A 6T SRAM Based Two-Dimensional Configurable Challenge-Response PUF for Portable Devices

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

***Abstract*— This work proposes a 2-dimensional programable SRAM-based PUF. The selection of challenge groups, orders, and sequence lengths dominates the responses with challenge-response pairs (CRPs) by order of rows$^{(\text{sequence length}-1)}$ × columns$^{(\text{sequence length}-1)}$. The PUF bit cell has split word-lines with vertical and horizontal connections, the bit-lines are placed orthogonally to generate one-bit data with four cells, the entropy source is enriched to 24 transistors. The proposed PUF supports multiple data maps from a single chip. A test chip was fabricated in 65 nm CMOS technology. Under 0.8V and 20 °C (nominal point), the bit error rate reaches 3%. In a single chip, the hamming distance achieves 42.49% within the same group and different orders of challenges, and 47.32% within the different groups of challenges (when the sequence length is 5). The measured inter-hamming distance between chips is improved to 49.47%.**

***Index Terms*— SRAM, PUF, sequence-dependent, two-dimension, challenge-response pairs, hardware security.**

I. Introduction

THE trend of implementing security in IoT systems has no consensus since the cyber defensive solutions are limited by physical constraints and different traits. Software security implementations are flexible and easy to maintain and update. However, it largely relies on the operating system of edge computers, which is easily deluded into grave decisions [1]. Although software implementation is cheaper, it is easy to be tampered with or attacked. As a consequence, cyber security is shifting from software methods to hardware methods. Because hardware security modules use complicated mathematical models to encipher, they become targets for rival companies and attackers [2]. Physically unclonable functions (PUFs) rely on the intrinsic difference and irreplicability of the security system to replace complex mathematic puzzles with hardware modules [3], [4]. A critical property of PUFs is a unique reproducible response, serving to produce and store a secret golden key for secure cryptography. Since it is difficult to forecast or identify intractable variations caused by the fabrication process, PUFs are engaging with security implements such as banking systems, critical infrastructure, etc. [5].

An ideal on-chip PUF needs to meet three major requirements: uniqueness, reliability, and randomness [6]. Uniqueness means that each PUF is unique. Even if PUFs are fabricated by the same process, they must differ from each other. Uniqueness is measured in hamming distance. Reliability implies that PUF can reproduce a key pattern, has tolerance to environmental noises and non-technology-related parameters, such as supply voltage, temperature, and device aging. Lastly, randomness requires PUF cells to be non-predictable. The deviation in the hardware manufacturing process determines the PUF data.

PUFs are categorized into strong and weak types. The strong PUF increases challenge-response pairs (CRPs) exponentially in the direct correlation with the number of basic blocks. It is usually employed with authentication protocols because the large CRP size is challenging to be evaluated in an operable period. However, the response could be affected by a random noise because of the complex combinations of the inherent mismatches. Weak PUFs have limited CRP spaces. The CRP size of weak PUFs grows polynomially with the number of basic blocks. In the worst case, the CRP could be only 1, which works as a chip ID. Since the weak PUF merely relies on the physical manufacturing process's inaccuracies, every individual device is uncorrelated. Because of this, it is generally used for golden key generation, which is challenging to be interfered with. SRAM-based PUF (SPUF), as one kind of weak PUF, uses a memory array on a chip to realize a PUF function. It is devoid of additional components to minimize the area overhead and save the effort for integration [7].

SRAM-based PUF generates random data using a start-up procedure. Fig. 1(a) shows a conventional 6T SPUF bit-cell structure and its voltage transfer curve. The solid line and the dashed line represent 'Q' in INV1 and 'QB' in INV2, respectively. When the power ramps up, the pull-up strength of two inverters determines the value at 'Q' and 'QB'. SPUF can work alternatively in the PUF mode and the memory mode. However, SPUF requires larger process variations to increase randomness. Depending on the mismatches between the cross-coupled inverters, SPUF cells are classified into three types: non-skewed, partially skewed, and fully skewed cells. For the start-up value (SUV), a non-skewed cell is easily affected by noise, while a fully skewed cell can reliably reproduce the code. Assuming that the SUV is affected only by the noise and mismatches between two inverters, the PUF's static noise margin (PSNM) [9] evaluates the impacts of mismatches on the SUV generation.

Manuscript received November 13, 2021; revised February 4, 2022; accepted March 2, 2022. Date of publication March 17, 2022; date of current version May 27, 2022. This article was recommended by Associate Editor R. Azarderakhsh. *(Corresponding author: Lu Lu.)*

Lu Lu is with the Institute of Microelectronics, Agency for Science, Technology and Research, Singapore 138634 (e-mail: lu_lu@ime.a-star.edu.sg).

Taegeun Yoo is with Samsung Electronics, Hwaseong 16677, South Korea (e-mail: ytgzero@nate.com).

Tony Tae-Hyoung Kim is with the Electrical and Electronic Engineering Department, Nanyang Technological University, Singapore 639798.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCSI.2022.3156983.

Digital Object Identifier 10.1109/TCSI.2022.3156983

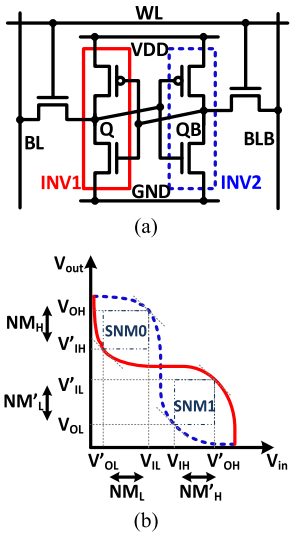

Fig. 1. Conventional PUF cells: (a) unit PUF cell and (b) voltage transfer curve of noise margin.

The largest squares inside the curves (SNM0 and SNM1) in Fig. 1(b) define the stability of the bit-cell in SRAM. SNM depicts the noise tolerance in the SRAM operation, the value is decided by the smaller number between SNM0 and SNM1. It restricts many key indexes such as min. operating voltage. Minimum values of SNM0 and SNM1 are as follows [9]:

$$SNM0 = min\left(NM_H = V_{OH} - V'_{IH}, NM_L = V_{IL} - V'_{OL}\right)$$
$$SNM1 = min\left(NM'_H = V'_{OH} - V_{IH}, NM'_L = V'_{IL} - V_{OL}\right) \quad (1)$$

V'_{xy} indicates the voltage of V_{in} in the critical points and V_{xy} points to V_{out}. The $PSNM_{ratio}$ is calculated as

$$PSNM_{ratio} = {}^{SNM0}/_{SNM1} \quad (2)$$

The $PSNM_{ratio}$ represents the reliability of SUVs. If the value is larger than 1, meaning the raw data has a higher chance to be 1. If the value is less than 1, the raw data tends to be 0. The conventional 6T SPUF uses the SUVs as the response. If the $PSNM_{ratio}$ is further away from 1, the cells are less stable in the SRAM mode while more reliable in the PUF mode. If the value of $PSNM_{ratio}$ is close to 1, the security code will be highly affected by the environmental noise. Low mismatch in SRAM mode and High mismatch in PUF mode are conflicting requirements between two coupled inverters.

