Memristor PUFs: A New Generation of Memory-based Physically Unclonable Functions

Patrick Koeberl
Intel Collaborative Research Institute
for Secure Computing
Darmstadt, Germany
patrick.koeberl@intel.com

Ünal Kocabaş
TU Darmstadt/CASED
Darmstadt, Germany
unal.kocabas@trust.cased.de

Ahmad-Reza Sadeghi
Intel Collaborative Research Institute
for Secure Computing
Darmstadt, Germany
ahmad.sadeghi@trust.cased.de

***Abstract*—Memristors are emerging as a potential candidate for next-generation memory technologies, promising to deliver non-volatility at performance and density targets which were previously the domain of SRAM and DRAM. Silicon Physically Unclonable Functions (PUFs) have been introduced as a relatively new security primitive which exploit manufacturing variation resulting from the IC fabrication process to uniquely fingerprint a device instance or generate device-specific cryptographic key material. While silicon PUFs have been proposed which build on traditional memory structures, in particular SRAM, in this paper we present a memristor-based PUF which utilizes a weak-write mechanism to obtain cell behaviour which is influenced by process variation and hence usable as a PUF response. Using a model-based approach we evaluate memristor PUFs under random process variations and present results on the performance of this new PUF variant.**

I. Introduction

Physically Unclonable Functions (PUFs) have been introduced as a relatively new security primitive which exploit manufacturing variation resulting from the IC fabrication process to uniquely fingerprint a device instance or generate device-specific cryptographic key material. A number of PUF variants have been proposed which build on traditional memory structures, in particular SRAM [4]. In this paper we consider whether PUFs based on memristors are feasible.

In 1971 Leon Chua predicted [3] the existence of a fourth fundamental circuit element in addition to the resistor, capacitor and inductor for which he coined the term memristor (memory resistor). In simple terms the memristor behaves like a charge-controlled resistor with memory. The first practical realization of a memristor was developed by HP Labs in 2008 [13] leading to proposals ranging from neural network realizations [12], [8] and digital logic [11], [14]. Memristor memory technologies [6], [9] are of particular interest with the promise of non-volatility combined with high density and performance being suitable for use as a next generation universal memory in computer systems [2].

Contribution. We explore the feasibility of using memristor technology as Physicaly Unclonable Functions (PUFs). Two methods are proposed to obtain PUF-like behaviour from the underlying memristor technology and a memristor PUF model is presented which includes random process variation. The performance of the memristor PUF is analyzed and the results show that the concept of a memristor PUF is in principle feasible.

Outline. We introduce memristors in Section II and our memristor-based PUF mechanism and model in Section III. In Section IV we present our analysis methodology together with results and conclude the paper in Section V.

II. Memristors

A. Physical Structure

The physical structure of a thin-film memristor along with its equivalent circuit model is depicted in Figure 1. The device consists of a semiconductor thin-film of length D sandwiched between two metal contacts consisting of a doped (TiO_{2-x}) and un-doped region (TiO_2). The internal state variable w represents the length of the doped region. The doped region has a low resistance (R_{ON}) while that of the un-doped region has a much higher resistance (R_{OFF}). The overall resistance of the memristor is given in Equation 1.

$$R(w) = (R_{ON} \cdot \frac{w}{D} + R_{OFF} \cdot (1 - \frac{w}{D})) \qquad (1)$$

The state variable w exhibits a dependence on the charge flowing through the device allowing the total resistivity to be controlled. When the flow of charge stops the resistance value is retained, an effect that persists even when power is removed from the device. For brevity the details are omitted and the reader is referred to the references [3], [15], [6].

