Performance Analysis of a Memristive Crossbar PUF Design

Garrett S. Rose and Chauncey A. Meade

Design Automation Conference (DAC), San Francisco, California, May 2015.

DOI: https://doi.org/10.1145/2744769.2744892

Citation Information (BibTex):

```
@INPROCEEDINGS{Rose:DAC2015,
  author="Garrett S. Rose and Chauncey A. Meade",
  title="Performance Analysis of a Memristive Crossbar PUF Design",
  booktitle="Proceedings of the Annual Design Automation Conference
      {(DAC)}",
  month="June",
  year="2015",
  pages="75:1-75:6",
  location="San Francisco, California"
}
```

Performance Analysis of a Memristive Crossbar PUF Design

Garrett S. Rose
The University of Tennessee
Department of Electrical Engineering and
Computer Science
Knoxville, TN 37996 USA
garose@utk.edu

Chauncey A. Meade
The University of Tennessee
Department of Electrical Engineering and
Computer Science
Knoxville, TN 37996 USA
cmeade3@vols.utk.edu

ABSTRACT

Physical unclonable functions (PUF) provide a hardware specific unique signature or finger print for an integrated circuit that can be leveraged to mitigate several security vulnerabilities. A dense memristive crossbar PUF is described which utilizes variations in the write-time of memristors as the primary entropy source. For this work, the write-time varies according to six specific device parameters which can be directly measured from fabricated memristors and easily included in an accurate model for circuit simulation. The results presented show strong statistical performance for the proposed design in terms of entropy, uniqueness and uniformity. Furthermore, the nature of sneak path currents in the crossbar structure are leveraged to provide an exponential number of unique configurations for each response bit. Results also show that the proposed crossbar-based PUF provides improved power consumption and smaller area utilization when compared to CMOS-based and other nanoelectronic PUF circuits.

Categories and Subject Descriptors

B.7.1 [**Integrated Circuits**]: Types and Design Styles

General Terms

Design, Performance

Keywords

Hardware security, physical unclonable function, nanoelectronics, memristor

1. INTRODUCTION

Electronic counterfeiting and recirculation have become particularly important issues of concern when designing integrated circuits. For example, analysts have estimated that about 10% of global electronic products are counterfeits, resulting in billions of U.S. dollars in yearly losses for the semiconductor industry. These issues necessitate secure devices and techniques to verify the authenticity and trust of electronic products. One popular solution that emerged in recent years is the Physical Unclonable Function (PUF) [6].

PUFs [1, 2, 6–8, 11, 15, 16] are functions that map intrinsic properties of hardware devices (e.g. process variability) into unique digital information. This unique data has been used or proposed for use 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 more PUF sources in nano-scale devices. The ability to fabricate robust PUF circuits using nano-scale components also has the advantage of providing improved security with minimal area utilization and reduced power consumption.

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 demonstrated sensitivity to process variation and relative compatibility with CMOS fabrication standards.

In this work, an empirical memristor device model [9, 10] is used in the simulation and analysis of a PUF circuit constructed from a dense crossbar array of memristive devices, the memristive crossbar PUF (XBARPUF). The XBARPUF is similar to prior attempts at the design of a memristor-based PUF in that the write-time of the memristor is used as the primary source of entropy [13]. However, the XBARPUF depends on the relative write-time of pairs of memristors leading to more robust behavior that does not require exact knowledge or control of the minimum write-time of the device. Furthermore, the XBARPUF proposed here is constructed in such a way that the circuit is denser and thus more effecient than prior designs.

