Foundations of Memristor Based PUF Architectures

Garrett S. Rose[1], Nathan McDonald[1], Lok-Kwong Yan[1], Bryant Wysocki[1], and Karen Xu[2]
[1]Air Force Research Laboratory, Information Directorate, Rome, New York 13441 USA
[2]University of California, Los Angeles, Los Angeles, CA 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

Electronic counterfeiting and recirculation is a growing problem. Analysts estimate that nearly 10% of global technology products are likely counterfeits totaling over $7.5 billion in yearly losses to the U.S. semiconductor industry as a whole with an approximate number of over one million suspect parts associated with the U.S. Department of Defense supply chain alone [1]. Much of this stems from the lack of a secure, unique identifier to verify the authenticity and trust of electronic products to which researchers have proposed Physical Unclonable Functions (PUFs) as a solution.

PUFs [2–4] are functions that map intrinsic properties of hardware devices (e.g. process variability) into usable and unique “bits” of information. These unique bits have been used as security primitives in several ways including: as unique identifiers, as secret keys, and in pseudo-random bit generators. While previous researchers have focused on designing PUFs that take advantage of measurable/quantifiable characteristics in CMOS devices (such as propagation delay due to process variability), ongoing advancements in the synthesis, manipulation, and testing of materials on a control level approaching atomic scales opens up possibilities in identifying PUF sources in nano-scale devices. In recent years, a wide variety of nano-devices have been successfully realized. Examples of these emerging nano-devices include metal-oxide memristors, phase change devices, spin-torque transfer devices, carbon nanotubes, graphene, and quantum-dots. Memristors are particularly well suited for PUF implementation due to their controlled sensitivity to process variation and relative compatibility with CMOS fabrication standards.

In this work, we study the feasibility of memristors-based PUFs. We first present a background on two theoretical models of memristors, discuss the limitations of the models when compared to real devices, and assess their potential for use as PUF sources in Section II. We then propose two new memristor-based PUFs in Section III and evaluate their effectiveness using Monte-Carlo simulations and experimentation on actual memristor devices in Section IV. Results and future work are discussed in Section V.

II. Memristive Device Behaviors Useful for Hardware Security Applications

Memristive devices or resistive RAM (ReRAM) are effectively two terminal electrical potentiometers. That is to say, memristive devices have tunable resistance values yet do not require energy to persist at any resistance state or are non-volatile. By applying the appropriate electrical bias for the required duration, the device may be repeatedly switched between at least two resistance states: a high resistance state (HRS) and a low resistance state (LRS). A SET operation switches the device from the HRS to the LRS; a RESET operation does the reverse. For the purposes of this paper, an HRS is a logic ‘0’, and an LRS is a logic ‘1’.

There is no single memristor device design. Typically, these devices are as simple as metal-insulator-metal (MIM) structures, where the insulating materials have been chalcogenides [7, 8], metal oxides [9, 10], perovskites [11, 12], or organic films [13, 14]. Though the gambit of devices demonstrating the switching behaviors thus described may be understood to be “memristors” [13], the exact switching mechanism, parameters, and style will depend upon the specific material stack.

The variations in device properties mean that certain flavors of memristive devices may be optimally suited for different applications. Typically, memristive devices considered for digital logic or memory applications are engineered for binary or multi-level states, where abrupt state transitions are desirable. Other devices demonstrate a more analog transition between the two extreme resistance states. In this paper, we will show that both behaviors may be used to create PUFs.

A. Analog Memristors and Write Time

In the simplest analog model, memristors are modeled as two resistors, R_{on} as the LRS value and R_{off} as the HRS value, weighted by a factor α that varies between 0 and 1 over time. In short, the memristance may be written as $M(t) = \alpha(t)R_{on} + (1 - \alpha(t))R_{off}$. While the model is more complex in practice, the idea remains the same.

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 [14]. Though conical phase change regions were later shown to be responsible for device switching [15], this device can still be modeled as two series resistors (R_{on} and R_{off}) that represent doped and undoped regions of TiO_2, respectively. In the model, the boundary between the regions (w), the thickness of the active layer, moves between 0 and D as a function of an applied electric field while $\alpha = w/D$. In this way, the transition from the LRS to the HRS is an analog process.

