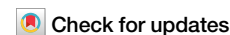


<https://doi.org/10.1038/s44335-025-00027-3>

Enhancing Johnson-Nyquist noise for high-performance Mott memristor-based oscillatory TRNG



Gwangmin Kim, Jae Hyun In, Hakseung Rhee, Woojoon Park, Hanchan Song & Kyung Min Kim ✉

Genuine stochastic information represented by true random numbers (TRNs) is essential for entropy-associated applications such as cryptography and energy-based computing. They demand specialized hardware called true random number generators (TRNGs) capable of rapid, energy-efficient TRN generation. In this study, we enhance Johnson-Nyquist noise to demonstrate the fastest, most energy-efficient memristor-based TRNG. The TRNG comprises an NbO_x -based negative resistance oscillator, a T flip-flop for digitalization, and a heater as a noise source. The heater enhances Johnson-Nyquist noise, achieving a TRNG speed of 100 kbit/s, 2.5× faster than without the heater. Furthermore, we propose a TRNG array that utilizes heat across the array for energy-efficient, parallel TRN generation. The 128-sized TRNG array is expected to achieve 0.65 $\mu\text{J/bit}$ at 1.28 Mbit/s, demonstrating significant improvements in speed and efficiency. By focusing on noise engineering rather than conventional material- or circuit-based methods, our approach enables broader applications in entropy-based computing.

The rapid expansion of the Internet of Things (IoT) has led to an explosion of data traffic, significantly increasing the demand for robust cryptography. Cryptography inherently relies on stochastic elements, such as random numbers, to ensure the security and robustness of its processes. The random numbers derived from deterministic algorithms using digital hardware and software are considered pseudo-random numbers (PRNs), which are vulnerable to security threats as PRNs can be predicted and manipulated if one gains control over the hardware or software¹. In contrast, true random numbers (TRNs) are generated from the natural laws of physics, making them entirely non-artificial and, therefore, capable of ensuring complete security.

A true random number generator (TRNG) is an electronic device that converts such unpredictable phenomena in nature to a bitwise digital signal. In this context, memristors are effective components as a source of unpredictable phenomena as their transition dynamics are inherently stochastic due to thermal noise^{2–15}. Various studies have demonstrated the feasibility of memristive TRNGs^{2–9}, and recently, these TRNGs have been employed in energy-based computing, where their inherent stochasticity helps in finding solutions to optimization problems^{11–15}. Considering such a wide range of potential future applications for TRNGs, the development of high-speed and energy-efficient TRNGs is crucial for accelerating their practical implementation.

For improving the TRNG performance, previous studies have primarily focused on finding more effective entropy sources in memristors and more efficient ways to convert the source information to digital data. For example, Jiang, H. et al. utilized multi-bit counters², and Woo et al. introduced nonlinear feedback shift register³. These approaches enabled the generation of multiple random numbers from a single memristor switching, thereby improving the TRN rate and energy efficiency. Subsequently, TRNGs have evolved to utilize dynamic changes rather than static ones to achieve faster and more efficient operation. Kim et al.⁴ introduced a NbO_x -based Mott oscillator, and Woo et al.¹⁵ utilized a similar approach but using a LaCoO_3 -based memristor exhibiting spin crossover mechanism. Consequently, memristive TRNG achieved improved speed and energy efficiency. However, further improvements in TRNG performance are still necessary, and achieving this will require a new approach beyond traditional ways such as circuit optimization and the exploration of new memristors.

In this study, we propose a physical approach to improve the TRNG performance by manipulating the noise source. The operating principle of the proposed TRNG is based on our previous TRNG using a Mott memristor featured by intrinsic large electrothermal nonlinearities^{4,16–18}. When the Mott memristor oscillates, the magnitude of thermal noise is temperature-dependent; high temperature correlates to increased thermal noise¹⁹. In this context, we introduced a cell-integrated heater to increase device temperature and, thus, the thermal noise. The heater amplifies the thermal

Department of Materials Science and Engineering, Korea Advanced Institute of Science and Technology (KAIST), Yuseong-gu, Daejeon, Republic of Korea.

✉ e-mail: km.kim@kaist.ac.kr

noise and shortens the required time to accumulate sufficient noise for TRNG generation. Consequently, the proposed TRNG showed the fastest operation (100 kbit/s) with a high energy efficiency (0.68 $\mu\text{J}/\text{bit}$), outperforming all previously reported memristor-based TRNGs that have passed the NIST randomness test. Moreover, the heater can be integrated underneath the TRNG, making its array integration feasible without complex electrical interconnection among them. Therefore, we exploit it for a more practical TRNG system. Specifically, we demonstrate an 8×1 TRNG array capable of generating 8 TRNGs simultaneously using only 46% of energy per bit compared to the single TRNG. This efficiency could be further improved as the array sizes extended, suggesting the proposed approach is highly applicable in future electronics^{11–14,20}.

Results and discussions

A resistive heater integration and its performance characterization

Figure 1a illustrates the cell stack of the heater-embodying Mott memristor fabricated on a SiO_2/Si substrate, consisting of a Mott memristor ($\text{Ti}/\text{NbO}_x/\text{Pt}$)

(Pt) and a resistive heater (Pt) separated by a dielectric Al_2O_3 layer. Details of the device fabrication process are described in the experimental section. The equivalent electrical circuit of the integrated device is shown in Fig. 1b. Here, V_{in} and V_{H} are the voltage sources for the Mott memristor and the heater, and R_{M} and R_{H} are the resistances of the Mott memristor and the heater, respectively. At this configuration, the heater generates Joule heat, which transfers to the Mott memristor through the thermally conducting but electrically insulating Al_2O_3 layer. Figure 1c shows the thermal circuit of the integrated device (left panel) and its simplified equivalent one (right panel). Here, the θ denotes the thermal resistance of the components, and P_{H} is the electrical power applied to the heater. The T_{H} , T_{M} , and T_{amb} are the heater, Mott memristor, and ambient temperatures, respectively. The heat is transferred to the Mott memristor through $\theta_{\text{Al}_2\text{O}_3}$, and is laterally diffused through θ_{L} while heat is lost to the air and substrate through θ_{air} and θ_{sub} , respectively. The thermal circuit can be simplified by Wye-Delta transformation, and the equivalent thermal resistance (θ_{eq}) to the surroundings can be derived²¹.

