**QUEEN'S
UNIVERSITY
BELFAST**

Dynamically Configurable Physical Unclonable Function based on RRAM Crossbar

Li, J., Cui, Y., Gu, C., Wang, C., & Liu, W. (2021). Dynamically Configurable Physical Unclonable Function based on RRAM Crossbar. In *2021 : 2021 IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH): Proceedings* (2021 IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH)). Institute of Electrical and Electronics Engineers Inc..
<https://doi.org/10.1109/NANOARCH53687.2021.9642245>

Published in:

2021 : 2021 IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH): Proceedings

Document Version:

Peer reviewed version

Queen's University Belfast - Research Portal:

[Link to publication record in Queen's University Belfast Research Portal](#)

Publisher rights

Copyright 2021 IEEE. This work is made available online in accordance with the publisher's policies. Please refer to any applicable terms of use of the publisher.

General rights

Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy

The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.

Special Session-Dynamically Configurable Physical Unclonable Function based on RRAM Crossbar

Abstract—Physical unclonable function (PUF) has been an effective solution for hardware security with the popularity of the internet of things (IoT). Due to low power consumption and high area efficiency, an emerging nonvolatile memory, resistive random access memory (RRAM) based PUF designs have attracted many attentions. Due to the bottleneck in the existing RRAM PUFs that it can not be fully compatible with the memory architecture, a dynamically configurable PUF based on the mainstream RRAM crossbar is proposed in this paper. Utilizing the device-to-device variation of the RRAM resistance, abundant challenge-response pairs (CRPs) are generated with a flexible configuration of an RRAM crossbar. Furthermore, different from the existing RRAM-based PUF designs, the proposed RRAM PUF can be dynamically configured between a memory cell and a PUF cell, without requiring additional sense circuits, leading to a minimal design overhead. The simulation results show that the proposed PUF exhibits good performance with a high uniqueness and reliability. Moreover, it achieves a great resistance against machine learning (ML) attack.

Index Terms—Physical unclonable function (PUF), resistive random access memory (RRAM), RRAM crossbar, dynamically configuration

I. INTRODUCTION

DUE to the ubiquity of IoT and cloud computing, the edge devices encounter big challenges of security threats. Most keys are stored in non-volatile memories (NVMs), and physical attacks, such as side channel analysis, can easily reveal the keys. Therefore, IoT devices are in demand of a more secure key storage method to protect the security of the system.

As a promising hardware security primitive, PUF, which uses manufacturing process variations introduced by the changed fabrication process of an integrated circuit (IC), has got a fast development with the explosive growth of electronic devices in recent decades [1], [2]. PUFs are based on challenge-response pairs (CRPs) to implement authentications by comparing CRPs in a database with that of a PUF circuit. According to the number of CRPs in a PUF, PUFs can be generally categorized as weak PUFs and strong PUFs. The number of CRPs in a strong PUF increases exponentially, while the number of CRPs in a weak PUF is small, e.g., only one in most cases. Strong PUFs are normally utilized for device authentications [3], [4], and weak PUFs are commonly used for key generation [5], etc.

RRAM is a state-of-the-art memory architecture for novel PUF designs [6], [7]. However, the effects, such as instability, retention loss or thermal sensibility of the resistance transformation of RRAM during the write process, may give a rise to bit-flippings in a response generation phase. When applying

a precise voltage, one-transistor-one-RRAM (1T1R) cells set half 1T1R cells to high-resistance state (HRS) and others to low-resistance state (LRS) to generate the random key, which are vulnerable to various supply voltage and environment temperature [8]. The basic cells, e.g., one-transistor-two-RRAM (1T2R) and two-transistor-two-RRAM (2T2R) cells require more circuits to generate the same number of response bits [9]. Comparing the resistance of two RRAMs from different arrays can generate a low bit error rate response. However, the mismatch of sense amplifier and the variations of symmetric cells between different arrays may generate bias, i.e., a bias of the number of ‘1’ or ‘0’ [10]. A strong PUF structure using the RRAM/CMOS hybrid circuits was proposed to achieve a significant number of CRPs [11]. The usage of multiplexers or inverters increases the randomness of RRAM PUFs. However, the additional and dedicated circuits also increase the hardware resource consumption. Although RRAM is widely utilized to memories [12], the compatibility of RRAM PUFs with the memory architectures is still unknown.

