A Programmable 6T SRAM-Based PUF with Dynamic Stability Data Masking

Lu Lu and Tony Tae-Hyoung Kim

School of EEE, Nanyang Technological University, Singapore

2021 IEEE Asian Solid-State Circuits Conference (A-SSCC) | 978-1-6654-4350-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/A-SSCC53895.2021.9634755

SRAM-based physically unclonable function (SPUF) generates a random code by utilizing deep submicron variations in the fabricating process. It offers a mature and practical security module which widely adopted in commercial products. Advantages of SPUF (as shown in Fig. 1) are that no data are kept when the power is off, and it can generate the secret key by reusing the SRAM structure in the system with a minimum area overhead and least effort on integration. Therefore, SPUF should support both the SRAM mode and the PUF mode without significant performance degradation and area overhead.

Conventional SPUF works as a chip ID with the challenge-response pair (CRP) of 1. The response of the SPUF from start-up states is a noisy fingerprint and needs further processing to become a reliable secret key. To expand CRP, the works in [1-2] proposed programable approaches involving multiple bit cells in the random data generation. For reliability improvement, Mathew *et al.* developed several techniques like temporal majority voting, error correction, and transistor aging [3]. However, these techniques suffer from either an area overhead or memory performance degradation. This work proposes a novel SPUF structure to address the above issues. First, it expands the CRPs to (rows$^{\text{(sequence length + 2)}}$ × columns), which increases proportionally with the array size. Second, a novel bit selection algorithm is employed to produce a dynamic stability map for each set of random code. This enhances the reliability of the SPUF in the full voltage and temperature (VT) range.

Fig. 2(a) and (b) illustrate the schematic and the layout of the proposed 6T SRAM based PUF bit cell. The proposed unit cell uses the split left word-line (WLL) and right word-line (WLR) for separate control of two pass-gate transistors. To eliminate the offset from the layout placement, symmetric drawing is required in the front-end layers to create the original secure data from process variations. As shown in Fig. 2(c), at the PUF mode, we assert two WLLs and two WLRs in three rows simultaneously. In each column, two half-selected bit cells will have one pass-gate transistor turned on, and the fully-selected cell (with * asterisk) will have both pass-gate transistors that are on. To improve the weak write ability in the single-ended writing, we doubled the size of the pass-gate transistor. The proposed SPUF enriches the entropy from 6 devices to 18 devices.

Reliability is a critical criterion of PUF performance. Fig. 3 illustrates the reliability enhancement by applying for the multiple-rows selection program. We classify all bit cells into 50% stable cells and 50% unstable cells by the strength of intrinsic mismatching. In Fig. 3, Cell C (marked with *) is a fully-selected cell. The stability of the fully-selected cell can be amended based on the precondition of the stability and the stored data in the bit cells. After the PUF operation, the possibility of Cell C being a stable cell increases to 75%.

To improve the security level, a secret key needs to be updated regularly. Using the multiple-rows selection program to generate one random data as one step, we could repeat several steps and involve more rows successively to obtain multiple CRPs. Fig. 4 displays 3 examples of using 3 different permutations in 3 columns within two steps. The darker bits indicate more stable cells, while the lighter color bits represent less stable ones. From example 1 to example 2, we chose the same sequence (selected rows) in different orders (which rows are first selected), obtaining different responses in the final data. Example 2 and example 3 indicate that different locations of the fully-selected cell also affect the final response for the same sequence and order. When the sequence length is 2 within m rows and one column, the number of combinations to select 4 rows from m is C_m^4. From these 4 rows, we have $C_4^3 \times C_2^1$ choices for the two steps operation. Starting with m = 4, the CRPs is 8. Similarly, the CRPs in 5 rows with 3 steps and 6 rows with 4 steps are 120 and 2880, respectively. Using induction in size of m × n array, with a sequence length of r, the formula of the number of CRPs is:

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

Since we can generate multiple CRPs by programming a single SPUF, the hamming distance (HD) can be calculated from the data sets. For the same sequence in different orders, the data patterns are different. The HDs between the distinct data patterns are improved by increasing the sequence length. In the same environment, for sequence #1 order #1~#100, the average value of HD is improved from 23.8% with 2 steps sequence length to 41.29% with 5 steps sequence length. The HD between sequence #1 to #100 within a single chip is 44.93%, and the HD between different chips achieves 49.64%. The high CRPs provide stronger defense from attacks. Also, by averaging the current and the voltage between connected cells with multiple steps, it is more difficult for an attacker to extract the information using a side-channel attack.