B. Memristor as a memory cell

The controlability of the memristor's resistance can be exploited to create a memory device. For simplicity, a memristor is defined at logic 0 when $0 < w/D < 0.5$ and

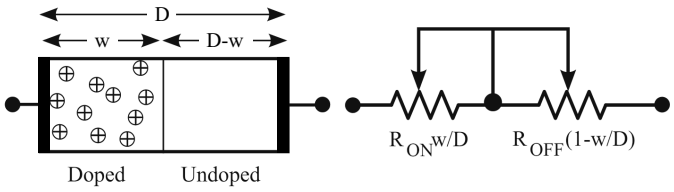

Figure 1: Memristor device model

978-3-9815370-0-0/DATE13/©2013 EDAA

logic 1 when $0.5 < w/D < 1$. In reality, a safety margin is specified for each logic output: $0 \leq w/D \leq O_L$, for logic 0, and $O_H \leq w/D \leq 1.0$ for logic 1. The region between $O_L \leq w/D \leq O_H$ is an undefined region that should be avoided for data integrity. In this section we briefly explain the realization of read and write schemes for memristors [6].

In order to write $logic\ 1$ to the device, input voltage V_{in} generates a square-wave pulse that has magnitude $+V_A$ and width T_{w1} as shown in Figure 2 (left). Here, pulse width T_{w1} must be longer that the minimum required time and $+V_A$ must be high enough to ensure the state settles inside the $logic\ 1$ region after write. If the initial state w_0 is $w_0 \neq 0$, a successful write can be guaranteed as long as $T_{w1} \geq T_{w1}^{O_H}$.

To write $logic\ 0$, the input voltage V_{in} is a negative square-wave pulse $(-V_A)$ with duration T_{w0} as shown in Figure 2 (right). The write 0 process will be successful if pulse width T_{w0} is at least greater than $T_{w0}^{O_L}$.

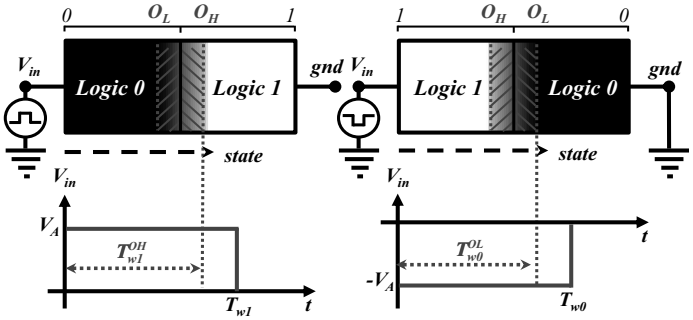

Figure 2: Write 1 and write 0 signals

To read a logic value from a memristor cell, one first perturbs the memristor state to detect the internal state and then recovers the internal state to the initial position. The proposed read signal pattern in [7] has a negative pulse followed by a positive pulse with equal magnitude and duration. This read pattern ensures zero net flux injection over one period ensuring that the memristor state is unaltered after the read access. Figure 3 depicts this read pattern, internal memristor state and output voltage V_o when the memristor stored logic state is zero (top) and one (bottom). The logic state should be read out between t_1 to t_2, since only the second half period of v_o reflects the correct logic state stored in the memristor.

C. Memristor Memory Array

Figure 4 illustrates a memristor memory structure which has similarity to an SRAM array. It consists of a row/column decoder, a sense amplifier, a pulse generator and a read/write (R/W) selector. While the pulse generator generates read or write pattern signals, the R/W selector switches the memristor cells to ground for a write operation and a reference resistance R_x for a read operation [6].

III. Memristor-based Physically Unclonable Functions (PUFs)

A PUF is a physical challenge-response system which when queried with a challenge x, generates a response y that is *robust*, *unclonable* and *unpredictable*. Informally, robustness

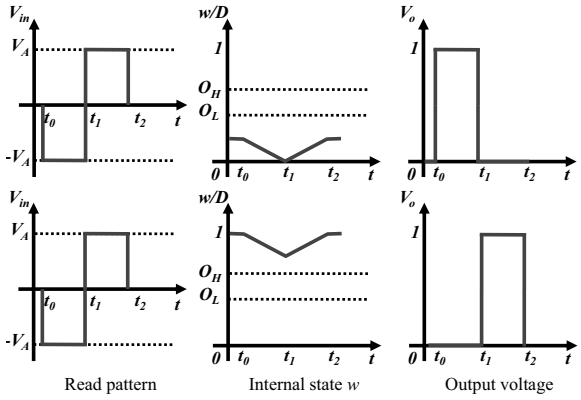

Figure 3: Graphical illustration for the read scheme

means that, when queried with the same challenge multiple times, the PUF returns similar responses with high probability. Unclonability means that it is infeasible to produce two PUFs that are indistinguishable based on their *challenge-response* (CRP) behaviour. Unpredictability requires that it is infeasible to predict the PUF response to an unknown challenge.

