A PUF Based on the Non-Linearity of Memristors

Callum Aitchison, Basel Halak
Electronics and Computer Science
University of Southampton
Southampton, United Kingdom
callum.aitchison@soton.ac.uk, basel.halak@soton.ac.uk

Alex Serb, Themis Prodromakis
Centre for Electronics Frontiers
Institute for Integrated Micro and Nano Systems
School of Engineering
University of Edinburgh
Edinburgh, United Kingdom
aserb@exseed.ed.ac.uk, t.prodromakis@ed.ac.uk

***Abstract*—As autonomous devices are increasingly used in security and safety-critical applications the security of the systems they comprise is of increasing concern. In such situations it is important that devices can be securely identified and trusted. When an IC or device is in the supply chain, or in the field, the lack of control over actors who can obtain physical access can compromise the trust and overall security of a system. Counterfeit chips may be incorporated into the device, compromising reliability or security. Additionally, for implemented devices, keys stored on-device may be copied by a bad actor. To help improve the security of such devices this paper proposes a new physical unclonable function (PUF) architecture, based on a TiO$_x$ memristor-based resistive memory (RRAM), that exploits the inherent analogue non-linearity in resistance of some memristor technologies. By directly exploiting non-linearity of memristor cells, rather than relying on the devices' absolute resistance at a single test voltage, a multi-bit-per-comparison PUF is created. As the architecture directly exploits cells' non-linearity, an additional source of hard-to-clone entropy is incorporated.**

***Index Terms*—hardware security, physical unclonable functions, RRAM, memristor**

I. Introduction

Trust is an important part of modern security and safety-critical systems. Counterfeit, tampered or otherwise illegitimate hardware can compromise the robustness or trustworthiness of a system resulting in anything from early failure to compromise by a bad actor. Counterfeit ICs may be unwittingly incorporated into deployed systems. Such a chip may not perform to the expected standard, having subpar performance or even incorporating security vulnerabilities. Vulnerabilities could be introduced either intentionally or unintentionally, depending on the motivations of the counterfeiter. To ensure proper security of a deployed device it is imperative that devices in the field can be securely and uniquely identified in a way that is difficult, or impossible, for an attacker to effectively clone.

As autonomous systems may be targeted towards high security, high trust scenarios it is necessary that these devices can be relied upon to work securely and as intended. A loss of reliability caused by the poor performance of an illegitimate chip could result in the failure of a critical system. Further, a bad actor may seek to intentionally compromise a system by introducing vulnerable hardware. Complete, unclonable, keys can be used to identify these counterfeits and secure data, thereby preventing such failures or compromise.

Tampering can occur in the supply chain or after deployment. Serial numbers and watermarking [1], [2] can be used for identifying chips, but do not offer complete security against clones. Serial numbers, for example, may be cloned from a legitimate chip and programmed onto a counterfeit. Watermarking aims to make that more difficult by introducing intentional changes to the design of a chip that don't affect the normal operation but may be identified later. Such features will not be copied in a functional clone of the chip. This, however, may require difficult checking procedures, does not uniquely identify chips and does not protect against overproduction. Physical Unclonable Functions (PUFs) have been proposed as a method to address these issues [3]. A PUF exploits intrinsic and uncontrollable variation between chips to produce a unique response that cannot be copied by an attacker. Because of these improvements, PUFs have been proposed as an anti-counterfeit methodology [4]. The keys generated by a PUF can also be used to encrypt data in a way such that the private key is never known outside the device and cannot be effectively extracted from it.

Current electronic PUFs tend to be based on CMOS designs. Resistive RAM (RRAM), a type of memory based on memristors, is a type of non-CMOS memory which can be incorporated into existing CMOS technologies [5], [6]. RRAM offers potential advantages in power consumption and density when compared to SRAM memories [7] and may find applications in neuromorphic computing for Artificial Intelligence (AI) [8].

