International Journal of Safety and Security Engineering
Vol. 13, No. 2, April, 2023, pp. 349-358
Journal homepage: http://iieta.org/journals/ijsse

Memristive Physical Unclonable Functions: The State-of-the-Art Technology

Nawras Hussain Al-Khaboori, Israa Badr Al-Mashhadani*

Department of Computer Engineering, College of Engineering, Al-Nahrain University, Baghdad 10070, Iraq

Corresponding Author Email: israa.b.al-mashhadani@nahrainuniv.edu.iq

https://doi.org/10.18280/ijsse.130217

Received: 7 March 2023
Accepted: 30 March 2023

Keywords:
memristor, physical unclonable functions, PUF, memristive PUF, hardware security

ABSTRACT

Internet of Things connected many useful electronic devices to each other through the internet, and sharing private and sensitive data between these devices needs secure access and communication. One of the best solutions for this purpose is hardware security primitives such as Physically Unclonable Functions (PUFs). PUFs are cryptographic primitives that are employed to produce a unique and reliable digital fingerprint for a particular electronic circuit. This digital fingerprint is used in many security applications such as chip identification, authentication, and secret key storage and generation. The emergence of memristors (Memory-Resistor) as new nanotechnologies are utilized extensively in hardware security applications such as Memristive PUFs. Research progress in Memristive PUFs resulted in improved performance metrics of PUFs due to memristors' unique characteristics. This article provides an investigation of different design approaches of Memristive PUFs that were introduced in the literature. Then, provide detailed performance evaluation results obtained by simulation and fabrication processes for different Memristive PUFs designs, and make a comparison between these results. Finally, concluded that most of the circuits are evaluated by simulation, whereas few other circuits were evaluated by fabrication owing to the expensive fabrication process. Since the memristor is a prototype and not commercialized yet, it is expected to be adopted and marketed in the next generation of hardware security.

1. INTRODUCTION

Physical Unclonable Functions (PUFs) are primitives for hardware security that are designed to address security issues with less power consumption and performance overhead while enhancing security [1]. In the PUF scenario, each PUF instance generates a different output for a given applied input. The output depends not only on the input but also on the PUF instance's built-in randomization, which means two identical PUF devices will generate different outputs for the same input [1]. The emergence of a memristor as new nanotechnology with PUF design made a new challenge that gained the attention of researchers [2]. Due to the stochastic switching mechanism and the model complexity resulting from the inherent variations of memristors, the implementation of PUF with nanotechnologies like memristors was strongly motivated. Memristive PUFs (M-PUFs) are the improved version of PUFs that is based on memristor device which has been offered for numerous security applications, such as a lightweight solution to secure IoT device identification, authentication, and secret key storage and generation.

Compared to other traditional cryptographic solutions, in traditional cryptographic solutions, secret keys are kept in either volatile or non-volatile memory. An adversary can access the system and read the content of memory to steal the key such as side-channel attacks toward memory [3]. The fundamental goal of the first PUF development is to offer hardware security that is resistant to any computational power supplied by an attacker, it is an effective method of protecting the secret keys [1]. The secret keys generated by PUF are generated only when required and not permanently stored on the chip, this will increase the Integrated Circuits (ICs) tamper resistance. The focus of this paper was on the state-of-the-art of M-PUF designs, which depend on manufacturing process changes, stochastic processes, and the memristor's I-V characteristics to produce a distinctive and trustworthy digital fingerprint for a different electronic circuit. Since M-PUFs take advantage of the inherent physical changes that occur naturally during the manufacture of hardware devices and which cannot theoretically be reproduced as some of them are unpredictable and uncontrollable. These differences are the source of the entropy that makes the responses unique. While the emergence of memristors provides a new opportunity for low-power devices with fast ON-OFF switching speeds. These characteristics are desirable for building secure, lightweight, low-power, and fast PUFs for object authentication. The current-voltage (I-V) characteristic, which displays a hysteresis loop that pinched in the I-V plane, is the memristor's unique property. This pinched hysteresis loop serves as a memristor's fingerprint. Where the input signal's voltage or current waveform is zero and always passes through the origin at all times. Assuming that each IoT-communicated device has its memristor device and applying a current over each memristor device will produce unique voltage values.

2. MEMRISTOR BACKGROUND

Memristor (memory-resistors) is a two-terminal non-linear passive element that was authorized by Chua [4] in 1971, as a fourth passive element and added to the first three: resistors, capacitors, and inductors. Memristor's mathematical

expression is **M=dq/dφ**, which represents the connection between the flux φ and the charge q, as shown in Figure 1. Memristors are compatible with Complementary Metal Oxide Semiconductor (CMOS) technology and are frequently used for crossbar arrays on silicon (Si) wafers [5]. Every two crossing wires in the crossbar are connected by a memristor, forming a fully interconnected mesh of vertical wires. These arrays have been proposed for use in memory applications owing to the memristor's non-volatility, non-linearity, nano-scalability, and programmability. Memristors are recently used for many applications but one of the most important applications is using it in a hardware security application.

In 2008, researchers at Hewlett-Packard (HP) labs presented the first physical model of memristors [6]. After that, different memristors models with various switching behaviors have been suggested, such as inter-facial switching [7], Phase-Change Memory (PCM) [8], filamentary switching [9], Valence-Charged Memory (VCM) [10], Electrochemical Metallization Memories (EMM) and VCM [11], EMM [12]. A complete understanding of the switching mechanisms of memristors is given in [13]. The linear and non-linear ion drift memristor models are the most used with PUF. Before the fabrication of the memristor device, it was just a theoretical concept. The HP laboratory team created the first physical memristor model utilizing titanium dioxide (TiO_2), and they presented the most basic design of the device [14] as shown in Figure 2.

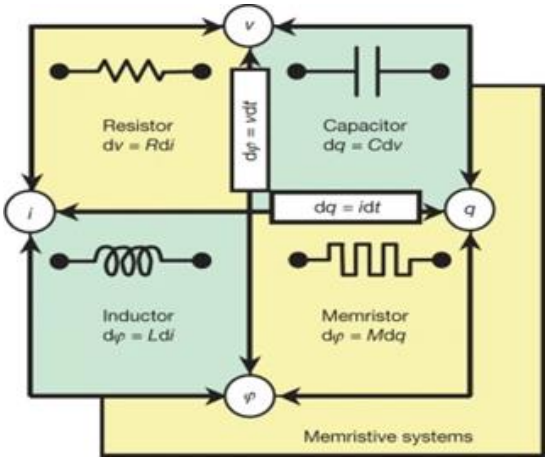
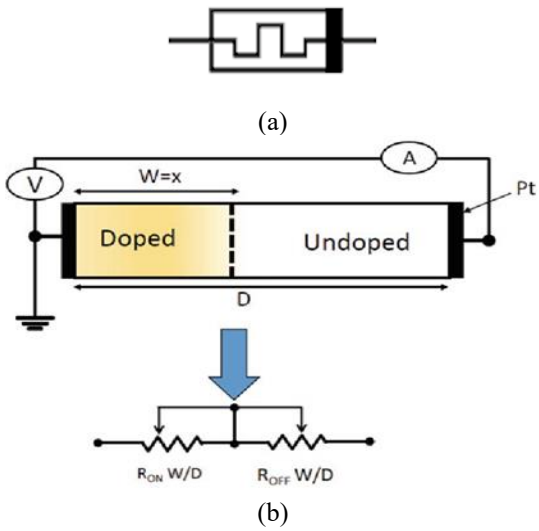
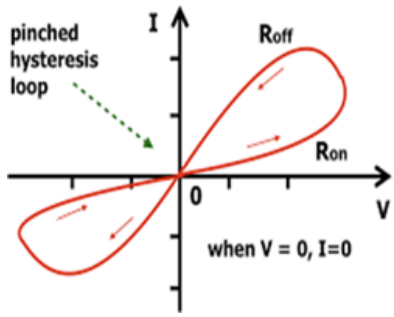


