

ML-Resistant and Reliable ChainX PUF Based on FeFET Arrays for Resource-Limited IoT Security

Hanyong Shao^{1,2}, Zhiyuan Ning¹, Yuejia Zhou¹, Wenpu Luo¹, Xinyu Bin⁴, Meng Li^{1,3}, Kechao Tang^{1,5*} and Ru Huang^{1,3,5*}

¹School of Integrated Circuits & ²Academy for Advanced Interdisciplinary Studies & ³Institute for Artificial Intelligence, Peking University, Beijing 100871, China; ⁴University of Science and Technology of China, Hefei, Anhui 230026, China;

⁵Beijing Advanced Innovation Center for Integrated Circuits, Beijing 100871, China. *E-mail: {tkch, ruhuang}@pku.edu.cn

Abstract—Resistance to machine learning (ML) modeling attacks remains challenging for Physical Unclonable Functions (PUFs), particularly considering the increasing parameter scale of AI models and escalating computational power. In this work, we propose ChainX PUF, a strong PUF macro design based on 2T ferroelectric FET (FeFET) arrays, with advantages in ML resistance, reliability and efficiency. This PUF design utilizes bitwise XOR of the input challenges with stored matrix weights in the spatial dimension, where the outputs are chained to the next round of inputs for nonlinear coupling in the temporal dimension. This spatial-temporal coupling results in a modeling accuracy of no higher than 55% under various advanced ML modeling attacks. Benefiting from the optimized entropy source and the high on/off ratio of FeFETs, experimental results demonstrate a reliably low native bit error rate (BER) down to 1.7% at 100°C. Based on the area-saving iterative design and the low power operation of FeFETs, the ChainX PUF achieves low hardware overhead and superior energy efficiency of 3 fJ/bit.

Keywords—FeFET, PUF, ML resistance, IoT security

I. INTRODUCTION

The rapid proliferation of edge devices has significantly increased data interactions between cloud and edge networks, making the authentication of widely deployed edge devices a critical aspect of IoT security [1],[2]. As hardware security primitives, PUFs utilize unpredictable physical randomness to generate unique challenge-response pairs (CRPs) for cloud-edge verifications. Therefore, the reproducible reliability and ML modeling resistance of CRPs are essential prerequisites for trustworthy deployment of PUFs in edge scenarios.

However, with the rapid advancement of AI algorithms—particularly the continuous growth in model parameters and computational power, existing strong PUFs including CMOS-based PUFs and non-volatile memory (NVM)-based RRAM PUFs [3]–[9], are becoming increasingly vulnerable to the emerging ML attacks [10]–[12]. Moreover, resource-limited edge scenarios pose significant area- and energy-efficiency challenges for CMOS PUFs. Although NVM PUFs exhibit substantially lower hardware and power overhead compared to CMOS, they are notably more sensitive to PVT fluctuations, leading to additional reliability concerns, as shown in Fig. 1a.

To address these issues, we propose and experimentally demonstrate **ChainX PUF**, a novel strong PUF design based on a compact 2T FeFET array. Its name reflects a distinctive chained XOR coupling feature, which iteratively combines current output bits with historical input bits (Fig. 1b). For the first time, ChainX PUF introduces nonlinear coupling in the temporal dimension, transforming correlated inputs into independent outputs to mitigate the differential cryptanalysis. Furthermore, by employing bitwise XOR operations between input vectors and stored weight matrix in the spatial domain, ChainX PUF achieves significantly enhanced ML-resistance. Benefiting from the high on/off ratio of FeFETs compared to other NVM devices, as well as our optimized entropy source and device endurance, its high reliability is experimentally verified. By further leveraging the compact 2T array structure, our design achieves superior area- and energy-efficiency.

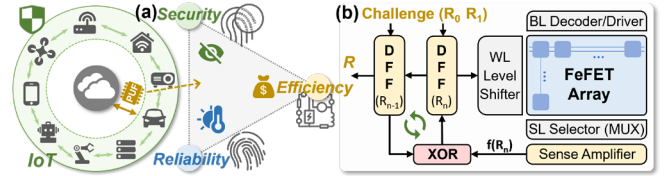


Fig. 1. (a) Triangle requirements of security, reliability, and cost that a PUF must satisfy for practical IoT security. (b) Schematic illustration of ChainX PUF, which introduces chained XOR coupling in the temporal dimension.

