A Concealable RRAM Physical Unclonable Function Compatible with In-Memory Computing

Jiang Li*, Yijun Cui*, Chenghua Wang*, Weiqiang Liu*, and Shahar Kvatinsky†
* *Nanjing University of Aeronautics and Astronautics, Nanjing, China*
† *Technion - Israel Institute of Technology, Haifa, Israel.*
Email: yijun.cui@nuaa.edu.cn and liuweiqiang@nuaa.edu.cn

***Abstract*—Resistive random access memory (RRAM) has been widely used in physical unclonable function (PUF) design due to its low power consumption, fast read/write speed, and significant intrinsic randomness. However, existing RRAM PUFs cannot overcome the cycle-to-cycle (C2C) variations of RRAM, leading to poor reproducibility of PUF keys across cycles. Most prior designs directly store PUF keys in RRAMs, increasing vulnerability to attacks. In this paper, we propose a concealable RRAM PUF based on an RRAM crossbar array, utilizing the differential resistive switching characteristics of two RRAMs to generate keys. By enabling the reproducibility of PUF keys across cycles, a concealment scheme is proposed to prevent the exposure of PUF keys, thus enhancing the security of the RRAM PUF. Through post-processing operations, the proposed PUF exhibits high reliability over ±10% VDD and a wide temperature range from 248K to 373K. Furthermore, this RRAM PUF is compatible with in-memory computing (IMC), and they can be implemented using the same RRAM crossbar array.**

***Index Terms*—Resistive random access memory, physical unclonable function, concealable, in-memory computing**

I. Introduction

Resistive random access memory (RRAM), featuring low power consumption and high density, has found wide applications in various fields, including embedded systems, data storage, artificial intelligence, and edge computing [1]. In-memory computing (IMC) based on RRAM crossbar arrays aims to overcome the "memory wall" bottleneck of the von Neumann architecture [2]. While the intrinsic randomness of RRAM poses challenges for its large-scale commercial applications, this randomness makes it highly suitable for hardware security applications [3]. RRAM-based physical uncolnable function (PUF) design is one of the most promising hardware security primitives [4]. PUFs extract random errors introduced during the manufacturing process of a chip to generate unique keys, which can be used for key generation and device authentication. Even if an adversary replicates the PUF circuit under the same manufacturing conditions, obtaining the same key is practically impossible.

The development of attack methods poses a great threat to existing security systems. Despite the high security of PUFs, physical attacks such as micro-probing and side channel analysis could still steal sensitive information from PUFs. This threat arises from the fixed structure of PUFs and the physical accessibility of their data. CMOS-based PUF designs extract process variations or mismatches between transistors, but these PUF keys cannot be concealable and become irreversibly exposed. To enhance PUF security, probe detection circuits or redundant circuits are employed [5]. However, these additional circuits significantly increase the area and power consumption.

Due to the intrinsic stochasticity, various random sources in RRAM, such as randomness in the state switching delay [6], probabilistic switching [7], and randomness in the resistance distribution [4], [8], are used to implement PUFs. However, most designs store PUF keys in the resistive state of RRAMs, using high resistance state (HRS) and low resistance state (LRS) to represent the keys "0" and "1", respectively, which results in the key always being exposed. An adversary can use a probe to directly access the keys, thereby compromising the security of these PUFs. These PUFs do not comply with the characteristics of online key generation. Furthermore, while IMC has similarities to RRAM-based PUF since it also uses RRAM arrays to compute data in-place, IMC is usually incompatible with PUFs and cannot be implemented on an array due to the non-reproducibility of PUF keys across cycles.

In this paper, we propose a concealable RRAM PUF. Due to the differences in the formation of conductive filaments, when applying a parallel SET operation on two RRAMs in a HRS, one of them will switch to a LRS first, while the other device remains in HRS, generating an unpredictable PUF key. Importantly, this process can be repeatedly achieved in continuous parallel SET operations. Consequently, PUF keys can be successfully concealed by resetting all RRAMs to HRS and efficiently recovered by subsequent parallel SET operations, preventing the risk of being directly accessed. We tested the proposed PUF using an RRAM crossbar array fabricated using Winbond's 90nm technology, and experimentally demonstrated its excellent concealability as well as the high reliability. Furthermore, the proposed RRAM PUF can be implemented on the same array as IMC, demonstrating high compatibility and reducing hardware overhead.

