A Survey on Memristor Modeling and Security Applications

M. T. Arafin[1], C. Dunbar[2], G. Qu[3], N. McDonald[4], L. Yan[5]
[1, 2, 3] ECE Department, University of Maryland College Park, MD, USA
[4, 5] Air Force Research Laboratory, Information Directorate, Rome, NY, USA
[1, 2, 3]E-mail: {marafin, cdunbar, gangqu}@umd.edu

Abstract

With the recent advances in memristors as a potential building block for future hardware, it becomes an important and timely topic to study the role that memristors may play in hardware security. To address this issue, this paper presents a survey on research activities on memristor modelling and potential application of memristors in hardware security. First, we give an overview of the current literature on memristor experimentation, characterization, and modeling which includes Chua's original theoretical prediction model, more detailed models based on recent memristor implementations, and the SPICE simulation models. Then, we report the current research efforts on memristor-based security in three major areas: (1) memristor hardware primitives (*e.g*., physical unclonable function) that are based on the memristor effective resistance model, (2) encryption schemes that leverage the chaotic behavior of the memristor circuit, and (3) security concerns in memristor-based memory systems.

We observe that most of these works have limited scope and are based on simplified memristor models which diminish their practical value in security applications. Security applications have strict demands on repeatability, reliability, robustness, unforgeability, cost, resilience, and so on. To address these deficiencies, we propose a list of research areas that need to be addressed for building memristor-based security applications. We also analyze how memristors, as a new hardware building block, will impact major challenges in hardware security.

Keywords

Hardware Security, Physical Unclonable Functions (PUFs), Intellectual Property (IP) Protection, Memristors, Non-volatile memory, Non-linear Circuit Theory

1. Introduction

We start with a short description of the history of memristor from Wikipedia [1]: "The concept of a memristor was originally envisioned in 1971 by circuit theorist Leon Chua as a missing non-linear passive two-terminal electrical component relating electric charge and magnetic flux linkage [2]. According to the governing mathematical relations, the resistance of a memristor is not constant but depends on the history of current that had previously flowed through the device, *i.e.,* its present resistance depends on how much electric charge has flowed through it and in which direction in the past. The device remembers its history. When the electric power supply is turned off, the memristor maintains its most recent resistance state until it is turned on again [2, 3]. Chua has more recently argued that the definition could be generalized to cover all forms of two-terminal non-volatile memory devices based on resistance switching effects [4] although some experimental evidence contradicts this claim. For example, a non-passive nano-battery effect is observable in resistance switching memory [5].

In 2008, a team at HP Labs claimed to have found Chua's missing memristor based on an analysis of a thin film of titanium dioxide [6]." After the first demonstration on TiO_2 based memristors, other research groups have proposed different memristor implementations. Nearly all of these implementations follow a metal-insulator-metal (MIM) structure, which affords a rich research space of possible material stack combinations. For example, [7] uses chalcogenides and [8, 9] use metal oxides insulators *etc*. According to Wikipedia- "In March 2012, a team of researchers from HRL Laboratories and the University of Michigan announced the first functioning memristor array built on a CMOS chip" [1], [10].

As memristors are becoming a prominent component for the next generation computer hardware, it is imperative to investigate security and trust issues related to this emerging technology. This is because security at software, network, and system levels all need assistance from the hardware platform. To other components the hardware, or the computer chip, is considered to be trusted and secure, an assumption which is often not true. Hardware itself is facing more and more severe security and trust threats, from hardware Trojans and backdoors inside the integrated circuit (IC), to various side-channel and physical attacks from outside, as well as intellectual property (IP) protection problems that arise with the outsourcing of design, testing, and manufacturing. Therefore, the securities at other levels are negatively impacted by the (lack of) security of the underlying hardware.

From the perspective of hardware designers there are three major challenges in hardware security: ***securing the design***, ***securing the computation and data***, and ***building hardware security primitives.*** For instance, research on digital watermarking schemes and circuit obfuscation techniques are trying to prevent hardware counterfeiting and thus ensure the security of the design and design IPs. Secure computer architectures and trusted integrated circuits (IC) or co-processors have been designed to secure the data that are being used for computation and communication. Studies on physically unclonable functions (PUFs) explore the applicability of intrinsic randomness found in an IC for generating unique device identifiers, cryptographic keys and seeds for random number generators.

This work is supported in part by the National Natural Science Foundation of China under Grant No. 61228204.

These hardware security research works are mostly built on the available traditional circuit building blocks and components. The addition of memristor-based circuits will enrich the toolset for designing hardware security primitives, but may also introduce new security vulnerabilities. In this paper, our objective is to present a survey on the current state of research in memristor-based hardware security and the opportunities and challenges in this research. We will first give an overview on memristor models that are commonly used for designing memristor-based systems.

2. Memristor Modeling

Most of the reported research works in current literature on memristors are built on theoretical models due to the limited access to memristor devices and fabrication facilities. In this section, we briefly survey popular theoretical models on the instantaneous resistance of a memristor based on their nature and implementation. Polynomial approximation models for the chaotic property of memristors can be found in section 3.2 when we survey their applications in encryption and secure communications.

