S2RAM PUF: An Ultra-low Power Subthreshold SRAM PUF with Zero Bit Error Rate

Li Ni
Hunan University, China
nili@hnu.edu.cn

Jiliang Zhang*
Hunan University, China
zhangjiliang@hnu.edu.cn

ABSTRACT

The reliability of physical unclonable function (PUF) has become the biggest challenge for key generation. Existing reliability improvement technologies incur high hardware overhead or testing costs. This paper proposes S2RAM-PUF, a novel, highly reliable and energy-efficient subthreshold SRAM PUF fabricated in 65nm process, with zero bit error rate (BER) across all voltage/temperature corners from 0.5V to 0.8V and from −40°C to 120°C. The 20480 bits generated by the fabricated 5 S2RAM PUF chips pass the NIST 800-22 randomness test and exhibit almost ideal uniqueness with a mean inter-die hamming distance of 0.5007. The total energy per bit is as low as 3.12fJ at 0.5V supply voltage. Both stabilization BER and energy outperform the two state-of-the-art SRAM-type PUFs reported in JSSC 2020 and 2021.

CCS CONCEPTS

• **Security and privacy → Hardware security implementation**; • **Hardware → Process, voltage and temperature variations**.

KEYWORDS

Hardware security, Physical unclonable function, SRAM PUF, Key generation, Reliability

ACM Reference Format:
Li Ni and Jiliang Zhang*. 2024. S2RAM PUF: An Ultra-low Power Subthreshold SRAM PUF with Zero Bit Error Rate. In *61st ACM/IEEE Design Automation Conference (DAC '24), June 23–27, 2024, San Francisco, CA, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3649329.3658246

1 INTRODUCTION

The physical unclonable function (PUF) is a promising lightweight hardware security primitive. It exploits process variations during chip fabrication to provide each device with a unique random key, which makes it naturally resistant to physical attacks [1]. Ideally, a PUF must provide the same output response for a given challenge input. However, these responses may change under noise or environmental fluctuations. Currently, reliability has become a critical challenge for PUF applications.

Table 1: Existing PUF reliability improvement techniques.

Reliability Techniques	Area Overhead	Power Consumption	Testing Costs	Anti-reverse Engineering
ECC [3]	High	High	Low	Yes
TMV [14]	Medium	Medium	Medium	Yes
Masking [4]	Low	Medium	High	Yes
Aging[6]	Low	Low	High	Yes
Oxide-breakdown[16]	Low	Low	Medium	No
Contact PUF[15]	Low	Low	High	No
Ours	**Low**	**Ultra-low**	**Low**	**Yes**

The most straightforward approach to improve reliability is to use error correction codes (ECC). However, the area, power, and latency overheads of ECC are unacceptable. For example, just for error correction of a 1-bit PUF cell, the area overhead of ECC is approximately equal to 1800 PUF cells [2]. Other reliability improvement techniques, such as temporal majority voting (TMV) [13, 14], masking strategy [3–5] and aging method [6], require large testing costs to detect unstable bits. For example, the masking technology in [3, 5] requires evaluating PUF with 100-1500 times for each set of temperature and voltage parameters.

Recently, oxide-breakdown PUF [16] and via/contact PUFs [15, 17] with zero bit error rate (BER) is proposed. The oxide-breakdown phenomenon is utilized to implement PUF function without ECC [16]. However, a significant overhead for generating and handling high voltages for oxide breakdowns is incurred [14]. The contact PUF utilizes small contacts whose size is set to be smaller than regular contacts allowed by the design rule. Thus, their connection is formed with a 50% probability for a random response generation. However, complex post-processing/post-silicon calibration or careful sizing adjustment is required to guarantee random response generation, bringing a large testing overhead. Most importantly, oxide-breakdown PUFs and contact PUFs are vulnerable to reverse engineering [18].

As shown in Table 1, unlike the above PUFs using ECC or oxide-breakdown/via/aging, this paper proposes an ultra-low power subthreshold SRAM PUF with zero BER based on a leakage-time-based one-time-test masking scheme. The main contributions of this work are summarized as follows.

- **Mono-stable SRAM Entropy Source**: We propose an ultra-low power subthreshold SRAM PUF with the mono-stable feature. It uses cross-coupled PMOS pairs to compete in the subthreshold region, which shows the lowest energy consumption and temperature sensitivity compared with the state-of-the-art SRAM PUFs.
- **One-time-test Masking**: We first reveal the phenomenon of a positive exponential relationship between the mismatch in PUF cells and the leakage time difference. Based on this phenomenon, we propose a new leakage-time-based masking scheme to precisely identify unreliable PUF cells with only one-time test on normal working conditions.

*Corresponding author: Jiliang Zhang.

