True Random Number Generator Based on Memristors with Conductive Filament Modulation by Grown Silicon Nanowires for Image Encryption

Minghao Wei†, Lei Yan†, Yifei Zhang, Junzhuan Wang and Linwei Yu[a)]

AFFILIATIONS

School of Electronic Science and Engineering, Nanjing University, 210023 Nanjing, China

†These authors contributed equally to this work

[a)] Author to whom should be addressed: yulinwei@nju.edu.cn

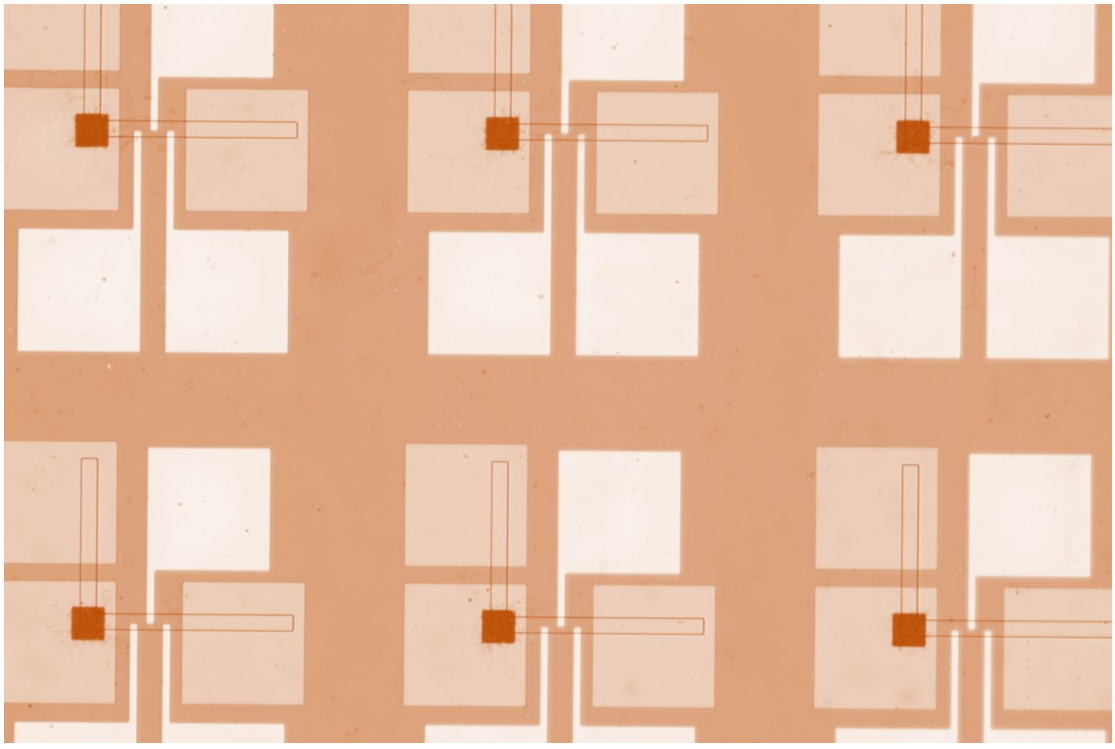

Figure S1. Optical microscope image of the fabricated device array. The IPSLS technique not only enables the low-cost growth of ultrathin SiNWs but also allows their direct growth at precisely predetermined locations, facilitating large-scale and scalable integration without the need for post-growth transfer or rearrangement[1-5].

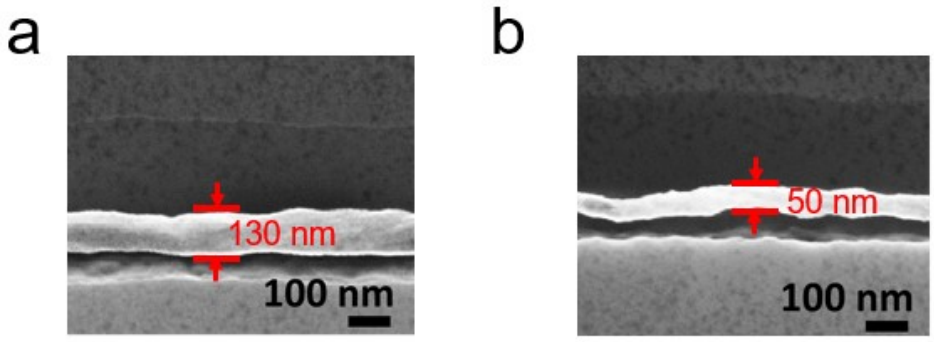

Figure S2. SEM images of the thick nanowire (a) and the thin nanowire (b).

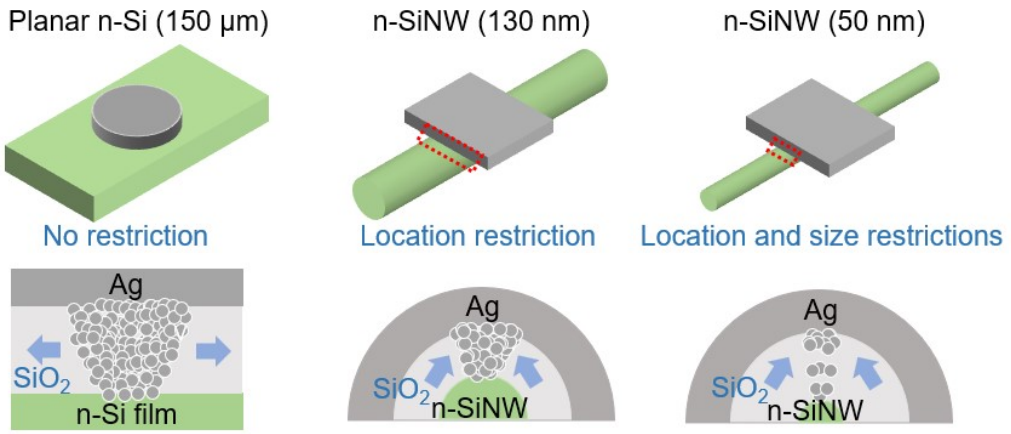

Figure S3. Schematic illustration of the confinement effects on CF growth in planar n-Si film (150 μm), n-SiNW (130 nm), and n-SiNW (50 nm) devices.