The conventional SPUF has one response to a certain address challenge only. It becomes a target exploited using various attack techniques since all of the possibilities could be easily evaluated in a short time. To address these issues, we propose a novel SPUF structure. It uses conventional six transistors in each bit-cell to avoid significant performance degradation in SRAM operation. In addition, PUF data is generated by configurable multiple steps operations. If $PSNM_{ratio}$ is close to 1, other nearby skewed cells could help to improve the reliability of the non-skewed cells. Compared to the conventional chip ID, the proposed structure is a two-dimensional sequence-dependent SPUF cell, which expands the challenge-response space significantly [10]. Therefore, it becomes much more difficult to test all the combinations within a limited time.

The paper is organized as follows. Section II presents an overview of previous works. Section III explains the principle of the proposed PUF, followed by discussions on CRP space expansion in Section IV. Section V presents the measurement results of test chips in 65 nm CMOS to validate the proposed technique. The conclusion is drawn in Section VI.

II. Related Work

Current PUF designs implement several existing techniques, such as bias temperature instability (BTI), temporal majority voting (TMV), bit masking, oxide breakdown (BD), and others. Accelerating the aging of transistors using the NBTI effect improves reliability [11] and uniformity [12], which is a valid way to reduce the cost of error correction. However, the performance of the SRAM cell inevitably degrades due to the contraction of the drain to source current and the delay of propagation on the device. The work in [12] proposed a post-fabrication technique to modify the ratio of '0' and '1' in the power-up data. They have injected device aging to increase the mismatch between the cross-coupled inverters to improve the steadiness of code regeneration. However, this causes an over-stress on transistors, degrading their performance and lifetime. Error correction coding (ECC) and TMV are also utilized together with burn-in techniques to improve reliability [13]. However, the sizes of both ECC and TMV circuits are significant, increasing the area overheads. In [14], instead of the coupled inverters, they use the mismatch between the threshold voltages of the access transistors to generate highly reliable random data with conventional 6T SRAM. However, it needs native devices, and it is challenging to keep an analog voltage that is generated asynchronously. The SPUFs in [15]–[17] involve additional entropy sources from the manufacturing process variations to improve the uniqueness. In [15], they adopted a dual-port SRAM structure to engage more variations. by turning on both access transistors on each side, the conflicts are aggravated with 8 transistors. In [16] and [17], they connected two or three rows with complementary states to regenerate one-bit data. The entropy sources are enriched to 12 and 18 transistors respectively. Furthermore, these two SPUFs have a sequence-dependent response. The CRPs can be expanded by programming the selection of challenges. The final data is not only affected by the SRAM innate properties but also the groups and orders of the selection. The CRPs are enhanced from 'm' to '$\sim$ m^r' depending on the rows' combinations ('m' is the number of rows, and 'r' represents the sequence length). However, due to the one-directional selection, the improvement of CRPs in SPUFs [16] and [17] is still limited.

III. Proposed Sequence-Dependent PUF

SUVs as the final data in conventional SPUF that generated during power ramp-up are mainly steered by the discrepancy between two cross-coupled inverters.

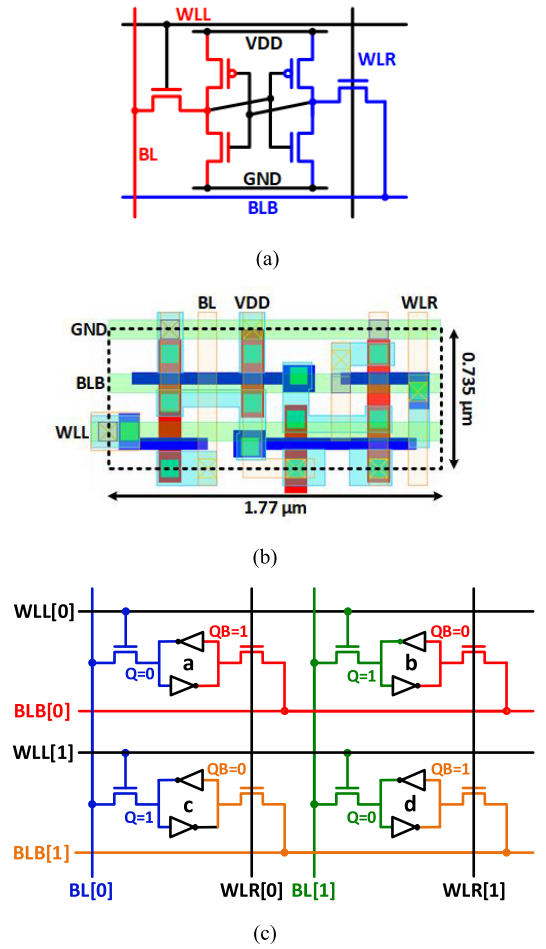

Fig. 2. Proposed SPUF unit: (a) schematic, (b) layout and (c) 2 × 2 array for on step PUF operation.

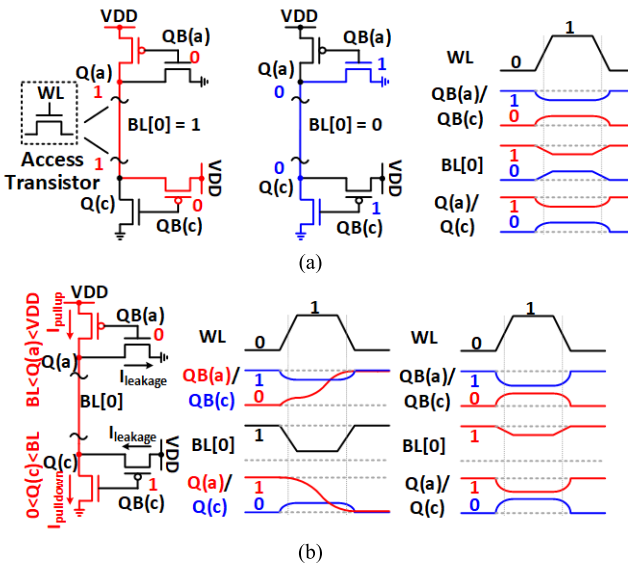

Fig. 3. Principle of the PUF mode operation.

Fig. 2 (a) shows the schematic of the proposed 6T SPUF bit-cell, it keeps the structure of 6 transistors from conventional 6T SRAM bit-cell with modified signal lines. The proposed SPUF bit-cell adopts two split word-lines (WLL and WLR) and two bit-lines (BL and BLB) running orthogonally, allowing multiple bit-cells to generate one-bit PUF data. Fig. 2(b) shows the bit-cell layout following the same arrangement as the conventional 6T SRAM layout for minimizing the mismatch caused by the layout drawing. The size of each bit-cell is $1.77\mu\text{m} \times 0.735\mu\text{m}$ when using a logic design rule. Fig. 2 (c) depicts a sample 2 × 2 array operation with complementary initial values in the PUF mode. To generate one-bit data, we turn on two vertical (WLR[0] and WLR[1]) and two horizontal (WLL[0] and WLL[1]) word-lines simultaneously. This connects 4 bit-cells through the orthogonal bit-lines (BL[0], BLB[0], BL[1], and BLB[1]). The voltage levels of BL[0], BL[1], BLB[0], and BLB[1] are determined by the data sets of {Q(a), Q(c)}, {Q(b), Q(d)}, {QB(a), QB(b)} and {QB(c), QB(d)}, respectively. If both QB(a) and QB(c) are '0' or '1' as depicted in Fig. 3(a), BL[0] will also be '1' or '0', and the data in QB(a) and QB(c) will not change. However, if QB(a) and QB(c) have opposite states, as shown in Fig. 3(b), the voltage level of BL[0] is decided by the strength of the pull-up and the pull-down transistors at Q(a) and Q(c). If the pull-down transistor is much stronger than the pull-up one, Q(a) will be overwritten. If the mismatch between Q(a) and Q(c) is insignificant, they will fight at BL[0] and return to their original states. Meaning, the value of Q(a) is affected by both QB(a) and Q(c), and the data in weak bit-cells can be overwritten by strong bit-cells.

