# A High Reliable SRAM-Based PUF With Enhanced Challenge-Response Space

Lu Lu, *Member, IEEE*, and Tony Tae-Hyoung Kim, *Senior Member, IEEE*

***Abstract*—This brief proposes a sequence-dependent SRAM-based PUF with enhanced reliability. It expands the CPRs by order of (rows$^{(sequence\ length\ +\ 2)}$ × columns) for reliable authentication. The proposed bitcell utilizes split word-lines to control two access transistors separately. The PUF mode turns on two left word-lines and two right word-lines simultaneously, including 18 transistors for generating one-bit data. This proposed technique supports rendering multiple data maps from one chip. Besides, various temperature and voltage combinations can create a reliability map for each data map. A test chip was fabricated in 40 nm CMOS technology. The measured worst bit error rate is 0.8% at the nominal point (1V, 20° C). From a single chip, the proposed PUF achieved the hamming distances of 41.29% for one sequence with different orders and 44.93% for other sequences, respectively. The measured inter-chip hamming distance is 49.64%.**

***Index Terms*—SRAM, PUF, reliability, sequence length, permutation, hardware security.**

## I. Introduction

PHYSICALLY unclonable function (PUF) is a promising essential primitive device for authentication and secret key generation in modern IoT systems. PUF uses the intrinsic characteristic of hardware modules to generate an irreplicable and irreproducible secret key. PUF is widely used in the payment platform, encrypting communication, authorized access, and other applications [1]. Three essential requirements in PUF include randomness, reliability, and uniqueness [2]. The randomness monitors the proportion and distribution of the data map; the reliability requires the device to regenerate the same pattern in different environments; the uniqueness confirms whether the encryption device is irreplaceable.

SRAM-based PUF (SPUF) produces a secret key by utilizing unpredictable variations in the manufacturing process. In various systems, we can reuse SRAM as PUF to minimize the area overhead [3]. Therefore, SPUF should work functionally in both SRAM mode and PUF mode. The larger physical mismatch between the coupled inverters in a bitcell will improve the PUF stability while degrading the static noise margin of the SRAM mode.

Manuscript received June 17, 2021; revised July 7, 2021; accepted July 15, 2021. Date of publication July 21, 2021; date of current version January 31, 2022. This work was supported by MediaTek's IC Shuttle Programme. This brief was recommended by Associate Editor A. J. Acosta. *(Corresponding author: Lu Lu.)*

Lu Lu is with Nanyang Technological University, Singapore (e-mail: lulu@ntu.edu.sg).

Tony Tae-Hyoung Kim is with the Department of Electrical and Electronic Engineering, Nanyang Technological University, Singapore.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCSII.2021.3099010.

Digital Object Identifier 10.1109/TCSII.2021.3099010

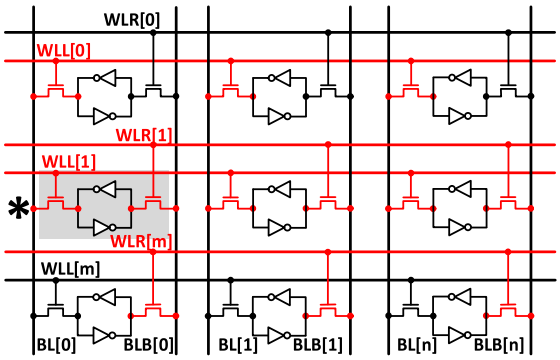
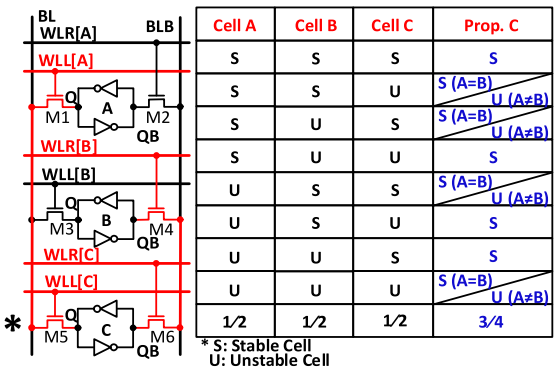



Fig. 1. Operation principle of the proposed PUF data generation.