2.1 Models of Chua's Predicted Memristor

In his seminal paper [2], Chua mathematically predicted the possible existence of a fourth fundamental circuit element – the memristor. For a charge-controlled memristor, he reasoned that the instantaneous resistance of a memristor could be written as,

$$M(q) = \frac{d\phi(q)}{dq} \equiv \frac{v(t)}{i(t)} \tag{1}$$

where $q(t) = \int_{-\infty}^{t} i(\tau)\,d\tau$ is the electric charge, *φ(q)* is the magnetic flux, *v(t)* is the voltage across the device, and *i(t)* is the electric current flowing in the device at time *t*. Therefore, from equation (1), we can see that the resistance (also known as memristance *M(q)*) of an ideal memristor is dependent on the current that has previously passed through the device.

Later, Chua and Kang generalized the concept of memristors and memristive system in [3]. It was theoretically argued that the dynamic properties of a current controlled memristive system can be expressed with the help of an internal state variable *w* such that:

$$\frac{dw}{dt} = f(w,i) \tag{2}$$

$$v(t) = \mathsf{M}(w,i) \times i(t) \tag{3}$$

where $\mathsf{M}(w,i)$ is the generalized resistance of the memristive system and *f(w,i)* is a function that captures the boundary behavior and various nonlinear dynamical effects.

It can be seen from equation (3) that for zero input current there will be a zero output voltage, irrespective of the state variable *w*. Hence, this dynamic system has a zero-crossing Lissajous figure-like input-output relationship [3]. This input-output characteristic in the *v-i* plane is also known as *pinched hysteresis loop* of memristors, and it is considered to be a signature property of this circuit element [4, 11]. As the frequency of the signal along the memristor increases, this zero-crossing pinched hysteresis loop shrinks in size, and it becomes a straight line when the frequency approaches infinity [11]. We will briefly discuss existing memristor models (*i.e.*, definitions of *f(w,i)* and $\mathsf{M}(w,i)$) and their motivations in the following section.

2.2 Models of Existing Memristors

The memristor discovered by HP Labs consists of a thin film (5 nm) with one layer of insulating TiO_2 and another layer of oxygen deficient TiO_{2-x}, sandwiched between platinum contacts in the simple metal-insulator-metal (MIM) structure [6]. Several models have been proposed to explain the electronic properties of this memristive device and devices of similar construction.

2.2.1 The Primary Model and Effective Resistance

Strukov *et al.* used a simple model to express the current-voltage relationship of the HP memristor with the following equations, which can be considered as a special case of equations (2)-(3) with specific expressions for the generalized resistance $\mathsf{M}(w,i)$ and function *f(w,i)* [6]:

$$\frac{dw}{dt} = \frac{\mu_v R_{on}\, i(t)}{D} \tag{4}$$

$$v(t) = \left(\frac{w(t)}{D} R_{on} + \left(1 - \frac{w(t)}{D}\right) R_{off} \right) i(t) \tag{5}$$

where *D* is the film thickness of the memristor, μ_v is the average ion mobility of oxygen vacancies in TiO_2, and *w(t)* is the state variable or system state. Physically, *w(t)* can be viewed as the thickness of the doped region in the thin-film which is created by the linear drift of charged oxygen vacancies (dopants) at a given applied bias. Thus (*D-w*) is the size of the undoped region. R_{on} is the resistance of the memristor when it is completely doped (*i.e., w=D*), and R_{off} is the resistance when it is completely undoped (*i.e.*, *w=0*). Therefore, under this *linear ion drift model*, the *effective resistance* of this structure can be expressed as:

$$\mathrm{M(w)} = \frac{w}{D} R_{on} + \left(1 - \frac{w}{D}\right) R_{off} \tag{6}$$

2.2.2 Models Considering the Boundary Behavior

In the above *linear ion drift model*, the value of the state variable *w* is limited over [0, D]. For proper device modelling, the boundary effects should be taken into consideration as well. To implement boundary behaviors, equation (4) can be modified as:

$$\frac{dw}{dt} = \frac{\mu_v R_{on}}{D} i(t)\; g(w,i) \tag{7}$$

where $g(w,i)$ is a *window function* that captures the physics near the device boundary.

Several approximations for the window function can be found in the literature [12-15]. In [12], Joglekar *et al*. define the window function as:

$$g(w,i) = 1 - \left(\frac{2w}{D} - 1\right)^{2p} \tag{8}$$

where *p* is a positive integer that controls the rate of change of *w* near the device boundary. This window function provides a control for the nonlinearity in the device boundary. However, at the terminal state (*e.g., w* = 0), this window leaves the device stuck in that state. This is referred to as *terminal state problem*. Biolek *et al.* [14] solved this problem by redefining the window function as:

$$g(w,i) = 1 - \left(\frac{w}{D} - \mathrm{u}(-\mathrm{i})\right)^{2p} \tag{9}$$

where *u(i)* is a step function. This model is referred as *non-linear dopant drift model.*

Prodromakis *et al.* [15] proposed the following improved window function that can account for both the linear and non-linear dopant kinetics.

$$g(w,i) = \mathrm{j}\left(1 - \left[\left(\frac{w}{D} - 0.5\right)^2 + 0.75\right]^p\right) \tag{10}$$

where j controls the maximum value of *g(w)*.

