A Sequence-Dependent Configurable PUF Based on 6T SRAM for Enhanced Challenge Response Space

Lu Lu and Tony Tae-Hyoung Kim
School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore
Email: LLU010@e.ntu.edu.sg

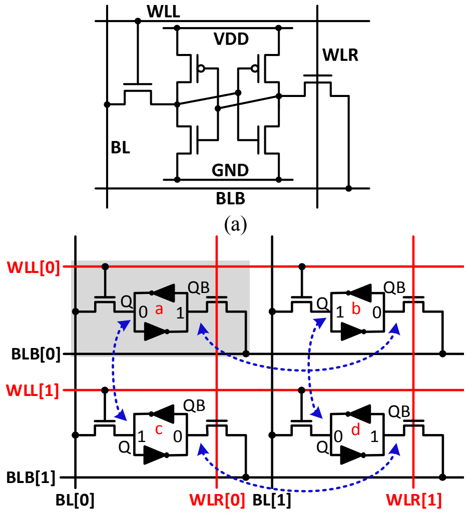
***Abstract*—This work proposes a 2D sequence-dependent PUF based on SRAM. It expands challenge to response pairs (CRPs) by the order of rows$^{(\text{sequence length - 1})}$ × columns$^{(\text{sequence length - 1})}$ for reliable authentication. This is achieved by configuring the sequence of SRAM cell selection. Each bit cell has a vertical word-line and a horizontal word-line to utilize the orthogonal word-lines to connect four cells simultaneously to generate one bit data. The proposed technique allows us to generate multiple data maps from one chip. This non-linear behavior also makes the chip more secure. A test chip was fabricated in 65 nm CMOS technology with the area of area is 12580 µm^2. The bit error rate is 3% at the nominal point (0.8 V/20℃) and the inter-hamming distance between chips is 0.497. The hamming distance of 0.427 was measured when using the same sequence length with different orders.**

Keywords—SRAM, PUF, sequence length, permutation, hardware security.

I. Introduction

Physically unclonable function (PUF) serves to generate and store a secret key for a semiconductor device. The key property of PUF is unique reproducible response, which makes it difficult to predict or characterize uncontrollable variations from manufacturing. Therefore, PUFs are attractive for security applications such as banking infrastructure, critical communication links, etc [1]. Compared with other existing PUF devices, SRAM based PUFs can be implemented without additional components for generating response. SRAM based PUFs (SPUFs) operate as weak PUFs. They generate data based upon the physical mismatches produced during fabrication.

An ideal on-chip PUF needs to meet three factors: uniqueness, reliability, and uniformity [2]. A challenge of PUF design is keeping the unique secure interactions between devices and maintaining the steadiness to regenerate the code at the same time. Typically, error correction code (ECC), temporal majority voting (TMV) and directed aging have been utilized to improve the reliability [3]. However, both ECC and TMV need additional circuits, which increases silicon area. Directed aging is an effective way to reduce the cost of error correction. Here, selected devices are subject to temperature and voltage stress to accelerate transistor aging. However, the aged devices degrade the SRAM performance and the lifetime. In [4], they use a native device to sense the threshold voltage difference between two access transistors in conventional 6T SRAM cells to generate highly reliable PUF. However, it is challenging to keep an analog voltage and compare with a slight difference that is generated asynchronously. The SPUFs in [5],[6] generate more variations in addition to the mismatches coming from fabrication process so that the added variations improve the uniqueness. In [5], they adopted the dual port SRAM structure to aggravate the conflicts during the data generating. In [6], they connect two cells to regenerate one bit data. This involves 12 transistors and increases the randomness compared with 8 transistors in [5]. Furthermore, the PUF in [6] introduces a sequence dependent response to make the PUF data programmable. The data is not only affected by initial intrinsic mismatches, but also the sequence length and the order. However, the PUF in [6] only changes the sequence of selected rows, which provides limited improvement.



(a)

(b)

Fig. 1. Proposed PUF cells: (a) unit PUF cell and (b) 2×2 array for on bit PUF data generation.

This work proposes a two dimensional sequence dependent SRAM-based PUF. The proposed novel PUF cell structure with full SRAM functions generate multiple reliable PUF data sets and expand the challenge response space by the order of rows$^{(\text{sequence length - 1})}$ × columns$^{(\text{sequence length - 1})}$.