Memristors have already been applied for random number generation [9] and cryptographic accelerators [10] and have shown advantages in power efficiency. Incorporating memristors has also been proposed as a method to harden against side channel attacks, for example by using hybrid memristor/CMOS gates to increase the difficulty of power analysis attacks [11]. The potential of hybrid CMOS/RRAM approaches to offer advantages ranging from power consumption and density paves the way for further exploitation as a security primitive on hybrid chips.

Previous work on using memristors in PUFs tend to be based on specific RRAM technologies, relying on crossbar

This work was supported by the UK Research and Innovation Centre for Doctoral Training in Machine Intelligence for Nano-electronic Devices and Systems [EP/S024298/1].

memories, or reading memristors' values at only a single voltage level when set to a specific state [12]–[14]. This work aims to improve memristor-based PUFs by differential comparison of the memristors' performance across a range of voltages. The approach incorporates the analogue I-V behaviour of memristors, introducing an additional unique parameter and making the potential of cloning more difficult for an attacker. Because the I-V behaviour of individual memristors is exploited, a successful clone must have the same resistive behaviour at multiple voltage levels, rather than just one. As the approach can be applied to a set of individual memristors it remains technology agnostic, so long as the technology offers non-linear I-V behaviour. By incorporating differential comparison between different memristors, a chip can be uniquely identified in a way which also improves noise immunity and ageing resilience [15].

The proposed PUF architecture is based on the idea of selecting individual memristors from a set, which may then be compared to one another to produce a unique key. This architecture differentiates itself from existing designs by directly relying on variation in non-linear I-V behaviour, rather than resistances at a single, set read voltage. As such it will remain applicable to any memristor technology with variation in resistance and non-linear I-V responses.

This paper will first introduce the proposed PUF architecture, including a proposed method of comparison. Later, the applicability is demonstrated using data collected from fabricated memristors. Finally, the approach is compared to existing work and conclusions are drawn.

II. PUF Design

Memristors exhibit a varying I-V characteristic from device-to-device [16] as well as from cycle-to-cycle [17], [18] when programmed between resistance states. The disparity in the cells' characteristics gives each cell a different behaviour, which can be exploited to produce unique keys.

Since these characteristics vary from cell-to-cell, the potential for use as a PUF is evident. As such, this paper proposes a new architecture for an analogue PUF which reads and compares the I-V variation of memristors.

A. System Architecture

In its simplest form the system architecture, shown in Fig. 1, is a combination of a DAC and ADC for stimulating the memristor and gathering a raw I-V sweep of the device. The voltage, current (V,I) pairs generated by the sweep are then used to determine the resistance of the cell for each test voltage to produce resistance, voltage (V,R) pairs. This collected data represents the non-linearity of the cell's resistance over the range of swept voltages.

The extent to which this architecture is implemented on-chip is variable. For an IC to be able to create and use its own keys the whole architecture, including an analysis system for the (V,R) pairs, must be built onto the design. This means that the curve response data must be analysed in either software or hardware as a separate piece of logic on the chip. As well as this, selection logic for individual memristors would be required. For this work, these additional options are bypassed by directly characterising the memristors on a die and performing processing off-chip. As well as simplifying the design process, this reduces the amount of on-chip hardware to simply an array of memristors. In an implemented system, however, it is likely to be more useful for the chip to be able to produce its own keys without the intervention of external hardware and therefore the whole system must be implemented in CMOS.

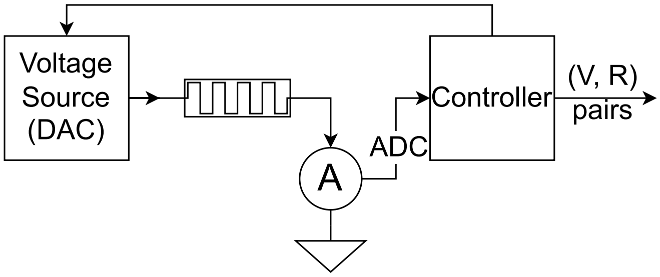

Fig. 1. System architecture. The controller sweeps the memristor cell across a range of voltages to obtain V-I measurements, which are then used to calculate (V,R) pairs.

