Self-clocking fast and variation tolerant true random number generator based on a stochastic mott memristor

Gwangmin Kim
Korea Advanced Institute of Science and Technology
Jae Hyun In
Korea Advanced Institute of Science and Technology
Hakseung Rhee
Korea Advanced Institute of Science and Technology
Woojoon Park
Korea Advanced Institute of Science and Technology
Hanchan Song
Korea Advanced Institute of Science and Technology
Kyung Min Kim (km.kim@kaist.ac.kr)
Korea Advanced Institute of Science and Technology

Article

Keywords: Non-decryptable Hardware-based Security Devices, Stochastic Oscillation Behavior, TRNG Devices, Dimensionless Operating Principles

Posted Date: December 7th, 2020

DOI: https://doi.org/10.21203/rs.3.rs-118145/v1

Version of Record: A version of this preprint was published at Nature Communications on May 18th, 2021. See the published version at https://doi.org/10.1038/s41467-021-23184-y.

Self-clocking fast and variation tolerant true random number generator based on a stochastic mott memristor

Gwangmin Kim, Jae Hyun In, Hakseung Rhee, Woojoon Park, Hanchan Song and Kyung Min Kim*

Department of Materials Science and Engineering, Korea Advanced Institute of Science and Technology (KAIST)
291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea

G. Kim and J. H. In contributed equally to this work.
*Correspondence and requests for materials should be addressed to K.M.K. (email: km.kim@kaist.ac.kr).

The intrinsic stochasticity of the memristor can be used to generate true random numbers, essential for non-decryptable hardware-based security devices. Here we propose a novel and advanced method to generate true random numbers utilizing the stochastic oscillation behavior of a NbO_x mott memristor, exhibiting self-clocking, fast and variation tolerant characteristics. The random number generation rate of the device can be at least 40 kbs^{-1}, which is the fastest record compared with previous volatile memristor-based TRNG devices. Also, its dimensionless operating principle provides high tolerance against both ambient temperature variation and device-to-device variation, enabling robust security hardware applicable in harsh environments.

In future electronics, as the internet of things (IoT) expands the reach of technologies, chip authentication for secure communication will be increasingly important[1]. Accordingly, developing a hardware-based true random number generator (TRNG) is crucial, since it is intrinsically non-decryptable, unlike the software-based TRNG. For better security, researchers have proposed novel methods for realizing a TRNG, utilizing the stochastic switching phenomena in memristors[2-8]. The early TRNGs utilized the stochastic characteristics in the switching voltages or the programmed states of the non-volatile memristors. Although the proposed methods were viable, they commonly relied on stochastic variation in relation to reference values, which can be vulnerable if the reference value changes over time or over cycling.

To overcome the problem, H. Jiang et al. proposed a volatile memristor-based TRNG [6]. They observed the stochasticity in the switching delay in the Ag:SiO_2-based diffusive memristor and designed a novel circuit which converted the stochasticity to randomness by introducing a clock and counter. The device counted the number of clocks after the stochastic turn-on switching and digitalized it. This method suggested a way to generate dimensionless values that required no reference value to define the randomness. Afterward, K. S. Woo et al. introduced a nonlinear feedback shift register (NFSG) with a HfO_2-based volatile memristor to further increase the TRNG rate. The NFSG can increase the bit size proportional to the number (n) attached to the device, making the rate n times faster. However, in both methods, the switching delay time was intrinsically long, several hundreds of μs, preventing fast TRNG operation. Also, they required an exterior clocking circuit, which can be difficult to integrate.

In this study, we propose a novel TRNG device utilizing the oscillating behavior of a mott memristor. We identified the origin of the randomness to be thermal fluctuations during oscillation, using a numerical simulation and a thermodynamic simulation. The oscillation speed is fast, [9] allowing the fastest random bit generation rate of 40 kb s^{-1} at least. Also, it has

an inherent self-clocking capability, so that no external clocking circuit is needed. From the integrated device, we collected 130 millions random bits and they passed all of the NIST random number tests successfully. Furthermore, we confirmed that the device worked well under a wide range of ambient temperatures, ranging from 300 K to 390 K, and in different characteristic devices, suggesting the high tolerance of the TRNG system.

Stochastic oscillation of NbO_x threshold switching device

Figure 1a shows a top view optical microscopy image of a 5 μm × 5 μm cross-point NbO_x-based threshold switching (TS) device. The inset shows the device stack. The detailed device fabrication process can be found in the Methods section. **Figure 1b** shows the current-controlled negative differential resistance (NDR) characteristic of the device. An electroforming process was preceded by applying -5 V with a 5 mA of compliance current to the top Pt electrode. The device has two distinct NDR regions, at a low current ranging from 50 μA to 100 μA, and at a high current ranging from 400 μA to 550 μA. We designated them NDR-1 and NDR-2, respectively. Both NDRs are well understood as thermally-activated transport and mott transition, respectively[10-16]. NDR-1 is attributed to the thermally-activated transport mechanism; as the current increases, the device temperature increases by Joule-heating, and this activates the carrier injection, leading to the current increase. Such positive feedback of carrier generation and Joule heating drastically reduces the device resistance to the NDR-1. When the temperature reaches around 1070 K at the higher current, mott transition occurs, producing the box-shaped NDR-2[12-14,17]. The inset in Fig. 1b shows the voltage-controlled threshold switching characteristic of the device, with a compliance current ranging from 0.1 mA to 1 mA for reference.

When a constant voltage is applied with a proper series resistor, the NbO_x TS device can exhibit oscillating current behavior [12,18-21]. **Figure 1c** shows a set-up to test the oscillation characteristic of the device. In this configuration, when the applied bias exceeded the threshold voltage (V_{th}) of the device, the device turned on, and the device's potential decreased due to the voltage divider effect between the resistor and the on state of the device. Then, the TS device turned-off spontaneously, resulting in the oscillation.

During the oscillation, the capacitive components in the device influence the frequency of the oscillation by inducing an RC delay. **Figure 1d** shows current oscillation waves generated from the circuit. The pulse amplitude and width were 1.65 V and 34 μs, respectively, with a 1.8 μs of pulse rising and falling time. The load resistance was 2 kΩ. This included 20 waves, which were consecutively collected under the same conditions. The bottom left inset in Fig. 1d shows that all waves overlapped with a little variation at the beginning of the oscillation. However, as the stochastic oscillation repeated, as shown in the bottom right inset in Fig. 1d, their variation became irregular due to the accumulation of the variation, making the oscillation hard to predict.

Figure 1e shows the distribution of peak intervals (t_{intv}) during the oscillations collected from 100 waves. The first and last distributions are shown as red and blue curves representatively, while others are in gray. The inset plots the average time of intervals and its standard deviation at each wave. It shows that both the average and deviation were fluctuating inconsistently, which is regarded as a completely random process.

Thermal fluctuation induced stochastic oscillation modeling

We conducted a numerical simulation to confirm the influence of the random thermal fluctuation on the stochastic oscillation. Because the threshold switching originates from a thermally-activated transport mechanism, we adopted a 3D-modified Poole-Frenkel transport

model to emulate the threshold switching characteristic of the device[11-14]. The following equation describes the model.

$$i_m = AV_m\left[\sigma_0 e^{-\frac{E_a}{k_bT}}\left\{\left(\frac{k_bT}{\beta}\right)^2\left(1+\left(\frac{\beta\sqrt{V_m/d}}{k_bT}-1\right)e^{\frac{\beta\sqrt{V_m/d}}{k_bT}}\right)+\frac{1}{2d}\right\}\right] \quad (1)$$

, where k_b is the Boltzmann constant, d and A are the thickness and area of the switching region, respectively. The σ_0, β, and E_a are material constants[11,22]. To represent the mott transition, we introduced an abrupt change in thermal resistance from 1.8×10^6 KW^{-1} to 2.1×10^6 KW^{-1} at 1070 K, the mott transition temperature of NbO_2. Considering the thermodynamics, we adopted Newton's cooling law with a harmonic thermal fluctuation, as follows[12].

$$\frac{dT}{dt} = \frac{i_{\mathrm{m}}v_{\mathrm{m}}}{C_{\mathrm{th}}} - \frac{T-T_{\mathrm{amb}}}{C_{\mathrm{th}}R_{\mathrm{th}}} + T\left(\frac{k_{\mathrm{b}}}{C_{\mathrm{th}}}\right)^{\frac{1}{2}}\frac{4\pi}{R_{\mathrm{th}}C_{\mathrm{th}}}\cos\frac{2\pi t}{R_{\mathrm{th}}C_{\mathrm{th}}} \quad (2)$$

, where T_{amb} is an ambient temperature, C_{th} and R_{th} are thermal capacitance and resistance respectively, and t is a variable time constant describing the time variation in heat generation and dissipation. Here, we set the t as a random variable to mimic the random thermal fluctuation.

