Hardware Security Strategies Exploiting Nanoelectronic Circuits

Garrett S. Rose[1], Jeyavijayan Rajendran[2], Nathan McDonald[1], Ramesh Karri[2], Miodrag Potkonjak[3] and Bryant Wysocki[1]
[1]Air Force Research Laboratory, Information Directorate, Rome, New York 13441 USA
[2]Polytechnic Institute of New York University, Brooklyn, New York 11201 USA
[3]University of California, Los Angeles, Los Angeles, California 90095 USA

Abstract - Hardware security has emerged as an important field of study aimed at mitigating issues such as piracy, counterfeiting, and side channel attacks. One popular solution for such hardware security attacks are physical unclonable functions (PUF) which provide a hardware specific unique signature or identification. The uniqueness of a PUF depends on intrinsic process variations within individual integrated circuits. As process variations become more prevalent due to technology scaling into the nanometer regime, novel nanoelectronic technologies such as memristors become viable options for improved security in emerging integrated circuits. In this paper, we provide an overview of memristor based PUF structures and circuits that illustrate the potential for nanoelectronic hardware security solutions.

I. Introduction

Since the mid 1970s, information security has evolved from primarily focusing on the privacy of stored and in-transit data to incorporating trust, anonymity, and remote ground truthing. Over this forty year time frame, the usage scenario of security technologies has evolved from securing physical premises with mainframe computers to securing lightweight, low-cost, and low-power mobile phones, tablets, and sensors. Concurrently, new security metrics such as resiliency against physical and side channel attacks have emerged.

In addition to traditional computer security issues, the fabless integrated circuit (IC) production model has added increased concerns from the perspective of trusted hardware. Specifically, untrusted parties involved on the foundry side of the IC manufacturing process could potentially reverse engineer, overproduce, or insert trojans into ICs designed by a fabless design house. Obviously, the ability to mitigate such issues within the production of ICs is important to the protection of IP and the prevention of untrusted or malicious elements being included in critical computer systems.

The use of unique hardware signatures or identification circuits provide one popular way to mitigate issues such as IC counterfeiting and piracy. For example, a physical unclonable function (PUF) leverages unclonable physical disorders in the IC design process to produce unique responses (outputs) upon the application of challenges (inputs) [18]. PUFs [19-21] are hardware-based secret key mechanisms where the function that maps a challenge to a response is the secret. These unique responses have been used in several ways to enforce security. It is also important to note that process variations become more pronounced as IC technology is scaled further into the nanometer regime. Thus, nanoelectronic devices and circuits provide an opportunity to develop robust hardware security primitives (e.g. PUFs).

In many cases, nanoelectronic security primitives are potentially more robust than conventional CMOS security primitives. They can also serve as the basis for provable security in an information theoretic sense as the complexity of attacking a nanoelectronic security primitive is equivalent to the difficult problem of solving a large system of nonlinear equations [1]. Finally, emerging nanoelectronics have the potential to yield miniscule form factors, ultra low power consumption, and fast computation times relative to current semiconductor technologies.

A variety of materials and devices including memristors, graphene, plasmonics, and quantum dots are being explored for use in nanoelectronics. These nanoelectronic devices often have highly non-linear input-output responses and exhibit inherent process variations much like current CMOS technologies [2-5]. Examples of how the properties of nanoelectronic devices can be leveraged are provided in this work with a specific focus on nanoscale memristor devices.