Conventional SPUF has only one result corresponding to one address. Therefore, the challenge-response pair (CRP) is 1, and it works as a chip ID. To upgrade the security level, multiple CRPs can update the secret key regularly. Furthermore, the password can be amended when the chip ownership is changed. To expand CRP, the SPUF in [4] involved two bitcells to generate one random data. They utilized the initial data by connecting them in different sequences and orders to produce a programmable sequence-dependent response. Both the intrinsic physical variations from fabrication and the permutation/combination of the code affect the PUF data. However, it only selected two rows at one time, which shows limited improvement.

Another significant challenge in PUF is reliability. Various PUF designs focused on the bit error rate (BER) only under a specific operating condition [5], [6]. However, it is significant to provide stability in the whole voltage and temperature (VT) range. Some data may behave reliably in certain VT corners but may flip in other VT conditions. Several PUF techniques for reliability have been reported in the literature [7]–[11]. To improve reliability, transistor aging, error correction code (ECC), and temporal majority voting (TMV) are widely utilized [7]. However, aging can degrade the performance of the SRAM function. ECC and TMV require large areas with additional circuits. In [8], the threshold voltage of two access transistors in conventional 6T SRAM cells is converted into the data. However, the limited variations can degrade the randomness.

This brief proposes a novel sequence-dependent SRAM-based PUF with improved reliability. The proposed PUF cell structure generates multiple reliable PUF data sets and expands the challenge-response space by the order of (rows$^{(\text{sequence length}+2)}$ × columns). Besides, we employed the bit selection algorithm to generate a data mask for each data map, which further improves the reliability in the whole VT range.




| Cell A | Cell B | Cell C | Prop. C |
|---|---|---|---|
| S | S | S | S |
| S | S | U | S (A=B) / U (A≠B) |
| S | U | S | S (A=B) / U (A≠B) |
| S | U | U | S |
| U | S | S | S (A=B) / U (A≠B) |
| U | S | U | S |
| U | U | S | S |
| U | U | U | S (A=B) / U (A≠B) |
| 1/2 | 1/2 | 1/2 | 3/4 |

Fig. 2. Reliability enhancement for PUF operation.

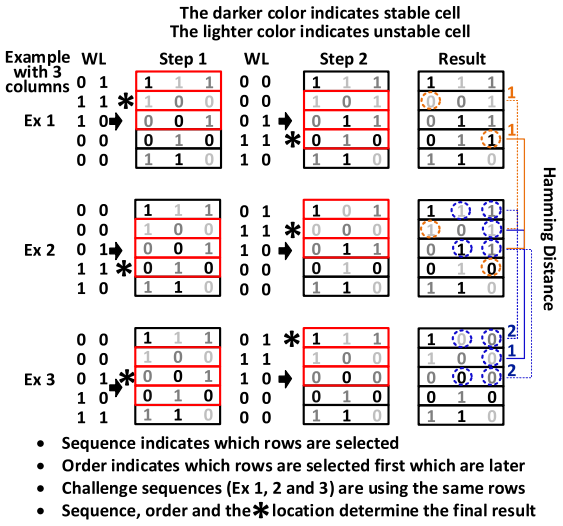



Fig. 3. Dependency of SPUF data on selection sequence order.

## II. Proposed Reliable PUF

### A. Proposed SPUF Cell

Conventional SRAM-based PUF (SPUF) generates raw data during power-up utilizing a traditional 6T SRAM bitcell structure. The data is affected by noises and mismatches between the cross-coupled inverters. The likelihood of the raw data becoming '0' or '1' depends on the PVT variations created during the fabrication process.

Fig. 1 illustrates the schematic of the proposed 6T SPUF array. Each cell consists of two cross-coupled inverters with minimum-sized transistors and two pass-gate transistors with doubled width. Compared to the conventional 6T SRAM cell, the proposed bitcell splits the word-line (WL) into the left word-line (WLL) and the right word-line (WLR). They control the two access transistors independently. Unlike the conventional SPUF, which directly uses raw data as a security key, the proposed design utilizes sequence-dependent programming to generate one-bit data, improving reliability. During the PUF operation, both BL and BLB are pre-charged to high potential, and the selected row marked with * (asterisk) is turned on through both WLL [1] and WLR [1]. We also choose additional two rows by asserting either WLL or WLR in each of them. Note that only one access transistor is on in the half-selected cells. The write ability is weak due to the single-ended writing. Therefore, the size of access transistors is doubled to provide a proper write margin. We define a cell with a large mismatch as a stable cell and a cell with a smaller mismatch as an unstable cell. When the three selected cells are connected to BL and BLB, the stable cell may overwrite the unstable one in each column. This proposed scheme can enrich the entropy with the fabrication process variations from conventional 6 transistors to 18 transistors to contribute to the arms race.