The thickness of CFs is positively correlated with the electrode dimension. The effect of SiNW diameter on constraining the growth space of CFs has been systematically investigated in our previous work[1]. As illustrated in Figure R5, for planar n-Si thin-film devices, the switching region is subject to almost no location or size confinement, allowing Ag CFs to nucleate relatively freely within the dielectric layer and continue to grow, thereby making the formation of thicker CFs more likely. For SiNW devices with a diameter of approximately 130 nm, the one-dimensional geometry provides a certain degree of confinement on the filament formation site, causing CF growth to evolve from a two-dimensional mode toward a quasi-one-dimensional mode. However, such confinement is still insufficient for nanoscale CFs, and relatively thick CFs may still form, leaving more residual Ag clusters after rupture and thus resulting in more

pronounced resistance-state fluctuations. In contrast, for SiNW devices with a diameter of approximately 50 nm, the nanowire imposes a stronger restriction on the filament location and size, making it easier for the CF to form a thinner and more confined conductive path within a localized quasi-zero-dimensional region.

For such fine CFs, the possible mechanism of spontaneous rupture is mainly associated with their poorer thermodynamic stability. Because thin metallic CFs possess a higher surface-to-volume ratio and higher surface energy, once the external bias is removed, they are more susceptible to atomic surface diffusion driven by the tendency of the system to minimize its free energy, and rupture is therefore more likely to occur at the weakest part of the filament. After rupture, Ag can no longer maintain a continuous conductive path and instead tends to remain in the dielectric layer in the form of separated nanoclusters.

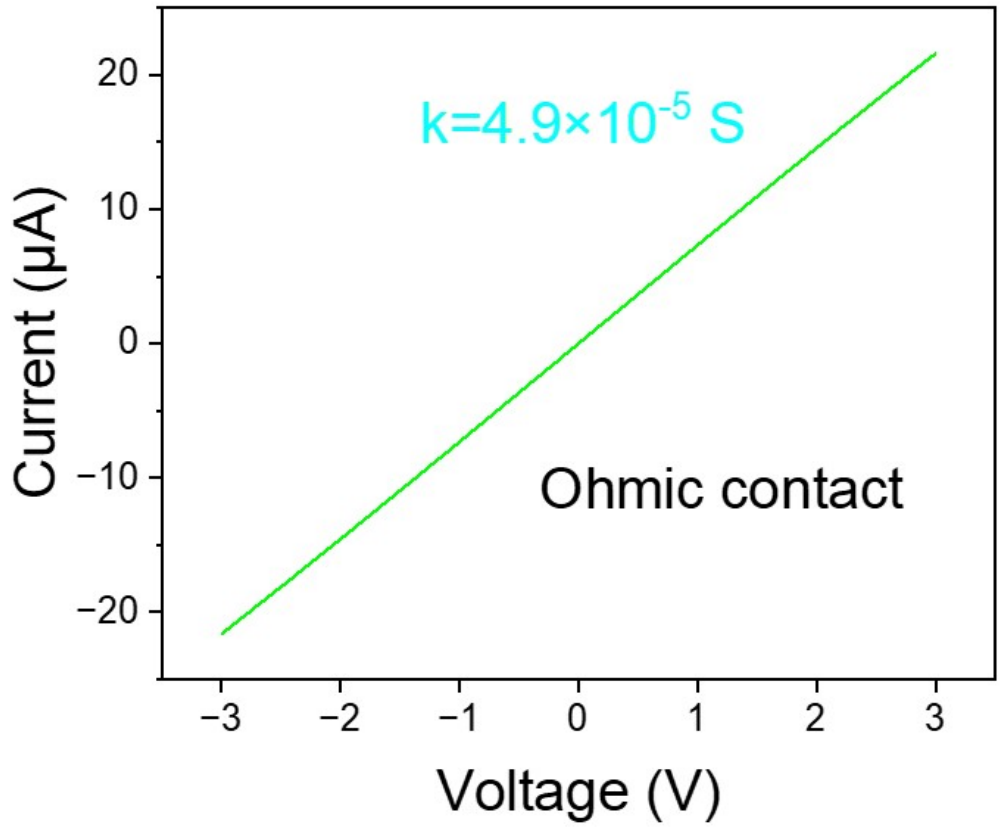

Figure S4. The linear I–V curve indicates an ohmic contact between the n-SiNW and the pad, eliminating the influence of contact barriers.