Figure 2a shows the experimental and simulated current – voltage curves. Although there is some mismatch in the NDR-1 region, the model reproduced the experimental data quite well.

Then, the oscillation behavior of the oscillator circuit in Fig 1c was numerically calculated under the same conditions as the experiments. **Figure 2b** shows 20 simulated oscillation waves obtained by the calculation, reproducing the experimental oscillation data in Fig. 1d very well. **Figure 2c** shows the distribution of peak intervals in the simulated oscillation, which also reproduced the experimental results in Fig. 1e. The accurate simulation results confirm that the origin of the randomness is the thermal fluctuation.

Next, we conducted a finite element method (FEM)-based heat simulation to further understand the influence of thermal fluctuations on the stochastic oscillation, using the Field

Triggered Thermal Runaway (FTTR) model in COMSOL[22]. **Figure 2d** shows the device geometry used in the simulation, referring to the device stack in Fig. 1a. Inside the device, we assumed a filamentary Nb_2O_{5-x} region connected to a NbO_2 in series at a Ti-NbO_x interface[22]. To mimic the oscillation, a sinusoidal voltage wave (0.4 Mhz, 0.67 V – 1.07 V) was applied to the top Pt electrode. **Figure 2e** shows the 20 consecutive switching curves under the sinusoidal voltage wave application. From point ① to ②, heat was generated in the NbO_2. Then, the heat ran away along the Nb_2O_{5-x} filament while accelerating the thermally-activated conduction in the NbO_2 until point ③. Afterward, from point ③ to ④, the heat dissipated, and the device returned to point ①. **Figure 2f** shows the temperatures at point ② (red) and point ④ (blue) for each simulation cycle. The variation in switching temperature confirms that the residual heat was not a fixed value during the device oscillation. More detailed thermodynamic simulation results can be found in **Supplementary Fig. S1**.

A self-clocking TRNG device

The origin of the stochastic oscillation is the random thermal fluctuation. To extract the randomness from it, we developed a novel TRNG circuit embodying a self-clocking capability. **Figure 3a** shows the TRNG circuit, including an operational amplifier (op-amp), a JK flip-flop, and three external resistors. The JK flip-flop is functionally equal to a T flip-flop when the J and K terminals are biased to 'High' (or '1'). The 50 Ω of resistor represents the oscilloscope's internal resistance.

Figures 3b-e show the monitoring signal at nodes 1-4 in Fig. 3a obtained by a PSPICE simulation. **Figure 3b** shows the input voltage pulse at node 1 and the stochastic oscillation current at node 2, which are identical with the oscillation data in Fig. 1e. **Figure 3c** displays the currents at node 2 and node 3. The op-amp amplifies the input signal to trigger the

subsequent flip-flop properly. **Figure 3d** shows the output signal at node 4 with the clocking signal at node 3. At every pulse falling moment per clocking, the flip-flop toggles its bit data. Therefore, depending on whether the number of clocks at a given period are either odd or even, the bit data can be either 1 or 0, respectively. **Figure 3e** shows the input voltage pulse and the output signal from the device for generating one random bit. In the given period, the number of oscillation pulses is stochastically variable, but their probability of odd or even can be random, which allows true random number generation.

Experimental demonstration of the TRNG

Figure 4a schematically shows the TRNG configuration. The Keithley 4200A-SCS applied an input voltage pulse to the breadboard and received the output signal from it. **Figure 4b** shows the TRNG integrated on the breadboard where the op-amp, flip-flop, and the resistors are shown (left panel). The right panel shows the corresponding circuit diagram. The non-inverting amplifier consisted of 1 kΩ R_s, 200 Ω R_f, and the op-amp (Model: NE5534D of Texas Instruments). The V+ terminal of the op-amp was connected to a 9 V battery and the V- terminal was grounded. The DC power supply was used to apply 2.5 V to the inputs J, K, ($\overline{CLR}$), and V_{CC} terminals of the flip-flop (Model: SN74LS73AN of Texas Instruments). The NbO_x TS device was loaded in the probe station and connected to the breadboard via cables.

Figure 4c shows the monitored input and output signals for 5 random bit generation cycling. The black, red, and green lines represent the input voltage pulse, the oscillation current of the device, and the output current, respectively. The input pulse amplitude and width were 1.1 V and 20 μs, respectively, with an 1 μs of pulse rising and falling time. The video recorded TRNG operation can be found in the **Supplementary Video.**

Figure 4d plots a P-value of the monobit test as a function of the input pulse period. Here, 100 random bits were used for the evaluation. The P-value can be obtained by following equation.

$$P\text{-}value = erfc(\sum_{i=1}^{n} \frac{|2\varepsilon_i - 1|}{\sqrt{2n}}) \quad (3)$$

, where n and ε_i are the length of the bit string and the datum of i^{th} bit in the bit string, respectively. The monobit test is the first test among the 15 tests in NIST (National Institute of Standards and Technology) random number test suite (NIST 800-22)[23] checking whether the fraction of ones in the given random bits is close to 1/2 or not. It is the essential test because other tests would fail if the monobit test fails[23]. The P-value is an indicator showing the randomness of the dataset; when the value is higher, the dataset is more random. In general, if the P-value exceeds 0.01, the dataset can be regarded as true random numbers.

When the time was short, the accumulation of thermal fluctuations was not sufficient, resulting in a low P-value. When the time was longer than ~10 μs, the P-value exceeded 0.01 continuously, guaranteeing that the output is a random number. This gives a random bit generation rate of 100 kbs^{-1}, which is the fastest record, compared with previous TS device-based TRNGs[4,6,8].

We collected 130 sets of one Mbits (total 130 Mb) from the device using a 25 μs pulse (equivalent to 40 kbs^{-1}) for NIST testing. **Table 1** shows the testing results. The dataset passed all 15 NIST randomness tests successfully.

Variation tolerance of the self-clocking TRNG device

The proposed TRNG device utilizes the accumulation of thermal fluctuations as the randomness source. Actually, the amount of thermal fluctuations is time-variable and predictable, so that it cannot be random. However, by binarizing the thermal fluctuation and

taking the remainder, the time-variant dimension can be eliminated, and a random output can be achieved (see **Supplementary Fig. S2** for more discussion). This suggests that the device can be tolerant against any physical variation influencing the time-variable. Based on this observation, we further investigated the influence of two representative variations on device performance: a temperature variation and a device-to-device inherent performance variation.

Figure 5a shows the current controlled NDR curves measured at different ambient temperatures ranging from 300 K to 390 K. Both the V_{th} and V_h decrease as the temperature increases, which is consistent with the previous report[24]. **Figure 5b** shows the oscillation waves at each temperature. Under the same input voltage and load resistance conditions, the oscillation frequency increased due to the decrease in V_{th} and V_h with increasing ambient temperature.

Figure 5c shows the P-value of the NIST monobit test as a function of the pulse time at different temperatures. The inset summarizes the required time (t_{TRNG}) for the P-value to exceed 0.01, indicating a true random number, as a function of temperature. The TRNG worked well regardless of the ambient temperature. Moreover, as the ambient temperature increased, the random number generation speed became faster; at 300 K, the P-value exceeded 0.01 after 21.5 μs, giving a 46 kbs^{-1} rate, while at 380 K, it was 15 μs, giving 66 kbs^{-1}. According to Eq. 2, the thermal fluctuation amplitude becomes higher with increasing ambient temperature. Therefore, the thermal fluctuation is more active at a higher temperature, resulting in a faster random number generation speed.