To ensure energy-efficient operation, minimizing heat loss to the surroundings is important, as it directly increases energy consumption. In

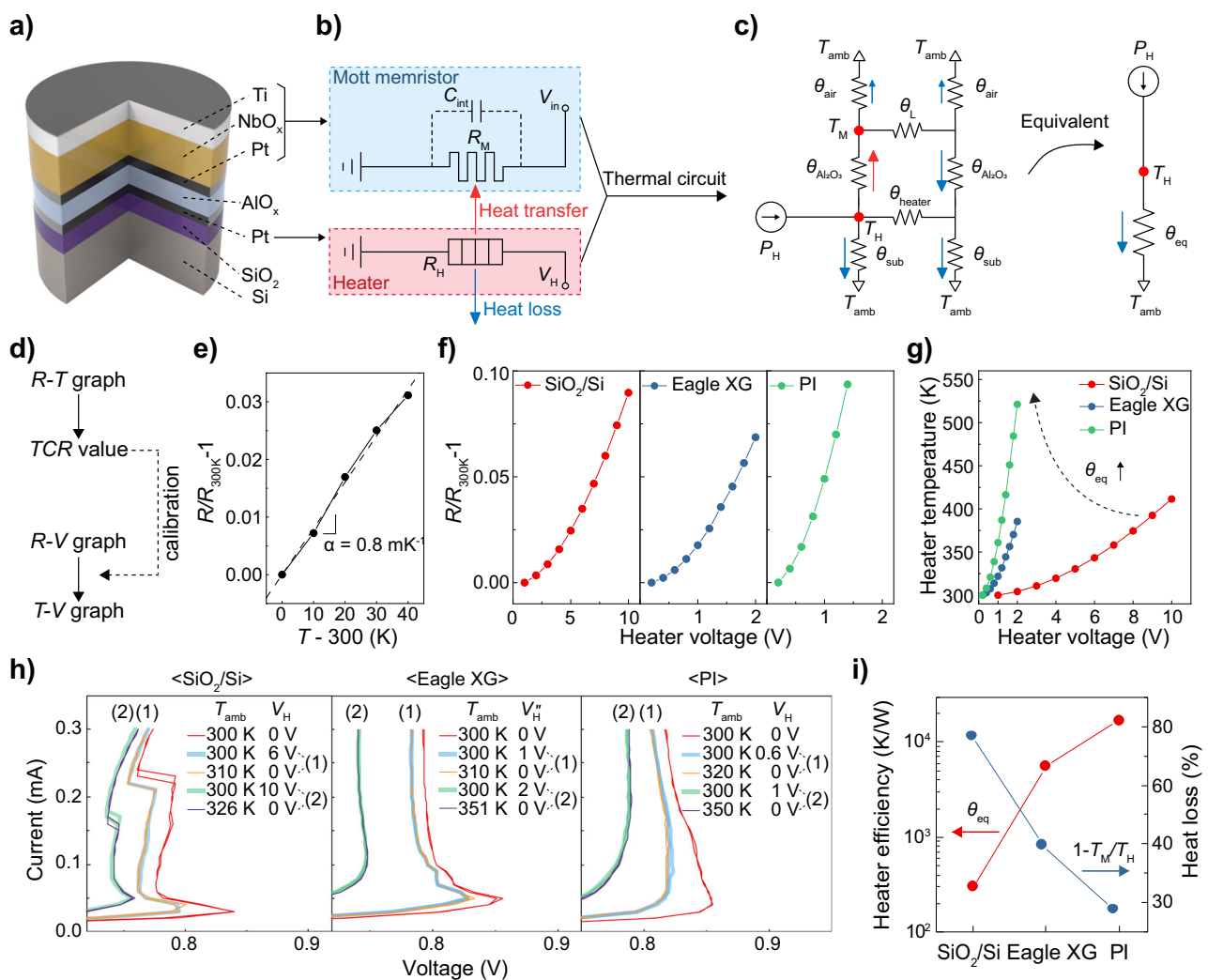


Fig. 1 | A heater embodying NbO_x -based Mott memristor and its electrical characteristics. **a** A schematic illustration of the device stack where a NbO_x Mott memristor and a heater are integrated. **b** The equivalent electrical circuit of the device. The NbO_x Mott memristor and the heater are electrically isolated but thermally connected. **c** The thermal circuit of the integrated device and its equivalent circuit. **d** The effective heater temperature estimation scheme. **e** $A(R/R_{300\text{K}} - 1) - (T_{\text{H}} - 300\text{K})$ plot for fitting the empirical thermal coefficient of resistance (TCR) of the heater. Each point was obtained by averaging the last three period of resistances in Supplementary Fig. 2. The standard deviation of each points was less than 0.0002.

f The heater resistance as a function of the heater voltage (V_{H}) fabricated on the three substrates. **g** The heater temperature as a function of heater voltage calibrated from (f) using the TCR. **h** The NDR I - V curves of Mott memristors at various V_{H} and the ambient temperatures, fabricated on the three substrates. Here, Set (1) and Set (2) each consist of two NDR curves, one obtained by varying the heater voltage and one by varying the ambient temperature, where the curves in each set are identical. **i** The thermal resistance representing the heater efficiency and the heat loss ($1 - T_{\text{M}}/T_{\text{H}}$) of the integrated device fabricated on the three different substrates.