Although the models described above capture basic device properties, they are insufficient to describe the underlying higher order non-linearity of actual devices. To address this issue, Lehtonen *et al.* proposed another non-linear model in [16] based on the experimental results presented in [17]. This model can be expressed by the following equations:

$$\frac{dw}{dt} = a\, g(w)\, v(t)^q \tag{11}$$

$$i(t) = w(t)^n \beta \sinh(\alpha v(t)) + \chi[exp(\gamma v(t) - 1)] \tag{12}$$

where *a* and *q* are constants; *g(w)* is the window function; and *α, β, χ, γ* are fitting parameters that depend on the physical properties of the memristor being characterized.

2.2.3 Pickett's Model

Both linear and non-linear drift models assume that electron transport in memristors is due to the drift of carriers under electric field in the doped and undoped regions. These models do not take the underlying quantum mechanical effects into account. Pickett *et al.* proposed a more accurate physical model of TiO_2 memristor that tries to explain the observed complex dynamics using Simmons tunneling theory [18] and drift mechanisms of the carriers. A tunnel barrier is assumed to be formed between the conducting channel of the device and the opposite platinum electrode. An ohmic resistor in series with this tunnel barrier is used to explain the device characteristics. The state variable in this model is represented by the width of the tunnel barrier. This model is called the *Pickett's model* or *Simmons tunnel barrier model* and can be expressed with the following equations [19]:

$$\frac{dw}{dt} = \begin{cases} f_{off} \sinh\left(\frac{|i|}{i_{off}}\right) exp\left[-\exp\left(\frac{w - a_{off}}{w_c} - \frac{|i|}{b}\right) - \frac{w}{w_c}\right], i > 0 \\ -f_{on} \sinh\left(\frac{|i|}{i_{on}}\right) exp\left[-\exp\left(\frac{w - a_{on}}{w_c} - \frac{|i|}{b}\right) - \frac{w}{w_c}\right], \; i < 0 \end{cases} \tag{13}$$

$$i = \frac{j_0 A}{(\Delta w)^2} \{\phi_I e^{-B\sqrt{\phi_I}} - \left(\phi_I + q|v_g|\right) e^{-B\sqrt{\phi_I + q|v_g|}} \tag{14}$$

$$v = v_g + v_R = v_g + iR_s \tag{15}$$

where f_{off}, f_{on}, i_{off}, i_{on}, a_{off}, a_{on}, w_c, and *b* are fitting parameters; *q* is the elementary electronic charge; *A* is the average channel are; R_s is the series resistance of the channel; ϕ_I is the modified barrier height; $j_0 = \frac{q}{2\pi h}$; $B = 4\pi\Delta w \frac{\surd(2m)}{h}$; *h* is Planck's constant; *m* is the average effective mass of the carrier; and v_g is the voltage across the tunnel barrier.

Pickett's model provides good insight of the carrier dynamics and considered a near accurate physical model. However, this model is computationally expensive. Kvatinsky *et al.* proposed a simplified version known as the *threshold adaptive memristor model* to reduce the computational complexity of Pickett's model. This model can be described using the following equations [20]:

$$\frac{dw}{dt} = \begin{cases} k_{off}\left(\frac{i(t)}{i_{off}} - 1\right)^{\alpha_{off}} g_{off}(w); 0 < i_{off} < i \\ 0 \qquad ; i_{on} < i < i_{off} \\ k_{on}\left(\frac{i(t)}{i_{on}} - 1\right)^{\alpha_{on}} g_{on}(w); i < i_{on} < 0 \end{cases} \tag{16}$$

$$v(t) = \left[R_{on} + \frac{R_{off} - R_{on}}{w_{off} - w_{on}}(w - w_{on})\right] i(t) \tag{17}$$

where k_{off}, k_{on}, α_{off}, α_{on} are constants; i_{on}, i_{off} are current thresholds; *w* is the state variable representing the effective tunnel width; $g_{on}(w)$, $g_{off}(w)$ are window functions; and R_{on}, R_{off} are the equivalent effective resistances at the bounds w_{on} and w_{off}. There exist similar models such as the Boundary Condition Memristor (BCM) model presented in [21] that are based on the simplified versions of equations (13)-(15).

2.3 SPICE Simulation Models

Several circuit simulation models using the equations (1) – (17) can be found in the current literature. SPICE models based on linear and non-linear drift models are presented in [14, 13, 16] *etc*. The SPICE model proposed by Biolek *et al.* in [14] and its derivatives have been widely used in the literature for simulating memristors. In this circuit, the window function is incorporated using user-defined function *f()* and the memory effects are incorporated using a feedback controlled integrator. The circuit diagram for the model is given in figure 1.

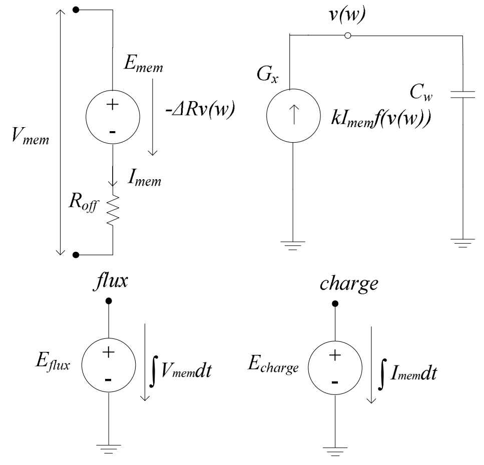
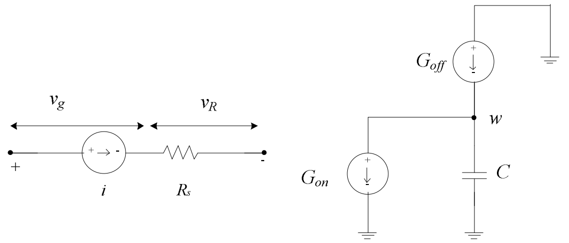


Figure 1: SPICE model of a memristor proposed in [14]. Here V_{mem} and I_{mem} are the voltage and current across the memristor; $k=\mu_v R_{ON} / D^2$; $\Delta R=R_{on} - R_{off}$; C_w represents the doped layer of width w; $v(w)$ is the voltage across the layer; and E_{flux} and E_{charge} represent the calculated time-integral of voltage and current (*i.e.,* flux and charge).