We first present some background on the memristor model used and on PUF circuits in Section 2. We then present and describe the memristive crossbar-based PUF design in Section 3 and evaluate its effectiveness using Monte Carlo simulations in Section 4. Some analyses and discussion are provided in Section 5 on the area utilization of the proposed

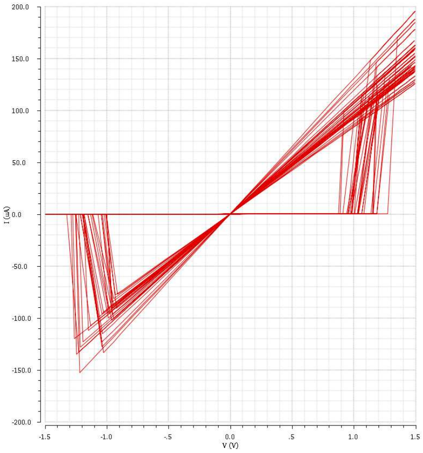

Figure 1: Simulation result showing the I-V response for the memristor model as described by equations 1 and 2. The results demonstrate the impact of 5% variation in all parameters considered.

crossbar-based PUF as compared to related designs. Finally, concluding remarks are provided in Section 6.

2. BACKGROUND

2.1 Memristor Modeling

First envisioned by Leon Chua in 1971 [4], HP Labs recently discovered and demonstrated that a variety of metal-oxide devices can properly be classified as memristive systems [14]. A memristor is a fourth fundamental device that relates charge (q) and flux linkage (ϕ). Memristors are considered "fundamental" just as resistors, capacitors, and inductors are fundamental and cannot be completely modeled using other fundamental constructs. The relation between q and ϕ gives the memristor interesting properties, most notably it's namesake ability of variable resistance with memory. The memristor behaves as a sort of switch; given some set of input conditions (such as exceeding some voltage for a given amount of time), its resistance will change, and then remain at that resistance until some separate set of input conditions are met. The concept of a "memristive system" [5] builds on that of a memristor with the exception that the change of resistance for a memristive system is nonlinear with electric field. This nonlinear behavior leads to thresholds (usually voltages) below which the device resistance is relatively constant. The memristive devices considered are actually nonlinear memristive systems with positive and negative threshold voltages. These devices are generally referred to as "memristors" in this paper for brevity.

The model used for the simulation work in this paper was developed and presented by McDonald et al. in [9,10]. While the original model could be used for unipolar, nonpolar and bipolar behavior, this work is restricted to bipolar behavior. Specifically, for applied voltages greater than some positive threshold (V_p) the memristor will switch away from the high resistance state (HRS) and toward the low resistance state (LRS). Likewise, a negative voltage below a negative threshold (V_n) will cause the resistance of the memristor to increase toward the HRS. This behavior is shown in Fig. 1 where the positive and negative thresholds are 1.1 V and -1.1 V, respectively. The device parameters for the simulations that produced Fig. 1 were allowed to vary by ±5%.

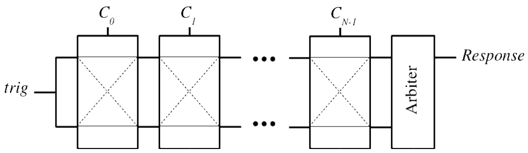

Figure 2: Schematic of an arbiter PUF with N challenge bits.

The McDonald model works by incrementing or decrementing the memristance at each time step of the simulation depending on bias conditions. If the memristor is already at either the HRS or LRS the model will not switch and will remain at that bounding resistance level. During a SET (from HRS to LRS) operation the memristance is updated by:

$$M(t_{i+1}) = M(t_i) - \frac{\Delta r \Delta t V(t_{i+1})}{t_p V_p} \tag{1}$$

while for the RESET (LRS to HRS) operation the memristance is updated by:

$$M(t_{i+1}) = M(t_i) + \frac{\Delta r \Delta t V(t_{i+1})}{t_n V_n} \tag{2}$$

where M is the memristance, Δr is the absolute difference between LRS and HRS resistance, Δt is the time step-size, $V(t)$ is the applied voltage bias, t_p (t_n) is the time to effect a resistance change under positive (negative) bias, and V_p (V_n) is the threshold voltage under positive (negative) polarity. The simulated current-voltage response shown in Fig. 1 is representive of this model.

