Application of Memristors in Hardware Security: A Current State-of-the-Art Technology

Shiya Lv, Jian Liu,* and Zhaoxin Geng*

Memristors are widely used in hardware security applications. Research progress in memristor-based physical unclonable functions (PUFs), random number generators (RNGs), and chaotic circuits is reviewed. To enhance device security, PUFs and RNGs apply randomness of memristors and incorporate 3D crossbars to amplify the number of challenge-response pairs and provide proof of the destruction of the key, which enables the administrator to firmly control the device information. In addition, the image encryption technique based on the chaotic system is summarized. Furthermore, an assessment of the research advancement in PUFs, RNGs, and chaotic circuits is conducted. This Review examines the characteristics, applications, progress, and challenges of memristors in hardware security and compares the benefits and limitations of different schemes as accelerators for hardware information protection.

1. Introduction

With the development of the Internet, electronic gadgets are increasingly intertwined with day-to-day activities and they unavoidably interfere with the privacy of individuals, enterprises, and institutions.[1–5] To steal private information, hackers often attack electronic equipment,[6,7] for instance, side-channel attacks,[8,9] wormhole attacks,[10–12] hardware attacks,[13,14] reverse new attacks,[15,16] and Internet protocol piracy attacks.[17] Therefore, a cost-effective approach to improve security is urgently required.

A memristor is an emerging device capable of solving such issues. Chua defined and derived the memristor in 1971 using circuit completeness theory (Figure 1a). The expression of the memristor is presented as $M = \frac{d\phi}{dq}$ which depicts the correlation between the charge and the flux $q$.[19] The HP laboratory discovered the sandwich structure of Pt/TiO$_2$/Pt along with its voltage scanning attributes in 2008.[18] (Figure 1b). Less power consumption and tighter security are observed in devices with small geometries when compared with semiconductor devices. Hence, they are forecasted as substitutes for a metal-oxide–semiconductor field-effect transistor (MOSFET).[20–22]

Presently, in the field of hardware security, the memristor has become an essential discovery. There has been a rapid development of physical unclonable functions (PUFs), random number generators (RNGs), and chaotic circuits, which can be classified into two primary research directions. The first method replaces the transistor with a single memristor. Hybrid devices of memristors and complementary metal–oxide–semiconductor (CMOS) technology are usually produced. The second method replaces transistors completely with memristor crossbars, creating an emerging device that can significantly improve the performance of safety equipment. This review first presents the properties of memristors and its applications within the context of information security, and subsequently summarizes innovations of memristors in PUFs, RNGs, and chaotic systems. Finally, a comparative analysis of the advantages and drawbacks of the method is presented, followed by future challenges.

2. Characteristics and Structural Classification of Memristors

The structure of the memristor can extend from a 3D to a 1D assembly. Initially, 3D structures of memristors were discovered comprising certain metal oxides, including TiO$_2$, MoO$_3$, and AgSiO$_2$. Memristors will result in more power consumption when the memristor becomes thicker along the Z-direction. Consequently, researchers slowly compressed the thickness of the memristors to reduce the rate of power consumption. At a thickness of 10 nm, the memristor is classified as a 2D memristor.[23] The requirements of lower power consumption and higher flexibility encourage the study of efficient neural network learning and training. Abunahla et al. proposed a mathematical model for a 1D memristor in 2016. The model can stimulate anion-based memristor devices and predict their performance.[24] The model is classified as a 1D memristor.
because ions move only in a single direction. The drawback of the 1D model is that it only considers the thickness of the oxide layer, operating temperature, and materials of memristors. However, the practical implementation of 1D memristors has not yet occurred. A common feature of memristor materials is the variation of the resistance with the current. We can present an analogy between memristors and pipes. Large flows increase the thickness of the pipe. Similarly, a large current increases the resistance. Moreover, due to the nonlinear change in the resistance and current, the output of the voltage will also change. The various output voltage values of a memristor can form a key that is applicable in diverse fields of hardware security. It is impossible for the conventional semiconductor material Si to achieve this type of attribute related to current memory. Meanwhile, different properties are demonstrated by the memristors of different materials and structures. Table 1 (Figure 2) lists the summary and several relevant characteristics are extracted, such as switching characteristics, reliability, and randomness, to provide a comprehensive explanation. Due to these attributes, it is feasible to widely apply memristors in the hardware security field.

### 2.1. Switching Characteristics of Memristors

When the voltage changes continuously, the formation of the two states in resistance conversion is referred to as switching characteristics. The values of both the high-resistance state (HRS) and low-resistance state (LRS) correspond to ‘0’ and ‘1’, respectively (Figure 3a). The switching principles of the different types of memristor materials vary and are described based on three mechanisms: 1) fuse–antifuse, 2) electrochemical metallization memory, and 3) valence change memory.[24] Table 2 lists the principles and corresponding materials of different mechanisms. From the table, it is clearly observed that the mechanisms of fuse–antifuse and valence memory primarily depend on electron migration or oxygen vacancy recombination. Moreover, the electrochemical metallization memory is affected by metal cations produced during oxidation.

### Table 1. Common structures and properties of memristors.

| Dimension | Common material | Major material properties | Application materials | Ref. | Figure |
|-----------|-----------------|---------------------------|-----------------------|------|--------|
| 1D        | ZnO             | High flexibility          | Flexible electronic design | [25] | 2a     |
| 2D        | WS₂             | Low power consumption, short switching time (13 ns), low switching program current (1 A) | Simulates the basic function of biological synapses | [26] | 2b     |
| MoS₂      | Switch has good durability and reliability | Simulated synaptic activity | [27,28] | 2c     |
| In₃Se₁ₓ/WSe₂ | Conductance of continuous modulation, under nanosecond pulse, to complete the long-term enhancement to short-term enhancement conversion | Efficient training using biological synapses | [29] | 2d     |
| Ti₃C₂Tₓ    | Ferroelectric heterostructure, reversible, nonvolatile | Development information store | [30] | 2e     |
| 3D        | Ag:SiO₂         | Strong randomicity        | TRNG                  | [31] | 11a    |
| TiO₂      | Ag/TiO₂ switch is fast and stable | Build a synapse simulator | [32] | 2f     |
| MoO₃      | Low voltage, low power | Neuromorphic computation | [33] | 2g     |
| Hybrid COMS-memristor | Feasibility to modify the original transistor | TRNG, PUF, biological synapse construction | [34,35] | 12c    |
It is feasible to apply Equation (1) for computing the distribution of electrons, assuming it is possible to summarize the switching mechanism of the device based on the tunneling of electrons through the insulation gap. At this moment, the width of this gap and the corresponding device resistance can be changed by applying an input voltage or current. Therefore, through the adjustment of the appropriate voltage, the switching characteristics of memristors can be controlled.

\[
F(t; \tau, \sigma_t) = \int_0^t \frac{1}{\sqrt{2\pi} \sigma_t} e^{-\frac{(\ln t - \ln \tau)^2}{2\sigma_t^2}} \, dt = \frac{1}{2} \text{erfc}\left(\frac{\ln t}{\sqrt{2\sigma_t^2}}\right)
\]

(1)

Here, \( F \), \( t \), and \( \text{erfc} \) represent the cumulative distribution function of the lognormal distribution, cumulative time, and complementary error function, respectively. Deviation \( \sigma_t \) depends on the applied voltage amplitude, and \( \tau \) depends on the voltage (any further modification here will alter the context and lower the standard).