Abdalla *et al.* provided a SPICE model based on equation (13)-(15) in [22] as given in figure 2. This circuit is derived from equations (13)-(15) and uses experimental values to define its parameters. Although this model tries to accurately represent the device physics, simulating this model overestimates current by around 20% and causes the simulated memristor to switch faster than the experimental memristor. Kvatinsky *et al.* have presented a SPICE model in [20] which is claimed to be more accurate than drift models. Other models have been proposed and implemented in MATLAB based on equation (3)-(15) and different forms of the window functions.

A comprehensive comparative study on some representative models with taking Pickett's model as a standard reference can be found in a recent article [23]. Overall, both simplified models that coarsely approximate the behavior of memristors and complex physical models of memristors are available for further analysis. We will discuss the implications of these models on memristor-based security applications next.



(a) **(b)**

Figure 2: SPICE model of a memristor proposed by Abdalla *et al* [22]. Here, the current and voltages are given by equations (14) - (15). (b) represents the state-space model of the device where C is the width of the tunnel barrier; w is the voltage across the barrier; and $\frac{dw}{dt}=\frac{1}{C}(G_{off}-G_{on})$, where G_{off} and G_{on} are the right hand side of equation (13) for i>0 and i<0 respectively.

3. Memristor-based Security Applications

There have been many reported efforts on memristors related to security. We focus our survey on memristor PUFs that are based on the effective resistance model (see equation (6)), encryption schemes that leverage the chaotic behavior of the memristor circuit, and security concerns in memristor-based memory system.

3.1 Memristor-based PUFs

Silicon PUFs are on-chip circuitry that can extract fabrication variations, such as the discrepancy from the expected delay or the instable power-on states of the memory cells, to generate chip-dependent PUF data that can be used as secret keys or as seeds of random number generators, and/or to create challenge response pairs (CRPs) for authentication and attestation. These capabilities have opened up new avenues for implementing hardware intrinsic security and trust. The memristor system state variable *w(t)* or the corresponding effective resistance $\mathsf{M}(w,i)$ provides an ideal situation to build memristor PUFs.

Rose *et al.* studied several properties of the memristive device and the potential security applications [24]. These properties include the nonlinear and bidirectional input-output response, inherent non-volatility combined with temporal drift, and unique device forming step of memristors. The possible applications include authentication, key exchange, bit commitment, and time stamping. In the following, we elaborate two representative works and their extensions.

A public PUF, called nano-PPUF, is reported in [25]. It is built using memristor-based crossbar array and supporting challenge-response circuits. It utilizes features including sneak path currents, process variations, and computationally intensive SPICE models. First, an accurate simulation model for the memristor crossbar is constructed using physical measurements. The challenge for this PUF can be constructed as an applied voltage in a given polymino (a selection of specific memristors) in the crossbar and the response can be measured from the output voltage or current. The key idea is that although the complete physical model for the crossbar is known to public, accurate simulation for a large polymino is hard and therefore, without the physical crossbar and the knowledge of correct polymino to choose, it would be computationally prohibitive to calculate the response for a given challenge under timing constraint. With a few hundreds of memristors, the following time-bounded authentication protocol is implemented [25]. Additional improvements on this PUF circuit are discussed in [26] and [27].

Two discrete device CMOS-memristive PUF circuits were proposed in [28]. The first one is a memristive memory based PUF cell with one memristor and four MUXes as shown in figure 3. It leverages the variations in the memristor's write time to generate one bit of information. First, a *RESET* operation is performed by applying *NEG* = 1 and $\overline{R}/W=1$. This sets the memristor in high resistive state. Then a *SET* operation is executed by applying *NEG* = 0 and $\overline{R}/W=1$ pulse for a time $t_{wr,min}$. If $t_{wr,min}$ is greater than the time required to switch the memristor from a high resistive state (HRS) to a low resistive state (LRS), then the memristor will be in the LRS; otherwise, the memristor will be in the HRS (assuming binary resistance states). Finally, for *READ* operation $\overline{R}/W$ is set to 0 and a challenge bit is applied at the *challenge* terminal. $t_{wr,min}$ must be chosen properly such that the memristor will be equally likely to be in the HRS or the LRS. Therefore, the state of the memristor will be determined by the random variations in its physical implementation which leads to this cell's physical unclonability. The second PUF proposed in [28] is a lateral switching cell, which leverages the stochastic nature of filament formation in memristors to create PUF bits. Rose *et al.* improve the PUF design in figure 3 with a circuit of *N* memristors that can generate *N* response bits from *N* challenge bits and the proper *SET* time to ensure the uniqueness, uniformity, and bit-aliasing of the response bits [29].

