Supporting Information

Concealable Physical Unclonable Function Generation and In-Memory Encryption Machine using Vertical Self-Rectifying Memristors

Jea Min Cho[a], Seung Soo Kim[a], Tae Won Park[a], Dong Hoon Shin[a], Yeong Rok Kim[a], Hyung Jun Park[a], Soo Hyung Lee[a], Taegyun Park *[a], and Cheol Seong Hwang*[a]

[a] *Department of Materials Science and Engineering and Inter-University Semiconductor Research Center, Seoul National University Gwanak-ro 1, Gwanak-gu, Seoul 08826, Republic of Kore*

corresponding author: tagyun@snu.ac.kr, cheolsh@snu.ac.kr

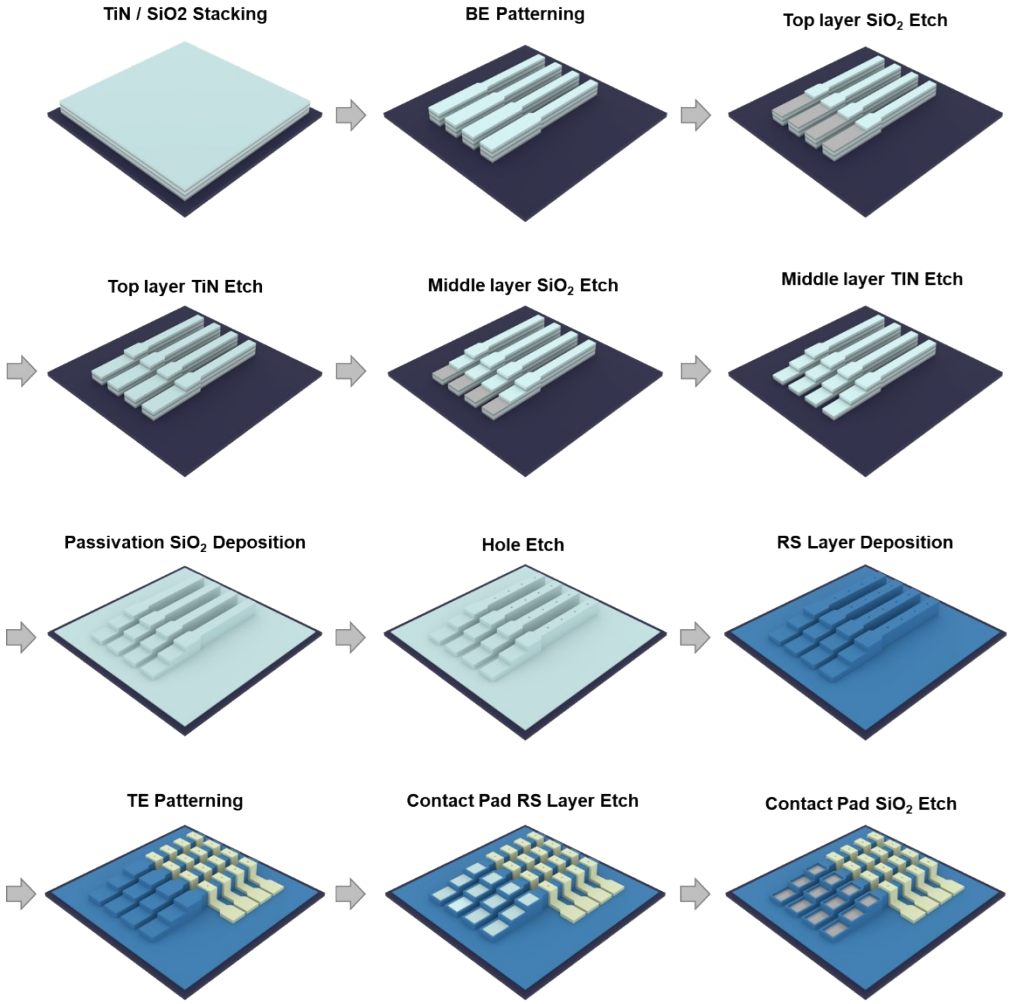


Fig. S1 | Fabrication process of the proposed VRRAM structure

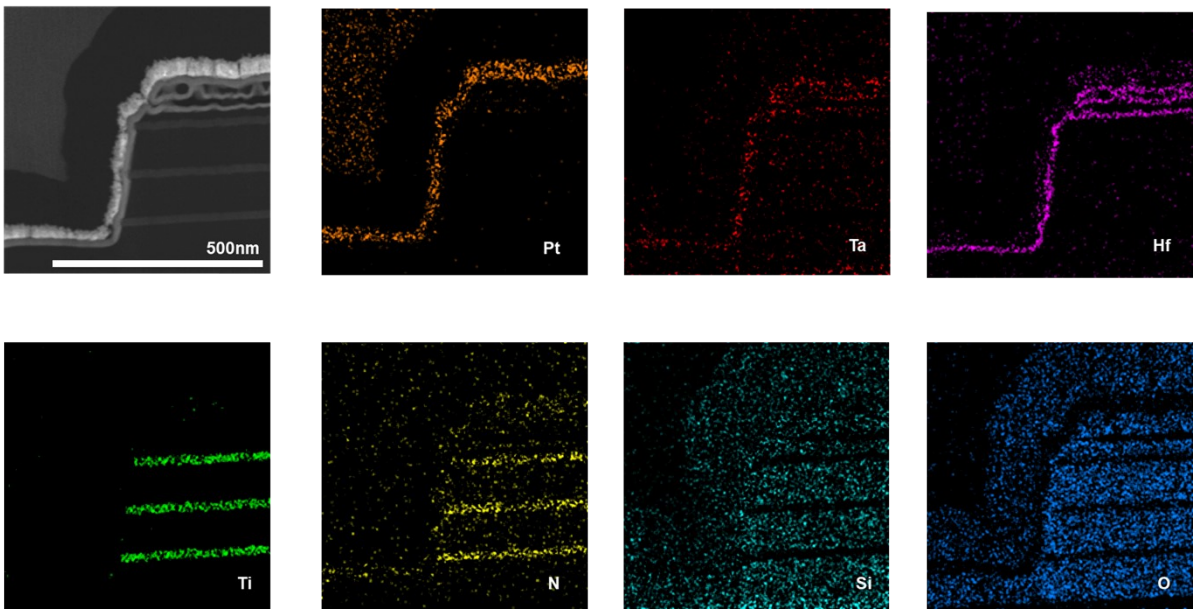


Fig. S2 | Scanning Transmission Electron Microscopy (STEM) and Energy Dispersive Spectroscopy (EDS) analysis for the V-RRAM