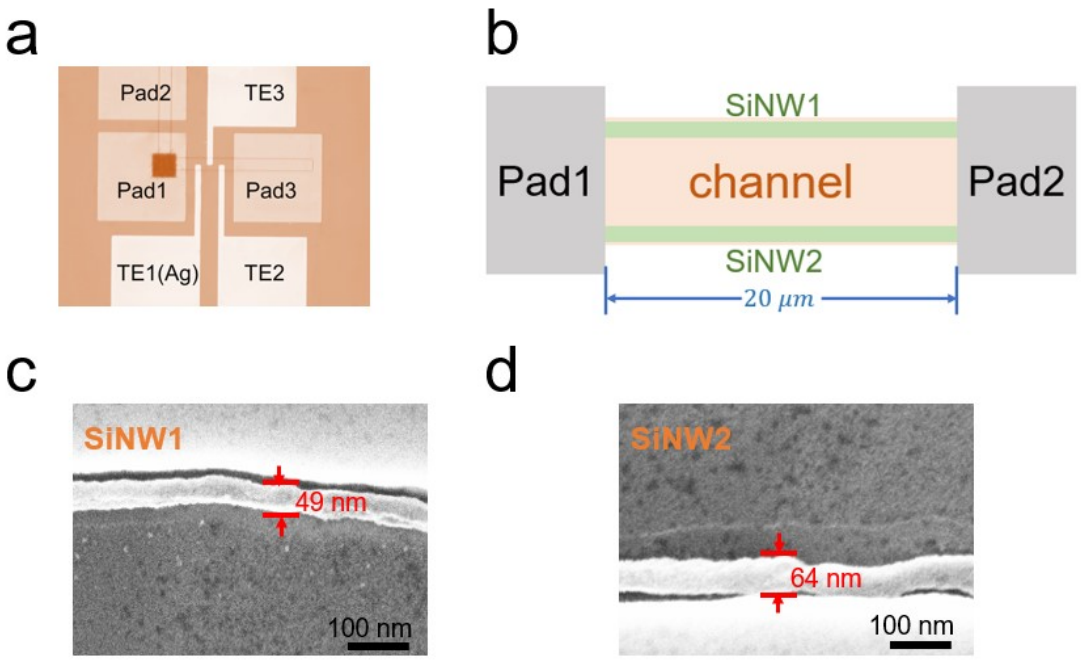

Figure S5. (a) Optical microscope image of the fabricated memristor device. (b) Schematic illustration of the Pad1–Pad2 region used for conductivity estimation, where two parallel SiNWs bridge the two pads and form a channel with a length of approximately 20 μm. (c–d) SEM images of the two individual SiNWs located between Pad1 and Pad2.

By measuring the ohmic conduction characteristic between Pad1 and Pad2, the total conductance was determined to be approximately $4.9 \times 10^{-5} S$. The device channel contains two parallel conducting SiNWs with diameters of approximately 49 nm and 64 nm, respectively, and a channel length of approximately 20 μm. Therefore, based on the cylindrical nanowire cross-sectional area formula, $A = \pi d^2/4$,the total effective conduction area was taken as the sum of the cross-sectional areas of the two SiNWs. By further applying the relation $G = \sigma A/L$, the equivalent conductivity of the SiNWs in this structure was estimated to be approximately $1.92 \times 10^3 S/cm$.

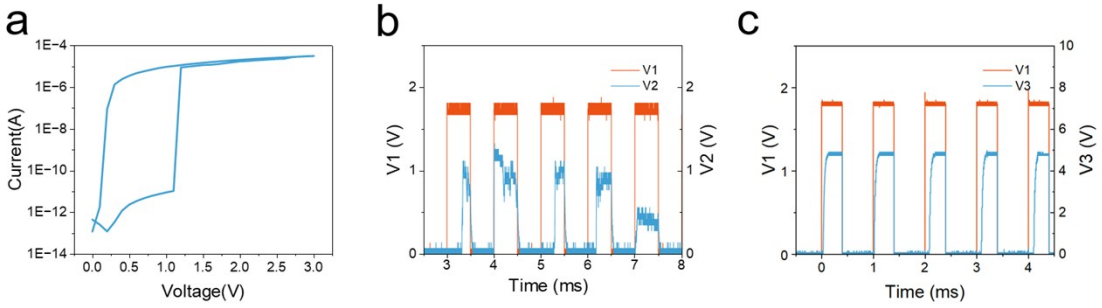

Figure S6 The robustness of the edge-contact Ag/SiO_2/n-SiNW memristor-based TRNG at 85 °C.

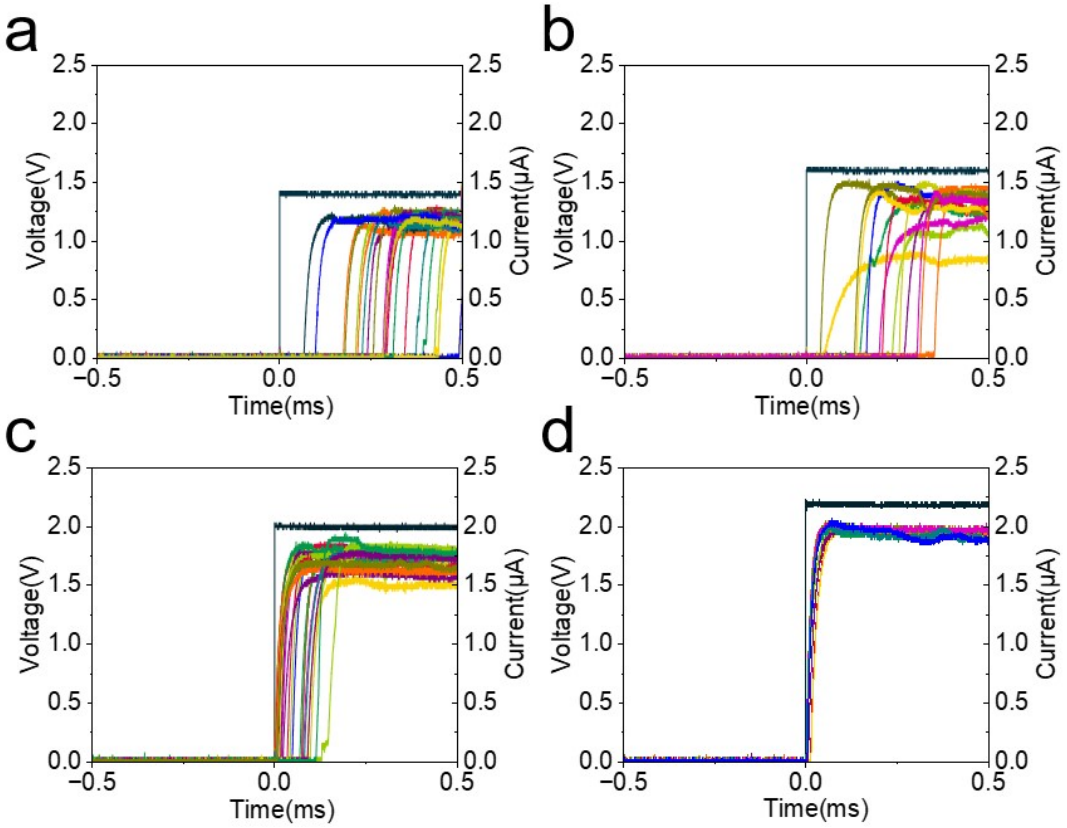

Figure S7. Response of the memristor under single-pulse stimulation at varying voltages (1.4 V, 1.6 V, 2.0 V, and 2.2 V).