To further enrich the entropy from the fabrication variations, the proposed SPUF connects any four SPUF bit-cells by enabling two pairs of orthogonal word-lines. The innate strengths in the involved 24 transistors contribute to the final random data, the interaction among the data stored in the selected four bit-cells can overwrite the bit-cells with smaller strength. Therefore, the significant enhancement of CRPs attributes to the substantially increased combinations of selecting in 2 dimensions.

The stability of each SPUF cell depends on the discrepancies of two cross-coupled inverters. A stronger bit-cell indicates a larger mismatch. According to the mismatch strengths, we can classify a SPUF bit-cell into four degrees. The STRONGEST bit-cell has substantial mismatches while the WEAKEST bit-cell includes only insignificant mismatches. When we connect four cells, it can create conflicts in the selected bit-lines. Strong adjacent bit-cells try to overwrite data into weaker bit-cells. In Fig. 4, the difference between the STRONGEST bit-cell and the WEAK bit-cell becomes dominant in the PUF data generation since it is larger than that between the STRONG bit-cell and the WEAK bit-cell (subordinate). Therefore, the data in the WEAK bit-cell will be overwritten by the data in the STRONGEST bit-cell. This operation is verified through Monte Carlo simulation using a 2 × 2 array.

In the PUF mode, we can use a single step or multiple steps to generate one-bit data, and each step chooses four orthogonal cells with complementary states. Multiple steps are repeated several times with random combinations which are interrelated to other steps, meaning at least one overlapped

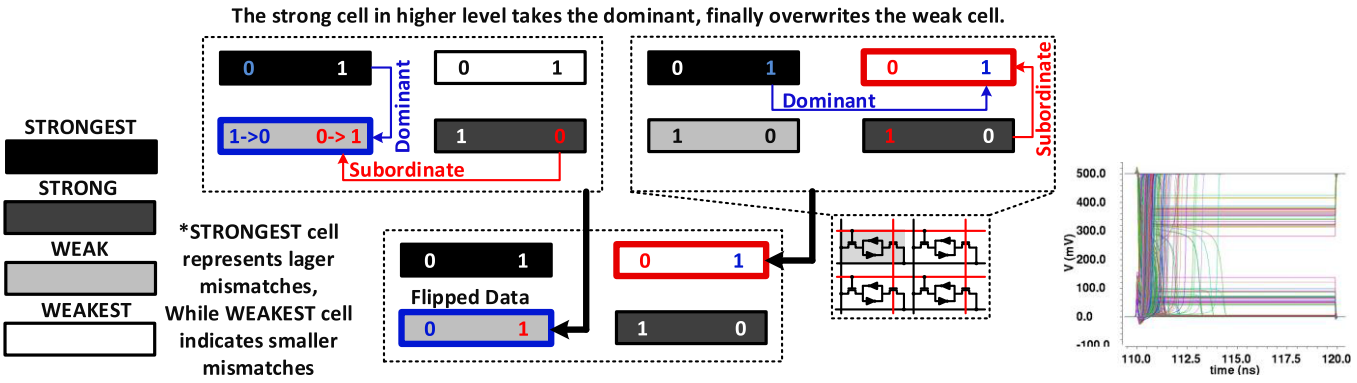

Fig. 4. Operation principle of the proposed SPUF data generation.

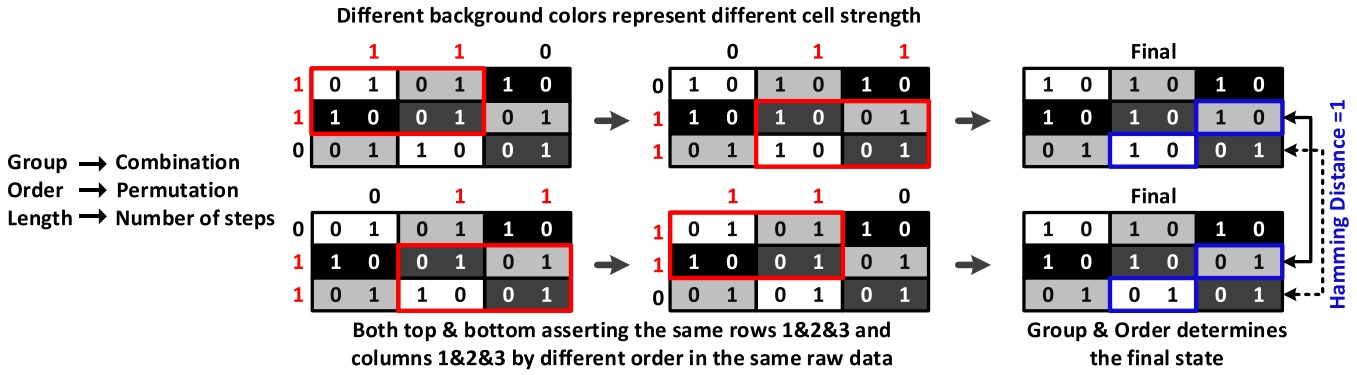

Fig. 5. Dependency of PUF operation on selection of groups and orders.

cell is necessary between two subsequent steps. Power-down is not required until one set of the secret key is obtained. We use group to represent the selected rows and columns (combination), and order to indicate which rows and columns are selected first (permutation). The sequence is the group with an order, and the length is the number of steps. As depicted in Fig.5, the first example asserting the top two rows and the left two columns simultaneously, followed by the bottom two rows and right two columns, written as the group & order of {(1, 2), (2, 3); (1, 2), (2, 3)}. Similarly, the bottom example can be written as {(2, 3), (1, 2); (2, 3), (1, 2)}. The cell strengths are represented by the different background color bits. Note that a group with different orders produces different final data even with the same election of rows and columns. In both the 2nd and 3rd rows of the final state, the hamming distances are equal to 1. Therefore, the selection of rows and columns, and the order of the selection affect the final PUF data. This allows one PUF chip to generate many PUF data maps, which makes the chip to be more resilient to attacks.

IV. The Enhancement of Challenge-Response Space

A. CRPs Enhancement in Two-Dimension Movement

The number of CRPs is limited in weak PUF, making brute-force attacking go through all the possibilities in a finite time. However, for larger CRPs, the attack algorithms need more effort to break the security. If the CRPs could increase

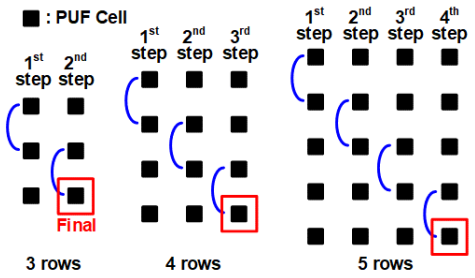

Fig. 6. Literature approach for increasing sequence lengths [16].

polynomially by the quantities of unit cells, the security would be improved significantly. So far, most of the SPUFs generate reliable chip ID by aging or utilizing the local transistor's characteristic, where CRP is 1. These types of SPUFs are easy targets of an attack.

