Check for updates

Advanced Functional Materials

ADVANCED FUNCTIONAL MATERIALS
www.afm-journal.de

RESEARCH ARTICLE OPEN ACCESS

True Random Number Generator for Robust Data Security via Intrinsic Stochasticity in a 2D hBN Threshold Switching Memristor

Yooyeon Jo[1] | Gichang Noh[2] | Eunpyo Park[2] | Dae Kyu Lee[2] | Heerak Wi[3] | Joon Young Kwak[3]

[1]Department of Semiconductor Materials Engineering, Sun Moon University, Asan, Republic of Korea | [2]Center for Semiconductor Technology, Korea Institute of Science and Technology (KIST), Seoul, Republic of Korea | [3]Division of Electronic and Semiconductor Engineering, Ewha Womans University, Seoul, Republic of Korea

Correspondence: Joon Young Kwak (jykwak@ewha.ac.kr)

Received: 27 August 2025 | **Revised:** 10 January 2026 | **Accepted:** 12 January 2026

Keywords: 2D materials | data encryption | threshold switching memristor | true random number generator

ABSTRACT

The explosive growth of Internet of Things (IoT) devices has demanded the urgency of robust data security to protect private information. The random numbers generated by pseudo-random number generators (PRNGs) play a crucial role in cryptographic algorithms. However, these sequences have become increasingly predictable due to advances in computing power and machine learning. Therefore, the development of true random number generators (TRNGs), which exploit the intrinsic hardware-level randomness as an entropy source, is important for future data security. In this study, we present TRNG circuits that harness the inherent stochasticity of a multilayer hBN volatile memristor. The fabricated device exhibits highly stable threshold switching with low set/hold voltages and a significantly high on/off ratio. We implement a spike generator by integrating the threshold switching memristor with passive components. Digitization with a fixed-reference comparator directly converts output spikes into bitstreams that successfully pass NIST randomness tests without postprocessing. The practical utility of the TRNG is demonstrated through XOR-based encryption and decryption of black-and-white and grayscale images, resulting in noise-like encrypted data and perfect recovery of the originals using identical keys. These results establish 2D hBN-based threshold switching memristors as compelling hardware entropy sources for secure, next-generation electronic systems.

1 | Introduction

In the new industrial era, the convergence of technologies across the physical, digital, and biological domains has enabled significant advancements in fields such as artificial intelligence (AI), robotics, the Internet of Things (IoT), and biotechnology, thereby huge impact on both industry and society [1]. These emerging technologies have facilitated the development of autonomous vehicles, remote control of home appliances, health monitoring systems, and e-commerce platforms, all of which contribute to improving the quality of human daily life [2]. In particular, with the exponential expansion of the number of IoT devices (estimated to be more than 100 billion in 2050 [3]), the amount of data produced, stored, and transmitted is expected to increase significantly [4–6]. As a result, the necessity for advanced data security solutions against hacking or cyber-attack is essential to protect private and sensitive information. Many data security protocols have been developed to prevent unauthorized access using various cryptographic techniques, in which the random number plays a critical role in the secure algorithm [7–9]. Although pseudo-random number generators (PRNGs), which generate random keys through software-based

This is an open access article under the terms of the Creative Commons Attribution-NonCommercial License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited and is not used for commercial purposes.
© 2026 The Author(s). *Advanced Functional Materials* published by Wiley-VCH GmbH

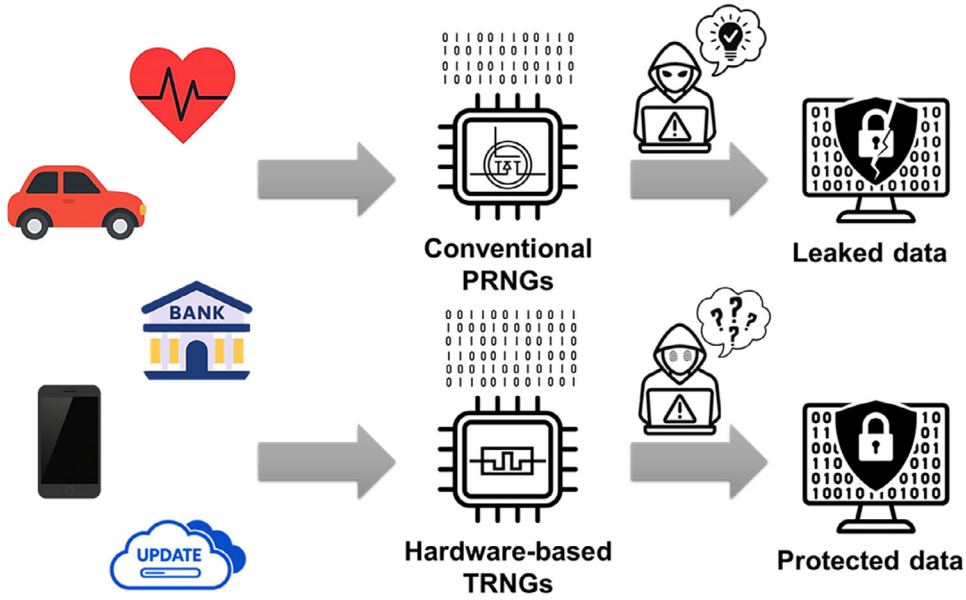


FIGURE 1 | Schematic comparison between conventional PRNGs and memristor-based TRNGs for enhancing private data security.

algorithms and predetermined seeds, are widely used for current data encryption systems, it is becoming increasingly vulnerable due to advances in computing power and machine learning, as shown in Figure 1 [10–12]. In contrast, true random number generators (TRNGs) can provide unpredictable sequences of random numbers by exploiting their intrinsic stochasticity at the hardware level [13–15]. Therefore, many researchers have focused on developing TRNGs using various materials and device architectures.

