SUPPLEMENTARY INFORMATION OF THE MANUSCRIPT

Hardware implementation of a true random number generator integrating a hexagonal boron nitride memristor with a commercial microcontroller

Sebastian Pazos[1-2], Wenwen Zheng[1,3], Thales Becker[4], Tommaso Zanotti[5], Fernando Aguirre[1], Yaqing Shen[1,3], Kaichen Zhu[6], Yue Yuan[1], Gilson Wirth[4], Francesco Maria Puglisi[5], Juan Bautista Roldán[7], Felix Palumbo[2], and Mario Lanza[1]*

[1] Physical Science and Engineering Division, King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia
[2] Unidad de Investigación y Desarrollo de las Ingenierías-CONICET, Facultad Regional, Buenos Aires, Universidad Tecnológica Nacional (UIDI-CONICET/FRBA-UTN), Medrano 951 (C1179AAQ), Buenos Aires, Argentina.
[3] Institute of Functional Nano & Soft Materials (FUNSOM), Collaborative Innovation Center of Suzhou Nanoscience and Technology, Soochow University, 199 Ren-Ai Road, Suzhou 215123, China
[4] Electrical Engineering Department, Federal University of Rio Grande do Sul, Porto Alegre, 90035-190, Brazil
[5] Dipartimento di Ingegneria "Enzo Ferrari", Università di Modena e Reggio Emilia, Modena, 41125, Italy
[6] MIND, Department of Electronic and Biomedical Engineering, Universitat de Barcelona, Martí i Franquès 1, E-08028 Barcelona, Spain
[7] Departamento de Electrónica y Tecnología de Computadores, Facultad de Ciencias, Universidad de Granada, Avd. Fuentenueva s/n, 18071 Granada, Spain