II. Concealable RRAM PUF Design

A. Entropy Source in RRAM

The TiN/HfO_2/Ti/TiN RRAM devices [9] are fabricated and used in the measurements. Fig. 1 shows the typical resistive

This work was supported by grants from Natural Science Foundation of Jiangsu Province (BK20210287), National Natural Science Foundation of China (62104107, 62022041, 62134002) and NSF-BSF (2020-613).

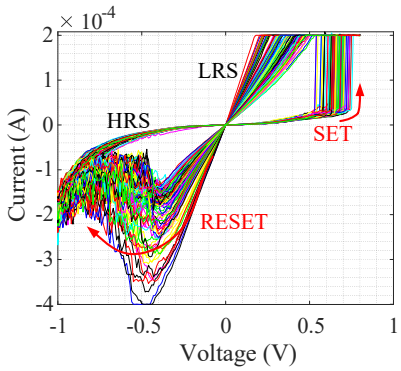


Fig. 1: Resistive switching characteristic of a TiN/HfO_2/Ti/TiN RRAM under DC conditions over 100 cycles with successive RESET and SET operations measured using the fabricated RRAM devices.

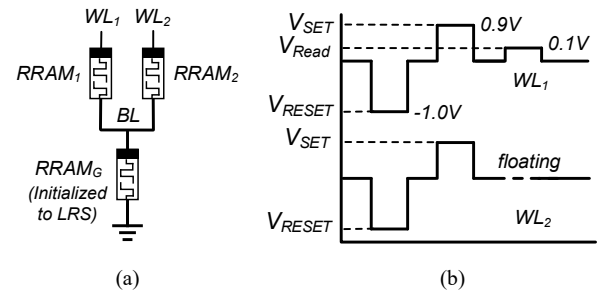


Fig. 2: (a) Schematic of the proposed RRAM PUF cell including two parallel RRAMs and a grounded RRAM. (b) Diagram of voltage pulses to generate PUF keys.

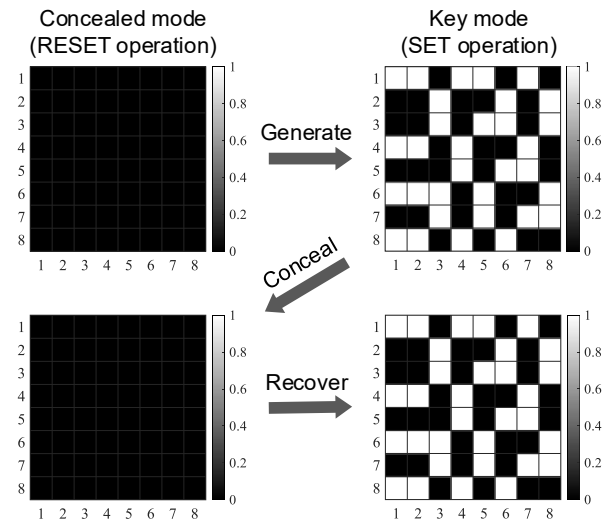


Fig. 3: Concealable scheme of the proposed RRAM PUF, including concealed mode and key mode. With the SET and RESET operation, the proposed PUF can be easily changed between the two modes.

switching characteristic of an RRAM, collecting the I-V curves of an RRAM over 100 cycles under DC conditions. RRAM has two resistive states: HRS and LRS, respectively. When the applied voltage exceeds the forward or reverse thresholds, the RRAM will switch its state. The operation of switching from HRS to LRS is commonly referred to as SET, while the reverse process from LRS to HRS is known as RESET. The forward and reverse threshold voltages of the RRAM are approximately 0.65V and -0.85V, respectively. In different cycles, the RRAM experiences random variations in HRS and LRS resistances, as well as in the threshold voltages. The resistance of the RRAM is determined by the internal conductive filament's morphology and structure. The formation and rupture of these filaments occur randomly and independently in each RRAM, and even in a single RRAM. Therefore, there are significant cycle-to-cycle (C2C) and device-to-device (D2D) variations in RRAM.