II. Proposed Sequence-Dependent PUF

Conventional PUFs are based on start-up values during power-up reset and they are mainly determined by the mismatches between two cross-coupled inverters. Since each address accords to one value, the challenge and response space is equal to the number of bits in the memory.

Fig.1 (a) shows the proposed 6T SRAM PUF cell, consisting of two symmetrical cross-coupled inverters and two access transistors. The proposed PUF cell includes two word-lines (WLL and WLR) running orthogonally as shown in Fig. 1(a). The bit-lines (BL and BLB) are also routed orthogonally with the corresponding word-lines. During the PUF mode, we turn on two vertical and two horizontal word-lines together to generate one bit data using 4 cells. Fig. 1(b) shows a sample 2×2 PUF array with complementary initial values. In the PUF mode, the word-lines, WLL [0], WLL [1],

978-1-7281-0397-6/19/$31.00 ©2019 IEEE

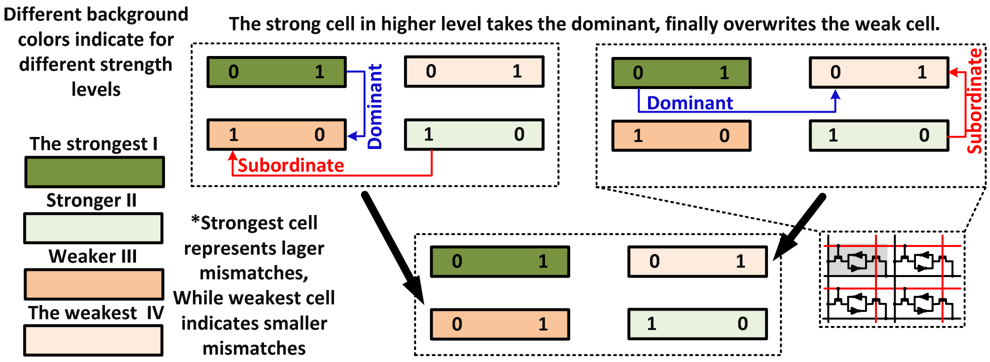

Different background colors indicate for different strength levels
The strongest I
Stronger II
Weaker III
The weakest IV
The strong cell in higher level takes the dominant, finally overwrites the weak cell.
0 1
1 0
Dominant
Subordinate
*Strongest cell represents lager mismatches, While weakest cell indicates smaller mismatches

Fig. 2. Operation principle of the proposed PUF data generation.

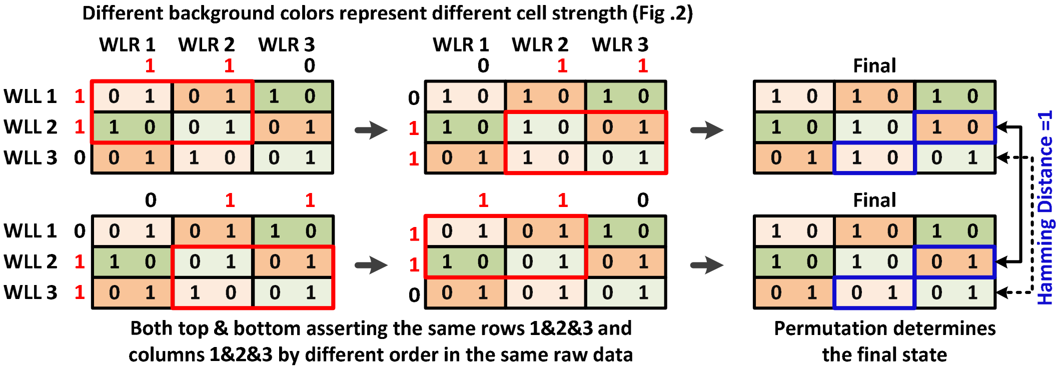

Different background colors represent different cell strength (Fig .2)
WLR 1 WLR 2 WLR 3
1 1 0
WLL 1 1 | 0 1 | 0 1 | 1 0
WLL 2 1 | 1 0 | 0 1 | 0 1
WLL 3 0 | 0 1 | 1 0 | 0 1
WLR 1 WLR 2 WLR 3
0 1 1
0 | 1 0 | 1 0 | 1 0
1 | 1 0 | 1 0 | 0 1
1 | 0 1 | 1 0 | 0 1
Final
1 0 | 1 0 | 1 0
1 0 | 1 0 | 1 0
0 1 | 1 0 | 0 1
0 1 1
WLL 1 0 | 0 1 | 0 1 | 1 0
WLL 2 1 | 1 0 | 0 1 | 0 1
WLL 3 1 | 0 1 | 1 0 | 0 1
1 1 0
1 | 0 1 | 0 1 | 1 0
1 | 1 0 | 0 1 | 0 1
0 | 0 1 | 0 1 | 0 1
Final
1 0 | 1 0 | 1 0
1 0 | 1 0 | 0 1
0 1 | 0 1 | 0 1
Hamming Distance =1
Both top & bottom asserting the same rows 1&2&3 and columns 1&2&3 by different order in the same raw data
Permutation determines the final state

