Science Advances
AAAS

Supplementary Materials for

Concealable physically unclonable function chip with a memristor array

Bin Gao *et al.*

Corresponding author: Bin Gao, gaob1@tsinghua.edu.cn; Huaqiang Wu, wuhq@tsinghua.edu.cn

Sci. Adv. **8**, eabn7753 (2022)
DOI: 10.1126/sciadv.abn7753

This PDF file includes:

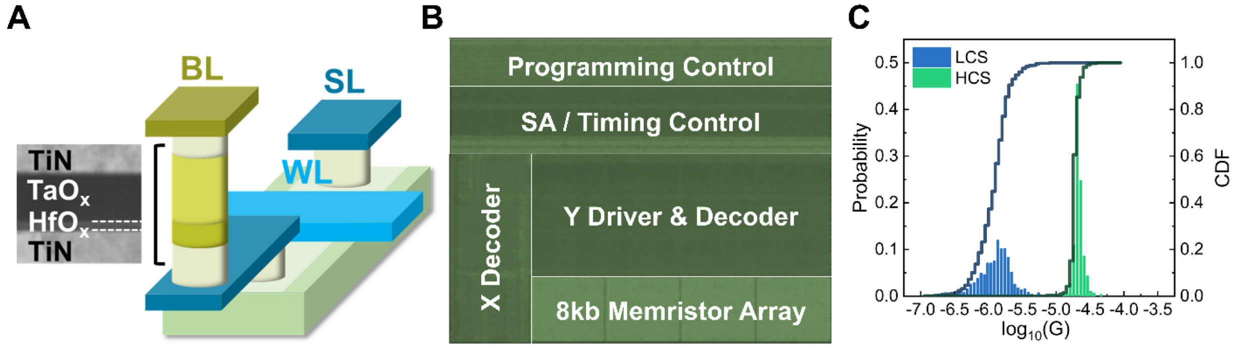


Fig. S1. PUF chip, memristor device, and D2D variation. (**A**) Basic 1T1R structure with a memristor integrated between M5 and M6. The inset is the cross-section transmission electron micrograph (TEM) of the memristor material stack. (**B**) Micrograph of the fabricated PUF chip. (C) The D2D variation in conductance values measured from 1024 memristors.

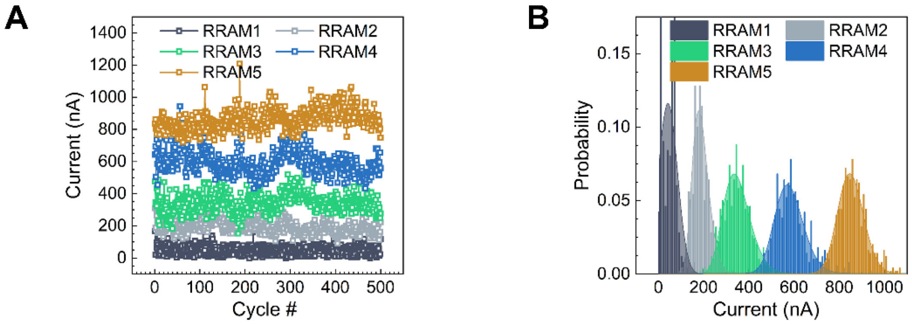


Fig. S2. C2C correlation in memristor conductance values. (**A**) The change in conductance values of 5 memristors with incremental SET/RESET cycle. The conductance values are read out after RESET. (**B**) The corresponding probability distributions of these conductance values.

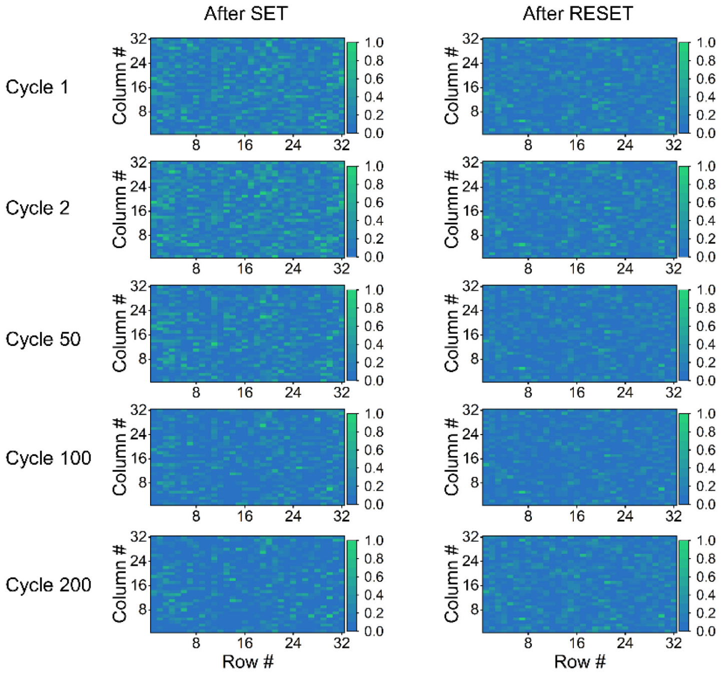


Fig. S3. Change in the conductance distributions. Colormaps of the conductance distributions for 1 kb memristors with incremental SET-RESET cycle. The conductance values are normalized for each colormap individually.

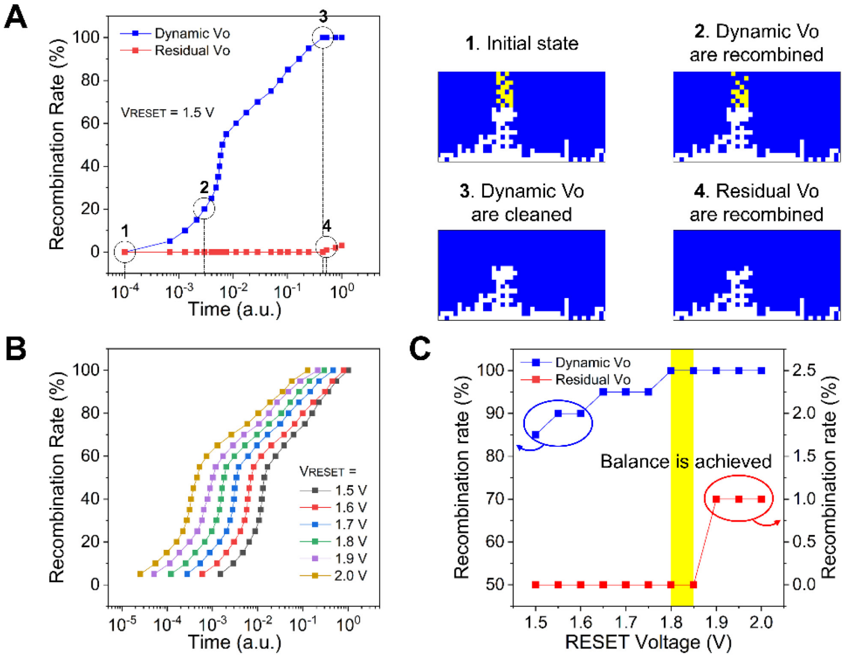


Fig. S4. Simulated change of Vo during the RESET process. (**A**) The change in the recombination rate of dynamic Vo and residual Vo with incremental RESET time. The insets show the corresponding change in filament morphology. (**B**) Dynamic Vo are combined at a higher speed with incremental RESET voltage. (**C**) The change in recombination rate of dynamic Vo and residual Vo with different RESET voltages. With RESET voltage approximately 1.825 V, a perfect balance between SET and RESET is achieved with 100% recombination of dynamic Vo and 0% recombination of residual Vo.

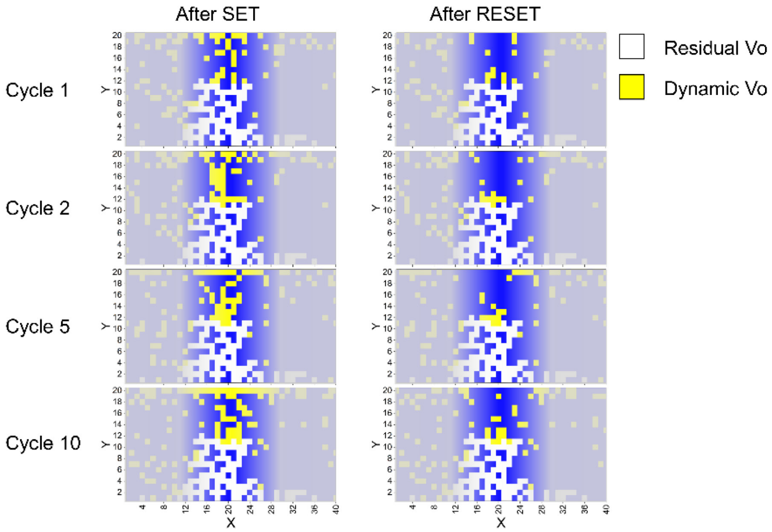
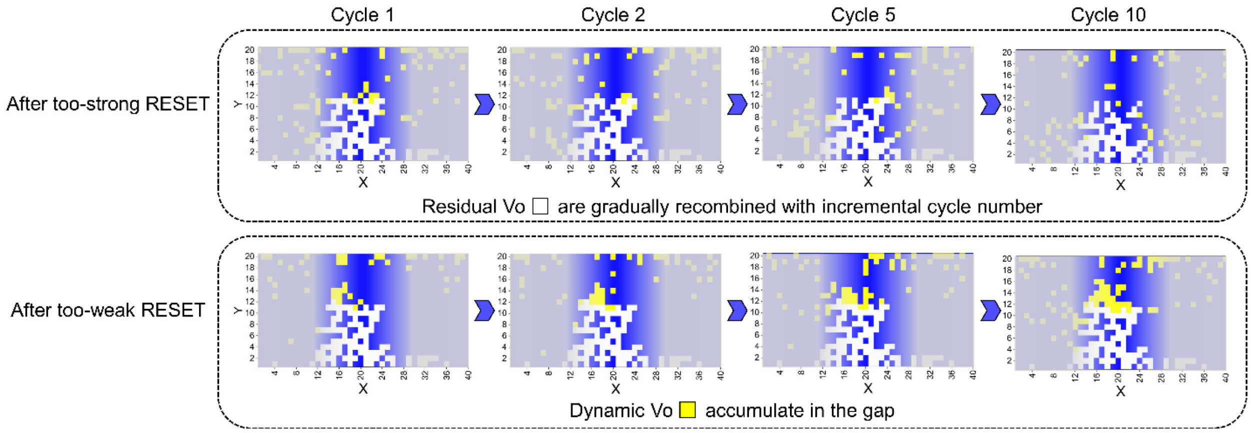


Fig. S5. KMC simulation results with balanced SET and RESET conditions. The simulated change in filament morphology after multiple RESET-SET operations. The filaments mainly formed at the center, contributing the most to the device conductivity. The other marginal parts are less important and thus are covered in translucent gray in these subfigures. The yellow cells represent the dynamic Vo, which are randomly generated in the filament gap to bridge a conductive path after SET and erased after RESET. The white cells represent the residual part, which remains unchanged among the switching cycles. The SET and RESET voltages are 1.6 V and 1.85 V, respectively.


Cycle 1

Cycle 2

Cycle 5

Cycle 10

After too-strong RESET

Residual Vo □ are gradually recombined with incremental cycle number

After too-weak RESET

Dynamic Vo 🟨 accumulate in the gap

Fig. S6. KMC simulation results with unbalanced SET and RESET conditions. The simulated change in filament morphology after RESET with RESET condition that is too strong (e.g., V_{RESET} = 2.0 V) and RESET conditions that is too weak (e.g., V_{RESET} = 1.6 V).

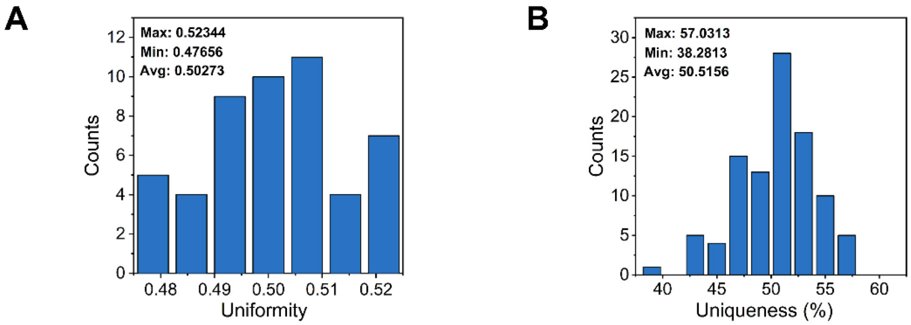


Fig. S7. Randomness evaluation results. (**A**) The uniformity distribution of 50 128-bit PUF keys. The uniformity measures the probability of a PUF bit being 1, and its ideal value is 0.5. From the distribution, the average uniformity is 0.50273. (**B**) The uniqueness distribution of 50 128-bit PUF keys collected from 5 chip (i.e., 10 PUF keys per chip). The uniqueness measures the difference between the two responses from two PUF chips which are inquired with the same challenge, and its ideal value is 50%. From the distribution, the average uniqueness is 50.5156%.

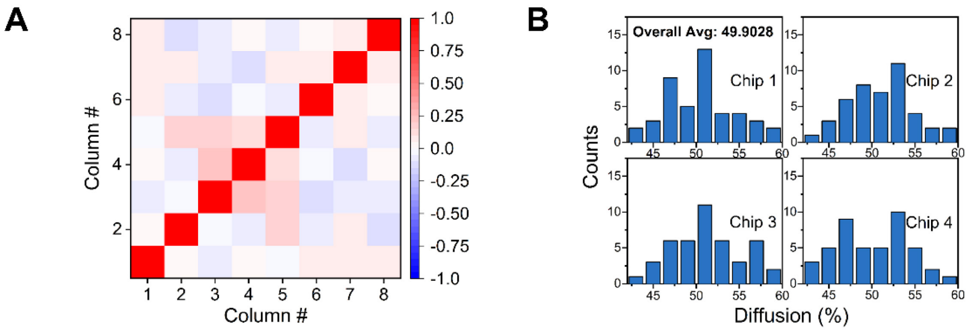


Fig. S8. Diffusion evaluation results. (**A**) The correlation coefficient matrix of the resistance values of any two columns in a PUF chip, where negligible correlation can be found, indicating that the resistance distribution is highly random. (**B**) The diffusion distribution of 40 128-bit PUF keys collected from 4 chip (i.e., 10 PUF keys per chip). The diffusion measures the difference between any two responses from one PUF chip, and its ideal value is 50%. In most case, the diffusion ranges from 43% to 57%, and the average is 49.9028%.

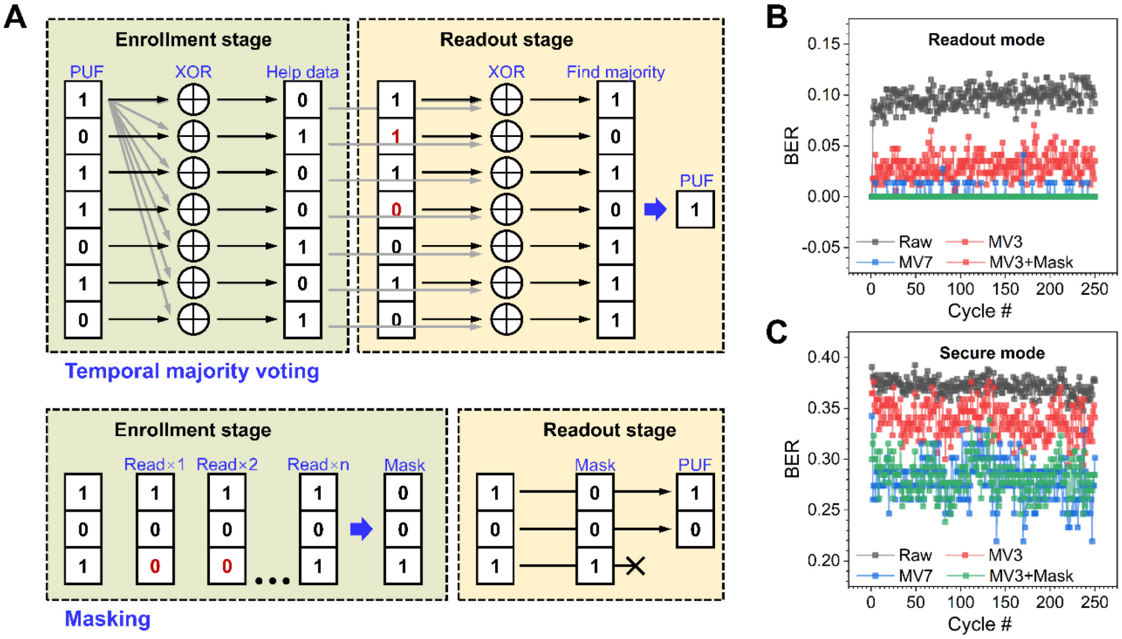


Fig. S9. Measured BER with reliability enhancement techniques. (**A**) The implementations of temporal majority voting (TMV) and masking techniques. TMVx means using x memristors to represent 1 PUF bit. (**B**) The change of BER in readout mode with different methods. (**C**) The change of BER in secure mode with different methods.

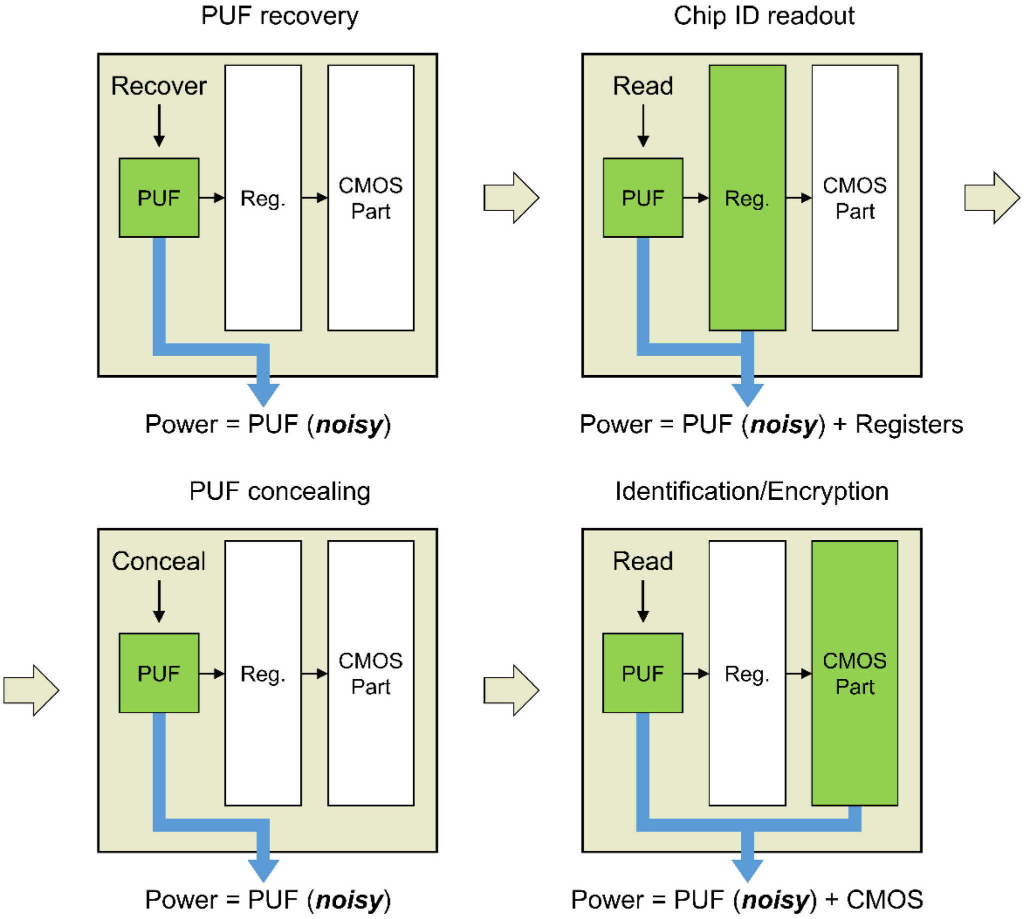

PUF recovery
Recover
PUF
Reg.
CMOS Part
Power = PUF (***noisy***)
Chip ID readout
Read
PUF
Reg.
CMOS Part
Power = PUF (***noisy***) + Registers
PUF concealing
Conceal
PUF
Reg.
CMOS Part
Power = PUF (***noisy***)
Identification/Encryption
Read
PUF
Reg.
CMOS Part
Power = PUF (***noisy***) + CMOS

Fig. S10. A side-channel secure system based on the concealable PUF . Side-channel attacks such as differential power attacks break a security system by understanding the relationship between power consumption and CMOS circuit operations. The concealable PUF provides a feasible and efficient countermeasure by leveraging its inherent write/read noise, making the side-channel signal extremely noisy whenever the chip is working.

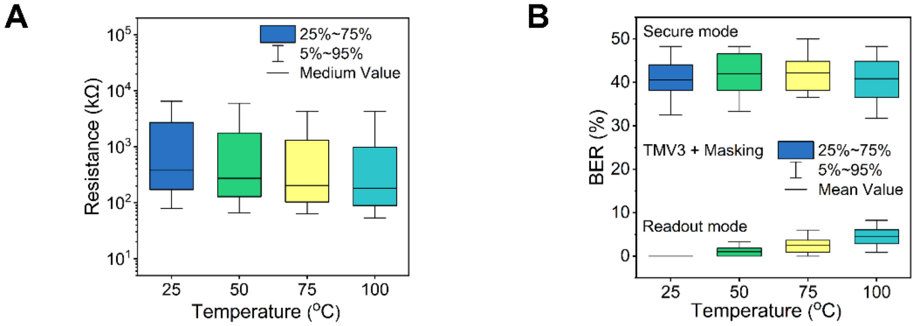


Fig. S11. High temperature test result of the concealable memristive PUF. (**A**) The change of the resistance distribution with incremental temperature. (**B**) The change of the BER in secure mode and readout mode with incremental temperature.

Table S1. NIST SP800-22 randomness evaluation results

NIST SP800-22	PUF (1280 bits per chip)				
	Chip1	Chip2	Chip3	Chip4	Chip5
1. Approximate Entropy	0.6105	0.5016	0.8116	0.8118	0.8934
2. Block Frequency	0.9110	0.2472	0.0716	0.8738	0.9989
3. Cumulative Sum	0.8768	0.7013	0.3415	0.8052	0.8982
4. FFT	0.7975	0.3049	0.1238	0.6079	0.3049
5. Frequency	1.0000	0.9554	1.0000	1.0000	1.0000
6. Longest Runs	0.9542	0.7160	0.4544	0.0633	0.8572
7. Rank	0.6937	0.6937	0.6937	0.6937	0.6937
8. Runs	0.3143	0.6149	0.4673	0.0736	0.5023
9. Serial	0.0122	0.4423	0.9218	0.1977	0.7596

Table S2. Power consumption/efficiency and delay with TMVx technique

130nm **VDD = 1.80 V** **System Clock = 10 MHz**	**Power Consumption (µW)**	**Delay (ns)**
TMV3 post-process circuit	0.891	0.0699
TMV5 post-process circuit	4.604	0.2740
D flip-flop	0.753	0.2786
SA	24.04	100.00
	Power Efficiency (pJ/bit)	**Delay (ns)**
Read without TMV circuit	2.404	100.28
Read with TMV3	7.213	300.35
Read with TMV5	12.03	500.55

Table S3. Comparison to different PUF devices

	This work	**(*7*)**	**(*38*)**	**(*22*)**	**(*52*)**	**(*53*)**	**(*54*)**
Device	Memristor	Memristor	Memristor	SRAM	Anti-fuse	CNT	MJT
Unit Area (F^2)	108	-	-	9,628	219	-	172
Uniformity	0.5013	0.501	~50	0.4805	0.5009	0.5047	0.4980
Diffuseness (%)	49.903	50.01	-	-	-	-	-
Uniqueness (%)	50.516	49.96	50.06	49	49.999	50.00	-
NIST Test	Passed	Passed	Not reported	Passed	Passed	Passed	Not reported
BER (%)	0.00	1.22	13.82	2.58	0.00	~3.00	<0.01
Concealable?	Yes	No	No	No	No	No	No

REFERENCES AND NOTES

1. Y. Gao, S. F. al-Sarawi, D. Abbott, Physical unclonable functions. *Nat. Electron.* **3**, 81–91 (2020).

2. C. Herder, M. D. Yu, F. Koushanfar, S. Devadas, Physical unclonable functions and applications: A tutorial. *Proc. IEEE* **102**, 1126–1141 (2014).

3. R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, Physical one-way functions. *Science*, **297**, 2026–2030 (2002).

4. Z. Wang, H. Wu, G. W. Burr, C. S. Hwang, K. L. Wang, Q. Xia, J. J. Yang Resistive switching materials for information processing. *Nat. Rev. Mater.* **5**, 173–195 (2020).

5. R. Arppe, T. J. Sørensen, Physical unclonable functions generated through chemical methods for anti-counterfeiting. *Nat. Rev. Chem.* **1**, 0031 (2017).

6. J. Feng, W. Wen, X. Wei, X. Jiang, M. Cao, X. Wang, X. Zhang, L. Jiang, Y. Wu, Random organic nanolaser arrays for cryptographic primitives. *Adv. Mater.* **31**, 1807880 (2019).

7. H. Nili, G. C. Adam, B. Hoskins, M. Prezioso, J. Kim, M. R. Mahmoodi, F. M. Bayat, O. Kavehei, D. B. Strukov, Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors. *Nat. Electron.* **1**, 197–202 (2018).

8. M. H. Ameri, M. Delavar, J. Mohajeri, Provably secure and efficient PUF-based broadcast authentication schemes for smart grid applications. *Int. J. Commun. Syst.* **32**, e3935 (2019).

9. A. Aysu, E. Gulcan, D. Moriyama, P. Schaumont, M. Yung, End-to-end design of a PUF-based privacy preserving authentication protocol, in *Cryptographic Hardware and Embedded Systems* (CHES, 2015), pp. 556–576.

10. J. W. Lee, D. Lim, B. Gassend, G. Edward Suh, M. van Dijk, S. Devadas, A technique to build a secret key in integrated circuits for identification and authentication applications, in *IEEE Symposium on VLSI Circuits* (IEEE, 2004), pp. 176–179.

11. G. E. Suh, S. Devadas, Physical unclonable functions for device authentication and secret key generation, in *ACM/IEEE Design Automation Conference (DAC)* (IEEE, 2007), pp. 9–14.

12. M. Alioto, Trends in hardware security: From basics to ASICs. *IEEE Solid-State Circuits Magazine* **11**, 56–74 (2019).

13. C.-H. Chang, Y. Zheng, L. Zhang, A retrospective and a look forward: Fifteen years of physical unclonable function advancement. *IEEE Circuits Syst. Magazine* **17**, 32–62 (2017).

14. D. Das, A. Golder, J. Danial, S. Ghosh, A. Raychowdhury, S. Sen, X-DeepSCA: Cross-device deep learning side channel attack, in *ACM/IEEE Design Automation Conference (DAC)* (IEEE, 2019), pp. 1–6.

15. M. S. E. Mohamed, S. Bulygin, M. Zohner, Annelie Heuser, M. Walter, J. Buchmann, Improved algebraic side-channel attack on AES, in *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)* (IEEE, 2012), pp. 146–151 2012.

16. S. Skorobogatov, How microprobing can attack encrypted memory, in 2017 *Euromicro Conference on Digital System Design (DSD)* (IEEE. 2017), pp. 244–251.

17. M. Rostami, J. B. Wendt, M. Potkonjak, F. Koushanfar, PUF: Trends and challenges of emerging physical-disorder based security, in *2014 Design,* in *Automation & Test in Europe Conference & Exhibition (DATE)* (IEEE, 2014), pp. 1–6.

18. A. B. Alvarez, W. Zhao, M. Alioto, Static physically unclonable functions for secure chip identification with 1.9–5.8% native bit instability at 0.6–1 V and 15 fJ/bit in 65 nm. *IEEE Journal of Solid-State Circuits* **51**, 763–775 (2016).

19. M. Barbareschi, G. di Natale, L. Torres, A. Mazzeo, A ring oscillator-based identification mechanism immune to aging and external working conditions. *IEEE Trans. Circuits Syst. I Regul. Pap.* **65**, 700–711 (2018).

20. K. Liu, X. Chen, H. Pu, H. Shinohara, A 0.5-V hybrid SRAM physically unclonable function using hot carrier injection burn-in for stability reinforcement, in *IEEE Journal of Solid-State Circuits* (IEEE, 2020), pp. 2193–2204.

21. K. Liu, Y. Min, X. Yang, H. Sun, H. Shinohara, A 373-F2 0.21%-native-BER EE SRAM physically unclonable function with 2-D power-gated bit cells and bias-based dark-bit detection. *IEEE J. Solid-State Circuits* **55**, 1719–1732 (2020).

22. S. K. Mathew, S. K. Satpathy, M. A. Anders, H. Kaul, S. K. Hsu, A. Agarwal, G. K. Chen, R. J. Parker, R. K. Krishnamurthy, V. De, A 0.19pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS, in *IEEE International Solid-State Circuits Conference (ISSCC)* (IEEE, 2014), pp. 278–279.

23. K. Yang, Q. Dong, D. Blaauw, D. Sylvester, A physically unclonable function with BER <10–8 for robust chip authentication using oscillator collapse in 40nm CMOS, in *IEEE International Solid-State Circuits Conference (ISSCC)* (IEEE, 2015), pp. 1–3.

24. D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, S. Sen, ASNI: Attenuated signature noise injection for low-overhead power side-channel attack immunity. *IEEE Trans. Circuits. Syst. I Regul. Pap.* **65**, 3300–3311 (2018).

25. Y. He, K. Yang, A 65nm edge-chasing quantizer-based digital LDO featuring 4.58ps-FoM and side-channel-attack resistance, in *IEEE International Solid- State Circuits Conference (ISSCC)* (IEEE, 2020), pp. 384–386.

26. A. Singh, M. Kar, S. Mathew, A. Rajan, V. De, S. Mukhopadhyay, Exploiting on-chip power management for side-channel security, in *Design, Automation & Test in Europe Conference & Exhibition (DATE)* (IEEE, 2018), pp. 401–406.

27. G. C. Adam, *A. Khiat, T. Prodromakis*, Challenges hindering memristive neuromorphic hardware from going mainstream. *Nat. Commun.*, **9**, 5267 (2018).

28. G. S. Lee, G. H. Kim, K. Kwak, D. S. Jeong, H. Ju, Enhanced reconfigurable physical unclonable function based on stochastic nature of multilevel cell RRAM. *IEEE Trans. Electron Devices* **66**, 1717–1721 (2019).

29. M. R. Mahmoodi, H. Nili, Dmitri. B. Strukov, RX-PUF: Low power, dense, reliable, and resilient physically unclonable functions based on analog passive RRAM crossbar arrays, in *IEEE Symposium on VLSI Technology* (IEEE, 2018), pp. 99–100.

30. Y. Pang, et al., A reconfigurable RRAM physically unclonable function utilizing post-process randomness source with <6×10–6 native bit error rate, in *IEEE International Solid-State Circuits Conference (ISSCC)* (IEEE, 2019), pp. 402–404.

31. Y. Pang, H. Wu, B. Gao, N. Deng, D. Wu, R. Liu, S. Yu, A. Chen, H. Qian, Optimization of RRAM-based physical unclonable function with a novel differential read-out method. *IEEE Electron Device Lett.* **38**, 168–171 (2017).

32. X. Xue, J. Yang, Y. Zhang, M. Wang, H. Lv, X. Zeng, M. Liu, A 28nm 512Kb adjacent 2T2R RRAM PUF with interleaved cell mirroring and self-adaptive splitting for extremely low bit error rate of cryptographic key, in *IEEE Asian Solid-State Circuits Conference (A-SSCC)* (IEEE, 2019), pp. 29–32.

33. J. Yang, X. Li, T. Wang, X. Xue, Z. Hong, Y. Wang, D. W. Zhang, H. Lu, A physically unclonable function with BER < 0.35% for secure chip authentication using write speed variation of RRAM (IEEE, 2018), in *European Solid-State Device Research Conference (ESSDERC),* pp. 54–57.

34. A. Chen, Reconfigurable physical unclonable function based on probabilistic switching of RRAM. *Electron. Lett.* **51**, 615–617 (2015).

35. X. Zhao, Q. Zhao, Y. Liu, F. Zhang, An ultracompact switching-voltage-based fully reconfigurable RRAM PUF with low native instability. *IEEE Trans. Electron Devices* **67**, 3010–3013 (2020).

36. G. Khedkar, D. Kudithipudi, G. S. Rose, Power profile obfuscation using nanoscale memristive devices to counter DPA attacks. *IEEE Trans. Nanotechnol.* **14**, 26–35 (2015).

37. Y. Xie, X. Xue, J. Yang, Y. Lin, Q. Zou, R. Huang, J. Wu, A logic resistive memory chip for embedded key storage with physical security. *IEEE Trans. Circuits Syst. II Express Briefs* **63**, 336–340 (2016).

38. H. Jiang, C. Li, R. Zhang, P. Yan, P. Lin, Y. Li, J. J. Yang, D. Holcomb, Q. Xia, A provable key destruction scheme based on memristive crossbar arrays. *Nat. Electron.* **1**, 548–554 (2018).

39. B. Lin, Y. Pang, B. Gao, J. Tang, D. Wu, T. W. Chang, W. E. Lin, X. Sun, S. Yu, M. F. Chang, H. Qian, H. Wu, A highly reliable RRAM physically unclonable function utilizing post-process randomness source. *IEEE J. Solid-State Circuits* **56**, 1641–1650 (2021).

40. R. Degraeve, A. Fantini, N. Raghavan, L. Goux, S. Clima, B. Govoreanu, A. Belmonte, D. Linten, M. Jurczak, Causes and consequences of the stochastic aspect of filamentary RRAM. *Microelectron. Eng.* **147**, 171–175 (2015).

41. V. G. Karpov, D. Niraula, Log-normal statistics in filamentary RRAM devices and related systems. *IEEE Electron Device Lett.* **38**, 1240–1243 (2017).

42. S. Yu, X. Guan, H. -S. P. Wong, On the stochastic nature of resistive switching in metal oxide RRAM: Physical modeling, monte carlo simulation, and experimental characterization, in *IEEEE International Electron Devices Meeting (IEDM)* (IEEE, 2011), pp. 17.13.11–17.13.14.

43. A. Chen, Comprehensive assessment of RRAM-based PUF for hardware security applications, in *IEEE International Electron Devices Meeting (IEDM)* (IEEE, 2015), pp. 10.17.11–10.17.14, 2015.

44. Y. Yoshimoto, Y. Katoh, S. Ogasahara, Z. Wei, K. Kouno, A ReRAM-based physically unclonable function with bit error rate < 0.5% after 10 years at 125°C for 40nm embedded application, in *IEEE Symposium on VLSI Technology* (IEEE, 2016), pp. 1–2.

45. J. Park, J. Park, S. Bhunia, Variable data-length error correction code for embedded memory in DSP applications. *IEEE Trans. Circuits Syst. II: Express Br.* **61**, 120–124 (2014).

46. Y. Dodis, L. Reyzin, A. Smith, Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, in *Advances in Cryptology–EUROCRYPT* (2004). pp. 523–540.

47. A. O. Aseeri, Y. Zhuang, M. S. Alkatheiri, A machine learning-based security vulnerability study on XOR PUFs for resource-constraint Internet of Things, in *2018 IEEE International Congress on Internet of Things (ICIOT)* (IEEE, 2018), pp. 49–56.

48. M. S. Alkatheiri, Y. Zhuang, Towards fast and accurate machine learning attacks of feed-forward arbiter PUFs, in *2017 IEEE Conference on Dependable and Secure Computing* (IEEE, 2017), pp. 181–187, 2017.

49. Y. Yoshimoto, Y. Katoh, S. Ogasahara, Z. Wei, K. Kouno, A ReRAM-based physically unclonable function with bit error rate < 0.5% after 10 years at 125°C for 40nm embedded application, in *2016 IEEE Symposium on VLSI Technology* (IEEE, 2016), pp. 1–2, 2016.

50. B. Gao, H. Wu, W. Wu, X. Wang, P. Yao, Y. Xi, W. Zhang, N. Deng, P. Huang, X. Liu, J. Kang, H.-Y. Chen, S. Yu, H. Qian, Modeling disorder effect of the oxygen vacancy distribution in filamentary analog RRAM for neuromorphic computing, in *2017 IEEE International Electron Devices Meeting (IEDM)* (IEEE, 2017), pp. 4.4.1–4.4.4.

51. B. Karpinskyy, Y. Lee, Y. Choi, Y. Kim, M. Noh, S. Lee, 8.7 Physically unclonable function for secure key generation with a key error rate of 2E-38 in 45nm smart-card chips, in *2016 IEEE International Solid-State Circuits Conference (ISSCC)* (IEEE, 2016), pp. 158–160.

52. M.-Y. Wu, T.-H. Yang, L.-C. Chen, C.-C. Lin, H.-C. Hu, F. Su, C.-M. Wang, James Po-Hao Huang, H.-M. Chen, C. Lu, E. Yang, R. Shen, A PUF scheme using competing oxide rupture with bit error rate approaching zero, in *2018 IEEE International Solid - State Circuits Conference (ISSCC)* (IEEE, 2018), pp. 130–132.

53. Z. Hu, J. M. M. L. Comeras, H. Park, J. Tang, A. Afzali, G. S. Tulevski, J. B. Hannon, M. Liehr, S. J. Han, Physically unclonable cryptographic primitives using self-assembled carbon nanotubes. *Nat. Nanotech* **11**, 559–565 (2016).

54. S. Lim, B. Song, S. O. Jung, Highly independent MTJ-based PUF system using diode-connected transistor and two-step postprocessing for improved response stability. *IEEE Trans. Inf. Forensics Secur.* **15**, 2798–2807 (2020).