B. Concealable RRAM PUF Design

From Fig. 1, it can be observed that the RESET process of RRAM is gradual, while the SET process is abrupt. Therefore, due to D2D variations, when parallel SET operation is applied to two RRAMs in the HRS, one of the RRAMs will switch to LRS first. At this point, if the applied voltage is powered off, one of the two RRAMs is in LRS, while the other device remains in HRS. In different cells, which RRAM will switch to LRS is random and unpredictable, making this behavior a randomness source for PUF. The proposed concealable RRAM PUF is shown in Fig. 2(a). Two RRAMs are connected in parallel and jointly connected to a ground RRAM $RRAM_G$, initialized to LRS. A voltage pulse sequence is applied to WL_1 and WL_2 to generate a PUF key, as depicted in Fig. 2(b). First, both RRAMs are reset to HRS, and then a parallel SET operation is applied. Due to intrinsic process variations, one RRAM will switch to LRS first. At this time, the voltage at the BL node rises due to the voltage divider with $RRAM_G$, which prevents the switching of the resistive state of the other RRAM. PUF key generation is achieved by reading the resistance state of RRAM1. If $RRAM_1$ is in LRS, the PUF key is "1"; otherwise, it is "0".

Importantly, this behavior is repeatable as D2D variation is more dominant in the parallel SET process than C2C variation. During the subsequent parallel SET operations, only the RRAM that had previously performed the state switching will switch to LRS (to be verified in Section III-A), while the other RRAM will always remain in HRS. Based on this property, we propose a concealable scheme, as shown in Fig. 3. The proposed RRAM PUF has two modes: concealed mode and key mode. After a parallel SET operation, the PUF switches to key mode, and the PUF key can be read out directly. When there is no need to use the PUF key, RESET operation is applied to all RRAMs and the PUF switches to concealed mode. All RRAMs are in HRS, and the PUF key is concealed. Subsequently, the PUF key can be easily recovered by a parallel SET operation. Conversely, traditional PUFs have their keys constantly exposed. If an adversary gains direct access to the chip, they can use probing and analysis methods

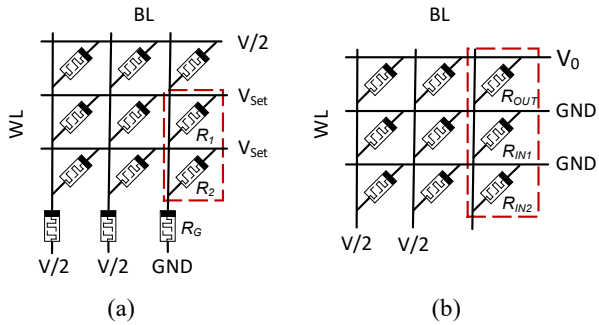


Fig. 4: (a) Implementation of the proposed PUF on RRAM crossbar array. (b) Implementation of MAGIC OR gate on RRAM crossbar array. IN1 and IN2 are the gate inputs, OUT is the gate output that is initialized to HRS.

to obtain the key. The proposed concealable PUF generally remains in concealed mode. Even if adversaries can steal PUF information unhindered, they cannot obtain the correct key.

C. Compatibility with In-memory Computing (IMC)

Due to the concealable and recoverable property of the proposed PUF, the RRAM crossbar array can conceal the PUF key when the PUF key is not needed and can be used for other purposes, such as IMC. The compatibility design of the proposed PUF with IMC is shown in Fig. 4. By using selectors, bitlines (BLs) can be connected either to the grounded RRAM or to the source. All read-and-write operations adopt the V/2 scheme to enhance reliability. When implementing a PUF, the BL is connected to the ground RRAM (R_G), as shown in Fig. 4(a). By applying V_{SET} to the two selected wordlines (WLs) and grounding the corresponding R_G, a parallel SET operation can be performed to generate a PUF key.

Theoretically, all in-memory logic computations, including the stateful logic family and non-stateful logic family [10], can be implemented. As an example, the implementation of the memristor-assisted logic (MAGIC) OR gate is shown in Fig. 4(b), and the other logics are implemented similarly. During the IMC, the BL is connected to the source. V_0 is applied to one WL, while the other two WLs are grounded. R_{IN1} and R_{IN2} are the inputs of the OR gate, and R_{OUT} is the output. In this work, HRS and LRS represent, respectively, logic "0" and "1". Before the logic operation, R_{OUT} is initialized to HRS. When both inputs, IN1 and IN2, are "0", the voltage across R_{OUT} is approximately $\frac{2}{3}V_0$, and its state should remain at logic "0". When there is a "1" in either of the inputs, the voltage on R_{OUT} is approximately V_0, and its state should switch to logic "1". Therefore, to correctly implement the OR logic, V_0 should fulfill the following condition:

$$V_{SET} < V_0 < 1.5V_{SET}, \tag{1}$$

When R_{OUT} is switched from logic "0" to logic "1", the voltage across R_{IN} is insufficient to change the state of R_{IN1}, thus ensuring the stability of the operation.

