A Write-Time Based Memristive PUF for Hardware Security Applications

Garrett S. Rose, Nathan McDonald, Lok-Kwong Yan, and Bryant Wysocki
Air Force Research Laboratory, Information Directorate
Rome, New York 13441 USA
{Garrett.Rose, Nathan.McDonald, Lok.Yan, Bryant.Wysocki}@rl.af.mil

***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 describe a novel memristive PUF (M-PUF) architecture that utilizes variations in the write-time of a memristor as an entropy source. The results presented show strong statistical performance for the M-PUF in terms of uniqueness, uniformity, and bit-aliasing. Additionally, nanoscale M-PUFs are shown to exhibit reduced area utilization as compared to CMOS counterparts.**

Keywords—VLSI; digital integrated circuits; hardware security; nanoelectronics; memristors

I. Introduction

Electronic counterfeiting and recirculation is a growing problem. Analysts estimate that nearly 10% of global technology products are likely counterfeits resulting in over $7.5 billion in yearly losses to the U.S. semiconductor industry. With respect to the U.S. Department of Defense, there are approximately over one million suspect parts within its supply chain alone [1]. This problem is systemic of the lack of a secure, unique identifier to verify the authenticity and trust of electronic products. Researchers have proposed Physical Unclonable Functions (PUFs) as a solution.

PUFs [2–8] 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 research has focused on designing PUFs that take advantage of measurable/quantifiable characteristics in CMOS devices (e.g. varied 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, e.g. metal-oxide memristors, phase change devices, spin-torque transfer devices, and devices built with 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 describe a write-time based memristive PUF (M-PUF) [9]. Results are presented which show excellent statistical performance for the M-PUF as compared to CMOS counterparts. Further, a clear advantage of any nanoelectronic PUF, including the M-PUF, is a reduction in area utilization as compared to CMOS.

We first present some background on PUFs and memristors in Section II. We then describe the new write-time based M-PUF in Section III and evaluate its effectiveness using Monte Carlo simulations in Section IV. Some analysis and discussion is provided in Section V on the area utilization of the M-PUF as compared to CMOS counterparts. Finally, concluding remarks are provided in Section VI.

II. Background

A. Physical Unclonable Functions

Physical Unclonable Functions have emerged as solutions to a variety of potential threats and attacks including integrated circuit (IC) piracy, counterfeiting, malicious Trojan insertion, and side-channel analysis [3, 4]. A PUF is a unique hardware identifier where intrinsic process variations are used to create a "fingerprint" for a particular device. For example, it can be shown that the frequency of a CMOS ring oscillator is sensitive to variations in transistor device parameters such that the same ring oscillator PUF (RO PUF) implemented on two different ICs will generate unique signatures for each IC due to differences in the resonant frequencies [7].

Another example is a delay-based arbiter PUF (APUF) [2,8] where the signature is a function of the propagation delay through a circuit. In an APUF, two-input/two-output switches are chained together to create a circuit with two separate paths for a signal to propagate through. Process variations dictate that a single input signal will propagate through one path faster than the other. An arbiter (e.g., comparator) is then used to translate the difference in path delays into unique signature bits. The switches can be further configured into two different modes: straight-through and cross-over. Given the same physical APUF, changing the modes results in different overall

The material and results presented in this paper have been cleared for public release, unlimited distribution by AFRL, case number 88ABW-2013-2932. 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.

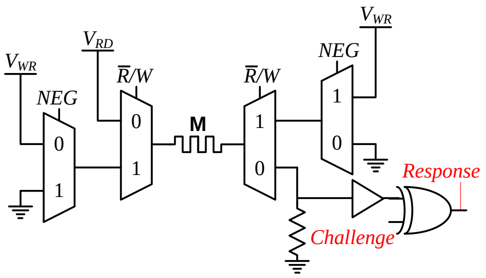

Fig. 1. A 1-bit memristive memory-based PUF cell that leverages variations in memristor write times [9].

path configurations through the switches, which in turn leads to a different output signature bits.