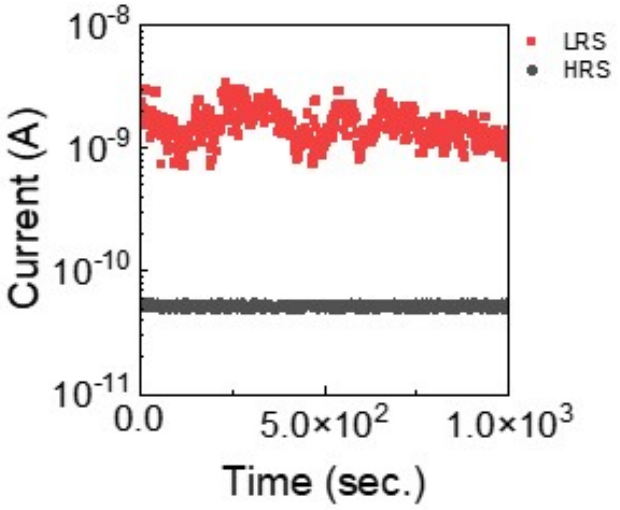


Fig. S3 | **Retention of V-RRAM device**

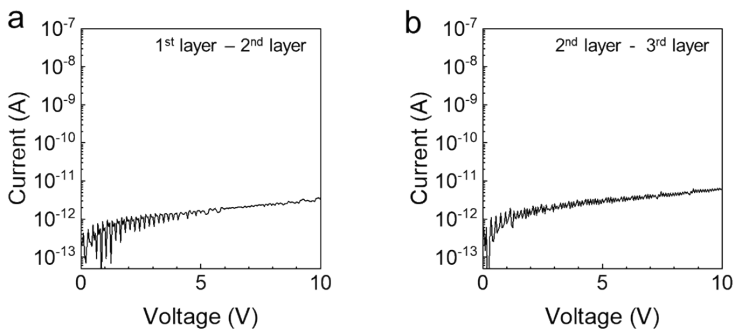


Fig. S4 | Leakage current between layers in V-RRAM, which are separated by a 100-nm-thick SiO_2 layer. For the current measurement, the contact pad of one selected layer was grounded, while a DC bias of up to 10 V was applied to the contact pad of another layer. (a) Leakage current between the first layer and the second layer. (b) Leakage current between the second layer and the third layer.

The leakage current remained below 7 pA up to 10 V, as shown in Figure S4. This level of leakage current is sufficiently low to ensure that it does not interfere with the proper execution of key generation and logic operations.

