Supplementary Information (SI) for Nanoscale.

Supplementary Materials for

Asymmetric cryptography enabled by TaO_x-Based complementary memristors with tunable pulse dynamics

Yunlai Zhu [1], Xiaoling Wu [1], Junjie Zhang [1], Hao Chen [1], Shuhao Rao [1], Junjie Yan [1], Xi Sun [1], Yongjie Zhao [1], Ying Zhu [1], Liang Yao[1], Zuyu Xu [1], Zuheng Wu [1]*, and Yuehua Dai [1]*

[1] School of Integrated Circuits, Anhui University, Hefei, Anhui, 230601, China.

Corresponding Authors

*E-mail: wuzuheng@ahu.edu.cn (Z.-H. Wu), daiyuehua@ahu.edu.cn (Y.-H. Dai)

S1. Device Modeling Methodology.

In this work, a modeling methodology proposed by Saludes-Tapia et al. for complementary resistive switching (CRS) devices was adopted [1]. The CRS behavior is represented through a six-terminal subcircuit: the terminals "+, c, –" reproduce the device's current-voltage (I–V) characteristics and provide access to the central node voltage, while the additional "G+, G–, G" terminals output the low-bias conductances of the two individual memdiodes and the complete CRS device, respectively. This design enables the reconstruction of the characteristic "table-with-legs" resistance-voltage (R–V) curve, allowing direct comparison with experimental data for parameter calibration.

Within the subcircuit (**Figure S1**), each memdiode is modeled using the Quasi-static Memdiode Model (QMM). The instantaneous current follows the transport relation:

$$I(V) = I_0(\lambda) sinh\{\alpha(\lambda)[V - (R_s(\lambda) + R_i)I]\}$$

where $I_0(\lambda)$, $\alpha(\lambda)$ and the state-dependent resistance $R_s(\lambda)$ define the current amplitude and the low-bias conductance for different resistance states. The constant series resistance R_i sets the load-line slope and adjusts the amplitude of the snapback effect.

The state variable λ evolves under the control voltage:

$$V_c = V - R_i I$$

with its dynamics governed by recursive ridge functions that describe the SET and RESET processes. The parameters η_S, $\eta_R$determine the switching rates, while V_S, and V_R define the threshold voltages. The threshold current I_{SB} triggers the snapback transition during SET, and the factor γ accounts for the snapforward effect during RESET.

With these elements, the model is able to reproduce both abrupt (digital-like) and gradual (analog-like) CRS switching behaviors. The influence of model parameters on CRS device behavior are summarized in **Table S1**. It has been validated through successful application to symmetric TaOx-based CRS devices [2], demonstrating its capability to capture full *I–V* hysteresis loops and the low-bias "table-with-legs" characteristics essential for device analysis and optimization.

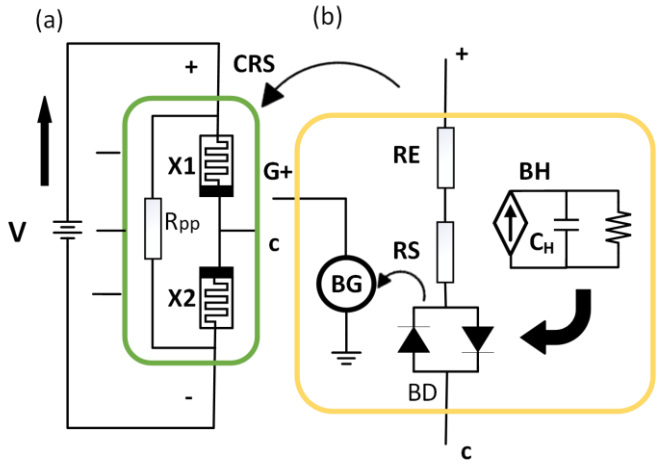

Figure S1. Schematic circuit for (a) the CRS structure consisting of two memdiodes (X1 and X2) anti-serially connected. The CRS model consists of a six-port subcircuit: three for the I-V characteristics. Thanks to the accessible central terminal, the subcircuit allows representing the curves of the individual RS devices and the CRS device; three terminals are useful for obtaining the conductance of each device in the CRS structure, and the total conductance; (b) internal implementation of the QMM for the X1 memdiode.