### B. Reliability Enhancement

Reliability is a crucial criterion for PUF design. The response to the same challenge should be reproducible under different environmental circumstances. BER represents the percentage of the flipped bits during multiple PUF operations at different times in one device, which indicates the reliability of a PUF. Fig. 2 illustrates the proposed PUF reliability enhancement technique. We divide cells into stable cells and unstable cells and assume that the probability for a cell to be stable is 50%. Here, cell C is marked with an asterisk as a fully selected cell, Q[A] and Q[C] are connected through BL, QB[B], and QB[C] are connected through BLB, respectively. If the stabilities of the cells are: A = S, cell B = U, and cell C = S (S represents a stable cell and U represents an unstable cell), when the initial values of cell A and B are the same, the data of cell C will flip according to the value of cell A and B stably. If cell A and cell B store different data, cell C is written different data from two sides, becomes unstable. Therefore, the stability of proposed cell C from stable becomes conditionally stable (50%). If A = S, cell B = S, and cell C = S, regardless of the initial values in cell A and B, the proposed cell C is stable. When cell A = cell B, the proposed technique makes cell C stable. If cell A ≠ cell B under (cell A = S, cell B = U, and cell C = S), (cell A = U, cell B = S, and cell C = S), (cell A = S, cell B = S, and cell C = U), and (cell A = U, cell B = U, and cell C = U), cell C becomes conditional unstable. To sum up, the stability of cell C using the proposed technique is 0.75, which is improved compared to 0.5 in the conventional scheme.

### C. Sequence Dependent SPUF Analysis

Besides using three cells to generate one-bit data, we could also compose multiple steps to generate one-bit data in one column by choosing different three cells successively. For instance, after the first PUF operation, we choose two cells in the first step, one of them is the fully selected cell with the asterisk. Then combine these two cells with one cell from another row which is unselected before. Fig. 3 displays three examples using two steps with different combinations, the darker bits indicate stable cells, and lighter bits are overwritten by the darker ones. In the first example, the first sequence connects the top three rows (the second row is fully selected), and the second step links the bottom three rows together (the fourth row is fully selected), written as a sequence of (1, 2*, 3) (3, 4*, 5). The second example could be written as a sequence of (3, 4*, 5) (1, 2*, 3). So, the final value of the SPUF is affected by the sequence order even if we choose the same rows with the same location of fully selected cells. In the 2nd and 4th rows, the hamming distances are both 1. Furthermore, the sequences of the second and third examples are (3, 4*, 5) (1, 2*, 3) and (3, 4, 5*) (1*, 2, 3), respectively. Note that even with the same rows and sequence permutations, the final

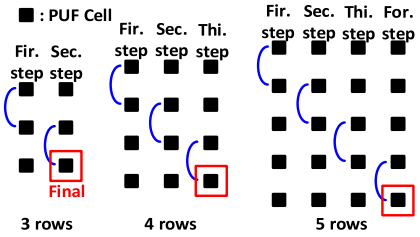



Fig. 4. Previous technique for changing sequence lengths [4].

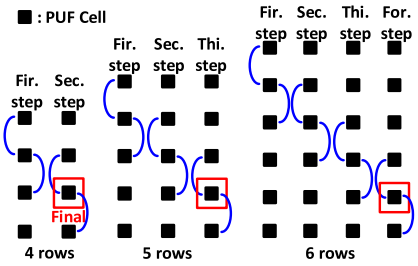



Fig. 5. Changing sequence length in proposed SPUF.

states are also influenced by the location of the fully selected cell. The hamming distances of final data are 2, 1, and 2 in the 1st, 2nd, and 3rd rows respectively. Therefore, the PUF key is not only decided by the selected rows and the sequence order of the selection, but also the location of the fully selected cell. This explains that the proposed SPUF can generate different security maps from one device, more resilient when facing attacks as a weak PUF. The power overhead is 4.55% in each step compared to the conventional operation.

### D. CRPs Enhancement

Typically, SRAM-based PUF has limited CRPs. The worst-case CRP is only 1. The limited CRP easily becomes an attack target. To improve security, CRP extension is addressed in this work.