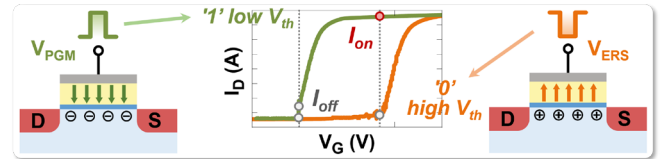


Fig. 2. Device structure and I_D - V_G curves of FeFET, where the positive or negative gate pulses change the polarization of FE layer, affect the channel charge, shift the I-V curve left or right, and enable weight program or erase.

II. PROPOSED DESIGN OF CHAIN-XOR PUF MACRO

A. Entropy source and PUF enrollment

HfO₂-based FeFET is promising for future computing due to its non-volatility, high efficiency, and CMOS-compatibility [13]. By applying V_{PGM} or V_{ERS} , the polarization direction of FE layer can be switched, modulating the I_D - V_G in Fig. 2. The high and low threshold voltages V_T correspond to the stored weight of '0' and '1', respectively. A single FeFET outputs high I_D only when a high V_G is applied to the '1' state (low V_T), performing a near-digital AND logic between the input and stored weight. The high on/off ratio improves sense margin of ADCs and enhances reliability while reducing energy cost.

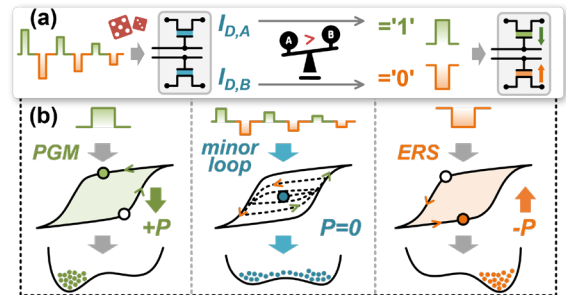


Fig. 3. (a) Enrollment of PUF, where minor loop induces random switching of domains, leading to higher I_D variations as the entropy source. This is due to the minor loop in (b) leaving more unstable domains in metastable state.

Enrollment is the first step for our PUF, leveraging the entropy source to pre-program the FeFETs into unpredictable yet stable V_T states. A random and reliable entropy source is generated based on minor loop program, as shown in Fig. 3a. Specifically, ChainX PUF uses an alternating and decreasing waveform to program two FeFETs in the same cell through minor loops, resulting in significant variations in drain current. Subsequently, a differential comparison generates '1' and '0' complementary pairs, which represent random bits. These bits are stored as secret weights W , forming unique fingerprints of ChainX PUF. The randomness originates from the inherent instability of FE domains depicted in Fig. 3b. Both the spatial distribution and stochastic switching of domains contribute to these variations at the middle V_T across different cycles.

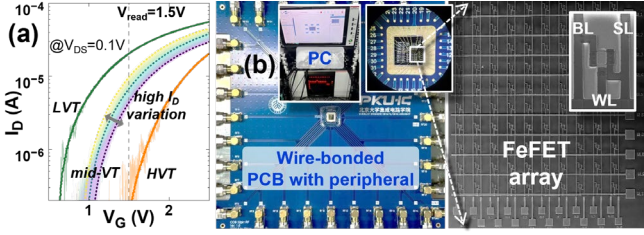


Fig. 4. (a) Measured I_D - V_G broadening of FeFET over 1k cycles during PUF enrollment. Mid- V_T exhibits significant variation, ideal as an entropy source. (b) SEM images of FeFET array, wire-bonded to PCB with peripheral.

The measured I_D - V_G and middle V_T fluctuations during enrollment are shown in **Fig. 4a**, exhibiting a memory window of 1.1V. ChainX PUF utilizes FeFETs with an $\text{Hf}_{0.95}\text{Al}_{0.05}\text{O}_2$ (HAO) as the FE layer and Al_2O_3 interlayer to enhance the endurance and stochasticity during the enrollment, as reported in our previous work [9]. **Fig. 4b** illustrates the wire-bonded FeFET arrays integrated with a PCB and peripheral circuitry, used for demonstration and further evaluations.