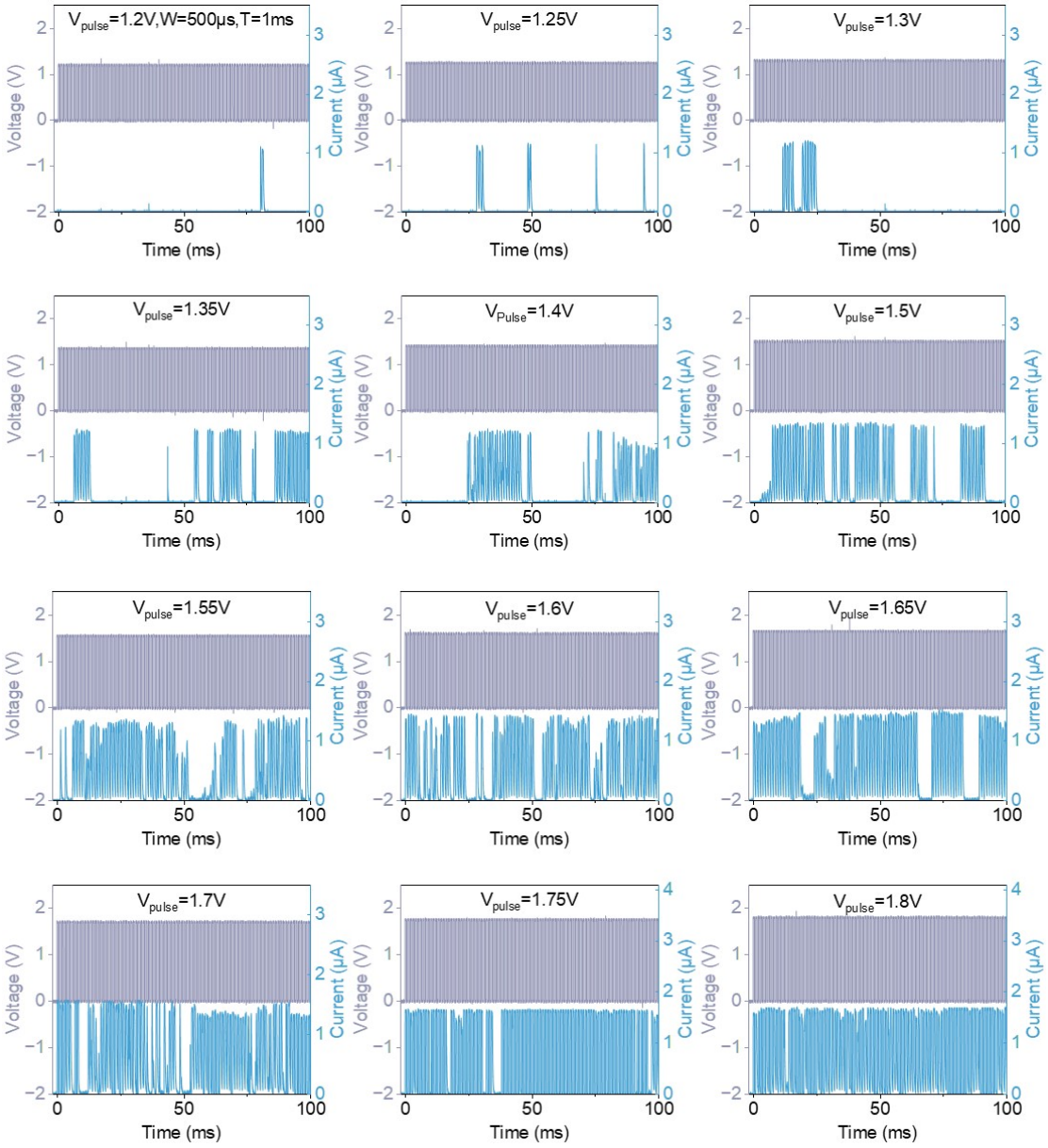

Figure S8. Frequency response of Ag/SiO_2/n-SiNW memristors under pulses with varying high-level amplitudes and fixed pulse width.

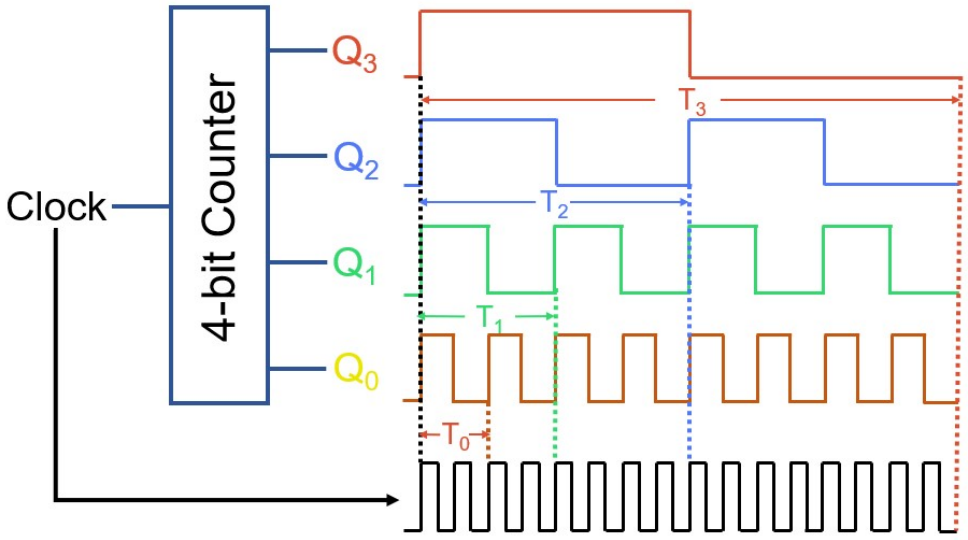

Figure S9. A 4-bit counter employed in the TRNG circuit, where Q_0–Q_3 represent the four counting bits, with Q_0 as the least significant bit and Q_3 as the most significant bit.