Recently, the control of switching characteristics has become a trending topic. The switching rate of metal oxides can be controlled by changing the driving force of the oxygen vacancy drift.\[43,44\] To examine the switch mutation of the memristor, the gradients of the electric potential, temperature, and concentration can be changed to allow the transportation of vacant oxygen inside the metal oxide (Figure 3d). Based on this, a new current–voltage (I–V) curve was discovered by Abunahla et al., to be generated in each switching event. Alternatively, a single memristor was incorporated by Abunahla et al. into the original coding circuit. Through this memristor, a new session key can be generated for every new communication. Internet communication security can be further developed by including a session key to the host/trusted third party. The memristor structure that generates the session key is shown in Figure 3d.

Memristor materials can be created from metal oxides and metal sulfides. The direction of the conductor-mediated DC in programmable switches using sulfur compounds can result in innovative developments (Figure 3i).\[42\] Therefore, assuming we want to explore the features of mediated rectification, a memristor model that considers the sulfur vacancy in MoS\(_2\) can be established. Recently, a neural network was developed by Liang and co-workers using MoS\(_2\) to simulate the ion interaction between neurons.
2.2. Reliability and Randomness of Memristors

From the analysis listed in Table 2, it can be noted that the randomness of the memristor is caused by the unpredictability of wire formation/fracture and vacancy migration. Thus, because of this specific property, it becomes complicated to estimate devices, including the true random number generator (TRNG), PUF, chaotic circuit, and transmission electron microscope (TEM) image of Pt/ZnO/Pt switching device; Reproduced with permission. Copyright 2019, The Royal Society of Chemistry. b) Three switching mechanisms (fuse–antifuse on the left, electrochemical metallization memory in the middle, valence change memory on the right); c) Schematic, I–V characteristic diagram, and a transmission electron microscope (TEM) image of Pt/HfO2/Pd memristors; Reproduced with permission. Copyright 2013, ACS. d) Schematic representation of the prevalent electrical switching pathway occurring inside the microscale Pd/HfO2/Pd memristors; Reproduced with permission. Copyright 2018, Elsevier. e) Schematic, I–V characteristic diagram, and TEM image of TiN/TaOx/Pt switching device; Reproduced with permission. Copyright 2009, The Royal Society of Chemistry. f) Schematic, I–V characteristic diagram, and TEM image of Ag/a-LSMO/Pt switching device; Reproduced with permission. Copyright 2013, The Royal Society of Chemistry. g) Schematic, I–V characteristic diagram, and TEM image of Au/TaOx/Au switching device; Reproduced with permission. Copyright 2013, Wiley-VCH. h) Schematic, I–V characteristic diagram, and TEM image of Au/TaOx/Au switching device; Reproduced with permission. Copyright 2015, Wiley-VCH. i) Schematic, I–V characteristic diagram of the Au/MoS2/Au switching device. Reproduced with permission. Copyright 2018, ACS.

Figure 3. Switching characteristics of memristors: a) Cumulative switching probability distribution for ON and OFF switching under different applied voltage amplitudes; Reproduced with permission. Copyright 2019, The Royal Society of Chemistry. b) Three switching mechanisms (fuse–antifuse on the left, electrochemical metallization memory in the middle, valence change memory on the right); c) Schematic, I–V characteristic diagram, and a transmission electron microscope (TEM) image of Pt/ZnO/Pt switching device; Reproduced with permission. Copyright 2013, ACS. d) Schematic representation of the prevalent electrical switching pathway occurring inside the microscale Pd/HfO2/Pd memristors; Reproduced with permission. Copyright 2018, Elsevier. e) Schematic, I–V characteristic diagram, and TEM image of TiN/TaOx/Pt switching device; Reproduced with permission. Copyright 2009, The Royal Society of Chemistry. f) Schematic, I–V characteristic diagram, and TEM image of Ag/a-LSMO/Pt switching device; Reproduced with permission. Copyright 2013, The Royal Society of Chemistry. g) Schematic, I–V characteristic diagram, and TEM image of Au/TaOx/Au switching device; Reproduced with permission. Copyright 2013, Wiley-VCH. h) Schematic, I–V characteristic diagram, and TEM image of Au/TaOx/Au switching device; Reproduced with permission. Copyright 2015, Wiley-VCH. i) Schematic, I–V characteristic diagram of the Au/MoS2/Au switching device. Reproduced with permission. Copyright 2018, ACS.

2.2. Reliability and Randomness of Memristors

From the analysis listed in Table 2, it can be noted that the randomness of the memristor is caused by the unpredictability of wire formation/fracture and vacancy migration. Thus, because of this specific property, it becomes complicated to estimate devices, including the true random number generator (TRNG), PUF, chaotic circuit, and transmission electron microscope (TEM) image of Pt/ZnO/Pt switching device; Reproduced with permission. Copyright 2019, The Royal Society of Chemistry. b) Three switching mechanisms (fuse–antifuse on the left, electrochemical metallization memory in the middle, valence change memory on the right); c) Schematic, I–V characteristic diagram, and a transmission electron microscope (TEM) image of Pt/ZnO/Pt switching device; Reproduced with permission. Copyright 2013, ACS. d) Schematic representation of the prevalent electrical switching pathway occurring inside the microscale Pd/HfO2/Pd memristors; Reproduced with permission. Copyright 2018, Elsevier. e) Schematic, I–V characteristic diagram, and TEM image of TiN/TaOx/Pt switching device; Reproduced with permission. Copyright 2009, The Royal Society of Chemistry. f) Schematic, I–V characteristic diagram, and TEM image of Ag/a-LSMO/Pt switching device; Reproduced with permission. Copyright 2013, The Royal Society of Chemistry. g) Schematic, I–V characteristic diagram, and TEM image of Au/TaOx/Au switching device; Reproduced with permission. Copyright 2013, Wiley-VCH. h) Schematic, I–V characteristic diagram, and TEM image of Au/TaOx/Au switching device; Reproduced with permission. Copyright 2015, Wiley-VCH. i) Schematic, I–V characteristic diagram of the Au/MoS2/Au switching device. Reproduced with permission. Copyright 2018, ACS.

modifications in the exterior of the devices are not expected to generate different results, which is a property known as reliability. Thus, the randomness of memristors and reliability are properties that contradict each other. In this context, by analyzing the reliability, the randomness of memristors and reliability are elaborately examined (Table 3).