Figure 5d shows the current controlled NDR curves from five distinct devices, where they were intentionally manipulated for comparison. The load line by the R_L of 3 kΩ is included, suggesting all devices will oscillate at the given R_L. **Figure 5e** shows the oscillation waves from the devices under identical voltage pulse conditions. Despite the different oscillation frequencies, all of the devices generated true random numbers successfully.

Figure 5f shows the P-value of the NIST monobit test as a function of the pulse time for the different devices depicted in Fig. 5d. The inset plots the t_{TRNG} of each device. Interestingly, the frequency of the oscillation was not directly correlated with the t_{TRNG}, while the amplitude of the thermal fluctuation was closely correlated with the t_{TRNG}. The results suggest that the thermal fluctuation is proportional to the maximum temperature, but not to the temperature change. Therefore, as long as the TS devices oscillate, TRNG operation is possible, meaning the device is intrinsically variation tolerant.

In conclusion, we proposed a fast and highly tolerant TRNG device utilizing the stochastic self-oscillation behavior of the NbO_x TS device. We found intrinsic stochasticity in the thermal fluctuation during the oscillation, and confirmed it by numerical and thermodynamic simulations. We developed a self-clocking TRNG circuit, extracting the random components by binarizing the thermal fluctuation, and successfully demonstrated the device operation by experiment. We collected 130 Mbits from the integrated device and confirmed that they passed all the NIST 800-22 random number tests. Also, we proved the variation tolerant characteristics of the device at various ambient temperatures and at various manipulated cells.

The proposed method utilizes a dimensionless quantity to generate the random number. Thus, as long as the device oscillates, the device can work, making the practical device application highly viable. Such high device reliability means it can be applied in various harsh environments in future electronics, wherever security is needed.

Methods

Device fabrication. A Pt/Ti/NbO_x/Pt device was fabricated using the following procedure. An adhesive 2-nm Ti followed by a 25-nm Pt bottom electrode were deposited by e-beam

evaporation and patterned by a lift-off process on a SiO_2/Si substrate. Then, a 40-nm NbO_x layer was deposited by a reactive sputtering process at 170 ºC in Ar:O_2 (13:7, 4 mtorr) mixed gas ambient using Nb target. Then, a 50-nm Ti top electrode followed by a 15-nm Pt contact electrode were deposited by e-beam evaporation and patterned by a lift-off process.

Electrical characterization. In the TRNG circuit, a DC voltage was generated using EXO K-6135 power supply and 9 V battery. Also, the circuit components SN74LS73AN for JK flip-flop and NE55322P for op-amp made by Texas Instruments were used. All electrical characterization was performed using Keithley 4200A-SCS.

Circuit simulation and NIST test. The circuit simulation was executed by PSPICE. In PSPICE simulation, a model of u741 for amplifier and 7476 for JK flip-flop were used. The randomness test code was built in the Python environment, referring to the NIST Statistical Test Suite (Special Publication 800-22).'.

Received:
Published online:

References

1 Carboni, R. & Ielmini, D. Stochastic Memory Devices for Security and Computing. *Advanced Electronic Materials* **5**, 1900198 (2019).

2 Huang, C.-Y., Shen, W. C., Tseng, Y.-H., King, Y.-C. & Lin, C.-J. A Contact-Resistive Random-Access-Memory-Based True Random Number Generator. *IEEE Electron Device Letters* **33**, 1108-1110 (2012).

3 Balatti, S., Ambrogio, S., Wang, Z. & Ielmini, D. True Random Number Generation by Variability of Resistive Switching in Oxide-Based Devices. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* **5**, 214-221, (2015).

4 Balatti, S. *et al.* Physical Unbiased Generation of Random Numbers With Coupled Resistive Switching Devices. *IEEE Transactions on Electron Devices* **63**, 2029-2035, (2016).

5 Wei, Z. *et al.*, *IEEE International Electron Devices Meeting (IEDM),* 4.8.1-4.8.4. (2016).

6 Jiang, H. *et al.* A novel true random number generator based on a stochastic diffusive memristor. *Nat Commun* **8**, 882 (2017).

7 Woo, K. S. *et al.* A True Random Number Generator Using Threshold-Switching-Based Memristors in an Efficient Circuit Design. *Advanced Electronic Materials* **5**, 1800543 (2019).

8 Woo, K. S. *et al.* A Combination of a Volatile‐Memristor‐Based True Random‐Number Generator and a Nonlinear‐Feedback Shift Register for High‐Speed Encryption. *Advanced Electronic Materials* **6**, 1901117 (2020).

9 Pickett, M. D. & Williams, R. S. Sub-100 fJ and sub-nanosecond thermally driven threshold switching in niobium oxide crosspoint nanodevices. *Nanotechnology* **23**, 215202 (2012).

10 Gibson, G. A. Designing Negative Differential Resistance Devices Based on Self-Heating. *Advanced Functional Materials* **28**, 1704175 (2018).

11 Gibson, G. A. *et al.* An accurate locally active memristor model for S-type negative differential resistance in NbOx. *Applied Physics Letters* **108**, 023505 (2016).

12 Kumar, S., Strachan, J. P. & Williams, R. S. Chaotic dynamics in nanoscale NbO2 Mott memristors for analogue computing. *Nature* **548**, 318-321 (2017).

13 Kumar, S. *et al.* Physical origins of current and temperature controlled negative differential resistances in NbO2. *Nat Commun* **8**, 658, (2017).

14 Kumar, S. & Williams, R. S. Separation of current density and electric field domains caused by nonlinear electronic instabilities. *Nat Commun* **9**, 2030, (2018).

15 Li, S., Liu, X., Nandi, S. K. & Elliman, R. G. Anatomy of filamentary threshold switching in amorphous niobium oxide. *Nanotechnology* **29**, 375705 (2018).

16 Wang, Z., Kumar, S., Nishi, Y. & Wong, H. S. P. Transient dynamics of NbOx threshold switches explained by Poole-Frenkel based thermal feedback mechanism. *Applied Physics Letters* **112**, 193503 (2018).

17 Zhang, J. *et al.* Thermally induced crystallization in NbO2 thin films. *Sci Rep* **6**, 34294 (2016).

18 Pickett, M. D., Medeiros-Ribeiro, G. & Williams, R. S. A scalable neuristor built with Mott memristors. *Nat Mater* **12**, 114-117 (2013).

19 Liu, X., Li, S., Nandi, S. K., Venkatachalam, D. K. & Elliman, R. G. Threshold switching and electrical self-oscillation in niobium oxide films. *Journal of Applied Physics* **120**, 124102 (2016).

20 Li, S., Liu, X., Nandi, S. K., Venkatachalam, D. K. & Elliman, R. G. Coupling dynamics of Nb/Nb2O5 relaxation oscillators. *Nanotechnology* **28**, 125201 (2017).
21 Zhang, X. *et al.* An artificial spiking afferent nerve based on Mott memristors for neurorobotics. *Nat Commun* **11**, 51 (2020).
22 Funck, C. *et al.* Multidimensional Simulation of Threshold Switching in NbO2Based on an Electric Field Triggered Thermal Runaway Model. *Advanced Electronic Materials* **2**, 1600169 (2016).
23 Rukhin A., S. J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Heckert A., Dray J., Vo S. *NIST Special Publication 800-22* (2010).
24 Nandi, S. K., Li, S., Liu, X. & Elliman, R. G. Temperature dependent frequency tuning of NbOx relaxation oscillators. *Applied Physics Letters* **111**, 202901 (2017).

Acknowledgements

This research was supported by the MOTIE (Ministry of Trade, Industry & Energy) (Grant numbers 20003655 and 20003789) and KSRC (Korea Semiconductor Research Consortium) support program for the development of the future semiconductor device; and 2020 UP Research Project of KAIST.