Corresponding author email: mario.lanza@kaust.edu.sa

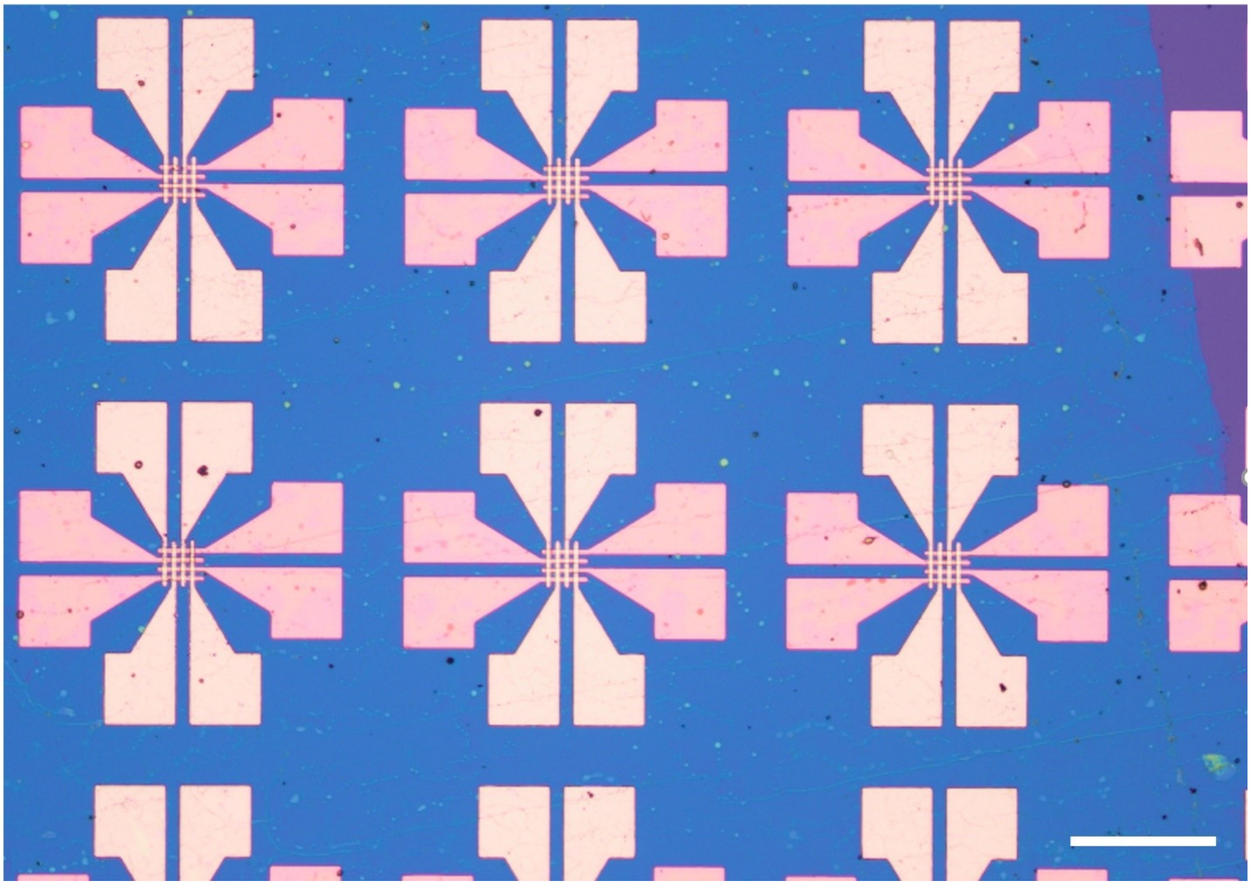
Ref.	Entropy source	Implementation	Conditioning block	Post-processing	Output Bitrate	Power/Energy overhead	NIST
OUR WORK	· **h-BN based memristor** · **RTN**, wide current range. · Volatile switching.	**Experimental** Low cost, Fully COTS, Arduino Python (PC only for demonstration)	TIA + PWM filters + Comparator or ADC	19-bit NLFSR (or longer)	**High** **>7.8 Mbps** (30 Kbps w/PC log)	**Max. overhead** **Very Low** ~ 10 μW	**PASS** p > .001 15/15 > 5Mbit bitstreams
Gao 2022[1]	1T1R TaOx Noise (including **RTN**)	40 nm **1T1R crossbar** + **FPGA**	Voltage divider + Volt amplif.	ADC truncate	**High** 1.5 Mbps/ES	**Low**	**PASS** 15/15
Yeh 2019[2]	4T2R SRAM with **RTN** from paired CRRAM	Allegedly 28 nm CMOS, external CRRAM, unclear implementation	SRAM cell with trimming using Self-Aligned Nitride devices (non-convent.)	None (at low throughput)	**Low** 1 Kbps (max. per cell)	**Low**	**10/15 shown**
Tseng 2021[3]	**Suggests** ReRAM **RTN**, but not shown nor simulated	WOx ReRAM 180 nm, **no implementation nor simulation**	Not specified but required	LFSR	N/A (allegedly Gbps)	N/A	15/15 but not from the full TRNG
Wen 2021[4]	Ni/h-BN/Au memristor **RTN**	**Simulations only**	TIA + AC Coupling + Comparator	Latch + NLFSR	**High** 1 Mbps	**Low**	**PASS** 15/15
Huang 2012[5]	1T-1R CR-RAM **RTN**	**Experimental** CMOS Vref ~mV	Comparator + D-FF	None or LFSR for high throughput	**Low** 1 Kbps	N/A	5 tests shown
Wei 2017[6]	TaOx **1T1R array** Noise (**RTN** or other) in LRS	**Experimental** CMOS RRAM demonstrator	TSA + RTC + readout of array (current difference)	Not described Uses array peripherals	**High** 32 Mbps (multiple devices)	**Low** 0.4 nJ/bit	**PASS** 1Mbit streams
Vasileiadis 2021[7]	SiO2/SiN read noise (include **RTN**)	**Lab equipment + labview +** COTS	TIA + Comp	XOR + Shift (up to 40 D-FF)	N/A	**Low**	FIPS 140-2
Yang 2016[8]	AlOx Wox **1T1R array RTN**	**Experimental** CMOS implementation	Ring oscillators + comparators	Large CMOS architecture + Von Neumann	N/A	N/A	**10/15 shown**
Govindaraj 2018[9]	**Switching + RTN**	**Simulation only** CMOS	Curr starved Ring Osc	None	**High** 6 Mbps	**Very Low** 22.8 fJ/bit	**PASS** 15/15
Wang 2015[10]	TiOx MIM **Switching**	**Simulations only**	6T + D-FF	XOR + D-FF	**High** 1 Gbps	Regular 31 uW	N/A
Balatti 2015[11]	1T1R **Switching**	**Simulations only**	CMOS Inverter	None	1 Mbps **unproven**	High Only 10s shown	N/A
Balatti 2016[12]	1T1R **Switching**	**Simulations only**	CMOS Comparators	Von Neumann (costly)	N/A	High Only 10s shown	**14/15 tests shown**
Sahay 2017[13]	1T2R **Switch time**	**Simulations only**	CMOS analog condit. + ADC	N/A	N/A <10 Kbps	High 100s shown	N/A
Jiang 2017[14]	Ag/SiO_2 **Switching**	**Experimental** COTS + **Lab equipment**	Divider + Comparator + Counter	None	**Low** 6 Kbps	**N/A** Expected Low	15/15 p > .0001