In order to address the above challenges in RRAM PUFs, a dynamically configurable PUF design based on the native instability of RRAM crossbar circuits is proposed. Utilizing the device-to-device (D2D) variation of an RRAM, the proposed RRAM PUF design can generate a significant number of CRPs. It generates responses by comparing the resistance of different combinations of RRAMs, which can generate more than 2^{38} CRPs in a 32×32 (1kb) RRAM array. Owing to the sneak current in RRAM crossbar, the relationship between the challenge and response is nonlinear. Hence, the RRAM PUF features high resistance against ML attacks. Furthermore, based on 1T1R crossbar scheme, the RRAM PUF is compatible to mainstream RRAM-based memory architectures without requiring additional peripheral circuits, and all RRAMs can be dynamically configured from a PUF cell to a memory cell, or vice versa. This makes the RRAM array can be reused by memory or PUF, leading to minimal circuitry overheads. Through the National Institute of Standards and Technology (NIST) tests, the true randomness of the proposed PUF using self-directed channel (SDC) RRAMs is validated, and the simulation results demonstrate a high uniqueness and reliability of the proposed RRAM PUF.

The rest of this paper is organized as follows. In Section II, the randomness source of RRAM, which is used to implement configurable RRAM PUF, is described. Section III elaborates PUF design and dynamically configurable scheme. Section IV gives the performance results of the proposed PUF. And a conclusion is provided in Section V.

II. CHARACTERISTIC OF RRAM

An RRAM is one of the emerging NVMs that are extensively applied in industrial developments [13]. RRAM devices are based on redox or electronic, in which the metal-ion based SDC RRAM is relatively new [14]. Silver ions move in the cracks between the electrode of SDC RRAM, and the resistance is tunable by applying a positive or negative potential. SDC RRAM has a high endurance, analog state retention and low switch voltages. There are two tunable resistance states of an RRAM: LRS and HRS for memory applications, and an RRAM can persist at any resistance state without requiring power. By applying the pulse of appropriate amplitude that is more than a threshold voltage, an RRAM can repeatedly switch between these two resistance states. The operation which changes the state of the RRAM from HRS to LRS is defined as RESET. The operation, which changes the state of RRAM from LRS to HRS, is defined as SET. In this paper, the LRS is a logic '0', and the HRS is a logic '1'. The structure of a 1T1R cell, that uses the NMOS transistor as a selected device, is shown in Fig. 1(a). SDC RRAM, equipped with tungsten (W) as the dopant to enhance and optimize device properties, changes its resistance by restricting the movement of silver (Ag) ions into a chemically created channel. Fig. 1(b) presents the switch of RRAM resistance states between HRS and LRS by RESET and SET operations. When the applied voltage exceeds the backward threshold (approximately -0.11V), the RRAM will switch to the HRS abruptly by a RESET operation.

Fig. 1: (a) The typical structure of a 1T1R cell that uses an NMOS transistor. (b) The switch process between the LRS and HRS of a RRAM.

Since there is a tendency that Ag agglomerates with other Ag atoms, the RRAM resistance will change by adding or removing Ag from the agglomeration sites within generated channel, and the number of Ags determines the RRAM resistance of LRSs and HRSs. Due to manufacture process variations, the number of Ags in RRAMs differs which leads to the variation of the RRAM resistance. Therefore, there are significant device-to-device (D2D) and cycle-to-cycle (C2C) variations in RRAMs. For example, as shown in Fig. 2(a), when a SET or RESET operation is applied, the RRAM

Fig. 2: (a) The D2D variation of a RRAM, providing an entropy source for PUFs. (b) The C2C variation of a RRAM, which can refresh PUF instances.