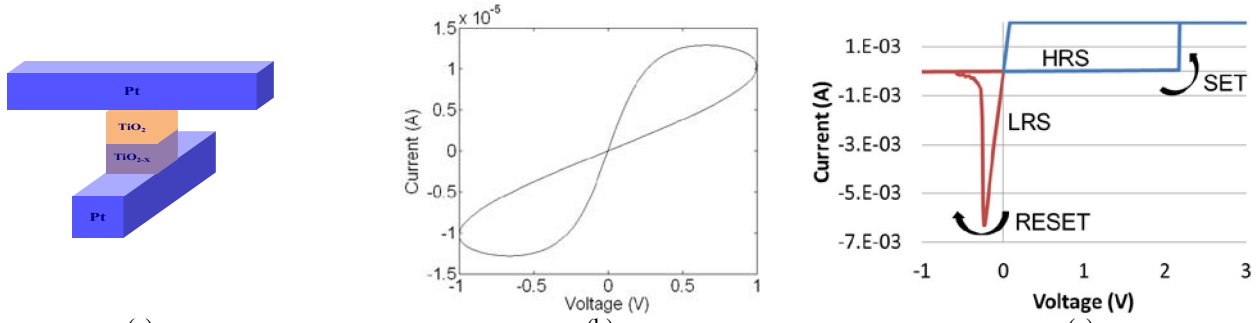
Our objective is to explore the security relevant capabilities of nanoelectronic devices. Specifically, we explain why the nonlinear, bidirectional input-output response characteristics, inherent nonvolatility combined with temporal drift, and the unique device forming step of memristors are interesting from a security perspective. We also introduce nanoelectronic security primitives for device identification and security authentication.

II. Memristive Nanoelectronics

In recent years, a wide variety of nanodevices have been successfully realized. Examples of these emerging nanodevices include metal-oxide memristors, phase change devices, spin-torque transfer devices, carbon nanotubes, graphene, and quantum-dots. In this work, we discuss security primitives mainly using metal-oxide memristors due to their unique features that lend themselves to improved security.

The memristor (memory resistor) was first theorized by Leon Chua in [6]. In that seminal work, Chua showed that memristance $M(q)$ relates charge q and flux φ such that the

978-1-4673-3030-5/13/$31.00 ©2013 IEEE



(a) (b) (c)

Figure 1. (a) Metal-insulator-metal (MIM) memristor structure [2], (b) theoretical current-voltage characteristics of a bipolar memristor and (c) experimental characteristics for a 3rd generation Al/Cu_xO/Cu memristive device depicting typical SET and RESET values [17].

resistance of the device will change with the applied electric field and time:

$$M(q) = \frac{d\varphi(q)}{dq}. \quad (1)$$

The parameter $M(q)$ denotes the memristance of a memristor, measured in ohms. The memristance at any particular time depends on the integrals of the current and the voltage through the device from $-\infty$ to that time. Thus, the memristor behaves like an ordinary resistor at any given instance of time, where its memristance depends on the complete history of the device [2, 6].

One method for fabricating memristors consists of placing a TiO_{2-X} layer with oxygen vacancies on a TiO_2 layer without oxygen vacancies and sandwiching them between metallic electrodes as shown in Figure 1(a) [2]. Apart from the structure shown in Figure 1(a), memristors can be fabricated as metal-insulator-metal (MIM) structures, where the insulating layer may be a variety of materials including chalcogenides [7, 8], metal oxides [9, 10], perovskites [11, 12], or organic films [13, 14].

Memristors have at least two resistance states: a high resistance state (HRS) and a low resistance state (LRS). To change a memristor from the HRS to the LRS (termed a SET operation), a voltage bias of the appropriate polarity and magnitude, V_{SET}, must be applied across the device. A device in the LRS may then be returned to the HRS via a RESET operation, typically by applying a voltage of lower magnitude, V_{RESET}. For example, Figure 1(b) depicts the theoretical bowtie I-V curve demonstrated by a memristor. Also shown in Figure 1(c) are experimental results for an Al/Cu_xO/Cu memristor. Additional resistance states are attainable by limiting the applied voltage or current.

In some memristors, when the device is first fabricated, it will not switch for the usual toggle voltages (V_{SET} and V_{RESET}) and behaves like a resistor [15]. Such a device is initialized by applying a large formation voltage, V_f, which will force the memristor to the LRS and thereafter switch whenever the toggle voltages (V_{SET} and V_{RESET}) are applied across the device.

The memristance of a memristor is affected by process variation induced changes in device size and dopant concentration. Furthermore, the effect of variation in the thickness of the device on the memristance value is highly non-linear (this effect is more evident in the LRS than HRS [16]).

Some of the aforementioned characteristics of memristors (e.g., process variations) pose problems when designing memory and logic circuits. However, we show that these problematic characteristics can actually be leveraged as features in the context of security.

