every clock cycle. For example, with a seed value fed in D4, the output of this pure cycling connection will be the repetition of this cycle: (0001) → (0010) → (0100) → (1000) → (0001). The LFSR structure of panel ii in Figure S4a (Supporting Information) has a feedback connection, *f*, formed by the tap. Figure S4b (Supporting Information) shows that with a seed value fed into D4, the output will be the repetition of this turn: (0001) → (0010) → (0100) → (1001) → (0011) → (0110) → (1101) → (1010) → (0101) → (1011) → (0111) → (1111) → (1110) → (1100) → (1000) → (0001). The XOR operation from D1 and D2 results in the feedback value in the fifth row of the table in Figure S4b (Supporting Information), and in the following clock signal, the feedback value goes into D4. The problem of the LFSR is that its simple linear feedback connection is predictable. For the proposed NFSR (panel iii in Figure S4a, Supporting Information), the feedback function is formed not only by the XOR gate, but also the NXOR gate and the logic function from the memristor. The memristor changes the old feedback value (f_{old}) to a new feedback value (f_{new}), depending on its response to the input pulse. For example, assume that the memristor's behavior under a certain pulse stimulus is "0" (TS-off state), "0," "0," "1" (TS-on state), "1," "1," as shown in the table of Figure S4c (Supporting Information). When the memristor stays in the TS-off state, the new feedback value becomes the opposite of the old feedback value. Otherwise, the new feedback value does not change. This inverter-like function comes from the memristor's output and the XNOR gate. The memristor's stochastic behavior destroys the pure dependence of the XOR gate, avoiding foreseeable pattern of the output. The flow chart of Figure S4c (Supporting Information) shows the feedback generation. The input pulse is used to switch the memristor to the TS-on state ("1"), and the output of the memristor can be read as logic "0" or "1." Depending on the logic value from the memristor, the feedback function can be either f_{old} or f_{new}. Furthermore, the XNOR gate can prevent the locked-up state. In the case of all "0" states when the XOR gate is used as a feedback function, the output of D flip-flops will always be "0." With the additional XNOR gate, this locked-up state problem can be solved. To experimentally demonstrate this new concept, a single cycle and two consecutive cycles of the lowest-order bit were monitored, as shown in **Figures 3**a,b, respectively. The input pulse was 10.0 V, and the pulse width was 350 µs with 25 µs leading and trailing times. The random output bits were monitored by an oscilloscope. To fully relax the memristor, a rest time of 600 µs was given before the next input pulse. The bit generation rate was 16 kb s^{-1}, which is the highest rate among the reported volatile-memristor-based TRNGs. The bit generation rate can potentially reach 100 Mb s^{-1} with further optimization, so encryption applications requiring high speed would be possible.[10,12] Increasing the number of D flip-flops is one way to improve the bit generation rate though there will be size and complexity issues in the circuit. In addition to the circuit modification, the bit generation rate can also be increased by device engineering. With the higher switching speed of the memristor, the width of the input pulse can be reduced, and therefore, more bits can be obtained.

The NIST randomness tests were carried out to evaluate the performance of the TRNG. A total of 90 sequences of 10^6 bits were collected for the NIST tests. Tests were considered "passed" if the *P*-value was higher than 0.0001 and the minimum pass rate was secured. The *P*-value is the probability of the degree to which the experimental data supports the null hypothesis when the null hypothesis is true. In this case, the null hypothesis is that the output bits collected from the TRNG are random. The significance level is the probability value that the experimental data reject the null hypothesis. In order to accept the null hypothesis, the *P*-value has to be greater than

