Chinese Journal of Electronics
vol. 33, no. 2, pp. 371–379, March 2024
https://doi.org/10.23919/cje.2022.00.406

RESEARCH ARTICLE

A Design of 2-Stage Voltage Ramp-Up SRAM Physical Unclonable Function

Minte SONG[1,2], Nan LIU[1,2], Shuaiyang ZHOU[1,2], Zhengguang WANG[1,2], Zhanqiang RU[2], Peng DING[2], Wei HUANG[2], and Helun SONG[2]

1. *School of Nano-Tech and Nano-Bionics, University of Science and Technology of China, Hefei 230026, China*
2. *Suzhou Institute of Nano-Tech and Nano-Bionics, Chinese Academy of Sciences, Suzhou 215123, China*

Corresponding author: Helun SONG, Email: hlsong2008@sinano.ac.cn
Manuscript Received December 1, 2022; Accepted April 26, 2023

Abstract — Silicon physical unclonable function (PUF) implemented by static random access memory (SRAM) exists inherent demerit of unstable cells due to noise of environment and circuits, which significantly restricts its reproducibility. In this paper, a 16T SRAM cell with reset-delay circuit and a 2-stage voltage ramp up is fabricated and reported. Compared to conventional SRAM structure, each PUF cell adds a pair of pull-up PMOS (P-channel metal oxide semiconductor) and pull-down NMOS (N-channel metal oxide semiconductor) controlled by reset and delayed-reset signals respectively, resulting in two positive feedback stages with different amplification coefficients when the voltage is ramped up. PUF array consists of 4064 cells, 322 dummy cells and a group of 8 series-connected inverters with an area of 304 μm × 650 μm to match the digital post-processing module. PUF test chip was fabricated in HH-Grace 110 nm platform with total area 1140 × 1140 μm^2. The average HDintra (intra-chip Hamming distance, also bit error rate, BER) and HDinter (inter-chip Hamming distance) values of the 50 PUF chips in SOP16 package measured at normal point (1.5 V/25 ℃) were 1.92% and 49.85%, respectively.
Keywords — Physical unclonable function, Static random access memory, Integrated circuits.
Citation — Minte SONG, Nan LIU, Shuaiyang ZHOU, *et al.*, "A Design of 2-Stage Voltage Ramp-Up SRAM Physical Unclonable Function," *Chinese Journal of Electronics*, vol. 33, no. 2, pp. 371–379, 2024. doi: 10.23919/cje.2022.00.406.

I. Introduction

Silicon physical unclonable function (PUF) is a physical device implemented by silicon integrated circuits which provides a unique binary sequence as a function of the existing inputs. The unique binary sequences generated by a PUF are referred to as responses, and the inputs to the PUF are referred to as challenges. Challenge-response pairs (CRPs) of PUFs are commonly considered be unclonable, unpredictable, and tamper-resistant, which enables PUF-equipped chips to possess the advantages of lower cost and higher security [1], [2].

Silicon PUFs can be implemented in a variety of forms. Typical silicon PUFs are designed with identical circuit structures with competing relationships, while the microscopic uncertainty of the integrated circuit leads to the random inter-chip characteristics of the circuit's competing outputs. The most widespread types of silicon PUFs based on circuit delay characteristics are arbiter-PUF [3], [4], and RO-PUF (ring oscillator PUF) [5], [6], which obtain the PUF response by determining two voltage or frequency features with competing relationships. Whereas, there are other PUFs are based on a certain type of digital memory such as SRAM-PUF (static random access memory PUF) [7], [8], DRAM-PUF (dynamic random access memory PUF) [9], MRAM-PUF (magnetic random access memory PUF) [10], RRAM-PUF (resistance random access memory PUF) [11], [12], butterfly-PUF [13] and flip-flop-PUF [14]. To obtain binary response data, these PUFs can achieve a competitive relationship of voltage or current ascribed to the structure of memory cells.

Since more and more attention has been attracted in PUF technology, some innovative types of PUFs appeared in chip designs. For instance, a spin-transfer torque magneto resistive random-access memory (STT-

Associate Editor: Prof. Gaofeng WANG, Hangzhou Dianzi University.

MRAM) was proposed by Hu *et al.* [15]. The STT-MRAM achieved bit error rate (BER) of 2.13% and uniqueness of 50.64% with the assistance of crossing switches and gap-enlarging algorithms. Besides, an intrinsic PUF, G-PUF, introduced by exploiting the location of soft errors that occur when the GPU operates under unstable conditions, achieves 90.09% reliability and 55.61% uniformity in test results [16]. A new lightweight PUF structure is proposed based on an arbitration PUF and a linear feedback shift register with reconfigurable connections, CRC-PUF, which effectively circumvents the drawbacks of arbitration PUFs against modeling attacks and achieves 50.0777% uniformity and 49.9978% uniqueness as shown in test results [17]. Reference [18] proposed a new 64-bit memory-based control PUF (Mc-PUF) architecture in serial and parallel, which utilizes threshold voltage variation of the transistors that constitute the decoupled non-gates in SRAM. Test results show that the 3-XOR Mc-PUF can achieve 48.34% randomness and 49.58% uniqueness, and exhibits high resilience to modelling attacks and possesses better lightweight characteristics. Previous study [19] reported an interconnect line mismatch owing to coupling capacitance and mutual inductance between the interconnection lines, which resulted in a longer delay of the wire.

Main applications of PUF concentrate on the scenarios related to unique identification and cryptography. Based on the inherent physical characteristics of the integrated circuit, PUF technology forms a function which can produce stable and repeatable response signal for the same challenge. Related applications can be derived upon this chip signature-like functionality, such as primitive key generation, secret key management, device anti-counterfeiting and authentication, software root of trust, etc. [20]–[22]. An invasive probing attack on the non-volatile memory (NVM) with the support of the chip decapsulation and internal circuit nodes exposing allows the attacker to access the stored keys. Under the circumstance of primitive key generated by PUF, the repeatable and instant generation of response obviates storing key directly in NVM, which effectively reduces the NVM and cryptographic management IP cost of the chip. On the other hand, PUFs gain variation between chips, which derive from a chip manufacturing process without artificial control. Compared to the classic one-time-programming (OTP) solution for trusted data storing, chips equipped with PUF IP can generate root keys when the system requires. For cryptographic chips such as secure elements (SEs), this feature eliminates the need of initial key burning into OTP thus reducing the cost of trust between chip designers and manufacturers [23].