resistances of the LRS or HRS are different. The median of LRS resistance is about 3.57kΩ, while the median of HRS resistance is about 126kΩ. The distributions of both LRS and HRS resistance are in a wide range, which provide suitable entropy sources for the response generation of a PUF. Moreover, in different cycles, the resistance of the same RRAM fluctuates considerably. One cycle includes a switch operation between LRS and HRS. Fig. 2(b) gives the resistance variation of an RRAM in different cycles and the RRAM resistance varies dramatically and unpredictably. The C2C variation endows the proposed RRAM PUF with unique configurability and provides an approach to refresh PUF instances. Most existing RRAM PUFs are constructed by 1T1R, 1T2R, 2T2R cells, or RRAM crossbars. Two common mechanisms are utilized to generate random responses including the transformation of two different resistance states for weak PUFs, and the resistance comparison of the same state for strong PUFs. Regardless of the mechanism, there is a uniform implementation approach, firstly applying the same voltage to induce the same transformation process to each RRAM, then performing the resistance sensing procedure, which compares the resistance values of the RRAM with a reference or another RRAM.

III. PROPOSED DYNAMICALLY CONFIGURABLE PUF BASED ON A RRAM CROSSBAR

A. Architecture and Dynamically Configurable Scheme of the RRAM PUF

The proposed RRAM PUF is designed to be compatible with a normal memory structure. Based on RRAM crossbar, the architecture of the proposed dynamically configurable PUF is shown in Fig. 3(a), which includes a 1T1R RRAM crossbar array, a row/column decoder, a timing control circuit and a sense amplifier (SA). Fig. 3(b) shows the RRAM crossbar with three types of control lines, WL, WLB and BL. By applying the bias voltage to the WLB and BL, the RRAMs can be flexibly switched to the LRS (or HRS) after SET (or RESET). The WL lines, connected to the gate of NMOS transistors in the same rows, are used to enable or disable the NMOS transistors. Before SET or RESET process, the WL should be enabled. To avoid an entropy loss and unstable bit flip during the response generation process of the PUF, an offset-tolerant current-sampling-based SA is adopted [15]. The schematic

Fig. 3: (a) Schematic of the proposed dynamically configurable PUF which includes RRAM crossbar circuit and complete peripheral circuits. (b) Schematic of the RRAM crossbar circuit with three types of control lines, i.e. WL , WLB and BL . (c) Schematic of the SA with an offset tolerance for a small-cell-current read.

of SA, which is used to implement the read process of the PUF cell and memory cell, is shown in Fig. 3(c). The SA samples the current and amplifies the current difference across operating phases using the same MOS device, i.e. M1 and M2. Therefore, it can implement the V_{TH} -independent current sampling schemes for different I_{ref} and I_{cell} inputs. The current fed into the SA from either RRAM cells or voltage-controlled current source is selected by *switch5* (S5) and *switch6* (S6).

S5 of the proposed PUF design should be enabled, while S6 should be disabled in Fig. 3(c). Two column currents of the RRAM crossbar are selected to feed into SA. The read current I_{cell} of the $RRAM_{P1}$ is compared with I_{ref} of the $RRAM_{P2}$ through the SA, and a 1-bit PUF response is generated by comparing the magnitude of two currents. Since the resistance distribution of RRAMs is wide, the current difference is large enough to generate stable PUF responses and no post-processing is required. For a generated memory, S5 should be disabled, while S6 should be enabled. The SA is fed with the currents of the RRAM and current source to read the resistance state of the RRAM. By comparing the current magnitude of the RRAM with I_{ref} of the current, whether the selected RRAM is in HRS or LRS can be read out, and a memory bit can be generated based on the logic state of the RRAM. The reference current should be tuned to a suitable magnitude, which can be searched automatically by calculating and minimizing the bit error rate (BER), to distinguish LRS and HRS.

Furthermore, based on the proposed PUF, the RRAM becomes fully configurable between a PUF cell and a memory cell, enabling the functions of both PUF and memory, as shown in Fig. 4. The RRAM array1 (A1) is firstly used as

Fig. 4: The dynamically configurable scheme between a PUF cell and a memory cell which share the same SA circuit. If the CRPs of a PUF cell have exhausted, a new PUF cell can be rebuilt from other memory cells.