Another PUF that integrates a memristor device into the conventional ring oscillator PUF (RO-PUF) structure is proposed in [30]. The authors demonstrate that the randomness in the resistance values increases the number of CRPs of conventional RO-PUFs. The feasibility of building a memristor-based PUF is discussed in [31]. The authors suggested a weak write mechanism that leverages the resulting unpredictable logic states to implement the PUF. However, the evaluations only focused on the uniqueness of the PUF secret without considering its stability.

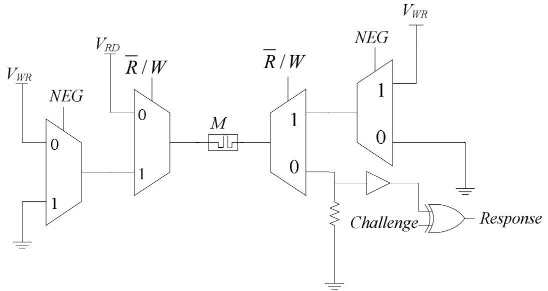


Figure 3: The 1-bit memristive memory based PUF cell proposed in [28].

A common limitation with memristive PUFs is that their security analyzes was based solely on simulations of small circuits. These initial results still need to be verified against fabricated circuits, modules and chips.

3.2 Memristor-based Chaotic Circuits for Encryption and Secure Communications

A Chua circuit is an RLC-type circuit with a memristor in a branch as shown in figure 4. This circuit offers interesting chaotic and dynamic properties relevant for chaos generation and related experimentation. Interestingly, the *φ-q* relationship of the memristor is approximated by polynomials in most of the works in this field. For instance, [32] uses a continuous cubic monotonically increasing function to build a smooth memristor oscillator; [33] uses a piece-wise linear model to generate chaos for image encryption; [34] uses the model that describes a particle in a multi-well potential to realize the chaotic behavior of memristor; and [35] also uses cubic equations to demonstrate the compound synchronization of a four memristor chaotic oscillator system. Muthuswamy *et al.* have provided a standard model and experimental realization of a Chua circuit using resistors, capacitors, and op-amps [36].

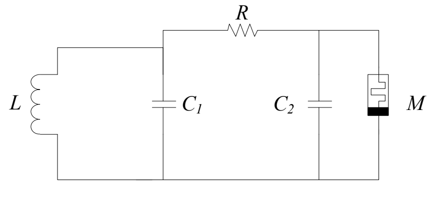


Figure 4: Chua's circuit for chaos generation [37].

Chaos theory researchers have proposed using chaotic circuits as stream ciphers in the past and have naturally extended the idea to include memristor-based hardware. For example, in [38] a memristor-based Van der Pol oscillator has been proposed for secure communication. For this communication protocol, Alice sends messages to Bob using a chaotic transmitter system containing a Van der Pol oscillator. Bob has an identical Van der Pol oscillator in his receiver too. Since chaotic circuits are sensitive to noise, the authors of [38] designed an adaptive synchronization feedback protocol which can be used for reconstructing the message from the received chaotic signals. Security of this communication protocol depends on the difficulty of matching two non-identical Van der Pol oscillators. This work uses PSpice models similar to the one discussed in [36] to simulate the protocol and validate the design. A compound synchronization technique for multiple memristor chaotic oscillators is discussed in [35] which can be used in multi-party secure communication.

Image encryption techniques using a chaotic memristive system is discussed in [33]. Chaotic sequences can be generated from a Chua circuit based on unique initial values of the system parameters. These generated sequences can then be used with scrambling or pixel replacement techniques to perform image encryption. Image scrambling based on these chaotic sequences are claimed to be more resistive towards attacks [33]. Initial values of the system parameters are used as the user keys for the encryption and decryption process.

Similar to the memristive PUF work, the security claims of these works are also only based on simulation results and need to be verified against real devices. More importantly though, these designs have not yet been vetted by the cryptography community and should not be used in security applications until that happens.

3.3 Secure Memory Systems with Memristors

Memristors are considered to be a promising building block of next generation high-density memory systems due to their energy efficiency. Several memory architecture and designs have been proposed for realizing memristor-based main memory units [39, 40]. However, memristors are non-volatile, and therefore, sensitive data written in memristor-based main memory can be probed even after the system is turned off. Moreover, the lower write endurance of memristors can lead to DoS attack on a targeted memory location of a non-volatile memory system.

To mitigate against these emerging security vulnerabilities, a hardware intrinsic encryption technique named *sneak path encryption* (SPE) is discussed in [41]. Fundamentally, cross-bar based memories exhibit sneak path currents where a current through one memory cell will also induce current flowing through adjacent memory cells. This sneak path current creates a voltage difference across adjacent cells and the resistances of the cells change if the voltages across them are over a given threshold. This fundamental idea is used for designing the SPE protocol in [41] where the applied current is from a read operation. In other words, a crossbar-based memristive memory can be designed in such a way that reading one memory cell can effectively corrupt adjacent cells such that the decryption process will fail. A secure memory architecture is developed in [42] using a SPE control unit between the main memory and L2 cache. It follows then that if the current is from a write operation, adjacent cells can be used as sensors or counters to detect DoS attacks and assist in wear-leveling algorithms.