Figure 1. Relationship between individual RCLM elements and the equivalent representations [6]



(a)

(b)



(c)

Figure 2. Memristive device and its equivalent circuit proposed by the HP Lab (a) memristor symbol (b) memristor equivalent circuit (c) pinched hysteresis loop in I-V plane [6]

The HP model was the first two-terminal nano-technology device that displayed a hysteresis loop that was squeezed in the I-V plane [6], but researchers found that this model has some drawbacks that need to be fixed. Since a genuine memristor is a nonlinear device, the initial linear HP model is not appropriate for creating a functional emulation circuit or application. To overcome this device's limitations, researchers directed using a nonlinear window function to add nonlinearity behavior to linear HP model. Different window functions are proposed, the first window function was proposed in the study [15], it is called the Joglekar window function. this window function had some limitations that prompted to the improvement of a new window function called by Biolek et al. [16] window function. However, these early window functions do not offer a scale factor or threshold mechanism, therefore it cannot be managed [17], in order to overcome this restriction, a different window function with the scaling factor was offered, called by Prodromakis et al. [18] window function. This window function is likewise inappropriate for programming analog circuits due to the boundary lock problem, in order to address this problem, a new window function is proposed in the study [19]. All of the window functions described above are fully compared in the study [20]. An exponential nonlinear memristor model was proposed based on the experimental results in the study [21], Recent memristor applications have used this model extensively. There are other models of memristor, these models are Simmons Tunneling Barrier Model (STBM) [22], Threshold Adaptive Memristor Model (TEAM) [17], the Generalized Memristor Model (GMM) [23], and the Voltage Threshold Adaptive Memristor model (VTEAM) [24].

3. PHYSICAL UNCLONABLE FUNCTION (PUF) BACKGROUND

PUF is a lightweight primitive for hardware security, that maps a series of challenges (inputs) to a series of responses (or outputs) through a physical system to generate a device-specific cryptographic key [1]. PUFs are unclonable, robust, and unpredictable. PUF's unclonability characteristic specifies that its Challenge-Response Pairs (CRPs) can't be duplicated by other PUF instances. PUF's robustness comes from consistently producing identical responses to a given applied challenge every time. And PUF's unpredictability refers to its random procedure. PUFs are resistant to assaults since these variances are concealed from physical inspection and only detected when necessary [25].

PUFs make use of several physical electrical parameters, including frequency, voltage, current, time, bistable states, and capacitance to produce a unique identifier for each IC [26]. For example: in Arbiter PUF (A-PUF), to create one random bit, the propagation delays of two signals across two symmetric paths are compared [27]. Similarly in Ring-Oscillator PUF (RO-PUF), in order to create random response bits, the frequencies of two identical PUFs are compared [28], where Butterfly PUF (B-PUF), a cross-coupled circuit that is capable of being brought to a floating unstable state before being allowed to settle into one of the two potential stable states [29]. In the case of PUF, different performance metrics are measured such as uniformity, uniqueness, reliability and bit-aliasing [30], a short description of these performance metrics will be discussed below:

Uniformity: characterizes how the proportion of '0' and '1' in the responses of one PUF is uniform, the probability of '1's should be equal to the probability of '0's ideally. And it is computed as the fractional Hamming Weight (HW) of the total responses as in Eq. (1).

$$Uniformity(i) = \frac{1}{n} * HW(Ri) \times 100\% \quad (1)$$

where, *Ri*: is the n-bit responses from the chip *i*, *HW*(*Ri*): is the number of '1's in the responses. The value is predicted to be close to 50% in the ideal case.

Uniqueness: characterizes how can easily distinguish one PUF instance from another PUF instance. Uniqueness is a measure of inter-chip differences, so each pair of chips should be considered. It can be evaluated with the average fractional inter-chip Hamming Distance (HD) among responses generated by the same challenges from different chips as in Eq. (2).

$$Uniq. = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(R_i,R_j)}{n} \times 100\% \quad (2)$$

where, *k*: is the number of PUF chips and R_i, R_j: are the n-bit responses generated by chips *i* and *j* respectively. The value is predicted to be close to 50% in the ideal case.

Reliability: characterizes the ability of PUF to generate responses in different environmental conditions such as temperature and supply voltage. The average fractional HD intra-chip among responses generated by the same challenges on the same chip is used to calculate reliability as in Eq. (3) and (4):

$$HDintra(i) = \frac{1}{x} \sum_{y=1}^{x} \frac{HD(Ri,R'i,y)}{n} \times 100\% \quad (3)$$

where, *x*: is the number of samples that be collected from chip *i*, all are in the same environment, R_i: is the n-bit responses from chip *i* in some environmental condition, and $R'_{i,y}$: the responses of the *y*th sample in a different condition. The reliability of the PUF on chip *i* is defined as in Eq. (4):

$$Reliability = 100\% - HDintra\ (i) \quad (4)$$

The value is predicted to be close to 100% in the ideal case.

Bit-aliasing: identifies the similarities between PUFs' responses. Different ICs may generate similar results when bit-aliasing occurs. The bit-aliasing of the *l*-th bit of an n-bit response is the average hamming weight of the *l*-th bit across several *k* devices. The ideal value is 50% and it is defined as in Eq. (5):

$$Bit - aliasing\ = \frac{1}{k} * \sum_{i=1}^{k} ri,l \times 100\% \quad (5)$$

where, *k*: is the number of PUF chips, and *ri, l,*: is the *l*-th bit of the response in n-bit response. For more information, an overview of many PUF circuits is available in the study [31-33].

4. IMPLEMENTATION OF MEMRISTIVE PUF (M-PUF)

PUF is a hardware security primitive, that aims to mitigate counterfeiting, side-channel assaults, and piracy [34]. After emerging new nanotechnologies such as memristors, PUF has been gaining more attention [35]. Physically Unclonable Functions (PUFs) are mainly used in hardware security for chip identification and authentication. PUFs for semiconductor devices use natural cell-level variations inherent in silicon to create a unique, non-clonable device response to a specific input. Every chip ever produced has natural process variations that make them physically different, even for chips from the same wafer. Differences in threshold voltages, for example due to microscopic variations between transistors, are inherently random and can be exploited to create a truly unique cryptographic key in each chip (hardware level). Therefore, we can call this unique key a chip's fingerprint.