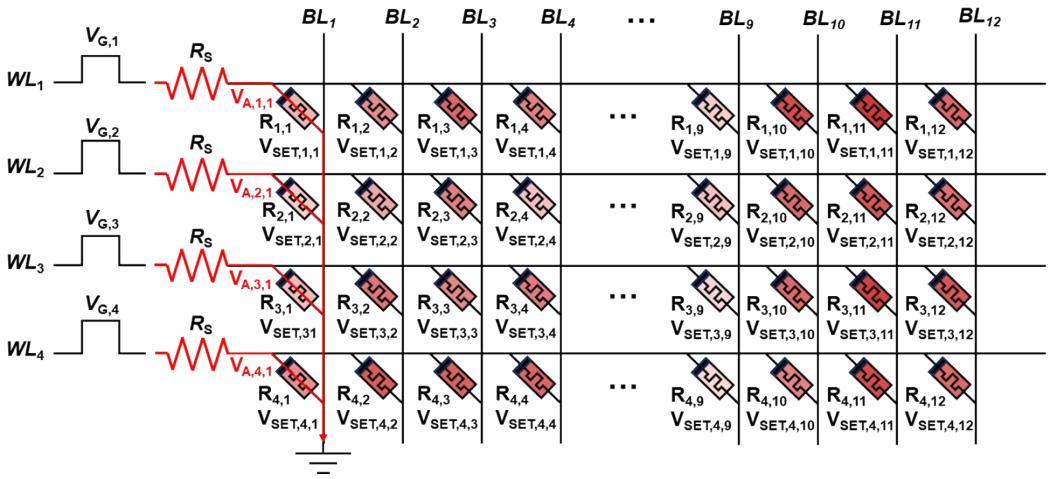


Fig. S5 | Schematic diagram of voltage division process during PUF Generation.