The output value of most PUF cells can hardly remain completely stable with external circuit noise, thermal noise and operation conditions attributed to the difficulty of fully effective control on competition parameters. Nonetheless, PUF applied in key generation is required to be sufficiently stable during entire life cycle of crypto-system to maintain reliable operation of security applications [24]. Generally, two available solutions are suggested for these conflicts. On the one hand, the intrinsic instability of PUF cells can be reduced by regulating operating conditions or optimizing circuit structure. Reference [25] presents a novel 8T SRAM architecture that achieves low voltage evaluation and low power operation using three modes of operation, which has 100% enhanced stability through hot carrier injection (HCI) aging on alternating direction nMOS loads. Reference [26] proposes an 18T design which uses sequence correlation planning and bit selection algorithms to improve the reliability and randomness of the chip, the test of which showing a BER of 0.8% at 1V at 20 ℃, with an inter-chip Hamming distance of 49.64%. Moreover, reference [27] indicated that PUF biasing operated by HCI burn-in stabilization was compatible with 8T hybrid SRAM PUF, which realized 0.29% BER with NIST SP 800-22 tests passed. The stability of PUF can be improved by matching voltage ramp up time with environment temperature. On the other hand, a post-processing method can be performed if reproducibility of existing PUF arrays is insufficient. In literature [2], [28], [29], error-correction techniques were implemented for PUF post-processing to revert PUF data, which intensified the PUF reproducibility with external storage. A trimming method implemented by data remanence-based technique was proposed in [30]. In this approach, the strongest “1” and strongest “0” cells in a large-scale SRAM array can be identified in 2 times of power-ups by writing “1” or “0” to the entire array and recording the bit flip position after a short break in power. Moreover, an SRAM mismatch factor (MF) was proposed as a function separates cells with different start-up values by evaluating the threshold voltage of the transistor [31], which provided a basis for assessing stability of a substantial number of PUF cells.

Notably, the two described approaches for higher PUF reproducibility can be mutually beneficial for each other. Stability of cells can be improved by optimizing the PUF circuit structure or process, which can conversely match post-processing modules with smaller gate counts, or isolates out more strong cells among the same amount of PUF cells. Overall, the reproducibility problems can be optimized by a simple idea: a close-to-ideal PUF cell design is the most convenient way to reduce on-chip resource waste. Consequently, in this paper, we designed a 16T optimized SRAM cell with reset and delayed-reset ports which brought a 2-stage voltage ramp up process. The test chip was fabricated on HHGrace 110 nm technology with PUF area of 304 μm × 650 μm. Results from the test show that the average intra-chip Hamming distance (HDintra) and inter-chip Hamming distance (HDinter) in normal point can reach 49.85% and 1.92% with NIST test passed. The PUF cells operated normally at the V_{dd} voltage of 1.3–1.7 V.

The rest of this paper is summarized as follows: In

Section II, the authors describe the topology and simulation results of PUF cells, followed by layout design of PUF cells and architecture of test chip. Statistics and analysis of PUF arrays in chips are shown in Section III. At the end, Section IV concludes this paper.

II. PUF Cell Circuit Design

1. Design concepts

A prototypical SRAM structure produces a random output between cells during voltage ramp up, where the positive feedback of the SRAM circuit amplifies the threshold voltage mismatch of the transistor. The inherent shortcoming of SRAM cells is inferior reproducibility, which is mainly caused by the Gaussian distribution of the voltage mismatch between a pair of transistors. As is shown in Figure 1(a), all PUF cells can be divided into 2 main parts, positive mismatch (PM) and negative mismatch (NM). Further, each part has a demarcation, dividing it into unstable (e.g., PUM) and stable (e.g., PSM) area. There are two main types of approaches reducing the number of cells in PUM and NUM: The most straightforward way is filtering and removing cells in UM area by post-processing testing, which leads to Figure 1(b); The voltage mismatch can be changed by PUF biasing [27] which can minimize the loss of PUF cells, and the distribution curve is shown in Figure 1(c). From the perspective of the chip manufacturing, PUF biasing can be realized by transistor aging methods like positive/negative bias temperature instability (NBTI/PBTI) or HCI.

However, aging method usually requires additional processes during chip probing (CP) test, resulting in difficulty raising of IP merge and higher cost of full chip. That's why we choose circuit design to realize PUF biasing. The voltage ramp-up time of standard 6T SRAM cell is quite short. For SRAM cells with smaller mismatch, positive feedback intervenes when the difference in voltage between both ends of the SRAM is insufficient to form a decisive difference, leading to the possible variation in the output. Another inescapable phenomenon is that the positive feedback outcome of the cell will be dominated by unpredictable noise when the voltage fluctuations generated by thermal noise are greater than the mismatch voltage of the SRAM PUF. Taking the above situation into consideration, we optimized the design of the SRAM structure based on ID circuit [32], followed by an optimization of PUF array arrangement.

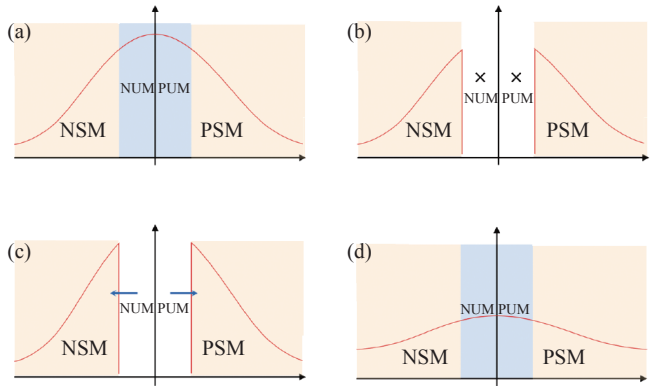


Figure 1 (a) Transistor mismatch voltage statistics of PUF cells shows a bell curve distribution. (b) PUF biasing by filtering unstable bits. (c) PUF biasing by increasing the mismatch of unstable cells. (d) PUF biasing by amplify the mismatch of all cells.