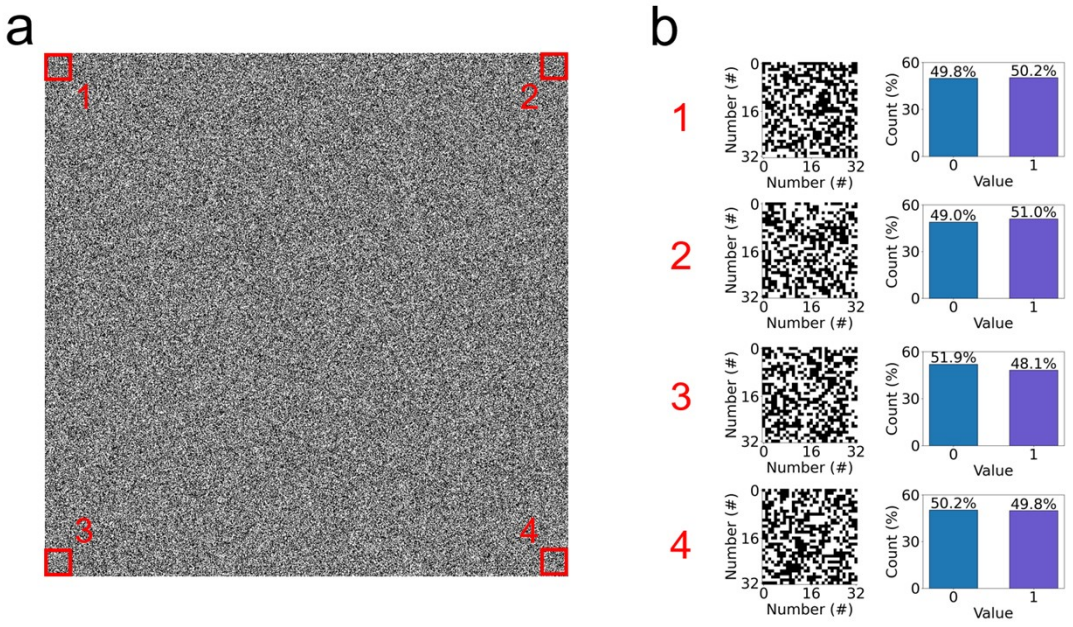

Figure S10. (a) A 1024×1024 noise image generated from true random numbers produced by the TRNG circuit. (b) Magnified views of the four corners in (a) and the corresponding 0/1 ratios in the random number sequences associated with these regions.

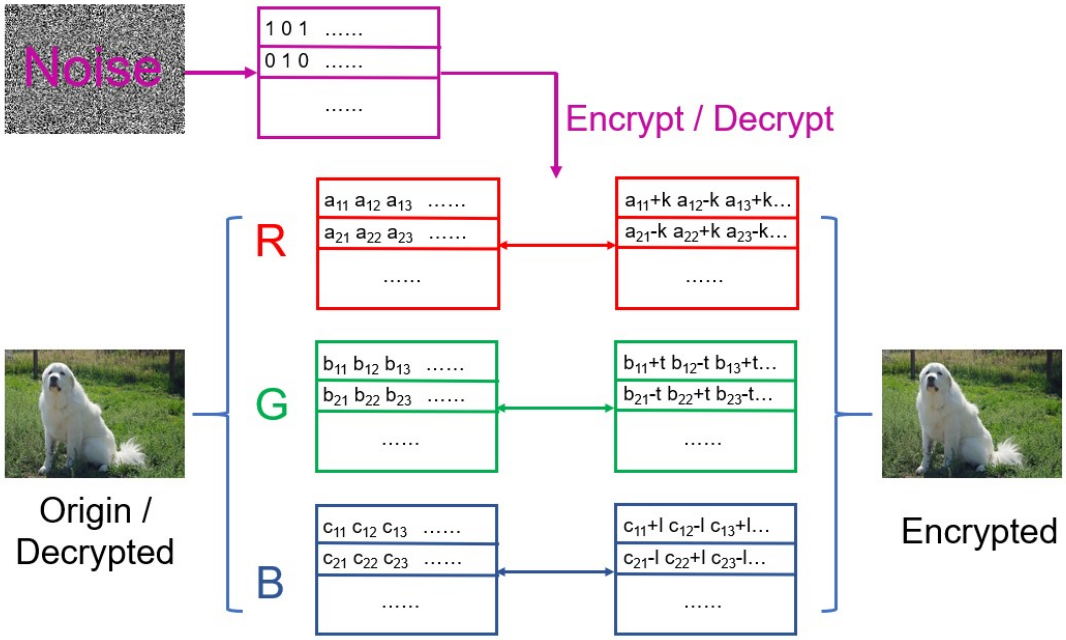

Figure S11. The principle of encrypting and decrypting images using noise maps generated by true random numbers.

The representative dog image shown here has an original size of 500 × 357 pixels. It should be noted that the images in The Oxford-IIIT Pet Dataset are not uniform in size.

We employ a noise map of identical spatial dimensions to the original image as a cryptographic key to achieve reversible image encryption and decryption. The original image is first decomposed into its R, G, and B color channels. During the encryption process, for each pixel location where the corresponding noise map value is 255 (indicating a random bit of 1), the pixel values in all three channels are incremented by predefined perturbation magnitudes, which can be either positive or negative. Conversely, when the noise map value is 0 (random bit 0), the pixel values are decremented by the respective perturbation values.

To enhance the adversarial strength against deep neural network recognition, a channel-wise adaptive perturbation strategy is adopted, assigning distinct perturbation magnitudes to each color channel (denoted as k, t, and l in the figure). The resulting perturbed image constitutes the encrypted version. In the decryption stage, the original image can be faithfully reconstructed by applying the inverse operation using the same noise map as the decryption key, thus achieving high-fidelity and reversible encryption.