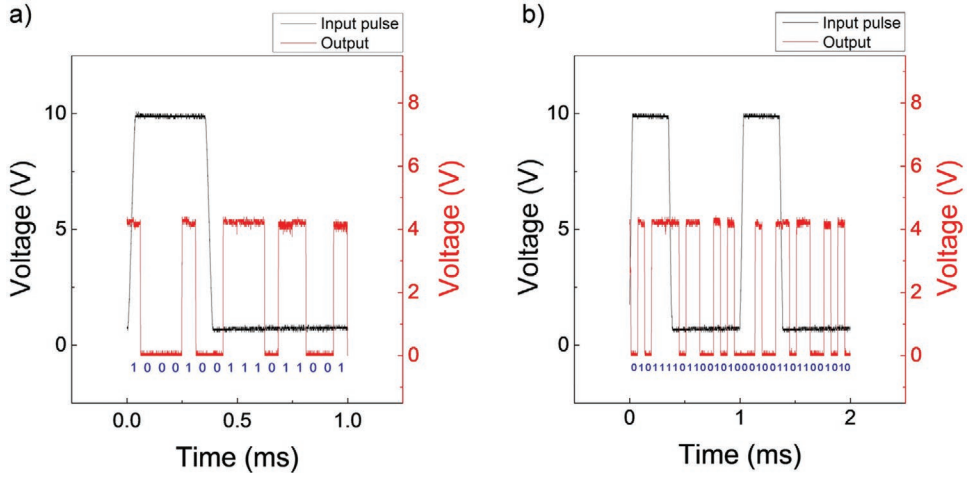


Figure 3. Experimental demonstration of the TRNG with a) a single cycle and b) 2 consecutive cycles.

Table 1. NIST randomness test results.

Test	*P*-value	Pass rate	Minimum pass rate	Pass/fail
1. Frequency Test	0.189397	88/90	86/90	Pass
2. Frequency Test within a Block	0.107371	90/90	86/90	Pass
3. Runs Test	0.911413	90/90	86/90	Pass
4. Test for the Longest Run of Ones in a Block	0.268170	87/90	86/90	Pass
5. Binary Matrix Rank Test	0.000259	87/90	86/90	Pass
6. Discrete Fourier Transform Test	0.407091	88/90	86/90	Pass
7. Non-overlapping Template Matching Test	0.076154	89/90	86/90	Pass
8. Overlapping Template Matching Test	0.002043	90/90	86/90	Pass
9. Maurer's "Universal Statistical" Test	0.238042	86/90	86/90	Pass
10. Linear Complexity Test	0.139036	88/90	86/90	Pass
11. Serial Test	0.050485	89/90	86/90	Pass
	0.100508	86/90		
12. Approximate Entropy Test	0.602458	89/90	86/90	Pass
13. Cumulative Sums Test	0.019334	89/90	86/90	Pass
	0.387648	89/90		
14. Random Excursions Test	0.399443	88/90	86/90	Pass
15. Random Excursions Variant Test	0.042708	89/90	86/90	Pass

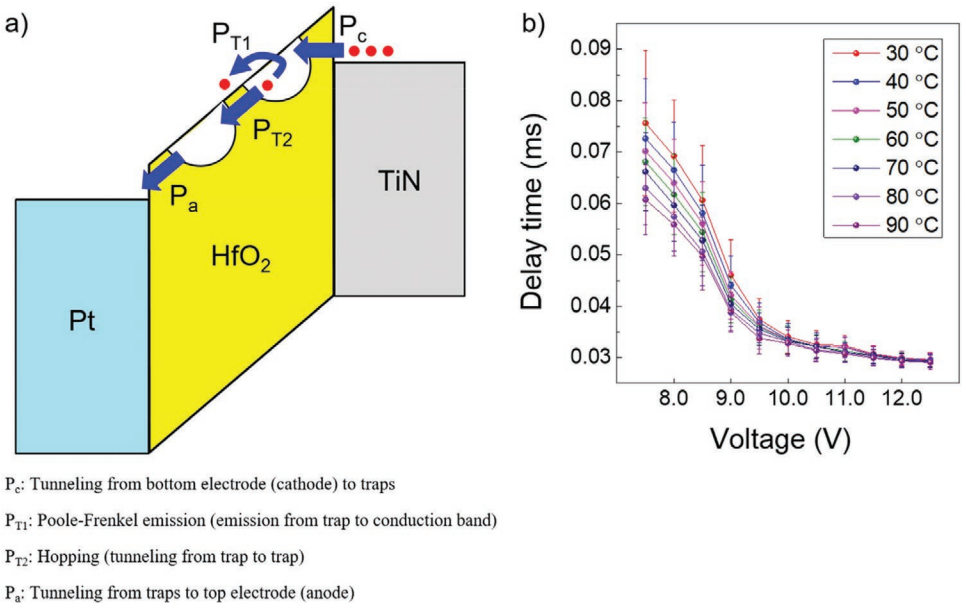
the significance level (0.0001 in this study). **Table 1** shows that all 15 NIST tests were passed without any post-processing step.