B. Preparation of Memristor Cells

To ensure that the only variation between cells is due to device variation, rather than introduced biases, all cells are treated equally after fabrication. After fabrication the cells are considered "pristine" and from this point the same forming and programming methodology is applied equivalently to every cell. All the memristors in the array used for identification must be initially programmed to the same state using a large programming voltage. This could be their individual high or low resistance states, or a specific resistive state at a selected voltage (for example, $1.45\ M\Omega$ at $0.15\ V$).

Due to the cycle-to-cycle variability between memristors it may be possible to create a new response by cycling each cell individually. This also means that once the cell is programmed to its PUF state it should not be reprogrammed before it is used for identification.

Once the memristors have all been programmed to the same state, their sub-threshold I-Vs may be collected without affecting their state. These pairs can then be used to generate a key.

C. Comparing Cells

After the memristor cells have been prepared to the "same" state they may then be characterised using the system architecture (Fig. 1) to obtain the (V,R) pairs. These pairs can then be used for comparisons between memristor cells, ultimately leading to key generation and therefore identification.

Depending on the design aims, a different method of comparison could be used. For example, with a set of cells a comparison can be made between them as to which has the greater resistance. This could follow a standard approach in which the complete set of cells are split into subsets. Each memristor in each one subset can then be compared to each memristor in another subset. This approach is commonly used in memristor-based PUFs where memristors are programmed to either their low or high resistance states and then compared at one voltage.

To exploit this type of comparison with an architecture designed to rely on the non-linearity of the I-V response, the cells must be prepared in such a way they are all of equivalent resistance at a set "base" voltage. This leaves the memristors in a state where the resistance at that "base" voltage level is approximately equal across all cells. The comparison for the generation of a PUF response bit would then be determined by which has a greater resistance at an alternative read voltage. This could be lower or higher than the "base" voltage, so long as the non-linearity is substantial enough that a comparison can be made.

III. Analysis with Fabricated Memristors

The ArC One memristor characterisation platform was used to setup and characterise a set of memristors. The chracterisation setup was designed to conform to the proposed system architecture, enabling accurate testing and characterisation for a real PUF architecture.

A wafer of standalone Pt/TiO$_x$/Pt memristors, fabricated onsite, were used to test the proposed architecture.

A. Memristor Fabrication

Pt/TiO$_x$/Pt memristors were used for testing. The devices were fabricated with e-beam evaporation for the metals and reactive magnetron sputtering for the active layer. Negative tone lithography and lift-off have been used throughout to define all the layers. First, the 12 nm thick Pt layer (bottom electrode) is deposited with e-beam evaporation using 5 nm of Ti as adhesion layer. Afterwards, a second lithography TiO$_x$ is deposited using reactive magnetron sputtering (Leybold Vacuum HELIOS) from a metallic Ti source in an oxygen/argon plasma (8 sccm O$_2$, 35 sccm Ar). The thickness of the active layer is 25 nm. The device is finalised with a further 15 nm Pt deposition to define the top electrode. The overlapping area defines the active device. Available device active areas range from 2 to 60 μm^2, and in this work the 5 μm^2 devices were used. Devices produced using this process are typically in the $G\Omega$ range and need to undergo an electroforming step prior to use. An image of a die of fabricated standalone memristors, as used in this work, is presented in Fig. 2.