Non-Volatile Memory-based PUFs such as Memristor-based PUFs' feasibility and quality are investigated in the study [36]. M-PUFs have been proposed to enhance the performance metrics for numerous applications, including tamper detection, digital signature, authentication, identification, and random number generation [37]. The authors [2] proposed Memristor-based Public Physical Unclonable Functions (M-PPUFs) to enable second-secure party protocols like time-limited authentication and remote secret key exchange that will take many years for an adversary to compromise. In the study [34], the authors introduced a unique M-PUF design that uses differences in a memristor's write-time as an entropy source. The results demonstrate good statistical performance in terms of reliability, uniformity, and bit aliasing. In the study [38], in order to avoid the requirements for statically assigned input and output pins, the authors suggested using bidirectional memristors in a suggested architecture for public PUF polyomino partitioning. They also clarified how to implement authentication and remote secret key exchange protocols. In the study [39, 40], in order to validate the possibilities of nanoelectronics hardware security solutions, the authors give an overview of PUF architectures and circuits based on memristors. In the study [41], the author presented a memristor-based PUF that makes use of a weak-write method to obtain process-variable, cell-based behavior that is used as a PUF response. They also evaluated memristor PUFs under random process changes. The authors [42] presented the use of a readout method that uses the non-volatile resistive memory (RRAM) device's total resistance variation to control the delay of a current-controlled ring oscillator. The authors [36] investigated the memory-based PUFs' viability and quality, they suggested an emerging Nonvolatile Memory (e-NVM) -based PUF.

The authors [43] suggested a Non-Volatile Memory-based PUF (NVM-PUF) that can eliminate bit flips without using

auxiliary data. This NVM-PUF is mostly helpful for encoding applications that demand the exact regeneration of secret bitstrings. In the study [44], the fabricated Memristor-based PUFs (M-PUFs) were reported by the playwrights. The six memristors they created exhibit good reliability and a PUF response with a 50% uncertainty with repeated interrogation. The authors [45] created a strong PUF based on on-chip memristors (M-sPUF), which serve as a reconfigurable PUF (r-PUF). This model illustrates the desired properties of PUFs, such as uniqueness, reliability, and the quantity of CRPs. The authors [46] provided instructions for developing hardware security primitives by making use of the distinct characteristics of newly developed nanoelectronics components including memristors, in addition to talking about hardware security fundamentals for topics like data encryption, digital signatures, and authentication.

The study [47] reported the crossbar memristive PUF (M-XbarPUF) for many applications, including key generation for encryption and authentication. The authors [48, 49] suggested a CMOS-memristive delay-based PUF. In the study [50], a two-dimensional crossbar array was used to improve the write-time-based memristive PUF that was presented previously in the study [42]. The authors [51] provide a summary of the M-PUF circuits proposed in the study [42, 50]. The authors [52] proposed a PUF based on reconfigurable Resistive RAM (RRAM). In the study [53], an evaluation strategy for RRAM PUF was described. The authors [54] presented an RRAM PUF model, to reduce the possibility of early lifetime failure, one response bit was generated using the total of read-out currents from several RRAMs. The authors [35] provide an overview of existing PUF devices based on several technologies, including memristors. They came to the conclusion that M-PUFs have promising reproducibility, uniqueness, uniformity, and bit-aliasing properties.

In the study [55], an optimization-theoretic attack on the target PUFs which include the Arbiter PUF (APUF) and the Memristor Crossbar PUF (M-XbarPUF) is proposed by the authors. In the study [56], in order to understand how such nanoscale technologies, affect power, area, and latency in comparison to traditional CMOS-based approaches, the authors investigate a few instances of nanoelectronics security. In the study [57], the expression "hardware security primitive" was used by the authors to refer to memristor PUFs, moreover, they proposed a modification to the CMOS-memristor-based PUF structure initially described in the study [49] to make it resistant against cryptanalysis. The authors [58] investigated Memristor-based XbarPUFs under different temperature conditions and supplied voltage. They also suggested a technique to make such circuits more reliable. In this paper [59], circuit configurations are suggested to boost differences and enhance the Memristive Arbiter PUF (APUF) statistical performance including uniqueness, uniformity, and bit-aliasing. The authors [60] showed how to physically implement a trustworthy and tamper-resistant RRAM-based PUF, they also demonstrated trade-offs between performance and security, on the one hand, and latency, area, and energy consumption, on the other. The authors [61] proposed a new M-PUF as a hardware security solution. A new NVM-based PUF with a memristor technology survey was provided [62].

The paper's [63] main topic was crossbar PUF design factors. Additionally, several design changes were suggested to increase the PUF's resistance to machine learning attacks. RRAMs are used by the authors to modify the conventional CMOS time-delay-based PUF (TD-PUF) [64]. The authors [65] presented memristor-based XbarPUF with a large number of CRPs. The researchers [66] reported a PUF circuit that minimizes the impact of resistance window degradation based on RRAM's inherent resistance variations and the differential read-out technique. They enhanced the RRAM PUF's performance and reliability and showed its potential for use in IoT applications as a lightweight security solution. Detailed overviews and tutorials on recently created NVM-based PUFs, including memristors, were provided by the authors [67, 68]. The authors [69] suggested an attacking strategy based on side-channel information and optimization theory, where they estimate manufacturing variances of the circuit parts and estimate the PUF's responses to challenging vectors whose actual responses are unpredictable. They use this attack strategy on a variety of well-known PUF designs, including the APUF, M-XbarPUF, and the XOR Arbiter PUFs (XOR-APUF). In the study [70], the sensing amplifier was proposed by the authors and combined with an XbarPUF. The authors [71] demonstrated how memristors can be used to define safe and compact user authentication systems. In the study [72], a strategy based on memristive PUFs was suggested for protecting IoT devices. The authors [73] experimentally proved the ability of a physical fingerprint to execute verified key destruction. They also created a comprehensive procedure based on verifiable key destruction for re-lockable logic modules that combine computing, memory, and security functions. The authors [74] validated a PUF circuit by experiment. In the study [75], to authenticate users and perform sneak path integrity checks on stored data in the crossbar array, the authors included a PUF circuit. They showed how memristive crossbar arrays might be used for both memory and PUF applications.