B. Chained XOR and PUF authentication

The critical challenges faced by existing PUFs include ML modeling of CRP relationships and differential analysis attack (similar inputs C are used to infer R). To mitigate these risks, we propose and verify a novel chain-XOR scheme during the generation of CRPs as shown in **Fig. 5**, using XOR coupling in both temporal and spatial dimensions for authentication, which significantly enhances the complexity and diffuseness.

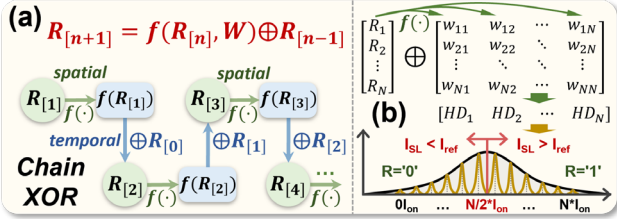


Fig. 5. (a) The spatial-temporal coupling method of ChainX PUF. The spatial operation $f(\cdot)$ on R and W is illustrated in (b), where the Hamming distances are summed and compared to $I_{\text{ref}} = N/2 \cdot I_{\text{on}}$ to generate output $f(R_{[n]})$.

The initial inputs $R_{[0]}$ and $R_{[1]}$ pass through the ChainX PUF to generate a new response R , iteratively updated by the following equation. Each iteration involves two nonlinear functions, $f(\cdot)$ in spatial and \oplus in temporal dimensions:

$$R_{[n+1]} = f(R_{[n]}, W) \oplus R_{[n-1]} \quad (1)$$

Spatial dimension $f(\cdot)$: This describes the relationship $R = f(C, W)$ of strong PUFs, which generate responses from input challenges combined with internal fingerprints W (weights). In the proposed ChainX PUF, the spatial function $f(\cdot)$ maps an input binary vector into a new binary vector through bitwise-XOR, column-wise summation, and split-comparisons, as illustrated in **Fig. 5b**. To implement $f(\cdot)$, the complementary 2T FeFET arrays with paired WLs are utilized as shown in **Fig. 6a**. The weight matrix of the array forms W in Eq. (1), where each basic cell consists of two FeFETs with opposite states to store a single w_{ij} . As mentioned before, a single FeFET can perform an AND logic. Since the WL input R_i and w_{ij} within single cell are paired, this achieves XOR in the i^{th} row cell: $R_i \cdot \bar{w}_{ij} + \bar{R}_i \cdot w_{ij} = R_i \oplus w_{ij}$. Therefore, SLs of the j^{th} column output $SL_j = \sum_i (R_i \oplus w_{ij}) = HD(R \oplus w_j)$, meaning I_{SL} is proportional to the Hamming distance (HD) between R and w_j of j^{th} column. SA compares the I_{SL} with I_{ref} to generate new binary vector $f(R_{[n]})$, completing the spatial XOR coupling step (note that N is the array size while n represents the total iteration count).

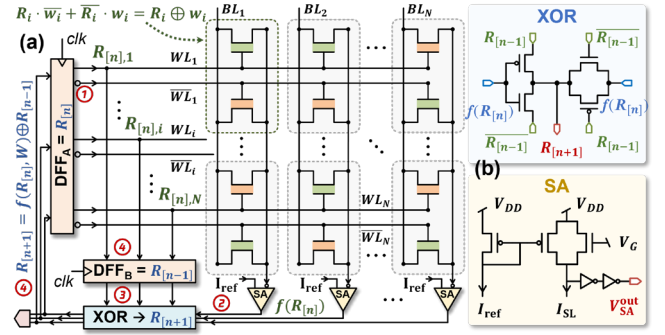


Fig. 6. (a) Circuit design of the 2T FeFET array-based ChainX PUF. DFFs sequentially feed input vectors into the array following the red numbering and update iteratively based on the outputs from SA and XOR. (b) Peripheral XOR and SA circuits are optimized to balance latency and area overhead.