The work in [16] proposed a sequence-dependent SPUF design, which connects two cells to generate new data. It uses multiple steps to generate one-bit data, which is group- and order-dependent. The CRPs are enhanced polynomially by the number of unit cells without changing the conventional 6T bit-cell structure. Fig. 6 illustrates the combinations of increasing sequence lengths in [16] (only one column is shown to clarify the analysis), steps indicate the number of times the process is repeated. For example, when 3 rows are used to

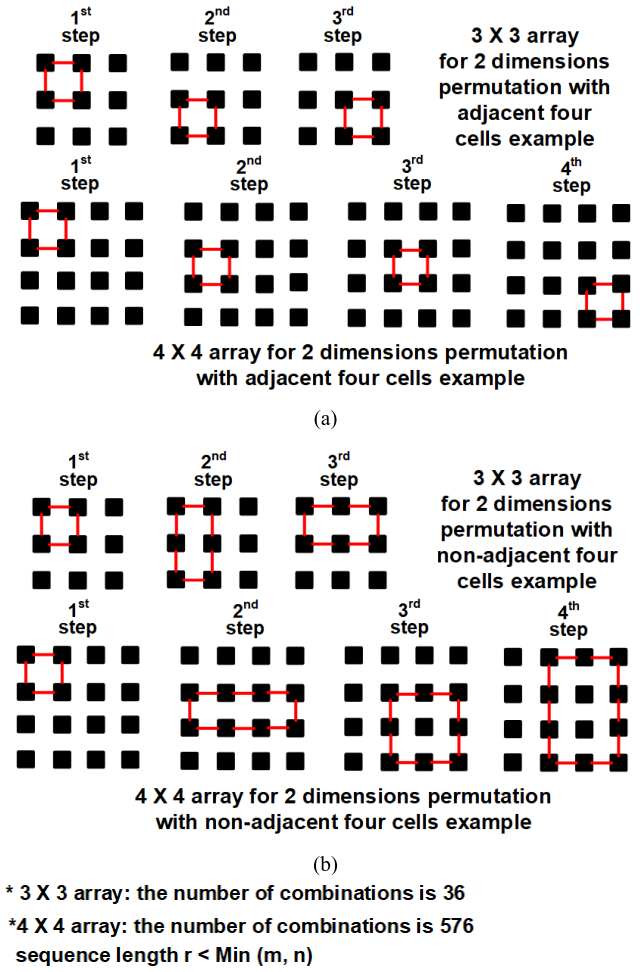

Fig. 7. Diverse selections of four cells in the proposed PUF operation. (a) with an adjacent four cells example and (b) with a non-adjacent four cells example.

generate random data, 2 steps are feasible. They have 3 choices in the first step and 2 choices in the second step, in total it is 6 permutations. Similarly, if 5 rows are used, 4 steps (Fig. 6(Right)) are considered, which produces 120 permutations. Even though the technique in [16] improves CRPs by utilizing the sequence programming, the employment of one dimension limits the number of permutations, which is addressed in this work.

As depicted in Fig. 2 (c), the proposed approach uses the selection in two dimensions for random data generation. For m rows $\times$ 1 column array with a sequence length of r, the sequence combination is the same as the movement in [16], which is analyzed above. The number of challenges to response pairs (CRPs) is written as follows:

$$m \times (m-1) \times \ldots \times (m-r) \tag{3}$$

In two dimensions movement, any two word-lines in each horizontal and vertical directions could be chosen. Fig. 7 depicts sample combinations of cell selection using 4 $\times$ 4 arrays, and we could choose 4 steps. Fig. 7 shows how the movement goes in two directions for four cells. It is possible to choose either adjacent or non-adjacent cells with any orientations, and the arrangement of selected cells in each step does not need to be consistent. The generated data in the final step is influenced by all movements, and it depends on both groups and orderings. Compared to [16], the proposed technique moves in two dimensions. This makes the number of permutations of formulas in (3) squared (assuming m = n). The number of CRPs of the proposed scheme can be estimated by the following expression:

$$[m \times (m-1) \times \ldots \times (m-r)] \times [n \times (n-1) \times \ldots \times (n-r)] \tag{4}$$

where m is the number of rows, n is the number of columns, and r is the sequence length. Note that r must be less than or equal to the lower one from m and n. ($r \leq \min(m,n)$)

B. Security Enhancement Analysis

In a security system, one of the most critical points of SPUF design is unpredictability. According to an arbitrary challenge, the generated responses must be unpredictable, so they could not be reproduced by the same CRPs from another PUF device or another CRPs from the same PUF device. It is challenging to quantify unpredictability. Usually, it is evaluated by measuring its uniqueness. For the proposed SPUF, multiple responses are generated from the same challenge to increase the CRPs. Each response should be distinguishable according to the programming groups or orders in a single instance, which makes the chip configurable. This uniqueness is estimated by the hamming distance of response bit from the different permutations or devices [18], which is shown as follows:

$$Uniqueness = \frac{2}{m \times (m-1)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} \frac{HD\left(R_i, R_j\right)}{l} \tag{5}$$

where m is the number of response bit strings, n is the length of the bit string. HD (R_i,R_j) is the hamming distance between the two-bit strings R_i and R_j. The response strings are from different permutations or devices, which indicates the diversity of the key data generated by various groups and orders.

For the proposed SPUF array, according to the different sequences of operations, the SPUF could generate multiple data maps in a single device. The uniqueness is proofed by the hamming distance from each sequence to guarantee that the key cannot be generated from other orders within the same group. It improves the security of the SPUF device significantly.

V. SRAM Function Analysis Result

The proposed SPUF works as a dual-mode device, which builds the PUF function on the existing hardware environment to minimize the area overhead and the effort of integration. It requires the SPUF to work in both modes without significant degradation in the performance. The proposed bit-cell structure only changes the route of connections without touching the placement of 6 transistors in the conventional SRAM. The unit cell is explained in section III.

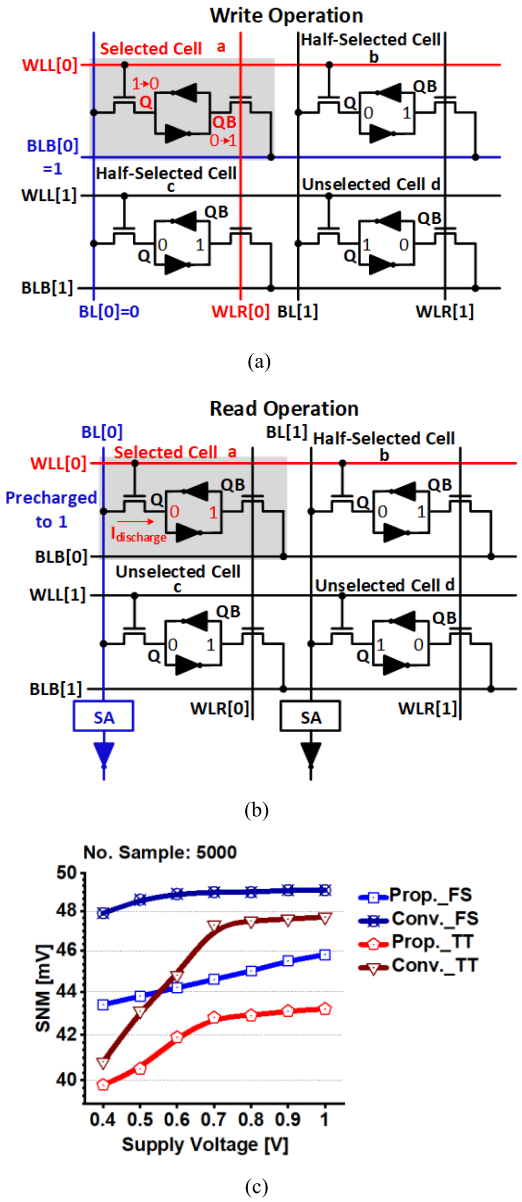

Fig. 8. Proposed SPUF cells in SRAM mode: (a) Write operation, (b) Read operation, and (c) read/write SNM comparison between proposed SPUF cell and conventional SRAM cell.