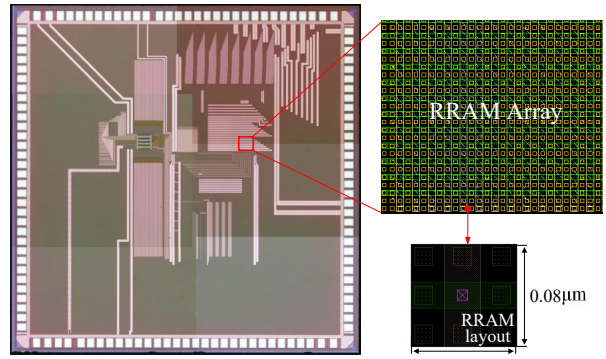


Fig. 5: Top view of the chip micrograph and the layout of an RRAM crossbar array, fabricated using Winbond's 90nm HfO_2 RRAM technology.

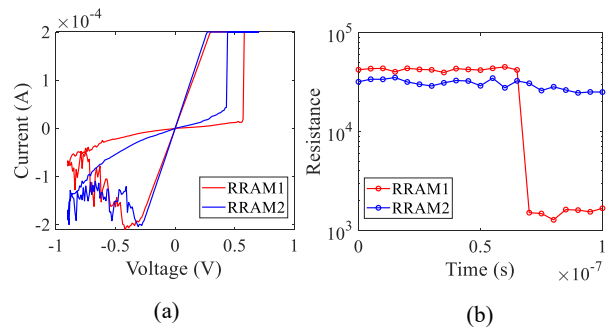


Fig. 6: (a) Resistive switching characteristics of two RRAMs in a PUF cell. (b) State transient switching of the two RRAMs during a parallel SET operation.

III. Experimental Results

To experimentally validate the proposed RRAM PUF, RRAM devices were fabricated using Winbond's 90nm HfO_2 RRAM technology [9], with a cell size of 0.08μm×0.08μm, as shown in Fig. 5. The HfO_2-based Transition-Metal-Oxide (TMO) stack has top and bottom electrodes of TiN and Ti/TiN conventional metals, respectively. The TMO is deposited using the conventional ALD technique. The RRAM devices exhibit high reliability with a million-cycle endurance and can operate at temperatures as high as 150$C°$, while also boasting a state retention capability of over 100 years, ensuring the reliability of the PUF. The electrical characteristics of the devices and the performance of the PUF were measured using a Keysight B1500A Semiconductor Device Analyzer and a SUMMIT 12000 Probe Station. A PUF has several important metrics including uniformity, uniqueness and reliability [11], which were used to assess the performance of the proposed PUF.

A. Functional Verification of the Proposed RRAM PUF

Fig. 6 shows the experimental results for a single PUF cell. Fig. 6(a) shows the resistive switching characteristics of two RRAM devices in the PUF cell. Their threshold voltages and the resistance values of HRS and LRS are different, although the SET process is abrupt for both devices. The state switching

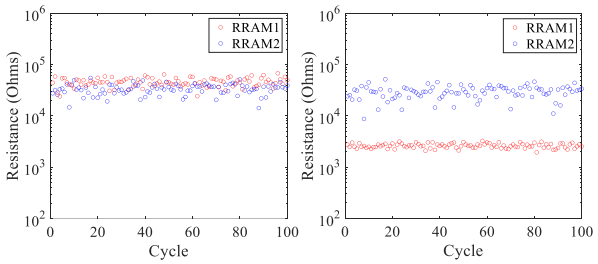


Fig. 7: (a) Initial resistances of the two RRAM devices in successive 100 cycles. (b) State switching of the two RRAMs after successive parallel SET operations in 100 cycles.