Temporal dimension \oplus : The XOR operation \oplus in Eq. (1) is implemented using the peripheral D flip-flop (register) and XOR module shown in **Fig. 6a**. The red numbers in the figure indicate the sequence of iterative operations. The XOR module performs nonlinear logic between the output $f(R_{[n]})$ and the previous sequence $R_{[n-1]}$. The two registers store the current $R_{[n]}$ and the previous $R_{[n-1]}$. After the XOR module generates a new $R_{[n+1]}$, the registers are updated sequentially to store $R_{[n+1]}$ and $R_{[n]}$. This peripheral circuitry in **Fig. 6b** features low area cost and minimal authentication latency.

During identity verification, the challenges are the initial inputs $R_{[0]}$, $R_{[1]}$ and the iteration counts k_1, k_2, \dots, k_n , while outputs correspond to $R_{[k_1]}, R_{[k_2]}, \dots, R_{[k_n]}$. Unlike existing strong PUF implementations that need multiple inputs to verify CRP relationships, this approach leverages the unique pattern of the iteration sequence from a single input, avoiding exposure of CRPs and mitigating ML attacks. The chained XOR amplifies minor differences in the initial inputs during iteration, achieving ideal diffuseness to resist differential attacks. The high on/off ratio of FeFET enables near-digital XOR logic, preventing errors during iterations. Therefore, unlike all other PUF designs, ChainX PUF can continuously generate new $R_{[n]}$ using the initial inputs $R_{[0]}$ and $R_{[1]}$, similarly to a pseudo-random number generator (PRNG).

III. DISCUSSION AND EVALUATIONS

Based on the test platform in **Fig. 4b**, we comprehensively evaluate metrics including security, reliability, and overhead.

A. Security evaluations

The key of ChainX PUF lies in its time-domain coupling, enabling high-quality pseudo-random bit streams. Different inputs will yield distinct random output patterns. Notably, our approach cycles multiple iterations but generates multi-bit responses per iteration (e.g., 64-bit), while traditional PUFs need to generate 1-bit responses repeatedly. As a result, the overall CRP generation latency remains comparable.

Compared to similar coupling methods in control groups, our chained XOR in Eq. (1) demonstrates higher randomness. **Fig. 7a** benchmarks the randomness of four different schemes: (i) the proposed method (Eq. 1); (ii) CycPUF from [14], which directly uses the output as the new input (Eq. 2); and two schemes where (iii) the new input is generated by XORing the current input with the current output (Eq. 3); and (iv) XORing the current output with the previous output (Eq. 4):

$$R_{[n+1],ctrl1} = f(R_{[n]}, W) \quad (2)$$

$$R_{[n+1],ctrl2} = f(R_{[n]}, W) \oplus R_{[n]} \quad (3)$$

$$R_{[n+1],ctrl3} = f(R_{[n]}, W) \oplus f(R_{[n-1]}, W) \quad (4)$$

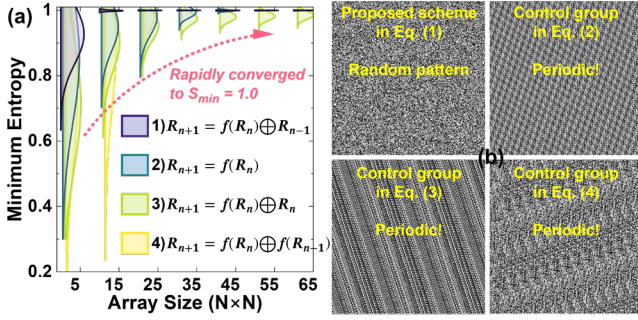


Fig. 7. (a) Minimum entropy of the output 1Mbits for four temporal coupling schemes Eq. 1~4 vs. array size N , showing significant higher randomness in the Eq. 1. (b) Only output of Eq. 1 exhibits a random spatial bit distribution.

In simulations with different array sizes N , the minimum entropy of the output response converged to 1 as N increased. The proposed $R_{n+1} = f(R_n, W) \oplus R_{n-1}$ already reaches near 1 at smaller N . Additionally, the pattern of output bits in Fig. 7b reveals that only our scheme exhibits random distribution.