2. 16T SRAM PUF cell circuits and simulation

As shown in Figure 2, each PUF cell consists of 16 transistors. The main part of the PUF cell consists of PMOS P1–P4, and NMOS N1–N6. Two inverters are placed symmetrically on both sides of each PUF cell to maintain the symmetry of the single-ended output loading. These inverters can also isolate external parasitic ca-

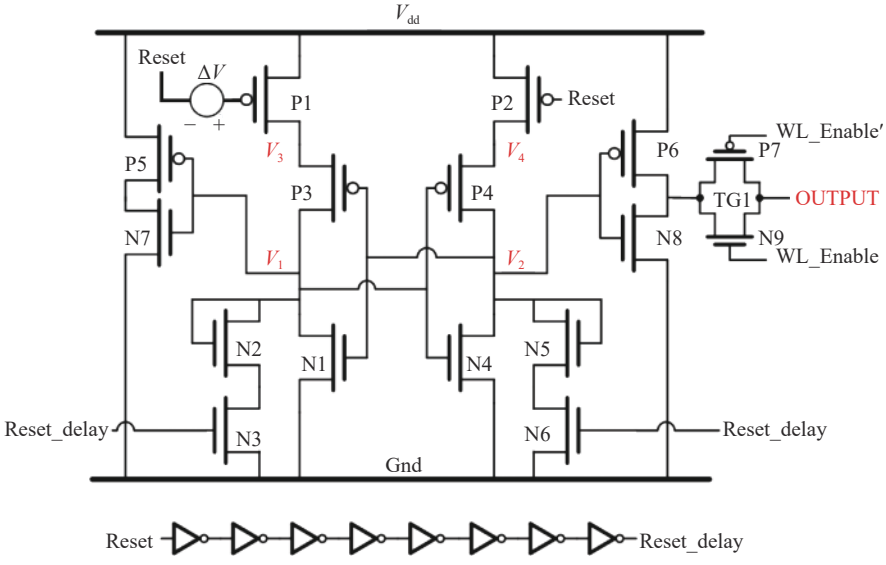


Figure 2 16T SRAM-PUF cell. Each PUF cell consists of 16 transistors with 4 reset ports, and the outputs are enabled by WL_enable. The PUF array consists of an 8-stage inverter, 32×127 PUF cells, a surrounding circle of dummy PUF cells, and a readout circuit at the bottom.

pacitance. Low gate voltage (1.5 V) single NMOS gates cannot transmit high levels (1.5 V) of circuits, so CMOS transfer gates TG are placed. ΔV is the offset voltage from the mismatch of two sets of transistors equivalent to the input, i.e., the equivalent input signal, which can be presented as

$$\Delta V \propto \left(k_1 \times \left[\frac{\Delta(W/L)}{W/L} \right]_P^2 + k_2 \times \left[\frac{\Delta(W/L)}{W/L} \right]_N^2 + k_3 \times \Delta V_{\mathrm{TH},P}^2 + k_4 \times \Delta V_{\mathrm{TH},N}^2 \right) \quad (1)$$

where $k_{1\text{–}4}$ is constants, ΔV_{TH} is the mismatch of threshold voltage of symmetric transistors. The offset voltage is proportional to ratio of size mismatch and ΔV_{TH} of symmetric transistors. Besides, ΔV_{TH} can be presented as

$$\Delta V_{\mathrm{TH}} = \frac{A_{\mathrm{VTH}}}{\sqrt{WL}} \quad (2)$$

In order to create a larger initial offset voltage and mismatch threshold voltage, a smaller size of the transistor was chosen, and width-length ratio (W/L) was set to 240 nm/110 nm. In the simulation, HHGrace 110 nm PDK was used and we defined that the voltage of the Reset port controlled by POR began to drop at 1.1 ns and decreased to 0 V at 1.15 ns; moreover, the Reset_delay was enabled by an 8-stage series-connected inverter with a delay of about 0.4 ns. Simulation conditions of TT corner and 27 ℃ was chosen. According to the voltage state of Reset and Reset_delay port, the operating modes of PUF cell can be divided into reset mode M1, amplification mode M2, latching mode M3 and stabilization mode M4, which is illustrated in Figure 3(a).

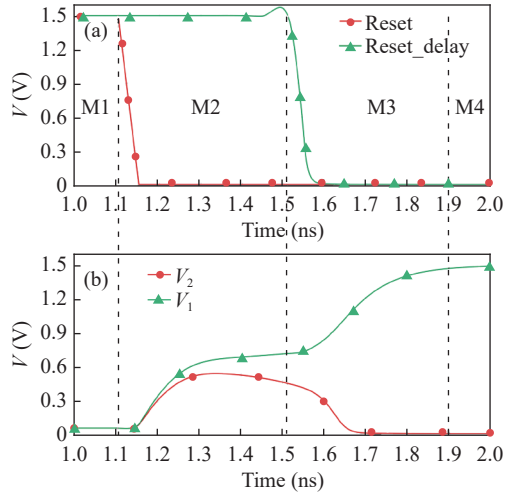


Figure 3 (a) The reset signal is defined to start dropping at 1.1 ns, and the voltage is 0 V at 1.15 ns in the simulation. Delayed-reset starts dropping about 400 ps later. (b) Simulation of V_1 and V_2 voltage of a PUF cell with delayed-reset.

When the chip is powered on, it first enters M1 mode with Reset and Reset_delay ports at 1.5 V. Currently, NMOS transistors N3 and N6 were on, PMOS P1, P2, N2, and N5 were off. Potentials V_1, V_2, V_3, and V_4 were pulled low, causing P3 and P4 to turn off.