A. Memristor PUF Mechanism

Our memristor PUF exploits the unpredictable logic state of memristor cells within the undefined region between $O_L \leq w/D \leq O_H$ as shown in Figure 2. A related concept proposed as a Design-for-Testability (DfT) mechanism for seeking defective memristor cells in a memory array is proposed in [5]. As discussed in Section II-B memristor memory operations rely on the *duration of access time* and the *value of supply voltage*.

- *Duration of access time.* Every normal write operation requires a proper amount of time to set the memristor internal state to a defined state such as $T_{w1}^{O_H}$ or $T_{w0}^{O_L}$. If the access time is reduced, the cell will not have enough time to change its state from logic 1 to logic 0 or vice versa and will remain in the undefined state. This scheme is referred to as *Short Write Time (SWT)* and the write operation with a shorter access time (T_{SWT}) is referred to as *weak write*.

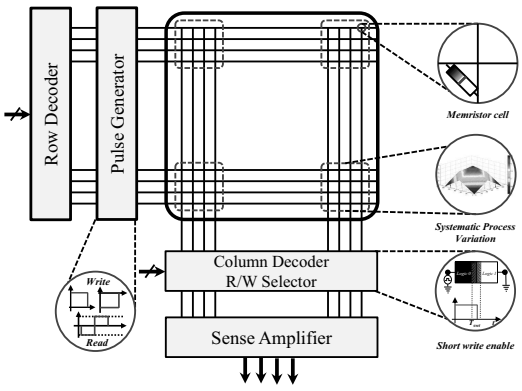

Figure 4: Memristor memory structure

- *Value of supply voltage.* Every write operation requires a specific write voltage for reliable operation. If the voltage supply is reduced, the induced electric field will not enough to change the cell's state which will remain in the undefined state. This scheme is referred to as *Low Write Voltage (LWV)* with the reduced supply voltage being referred to as V_{LWV}.

In order to the evaluate the PUF response of a memristor cell array first the array must be first calibrated in order to determine the optimum write time T_{SWT} and voltage supply (V_{LWV}). The calibration is required to ensure the overall PUF response is not biased to either '1' or '0'.

Figure 5 illustrates driving two memristor cells with the *SWT* scheme. We first write 1 to both memristor cells ($t_0 \rightarrow t_1$) and then we perform a weak write 0 operation ($t_1 \rightarrow t_2$). After reading operation ($t_2 \rightarrow t_3$) while one memristor stays in logic 1 state, second one flips to logic 0 state. In Figure 6, we follow the *LWV* scheme. First we write 1 to both memories cells and we perform a weak write with low supply voltage ($V_{in} \neq +V_A$) in writing time $T_{w1}^{O_H}$.