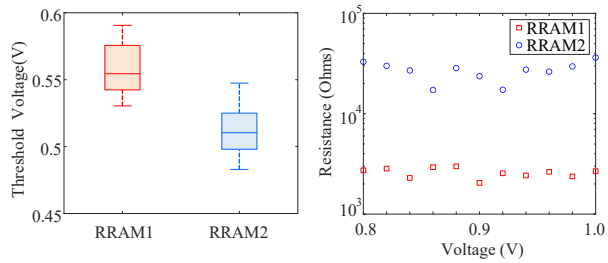


Fig. 8: (a) Threshold voltages of SET operation obtained in 50 cycles during DC characterization of the two RRAMs. (b) Average resistances of the two RRAMs after parallel SET operations with different SET voltage, where 50 cycles were considered.

of the two RRAMs during a parallel SET operation is shown in Fig. 6(b), with an interval of 5 ns for each measurement point. Initially, both RRAM1 and RRAM2 are in the HRS, and the resistance of RRAM1 is higher than that of RRAM2. After applying a parallel SET operation, RRAM1 switches to the LRS at approximately 65 ns, while the resistance of RRAM2 slightly decreases but remains in the HRS. The difference between the resistances of the two RRAM devices is greater than 10 times, providing a high readout margin.

The output of this PUF cell in different cycles is shown in Fig. 7. The two RRAM devices are initialized to HRS. Fig. 7(a) shows significant variations in the resistance of both devices in the HRS over different cycles, and there is a crossover of their HRS resistances. The resistive state switching after applying a parallel SET operation is shown in Fig. 7(b). In 100 cycles, RRAM1 switches the resistance state, while RRAM2 consistently maintains the HRS, demonstrating the excellent concealability of the proposed PUF over cycles. Due to the large C2C variations in RRAM, the HRS resistance of RRAM2 is lower in some cycles, resulting in a decrease in the resistance ratio of the two RRAMs.

Additionally, the effect of the SET threshold voltage and the pulse voltage of the parallel SET operation on the PUF key is explored. Fig. 8(a) shows the distribution of SET threshold voltages of two RRAMs over 50 DC scan cycles. The SET threshold voltage of RRAM1 is slightly higher than that of RRAM2, and there is an overlap in their SET threshold voltages. The output of the PUF is shown in Fig. 8(b) by varying the pulse voltage of the parallel SET operation with 0.02V steps in the range of 0.8V to 1V. 50 cycles were measured at each voltage and the average resistance of the two RRAMs was determined. The resistance difference between the two RRAMs is significant. Therefore, the PUF has a stable output over the range of applied voltages, indicating that the PUF key is independent of the pulse voltage of the parallel SET operation. Furthermore, the variation of the threshold voltage of RRAMs has no effect on the reliability of the PUF.

B. Uniformity and Uniqueness

Uniformity is used to evaluate the proportion of "0" and "1" in PUF keys. An ideal PUF should generate keys with

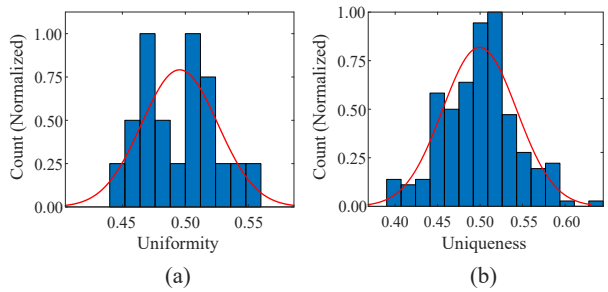


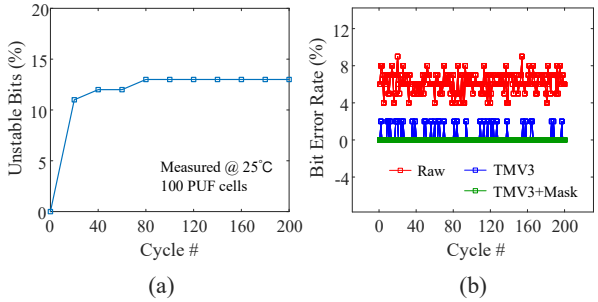
Fig. 9: (a) Uniformity of the proposed PUF for 20 chips with 128-bit keys. (b) Uniqueness of the proposed PUF for 20 chips with 128-bit keys.

a proportion of 50% of both "0" and "1". Any bias in the PUF key can decrease security. Collecting 128-bit keys from each of 20 chips, Fig. 9(a) shows the uniformity results of the proposed PUF. The uniformity of this PUF is 49.55%, with a maximum deviation of 5.47%.