PUF cells, while the other arrays are used as memory cells. If the CRPs of the PUF cell have been exhausted or the PUF cell have been attacked and insecure, the PUF cell can transfer to other RRAM arrays. For example, if the CRPs of PUF cell in A1 have exhausted, it can be configured as a memory cell and store the data from A2. Then, A2 can be configured as a PUF cell to generate responses. The RRAM array in any size for memory cells can be used as a PUF. Therefore, according to the requirements of PUF applications, RRAM arrays with a sufficient size can be used as a PUF, which minimize the circuit overhead and improve the device utilization rate.

B. Configurable Scheme and Exploiting Sneak Paths to Enhance Security of PUF

Fig. 5: The configurable scheme of the propose PUF architecture which includes a 32×32 RRAM crossbar, row and column selectors, and a SA. 1-bit response is generated by comparing the current of two columns.

The proposed RRAM PUF generates a 1-bit response by comparing the current of two columns. Therefore, it is a flexible and configurable scheme, and any number of RRAMs in the column can be selected, as shown in Fig. 5. The transmission gate is used to be the row selector (RS), and the

column selector (CS) is based on a 4-transistor structure. A single bit response is generated in a 96-bit challenge. Since the HRS resistance is larger than that of the LRS, and the HRS can also reduce the power consumption. Hence, the RRAM should be configured as an HRS by a RESET operation before the generation of a response. The 32-bit challenge (C_{bi}) uniquely determines which two columns are enabled, and another 32-bit challenge C_{bia} is used to determine that the current of column feed into I_{cell} or I_{ref} of SA. The remaining 32-bit challenge C_{wi} enables the rows to select any number of RRAMs, and all unselected rows and columns are floated. Therefore, the number of CRPs generated based on 1kb RRAM crossbar is $\sum \binom{32}{m} \binom{32}{2}$, and it is more than 2^{38} for $m = 16$.

Fig. 6: The sneak current in the RRAM crossbar with the selected and unselected RRAMs.

When the bias voltage is applied on the selected rows and the unselected rows/columns in the array are floated, the sneak currents will flow through the entire RRAM array, as shown in Fig. 6. As for the enabled row and columns, the crossed RRAM is selected, while the RRAMs is half-selected in the single enabled row or column. Therefore, apart from the entropy of RRAM resistance, the more randomness of abundant sneak current can be utilized to enhance the security of the PUF. However, such sneak current influences the accuracy of the read-out sense, which is detrimental to memory applications [16]. By using a selector device, such as a transistor, the affection of the sneak current can be mitigated [17]. Therefore, the NMOS transistors of the PUF are enabled all the time, while in the memory process, the read scheme based on sneak current compensation can be adopted using the NMOS transistors [18].

IV. SIMULATION RESULTS

The performance of a PUF can be evaluated by some metrics, such as uniformity, uniqueness, reliability and randomness [19], which are adopted to evaluate the performance of the proposed RRAM PUF. The compact Spice model of SDC RRAM from [20] is used in the simulation. Uniformity measures the probability of ‘0’ and ‘1’ in the response, representing the randomness of generated bits. The ideal value

of uniformity is 50%. The uniqueness indicates the differences between the responses of different PUF instances, and its ideal value is 0.5. Reliability measures the ability of a PUF to regenerate response with the same challenge and the ideal value is 0. Moreover, the randomness of a PUF is evaluated by using NIST SP800-22 statistical test suite [21].

A. Uniformity and Randomness

The spectral pattern of collected 100 128-bit responses is shown in Fig. 7(a). The distribution of ‘0’ and ‘1’ is random and homogeneous, and there is no apparent spatial correlations. From the generated responses, the uniformity can be analyzed and calculated by percentage Hamming Weight (HW):

$$Uniformity = \frac{1}{n} \sum_{i=1}^n r_i \times 100\% \quad (1)$$

where r_i is the i -th bit of an n -bit response. Fig. 7(b) shows the uniformity result of different PUF instances. It can be observed that the maximum deviation of the uniformity result from 50% for the 10 PUF instances is 0.04%, and the mean value is 49.99%, which represents that the probability of ‘0’ or ‘1’ generated by the PUF is close to an ideal value, 50%.