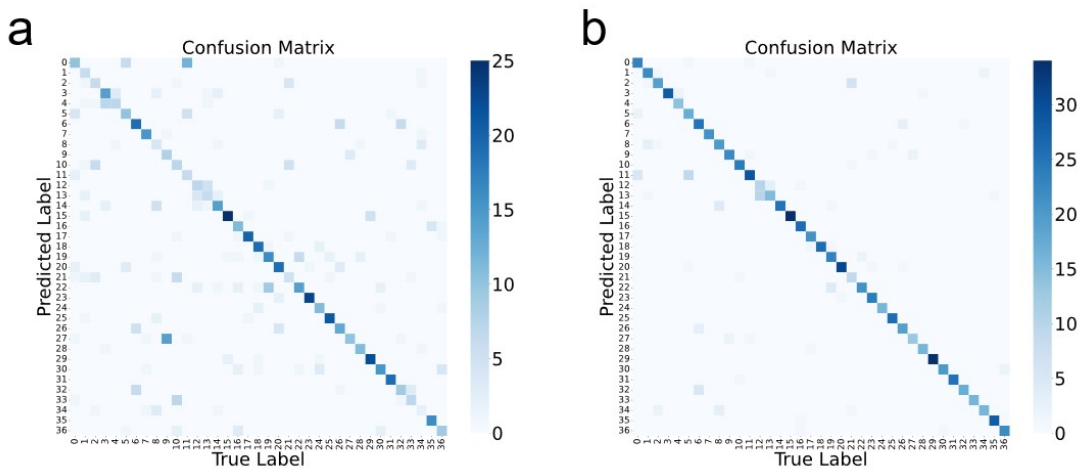

Figure S12. Confusion matrix after encryption (a) and decryption (b)

The x-axis and y-axis represent the predicted labels and true labels, respectively, for the 37 classes in the Oxford-IIIT Pet dataset. The confusion matrix visualizes classification performance through color intensity, where darker shades along the diagonal indicate higher agreement between predictions and ground truth. After encryption, the diagonal colors fade and the distribution becomes less distinct, reflecting a decline in classification accuracy due to the data being obfuscated. Following decryption, the diagonal colors deepen significantly, demonstrating an effective restoration and improvement in the detection accuracy of the YOLO model.

Table S1. Comparison of noise-, chaos-, and quantum-based TRNGs in terms of area, power consumption, and speed.

TRNG	Type	Area (mm^2)	Power (mW)	Speed (bit/s)	With/Without Post-processing	Advantage	Ref.
Tent mapping	chaos	0.07	0.15	0.25M	YES	High tunability	(6)
PWAM mapping	chaos	0.752	29	40M	YES		(7)
Jerk system	chaos	0.038	1.32	50M	YES		(8)
Laser phase fluctuation	quantum	381	N/A	4.68G	YES	High throughput	(9)
photonic integrated circuits	quantum	N/A	7.93	2G	YES		(10)
TiO_x/Al_2O_3	noise	N/A	1.39	10	YES	Low-cost implementation	(11)
Au/Ag:*ι*-car /Pt	noise	1×10^{-6}	N/A	5k	NO		(12)
Ti_3C_2 Mxene -doped	noise	6.25×10^{-4}	N/A	20	NO		(13)
$Ag:SiO_2$	noise	2.5×10^{-5}	N/A	6k	NO		(14)
3D-NAND flash memory	noise	N/A	N/A	43.2k	NO	High scalability	(15)
Read Noise of Flash Memory Cells	noise	N/A	N/A	>1M	YES		(16)
This work	noise	5×10^{-8}	2.7	4k	NO	High CMOS compatibility	-

Note for Table S1.

(1) Advantages of the TRNG in This Work

The key advantage of the Ag/SiO_2/n-SiNW memristive TRNG proposed in this work lies in the fact that its randomness does not rely on any external reset operation or post-processing procedure, but instead originates from the intrinsic dynamic evolution of CFs within the device. The effective geometrical confinement provided by the nanowire not only localizes the formation sites of CFs, but also further restricts their lateral dimensions, thereby suppressing the formation of thick and stable conductive paths and favoring the generation of fine and spatially confined filaments. Such filaments are more prone to rupture and revert to the high-resistance state once the external bias is removed. As a result, the device can continuously undergo filament formation and rupture under repeated electrical stimulation, rather than simply converging to a stable conductive state. Owing to this intrinsic operating mechanism, the TRNG developed in this work requires neither additional reset operations nor post-processing for random number generation, highlighting its unique advantages at both the device-structure and operating-mechanism levels.

(2) Calculation of power consumption and bit generation rate.

The total power consumption of the TRNG circuit is estimated as the sum of the power consumptions of the memristor-resistor branch, the comparator, the AND gate, and the counter:

$$P_{total} = P_{MR} + P_{CMP} + P_{AND} + P_{CNT}$$

For the memristor-resistor branch, the input pulse amplitude is $1.8\,V$, the duty cycle is 50%, the series resistor is $1\,M\Omega$, and the measured voltage drop across this resistor during the high level is about $1.0\,V$. Therefore, the branch current in the high state is $I = 1.0\,V/1\,M\Omega = 1.0\,\mu A$, and the average power consumption of this branch is

$$P_{MR} = D \cdot V_{in} \cdot I = 0.0009\,mW$$

For the LM393 comparator, the supply voltage is taken as $5\,V$, and the typical quiescent current is taken as $400\,\mu A$. Thus, its power consumption is

$$P_{CMP} = V_{CMP} \cdot I_Q = 2.0\,mW$$

For the 74HC08 AND gate, the supply voltage is $5\,V$, the clock frequency is $1\,MHz$, and the power dissipation capacitance is taken as $10\,pF$. Its dynamic power consumption is estimated by

$P_{AND} = C_{PDAND} \cdot V_{AND}^2 \cdot f_{AND} = 0.25\,mW$

For the 74HC161 counter, the supply voltage is $5\,V$, the power dissipation capacitance is taken as $33pF$, and the effective switching frequency is estimated as $0.5\,MHz$ because the counter is driven by the gated random pulse stream rather than by the raw clock. Its dynamic power consumption is therefore

$P_{CNT} = C_{PDCNT} \cdot V_{CNT}^2 \cdot f_{CNT} = 0.4125\,mW$

Accordingly, the total power consumption of the TRNG circuit is $P_{total} \approx 2.7mW$.