Of particular importance to the memristive PUF circuits considered in this work is the impact of variations on device behavior. More specifically, process variability translates to variations in the read and write times of a memristor when using the device as a memory cell [12]. 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 process variations 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.

2.2 Physical Unclonable Functions

Physical Unclonable Functions have emerged as solutions to a variety of security concerns, including integrated circuit (IC) piracy, counterfeiting, and secret key storage [6]. 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) design implemented on two different ICs will generate unique signatures for each IC due to differences in their frequencies of oscillation [7].

Another example is a delay-based arbiter PUF (APUF) [2, 15] where the signature is a function of the propagation delay through a circuit. Fig. 2 illustrates the basic structure

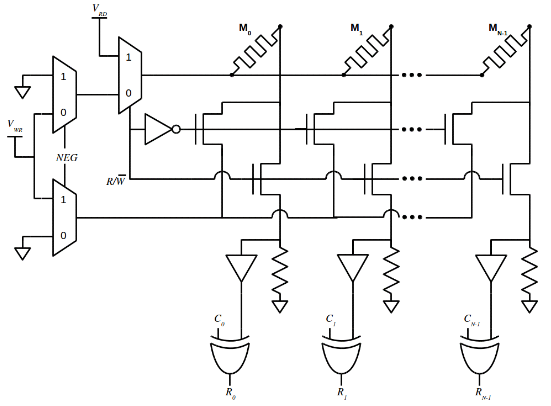

Figure 3: Schematic of write-time memristive PUF circuit [13].

of an APUF. 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., flip flop) is then used to translate the difference in path delays into unique signature information.

The switches in an APUF can be configured into two different modes: straight-through and cross-over. Given the same physical APUF, changing the modes results in different overall path configurations through the switches, which in turn leads to different output signature bits. The straight-through and cross-over modes are selected for each switch with one bit in an N-bit challenge where the total APUF consists of N total switches. Each N-bit challenge will produce a single unique response bit.

The inherent uniqueness of a PUF can be used to generate a number of challenge-response-pairs (CRPs). By recording a number of known CRPs during an enrollment phase, 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 [11]. In this paper, we consider uniqueness, uniformity, and power consumption to assess the quality of the memristive crossbar-based PUF circuit.

2.3 The Write-Time Memristive PUF

The circuit shown in Fig. 3 is an implementation of the write-time memristive PUF (WTMPUF) proposed in [13]. Two control signals are used to determine whether the circuit is reading or writing ($R/\overline{W}$) the memristor and, if writing, 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 $R/\overline{W} = 0$ long enough to guarantee the memristor is in the HRS state. Next, a SET pulse is applied for the nominal write time corresponding to the minimum SET time ($NEG = 0$ and $R/\overline{W} = 0$). After the SET operation, the memristor can be read at the output by applying $R/\overline{W} = 1$.

The $Challenge$ for the WTMPUF and the random output of the memristive memory cell are 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 [13]. 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 WTMPUF resides. The performance for the WTMPUF as described in prior work shows that the circuit achieves strong results for uniqueness, bit-aliasing and uniformity [13]. However, the minimum write-time must be precisely known such that the SET voltage is applied for exactly that amount of time in order to achieve strong statistical behavior. This sensitivity to the write-time for the WTMPUF motivates the proposed XBARPUF which depends on the relative write-time of pairs of memristors.

3. THE CROSSBAR MEMRISTIVE PUF

3.1 Motivation

Using memristors as opposed to CMOS circuits is largely motivated by area and power constraints. Memristor-based designs are expected to take up less physical area and use fewer transistors than their CMOS counterparts. In order to maximize this property, we have chosen a 2D crossbar array design as it makes very efficient use of the available space. Improved area efficiency results from the fact that the crossbar array consists of memristive devices at the crosspoints of perpendicular nanowires.