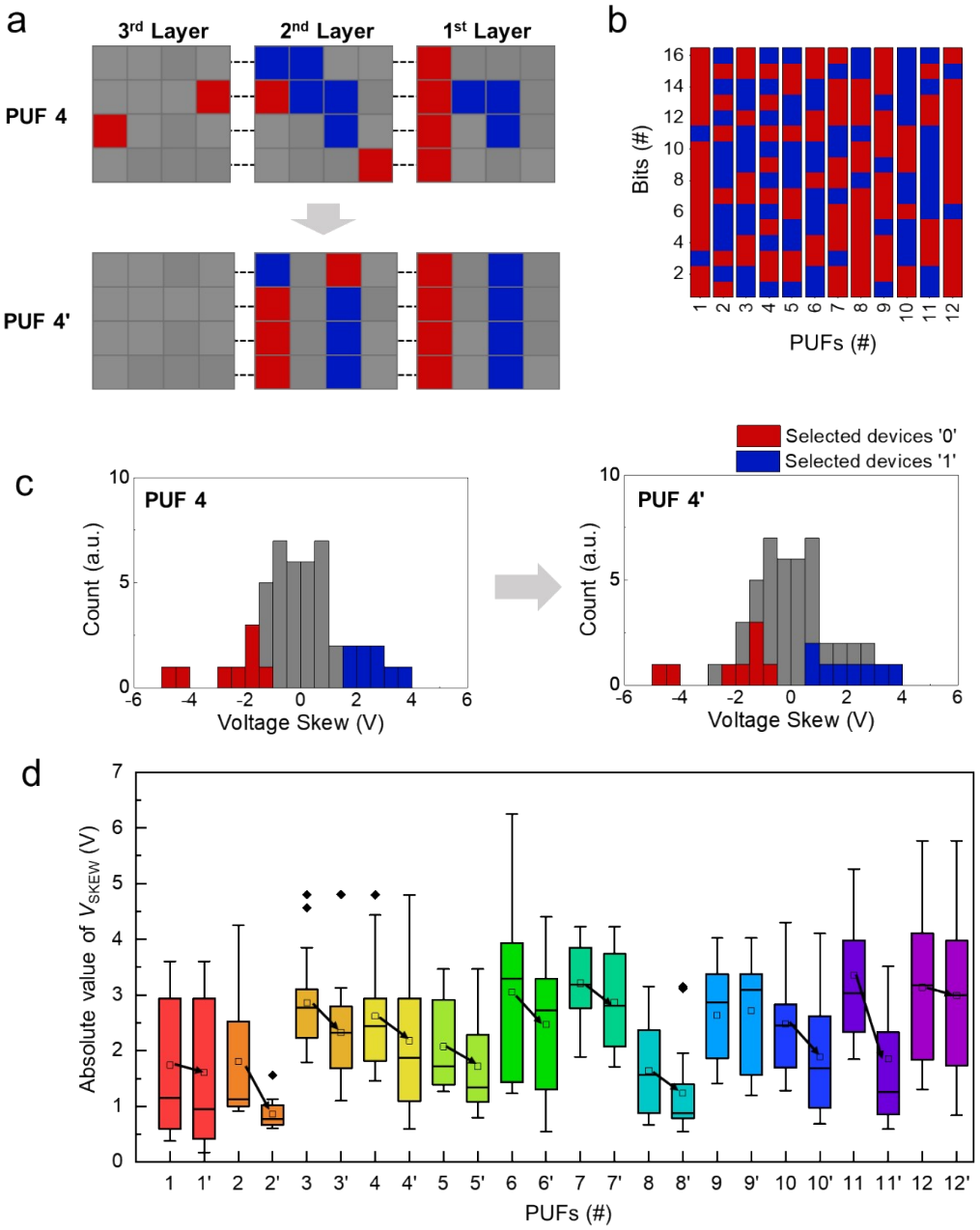


Fig. S6 | Comparison of key selection results depending on key relocation. (a) The key selection results with relocation (PUF 4) are compared to the key selection results without relocation (PUF 4'). In this figure, an apostrophe (') denotes the PUF key selected when relocation is not performed. (b) 12 PUF keys were generated by selecting four BLs without relocation. (c) V_{SKEW} distribution of all devices in the V-RRAM array and selected devices depending on the implementation of key relocation. When relocation is not performed, devices with low absolute value of V_{SKEW} are selected due to the constraint of selecting four BLs. (d) The variations in the absolute value of V_{SKEW} for the 16 selected devices across the 12 PUFs, comparing the conditions with and without relocation.

Relocation enhances the parallelism of logic operations and the efficiency of key selection. In the proposed V-RRAM encryption machine, data encryption is performed by applying a bias to two BLs that contain the key and

data bits. If the relocation is not employed in a 4x4 array, the key criterion is not satisfied, resulting in lower uniformity and the V_{SKEW}.

The four keys are selected on a single BL to encrypt the four data located on the other BL, as shown in PUF 4' of Figure S6a. In this case, the four BLs with the highest means of the absolute value of V_{SKEW} of the devices located on each BL were selected. This method introduces a constraint in key selection. Figure S6b shows the 12 PUF keys selected without relocation. Without relocation, selecting 8 devices from each group of 0s and 1s is impossible, resulting in a decrease in uniformity to 0.427, compared to the ideal value of 0.5. Also, as shown in Figure S6c, this constraint may lead to selecting devices with lower V_{SKEW}. Figure S6d shows how the V_{SKEW} distribution across the 12 PUFs changes when such a constraint is applied. It can be observed that the absolute value of V_{SKEW} decreases across the PUFs, except for PUF 9. The average absolute value of V_{SKEW} decreased by 19%, from 2.55 to 2.06. This reduction in V_{SKEW} increases the probability of bit errors. V_{SKEW} did not decrease for PUF 9 because its uniformity dropped to around 0.25. Therefore, degradation in either V_{SKEW} or uniformity can occur when relocation is not applied. Consequently, Figure S6 demonstrates that relocation is more effective in decreasing the bit error rate and achieving ideal uniformity from the perspective of key selection.

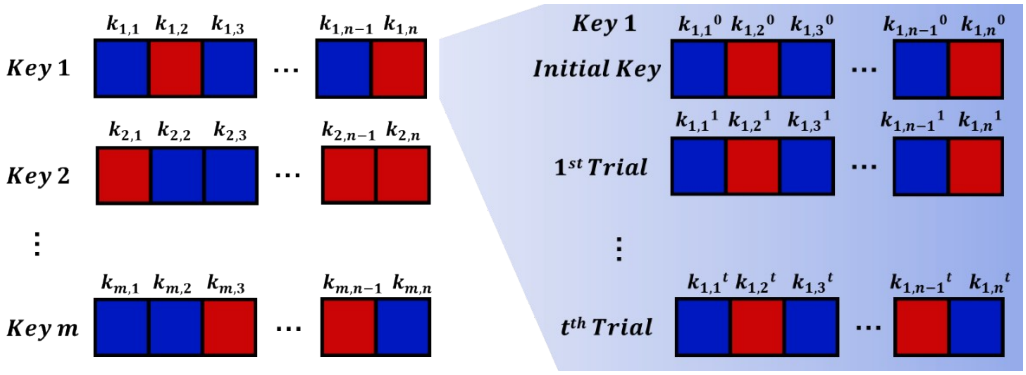


Fig. S7 | Security Metrics for PUF key and notations for representing the PUF key number (*m*), key bit position (*n*), and key generation trial (*t*).

The primary metrics for evaluating PUFs include uniformity (UF), uniqueness (UQ), and bit error rate (BER). The UF and UQ are metrics used to assess the randomness of a PUF, while BER evaluates the reliability of the PUF. These metrics are calculated based on the hamming weight of the key vector and the intra- and inter-hamming distances between key vectors. In Figure S7, The subscript m and n represent the number of PUFs and key bit position, respectively. The superscript t denotes the key generation trial.