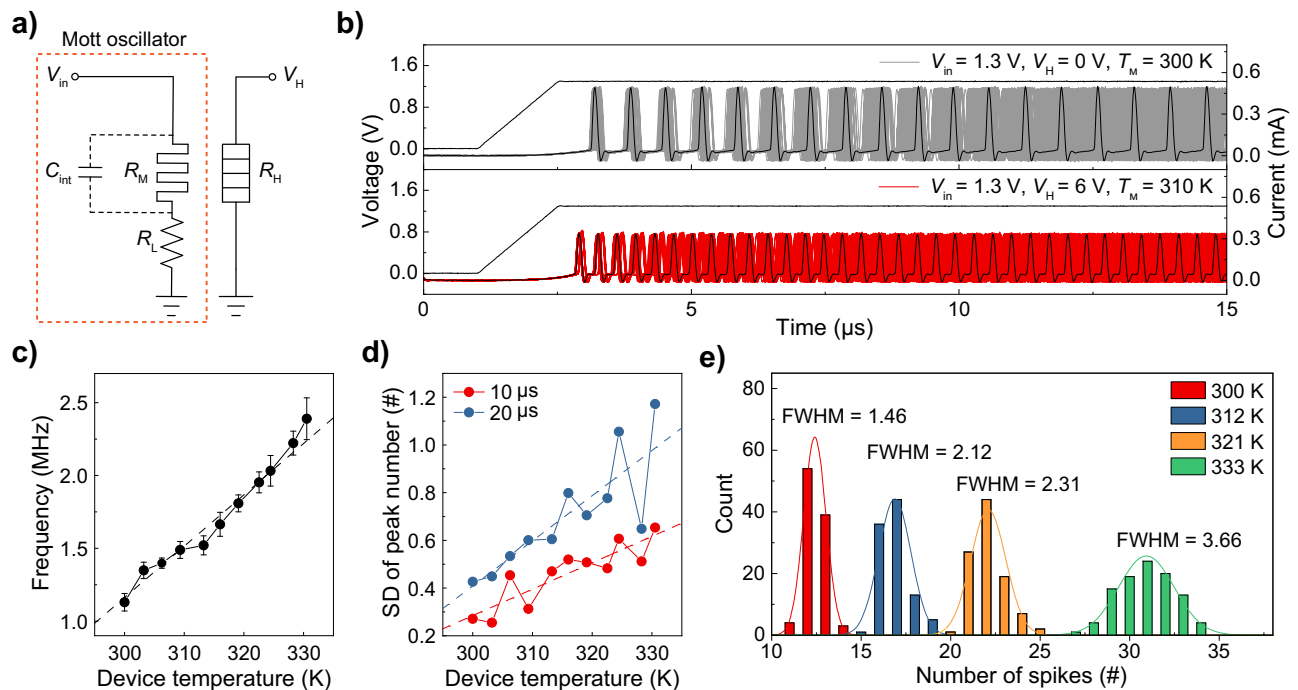


Fig. 2 | The enhanced stochastic oscillation of the Mott oscillator by the heater on the SiO₂/Si substrate. **a** A Mott oscillator circuit scheme with the heater. **b** Oscillation current outputs when the heater is inactive (top panel, gray) and active (bottom panel, red). Each graph includes 100 times of testing results. The black lines are one of the results of each condition. **c** The oscillation frequency shows a linear

relationship with temperature. **d** The standard deviation (SD) of the peak number within 10 μs and 20 μs of 100 oscillations at various temperatures. **e** The spike number distribution of 100 oscillations, each lasting 10 μs , at various temperatures, including their FWHMs. The FWHM was increased with temperature implying the oscillation gets more dispersed at elevated temperature.

the integrated device, the heat dissipation mainly occurs through the substrate (i.e., $\theta_{eq} \sim \theta_{sub}$). Therefore, we introduced thermally insulating substrates with a higher θ_{sub} to reduce heat dissipation (finite-element-based simulation results can be found in Supplementary Fig. 1). Then, the heater performance (i.e., the amount of heat generated and transferred to the Mott memristor) was investigated on three substrates: SiO₂/Si, Corning Eagle XG, and polyimide (PI) which have distinct thermal conductivities of 130 W/mK, 1.3 W/mK, 1.09 W/mK, and 0.12 W/mK for Si, SiO₂, Eagle XG, and PI, respectively^{22–24}.

The heater temperature can be estimated by measuring the temperature dependence of resistance:

$$R(T_H) = R_0[1 + \alpha(T_H - T_0)] \quad (1)$$

where R_0 is the resistance at the reference temperature (T_0) which was 220 Ohms, α is the temperature coefficient of resistance (TCR). Although α is well known for bulk metals, its accurate value in the integrated device is unclear due to the size effect of resistivity in a thin film²⁵. Therefore, we first calculated the empirical TCR value of the heater by measuring the heater resistance at various temperatures and calibrated the heater resistance to heater temperature using the TCR, following the process of Fig. 1d. The obtained TCR from the slope was 0.000802 K⁻¹ (Fig. 1e). The details of TCR calculation can be found in Supplementary Fig. 2. Although the TCR value was obtained over a temperature change of 40 K, we assumed that the TCR of the metal remains constant over a wide temperature range, allowing this value to be validly applied within the operating temperature range of the TRNG. Then, the heater resistances as a function of the V_H were measured (Fig. 1f). Lastly, the heater resistances were calibrated to the heater temperatures using the TCR (Fig. 1g). On the thermally insulating substrates (Eagle XG and PI) the heater temperature increased more than on the SiO₂/Si substrate, implying a higher θ_{eq} was achieved on the Eagle XG and PI.

The Mott memristor exhibits the negative differential resistance (NDR) behavior, which is highly sensitive to changes in ambient temperature^{4,26,27}. Therefore, to provide an intuitive comparison of how the

V_H affects the T_M , we measured the NDR behaviors varying the V_H , and compared them to the NDR behaviors at various T_{amb} . Through this, we can correlate the V_H condition and the T_{amb} condition, resulting in identical NDR behaviors. Figure 1h shows the NDR curves measured on the three substrates in various V_H and T_{amb} conditions. It includes the reference NDR curves (red line) at $T_{amb} = 300$ K and $V_H = 0$ V. Also, each panel includes two representative sets of identical NDR curves obtained by varying either V_H or T_{amb} . On the SiO₂/Si substrate, the NDR curves by $V_H = 6$ V (thick skyblue, Set (1)) and $T_M = 310$ K (orange, Set (1)) overlap, indicating that the $V_H = 6$ V condition has an identical effect to the $T_M = 310$ K condition. Similarly, $V_H = 10$ V condition (thick green, Set (2)) was identical to $T_M = 326$ K condition (purple, Set (2)). On the Eagle XG substrate, $V_H = 1$ V condition was identical to $T_M = 310$ K condition, and $V_H = 2$ V was to $T_M = 351$ K. On the PI substrate, $V_H = 0.6$ V and 1 V conditions were identical to $T_M = 320$ K and 350 K conditions, respectively.