There are two important points when considering the area of memristive circuits. First, the area of a single memristor is potentially as small as the width-squared of the narrowest nanowire that could be implemented in the given process. This is significantly smaller than the area of a transistor which consists not only of the gate length but also the source and drain diffusion regions. Second, memristors are fabricated between metal interconnect wires and thus exist in the back-end-of-line metal layers. This means that a memristive design is inherently 3D in that the memristive devices are physically above the silicon transitors. For the area estimates in this paper we assume the memristors are essentially free as they do not direcly take up space in the lateral dimensions of the underlying silicon. Area is thus estimated simply in terms of transistor count.

3.2 Design Details

The proposed crossbar memristive PUF (shown in Fig. 4) is based on the write-time memristive PUF described in [13]. As with the WTMPUF, the XBARPUF's primary entropy source is the minimum time it takes for memristors to SET

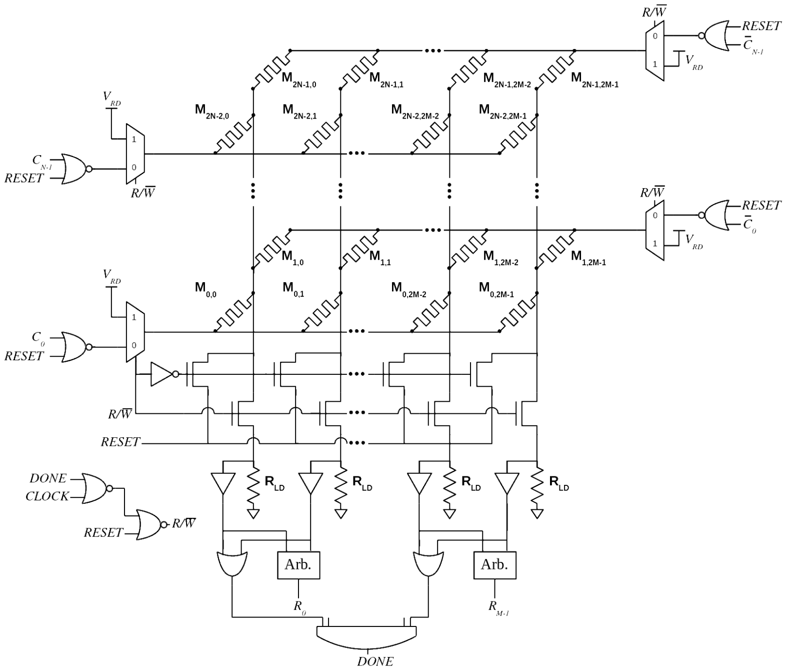

Figure 4: Schematic of the proposed crossbar-memristive PUF design for N configuration and M response bits. The design as proposed requires a memristive crossbar of size $2N \times 2M$ including $4NM$ total memristors.

during a write operation. Additionally, the XBARPUF is somewhat a reimagining of the APUF where memristors are essentially used in place of switch boxes. Specifically, for each challenge bit, there are two corresponding rows of memristors: one written based on the challenge bit and another by the inverted challenge bit. If the challenge bit is high, then memristors driven by the true challenge bit are incrementally SET while those driven by the inverted challenge bit remain in the HRS. Likewise, a low or '0' challenge bit causes the memristors driven by the inverted challenge bit to SET while the others remain in the HRS. This ensures one row will be actively written to while the other remains inactive (remains at HRS) during the write operation. To generate each response bit, two columns are compared during a write. The current from both colums, dependent on all memristors connected to the columns, are pulled down over identical loads. Once the output of one column reaches a certain threshold the arbiter selects a "winner" which determines the corresponding response bit.