Uniformity (UF)

UF is calculated as the normalized hamming weight of a single PUF key. The UF of the mth PUF for the *N*-bit key is as shown in Equation S1. This metric reflects the balance between the number of '0's and '1's in the PUF key. An ideal value of 0.5 indicates an equal distribution of '0's and '1's, which maximizes the difficulty of key prediction. In this study, since an equal number of 0s and 1s (eight of each) were selected, the UF for all PUFs is 0.5, representing a perfectly balanced distribution of bits.

$$UF_m = \frac{\sum_{n=1}^{N} k_{m,n}}{N} \tag{S1}$$

Uniqueness (UQ)

UQ is calculated as the normalized inter-hamming distance between different PUF keys. The UQ between the p^{th} PUF key and the q^{th} PUF key is shown in Equation S2. UQ represents the degree of dissimilarity between different PUF keys, and the ideal value for UQ is 0.5.

$$UQ_{p,q} = \frac{\sum_{n=1}^{N} \left| k_{p,n} - k_{q,n} \right|}{N} \tag{S2}$$

Bit Error Rate (BER)

BER is the normalized intra-hamming distance between the same key generated across different trials. The BER

of the m^{th} PUF for T-trial is as shown in Equation S3. BER serves as a metric for assessing the reliability of the concealable key, with 0 being the ideal value.

$$BER_m{}^T = \frac{\sum_{t=1}^{T}\sum_{n=1}^{N}\left|k_{m,n}{}^t - k_{m,n}{}^0\right|}{NT} \tag{S3}$$

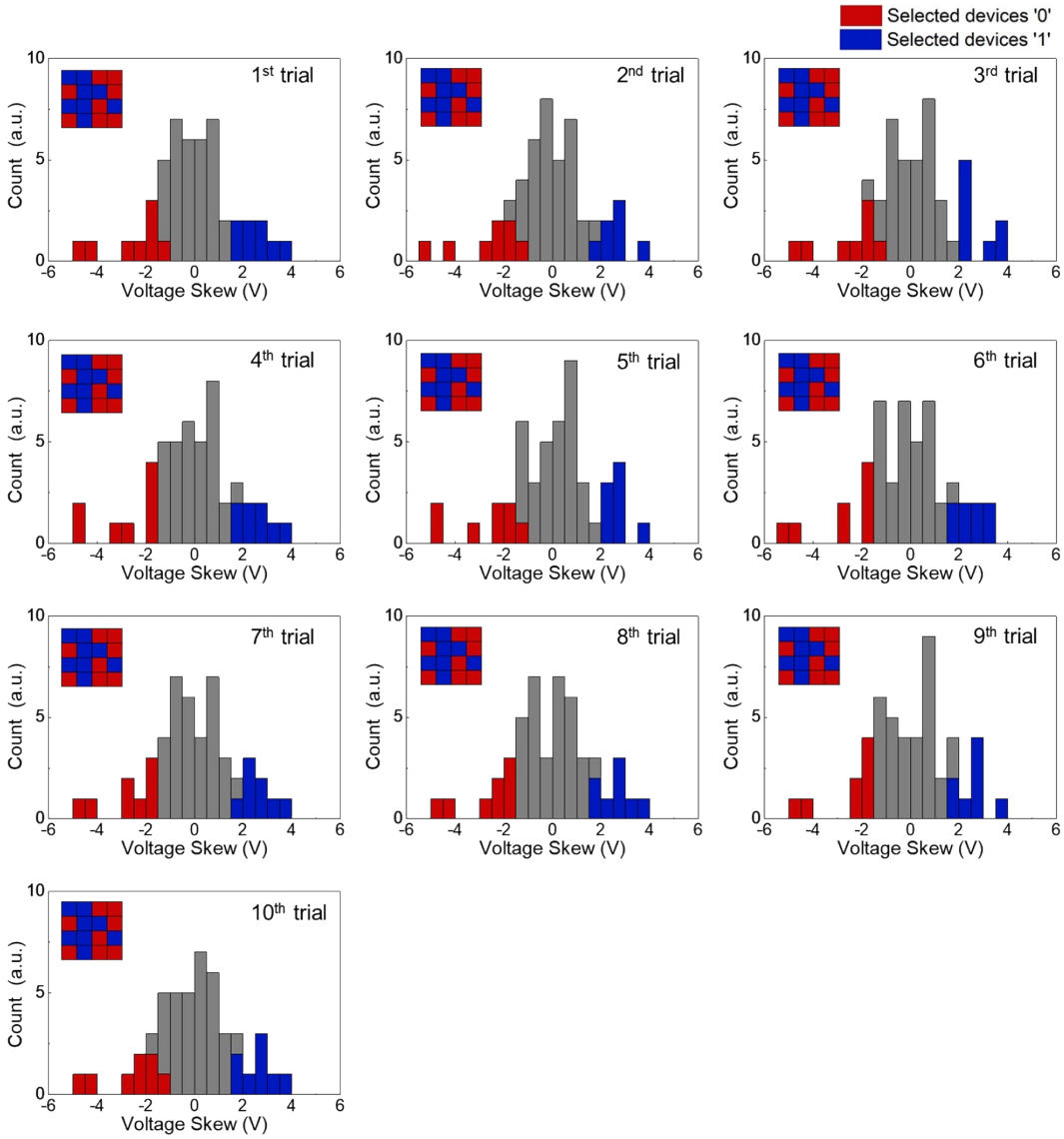
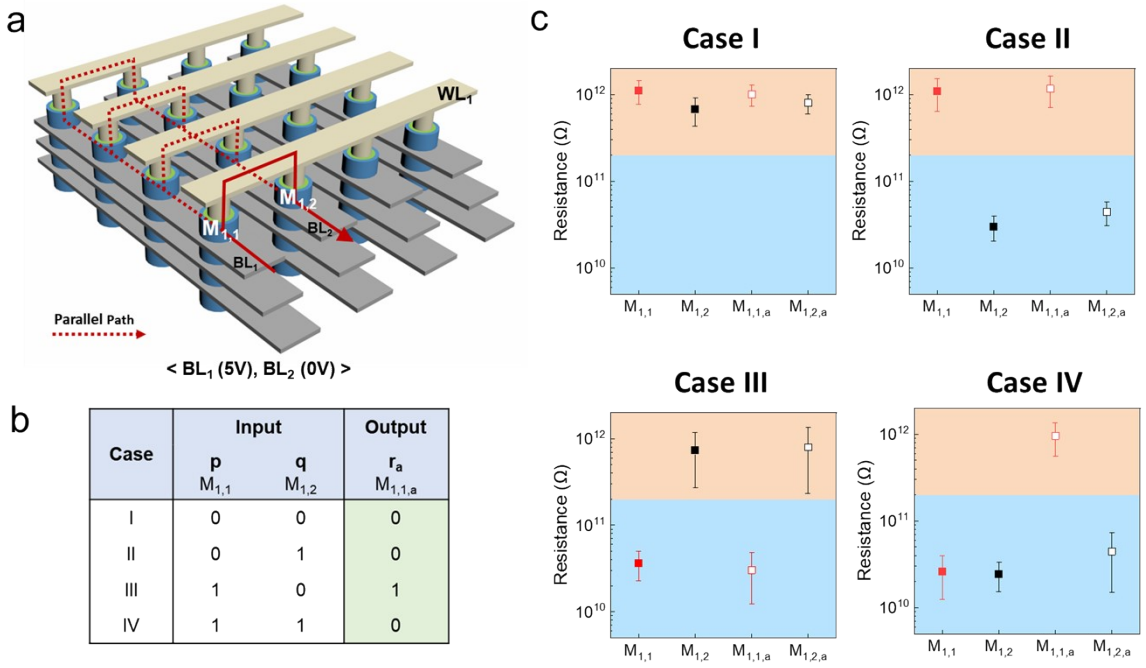