Fig. 8(a) displays the schematic of the write operation in SRAM mode. It starts asserting one horizontal word-line WLL [0] and one vertical word-line WLR [0] simultaneously to write data '0' into the selected cell a. The selected BL [0] and BLB [0] are loaded '0' and '1', respectively. The write ability is a copy of the conventional 6T SRAM for the selected cell. Due to the orthogonal arrangement for the word-lines, both selected row and column have half-selected cells (b and c). In the selected row, WLL [0] is set to VDD, and the unselected bit-line BL [1] is pre-charged to high potential. If the data stored in cell b is '0', the disturbing current will flow from BL [1] to Q, and no current flows through QB from BLB [1] because WLR [1] is GND. In the conventional half-selected cell, BLB is charging QB while Q is raised by the disturbing current since two access transistors are turned on. Therefore, the worst SNM for the proposed SPUF cell is 2.6 mV (TT corner) lower than the conventional SRAM cell (as shown in Fig. 8(c)). Since the SNM is critical in low voltage, under 0.4 V the difference is negligible (around 1 mV in TT corner) for a write operation. If the data stored in selected row cell b is '1', both pre-charged BL [1] and Q are high potential with no current flowing between them. For the half-selected cell c, the situation is opposite to cell b. If the data in cell c is '0', although WLR [0] is asserted, both QB and BLB [1] are '1'with no disturbing current. If cell c holds high potential, the disturbing current will drop in QB. It's a mirrored case of cell b with the same worst SNM.

Fig. 8(b) shows the schematic of the read operation. Because the bit-lines are not running parallel, a differential sensing amplifier is not eligible in this case. So that, only WLL [0] is asserted during the read operation to discharge the BL [0]. For the half-selected cell, cell b suffers from the read disturbing current from BL [1], while the read SNM is the same as writing one as shown in Fig. 8(c). It shows the proposed structure can work reliably in the promised voltage range as SRAM-mode.

Fig. 9 shows the architecture of the proposed 4k SPUF. To support the proposed configuring ability, the SRAM has a decoder and a write circuit for both rows and columns. Transmission gate flip flop is used to select multiple word-lines at the same time. A single-ended sensing amplifier is required to detect the value of BLs, placed at the bottom of the macro. The proposed SPUF could switch between PUF mode and SRAM mode without degrading the performance. In comparison with a conventional SPUF, the power consumption of the proposed SPUF is 3.7% more in each single step. The area overhead caused by the dual dimension WL/BL is 4.47%, and the latches consume 8.1% extra area for the address signals.

VI. Measurement Results and Discussion

A 4kb (64 × 64) SRAM PUF array test chip is fabricated in 65nm CMOS technology. The die photo is shown in Fig. 10. The total area is 170 × 74 μm^2, and the size is 1.3 μm^2 per bit cell. The throughput of the PUF operation is 4 Gbps with a sequence length is 5.

A. Reliability

For the academic community in PUFs designs, it is necessary to consider reliability as a critical requirement. The proposed SPUF should be reliable to reproduce the response by the same challenge many times, which has different tolerance in the different operating environments. Generally, the SPUF should work well in a wide range of voltage and temperature setups.

First, we tested the reliability of output using various voltage values, which were measured using the bit error rate (BER). We swept the supply voltage from 0.5 V to 1 V at a nominal temperature of 27°C. As shown in Fig. 11(a), the measured BER is 3% at 0.8 V with 9% at 0.5 V.

Second, we evaluated the reliability of the SPUF output for temperature variations by sweeping the temperature from

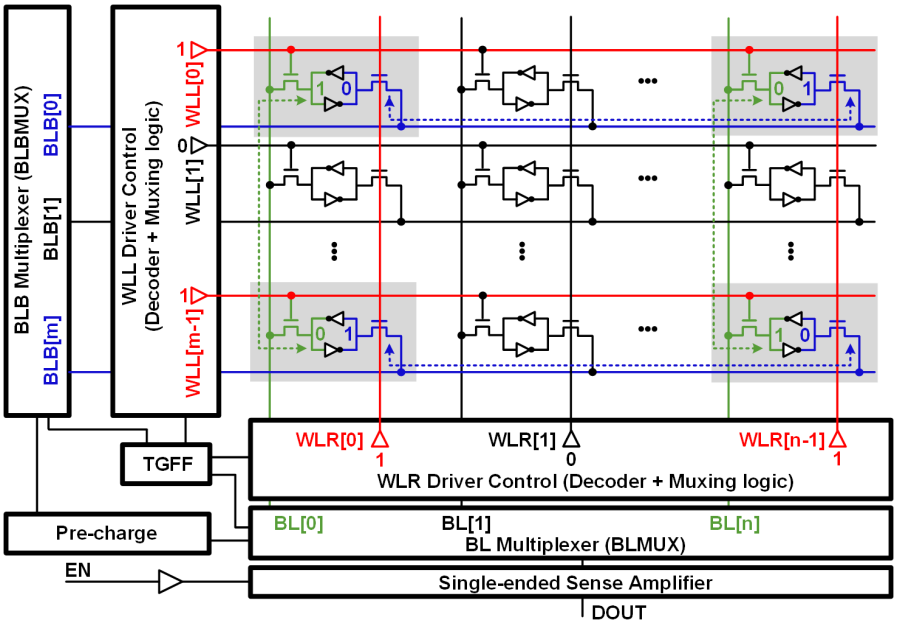

Fig. 9. Architecture of the proposed SPUF.

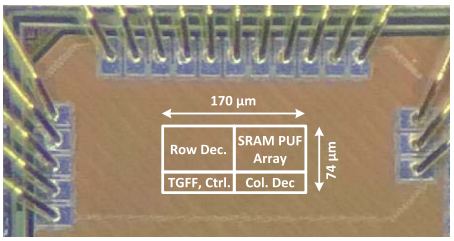

Fig. 10. Proposed SPUF die photo.

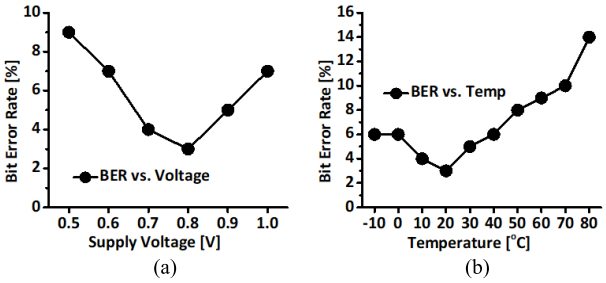

Fig. 11. Measured BER: (a) varying voltage and (b) varying temperature.

−10°C to 80°C under the supply voltage of 0.8 V. Fig. 11(b) shows the measured BER over temperature. The BER is 3% at 20° C, and the worst BER is 14% at 80° C.

At the nominal operation with 0.8 V and 20° C, the golden data demonstrates the BER of 3%. When considering temperature and voltage variations, the BER can be further improved by utilizing the bit selection algorithm [17], the temporal majority voting [13], and the masking techniques [19].