Uniqueness measures the difference between the keys of two PUF chips, indicating the PUF's ability to distinguish a particular chip from other chips. The ideal value of uniqueness is 0.5. Fig. 9(b) shows the uniqueness result of the proposed PUF. This PUF achieves a high uniqueness of 0.4994 with a standard deviation of 0.0019, which is close to the ideal value. Therefore, the proposed PUF provides good uniformity and uniqueness.

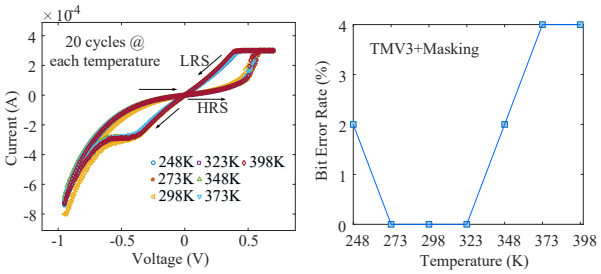
C. Reliability

Reliability is determined by assessing the reproducibility of the PUF key under different environmental conditions, such as varying voltages and temperatures. It can be quantified using the bit error rate (BER). An ideal PUF should be able to regenerate the key regardless of the conditions, and the BER should be 0. However, due to C2C variations and sensitivity to temperature, the reliability of RRAM PUFs is not ideal. To evaluate the reliability of the proposed RRAM PUF, both the unstable bits and the bit error rate are measured, represent the ratio of unstable bits with the output flipped at least once in different cycles, and the bit error rate of the current cycle. Fig.



(a) (b)

Fig. 10: (a) Measured unstable bits of 100 PUF cells in 200 cycles under normal condition. (b) Measured BER of 100 PUF cells in 200 cycles with different post-processing methods.



(a) (b)

Fig. 11: (a) Effect of temperature from 248K to 373K on the resistive switching characteristics. 20 cycles were measured at each temperature. (b) Measured BER of 100 PUF cells at various temperature, with 298K as the reference standard.

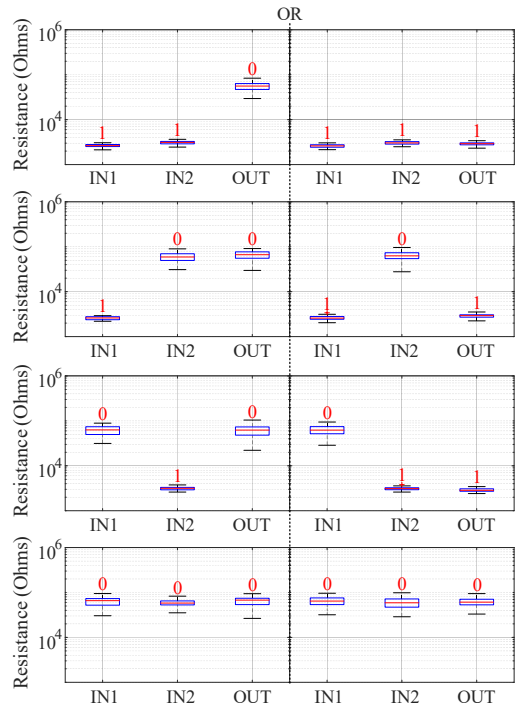


Fig. 12: Results of 50 cycles of MAGIC OR operation measured on the RRAM crossbar array. The results show correct logic operation and exhibit output stability.

10(a) shows the unstable bits in 100 PUF cells over 200 cycles under normal conditions (298K, 0.9V), demonstrating that 13% of the PUF cells have unstable keys. Additionally, Fig. 10(b) presents the BER of these 100 PUF cells over different cycles. The raw PUF keys show a BER of approximately 6%, which is due to the C2C variation of the RRAM. If two RRAMs in a PUF cell have similar switching capabilities, the C2C variation may cause bit flips. To enhance reliability, post-processing techniques such as temporal majority voting (TMV) and masking [12] are necessary. TMVx utilizes adjacent x PUF cells to generate a 1-bit key, so even with unstable PUF cells, reliable keys can still be generated. The masking technique improves reliability by masking out highly unstable PUF bits. In this work, TMV3 and masking (2% of bits) techniques are employed, and the BER is significantly reduced. During 200 cycles, the BER of these 100 PUF cells is 0. It is worth pointing out that when the number of PUF keys is increased, unstable bits may still occur. It can be improved by employing more sophisticated voting and higher masking rates.