DAC '24, June 23–27, 2024, San Francisco, CA, USA

ACM ISBN 979-8-4007-0601-1/24/06
https://doi.org/10.1145/3649329.3658246

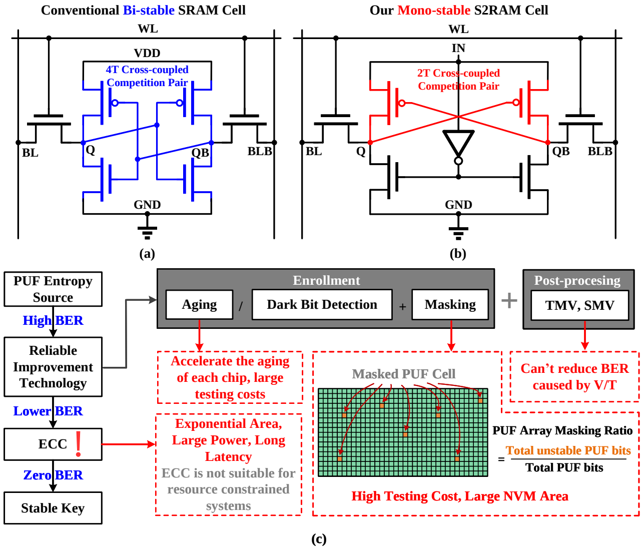
Conventional Bi-stable SRAM Cell
WL
VDD
4T Cross-coupled Competition Pair
BL
Q
QB
BLB
GND
(a)
Our Mono-stable S2RAM Cell
WL
IN
2T Cross-coupled Competition Pair
BL
Q
QB
BLB
GND
(b)
PUF Entropy Source
High BER
Reliable Improvement Technology
Lower BER
ECC !
Zero BER
Stable Key
Enrollment
Aging
/
Dark Bit Detection
+
Masking
+
Post-procesing
TMV, SMV
Accelerate the aging of each chip, large testing costs
Exponential Area, Large Power, Long Latency
ECC is not suitable for resource constrained systems
Masked PUF Cell
PUF Array Masking Ratio
= Total unstable PUF bits / Total PUF bits
High Testing Cost, Large NVM Area
Can't reduce BER caused by V/T
(c)

Figure 1: (a) Conventional bi-stable SRAM PUF cells. (b) Our S2RAM PUF cells. (c) Existing mainstream PUF reliability improvement technologies

- **Prototype and Evaluation**: An S2RAM-PUF is fabricated in 65nm CMOS process, and test results on 5 chips demonstrate ultra-low power consumption about 3.12 fJ/bit with zero BER across the operating environment of −40 to 120°C and 0.5 to 0.8V.

The remainder of this paper is organized as follows. Section II introduces background and related work. The proposed S2RAM-PUF with a leakage-time-based masking scheme is presented in Section III. The experimental results are discussed in Section IV. Conclusion is drawn in Section V.

2 BACKGROUND AND RELATED WORK

SRAM PUFs are one of the most mature PUFs available today and have been successfully commercialized. SRAM-based PUFs are typical bi-stable PUFs [3, 6–8]. Figure 1(a) shows the conventional bi-stable 6T SRAM bit cell structure [8], which utilizes the power-up state of the bit cell as the PUF response. The mismatch between a pair of cross-coupled inverters determines the PUF response. SRAM PUF reliability can be improved by post-processing such as aging and masking due to the usage of differential circuit structures. However, bi-stable PUFs are sensitive to noise which reduces native reliability. To improve native reliability, several mono-stable PUFs such as two-transistor amplifier PUFs [11], leakage PUF [9] and current mirror PUF [5, 12] have been proposed in recent years. However, their entropy sources strongly rely on the process variation of the amplification's first stage. In addition, unlike bi-stable PUFs, mono-stable PUFs cannot benefit from the advantages of differential circuit structures.

Figure 1(c) illustrates the mainstream PUF reliability improvement technologies including ECC [3], TMV [13, 14], aging [6], and masking [7, 8, 10]. The ECC incurs high area, power, and latency overheads. The TMV reads the same PUF cell multiple times with high repetition probability to select reliable response bits, which can eliminate the BER caused by random noise, but hardly mitigate PUF bit errors generated from the voltage/temperature (V/T) effects. In addition, repeated readouts of PUF cells bring high power consumption. The aging is to improve reliability by enlarging V_{th} mismatch of PUF cells. However, a higher-than-nominal supply voltage/temperature stressed to PUF transistors would bring high testing costs. The masking technique reduces BER by finding potentially unstable PUF cells that may flip under V/T variations. All PUF cells will be evaluated many times under different V/T corners, which results in a large testing overhead. To reduce testing overhead, recent masking methods [7, 8, 11] add a positive and negative mismatch in the PUF circuit to find unreliable cells. However, these methods still require multiple adjustments for positive and negative mismatches, and they require masking of a large number of PUF cells to achieve zero BER.