Author contributions

G. Kim and J. H. In contributed equally to this work. G. Kim, and J. H. In conceived the idea, performed the experiments, and wrote the manuscript. H. Rhee, W. Park, and H. Song helped with data analysis and discussed the results. K. M. Kim supervised this study.

Additional information

Competing interests: The authors declare no competing financial interests.

Tables

Table 1. The NIST test (800-22 test suite) results of the NbO_x-based TRNG

Statistical test	P-value	Proportion	Result
1. Frequency (monobit) test	0.010751	1.0000	PASS
2. Frequency test within a block	0.451595	0.9846	PASS
3. Runs test	0.082824	0.9923	PASS
4. Test for the longest run of ones in a block	0.066882	1.0000	PASS
5. Binary matrix rank test	0.046361	1.0000	PASS
6. Discrete Fourier transform (spectral test)	0.001173	0.9846	PASS
7. Non-overlapping template matching test	0.095249	0.9846	PASS
8. Overlapping template matching test	0.125088	1.0000	PASS
9. Maurer's "universal statistical" test	0.017912	1.0000	PASS
10. Linear complexity test	0.020984	1.0000	PASS
11. Serial test	0.217681	1.0000	PASS
12. Approximate entropy test	0.001106	0.9846	PASS
13. Cumulative sums (cusum) test	0.003951	0.9769	PASS
14. Random excursions test	0.009640	1.0000	PASS
15. Random excursions variant test	0.001527	1.0000	PASS

Figures

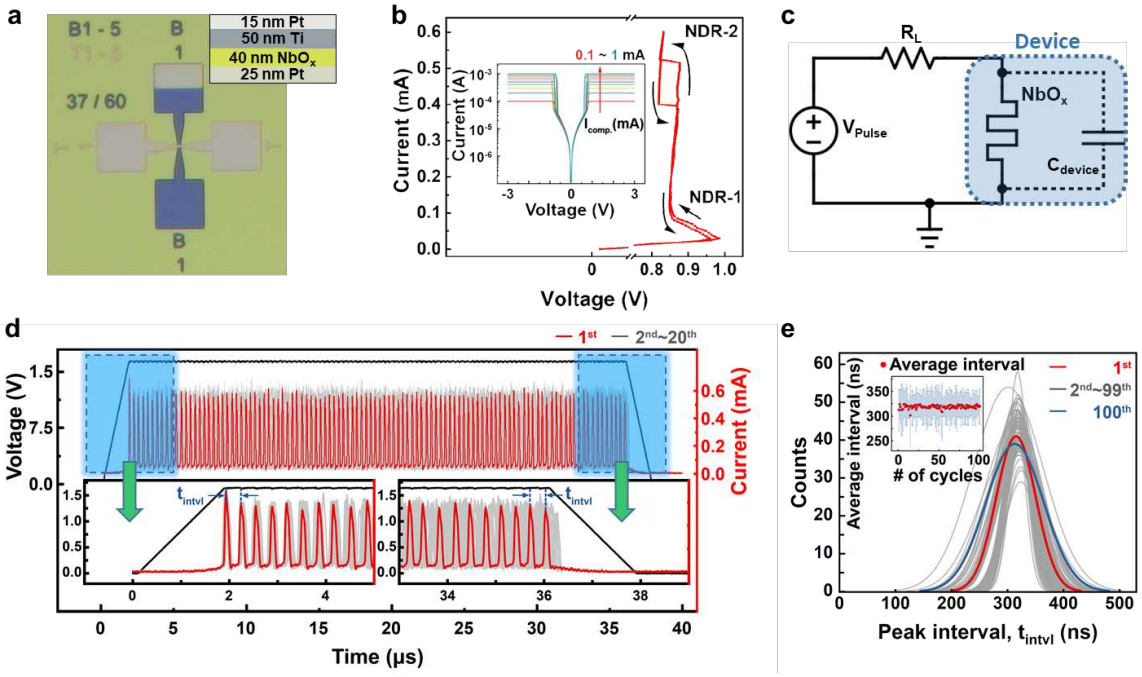

Figure 1 | Electrical properties of NbO_x-based threshold switching (TS) device, and its stochastic oscillation. a, An optical microscope image of the NbO_x-based two terminal device. The inset shows the stack of the device. **b,** A representative I – V curve with a current sweep mode showing two negative differential resistance behaviors, noted to NDR-1 and NDR-2. The inset shows I -V curves in a voltage sweep mode with compliance currents ranging from 0.1 mA to 1 mA. **c,** An oscillator circuit composed of the device and a series resistor. The TS device composed of a volatile memristor and an internal capacitor. **d,** Experimentally obtained 20 oscillation current outputs under a fixed input voltage pulse. The left and right insets magnify the initial and final oscillation outputs, respectively. **e,** A distribution of peak intervals ($\mathbf{t_{intvl}}$) at each oscillation output. It shows 100 distributions collected from 100 testing cycles. Inset shows the average and standard deviation of the t_{intvl} for 100 testing cycles.

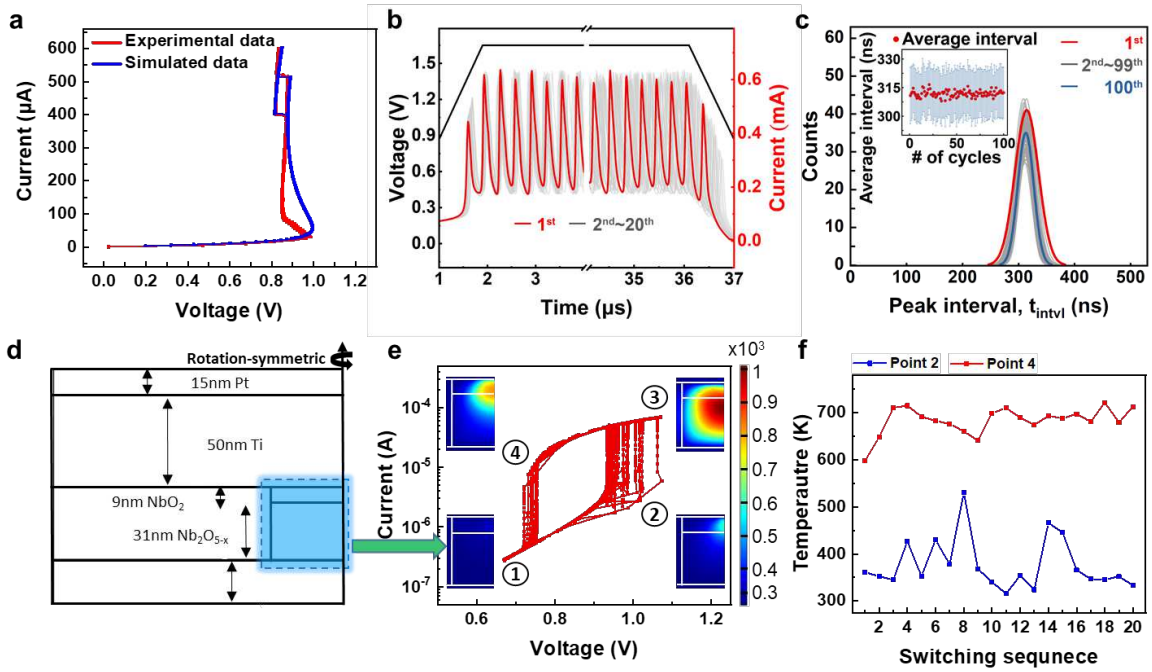

Figure 2 | Simulations of stochastic oscillation characteristic induced by thermal fluctuation. a, A numerically simulated I – V curve (blue) compared with an experimental one (red line). **b,** Simulated 20 oscillation currents under a fixed voltage input. The oscillation outputs overlap well at the beginning, but they disperse at the end. **c,** Simulated distributions of the peak intervals for 100 cycles. Inset shows an average and a standard deviation of intervals. The results reproduce the experimental results in Fig. 1e. **d,** A geometry used for a thermodynamic simulation, which is identical with the fabricated device in Fig. 1a. **e,** Simulated I – V curves from the thermodynamic simulation under a sinusoidal input voltage. The insets show heat distribution at each moment. **f,** The maximum temperatures at the moment of switch on (②, blue) and switch off (④, red) for 20 cycles of simulation, showing they fluctuate.