Figure 1i summarizes the heater efficiency (θ_{eq}) and heat loss ($1 - T_M/T_H$) of the integrated device on the three substrates. The θ_{eq} was calculated from the Newton's cooling law ($T_H = \theta_{eq}P_H + T_{amb}$) at the equivalent thermal circuit in Fig. 1c. The θ_{eq} on SiO₂/Si, Eagle XG, and PI were 300.37 K/W, 5631.5 K/W, and 16779 K/W, respectively (See Supplementary Fig. 3 for detailed calculations.). Furthermore, the heat loss was reduced from 76.7% on SiO₂/Si to 39.8% on Eagle XG and 17.9% on PI. Consequently, the thermally insulating substrates increased the overall thermal resistance of the integrated device, allowing more effective heat utilization.

A heater-embodying Mott TRNG and its operation

A Mott oscillator can be composed by connecting a series load resistor to a Mott memristor, as shown in Fig. 2a^{4,13,28,29}. Here, R_L is the load resistance. Figure 2b overlays 100 current oscillations generated from the Mott oscillator on the SiO₂/Si substrate when the heater is inactive ($V_{in} = 1.3$ V, $V_H = 0$ V; $T_M = 300$ K) in the top panel and active ($V_{in} = 1.3$ V and $V_H = 6$ V; $T_M = 310$ K) in the bottom panel. The black lines in each panel are representative ones out of the 100 oscillations. In both cases, the

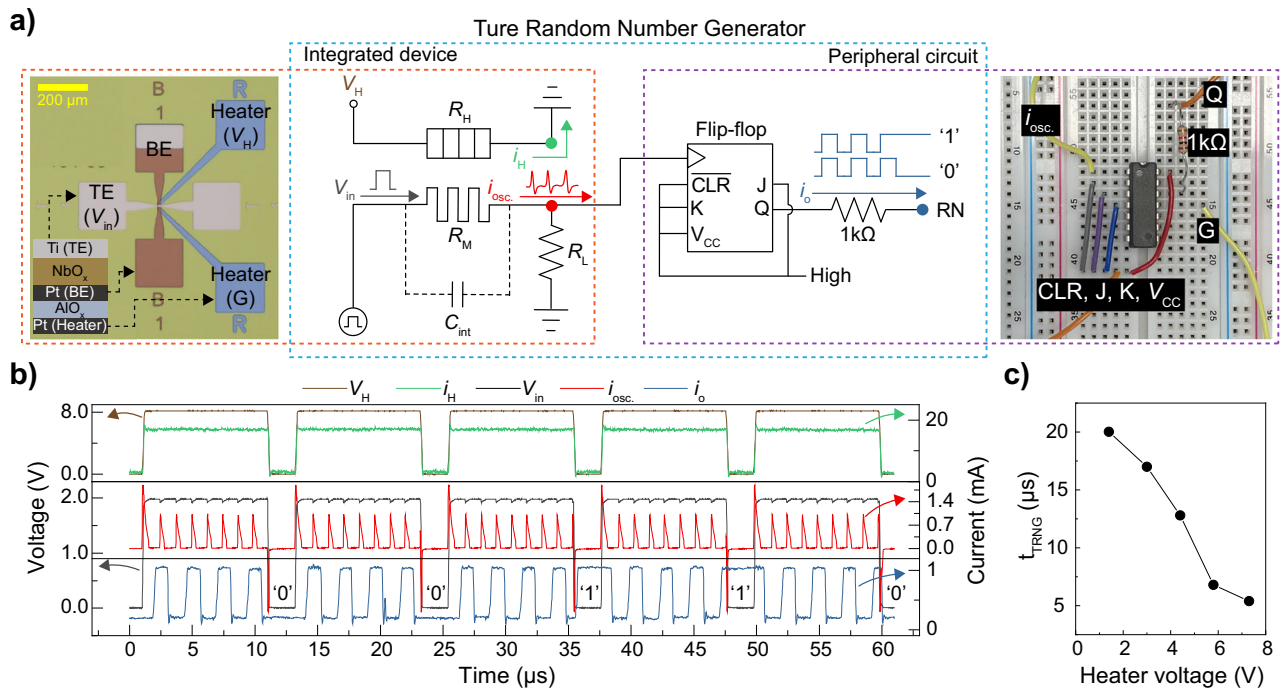


Fig. 3 | The demonstration of the heater-embodying Mott TRNG. a The overall system configuration including the electrical circuit layout and the optical microscopy image of the components of the proposed TRNG. The integrated device was loaded in the probe station, while the T flip-flop was built on the breadboard. **b** The 5

bits random number generation demonstration of the TRNG. In the demonstration, the random numbers of '00110' were generated. **c** The minimum time required to generate a random number (t_{TRNG}) as a function of V_H .

oscillations initially overlapped, gradually dispersed, and eventually became stochastic. This time-varying stochastic behavior is due to the accumulation of thermal noise⁴. When the V_H was applied (bottom panel), the oscillation became more stochastic at an earlier moment than the other case. This stochasticity, caused by the accumulation of thermal noise, is reflected in the variation in the number of oscillation peaks over a given time.

Figure 2c shows the oscillation frequency at various temperatures increased by the heater. Here, the oscillation frequency monotonically increased with temperature^{26,27,30}. Fig. 2d shows the standard deviation (SD) of the peak numbers during 10 μs (red) and 20 μs (blue) varying the device temperature by the heater. The results indicate that as both the oscillation frequency and thermal noise are proportional to the temperature, the SD of the peak number increases with temperature (see Supplementary Note 1 for a more detailed discussion). Consequently, the peak number distribution becomes more dispersed during the given time at high temperatures. Figure 2e shows the peak number distribution during 10 μs at various temperatures modulated by the heater. The full width at half maximum (FWHM) is also shown. The greater the dispersion in the peak number, the more quickly the TRNG can generate the TRN⁴. When the temperature is increased by the heater, the peak number distribution gets more dispersed having a higher FWHM, indicating that a faster TRNG is achievable at higher temperatures. Unlike peak number deviation, the relative standard deviation of interspike interval (ISI) in the oscillation does not change by temperature making it hard to achieve a faster TRNG exploiting the ISI instead of the peak number (Supplementary Fig. 4). Therefore, controlling temperature to increase peak number deviation is the only viable way to achieve high-performance TRNG in our system.