The $R/\overline{W}$ signal in the XBARPUF circuit is determined based on whether or not a $RESET = 1$ condition exists and whether or not all arbiters in the circuit have latched their respective response bits, as indicated by $DONE = 1$. If the memristors are not being RESET and $DONE = 0$ then a clock pulse is used to incrementally "nudge" the selected memristors toward a SET condition until all response bits have been determined. Using a clock signal in this way enables a "read-monitored-write" of the memristors whereby the memristors are altered slightly and then examined before altering the resistance again in the next cycle. The need for the "read-monitored-write" is based on the use of a load resistance to determine the state of each column output. If not performing a read-monitored-write, the presense of the load resistance necessitates a large write-voltage V_{WR} in order to read the memristor state during the write operation. While a vulnerability may exist (assuming the clock is externally controlled) for the read-monitored-write technique described the given structure is adequate to provide a proof of concept for the XBARPUF. An alternative approach is to make use of sense amplifiers in such a way that V_{WR} doesn't need to be too high and the output can be monitored *during* a write operation.

It has been noted in prior work that an APUF depends on 2^N possible delay paths given N challenge bits. Likewise, the XBARPUF depends on 2^N possible memristor configurations per each column pair for N challenge bits. By making each response bit a function of multiple memristors across a column, as opposed to the single memristor/response bit in the WTMPUF, the XBARPUF depends on a signficantly more complex source of entropy. As mentioned above, this is an attempt to build from the idea of the APUF. Further, the proposed design directly incorporates the challenges into the source of entropy, as opposed to the WTMPUF which uses externally applied challenges.

3.3 Reliability

A major concern of the WTMPUF is reliability over changing operating conditions. The design of the WTMPUF requires the precise knowledge of the nominal set time for the memristors. However, this can be shown to change with operating conditions. Our design attempts to combat these issues by comparing columns of multiple memristors, as described above. Since the compared columns are physically close, operating conditions should be the same for both even as they change. As the memristors of one column trend in a particular direction, either writing faster or slower, those in its companion column should follow that trend. Since the final result is a comparison, the response bit should remain unchanged. However, a good model for memristor changes over various operating conditions (e.g. temperature) does not yet exist and requires more experimental work before one can be realized. We leave the development and testing of such a model to future work.

4. XBARPUF PERFORMANCE RESULTS

To assess the performance potential of the XBARPUF, 250 Monte Carlo simulation runs are performed using Cadence Spectre over several sets of design parameters. For the purposes of this demonstration, an XBARPUF circuit with 4 challenge bits and 2 response bits was modeled and simulated. For all simulations included here, 45 nm CMOS technology is used for the transistors with models from the predictive technology model (PTM) library from Arizona State University [3, 17]. Design parameters considered for the hybrid CMOS-memristive XBARPUF circuit come in two flavors: (1) circuit design parameters such as write and read voltages that can be controlled post-fabrication and (2) device design parameters such as threshold voltages which must be defined when fabricating the devices themselves.

The design parameters are actually related. Specifically, the read and write voltages are determined based on the given threshold voltage of the device. As can be seen in Table 1, it is desirable that the write voltage be as low as possible in order to reduce the power consumption. Not clear from the results is that there is also a minimum for the threshold voltages of the memristors, defined by the threshold voltages of the transistors used to control them. Table 1 shows results for threshold voltages of 1.1/-1.1, 1.0/-1.0 and 0.9/-0.9. Each set of threshold voltages comes with corresponding read and write voltages. The results show that entropy and uniqueness are fairly high and are consistent regardless of the voltage levels used.

Table 1 also shows the impact of the level of variability that exists for the device parameters themselves. Six specific device parameters are allowed to vary in order to generate variability in the write-time which is used in turn as the entropy source of the PUF. These parameters are the HRS and LRS resistance levels, the switching rates and the threshold voltages. For these simulations, all parameters considered were varied by the same percentage. The results show fairly consistent entropy and uniqueness as variations become less pronounced. Specifically, there is little change in performance when the variability is reduced from 10% to 2%. However, there is a small drop in entropy and uniqueness when variability is reduced to 0.5%, regardless of the read and write voltage levels applied. This is somewhat expected but further work is needed to assess the impact of each individual device parameter.