The biggest problem of the LFSR is the linear connection, which results in easy cryptanalysis. In contrast, the memristor's random seed and the NFSR's nonlinearity pave the way for random and unpredictable security applications. The input voltage (10.0 V) was set according to the operating voltage specifications of the circuit components. Assuming that the circuit components are not constrained by the operating voltage, a lower input voltage is possible, as this leads to a wider distribution of the delay time (**Figure 4**b), also enabling low power consumption. Increasing the temperature at 10.0 V of input voltage shows almost no difference in the delay time distribution, so this also should not be a problem for TRNG operation. On the other hand, the reliability issue of the device might arise. The performance of the circuit without the memristor was further investigated. In this case, the circuit itself could not pass the NIST tests, as shown in Table S1 in the Supporting Information. The results prove that the memristor-based seed does play a crucial role during the TRNG operation.

As previously reported, the stochasticities of the delay and relaxation times are attributed to the electron trapping processes. Figure 4a illustrates all the possible electron trapping processes. These include 1) P_c: tunneling from bottom electrode (cathode) to traps, 2) P_{T1}: Poole–Frenkel emission (emission from trap to conduction band), 3) P_{T2}: Hopping (tunneling from trap to trap), and 4) P_a: tunneling from traps to top electrode (anode). Among the possible electron trapping processes, P_{T2} is known as the main conduction process as it has the largest transition rate. The transition rate of P_{T2}, $\nu = \nu_0 \exp\left(-\frac{2R}{\xi}\right)$, is much larger than that of P_{T1}, $\nu = \nu_0 \exp\left(-\frac{E_t}{kT}\right)$, where ν_0 is 10^{13} Hz, E_t is the trap energy in the HfO_2 layer (≈0.7 eV), R is the distance between the traps (≈0.3–0.6 nm), and ξ is the electron wavefunction localization length (≈0.3 nm).[25] Therefore, only the hopping process is considered in this experiment for the sake of simplicity. It should be noted that the process with the higher transition rate governs the overall transition rate because the P_{T1} and P_{T2} operate in parallel. Nasyrov and Gritsenko developed a theory of the hopping process under the assumption of a multi-phonon mechanism of trap ionization.[26] Here, the electron traps are represented as oscillators. From this model, the transition rate of the phonon-assisted hopping (PAH) process can be expressed as follows

$$\nu = \frac{\sqrt{\pi}\hbar W_T}{m^* D^2 \sqrt{2kT\left(W_{opt} - W_T\right)}} \exp\left(-\frac{W_{opt} - W_T}{2kT}\right) \exp\left(-\frac{2D\sqrt{2m^* W_T}}{\hbar}\right) \exp\left(-\frac{eED}{2kT}\right) \quad (1)$$

where D is the distance between the electron traps, W_{opt} is the optical trap ionization energy, W_T is the thermal trap ionization energy, and E is the electric field. The first exponential refers to the thermal activation process of for the tunneling. The second exponential is the tunneling factor. The last factor is the barrier lowering from the electric field. This equation indicates that the hopping process is a thermally stimulated process whose activation energy equals half the difference between the optical and thermal ionization energies of the traps. Hence, Figure 4b shows that the variation in the delay time when the temperature and voltage were varied. While the delay time was slightly shortened and its distribution became narrower with higher temperature, increasing the voltage decreased the delay time with less fluctuation. Temperature-dependency was also diminished at higher voltages. These results can be explained by the PAH model. The transition rate of PAH is temperature-dependent, so more tunneling occurs at higher temperature. As more tunneling



P_c: Tunneling from bottom electrode (cathode) to traps

P_{T1}: Poole-Frenkel emission (emission from trap to conduction band)