Jeloka *et al.* presented a sequence-dependent SPUF with the conventional SRAM 6T cell structure [4], which utilizes two cells to generate one-bit data. The final data is determined by the length of the sequence and the permutations. Fig. 4 explains the way of combining sequence lengths [4]. If sequence length is r, the number of CRPs for an array with m rows and n columns is:

$$m \times (m-1) \times \cdots \times (m-r) \times n \tag{1}$$

In the proposed SPUF, we connect three rows to generate one final data and use multiple operations to increase the CRPs space. If the sequence length is 2, we will choose 4 rows from m rows, the combination is $C_m^4$. Then we have $C^3{}_4 \times C^1{}_2$ choices. As illustrated in Fig. 5, we can get the different permutations with higher sequence length and larger scale array. Using the analogy, in 6 rows, the CRPs in one column is 2880 with four-step PUF operations. In an array with m rows and n columns, and the sequence length of r, the number of CRPs could be written as follow:

$$\left[r!/6\right] \times [m \times (m-1) \times \cdots \times (m-r) \times (m-r-1)] \times n \tag{2}$$

where r $\leq$ (m $-$ 2).

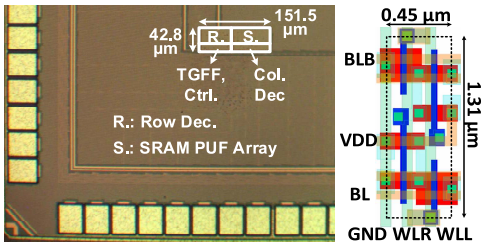



Fig. 6. Die photo of the proposed SPUF and the layout of the bitcell.

To sum up, the responses of the proposed SPUF are decided by the initial start-up data, the sequence length, the applied order, and the location of cells which are with an asterisk. The expanded CRP space increases randomness and improves the security of the PUF.

## III. Operation Flow and Measurement Results

A 4kb (64 ×64) SRAM PUF array test chip was fabricated in 40nm CMOS technology. The die photo and the layout of the bitcell are shown in Fig. 6. The total area is 151.5 × 42.8 $\mu m^2$ and the size is 0.59 $\mu m^2$ per bit cell. Since the start-up data is generated by the mismatches from fabrication, the placement in the front-end layers of the layout should be symmetric. A logic analyzer was used to build the experiment platform. The operating frequency for one-step PUF operation is 10MHz under 1V/20°C.

For the proposed SPUF, the data map is determined by the sequence length and sequence order. We could generate multiple data maps by programming the sequence. When sequence length equals 5, the CRP reaches 4.01 × $10^{15}$. To further improve the stability, a bit selection algorithm generates a stability map to identify the stable cells in one device [12]. The environment in the testing setup is in the voltage range (0.7V∼1.2V) and temperature range (20°C ∼80°C). After one or multiple PUF operations, we could measure the data in high voltage 1.2V with low temperature 20° C (HVLT), repeating the operation ten times. Then we could generate a table of the array with each cell's stability coefficient, which is calculated from the number of times these cells could reproduce the same data. For example, if one cell produced 7 times '1' and 3 times '0', the stability coefficient is 0.7. Another table could be created by low voltage 0.7V and high temperature 80° C (LVHT) condition. Combining these two tables, we could produce the stability map by filtering weak cells which coefficient 0.2 < $C_{HVLT}$ < 0.8 or 0.2 < $C_{LVHT}$ < 0.8. This filtering criterion keeps the masking ratio at a certain level. The proposed SPUF can provide a highly reliable PUF device with large CRPs by associating the data map and the stability map. The operation flow is shown in Fig. 7.

Fig. 8 shows the NIST SP800-22 test result. The proposed SPUF passed 11 out of 15 NIST tests. The failures in the four tests are caused by the insufficient data from the limited bitstream size. Note that this is an inherent limit of weak PUFs. It shows the generated data suffices the randomness standard.