Subsequently, the Reset port switched to 0 V under the control of power on reset (POR); Reset_delay remains at 1.5 V under the effects of the delay cells, whereby the PUF cell enters M2. Currently, transistors P1 and P2 turn on, causing potentials V_3 and V_4 to rise, which in turn switching transistors P3 and P4, rising potentials V_1 and V_2, and turning on N1 and N4. Transistors N1–N6 and P1–P4 formed the amplifier. In the amplification mode M2, the signal-to-noise ratio SNR of the output signal, also the input signal before entering the latch mode M3 can be presented as follows:

$$\mathrm{SNR} = \frac{\Delta V^2 A_{\mathrm{v}}^2}{\gamma A_{\mathrm{v}} \dfrac{kT}{C_{\mathrm{L}}}} = \frac{\Delta V^2 (G_{\mathrm{m}} R_{\mathrm{out}})^2}{\gamma G_{\mathrm{m}} R_{\mathrm{out}} \dfrac{kT}{C_{\mathrm{L}}}} = \frac{\Delta V^2 G_{\mathrm{m}} R_{\mathrm{out}}}{\gamma \dfrac{kT}{C_{\mathrm{L}}}} \quad (3)$$

where ΔV is the equivalent input signal; A_{v} is the gain in the amplification mode of the circuit; the coefficient γ is related to the process only; k is the Boltzmann constant; T is the absolute temperature; and C_{L} is the load capacitance of the output. It can be concluded from equation that the input signal has been amplified by a factor of $\sqrt{A_{\mathrm{v}}}$ before entering the latching mode, yet the output noise is not amplified. Hence, the output signal at the end of M2 has a higher SNR compared to the circuit without the amplification mode.

When Reset_delay flips to 0 V, the stage of PUF cells enter latch mode M3. Although the branches located by N2 and N5 are at the output, V1-N2-N3, V2-N5-N6 branch is disconnected as N3 and N6 enter the off state, latch form strong positive feedback, which makes V_1 and V_2 amplified rapidly and finally stabilized at a certain voltage based on the existing voltage difference in M2. The voltage of the output port OUTPUT will remain constant for the cells in the stable status after M3. The signal latched by M3 has been amplified by M2 with higher SNR, which will result in higher output reproducibility.

When the PUF cells are in the stabilization mode M4, the output efficiency of the cell is controlled by word line enable port (WL_enable). The simulation results indicate that the power consumption of PUF cell is 75 fJ/bit.

M1, M2 and M3 are all short-time stage after the chip is powered on; M4 is a constant stage when the chip is operating normally. All PUF cells undergo 2 voltage ramp-up stage M2 and M3. The mismatch of the signal voltage is amplified while the noise voltage remains unchanged. Since the mismatch of all cells is amplified, most cells in the UM region migrate to SM region, with few cells remaining in the UM region to create HDinter.

3. PUF layout

As shown in Figure 4(a), each PUF cell has a guard ring, which is designed to reduce the resistance between the MOS transistor and the substrate, avoiding the

latch-up effect and isolate the external noise better. PUF cells were combined in an array of 32 rows and 127 columns to match the error correction code (ECC) parameters in the digital design section. Each row of PUF cells shares a common WL_enable port, and the Reset_delay ports of all PUF cells share a common 8-stage inverter. As displayed in Figure 4(b), PUF cells in each interval row are placed by rotating 180°, which ensure that the guard ring between two adjacent rows of PUF cells can be merged, thus reducing the area of PUF array and the probability of latch-up effect. Dummy cells were placed around PUF array to prevent digital noise and edge-effects, as a result, total number of SRAM cells in PUF array is 4079 and the final layout size of the PUF array is 304 μm × 650 μm. Digital circuit part consists of address decoder, error correction circuit, PAD control and interface logic, which realized the challenge response function of PUF.

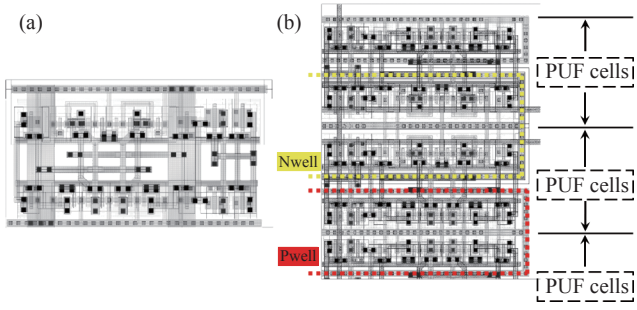


Figure 4 (a) Single PUF cell layout; (b) Part of PUF array layout.

III. Testing and Measured Results

1. Design concepts

The test chips with 16T PUF cell array in this study were fabricated on the HHGrace 0.11 μm CMOS platform. Figure 5(a) presents full vision of test chip layout, which consists of PUF array, PUF post-processing circuits and interface controller. The chip size of full test chip is 1140 μm × 1140 μm with die thickness of 480 μm. A micro-scope photo of the test chip with bonding Au wire can be seen in Figure 5(b). In Figures 5(c) and (d), a dedicated test board with a socket was prepared to carry the PUF chip in SOP16 package. The test board is connected to host computer STM32F103ZET6 and outputs of chips are uploaded to PC for statistics.

2. Statistics and analysis

Mean value of 50 PUF test chips are counted, which is the sum of all cell values divided by total number of cells. Assuming that the PUF cells are independent of each other, the ideal mean values should satisfy the binomial distribution. The red dots in Figure 6 indicate the mean value of PUF arrays of 50 chips, and the calculated theoretical curve from binomial distribution is shown as a blue line. All mean values are situated around the ideal mean 0.5 with a 95% confidential interval from 0.4846

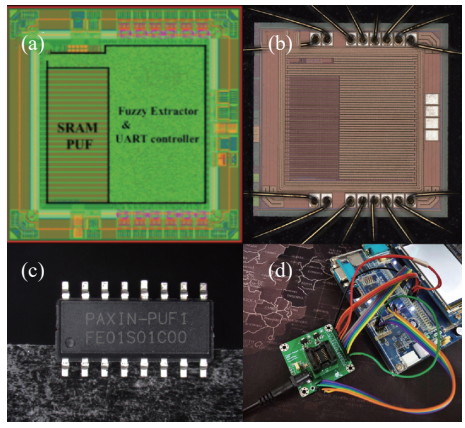


Figure 5 (a) Layout of test chip; (b) A die of test chip with bonding wires; (c) Full view of test chip with SOP16 package; (d) Test board and a host for test chip.