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

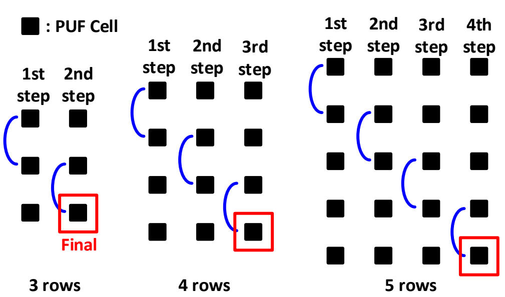


Fig. 4. Previous technique for changing sequence lengths [6].

WLR [0], and WLR [1] are enabled, 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. Finally, the weak cells are overwritten by the strong cells.

Unlike the conventional SRAM-based PUFs, the proposed PUF does not directly use the start-up values. To improve the randomness, the proposed technique connects any two nodes from adjacent PUF bit cells by enabling their word-lines. By doing this, the initial strengths of all the 24 transistors from the selected four PUF cells contribute to the final PUF value. In addition, the generated value depends on the rows and columns we chose. Therefore, the challenge response pairs are significantly expanded because of the substantially increased combinations of selecting two rows and columns.

The reliability of each PUF cell depends on the mismatch level of two cross-coupled inverters. A larger mismatch produces a stronger cell. Based on the strength of mismatch, we could define a PUF cell into four levels. As shown in Fig. 2, the strongest cell (I) represents larger mismatches while the weakest cell (IV) indicates smaller mismatches. When we enable both WLL and WLR, it can create conflicts in the selected bitlines. As shown in Fig. 2, two strong adjacent cells try to overwrite data into the weakest cell with opposite data.

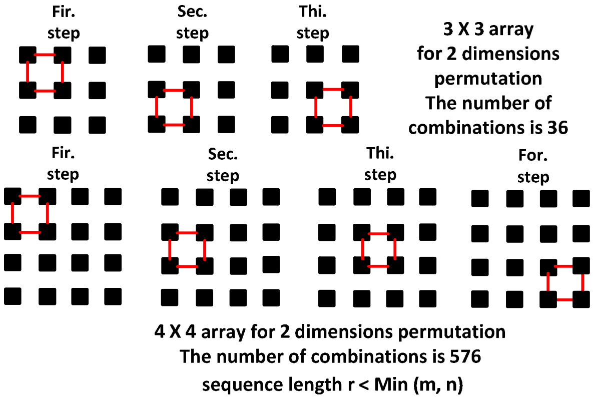

Fir. step
Sec. step
Thi. step
For. step
3 X 3 array for 2 dimensions permutation
The number of combinations is 36
4 X 4 array for 2 dimensions permutation
The number of combinations is 576
sequence length r < Min (m, n)

Fig. 5. Different cell selection combinations in the proposed PUF.

In this situation, the difference between I and IV becomes dominant in this operation, which is larger than that between II and IV (subordinate). Therefore, the data in IV will be overwritten by the data in I.

Moreover, the generated PUF value is affected by the applied permutation. As depicted in Fig. 3, the top sequence connects the first two rows and the first two columns, followed by last two rows and last two columns, written as the sequence of {(1, 2), (2, 3); (1, 2), (2, 3)}. Similarly, the bottom sequence can be written as {(2, 3), (1, 2); (2, 3), (1, 2)}. The different background color bits represent various cell strengths. Note that a different ordered sequence produces a different final value even if we chose the same rows and columns. In the 2nd row and the 3rd row of the final state, the hamming distances are equal to 1. Therefore, both the row and column selection, and the permutation order in the selected rows and columns affect the final PUF value.