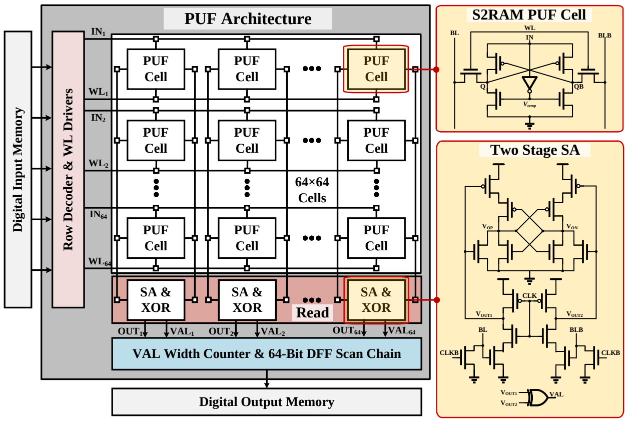

Figure 2: Top-level architecture of a 64-bit S2RAM-PUF.

This paper proposes an S2RAM-PUF cell as shown in Figure 1(b). It converts the bi-stable PUF into the mono-stable PUF and utilizes cross-coupled PMOS pairs to reduce noise impact and improve native reliability effectively. A new masking scheme based on leakage time is further proposed to accurately detect a wide range of unreliable bits without scanning test conditions, achieving ∼100% reliability with only one-time testing.

3 THE PROPOSED S2RAM-PUF

In this section, we first describe the top architecture of S2RAM-PUF, then introduce the cell circuit and its functional principle and characteristics in detail. And finally, the leakage-time-based masking scheme for S2RAM-PUF is presented.

3.1 The top architecture of S2RAM-PUF

Figure 2 gives the top-level architecture of a 64-bit S2RAM-PUF with a total of 4096 bits, including the cell array, decoder, two-stage sense amplifier (SA) circuit, XOR circuit, VAL width counter, and scan chain circuit. The cell array includes 64×64 PUF cells. Each cell consists of a subthreshold SRAM PUF entropy source and row control circuit. Each column of PUF cells shares the same two-stage sense amplifier circuit and XOR circuit. The word-line (WL) of the selected row turns on, which is controlled by the decoder. Then, the selected cell begins to generate differential voltages on the bit-line (BL and BLB) columns. The voltage difference between BL and

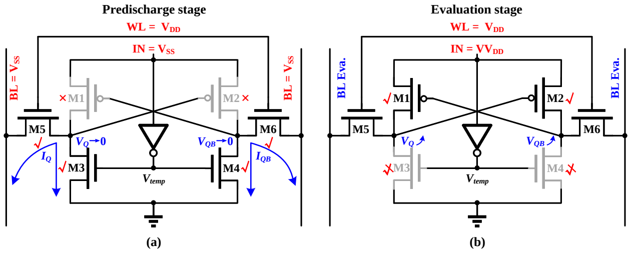

Figure 3: Circuit schematic of the S2RAM-PUF cell. (a) Predischarge stage. (b) Evaluation stage.

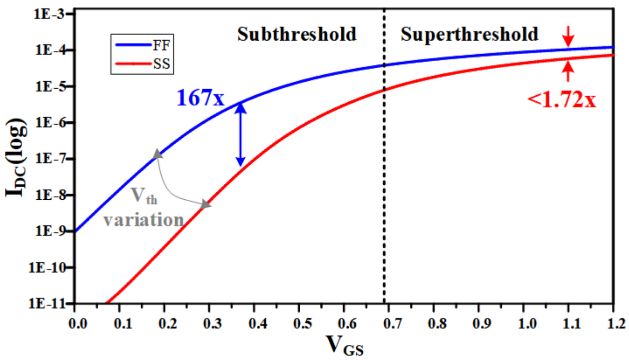

Figure 4: I-V characteristics according to variation in 65-nm CMOS process.

BLB is then sensed by the two-stage SA. The XOR gate and VAL width counter are used to detect unreliable cell. The final result is generated through parallel-to-serial conversion with two 64-bit scan chain circuits to save IO resources.

3.2 S2RAM-PUF cell

To reduce power consumption and improve native reliability, we design an S2RAM-PUF cell, as shown in Figure 3. Transistors M1 and M2 form a cross-coupled structure, and M3 and M4 form a set of leakage transistors. The working process of S2RAM-PUF includes predischarge and evaluation:

- **Predischarge stage**: As shown in Figure 3(a), when IN connects to V$_{SS}$ and WL connects to V$_{DD}$ voltage, M1 and M2 are turned off, and M3 and M4 are turned on. Thus, the voltage of BL/BLB leaks to V$_{SS}$. Then, Q/QB will be metastable state “0/0”.
- **Evaluation stage**: As shown in Figure 3(b), when the IN connects to VV$_{DD}$, M1 and M2 are turned on and enter in the subthreshold region. M3 and M4 are slowly turned off. Then, Q/QB immediately transitions from the metastable state “0/0” to the stable state.