to 0.5154. Figure 7(a) shows HDinter and HDintra of 10 PUF test chips at the environment condition of 25 ℃ and typical 1.5V core voltage. HDintra represents the stability of PUF cells, which is calculated by comparing the same PUF array in different power-up cycles. Statistics result of HDintra in Figure 7(a) revealed that the optimized PUF arrays have an average HDintra of 1.92%. HDinter represents the variability between each two PUF chips with ideal volume of 50%. As presented in Figure 7(b), the HDinter was described as a histogram with a fitted curve and the average value is 49.85% regarding to initial values of 4064-bit PUF array.

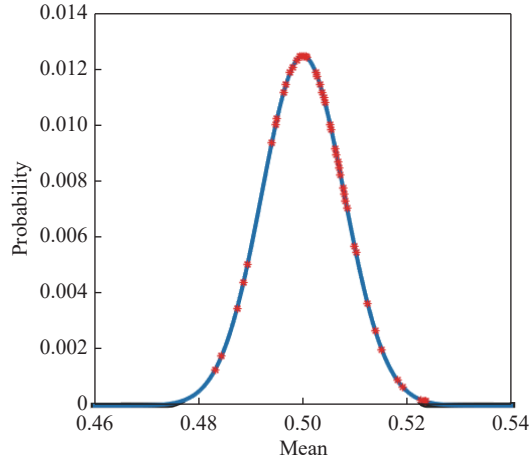


Figure 6 Mean values of 50 test chips. Each chip has an array of 4064 PUF cells.

One PUF test chip is selected for temperature reliability test with range of −40 ℃ to 105 ℃ and the result of HDinter (also unstable bit ratio) is evaluated. All the temperature tests were carried in a laboratory temperature chamber and the test chip is reset for 500 times at each temperature point, the average HDintra with an error bar is shown in Figure 8. In the range of operating temperature, the average HDintra of PUF test chip is 2.24%. As shown in Table 1, the proposed PUF has successfully passed NIST randomness tests, indicating ac-

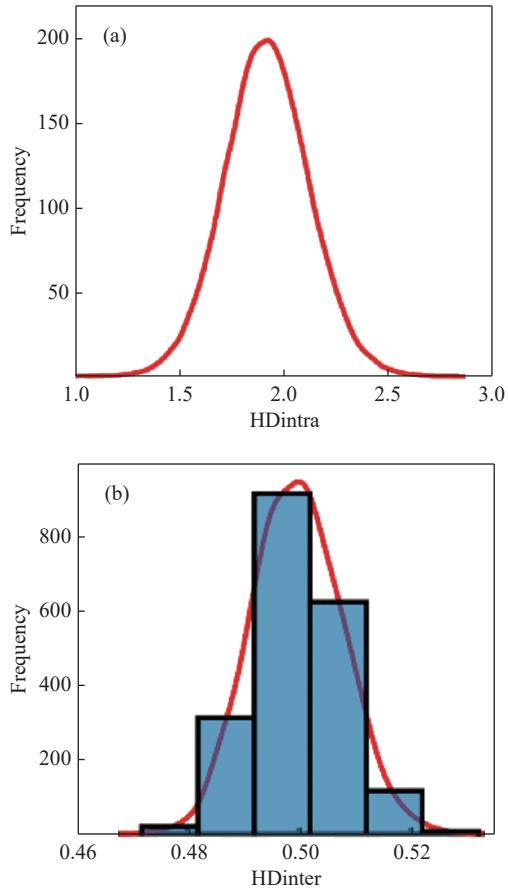


Figure 7 Test results at the condition of 25 ℃ and typical 1.5 V core voltage. (a) Fitted curve of HDintra of PUF chips; (b) Histogram of HDinter between 50 PUF chips and a fitted curve.

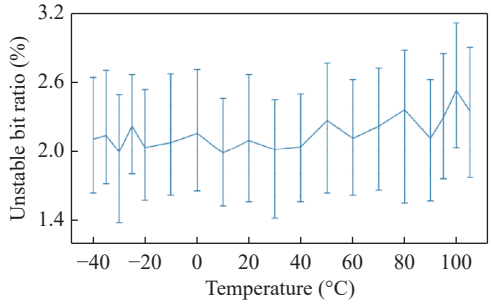


Figure 8 Reliability test of one PUF test chip. A small variation appears in HDintra as the temperature rises.

Table 1 Random test of SRAM PUF in this paper

Test name	Stream length (bit)	Runs No.	Pass rate	Average P-value	Pass?
Frequency	40640	10	9/10	0.9114	Yes
Block frequency	40640	10	10/10	0.1223	Yes
Runs	40640	10	10/10	0.5341	Yes
Longest run of ones	40640	10	10/10	0.5688	Yes

ceptable randomness.

Figure 9 shows the variation of HDintra in response to the V_{dd} voltage changed from 1.3 V to 1.7 V. The gain of reset transistors P1 and P2 at different supply voltages can be described as

$$A_v = \frac{g_{m1,2}|V_{thp1,2}|}{I_{CM1,2}} \propto \frac{|V_{thp1,2}|}{|V_{gsp1,2}| - |V_{thp1,2}|} = \frac{|V_{thp1,2}|}{V_{dd} - |V_{thp1,2}|} \quad (4)$$

where $g_{m1,2}$, $V_{thp1,2}$, $I_{CM1,2}$, $V_{gsp1,2}$ are transconductance, threshold voltage, common mode current, and gate-source voltage of reset transistors P1 and P2, respectively. The gain PUF circuit decreases as the supply voltage increases, which will lead to an increase in the output instability bits of the PUF cell.