Fig. 7: (a) The spectral pattern of the collected 100 128-bit responses. (b) The uniformity of 10 different PUF instances.

Additionally, the 10Mb response is collected and fed into the NIST SP800-22 statistical test suite [21]. The NIST test results are summarized in TABLE I. “P-value > 0.01” represents that the test data passes the corresponding test item. As seen in TABLE I, the proposed RRAM PUF passes all the listed NIST statistical tests, which verifies the excellent randomness of the proposed PUF.

B. Uniqueness, Reliability and Security

The uniqueness measures the difference between two responses of different PUF instances with the same challenge, which indicates the capacity of a PUF to distinguish a particular instance from others. Uniqueness can be calculated by the inter-chip Hamming Distance (HD) and defined as:

$$Uniqueness = \frac{2}{N(N-1)} \sum_{u=1}^{N-1} \sum_{v=u+1}^N \frac{HD(R_u, R_v)}{n} \quad (2)$$

where R_u and R_v respectively represent the n -bit responses of two chips, u and v , $u \neq v$, with the same challenge, and

TABLE I: NIST SP800-22 STATISTICAL TEST RESULTS OF THE PROPOSED RRAM PUF.

NIST Test 800-22	Prop.	P-Value	Pass?
Frequency	99/100	0.452424	Yes
Block Frequency	100/100	0.276526	Yes
Cumulative Sums	100/100	0.526778	Yes
Runs	98/100	0.725467	Yes
LongestRun	100/100	0.267653	Yes
Rank	98/100	0.862543	Yes
FTT	99/100	0.476525	Yes
Universal	98/100	0.254657	Yes
ApproximateEntropy	99/100	0.265768	Yes
*NonOverlappingTemplate	PASS	PASS	Yes
OverlappingTemplate	99/100	0.326572	Yes
*RandomExcursions	PASS	PASS	Yes
*RandomExcursionsVariant	PASS	PASS	Yes
*Serial	PASS	PASS	Yes
LinearComplexity	98/100	0.724325	Yes

* There are more than one sub-tests in this item.

N is the total number of tested PUF instances. According to Eq. (2), 200 128-bit responses generated by 20 PUF instances with 10 responses from each PUF instance is used to evaluate uniqueness. Therefore, based on total 200 128-bit responses, there are $\binom{200}{2} = 19900$ pairs of 128-bit responses for the calculation of the HD. Fig. 8(a) shows the histogram of the HD of 10 PUF instances, and provides the best-fit Gaussian distribution curve. The mean μ and standard deviation σ are 0.4999 and 0.0186, respectively.

In order to measure the efficiency of the proposed RRAM PUF in regenerating the response bits with the same challenge, the reliability which is calculated by the intra-chip HD between two responses of the same PUF, is used to evaluate it. The intra-chip HD is expressed as follows:

$$Reliability = \frac{1}{N} \sum_{u=1}^N \frac{HD(R_v, R_{v,u})}{n} \quad (3)$$

where the same challenge is applied N times to generate responses, R_v is the n -bit standard response and $R_{v,u}$ is the u -th sample of R_v . The 128-bit responses are generated by 10000 times with the same challenge. The reliability results are plotted in Fig. 8(b), and it can be observed that the mean μ and standard deviation σ are 0.00074 and 0.00019, respectively. Moreover, the relationship between the inter and intra HDs is presented. As seen in Fig. 8(b), the distance between the inter and intra HD is calculated to be $\sim 676\times$, which shows a low Fault Failure Rate (FFR) and a Fault Acceptance Rate (FAR).