[16,17] expanded this model to account for variable mobility as described by:

$$M(t) = R_0 \sqrt{\left(1 - \frac{2\eta \Delta R \varphi(t)}{D^2 R_0{}^2} \cdot \mu R_{on}\right)}, \qquad (1)$$

where constants R_0 is the maximum resistance ($R_0 \approx R_{off}$), ΔR is the difference between R_{off} and R_{on}, and η (±1) is the polarity of the applied voltage signal. The flux $\varphi(t)$ is simply the integral of the applied voltage over the entire usage history of the device:

$$\varphi(t) = \int V_{appl}(t)dt. \qquad (2)$$

Of particular importance to the memristive memory-based PUF considered in this work is the impact of variations in the device thickness D. More specifically, variability in D translates to variations in the read and write times of the memristor when using the device as a memory cell [18]. For example, a memristor being SET from HRS to LRS will only exhibit a logic '1' output if the SET time (i.e. write time to SET the memristor) is greater than some minimum $t_{wr,min}$. If, however, the SET time is chosen to be at or near the nominal $t_{wr,min}$, then variations in D will dictate that the output is nearly as likely to be a logic '0' as it is a logic '1'. This probabilistic status for the output voltage is undesirable for conventional memory systems but can be leveraged in the implementation of PUF circuits.

B. Discrete Memristors

Binary state memristors have only two distinct states, and the transition between the two is typically abrupt. These properties make these devices ideally suited for digital logic and memory elements. Filament creation and rupture is frequently cited as the switching mechanism for these devices.

A PUF circuit was designed specifically for $Al/Cu_xO/Cu$ memristive devices to exploit unique properties detailed in prior research [19]. Unlike most other memristive devices, the $Al/Cu_xO/Cu$ devices switch for any voltage polarity combination, i.e. they are completely nonpolar. The Cu_xO layer is grown via a plasma oxidation process [5]. By virtue of this fabrication process, the oxide thickness and oxygen concentration will vary slightly across the sample. Figure 1 depicts lateral switching (devices in series) of a pair of $Al/Cu_xO/Cu$ devices.

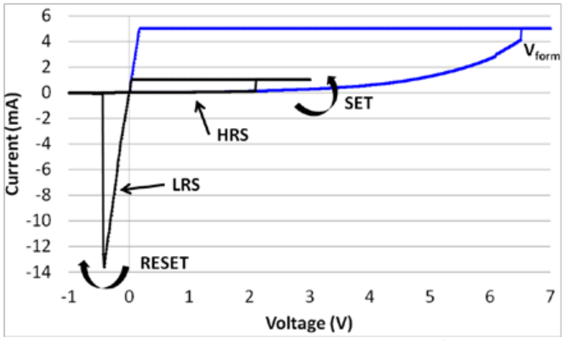


Figure 1. Representative experimental data from a laterally switched 100x100µm $Al/Cu_xO/Cu$ memristive devices described in [19]. The blue curve shows the required initial forming step. The black curve shows typical switching values.

In practice, many memristive materials, including the TiO_2 [21] and $Al/Cu_xO/Cu$ [19] devices considered here, require a forming step to initialize the devices. An elevated voltage is applied across the device to cause the first SET, after which the device can cycle between the HRS and LRS at significantly lower voltages. Prior to this step, the device operates as a regular resistor. The difference in behavior is easy to detect and thus is a prime candidate for tamper detection. In our designs, the memristors are only formed during device provisioning where the PUF challenge response pairs are recorded in a secure environment.

The forming step required to initialize memristor functionality is of great value for the certification of trust. It serves as a red flag when a device has been activated signaling that the security of the PUF may have been compromised. In addition, such evidence can function as a warning sign alerting the user to suspect fabrication and supply chains.

Figure 2 shows a simple state representation for how a binary state memristor, e.g. $Al/Cu_xO/Cu$, can be modeled at a higher level. As represented in the diagram, once the formation step has occurred, the device is only allowed to switch between the HRS and LRS states.