To amplify the voltage/current differences between PUF cells induced by process variation, we exploit the large variation of subthreshold leakage current to design PUF. Figure 4 shows that the drain current (I$_{DS}$) curves as a function of gate–source bias voltage. We fix the drain voltage (V$_D$) and sweep the gate voltage (V$_G$) from 0V to 1.2V in FF and SS corners. We can see that the drain current is only 1.72× different in the superthreshold region, but this difference becomes 167× in the subthreshold region. The subthreshold current is shown as Formula (1).

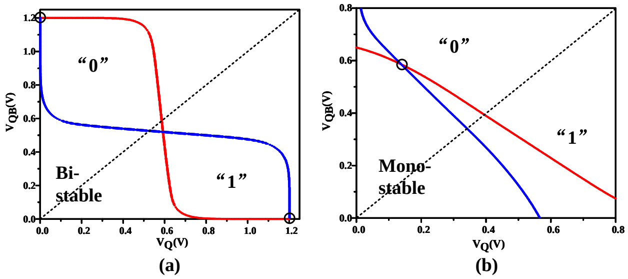

Figure 5: Simulated butterfly curves in (a) SRAM (b) proposed PUF.

$$I_{sub}{=}I_s\exp\left(\frac{V_{GS}-V_{th}}{nV_T}\right), \tag{1}$$

where V$_{th}$ represents the threshold voltage of transistors, V_T denotes the thermal voltage kT/q, and I_s is the characteristic current. The proposed structure makes full use of this characteristic to reduce the gain of PUF cells, allowing it to accumulate more differences in the subthreshold region to improve reliability. As shown in Figure 3, the M1 and M3 transistors are in the subthreshold region. We can get the following formula from the subthreshold model:

$$I_{s,M1}\exp\left(\frac{VV_{DD}-V_{QB}-\left|V_{th,M1}\right|}{nV_T}\right){=}I_{s,M3}\exp\left(\frac{V_{temp}-V_{th,M3}}{nV_T}\right), \tag{2}$$

$$V_{QB}=VV_{DD}-\ln(I_{s,M3}-I_{s,M1})\left(V_{temp}-V_{th,M3}\right)-\left|V_{th,M1}\right|, \tag{3}$$

where VV_{DD} is the subthreshold supply voltage. $I_{s,M1}$ and $I_{s,M3}$ are characteristic current of M1 and M3, respectively. V$_{th,M1}$ and V$_{th,M3}$ are threshold voltages of M1 and M3, respectively.

$$\begin{aligned} V_Q = VV_{DD}-\left|V_{th,M2}\right|+\frac{\beta}{\alpha}\left(V_{QB}+\left|V_{th,M1}\right|-VV_{DD}\right)& \\ +\beta\left(V_{th,M4}-V_{th,M3}\right),& \\ \alpha=\ln(I_{s,M3}-I_{s,M1}),\beta=\ln(I_{s,M4}-I_{s,M2}),& \end{aligned} \tag{4}$$

It can be seen from Formula (4) that V_Q is linearly related to V_{QB}. As VV_{DD} increases, V_Q keeps increasing. Compared with traditional CMOS inverters, its transfer curve tends to be flatter. Therefore, the proposed S2RAM cell has a smaller gain. According to Formula (4), the gain of the subthreshold inverter is derived as:

$$\text{Gain}=\left|\frac{dV_Q}{dV_{QB}}\right|{=}\frac{\beta}{\alpha}. \tag{5}$$

The Formula (5) shows that the gain is related to the characteristic current of transistor and is close to linearity. Figure 5 shows the butterfly curves of traditional SRAM and S2RAM PUF, where the solid circles represent the circuit solutions. It can be clearly seen that the butterfly curve of SRAM has two solutions, which means that the SRAM PUF is a bi-stable structure. Due to the low gain of the subthreshold inverter, the proposed PUF has only one cross-point (mono-stable). This mono-stable characteristic makes the transistor enter a stable state smoothly. When the ramp-up is