In study [76], on the RO-PUF, two major modifications are suggested. The first modification is the addition of the memristor to the RO's inverting units, and the second is a change in how the PUF's response is generated. Other ROPUF designs only produce one response bit from each pair of RO, whereas the proposed memristor-based ROPUF produces many response bits from each sequence of pairs of RO. The authors [77] proposed a security system that utilizes a memristor-based PUF along with memristors as non-volatile backup memory. The proposed system is highly lightweight and offers enough security. The authors [78] introduced reconfigurable RRAM PUF based on the shared jitter noise's random dynamic entropy. The authors [79] reviewed experimental work on emerging nonvolatile memory-based security primitives. The author [80] reviewed emerging nanotechnologies including memristors in terms of hardware security, and also explored how they could be used to improve hardware security. The authors [81] reconstruct a variety of memristor-PUFs and comprehensively evaluate their unpredictable properties. They demonstrate that modeling memristor-PUFs with high prediction rates of 98% is possible by utilizing machine learning algorithms. The authors [82] proposed the PUF to overcome the limitations of current security strategies, TiO_x/Al_2O_3-based memristors are used to fabricate a 32x32 crossbar array, and its electrical properties, including its set voltage distribution, are examined. The authors [83] reviewed memristive PUFs (Physical Unclonable Functions) mentioned in the literature and defined the inducement for the usage of memristor technology for enforcing PUFs. they focused on PUFs' applications, sizes, analysis, and physical variations. In addition, they provided the variety of samples generated the usage of Monte Carlo

simulation for evaluating the PUF circuits and additionally defined the protocols, functionality, and methodologies proposed in the memristive PUF literature.

In the study [84], a transient form of diffusive memristors with W/Ag/MgO/Ag/W cross-point structures was developed for physical unclonable functions (PUF) for the first time. In the study [85], It is shown how to create a highly secure neuromorphic system utilizing a physically unclonable function (PUF) that makes use of high entropy produced by a memristor's stochastically switching made of poly (1,3,5-trivinyl-1,3,5-trimethyl cyclotrisiloxane) (pV3D3). The authors [86] suggest two methods for enhancing PUFs' resistance to ML attacks. Each cross-point device should contribute as much as possible to the PUF output in order to reduce the predictability of the response, which is the general concept behind both ideas.

5. CLASSIFICATION AND COMPARISON OF DIFFERENT DESIGN APPROACHES OF MEMRISTIVE PUF (M-PUF)

The classification of different design approaches of Memristive PUFs that were investigated in the previous section has been summarized in Table 1, which contained detailed information on the proposed models including the model type, the implementation process type if it's simulated or fabricated, and the size of both M-PUF and CRPs. The increase in the size of the memristor circuit appears to be the cause of the growth in the size of M-PUF circuits, and it is expected that the number of challenge-response bits will increase when the real implementation of memristor PUFs occurs. Tables 2 and 3 investigate the comparison in performance metrics results obtained by the simulation process and fabrication process respectively. The results demonstrated that uniqueness and uniformity are almost at the 50% optimum value and also point to M-PUFs' resistance to modeling threats. Comparing between different results of performance metrics obtained by both simulation and fabrication processes, it's clear that the highest value of uniformity metric is equal to 52.3% obtained from the simulated design [49]. Where the highest value of the uniqueness metric is equal to 51.06% obtained from the simulated design [57], the highest value of the bit-aliasing metric is equal to 52.35% obtained from the simulated design [52], and the highest value of the reliability metric is equal to 100% obtained from the fabricated design [61].

Table 1. Classification of different design approaches of M-PUFs

Ref.	Year	Model	Process Type		Memristive PUF circuit size and the number of used CRPs		
			Simulation	Fabrication	M-PUF size	Challenge-Number C	Response-Number R
[2]	2012	Memristor-based Public Physically Unclonable Functions (M-PPUFs)	Yes	No	n×m	n-bit	m-bit
[34]	2013	Write-time memristor-based PUF	Yes	No	n×n	n-bit	n-bit
[38]	2013	Memristor-based Public Physically Unclonable Functions (M-PPUFs)	Yes	No	n×m	n-bit	m-bit
[41]	2013	memristor-based PUF (M-PUF)	Yes	No	n×m	n-bit	m-bit
[42]	2013	memristor-based Ring Oscillator PUF(M-ROPUF)	Yes	No	1600	40	40
[36]	2014	emerging Non-Volatile Memory Based PUF (eNVM-PUF)	Yes	No	n×m	m/2 bit	m/2 bit
[43]	2014	Non-Volatile Memory Based PUF (NVM-PUF)	No	Yes	1600	40	40
[44]	2014	Memristor-based Polyomino PUFs	No	Yes	1×1	1	1
[45]	2015	Memristor-based strong PUF (M-sPUF)	Yes	No	1600	40	40
[47]	2015	Memristive Crossbar PUF	Yes	No	n×m	n-bit	m-bit
[48]	2015	Memristor-CMOS hybrid XOR/XNOR PUF	Yes	No	4n	n-bit	1
[49]	2015	Hybrid memristor- CMOS PUF	Yes	No	2n	n-bit	1
[50]	2015	Two dimensions one Zener diode-one memristor (1ZD1M) based PUF	Yes	No	n×n	n/2-bit	n/4-bit
[52]	2015	PUF is based on reconfigurable Resistive RAM (RRAM).	Yes	No	m×n	n-bit	m-bit
[54]	2015	Resistive RAM (RRAM) based PUF	No	Yes	1024	7	128
[57]	2016	Memristor-Based Arbiter PUF	Yes	No	2n	n-bit	1
[58]	2016	memristive crossbar PUF (XbarPUF)	Yes	No	m×n	n-bit	m-bit
[59]	2016	memristive Arbiter PUF (APUF)	Yes	No	160 or 320	32 or 64	4 or 8
[60]	2016	Resistive RAM (RRAM) based PUF	No	Yes	1024	7	128
[61]	2016	Resistive RAM (RRAM) based PUF	No	Yes	144	12	12
[63]	2017	XORed memristive crossbar PUF (XbarPUF	Yes	No	m×n	n-bit	m-bit
[64]	2017	Resistive RAM (RRAM) based time delay PUF	Yes	No	48	1	1
[65]	2017	Memristive crossbar PUF (XbarPUF)	Yes	No	m×n	n-bit	m-bit
[66]	2017	Resistive RAM (RRAM) based PUF	No	Yes	1024	3	128

[71]	2018	Memristor-based weak PUF	Yes	No	4×4	4	16
[73]	2018	Memristor-based PUF	No	Yes	8192	7	4096
[74]	2018	Memristor-based PUF	No	Yes	10×20	10	20
[75]	2019	Memristor-based APUF	Yes	No	m×n	8, 16, 32	4 or 8
[76]	2019	Memristor-based ROPUF	Yes	No	m×n	n-bit	m-bit
[77]	2019	Memristive crossbar PUF (XbarPUF)	Yes	No	m×n	n-bit	m-bit
[78]	2019	Resistive RAM (RRAM) based PUF	No	Yes	m×n	n-bit	m-bit
[81]	2020	Hybrid RRAM based APUF	Yes	No	m×n	n-bit	m-bit
[82]	2021	Selected Bit-Line Current PUF based on crossbar array	No	Yes	2^n	n-bit	m-bit
[83]	2022	Transient Form of Memristors-based PUF	No	Yes	n×n	n-bit	n-bit
[84]	2022	pV3D3 memristor-based PUF	No	Yes	n×n	n-bit	n-bit
[85]	2022	Memristive Strong PUFs	Yes	No	n×n	n-bit	n-bit