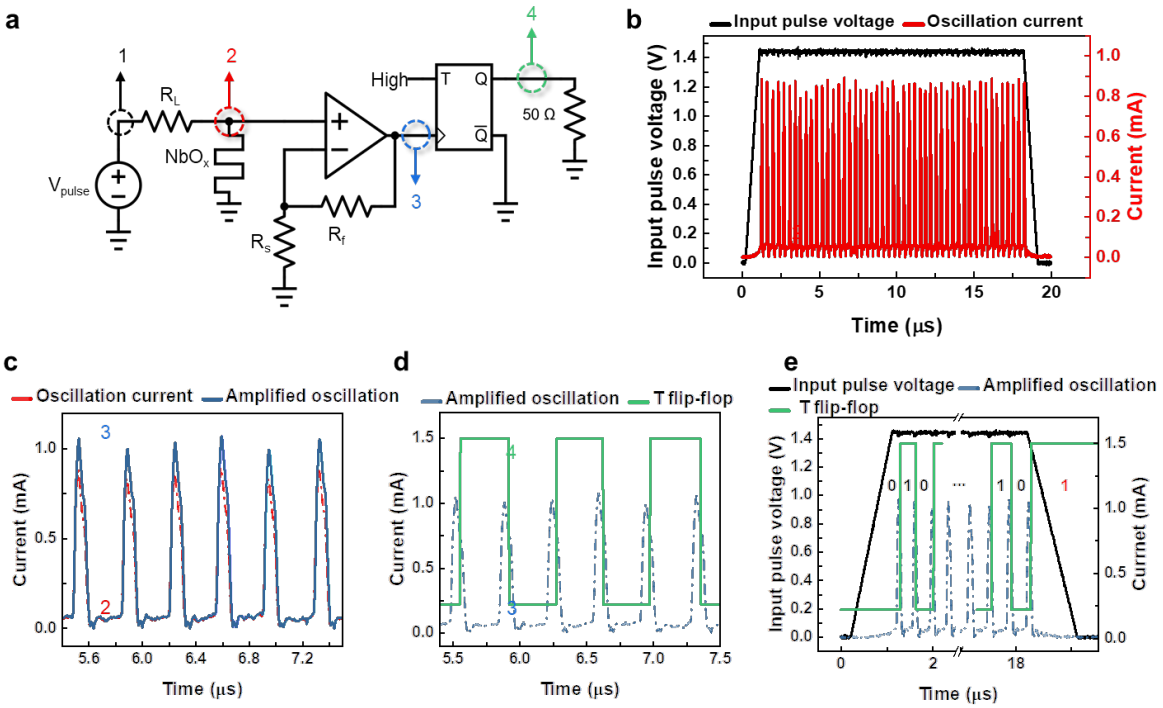

Figure 3 | A TRNG circuit and its simulation. a, The proposed TRNG circuit composed of an op-amp, a T flip-flop, and three resistors. **b,** An input voltage pulse (black) and an output current (red) at node 2 in **a. c,** An amplified oscillation current at node 3 (blue) compared with the output current (red). **d,** An output signal at node 4 (green) after the amplified oscillation current passed the T flip-flop. **e,** A random bit is generated according to the final state of the T flip-flop when the input pulse finishes.

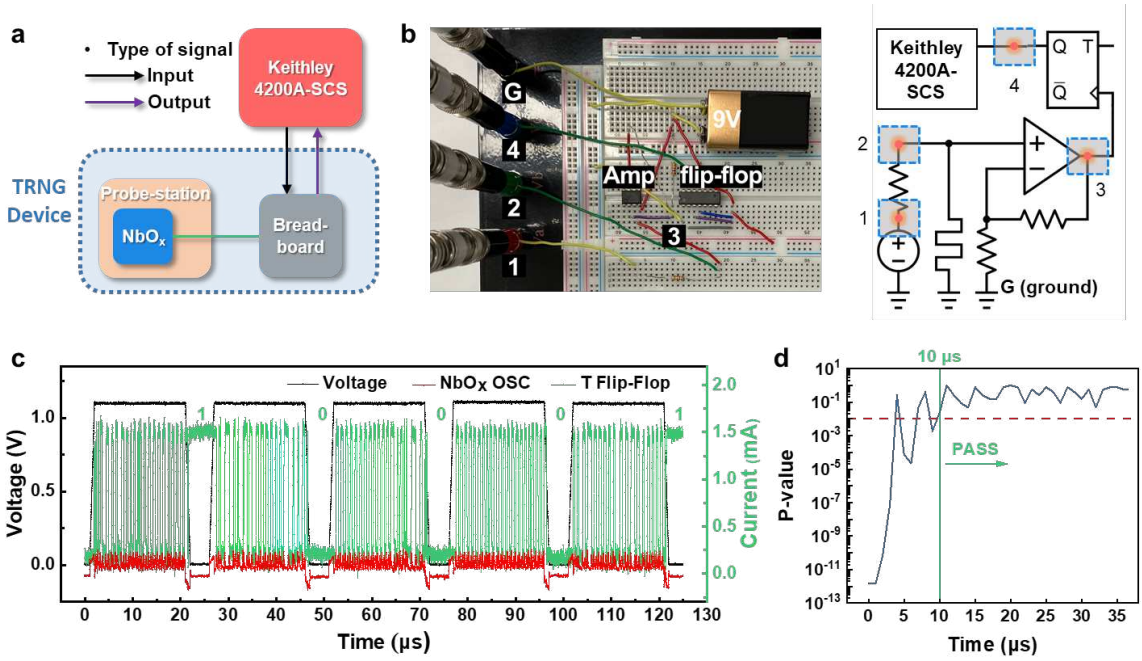

Figure 4 | Experimental demonstration of the TRNG. a, An operating scheme of the proposed TRNG in experiments. **b,** A photograph of the circuit built on a breadboard (left) and a circuit layout (right). **c,** A demonstration of the random bit generation for 6 consecutive cycles. A black, red, and green lines show the input pulse voltage, the oscillation current, and the output current of the T flip-flop, respectively. **d,** A P-value of the monobit test as a function of the input voltage pulse time. Above the P-value of 0.01 (red dashed line), it is regarded as random numbers. After 10 μs of pulse time, the outputs become true random numbers.