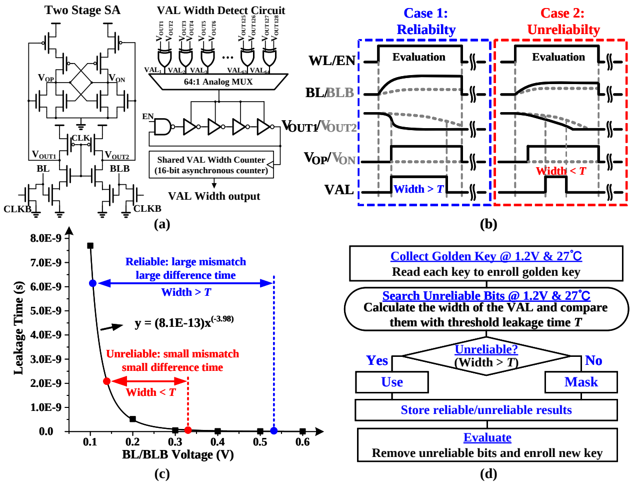
Two Stage SA
VAL Width Detect Circuit
V_{OUT1} V_{OUT2} V_{OUT3} V_{OUT4} V_{OUT5} V_{OUT6} V_{OUT125} V_{OUT126} V_{OUT127} V_{OUT128}
VAL_1 VAL_2 VAL_3 VAL_{63} VAL_{64}
64:1 Analog MUX
EN
Shared VAL Width Counter (16-bit asynchronous counter)
VAL Width output
V_{OP} V_{ON}
CLK
V_{OUT1} V_{OUT2}
BL BLB
CLKB CLKB
(a)
Case 1: Reliabilty
Case 2: Unreliabilty
WL/EN
Evaluation
Evaluation
BL/BLB
V_{OUT1}/V_{OUT2}
V_{OP}/V_{ON}
VAL
Width > T
Width < T
(b)
Leakage Time (s)
8.0E-9
7.0E-9
6.0E-9
5.0E-9
4.0E-9
3.0E-9
2.0E-9
1.0E-9
0.0
0.1
0.2
0.3
0.4
0.5
0.6
BL/BLB Voltage (V)
Reliable: large mismatch large difference time
Width > T
y = (8.1E-13)x^(-3.98)
Unreliable: small mismatch small difference time
Width < T
(c)
Collect Golden Key @ 1.2V & 27˚C
Read each key to enroll golden key
Search Unreliable Bits @ 1.2V & 27˚C
Calculate the width of the VAL and compare them with threshold leakage time T
Unreliable? (Width > T)
Yes
No
Use
Mask
Store reliable/unreliable results
Evaluate
Remove unreliable bits and enroll new key
(d)

Figure 6: (a) The circuit for masking. (b) Waveform of masking scheme. (c) Relationship between BL/BLB voltages and leakage time. (d) Leakage-time-based masking scheme.

slow enough, the chance of bits flipping is small. Thus, the native reliability is improved by reducing the gain.

3.3 Leakage-time-based masking scheme

We first reveal the phenomenon of positive exponential relationship between the mismatch of PUF cells and the leakage time difference. Based on this phenomenon, we propose a leakage-time-based masking scheme which only requires measuring the time difference of node capacitor leakage to fast detect the mismatch of PUF cells. As illustrated in Figure 6(a), the specific circuit for masking is designed. The XOR gate and VAL width counter are used to detect unreliable cells. We can derive the leakage time difference from the capacitor leakage of the V_{OUT} node in the two-stage SA. The formula of leakage time difference $\Delta T_{leakage}$ is as follows:

$$\Delta T_{\text{leakage}} \approx \frac{CV_{OUT}\left(I_s \exp\left(\frac{V_{BL}-V_{th}}{nV_T}\right) - I_s \exp\left(\frac{V_{BLB}-V_{th}}{nV_T}\right)\right)}{I_s \exp\left(\frac{VV_{DD}-2V_{th}}{nV_T}\right)} \qquad (6)$$

where C is the node capacitance, V_{OUT} is the output of the first stage SA, V_{BL} and V_{BLB} are the voltages on the BL and BLB columns respectively. We can see from the Formula (6) that the leakage time difference of V_{OUT} and the voltage difference between BL and BLB (V_{BL} - V_{BLB}) are positive exponential relationship. Since V_{BL} - V_{BLB} can represent the mismatch of PUF cells, the mismatch and the leakage time difference have the same positive exponential relationship.

In what follows, we further validate this phenomenon through experiments and simulations. The waveform of leakage-time-based masking scheme is illustrated in Figure 6(b). As the S2RAM cell begins evaluation, the voltage difference on the BL and BLB columns gradually stabilizes. The corresponding V_{OUT1} and V_{OUT2} will begin to leak charges according to the voltages of BL and BLB. When there is a large mismatch in the PUF cell (Case 1), VAL exhibits a longer duration of high-level voltage. Conversely, VAL has a shorter duration of high-level voltage (Case 2). Then, we simulated the relationship between the leakage time of V_{OUT} and the voltages of V_{BL} and V_{BLB}, as shown in Figure 6(c). We can clearly observe an inverse exponential relationship between the leakage time and the voltages of BL or BLB. The greater the voltage difference between BL and BLB, the larger the leakage time difference. Since the voltage difference between BL and BLB represents the mismatch of PUF cells, the larger the voltage difference means the higher reliability for PUF cells.

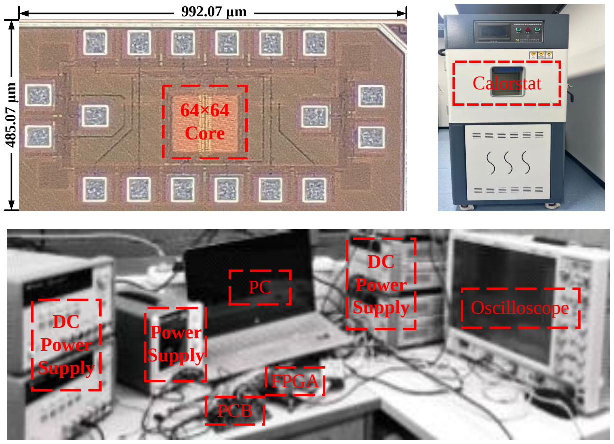

Figure 7: Experimental platform.