Fig. S8 | The changes in the V_{SKEW} distribution of the selected devices and all devices in V-RRAM array over 10 cycles of conceal and reveal for PUF 4.

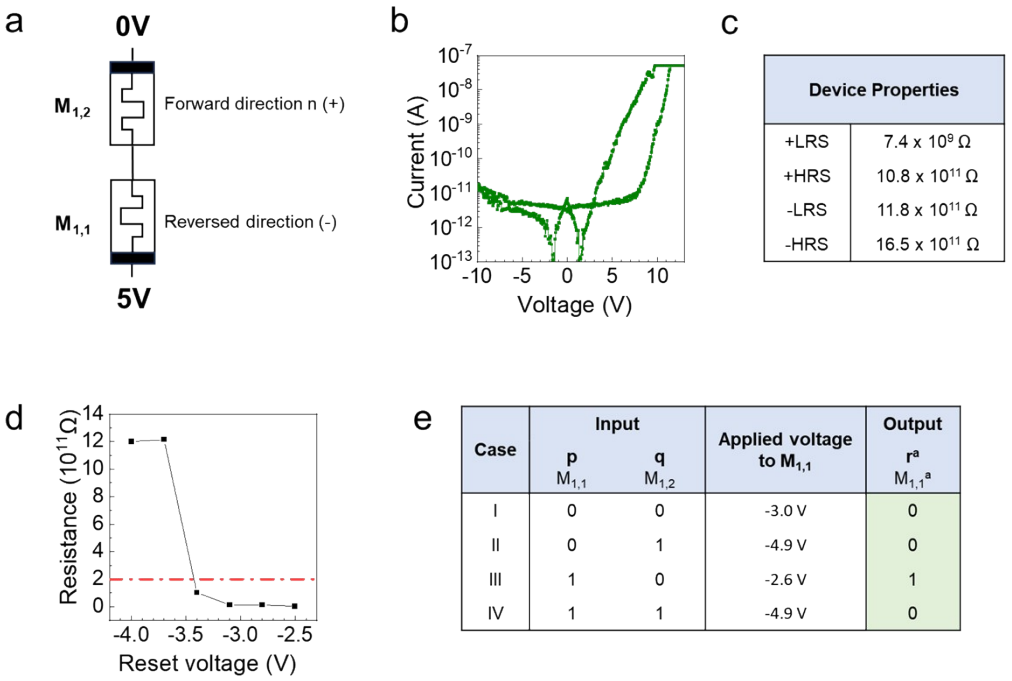
The key generation method utilizes the distribution of HRS to generate the random key, and the voltage division provides the reference line along with the applied bias to select the keys to have a certain probability of '1' and '0'. If the D-to-D variation is insufficient compared to the C-to-C variation, it affects the accuracy drop in the key generation. However, this work shows sufficient D-to-D variation due to the process variation of V-RRAM. The D-t-D variations in the V-RRAM arrays (CoV = 0.33, 0.41, and 0.34 for the first, second, and third layers) are significantly larger than the C-t-C variations (CoV = 0.008), enabling a reliable and concealable PUF key generation. Figure S8 shows the changes in the V_{SKEW} distribution of the selected devices over 10 cycles of conceal and reveal for PUF 4 While the distribution exhibits slight variations due to the C-t-C variations in HRS and V_{SET}, these shifts are negligible compared to D-t-D variations, confirming that the selected key remains consistent.