In this design, the physical uniqueness of a PUF can be used to generate a number of challenge-response-pairs (CRPs). By recording a number of known CRPs during device provisioning, an IC can be authenticated in the field by ensuring that it returns the same response given a known challenge. A PUF can also be used to generate encryption keys based on CRPs providing an advantage in that the key does not need to be stored in memory. In this case, the key is always a function of the hardware itself.

There are two fundamental requirements for building a PUF: random and uncontrollable variation. The variations must be random, thereby drastically reducing the probability that a unique signature will be repeated. Also, the variations must be uncontrollable, else an adversary could clone (i.e. mount an impersonation attack against) devices. In both cases, the signatures would no longer be unique. In the RO PUF mentioned above, the ring-oscillator frequency is dependent on parameters such as transistor sizing, which is known to be variable in the CMOS manufacturing process [7]. In the literature, the quality of a PUF is measured using a number of different metrics: uniqueness, uniformity, reliability, steadiness, diffuseness, and bit-aliasing [5]. In this paper, we use uniqueness, uniformity, and bit-aliasing to measure the statistical quality of the M-PUF and compare the results to those for CMOS based RO PUF and APUF architectures.

B. Memristor Behavior for Hardware Security

Memristors, memristive devices, or resistive RAM (ReRAM) are effectively two terminal electrical potentiometers with nonvolatile resistive states. That is to say, memristive devices have tunable resistance values that persist when power is removed. By applying the appropriate electrical bias for the particular 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 design. Typically, these devices are as simple as metal-insulator-metal (MIM) structures, where the insulating materials have included such diverse materials as chalcogenides [10, 11], metal oxides [12, 13], perovskites [14, 15], and organic films [16, 17]. Though the gambit of devices demonstrating the switching behavior thus described may be understood to be "memristors" [16], the exact switching mechanism, parameters, and style will depend upon the specific material stack.

The range of realizable device properties allows for device engineering to optimally satisfy different application specific requirements. 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 the simplest analog model, memristors are modeled as two resistors, R_{on} as the LRS value and R_{off} as the HRS value, where the contribution of each to the total device resistance is modulated by a factor α that varies between 0 and 1 over time. In short, the memristance may be written as

$$M(t) = \alpha(t)R_{on} + (1 - \alpha(t))R_{off}. \qquad (1)$$

The rate of change of α is a function of the physical properties of the device. In the case of a mobile ion switching mechanism [17], the device thickness D and the ion mobility μ have the strongest influence on the rate of switching. [19] expanded on the model in [17, 20] to account for nonlinear behavior.

The impact of variations in D is of particular importance to the M-PUF considered in this work. 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 [21]. 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.

III. Memristive PUF Circuits

A. Write-Time based Memristive PUF Cell

The effects of variations in the thickness D of a memristor upon the write time (and by extension the read time) of the device may be leveraged in the construction of a simple write-time based M-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 memristor memory cell is likely a logic '1'. Likewise, $t_{wr,actual}$ less than $t_{wr,min}$ will likely lead to an output voltage of logic '0'. 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 Fig. 1 is an implementation of a single bit of an M-PUF. This circuit is based on a one bit equivalent of the memristive memory presented in prior work [22–24]. Two control signals are used to determine first whether the circuit is reading or writing the memristor $(\overline{R}/W)$, then, if writing, what is the polarity of the write signal (NEG). The circuit works as a PUF by first performing a RESET of the memristor by 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 to $t_{wr,min}$ (NEG = 0 and $\overline{R}/W = 1$). After the SET operation, the memristor can be read at the output by applying $\overline{R}/W = 0$. An example timing diagram for the M-PUF is shown in Fig. 2.

The *Challenge* for the M-PUF and the random output of the memristive memory cell are then applied to an XOR gate. The output of this XOR is the *Response* bit of the PUF 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 coin flip. Given the nature of the *Response*, the *Challenge* and *Response* constitute a Challenge-Response Pair (CRP) that uniquely identifies the integrated circuit on which the M-PUF resides.