As listed in Table 3, the reliability of memristors is affected by three factors, namely variability, [52–58] durability,[57,58,62] and random telegraph noise (RTN).[53,64] To obtain process variability, it is feasible to apply a memristor that utilizes different materials or to utilize the same memristor under different voltage scanning cycles to obtain the HRS and LRS at a variety of voltage ranges. Moreover, variability can be achieved using the
equipment in varied operating conditions, such as voltage, pulse width, and temperature. The changes in the speed and level of switching between the two states of a memristor are due to an increase in the number of switches. This is sometimes known as durability.\cite{65,66} The figure on the left side of Figure 4a shows that once the proportion of switches arrives at a particular level, the memristors are degraded and their memory properties are lost. From the comparison of the picture located on the left and right sides of Figure 4a, it can be observed that the durability of the memristor can be affected by the setting of the switching voltage. The wear of the memristor tends to be significantly reduced in the course of the same switching period by applying an adequate switching voltage. RTN represents the third factor that impacts the reliability of memristors. The RTN causes distinct random fluctuations at consistent values in memristors, which denotes a regular phenomenon that occurs within the semiconductor devices. The fluctuation occurs between two values. This distance is designated as RTNp (Figure 4b).\cite{59,63,64} As the fluctuation becomes smaller, the impact of external noise on the memristor is reduced and consequently its reliability is enhanced.

| Switch mechanism (Figure 3b) | Principle | Examples of corresponding materials | Application | Ref. | Figure |
|-----------------------------|-----------|-------------------------------------|-------------|------|--------|
| Fuse–antifuse                | Generation and recombination of oxygen vacancies through joule heating is the basis for creating and rupturing of conducting filaments. | Pt/ZnO thin film/Pt, Pd/Hf/HfO2/Pd | Multistate storage, Resistive random access memory (RRAM) | [36,37,43–45] | 3c, 3d |
| Electrochemical metatization memory | Oxidation of the active electrode occurs under the scanning voltage, and the resulting metal cation migrates to the inert electrode along the electric field. In the course of moving, there is a reduction in the metal guide wire that subsequently changes the device from HRS to LRS.\cite{46,47} During amplification of the reverse voltage, the conductance wire breaks to produce a HRS resulting in resistance switching, which ensures that the switching procedure is completed. | Pt/TiN/TaOx/Pt, Ag/a-LSMO/Pt, Ag/SiO2/Ta2O5/Pt | RRAM | [38,39,40] | 3e, 3f, 3g |
| Valence change memory       | It relies on the vacancy migration that causes redox reactions and results in the modification of the insulator layer stoichiometry. | Au/Ta2O5/Au | RRAM | [41] | 3h |

| Table 3. Reliability of memristors. |
| Factors affecting reliability | Generating principle | Result | Resolution | Limitation | Utilization | Ref. |
| Variability                  | Variation of oxygen vacancy in doped concentration, a difference in area (S) and thickness (L) | – | High voltage, large pulse width, low temperature | Reduces RRAM reading stability | PUF, TRNG, RRAM | [58–61] |
| Endurance                    | Degradation mechanism and endurance failure | Distance between high and low-resistance values | Optimize setting and reset voltage | HRS and LRS parameters change | – | [27,58,62] |
| RTN                         | Capture and emission of charge carriers near the interface | Causes changes in the threshold voltage (Vth) and drain current (Id) in the MOSFET | – | Reading instability of RRAM memory | – | [59,63,64] |

Figure 4. Reliability and randomness of memristors: a) Endurance behavior in memristive devices; Reproduced with permission.\cite{66} Copyright 2018, Elsevier. b) Current fluctuations in resistive random access memory because of RTNp.
In summary, the three factors listed earlier restrict the dependability of memristors. The switching voltage values, voltage pulses, and temperature impact these three factors. Thus, to ensure that the memristor is reliable, it becomes imperative for the manufactured devices to pass complex tests, such as cycle and temperature tests. Concurrently, it is impossible for the manufactured devices to pass complex tests, such as cycle and temperature tests. Moreover, other properties of memristors as the reliability is enhanced, and randomness is weakened.

2.3. Other Characteristics

In contrast to digital circuit devices, transistor memristors have additional excellent features, as (Table 4): 1) Uniqueness: Under different initial conditions, it is feasible for the same input signal to output different I–V orbitals. Hence, different keys can be generated using similar devices, and the manager can ensure the destruction of keys in the random fingerprint that is returned from the device. 2) Nonvolatile: In the absence of power excitation, the original resistance value can be maintained by the memristor (Figure 5, Panel 1). Memristors are classified into positive and negative poles. A HRS is attained when the memristor is placed at the positive pole, whereas a LRS is achieved when the placement is at the negative pole. It is feasible for the memristor to switch from a HRS to a LRS as the position of the positive pulse occurs at both the positive and negative terminals. The memristor obtains a LRS once the positive pulse is input at the negative pole. Based on the resistance attribute of the memristor, the resistance state of the positive pulse requires considerable time before it can return to a high state from a low state if the positive pulse is input at the positive pole at a particular time duration. 3) Integration: It is feasible to incorporate a memristor into a 3D crossbar. From Figure 5, the capability of arranging multiple 3D memristor crossbars periodically in an integrated memristor array is revealed. In addition to the aforementioned features, the other features of a memristor include multiple choices, low cost, low power consumption, high compatibility as well as being considered as a circuit component that can be used in the future.

3. Applications

3.1. Memristor-Based PUFs

The term uniqueness insinuates the tendency of the PUF to produce a single, random identity document (ID) based on the structural configuration of the chip generated through uncontrollable parameters during the production procedure. In several circumstances, it is feasible to use the unique ID to protect information. To avoid malicious changes to the encryption parameter in the one-time programmable memory, information managers integrate the ID with parameters. Furthermore, to prevent transport attacks, the manager can connect the ID to specific models. The data is certain to record failure in other models, assuming the model and data of ID are integrated into the ciphertext, even if the encrypted data theft occurs during transmission. This is because the application of the encrypted data is possible only when the decryption of the ID is performed in combination with the model. Other scenarios that often occur in the field of artificial intelligence are malicious reverse engineering, hardware analysis, and inconspicuous stealing. It is conducive for the ID of the PUF output to counterbalance reverse engineering. Thus, before the utilization of the chip, it is mandatory for users to have a special ID. However, it is possible to clone the entire conventional PUF developed by CMOS. The moment the attacker clones the PUF, it becomes easy for him to break the encryption algorithm by obtaining the ID of the output. The solution to this problem is to apply memristors to the PUF. The discrete nature of memristors is further increased due to the randomness of the memristor while building a PUF, which is now adjudged to be similar to placing an enhanced RNG in PUF. The randomness along with reliability of the PUF is enhanced and reinforced by the uniqueness of the PUF and the reliability of the memristors. Reliability is a factor that indicates the potential of equipment to maintain its original performance when subjected to varying conditions, such as different temperatures, responses, and other external environmental conditions. In Section 2.2, it is discussed that the external environment can impact the reliability of memristors. Thus, to confirm their reliability, it is necessary to perform temperature and voltage cycle tests for PUFs. Moreover, other properties of the PUF should also be considered. Table 5 lists the catalog of key features as well as the specific computational approaches. The attributes of memristors can be quantified based on the uniqueness, uniformity, reliability, diffuseness, and bit-aliasing of the PUF, as listed in the table; moreover, based on these properties, memristors can be adjusted into more suitable conditions. PUFs are of various forms. It can be categorized into strong and weak PUFs based on the excitation response algorithm.

From the perspective of different applications, the PUF can be divided into the following categories: arbiter PUF (APUF), ring oscillator PUF (ROPUF), and public PUF (PPUF). Figure 6 shows other classification methods. Presently, the integration of memristors into PUF has been performed by researchers using two approaches. In the first approach, independent memristors are applied to modify the existing circuit.

| Characteristics | Transistor | Memristor | Applications | Ref. |
|----------------|------------|-----------|--------------|------|
| Uniqueness     | No         | Yes       | Forms a key, proof that the key is destroyed | [68–72] |
| Nonvolatile    | Loss of power, loss of state | Loses power, still in the previous state | Brain-like nerve morphology calculation, nonvolatile memory, nonvolatile logic operation | [73–77] |
| Integration    | Low integration | High integration level | Microchip miniaturization | [34,35,78] |
second method, rather than utilizing the existing design, the memristor crossbar is used. The diffusion memristor crossbar is the most frequently used method. This technique is comprehensively discussed in the subsequent section.