Table S1. Model parameters and influence

Parameter	Definition	Role/Influence on Model Behavior
$I_0(\lambda)$	Current amplitude factor dependent on state λ	Sets the baseline current and low-bias conductance.
$\alpha(\lambda)$	State-dependent nonlinearity factor	Controls I − V steepness at medium/high bias.
$Rs(\lambda)$	State-dependent resistance	Determines ON/OFF ratio and readout current.
R_i	Constant series resistance	Tunes load-line slope and snapback magnitude.
V_s	SET threshold voltage	Defines the onset of the SET transition.
V_R	RESET threshold voltage	Defines the onset of the RESET transition.
η_S	SET rate parameter	Controls sharpness of the SET edge.
η_R	RESET rate parameter	Controls slope of the RESET edge.
I_{SB}	Snapback trigger current	Triggers abrupt SET snapback.
γ	Snapforward control factor	Modulates residual current in RESET.
$\alpha_{min}/\alpha_{max}$	Limits of α(λ)	Constrain nonlinearity range.
I_{min}/I_{max}	Limits of $I_0(\lambda)$	Constrain current amplitude range.
R_{Smin}/R_{Smax}	Limits of $R_S(\lambda)$	Constrain resistance range.

S2. Noise tolerance of the CRS device.

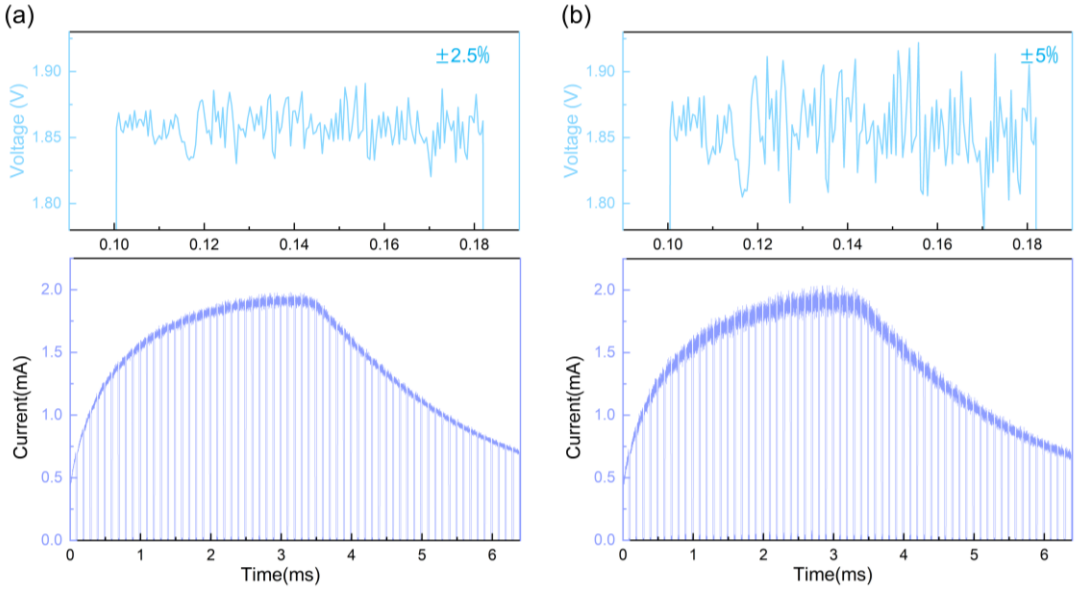

Figure S2. The response characteristics of the CRS device under (a)2.5% noise and (b)5% noise within which the input is 1.86 V.

S3. Reversibility and repeatability of LTP/LTD behavior.