2D materials-based memristors, which depict a vertically stacked two-terminal sandwich structure, hold significant promise as emerging electronic devices due to their many advantages, including excellent scalability, compatibility with CMOS technology, low power consumption, and fast switching speeds [16–21]. In addition, the coexistence of volatile and nonvolatile memory characteristics depending on the electrode composition allows it for various applications such as next-generation memory devices, logic circuits, neuromorphic computing, etc [22–25]. Despite these properties, the formation of conductive filaments through defects or grain boundaries and the variability in the fabrication process lead to the inherent performance fluctuations, including variations in set/reset voltages, current instability, and delay time, observed in both cycle-to-cycle (C-to-C) and device-to-device (D-to-D) operations, hindering the commercialization of memristors [26, 27]. Nevertheless, this intrinsic randomness of memristors can be harnessed as an entropy source for TRNGs, offering a promising approach for hardware-based data encryption [10, 13, 15].

Numerous studies have been published about the investigation of TRNGs using the intrinsic stochastic characteristics of 2D materials-based memristors [28–30]. Wen et al. reported a highly stable TRNG circuit based on a multilayer hBN memristor integrated with peripheral circuits, where random telegraph noise (RTN) signals originated from confined native defects in the layered structure of hBN [31]. The generated random number sequences from the proposed TRNG passed all National Institute of Standards and Technology (NIST) randomness tests. Liu et al. investigated a high-performance TRNG using a Bi_2O_2Se memristor, in which RTN served as an entropy source [32]. The layered structure of Bi_2O_2Se facilitated stable RTN signals due to the spatial confinement of oxygen vacancies. The produced random bitstream was employed to implement the Diffie–Hellman Key Exchange protocol. However, the limited stability of RTN current signals and the requirement for multiple active components, such as a high-pass filter, a comparator, and a toggle flip-flop, have hindered the use of RTN as a reliable entropy source for TRNGs [33]. Consequently, the development of TRNGs based on other random sources remains necessary, but it still lacks investigation [34, 35].

Here, we demonstrate TRNG circuits that exploit the intrinsic stochastic behavior of a multilayer hBN volatile memristor. The fabricated device exhibits repeatable, low-voltage threshold switching characteristics with an ultrahigh on/off ratio. A spike generator, composed of a 2D hBN-based threshold switching memristor and passive components, exhibits stochastic behaviors in the delay time and output spike amplitude. By digitizing the output spike amplitudes with a comparator referenced to a fixed voltage, we obtain bitstreams without any postprocessing that successfully pass NIST SP 800-22 tests. The practical utility of the proposed TRNG is further validated by encrypting and decrypting black-and-white (B&W) and grayscale images via exclusive OR (XOR) logic operations using the generated keys. The encrypted images closely resemble random noise, confirming the effectiveness of the TRNG-based encryption, and reapplication of the XOR logic with the identical key restores the original images without data loss. These results shed light on the promising potential of threshold switching memristors based on 2D hBN in providing hardware-level randomness for next-generation data protection.

16163028, 2026, 22, Downloaded from https://advanced.onlinelibrary.wiley.com/doi/10.1002/adfm.202522597 by Ewha Womans University Library, Wiley Online Library on [30/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

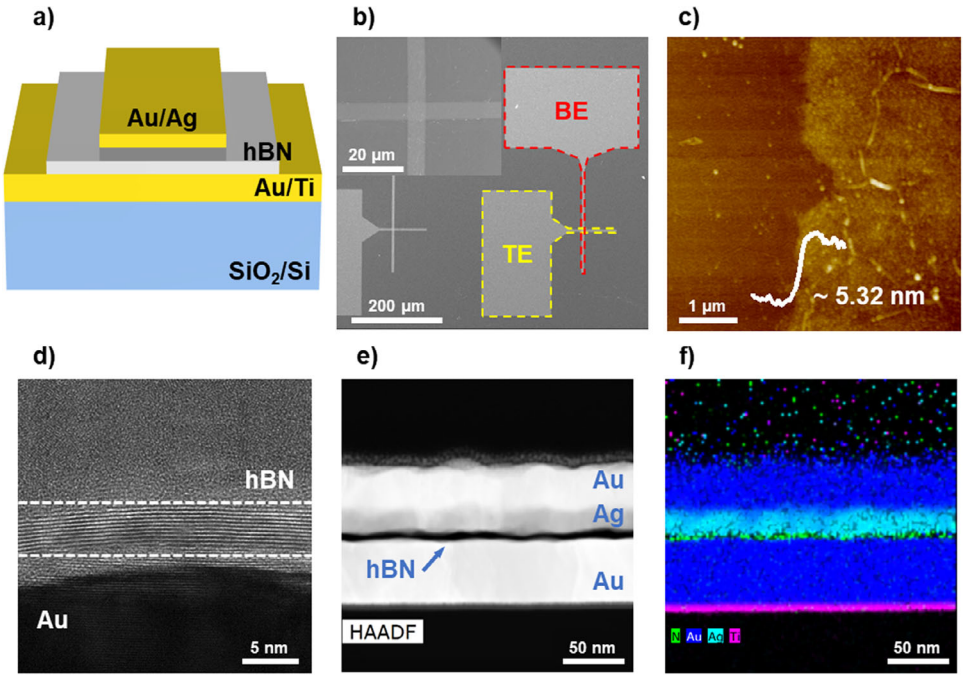


FIGURE 2 | Structural and morphological characterization of the fabricated hBN-based memristor. a) Schematic design of a volatile memristor based on a multilayer hBN. b) SEM image of the fabricated devices and a magnified view of the cross-point region (inset); scale bar: 200 and 20 μm, respectively. c) AFM image and d) cross-sectional TEM image of the multilayer hBN film; scale bar: 1 μm and 5 nm, respectively. e) STEM-HAADF image and f) corresponding EDS elemental mapping of the fabricated volatile memristor; scale bar: 50 nm.