Table 2. M-PUF Performance metrics analysis obtained by the simulation process

Ref.	Year	Performance Metrics			
		Uniformity (50%)	Uniqueness (50%)	Bit-aliasing (50%)	Reliability (100%)
[2]	2012	-	49%	-	49%
[34]	2013	49.99%	-	49.99%	99.7%
[38]	2013	-	-	-	-
[41]	2013	50%	-	-	-
[42]	2013	-	50%	-	-
[36]	2014	-	49%	-	-
[45]	2015	50.76%	50.07%	-	-
[47]	2015	50.6%	49.98%	-	-
[48]	2015	47.27%	49.57%	52.35%	-
[49]	2015	52.3%	50.04%	50.7%	96%
[50]	2015	50.2%	50%	-	95.1%
[52]	2015	50%	50%	-	-
[57]	2016	51.2%	51.06%	50.6%	99.7%
[58]	2016	51.43%	48.57%	51.43%	-
[59]	2016	49.795%	50.006%	49.8%	-
[63]	2017	-	-	-	-
[65]	2017	-	-	-	-
[71]	2018	-	50.68%	-	-
[75]	2019	49.7%	49.9%	49.8%	-
[76]	2019	51.43%	48.57%	51.43%	-
[77]	2019	-	50.09%	50.833%	99.904%
[81]	2020	50.1%	49.5%	-	-
[85]	2022	-	-	-	-

Table 3. M-PUF performance metrics analysis obtained by the fabrication process

Ref.	Year	Performance Metrics			
		Uniformity (50%)	Uniqueness (50%)	Bit-aliasing (50%)	Reliability (100%)
[43]	2014	-	-	-	-
[44]	2015	-	50%	-	-
[54]	2015	49.8%	49.8%	-	-
[60]	2016	-	49.8%	-	-
[61]	2016	-	46.2%	-	100%
[64]	2017	-	-	-	97.3%
[66]	2017	-	49.8%	-	99%
[73]	2018	-	50.06%	-	86.18%
[74]	2018	49.5%	-	-	-
[78]	2019	-	-	-	-
[82]	2021	50.3%	48.1%	-	99.9%
[83]	2022	-	49.1%	-	-
[84]	2022	50%	50%	-	-

6. CONCLUSION

M-PUFs are being investigated by researchers for different applications, which include device identification, authentication, storage and generation of secret keys. M-PUFs take advantage of memristors' distinct characteristics, such as bi-directionality, model complexity, nonlinearity, non-volatility and nano-scalability to enhance performance metrics of PUF which include bit aliasing, uniformity, reliability, and uniqueness. Different applications of M-PUFs such as memory applications because of memristor non-volatility property and hardware security applications such as chip identification, authentication, and key generation since PUF is very sensitive to manufacturing process variation, therefore it will give different responses for each input. Also, the size of the M-PUF circuit is expected to increase after the real

marketing of the memristor device. The analysis of the result obtained by the fabrication process and simulation process shows the development of the fabrication before it is commercialized. Most of the circuits were evaluated by simulation, whereas few other circuits were evaluated by fabrication owing to the expensive fabrication process. In general, the results of M-PUF for different design approaches proposed in the literature display the advantages of M-PUFs over traditional CMOS PUFs with respect to performance metrics that were mentioned previously. Noting that the results obtained by the simulation process are superior to the results obtained by the fabrication process, since the focus in the fabrication was on the success of the operation more than the results achieved. The results also point to M-PUFs' resistance to modeling attacks, side-channel attacks, fault-injection attacks, and machine-learning attacks.

7. FUTURE WORK

It is important to understand the characterization, modeling, and design strategy of M-PUF devices in order to understand their security scheme. Memristor nanotechnology device is still under development and has not yet been made commercially available. The future challenges are to determine appropriate security measures for M-PUF evaluation because of the commonly used performance measures for CMOS PUFs only, and another challenge is understanding attacks against the memristive circuits, there could be new and unanticipated assaults that directly affected on memristor circuits and need to be taken into consideration. Technology research and prototype development of a memristor provided good statistical results that are utilized to improve PUF performance metrics that will be used in the next hardware security generation.

REFERENCES

[1] Gassend, B., Clarke, D., Van Dijk, M., Devadas, S. (2002). Silicon physical random functions. In Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 148-160. https://doi.org/10.1145/586110.586132

[2] Rajendran, J., Rose, G.S., Karri, R., Potkonjak, M. (2012). Nano-PPUF: A memristor-based security primitive. In 2012 IEEE Computer Society Annual Symposium on VLSI, pp. 84-87.

[3] Unterluggauer, T., Mangard, S. (2016). Exploiting the physical disparity: Side-channel attacks on memory encryption. In: Standaert, FX., Oswald, E. (eds) Constructive Side-Channel Analysis and Secure Design. COSADE 2016. Lecture Notes in Computer Science(), vol 9689. Springer, Cham. https://doi.org/10.1007/978-3-319-43283-0_1

[4] Chua, L. (1971). Memristor-the missing circuit element. IEEE Transactions on Circuit Theory, 18(5): 507-519. https://doi.org/10.1109/TCT.1971.1083337

[5] Xia, Q., Robinett, W., Cumbie, M.W., Banerjee, N., Cardinali, T.J., Yang, J.J., Wu, W., Li, X., Tong, W.M., Strukov, D.B., Snider, G.S., Medeiros-Ribeiro, G., Williams, R.S. (2009). Memristor−CMOS hybrid integrated circuits for reconfigurable logic. Nano Letters, 9(10): 3640-3645. https://doi.org/10.1021/nl901874j

[6] Strukov, D.B., Snider, G.S., Stewart, D.R., Williams, R.S. (2008). The missing memristor found. Nature, 453(7191): 80-83. https://doi.org/10.1038/nature06932

[7] Di Ventra, M., Pershin, Y.V. (2011). Memory materials: a unifying description. Materials Today, 14(12): 584-591. https://doi.org/10.1016/S1369-7021(11)70299-1

[8] Meister, S., Kim, S., Cha, J.J., Wong, H.S.P., Cui, Y. (2011). *In situ* transmission electron microscopy observation of nanostructural changes in phase-change memory. ACS Nano, 5(4): 2742-2748. https://doi.org/10.1021/nn1031356

[9] Xu, X., Lv, H., Liu, H., Gong, T., Wang, G., Zhang, M., Li, Y., Liu, Q., Long, S., Liu, M. (2014). Superior retention of low-resistance state in conductive bridge random access memory with single filament formation. IEEE Electron Device Letters, 36(2): 129-131. https://doi.org/10.1109/LED.2014.2379961

[10] Lim, E.W., Ismail, R. (2015). Conduction mechanism of valence change resistive switching memory: a survey. Electronics, 4(3): 586-613. https://doi.org/10.3390/electronics4030586

[11] Wedig, A., Luebben, M., Cho, D.Y., Moors, M., Skaja, K., Rana, V., Hasegawa, T., Adepalli, K.K., Yildiz, B., Waser, R., Valov, I. (2016). Nanoscale cation motion in TaO_x, HfO_x and TiO_x memristive systems. Nature Nanotechnology, 11(1): 67-74. https://doi.org/10.1038/nnano.2015.221