5. ANALYSES AND DISCUSSION

The performance of the XBARPUF is similar to that of the WTMPUF, while removing the dependency on a precise write-time. Additionally, the XBARPUF has comparable performance to that of the APUF, while decreasing the transistor count (Fig. 5). For the transistor count of the APUF, we make the assumption that we want all response bits simultaneously, as opposed to computing them over multiple cycles, due to the difference in nature of the different PUF designs. A comparison of the three PUF designs (CMOS APUF, WTMPUF, XBARPUF) in terms of transistor count can be seen in Fig. 5. Due to the constraint of single-cycle response generation, the APUF transistor count is quadratic with the number of challenge-response bits while that of the two memristive PUF designs is linear. This is an expected result as the entropy source for the memristive PUFs is the memristor itself which isn't being counted toward the area even though the XBARPUF does include a quadratic number of memristors as a function of number of challenge-response bits.

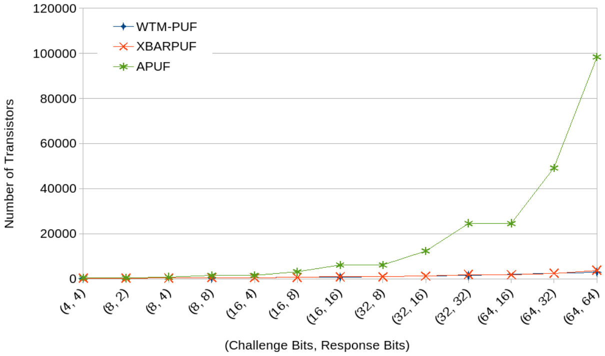

Figure 5: Plot of area (transistor count) vs. number of challenge and response bits for three different PUF designs. CMOS APUF area increases quadratically in area while the memristive PUF designs only require a linear increase in the number of transistors.

The reliability of the XBARPUF needs to be tested across a wider range of operating parameters. To do so, current memristor models need to be expanded and improved upon. As more experimental data is obtained from real memristors this will become possible. We expect high reliability from the XBARPUF as it depends on the relative write-time based on a comparison, as opposed to relying on the actual output of a group of memristors as in previous work. Verification of this expectation is left for future work.

6. CONCLUSIONS

A novel memristive crossbar-based PUF circuit is presented which builds on a previous design that depends on the write-time of memristors to generate unique responses. The proposed XBARPUF relies on the relative write-times of pairs of memristive circuits to generate the response, as opposed to an absolute write-time that would be sensitive to operating conditions. Further, the write operation itself is governed by the challenge such that one memristor in a pair will be written while the other is not. This leads to an exponential number of unique combinations of altered memristors to select from when generating each response bit. In this way, the memristive circuits in an XBARPUF race one another until one is SET first, similar to how signals race in a delay-based APUF.

While reliability is left for future work due to the experimental nature of memristors, early results shown here for entropy and uniqueness are promising for the XBARPUF. The result not only shows uniqueness is near the ideal of 50% for a high degree of variability but that the uniqueness is fairly steady even when smaller variations are expected. This robustness is understandable given that the circuit re-

Table 1: Performance Results for the Memristive Crossbar PUF

V_{WR} (V)	V_{RD} (V)	R_{LD} (kΩ)	V_{tp}/V_{tn}	% var. (all)	Entropy	Uniqueness (%)	Uniformity (%)	Power (μW)
1.5	0.9	176	1.1/(-1.1)	0.5	0.97166	48.26	52.45	1633.95
				2.0	0.99565	49.90	50.50	1634.02
				10.0	0.99688	49.98	50.60	1634.17
1.3	0.8	176	1.0/(-1.0)	0.5	0.97110	48.22	52.60	990.80
				2.0	0.99559	49.89	50.25	990.95
				10.0	0.99688	49.98	50.90	991.01
1.1	0.7	176	0.9/(-0.9)	0.5	0.97369	48.39	52.45	565.49
				2.0	0.99298	49.71	51.05	565.37
				10.0	0.99659	49.96	50.15	564.83

lies on comparisons between small differences in operation of two independent circuit paths.