2 | Results and discussions

Figure 2a provides a schematic illustration of the multilayer hBN-based volatile memristor device. The device exhibits a vertically arranged two-terminal structure, wherein the hBN active layer is placed between the top and bottom electrodes. The detailed methods used to fabricate this device are provided in the Experimental section. The surface morphology of the memristor was examined using scanning electron microscopy (SEM), as shown in Figure 2b. The bottom and top electrodes are indicated by red and yellow dashed lines, respectively, and the magnified image clearly shows wrinkles on the hBN surface near the cross-point region (inset of Figure 2b). Atomic force microscopy (AFM) measurements determined the thickness of the multilayer hBN film to be approximately 5.32 nm, as depicted in Figure 2c. Cross-sectional transmission electron microscopy (TEM) was utilized to reveal the layered structure of the hBN film, having a thickness of approximately 4.69 nm (13–15 atomic layers), consistent with the AFM measurements (Figure 2d). Figure 2e,f show scanning TEM (STEM) images obtained using high-angle annular dark-field (HAADF) detection, along with energy-dispersive X-ray spectroscopy (EDS) mapping, clearly demonstrating the well-defined multilayer structure consisting of the hBN active layer, Au/Ti bottom electrode, and Au/Ag top electrode on a SiO_2/Si substrate. Figure S1 provides additional EDS maps for each element.

Figure 3a presents the current–voltage (I–V) curve of the fabricated volatile memristor based on the multilayer hBN film. When we apply a voltage to the top electrode, the Ag ions are diffused into the hBN layer through the defects of the hBN, providing the diffusion path for the metal ions. As a result, the conductive filaments are formed and the device resistance can be switched. After the removal of the applied set voltage, the Ag filaments spontaneously break down and return to the metal clusters by minimizing the interfacial energy [5, 6, 36]. It clearly demonstrates the stable threshold switching behavior over 1,000 I–V cycles with a 1 μA compliance current. To evaluate the C-to-C variation, the distributions of set and hold voltages are shown in the inset of Figure 3a. The average values of set and hold voltages were calculated to be 0.22 ± 0.04 V (coefficient of variation, C_v = 0.18) and 0.03 ± 0.01 V (C_v = 0.33), respectively. Figure 3b,c illustrate the D-to-D variation via box plots and histograms derived from 100 I–V measurements performed on each of twenty distinct 2D hBN-based volatile memristors. The set and hold voltages were determined to be 0.26 ± 0.06 V (C_v = 0.23) and 0.04 ± 0.02 V (C_v = 0.50), respectively. The resistance values of the high resistance state (HRS) and the low resistance state (LRS) were measured at 0.1 V read voltage, as shown in Figure 3d. The fabricated devices exhibited remarkably high resistance in the HRS (Avg. 4.1 TΩ), and the calculated on/off ratio exceeded 10^7.

Figure 4a presents a circuit schematic of a spike generator used to demonstrate output spike firing behavior using the 2D hBN-based threshold switching memristor integrated with passive components. The detailed values of passive components are provided in Table S1. Upon the application of input voltage pulses, the leakage current through the volatile memristor remained negligible due to its high resistance in the HRS, resulting in an increase in membrane potential via capacitor charging. Once the membrane potential reached the threshold voltage of the device, it abruptly transitioned to a LRS, triggering the generation of an output spike as the accumulated charges in the capacitor were released.

16163028, 2026, 22, Downloaded from https://advanced.onlinelibrary.wiley.com/doi/10.1002/adfm.202522597 by Ewha Womans University Library, Wiley Online Library on [30/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

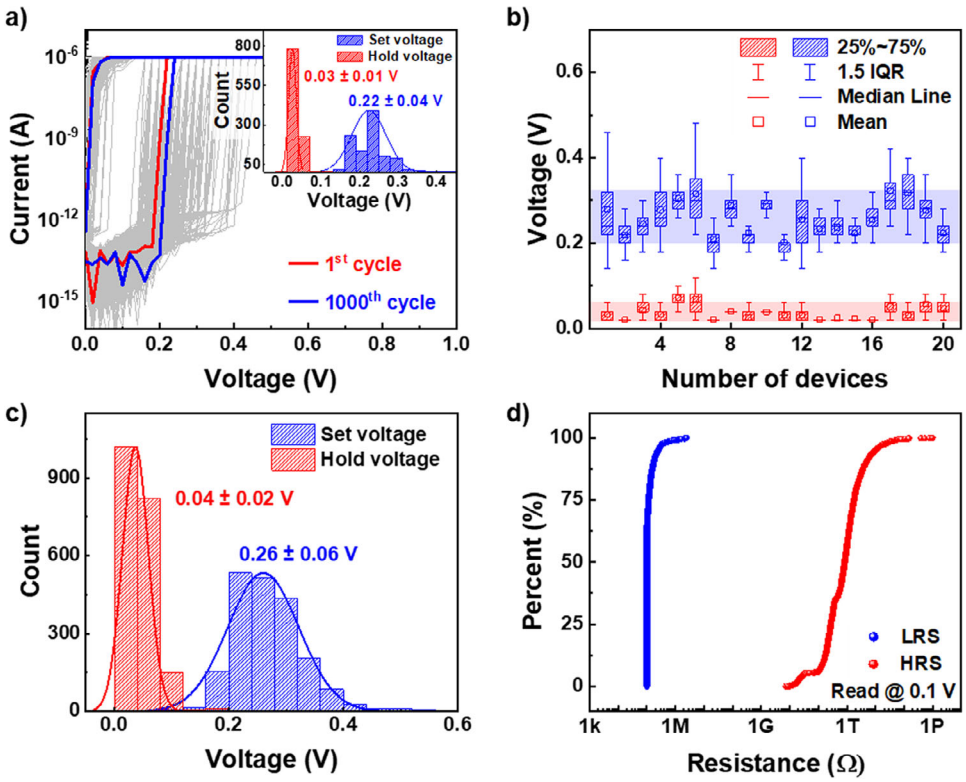


FIGURE 3 | Electrical performance of the 2D hBN-based volatile memristor. a) Representative I–V curve measured under a compliance current of 1 μA and corresponding histograms of the set and hold voltages over 1,000 IV cycles of a single device (inset). b) Box plots and c) histograms of the set and hold voltages obtained from 100 IV measurements for each of 20 distinct 2D hBN-based volatile memristors. d) Cumulative distribution of resistance values for both the LRS and HRS at a read voltage of 0.1 V.