The mathematics behind it can be attributed to the high-order nonlinear recursive operation, which creates diffusion, meaning that a change in a single bit affects subsequent bits, and confusion, in which the XOR operation masks the original bit. This leads to chaotic behavior during iterations, extremely sensitive to initial conditions. It resembles a second-order nonlinear feedback shift register (NLFSR) [15], with a state space and cycle length much larger than the LFSR. Its statistical properties are very close to those of a true random sequence. The randomness of the ChainX PUF is confirmed by 10M-bit random bits that pass both NIST SP 800-22 and the more stringent SP 800-90B shown in Table I.

TABLE I. ChainX PUF passes all the NIST SP 800-22 and 800-90B tests.

SP 800-22 Test items	PRN ₁	PRN ₂	PRN ₃	PRN ₄	PRN ₅	Pass rate	SP 800-90B Test items	Pass rate
Frequency	0.53	0.91	0.07	0.53	0.53	5/5	IID Permutation	5/5 PASS
Block Freq.	0.91	0.53	0.35	0.74	0.74	5/5	Chi-Square (χ^2)	5/5 PASS
Com. Sums	0.53	0.74	0.07	0.74	0.35	5/5	Independence	score>2001 dof=2046
Runs	0.53	0.12	0.74	0.74	0.74	5/5	Chi-Square (χ^2)	5/5 PASS score>3.33 dof=9.00
Longest Run	0.99	0.07	0.12	0.07	0.02	5/5	Goodness-of-fit	
Rank	0.74	0.74	0.04	0.74	0.91	5/5	LRS Test	5/5 PASS Pr>0.60
FFT	0.53	0.53	0.07	0.12	0.12	5/5	Min Entropy	>0.993528
Non-Over. Tem.	0.35	0.12	0.35	0.35	0.74	5/5	Restart Test	5/5 PASS
Overlap. Tem.	0.12	0.53	0.74	0.99	0.21	5/5	Non-IID 10 items (MCV, ... LZ7Y)	5/5 PASS >0.829092
Universal	0.99	0.21	0.53	0.91	0.91	5/5		
Approx. Entropy	0.53	0.21	0.53	0.53	0.74	5/5		
Rand. Excursion	0.18	0.02	0.14	0.16	0.39	5/5		
Rand. Exc.Var.	0.41	0.04	0.05	0.05	0.86	5/5		
Serial	0.91	0.74	0.35	0.12	0.91	5/5		
Lin. Complexity	0.34	0.35	0.35	0.74	0.35	5/5		

Diffuseness is a critical metric for a secure PUF that is resistant to differential cryptanalysis. It requires that the PUF, like a hash function, maps similar input vectors to orthogonal and independent outputs [16]. However, in most PUF designs, when inputs change slightly (e.g., a 1-bit change), the output is unlikely to change. This is because most PUF designs rely on the accumulation of analog quantities (delay, current or charge) and use a comparator (e.g., arbiter, sense amplifier, comparator) to convert the aggregated result into binary. This vulnerability allows adversaries to exploit plaintext selection combined with differential attacks, using known inputs that are close to the target CRP to infer the correct outputs [17].

Due to the nonlinear recursive operation inside ChainX PUF, which induces chaotic behavior with high sensitivity to initial inputs, it shows excellent diffuseness, approaching 0.5. As demonstrated in Fig. 8a, even when the 130-bit initial input changes by just a single bit, the diffuseness between the outputs $R_{n, \text{before}}$ and $R_{n, \text{change}}$ approaches 0.5 quickly after fewer than 10 iterations.

We conduct ML modeling attacks on ChainX PUF using three kinds of algorithmic approaches. As depicted in Fig. 8b, we first applied eight common neural networks to fit the PUF's inputs and outputs, assessing its security. These algorithms,