Results are also shown for power consumption for the proposed design. It should be noted that the power is considered for different threshold voltages and thus different read and write voltages. Typically, device parameters such as the threshold voltage would not be determined by design. Memristors, however, come in a variety of flavors based on their dimensions, composite materials, and so on. Thus, it is reasonable that memristors can be tailored for specific applications. Based on the results shown, the XBARPUF exhibits relatively small power consumption when the threshold voltage can be scaled below 1 V. Combining the reduction in power with the small area, the XBARPUF is a resource efficient alternative to pure CMOS PUF circuit designs.

7. ACKNOWLEDGMENTS

The authors would like to thank Nathan McDonald, Lok-Kwong Yan and Bryant Wysocki of the Air Force Research Laboratory, Rome, NY, for their valuable discussions.

8. REFERENCES

[1] Y. Alkabani and F. Koushanfar. Active control and digital rights management of integrated circuit ip cores. In *Proceedings of the 2008 International Conference on Compilers, Architectures and Synthesis for Embedded Systems*, pages 227–234, 2008.

[2] 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. In *Symposium Q–New Functional Materials and Emerging Device Architectures for Nonvolatile Memories*, volume 1337 of *MRS Proceedings*, January 2011.

[3] Y. Cao. *PTM: Predictive Technology Model*, 2012 (Accessed December, 2014). `http://ptm.asu.edu`.

[4] L. O. Chua. Memristor-the missing circuit element. *IEEE Transactions on Circuit Theory*, 18(5):507–519, September 1971.

[5] L. O. Chua and S. M. Kang. Memristive devices and systems. *Proceedings of the IEEE*, 64(2):209–223, February 1976.

[6] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas. Silicon physical random functions. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 148–160, 2002.

[7] L. Goux, J. G. Lisoni, M. Jurczak, D. J. 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*, 107(2), January 2010.

[8] J. Guajardo, G. Kumar, S. Schrijen, and P. Tuyls. Physical unclonable functions and public-key crypto for FPGA IP protection. In *Proceedings of the IEEE International Conference on Field Programmable Logic and Applications*, pages 189–195, August 2007.

[9] N. R. McDonald. Al/Cu_xO/Cu memristive devices: Fabrication, characterization, and modeling. Master's thesis, College of Nanoscale Science and Engineering, University at Albany, Albany, NY, 2012.

[10] 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*, 78:46–50, December 2012.

[11] A. S. Oblea, A. Timilsina, D. Moore, and K. A. Campbell. Silver chalcogenide based memristor devices. In *Proceedings of The 2010 International Joint Conference on Neural Networks (IJCNN)*, pages 1–3, July 2010.

[12] J. Rajendran, R. Karri, J. B. Wendt, M. Potkonjak, N. McDonald, G. S. Rose, and B. Wysocki. Nanoelectronic solutions for hardware security. Cryptology ePrint Archive, Report 2012/575, 2012. `http://eprint.iacr.org/`.

[13] G. S. Rose, N. McDonald, L. Yan, and B. Wysocki. A write-time based memristive puf for hardware security applications. In *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pages 830–833, November 2013.

[14] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams. The missing memristor found. *Nature*, 453:80–83, May 2008.

[15] 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 *Proceedings of the 32Nd Annual International Symposium on Computer Architecture*, pages 25–36, 2005.

[16] R. Waser and M. Aono. Nanoionics-based resistive switching memories. *Nature Materials*, 6:833–840, November 2007.

[17] W. Zhao and Y. Cao. New generation of predictive technology model for sub-45nm early design exploration. *IEEE Transactions on Electron Devices*, 53(11):2816–2823, November 2006.