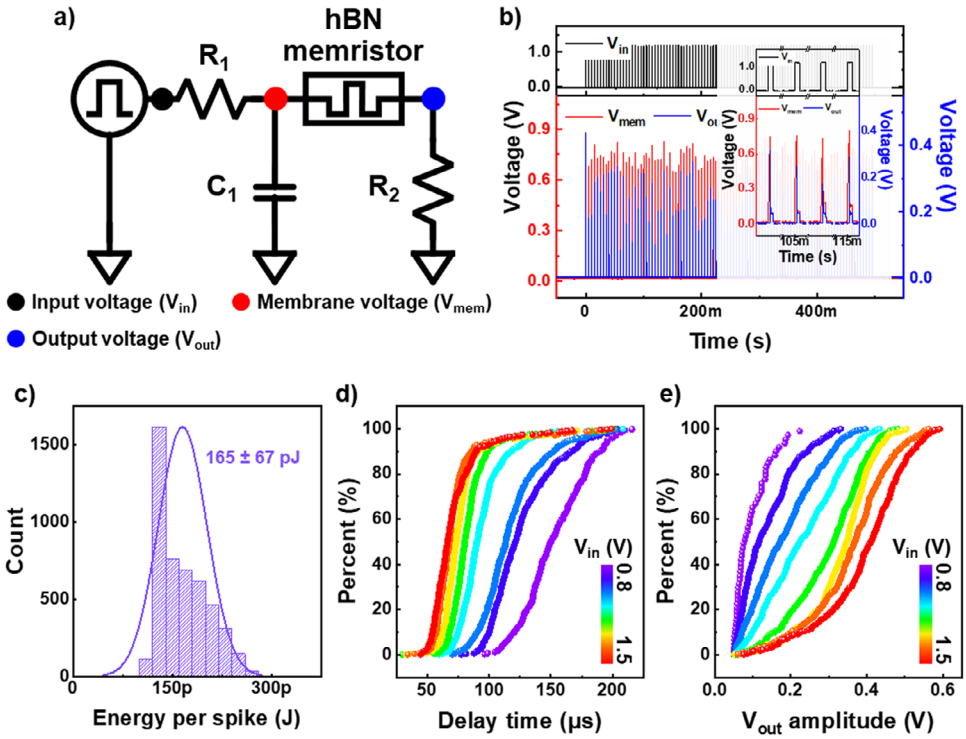


FIGURE 4 | Performance of the spike generator. a) Schematic circuit diagram of a spike generator comprising an hBN-based threshold switching memristor integrated with passive components. b) Electrical time transient graph of output spike generation in response to an input voltage pulse train. c) Calculated energy consumption per output spike. Cumulative distribution of d) delay time and e) output spike amplitude as a function of the input voltage amplitude.

16163028, 2026, 22, Downloaded from https://advanced.onlinelibrary.wiley.com/doi/10.1002/adfm.202522597 by Ewha Womans University Library, Wiley Online Library on [30/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Following the spike firing, the membrane potential decreased because of the discharge of the capacitor, and the threshold switching device spontaneously returned to the HRS. Figure 4b shows the transient electrical response of the spike generator under the applied input voltage pulses, having 1.2 V amplitude, 200 μs pulse width, and 5 ms pulse period. The aforementioned operation was repeatedly observed under continuous application of input voltage pulses, as shown in the inset of Figure 4b. Figure 4c depicts the histogram of the energy consumption per output spike (E_{spike}), which was calculated as follows:

$$E_{spike} = \int P_{spike}(t)\,dt = \int V_{mem}(t) \times I_{out}(t)\,dt \quad (1)$$

where P_{spike} is the power consumption per output spike, V_{mem} is the membrane potential, and I_{out} is the output current. The calculated average energy consumption per spike was 165 ± 67 pJ. Figure 4d,e presents the probability plots illustrating the effect of input voltage pulse amplitude on the delay time and output spike amplitude, respectively. The corresponding histogram data can be found in Figure S2. As the amplitude of the input voltage pulse increased from 0.8 to 1.5 V, the median delay time decreased from 150.20 to 66.34 μs, while the median output spike amplitude increased from 0.08 to 0.41 V. It is noteworthy that both parameters exhibited inherent stochastic behavior even under identical input voltage pulse amplitudes, which enables the hBN-based threshold switching device to be used in TRNG applications. In the following section, we employed the amplitude distribution of the generated output spikes to design TRNG circuits based on the 2D hBN threshold switching memristor.

Figure 5a illustrates a schematic circuit diagram of the TRNG, which integrates the 2D hBN-based threshold switching memristor with passive components and a comparator. The spike generator, based on the 2D hBN volatile memristor integrated with passive components, produced output signals. A comparator was then employed to generate a bitstream by binarizing the output spikes using a specified reference voltage (V_{ref}). Figure 5b presents the transient electrical response of the TRNG circuit under input voltage pulses with an amplitude of 2.0 V, pulse width of 200 μs, and pulse period of 5 ms. The output spikes generated by the spike generator were digitized into binary values (e.g., "0" or "1") through the comparator with a reference voltage of 0.12 V. In Figure 5c, it clearly depicts representative "0101" and "1010" bitstreams from the 2D hBN-based TRNG circuit. Figure S3 provides additional examples of the generated bitstreams obtained from the same device. The 2D matrix barcode, consisting of 120 × 100 pixels, was constructed using the generated bitstreams, where the black and white squares represent "1" and "0", respectively, as shown in Figure 5d. Figure 5e shows the calculated turn-on rate of the TRNG circuit, resulting in a value of 49.52% based on 12,000 generated bits. Additional examples of 2D matrix barcode, each comprising 100 × 100 pixels and obtained from different threshold switching memristors based on a multilayer hBN, are demonstrated, as shown in Figure S4. The average turn-on rate was found to be 50.04 ± 3.60%, measured across ten distinct TRNG circuits. Figure 5f,g depict the histogram of generated numbers for each individual cycle and the cumulative results, respectively. To represent numerical values, four consecutive pulses were grouped with sequences from "0000" to "1111" corresponding to hexadecimal values "0" through "F". Each cycle consisted of 1,000 bits generated by the 2D hBN-based TRNG, resulting in a total of 250 numbers per cycle. The distribution of the generated numbers was approximately uniform, exhibiting a standard deviation (σ) of 0.41%.