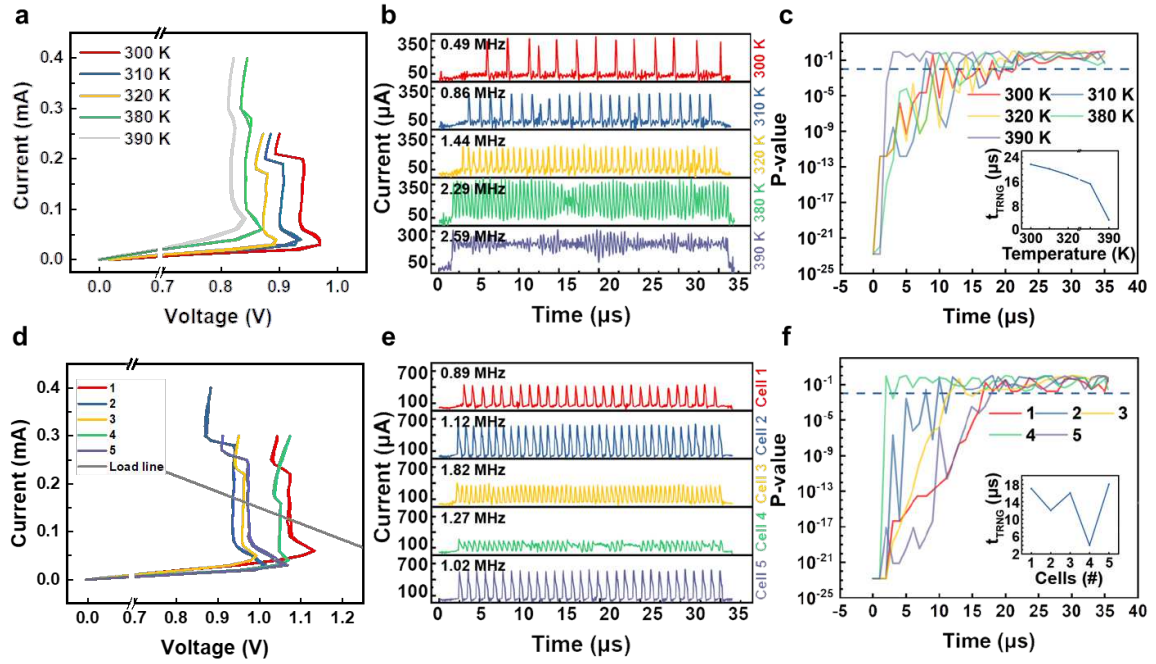

Figure 5 | Variation tolerant test results at different ambient temperature and at different cells. a, The I – V curves at different temperatures from 300 K to 390 K from the same cell. **b,** The oscillation current outputs at different temperatures. The frequency of oscillation increases as the temperature increases at the identical input voltage pulse. **c,** The P-value of the monobit test as a function of the input voltage pulse time using 100 bits per each temperature. The random bit reference line of 0.01 is included. The inset shows the minimum pulse time for random number generation as a function of the temperature. **d,** Representatively distinguishable I – V curves from 5 different cells. **e,** The oscillation current outputs and their frequency from each cell. **f,** The P-value for the monobit test obtained from 100 bits collected from each cell. They all pass the test at different random number generation time as shown in the inset.

Figures

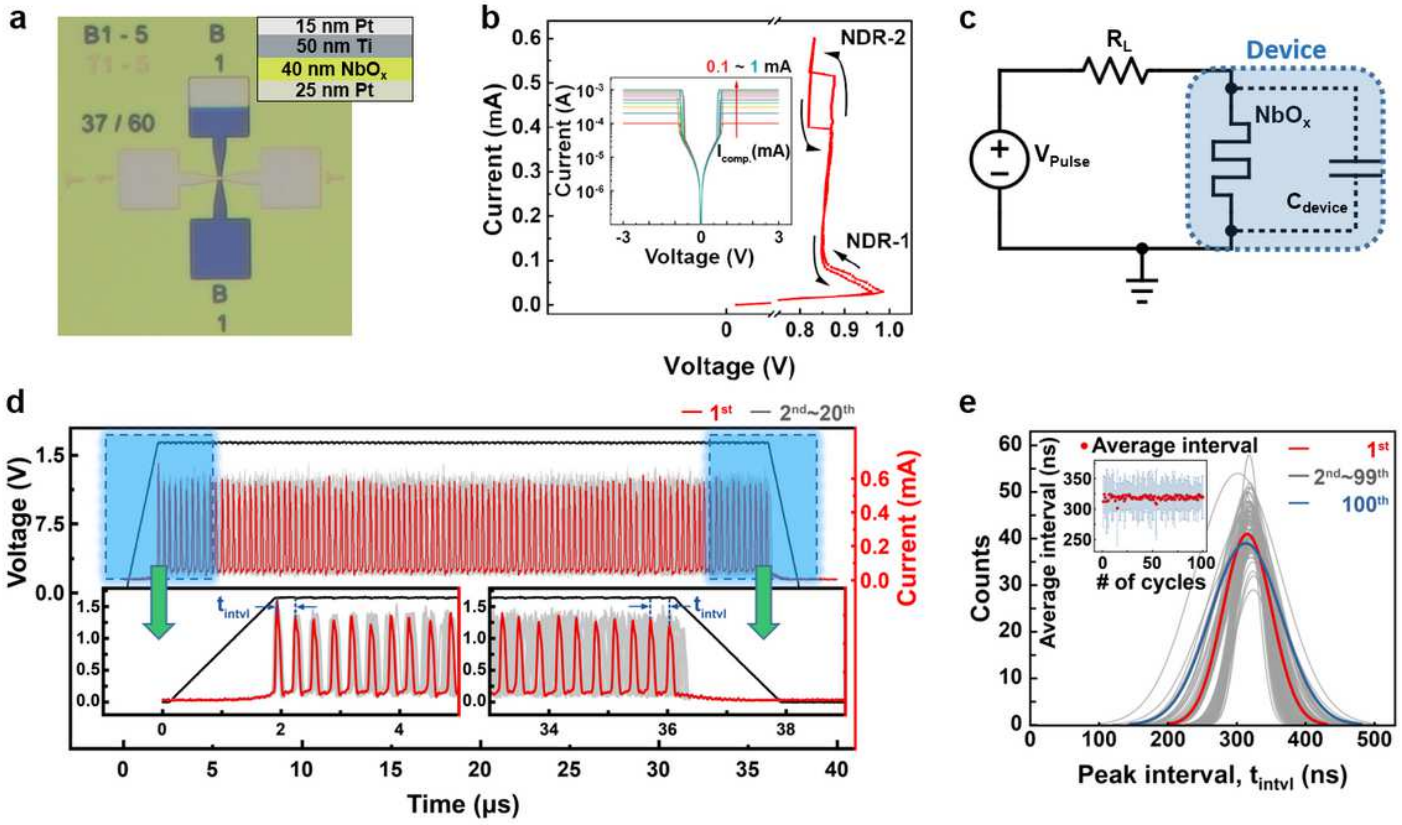

Figure 1

Electrical properties of NbOx-based threshold switching (TS) device, and its stochastic oscillation. a, An optical microscope image of the NbOx-based two terminal device. The inset shows the stack of the device. b, A representative I – V curve with a current sweep mode showing two negative differential resistance behaviors, noted to NDR-1 and NDR-2. The inset shows I -V curves in a voltage sweep mode with compliance currents ranging from 0.1 mA to 1 mA. c, An oscillator circuit composed of the device and a series resistor. The TS device composed of a volatile memristor and an internal capacitor. d, Experimentally obtained 20 oscillation current outputs under a fixed input voltage pulse. The left and right insets magnify the initial and final oscillation outputs, respectively. e, A distribution of peak intervals (t_intvl) at each oscillation output. It shows 100 distributions collected from 100 testing cycles. Inset shows the average and standard deviation of the t_intvl for 100 testing cycles.