Different aspects of analog designs based on a memristor's high and low resistive states and their use in implementing a secure sense amplifier are discussed by Hoe *et al.* in [43]. This work adds security measures in the sense amplifier circuit used for reading out memory locations. The sense amplifier used in this work is similar to those used in SRAM circuits; however, the body bias for some MOSFETs in the design is controlled by a memristor. This results in a controllable mismatch in the differential amplifier present in the circuit, and for successful readout of the memory this mismatch needs to be minimized. To achieve the resistance that can nullify the mismatch, a certain current profile must be applied to the memristor, where this current profile may be used as the secret key for accessing the memory

3.4 Other Security Applications of Memristors

Several other security applications have also been proposed in recent literature. Design for a true random number generator is discussed in [44]. This random number generator is based on the random trapping and detrapping of carriers in the defects of the oxide thin film. This trapping process results in random fluctuations of the resistance of the device. [44] provides the required circuits to convert these fluctuations to measurable voltage signals. The fabricated circuit passed several statistical randomness tests designed by National Institute of Standards and Technology (NIST).

With respect to cryptography, Khedkar *et al.* have proposed a cryptographic module using memristors and CMOS circuits to employ power profile obfuscation techniques in encryption systems [45, 46]. This module uses a CMOS circuit for AES encryption unit and memristors for state memory. The memristive memory is assumed be a 1-transistor-1-memristor crossbar system. This state memory consists of two parts: regular and inverse state memory. The power profile of the encryption system depends on the power consumed in data-read and data-write to the memory which creates a side channel for differential power analysis (DPA) attacks. To obfuscate the power profile, [46] suggested simultaneous read and write to both regular and inverse state memory. Simulation results demonstrate this approach to be successful in counteracting DPA attacks.

Finally, we mention the tamper detection technique in memristive circuits and systems [27] and memristor-based neuromorphic computing for cybersecurity [47, 48].

4. Opportunities and Challenges

With the great promise in terms of energy efficiency of memristors, it is a question of when, not whether, memristors will be used routinely in system design. First, we analyze the three major challenges in hardware security for hardware designers listed in the introduction.

- *securing the design*: Memristor designs and design IPs will face the same security and protection questions for CMOS design. Given the non-volatile nature of memristors and the simplicity of the memristor-based system design (*e.g.* crossbar architecture), attacks such as reverse engineering will be much easier and protections by watermarking, fingerprinting, or obfuscation might become less effective. It will be important to *develop dedicated protection techniques for memristor-based systems and IPs*.
- *securing the computation and data:* For the same aforementioned reasons, validating the trustworthiness of memristor-based system could be less challenging because there will be less room to insert hardware Trojans and introduce backdoors. However, keeping data secure will be non-trivial. Ideally, we need to *build design methodologies for memristor-based memory and systems with security and trust as one of the top objectives*.
- *building hardware security primitives:* As we have surveyed in section 3, researchers have investigated memristors in many fields for security applications. Despite the success at various levels, many unanswered questions remain as we will show next. It is crucial to *deliver usable memristor-based security primitives*.

We now give a list of questions that are important for memristor-based security.

1. Design methodology with security and trust. We have learned from CMOS design that security and trust cannot be added as a patch after the system is built. To avoid making the same mistake, we need to study the potential security vulnerabilities in memristor-based memory and system design (*e.g.,* backdoors and hardware Trojans), develop corresponding countermeasures, and integrate them into the design methodology to be developed for memristor systems.
2. Experimental validation. We have seen many models for memristors in Section 2 and it is expected that memristors with different materials or different structure will exhibit different behaviors. However, there are no industry compatible models for any type of memristors. There is need for circuit designers to work more closely with device engineers and physicist to implement realistic models of their memristors. Even then, and although it may not be feasible for now, it is vital to have experimental validation of any memristor-based security applications, particularly hardware security primitives, before we adopt them.
3. Performance evaluation. For most security primitives (*e.g.,* user or device authentication protocols) to be usable there will be extremely high requirements on properties such as repeatability, reliability, robustness, unforgeability, resilience, cost, *etc.* Whether experimental (or simulation) study can provide satisfactory confidence remains unclear. Such evaluation should consider factors such as operating voltage, humidity, temperature, device

aging, as well as known attacking methods such as side channel analysis, tampering and physical attacks.

4. New features and new applications. There are many types of memristors, each may exhibit different behavior. Close collaboration between hardware security researchers and device engineers should be encouraged further to improve the transition of new memristor properties and behaviors in the laboratory to the development of security applications.

5. Conclusions

With the implementations of the recently popularized memristor, there is an emerging trend of studies on the applications of memristors beyond simply nonvolatile memory to hardware security primitives. As the availability of memristors is still limited and there are no sufficiently accurate memristor models, the usability of these memristor-based approaches is still speculative, particularly for security applications. In this paper, we survey the existing memristor models and the memristor-based security applications. We discuss possible impacts memristors may make on major hardware security challenges and identify important problems to be solved. By improving the collaboration between device engineers and hardware security researchers, more significant progress can be made in implementing memristors for hardware security.

6. Acknowledgement

This work is supported in part by the Air Force Research Laboratory under agreement number FA8750-13-2-0115, a MURI grant under Air Force Office of Scientific Research, and by a University Partnership with the Laboratory of Telecommunications Sciences contract number H9823013D00560002.