B. *N-bit Memristive PUF*

There are several ways in which the write-time M-PUF cell can be used to construct a PUF with a multi-bit *Challenge* and a multi-bit *Response*. One straightforward embodiment of an *N*-bit M-PUF is illustrated in Fig. 3, consisting of *N* memristive devices, *N Challenge* bits, and *N Response* bits. Each column in the PUF consists of one M-PUF cell like that illustrated in Fig. 1. Of note in Fig. 3 is that much of the selection circuitry can be shared amongst all PUF cells. However, the output side $\overline{R}/W$ selection circuit must still be implemented for each memristive PUF cell. In Fig. 3, the output side $\overline{R}/W$ selection circuits are implemented with two pass transistors per M-PUF cell and one shared inverter, showing a reasonable transistor level implementation of the multiplexers used for the selection circuitry.

IV. Experimental Results

A. *Statistical Behavior of Memristive PUF Cells*

The variable mobility model [19] 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, and μ_0 is 5×10^{-18} m^2/V·s. For an operating voltage less than ±1.2V (threshold voltage for D = 50nm), 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 effectively constant. Consequently, during the write mode, where the memristance is SET or RESET, programming voltages greater than 1.2V must also be used.

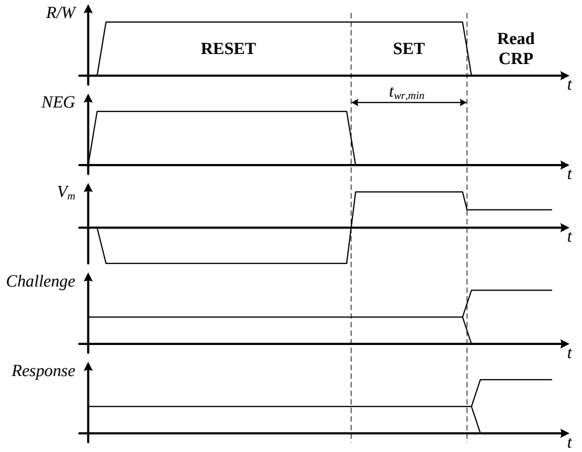

Fig. 2. Timing diagram of sequence to setup write-time M-PUF and issue a challenge.

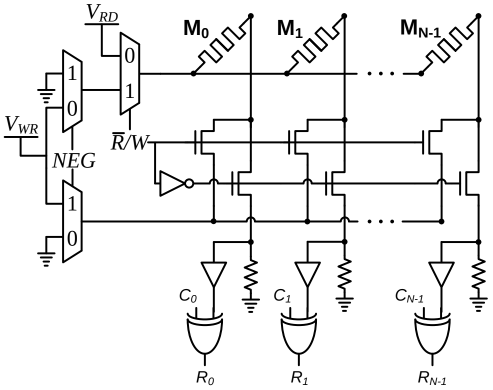

Fig. 3. An *N*-bit write-time based M-PUF with *N* memristors, *N* response bits, and *N* challenge bits.

To determine the nominal $t_{wr,min}$ using the nonlinear memristor model, Monte Carlo simulations for 1000 iterations were run to produce a histogram of the minimum SET time for a TiO_x memristor described in [15]. Using a 1.5V write voltage on simulated devices whose thickness varied by 10%, it was determined that the expected minimum SET time for the circuit in Fig. 1 is around 7.1µs [9].

B. *Performance Characteristics of N-bit M-PUF*

We use three parameters to demonstrate the statistical performance of the N-bit M-PUF shown in Fig. 3: uniqueness, uniformity, and bit-aliasing [5, 6]. An important fourth parameter that would typically be shown is reliability but more experimental data is required to better understand the environmental sensitivity of memristors. Maiti *et al.* presents a detailed description of these PUF parameters in [5]. The ideal value for the parameter uniqueness is 100% while that of uniformity and bit-aliasing are both 50% for strong PUF performance.

The M-PUF was also compared against hardware experimental data from two common CMOS based PUFs: the arbiter PUF (APUF) [2, 5, 8] and the ring oscillator PUF (RO PUF) [5, 7] (Table I). The APUF considered is based on 45 chips and 1024 samples, each consisting of 128 response bits. Data for the RO PUF is based on 193 chips and 100 samples per chip, each consisting of 511 response bits. It is also useful to point out that the APUF and RO PUF implementations were prototyped on FPGAs [5] to generate the results shown in Table I. The M-PUF data is based on Monte Carlo simulations for an 8-bit write-time based M-PUF simulated for 100 unique challenges/samples and 100 chips. The write-time used in the simulation of the M-PUF was 7.1 µs.