3.1.1. Hybrid Memristor–CMOS PUF Circuit (APUF and ROPUF)

An increasing number of systems are now developing conventional PUFs based on CMOS devices. Due to the suitable attributes of memristors as well as the compatible nature of the manufacturing technologies used for memristors and CMOS devices, research has been intensified by scientists on hybrid memristor–CMOS circuits. With a lower power consumption and more suitable integration, PUF circuits based on memristors have eclipsed the CMOS-oriented circuit. A study conducted by Mathew et al. provides an illustrated example of research on the hybrid memristor–CMOS PUF.

A report was published pertaining to the hybrid memristor–CMOS PUF based on delay variation. The core concept is focused on saving hardware overhead. The most significant challenge is in attempting to ascertain whether it is possible to select the fragments in the delayed path. It is feasible to combine the delay fragments for producing the delayed path and obtain the response bit. Thus, the amount of memristor–CMOS hardware entering a multibit response can be controlled through the selection of a delayed fragment.

The general layout of the circuit along with its associated control signals is shown in Figure 7. From Figure 7, it can be observed that the circuit is composed of the time-control module, delay path, reset element, and n-type metal–oxide–semiconductor
(NMOS) switch. When the signal is input at one terminal, the movement of the signal passes through two delay paths. Through the timing and control unit, the excitation pulse is provided. In contrast to the conventional PUFs and certain memristor–CMOS hybrid PUFs proposed in the past, the aim of the researcher was to ensure the reduction in circuit area, hardware resources, and the eradication of the complex and costly post-processing. These forms of processing ensure the easy applicability of PUF to actual security protocols.

The path delay distribution of APUF is shown in Panel 1b of Figure 7. It is not easy to model machine-learning-based attacks for this new PUF because an unpredictable signature through multiple delayed paths is generated by the hybrid APUF. Concurrently, more stability is conferred on the security protocol and hardware encryption due to the impressive statistical randomness of the PUF. However, this scheme can be subjected to cryptanalysis attacks.\[91\] The reason for improving the scheme is to ensure that the memristor is controlled in correspondence with NMOS and to limit the exposure to attack.\[91\] As listed in Table 6, despite the improved reliability of the scheme, the different bits are inconsistent and the hardware resources are utilized at a low rate. Hence, based on the actual requirement, two options are available for reasonable selection.

Similarly, the modification of the ROPUF was performed using memristors (Figure 7, Panel 2). To lower the circuit size and rate of power consumption, the ring oscillator inverter is incorporated with a memristor.\[96\] Thus, the number of challenge-response pairs (CRPs) can be amplified without enhancing the circuit overhead.

Modification of the memristor-oriented PUF can be performed by replacing the CMOS with independent memristors and by enhancing the number of CRPs with memristor crossbars. In the subsequent section, the modification of memristor crossbars is discussed.

3.1.2. Nano-PPUF Based on Memristor Crossbars

From the PUF, the PPUF, which is a hardware encryption method, was developed. Researchers are required to provide a public model of PPUF, because, when compared to other devices, it is different. However, the published simulation model can be used by attackers to quickly traverse the entire results, assuming that the model lacks a sufficient number of CRPs. Thus, it is anticipated that the PPUF should enhance the number of CRPs and conceal the boundary conditions to lower the prospect of an attacker obtaining the right response.\[97\] Rajendran et al. suggested that the memristor can accomplish this function. The author proposed a time-constraint authentication scenario,\[93\] as shown in Figure 8, Panel 1.

The possibilities of the nano-PPUF are diverse (>10\(^10\)). Furthermore, it is possible for the correct response and boundary voltage to be promptly secured by the owner of the proposed PPUF. The only information that the attacker can possibly retrieve from the public registry is the simulation model of Person A, as it is forbidden to access the input excitation and

![Figure 6. Classification of different PUF implementations.](image-url)
boundary conditions. Thus, it appears to be extremely improbable that the note chosen by the attacker will be similar to that selected by Person B. Consequently, the attacker will require several years to simulate the CRPs. Furthermore, the feasibility of implementing a time-limit security basis for authentication was also verified in this article. The exponential increase in the size of the selected area simultaneously generates a linear increase in the simulation time, as shown in Figure 8, Panel 3a. For example, if a $20 \times 20$ memristor crossbar is considered, the time required for the simulation is in decades, i.e., $10^9$ s. As the crossbar size increases, the time required by the attacker to perform a simulation significantly increases. This also marginally enhances the actual execution time of the PPUF model holder by a few microseconds, as shown in Figure 8, Panel 3b. The time interval between simulation and execution is $10^{15}$ s, which is considerably beyond the normal time of validation.

In summary, using this design, the originally weak PUF is converted into a strong PUF by modifying the memristor, which
subsequently enhances the number of CRPs, reduces the complementary excitation of hackers, and enhances the time cost of the attackers, thereby preventing attacks. Hence, the long duration required by the attacker to crack the response should not be considered as it is beyond the validation time.

3.1.3. PUFs Based on Nanoscale Diffusive Memristor Crossbars

Zhang et al. demonstrated the method and principle of establishing PUFs using nanoscale diffusion memristor crossbars. The development of PUFs exploits the random distribution of clusters of metallic Ag ions in the SiO2 matrix. The difference in the switching ability of diffusion memristors is due to the uneven distribution of Ag ions present at the intersections, which is performed to construct a distinct binary bitmap. The 16-bit PUF proposed is actually a 4x4 crossbar with an area of 100 x 100 nm². A crossbar is composed of memristor units embedded at its intersection points. The components of the memristor units include an Ag-doped SiO2 layered in the middle to conduct switching, as well as a top electrode (TE) of 40 nm Au and a bottom electrode (BE) of 15 nm Au or 2 nm Ti (Figure 9, Panel 1a). The switching features of memristors are comprehensively applied in this scheme (Figure 9, Panel 1b).

Furthermore, an inter-class fractional Hamming distance distribution histogram was demonstrated by Zhang, which was performed through a comparison of bit–bit differences between different 16-bit strings. Using the Gaussian function with a center of 0.5068 and variance of 0.0144, the distribution histogram was appropriately expressed. The mean value and variance of approximately 50% and 0%, respectively, indicate that the randomicity of the PUF integrated with a diffusion memristor crossbar is suitable. The attribute that results in the uncrackability of the PUF and ensures the consistency of PUF-generated keys is uniqueness. Furthermore, the experiment evaluated the changes in binary bitmaps obtained through the conversion of memristor crossbars under conditions of high temperatures and persistent challenge cycling. The output current generated by ten randomly selected memristors was recorded in the temperature range of 300–500 K; moreover, the 1.8 V analysis is shown in Figure 9, Panel 2. From the figure, it is revealed that it is feasible for the diffusion memristors to maintain the original output characteristics even at a significantly higher temperature, which is beyond the range that an integrated circuit can withstand. Figure 9, Panel 3 shows the binary bitmap following 30 and 50 challenge cycles with significantly minimal changes to the PUF. Moreover, the endurance limit of the diffusion memristors tends to be more than 10⁶ switching cycles. Assuming that subsequent research will continue to enhance the durability of the diffusion memristor, a significant enhancement in the reliability of the PUF can be expected. Future advancements in engineering materials are also expected to enhance the reliability of PUFs. For example, the controlled drop of large particles in Ag casting that are embedded through random dispersal, the reliability of PUFs can be enhanced on the basis of diffusion memristors.