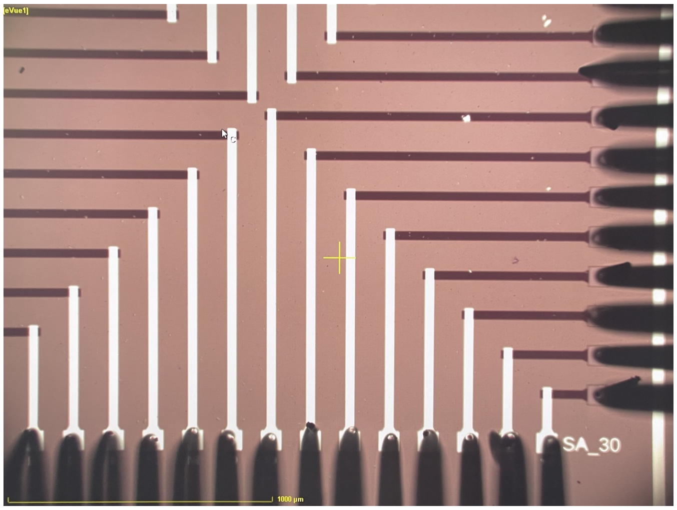

Fig. 2. Standalone memristor die, 30 μm width. Note: 5 μm devices used in this work.

All cells in the array are treated equally from pristine to avoid incorporating any bias in the results. The cells were initially formed using the ArC One "FormFinder" tool, using a minimum voltage of 4 V and a maximum of 9 V with a 0.1 V step, minimum pulse width of 100 μs and maximum 1000 μs with a 100% step, and 1 $M\Omega$ resistance threshold. This gradually increases the voltage until a sub-1 $M\Omega$ resistance is achieved on read, indicating the device has successfully formed a conductive filament in the memristive substrate.

B. Results and Analysis

1) Basic Comparison: Using the ArC One's "CurveTracer" tool I-V curves were obtained, which were then transformed into R-V curves. Fig. 3 shows two memristor cells, both programmed to approximately 1.45 $M\Omega$ at 0.15 V. Despite being programmed to approximately the same state at that single voltage, it is visually evident that the two cells differ greatly in linearity. The result is that, if you were to compare the cells with cell $(5, 5)$ in the "zeroes" set, and $(6, 27)$ in the "ones" set then the comparison would give a '1' PUF bit if the higher resistance at -0.5 V is considered the winner of the comparison.

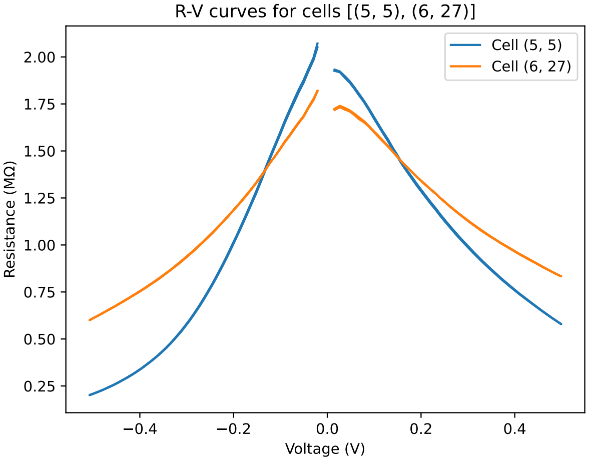

Fig. 3. Curves obtained from averaged read voltage sweeps of two memristors (-0.5 V to $+0.5$ V) in similar resistive states.

It is evident how this methodology could be scaled up with greater numbers of cells to produce a much longer PUF response.

2) Cells Programmed to Non-Specific Resistive States: In this comparison, shown in Fig. 4, cells were left programmed to non-specific states. This was achieved by leaving them in the state they ended up in after forming. Every cell was treated equally to avoid introducing biases, following the same setup procedure as stated previously. The four cells were selected out of one die of thirty-two standalone cells. These cells were chosen due to being similar to each other in resistive state and could be reliably read in the lab over the sample period, enabling complete analysis from the beginning to the end of the measurement period.