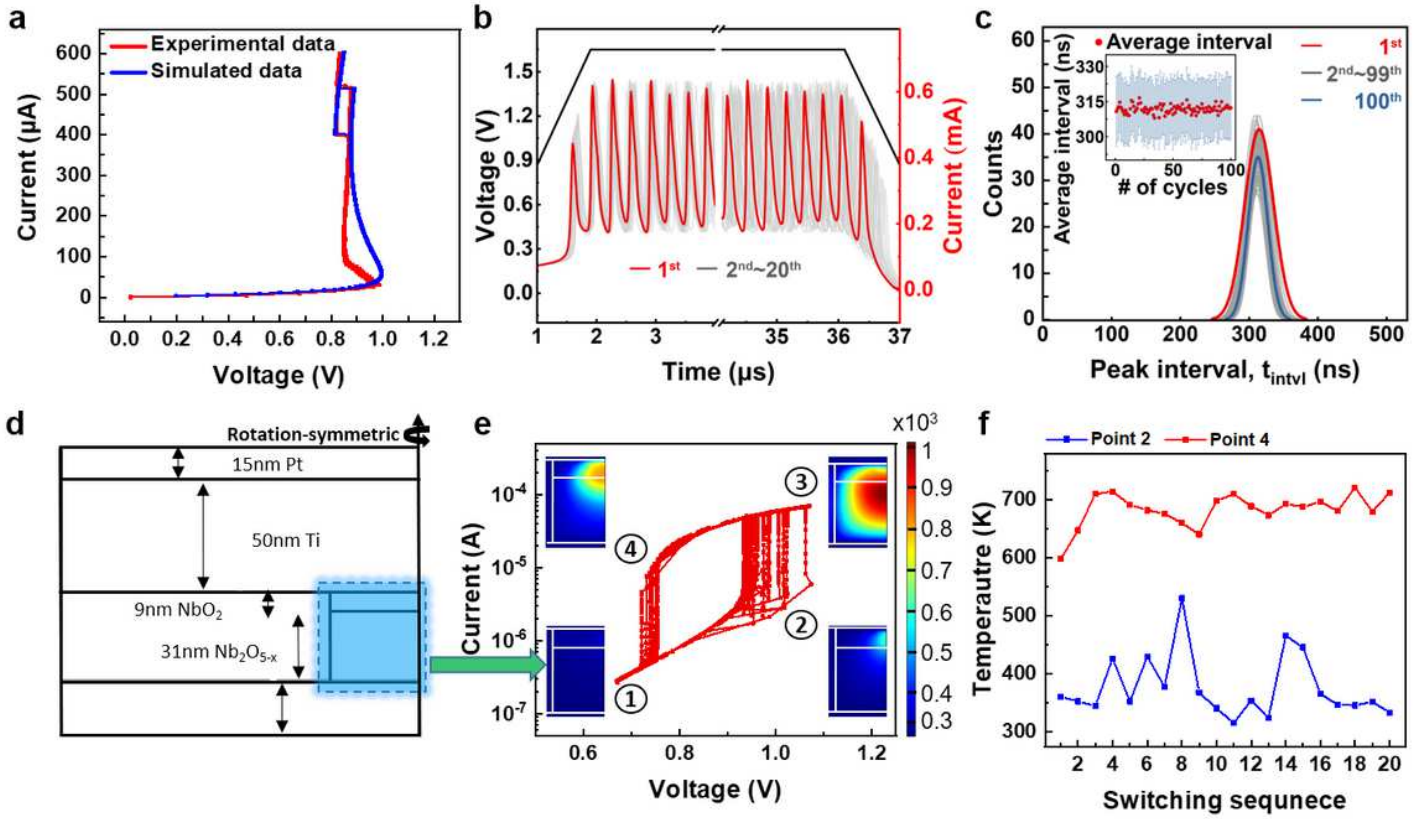

Figure 2

Simulations of stochastic oscillation characteristic induced by thermal fluctuation. a, A numerically simulated I – V curve (blue) compared with an experimental one (red line). b, Simulated 20 oscillation currents under a fixed voltage input. The oscillation outputs overlap well at the beginning, but they disperse at the end. c, Simulated distributions of the peak intervals for 100 cycles. Inset shows an average and a standard deviation of intervals. The results reproduce the experimental results in Fig. 1e. d, A geometry used for a thermodynamic simulation, which is identical with the fabricated device in Fig. 1a. e, Simulated I – V curves from the thermodynamic simulation under a sinusoidal input voltage. The insets show heat distribution at each moment. f, The maximum temperatures at the moment of switch on (□, blue) and switch off (□, red) for 20 cycles of simulation, showing they fluctuate.

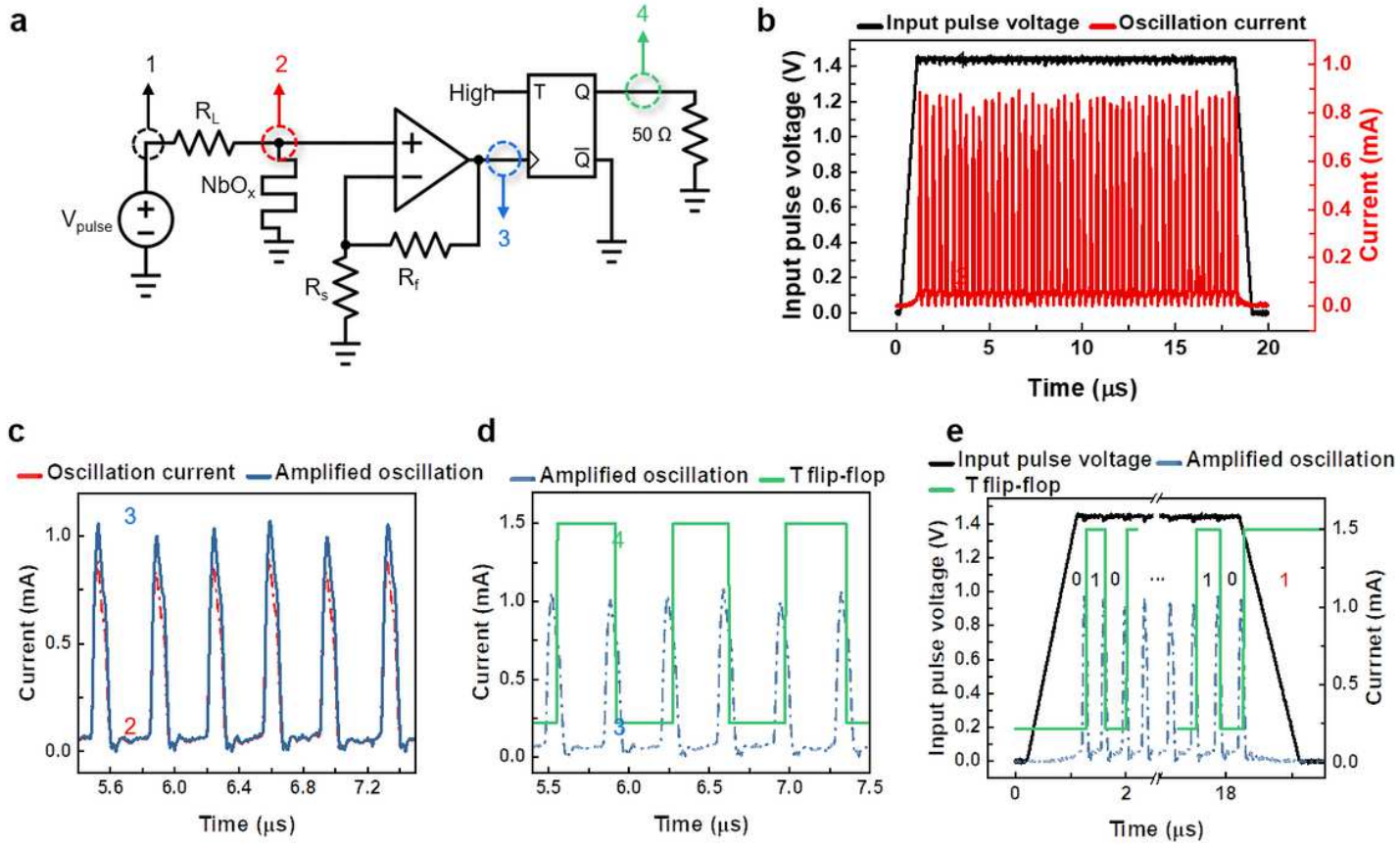

Figure 3

A TRNG circuit and its simulation. a, The proposed TRNG circuit composed of an op-amp, a T flip-flop, and three resistors. b, An input voltage pulse (black) and an output current (red) at node 2 in a. c, An amplified oscillation current at node 3 (blue) compared with the output current (red). d, An output signal at node 4 (green) after the amplified oscillation current passed the T flip-flop. e, A random bit is generated according to the final state of the T flip-flop when the input pulse finishes.