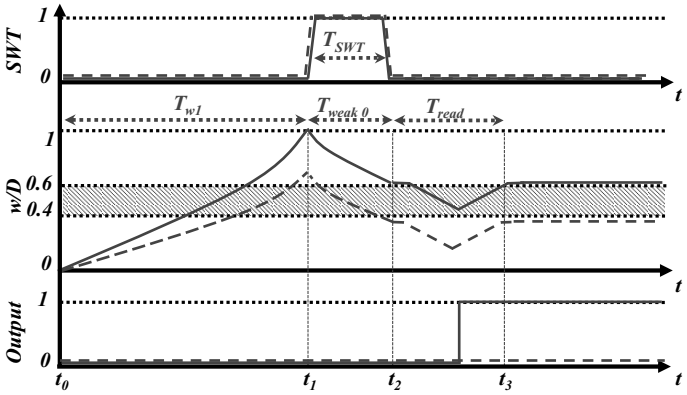

Figure 5: SWT scheme on two memristor cells, dashed line is second cell

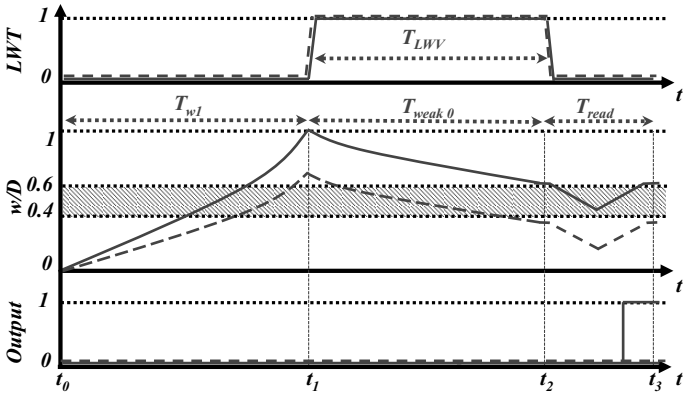

Figure 6: LWV scheme on two memristor cells, dashed line is second cell

B. Memristor PUF Model

Using the linear ion drift equations the device parameters for one memristor cell were developed using Matlab and incorporated into a higher-level model of a complete 1MB memristor array. As the fundamental phenomenon underlying PUF behaviour, modelling of process variation to some degree of accuracy is essential. A first-order approach is to consider process variations over the doped resistance R_{ON}, the updoped resistance R_{OFF} and the memristor cell thickness D as defined in Equation 1. Standard CMOS manufacturing technologies are subject to two process variation components, random and systematic and we assume that memristor technolgies will be similarly affected. Parameters subject to random variation in thin-film memristor implementations include dopant concentration and thin-film thickness. Systematic variations show a strong spatial correlation as a result of lithographic proximity effects, density effects and the relative distance of devices.

Random process variation was applied to the base device parameters of each memristor cell in the array using the Monte Carlo method. Three ranges of random variation were applied, 'best-case', 'typical-case' and 'worst-case' representing maximum variations of $\pm 1\%$,$\pm 3\%$ and $\pm 5\%$, respectively.

IV. Analysis

A. Methodology

Many PUF-enhanced applications, including PUF-based identification and key storage, require PUF responses to be reliably reproducible (robust) while at the same time being unpredictable (see, e.g., [10], [1]). However, since we modelled the memristor memory behaviour with process variation but not with environmental variations, our evaluation only focuses on unpredictability.

Unpredictability ensures that an adversary cannot fully compute the PUF response of a device to an unknown challenge, even if she can obtain a certain amount of challenge/response pairs. We assess the unpredictability of memristor PUFs by analyzing the hamming weight and hamming distance of 150 1MB memristor PUFs:

- *Hamming Weight.* We examine each PUF response to see if it exhibits a bias towards 0 or 1. The optimum value for hamming weight should be $\simeq 0.5$.
- *Hamming Distance.* We compute the inter-distance [10] between two memory blocks of size 1MB indicating whether responses of *different* memristor PUFs are independent. Similarly the optimum value for inter-distance is $\simeq 0.5$.

B. Parameters & Results

This section presents the parameter selection and analysis results for the modelled memristor PUFs. We considered the memristor fabricated by Hewlett Packard [15], [13] in this work. The oxide thickness D of the modelled memristor is $10\ nm$ and R_{ON} and R_{OFF} are selected as 60Ω and 16kΩ respectively. In addition to using the linear ion drift model, these model parameters exhibit near-symmetric I-V characteristics for both positive and negative voltage differences across the device.

In our results, we used 150 memory blocks of 1 MB from three different random variation ranges previously mentioned in Section III-B. Figure 7 shows the hamming distance between

two memory blocks under worst-case, typical- and best-case process variations. Analysis of the hamming weights revealed that their mean value are close to the optimum which is 0.5. These preliminary results reveal that memristor arrays show promise as a PUF building block.