Fig. 4 illustrates a previous way of varying sequence lengths in [6] (only one direction is displayed to simplify the analysis). When 3 rows are used for generating a PUF value, 2 steps are necessary. In the first step, we have 3 choices and

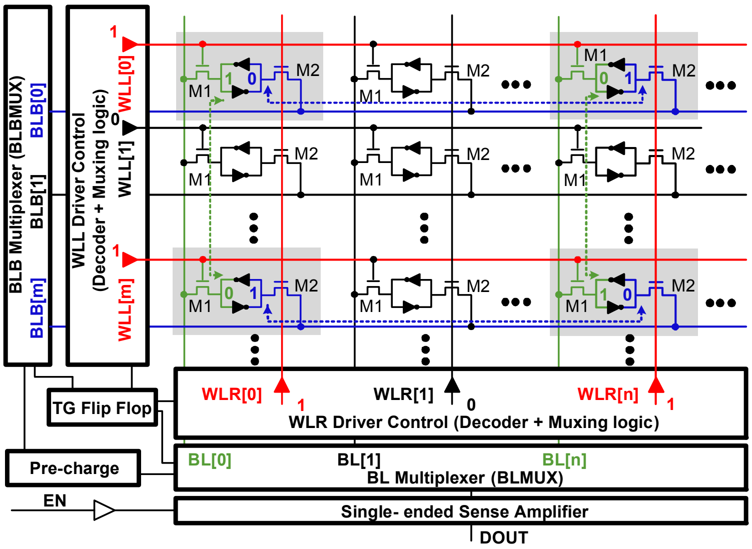


Fig. 6. Proposed SRAM PUF architecture.

in the second step we have 2 choices, which provides 6 permutations. Similarly, when 5 rows are employed, 4 steps (Fig. 4(Right)) are required and we can obtain 120permutations. Even though the technique in [6] improves CRPs by utilizing the sequence dependency, the employment of single column limits the number of permutations, which is addressed in this work.

As illustrated in Fig. 1, the proposed technique can select 2 rows and 2 columns for PUF data generation. For an m rows × 2 columns array with a sequence length of r, the number of challenge to response pairs (CRPs) is written as follows.

$$m \times (m-1) \times \ldots \times (m-r) \qquad (1)$$

Fig. 5 exhibits sample combinations of cell selection using 3 × 3 and 4 × 4 arrays. Compared to Fig. 4, the permutation moves in two directions, which makes the number of combinations square of that expressed in (1). For example, when considering a 3 × 3 array, the CRPs of the proposed technique is 36, which is 2× of the CRPs in [6]. The CRPs become 576 when using a 4 × 4 array. The number of CRPs of the proposed scheme can be estimated by the following expression.

$$[m \times (m-1) \times \ldots \times (m-r)] \times [n \times (n-1) \times \ldots \times (n-r)]. \qquad (2)$$

Here, m is the number of rows, n is the number of columns, and r is the sequence length. Note that r is less than m and n.

Fig.6 shows the architecture of the proposed SRAM PUF. To support the proposed configurability, the SRAM has a decoder and a write circuit for both rows and columns. In the SRAM mode, write operation starts by asserting WLL and WLR and loading data in selected BL and BLB. Therefore, the selected cell has the same write condition as the conventional cell. Since the word-lines and bit-lines run orthogonally, the noise margin of the half-selected cells remains the same as the conventional one. For the read operation, because the bit-lines are not placed parallel, single-ended sensing amplifier is required to sense the read data.

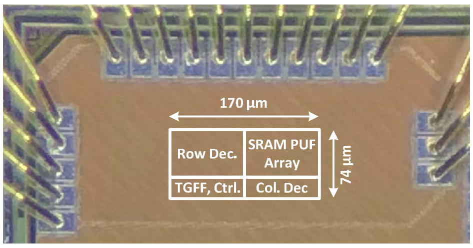
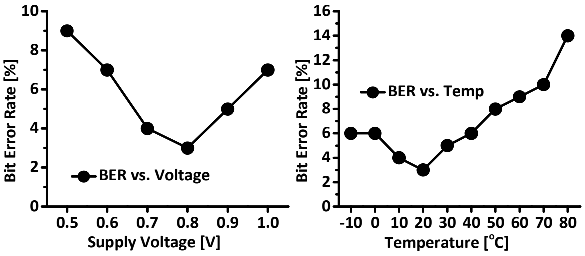


Fig. 7. Die photo of the proposed SRAM PUF.



(a) (b)

Fig. 8. Measured BER sweeping: (a) voltage and (b) temperature.