b

Case	Input		Output
	p $M_{1,1}$	q $M_{1,2}$	r_a $M_{1,1,a}$
I	0	0	0
II	0	1	0
III	1	0	1
IV	1	1	0

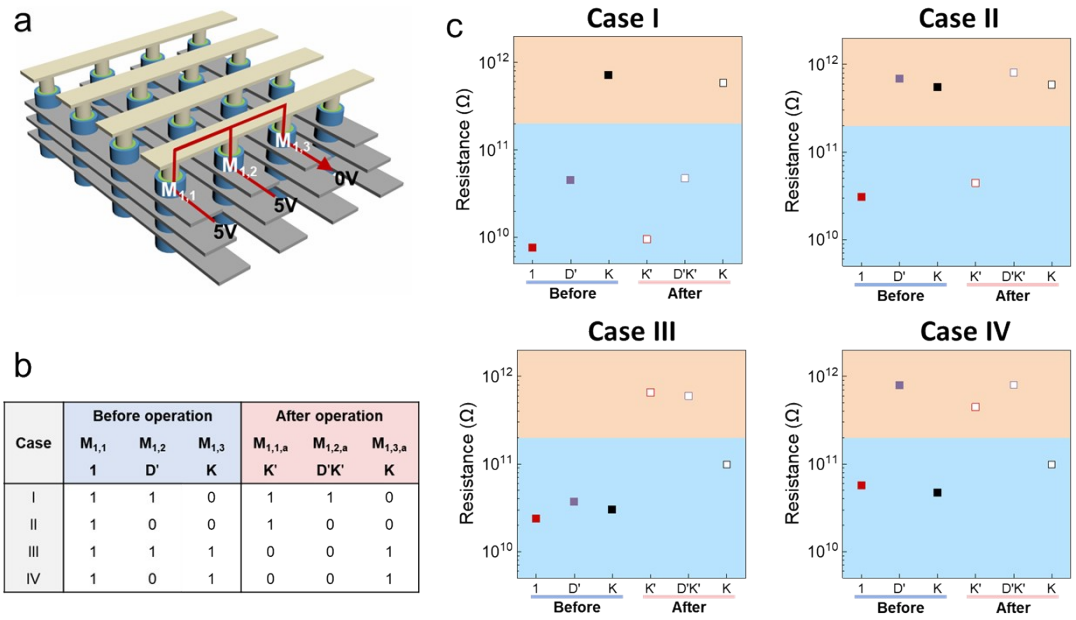
Fig. S9 | **Demonstration of the NIMP operations**. (a) The bias configuration in the schematic diagram of V-RRAM. (b) The truth table of the NIMP logic gate. A resistance larger than 200GΩ is encoded to "1". (c) The results of the NIMP operation in $M_{1,1}$ for each input case. The results were obtained by conducting 12 measurements for each case.



e

Case	Input p $M_{1,1}$	Input q $M_{1,2}$	Applied voltage to $M_{1,1}$	Output r^a $M_{1,1}{}^a$
I	0	0	-3.0 V	0
II	0	1	-4.9 V	0
III	1	0	-2.6 V	1
IV	1	1	-4.9 V	0

Fig. S10 | **Details about NIMP operation.** (a) Anti-serial configuration during NIMP operation. (b) Representative I-V curve of the V-RRAM device. I_{cc} was set to 50 nA. (c) Device properties of V-RRAM device. (d) The resistance state of the V-RRAM device according to applied reset voltage. The reset occurs abruptly around -3.7 V. (e) The voltage applied to M1,1,t in the reverse direction for each case during the NIMP operation, resulting from voltage division. Therefore, $M_{1,1,t}$ can only maintain LRS in Case 3



b

Case	Before operation			After operation		
	$M_{1,1}$	$M_{1,2}$	$M_{1,3}$	$M_{1,1,a}$	$M_{1,2,a}$	$M_{1,3,a}$
	1	D'	K	K'	D'K'	K
I	1	1	0	1	1	0
II	1	0	0	1	0	0
III	1	1	1	0	0	1
IV	1	0	1	0	0	1

Fig. S11 | Parallel NIMP operation simultaneously conducted on two devices. (a) The bias configuration in the schematic diagram of V-RRAM. (b) The truth table of the Parallel NIMP operation. (c) The results of the parallel NIMP operation in $M_{1,1}$ and $M_{1,2}$ for each input case. The initial state of $M_{1,1}$ is always '1', as in the case of XOR encryption. The initial states of $M_{1,2}$ and $M_{1,3}$ represent D' and K, respectively.