Zhang 2017[15]	TaOx paired memristors **Switching**	**Lab equipment** Not implement	Comparator + complex read scheme	N/A	N/A	**Large (mA),** high V forming	**PASS** 15/15
Woo 2019[16]	HfO_2 paired memristors **thresh. switch**	**Lab equipment** Not implement	AND + Counter + Pulsed write	None	**Low** 3 Kbps	Low (nA) **high volt (6V)**	**8/15 shown** $p > .0001$
Woo 2020[17]	HfO_2 paired memristors **thresh. switch**	Experimental COTS + **Lab Equipment**	Previous + NLFSR	NLFSR	Regular 16 Kbps	Low (nA) **high volt (10V)**	15/15 $p > .0001$
Woo 2021[18]	Cu_xTe_{1-x}/HfO_2 paired memris. **thresh. switch**	COTS + **Lab Equipment**	Identical to Woo 2020	NLFSR	**High** 32 Kbps	Low (10 nA) **high volt (8V)**	**PASS** 15/15 $p >.0001$
Aziza 2020[19]	1T1R HfO_2 array HRS variability **Switching**	**Lab equipment** + probe card, slow and complex	Array readout circuitry	LFSR + XOR	**Very low** (42 kbits in 1 week)	**Very High** (up to mA)	12/15 after post-proc.
Hagras 2020[20]	**Emulated** chaotic memristor	FPGA chaotic implementation	FPGA	FPGA filter	**High**	**Very High**	**PASS**
Kim 2021[21]	NbOx Relax. Times **Switching**	**Lab Equipment** + COTS	Voltage divider + Volt amplif.	T-FF	**High** 40 Kbps	**Very High** (low endurance)	**PASS**
Yang 2021[22]	FinFET Pulse count until reset **Switching**	**Lab equipment**	Voltage divider + comparator	Counter	**N/A**	**Low**	**11/15 shown**
Gu 2021[23]	1T1R NbOx relaxation **Switching**	OSC meas + **Simulations**	Comparator + D-FF	None	**High** 500 Kbps	**High** (low endurance)	**8/15 shown 50 Kbits**
Lin 2020[24]	4Kbit 1T1R HfOx read disturbance	Device charact. + TRNG model **(behavioural Simulations)**	Sample & hold + Comparator Pulsed write/read	Uses array peripherals	**Very High** 230 Mbps (parallel.)	**N/A** Expected High	**15/15**
Lin 2019[25]	1T1R HfOx **Switching** pulse count	Device Write/Verify experiment data	N/A	Uses array peripherals	**High** 1 Mbps	**Only power of RRAM considered 3.72 pJ/bit**	**15/15**
Yang 2020[26]	1T1R NOR Resist. Gate FinFET array	Memory array measurements + post process	Comparator + D-FF string	Uses array peripherals + XNOR	**Very High** 62.5 Mbps	**N/A Cell current reaches 10 µA**	**15/15**

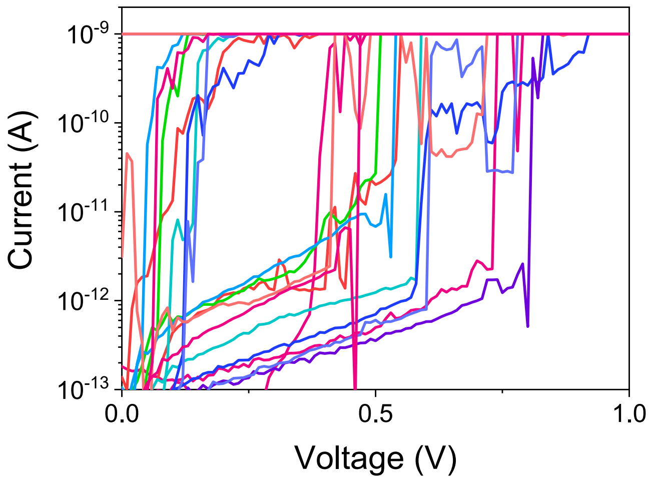
Supplementary Table 1 | Characteristics of representative resistive RAM TRNG reported in the literature. A comparison of the main characteristics of TRNG circuits that use different characteristics of resistive RAM as entropy source. While multiple works use only simulations at the circuit level to demonstrate functionality after performing some characterization at the device level, those that show hardware implementations often rely on laboratory equipment (stan-alone) or vast resources (as RRAM 1T1R arrays, costly post-processing or FPGAs). Our work offers a low-cost, practical implementation that is affordable and of potential integration directly into IoT applications, with competitive performance and boosted by the unique characteristics of carefully engineered h-BN based memristors. In the table, the green highlights are advantages, and the red highlights are disadvantages.

Ref.	RTN source	Maximum RTN ratio reported
OUR WORK	Ag Ink/Multilayer h-BN/Ag memristor RTN	**Max 2.57,** Avg. 1.69, Min. 1.28
Gao 2022[1]	1T1R TaOx Noise (including **RTN**)	16.5 uA / 15.5 uA = 1.0645
Yeh 2019[2]	4T2R SRAM with **RTN** from paired CRRAM	Max. 8% = 1.08
Tseng 2021[3]	ReRAM **RTN**	90K / 80 K = 1.125
Wen 2021[4]	Ni/h-BN/Au memristor **RTN**	204 nA / 200 nA = 1.02
Huang 2012[5]	1T-1R CR-RAM **RTN**	0.15 V / 0.12 V = 1.25
Wei 2017[6]	TaOx **1T1R array** Noise (**RTN** or other) in LRS	44 uA / 42 uA = 1.0476
Vasileiadis 2021[7]	SiO2/SiN read noise (include **RTN)**	420 nA / 380 nA = 1.1053
Yang 2016[8]	AlOx Wox **1T1R array RTN**	1.15 V / 0.8 V = 1.4375
Govindaraj 2018[9]	**Switching + RTN**	37 nA / 32 nA = 1.15