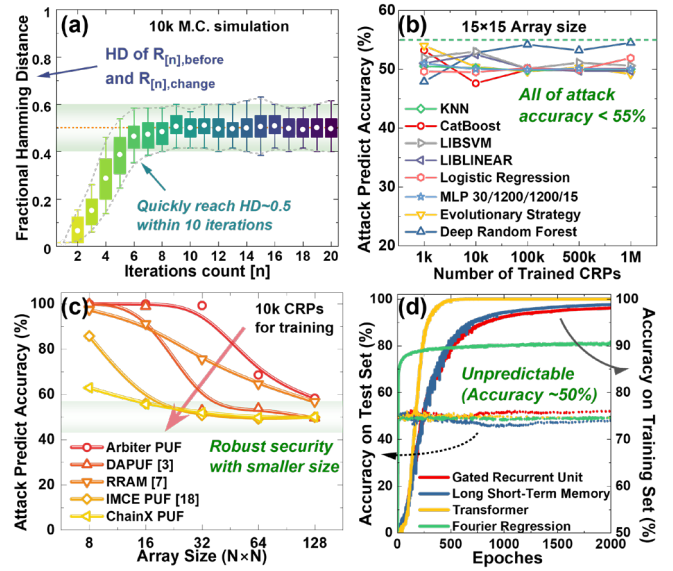


Fig. 8. Security evaluations. (a) An ideal diffuseness means that a single-bit change in the initial input leads to significant output differences during iteration. (b) Nonlinear fitting of CRPs using black-box neural networks. (c) Modeling of W using white-box Simulated Annealing, considering the PUF circuit design. (d) Time-series modeling results of ChainX PUF outputs.

covering a broad range of ML algorithms [10], model the PUF as a black box for nonlinear fitting. All the accuracies on the test set remain 50%, equivalent to random guessing. Since the PUF circuit is public to attackers, incorporating it into ML models can significantly increase the attack success rate [18]. Fig. 8c demonstrates Simulated Annealing using a white-box model, targeting the hidden W of the PUF by exploiting its design and CRPs relationship. ChainX PUF exhibits higher security even with a smaller N due to the exhaustive search complexity for W , which reaches $O(2^{N^2})$. Fig. 8d further illustrates direct predictions of ChainX PUF's random output bit utilizing time-series modeling algorithms such as RNN, LSTM and GRU, proving superior ML resistance across algorithms targeting sequential relationships.

B. Reliability evaluations

The reliability of the PUF includes the entropy source's resistance to degradation during enrollment and the stability and reproducibility of CRPs during authentication, ensuring accurate and reliable identity verification. We first evaluate the proposed entropy source under different temperatures, as depicted in Fig. 9a. The read current at the middle V_T always follows a normal distribution, and the minimum entropy S of random bits remains greater than 0.98, indicating high quality. Due to the variations in FeFET and circuitry, random bit flip occurs in the output responses when the same input is applied, reflected in the intra-PUF Hamming distance (bit-error-rate, BER). As shown in Fig. 9b, the variability and uniqueness of ChainX PUF approach ideal values.

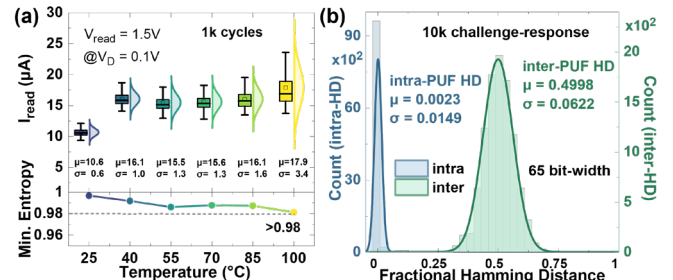


Fig. 9. (a) The I_{read} of middle V_T during enrollment remains random normal distribution in the range of $25^{\circ}\text{C} \sim 100^{\circ}\text{C}$, while the minimum entropy always larger than 0.98. (b) Intra- and inter-PUF Hamming distance of ChainX PUF, indicating robust CRP reproducibility and uniqueness during authentication.

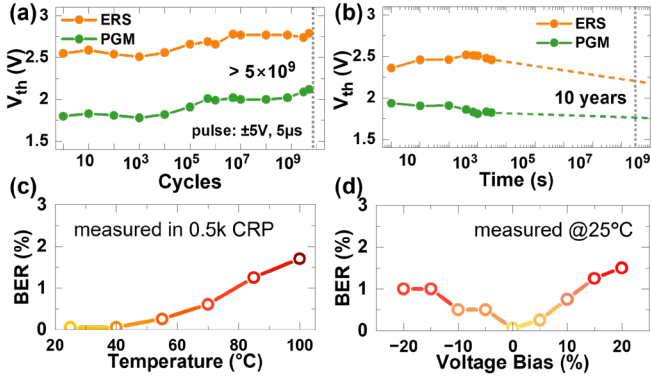


Fig. 10. Measured high endurance (a) and retention (b) of our HAO FeFETs. Measured native BER under (c) various supply voltage fluctuations and (d) different environment temperature conditions between 25°C~100°C.