III. Memristive PUF Circuits

A. Memristive Memory Based PUF Cell

As mentioned for the analog memristors, variations in the thickness D of a memristor leads to variability in the write time (and by extension the read time) of the device. This

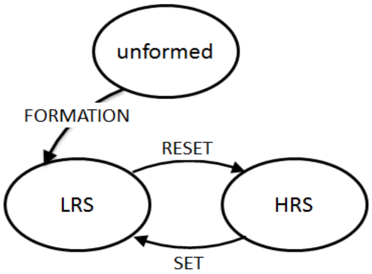


Figure 2. State representation of discrete (specifically binary) operation of $Al/Cu_xO/Cu$ memristor.

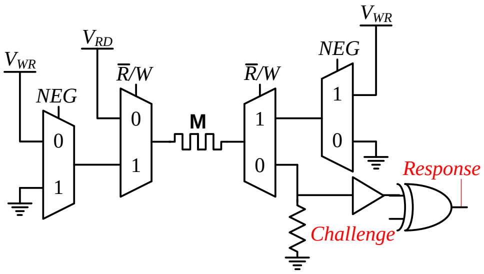


Figure 3. A 1-bit memristive memory-based PUF cell that leverages variations in memristor write times.

property is leveraged in the construction of a simple memory-based PUF cell where the SET time t_{wr} is chosen to be the minimum SET time required to switch the memristor from the HRS to the LRS state, $t_{wr,min}$. If the actual SET time of a particular memristor, $t_{wr,actual}$ is greater than $t_{wr,min}$, then the output voltage when reading the memory cell is likely a logic '0'. Likewise, $t_{wr,actual}$ less than $t_{wr,min}$ will likely lead to an output voltage of logic '1'. By choosing the SET time close to $t_{wr,min}$, the likelihood that the output is logic '1' or logic '0' should each be nearly 50%.

The circuit shown in Figure 3 is an implementation of a single bit of a memristive memory-based PUF. This circuit is essentially a one bit equivalent of the memristive memory presented in prior work [22–24]. Two control signals are used to determine whether the circuit is writing or reading the memristor $(\overline{R}/W)$ and, if writing, the polarity of the write (*NEG*). The circuit works as a PUF by first performing a RESET of the memristor and applying *NEG* = 1 and $\overline{R}/W = 1$ long enough to guarantee the memristor is in the HRS state. Next, a SET pulse is applied for the nominal write time corresponding the $t_{wr,min}$ ($NEG = 0$ and $\overline{R}/W = 1$). After the SET operation, the memristor can be read at the output by applying $\overline{R}/W = 0$.

The *Challenge* for this particular memristive PUF is applied as an input to an XOR function with the output of the simple memory cell as the other input. The output of this XOR is the *Response* bit of the PUF cell which depends on the *Challenge* and the random output of the memristive memory cell. When the likelihood that the output of the memory cell is logic '1' is 50%, then the chance that the *Response* can correctly be guessed is equivalent to guessing the outcome of a fair coin flip.

B. *Lateral Switching PUF Cell*

It has been experimentally demonstrated that Al/Cu_xO/Cu memristive device switching is filament-based [19]. A consequence thereof is a required forming step. The devices will SET at lower voltages only after the forming operation. Thus, by performing a SET operation first, one can test the forming status to verify that all the devices are still in their virgin state. Since the initial switching properties of these devices will be used for the proposed PUF circuit, the ability to verify that the devices have not been previously SET/RESET is critical.

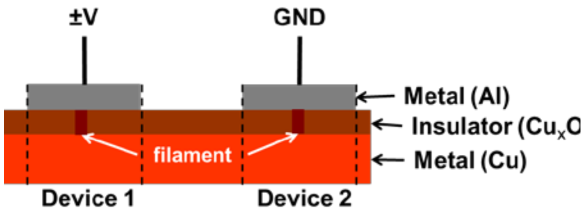


Figure 4. Physical structure of the lateral switching configuration.

The details of experimentally demonstrated lateral switching (switching two devices in series) are described in detail in [19,25]. In brief, a pair of MIM devices with a common ground may be switched laterally, where one top electrode (TE) is biased and the other TE is electrically grounded (Figure 4). While this configuration is merely two devices in series, the applied voltage polarity is reversed across the second device. Thus, lateral switching in this configuration (where two devices have a common substrate) has only been observed for devices demonstrating completely nonpolar switching. However, this protocol in theory may also be achieved using other memristive devices asymmetrically arranged in series.