As can be seen in Table I, the M-PUF uniqueness is very close to the ideal of 100% while uniformity and bit-aliasing are both near the ideal of 50%. This is very similar to results for the RO PUF except that uniqueness is only slightly better for the M-PUF. As presented in [5], the APUF demonstrated a fair result for uniformity but is poor in terms of uniqueness and bit-

TABLE I
COMPARISON OF APUF, RO PUF AND M-PUF USING PARAMETERS DEFINED BY MAITI ET AL. [25] AND HORI ET AL. [5]

	APUF*	RO PUF*	M-PUF†	Ideal
Uniqueness	36.75%	94.07%	99.70%	100%
Uniformity	55.69%	50.56%	49.99%	50%
Bit-Aliasing	19.57%	50.56%	49.99%	50%

* Results as presented by Maiti et al. in [25].
† Results obtained for write-time of 7.1 μs.

aliasing for that particular study. These results demonstrate that the M-PUF is expected to exhibit strong PUF performance.

It is important to note that the CMOS PUF results were obtained from implemented devices described in the literature [5] while the M-PUF was merely simulated. Moreover, the model used to simulate the M-PUF assumes that memristor variability is random and independent of the relative location of the memristor on a particular die. It is known that statistical performance is improved when random variability dominates any systematic (i.e. location dependent) variability [25]. While random variability in memristors is assumed and is desirable for PUF performance, further study is required to better understand sources of variability in memristors.

V. CONCLUSION

As shown in this paper, memristive devices are good candidates for PUFs due to the heightened effects of process variations on system characteristics. A write-time based memristive PUF is presented which leverages variability in the SET time of the memristor. More experimental work needs to be done to better understand which memristor switching mechanisms are best suited for this application. Furthermore, more experimental data should also be collected for the particular structures considered in this paper. 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. With an improved understanding of memristor characteristics such as any dependence on temperature, the M-PUF described in this paper can be characterized in terms of reliability. That said, the M-PUF circuit design presented here shows promise as a PUF in terms of uniqueness, uniformity and bit-aliasing.

REFERENCES

[1] "Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain," Committee on Armed Services, 112th Congress, 2nd Session, United States Senate, U.S. Government Printing Office, Washington, D.C., Report 112-167, May 21, 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," in *Proc. of IEEE/ACM Intl. Symp. on Computer Architecture*, Madison, WI, May 2005, pp. 25–36.

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

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

[5] A. Maiti, V. Gunreddy, and P. Schaumont, "A Systematic Model to Evaluate and Compare the Performance of Physical Unclonable Functions," in *Embedded Systems Design with FPGAs*, pp. 245-267, P. Athanas, D. Pnevmatikatos, and N. Sklavos, Eds., Springer, 2013.

[6] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs," in *Proc. Intl. Conf. Reconfigurable Computing and FPGAs*, Dec. 2010, pp. 298-303.

[7] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security*, Springer, 2010.

[8] D. Lim, J.W. Lee, B. Gassend, G.E.Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, no. 10, Oct. 2005.

[9] G. S. Rose, N. McDonald, L.-K. Yan, B. Wysocki, and K. Xu, "Foundations of Memristor Based PUF Architectures," in *Proceedings of the IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH)*, July 2013.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

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

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] G. S. Rose, H. Manem, J. Rajendran, R. Karri, and R. Pino, "Leveraging Memristive Systems in the Constructure of Digital Logic Circuits and Architectures," *Proc. IEEE*, vol. 100, no. 6, pp. 2033–2049, June 2012.

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

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

[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," *in Proc. IEEE Intl. Symp. Circuits and Systems*, Rio de Janeiro, Brazil, May 2011.

[25] A. Maiti and P. Schaumont, "Improved Ring Oscillator PUF: An FPGA-friendly Secure Primitive," *Journal of Cryptology, vol. 24, no. 2, pp. 375*–397, 2011.