Since ChainX PUF utilizes the FE layer in FeFETs to store unpredictable random weights for chained XOR based CRP generation, the stored weights W must remain unchanged. Furthermore, ChainX PUF supports continuous erasure and rewrite for user re-enrollment. This also imposes reliability requirements on the FeFETs in the array. As demonstrated in **Fig. 10a** and **10b**, our devices exhibit excellent endurance over 5×10^9 cycles, with stable polarization extrapolated to over 10 years, ensuring the stability of ChainX PUF.

As shown in **Fig. 10c** and **10d**, under varying temperatures (25°C~100°C) and voltage biases ($\pm 20\%$), the worst-case native BER (n-BER) during PUF authentication is measured to be less than 1.7%. This is because FeFETs are programmed into stable '0' and '1' states, minimizing V_T variations. In this state, the FeFETs rest at its energy minimum, ensuring stable polarization. Additionally, the high on/off ratio of FeFETs effectively increases the ADC's sense margin, enhancing the PUF's reliability and reducing the n-BER.

C. Efficiency evaluation and benchmarks

Fig. 11 evaluates the area and energy efficiency of ChainX PUF, comparing it with existing PUF implementations under the BSIM model in HSPICE for the same technology node. Due to the compact cell structure and XOR design activating only half of the array per operation, ChainX PUF significantly reduces both area and energy cost compared to CMOS PUFs. It also outperforms RRAM in energy consumption, benefiting from the much lower I_{off} . Energy consumption is normalized to the same array size that generates 1-bit response.

Table II benchmarks ChainX PUF against prior designs. By introducing nonlinear coupling in both the temporal and spatial dimensions, it demonstrates significant improvements in ML resistance, reliability, area- and energy-efficiency. The evaluation of attack accuracy is conducted using the same algorithms, including both black-box and white-box ML attack models, while ensuring identical CRP training set sizes. In the table, higher attack accuracy ($>50\%$) indicates greater potential vulnerability to modeling attacks.

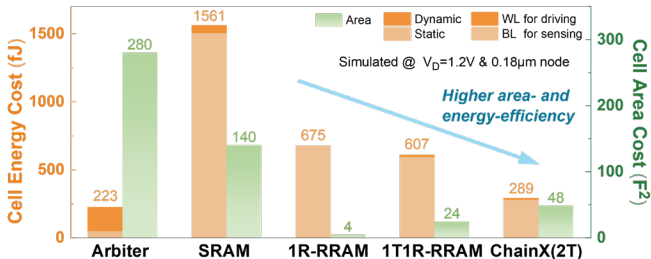


Fig. 11. The hardware and power consumption of different PUF designs. ChainX PUF shows significant energy-efficiency advantages and lower area overhead. The area values are typical ones reported in previous research.

TABLE II. Comparison with prior PUF implementations.

	ISSCC[4]	ESSCIRC[5]	TCAS-[6]	Nat Ele[7]	Nat Com[8]	This work
Technology	8T	3T	2T-1M	1R	2T-1C	2T
Coupling dimensions	CMOS	CMOS	MRAM	RRAM	FeFET	FeFET
Uniqueness	Spatial	Spatial	N/A	Spatial	Spatial	Spatial+temporal
Diffuseness	50.3%	46.8%	50.1%	48.3%	49.9%	50.0%
ML attack acc.	-	-	49.7%	~50%	-	50.0%
SA attack acc.	N/A	50.6%	N/A	~50%	52.1%	50.0%
Worst n-BER	99.3%	-	68%	69%	-	50.0%
Area (F²/cell)	3.84%	8.8%	0.2%	3.0%	0.7%	1.7%
Energy (fJ/bit)	1125	295	85	4	>200	48
	78-128	690	60	20	1.89	3

IV. CONCLUSION

This work presents the first demonstration of nonlinear coupling in both spatial and temporal dimensions for a strong PUF. Based on an optimized entropy source and chained XOR in compact 2T FeFET arrays, ChainX PUF exhibits high security, reliability, and low cost. Experimental results confirm the unprecedented ML resistance and the low native BER, showcasing its strong potential for security solutions in resource-limited IoT applications.