III. Nano-Enabled Security Tokens

Certain memristors can be used to generate a unique signature for hardware. This approach exploits two different features of memristors: 1) the inherent, non-uniform, irreproducible process variations during fabrication and 2) the requirement of "forming" to make them functional. As described in [17], nonpolar memristors in series of pairs can be used as random bit generators (RBG), where the bit generation is a function of the location of a low resistance filament. Multiple instances of such random bit generators can produce a random word. This signature is non-volatile and thus may be used for hardware identification purposes. Such hardware IDs are used to mitigate issues such as electronic counterfeiting.

Consider a pair of memristors in series as shown in Figure 2. The bottom metal electrode (BE) and the insulator layer are common for the two devices. Each memristor has its own top metal electrode (TE). This particular structure can be written as a unit of two series memristors by leaving BE floating and applying the write voltage across the top electrodes. In this particular case, writing both devices as if they are one unit constitutes the forming step for both memristors.

During the forming step, one TE is biased while the other TE is grounded. Two low resistance filaments are formed, one beneath each TE through the memristive layer to the BE. Then during the RESET operation, the resistance value of the two series memristors is returned to the HRS. During this switch, only one of the low resistance filaments becomes highly resistive; the other filament remains of low resistivity. The

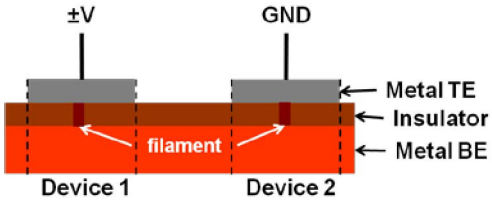


Figure 2. Electrical configuration for random bit generation.

location of this latter filament serves as the random bit value, since under which TE the low resistance filament is located is random due to fabrication variations. Additionally, after operation in this manner, the low resistance filament location is impervious to additional SET and RESET operations. Thus, a unique signature is established for the hardware that may not be determined prior to the irreversible "formation" step.

Figure 3 illustrates a simple CMOS-memristive circuit that leverages the structure from Figure 2 in the construction of a cell that can be used to build a PUF. Specifically, a PUF leverages unclonable physical disorders in the IC design process to produce unique responses (outputs) upon the application of challenges (inputs) [18]. PUFs [19—21] are hardware-based secret key mechanisms where the function that maps a challenge to a response is the secret. These unique responses have been used in several ways to enforce security.

There is one control signal (*Sel*) in the circuit in Figure 3 which is used to select between the forming step and the operating mode of the two series memristors M1 and M2. If *Sel* is 0 then the node between M1 and M2 is left floating and either V_{WR} (SET) or $-V_{WR}$ (RESET) is applied across the pair. On the other hand, when Sel is 1 the circuit is in an operation or read mode where V_{RD} is driven across both devices and a load resistance.

As described for the structure in Figure 2, after formation and a RESET, one memristor will be in the HRS state while the other remains in the LRS state. Due to the inherent variability of both memristive devices, which memristor is in the HRS and which the LRS is entirely random. Figure 3 also shows how one of the outputs from one of the two memristors can be selected using an arbitrary *Challenge* bit. The *Challenge* bit could be one bit of an externally supplied PUF challenge. The corresponding output or *Response* bit would then be one bit of the hardware specific response portion of the security key. Thus, the circuit shown in Figure 3 constitutes one bit of a memristive PUF circuit.

As a point of comparison, the inherent process variations in a CMOS Field Programmable Gate Array (FPGA) can be leveraged to generate random numbers [22]. Circuits such as ring oscillators were used for randomness extraction. However, the extracted random values are unstable as the frequency of the ring oscillators is strongly dependent on temperature.