We built a Mott TRNG comprising an integrated device and a breadboard circuit as shown in Fig. 3a. In the circuit, a falling-edge triggered T flip-flop is used, which receives an oscillation input from the Mott oscillator and returns a binary output depending on the number of oscillation peaks. More detailed system configuration can be found in the experimental section. Please note that the Mott TRNG system in this study is a more compact version than our previous work⁴, in which the positions of

the Mott memristor and the R_L was changed. See Supplementary Fig. 5 for more details on the TRNG modification. The integrated device was placed in the probe station, and it was connected to the breadboard via cable. Figure 3b demonstrates 5 bits ("00110") of random number generation sample from the TRNG with a 10 μs-long pulse per bit while applying 8 V to the heater. The Mott TRNG operation video can be found in Supplementary Movie 1. We introduced a 2 μs interval between pulses to show the reading result of the T flip-flop. However, this interval can be omitted during actual operation.

We evaluated the TRNG rate (t_{TRNG}), which is the minimum time required for the generated bits to become truly random. We collected 100 bitstreams from the TRNG varying the V_H , and tested them using a monobit test, which is one of the 15 randomness tests in the NIST 800-22 standard³¹. The test results are summarized in Supplementary Fig. 6. Although the monobit test cannot solely determine whether the random numbers are TRNs, it can quickly examine the randomness of the dataset. In the test, the P -value serves as a measure of the randomness of the dataset, and if the P -value is higher than 0.01, the dataset can be considered a set of random numbers. Figure 3c plots the estimated t_{TRNG} from the monobit test results (i.e., the time for the P -value to be higher than 0.01). The t_{TRNG} decreased with increasing V_H , confirming that a faster TRNG is viable by increasing the thermal noise in the Mott memristor through the heater. The t_{TRNG} was not dependent on the operating point and frequency controlled by V_{in} (Supplementary Fig. 7). Therefore, V_H is the only parameter for reducing the t_{TRNG} . However, it should be noted that the oscillation amplitude decreases with increasing temperatures^{4,26,27}. Therefore, at a higher heater voltage for faster operation, an amplifier can be added to address the reduced oscillation amplitude issue and to ensure proper operation of the T flip-flop⁴.

We collected 55 sets of 10^6 random bits (so a total of 55 Mbits) at $V_H = 8$ V, and they passed all 15 NIST 800-22 statistical randomness tests, whose results are summarized in Supplementary Table 1. These results demonstrate t_{TRNG} of 100 kbit/s, which is 2.5 times faster than our previous work⁴, and the fastest among the volatile memristive TRNGs.

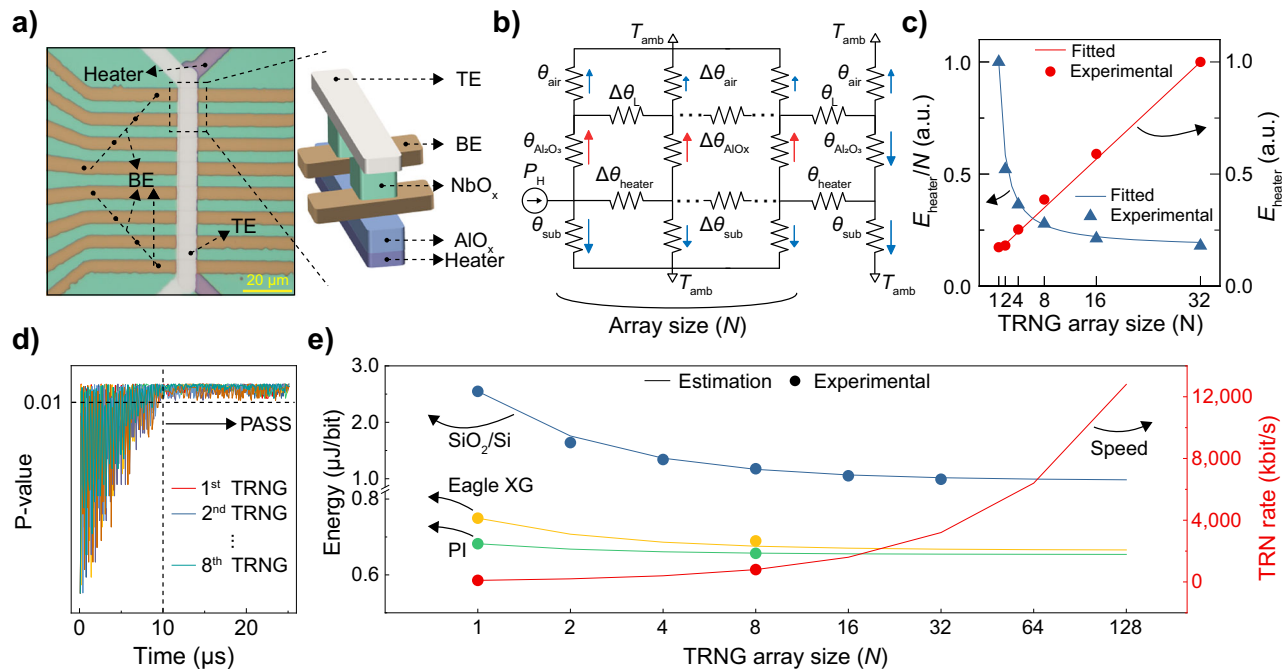


Fig. 4 | A Mott TRNG array and its performance. **a** An optical microscope image of the 8 × 1 TRNG array and a schematic illustration of a part of the array. **b** The thermal circuit of the TRNG array. **c** The normalized heater energy (E_{heater}) and normalized heater energy per TRNG (E_{heater}/N) as a function of the array size (N). **d** The monobit

test results of eight individual TRNGs obtained from the array. All passed the test in 10 μs . **e** The energy per bit and the TRN generation rate of the heater-embodying Mott-TRNG, fabricated on the three substrates, as a function of the array size. Symbols are experimentally obtained, and lines are modeled by calculation.