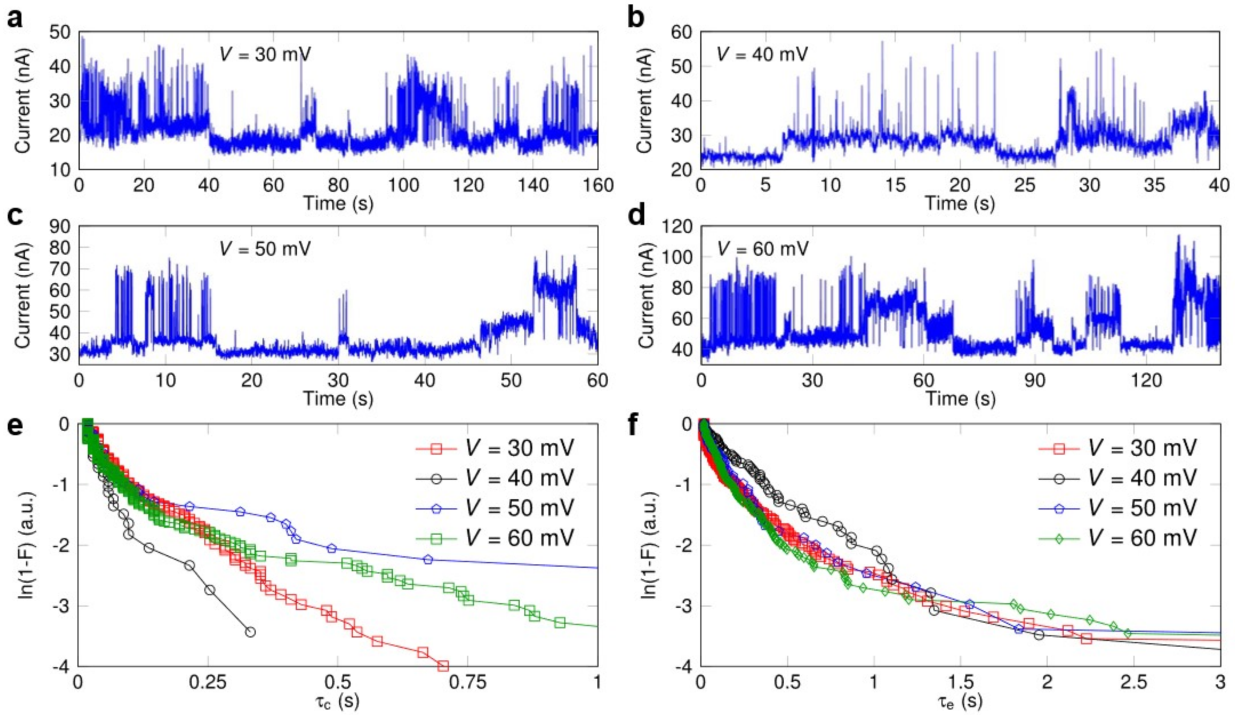
Supplementary Table 2 | RTN ratio of Ag Ink/h-BN/Ag memristors in comparison to other devices used in RTN-based TRNG. For other proposed TRNG based on RTN generated by memristors, most works don't show a full analysis of the experimental RTN signals generated by the devices. From the short experimental traces shown by most of them, we extracted the maximum observed RTN ratio, whereas this is current in 1R devices or voltage in 1T1R cells. Our work shows that in our Ag Ink/h-BN/Ag devices, the minimum ratio observed from all the RTN transitions in a >1 hour long trace (see Figure 2a) is inferior to only one report[8], while the mean and the maximum observed ratios are well above all the proposed devices in the literature, highlighting a clear advantage of our device in terms of RTN signal quality.



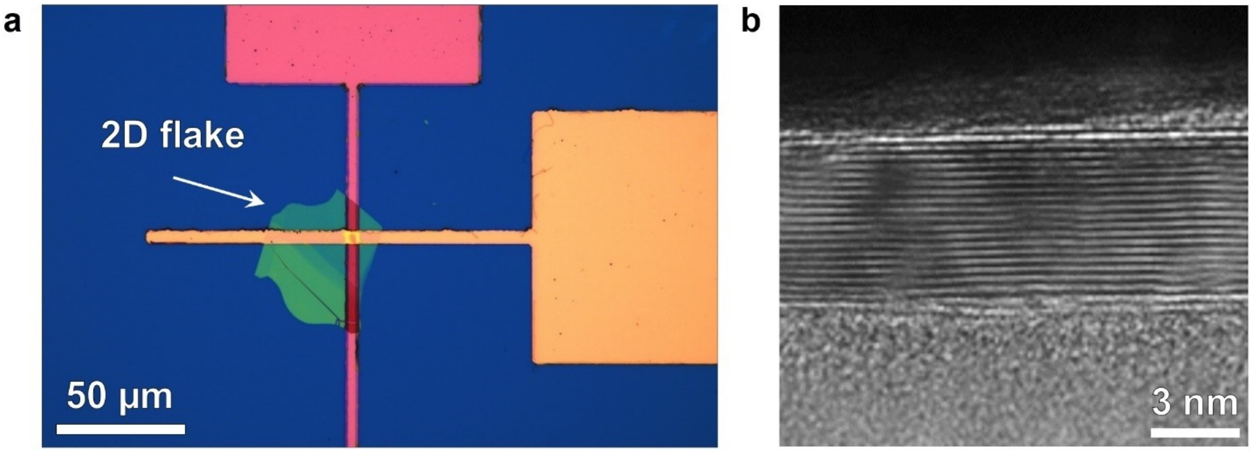
Supplementary Figure 1 | Compatibility of the fabrication process with large-area circuit fabrication. Top-view optical microscope image of a SiO_2 wafer with multiple crossbar arrays of h-BN memristors patterned on it. The purple colour at the top-right part of the image is the SiO_2, and the rest of the image is covered by the h-BN, which appears to be blue given its ~6 nm thickness. This confirms the absence of cracks for a large portion of the h-BN. The scale bar is 200 µm. This image confirms that this fabrication process is suitable for the large-area fabrication of solid-state micro/nano-electronic circuits.