The flow chart of the proposed leakage-time-based masking scheme is shown in Figure 6(d). At first, we read the PUF key and record the golden key under normal working conditions. Then, we calculate the width of VAL and compare it with threshold leakage time T to search for unreliable bits. If width > T, the PUF cell is reliable. Otherwise, we mask the cell. Finally, we can remove enough unreliable bits based on reliability requirements. At normal working conditions, we only calculate the leakage time difference one time to obtain reliable information for all cells. The proposed masking scheme only requires 64 XOR gates and the shared VAL width counter with 252.2μm^2 area overhead (0.052% of the total chip area). It eliminates expensive and time-consuming temperature sweeps in previous masking techniques.

4 EXPERIMENT AND ANALYSIS

The proposed S2RAM-PUF is fabricated in a 65nm CMOS process. The 64×64 cell array occupies 0.016mm^2, and area per bit is 521F^2. The entire 64×64 PUF array, including the readout circuit, occupies an area of ~24534μm^2 (174 μ m×141 μ m). Figure 7 shows the entire PUF test platform consisting of a calorstat, PC with Intel (R) Core (TM) i7-12700H, Zedboard Zynq-7000 FPGA Development Board, dual-output DC voltage source, printed circuit board (PCB) and digital oscilloscope.

4.1 Native PUF Reliability

The reliability of PUF is evaluated using BER and the percentage of unreliable bits. Reliability testing is performed on 5 chips (20k bits) at 0.6V/25°C. As shown in Figure 8, The native BER is 2.64E-3, and the unreliable bits are 2.82E-2. The BER with TMV11 [14] is

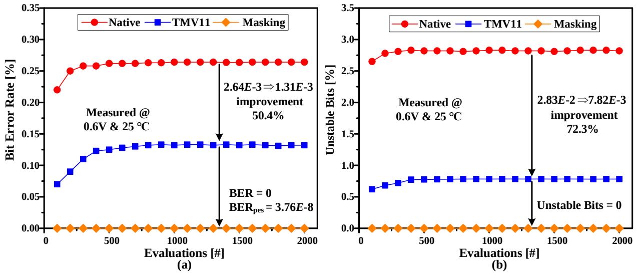

Figure 8: BER and unstable bits evaluated at the nominal condition.

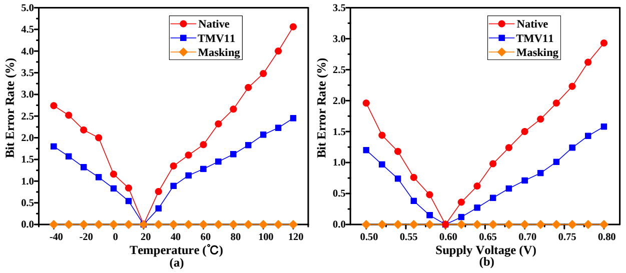

Figure 9: (a) BER versus temperature variation under different reliability methods. (b) BER and flipping bits versus supply voltage.

reduced to 1.31E-3, and the unreliable bits are reduced to 7.82E-3, which are reduced by 50.4%/72.3% respectively. Using the proposed masking scheme, only 35% of the bits are masked, and the BER and unreliable bits are reduced to 0. At 2000 times evaluations, the pessimistic BER according to (7) is 1/(5 × 4096 × (1 - 35%) × 2000) = 3.76E-8.

$$\mathrm{BER_{pes}} = \frac{1}{\#\mathrm{Bit} \times (1 - \mathrm{MaskingRatio}) \times \#\mathrm{Evaluation}}, \qquad (7)$$

4.2 PUF Reliability over Voltage and Temperature Variations

The PUF reliability over environmental variation is evaluated across the temperature range of −40°C ∼ 120°C and a voltage range of 0.5V ∼ 0.8V. The golden key is enrolled at 0.6V/20°C. Figure 9(a) shows the BER across temperature variation. The PUF has an average native BER of 2.74% at −40°C and 4.57% at 120°C; the native sensitivity to temperature is 0.457%/10°C; the average BER is reduced to 2.45% by TMV. Figure 9(b) shows the BER as a function of voltage using different stabilization methods. The average native BER is 1.96% at 0.5V and 2.93% at 0.8V, native sensitivity to voltage is 1.63%/0.1V. The average BER is reduced to 1.58% with the TMV method. After adopting the proposed masking scheme, the BER is reduced rapidly, and there are no errors across the entire testing V/T range.