A unique device signature in CMOS can also be derived

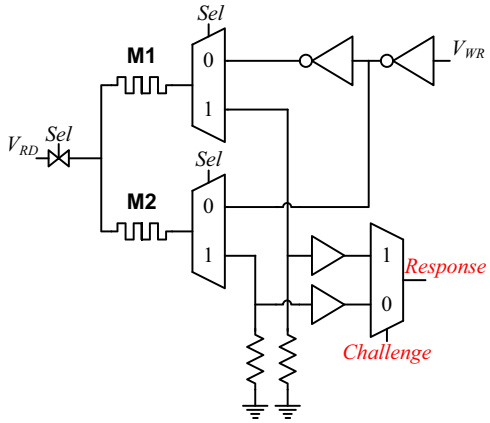


Figure 3. A possible memristive 1-bit PUF cell configuration.

from an unwritten Static Random Access Memory (SRAM) circuit. An SRAM cell consists of two transistors connected in a butterfly like fashion. Due to threshold voltage mismatch caused by process variations, one transistor will be stronger than the other. This mismatch is then used to generate the random signature. However, an attacker in the manufacturing chain can easily read this unique signature and use it to spoof the hardware. Unlike with the memristor-based RBG, this tampering is not irrefutable.

IV. A Memristor Based Nano-PPUF

The memristor based NanoPPUF is a security primitive used to implement a variety of security protocols such as authentication, key exchange, bit commitment and time stamping. Two protocols, authentication and key exchange, are described here. The NanoPPUF exploits several features of memristors such as process variations, bi-directionality, crossbars, complex simulation models of memristors and crossbars.

Unlike a PUF, simulation models of a PPUF circuit are made public [23]. Although an attacker can simulate the PPUF on a given challenge to obtain a response, the simulation time is too large (several years) compared to the time it takes to apply the challenge and obtain the response on the PUF (a few seconds). Nanocircuits, e.g., memristor crossbars, can be used to implement PPUF circuits, hence the name NanoPPUF. Simulation complexity of a memristor crossbar circuit arises from the non-linearity and bi-directionality of the devices and the exponential number of sneak paths in the crossbar [1].

NanoPPUFs leverage special geometric structures called polyominoes. Polyominoes are formed by connecting a certain number of individual blocks. A polyomino is called an *M*-omino if it is formed by *M* connected blocks. An *M*-omino in a crossbar can be visualized by considering *M* resistive devices connected by nanowires either in the horizontal or vertical directions [1].

The number of possible *M*-omino shapes is exponential. The total number of possible polyomino shapes with *M*

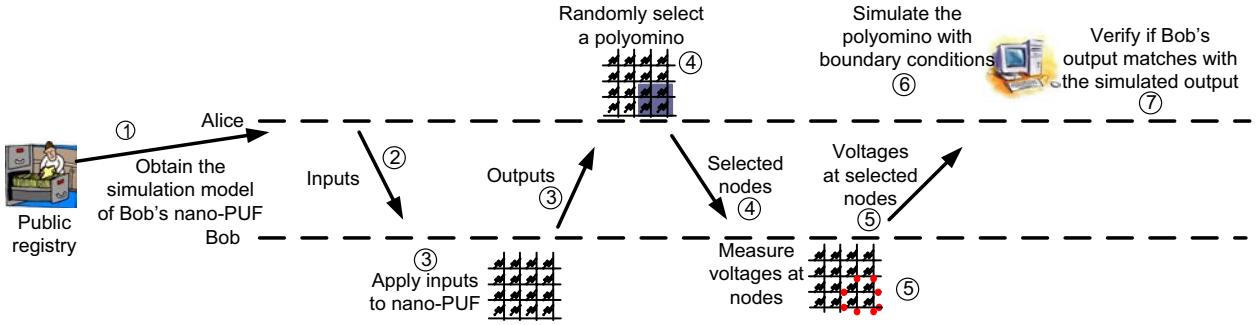


Figure 4. Protocol for time-bounded authentication using NanoPPUF [1].

resistive devices in a crossbar is $\frac{c\lambda^M}{M}\times N$, where λ and c are 4.0626 and 0.3169, respectively [24].

We define the challenge, C, as the vector of inputs and the response, R, as the vector of outputs such that $C \rightarrow R$ when C is applied to the NanoPPUF. R represents the set of boundary conditions (voltage values) of a selected polyomino in the NanoPPUF. The challenge set X represents the list of pins on which the challenge vector C is applied; the length of C and X are equal. The communicating parties, Alice and Bob, are represented by A and B, and their respective NanoPPUFs are denoted by $PPUF_A$ and $PPUF_B$.