The randomness of the generated bitstreams from the TRNG circuit based on the 2D hBN was analyzed by adopting the NIST randomness test suite [36]. A p-value greater than 0.001 in each test indicates that the generated bit sequences can be determined to be truly random numbers. The 2D hBN-based TRNG circuits passed eleven tests of NIST successfully without any postprocessing, as shown in Table 1. These results demonstrate that the proposed threshold switching device based on the multilayer hBN film can provide excellent randomness suitable for TRNG circuits, leading to applications for data encryption to secure information protection.

Figure 6a,b presents schematic diagrams illustrating data encryption and decryption processes using an exclusive OR (i.e., XOR) logic gate. This operation was simulated via software by utilizing a generated random key from TRNG circuits based on the measured output results of a 2D hBN threshold switching memristor. In an XOR logic operation, the output is "0" when both input bits are the same (e.g., "00" or "11"), and "1" when the input bits differ (i.e., "01" or "10"). For example, if the XOR logic gate receives the input data "101101" and the TRNG-generated random key "011001", the resulting encrypted output is "110110". Decryption can be performed by applying the same random key to the encrypted data using the XOR logic again, restoring the original input data. Figure 6c shows the image encryption and decryption process using a generated random key by the 2D hBN-based TRNG circuits, conducted through XOR logic operations. The black-and-white (B&W) image with a resolution of 256 × 256 pixels and a grayscale image with 90 × 90 pixels were used to demonstrate the data security process. In the B&W image, each pixel is represented by a single-bit binary value: "0" for black and "1" for white. For the grayscale image, the intensity of each pixel is denoted by an eight-bit binary number, with the higher values corresponding to the brighter pixels. Initially, both images were encrypted using a TRNG-generated random key through XOR logic operations, resulting in encrypted outputs that were visually indistinguishable from random noise. Subsequently, the original images were successfully recovered by applying XOR logic again using the identical random key, thereby completing the encryption–decryption cycle.

3 | Conclusion

In this study, we fabricated a volatile memristor based on a multilayer 2D hBN film to demonstrate TRNG circuits for data encryption applications. The fabricated volatile memristor exhibited stable threshold switching characteristics over 1,000 I–V cycles, with low set and hold voltages and a high on/off ratio exceeding 10^7. A spike generator was implemented using a 2D hBN-based threshold switching device integrated with passive components, producing continuous output spike signals in response to input voltage pulses. As the input pulse amplitude increased, the delay time of the output spike decreased, while the output spike amplitude increased. Additionally, both delay time and output spike amplitude depicted the probability distributions under the same amplitude of input voltage pulses because of

16163028, 2026, 22, Downloaded from https://advanced.onlinelibrary.wiley.com/doi/10.1002/adfm.202522597 by Ewha Womans University Library, Wiley Online Library on [30/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