While the heater consumes additional energy, the increased speed may offset this energy consumption. On the SiO₂/Si substrate, the total energy consumption was 2.55 $\mu\text{J}/\text{bit}$, which is compatible with 2.87 $\mu\text{J}/\text{bit}$ of our previous TRNG, although the TRNG speed was improved by 2.5 times⁴. An effective way to further reduce energy consumption is to improve heater efficiency by using thermally insulating substrates. As a result, the total energy consumption can be reduced to 0.75 $\mu\text{J}/\text{bit}$ and 0.68 $\mu\text{J}/\text{bit}$ on the Eagle XG and PI substrates, respectively. (See Supplementary Fig. 8 and Supplementary Note 2 for the detailed energy consumption comparison.) Additionally, chip packaging, which primarily uses polymers with low thermal conductivity, has a heat-trapping effect. Therefore, it can enhance heat efficiency, similar to the application of PI substrates³². Furthermore, an array integration of the heater can further improve heater efficiency, which will be discussed in the following section.

A heater-embodying Mott TRNG array

IoT devices primarily communicate over the Internet, and securing these communications requires proper authentication. Cryptographic communication requires random tokens, such as nonce, which are generated and refreshed with each authentication. Thus, a large number of TRNs generated in real-time is required. Moreover, the exponential growth in data volume has resulted in a surge of parameters that need to be optimized for computing. This, in turn, necessitates the incorporation of substantial stochastic functions to address large-scale problems. Here, TRNG array is a viable way to generate massive TRNs for these purposes³³.

We fabricated an $N \times 1$ (where $N = 1, 2, 4, 8, 16$, and 32) size of the heater-integrated TRNG array to demonstrate a massive TRN generation and assess its performance. Figure 4a shows an optical top-view image (left) and a schematic illustration (right) of a representative 8×1 array. Here, the heater was integrated parallel to the memristor array beneath it, supplying heat with high efficiency. This is viable as our heater has vertical stack distinguished to previous studies where heater was integrated with lateral device^{30,34}. Fig. 4b shows the thermal circuit of the TRNG array. As the array size increases, more heat is dissipated to the surroundings by the increased heater area compared to a single TRNG. This results in the decrement of the

thermal resistance, thereby a higher V_H is necessary to reach the target temperature, accompanying more energy consumption (see Supplementary Fig. 9 for more details on the thermal resistance of the array.) However, the energy consumption per bit can be reduced, making the array more energy efficient.

Figure 4c plots the experimentally measured normalized heater energy consumption (E_{heater}) and the normalized heater energy consumption per bit (E_{heater}/N). Also, it includes numerical calculation results. (See Supplementary Note 3 for the details of the heater energy consumption.) The E_{heater} increased linearly with N ($E_{\text{heater}}(N) = N \times E_{\Delta} + E(1) - E_{\Delta}$). Here, $E(1)$ is the heater energy when $N = 1$, which includes the original heat loss by θ_{sub} and θ_{air} , and E_{Δ} is the unit heater energy increased by array size through $\Delta\theta_{\text{sub}}$ and $\Delta\theta_{\text{air}}$. However, as the array size increases, the original heat loss becomes negligible, and the heater energy consumption per bit ($= E_{\Delta} + (E(1) - E_{\Delta})/N$) is reduced and converges to E_{Δ} . This suggests that the heater can be more energy-efficiently utilized in the TRNG array.

We demonstrated an 8×1 TRNG array of Fig. 4a, generating 100 random numbers simultaneously from each TRNG in the array. The random numbers passed the monobit test, confirming successful TRNG array operation in 10 μs (Fig. 4d). Figure 4e shows the energy consumption per bit (E_{bit}) of the TRNG array and t_{TRNG} . The E_{bit} of octuple ($N = 8$) TRNG on SiO₂/Si substrate was reduced to 46% of the single TRNG. Furthermore, on the SiO₂/Si substrate and when $N = 128$ (for 128-bit nonce cryptography³⁵), the energy consumption could be further reduced to 0.981 $\mu\text{J}/\text{bit}$. The energy consumption could be further reduced on Eagle XG or PI substrates, as they can drastically improve the heater efficiency. For example, the E_{bit} on the PI can be as low as 0.654 $\mu\text{J}/\text{bit}$ when $N = 128$. We compared the proposed TRNG system on the SiO₂/Si substrate to other TRNG works, which passed all the NIST tests with proper data size (≥ 55 Mbit) in terms of speed, energy consumption, and circuit components (Table 1)^{2-4,15}. Our TRNG system outperformed them in all aspects, highlighting the excellence of this work. The heater undergoes a very weak electrical stress that does not cause electromigration issues in the heater^{36,37}. Therefore, incorporating the heater is a reliable solution that enhances performance.

Table 1 | Benchmarking of volatile memristor-based TRNG passed all 15 NIST tests

	Speed (kbit/s/cell)	Memristor			Active components			Energy ($\mu\text{J/bit}$)
		Voltage (V)	Current (μA)	Energy (pJ/bit)	Clock source	Electronic components	Others	
Jiang et al. ²	6	0.4	~ 10	0.8	1	Comparator AND gate 2 Counters		425.1
Woo et al. ³	32	7	~ 0.010	1.16	1	XNOR gate XOR gate 4 D flip-flops		50.3
Kim et al. ⁴	40	1.45	144 (avg.)	5,220		T flip-flop Op-amp		2.9
Woo et al. ¹⁵	50	12	1,500 (avg.)	360,000		T flip-flop		1.7
This work	100 ($N = 1$)	2.0	177 (avg.)	3,540		T flip-flop	Heater	2.6
	800 ($N = 8$)		1,400 (avg.)	28,320		8 T flip-flops	Heater	1.2

Table 2 | The energy consumption of TRNG systems at different scales and array sizes.