4.3 Uniqueness and Randomness

The uniqueness of S2RAM-PUF was evaluated by measuring the inter-/intra-die hamming distance (HD). Figure 10(a)shows the measured HD of 5 PUFs. The inter-die HD has a mean value of 0.5007, and the average intra-die HD is 0.0062, achieving 80.8 times separation between inter- and intra-die HDs. The autocorrelation of 20480 PUF bits with 95% white noise confidence level at 0.0141 is shown in Figure 10(b). The near-ideal HD and autocorrelation results validate the proposed PUF.

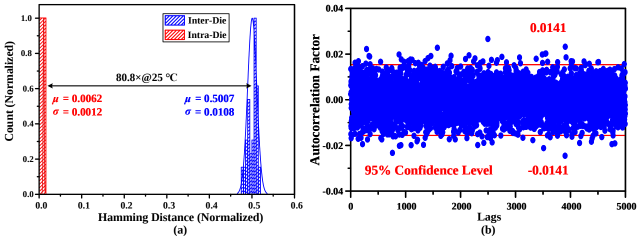

Figure 10: (a) Measured normalized HD. (b) Measured autocorrelation of bit cells.

Table 2: NIST 800-22 randomness test.

Test	Stream length	No. of runs	Average P-value	Pass?
Frequency	2048	10	0.5451	100
Block Frequency	2048	10	0.5539	100
Runs	2048	10	0.4243	100
Rank	2048	10	0.3438	100
Longest Runs	2048	10	0.3460	100
FFT	2048	10	0.3004	100
Cumulative Sums	2048	10	0.5703	100
Non-overlapping	2048	10	0.5577	100
Overlapping Template	2048	10	0.4323	100
Serial	2048	10	0.5761	100
Approximate Entropy	2048	10	0.1935	100

To evaluate the randomness of PUF responses, NIST 800-22 randomness test suites [19] are performed on 20480 bits collected from 5 chips. With the limited number of bits, 11 out of 15 subtests are available. Table 2 shows that the proposed S2RAM PUF has successfully passed all 11 randomness tests, showing high-quality randomness.

4.4 Comparison with Prior Works

S2RAM-PUF is compared with the state-of-the-art PUFs in Table 3. Compared with the SRAM-based PUFs [6–8], S2RAM-PUF shows the lowest temperature sensitivity with only 0.457%/10°C and the lowest energy about 3.12fJ/bit at 0.5V supply voltage. Compared with other PUF types [10], [9], [14], S2RAM-PUF exhibits the lowest native BER about 0.264%. When the temperature rises to 80°C, the native BER of S2RAM PUF is 2.66%, while the BER of [14] is 4.54%. The BER for S2RAM-PUF after post-processing becomes 0, which is better than the 6.1E-5/9E-6 BER in [9] and the 0.088/0.085 BER in [14]. Specially, the proposed masking in this paper has the lowest masking rate. BER$_{pes}$ of S2RAM-PUF is better than [6, 7] but worse than [8]. However, [8] requires to mask 59% of PUF cells and up to 120,000 evaluations within a restricted temperature range (−10°C to 85°C).

5 CONCLUSION

This paper proposes a high reliability and energy efficiency S2RAM-PUF. The mono-stable S2RAM cell is designed for reducing the gain

Table 3: Comparison with the state-of-the-art PUFs.

	ESSCIRC'22 [10]	DAC'22 [9]	JSSC'22 [14]	TCAS1'20 [8]	JSSC'20 [7]	JSSC'21 [6]	**Proposed**
Technology (nm)	65	55	180	65	130	130	**65**
Type	Leakage Mismatch	INV/ Leakage Mismatch	NAND Mismatch	SRAM Mismatch	SRAM Mismatch	SRAM Mismatch	**SRAM Mismatch**
Reliability Technique	Current Tilt based, Masking	BCS	Remapping and TMV	Capacitive Tilt based, Masking	VSS Bias based, Masking	Aging	**Leakage time based Masking**
Normalized Bitcell Area (F^2/bit)	926.4	1071.5	20	3001	373	497	**521**
Total Energy (fJ/bit)	-	910.4/266.9	1380000	15.39	128	47.88 (0.6V) 16.76 (0.5V)	**28.75 (0.6V)** **3.12 (0.5 V)**
Temp. Range (°C)	0 ∼ 100	−40 ∼ 125	−20 ∼ 80	−10 ∼ 85	−40 ∼ 120	−40 ∼ 120	**−40 ∼ 120**
VDD Range (V)	0.9 ∼ 1.5	0.96 ∼ 1.44	1.5 ∼ 1.9	0.8 ∼ 1.2	0.8 ∼ 1.4	0.5 ∼ 0.7	**0.5 ∼ 0.8**
Native BER (%)	0.77	0.54/0.50	0.798/0.937	2.24	0.21	0.29	**0.264**
Temperature Sensitivity (%/10°C)	0.656	0.404/1.089	1.01/0.96	0.67	0.659	0.547	**0.457**
Masking Ratio (%)	47	-	-	59	67	-	**35**
BER after Post-processing	0 2.05E-8	6.1E-5/9E-6	0.088/0.085	0 1.0E-9	0 4.0E-7	0 5.99E-7	**0** **3.76E-8**
Number of evaluations	4000	1000	2000	120000	1000	2000	**2000**
Inter-die HDs (Uniqueness)	0.5009	0.4681/0.4788	0.4998/0.4975	0.4825	0.4923	0.4873	**0.5007**