The speed was calculated from the raw TRNG output rate. Since the circuit outputs a 4-bit random word in each 1 ms pulse cycle, the bit generation rate is $\frac{4bits}{1ms} = 4\,kbit/s$.

Table S2. Key parameters used for the NIST SP 800-22 statistical tests[17].

Test metric	Value
Sequence length	1 Mbit
Number of bitstreams	66
Block Frequency Test – block length (M)	128
Non-overlapping Template Matching Test – block length (m)	9
Overlapping Template Matching Test – block length (m)	9
Approximate Entropy Test – block length (m)	10
Serial Test – block length (m)	16
Linear Complexity Test – block length (M)	500

Table S3. NIST test of the true random numbers[17].

#	Name	P-Value	Proportion	SUCCESS/FAILUR
01	Approximate Entropy	0.468595	66/66	SUCCESS
02	Block Frequency	0.213309	66/66	SUCCESS
03	Cumulative Sums	0.379722	130 / 132	SUCCESS
04	FFT	0.602458	65/66	SUCCESS
05	Frequency	0.122325	65/66	SUCCESS
06	Linear Complexity	0.437274	65/66	SUCCESS
07	Longest Run	0.888137	64/66	SUCCESS
08	Non Overlapping Template	0.566887	9511/9768	SUCCESS
09	Overlapping Template	0.534146	66/66	SUCCESS
10	Random Excursions	0.125518	272 / 273	SUCCESS
11	Random Excursions Variant	0.111079	700 / 702	SUCCESS
12	Rank	0.213309	64/66	SUCCESS
13	Runs	0.160239	64/66	SUCCESS
14	Serial	0.203765	132 / 132	SUCCESS
15	Universal	0.706149	65/66	SUCCESS

We employed the NIST SP 800-22 test suite to perform a statistical evaluation of the generated random sequences. In total, 66 independent sequences were collected, each with a length of 1 Mbit. For each test item, the overall randomness was assessed by jointly considering both the P-value and the passing proportion: a test was regarded as passed when the P-value exceeded 0.01 and the passing proportion was greater than a threshold value of 95%. For test items containing multiple internal subtests, such as Non-overlapping Template, Random Excursions, and Random Excursions Variant, the table presents their summarized statistical results.

Table S4. Parameters of the YOLO model for the original image[18,19].

Round	Precision	Recall	F1 Score	mAP@50	mAP@50-95
1	0.74252	0.95127	0.83403	0.91739	0.83928
2	0.75439	0.91938	0.82875	0.91323	0.82167
3	0.73213	0.94932	0.8267	0.91457	0.82628
4	0.72924	0.94398	0.82283	0.90701	0.81535
5	0.73202	0.95399	0.82839	0.91175	0.82207
6	0.72764	0.94417	0.82188	0.90348	0.81835
7	0.74231	0.94072	0.82982	0.91717	0.82843
8	0.72929	0.93728	0.82031	0.91071	0.8213
9	0.73682	0.93688	0.82489	0.9123	0.4455
10	0.74217	0.9397	0.82934	0.91152	0.81899
11	0.73357	0.93668	0.82278	0.91103	0.82289
12	0.74268	0.94385	0.83127	0.91278	0.82623
13	0.7325	0.95016	0.82725	0.91115	0.82443
14	0.74895	0.93537	0.83184	0.91457	0.8258
15	0.73123	0.94876	0.82591	0.9106	0.82251
16	0.73999	0.93743	0.82709	0.91133	0.82487
17	0.73133	0.93852	0.82207	0.9109	0.81706
18	0.73042	0.95857	0.82909	0.91323	0.82516
19	0.74032	0.94625	0.83071	0.91446	0.82758
20	0.73496	0.93684	0.82371	0.91029	0.82113
Average	0.73672	0.94246	0.82693	0.91197	0.80474

Table S5. Parameters of the YOLO model for the encrypted image.

Round	Precision	Recall	F1 Score	mAP@50	mAP@50-95
1	0.63144	0.7839	0.69946	0.78241	0.67314
2	0.64451	0.74992	0.69323	0.77719	0.66465
3	0.6552	0.76776	0.70703	0.78244	0.67074
4	0.63797	0.78113	0.70233	0.79191	0.67529
5	0.67603	0.76304	0.7169	0.80129	0.69366
6	0.64204	0.76561	0.6984	0.7854	0.67347
7	0.64732	0.75107	0.69535	0.77384	0.66349
8	0.68041	0.75598	0.71621	0.79871	0.68385
9	0.65793	0.72936	0.69181	0.76813	0.65593
10	0.64692	0.7578	0.69798	0.77312	0.65969
11	0.66498	0.7414	0.70111	0.77585	0.66376
12	0.65091	0.73434	0.69011	0.76952	0.65852
13	0.63236	0.77466	0.69631	0.78403	0.67241
14	0.65075	0.74511	0.69474	0.76871	0.65287
15	0.65003	0.77249	0.70599	0.79123	0.6804
16	0.65088	0.78433	0.7114	0.7932	0.68724
17	0.66825	0.74871	0.7062	0.78962	0.68189
18	0.64239	0.78098	0.70494	0.79238	0.67971
19	0.643	0.77206	0.70164	0.77856	0.66665
20	0.69253	0.74132	0.71609	0.78823	0.67439
Average	0.65329	0.76005	0.70236	0.78329	0.67159

Table S6. Parameters of the YOLO model for the decrypted image.