[12] Valov, I., Lu, W.D. (2016). Nanoscale electrochemistry using dielectric thin films as solid electrolytes. Nanoscale, 8(29): 13828-13837. https://doi.org/10.1039/C6NR01383J

[13] Sun, W., Gao, B., Chi, M., Xia, Q., Yang, J.J., Qian, H., Wu, H. (2019). Understanding memristive switching via in situ characterization and device modeling. Nature Communications, 10(1): 3453. https://doi.org/10.1038/s41467-019-11411-6

[14] Williams, R.S. (2008). How we found the missing memristor. IEEE Spectrum, 45(12): 28-35. https://doi.org/10.1109/MSPEC.2008.4687366

[15] Joglekar, Y.N., Wolf, S.J. (2009). The elusive memristor: properties of basic electrical circuits. European Journal of Physics, 30(4): 661. https://doi.org/10.1088/0143-0807/30/4/001

[16] Biolek, Z., Biolek, D., Biolkova, V. (2009). SPICE model of memristor with nonlinear dopant drift. Radioengineering, 18(2): 210-214.

[17] Kvatinsky, S., Friedman, E.G., Kolodny, A., Weiser, U.C. (2012). TEAM: Threshold adaptive memristor model. IEEE Transactions on Circuits and Systems I: Regular Papers, 60(1): 211-221. https://doi.org/10.1109/TCSI.2012.2215714

[18] Prodromakis, T., Peh, B.P., Papavassiliou, C., Toumazou, C. (2011). A versatile memristor model with nonlinear dopant kinetics. IEEE Transactions on Electron Devices, 58(9): 3099-3105. https://doi.org/10.1109/TED.2011.2158004

[19] Zha, J., Huang, H., Liu, Y. (2015). A novel window function for memristor model with application in programming analog circuits. IEEE Transactions on Circuits and Systems II: Express Briefs, 63(5): 423-427. https://doi.org/10.1109/TCSII.2015.2505959

[20] Elgabra, H., Farhat, I.A., Al Hosani, A.S., Homouz, D., Mohammad, B. (2012). Mathematical modeling of a memristor device. In 2012 international conference on

innovations in information technology (IIT), Abu Dhabi, United Arab Emirates, pp. 156-161. https://doi.org/10.1109/INNOVATIONS.2012.6207722
[21] Yang, J.J., Pickett, M.D., Li, X., Ohlberg, D.A., Stewart, D.R., Williams, R.S. (2008). Memristive switching mechanism for metal/oxide/metal nanodevices. Nature Nanotechnology, 3(7): 429-433. https://doi.org/10.1038/nnano.2008.160
[22] Pickett, M.D., Strukov, D.B., Borghetti, J.L., Yang, J.J., Snider, G.S., Stewart, D.R., Williams, R.S. (2009). Switching dynamics in titanium dioxide memristive devices. Journal of Applied Physics, 106(7): 074508. https://doi.org/10.1063/1.3236506
[23] Yakopcic, C., Taha, T.M., Subramanyam, G., Pino, R.E. (2012). Memristor SPICE modeling. In: Kozma, R., Pino, R., Pazienza, G. (eds) Advances in Neuromorphic Memristor Science and Applications. Springer Series in Cognitive and Neural Systems, vol 4. Springer, Dordrecht. https://doi.org/10.1007/978-94-007-4491-2_12
[24] Kvatinsky, S., Ramadan, M., Friedman, E.G., Kolodny, A. (2015). VTEAM: A general model for voltage-controlled memristors. IEEE Transactions on Circuits and Systems II: Express Briefs, 62(8): 786-790. https://doi.org/10.1109/TCSII.2015.2433536
[25] Pappu, R., Recht, B., Taylor, J., Gershenfeld, N. (2002). Physical one-way functions. Science, 297(5589): 2026-2030. https://doi.org/10.1126/science.1074376
[26] McGrath, T., Bagci, I.E., Wang, Z.M., Roedig, U., Young, R.J. (2019). A PUF taxonomy. Applied Physics Reviews, 6(1): 011303. https://doi.org/10.1063/1.5079407
[27] Lim, D., Lee, J.W., Gassend, B., Suh, G.E., Van Dijk, M., Devadas, S. (2005). Extracting secret keys from integrated circuits. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 13(10): 1200-1205. https://doi.org/10.1109/TVLSI.2005.859470
[28] Zhang, J.L., Qu, G., Lv, Y.Q., Zhou, Q. (2014). A survey on silicon PUFs and recent advances in ring oscillator PUFs. Journal of Computer Science and Technology, 29(4): 664-678. https://doi.org/10.1007/s11390-014-1458-1
[29] Kumar, S.S., Guajardo, J., Maes, R., Schrijen, G.J., Tuyls, P. (2008). The butterfly PUF protecting IP on every FPGA. In 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, Anaheim, CA, USA, pp. 67-70. https://doi.org/10.1109/HST.2008.4559053
[30] Maiti, A., Gunreddy, V., Schaumont, P. (2013). A systematic method to evaluate and compare the performance of physical unclonable functions. In: Athanas, P., Pnevmatikatos, D., Sklavos, N. (eds) Embedded Systems Design with FPGAs. Springer, New York, NY. https://doi.org/10.1007/978-1-4614-1362-2_11
[31] Chang, C.H., Zheng, Y., Zhang, L. (2017). A retrospective and a look forward: Fifteen years of physical unclonable function advancement. IEEE Circuits and Systems Magazine, 17(3): 32-62. https://doi.org/10.1109/MCAS.2017.2713305
[32] Babaei, A., Schiele, G. (2019). Physical unclonable functions in the internet of things: State of the art and open challenges. Sensors, 19(14): 3208. https://doi.org/10.3390/s19143208
[33] Gao, Y., Al-Sarawi, S.F., Abbott, D. (2020). Physical unclonable functions. Nature Electronics, 3(2): 81-91. https://doi.org/10.1038/s41928-020-0372-5
[34] Rose, G.S., McDonald, N., Yan, L.K., Wysocki, B. (2013). A write-time based memristive PUF for hardware security applications. In 2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, CA, USA, pp. 830-833. https://doi.org/10.1109/ICCAD.2013.6691209
[35] Bautista Adames, I.A., Das, J., Bhanja, S. (2016). Survey of emerging technology based physical unclonable funtions. In Proceedings of the 26th edition on Great Lakes Symposium on VLSI, pp. 317-322. https://doi.org/10.1145/2902961.2903044
[36] Zhang, L., Fong, X., Chang, C.H., Kong, Z.H., Roy, K. (2014). Feasibility study of emerging non-volatilememory based physical unclonable functions. In 2014 IEEE 6th International Memory Workshop (IMW), pp. 1-4. https://doi.org/10.1109/IMW.2014.6849384
[37] Rajendran, J., Karri, R., Wendt, J.B., Potkonjak, M., McDonald, N., Rose, G.S., Wysocki, B. (2012). Nanoelectronic solutions for hardware security. Cryptology ePrint Archive.
[38] Wendt, J.B., Potkonjak, M. (2013). The bidirectional polyomino partitioned PPUF as a hardware security primitive. In 2013 IEEE Global Conference on Signal and Information Processing, Austin, TX, USA, pp. 257-260. https://doi.org/10.1109/GlobalSIP.2013.6736864
[39] Rose, G.S., Rajendran, J., McDonald, N., Karri, R., Potkonjak, M., Wysocki, B. (2013). Hardware security strategies exploiting nanoelectronic circuits. In 2013 18th Asia and South Pacific Design Automation Conference (ASP-DAC), Yokohama, Japan, pp. 368-372. https://doi.org/10.1109/ASPDAC.2013.6509623
[40] Rose, G.S., McDonald, N., Yan, L.K., Wysocki, B., Xu, K. (2013). Foundations of memristor based PUF architectures. In 2013 IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH), Brooklyn, NY, USA, pp. 52-57. https://doi.org/10.1109/NanoArch.2013.6623044
[41] Koeberl, P., Kocabaş, Ü., Sadeghi, A.R. (2013). Memristor PUFs: a new generation of memory-based physically unclonable functions. In 2013 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, pp. 428-431. https://doi.org/10.7873/DATE.2013.096
[42] Kavehei, O., Hosung, C., Ranasinghe, D., Skafidas, S. (2013). mrPUF: A memristive device based physical unclonable function. arXiv preprint arXiv:1302.2191. https://doi.org/10.48550/arXiv.1302.2191
[43] Che, W., Plusquellic, J., Bhunia, S. (2014). A non-volatile memory based physically unclonable function without helper data. In 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, CA, USA, pp. 148-153. https://doi.org/10.1109/ICCAD.2014.7001345
[44] Mazady, A., Rahman, M.T., Forte, D., Anwar, M. (2015). Memristor PUF—A security primitive: Theory and experiment. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 5(2): 222-229. https://doi.org/10.1109/JETCAS.2015.2435532
[45] Gao, Y., Ranasinghe, D.C., Al-Sarawi, S.F., Kavehei, O., Abbott, D. (2015). Memristive crypto primitive for building highly secure physical unclonable functions.