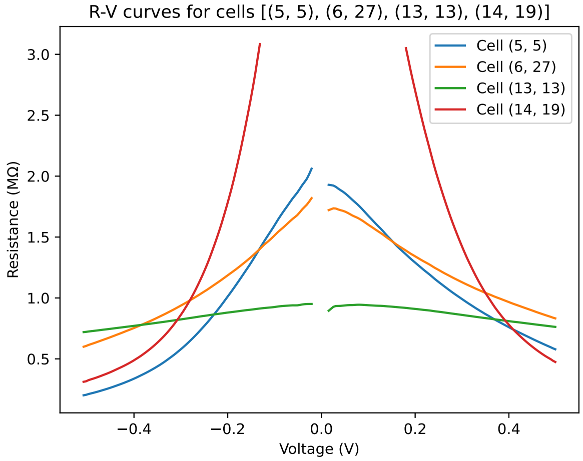

Fig. 4. Curves obtained from averaged read voltage sweeps of four memristors ($-0.5\ V$ to $+0.5\ V$) in various resistive states.

These results are similar to those shown previously, but include two more cells with very different resistive states. By taking the same methodology, using the resistance at $-0.5\ V$, and scaling up with the additional cells - $(5, 5)$, $(13, 13)$ in the "zeroes" set and $(6, 27)$, $(14, 19)$ in the "ones" set - a longer bit string can be generated. Based on comparing $(5, 5)$ with each of $(6, 27)$ and $(14, 19)$ first, the response would be '11', as both cells are greater in resistance than $(5, 5)$. The same comparison can then be made between $(13, 13)$ and cells $(6, 27)$ and $(14, 19)$, resulting in a response of '00', as both cells are lower in resistance than $(13, 13)$. The final PUF response would therefore be '1100'.

Because of the non-linearity, however, the response can vary depending on the test voltage. For example, at $-0.1\ V$, the PUF response is '0111' and at $+0.5\ V$ the response is '1010'. If these responses are then concatenated, a longer PUF string of '1100 0111 1010' is produced. Not only does this produce a much greater number of PUF bits per cell, but it also incorporates the non-linearity as an additional source of entropy. This additional entropy raises the difficulty in cloning the response considerably. Whilst three bits per comparison is proposed here as an example, by selecting different thresholds more bits per cell could be obtained. Additionally, the proposed architecture is general enough that different methods of generating a PUF response can be explored by attaching a different analysis to the gathered R-V curves.

C. Ageing Analysis

The same four memristor cells were separately characterised one month later to analyse the effects of ageing. These results are plotted in Fig. 5. Ageing was conducted by leaving the memristor wafer in room temperature and humidity for one month. Ideally the memristors should retain their state over this time.

The data measured at one month of ageing is based on fewer curves and less averaging, resulting in a much noisier plot than the original measurements.

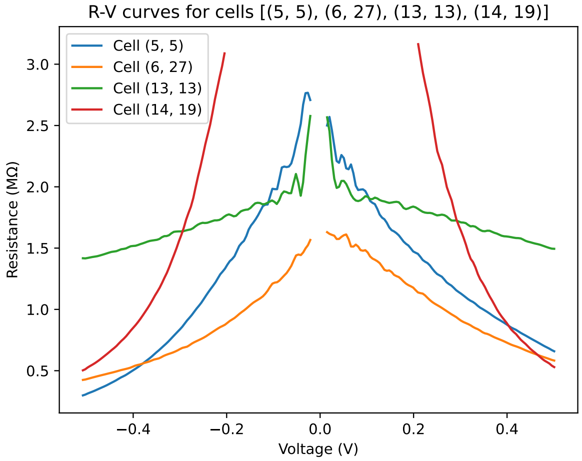

Fig. 5. Curves obtained from averaged read voltage sweeps of four memristors ($-0.5\ V$ to $+0.5\ V$) in various resistive states after one month of ageing.