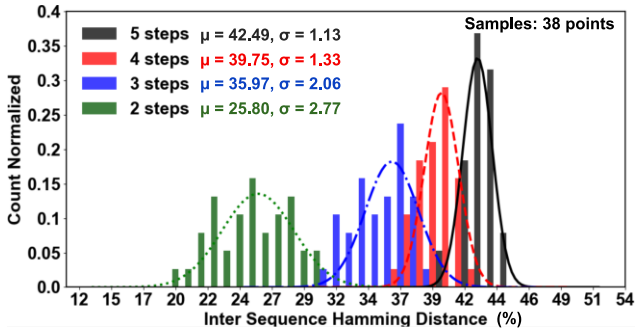

Fig. 12. Measured HD for Group #1 with Order #1 ∼ Order #38.

B. Uniqueness

Conventional SPUFs are weak PUFs, and as such their CRPs are limited. However, the proposed SPUF determines the data map using group, order, and length. Using a challenge (address), the proposed SPUF can generate multiple responses (data maps). For example, the CRPs could be as large as 8.37×10^{17} when using a 64 × 64 array and a sequence length of 5. Fig. 12 and 13 show the inter-sequence hamming distance and the inter-chip hamming distance to demonstrate that the responses obtained from the same challenge are distinguishable.

We have adopted 38 group combinations to implement in each device and labeled them as Group #1∼ #38. For each group, we also named the different orders as Order #1 ∼ #38. Fig. 12 exhibits the hamming distance of Group #1 with different orders and different lengths. Under the same temperature and voltage conditions (20° C, 0.5 V), using the same chip and Group #1, we only changed the order of Group #1 to evaluate hamming distances with a different number of steps (sequence length). The overall hamming distance is improved by increasing the sequence length. With two steps,

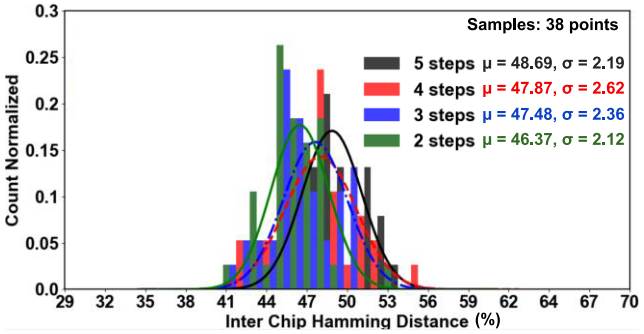

Fig. 13. Measured HD for Group #1 with Order #1 from different chips.

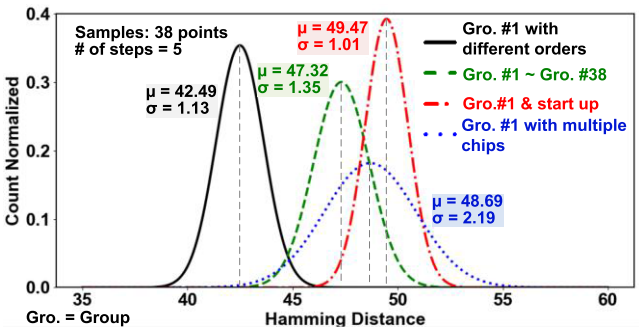

Fig. 15. Measured hamming distances.

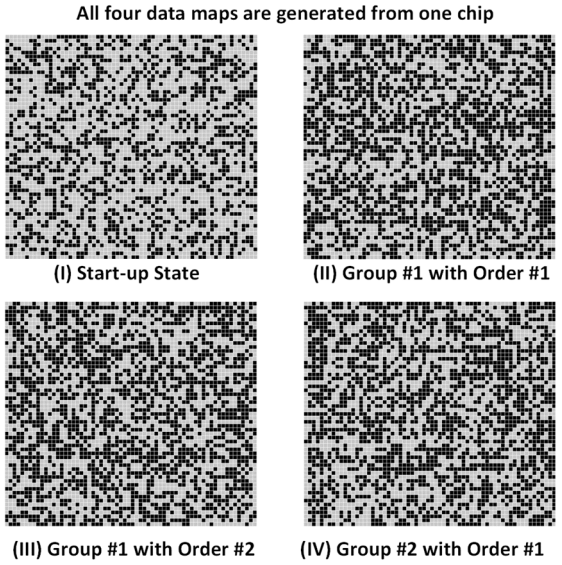

Fig. 14. Measured PUF data maps from one chip.

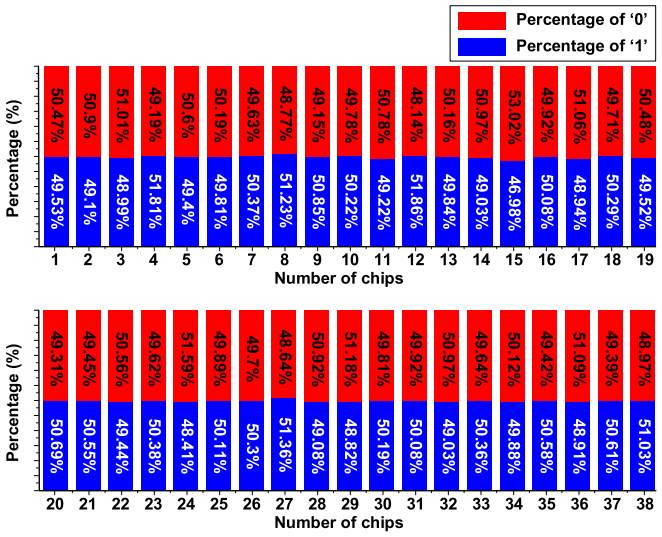

Fig. 16. Percentage of '0'&'1' of Group #1∼ Group #38 in normal condition in one test chip which raw data has 62.45% percentage of '0.'

the measured hamming distance is 25.62% with $\sigma = 2.77$. It is improved to 42.49% with $\sigma = 1.13$ when the sequence length becomes 5. This demonstrates that we can obtain multiple data maps using different orders within the same programming group and the hamming distance is improved by increasing the sequence length. Note that the sequence length is restrained by the distribution of the data. If we increase the sequence length by more than 5 steps, the randomness will start to degrade.

Fig. 13 presents the hamming distances for multiple chips with the same Group #1 Order #1. We used the same group and the order pattern in the tested chips with different sequence lengths under the same environment. The inter-chip hamming distance is 46∼49% due to the biased original start-up data (47.41%). The average hamming distance from the measurement is 48.69%.

Fig. 14 shows four data maps generated from a single chip under the same environment. Fig. 14(I) illustrates the start-up pattern. This data map could be seen as a chip ID since it depends on the unique PVT variations. The dark color represents data '1' while the grey color represents data '0'. Fig. 14(II) depicts the data map after employing the 5-step PUF operation for Group #1 and Order #1. The hamming distance between (I) and (II) is 0.501. Then we start from start-up status again using the same Group #1 but Order #2 (sequence length = 5) to generate a new data map whose pattern is shown in Fig. 14(III). The average hamming distance between (II) and (III) is 0.425. Fig.14(IV) presents the start-up data using Group #2 and Order #1 (sequence length = 5) from the same chip. The average inter-sequence hamming distance between (II) and (IV) is 0.473.