Fig. 9 exhibits the hamming distance (HD) in the same sequence #1 with different sequence lengths. In each sequence length, we ran sequence #1 in different orders. The HD is improving by running longer sequence length under the same VT condition, the mean value of HD increased from 23.8% to 41.29% when the sequence length is added from 2 steps to 5 steps. Fig. 10 shows the HD with 5 steps sequence length in

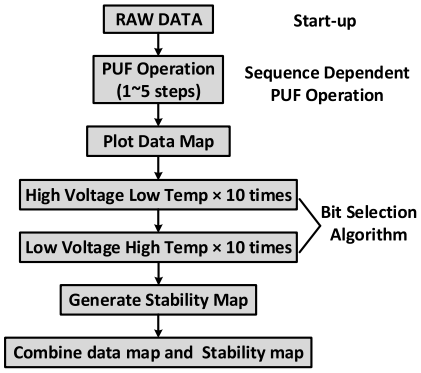



Fig. 7. The operation flow to generate stable data map.

TABLE I
COMPARISON WITH STATE-OF-THE-ART WORKS

| | JSSC '20 [13] | ISSCC '21 [14] | VLSI '17 [4] | ISCAS '19 [10] | This Work |
|---|---|---|---|---|---|
| Technology | 130nm | 65nm | 28nm | 65nm | 40nm |
| Area/PUF bits | 373 $F^2$ | 594 $F^2$ | 388-970 $F^2$ (2-5 cells) | 5.2 $\mu m^2$ (4 cells) | 987 $F^2$ (3 cells) |
| Energy efficiency (fJ/b) | 128 | 0.057 | 97 (seq-5, 0.7 V) | 81 (seq-5, 0.5 V) | 127 (seq-5, 1 V) |
| Throughput (Gbps) | — | 22 (0.6 V) | 1.1 (seq-5,0.7 V) | — | 8 (seq-5, 1 V) |
| Masking Ratio | 67% | 27% | — | — | 29.76% |
| Inter-PUF HD | 0.4923 | 0.4995 | 0.481 - 0.495 | 0.487 | 0.4964 |
| BER (%) | < 5.99E-7 (Worst VT) | < 3.34E-8 (Worst VT) | 3.17 (0.7V, 27°C) | 3 (0.8V, 20°C) | 0.8 (1V, 20°C) |
| # Possible CRPs | 1 | 1 | $1.17 \times 10^{11}$ (seq-5) | $8.37 \times 10^{17}$ (seq-5) | $4.01 \times 10^{15}$ (seq-5) |
| Weak/Strong | Weak | Weak | Weak | Weak | Weak |
| Dual Mode* | No | No | Yes | Yes | Yes |

*Dual Mode: If the chip can work in both memory mode and PUF mode.

three conditions. The red curve is the HD between sequence #1 with different orders in one chip, also shown in Fig . 9. The blue one is the HD between different sequences (#1∼ #100) in one chip, and the black curve is the HD between multiple chips. The HD between different sequences and different chips achieve 44.93% and 49.64%, respectively. Fig. 11 exhibits different data maps from one chip, the dark box indicates "0' and the light box indicates '1'. (I) shows the star-up data of this chip, the distribution is unbalanced, more data '0' cluster on the top. After the PUF operation in sequence #1 order #1 (sequence length = 5), the data map turns to (II), the data distribution is more evenly distributed. (III) is produced by rebooting this chip and repeating Sequence #1 with order #2, and (IV) is generated from running Sequence #2 with the same sequence length after resetting the chip. The distribution of data maps in (II), (III), and (IV) are distinct from each other. the distribution of the data maps manifests that the proposed SPUF could generate multiple CRPs by changing the orders and sequences with the same initial state under an unvarying environment.

Fig. 12 is the combination of the data map and stability map. The blue box indicates the stable cells which coefficients in both HVLT and LVHT are larger than 0.8 or smaller than 0.2.

| Test | P value | Result |
|---|---|---|
| Monobit_test | P = 0.97507 | Pass |
| Frequency_within_block_test | P = 0.57569 | Pass |
| Runs_test | P = 0.63724 | Pass |
| Longest_run_ones_in_a_block _test | P = 0.45077 | Pass |
| Discrete_fourier_transform_test | P = 0.09625 | Pass |
| Non_overlapping_template_matching_test | P = 0.9995 | Pass |
| Approximate_entropy_test | P = 0.21925 | Pass |
| Cumulative_sums_test | P = 0.34796 | Pass |
| Random_excursion_test | P = 0.68475 | Pass |
| Random_excursion_variant_test | P = 0.17556 | Pass |
| Serial_test | P = 0.80882 | Pass |

Fig. 8. NIST test result.