Memristors intensify the uniqueness and reliability of PUFs. Moreover, when the memristors are based on the aforementioned hybrid circuits and electronic PUFs based on silicon technology (e.g., APUF) and static random access memory
[SRAM] PUF\textsuperscript{[102,103]}, they can also lower the circuit components, enhance hardware integration, and actualize self-digitization. Furthermore, the manufacturing processes of the hybrid memristor–CMOS PUF and PUF based on diffusion are conducted without difficulty. Through further processing, security threats and data leakage are prevented. Hence, in contrast to the previous PUFs based on nonvolatile memristors, the proposed diffusive memristor PUFs are more secure.\textsuperscript{[104,105]}

However, for the PUF based on the diffusion memristor to actualize the self-digitizing procedure, the split method must...
be extensively applied; consequently, the selection and calibration of the reference resistors based on a considerable number of test devices must be cautiously performed.\cite{105,106}

3.1.4. Proving the Key Destruction Scheme

Aside from the replacement of CMOS and actualizing the original function, a new function that can be actualized by the memristors was developed by researchers. However, CMOS transistors cannot achieve this new function. Power retention during a power outage is achieved using a volatile device made of transistors, which is composed of memristors in contrast to the SRAM. In addition, temperature changes and the external environment have no significant impact on the characteristics of the memristor.

Based on the memristor crossbars, Jiang et al. proposed a verifiable key destruction scheme. This proposed system compares the conductance values of the left and right nodes and generates a special fingerprint\cite{69–71} as shown in Figure 10, Panel 1a. The off-chip database is used to store the fingerprint generated by the memristor. Whenever the key-based permission of users is about to be revoked by the chip designer, the designer simply presses the “erase fingerprint” command on the crossbar. Once this is performed, the entire cell switches to a LRS. Meanwhile, a set of fingerprints is externally generated by the device, in contrast to the correct fingerprint previously stored in the database. If the results are acceptable, then it is possible to erase the chip fingerprint and send it back as a proof of the destruction of the fingerprint to the chip designer (Figure 10, Panels 1b and 1c).

From the proposed chip, the integration of the security, memory, and computing functionalities is demonstrated, which uses both the in-chip memristor and the off-chip transistor to generate fingerprints and process and store data, respectively. In addition, the reliability and uniqueness of the generated fingerprints were proven by the researcher. The author compared the fingerprints generated at similar locations in different areas of the chip. Within the class, the mean value and variance of the Hamming distance were measured to be 0.5006 and 0.0452.

Figure 10. Proof of the key destruction scheme: Panel 1. Principle of provable key destruction: a) Schematic for fingerprint extraction by comparing the conductance values in the LRS between two adjacent memristor cells (differential pairs); b) Security problems of traditional keys; c) The chip stores the digital key as the resistance value of the memristor. Following the successful extraction of the memristor fingerprint, the removal of the key is proven by the chip; Panel 2. Array internal structure of memory; Panel 3. Uniqueness and reliability of the memristor array are demonstrated. Reproduced with permission.\cite{69} Copyright 2018, Springer Nature.
respectively. It was verified that the chip generates random fingerprints. Similarly, for the fingerprints produced at the same area of the chip, the average Hamming distance and variance were calculated to be 0.1382 and 0.0657, respectively. (Figure 10, Panel 3).

The aforementioned discussion shows that the scheme of comparing the resistances of adjacent memristors in the memristor crossbars demonstrates strong robustness and high randomness of the output key. However, this scheme did not provide a discourse on memristor crossbar consumption. When compared with a single memristor, greater randomness can be produced by memristor arrays in the circuit; however, higher integration results in a high rate of power consumption. A reason why the memristor arrays have a high integration is its applicability in portable devices that often have power constraints; thus, this represents a significant challenge that must be solved during the application of memristors arrays with reduced power. Overall, one way of reducing the power consumption of memristors is through the reduction of the bar thickness or substituting it with a highly sensitive material when subjected to low pressure.

3.1.5. Conclusion

Although the model of the PPUF is a public model, an attack is limited by the undisclosed boundary conditions and the considerable number of CRPs that extend the period of attack and ensure that the security performance of the device is enhanced. In contrast to the nano-PUF, the original CMOS circuit is enhanced by the hybrid memristor–CMOS. The APUF reduces the number of CRPs and the safety performance. The memristor is simply applied to the circuit element from the solution of the diffusion memristor, for instance, nanoscale PUF. This produces the following benefits: provides significant enhancement in randomness and reliability to the circuit, guarantees safety, lowers power consumption rate, and reduces the circuit element. The key destruction scheme derived from the PUF demonstrates that the applicability of the memristor is not merely limited to modifying the original PUF but is useful in developing further applications in the future.

It is also feasible to incorporate a PUF based on a single memristor into an Internet communication protocol. Various session keys were generated by altering the input voltage using a voltage pulse–stack pattern. During the procedures performed by the host and time-triggered protocol session, the session key generated by the memristor was included to improve the communication security. This represents a suitable course of action that can be pursued in the future.

3.2. Memristor for the Application of TRNG

RNGs are extensively used in information security fields, such as cipher systems, computer simulations, and communication security. The random number can be classified into two aspects: the TRNG and pseudo-RNG. To generate a random signal, the conventional TRN predominantly utilizes natural thermal noise, atmospheric noise, or direct amplification of the circuit noise. The internal state and input “seed” are included in the pseudo-RNG. The input “seed” is capable of determining the pseudo-random value. The “seed” of the pseudo-random number corresponds to the key of the generator and is applied to initialize the internal state. Thus, to internally generate a random number sequence, the pseudo-RNG primarily depends on the initial sequence of the artificial injection. Presently, there is a gradual development in CMOS-based RNGs; however, they have certain limitations. Because the prejudice of 0/1 bias and small noise amplitudes are recorded in the output sequence, it is necessary to ensure that the signal for the preamplifier circuit is processed, which was not anticipated during the development of this scheme. This inconvenience can be prevented using a random generator produced by the memristor. Meanwhile, the research considering RNGs based on memristors has been applied in the field of TRNGs. Hence, a more suitable option uses memristors to create a RNG.

The randomness test standard of the National Institute of Standards and Technology (NIST), which is the international standard for testing randomness of RNGs, is now considered as the evaluation rule based on which various research teams were developed. Approximately 15 different methods of assessment are involved in this system. As the TRNG passes more tests, it improves the randomness of the RNG.

3.2.1. RNG Based on Diffusion Memristor

A RNG for a diffusive memristor was proposed depending on the diffusion dynamics of the metal atom. The moment the operator removes the external pulse, it causes the memristor to switch to the LRS. The device experiences a random time delay following the input of the power pulse (Figure 11b). The probability that the Ag particle is discrete from the Ag reservoir is the basis on which the delay time of memristor switching is determined. The procedure for diffusion of Ag particles is as follows. Prior to the diffusion of Ag particles, the SiO2 forms a conduction channel. Through this conduction channel, it is possible to separate the Ag particles from the reservoir of Ag particles with a random time period. In Figure 11a, the unit of the diffusive memristor is shown.