The protocol for PUF bit retrieval (generation) is SET-RESET. During a lateral SET operation, both devices are written to the LRS; however, after a lateral RESET operation, only one of the two devices switches to the HRS. Experimental results suggest that which of the two devices persists in the LRS is independent of the device to which the voltage bias is applied. Additionally, over subsequent lateral SET/RESET operations, the persistent LRS device remains invariant.

Figure 5 illustrates a simple CMOS-memristive circuit that leverages the structure from Figure 4 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) [26].

There is one control signal $(R/\overline{W})$ in the circuit in Figure 5 which is used to select between the forming step and the operating mode of the two series memristors *M1* and *M2*. If $R/\overline{W}$ 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 $R/\overline{W}$ 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 4, 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 expected to be entirely random. Figure 5 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

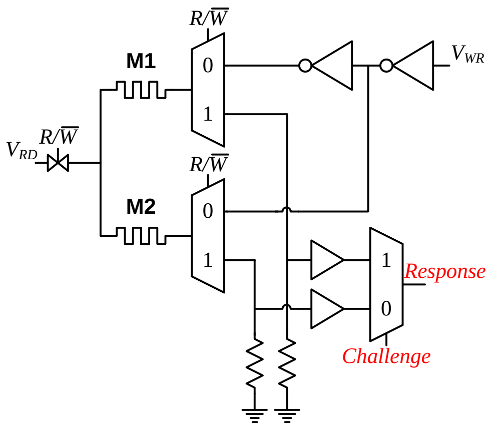


Figure 5. A 1-bit filament growth based PUF cell that leverages the stochastic nature of filament formation in some memristors.

response portion of the security key. Thus, the circuit shown in Figure 5 constitutes one bit of a memristive PUF circuit. Again, the requirement of a forming step means that the memristive device values cannot be read or determined in the foundary without tripping the tamper detection mechanism.

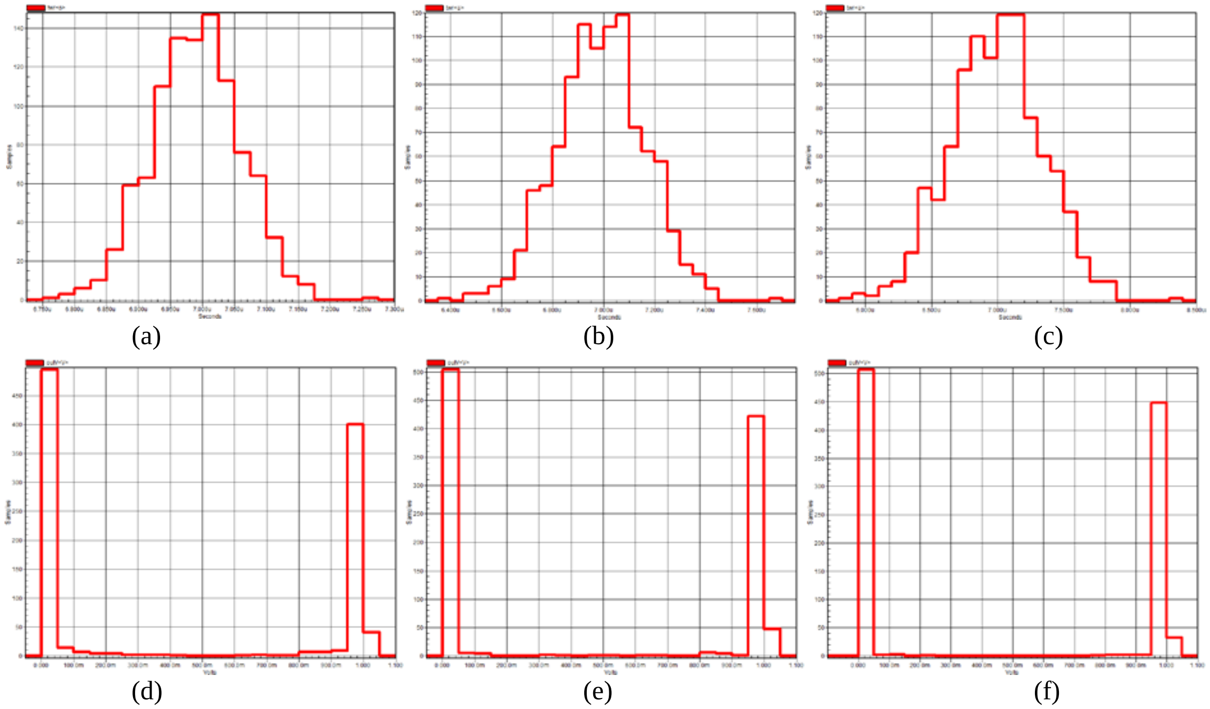
A unique device signature in CMOS can also be derived from an unwritten Static Random Access Memory (SRAM) circuit. An SRAM cell consists of two transistors connected in a butterfly like fashion. Due to threshold voltage mismatch caused by process variations, one transistor will be stronger than the 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 lateral switching PUF, this tampering is not irrefutable.

