

Supporting Information

High-Performance hardware primitives based on sub-10 nm nanodiodes for cryptography applications

Kun Chen[†], Nannan Li[†], Yi Luo^{}, and Yao Yao^{*}*

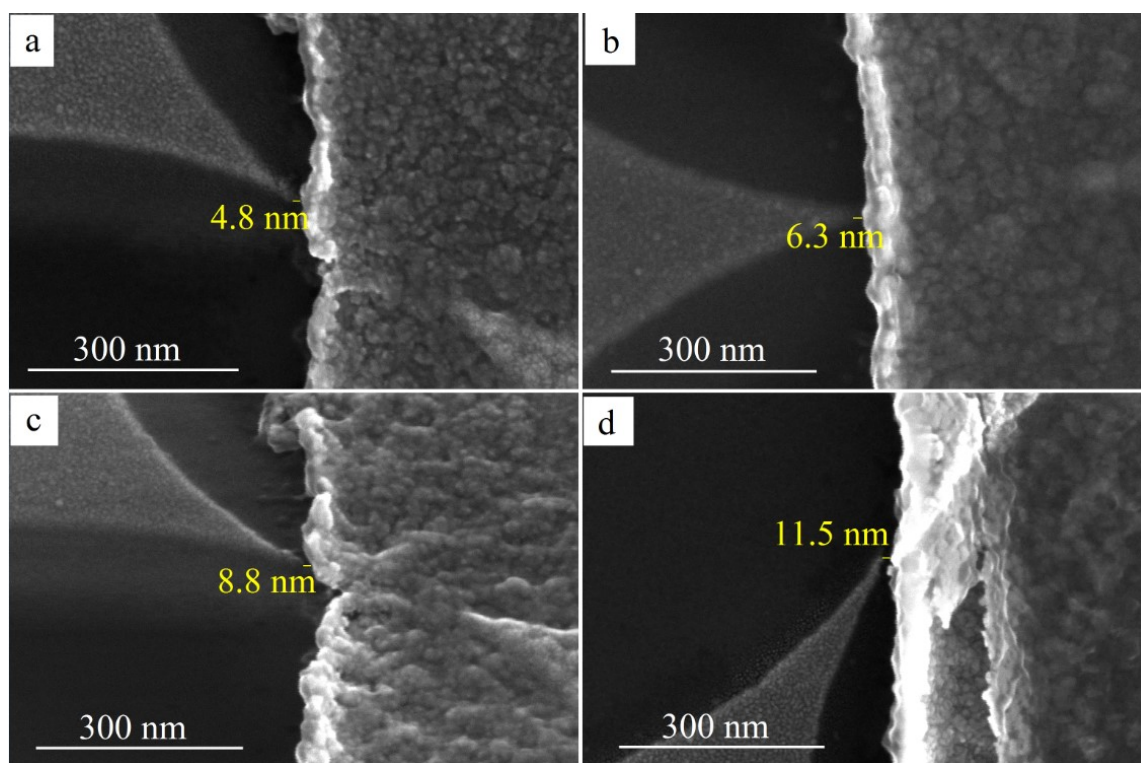


Figure S1. SEM images of nanodiodes with different tip-to-edge vacuum-like air-channel length.