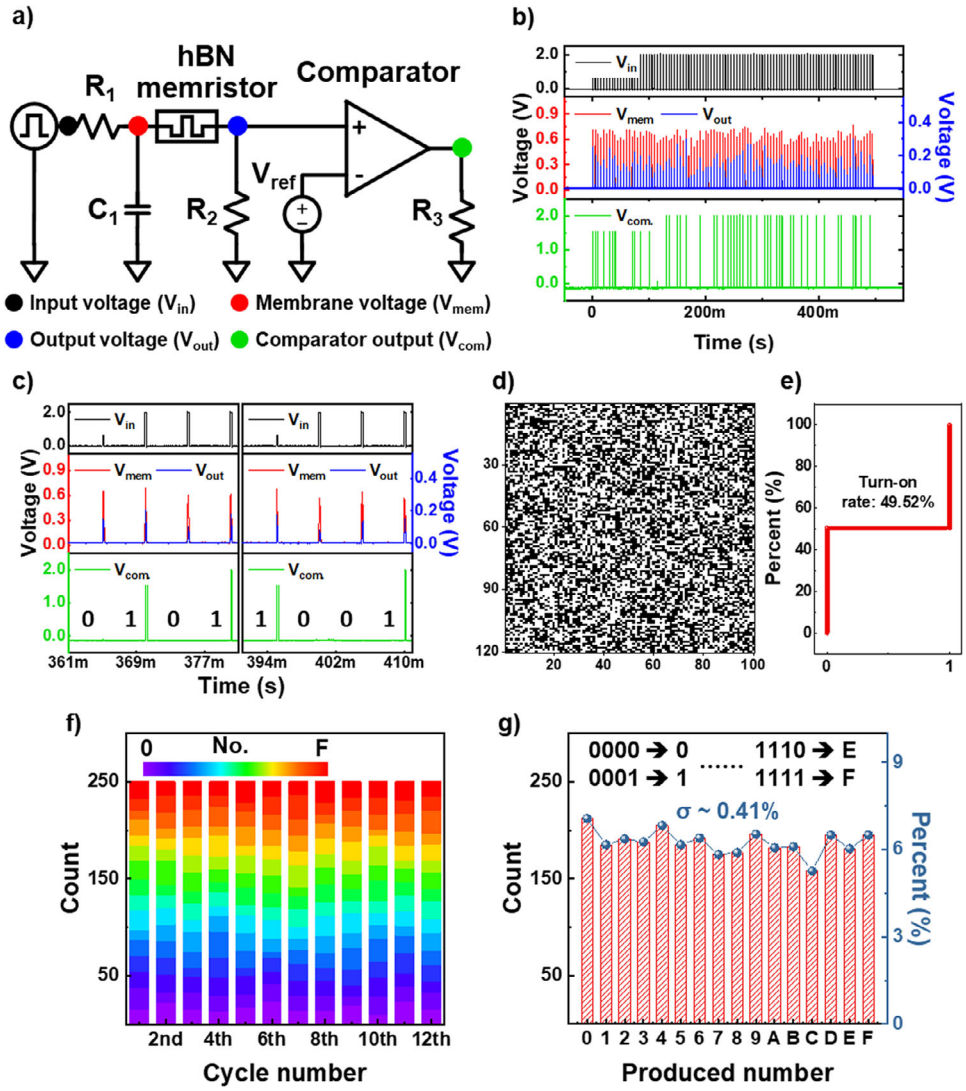


FIGURE 5 | Performance of the hBN memristor-based TRNG. a) Schematic circuit diagram of a TRNG consisting of a hBN-based spike generator and a comparator. b) Electrical time transient graph showing the conversion of output spikes into a bitstream using a comparator with a fixed-reference voltage. c) Representative example of generated bits, "0101" and "1001". d) 2D matrix barcode pattern and e) turn-on rate calculated from 12,000 generated bits. f) Histograms of generated numbers for each individual cycle and g) the corresponding cumulative distribution results.

TABLE 1 | Results of the NIST randomness test for bitstreams generated by the hBN memristor-based TRNG.

Statistical Test	*p*-value	Pass rate	Results
Monobit	0.010856	10/10	Pass
Frequency within block	0.266492	10/10	Pass
Runs	0.007275	10/10	Pass
Longest run ones in a block	0.004132	10/10	Pass
Discrete Fourier transform	0.081236	10/10	Pass
Non-overlapping template matching	0.964596	10/10	Pass
Serial test	0.001414	10/10	Pass
Approximate entropy	0.002498	10/10	Pass
Cumulative sums	0.012806	10/10	Pass
Random excursion	0.001628	10/10	Pass
Random excursion variant	0.016039	10/10	Pass

16163028, 2026, 22, Downloaded from https://advanced.onlinelibrary.wiley.com/doi/10.1002/adfm.202522597 by Ewha Womans University Library, Wiley Online Library on [30/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

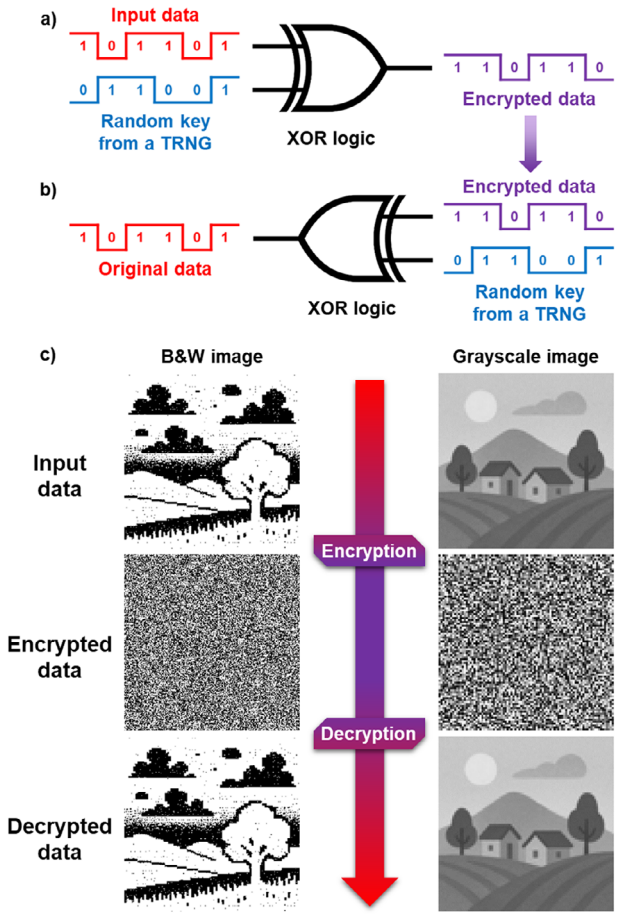


FIGURE 6 | Data encryption and decryption for information security. Schematic illustration of a) the data encryption and b) decryption process leveraging random keys generated by the hBN memristor-based TRNG through XOR logic operations. c) Encryption and decryption results for both black-and-white and grayscale images.

their intrinsic stochastic behavior of the device. We designed a TRNG circuit by integrating the 2D hBN-based spike generator with a comparator to generate bitstreams serving as random keys for data security. A specific reference voltage applied to the comparator was utilized to classify output spikes into binary bits. The randomness of the generated bit sequences was verified using the NIST statistical test suite, where our device passed eleven tests without postprocessing. Data encryption and decryption processes were demonstrated by applying XOR logic operations between the input data and the TRNG-generated random key via software simulation. Both B&W and grayscale images were successfully encrypted into unrecognizable, noise-like outputs and accurately restored to their original forms through XOR logic operations. These results highlight the potential of the 2D hBN-based threshold switching memristor for generating truly random keys and its promise for future data security applications.

4 | Experimental Section

4.1 | Fabrication of Volatile Memristors

Two-terminal volatile memristors were fabricated using multilayer hexagonal boron nitride (hBN) films grown via chemical vapor deposition (CVD), sourced from Graphene Supermarket. Silicon substrates with a 300 nm thermally grown SiO_2 layer were initially cleaned by ultrasonic treatment in acetone, isopropanol (IPA), and deionized (DI) water, each for 10 min. The bottom electrodes were patterned through photolithography, followed by electron-beam evaporation to deposit a 5 nm titanium adhesion layer and a subsequent 45 nm gold layer. Multilayer 2D hBN films were then transferred onto these substrates using a wet transfer technique involving a polymer support layer (Formvar, Alfa Aesar). The comprehensive details of the transfer process have been described in our previous publication [22]. Finally, the top electrodes, consisting of a 20 nm silver layer capped with a protective 30 nm gold layer, were fabricated using the same procedure applied to the bottom electrodes following the hBN film transfer.