This proposed memristor has a four-layer structure, which is different from most three-layered memristors. The diameter of the proposed optical image and geometry of the Ag:SiO2 indicates a 5 μm × 5 μm cross-point diffusive memristor. The memristor comprises a TE of 20 nm Pt/30 nm Au, BE of 15 nm Pt, and 15 nm Ag:SiO2 layer in the middle for switching. Furthermore, to prevent the deletion of Ag in the course of switching, an Ag layer was placed between the top and middle layers. The circuit model that is generally proposed includes a diffusion memristor, comparator, gate, and counter, as can be observed from Figure 11c. It is not necessary to perform electroforming of the device; moreover, it also demonstrates a low leakage current (picoampere), low operating current (<100 nA), reliable threshold voltage (>0.5 V), and small scanning duration. In addition, it is easy to limit or adjust the on/off current as well as the on/off window (>10). The applied voltage pulse and amplitude to the device are of a width of 300 μs and 0.5 V, respectively. A delay of a random period of time (∼130 μs) occurs before reaching the LRS (Ron) once the pulse amplitude (Vt) attains
the threshold voltage ($\approx 0.5 \, \text{V}$). However, the memristor returns to the HRS ($R_{\text{off}}$) within a random time duration of 100 $\mu$s once the voltage ($V_1$) returns to a voltage below 0.3 V. The counter accuracy is controlled by the local clock at 100 $\mu$s. The memristor relaxes back to the HRS ($R_{\text{on}}$) when the voltage ($V_1$) value is below 0.3 V. The local clock controls the accuracy of the counter. Both the output logic level and the specific applied voltage $V_{\text{off}}$ were compared. The output of the counter generates the period at which a logical high level is attained by both the local clock and $V_L$, which are random numbers. The random numbers generated are binary sequence bits, which after being subjected to the NIST randomness test, can be used without further processing.

The TRNG based on the diffusive memristor has the capacity to reduce power consumption because it can shut off automatically and not engage in the reset procedure, which is in contrast to the TRNGs centered on CMOS. Due to the intrinsic randomness of the diffusive memristor, the circuit complexity is lowered. The circuit can be easily incorporated in a small area with high integration and compatibility with the CMOS process due to the diffusion memristor. However, it is still possible to enhance the equipment in several ways. With respect to the bit rate, with a higher base, there will be an increase in power consumption as the clock signal frequency increases. Hence, it is feasible to integrate the diffusion memristor along with the linear feedback shift register to ensure that the bit rate is enhanced without increasing the consumption of power. In addition, one of the methods taken into consideration is parallel working of several diffusion memristors. While considering the circuit area, three vertically stacked devices can be applied to reduce the circuit area.

### 3.2.2. TRNG Based on Oxygen Vacancy Transformation

The circuits of the conventional TRNGs have thermal noise introduced into them. From the Brownian motion of electrons, changes in the conductor temperature generate thermal noise. However, the implementation of programming has no significant effect on the offset output bitstream. Deflection is prevented by the scheme presented later, and changing the input voltage can provide adjustment to the twisted bitstream. Other significant features of the system include low power consumption, high sampling rate, and high integration. This design scheme has a simple circuit structure consisting of simply a single memristor, six transistors, and a trigger, as shown in Figure 12a.[31] In the circuit unit, the Pt electrode is connected to the applied voltage and the bottom Pt electrode is grounded. The two layers of TiO$_2$ compressed in the middle represent a vertically stacked memristor. Figure 12b shows that the upper and lower layers of the TiO$_2$ are nondoped with inductance and oxygen vacancy, indicating high conductivity. The oxygen layer is pressurized into an upward movement to the upper layer of the nondoped TiO$_2$ layer when the researcher inputs a positive voltage in the top Pt electrode. This will subsequently bring about a reduction in the resistor value of resistance to the $R_{\text{on}}$ state. Assuming that there is a negative bias in the top Pt electrode, it will pressure the oxygen vacancy to migrate back toward the original lower doped TiO$_2$ layer. Furthermore, an enhancement in the memristors occurred in the $R_{\text{off}}$ state. Because the memristor has a random resistance value and a relationship with the pulse voltage amplitude and program width of the input, the lognormal probability density function is approximately the same as the $R_{\text{on}}$ and $R_{\text{off}}$ distributions of the steady-state resistance.[54]

Figure 12c shows the proposed overall circuit structure in the scheme. The author conducts modularization of the circuit. To control the reading mode and on/off switch programming, the external DC power supply is denoted by $V_{\text{dc},r}$, $V_{\text{dc, on}}$, and $V_{\text{dc, off}}$. The signal that controls the detection of the memristor status by the read mode is denoted as $V_{\text{read}}$. The memristors are programmed to the ON and OFF states by $V_{\text{p, on}}$ and $V_{\text{p, off}}$. The memristor state is also known as the offset voltage that regulates the generated output bits using a multiple TRNG (MTRNG), which is designated by $V_O$. To adjust $V_g$, which is used for generating bits, $V_g$ is applied. The clock signal is otherwise known as Clk, which is regulated by the data acquisition of the D flip-flop.

Furthermore, the alternating voltages of $V_{\text{p, on}}$ and $V_{\text{p, off}}$ and the amplitude and width of the input programming voltage are controlled by the scheme. The memristors are programmed to intensify the resistance change, thereby generating a random bitstream. Nevertheless, the bitstream randomness achieved through this method remains undeveloped. Hence, the scheme was upgraded to ensure that the entropy of the output bitstream is enhanced. To form the two-branch MTRNG design, the D flip-flop in the periphery is included, adopting the output bitstream of two circuit structures, such as two inputs of the XOR gate, and
subsequently passing the D flip-flop. Even though the structure enhances the randomness of the output bitstream, it increases the circuit complexity. Therefore, the coordination of the three D triggers is now considered a relatively complex issue. In addition, the sampling rate design of this scheme underscores its capability to accomplish the least power consumption of 31.1 GHz when the sampling rate is high. The only disadvantage of this scheme is the failure of the developed RNG to pass the NIST randomness assessment. Thus, it is impossible to evaluate the randomness of TRNG through a unified standard, thereby bringing into focus the security of the generated random numbers. However, in contrast to the conventional TRNG, the device is composed of a nonelaborate structure, small area, high frequency, low consumption, and flexible configuration. The future development of TRNGs is highlighted by improvements in these areas. While comparing with the scheme of diffusion memristors, it is readily observed that both designs prevent the complexity of high circuits by applying relatively basic circuit components. While considering the sampling rate, under the condition of a high sampling rate, low power consumption is observed for TRNG based on oxygen vacancy transformation. However, in terms of randomness, the comparison clearly favors a RNG based on the spread memristors. The aforementioned basic principle exploits electronic noise. In this context, examples of this electronic noise include defects in the charge tunneling layer and the interface defects in the polysilicon channel.\[^{[67]}\] When voltage is input, a defect is produced in the nanoscale transistor through the generated electric field. This will subsequently enable the semiconductor to generate a sudden change signal that denotes the essential attribute of the memristor.

3.2.3. Conclusion

The three-layer structure is broken by the TRNG-based diffusion memristor; moreover, to achieve higher randomness, we attempted to apply a four-layer structure. Thus, the TRNG based on diffusion material has the following advantages over the TRNG centered on oxygen vacancy changes, including high-temperature resistance, high reliability, small area, and high integration. The TRNG based on oxygen vacancy changes has a complicated process, albeit a simple principle of increasing randomness by repeatedly passing two single outputs through D flip-flops. During the NIST assessments, out of the earlier shortlisted series of RNG layouts, the RNG centered on the diffusion memristor was observed to have the highest performance. The Ag:SiO₂ switching delays the random time and generates random numbers by utilizing the diffusion dynamics of metal atoms. The migration of the oxygen vacancy in the memristor

---

**Figure 12.** TRNG based on oxygen vacancy transformation: a) One of the circuit branches of the multiple random number generator (MTRNG) scheme; b) Structure of a TiO₂ memristor; c) Scheme of the enhanced two-branch MTRNG design. Reproduced with permission.\[^{[31]}\] Copyright 2015, the Royal Society of Chemistry.
is regulated by the second RNG so that the changes that occur in the resistance value can initiate the bitstream, and further increase the bitstream output randomness of the digital circuit devices.