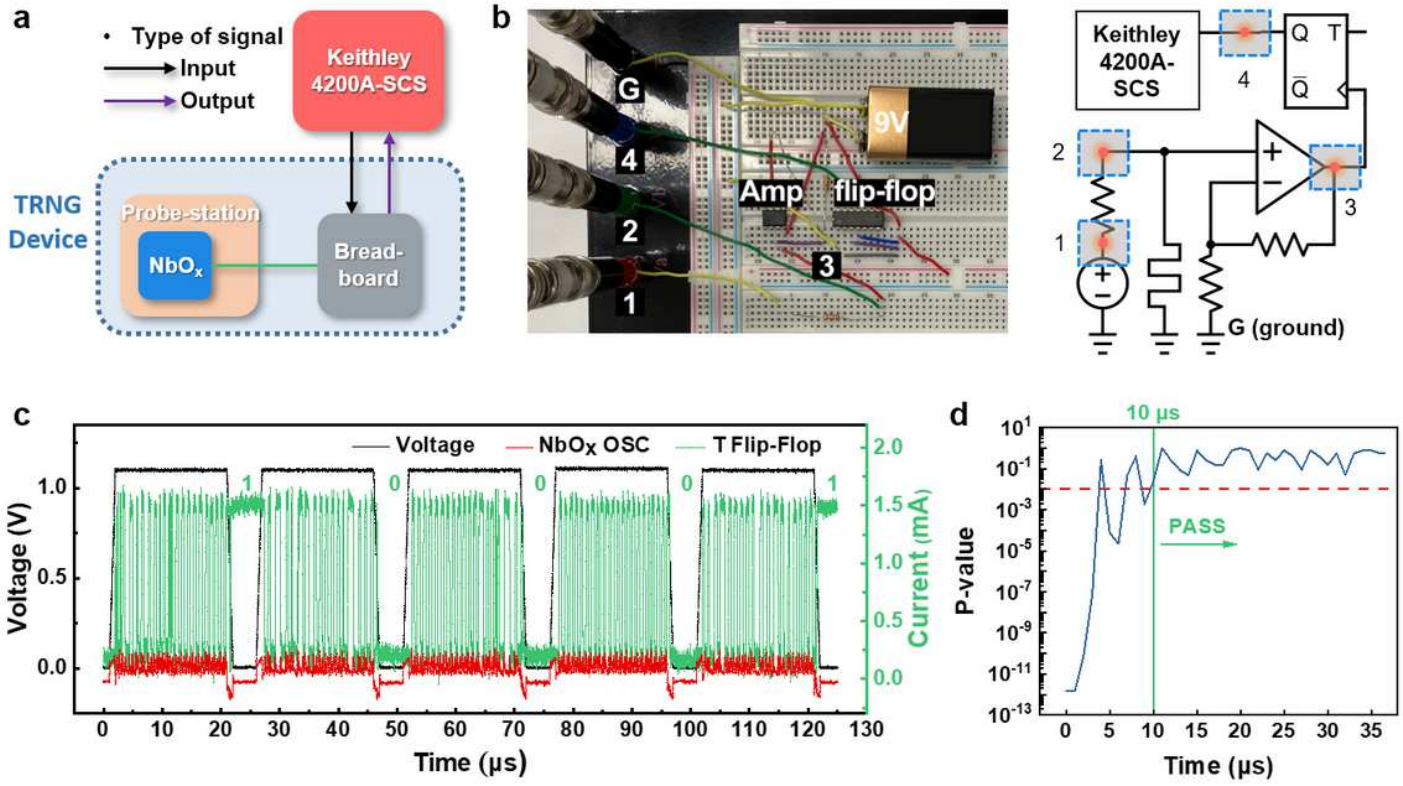

Figure 4

Experimental demonstration of the TRNG. a, An operating scheme of the proposed TRNG in experiments. b, A photograph of the circuit built on a breadboard (left) and a circuit layout (right). c, A demonstration of the random bit generation for 6 consecutive cycles. A black, red, and green lines show the input pulse voltage, the oscillation current, and the output current of the T flip-flop, respectively. d, A P-value of the monobit test as a function of the input voltage pulse time. Above the P-value of 0.01 (red dashed line), it is regarded as random numbers. After 10 μs of pulse time, the outputs become true random numbers.

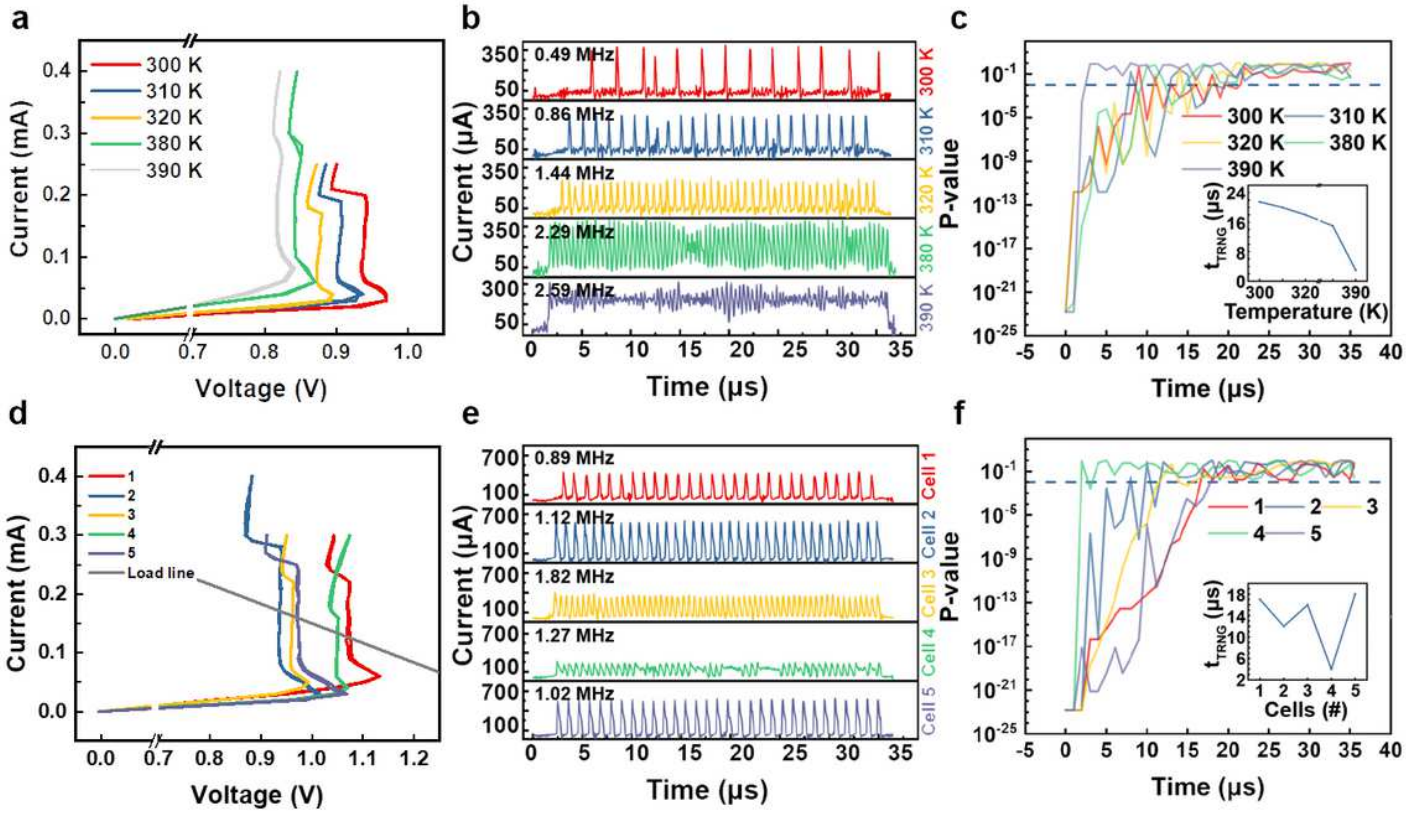

Figure 5

Variation tolerant test results at different ambient temperature and at different cells. a, The I – V curves at different temperatures from 300 K to 390 K from the same cell. b, The oscillation current outputs at different temperatures. The frequency of oscillation increases as the temperature increases at the identical input voltage pulse. c, The P-value of the monobit test as a function of the input voltage pulse time using 100 bits per each temperature. The random bit reference line of 0.01 is included. The inset shows the minimum pulse time for random number generation as a function of the temperature. d, Representatively distinguishable I – V curves from 5 different cells. e, The oscillation current outputs and their frequency from each cell. f, The P-value for the monobit test obtained from 100 bits collected from each cell. They all pass the test at different random number generation time as shown in the inset.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- TRNGSuppleVideo.mp4
- TRNGSuppl.docx