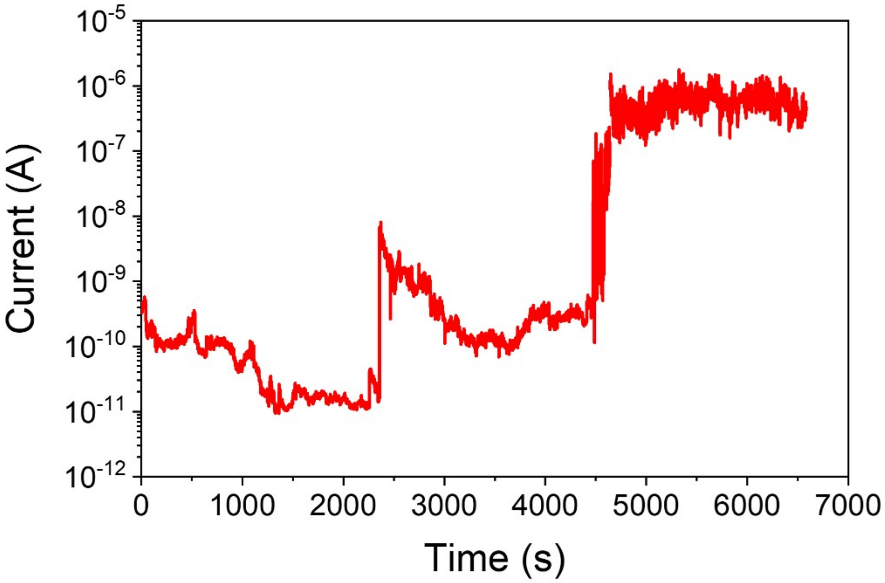
Supplementary Figure 2 | Current-voltage (I-V) characteristics of Ag/h-BN/Ag devices. Typical I-V curves for 10 devices acquired under a current limitation of 1 nA. Between 0.5 V and 1 V, a clear increase in current is observed, ascribed to the breakdown of the insulator through an intrinsically defective region in the h-BN.



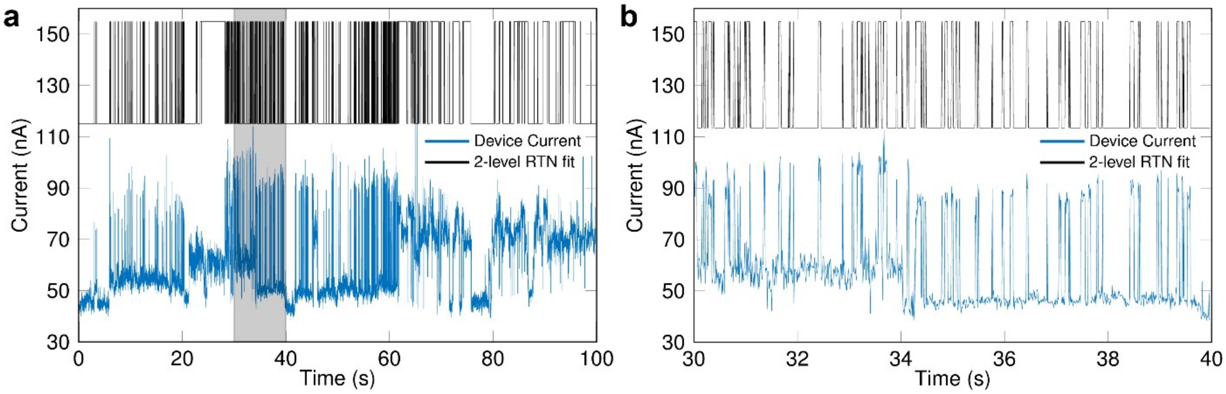
Supplementary Figure 3 | RTN signals at different applied voltages in Ag/h-BN/Ag devices. a, b, c, d, RTN characteristics obtained at different voltages, from 30 mV to 60 mV of the same sample from Figure 2. RTN signal is rather more unstable than at 70 mV but is still observed in all cases. **e, f**, Capture and emission times, respectively, for all the applied voltages. While capture times are sensitive to the applied voltage, emission times are distributed very similarly for all bias conditions.