TMV: TMV with 11 bits; BCS: the bit configuration strategy.

to improve the PUF's noise resilience. The low working voltage for the subthreshold PUF brings ultra-low power consumption. In addition, we first reveal the phenomenon that the mismatch of PUF cells has an exponential correlation with the leakage time difference. Based on this phenomenon, we propose a leakage time-based masking scheme to implement 0 BER with only one-time test. S2RAM-PUF is fabricated in 65nm CMOS process. Test results show that it has a low native BER of 0.264%. With the proposed masking scheme, BER is reduced to 0 (BER$_{pes}$ <3.76E8). The energy per bit is only 3.12fJ at 0.5V supply voltage. The uniqueness and autocorrelation of the responses are 0.5007 and ±0.0141, respectively.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China under Grant (No.U20A20202 and No.62122023) and the Hunan Provincial Key Research and Development Project (No. 2023GK2011).

REFERENCES

[1] G. E. Suh et al., "Physical unclonable functions for device authentication and secret key generation," in *DAC*, 2007, pp. 9–14.

[2] Z. Y. Liang et al., "A wide-range variation-resilient physically unclonable function in 28 nm," *IEEE JSSC* vol. 55, no. 3, pp. 817–825, 2019.

[3] S. Satpathy et al., "A 4-fJ/b delay-hardened physically unclonable function circuit with selective bit destabilization in 14-nm trigate CMOS," *IEEE JSSC*, vol. 52, no. 4, pp. 940–949, 2017.

[4] B. Karpinskyy et al., "8.7 Physically unclonable function for secure key generation with a key error rate of 2E-38 in 45nm smart-card chips," in *ISSCC*, 2016.

[5] A. B. Alvarez et al., "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 JSSC*, vol. 51, no. 3, pp. 763–775, 2016.

[6] K. Liu et al., "A 0.5-V hybrid sram physically unclonable function using hot carrier injection burn-in for stability reinforcement," *IEEE JSSC*, vol. 56, no. 7, pp. 2193–2204, 2021.

[7] K. Liu 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 JSSC*, vol. 55, no. 6, pp. 1719–1732, 2020.

[8] Y. Shifman et al., "An sram-based PUF with a capacitive digital preselection for a 1E-9 key error probability," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 12, pp. 4855-4868, 2020.

[9] J. Zhang et al., "DA PUF: dual-state analog PUF," in *DAC*, 2022, pp. 73–78.

[10] B. Park et al., "A 183F^2 gate leakage-based physically unclonable function with area efficient current tilting-based masking scheme," in *ESSCIRC*, 2022, pp. 517–520.

[11] K. Yang et al., "8.3 A 553F^2 2-transistor amplifier-based physically unclonable function (PUF) with 1.67% native instability," in *ISSCC*, 2017, pp. 146–147.

[12] S. Taneja et al., "PUF architecture with run-time adaptation for resilient and energy-efficient key generation via sensor fusion," *IEEE JSSC*, vol. 56, no. 7, pp. 2182–2192, 2021.

[13] J. Li et al., "Ultra-compact and robust physically unclonable function based on voltage-compensated proportional-to-absolute-temperature voltage generators," *IEEE JSSC*, vol. 51, no. 9, pp. 2192–2202, 2016.

[14] J. Lee et al., "A 20F^2/bit current-integration-based differential nand-structured PUF for stable and V/T variation-tolerant low-cost IoT security," *IEEE JSSC*, vol. 57, no. 10, pp. 2957–2968, 2022.

[15] D. Jeon et al., "A physical unclonable function with bit error rate< 2.3×108 based on contact formation probability without error correction code," *IEEE JSSC*, vol. 55, no. 3, pp. 805-816, 2020.

[16] K. H. Chuang et al., "A physically unclonable function using soft oxide breakdown featuring 0% native BER and 51.8 fJ/bit in 40-nm CMOS," *IEEE JSSC*, vol. 54, no. 10, pp. 2765-2776, 2019.

[17] T.W. Kim et al., "Zero bit error rate ID generation circuit using via formation probability in 0.18 μ m CMOS process," *IEEE EL*, vol. 50, no. 12, pp. 876-877, 2014.

[18] J. Lee et al., "A 354F^2 leakage-based physically unclonable function with lossless stabilization through remapping for low-cost IoT security," *IEEE JSSC*, vol. 56, no. 2, pp. 648-657, 2020.

[19] A. Rukhin et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-allen and hamilton inc mclean va, Tech. Rep., 2001.