To ensure reproducible switching behavior, we simulated and controlled the oxygen vacancy (Vo) distribution through the application of a negative bias voltage. Specifically, after completing one long-term potentiation/depression (LTP/LTD) cycle using 64 positive pulses (amplitude: 1.86 V, T_{on} = 82 μs, T_{period} = 100 μs), we applied 64 reverse pulses at different amplitudes (–2.5 V, –3.0 V, and –3.5 V) using identical pulse width and period parameters. This procedure was successfully repeated over five full cycles (see **Figure S3**). The results demonstrate that when an insufficient reverse bias is applied, oxygen vacancies cannot completely return to their initial depletion region. This leads to premature turn-on in subsequent cycles and a leftward shift of the current peak—behavior that is undesirable for the proposed encryption scheme. Only when a sufficiently large reverse bias is applied (–3.5 V in this case) can the device be fully recovered to its initial state, thereby ensuring reliable repetition of the LTP/LTD process. In summary, according to the Vo-based conductive filament (CF) model, CRS devices can be consistently reinitialized by applying a sufficiently large reverse voltage after a sequence of same-polarity excitations. This confirms that the proposed LTP/LTD process is not a one-time phenomenon but a stable and repeatable operation, which is essential for the feasibility and practicality of the encryption scheme. We note that no Monte-Carlo or process-variation simulations were performed; this section solely demonstrates bias-dependent recovery and device repeatability, not statistical variability.

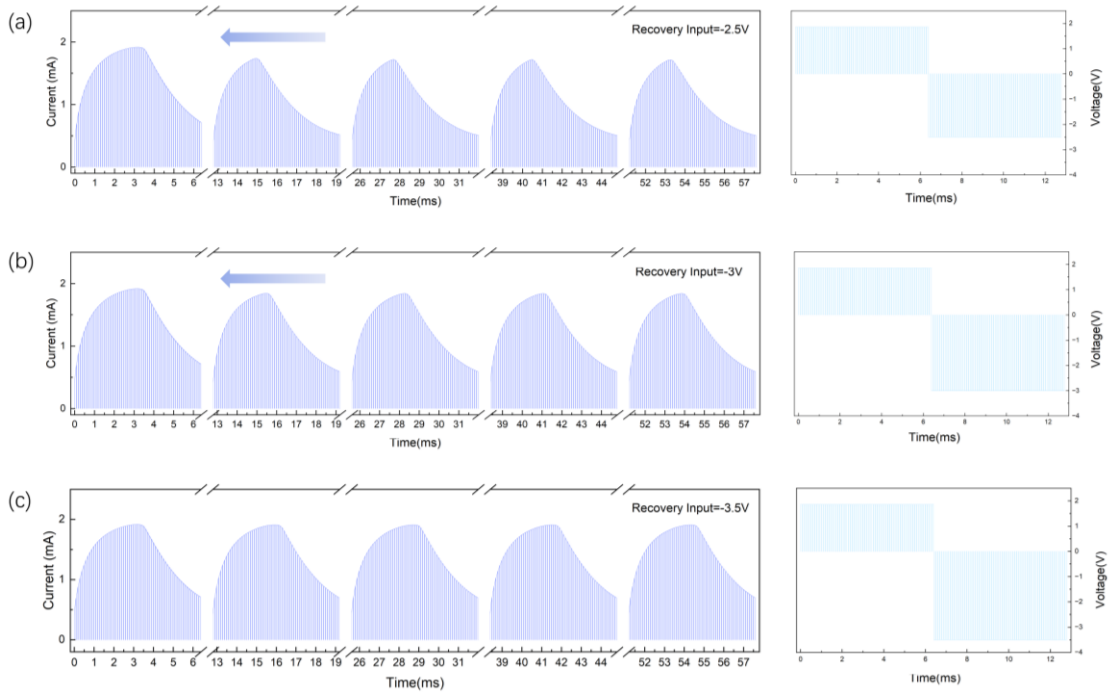

Figure S3. The output current values after five cycles of continuously applying a forward driving voltage and reverse recovery input voltages of (a) -2.5 V, (b) -3 V, and (c) -3.5 V.

S4. Illustration of the encryption and decryption process.

As shown in **Figure S4**, the encryption process begins with the sender initializing the device to the plaintext state (denoted as C1, corresponding to a predefined conductance level). The sender then applies a predefined public-key pulse sequence to transition the device to the ciphertext state (denoted as C2), after which it is transmitted in this ciphertext form. Although the public key is fixed and publicly known, the transformation rule linking public and private keys remains concealed. Without knowledge of this rule, a third party cannot determine the required number of private-key pulses, thus cannot revert the device to its original plaintext state.