3.3. Chaotic Circuit Based on Memristor Is Used for Information Encryption

The term chaotic system implies a form of stochastic behavior initiated by a deterministic nonlinear system that cannot be readily and comprehensively predicted.[118] In the state system of arrangements, after the equilibrium, periodic, and quasi-periodic states, the fourth state is occupied by the chaotic system. Chaotic systems generally have high sensitivity to the initial state and parameters. When small differences in parameters are observed in the chaotic state, the system will be subjected to significant changes.[119] Furthermore, for any chaotic circuit, the phase diagram assumes a singular attractor. However, the chaotic system is asymmetrical, as observed from the signal amplitude and duration. Thus, it is feasible to incorporate the signal generated by a chaotic circuit into the carrier wave to accomplish a chaotic secure communication.[120] The chaotic secure communication is centered on synchronization. The actualization of a chaotic system can be attained under weak signal coupling if both the transmitter and the receiver in the communication system are identical. Identical signal outputs are generated by the receiver and transmitter. To encrypt the signal, it is concealed through the chaotic signal of the carrier, which transmits a mixed signal of the chaotic carrier and information to the receiver. An attacker cannot easily decrypt it because it requires a transmitter and receiver with identical structural parameters to achieve a chaotic synchronization. Through this approach, the security risks associated with algorithm encryption can be prevented by hardware encryption.

For chaotic signals to occur, chaotic circuits must be generated because chaotic circuits are fundamentally constructed using complex mathematical models of differential equations. Conventional circuits require more components to construct differential equations. The differential equation is fitted by the nonlinear property of the memristor, which ensures that the original chaotic circuit is simplified and enables the construction of a differential equation to attain the chaotic state. Hence, chaotic circuits can be readily constructed using a single memristor. In 1963, the Lorentz system was established and was the first model to simulate weather changes to reveal complex chaotic dynamics.[121] Subsequently, the memristor was successfully integrated into the system by Chua. The type of circuit developed by Chua is a classical resistance–inductance–capacitance chaotic circuit. Its structural components include two capacitors, one inductor, a single resistor, and one memristor (Figure 13, Panel 1). From this circuit, the fundamental dynamic characteristics and characteristics of the memristor are revealed.[122] The gradual development of the chaotic circuit centered on the memristor occurred when the chaotic circuit based on the memristor was adjudged to be achievable.

A chaotic circuit was proposed by Wu et al., which was integrated with a heart-shaped attractor, and a comprehensive study on how memristors control and regulate the chaotic system was conducted.[122] The attributes of the chaotic circuit were discovered, which are presented subsequently. First, a mirror symmetry can be observed in the attractor of the chaotic system the moment there is a switch in the polarity of the memristor (Figure 13, Panel 2). A comprehensive discussion is provided on the specific mathematical model.[122] Second, as changes occur in the memristor parameters, it impacts the chaos degree of a system by either suppressing or enhancing it to various degrees. Thus, artificial intervention in a chaotic system can be conducted through controlled nonlinear devices, such as memristors. A significant proportion of the chaotic circuits based on memristors are constructed based on the differential equations of nonlinear systems; subsequently, through the adjustment of the number of components based on the circuits proposed by Chua, a new circuit structure model was proposed. Then, the parameters of the circuit were adjusted. The new system dynamics were confirmed to exhibit independence, as revealed from the numerical simulation, bifurcation diagram, and Lyapunov spectrum analysis. Eventually, the effectiveness of the new type of circuit structure was proven using images, along with the analysis of the correlation between adjacent pixels and the core sensitivity using an image histogram. To evaluate the image encryption ability of a chaotic system, an essential statistical feature to consider is the correlation of adjacent pixels.

\[
\rho_{xy} = \frac{\text{cov}(x,y)}{\sqrt{D(x)D(y)}}
\]  

(2)

Here, the pixel values of the two adjacent pixels in the image are denoted as \( x \) and \( y \). The covariance is mathematically represented as \( \text{cov}(x, y) \), i.e.,

\[
\text{cov}(x,y) = \frac{1}{N} \sum_{i=1}^{N} [x_i - E(x)][y_i - E(y)]
\]

(3)

where \( E(x) \) is the expected value of the pixel, \( D(x) \) is the variance of the pixels. Thus

\[
E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i
\]

(4)

and

\[
D(x) = \frac{1}{N} \sum_{i=1}^{N} [x_i - E(x)]^2
\]

(5)

Subsequently, we present a comparison between several chaotic circuits. In 2016, two memristor models of continuous smooth fifth-order hyperchaos was developed.[123] Using the referenced mathematical model,[52] the several parameters, namely image encryption, image spectrum graph, correlation between adjacent pixels, were compared by Wang et al. In addition, to construct chaotic circuits, several models were proposed. For instance, memristor chaotic systems can achieve finite-time synchronization through adequate control.[125] From the application of this algorithm, it can be noted that it is not necessary for the sender to transmit the key to the receiver; consequently, the interception and cracking of the key is prevented, which leads to security system enhancement. Thus, this system incorporates the
characteristic that the initial state of the memristor significantly impacts the chaotic system. The fuzzy control vector of the circuit proposed by Chua was deduced by Lin et al.,\textsuperscript{[126]} who proposed a synchronization method of fuzzy modeling and provided a verification of the effectiveness of the chaotic synchronization method. However, no suitable method has been discovered to assess the correlation of the chaotic circuit security, with the exception of adjacent pixel points correlation (Table 7). Moreover, similar to memristor-based PUF, the memristor-based chaotic image processing generally does not exceed the simulation stage, which has not yet been accomplished in actual engineering.\textsuperscript{[87]}

*Figure 13.* Chaotic circuit based on memristors: Panel 1. Circuit proposed by Chua for chaos generation; Panel 2. Y–Z planar phase diagram with heart-shaped attractor chaotic circuit when $g$ is changed and $a$, $b$, $c$, $d$, $e$ are set as $a = 12$, $b = 2.2$, $c = 0.1$, $d = 22$, $e = 0.5$; Reproduced with permission.\textsuperscript{[122]} Copyright 2016, Elsevier. Panel 3. a) Original and encrypted images; b) Histogram representation of both the original and encrypted images; c) Diagram of adjacent pixel correlation at the levels of the original and encrypted images; Reproduced with permission.\textsuperscript{[122]} Copyright 2018, Elsevier. Panel 4. a) Original and encrypted images; b) Histogram representation of both the original and encrypted images; c) Correlation diagram of adjacent pixels at the levels of the original and encrypted images. Reproduced with permission.\textsuperscript{[123]} Copyright 2016, AIP Publishing.
Memristor applications in hardware security have significant potential, but still face several challenges. The advantage of memristor crossbars is that the crossbar density and output key randomness of a memristor is higher and strong. Assuming all the components of the circuit are substituted with memristors, the circuit can be more innovative and have higher randomness. Therefore, memristor crossbars are suitable for schemes that significantly increase the number of CRPs. The drawbacks are as follows. First because the resistance value of memristors is nonlinear, the circuit principle and circuit model construction are more complex, which is harmful to the shortening development cycle. Second, the memristor crossbar always has a hidden current; consequently, it is difficult for the devices to have different logical states. Third, if we assume that the read/write current of one memristor is controlled by the researchers, then crosstalk is readily established, thereby limiting the parallel output of memristors. The properties of memristors cause the first problem and cannot be changed at present. The memristor crossbars or CMOS–memristor hybrid circuits can only be selected according to different scheme requirements. To solve the second type of problem, there is a requirement to reasonably apply and set the input voltage pulse along with the logical state voltage. The third problem is more challenging because of the structural limitation of the array itself.