Device	Substrate	Energy for Heater ($\mu\text{J/bit}$)	Energy for T flip-flop ($\mu\text{J/bit}$)	Energy for Mott oscillator ($\mu\text{J/bit}$)	Total Energy ($\mu\text{J/bit}$)
5 μm $N = 1$	SiO ₂ /Si	1.9	0.646	0.0035	2.55
	Eagle XG	0.1			0.75
	PI	0.03			0.68
5 μm $N = 128$	SiO ₂ /Si	0.33			0.98
	Eagle XG	0.02			0.67
	PI	0.006			0.66
130 nm $N = 1$	SiO ₂ /Si	0.0013	0.026		0.031
130 nm $N = 128$	SiO ₂ /Si	0.00023			0.030

In summary, we developed a physical method to improve TRNG by integrating a heater with the NbO_x-based Mott memristors and engineering the thermal noise. The proposed TRNG has been improved by directly controlling the thermal noise, representing a novel approach, and as a result, it achieved a speed of 800 kbit/s and energy consumption of 1.2 $\mu\text{J/bit}$ in an 8×1 TRNG array, making it the highest-performing TRNG reported to date.

It would be interesting to envision future advancements in achieving faster speeds and lower energy consumption of the proposed system. Achieving faster speeds can be achieved by increasing the device temperature to further enhance thermal noise; however, it also reduces the NDR region, potentially eliminating the oscillation characteristics. Due to this trade-off, the maximum achievable TRNG rate is likely to have a limit.

On the other hand, there can be more opportunities for energy improvement. In the proposed system, thermal resistance is the crucial factor for achieving high energy efficiency. As demonstrated, introducing a thermally insulating substrate is one solution for high thermal resistance. Additionally, thermal resistance can be enhanced through various methods, indicating the potential for further advancement of the proposed technology. For example, thermal resistance can be further increased by optimizing the heater geometry, such as by implementing a confined cell structure in the phase change memory³⁸. Moreover, device scaling is a fundamental method to increase thermal resistance; if the device feature size is scaled down from 5 μm to 130 nm, the heater energy consumption can be reduced to 0.07% in 128×1 TRNG array³⁹. (Table 2 summarizes the estimated TRNG performance, and a more detailed discussion on the device scaling can be found in Supplementary Fig. 10.) When scaled down, the flip-flop limits energy

efficiency, and the next step may involve developing an energy-efficient digitalization method.

In another aspect, there are attempts to utilize heat as information for energy-efficient computing^{27,40}. We remark that heat tunes the stochastic process in the device, and it may be viable to construct a device network modulating stochastic functions through inter-device heat transfer²⁷. As such, this work expands its utility of engineering stochastic processes through heat for next-generation encryption hardware and computing primitives.

Methods

A heater-embodying Mott device fabrication

A (top) Pt/Ti/NbO_x/Pt/(Ti)AlO_x/Pt/(Ti) (bottom) stack was fabricated using the following procedure. An adhesive 5-nm Ti followed by a 25-nm-thick Pt heater electrode was deposited by e-beam evaporation and patterned by a lift-off process on SiO₂/Si, Eagle XG glass, and PI substrates. Then, a 20-nm-thick AlO_x layer was deposited by a thermal atomic layer deposition (ALD) at 250 °C using a trimethylaluminum (TMA) precursor and an H₂O reactant. Next, an adhesive 5-nm-thick Ti and a 25-nm-thick Pt bottom electrode were deposited using an e-beam evaporator and patterned by a lift-off process. Then, a 35-nm-thick NbO_x layer was deposited by a reactive sputtering process at 170 °C in Ar:O₂ (13:7, 4 mtorr) mixed gas ambient using a Nb target. Then, a 50-nm-thick Ti top electrode followed by a 15-nm-thick Pt passivation contact electrode was deposited by e-beam evaporation and patterned by a lift-off process. The line width of the patterns was 5 μm .

Mott TRNG system configuration and operation

The TRNG system comprises a Mott oscillator, a heater, and a T flip-flop. The oscillation signal from the Mott oscillator is transmitted to the T flip-flop. The T flip-flop (Texas Instruments, SN74LS73AN) is triggered at the falling edge of the oscillation current signal, which is the identical timing of the voltage decrement at the load resistor. For an experimental demonstration of the proposed TRNG, the Mott oscillator was implemented in a probe station, and the T flip-flop was integrated on a breadboard. The V_{cc}, J, K, and CLR terminals of T flip-flop were sourced to 2.5 V by an EXO K-6135 DC power supply, while the Mott oscillator and the heater were biased by Keithley 4200-SCS. Their signals were transmitted via cables, and they were monitored by Keithley 4200-SCS.

Electrical characterization

All the electrical characterization was performed using Keithley 4200A-SCS.

Device ambient temperature control

The device was placed on a hot chuck (MSTECH, ST1), and the ambient temperature was controlled by a hot chuck controller (MSTECH,

MST10000H). The temperature was calibrated by a thermocouple before measurement.

NIST test

The randomness test code was built in the Python environment, referring to the NIST Statistical Test Suite (Special Publication 800-22).

Data availability

Data sets generated during the current study are available from the corresponding author on reasonable request.

Received: 13 December 2024; Accepted: 31 March 2025;