IV. Experimental Results

A. Memristive Memory-based PUF Cell

The variable mobility model is included as a Verilog-A model for circuit simulations using Tanner EDA T-Spice. For the device considered, R_{on} is 121kΩ, R_{off} is 121MΩ, D is nominally 50nm, μ_0 is 3×10^{-18} m^2/V·s, and E_0 ~ 25MV/m. Note that for an operating voltage less than ±1.2V (threshold voltage for D = 50nm and E_0 ~ 25MV/m), the memristor follows the linear drift model; and the device memristance does not alter much with respect to time (almost constant). So in the read mode, when the circuit is being used with an operating voltage ~1V, the memristance is essentially constant. During the write mode, where the memristance is SET or RESET, programming voltages greater than 1.2V must be used.

One way to determine the nominal $t_{wr,min}$ is by running Monte Carlo simulations and producing a histogram of the minimum SET time to SET the TiO_x memristor modeled earlier. Figures 6(a-c) show plots of the distribution of the SET time for 2, 5, and 10% variation in thickness, respectively. The write voltage for the results in Figure 3 is 1.5 V. From each of these plots, it is clear that the expected minimum SET time for the circuit in Figure 3 is around 7μs. Figures 6(a-c) also show that the standard deviation for the SET time increases with increasing variation in thickness, as is expected. The Monte Carlo simulations were run for 1000 iterations for each



(a) (b) (c)

(d) (e) (f)

Figure 6. Monte Carlo simulation results showing the distribution of the write time required to write a logic 1 (a-c) and the output voltage (d-f) given 2% (a, d), 5% (b, e) and 10% (c, f) variation in the thickness of the TiO_X memristor. Given such variability in device thickness, the chances that the output of a read operation yields a logic ‘1’ or logic ‘0’ can be made to be close to 50% by choosing a write time at the center of the write time distribution, in this case 7μs.

variation parameter considered.

Figures 6(d-f) show the distributions of the output of a read operation to the memory cell after a 7µs write pulse for 2, 5, and 10% variation in thickness. As was done for the write time distributions, Monte Carlo simulations were run for 1000 iterations using T-Spice. It is clear from Figure 6 that the likelihood that the output is logic ‘0’ is close to that of logic ‘1’, though it appears a logic ‘0’ is slightly more likely. It can also be seen that as the variation in thickness increases the likelihood for a logic ‘1’ is improved over that of logic ‘0’.

B. *Lateral Switching PUF Cell*

For the lateral switching configuration, preliminary testing was performed on a limited number of 100x100µm Al/Cu_xO/Cu memristive device pairs. For all tested devices a separate forming step was required (Figure 1). Switching results suggest a random distribution of the location for the LRS memristor [19].

Furthermore, already provisioned device pairs were tested over several SET/RESET cycles, resulting in no change in the HRS memristor location. This strongly suggests that the memristor that transitions from the LRS to the HRS during the first RESET is stable once established in this configuration. This stability may be further exploited to allow for hiding of the HRS memristor location and the corresponding bit value (setting both memristors to the LRS) and recovery at a later time (a RESET operation).