Meanwhile, diffused memristors can achieve higher integration and lower power consumption than the CMOS–memristor circuits. An increasing number of schemes are selecting diffusion memristors in the PUFs and RNGs used in their designs. Diffusion memristors have significant potential. In the future, chaotic circuits can also be exploited by diffusion memristors to enhance the encryption performance of chaotic systems.

The evaluation index of hardware safety devices must be improved. The judgment indicators of the horizontal analysis, PUFs, and TRNGs are more accurate; therefore, to accurately compute the uniqueness and reliability of PUFs, numerical formulas can be used. The randomness of the generated random numbers denotes the major criterion of the RNG, which can be determined through the NIST pass rate. The image encryption effect cannot be accurately determined through the chaotic circuit because it lacks an accurate judgment index for the process. Based on a data comparison of each scheme, another approach to ascertain the degree of chaos is by determining the correlation between adjacent pixels before and after image encryption is proposed. Even though TRNG, PUF, and chaotic circuits all have benefits in terms of memristor applications, they are still confronted with the following problems. 1) The state maintenance is affected by the extreme external temperature changes and continuous voltage cycles. 2) Optimization is still necessary for parameters such as circuit power consumption, stability, and frequency despite the tendency of the TRNG memristor application to provide a high degree of integrated circuit area. 3) To serve as the memristor, several chaotic circuits replaced the conventional CMOS tube, which necessitates significant innovation in the circuit design, whose implementation is currently not feasible.

### 4. Future Outlook

Memristor applications in hardware security have significant potential, but still face several challenges. The advantage of memristor crossbars is that the crossbar density and output key randomness of a memristor is higher and strong. Assuming all the components of the circuit are substituted with memristors, the circuit can be more innovative and have higher randomness. Therefore, memristor crossbars are suitable for schemes that significantly increase the number of CRPs. The drawbacks are as follows. First because the resistance value of memristors is nonlinear, the circuit principle and circuit model construction are more complex, which is harmful to the shortening development cycle. Second, the memristor crossbar always has a hidden current; consequently, it is difficult for the devices to have different logical states. Third, if we assume that the read/write current of one memristor is controlled by the researchers, then crosstalk is readily established, thereby limiting the parallel output of memristors. The properties of memristors cause the first problem and cannot be changed at present. The memristor crossbars or CMOS–memristor hybrid circuits can only be selected according to different scheme requirements. To solve the second type of problem, there is a requirement to reasonably apply and set the input voltage pulse along with the logical state voltage. The third problem is more challenging because of the structural limitation of the array itself.

Meanwhile, diffused memristors can achieve higher integration and lower power consumption than the CMOS–memristor circuits. An increasing number of schemes are selecting diffusion memristors in the PUFs and RNGs used in their designs. Diffusion memristors have significant potential. In the future, chaotic circuits can also be exploited by diffusion memristors to enhance the encryption performance of chaotic systems.

The evaluation index of hardware safety devices must be improved. The judgment indicators of the horizontal analysis, PUFs, and TRNGs are more accurate; therefore, to accurately compute the uniqueness and reliability of PUFs, numerical formulas can be used. The randomness of the generated random numbers denotes the major criterion of the RNG, which can be determined through the NIST pass rate. The image encryption effect cannot be accurately determined through the chaotic circuit because it lacks an accurate judgment index for the process. Based on a data comparison of each scheme, another approach to ascertain the degree of chaos is by determining the correlation between adjacent pixels before and after image encryption is proposed. Even though TRNG, PUF, and chaotic circuits all have benefits in terms of memristor applications, they are still confronted with the following problems. 1) The state maintenance

### 5. Conclusion

This review discussed the implementation of memristors in hardware security, in addition to research properties, methods, principles, and progress. The different schemes of PUF, RNG, and chaotic circuit were compared. The innovation of memristors in hardware safety was classified into two aspects: the application of a single memristor to a circuit and the complete replacement of a circuit with a memristor crossbar. The advantages and disadvantages of the two innovation directions are analyzed. Furthermore, an evaluation index of the safety-related performance of chaotic circuits is urgently required to compare the performance of different chaotic circuits and promote the development of memristors in chaotic systems.

### Acknowledgements

This work was supported by the National Key R&D Plan (2017YFB0405400 and 2016YFB0402700), the National Natural Science Foundation of China (61774175, 61674146, 61634006 and 61875140), the Key Program of National Natural Science Foundation of Beijing (4181001), the Opened Fund of the State Key Laboratory of Integrated Optoelectronics (No.IOSKL2017KF12), and Young and Middle-aged Talents Program of the State Ethnic Affairs Commission (2019).

### Conflict of Interest

The authors declare no conflict of interest.

### Keywords

chaotic circuits, hardware security, memristors, physical unclonable functions, random number generators

Received: June 10, 2020  
Revised: September 10, 2020  
Published online: October 29, 2020

[1] C. Konstantinou, M. Maniatakos, F. Saqib, S. Hu, J. Plusquellic, Y. Jin, in 20th IEEE European Test Symp, IEEE, Cluj-Napoca 2015, pp. 1–8.
[2] S. Park, M. Vosguerichian, Z. Bao, Nanoscale 2013, 5, 1727.
[3] W. Zeng, L. Shu, Q. Li, S. Chen, F. Wang, X.-M. Tao, Adv. Mater. 2014, 26, 5310.
[4] B. Chen, F. M. J. Willems, IEEE Internet Things J. 2019, 6, 435.
[5] Y. Lu, L. D. Xu, IEEE Internet Things J. 2019, 6, 2103.
[6] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, D. Qiu, Wirel. Netw. 2014, 20, 2481.
[7] P. McDaniel, S. McLaughlin, IEEE Secur. Priv. Mag. 2009, 7, 75.
Shiya Lv was born in Fujian, China, in 1999. She is an undergraduate student at the Department of Electronic Information Engineering, Minzu University of China, Beijing, China. Her current research interests include application of memristor in hardware security and biosensor.

Jian Liu received his PhD degree in physics from The University of Birmingham, Birmingham, United Kingdom, in 1998. Since 2005, he is a full professor in Institute of Semiconductors, Chinese Academy of Sciences, Beijing, China. His current research interests include semiconductor optoelectronic detectors, THz image and metamaterials.

Zhaoxin Geng received his PhD degree from Institute of Electronics, Chinese Academy of Sciences, in 2007. Presently, he is a professor in School of Information Engineering, Minzu University of China. His current research focuses on the micro/nanofluidic, biosensor and applications of nanoplasmonics, localized surface plasmon resonance, terahertz modulator, and metamaterials.