P_{T2}: Hopping (tunneling from trap to trap)

P_a: Tunneling from traps to top electrode (anode)

Figure 4. Stochastic delay time analysis. a) Band diagram of possible electron trapping processes. b) Distribution of delay time at different temperatures and voltages.

occurs, the delay time can decrease. Moreover, in the process of electron trapping, the instability of the trapping process due to a small trap energy level difference near the Pt and TiN electrodes causes electron detrapping, leading to a severe fluctuation in the delay time. This may be the reason for the stochasticity of the delay time. Higher transition rate at higher temperature means that the speed of the electron trapping is more significant. Thus, the electron detrapping is less influenced, reducing the delay time fluctuation (less stochasticity). At higher voltage, the barrier lowering from the electric field leads to more trapped electrons, decreasing the delay time. The trap level will also move to a level much lower than the Fermi level of TiN, so as the trapped electrons become more stable, the delay time distribution will become narrower (less stochasticity). When the electric field continues to increase, the electron will reach its saturation velocity, and the decrease of the delay time will slow down at high voltage region. Overall, the electron transport based on the PAH model is suitable for describing the stochasticity of the delay time.

In conclusion, a new type of TRNG combined with an NFSR is proposed. The TRNG is based on the intrinsic stochasticity in the electron trapping/detrapping mechanism of the PHT memristor, and the NFSR allows higher bit generation rate for high-speed encryption applications, without costing too much power consumption. The circuit is simple, and the memristor's electronic switching mechanism has advantages in switching speed, power consumption, and reliability. The output bits generated by the TRNG passed all the NIST randomness tests without post-processing step. Lastly, the analysis of delay time confirms that its stochasticity is attributed to the PAH process. With the increasing importance of hardware-based data encryption, this TRNG could be a breakthrough in security technology for the IoT era.

Experimental Section

For the fabrication of the crossbar geometry of the Pt/HfO_2/TiN device, 50 nm thick TiN BE was deposited on a SiO_2/Si substrate using a sputtering system (Endura, Applied Materials), followed by a lift-off process. Then, 10 nm thick HfO_2 film was deposited by thermal atomic layer deposition using $Hf[N(CH_3)(C_2H_5)_4$ and O_3 as Hf precursor and oxygen source, respectively, at a 280 °C substrate temperature. Finally, 50 nm thick Pt film was deposited using an e-beam evaporator (SRN-200, SORONA), followed by the lift-off, making the 8 μm × 8 μm crosspoint structure. The *I–V* characteristics were measured using a semiconductor parameter analyzer (Hewlett-Packard, HP4145B). The pulse was generated using an Agilent 81110A pulse generator. During the measurements, the Pt TE was biased, and the TiN BE was grounded. The estimated parasitic capacitance of the measurement setup was ≈100 pF. When the series resistance of the oscilloscope was set to 1 MΩ, the circuit delay time was ≈0.1 ms. This value is much smaller than the estimated relaxation time from the experiment.

Supporting Information

Supporting Information is available from the Wiley Online Library or from the author.

Acknowledgements

K.S.W. and Y.W. contributed equally to this work. This work was supported by the Future Semiconductor Device Technology Development Program (20003655) through the Ministry of Trade, Industry, & Energy (MOTIE, Korea) [Project Name: Development of self rectifying resistance switching materials and devices for selectorless crossbar application].

Conflict of Interest

The authors declare no conflict of interest.

Keywords

electron trapping, memristors, nonlinear-feedback shift registers, threshold switching, true random number generators

Received: October 12, 2019
Revised: December 13, 2019
Published online:

[1] D. B. Strukov, G. S. Snider, D. R. Stewart, R. S. Williams, *Nature* **2008**, *453*, 80.
[2] R. Waser, R. Dittmann, G. Staikov, K. Szot, *Adv. Mater.* **2009**, *21*, 2632.
[3] C. S. Hwang, *Adv. Electron. Mater.* **2015**, *1*, 140056.
[4] M. T. Arafin,C. Dunbar, G. Qu, N. McDonald, L. Yan, *Proc. IEEE Int. Symp. Quality Electronic Design (ISQED)*, IEEE, Piscataway, NJ **2015**, p. 440.
[5] S. Balatti, S. Ambrogio, Z. Wang, D. Ielmini, *IEEE J. Emerging Sel. Top. Circuits Syst.* **2015**, *5*, 214.
[6] S. Balatti, S. Ambrogio, R. Carboni, V. Milo, Z. Wang, A. Calderoni, N. Ramaswamy, D. Ielmini, *IEEE Trans. Electron Devices* **2016**, *63*, 2029.
[7] T. Zhang, M. Yin, C. Xu, X. Lu, X. Sun, Y. Yang, R. Huang, *Nanotechnology* **2017**, *28*, 455202.
[8] R. Zhang, H. Jiang, Z. R. Wang, P. Lin, Y. Zhuo, D. Holcomb, D. H. Zhang, J. J. Yang, Q. Xia, *Nanoscale* **2018**, *10*, 2721.
[9] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, NIST Special Publication 800-822, **2010**.
[10] 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, Q. Xia, *Nat. Commun.* **2017**, *8*, 882.
[11] K. S. Woo, Y. Wang, J. Kim, Y. Kim, Y. J. Kwon, J. H. Yoon, W. Kim, C. S. Hwang, *Adv. Electron. Mater.* **2019**, *5*, 1800543.
[12] C. Y. Huang, W. C. Shen, Y. H. Tseng, Y.-C. King, C. J. Lin, *IEEE Electron Device Lett.* **2012**, *33*, 1108.
[13] N. Liu, N. Pinckney, S. Hanson, D. Sylvester, D. Blaauw, presented at *Symposium on VLSI Circuits*, Kyoto, Japan, June **2011**.
[14] A. Klein, *Stream Ciphers*, Springer-Verlag, London, UK **2013**.
[15] A. Poorghanad, A. Sadr, A. Kashanipour, presented at *International Conference on Computational Intelligence and Security*, Suzhou, China, December **2008**.
[16] R. Dube, *Hardware-Based Computer Security Techniques to Defeat Hackers: From Biometrics to Quantum Cryptography*, John Wiley & Sons, Hoboken, NJ **2008**.
[17] Y. Khan, *Int. J. Engin. Res. Dev.* **2013**, *7*, 109.
[18] E. Dubrova, M. Teslenko, H. Tenhunen, presented at *Design, Automation, and Test in Europe*, Munich, Germany, March **2008**.
[19] K. Zeng, C.-H. Yang, D.-Y. Wei, T. R. N. Rao, *Computer* **1991**, *24*, 8.
[20] J. H. Yoon, K. M. Kim, S. J. Song, J. Y. Seok, K. J. Yoon, D. E. Kwon, T. H. Park, Y. J. Kwon, X. Shao, C. S. Hwang, *Adv. Mater.* **2015**, *27*, 3811.
[21] K. M. Kim, G. H. Kim, S. J. Song, J. Y. Seok, M. H. Lee, J. H. Yoon, C. S. Hwang, *Nanotechnology* **2010**, *21*, 305203.
[22] K. M. Kim, B. J. Choi, M. H. Lee, G. H. Kim, S. J. Song, J. Y. Seok, J. H. Yoon, S. Han, C. S. Hwang, *Nanotechnology* **2011**, *22*, 254010.
[23] J. J. Yang, D. B. Strukov, D. R. Stewart, *Nat. Nanotechnol.* **2013**, *8*, 13.
[24] Y. Kim, Y. J. Kwon, D. E. Kwon, K. J. Yoon, J. H. Yoon, S. Yoo, H. J. Kim, T. H. Park, J. W. Han, K. M. Kim, C. S. Hwang, *Adv. Mater.* **2018**, *30*, 1704320.
[25] S. Yu, X. Guan, H.-S. P. Wong, *Appl. Phys. Lett.* **2011**, *99*, 063507.
[26] K. A. Nasyrov, V. A. Gritsenko, *J. Appl. Phys.* **2011**, *109*, 093705.