Some protocols for using the NanoPPUF are described in more detail in [1]. As an example, a NanoPPUF based time-bounded authentication protocol is illustrated in Figure 4. The user Alice is able to validate the authenticity of Bob's response who possesses the physical NanoPPUF. Due to the polyominoes in the NanoPPUF and the bidirectionality of the NanoPPUF cell, Alice can simulate some selected polyominoes (a subset of the NanoPPUF) and validate that the inputs and outputs along the boundaries of the selected polyomino. However, an adversary pretending to be Bob would have to respond to Alice with a full output response R since he cannot guess which polyomino partition Alice will choose in a reasonable amount of time.

PPUFs in CMOS technology have been created using XOR networks. They operate on the similar operating principle that the simulation of the entire PPUF circuit is computationally impossible. However, the complexity of their simulation model is less complex than nanodevices because CMOS devices are unidirectional whereas nanodevices such as memristors are bidirectional. Thus, PPUFs based on CMOS technology are easier to attack than PPUFs based on nanotechnology.

A variant of PPUFs called SIMulation Possible but Nanoscale Technology Laborious (SIMPL) systems have also been developed. SIMPL systems were constructed using Cellular Non-linear Networks and Static Random Access Memory (SRAM) cells [25]. Such systems were used for time-bounded authentication of a user. Unfortunately, unlike PPUFs, the time difference between the execution time and simulation time is not exponential. Thus, it becomes possible for an attacker to determine the secret in a short enough time to spoof an authorized user. This prohibits the use of SIMPL for two-party protocols like bit commitment, oblivious transfer, zero-knowledge proofs, and coin flipping [26].

V. Conclusions

In this work, we had highlighted a few novel features of nanoelectronic devices, specifically memristors, and demonstrated how they can be used for constructing security primitives. The features listed in this paper are based on both experimental and theoretical device research. Using the features listed in the paper, device physicists can now engineer nanodevices, not only for memory and logic applications, but also for security applications. Similarly, security researchers can develop mathematical proofs for these security primitives by abstracting the features of nanodevices. Circuit designers can act as a bridge between device engineers and security researchers and construct circuits that will harness these devices to satisfy mathematical strengths. Overall, the idea of using nanoelectronics for security applications will be a new and interesting avenue of research for both electronic and security researchers.

VI. Acknowledgements

The material and results presented in this paper have been cleared for public release, unlimited distribution by AFRL, case number 88ABW-2012-6077. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of AFRL or its contractors.

References

[1] J. Rajendran, G. S. Rose, R. Karri, and M. Potkonjak, "Nano-PPUF: A Memristor-based Security Primitive", *in the Proc. of IEEE Intl. Conf. on VLSI*, pp. 84-87, 2012.

[2] D. B. Strukov, G. S. Snider, D. R. Stewart and R. S. Williams "How we found the Missing Memristor," Nature, vol. 453, pp. 80–83, 2008.

[3] Y.T. Chiu, "A Memristor True Random-Number Generator", *IEEE Spectrum*, 2012.

[4] 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," *IEEE Electron Device Letters*, vol.33, no.8, pp.1108-1110, 2012.

[5] N.R. McDonald, S.M. Bishop, B.D. Briggs, J.E. Van Nostrand, and N.C. Cady, "Influence of the plasma oxidation power on the switching properties of Al/Cu_xO/Cu memristive devices", *Solid-State Electronics*, Vol. 78, pp. 46-50 (2012).

[6] L. Chua, "Memristor-the missing circuit element," *IEEE Transactions on Circuit Theory*, vol. 18, no. 5, pp. 507 – 519, 1971.

[7] Oblea, A.S.; Timilsina, A.; Moore, D.; Campbell, K.A., "Silver chalcogenide based memristor devices," *Neural Networks (IJCNN), The 2010 International Joint Conference on*, pp.1-3, 18-23 July 2010.

[8] R. Waser and M. Aono, "Nanoionics-based resistive switching memories," *Nature Materials*, Vol. 6, pp. 833–840, 2007.

[9] L. Goux, J. G. Lisoni, M. Jurczak, D. J. Wouters, L. Courtade, and Ch. Muller, "Coexistence of the bipolar and unipolar resistive-switching modes in NiO cells made by thermal oxidation of Ni layers," J*ournal of Applied Physics*, vol. 107, no. 2, pp. 024512 - 024512-7, 2010.