In Fig. 15, the black line (solid) exhibits the hamming distance between different situations using 5 steps as the sequence length. Group #1 with different orders is also shown in Fig. 12 where the value is 42.49%. The green line (dashed) indicates the hamming distance between Groups (Group #1 ∼ Group #38) in a single chip. The mean value is 47.32%. The blue line (dotted) is the hamming distance between the start-up value and the data maps generated by Group #1 by varying the order. Here, we obtained a hamming distance of 48.69%. The red line (dash-dotted) represents the hamming distance for the same group and the order using different chips, which is 49.47%.

C. Randomness

During the start-up, the generated raw data is decided by the mismatches between 6 transistors for each one-bit cell.

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

		This work	*2017 VLSI [16]*	*2021 TCASII [17]*	*2020 CICC [20]*	*2020 TCASI [21]*	*2020 VLSI [22]*
Technology		65nm CMOS	28nm FDSOI	40nm CMOS	130nm CMOS	130nm CMOS	14nm CMOS
Area/PUF bits		5.2 μm^2 (4 cells)	388-970 F^2 (2-5 cells)	987 F^2 (3 cells)	497F^2	—	—
Energy efficiency (fJ/b)		81 (seq-5, 0.5 V)	97 (seq-5, 0.7 V)	127 (seq-5, 1 V)	15.4 (0.6V)	11	97
Inter-PUF HD		0.4947	0.481 - 0.495	0.4964	0.49	0.499	0.498
Native BER (%)		3 (0.8V, 20℃)	3.17 (0.7V, 27℃)	0.8 (1V, 20℃)	0.29	9	<0.26
# Possible CRPs		8.37×10^{17} (seq-5)	1.17×10^{11} (seq-5)	4.01×10^{15} (seq-5)	1	3.7×10^{19}	3×10^{28}
Tested Condition	Voltage (V)	0.5 - 1	0.5 – 0.9	0.7 – 1.2	0.8 – 1.2	1.08-1.32	0.65 – 0.85
	Temp (℃)	-10 - 80	0 - 80	20 - 80	-20 - 85	-20 - 80	0 - 100
Weak/Strong PUF		Weak	Weak	Weak	Weak	Strong	Strong
PUF Type		SRAM-PUF	SRAM-PUF	SRAM-PUF	SRAM	SCA-PUF	Coupled Inverter

Test	Result
Monobit_test Ones count = 2031, Zeroes count = 2065 P = 0.57348	Pass
Frequency_within_block_test n = 4096, N = 99, M = 36 P = 0.09958	Pass
Runs_test prop 0.48136, tau 0.03311, vobs 1816.0 P = 0.85620	Pass
Longest_run_ones_in_a_block_test n = 4096, K = 3, M = 8, N = 16, chi_sq = 3.5854 P = 0.30985	Pass
Discrete_fourier_transform_test N0 = 1732.80, N1 = 1728.00 P = 0.46583	Pass
Non_overlapping_template_matching_test P = 0.99585	Pass
Random_excursion_test P = 0.23396 ~ 0.74216	Pass
Random_excursion_variant_test P = 0.23836 ~ 0.84611	Pass
Approximate_entropy_test n = 4096, m = 3, AppEn = 0.665, chi_sq = 5.551 P = 0.23237	Pass
Cumulative_sums_test P = 0.12737	Pass
Serial_test P1 = 0.33665 P2 = 0.58948	Pass

Fig. 17. NIST test result.

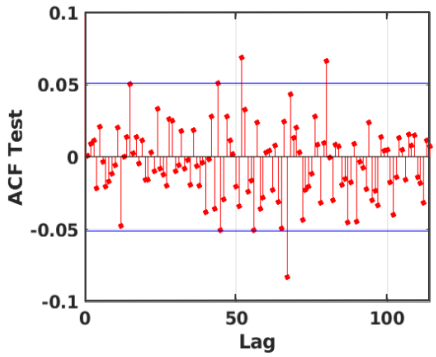

Fig. 18. Measured autocorrelation.

The generated data is affected by 24 transistors (4 cells) in a single program step, increasing the entropy with fabrication variations. After the PUF operation for Group #1 with sequence length 5, the percentage of '0' in the test chip is improved to 50.47%. Fig.16 shows the distribution of '0' and '1' for Group #1 to Group #38. The overall average percentage of '0' is 50.11%, the maximum deviation from 50% in the 38 configurations is 3.02%. Note that based on our experiments, to generate valid random data, the percentage of '0'/'1' should be less than 64% when the supply voltage ramps up, otherwise the final data will be too clustered.

Fig.17 shows the result of the NIST SP800-22 test, which is statistical testing widely employed to evaluate the randomness of data generated by random number generators or pseudo-random number generators. To pass the test, P-value should be larger than 0.01. The proposed SPUF passed 11 out of 15 NIST tests. Due to the limited size of the array of 4k bits, the proposed SPUF failed in linear complexity test, binary matrix rank test, overlapping template matching test, and maurers universal test. As a small size weak PUF, the NIST test demonstrates that the SPUF has good randomness for the data maps in one chip.

Fig. 18 shows the autocorrelation function (ACF) test result. 95% of the generated random data fluctuate within the range of 0.05. Thus, showing the data has good randomness.

In the PUF operation, we could use different sequence lengths to generate a data map. The power consumption increases linearly with the sequence length. As shown in Fig. 19, if sequence length is 2, the power consumption is

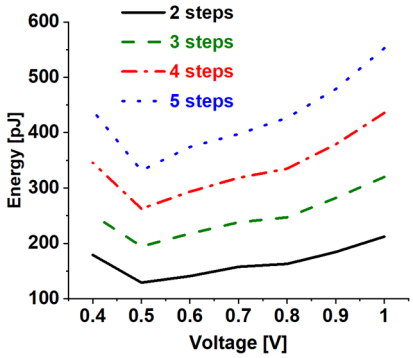

Fig. 19. Measured energy consumption.

minimal,73 pJ at 0.5 V. The consumption using the same voltage climbs to 186 pJ, 263 pJ, and 331 pJ for sequence lengths of 3, 4, and 5 respectively. In addition, when the sequence length is 5, the minimal power consumption per bit is 81 fJ at 0.5 V.

Table I compares the previous works with the proposed SPUF. The area to generate one-bit is around 5.2 μ m^2 to 14.6 μ m^2 (4∼10 cells will be used). However, these 4 to 10 cells could be re-utilized to generate other bits with a different combination. For a sequence length of 5, the energy consumption is 331 pJ at 0.5 V, and the minimum bit error rate is lower than [17] (since [17] contains data masks that blocked around 30% capacity). It achieves the highest CRPs in the weak PUF with functional dual-mode operations. This work provides the largest CRPs in the weak PUF type by applying the 2D sequence-dependent programming. However, it is noteworthy that the actual number of CRPs can be affected if the proposed PUFs are attacked by techniques such as machine learning.

VII. Conclusion

In this paper, we presented a 2D sequence-dependent PUF, which expands the CRPs by the orders of rows$^{(\text{sequence length}-1)}$ × columns$^{(\text{sequence length}-1)}$. Based on the conventional SRAM bit cell, we split the word-lines to orthogonal placement, to allocate four cells with mutual effects to generate a final random data. Using various sequence lengths, groups, and orders, we can produce multiple data maps using a single chip for privacy and security purpose. The chip is fabricated in 65 nm CMOS technology with an overall area of 12580 μ m^2 and bit cell of 1.3 μ m^2. When the sequence length is 5, the minimum energy consumption is 81 fJ/bit under 0.5 V and the bit error rate is 3% at the nominal point (0.8 V/20° C). In a single chip, using the same sequence group with different orders, the measured hamming distance is 42.49%. With different sequence groups, the hamming distance achieves 47.32%, and the average randomness is 50.11%. The inter-hamming distance between chips is 49.47%. In the promised voltage and temperature range, this PUF performs as expected. The proposed SPUF with enhanced CRPs can be easily altered from the conventional SRAM, works in dual-mode in the modern security system.