4.2 | Electrical Measurement of the Fabricated Devices

The electrical properties of the volatile memristors were characterized using a semiconductor parameter analyzer (Keithley, 4200A-SCS) coupled with a probe station (MS Tech, M5VC). A waveform generator (Rigol, DG1022Z) was utilized to supply AC input signals, while membrane potentials and output responses were recorded using an oscilloscope (Tektronix, MSO58). All electrical measurements were performed under standard ambient conditions.

4.3 | Characterization Techniques

Scanning electron microscopy (SEM, FEI Nova Nano SEM 200) was employed to investigate the device morphology. Cross-sectional transmission electron microscopy (TEM) samples of the volatile memristors were prepared using focused ion beam (FIB) milling (Hitachi, NX5000). High-resolution TEM and scanning TEM (STEM) images, along with energy-dispersive X-ray spectroscopy (EDS) mapping, were obtained using Titan 80-300 and Talos F200X instruments, respectively, to clearly illustrate the layered structure of the multilayer 2D hBN and overall device architecture. The thickness of the transferred hBN films was determined using atomic force microscopy (AFM, Park Systems XE-70).

4.4 | Image Encryption and Decryption Procedure

Image encryption was performed by applying an XOR operation between bitstreams converted from the input images and random keys generated by the hBN-based TRNG. Black-and-white images were encoded using one bit per pixel, and grayscale images were encoded using 8-bit intensity values. The TRNG output was obtained experimentally through oscilloscope measurements and digitized using a comparator to produce a key bitstream of equal length. Encryption was carried out by computing for each bit, and decryption was performed using the same XOR operation with the identical random key used in encryption.

16163028, 2026, 22, Downloaded from https://advanced.onlinelibrary.wiley.com/doi/10.1002/adfm.202522597 by Ewha Womans University Library, Wiley Online Library on [30/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Acknowledgements

This work was supported by the National Research Foundation of Korea (NRF) (Grant Nos. RS-2023-00262880, RS-2024-00468995, and RS-2025-00517637).

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

1. M. H. Lee, J. H. J. Yun, A. Pyka, et al., "How to Respond to the Fourth Industrial Revolution, or the Second Information Technology Revolution? Dynamic New Combinations Between Technology, Market, and Society Through Open Innovation," *Journal of Open Innovation: Technology, Market, and Complexity* 4 (2018): 21, https://doi.org/10.3390/joitmc4030021.

2. B. Liu, J. Ma, H. H. Tai, et al., "Memristive True Random Number Generator with Intrinsic Two-Dimensional Physical Unclonable Function," *ACS Applied Electronic Materials* 5 (2023): 714–720, https://doi.org/10.1021/acsaelm.2c01533.

3. M. Capra, R. Peloso, G. Masera, M. R. Roch, and M. Martina, "Edge Computing: A Survey on the Hardware Requirements in the Internet of Things World," *Future Internet* 11 (2019): 100, https://doi.org/10.3390/fi11040100.

4. A. Wali, H. Ravichandran, and S. Das, "A 2D Cryptographic Hash Function Incorporating Homomorphic Encryption for Secure Digital Signatures," *Advanced Materials* 36 (2024): 2400661.

5. A. Doricchi, C. M. Platnich, A. Gimpel, et al., "Emerging Approaches to DNA Data Storage: Challenges and Prospects," *ACS Nano* 16 (2022): 17552–17571, https://doi.org/10.1021/acsnano.2c06748.

6. C. Ezekannagha, A. Becker, D. Heider, and G. Hattab, "Design Considerations for Advancing Data Storage with Synthetic DNA for Long-Term Archiving," *Materials Today Bio* 15 (2022): 100306, https://doi.org/10.1016/j.mtbio.2022.100306.

7. K. S. Woo, A. Zhang, A. Arabelo, et al., "True Random Number Generation Using the Spin Crossover in $LaCoO_3$," *Nature Communications* 15 (2024): 4656.

8. M. S. Equbal, T. Ketkar, and S. Sahay, "Hybrid CMOS-RRAM True Random Number Generator Exploiting Coupled Entropy Sources," *IEEE Transactions on Electron Devices* 70 (2023): 1061–1066, https://doi.org/10.1109/TED.2023.3241122.

9. Y. Qin, Z. Wang, Y. Yang, et al., "A High-Speed True Random Number Generator Based on Unified Selector-RRAM," *IEEE Electron Device Letters* 44 (2023): 1967–1970, https://doi.org/10.1109/LED.2023.3322992.

10. K. S. Woo, Y. Wang, Y. Kim, J. Kim, W. Kim, and C. S. Hwang *Adv Electron Mater* 6 (2020): 1, https://doi.org/10.1002/aelm.201901117.

11. H. Jiang, D. Belkin, S. E. Savel'Ev, et al., "A Novel True Random Number Generator Based on a Stochastic Diffusive Memristor," *Nature Communications* 8 (2017): 882.

12. G. Kim, J. H. In, Y. S. Kim, et al., "Self-Clocking Fast and Variation Tolerant True Random Number Generator Based on a Stochastic Mott Memristor," *Nature Communications* 12 (2021): 2906, https://doi.org/10.1038/s41467-021-23184-y.

13. M. S. Song, T. H. Kim, H. Hwang, S. Ahn, H. Nili, and H. Kim, "Optimization of Random Telegraph Noise Characteristics in Memristor for True Random Number Generator," *Advanced Intelligent Systems* 5 (2023): 2200358.

14. S. Il Kim, H. J. You, M. S. Kim, et al., "Cryptographic Transistor for True Random Number Generator with Low Power Consumption," *Science Advances* 10 (2024): eadk6042.