V. Discussion and Future Work

A. *Noise Immunity and Analog vs. Binary Behavior*

Two basic types of memristors are considered for exploitation as PUF sources: analog and binary switching devices. Here, the switching mechanism refers to the available resistance states for a particular memristor. For an analog memristor, any memristance within a continuous range of possible values can be selected by controlling the magnitude and duration of the applied voltage. Binary memristors are similar in that the memristance is determined based on the magnitude and duration of an applied voltage. However, binary memristors exhibit only two possible memristance states: LRS and HRS. Multiple discrete memristance states have also been demonstrated for some memristors.

Whether the memristor is analog or binary (or even multi-level) has important implications for the performance of the device as a PUF source. Specifically, an analog memristor can be written to a memristance value at or near a resistance corresponding to the threshold voltage of the output buffer. Operating the buffer (e.g. inverter or sense amplifier) near the threshold voltage simply means the circuit is very sensitive to noise. Binary memristors, on the other hand, lead to larger noise margins since the memristance is forced to either LRS or HRS, presumably both being far from the threshold.

Large noise margins are desirable for a PUF since noise sensitivity could potentially lead to erroneous and inconsistent responses. Noise might also be a possible channel for attack in a circuit with small noise margins. Thus, based on desirability for large noise margins, binary or at least multi-level memristors may be preferred over analog memristors for the circuits considered in this paper.

B. *Preconditioning Attack*

In theory, it is possible for an attacker to influence the randomness of the proposed PUF circuits. By introducing voltage potentials to specific devices, the attacker can effectively reduce the write time in the memristive memory-based PUF for example. A similar attack can be used for the lateral switching PUF as well. In essence, the PUF output is no longer unclonable.

This attack might not be possible in practice though. First, the required formation step eliminates the preconditioning problem prior to device provisioning (i.e. at the device manufacturer). Second, [27] showed that when multiple successive RESETs are applied to memristors, the effects quickly wane and settle around a consistent HRS. This means that by changing the lateral switching PUF protocol from SET-RESET into RESETx4-SET-RESET, the initial four RESET stages can return all memristors to a nominal state where any extraneous inputs or attempts to precondition the memristor are effectively negated. Finally, the preconditioning attack can also be effectively nullified by applying the protocol once to reset the memristors to their nominal values and then applying the protocol a second time to retrieve the PUF bit. These procedures needs to be verified through experimentation and are left as future work.

VI. Conclusions

As shown in this paper, memristive devices are good candidates for PUFs due to the heightened effects of process variations on system characteristics. Two specific circuits are discussed which leverage different properties of memristors. First, a memristive memory cell based PUF is presented which leverages variability in the SET time of the memristor. While variability in SET time can be harnessed as a PUF source, the noise margins of the system are driven by whether or not the memristor is analog or discrete. For analog memristors, the noise margins will tend to be small and thus may be susceptible to certain types of attacks. However, discrete memristors provide sufficient separation between memristance states for larger noise margins.

The second memristive PUF considered depends on the ability to read and write two devices laterally, or as a single unit. Preliminary experimental results using Al/Cu_xO/Cu devices demonstrate lateral switching wherein, one of two devices becomes fixed in an LRS. Furthermore, preliminary results suggest that which particular device eventually ends up in LRS is random.

More experimental work needs to be done to better understand the switching mechanisms that drive memristors of various flavors, e.g. binary or analog. More experimental data should also be collected for the particular structures considered in this paper. For example, more measurements of many more lateral switching memristor pairs must be made to better demonstrate the random nature of the lateral switching mechanism. Furthermore, improved device models developed from sound experimentation can be leveraged to better understand the physical parameters of different types of memristors that can be leveraged for PUF operation.

VII. Acknowledgements

The material and results presented in this paper have been cleared for public release, unlimited distribution by AFRL, case number 88ABW-2012-6564. 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] "Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain," Report 112-167, Committee on Armed Services, 112th Congress, 2nd Session, United States Senate, U.S. Government Printing Office, Washington, D.C, 21 May 2012.

[2] 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," *Proc. of IEEE/ACM Intl. Conf. on Computer Architecture*, pp. 25–36, May 2005.