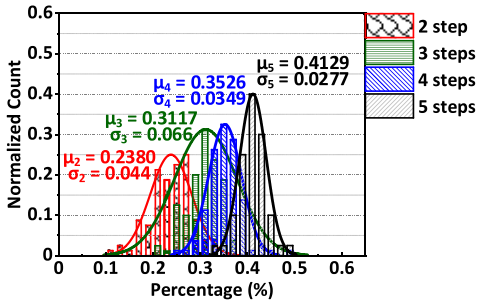



Fig. 9. Measured HD for sequence #1 with sequence length 2∼5.

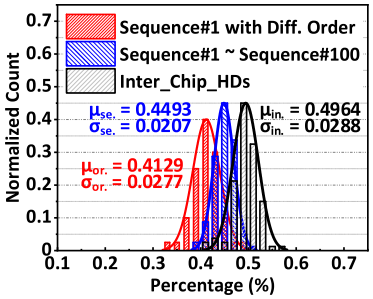



Fig. 10. Measured hamming distances.

The red box marks the unstable cells which should be filtered, the number of red boxes occupies 29.76% in the SPUF array. The black and white dots imply the data '0' and '1'. Every time we program the sequence or order of the PUF operation, the stability of each cell will also change. So each data map needs to match with one unique stability map.

Fig. 13 shows the BER with varying voltage and temperature. The green line is the BER of the original random data which is generated from instinct bias. The red line corresponds to the data after the sequence-dependent PUF operation. The BER is improved from the original 5.27% to 2.62% by overwriting the unstable cells. However, the worst BERs in the non-nominal condition is 8.41% (1V, 80°C) and 8.23% (0.7V, 20°C). The blue line is the BER after applying the bit selection algorithm, the minimum BER reduced to 0.8%, and the BER in the extreme condition (high temperature

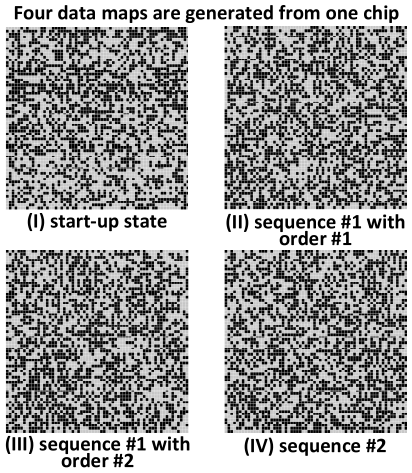



Fig. 11. Measured PUF data maps from one chip.

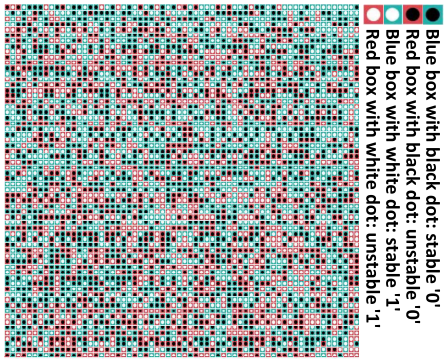



Fig. 12. Measured stability map associating with data map.

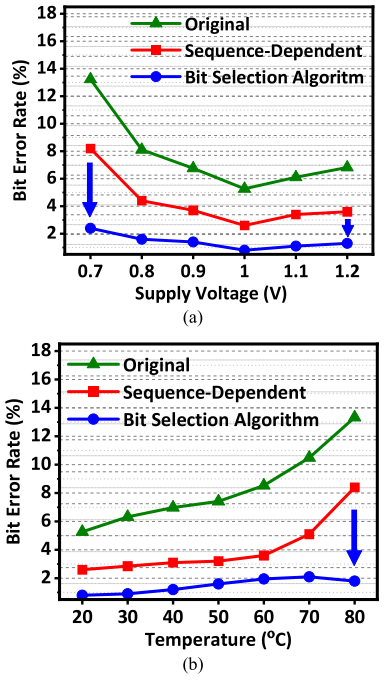



Fig. 13. Measured BER sweeping: (a) voltage and (b) temperature.

and high/low voltage) are improved to 1.8% (1V, 80°C) and 2.4% (0.7V, 20°C), which approximately 4 times compared to the data after the process of sequence programming.