III. Measurement Result and Discussion

A 4kb (64 ×64) SRAM PUF array test chip is fabricated in 65nm CMOS technology. The die photo is shown in Fig. 7. The total area is 170 × 74 μm^2 and the size is 1.46 μm^2 per bit cell. A logic analyzer is used to build the experiment platform.

For the common SRAM PUF array, as it is a weak PUF, the challenge to response pairs are limited, especially some of them only use the chip ID (CRP is equal to 1). For the proposed one, the data map is determined by the sequence length and sequence order. According to the same challenge (address), we could generate multiple responses (data maps). For the 64 ×64 PUF, when sequence length equal to 5, the CRPs could be achieved 8.37 × 10^{17}.

A. *Reliability*

First, we test the reliability of output over the voltage variation, which is measured as the bit error rate (BER). We sweep the voltage from 0.5 V to 1V at nominal temperature

TABLE I. COMPARISON WITH PREVIOUS WORKS

		This work	*2017 VLSI [6]*	*2015 ISSCC [7]*	*2014 ISSCC [3]*	*2004 VLSI [8]*	*2007 ISSCC [9]*
Technology		65nm CMOS	28nm FDSOI	40nm CMOS	22nm CMOS	180nm CMOS	130nm CMOS
Area/PUF bits		5.84 μm^2 (4 cells)	388-970 F^2 (2-5 cells)	—	4.66 μm^2	—	1092 F^2
Energy efficiency (fJ/b)		81 (seq-5, 0.5 V)	97 (seq-5, 0.7 V)	17750	13	—	930
Inter-PUF HD		0.497	0.481 - 0.495	0.5007	0.49	—	0.505
Native BER (%)		3 (0.8V, 20℃)	3.17 (0.7V, 27℃)	9 (worst VT)	~8	0.7 - 4.82	3.04
# Possible CRPs		8.37×10^{17} (seq-5)	1.17×10^{11} (seq-5)	~5.5×10^{28}	250k	1.4×10^{20}	1 (chip ID)
Tested Condition	Voltage (V)	0.5 - 1	0.5 – 0.9	0.7 – 1.2	0.7 – 0.9	±2%	0.9 – 1.2
	Temp (℃)	-10 - 80	0 - 80	-25 - 125	25 - 50	27 - 67	0 - 80
PUF Type		Bi-Stable	Bi-Stable	Ring Osc.	Bi-Stable	Arbiter	Bi-Stable

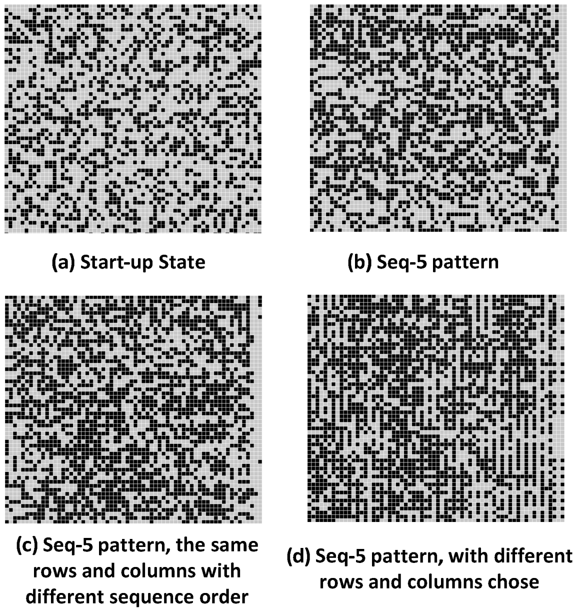


Fig. 9. Measured PUF data maps from one chip.

27℃. As shown in Fig. 8 (a), the BER achieved 3% under 0.8 V supply voltage. The maximal bit error ratio is 9% at 0.5 V.

Second, we evaluate the reliability of output against the temperature variation by sweeping the temperature from -10℃ to 80℃, under the nominal voltage 0.8 V. We measured the BER value per 10℃, as shown in Fig. 8 (b). The BER is 3% under 20℃ and the maximal bit error ratio in the temperature range is 14%.

B. Randomness

For a conventional PUF, the generated data is decided by strengths of mismatch between 6 transistors in one bit cell. In the testing chip, the distribution of 0 is 62.45% in raw data when supply voltage ramps up. For the proposed PUF, the generated data is affected by 24 transistors in single PUF step, the variation is increased significantly. After PUF operation the sequence length equals to 5, the distribution of 0 in this new map in Fig.9 (b) is 51.12%. In different configurations, the worst distribution we got through testing is 44%.