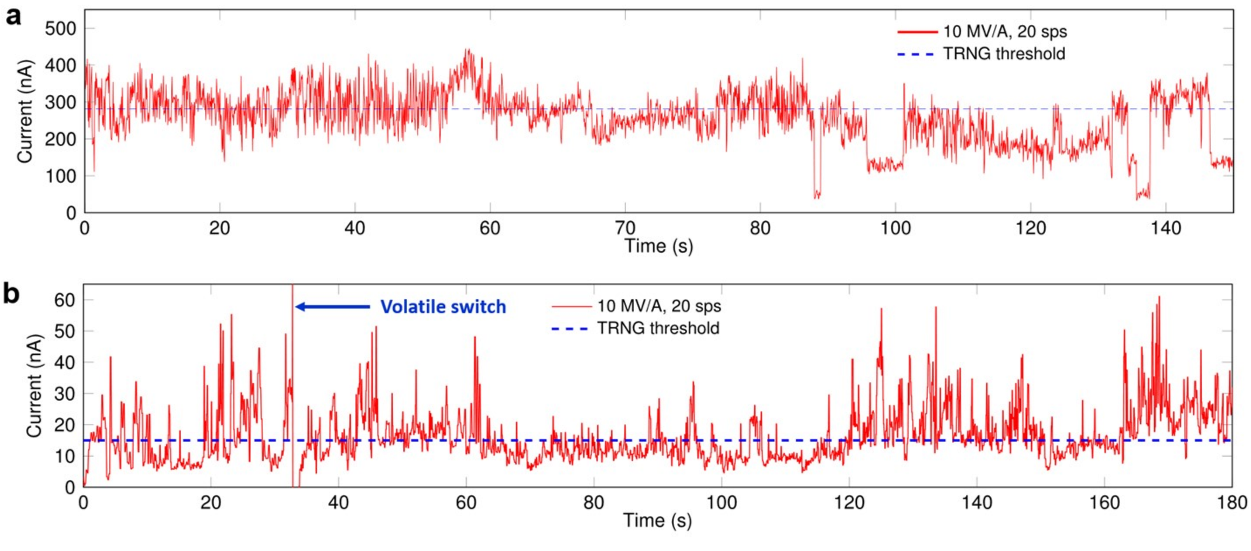
Supplementary Figure 4 | Structure of the mechanically exfoliated Au/h-BN/Au devices. a, Top-view optical microscope image of an Au/h-BN/Au device. **b**, Cross-sectional TEM image of the h-BN stack, proving that (unlike CVD-grown h-BN) its layered structure is free of defects. This image also serves to confirm that the defects observed in the CVD-grown h-BN stack are not produced by the focused ion beam cut for sample preparation. h-BN thickness is around 6 nm, and the number of visible layers is 16~18, consistent with a 0.33 nm atomic layer thickness in h-BN.



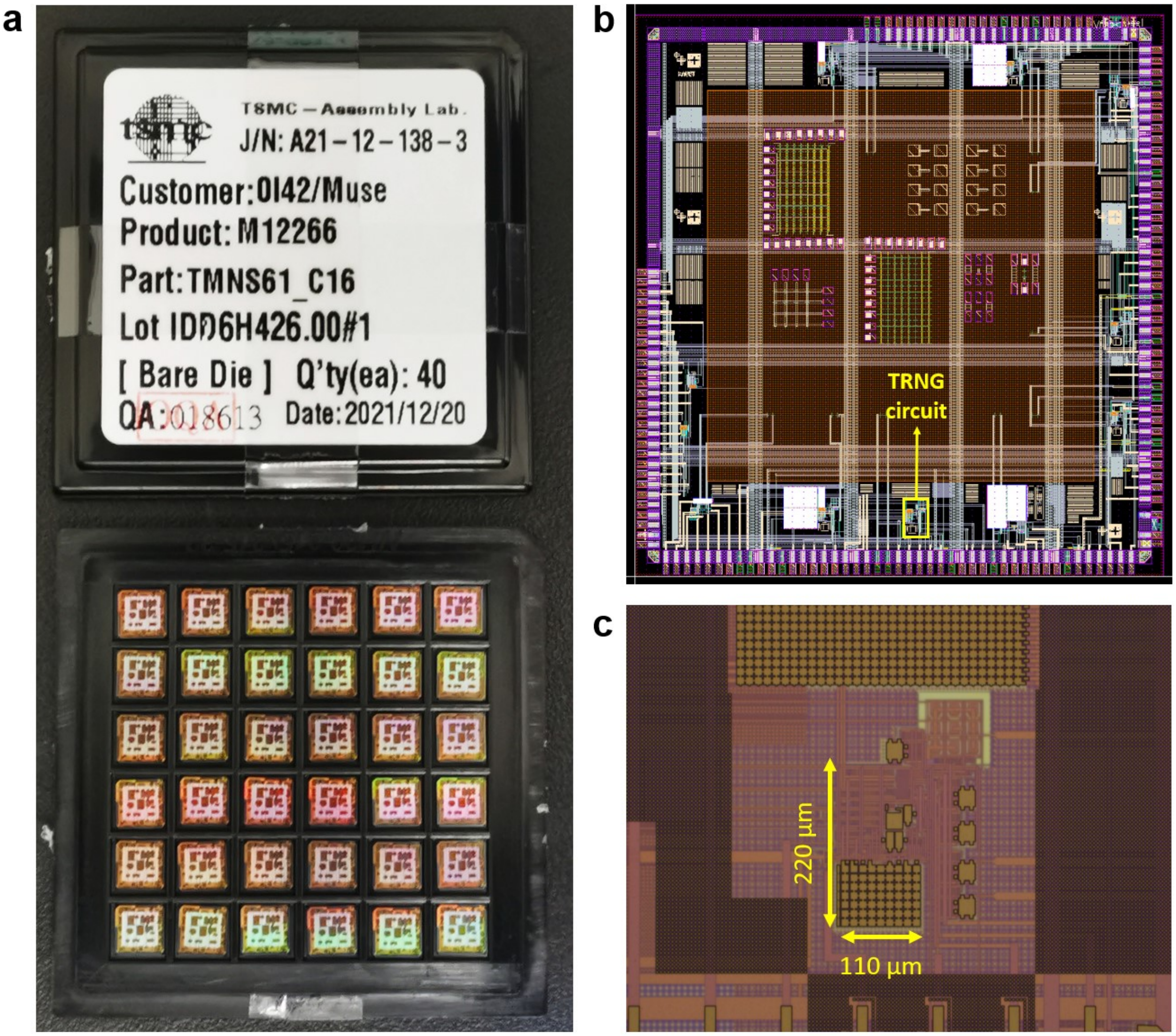
Supplementary Figure 5 | Constant voltage stress on exfoliated h-BN. Characteristic I-t curve of an h-BN dielectric fabricated through the exfoliation method. Note that there is no progressive increase in the current under CVS. Eventually, an abrupt current increase triggers the layer-by-layer dielectric breakdown, in agreement with previous observations.