During decryption, the receiver—who maintains a local reference of 64 valid conductance states (see **Table S2**) —first acquires the device in state C2. Upon receiving the device in the ciphertext state, the receiver, knowing the number of public-key pulses applied, can deduce the plaintext conductance index C1 (C1 = C2 − public-key pulse number). Based on the definition given in Equation (1), the corresponding private-key pulse number can then be determined. Finally, applying this private key sequence restores the device to its original plaintext state, C1, completing the decryption process.

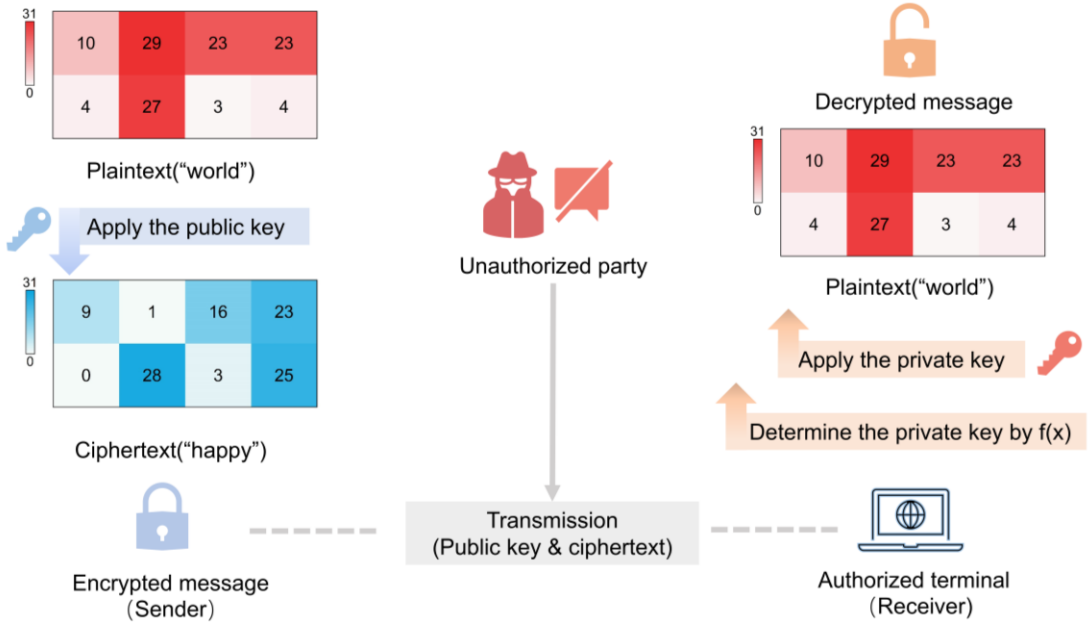

Figure S4. Schematic illustration of the encryption and decryption process.

Table S2. Conductance mapping rules

LTP Process				LTD Process			
No.	Current (mA)	No.	Current (mA)	No.	Current (mA)	No.	Current (mA)
0	0.6896	16	1.7679	32(31)	1.9136	48(15)	1.1658
1	0.8791	17	1.7876	33(30)	1.9061	49(14)	1.1247
2	1.0242	18	1.8056	34(29)	1.8879	50(13)	1.0852
3	1.1410	19	1.8218	35(28)	1.8477	51(12)	1.0474
4	1.2380	20	1.8365	36(27)	1.7905	52(11)	1.0111
5	1.3200	21	1.8498	37(26)	1.7313	53(10)	0.9766
6	1.3905	22	1.8619	38(25)	1.6731	54(9)	0.9435
7	1.4517	23	1.8726	39(24)	1.6155	55(8)	0.9120
8	1.5053	24	1.8823	40(23)	1.5583	56(7)	0.8819
9	1.5525	25	1.8908	41(22)	1.5029	57(6)	0.8533
10	1.5944	26	1.8982	42(21)	1.4494	58(5)	0.8261
11	1.6317	27	1.9045	43(20)	1.3977	59(4)	0.8003
12	1.6650	28	1.9096	44(19)	1.3477	60(3)	0.7758
13	1.6949	29	1.9135	45(18)	1.2996	61(2)	0.7526
14	1.7217	30	1.9158	46(17)	1.2533	62(1)	0.7306
15	1.7460	31	1.9161	47(16)	1.2087	63(0)	0.7098

S5. Image authentication process based on hash algorithm.