Table I shows the comparison result with the state of the art. This brief achieves the lowest worst BER 0.8% between the SPUFs with multiple CRPs. The SPUF of [14] has a similar masking ratio and much smaller BER, but the CRP is 1. And it only can work as a PUF not memory. Reference [10] has the highest number of CRP, with lower BER and larger area.

## IV. Conclusion

This brief proposes an SRAM-based PUF (SPUF) with high reliability and multiple CRPs. The proposed sequence-dependent programming and the bit selection algorithm improves the reliability and randomness. The test chip fabricated in 40nm CMOS technology achieves the BER of 0.8% under 1 V and 20°C. The measured HD is 41.29% for one sequence with different orders and 44.93% for other sequences, and 49.64% between multiple chips. The proposed SPUF can be easily designed after modifying 6T SRAM and supports both PUF and SRAM modes without noticeable performance degradation.

## References

[1] L. Kusters, T. Ignatenko, F. M. J. Willems, R. Maes, E. van der Sluis, and G. Selimis, "Security of helper data schemes for SRAM-PUF in multiple enrollment scenarios," in *Proc. IEEE Int. Symp. Inf. Theory*, Aachen, Germany, 2017, pp. 1803–1807.

[2] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," IACR Cryptol. ePrint Archive, Lyon, France, Rep. 2011/657, 2011.

[3] P. Koeberl, J. Li, R. Maes, A. Rajan, C. Vishik, and M. Wójcik, "Evaluation of a PUF device authentication scheme on a discrete 0.13 $\mu$m SRAM," in *Proc. Int. Conf. Trust. Syst.*, 2011, pp. 271–288.

[4] S. Jeloka, K. Yang, M. Orshansky, D. Sylvester, and D. Blaauw, "A sequence dependent challenge-response PUF using 28nm SRAM 6T bit cell," in *Proc. IEEE, Symp. VLSI Circuits*, Kyoto, Japan, 2017, pp. 270–271.

[5] Y. Shifman, A. Miller, O. Keren, Y. Weizman, and J. Shor, "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. 120, pp. 4855–4868, Dec. 2020.

[6] A. Roelke and M. R. Stan, "Controlling the reliability of SRAM PUFs with directed NBTI aging and recovery," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 10, pp. 2016–2026, Oct. 2018.

[7] S. K. Mathew *et al.*, "A 0.19pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS," in *IEEE Int. Solid-State Circuits Conf. Dig. Tech. Papers (ISSCC)*, San Francisco, CA, USA, 2014, pp. 278–279.

[8] J. Li, T. Yang, and M. Seok, "A technique to transform 6T-SRAM arrays into robust analog PUF with minimal overhead," in *Proc. IEEE Int. Symp. Circuits Syst.*, Baltimore, MD, USA, 2017, pp. 1–4.

[9] A. Garg and T. T. Kim, "Design of SRAM PUF with improved uniformity and reliability utilizing device aging effect," in *Proc. IEEE Int. Symp. Circuits Syst.*, Melbourne, VIC, Australia, 2014, pp. 1941–1944.

[10] L. Lu and T. T.-H. Kim, "A sequence-dependent configurable PUF based on 6T SRAM for enhanced challenge response space," in *Proc. IEEE Int. Symp. Circuits Syst.*, Sapporo, Japan, 2019, pp. 1–4.

[11] C. Q. Liu, Y. Zheng, and C.-H. Chang, "A new write-contention based dual-port SRAM PUF with multiple response bits per cell," in *Proc. IEEE Int. Symp. Circuits Syst.*, Baltimore, MD, USA, 2017, pp. 1–4.

[12] K. Xiao, M. T. Rahman, D. Forte, Y. Huang, M. Su, and M. Tehranipoor, "Bit selection algorithm suitable for high-volume production of SRAM-PUF," in *Proc. IEEE Int. Symp. Hardw. Orient. Security Trust (HOST)*, Arlington, VA, USA, 2014, pp. 101–106.

[13] K. Liu, Y. Min, X. Yang, H. Sun, and H. Shinohara, "A 373-F2 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 J. Solid-State Circuits*, vol. 55, no. 6, pp. 1719–1732, Jun. 2020.

[14] Y. He, D. Li, Z. Yu, and K. Yang, "36.5 an automatic self-checking and healing physically unclonable function (PUF) with $<3\times10$-8 bit error rate," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, San Francisco, CA, USA, 2021, pp. 35–37.