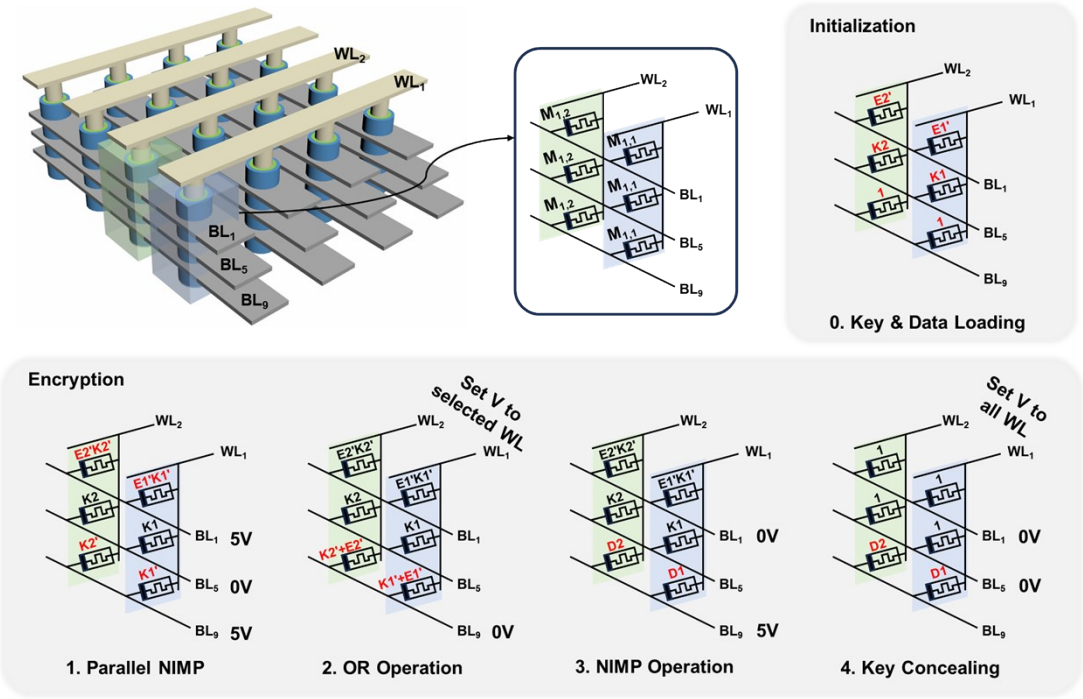


Fig. S12 | **Schematic diagram of the combination of NIMP and OR Operations for the XOR decryption process. E', K, and D represent the inversion of encrypted data, generated key, and original data.**

Decryption is conducted in the same manner as encryption, utilizing a combination of two NIMP operations and an OR operation to execute parallel XOR operations. The primary distinction lies in the data loading step, where, instead of loading the inversion of data onto the third layer, the inversion of encrypted data is loaded onto the third layer via a peripheral circuit. The generated key is loaded onto the second layer, and the devices on the first layer are initialized to '1' (LRS), consistent with the encryption process.

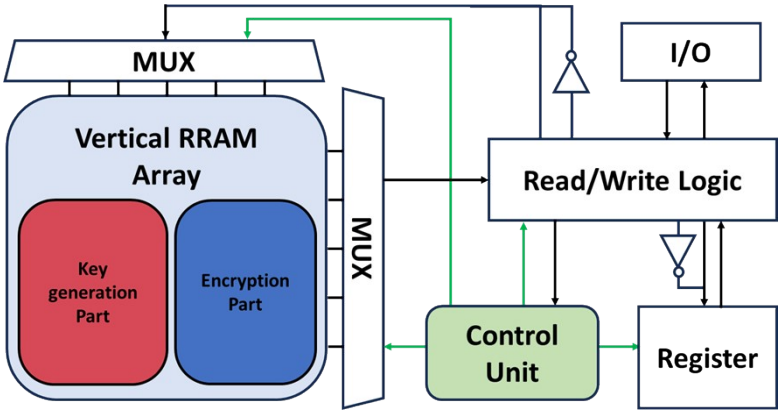


Fig. S13 | In-memory key generation and encryption/decryption system