As the stability improvement is limited by programming the sequence, a bit selection algorithm for creating the stability mask is adopted. It identifies the stable cells within a single device by mapping each random data set with a corresponding stability map [4]. The environmental conditions range is 0.7V ~ 1.2V for voltage and 20°C ~ 80°C for temperature. We have tested extreme conditions, a high voltage with a low temperature (HVLT) and a low voltage with a high temperature (LVHT). Repeating the PUF operation 10 times, two tables with stability coefficients are generated. If 8 out of 10 times the data we read is '1', then the coefficient is 0.8. The filter criterion is if the stability coefficient is within $0.2 < C_{HVLT} < 0.8$ or $0.2 < C_{LVHT} < 0.8$ in either table, it will be masked as unstable cell. This operation provides a highly reliable SPUF device by mapping the data to the stability distribution. Fig.5 (left) shows the operation flow.

Fig.5 (right) depicts the BER by sweeping the voltage at room temperature 20°C and sweeping the temperature at nominal voltage 1V. The green line corresponds to the BER from start-up data. The red line represents the data after the multiple-rows selection program. By overwriting the unstable cells, the programmable operation improved the BER from 5.27% to 2.62%. In extreme environmental conditions, the worst BERs are 8.41% at 80°C and 8.23% at 0.7V. The blue line with dot symbol shows the bit selection algorithm reduces the worst BER to 0.8% in the nominal condition. The worst BERs in the extreme condition (HVLT/LVHT) are reduced by around 70~80% from the data which applied sequence programming, achieving 1.8% at 80°C with nominal voltage and 2.4% at 0.7V under room temperature, respectively.

Table I compares the proposed work with other recently published works. As a dual-mode SPUF with multiple CRPs, this work achieves the lowest BER of 0.8%. With a similar mask ratio, [6] attains almost 0 BER in the worst VT conditions, but it cannot fulfill memory function, and the CRP is 1. [2] reaches the highest number of CRP, but it has higher BER and a larger area.

In conclusion, this work proposes an SPUF with multiple CRPs and improved reliability. The proposed programmable sequence-dependent operation increases the CRPS, and the bit selection algorithm filters the unstable cells. It can be easily implemented by modifying a conventional 6T SRAM. The dual-mode operation fits well in low-cost, high-quality hardware security applications.

References:

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

[2] L. Lu, et al., "A Sequence-Dependent Configurable PUF Based on 6T SRAM for Enhanced Challenge-Response Space," IEEE ISCAS, 2019.

[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, 2014.

[4] K. Xiao, et al., "Bit Selection Algorithm Suitable for High-Volume Production of SRAM-PUF," IEEE, HOST, 2014.

[5] K. Liu, et al., "A 373-F2 0.21%-Native-BER EE SRAM Physically Unclonable Function With 2-D Power-Gated Bit Cells and VSS Bias-Based Dark-Bit Detection," IEEE JSSC, 2020.

[6] Y. He, et al., "An Automatic Self-Checking and Healing Physically Unclonable Function (PUF) with <3×10-8 Bit Error Rate", IEEE ISSCC, 2021.