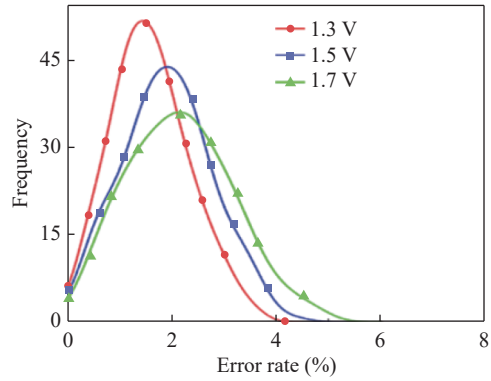


Figure 9 Test results at the condition of 25 ℃ and 1.3/1.5/1.7 V core voltage. As the voltage increases, the distribution of error rate broadens and the peak value increases.

The PUF test chip generates minimal static power consumption due to device leakage. Under the condition of typical 1.5 V core voltage and global clock switched off, the static power consumption of the chip is measured to be 156 nW. Average dynamic power consumption of fully chip in working status is 1.79 mW.

3. Comparison

Table 2 presents a comparison different implementation of SRAM PUF. The PUF cell designed in this paper utilizes the same typical gate voltage as the digital standard cell without pre-selection and aging method, which makes it more convenient for PUF IP merge: The full chip don't need any other CP test and aging process such as HCI and NBTI. There is no need of need special pre-selection circuits and isolate power domain for this design. Compared to work in [32], we have obtained smaller area by layout optimization; Meanwhile, a smaller native HDintra of less than 2% and a wider scale of temperature resistance of −40 ℃ to 105 ℃ were achieved by 2-stage voltage ramp-up process.

Since the optimized SRAM cells possess a smaller HDinter, the matching ECC module can achieve a reduced area and power consumption, which enables the SRAM PUF being applied in resource-constrained scenarios such as RFID and battery-powered devices.

Table 2 Comparison of different implementation of SRAM PUF

Ref.	[25]	[32]	[33]	[34]	[35]	[36]	This work
Node	130 nm	130 nm	65 nm	65 nm	65 nm	130 nm	110 nm
Topology	Hybrid SRAM	SRAM	SRAM	SRAM	SRAM	EE SRAM	SRAM
Pre-selection	None	None	Analog	Analog	Digital	Analog	None
Energy/bit	2.07 fJ	1.6 pJ	73 fJ	21 fJ	16 fJ	128 fJ	75 fJ
Area/bit	497F2	71.09 μm^2	11600F2	1420F2	3001F2	373F2	3265F2/45.05 μm^2
Voltage	0.5–0.7 V	0.9–1.1 V	0.8–1.2 V	0.8–.2 V	0.8–1.2 V	0.8–1.4 V	1.3–1.7 V
Temperature	−40 to 120 ℃	0 to 80 ℃	−10 to 85 ℃	−10 to 85 ℃	−10 to 85 ℃	−40 to 120 ℃	−40 to 105 ℃
Aging method	HCI	None	None	None	None	None	None
HDinter	48.73%	64.16%	49.30%	49.50%	49.90%	49.23%	49.85%
Native HDintra	2.71%	4%	20.60%	15.98%	19.60%	2.14%	1.92%
Pre-ECC BER	1.00E−07	–	2.70E−10	3.10E−10	1.40E−09	4.50E−08	–

IV. Conclusion

In this study, an optimized SRAM PUF was proposed, which based on a 2-stage voltage ramp up process implemented by combination of reset and delayed-reset ports. Each PUF cell consists of a basic latch and reset-optimized circuits, which amplifies the random mismatch in 2 stages, following with stable digital output. The PUF cell is designed without pre-selection and aging method, making it easier for PUF IP merged in a security chip.These cells constitute a 4064-bit PUF array. In addition, the simulation of voltage ramp-up process, the design of circuits and layout were discussed. The test chip was fabricated on HHGrace 0.11 μm process to demonstrate the feasibility of PUF scheme. Simulation and chip test results show that, without bit cell pre-selection and aging method, the optimized PUF array has a good reproducibility of 1.92% BER while maintaining near-ideal inter-chip variability of 49.85%. Based on this characteristic, digital post-processing module requires less error correction capacity, resulting in smaller area taken and power consumption.

Acknowledgement

This work was supported by the Vacuum Interconnected Nanotech Workstation (Nano-X) (Grant No. 2018-000052-73-01-000356), the Key Research and Development Program (Social Development) of Jiangsu Province (Grant No. BE2021667), and the "Six talent peak" High-level Talent Project of Jiangsu Province, China (Grant No. XYDXX-211).

References

[1] S. Satpathy, S. Mathew, J. T. Li, *et al.*, "13 fj/bit probing-resilient 250 k PUF array with soft darkbit masking for 1.94% bit-error in 22 nm tri-gate CMOS," in *ESSCIRC 2014 - 40th European Solid State Circuits Conference (ESSCIRC)*, Venice Lido, Italy, pp.239–242, 2014.

[2] J. L. Zhang, C. Q. Shen, H. H. Su, *et al.*, "Voltage over-scaling-based lightweight authentication for IoT security," *IEEE Transactions on Computers*, vol. 71, no. 2, pp. 323–336, 2022.

[3] M. H. Mahalat, S. Mandal, A. Mondal, *et al.*, "Implementation, characterization and application of path changing switch based arbiter PUF on FPGA as a lightweight security primitive for IoT," *ACM Transactions on Design Automation of Electronic Systems*, vol. 27, no. 3, article no. 26, 2021.

[4] Z. Q. He, W. B. Chen, L. C. Zhang, *et al.*, "A highly reliable arbiter PUF with improved uniqueness in FPGA implementation using Bit-Self-Test," *IEEE Access*, vol. 8, pp. 181751–181762, 2020.

[5] R. D. Sala, D. Bellizia, and G. Scotti, "A novel ultra-compact FPGA-compatible TRNG architecture exploiting latched ring oscillators," *IEEE Transactions on Circuits and Systems II:Express Briefs*, vol. 69, no. 3, pp. 1672–1676, 2022.