As can be seen in the plots, the resulting curves are visually very similar in shape to original measurements. There are, however, absolute differences between the results. Cell $(6, 27)$ in particular has become lower in resistance. Notably, however, is that the relative resistance priorities of the other cells at $-0.5\ V$ and $+0.5\ V$ has remained the same as previously. $-0.1\ V$ also marginally retains the same relative priorities between the other cells.

By analysing the curves in the same way as previously to generate a PUF response, a bit string of '1100 0101 0000' is produced. Compared to the original string this gives a BER of 25%.

Whilst this BER is not ideal, the curves do all appear visually similar in shape to the original, pre-ageing, response. The BER would also retain an effective > 1 bit per comparison PUF response, even after error correction [19]. A different scheme for identifying the curves to generate a fingerprint may be able to produce a better uncorrected response after ageing that is less affected by the shift in absolute resistances.

These ageing results are still positive and suggest the architecture has promise, particularly if a more ageing-resistant memristor technology is used.

IV. Comparison with Alternative Technologies

A comparison of this work (non-linearity memristor PUF) with alternative technologies is shown in table I.

TABLE I
Comparison with alternative technologies

	Technology			
Attack	***Key in Memory***	***SRAM PUF*** **[20]**	***Memristor PUF*** **[21]**	***Non-linearity MR PUF***
Over-production	N	Y	Y	Y
Cloning	Copying	Clonable	No Attacks	No Attacks
Key generation	N	Y	Y	Y
Unique ID	Y	Y	Y	Y
Auditable off-chip	N	Y	Y	Y
On-chip resources	Flash/ROM	SRAM	Crossbar RRAM	Standalone RRAM

The proposed architecture has a number of advantages over existing approaches. The most commonly used method of security for identification is a key which is then stored in memory. This, in itself, does not offer the ability to generate its own keys and requires an external system to produce a random key for storage. More problematic, however, is that keys stored in memory may be copied by an adversary with physical access in a way that is completely indistinguishable from the original key. Because the keys are stored only with binary data, with no physical variation from device-to-device, there is no way to determine whether the key is the original or a copy.

SRAM PUFs generate keys using the uncertainty in the initial power-on value of an SRAM memory. Because the state of an SRAM is undefined when power is applied, before resetting, the actual value of cells can depend in part on manufacturing variation. Whilst this has been exploited previously to create a PUF, this effect can be physically cloned in a way that the memories may be made indistinguishable by intentionally biasing the power on response. As an SRAM stores only digital data, a clone of that data cannot be effectively identified.

Many existing memristor-based PUFs ignore non-linearity and test at only a single voltage, or only depend on I-V characteristics weakly and incidentally [13], [21], [22]. In comparison, the main source of entropy in the proposed non-linearity based PUF is not on the state of the cell, but the variation in analogue I-V behaviour over a range of voltages. This variation is itself used to generate a PUF key, without depending on the resistive state of cells. When compared to [21], a memristive crossbar-based PUF which partly exploits variation in linearity, this work offers general applicability to any given reasonably-reliable memristive technology. This work also exploits the non-linearity directly as the main source of entropy, rather than relying on sneak paths in a crossbar slightly biasing results such as to have an effect in the resultant key. Some memristive technologies may be more suitable for this approach than others, however. Whilst the devices characterised for this analysis exhibit strong variation in linearity, other technologies may be more linear [14] or exhibit less variation.

V. Conclusions

This paper has proposed a new architecture for exploiting an emerging technology, memristive RRAM memories, as a PUF in a way which relies on the I-V non-linearity of the devices. The architecture differentiates itself from existing approaches by specifically targeting the non-linearity as a separate, more difficult to clone, characteristic of memristive memories. In analysing the data obtained by this approach, a three-bit-per-comparison PUF was demonstrated. This PUF offered a twelve-bit response with a 25% BER after one month of ageing using four tested memristor cells.