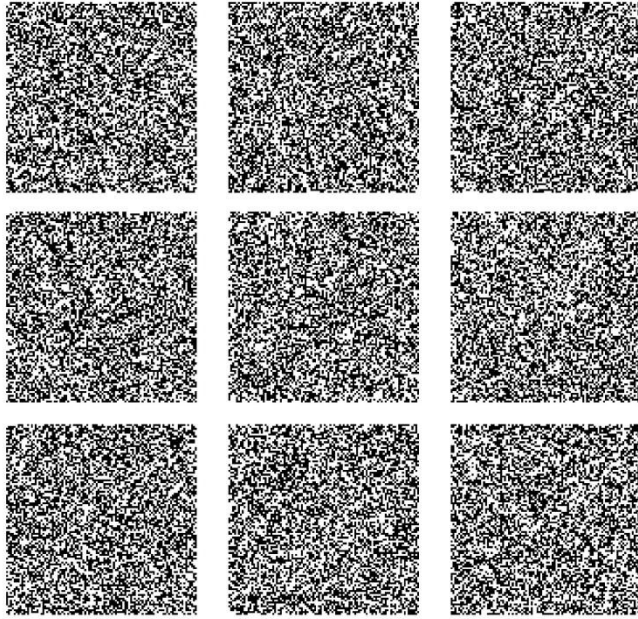


Figure S2. Bitmap of random sequences from nine repeated experiments. Black points represent bit '0' and white points represent bit '1'. Obviously, the bitmaps vary completely among the nine experiments. In addition, these bitmaps show a balanced distribution of black and white points and do not display any distinct repetitive patterns or regularity, illustrating a high degree of randomness.

Ref	Material and device	Power consumption
[1]	WSe ₂ and WS ₂ FETs	10 pJ/bit
[2]	h-BN MIM memristor	2 nJ/bit
[3]	Bi ₂ O ₂ Se-based memristor	0.2~2pJ/bit
[4]	MoS ₂ Fe-FETs	1~50 pJ/bit
This work	sub-10 nm air-channel nanodiode	1E-3pJ/bit

Table S1. Power consumption of typical schemes

Test name	Uniformity of p-values	Proportion	Assessment
Frequency	0.148094	63/64	PASSED
Block Frequency	0.911413	64/64	PASSED
Cumulative Sums	0.148094	63/64	PASSED
Runs	0.350485	63/64	PASSED
Longest Run	0.437274	64/64	PASSED
Rank	0.637119	62/64	PASSED
FFT	0.324180	64/64	PASSED
Non Overlapping Template	0.002316	64/64	PASSED
Overlapping Template	0.834308	64/64	PASSED
Approximate Entropy	0.074177	63/64	PASSED
Serial	0.162606	64/64	PASSED
Linear Complexity	0.468595	63/64	PASSED

Table S2. Results of NIST SP800-22 test for random bit streams from nano-TRNG. The minimum value is reported for test items with multiple outcomes. A test item is considered to pass when the uniformity of p-values exceeds a significance level of 0.0001 and the pass proportion is above the criterion of 60/64. Detailed results indicate that extracted random bits successfully pass all available tests.

Test name	P-value	Assessment
Multinomial Bits Over (L=2)	0.32	PASSED
Multinomial Bits Over (L=4)	0.12	PASSED
Multinomial Bits Over (L=8)	0.34	PASSED
Multinomial Bits Over (L=16)	0.97	PASSED
Hamming Independency (L=16)	0.71	PASSED
Hamming Independency (L=32)	0.52	PASSED
Hamming Correlation (L=32)	0.32	PASSED
Random Walk H (L=64)	0.21	PASSED
Random Walk M (L=64)	0.46	PASSED
Random Walk J (L=64)	0.37	PASSED
Random Walk R (L=64)	0.28	PASSED
Random Walk C (L=64)	0.11	PASSED
Random Walk H (L=320)	0.72	PASSED
Random Walk M (L=320)	0.05	PASSED
Random Walk J (L=320)	0.52	PASSED
Random Walk R (L=320)	0.83	PASSED
Random Walk C (L=320)	0.13	PASSED

Table S3. Results of TestU01 Alphabit test for random bit streams. The TestU01 Alphabit battery evaluates the randomness of random bits with the aim of evaluating physical entropy source. The worst case is selected when multiple p-values are produced in a test. For “pass,” each p-value should fall into the range of [0.001, 0.999]. As indicated by the results, the random bits from nano-TRNG are considered to successfully pass the Alphabit battery.

Test name	P-value	Assessment
Diehard_birthdays	0.78411886	PASSED
Diehard_operm5	0.18263935	PASSED
Diehard_rank_32x32	0.56313029	PASSED
Diehard_rank_6x8	0.71633706	PASSED
Diehard_bitstream	0.79034377	PASSED
Diehard_opso	0.50905934	PASSED
Diehard_oqso	0.52519766	PASSED
Diehard_dna	0.70139207	PASSED
Diehard_count_1s_str	0.84587460	PASSED
Diehard_count_1s_byt	0.24739316	PASSED
Diehard_parking_lot	0.72516127	PASSED
Diehard_2dsphere	0.57153969	PASSED
Diehard_3dsphere	0.23965050	PASSED
Diehard_squeeze	0.00591657	PASSED
Diehard_sums	0.02442857	PASSED
Diehard_runs	0.10196029	PASSED
Diehard_craps	0.53719022	PASSED
Marsaglia_tsang_gcd	0.40526218	PASSED
Sts_monobit	0.83012234	PASSED
Sts_runs	0.13520823	PASSED
Sts_serial	0.99938897	WEAK
Rgb_bitdist	0.05981224	PASSED
Rgb_minimum_distance	0.28108138	PASSED
Rgb_permutations	0.32418848	PASSED
Rgb_lagged_sum	0.03403859	PASSED
Rgb_kstest_test	0.11456695	PASSED

Dab_bytedistrib	0.85234119	PASSED
Dab_dct	0.54693658	PASSED
Dab_filltree	0.99922414	WEAK
Dab_filltree2	0.03518846	PASSED
Dab_monobit2	0.90574448	PASSED

Table S4. Results of DIEHARDER test for random bit streams. The test suite is a rather stringent and comprehensive statistical testing suite, consisting of 17 fundamental tests and 14 extended test items. The minimum value is reported for test items with multiple outcomes. In our case, the extracted random bits successfully pass all the test items, with only two tests marked as ‘weak’ (i.e., marginal success).

Test name	Assessment
Excursion test statistic	PASSED
Number of directional runs	PASSED
Length of directional runs	PASSED
Number of increases and decreases	PASSED
Number of runs based on the median	PASSED
Length of runs based on median	PASSED
Average collision test statistic	PASSED
Maximum collision test statistic	PASSED
Periodicity test statistic (lag = 1)	PASSED
Periodicity test statistic (lag = 2)	PASSED
Periodicity test statistic (lag = 8)	PASSED
Periodicity test statistic (lag = 16)	PASSED
Periodicity test statistic (lag = 32)	PASSED

Covariance test statistic (lag = 1)	PASSED
Covariance test statistic (lag = 2)	PASSED
Covariance test statistic (lag = 8)	PASSED
Covariance test statistic (lag = 16)	PASSED
Covariance test statistic (lag = 32)	PASSED
Compression test statistic	PASSED
Chi-square independence	PASSED
Chi-square goodness of fit	PASSED
Length of the longest repeated substring	PASSED
Sanity check	PASSED
Validation test	PASSED
Estimation of entropy	0.995817

Table S5. Results of NIST SP800-90B test. In our case, the entropy source successfully pass all tests and demonstrates a min-entropy of 0.995817 bits/bit.

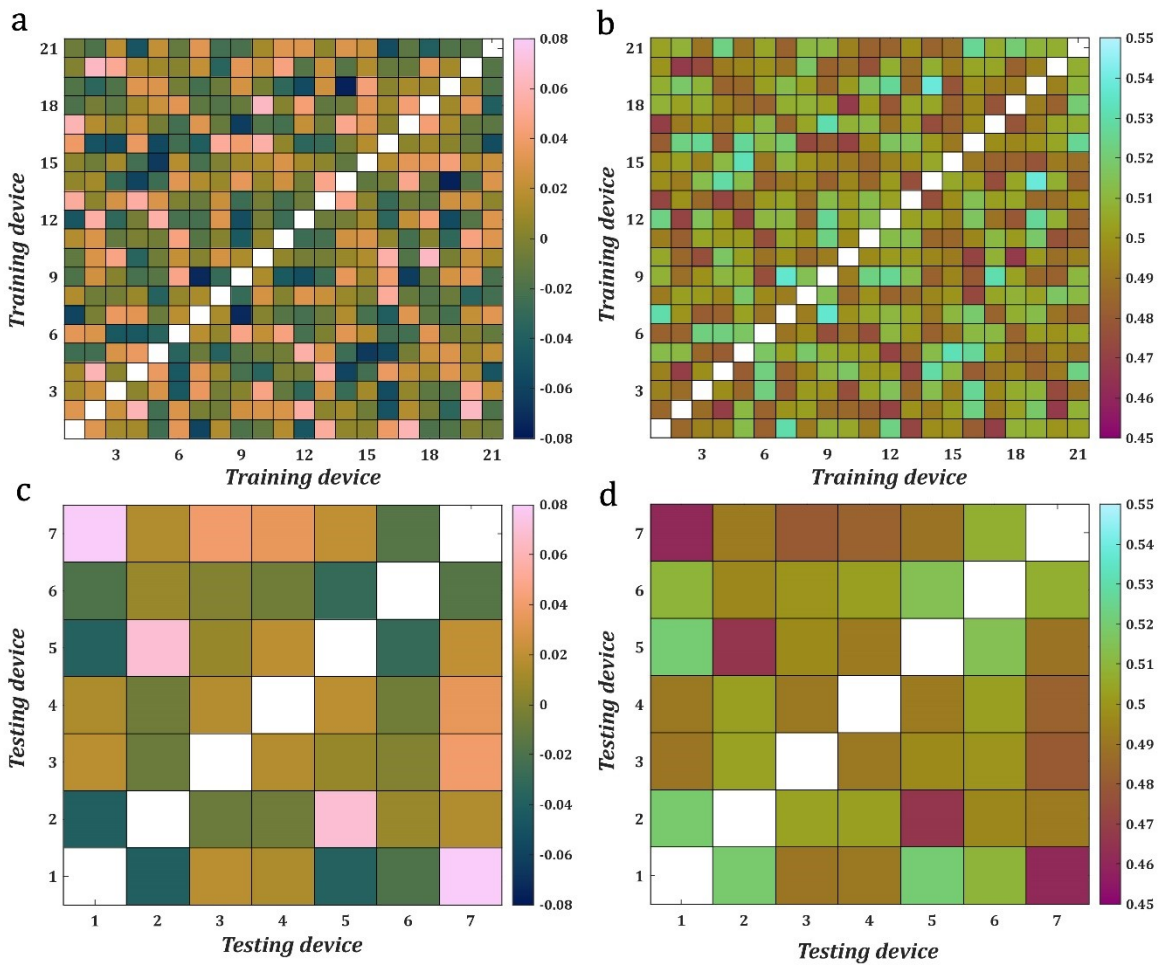


Figure S3. (a)-(d). Hamming distance (a) and correlation coefficient (b) for random bits of twenty-one devices in the training set. Hamming distance (c) and correlation coefficient (d) for random bits of seven devices used for test set.

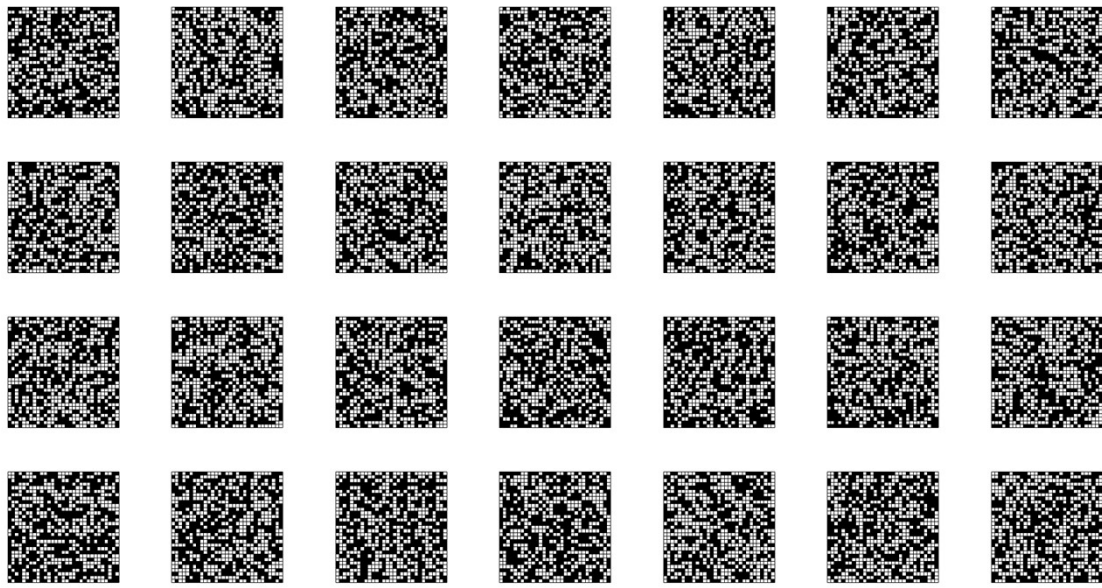


Figure S4. Bitmaps from 28 individual devices.