[6] A. K. Aasha, L. E. Hsu, A. Patyal, *et al.*, "Improving the quality of FPGA RO-PUF by principal component analysis (PCA)," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 17, no. 3, pp. 1–25, 2021.

[7] V. K. Rai, S. Tripathy, and J. Mathew, "2SPUF: Machine learning attack resistant SRAM PUF," in *2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP)*, Guwahati, India, pp.149–154, 20204.

[8] S. Baek, G. H. Yu, J. Kim, *et al.*, "A reconfigurable SRAM based CMOS PUF with challenge to response Pairs," *IEEE Access*, vol. 9, pp. 79947–79960, 2021.

[9] S. Rosenblatt, D. Fainstein, A. Cestero, *et al.*, "Field tolerant dynamic intrinsic chip ID using 32 nm High-K/metal gate SOI embedded DRAM," *IEEE Journal of Solid-State Circuits*, vol. 48, no. 4, pp. 940–947, 2013.

[10] R. Ali, D. M. Zhang, H. Cai, *et al.*, "A machine learning attack-resilient strong PUF Leveraging the process variation of MRAM," *IEEE Transactions on Circuits and Systems II:Express Briefs*, vol. 69, no. 6, pp. 2712–2716, 2022.

[11] X. J. Zhao, Q. Zhao, Y. P. Liu, *et al.*, "An ultracompact switching-voltage-based fully reconfigurable RRAM PUF with low native instability," *IEEE Transactions on Electron Devices*, vol. 67, no. 7, pp. 3010–3013, 2020.

[12] J. Li, Y. J. Cui, C. Y. Gu, *et al.*, "Dynamically configurable physical unclonable function based on RRAM crossbar," in *2021 IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH)*, Alberta, AB, Canada, pp.1–6, 2021.

[13] S. S. Kumar, J. Guajardo, R. Maes, *et al.*, "Extended abstract: The butterfly PUF protecting IP on every FPGA," in *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, Anaheim, CA, USA, pp.67–70, 2008.

[14] S. Hemavathy and V. S. K. Bhaaskaran, "Double edge-trig-

gered tristate flip-flop physical unclonable function for secure IoT ecosystem," in *2021 IEEE International Symposium on Smart Electronic Systems (iSES)*, Jaipur, India, pp.44–47, 2021.

[15] Y. P. Hu, L. J. Wu, Z. J. Chen, *et al.*, "STT-MRAM-based reliable weak PUF," *IEEE Transactions on Computers*, vol. 71, no. 7, pp. 1564–1574, 2022.

[16] B. Forlin, R. Husemann, L. Carro, *et al.*, "G-PUF: An intrinsic PUF based on GPU error signatures," in *2020 IEEE European Test Symposium (ETS)*, Tallinn, Estonia, pp. 1–2, 2020.

[17] E. Dubrova, O. Näslund, B. Degen, *et al.*, "CRC-PUF: A machine learning attack resistant lightweight PUF construction," in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS & PW)*, Stockholm, Sweden, pp.264–271, 2019.

[18] P. Williams, H. Idriss, and M. Bayoumi, "Mc-PUF: Memory-based and machine learning resilient strong PUF for device authentication in internet of things," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, Rhodes, Greece, pp.61–65, 2021.

[19] D. Lim, J. W. Lee, B. Gassend, *et al.*, "Extracting secret keys from integrated circuits," *IEEE Transactions on Very Large Scale Integration*, no. VLSI, pp. 1200–1205, 2005.

[20] R. Pappu, B. Recht, J. Taylor, *et al.*, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[21] S. Mathew, S. Satpathy, V. Suresh, *et al.*, "A 4fJ/bit delay-hardened physically unclonable function circuit with selective bit destabilization in 14nm tri-gate CMOS," in *2016 IEEE Symposium on VLSI Circuits (VLSI-Circuits)*, Honolulu, HI, USA, pp. 1–2, 2016.

[22] R. Maes, V. Rozic, I. Verbauwhede, *et al.*, "Experimental evaluation of physically unclonable functions in 65 nm CMOS," in *2012 Proceedings of the ESSCIRC (ESSCIRC)*, Bordeaux, France, pp.486–489, 2012.

[23] J. W. Lee, D. Lim, B. Gassend, *et al.*, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No. 04CH37525)*, Honolulu, HI, USA, pp.176–179, 2004.

[24] A. Garg and T. T. Kim, "Design of SRAM PUF with improved uniformity and reliability utilizing device aging effect," in *2014 IEEE International Symposium on Circuits and Systems (ISCAS)*, Melbourne, VIC, Australia, pp.1941–1944, 2014.

[25] K. Y. Liu, H. L. Pu, and H. Shinohara, "A 0.5-V 2.07-fJ/b 497-F^2 EE/CMOS hybrid SRAM physically unclonable function with < 1E-7 Bit error rate achieved through hot carrier injection burn-in," in *2020 IEEE Custom Integrated Circuits Conference (CICC)*, Boston, MA, USA, pp.1–4, 2020.

[26] L. Lu and T. T. H. Kim, "A high reliable SRAM-Based PUF with enhanced challenge-response space," *IEEE Transactions on Circuits and Systems II:Express Briefs*, vol. 69, no. 2, pp. 589–593, 2022.

[27] K. Y. Liu, X. P. Chen, H. L. Pu, *et al.*, "A 0.5-V hybrid SRAM physically unclonable function using hot carrier injection burn-in for stability reinforcement," *IEEE Journal of Solid-State Circuits*, vol. 56, no. 7, pp. 2193–2204, 2021.

[28] G. E. Suh, C. W. O'Donnell, I. Sachdev, *et al.*, "Design and implementation of the AEGIS single-chip secure processor using physical random functions," in *32nd International Symposium on Computer Architecture (ISCA'05)*, Madison, WI, USA, pp.25–36, 2005.

[29] K. Sun, Y. F. Shen, Y. J. Lao, *et al.*, "A new error correction scheme for physical unclonable function," in *2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, Chengdu, China, pp.374–377, 2018.