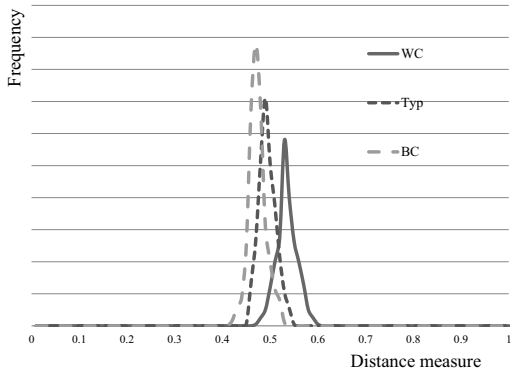

Figure 7: Hamming distance of memristor-PUFs

V. Conclusion

In this work we proposed the first PUF design building on thin-film memristor technology. While memristors are not yet avaiable commercially, preventing a full evaluation of their potential as a PUF solution, a model-based approach was used to evaluate the concept including a first-order treatment of random process variation. The preliminary results show that memristor PUFs provide high hamming distance between different memory blocks and good hamming weight ($\simeq 0.5$) within individual memory blocks. We consider this work to be a first step in the determination of whether memristor technology can be used as the basis of a novel PUF variant.

Process variation is a key determinant in defining PUF behaviour and performance and we consider the refinement of the process variation model to be an important next step. In addition the requirement of a calibration procedure is a disadvantage with respect to other memory-based PUFs such as SRAM PUFs. Future work will investigate the calibration requirements in more detail.

References

[1] Frederik Armknecht, Roel Maes, Ahmad-Reza Sadeghi, Francois-Xavier Standaert, and Christian Wachsmann. A formal foundation for the security features of physical functions. In *IEEE Symposium on Security and Privacy (SSP)*, pages 397–412. IEEE Computer Society, May 2011.

[2] G. W. Burr, B. N. Kurdi, J. C. Scott, C. H. Lam, K. Gopalakrishnan, and R. S. Shenoy. Overview of candidate device technologies for storage-class memory. *IBM J. Res. Dev.*, 52(4):449–464, July 2008.

[3] L. Chua. Memristor-The missing circuit element. *IEEE Transactions on Circuit Theory*, 18(5):507–519, January 1971.

[4] Jorge Guajardo, Sandeep Kumar, Geert-Jan Schrijen, and Pim Tuyls. FPGA intrinsic PUFs and their use for IP protection. In *Cryptographic Hardware and Embedded Systems (CHES)*, volume 4727 of *LNCS*, pages 63–80, Berlin, Heidelberg, 2007. Springer Berlin / Heidelberg.

[5] Nor Zaidi Haron and Said Hamdioui. Dft schemes for resistive open defects in rrams. In *DATE*, pages 799–804, 2012.

[6] Yenpo Ho, Garng M. Huang, and Peng Li. Nonvolatile memristor memory: Device characteristics and design implications. In *ICCAD*, pages 485–490, 2009.

[7] Yenpo Ho, Garng M. Huang, and Peng Li. Dynamical properties and design analysis for nonvolatile memristor memories. *IEEE Trans. on Circuits and Systems*, 58-I(4):724–736, 2011.

[8] Sung H. Jo, Ting Chang, Idongesit Ebong, Bhavitavya B. Bhadviya, Pinaki Mazumder, and Wei Lu. Nanoscale Memristor Device as Synapse in Neuromorphic Systems. *Nano Letters*, 10(4):1297–1301, April 2010.

[9] Hyongsuk Kim, Maheshwar Pd Sah, Changju Yang, and Leon O Chua. Memristor-based multilevel memory. *2010 12th International Workshop on Cellular Nanoscale Networks and their Applications CNNA 2010*, 1(5):1–6, 2010.

[10] Roel Maes and Ingrid Verbauwhede. Physically unclonable functions: A study on the state of the art and future research directions. In *Towards Hardware-Intrinsic Security*, 2010.

[11] Jeyavijayan Rajendran, Harika Manem, Ramesh Karri, and Garrett S. Rose. Memristor based programmable threshold logic array. In *Proceedings of the 2010 IEEE/ACM International Symposium on Nanoscale Architectures*, Nanoarch '10, pages 5–10, 2010.

[12] