Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Self-Instructed Reconfigurable Physical Unclonable Function Using Intrinsic Bit Alteration in CMOS-Integrated SOT-MRAM

Min Wang
Beihang University
Hanbin Wang
Beihang University
Zhongkui Zhang
Beihang University
Zhaohao Wang
zhaohao.wang@buaa.edu.cn
Beihang University
Jiaxue Deng
Beihang University
Xiaofei Fan
Truth Memory Corporation
Bi Wang
Beihang University
Kaihua Cao
Truth Memory Corporation
He Zhang
Beihang University
Yuanfu Zhao
Beijing Microelectronics Technology Institute
Hong-xi Liu
hongxi_liu@tmc-bj.cn
Truth Memory Corporation
Weisheng Zhao
weisheng.zhao@buaa.edu.cn
Beihang University

Research Article

Keywords:

Posted Date: November 17th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11754748/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

Self-Instructed Reconfigurable Physical Unclonable Function Using Intrinsic Bit Alteration in CMOS-Integrated SOT-MRAM

Min Wang[1,†], Hanbin Wang[1,†], Zhongkui Zhang[1,†], Zhaohao Wang[1,2*], Jiaxue Deng[1], Xiaofei Fan[3], Bi Wang[1,2], Kaihua Cao[3], He Zhang[1,2], Yuanfu Zhao[4], Hong-xi Liu[3,*], and Weisheng Zhao[1,2*]

[1]School of Integrated Circuit Science and Engineering, Beihang University, Beijing, China
[2]Shandong Laboratory of ASIC and Intelligent Instruments in Qingdao, Beihang University, Qingdao 266400, China
[3]Truth Memory Corporation, Beijing, China
[4]Beijing Microelectronics Technology Institute, Beijing, China
[†]These authors contributed equally
[*]Corresponding authors: zhaohao.wang@buaa.edu.cn, hongxi_liu@tmc-bj.cn, weisheng.zhao@buaa.edu.cn

Abstract

We have proposed a self-instructed reconfigurable physically unclonable function within CMOS-integrated SOT-MRAM chips, seamlessly integrating static entropy with uncertainty. By redefining bit alteration and unstable bits as entropy sources, our proposal enables reconfiguration without relying on analog modules, offering a novel perspective for hardware security design.

1 Introduction

Physical Unclonable Functions (PUFs) provide a hardware security solution with unique and device-specific fingerprint characteristics, as illustrated in Fig. 1(a). With the advancement of hardware attack technologies, reconfigurability has evolved into an important mechanism for improving PUF resilience against repeated exposure and advanced attacks, and existing designs primarily rely on cycle-to-cycle variations or adjustable operational parameters, such as timing windows or critical voltages [1–5]. However, such solutions typically suffer from narrow operating windows and high control complexity, necessitating dedicated analog modules (e.g., on-chip calibration circuits, dynamic threshold adjustment) to ensure stability, posing significant challenges for low-power and area-constrained integrated solutions.

In this work, we propose a reconfigurable PUF (rPUF) architecture that exploits intrinsic bit alteration as an entropy source in spin-orbit torque magnetic random access memory (SOT-MRAM). The key idea is to use the response generated in one reconfiguration cycle to determine the sensing configuration of the subsequent cycle. Specifically, the relative resistance ordering of two magnetic tunnel junctions (MTJs) may reverse between their P-P and AP-AP states, as illustrated in Figs. 1(b)-(c). The proposed digital self-instructed mechanism enables recursive reconfiguration without external random inputs, analog calibration, or modifications to the SOT-MRAM architecture.

2 Results

A. Self-Instructed Protocol

As illustrated in Fig. 2, the proposed protocol can be functionally interpreted as a recursive composition of mappings, in which each reconfiguration response serves as a self-instruction for generating the subsequent response. Bit alteration acts as the primary entropy source: the digital map generated in the previous cycle determines the sensing state of the next cycle (AP-AP or P-P), thereby forming a recursive reconfiguration chain. In addition, read instability from unstable bits provides an auxiliary entropy source, further enhancing the randomness of reconfiguration responses.

B. Carrier: SOT-MRAM

The proposed rPUF was evaluated on a 512 Kb SOT-MRAM. The inherent non-volatility and high endurance of SOT-MRAM make it a promising carrier for reconfigurable PUF implementation [6]. The SOT-MRAM test chip uses differential readout circuitry integrated with peripheral CMOS circuitry, with each basic unit containing a pair of SOT-MTJs (see Fig. 3). Through a multiplexer-based monitoring structure, four combinations of resistance states (AP-AP, AP-P, P-AP, and P-P) can be generated within each unit.

The bit alteration phenomenon is experimentally confirmed by comparing digital maps generated under all-AP and all-P states, as shown in Fig. 4. Both digital maps exhibit uniformity values centered near the ideal value of 50% after XOR post-processing. The experimental setup is presented in Fig. 5.

C. Primary Entropy Source: Bit Alteration

To clarify the physical origin of bit alteration, the P-state resistance R_P and the tunneling magnetoresistance ratio TMR are assumed to follow independent normal distributions, with the AP-state resistance given by $R_{AP} = R_P\,(1 + TMR)$. For a pair of MTJs, bit alteration occurs when their relative resistance ordering is reversed after switching from the P-P state to the AP-AP state, as illustrated in Fig. 6(a). The bit-alteration probability P_{BA} is given by the total probability of the two discordant ordering events. Under a bivariate normal approximation, it is related to Kendall's rank correlation coefficient τ by $P_{BA} = (1 - \tau)/2$, where

$$\tau = \frac{2}{\pi} arcsin \left[\frac{(1 + \mu_{TMR})\,\sigma_{R_P}}{\sqrt{\sigma_{R_P}^2 \left[\sigma_{TMR}^2 + (1 + \mu_{TMR})^2\right] + \mu_{R_P}^2 \sigma_{TMR}^2}} \right]. \tag{1}$$

Monte Carlo simulations further verify the analytical result under the modeled conditions. P_{BA} varies with the coefficient of variation of R_P and TMR, while remaining nearly insensitive to the mean values of R_P and TMR (Figs. 6(b)-(d)). Those results indicate that bit alteration is governed primarily by intrinsic device-to-device variations.

The equivalent entropy ($\hat{E}$) is introduced as a metric for evaluating bit alteration quality [2]. The binary comparison result of the dual-MTJ unit is defined as $X = (p_0, p_1)$, where p_0 and p_1 represent the comparison outcomes for the P-P state and AP-AP state, respectively. As shown in Fig. 7, after XOR post-processing, the four output combinations of each dual-MTJ unit become nearly equiprobable, resulting in an equivalent entropy of 1.9994, as the theoretical maximum is 2.

D. Auxiliary Entropy Source: Unstable Bits

In addition to intrinsic bit alteration, read instability associated with unstable bits is exploited as an auxiliary source of stochastic entropy. The multiple roles of unstable bits in the proposed design are illustrated in Fig. 8. In a single-read measurement, the unstable-bit rate derived from the read bit error rate (BER) is approximately 1.87% (see Fig. 8(a)). When error bits are accumulated over repeated reads, the observed proportion of total unstable bits increases and eventually approaches saturation (see Fig. 8(b)). While typically viewed as a drawback, these unstable bits are harnessed here as an auxiliary entropy source (see Fig. 2 and Fig. 8(c)). Unstable bits are exploited during response diversification, whereas a self-write-back (SWB) operation (see Fig. 8(d)) stabilizes them for reliable readout.

3 Discussion

A. Reconfiguration Evaluation

We next evaluate whether the combined entropy sources generate reconfiguration responses with low inter-response correlation. Without the inclusion of unstable bits, the correlation matrix exhibits a discernible band-like pattern, indicating residual inter-response dependence and potential predictability (see Fig. 9(a)). Figure 9(b) shows that incorporating unstable bits substantially reduces the inter-response correlation, as indicated by the more uniformly distributed off-diagonal correlation coefficients. The average inter-reconfiguration Hamming distance (HD) is 50.04% (see Fig. 9(c)). The inter-die HD remains close to 50%, whereas the intra-die HD for repeated readout approaches zero (see Fig. 9(d)), yielding a high inter-/intra-die HD ratio.

B. Robustness Against Environmental Variations

The temperature-dependent measurements were performed using the thermal test system, with experiments conducted at –40 °C and 85 °C. Read reliability is enhanced by the SWB operation. As demonstrated in Fig. 10, SWB suppresses the read BER across the tested temperature range. In addition to temperature robustness, MRAM non-volatility allows the reconfiguration map to be retained across power loss. The retained map can be used to resume reconfiguration after power is restored.

C. Security Evaluation

The randomness of the reconfigurable PUF is assessed via the NIST SP800-22, autocorrelation function (ACF) analysis, and machine-learning attack evaluations using single-bit prediction models (Figs. 11(a)-(c)). Under an m-bit matching rule, the probability of satisfying the authentication condition decreases rapidly as the number of required matches increases (Fig. 11(d)). Table I summarizes the performance comparison with state-of-the-art PUF designs, highlighting the reconfiguration flexibility of the proposed design.

4 Conclusion

This paper presents a self-instructed reconfiguration protocol evaluated on SOT-MRAM chips, in which intrinsic bit alteration serves as the primary entropy source and unstable bits provide an

auxiliary stochastic entropy source. The protocol eliminates the need for analog calibration modules and external random inputs, showing potential in hardware security.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant 62674012, the National Key Research and Development Program of China under Grant 2021YFB3601303, the National Program for Support of Top-notch Young Professionals, and the Fundamental Research Funds for the Central Universities.

References

[1] L. Zhang, Z. H. Kong, C.-H. Chang, A. Cabrini, and G. Torelli, "Exploiting process variations and programming sensitivity of phase change memory for reconfigurable physical unclonable functions," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 6, pp. 921–932, 2014.

[2] L. Zhang, X. Fong, C.-H. Chang, Z. H. Kong, and K. Roy, "Highly reliable spin-transfer torque magnetic RAM-based physical unclonable function with multi-response-bits per cell," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 8, pp. 1630–1642, 2015.

[3] H. Shao, Y. Zhou, Z. Ning, W. Luo, X. Bin, J. Yang, K. Tang, and R. Huang, "First demonstration of high throughput and reliable homomorphic encryption using FeFET arrays for resource-limited IoT clients," in *2024 IEDM*.

[4] Y. Pang, B. Gao, D. Wu, S. Yi, Q. Liu, W.-H. Chen, T.-W. Chang, W.-E. Lin, X. Sun, S. Yu, *et al.*, "A reconfigurable rram physically unclonable function utilizing post-process randomness source with $< 6\times10^{-6}$ native bit error rate," in *ISSCC*, IEEE, 2019.

[5] Y. Cao, H. Yang, J. Yang, Q. Liu, and M. Liu, "A 67F2 reconfigurable PUF using 1T2R RRAM switching competition in 28nm CMOS with 5e-9 bit error rate," in *2024 VLSI*.

[6] B. Dieny, I. L. Prejbeanu, K. Garello, P. Gambardella, P. Freitas, R. Lehndorff, W. Raberg, U. Ebels, S. O. Demokritov, J. Akerman, *et al.*, "Opportunities and challenges for spintronics in the microelectronics industry," *Nature Electronics*, vol. 3, no. 8, pp. 446–459, 2020.

[7] X. Li, B. Lin, B. Gao, Y. Lu, S. Yang, Z. Su, T.-Y. Shen, J. Tang, H. Qian, and H. Wu, "A memristor-based unified PUF and TRNG chip with a concealable ability for advanced edge security," *Science Advances*, vol. 11, no. 13, p. eadr0112, 2025.

[8] K. M. Lee, R.-H. Koo, M. Kim, J. Hwang, J.-J. Kim, and J.-H. Lee, "Concealable and bit error-free breakdown-based physical unclonable functions using magnetic tunnel junctions," in *2025 IEEE International Electron Devices Meeting (IEDM)*, pp. 1–4, IEEE, 2025.

[9] S. Lee, J. Kang, J.-M. Kim, N. Kim, D. Han, T. Lee, S. Ko, J. Yang, S. Lee, S. Lee, *et al.*, "Spintronic physical unclonable functions based on field-free spin–orbit-torque switching," *Advanced Materials*, vol. 34, no. 45, p. 2203558, 2022.

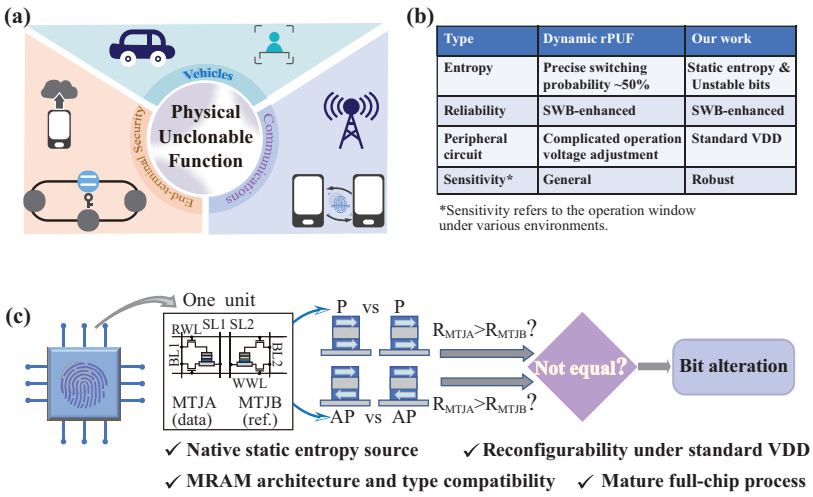


Figure 1: (a) Application scenarios of physical unclonable functions. (b) Comparison between conventional dynamic rPUFs and the proposed design. (c) Bit alteration means that the relative resistance order of two MTJs changes between P-P and AP-AP states. Bit alteration serves as the primary entropy source in this work.

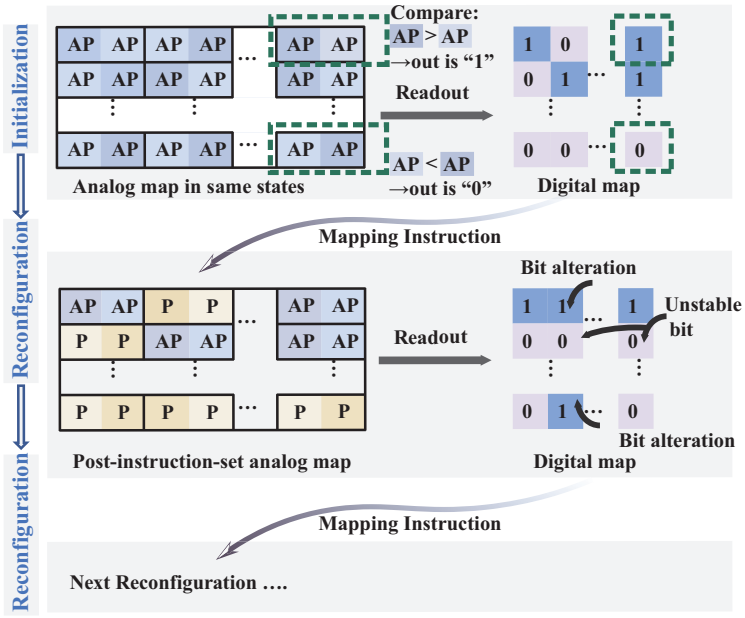


Figure 2: Workflow of the proposed self-instructed reconfiguration protocol. The response from the previous reconfiguration determines the mapping state of the current cycle. Darker colors indicate higher resistance, and unstable bits denote minor read instabilities.

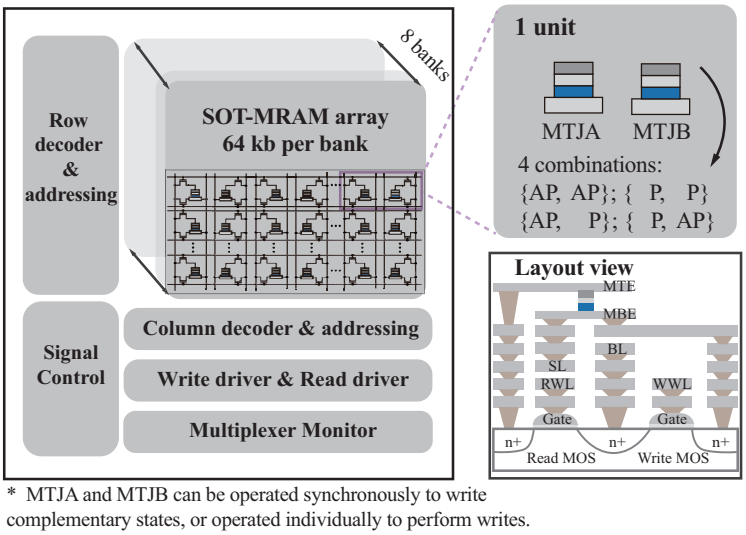


Figure 3: Overall schematic of the measured SOT-MRAM chips. Thanks to the multiplexer monitor, the two MTJs within one unit can be operated flexibly. In one unit, two MTJs can hold four combinations (upper right). The layout view (bottom right) illustrates the hybrid CMOS/SOT-MTJ integration.

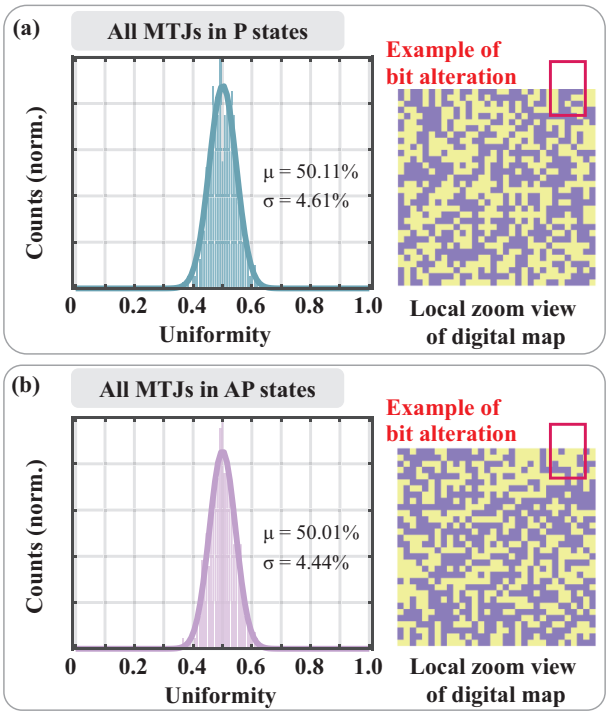


Figure 4: Uniformity and local views of digital maps for (a) all-P and (b) all-AP states. By default, uniformity is improved by XOR post-processing.

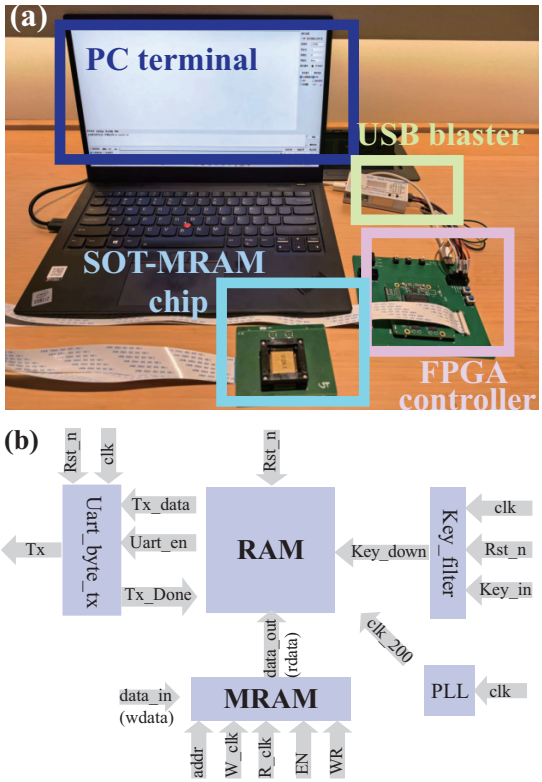


Figure 5: (a) Experimental setup for the SOT-MRAM chip. (b) Internal schematic of the test system.

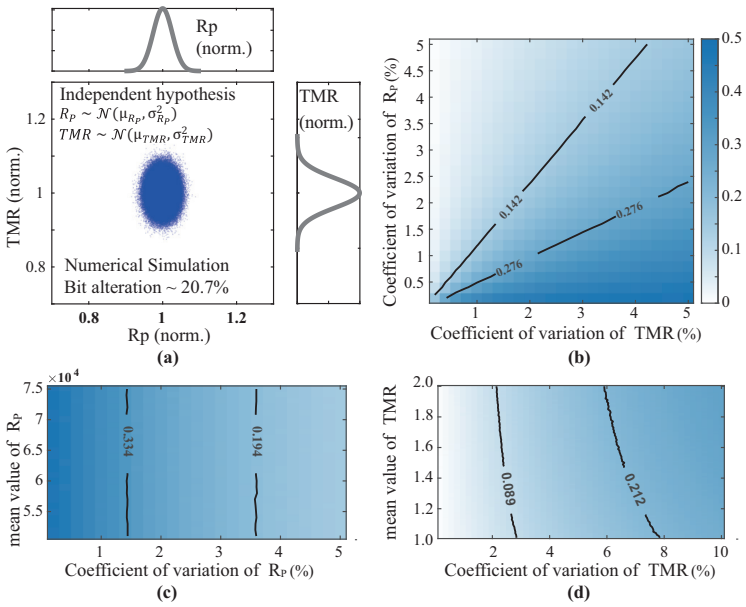


Figure 6: Statistical origin of bit alteration. (a) Numerical model of bit alteration derived from the statistical distributions of R_P and TMR. (b) Simulated bit alteration probability under different cases of process variations. Insensitivity of bit alteration to the mean values of (c) R_P and (d) TMR. The solid lines in subfigures (b)-(d) are contour lines. The calculated results demonstrate that bit alteration is mainly governed by intrinsic device-to-device variations and is largely insensitive to the mean values.

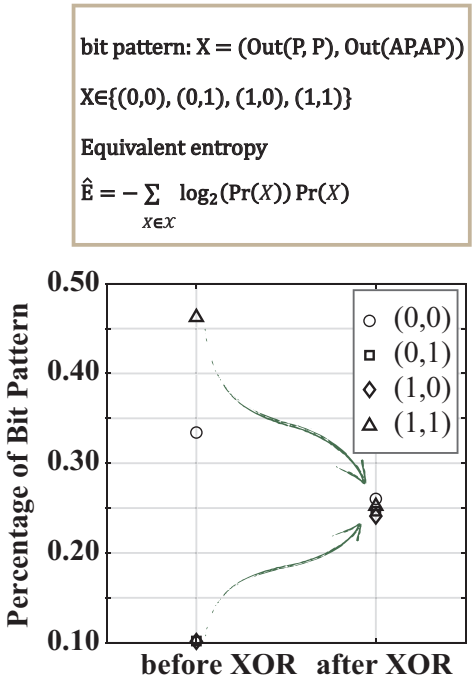


Figure 7: Calculation of equivalent entropy, enhanced by XOR post-processing. $\mathcal{X}$ means the set of X as the binary comparison result of the dual-MTJ unit.

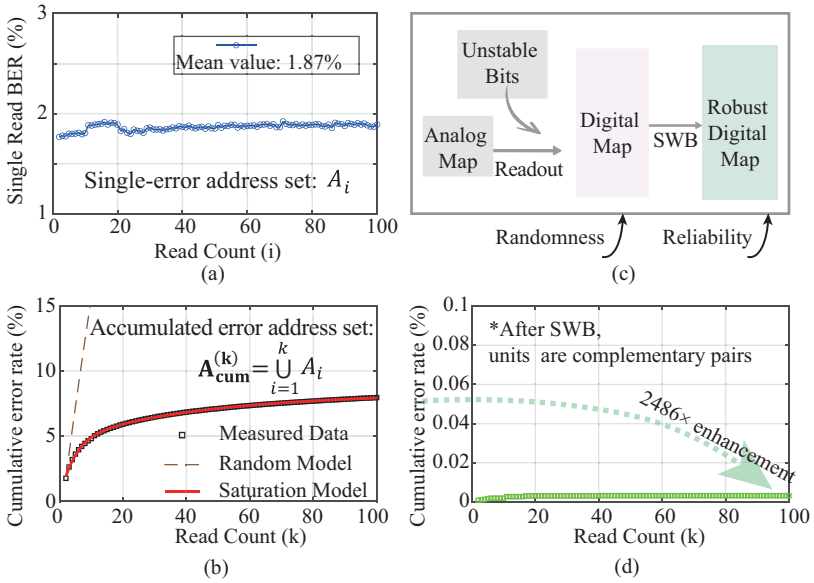


Figure 8: (a) Read BER in a single-read operation and (b) cumulative error rate as a function of read count under the same-state comparison. (c) Illustration: unstable bits provide auxiliary entropy and can be stabilized by the SWB operation. (d) Cumulative error rate after SWB operation.

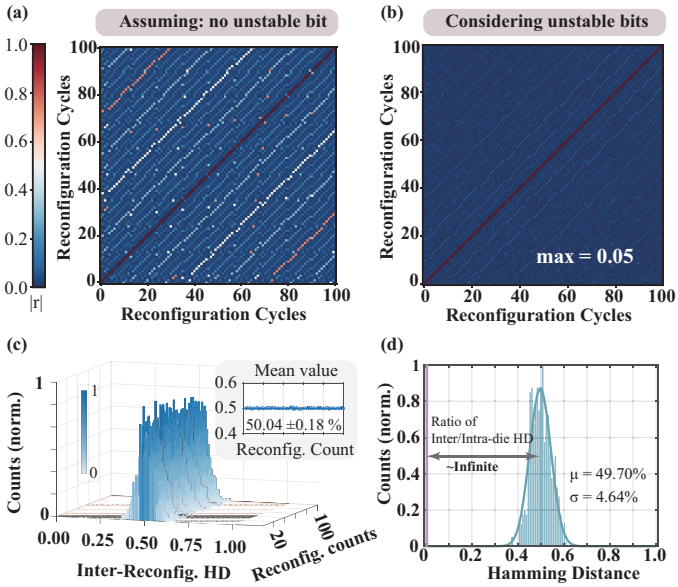
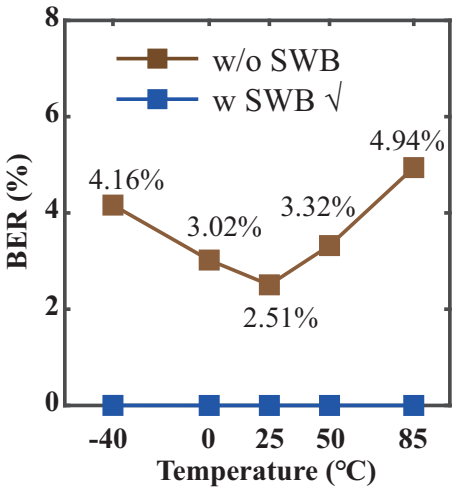


Figure 9: (a) Numerical simulation of the correlation matrix among reconfigurations without unstable bits. (b) Correlation matrix obtained by incorporating the measured unstable-bit characteristics. (c) Statistics of inter-reconfiguration Hamming distance (HD). (d) Intra- and inter-die HD.



*SWB mode:
The worst-case error bit count ≤8 bits,
corresponding to BER ~ 1.53×10^{-5}.

Figure 10: Measured read BER at various operating temperatures. The SWB operation enables reliable PUF readout by leveraging the inherent write and read reliability of SOT-MRAM in memory mode.

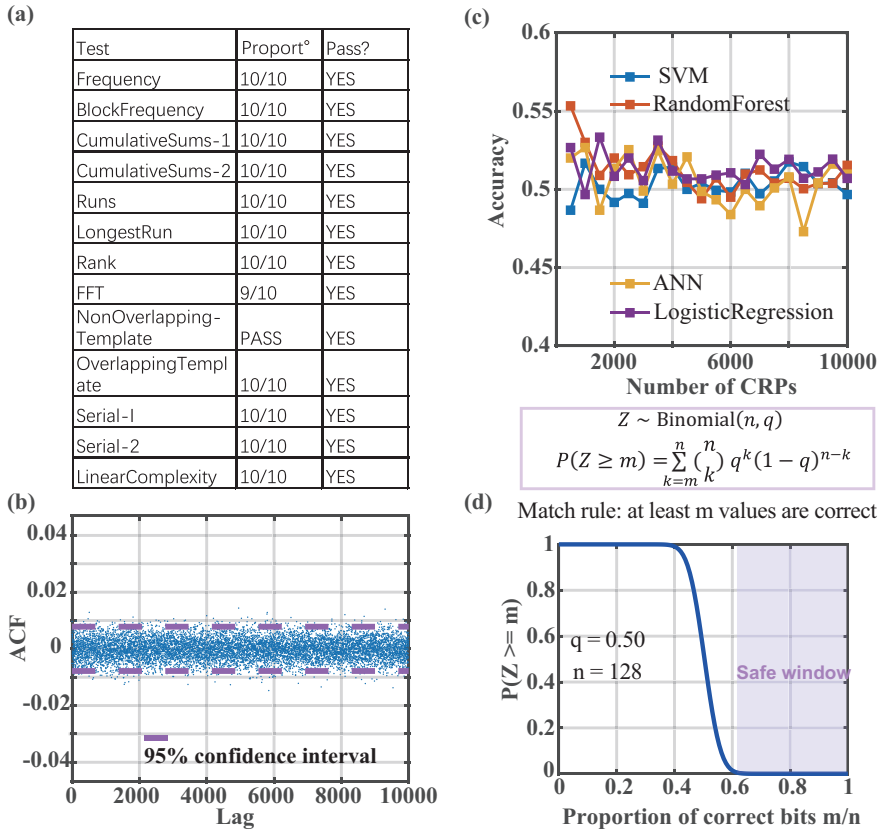


Figure 11: Security evaluation by (a) NIST SP800-22, (b) autocorrelation function test, (c) single-bit machine-learning attacks, and (d) matching-rule analysis.

Table 1: Comparison with state-of-the-art PUFs.

	VLSI'24 [5]	**Sci. Adv'25 [7]**	**IEDM'25 [8]**	**Adv. Mat.'22 [9]**	**Our Work**
Device / Tech	RRAM; Full chip test	Memristor; Full chip test	STT-MRAM; Macro	EB SOT; Device level	SOT-MRAM; Full chip test
Entropy Source	Switching time	Forming condition	Breakdown probability	Switching polarity	Bit alteration & Unstable bits
Reconfigurability	Yes	No	No	Yes	Yes
Control Complexity	High	Medium	Medium	Medium	Low
Uniqueness	∼50.01%	50.06 ± 6.45%	49.4%/50.0%	51.7 ± 0.4%	49.7% / 50.04%
Uniformity	Passed NIST	50.09 ± 0.25%	49.9%/50.0%	53.1%	50.01% ∼ 50.11%
Read reliability	0.021% [a] $< 5 \times 10^{-9}$ [b]	0.00% (Intra-HD)	0	0	$< 1.53 \times 10^{-5}$
Temperature	–40°C ∼ 125°C	–40°C ∼ 125°C	25°C ∼ 125°C	-100°C ∼ 125°C	–40°C ∼ 85°C
Anti-Attack	Yes	Concealable PUF	Yes	Magnetic-tampering robutness	Yes

[a] Native BER; [b] Calibrated.