Scientific Reports, 5(1): 12785. https://doi.org/10.1038/srep12785
[46] Rajendran, J., Karri, R., Wendt, J.B., Potkonjak, M., McDonald, N., Rose, G.S., Wysocki, B. (2015). Nano meets security: Exploring nanoelectronic devices for security applications. Proceedings of the IEEE, 103(5): 829-849. https://doi.org/10.1109/JPROC.2014.2387353
[47] Rose, G.S., Meade, C.A. (2015). Performance analysis of a memristive crossbar PUF design. In Proceedings of the 52nd Annual Design Automation Conference, pp. 1-6. https://doi.org/10.1145/2744769.2744892
[48] Mathew, J., Chakraborty, R.S., Sahoo, D.P., Yang, Y., Pradhan, D.K. (2015). A novel memristor based physically unclonable function. Integration, the VLSI journal, 51: 37-45. https://doi.org/10.1016/j.vlsi.2015.05.005
[49] Mathew, J., Chakraborty, R.S., Sahoo, D.P., Yang, Y., Pradhan, D.K. (2015). A novel memristor-based hardware security primitive. ACM Transactions on Embedded Computing Systems (TECS), 14(3): 1-20. https://doi.org/10.1145/2736285
[50] Potteiger, T., Robinson, W.H. (2015). A one Zener diode, one memristor crossbar architecture for a write-time-based PUF. In 2015 IEEE 58th International Midwest Symposium on Circuits and Systems (MWSCAS), Fort Collins, CO, USA, pp. 1-4. https://doi.org/10.1109/MWSCAS.2015.7282123
[51] Arafin, M.T., Dunbar, C., Qu, G., McDonald, N., Yan, L. (2015). A survey on memristor modeling and security applications. In Sixteenth International Symposium on Quality Electronic Design, Santa Clara, CA, USA, pp. 440-447. https://doi.org/10.1109/ISQED.2015.7085466
[52] Chen, A. (2014). Utilizing the variability of resistive random access memory to implement reconfigurable physical unclonable functions. IEEE Electron Device Letters, 36(2): 138-140. https://doi.org/10.1109/LED.2014.2385870
[53] Chen, A. (2015). Comprehensive assessment of RRAM-based PUF for hardware security applications. In 2015 IEEE International Electron Devices Meeting (IEDM), Washington, DC, USA, pp. 10.7.1-10.7.4. https://doi.org/10.1109/IEDM.2015.7409672
[54] Liu, R., Wu, H., Pang, Y., Qian, H., Yu, S. (2015). Experimental characterization of physical unclonable function based on 1 kb resistive random access memory arrays. IEEE Electron Device Letters, 36(12): 1380-1383. https://doi.org/10.1109/LED.2015.2496257
[55] Liu, Y., Xie, Y., Bao, C., Srivastava, A. (2016). An optimization-theoretic approach for attacking physical unclonable functions. In 2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), pp. 1-6. https://doi.org/10.1145/2966986.2967000
[56] Rose, G. S., Uddin, M., & Majumder, M. B. (2016, July). A designer's rationale for nanoelectronic hardware security primitives. In 2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Pittsburgh, PA, USA, pp. 194-199. https://doi.org/10.1109/ISVLSI.2016.114
[57] Chatterjee, U., Chakraborty, R.S., Mathew, J., Pradhan, D.K. (2016). Memristor based arbiter PUF: Cryptanalysis threat and its mitigation. In 2016 29th International Conference on VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID), Kolkata, India, pp. 535-540. https://doi.org/10.1109/VLSID.2016.57
[58] Uddin, M., Majumder, M.B., Rose, G.S., Beckmann, K., Manem, H., Alamgir, Z., Cady, N.C. (2016). Techniques for improved reliability in memristive crossbar PUF circuits. In 2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Pittsburgh, PA, USA, pp. 212-217. https://doi.org/10.1109/ISVLSI.2016.33
[59] Loong, J.T.H., Hashim, N.A.N., Hamid, F.A. (2016). Memristor-based arbiter Physically Unclonable Function (APUF) with multiple response bits. In 2016 IEEE student Conference on research and development (SCOReD), Kuala Lumpur, Malaysia, pp. 1-5. https://doi.org/10.1109/SCORED.2016.7810033
[60] Liu, R., Wu, H., Pang, Y., Qian, H., Yu, S. (2016). A highly reliable and tamper-resistant RRAM PUF: Design and experimental validation. In 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, USA, pp. 13-18. https://doi.org/10.1109/HST.2016.7495549
[61] Gao, L., Chen, P.Y., Liu, R., Yu, S. (2016). Physical unclonable function exploiting sneak paths in resistive cross-point array. IEEE Transactions on Electron Devices, 63(8): 3109-3115. https://doi.org/10.1109/TED.2016.2578720
[62] Gao, Y., Ranasinghe, D.C., Al-Sarawi, S.F., Kavehei, O., Abbott, D. (2016). Emerging physical unclonable functions with nanotechnology. IEEE Access, 4: 61-80. https://doi.org/10.1109/ACCESS.2015.2503432
[63] Uddin, M., Majumder, M.B., Rose, G.S. (2017). Robustness analysis of a memristive crossbar PUF against modeling attacks. IEEE Transactions on Nanotechnology, 16(3): 396-405. https://doi.org/10.1109/TNANO.2017.2677882
[64] Beckmann, K., Manem, H., Cady, N.C. (2016). Performance enhancement of a time-delay PUF design by utilizing integrated nanoscale ReRAM devices. IEEE Transactions on Emerging Topics in Computing, 5(3): 304-316. https://doi.org/10.1109/TETC.2016.2575448
[65] Rose, G.S., Majumder, M.B., Uddin, M. (2017). Exploiting memristive crossbar memories as dual-Use security primitives in IoT devices. In 2017 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Bochum, Germany, pp. 615-620. https://doi.org/10.1109/ISVLSI.2017.114
[66] Pang, Y., Wu, H., Gao, B., Deng, N., Wu, D., Liu, R., Yu, S., Chen, A., Qian, H. (2017). Optimization of RRAM-based physical unclonable function with a novel differential read-out method. IEEE Electron Device Letters, 38(2): 168-171. https://doi.org/10.1109/LED.2016.2647230
[67] Rahman, F., Nath, A.P.D., Bhunia, S., Forte, D., Tehranipoor, M. (2017). Composition of physical unclonable functions: from device to architecture. In Security Opportunities in Nano Devices and Emerging Technologies, CRC Press, pp. 177-196.
[68] Sahay, S., Suri, M. (2017). Recent trends in hardware security exploiting hybrid CMOS-resistive memory circuits. Semiconductor Science and Technology, 32(12): 123001. https://doi.org/10.1088/1361-6641/aa8f07
[69] Liu, Y., Xie, Y., Bao, C., Srivastava, A. (2017). A combined optimization-theoretic and side-channel approach for attacking strong physical unclonable functions. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 26(1): 73-81.