[10] B.D. Briggs, S.M. Bishop, K.D. Leedy, B. Butcher, R. L. Moore, S. W. Novak and N.C. Cady, "Influence of Copper on the Switching Properties of Hafnium Oxide-Based Resistive Memory," *MRS Proceedings*, vol. 1337, 2011.

[11] A. Sawa, T. Fujii, M. Kawasaki, and Y. Tokura, "Interfaces resistance switching at a few nanometer thick perovskite manganite layers," *Applied Physics Letters*, vol. 88, no. 23 pp. 232112 - 232112-3, 2006.

[12] K. Szot, W. Speier, G. Bihlmayer, and R. Waser, "Switching the electrical resistance of individual dislocations in single crystalline $SrTiO_3$," *Nature Materials*, vol. 5, pp. 312–320, 2006.

[13] J. C. Scott and L. D. Bozano, "Nonvolatile memory elements based on organic materials," *Advanced Materials*, vol. 19, pp. 1452–1463, 2007.

[14] N. B. Zhitenev, A. Sidorenko, D. M. Tennant, and R. A. Cirelli, "Chemical modification of the electronic conducting states in polymer nanodevices," *Nature Nanotechonlogy*, vol. 2, pp. 237–242, 2007.

[15] Q. Xia, et. al. "Memristor−CMOS Hybrid Integrated Circuits for Reconfigurable Logic", *Nano Letters,* vol. 9, no. 10, 2009.

[16] J. Rajendran, H. Manem, R. Karri and G.S. Rose, "Approach to Tolerate Process Related Variations in Memristor-Based Applications," Intl Conf. on VLSI Design, pp. 18–23, 2011.

[17] N. R. McDonald, *Al/Cu_xO/Cu Memristive Devices: Fabrication, Characterization, and Modeling* (Unpublished master's thesis). University at Albany, SUNY, College of Nanoscale Science and Engineering, Albany, NY.

[18] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," *in the Proc. of the ACM Intl. Conf. on Computer and Communications Security*, pp. 148–160, 2002.

[19] G. E. Suh, C. W. O'Donnell, I. Sachdev, and S. Devadas, "Design and implementation of the AEGIS single-chip secure processor using physical random functions," *in the Proc. of IEEE/ACM Intl. Conf. on Computer Architecture*, pp. 25–36, May 2005.

[20] Y. Alkabani and F. Koushanfar, "Active control and digital rights management of integrated circuit IP cores," *in the Proc. of the IEEE Intl. Conf. on Compilers, Architectures and Synthesis for Embedded Systems*, pp. 227–234, 2008.

[21] J. Guajardo, S. Kumar, G.-J. Schrijen, and P. Tuyls,"Physical unclonable functions and public-key crypto for FPGA IP protection," *in the Proc. of the IEEE Intl. Conf. on Field Programmable Logic and Applications*, pp. 189–195, 2007.

[22] P. Kohlbrenner and K. Gaj. "An embedded true random number generator for FPGAs", *in the Proc. of the ACM Intl. Conf. Field programmable gate array,* pp. 71-78, 2004.

[23] N. Beckmann and M. Potkonjak, "Hardware-Based Public-Key Cryptography with Public Physically Unclonable Functions", *in the Proc. of Intl. Workshop on Information Hiding*, pp. 206-220, 2009.

[24] I. Jensen and A. J. Guttmann, "Statistics of lattice animals (polyominoes) and polygons," *Journal of Physics A: Mathematical and General*, vol. 33, pp. L257–L263, 2000.

[25] U. Rührmair, Q. Chen, P. Lugli, U. Schlichtmann, M. Stutzmann, and G. Csaba, "Towards Electrical, Integrated Implementations of SIMPL Systems", *Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices, Lecture Notes in Computer Science*, vol. 6033, pp. 177-292, 2009.

[26] Marten van Dijk and Ulrich Rührmair, "Physical Unclonable Functions in Cryptographic Protocols: Security Proofs and Impossibility Results," *IACR Cryptology ePrint Archive 2012:228*, 2012, [Online] Available: eprint.iacr.org/2012/228.pdf.