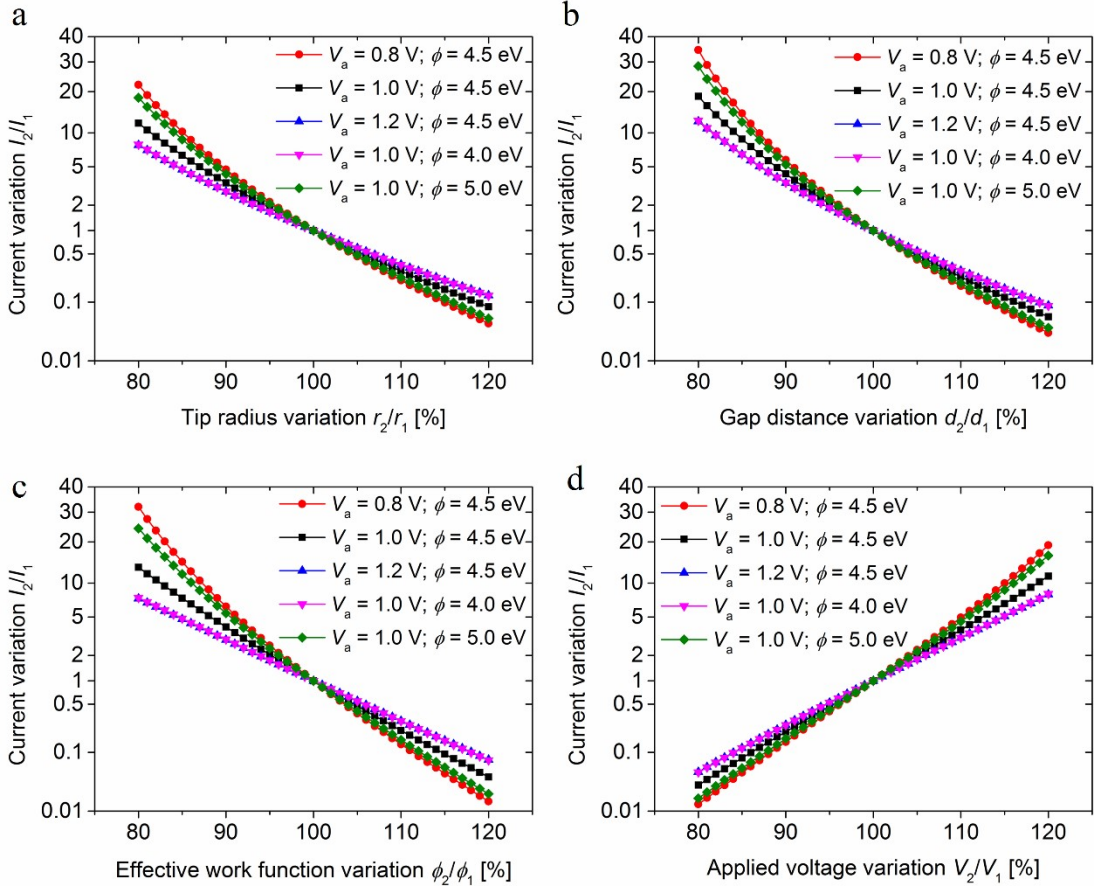


Figure S5. Theoretical current fluctuations under variations in physical geometry, material properties, and operating environments. (a) The effect of tip radius variation on emission current fluctuations when $\varphi_2 = \varphi_1 = \varphi$, $E_2/E_1 = r_1/r_2$, and gap distance $d = 10$ nm. (b) The effect of gap distance variation on emission current fluctuations when $\varphi_2 = \varphi_1 = \varphi$, $r_1 = r_2$, $E_2/E_1 = d_1/d_2$, and $d_1 = 10$ nm. (c) The effect of effective work function variation on emission current fluctuations when $r_1 = r_2$, $E_2 = E_1$, and $d_1 = d_2$. (d) The effect of applied voltage variation on emission current fluctuations when $r_1 = r_2$, $\varphi_2 = \varphi_1 = \varphi$, $E_2/E_1 = V_2/V_1$, and $d_1 = d_2 = 10$ nm.

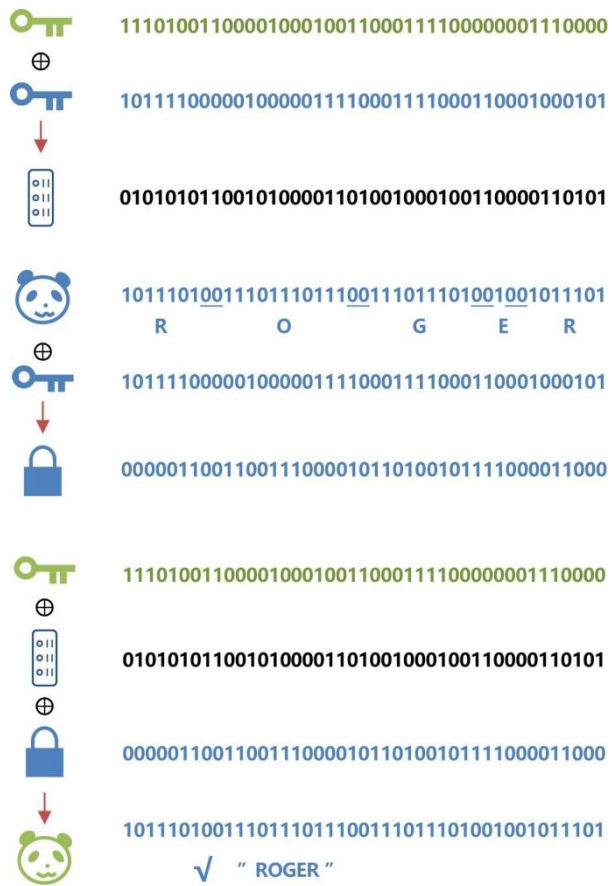


Figure S6. The encryption and decryption process of the feedback signal "ROGER". Alice accurately decrypts the message sent by Bob according to our encoding rules.

Supporting Information References

- [1] A. Wali, H. Ravichandran, S. Das, *ACS Nano* 2021, 15, 17804.
- [2] C. Wen, X. Li, T. Zanotti, F. Maria Puglisi, Y. Shi, F. Saiz, A. Antidormi, S. Roche, W. Zheng, X. Liang, J. Hu, S. Duhm, J B. Roldan, T. Wu, V. Chen, E. Pop, B. Garrido, K. Zhu, F. Hui, M. Lanza, *Adv. Mater.* 2021, 33, 2100185.
- [3] B. Liu, Y.-F. Chang, J. Li, X. Liu, L. A. Wang, D. Verma, H. Liang, H. Zhu, Y. Zhao, L.-J. Li, T.-H. Hou, C.-S. Lai, *ACS Nano* 2022, 16, 6847.
- [4] Y.-C. Chien, H. Xiang, J. Wang, Y. Shi, X. Fong, K.-W. Ang, *Small* 2023, 19, 2302842.