To further measure the resistance of the proposed PUF against ML attack, the online libraries LIBLINEAR and LIBSVM are used [22]. Based on the training of 80% CRPs and validation of 20% CRPs, the prediction rate of ML attack to the RRAM PUF is shown in Fig. 9. The prediction accuracy of ML attacks are close to the ideal value, 50%, indicating that the proposed PUF has a strong resistance against ML attacks. The performance of the proposed PUF is summarized and

Fig. 8: (a) The inter-chip HD of the PUF based on 10 128-bit responses. (b) The uniqueness and reliability distributions of the proposed RRAM PUF.

compared with previous designs in TABLE II. The proposed RRAM achieves excellent randomness and reliability, and it features the great resistance to ML attack, which well-verifies the superior security.

Fig. 9: The predictability of the ML attack to the proposed RRAM PUF.

V. CONCLUSION

In this work, a dynamically configurable PUF based on the RRAM crossbar has been proposed. Using the D2D variation of a RRAM, the proposed PUF can generate a significant number of CRPs with different combinations of current paths. Additionally, the RRAM can be dynamically configured from a PUF cell to a memory cell, reducing the circuitry overhead. The proposed PUF achieves a high randomness and reliability, enabling a potential for lightweight IoT application. The sneak current in a RRAM crossbar enhanced security, and the proposed PUF is resistant to ML attacks. The proposed RRAM PUF shows good uniformity, uniqueness, and reliability results.

REFERENCES

- [1] M. R. Mahmoodi, H. Nili, and D. B. Strukov, "RX-PUF: Low power, dense, reliable, and resilient physically unclonable functions based on analog passive RRAM crossbar arrays," in *Proc. IEEE Symposium on VLSI Technology*, pp. 99–100, 2018.

TABLE II: COMPARISON OF THE PROPOSED PUF WITH OTHER DESIGNS.

	Nanoarch'13 [8]	Scientific Reports'15 [23]	Nanoarch'16 [24]	IEEE TDSC'20 [25]	This work
Entropy	RRAM	RRAM	STT-MRAM	RRAM	RRAM
PUF type	Weak	Strong	Strong	Strong	Strong
NO. of CRPs*	1k	$n \times \binom{m}{i} \times \binom{m-i}{i} / 2$	$\binom{mn}{mn/2}^2 / 2$	$2^m \times 2^n$	$\sum \binom{m}{i} \binom{n}{i}$
Uniformity	N/A	50.76%	50.12%	50-53%	49.99%
Uniqueness	N/A	0.5007	0.4999	0.513	0.4999
Reliability	N/A	N/A	N/A	0.0013	0.00074
ML attack	N/A	N/A	N/A	Anti-attack	Anti-attack
Dynamical configuration	No	No	No	No	Yes
NIST tests	N/A	N/A	N/A	Passed	Passed

* The number of CRPs in an $m \times n$ RRAM array.