The reliability of the proposed PUF under different environmental conditions was also measured. As shown in Fig. 8(b), the PUF key does not change with the variation of supply voltage. Next, we measured the reliability of the PUF at different temperatures. Fig. 11(a) shows the variation of the resistive switching characteristics of an RRAM over the temperature range of 248K to 373K. 20 cycles were measured at each temperature. The characteristic of RRAM shows no significant variation with temperature, while C2C variations are more significant than the effect of temperature. The BER of the proposed PUF at different temperatures is shown in Fig. 11(b) with 298K as the normal condition. There is no bit flip in the range of 273K to 323K. However, the BER of the PUF increases as the temperature decreases or increases further. At 373K, the PUF reaches the highest BER of 4%. This indicates that the switching capability of RRAM varies with temperature. When there is a significant temperature change, the PUF key may become unstable, which is an inevitable issue for RRAM PUFs. Some auxiliary strategies can be employed to enhance the reliability of RRAM PUFs against temperature, such as the multiple reference response scheme [13], which reduces sensitivity to temperature by enrolling multiple PUF responses at several temperatures.

D. Compatibility

Since the proposed PUF can be concealed and can be recovered in different cycles, it can perform the IMC in concealed mode as shown in Fig. 3. To verify the compatibility of the proposed PUF with IMC, a MAGIC OR gate was designed, and its outputs were measured over 50 cycles, as shown in Fig. 12. The y-axis represents the measured resistance of the RRAMs on a logarithmic scale and their resistance states are labelled. The x-axis represents the states of the RRAMs. The output RRAM is initialized to HRS, and

TABLE I: COMPARISON OF THE PROPOSED RRAM PUF WITH OTHER DESIGNS.

	ISSCC'19 [4]	IEDM'20 [6]	TED'20 [7]	ISCAS'21 [8]	This work
Technology (nm)	130	130	130	40	90
Entropy Source (RRAM)	HRS Resistance	Memory Time	Switch Voltage	HRS Resistance	Switch Capability
Energy Efficiency (pJ/bit)	3.028	0.19	N/A	N/A	2.225
Uniformity	50.01%	N/A	N/A	50.01%	49.55%
Uniqueness	0.4999	0.4999	0.4989	0.498	0.4994
BER	0	0	0.12%	0	0
Stabilization Method	Split Resistance	Digital Storage	Digital Storage	Digital Storage	TMV3 & Masking
Concealable?	No	No	No	No	**Yes**
IMC Compatible?	No	No	No	No	**Yes**

the inputs IN1 and IN2 are programmed to four different combinations. After applying the OR operation, the result stored as the resistance state of the output RRAM. As can be seen in Fig. 12, there are significant C2C variations in the resistance of the input and output RRAMs. However, the outputs consistently have a distinguishable margin between the two logical states, demonstrating accurate logic operations and stable outputs of the OR gate. Furthermore, the inputs of the gates are not compromised during the computation. Therefore, the proposed PUF exhibits excellent compatibility with IMC.

Table I compares the proposed RRAM PUF with state-of-the-art weak RRAM PUFs. In [4] and [8], the distribution of the HRS resistance is used as the randomness source. A 1-bit key is generated by comparing the HRS resistances of two RRAMs. The short-term memory time of RRAMs is extracted to generate PUF keys in [6], but this PUF requires complex peripheral digital circuits. In [7], the PUF leverages D2D variations in the switching voltage of the RRAM to generate keys, exhibiting high density. However, due to C2C variations, these prior works cannot effectively reproduce the PUF key between cycles. To enhance PUF reliability, they directly store the PUF key as the resistance state of RRAMs, which contradicts the property of PUF to generate keys online and increases the risk of being attacked. An Attacker can directly read the PUF key through a probing attack. In contrast, the proposed RRAM PUF can reproduce the PUF key between cycles. Although the reliability of the PUF is reduced and post-processing is required, the PUF key can be concealed, preventing the risk of being read directly and improving the security of the RRAM PUF. Additionally, this PUF is compatible with IMC due to the concealability feature.