Published online: 04 June 2025

References

- Fischer, T. Testing cryptographically secure Pseudo random number generators with artificial neural networks. In *Proc. 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*, pp. 1214–1223 (2018).
- Jiang, H. et al. A novel true random number generator based on a stochastic diffusive memristor. *Nat. Commun.* **8**, 882 (2017).
- Woo, K. S. et al. A high-speed true random number generator based on a $\text{Cu}_x\text{Te}_{1-x}$ diffusive memristor. *Adv. Intell. Syst.* **3**, 2100062 (2021).
- Kim, G. et al. Self-clocking fast and variation tolerant true random number generator based on a stochastic mott memristor. *Nat. Commun.* **12**, 2906 (2021).
- Yan, X. et al. A high-speed true random number generator based on Ag/SiNx/n-Si memristor. *Front. Phys.* **19**, 13202 (2023).
- Balatti, S. et al. Physical unbiased generation of random numbers with coupled resistive switching devices. *IEEE Trans. Electron Dev.* **63**, 2029–2035 (2016).
- Zhang, T. et al. High-speed true random number generation based on paired memristors for security electronics. *Nanotechnol* **28**, 455202 (2017).
- Carboni, R. et al. Random number generation by differential read of stochastic switching in spin-transfer torque memory. *IEEE Electron Device Lett.* **39**, 951–954 (2018).
- Fu, Y. et al. A 2.22 Mb/s true random number generator based on a GeTe_x ovonic threshold switching memristor. *IEEE Electron Device Lett.* **44**, 853–856 (2023).
- Li, X. et al. Random telegraph noise in metal-oxide memristors for true random number generators: a materials study. *Adv. Funct. Mater.* **31**, 2102172 (2021).
- Rhee, H. et al. Probabilistic computing with NbOx metal-insulator transition-based self-oscillatory pbit. *Nat. Commun.* **14**, 7199 (2023).
- Woo, K. S. et al. Probabilistic computing using $\text{Cu}_{0.1}\text{Te}_{0.9}/\text{HfO}_2/\text{Pt}$ diffusive memristors. *Nat. Commun.* **13**, 5762 (2022).
- Kumar, S., Strachan, J. P. & Williams, R. S. Chaotic dynamics in nanoscale NbO₂ Mott memristors for analogue computing. *Nature* **548**, 318–321 (2017).
- Cai, F. et al. Power-efficient combinatorial optimization using intrinsic noise in memristor Hopfield neural networks. *Nat. Electron.* **3**, 409–418 (2020).
- Woo, K. S. et al. True random number generation using the spin crossover in LaCoO_3 . *Nat. Commun.* **15**, 4656 (2024).
- Kumar, S. et al. Physical origins of current and temperature controlled negative differential resistances in NbO₂. *Nat. Commun.* **8**, 658 (2017).
- Kumar, S. & Williams, R. S. Separation of current density and electric field domains caused by nonlinear electronic instabilities. *Nat. Commun.* **9**, 2030 (2018).
- Gibson, G. A. Designing negative differential resistance devices based on self-heating. *Adv. Funct. Mater.* **28** (2018).
- Nyquist, H. Thermal agitation of electric charge in conductors. *Phys. Rev.* **32**, 110–113 (1928).
- Song, H. et al. Memristive explainable artificial intelligence hardware. *Adv. Mater.* **36**, 2400977 (2024).
- Truemper, K. On the delta-wye reduction for planar graphs. *J. Graph Theory* **13**, 141–148 (1989).
- Shanks, H. R., Maycock, P. D., Sidles, P. H. & Danielson, G. C. Thermal conductivity of silicon from 300 to 1400°. *K. Phys. Rev.* **130**, 1743–1748 (1963).
- McKeen, L. W., *Film Properties of Plastics and Elastomers*, 147–185 (William Andrew Publishing, 2017).
- Corning, Eagle XG Glass product & Material Information. https://www.corning.com/media/worldwide/cdt/documents/EAGLE%20XG_PI%20Sheet_2021.pdf (2021).
- Zhai, Y. et al. Study on the resistance characteristic of Pt thin film. *Phys. Proced.* **32**, 772–778 (2012).
- Nandi, S. K., Li, S., Liu, X. & Elliman, R. G. Temperature-dependent frequency tuning of NbOx relaxation oscillators. *Appl. Phys. Lett.* **111** (2017).
- Kim, G. et al. Mott neurons with dual thermal dynamics for spatiotemporal computing. *Nat. Mater.* **23**, 1237–1244 (2024).
- Liu, X., Li, S., Nandi, S. K., Venkatachalam, D. K. & Elliman, R. G. Threshold switching and electrical self-oscillation in niobium oxide films. *J. Appl. Phys.* **120**, 124102 (2016).
- Pickett, M. D., Medeiros-Ribeiro, G. & Williams, R. S. A scalable neuristor built with Mott memristors. *Nat. Mater.* **12**, 114–117 (2013).
- del Valle, J., Salev, P., Kalcheim, Y. & Schuller, I. K. A caloritronics-based Mott neuristor. *Sci. Rep.* **10**, 4292 (2020).
- Rukhin A. et al. NIST Special Publication 800-822 (2010).
- Mahalingam, M. Thermal management in semiconductor device packaging. *Proc. IEEE* **73**, 1396–1404 (1985).
- Mao, H. et al. Amorphous indium–gallium–zinc–oxide memristor arrays for parallel true random number generators. *Appl. Phys. Lett.* **122**, 053503 (2023).
- Oh, S. et al. Energy-efficient Mott activation neuron for full-hardware implementation of neural networks. *Nat. Nanotechnol.* **16**, 680–687 (2021).
- Chang, D., Kang, J. & Turan, M. S. A new conditional cube attack on reduced-round ascon-128a in a nonce-misuse setting. In: *Proc. Light weight Cryptography Workshop* (NIST, 2022).
- Eliasson, O. et al. Power regulation and electromigration in platinum microwires. *Rev. Sci. Instrum.* **85**, 114709 (2014).
- Kim, J. et al. Electromigration Reliability of Barrierless Ruthenium and Molybdenum for Sub-10 nm Interconnection. *ACS Appl. Electron. Mater.* **5**, 2447–2453 (2023).
- Im, D. H. et al. In *Proc. IEEE International Electron Devices Meeting*. 1–4 (IEEE, 2018).
- Sharma, P. & Joshi, H. Implementation of high speed, low power NAND gate-based JK flip-flop using modified GDI technique in 130 nm technology. *Int. J. Eng. Technical Res.* **5**, 2454 (2016).
- Qiu, E., Zhang, Y.-H., Ventra, M. D. & Schuller, I. K. Reconfigurable cascaded thermal neuristors for neuromorphic computing. *Adv. Mater.* **36**, 2306818 (2024).

Acknowledgements

This research was supported by the National Research Foundation of Korea (NRF) (Grant numbers: RS-2023-00216619, RS-2023-00216992, 2022M3F3A2A01076569, 2022M3I7A4085484, and 2023R1A2C2005159), and NNFC (Grant number: 1711160154).

Author contributions

G.K. conceived the idea of engineering thermal noise and designed the TRNG. G.K. and J.H.I. performed the experiments. G.K. performed COMSOL simulation, and temperature and energy calculations. J.H.I. performed the NIST test. H.R., W.P., and H.S. performed data analysis and

discussed the results. G.K., J.H.I., and K.M.K. wrote the manuscript. K.M.K. supervised this study.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at <https://doi.org/10.1038/s44335-025-00027-3>.

Correspondence and requests for materials should be addressed to Kyung Min Kim.

Reprints and permissions information is available at <http://www.nature.com/reprints>

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

© The Author(s) 2025