ACKNOWLEDGMENT

This work was supported by National Key R&D Program of China (2022YFB4400300), NSFC (62274003, 61927901 and 92164203), 111 Project (B18001).

REFERENCES

- [1] Y. Gao *et al.*, "Physical unclonable functions," *Nat. Electron.*, vol. 3, no. 2, pp. 81–91, Feb. 2020.
- [2] Z. Wang *et al.*, "Safe, secure and trustworthy compute-in-memory accelerators," *Nat. Electron.*, Dec. 2024.
- [3] U. Chatterjee *et al.*, "Trustworthy proofs for sensor data using FPGA based physically unclonable functions," in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Dresden, Germany: IEEE, Mar. 2018.
- [4] S. Taneja *et al.*, "36.1 unified In-memory dynamic TRNG and multi-bit static PUF entropy generation for ubiquitous hardware security," in *2021 IEEE International Solid-State Circuits Conference (ISSCC)*, San Francisco, CA, USA: IEEE, Feb. 2021, pp. 498–500.
- [5] H. Lin *et al.*, "A 690fJ/bit ML-attack-resilient strong PUF based on subthreshold voltage attenuator ring with closed-loop feedback," in *Esscirc 2023- IEEE 49th European Solid State Circuits Conference (esscirc)*, Lisbon, Portugal: IEEE, Sep. 2023, pp. 113–116.
- [6] Z. Hou *et al.*, "Reconfigurable and dynamically transformable In-cache-MPUF system with true randomness based on the SOT-MRAM," *IEEE Trans. Circuits Syst. I Regul. Pap.*, vol. 69, no. 7, pp. 2694–2706, Jul. 2022.
- [7] H. Nili *et al.*, "Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors," *Nat. Electron.*, vol. 1, no. 3, pp. 197–202, Mar. 2018.
- [8] T. Li *et al.*, "Demonstration of high-reconfigurability and low-power strong physical unclonable function empowered by FeFET cycle-to-cycle variation and charge-domain computing," *Nat. Commun.*, vol. 16, no. 1, p. 189, Jan. 2025.
- [9] H. Shao *et al.*, "A Novel FeFET Array-Based PUF: Co-optimization of Entropy Source and CRP Generation for Enhanced Robustness in IoT Security," in *2023 International Electron Devices Meeting (IEDM)*, San Francisco, CA, USA: IEEE, Dec. 2023, pp. 1–4.
- [10] U. Ruhmair *et al.*, "PUF modeling attacks: an introduction and overview," in *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2014, Dresden, Germany: IEEE Conference Publications, 2014, pp. 1–6.
- [11] M. Khalafalla *et al.*, "PUFs deep attacks: enhanced modeling attacks using deep learning techniques to break the security of double arbiter PUFs," in *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Florence, Italy: IEEE, Mar. 2019, pp. 204–209.
- [12] D. Karakoyunlu *et al.*, "Differential template attacks on PUF enabled cryptographic devices," in *2010 IEEE International Workshop on Information Forensics and Security*, Seattle, WA, USA: IEEE, Dec. 2010, pp. 1–6.
- [13] A. I. Khan *et al.*, "The future of ferroelectric field-effect transistor technology," *Nat. Electron.*, vol. 3, no. 10, pp. 588–597, Oct. 2020.
- [14] M. Dominguez *et al.*, "CycPUF: cyclic physical unclonable function," in *2024 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2024.
- [15] J. Rajski *et al.*, "On near-maximum-length galois nonlinear feedback shift registers," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, pp. 1–1, 2024.
- [16] Y. Pang *et al.*, "Memristors for hardware security applications," *Adv. Electron. Mater.*, vol. 5, no. 9, p. 1800872, Sep. 2019.
- [17] J. Miao *et al.*, "SD-PUF: spliced digital physical unclonable function," *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, pp. 1–1, 2017.
- [18] H. Shao *et al.*, "IMCE: An In-Memory Computing and Encrypting Hardware Architecture for Robust Edge Security," in *2024 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Valencia, Spain: IEEE, Mar. 2024.