The identity authentication workflow operates as follows. The sender first appends the public key to the original message to form the target message and applies the SHA-256 hash function to generate a unique 256-bit MAC address. The public key serves as the identity (ID), while the resulting MAC address is stored as the verifier's registered response. As illustrated in **Figure S5(a)**, successful authentication occurs when the decrypted message yields a MAC identical to the registered value. Conversely, any inconsistency in either the message content or the cryptographic key leads to a different MAC address and authentication failure (**Figure S5(b) and (c)**). This process demonstrates how the combination of public-key cryptography and cryptographic hash functions ensures both the integrity and authenticity of transmitted information.

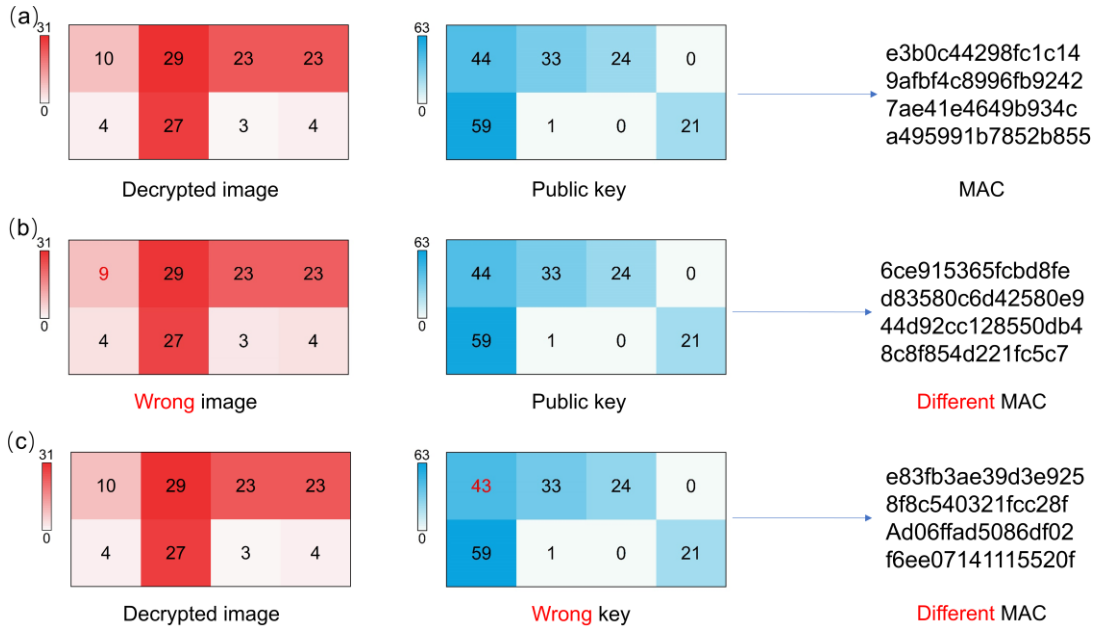

Figure S5. (a) Valid decrypted data and matching public key yield identical MAC, ensuring authentication success. (b) Wrong image or (c) wrong public key produces different MAC, resulting in authentication being denied.

REFERENCES

[1] Saludes-Tapia, M.; Gonzalez, M. B.; Campabadal, F.; Suñé, J.; Miranda, E. SPICE Model for Complementary Resistive Switching Devices Based on Anti-Serially Connected Quasi-Static Memdiodes. *Solid-State Electron.* **2022**, *194*, 108312. https://doi.org/10.1016/j.sse.2022.108312.

[2] Yang, Y.; Sheridan, P.; Lu, W. Complementary Resistive Switching in Tantalum Oxide-Based Resistive Memory Devices. *Appl. Phys. Lett.* **2012**, *100* (20), 203112. https://doi.org/10.1063/1.4719198.