References

[1] C.-H. Chang, Y. Zheng, and L. Zhang, "A retrospective and a look forward: Fifteen years of physical unclonable function advancement," *IEEE Circuits Syst. Mag.*, vol. 17, no. 3, pp. 32–62, Aug. 2017.

[2] S. P. Skorobogatov. (Aug. 2011). Illegitimi non Carborundum Santa Barbara, CA. USA. *Invited Keynote Talk Given at CRYPTO*. [Online]. Available: http://people.csail.mit.edu/rivest/2011-08-15-rivest-CRYPTO-keynote.pdf

[3] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS)*, Washington, DC, USA, 2002, pp. 148–160.

[4] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, Sep. 2002.

[5] 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 (ISIT)*, Jun. 2017, pp. 1803–1807.

[6] A. Maiti *et al.*, "A systematic method to evaluate and compare the performance of physical unclonable functions," in *Embedded Systems Design With FPGAs*. 2012, pp. 245–267.

[7] P. Koeberl *et al.*, "Evaluation of a PUF device authentication scheme on a discrete 0.13 μm SRAM," in *Proc. Int. Conf. Trusted Syst.* Berlin, Germany: Springer, 2011, pp. 271–288.

[8] L. Zhang, C.-H. Chang, Z. H. Kong, and C. Q. Liu, "Statistical analysis and design of 6T SRAM cell for physical unclonable function with dual application modes," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2015, pp. 1410–1413.

[9] M. Cortez *et al.*, "Modeling SRAM start-up behavior for physical unclonable functions," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFT)*, Oct. 2012, pp. 1–6.

[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. (ISCAS)*, May 2019, pp. 1–4.

[11] 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, Nov. 2018.

[12] A. Garg *et al.*, "Design of SRAM PUF with improved uniformity and reliability utilizing device aging effect," in *Proc. IEEE Intl. Symp. Circuits Syst.*, Jun. 2014, pp. 1941–1944.

[13] 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 ISSCC Dig. Tech. Papers*, Feb. 2014, pp. 278–279.

[14] 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. (ISCAS)*, May 2017, pp. 1–4.

[15] 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. (ISCAS)*, May 2017, pp. 1–4.

[16] S. Jeloka, K. Yang, M. Orshansky, D. Sylvester, and D. Blaauw, "A sequence dependent challenge-response PUF using 28 nm SRAM 6T bit cell," in *Proc. Symp. VLSI Circuits*, Jun. 2017, pp. C270–C271.

[17] L. Lu *et al.*, "A high reliable SRAM-based PUF with enhanced challenge-response space," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 2, pp. 1–5, Feb. 2021.

[18] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of RO-PUF," in *Proc. IEEE Int. Symp. Hardware-Oriented Secur. Trust (HOST)*, Jun. 2010, pp. 94–99.

[19] Y. He, D. Li, Z. Yu, and K. Yang, "36.5 an automatic self-checking and healing physically unclonable function (PUF) with <3×10-8 bit error rate," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 2021, pp. 35–37.

[20] K. Liu, H. Pu, and H. Shinohara, "A 0.5-V 2.07-fJ/b 497-F2 EE/CMOS hybrid SRAM physically unclonable function with < 1E-7 bit error rate achieved through hot carrier injection burn-in," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, Mar. 2020, pp. 1–4.

[21] H. Zhuang, X. Xi, N. Sun, and M. Orshansky, "A strong subthreshold current array PUF resilient to machine learning attacks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 1, pp. 135–144, Jan. 2020.

[22] V. Suresh, R. Kumar, M. Anders, H. Kaul, V. De, and S. Mathew, "A 0.26% BER, 1028 challenge-response machine-learning resistant strong-PUF in 14 nm CMOS featuring stability-aware adversarial challenge selection," in *Proc. IEEE Symp. VLSI Circuits*, Jun. 2020, pp. 1–2.

Lu Lu (Member, IEEE) received the B.E. degree in communication engineering from the Hefei University of Technology in 2007, the M.E. degree in microelectronics from Xiamen University, Xiamen, China, in 2010, and the Ph.D. degree in electrical and electronic engineering from Nanyang Technological University, Singapore, in 2019. From 2019 to 2021, she was with NTU as a Research Fellow. In 2021, she joined A∗Star, Singapore, as a Research Scientist. Her research interests include low power SRAM, hardware security, and RRAM design. She was a recipient of the IEEE SSCS Singapore Chapter Award in 2018.

Taegeun Yoo (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical and electronics engineering from Chung-Ang University, Seoul, South Korea, in 2009, 2011, and 2015, respectively.

From 2015 to 2016, he was with Chung-Ang University as a Research Professor. From 2016 to 2019, he was with Nanyang Technological University, Singapore, where he was a Senior Research Fellow and worked on the research of ultra-low-power image sensors and emerging memory architectures. He joined Samsung Electronics, Hwaseong, South Korea, in 2019, as a Staff Engineer. His research interests include analog mixed-signal ICs and low-power memory architecture.

Dr. Yoo has received an Encouragement Award and the Silver Award at the Human-Tech Paper Award hosted by Samsung Electronics in 2011 and 2014, respectively. He has also received the Silkroad Award at the IEEE International Solid State Circuits Conference (ISSCC) in 2014.

Tony Tae-Hyoung Kim (Senior Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Korea University, Seoul, South Korea, in 1999 and 2001, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Minnesota, Minneapolis, MN, USA, in 2009.

From 2001 to 2005, he was with Samsung Electronics, Hwasung, South Korea, where he performed research on the design of high-speed SRAM memories, clock generators, and IO interface circuits. From 2007 to 2009, he was with the IBM T. J. Watson Research Center, Yorktown Heights, NY, USA; and Broadcom Corporation, Edina, MN, USA, where he performed research on circuit reliability, low-power SRAM, and battery-backed memory design. In 2009, he joined Nanyang Technological University, Singapore, where he is currently an Associate Professor. He has authored/coauthored over 160 journals and conference papers and holds 17 U.S. and Korean patents registered. His current research interests include low-power and high-performance digital, mixed-mode, and memory circuit design, ultralow-voltage circuits and systems design, variation and aging-tolerant circuits and systems, and circuit techniques for 3-D ICs.

Dr. Kim has served on numerous conferences as a committee member. He has received the Best Paper Award (Gold Prize) at ICCE-Asia 2021; the Best Demo Award at APCCAS 2016; the Low Power Design Contest Award at ISLPED 2016; the Best Paper Awards at 2014 and 2011 ISOCC; the AMD/CICC Student Scholarship Award at the IEEE CICC 2008; the Departmental Research Fellowship from the University of Minnesota in 2008; the DAC/ISSCC Student Design Contest Award in 2008; the Samsung Humantec Thesis Award in 2008, 2001, and 1999; and the *ETRI Journal* Paper of the Year Award in 2005. He was the Chair of the IEEE Solid-State Circuits Society Singapore Chapter. He serves as an Associate Editor for the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, IEEE ACCESS, and the *IEIE Journal of Semiconductor Technology and Science*.