Supplementary Figure 6 | Analysis of RTN dynamics based on a Hidden Markov Model. a, Reconstruction of an ideal RTN signal (black, displaced to higher values in current axis for clarity) from a 100 second interval extracted the measurements (blue) of Figure 2a, to extract capture and emission times. **b,** detailed view of a 10 second interval were excellent fit to the subjacent RTN signal is observed. From this reconstruction, capture (τ_c) and emission (τ_e) times can be calculated after each abrupt change in the RTN signal and organized into an exponential density plot *ln(1-F)* vs. time, where *F* is the cumulative distribution function. In such representation, a straight line corresponds to an ideal exponential distribution for the values of τ_c and τ_e. Such results are displayed in Figure 2d and in Supplementary Figure 2e. In all cases, the same methodology is used.



Supplementary Figure 7 | Signals used as entropy sources for reliable TRNG. a, Example of an RTN signal from a different device, with significant flicker noise density superimposed, as captured by the Arduino microcontroller. **b**, A device showing RTN together with large current variations (spikes) under an volatile switching regime at an applied voltage of 1.5 V, also as captured by the Arduino microcontroller when used as entropy source. If the current reaches the TIA limitation, the proposed system interprets this as a conductance change and lowers the applied voltage to zero (aided by the bipolar transistor in Figure 3a as a discharge path for the PWM filter) for a short period of time (see abrupt change around 35 seconds pointed by the blue arrow). The device recovers its previous conductance state and the random number generation is never interrupted, showing results as good as in the case of RTN signals as entropy sources (see Figure 4).



Supplementary Figure 8 | 180 nm CMOS implementation of the TRNG conditioning circuit. a, Photograph of the box received from TSMC including the 5 mm × 5 mm microchips containing multiple types of circuits; one of them is the TRNG circuit presented in Figure 3. **b**, Layout of the microchip designed using the software from Synopsys. The analogue front-end (including TIA, high pass filters, feedback loop and passives) of an integrated version of the proposed TRNG is enclosed in yellow. **c**, Detailed photograph under the optical microscope of the analogue front-end for the TRNG circuit enclosed in yellow in panel **b**. The implementation also includes an embedded 24-bit NLFSR (not shown) and a configurable comparator that triggers the re-seed of the NLFSR. Total conditioning circuit area is roughly 220 µm × 110 µm = 0.024 mm^2, including passive components.