Round	Precision	Recall	F1 Score	mAP@50	mAP@50-95
1	0.72363	0.90047	0.80242	0.89496	0.79917
2	0.724	0.89995	0.80244	0.89464	0.79766
3	0.72143	0.89756	0.79991	0.89078	0.79224
4	0.73564	0.90172	0.81026	0.89564	0.79876
5	0.7246	0.91323	0.80805	0.8929	0.79597
6	0.71802	0.91251	0.80367	0.89501	0.79595
7	0.73331	0.89281	0.80524	0.89382	0.79765
8	0.7105	0.90959	0.79781	0.89261	0.79758
9	0.73237	0.91676	0.81426	0.89945	0.80189
10	0.7249	0.90255	0.80403	0.89215	0.80226
11	0.72438	0.92978	0.81433	0.89537	0.80124
12	0.72789	0.91172	0.8095	0.89097	0.79663
13	0.72708	0.89926	0.80406	0.89106	0.79738
14	0.71159	0.92629	0.80487	0.89333	0.79878
15	0.72458	0.91474	0.80863	0.89263	0.79365
16	0.72178	0.87986	0.79302	0.88248	0.77609
17	0.71713	0.81872	0.76457	0.86515	0.75881
18	0.71976	0.89575	0.79817	0.88153	0.78062
19	0.72753	0.90578	0.80693	0.89621	0.79867
20	0.71633	0.91161	0.80226	0.88867	0.78787
Average	0.72332	0.90203	0.80272	0.89097	0.79344

Note for Tables S4–S6.

(1) YOLOv8n model information[19].

The object detection results in Tables S4–S6 were obtained using the YOLOv8n model, which consists of a backbone, a neck, and a detection head. The network contains a total of 129 layers and 3,011,238 learnable parameters.

(2) Definition of evaluation metrics.

Precision measures the proportion of correctly predicted positive detections among all positive predictions made by the model. Recall measures the proportion of true positive targets successfully detected among all actual positive targets. The F1 score is the harmonic mean of precision and recall, and is used to reflect the balance between these two metrics. mAP@50 denotes the mean average precision at an intersection over union (IoU) threshold of 0.5, and evaluates the detection performance under a relatively lenient matching criterion. mAP@50–95 denotes the averaged mean average precision calculated over IoU thresholds from 0.5 to 0.95 with a step size of 0.05, and therefore provides a more comprehensive evaluation of the overall detection capability under different levels of matching strictness.

References

1. L. Yan, Y. Zhang and Z. Hu, *et al.*, High-performance edge-line contact memristors with in-plane solid–liquid–solid grown silicon nanowires for probabilistic neuromorphic computing, *ACS Nano*, 2025, **19** , 11001 —11011.
2. W. Liao, Y. Zhang and D. Li, *et al.*, High-density integration of uniform sub-22 nm silicon nanowires for transparent thin film transistors on glass, *Appl. Surf. Sci.*, 2025, **679** , 161213.
3. Y. Sun, T. Dong and L. Yu, *et al.*, Planar growth, integration, and applications of semiconducting nanowires, *Adv. Mater.*, 2020, **32** , 1903945 —1903955.
4. X. Song, R. Hu and S. Xu, *et al.*, Highly sensitive ammonia gas detection at room temperature by integratable silicon nanowire field-effect sensors, *ACS Appl. Mater. Interfaces*, 2021, **13** , 14377.
5. R. Hu, S. Xu and J. Wang, *et al.*, Unprecedented uniform 3D growth integration of 10-layer stacked Si nanowires on tightly confined sidewall grooves, *Nano Lett.*, 2020, **20** , 7489.
6. J. A. Aguilar Angulo, E. Kussener and H. Barthelemy, *et al.*, Discrete chaos-based random number generator, *Proc. IEEE Faible Tension Faible Consommation*, 2014, **1**, 1.
7. F. Pareschi, G. Setti and R. Rovatti, *et al.*, Implementation and testing of high-speed CMOS true random number generators based on chaotic systems, *IEEE Trans. Circuits Syst. I*, 2010, **57**, 3124 —3137.
8. C. Wannaboon, M. Tachibana and W. San-Um, *et al.*, A 0.18-μm CMOS high-data-rate true random bit generator through modulation of chaotic jerk circuit signals, *Chaos*, 2018, **28**, 063123.
9. Z. Huang, J. Li and Y. Chen, *et al.*, Hybrid integrated Gbps quantum random number generator based on laser phase fluctuation, *Opt. Express*, 2025, **33**, 11985 —11995.
10. O. M. Crampton, T. J. Dowling and T. Roger, *et al.*, A 2-Gbps low-SWaP quantum random number generator with photonic integrated circuits for satellite applications, *npj Quantum Inf.*, 2025, **11**, 153.
11. J. Park, H. Kim and H. Kim, *et al.*, Bias-independent true random number generator circuit using memristor noise signals as entropy source, *Adv. Intell. Syst.*, 2025, **7**, 2400648.
12. J. Bian, Y. Tao and Z. Wang, *et al.*, A true random number generator based on double threshold-switching memristors for image encryption, *Appl. Phys. Lett.*, 2023, **122**, 193503.
13. X. Wang, H. Wang and D. Yang, *et al.*, Low-voltage forming-free flexible memristors with multifunctionality for hybrid storage and cryptographic random number generation in edge devices, *Nano Energy*, 2025, **142**, 111225.
14. H. Jiang, D. Belkin and S. E. Savel'ev, *et al.*, A novel true random number generator based on a stochastic diffusive memristor, Nat. Commun., 2017, **8**, 882.
15. R. Zhou, J. Huang and X. Liu, *et al.*, A Low-Complexity True Random Number Generation Scheme Using 3D-NAND Flash Memory, *Proc. DATE*, 2025, 1 –7.

16. B. Ray and A. Milenković, True random number generation using read noise of flash memory cells, *IEEE Trans. Electron Devices*, 2018, **65**, 963 –969.
17. A. Rukhin, J. Soto and J. Nechvatal, *et al.*, A statistical test suite for random and pseudorandom number generators for cryptographic applications, *Natl. Inst. Stand. Technol., Spec. Publ.*, 2001, 800-22, 1.
18. O. M. Parkhi, A. Vedaldi and A. Zisserman, *et al.*, Cats and dogs, *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2012, 3498 —3505.
19. J. Redmon, S. Divvala and R. Girshick, *et al.*, You only look once: Unified, real-time object detection, *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2016, 779 —788.