- [2] C. Gu, W. Liu, Y. Cui, N. Hanley, M. O'Neill, and F. Lombardi, "A flip-flop based arbiter physical unclonable function (APUF) design with high entropy and uniqueness for fpga implementation," *IEEE Transactions on Emerging Topics in Computing*, 2019.
- [3] J. Zhang and G. Qu, "Physical unclonable function-based key sharing via machine learning for iot security," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 7025–7033, 2020.
- [4] J. Li, H. Gao, Y. Cui, C. Wang, Y. Wang, C. Gu, and W. Liu, "Theoretical analysis of configurable RO PUFs and strategies to enhance security," in *Proc. IEEE International Workshop on Signal Processing Systems*, pp. 91–96, 2019.
- [5] B. Lin, Y. Pang, B. Gao, J. Tang, D. Wu, T.-W. Chang, W.-E. Lin, X. Sun, S. Yu, M.-F. Chang, H. Qian, and H. Wu, "A highly reliable RRAM physically unclonable function utilizing post-process randomness source," *IEEE Journal of Solid-State Circuits*, vol. 56, no. 5, pp. 1641–1650, 2021.
- [6] J. Li, Y. Cui, C. Gu, C. Wang, W. Liu, and F. Lombardi, "A physical unclonable function using a configurable tristate hybrid scheme with non-volatile memory," *IEEE Open Journal of Nanotechnology*, vol. 2, pp. 31–40, 2021.
- [7] 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.
- [8] G. S. Rose, N. McDonald, L. Yan, B. Wysocki, and K. Xu, "Foundations of memristor based PUF architectures," in *Proc. IEEE/ACM International Symposium on Nanoscale Architectures*, pp. 52–57, 2013.
- [9] X. Xue, J. Yang, Y. Zhang, M. Wang, H. Lv, X. Zeng, and M. Liu, "A 28nm 512kb adjacent 2T2R RRAM PUF with interleaved cell mirroring and self-adaptive splitting for extremely low bit error rate of cryptographic key," in *Proc. IEEE Asian Solid-State Circuits Conference*, pp. 29–32, 2019.
- [10] 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 $< 6 \times 10^{-6}$ native bit error rate," in *Proc. IEEE International Solid-State Circuits Conference*, pp. 402–404, 2019.
- [11] Y. Cui, C. Wang, W. Liu, C. Gu, M. O'Neill, and F. Lombardi, "Lightweight configurable ring oscillator PUF based on RRAM/CMOS hybrid circuits," *IEEE Open Journal of Nanotechnology*, vol. 1, pp. 128–134, 2020.
- [12] Y. Xi, B. Gao, J. Tang, A. Chen, M.-F. Chang, X. S. Hu, J. V. D. Spiegel, H. Qian, and H. Wu, "In-memory learning with analog resistive switching memory: A review and perspective," *Proceedings of the IEEE*, vol. 109, no. 1, pp. 14–42, 2021.
- [13] 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.
- [14] K. A. Campbell, "Self-directed channel memristor for high temperature operation," *Microelectronics Journal*, vol. 59, pp. 10–14, 2017.
- [15] M.-F. Chang, S.-J. Shen, C.-C. Liu, C.-W. Wu, Y.-F. Lin, Y.-C. King, C.-J. Lin, H.-J. Liao, Y.-D. Chih, and H. Yamauchi, "An offset-tolerant fast-random-read current-sampling-based sense amplifier for small-cell-current nonvolatile memory," *IEEE Journal of Solid-State Circuits*, vol. 48, no. 3, pp. 864–877, 2013.
- [16] S. Yu and P.-Y. Chen, "Emerging memory technologies: Recent trends and prospects," *IEEE Solid-State Circuits Magazine*, vol. 8, no. 2, pp. 43–56, 2016.
- [17] IRDS, "International roadmap for devices and systems," 2020.
- [18] Y. Shang and T. Ohsawa, "Accurate measurement of sneak current in ReRAM crossbar array with data storage pattern dependencies," in *Proc. International Symposium on VLSI Technology, Systems and Application*, pp. 1–2, 2019.
- [19] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," in *Embedded Systems Design with FPGAs*, pp. 245–267, 2013.
- [20] T. Molter, *Memristor Models in LTSpice [online]*. Available from <https://knownm.org/memristor-models-in-ltspice>, 2017.
- [21] L. Bassham, A. Rukhin, J. Soto, J. Nechvatal, M. Smid, S. Leigh, M. Levenson, M. Vangel, N. Heckert, and D. Banks, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *NIST Special Publication, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 800-22 Rev 1a*, 2010.
- [22] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," *ACM Transactions on Intelligent Systems and Technology*, vol. 2, pp. 27:1–27:27, 2011.
- [23] Y. Gao, D. Ranasinghe, S. Al-Sarawi, O. Kavehei, and D. Abbott, "Memristive crypto primitive for building highly secure physical unclonable functions," *Scientific Reports*, vol. 5, p. 12785, 2015.
- [24] S. Khaleghi, P. Vinella, S. Banerjee, and W. Rao, "An STT-MRAM based strong PUF," in *Proc. IEEE/ACM International Symposium on Nanoscale Architectures*, pp. 129–134, 2016.
- [25] R. Govindaraj, S. Ghosh, and S. Katkouri, "Design, analysis and application of embedded resistive RAM based strong arbiter PUF," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 6, pp. 1232–1242, 2020.