7. References

[1] http://en.wikipedia.org/wiki/Memristor

[2] L. O. Chua, “Memristor-the missing circuit element,” IEEE Transactions on Circuit Theory, vol. 18, no. 5, pp. 507–519, 1971.

[3] L. O. Chua and S. M. Kang, “Memristive devices and systems,” Proceedings of the IEEE, vol. 64, no. 2, pp. 209–223, 1976.

[4] L. O. Chua, “Resistance switching memories are memristors,” Applied Physics A, vol. 102, no. 4, pp. 765–783, 2011.

[5] I. Valov, E. Linn, S. Tappertzhofen, S. Schmelzer, J. van den Hurk, F. Lentz, and R. Waser, “Nano batteries in redox-based resistive switches require extension of memristor theory,” Nature communications, vol. 4, p. 1771, 2013.

[6] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams, “The missing memristor found,” Nature, vol. 453, no. 7191, pp. 80–83, 2008.

[7] A. S. Oblea, A. Timilsina, D. Moore, and K. A. Campbell, “Silver chalcogenide based memristor devices,” 2010.

[8] L. Goux, J. Lisoni, M. Jurczak, D. Wouters, L. Courtade, and C. Muller, “Coexistence of the bipolar and unipolar resistive-switching modes in NiO cells made by thermal oxidation of Ni layers,” Journal of Applied Physics, vol. 107, no. 2, p. 024512, 2010.

[9] B. Briggs, S. Bishop, K. Leedy, B. Butcher, R. Moore, S. Novak, and N. Cady, “Influence of copper on the switching properties of hafnium oxide-based resistive memory,” in MRS Proceedings, vol. 1337. Cambridge University Press, 2011, pp. mrss11–1337.

[10] K.-H. Kim, S. Gaba, D. Wheeler, J. M. Cruz-Albrecht, T. Hussain, N. Srinivasa, and W. Lu, “A functional hybrid memristor crossbar-array/CMOS system for data storage and neuromorphic applications,” Nano Letters, vol. 12, no. 1, pp. 389–395, 2012.

[11] L. Chua, “The fourth element,” in Memristor Networks. Springer, 2014, pp. 1–13.

[12] Y. N. Joglekar and S. J. Wolf, “The elusive memristor: properties of basic electrical circuits,” European Journal of Physics, vol. 30, no. 4, p. 661, 2009.

[13] S. Benderli and T. Wey, “On SPICE macromodelling of TiO_2 memristors,” Electronics letters, vol. 45, no. 7, pp. 377–379, 2009.

[14] Z. Biolek, D. Biolek, and V. Biolkova, “SPICE model of memristor with nonlinear dopant drift,” Radioengineering, vol. 18, no. 2, pp. 210–214, 2009.

[15] T. Prodromakis, B. P. Peh, C. Papavassiliou, and C. Toumazou, “A versatile memristor model with nonlinear dopant kinetics,” IEEE Transactions on Electron Devices, vol. 58, no. 9, pp. 3099–3105, 2011.

[16] E. Lehtonen and M. Laiho, “CNN using memristors for neighborhood connections,” in 12th International Workshop on Cellular Nanoscale Networks and Their Applications (CNNA). IEEE, 2010, pp. 1–4.

[17] J. J. Yang, M. D. Pickett, X. Li, D. A. Ohlberg, D. R. Stewart, and R. S. Williams, “Memristive switching mechanism for metal/oxide/metal nanodevices,” Nature Nanotechnology, vol. 3, no. 7, pp. 429–433, 2008.

[18] J. G. Simmons, “Generalized formula for the electric tunnel effect between similar electrodes separated by a thin insulating film,” Journal of Applied Physics, vol. 34, no. 6, pp. 1793–1803, 1963.

[19] M. D. Pickett, D. B. Strukov, J. L. Borghetti, J. J. Yang, G. S. Snider, D. R. Stewart, and R. S. Williams, “Switching dynamics in titanium dioxide memristive devices,” Journal of Applied Physics, vol. 106, no. 7, p. 074508, 2009.

[20] S. Kvatinsky, E. G. Friedman, A. Kolodny, and U. C. Weiser, “TEAM: threshold adaptive memristor model,” IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 60, no. 1, pp. 211–221, 2013.

[21] A. Ascoli, R. Tetzlaff, F. Corinto, and M. Gilli, “PSpice switch-based versatile memristor model,” in IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, 2013, pp. 205–208.

[22] H. Abdalla and M. D. Pickett, “SPICE modeling of memristors,” in IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, 2011, pp. 1832–1835.

[23] A. Ascoli, F. Corinto, V. Senger, and R. Tetzlaff, “Memristor model comparison,” IEEE Circuits and Systems Magazine, vol. 13, no. 2, pp. 89–105, second quarter 2013.

[24] G. Rose, J. Rajendran, N. McDonald, R. Karri, M. Potkonjak, and B. Wysocki, “Hardware security strategies exploiting nanoelectronic circuits,” in 18th Asia and South Pacific Design Automation Conference (ASP-DAC), Jan 2013, pp. 368–372.

[25] J. Rajendran, G. Rose, R. Karri, and M. Potkonjak, “Nano-PPUF: A memristor-based security primitive,” in IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Aug 2012, pp. 84–87.

[26] J. B. Wendt and M. Potkonjak, “The bidirectional polyomino partitioned PPUF as a hardware security primitive,” in IEEE Global Conference on Signal and Information Processing (GlobalSIP), 2013.