https://doi.org/10.1109/TVLSI.2017.2759731
[70] Uddin, M., Rose, G.S. (2018). A practical sense amplifier design for memristive crossbar circuits (PUF). In 2018 31st IEEE International System-on-Chip Conference (SOCC), Arlington, VA, USA, pp. 209-214. https://doi.org/10.1109/SOCC.2018.8618502
[71] Zhang, R., Jiang, H., Wang, Z.R., Lin, P., Zhuo, Y., Holcomb, D., Zhang, D.H., Yang, J.J., Xia, Q. (2018). Nanoscale diffusive memristor crossbars as physical unclonable functions. Nanoscale, 10(6): 2721-2726. https://doi.org/10.1039/C7NR06561B
[72] Arafin, M.T., Qu, G. (2018). Memristors for secret sharing-based lightweight authentication. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 26(12): 2671-2683. https://doi.org/10.1109/TVLSI.2018.2823714
[73] Jiang, H., Li, C., Zhang, R., Yan, P., Lin, P., Li, Y., Yang, J.J., Holcomb, D., Xia, Q. (2018). A provable key destruction scheme based on memristive crossbar arrays. Nature Electronics, 1(10): 548-554. https://doi.org/10.1038/s41928-018-0146-5
[74] Nili, H., Adam, G.C., Hoskins, B., Prezioso, M., Kim, J., Mahmoodi, M.R., Bayat, F.M., Kavehei, O., Strukov, D.B. (2018). Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors. Nature Electronics, 1(3): 197-202. https://doi.org/10.1038/s41928-018-0039-7
[75] Teo, J.H.L., Hashim, N.A.N., Ghazali, A., Hamid, F.A. (2019). Configurations of memristor-based APUF for improved performance. Bulletin of Electrical Engineering and Informatics, 8(1): 74-82. https://doi.org/10.11591/eei.v8i1.1401
[76] Teo, J.H.L., Hashim, N.A.N., Ghazali, A., Hamid, F.A. (2019). Ring oscillator physically unclonable function using sequential ring oscillator pairs for more challenge-response-pairs. Indonesian Journal of Electrical Engineering and Computer Science, 13(3): 892-901. https://doi.org/10.11591/ijeecs.v13.i3.pp892-901
[77] Uddin, M., Shanta, A.S., Majumder, M.B., Hasan, M.S., Rose, G.S. (2019). Memristor crossbar PUF based lightweight hardware security for IoT. In 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, pp. 1-4. https://doi.org/10.1109/ICCE.2019.8661912
[78] Arumí, D., Gómez-Pau, Á., Manich, S., Rodríguez-Montañés, R., González, M.B., Campabadal, F. (2018). Unpredictable bits generation based on RRAM parallel configuration. IEEE Electron Device Letters, 40(2): 341-344. https://doi.org/10.1109/LED.2018.2886396
[79] Mahmoodi, M.R., Strukov, D.B., Kavehei, O. (2019). Experimental demonstrations of security primitives with nonvolatile memories. IEEE Transactions on Electron Devices, 66(12): 5050-5059. https://doi.org/10.1109/TED.2019.2948950
[80] Knechtel, J. (2021). Hardware security for and beyond CMOS technology. In Proceedings of the 2021 International Symposium on Physical Design, pp. 115-126. https://doi.org/10.1145/3439706.3446902
[81] Zeitouni, S., Stapf, E., Fereidooni, H., Sadeghi, A.R. (2020). On the security of strong memristor-based physically unclonable functions. In 2020 57th ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, pp. 1-6. https://doi.org/10.1109/DAC18072.2020.9218491
[82] Kim, D., Kim, T.H., Choi, Y., Lee, G.H., Lee, J., Sun, W., Park, B., Kim, H., Shin, H. (2021). Selected bit-line current PUF: Implementation of hardware security primitive based on a memristor crossbar array. IEEE Access, 9: 120901-120910. https://doi.org/10.1109/ACCESS.2021.3108534
[83] Aljafar, M.J., Acken, J.M. (2022). Survey on the benefits of using memristors for PUFs. International Journal of Parallel, Emergent and Distributed Systems, 37(1): 40-67. https://doi.org/10.1080/17445760.2021.1972295
[84] Sun, J., Wang, Z., Wang, S., Yang, M., Gao, H., Wang, H., Ma, X., Hao, Y. (2022). Physical unclonable functions based on transient form of memristors for emergency defenses. IEEE Electron Device Letters, 43(3): 378-381. https://doi.org/10.1109/LED.2022.3145487
[85] Oh, J., Kim, S., Choi, J., Cha, J.H., Im, S.G., Jang, B.C., Choi, S.Y. (2022). Memristor-based security primitives robust to malicious attacks for highly secure neuromorphic systems. Advanced Intelligent Systems, 4(11): 2200177. https://doi.org/10.1002/aisy.202200177
[86] Larimian, S., Mahmoodi, M.R., Strukov, D.B. (2022). Improving machine learning attack resiliency via conductance balancing in memristive strong PUFs. IEEE Transactions on Electron Devices, 69(4): 1816-1822. https://doi.org/10.1109/TED.2022.3152469