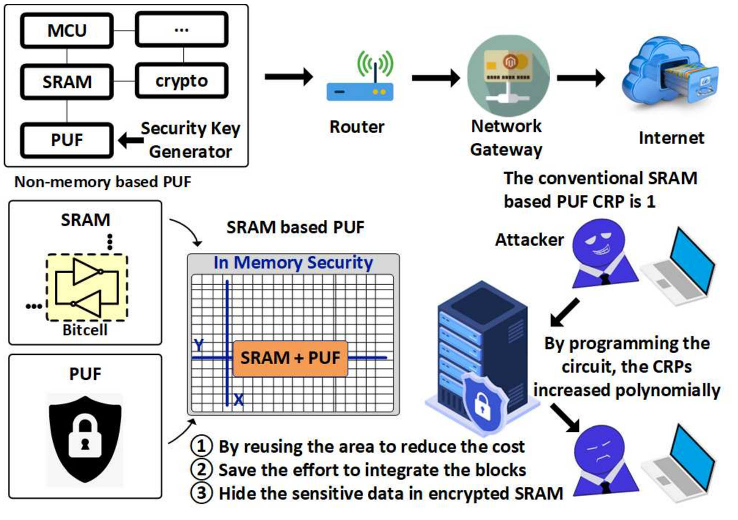

MCU
...
SRAM
crypto
PUF
Security Key Generator
Non-memory based PUF
Router
Network Gateway
Internet
SRAM
Bitcell
SRAM based PUF
In Memory Security
Y
SRAM + PUF
X
PUF
The conventional SRAM based PUF CRP is 1
Attacker
By programming the circuit, the CRPs increased polynomially
① By reusing the area to reduce the cost
② Save the effort to integrate the blocks
③ Hide the sensitive data in encrypted SRAM

Fig. 1. Proposed SPUF works in dual-mode and expands the CRPs in a single chip for low-cost, high-quality hardware security applications.

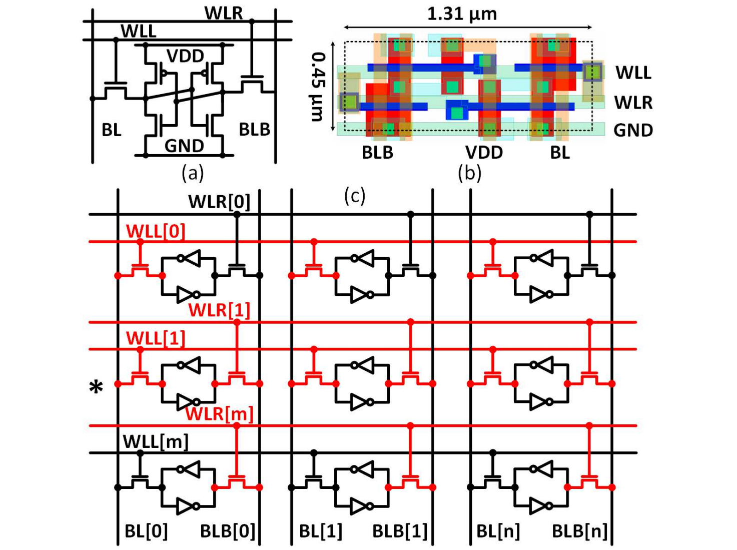
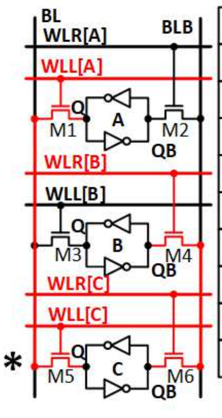


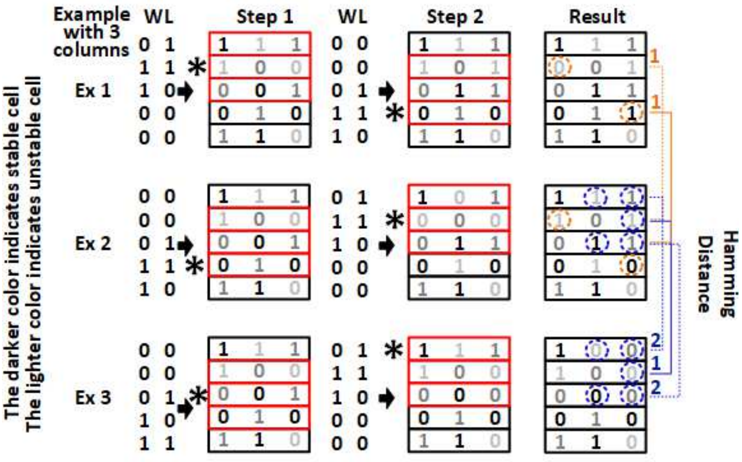
Fig. 2. Proposed structure: (a) bit cell schematic, (b) bit cell layout, and (c) principle of the proposed multiple-rows selection program.