Supplementary references

1. Gao, B. *et al.* A Unified PUF and TRNG Design Based on 40-nm RRAM with High Entropy and Robustness for IoT Security. *IEEE Trans. Electron Devices* **69**, 536–542 (2022).
2. Yeh, P. S. *et al.* Self-Convergent Trimming SRAM True Random Number Generation with In-Cell Storage. *IEEE J. Solid-State Circuits* **54**, 2614–2621 (2019).
3. Tseng, P. H. *et al.* ReRAM-Based Pseudo-True Random Number Generator with High Throughput and Unpredictability Characteristics. *IEEE Trans. Electron Devices* **68**, 1593–1597 (2021).
4. Wen, C. *et al.* Advanced Data Encryption using 2D Materials. *Adv. Mater.* **33**, 2100185 (2021).
5. 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 Lett.* **33**, 1108–1110 (2012).
6. Wei, Z. *et al.* True random number generator using current difference based on a fractional stochastic model in 40-nm embedded ReRAM. *Tech. Dig. - Int. Electron Devices Meet. IEDM* 4.8.1-4.8.4 (2017) doi:10.1109/IEDM.2016.7838349.
7. Vasileiadis, N., Dimitrakis, P., Ntinas, V. & Sirakoulis, G. C. True random number generator based on multi-state silicon nitride memristor entropy sources combination. *2021 Int. Conf. Electron. Information, Commun. ICEIC 2021* (2021) doi:10.1109/ICEIC51217.2021.9369817.
8. Yang, J. *et al.* A low cost and high reliability true random number generator based on resistive random access memory. *Proc. - 2015 IEEE 11th Int. Conf. ASIC, ASICON 2015* (2016) doi:10.1109/ASICON.2015.7516996.
9. Govindaraj, R., Ghosh, S. & Katkoori, S. CSRO-Based Reconfigurable True Random Number Generator Using RRAM. *IEEE Trans. Very Large Scale Integr. Syst.* **26**, 2661–2670 (2018).
10. Gupta, S. K., Sonvane, Y., Wang, G. & Pandey, R. Size and edge roughness effects on thermal conductivity of pristine antimonene allotropes. *Chem. Phys. Lett.* **641**, 169–172 (2015).
11. Balatti, S., Ambrogio, S., Wang, Z. & Ielmini, D. True random number generation by variability of resistive switching in oxide-based devices. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **5**, 214–221 (2015).
12. Balatti, S. *et al.* Physical unbiased generation of random numbers with coupled resistive switching devices. *IEEE Trans. Electron Devices* **63**, 2029–2035 (2016).
13. Sahay, S. & Suri, M. Recent trends in hardware security exploiting hybrid CMOS-resistive memory circuits. *Semicond. Sci. Technol.* **32**, 123001 (2017).
14. Jiang, H. *et al.* A novel true random number generator based on a stochastic diffusive memristor. *Nat. Commun.* **8**, 1–9 (2017).
15. Zhang, T. *et al.* High-speed true random number generation based on paired memristors for security electronics. *Nanotechnology* **28**, 455202 (2017).
16. Woo, K. S. *et al.* A True Random Number Generator Using Threshold-Switching-Based Memristors in an Efficient Circuit Design. *Adv. Electron. Mater.* **5**, 1800543 (2019).
17. 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. *Adv. Electron. Mater.* **6**, 1901117 (2020).
18. Woo, K. S. *et al.* A High-Speed True Random Number Generator Based on a CuxTe1−x Diffusive Memristor. *Adv. Intell. Syst.* **3**, 2100062 (2021).
19. Aziza, H. *et al.* True Random Number Generator Integration in a Resistive RAM Memory Array Using Input Current Limitation. *IEEE Trans. Nanotechnol.* **19**, 214–222 (2020).
20. Hagras, E. A. A. & Saber, M. Low power and high-speed FPGA implementation for 4D memristor chaotic system for image encryption. *Multimed. Tools Appl.* **79**, 23203–23222 (2020).
21. Kim, G. *et al.* Self-clocking fast and variation tolerant true random number generator based on a stochastic mott memristor. *Nat. Commun.* **12**, 1–8 (2021).

22. Yang, B. *et al.* RRAM Random Number Generator Based on Train of Pulses. *Electron. 2021, Vol. 10, Page 1831* **10**, 1831 (2021).

23. Gu, R., Sun, Y., Wang, Y., Wang, W. & Li, Q. A rate-adjustable true random number generator based on the stochastic delay of a TiN/NbOx/Pt memristor. *AIP Adv.* **11**, 125301 (2021).

24. Lin, B., Gao, B., Pang, Y., Zhang, W., Tang, J., Qian, H., & Wu, H. (2020). A high-performance and calibration-free true random number generator based on the resistance perturbation in RRAM Array. *Technical Digest - International Electron Devices Meeting, IEDM*, *2020-December*, 38.6.1-38.6.4. https://doi.org/10.1109/IEDM13553.2020.9371891

25. Lin, B., Gao, B., Pang, Y., Yao, P., Wu, D., He, H., Tang, J., Qian, H., & Wu, H. (2019). A High-Speed and High-Reliability TRNG Based on Analog RRAM for IoT Security Application. *Technical Digest - International Electron Devices Meeting, IEDM*, *2019-December*. https://doi.org/10.1109/IEDM19573.2019.8993486

26. Yang, W. Y., Chen, B. Y., Chuang, C. C., Hsieh, E. R., Li, K. S., & Chung, S. S. (2020). Novel concept of hardware security in using gate-switching FinFET nonvolatile memory to implement true-random-number generator. *Technical Digest - International Electron Devices Meeting, IEDM*, *2020-December*, 39.3.1-39.3.4. https://doi.org/10.1109/IEDM13553.2020.9371993