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

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

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

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

[7] 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. Appl. Phys.*, Vol. 107, No. 2, pp. 024512 - 024512-7 (2010)

[8] 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)

[9] A. Sawa, T. Fujii, M. Kawasaki, and Y. Tokura, "Interfaces resistance switching at a few nanometer thick perovskite manganite layers," *Appl. Phys. Lett.*, Vol. 88, No. 23 pp. 232112 - 232112-3 (2006)

[10] K. Szot, W. Speier, G. Bihlmayer, and R. Waser, "Switching the electrical resistance of individual dislocations in single crystalline SrTiO3," *Nat. Mat.*, Vol. 5, pp. 312–320 (2006)

[11] J. C. Scott and L. D. Bozano, "Nonvolatile memory elements based on organic materials," *Adv. Mat.*, Vol. 19, pp. 1452–1463 (2007)

[12] N. B. Zhitenev, A. Sidorenko, D. M. Tennant, and R. A. Cirelli, "Chemical modification of the electronic conducting states in polymer nanodevices," *Nat. Nanotech.*, Vol. 2, pp. 237–242.

[13] M. Di Ventra, Y. V. Pershin, L. O. Chua, "Circuit Elements With Memory: Memristors, Memcapacitors, and Meminductors," *Proc. IEEE*, Vol. 97, pp. 1717- 1724 (2009).

[14] 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)

[15] J. P. Strachan, D. B. Strukov, J. Borghetti, J. J. Yang, G. Medeiros-Ribeiro, and R. S. Williams, "The switching location of a bipolar memristor: chemical, thermal and structural mapping," *Nanotechnology*, Vol. 22, No. 25, 254015 (2011)

[16] G. S. Rose, H. Manem, J. Rajendran, R. Karri, and R. Pino, "Leveraging Memristive Systems in the Constructure of Digital Logic Circuits and Architectures," *Proceedings of the IEEE*, Vol. 100, No. 6, June 2012.

[17] Y. Joglekar and S. Wolf, "The elusive memristor: properties of basic electrical circuits," *Eur. J. Phy.*, Vol. 30, pp. 661–675.

[18] 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)

[19] N.R. McDonald, "Al/Cu_xO/Cu Memristive Devices: Fabrication, Characterization, and Modeling," M.S., College of Nanoscale Science and Engineering, University at Albany, SUNY, Albany, NY, 2012, 1517153

[20] 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).

[21] Q. F. Xia, W. Robinett, M. W. Cumbie, N. Banerjee, T. J. Cardinali, J. J. Yang, W. Wu, X. M. Li, W. M. Tong, D. B. Strukov, G. S. Snider, G. Medeiros-Ribeiro, and R. S. Williams, "Memristor− CMOS Hybrid Integrated Circuits for Reconfigurable Logic," *Nano Lett.*, Vol. 9, 3640 (2009)

[22] H. Manem, J. Rajendran, and G. S. Rose, "Design Considerations for Multi-Level CMOS/Nano Memristive Memory," *ACM Journal of Emerging Technologies in Computing Systems*, Vol. 8, No. 1, Feb. 2012.

[23] G. S. Rose, Y. Yao, J. M. Tour, A. C. Cabe, N. Gergel-Hackett, N. Majumdar, J. C. Bean, L. R. Harriott, and M. R. Stan, "Designing CMOS/Molecular Memories while Considering Device Parameter Variations," *ACM Journal of Emerging Technologies in Computing Systems*, Vol. 3, No. 1, April 2007.

[24] H. Manem and G. S. Rose, "A Read-Monitored Write Circuit for 1T1M Memristor Memories," *Proceedings of IEEE International Symposium on Circuits and Systems*, Rio de Janeiro, Brazil, May 2011.

[25] 3. J. Rajendran, R. Karri, J.B. Wendt, M. Potkonjak, N. McDonald, G.S. Rose, and B. Wysocki, "Nanoelectronic Solutions for Hardware Security," *in review*, http://eprint.iacr.org/2012/575

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

[27] Q. Liu, J. Sun, H. B. Lv, S. B. Long, K. B. Yin, N. Wan, Y. T. Li, L. T. Sun, and M. Liu, "Real-Time Observation on Dynamic Growth/Dissolution of Conductive Filaments in Oxide-Electrolyte-Based ReRAM," *Adv. Mater*, Vol. 24, pp. 1844–1849 (2012)