These results may be considered preliminary, but offer a strong foundation for further research and greater scaling. Such research should begin by analysing a large set of cells to lend stronger statistical significance to the demonstrated results. A larger pool of reliable RRAM cells could offer both greater entropy and the ability to produce a stronger PUF response. As well as this, a longer response would make the effects of error correction less consequential in terms of the reduction of entropy for the string. By researching alternative methods to generate a bit string from the obtained data, or using an architecture-specific error correction scheme, more reliable error rates may be attainable.

Since this work is based on only testing a specific TiO_x-based memristor technology, other memristive technologies should also be assessed for potential for use in an I-V non-linearity PUF. This could include whether variability remains unique for these technologies, or whether it may be strongly dependent on resistive state.

Acknowledgements

This work was supported by the UK Research and Innovation Centre for Doctoral Training in Machine Intelligence for Nano-electronic Devices and Systems [EP/S024298/1]. The authors would like to acknowledge the support of the EPSRC FORTE Programme Grant [EP/R024642/1] and the RAEng Chair in Emerging Technologies [CiET1819/2/93].

References

[1] F. Koushanfar, I. Hong, and M. Potkonjak, "Behavioral synthesis techniques for intellectual property protection," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 10, no. 3, p. 523–545, jul 2005. [Online]. Available: https://doi.org/10.1145/1080334.1080338

[2] E. Charbon, "Hierarchical watermarking in ic design," in *Proceedings of the IEEE 1998 Custom Integrated Circuits Conference (Cat. No.98CH36143)*, 1998, pp. 295–298.

[3] Y. Gao, S. F. Al-Sarawi, and D. Abbott, "Physical unclonable functions," *Nature Electronics*, vol. 3, no. 2, pp. 81–91, Feb 2020. [Online]. Available: https://doi.org/10.1038/s41928-020-0372-5

[4] Y. Yilmaz, V.-H. Do, and B. Halak, "Armor: An anti-counterfeit security mechanism for low cost radio frequency identification systems," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 4, pp. 2125–2138, 2021.

[5] X.-Y. Wang, P.-F. Zhou, J. K. Eshraghian, C.-Y. Lin, H. H.-C. Iu, T.-C. Chang, and S.-M. Kang, "High-density memristor-cmos ternary logic family," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 68, no. 1, pp. 264–274, 2021.

[6] F. Cai, J. M. Correll, S. H. Lee, Y. Lim, V. Bothra, Z. Zhang, M. P. Flynn, and W. D. Lu, "A fully integrated reprogrammable memristor–cmos system for efficient multiply–accumulate operations," *Nature Electronics*, vol. 2, no. 7, pp. 290–299, Jul 2019.

[7] S. S. Sarwar, S. A. N. Saqueb, F. Quaiyum, and A. B. M. H.-U. Rashid, "Memristor-based nonvolatile random access memory: Hybrid architecture for low power compact memory design," *IEEE Access*, vol. 1, pp. 29–34, 2013.

[8] X. Zhang, J. Lu, Z. Wang, R. Wang, J. Wei, T. Shi, C. Dou, Z. Wu, J. Zhu, D. Shang, G. Xing, M. Chan, Q. Liu, and M. Liu, "Hybrid memristor-cmos neurons for in-situ learning in fully hardware memristive spiking neural networks," *Science Bulletin*, vol. 66, no. 16, pp. 1624–1633, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2095927321002735

[9] F. Corinto, O. V. Krulikovskyi, and S. D. Haliuk, "Memristor-based chaotic circuit for pseudo-random sequence generators," in *2016 18th Mediterranean Electrotechnical Conference (MELECON)*, 2016, pp. 1–3.

[10] A. Dodda, N. Trainor, J. M. Redwing, and S. Das, "All-in-one, bio-inspired, and low-power crypto engines for near-sensor security based on two-dimensional memtransistors," *Nature Communications*, vol. 13, no. 1, p. 3587, Jun 2022. [Online]. Available: https://doi.org/10.1038/s41467-022-31148-z

[11] M. Masoumi, "Novel hybrid cmos/memristor implementation of the aes algorithm robust against differential power analysis attack," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 7, pp. 1314–1318, 2020.