[30] M. Q. Liu, C. Zhou, Q. Y. Tang, *et al.*, "A data remanence based approach to generate 100% stable keys from an SRAM physical unclonable function," in *2017 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)*, Taipei, China, pp. 1–6, 2017.

[31] A. Alheyasat, G. Torrens, S. Bota, *et al.*, "Selection of SRAM cells to improve reliable PUF implementation using cell mismatch metric," in *2020 XXXV Conference on Design of Circuits and Integrated Systems (DCIS)*, Segovia, Spain, pp.1–6, 2020.

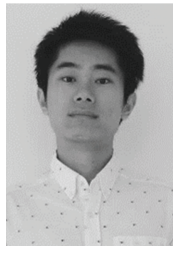
[32] Y. Su, J. Holleman, and B. P. Otis, "A digital 1.6 pJ/bit chip identification circuit using process variations," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 1, pp. 69–77, 2008.

[33] Y. Shifman, A. Miller, O. Keren, *et al.*, "A method to improve reliability in a 65-nm SRAM PUF array," *IEEE Solid-State Circuits Letters*, vol. 1, no. 6, pp. 138–141, 2018.

[34] Y. Shifman, A. Miller, Y. Weizmann, *et al.*, "A 2 Bit/Cell tilting SRAM-based PUF with a BER of 3.1E-10 and an energy of 21 FJ/Bit in 65 nm," *IEEE Open Journal of Circuits and Systems*, vol. 1, pp. 205–217, 2020.

[35] Y. Shifman, A. Miller, O. Keren, *et al.*, "An SRAM-based PUF with a capacitive digital preselection for a 1E-9 key error probability," *IEEE Transactions on Circuits and Systems I:Regular Papers*, vol. 67, no. 12, pp. 4855–4868, 2020.

[36] K. Y. Liu, Y. Min, X. Yang, *et al.*, "A 373-F^2 0.21 %-Native-BER EE SRAM physically unclonable function with 2-D power-gated bit cells and V_{SS} bias-based dark-bit detection," *IEEE Journal of Solid-State Circuits*, vol. 55, no. 6, pp. 1719–1732, 2020.

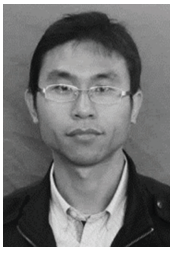


Minte SONG received the B.S. degree from Ocean University of China, Qingdao, China, in 2017. He is currently pursuing the Ph.D. degree in electrical engineering at University of Science and Technology of China, Hefei, China. His research interests include digital and analog integrate circuit design for physical unclonable functions (PUFs), and RISC-V ISA secure SoC design based on PUFs.
(Email: mtsong2018@sinano.ac.cn)

Nan LIU received the B.S. degree in computer science and technology from Beijing Technology and Business University, Beijing, China in 2003 and the M.S. degree in precision instrument and machinery from Beihang University, Beijing China, in 2007. From 2007 to 2022, she was a Research Assistant with the Suzhou Institute of Nano-Tech and Nano-Bionics, CAS, Suzhou, China. Her research interests include the hardware design and system integration. (Email: nliu2007@sinano.ac.cn)

Shuaiyang ZHOU received the B.S. degree in microelectronics science and engineering from Soochow University, Suzhou, China, in 2021. He is currently pursuing the M.S. degree in electrical engineering at University of Science and Technology of China, Hefei, China. His research interests include analog integrated circuit design of physical unclonable functions. (Email: syzhou2022@sinano.ac.cn)

Zhengguang WANG received the B.S. degree in Communication engineering from Anhui University of Technology, Ma'anshan, China, in 2020. He is currently pursuing the M.S. degree in electrical engineering at University of Science and Technology of China, Hefei, China. His research interests include digital signal process design and FPGA implementation. (Email: zgwang2021@sinano.ac.cn)



Zhanqiang RU received the B.S. degree in physics from Qiqihar University, Qiqihar, China, in 2003 and the M.S. degrees in electronics engineering from Changchun University of Science and Technology, Changchun, China, in 2010. From 2010 to 2019, he was a Research Assistant with Suzhou Institute of Nano-Tech and Nano-Bionics (SINANO), CAS, Suzhou, China. Since 2019, he has been a Senior Engineer with the SINANO. He is the author of 8 articles, and more than 15 inventions. His research interests include non-imaging optics design and integration, frequency locking technology of diode laser. (Email: zqru2008@sinano.ac.cn)

Peng DING received the B.S. degree from Anhui University of Technology, Hefei, China, in 2017 and the M.S. degree in integrated circuit engineering from University of Science and Technology of China, Ma'anshan, China in 2020. Since 2020, he was an Assistant Engineer with the Suzhou Institute of Nano-Tech and Nano-Bionics (SINANO), CAS, Suzhou, China. His interests include the hardware design for security system and other application development and design of III-V compound semiconductor devices.
(Email: pding2018@sinano.ac.cn)

Wei HUANG received the Ph.D. degree in optical engineering from Institute of Optics and Electronics, University of Science and Technology of China, Hefei, China, in 2005. He is now an Associate Researcher and M.S. supervisor of SINANO, CAS, and the Head of Laser Sensing and Imaging Laboratory.
(Email: whuang2008@sinano.ac.cn)

Helun SONG received the B.S. degree in electrical engineering from the Changchun University, Changchun, China, in 2002. He received M.S. degree in optical and electrical engineering from Changchun University of Science and Technology, Changchun, China, in 2005 and the Ph.D. degree in optical engineering from Institute of Optics and Electronics, CAS, Beijing, China, in 2008. From 2008 to 2015, he was Associated Professor in Division of System Integration and IC Design, Suzhou Institute of Nano-tech and Nano-bionics (SINANO), CAS, Suzhou, China. Since 2016, he has been a Professor and Associate Administrator in Nano-Device and Materials Division, SINANO. He is the author of more than 30 articles and more than 20 inventions or utility models. His research interests include silicon based and III-V compound semiconductor device integration and application, and system of high concentration photovoltaic.
(Email: hlsong2008@sinano.ac.cn)