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

* S: Stable Cell
U: Unstable Cell

Fig. 3. Reliability enhancement of the multiple-rows selection program.


Example with 3 columns
WL
Step 1
WL
Step 2
Result
Ex 1
Ex 2
Ex 3
The darker color indicates stable cell
The lighter color indicates unstable cell
Hamming Distance
1
1
2
1
2

- Sequence indicates which rows are selected
- Order indicates which rows are selected first which are later
- Challenge sequences (Ex 1, 2 and 3) are using the same rows
- Sequence, order and the * location determine the final result

Fig. 4. Data dependency on the multiple-rows selection program.

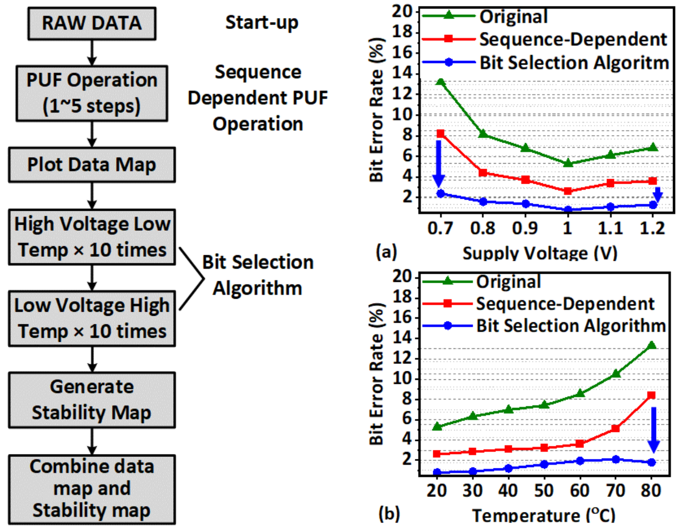


Fig. 5. Operating flow with the measured BER: (a) sweeping voltage in 20°C and (b) sweeping temperature at 1V.

TABLE I. COMPARISON WITH PRIOR ARTS

	JSSC '20 [5]	ISSCC '21 [6]	VLSI '17 [1]	ISCAS '19 [2]	**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 μm^2 (4 cells)	987 F^2 (3 cells)
Energy (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	1.17×10^{11} (seq-5)	8.37×10^{17} (seq-5)	**4.01×10^{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.

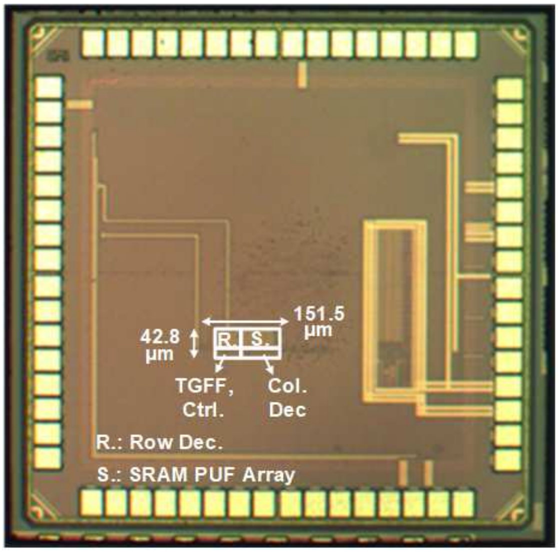


Fig. 6. Die micrograph of 40nm SPUF chip.