IV. CONCLUSION

This paper experimentally demonstrated a concealable RRAM PUF based on RRAM crossbar array. Based on the basic cell of three RRAM devices, the PUF key is generated using the randomness of the RRAM's resistance state switching capability. The PUF key can be reproduced between cycles, allowing the PUF to conceal the key and recover it when needed. Compared to previous RRAM PUF designs, this concealable feature enhances the security of the PUF. With post-processing, this PUF has good reliability over ±10% VDD and a temperature range of 248K to 373K. Additionally, the proposed RRAM PUF experimentally demonstrates excellent compatibility with IMC. In summary, the proposed concealable PUF provides a more secure solution to generate keys for security applications.

REFERENCES

[1] H.-S. P. Wong, H.-Y. Lee, S. Yu, Y.-S. Chen, Y. Wu, P.-S. Chen, B. Lee, F. T. Chen, and M.-J. Tsai, "Metal–oxide RRAM," *Proceedings of the IEEE*, vol. 100, no. 6, pp. 1951–1970, 2012.

[2] S. Kvatinsky, D. Belousov, S. Liman, G. Satat, N. Wald, E. G. Friedman, A. Kolodny, and U. C. Weiser, "MAGIC—Memristor-aided logic," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 61, no. 11, pp. 895–899, 2014.

[3] S. Balatti, S. Ambrogio, R. Carboni, V. Milo, Z. Wang, A. Calderoni, N. Ramaswamy, and D. Ielmini, "Physical unbiased generation of random numbers with coupled resistive switching devices," *IEEE Transactions on Electron Devices*, vol. 63, no. 5, pp. 2029–2035, 2016.

[4] Y. Pang, B. Gao, D. Wu, S. Yi, Q. Liu, W. Chen, T. Chang, W. Lin, X. Sun, S. Yu, H. Qian, M. Chang, and H. Wu, "A reconfigurable RRAM physically unclonable function utilizing post-process randomness source with $< 6\times10^{-6}$ native bit error rate," in *Proc. IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 402–404, 2019.

[5] Y. He and K. Yang, "A 65nm edge-chasing quantizer-based digital LDO featuring 4.58ps-FoM and side-channel-attack resistance," in *Proc. IEEE International Solid- State Circuits Conference (ISSCC)*, pp. 384–386, 2020.

[6] J. Yang, D. Chen, Q. Ding, J. Fang, X. Xue, H. Lv, X. Zeng, and M. Liu, "A novel PUF using stochastic short-term memory time of oxide-based RRAM for embedded applications," in *Proc. IEEE International Electron Devices Meeting*, pp. 39.2.1–39.2.4, 2020.

[7] X. Zhao, Q. Zhao, Y. Liu, and F. Zhang, "An ultracompact switching-voltage-based fully reconfigurable RRAM PUF with low native instability," *IEEE Transactions on Electron Devices*, vol. 67, no. 7, pp. 3010–3013, 2020.

[8] L. Lu, Y. Z. Chen, and T. T.-H. Kim, "A configurable randomness enhanced RRAM PUF with biased current sensing scheme," in *Proc. IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–5, 2021.

[9] C. Ho, S.-C. Chang, C.-Y. Huang, Y.-C. Chuang, S.-F. Lim, M.-H. Hsieh, S.-C. Chang, and H.-H. Liao, "Integrated HfO2-RRAM to achieve highly reliable, greener, faster, cost-effective, and scaled devices," in *Proc. IEEE International Electron Devices Meeting (IEDM)*, pp. 2.6.1–2.6.4, 2017.

[10] J. Reuben, R. Ben-Hur, N. Wald, N. Talati, A. H. Ali, P.-E. Gaillardon, and S. Kvatinsky, "Memristive logic: A framework for evaluation and comparison," in *Proc. International Symposium on Power and Timing Modeling, Optimization and Simulation (PATMOS)*, pp. 1–8, 2017.

[11] A. Maiti, V. Gunreddy, and P. Schaumont, *A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions*, pp. 245–267. Springer, 2013.

[12] S. Satpathy, S. K. Mathew, V. Suresh, M. A. Anders, H. Kaul, A. Agarwal, S. K. Hsu, G. Chen, R. K. Krishnamurthy, and V. K. De, "A 4-fj/b delay-hardened physically unclonable function circuit with selective bit destabilization in 14-nm trigate CMOS," *IEEE Journal of Solid-State Circuits*, vol. 52, no. 4, pp. 940–949, 2017.

[13] Y. Gao, Y. Su, L. Xu, and D. C. Ranasinghe, "Lightweight (reverse) fuzzy extractor with multiple reference PUF responses," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1887–1901, 2019.