15. Y. Pang, B. Gao, B. Lin, H. Qian, and H. Wu, "Memristors for Hardware Security Applications," *Advanced Electronic Materials* 5 (2019): 1800872, https://doi.org/10.1002/aelm.201800872.

16. C. Liu, H. Chen, S. Wang, et al., "Two-Dimensional Materials for Next-Generation Computing Technologies," *Nature Nanotechnology* 15 (2020): 545–557, https://doi.org/10.1038/s41565-020-0724-3.

17. Y. Huang, Y. Gu, S. Mohan, et al., "Reliability Improvement and Effective Switching Layer Model of Thin-Film MoS_2 Memristors," *Advanced Functional Materials* 34 (2023): 2214250.

18. L. Liao, E. Kovalska, J. Regner, Q. Song, and Z. Sofer, "Two-Dimensional Van Der Waals Thin Film and Device," *Small* 20 (2024): 2303638.

19. Y. Jo, G. Noh, E. Park, et al., "Effects of Voltage Schemes on the Conductance Modulation of Artificial Synaptic Device Based on 2D hBN Memristor: Its Applications for Pattern Classifications," *Chaos, Solitons & Fractals* 187 (2024): 115390, https://doi.org/10.1016/j.chaos.2024.115390.

20. Y. Yu, M. Xiao, D. Fieser, W. Zhou, and A. Hu, "Nanoscale Memristor Devices: Materials, Fabrication, and Artificial Intelligence," *Journal of Materials Chemistry C* 12 (2024): 3770–3810, https://doi.org/10.1039/D3TC04510B.

21. D. K. Lee, G. Noh, S. Oh, et al., "Crystallinity-Controlled Volatility Tuning of ZrO_2 Memristor for Physical Reservoir Computing," *InfoMat* 7 (2025): 12635.

22. Y. Jo, D. Y. Woo, G. Noh, et al., "Hardware Implementation of Network Connectivity Relationships Using 2D hBN-Based Artificial Neuron and Synaptic Devices," *Advanced Functional Materials* 34 (2023): 2309058.

23. S. J. Yang, L. Liang, Y. Lee, et al., "Volatile and Nonvolatile Resistive Switching Coexistence in Conductive Point Hexagonal Boron Nitride Monolayer," *ACS Nano* 18 (2024): 3313–3322, https://doi.org/10.1021/acsnano.3c10068.

24. S. Chen, M. R. Mahmoodi, Y. Shi, et al., "Wafer-Scale Integration of Two-Dimensional Materials in High-Density Memristive Crossbar Arrays for Artificial Neural Networks," *Nature Electronics* 3 (2020): 638–645, https://doi.org/10.1038/s41928-020-00473-w.

25. Y. Shi, X. Liang, B. Yuan, et al., "Electronic Synapses made of Layered Two-Dimensional Materials," *Nature Electronics* 1 (2018): 458–465, https://doi.org/10.1038/s41928-018-0118-9.

26. Y. Liu, Y. Zhang, X. Zhou, et al., "High-Performing Nanofiber Memristor via Field-Induced Ion Migration Concentration at Highly-Curved Interwoven Interface," *Small* 21 (2025): 2409951.

27. Q. Tian, X. Zhao, X. Tang, et al., "An Artificial Nerve with Complementary Memristor for Neuromorphic Self-Protection," *Advanced Functional Materials* 35 (2025): 2507503.

28. Y. Liu, P. Liu, Y. Wen, et al., "Harnessing Physical Entropy Noise in Structurally Metastable 1T′ Molybdenum Ditelluride for True Random Number Generation," *Nano Letters* 24 (2024): 14315–14322, https://doi.org/10.1021/acs.nanolett.4c03957.

29. H. Xiang, Y. C. Chien, Y. Shi, and K. W. Ang, "Application of 2D Materials in Hardware Security for Internet-of-Things: Progress and Perspective," *Small Structures* 3 (2022): 2200060, https://doi.org/10.1002/sstr.202200060.

30. K. Zhu, G. Vescio, S. González-Torres, et al., "Inkjet-Printed h-BN Memristors for Hardware Security," *Nanoscale* 15 (2023): 9985–9992, https://doi.org/10.1039/D3NR00030C.

31. C. Wen, X. Li, T. Zanotti, et al., "Advanced Data Encryption Using Two-Dimensional Materials," *Advanced Materials* 33 (2021): 1002.

32. B. Liu, Y.-F. Chang, J. Li, et al., "Bi_2O_2 Se-Based True Random Number Generator for Security Applications," *ACS Nano* 16 (2022): 6847–6857, https://doi.org/10.1021/acsnano.2c01784.

16163028, 2026, 22, Downloaded from https://advanced.onlinelibrary.wiley.com/doi/10.1002/adfm.202522597 by Ewha Womans University Library, Wiley Online Library on [30/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

33. A. Wali and S. Das, "Hardware and Information Security Primitives Based on 2D Materials and Devices," *Advanced Materials* 35 (2023): 2205365, https://doi.org/10.1002/adma.202205365.

34. X. Xing, S. Huang, Y. Gong, et al., "Stochastic Current Response in Diffusive Memristor for Security Applications," *Mater Today Nano* 22 (2023): 100315.

35. W. Choi, O. Kwon, J. Lee, et al., "Volatile Threshold Switching Devices for Hardware Security Primitives: Exploiting Intrinsic Variability as an Entropy Source," *Applied Physics Reviews* 11 (2024): 21323.

36. L. E. Bassham, A. L. Rukhin, J. Soto, et al., *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, Vol. 26, Gaithersburg, MD, 2010, https://doi.org/10.6028/NIST.SP.800-22r1a.

Supporting Information

Additional supporting information can be found online in the Supporting Information section.

Supporting File: adfm74080-sup-0001-SuppMat.docx.

16163028, 2026, 22, Downloaded from https://advanced.onlinelibrary.wiley.com/doi/10.1002/adfm.202522597 by Ewha Womans University Library, Wiley Online Library on [30/09/2026]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License