[27] J. Rajendran, R. Karri, J. B. Wendt, M. Potkonjak, N. R. McDonald, G. S. Rose, and B. T. Wysocki, “Nanoelectronic solutions for hardware security.” IACR Cryptology ePrint Archive, vol. 2012, p. 575, 2012.

[28] G. Rose, N. McDonald, L.-K. Yan, B. Wysocki, and K. Xu, “Foundations of memristor based PUF architectures,” in IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH), July 2013, pp. 52–57.

[29] G. S. Rose, N. McDonald, L.-K. Yan, and B. Wysocki, “A write-time based memristive puf for hardware security applications,” in IEEE/ACM International Conference on Computer-Aided Design (ICCAD). IEEE, 2013, pp. 830–833.

[30] O. Kavehei, C. Hosung, D. Ranasinghe, and S. Skafidas, “mrPUF: A memristive device based physical unclonable function,” arXiv preprint arXiv:1302.2191, 2013.

[31] P. Koeberl, Ü. Kocabas, and A.-R. Sadeghi, “Memristor PUFs: a new generation of memory-based physically unclonable functions,” in Proceedings of the Conference on Design, Automation and Test in Europe. EDA Consortium, 2013, pp. 428–431.

[32] B. Bo-Cheng, L. Zhong, and X. Jian-Ping, “Transient chaos in smooth memristor oscillator,” Chinese Physics B, vol. 19, no. 3, p. 030510, 2010.

[33] Z. hui Lin and H.-X. Wang, “Image encryption based on chaos with PWL memristor in Chua’s circuit,” in International Conference on Communications, Circuits and Systems, (ICCCAS), July 2009, pp. 964–968.

[34] T. Driscoll, Y. Pershin, D. Basov, and M. Di Ventra, “Chaotic memristor,” Applied physics A, vol. 102, no. 4, pp. 885–889, 2011.

[35] J. Sun, Y. Shen, Q. Yin, and C. Xu, “Compound synchronization of four memristor chaotic oscillator systems and secure communication,” Chaos: An Interdisciplinary Journal of Nonlinear Science, vol. 23, no. 1, p. 013140, 2013.

[36] B. Muthuswamy, “Implementing memristor based chaotic circuits,” International Journal of Bifurcation and Chaos, vol. 20, no. 05, pp. 1335–1350, 2010.

[37] L. O. Chua, The genesis of Chua’s circuit. Electronics Research Laboratory, College of Engineering, University of California, 1992.

[38] E. M. Ngouonkadi, H. Fotsin, and P. L. Fotso, “Implementing a memristive Van der Pol oscillator coupled to a linear oscillator: synchronization and application to secure communication,” Physica Scripta, vol. 89, no. 3, p. 035201, 2014.

[39] SS. H. Jo, K.-H. Kim, T. Chang, S. Gaba, and W. Lu, “Si memristive devices applied to memory and neuromorphic circuits,” in Proceedings of 2010 IEEE International Symposium on Circuits and Systems (ISCAS), IEEE, 2010, pp. 13–16.

[40] W. Lu, K.-H. Kim, T. Chang, and S. Gaba, “Two-terminal resistive switches (memristors) for memory and logic applications,” in 16th Asia and South Pacific Design Automation Conference (ASP-DAC). IEEE, 2011, pp. 217–223.

[41] S. Kannan, N. Karimi, O. Sinanoglu, and R. Karri, “Security vulnerabilities of emerging nonvolatile main memories and countermeasures,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 34, no. 1, pp. 2–15, Jan 2015.

[42] SS. Kannan, N. Karimi, and O. Sinanoglu, “Secure memristor-based main memory,” in Proceedings of the the 51st Annual Design Automation Conference on Design Automation Conference. ACM, 2014, pp. 1–6.

[43] D. Hoe, J. Rajendran, and R. Karri, “Towards secure analog designs: A secure sense amplifier using memristors,” in IEEE Computer Society Annual Symposium on VLSI (ISVLSI), July 2014, pp. 516–521.

[44] C.-Y. Huang, W. C. Shen, Y.-H. Tseng, Y.-C. King, and C.-J. Lin, “A contact-resistive random-access-memory-based true random number generator,” Electron Device Letters, IEEE, vol. 33, no. 8, pp. 1108–1110, 2012.

[45] GG. Khedkar, C. Donahue, and D. Kudithipudi, “Towards leakage resiliency: memristor-based AES design for differential power attack mitigation,” in SPIE Sensing Technology and Applications. International Society for Optics and Photonics, 2014, pp. 911907–911907.

[46] G. Khedkar, D. Kudithipudi, and G. Rose, “Power profile obfuscation using nanoscale memristive devices to counter DPA attacks,” IEEE Transactions on Nanotechnology, vol. PP, no. 99, pp. 1–1, 2014.

[47] M. Hu, H. Li, Y. Chen, Q. Wu, and G. S. Rose, “BSB training scheme implementation on memristor-based circuit,” in IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA). IEEE, 2013, pp. 80–87.

[48] R. E. Pino, M. J. Shevenell, H. Cam, P. Mouallem, J. L. Shumaker, and A. H. Edwards, “Computational intelligence and neuromorphic computing potential for cybersecurity applications,” in SPIE Defense, Security, and Sensing. International Society for Optics and Photonics, 2013, pp. 87510B–87510B.