C. Uniqueness

Fig. 9 (a) shows the chip raw data pattern. This data map could be seen as the chip ID, as it depends on the unique PVT variations. The dark color represent data 1 and grey color represent data 0.

Fig. 9 (b) shows the final data map after the PUF operation which sequence length is 5. The hamming distance between (a) and (b) is 0.501, as shown in Fig. 10. After that we use the same address and sequence length 5 with different sequence order to generate a new data map. The pattern is shown in Fig. 9 (c), the hamming distance between (b) and (c) is 0.427. It demonstrates that for the same columns and rows with the same initialization and sequence length, different permutations could provide unique data maps.

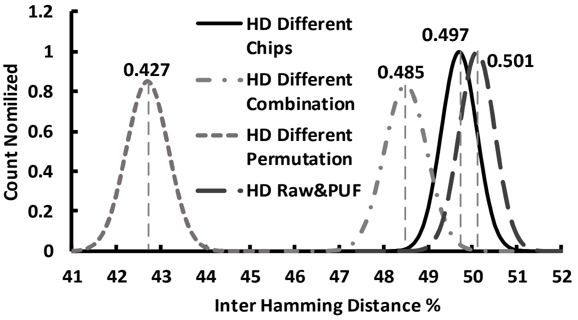


Fig. 10. Measured hamming distances.

In Fig.9 (d), it presents the data map after PUF operation with different configurations for the same chip, the sequence length equals to 5. The inter-PUF hamming distance between (b) and (d) is 0.485.

As shown in Fig. 10, all chips use the same sequence lengths (seq-5) and permutation, the inter-PUF hamming distance between them is 0.497. The minimal power consumption is 81 fJ per bit for the sequence is 5 at 0.5 V. Table I compares the previous works with the proposed SRAM PUF, as the SRAM based PUF, this work provides the largest CRPs in the weak PUF type.

IV. CONCLUSION

In this paper, we presented a 2D sequence dependent PUF, which expends the CRPs by the orders of rows$^{(\text{sequence length - 1})}$ × columns$^{(\text{sequence length - 1})}$. We split the word-lines and run them vertically and horizontally respectively, to connect four cells simultaneously to generate one data. According to various sequence length and order, we could generate multiple data maps in one chip. The chip area is 12580 μm^2 and 1.46 μm^2 per bit cell in 65 nm CMOS technology. The minimal energy consumption is 81 fJ/bit at 0.5 V, the bit error rate is 3% at nominal point (0.8 V/20℃), and inter hamming distance between chips is 0.497. For the same sequence length and different order in one chip, the hamming distance achieved 0.427. In the voltage range (0.5V – 1V) and temperature range (-10℃ – 80℃), this PUF works well. The measurement results demanstrate that the proposed PUF is configurable and reliable for the physical sercurity keys generation.

REFERENCES

[1] L. Kusters et al.," Security of Helper Data Schemes for SRAM-PUF in Multiple Enrollment Scenarios," IEEE Intl. Symp. on Information Theory., pp. 1803–1807, 2017.

[2] A. Maiti et al., "A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions," in IACR Cryptology ePrint Archive. 2011.

[3] 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," IEEE ISSCC, pp. 278-279, 2014.

[4] J. Li et al., "A technique to transform 6T-SRAM arrays into robust analog PUF with minimal overhead," IEEE Intl. Symp. on Circuits and Systems, pp. 1-4, 2017.

[5] C. Q. Liu, "A new write-contention based dual-port SRAM PUF with multiple response bits per cell," IEEE Intl. Symp. on Circuits and Systems, pp. 1-4, 2017.

[6] S. Jeloka et al., "A sequence dependent challenge-response PUF using 28nm SRAM 6T bit cell," IEEE, Symp. on VLSI Circuits, pp.l C270-271, 2017.

[7] K. Yanget al., "A Physically Unclonable Function with BER <10^8 for Robust Chip Authentication Using Oscillator Collapse in 40nm CMOS," IEEE ISSCC, pp. 1-3, 2015.

[8] J. W. Lee et al., "A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications," IEEE, Symp. on VLSI Circuits, pp. 176-179, 2004.

[9] Y. Su et al,. "A 1.6pJ/bit 96% Stable Chip-ID Generating Circuit using Process Variations", IEEE ISSCC, pp. 406-407, 2007.