[12] R. A. John, N. Shah, S. K. Vishwanath, S. E. Ng, B. Febriansyah, M. Jagadeeswararao, C.-H. Chang, A. Basu, and N. Mathews, "Halide perovskite memristors as flexible and reconfigurable physical unclonable functions," *Nature Communications*, vol. 12, no. 1, p. 3681, Jun 2021. [Online]. Available: https://doi.org/10.1038/s41467-021-24057-0

[13] A. Chen, "Utilizing the variability of resistive random access memory to implement reconfigurable physical unclonable functions," *IEEE Electron Device Letters*, vol. 36, no. 2, pp. 138–140, 2015.

[14] H. Jiang, C. Li, R. Zhang, P. Yan, P. Lin, Y. Li, J. J. Yang, D. Holcomb, and Q. Xia, "A provable key destruction scheme based on memristive crossbar arrays," *Nature Electronics*, vol. 1, no. 10, pp. 548–554, Oct 2018. [Online]. Available: https://doi.org/10.1038/s41928-018-0146-5

[15] M. S. Mispan, B. Halak, and M. Zwolinski, "Nbti aging evaluation of puf-based differential architectures," in *2016 IEEE 22nd International Symposium on On-Line Testing and Robust System Design (IOLTS)*, 2016, pp. 103–108.

[16] Y. S. Chen, H. Y. Lee, P. S. Chen, P. Y. Gu, C. W. Chen, W. P. Lin, W. H. Liu, Y. Y. Hsu, S. S. Sheu, P. C. Chiang, W. S. Chen, F. T. Chen, C. H. Lien, and M.-J. Tsai, "Highly scalable hafnium oxide memory with improvements of resistive distribution and read disturb immunity," in *2009 IEEE International Electron Devices Meeting (IEDM)*, 2009, pp. 1–4.

[17] F. Alonso, D. Maldonado, A. Aguilera, and J. Roldán, "Memristor variability and stochastic physical properties modeling from a multivariate time series approach," *Chaos, Solitons & Fractals*, vol. 143, p. 110461, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0960077920308535

[18] H. Jiang, D. Belkin, S. E. Savel'ev, S. Lin, Z. Wang, Y. Li, S. Joshi, R. Midya, C. Li, M. Rao, M. Barnell, Q. Wu, J. J. Yang, and Q. Xia, "A novel true random number generator based on a stochastic diffusive memristor," *Nature Communications*, vol. 8, no. 1, p. 882, Oct 2017. [Online]. Available: https://doi.org/10.1038/s41467-017-00869-x

[19] M. Hiller, L. Kürzinger, and G. Sigl, "Review of error correction for pufs and evaluation on state-of-the-art fpgas," *Journal of Cryptographic Engineering*, vol. 10, no. 3, pp. 229–247, Sep 2020. [Online]. Available: https://doi.org/10.1007/s13389-020-00223-w

[20] K. Liu, Y. Min, X. Yang, H. Sun, and H. Shinohara, "A 373-f2 0.21%-native-ber ee sram physically unclonable function with 2-d power-gated bit cells and V_{ss} bias-based dark-bit detection," *IEEE Journal of Solid-State Circuits*, vol. 55, no. 6, pp. 1719–1732, 2020.

[21] H. Nili, G. C. Adam, B. Hoskins, M. Prezioso, J. Kim, M. R. Mahmoodi, F. M. Bayat, O. Kavehei, and D. B. Strukov, "Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors," *Nature Electronics*, vol. 1, no. 3, pp. 197–202, Mar 2018. [Online]. Available: https://doi.org/10.1038/s41928-018-0039-7

[22] S. Lv, J. Liu, and Z. Geng, "Application of memristors in hardware security: A current state-of-the-art technology," *Advanced Intelligent Systems*, vol. 3, no. 1, p. 2000127, 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/aisy.202000127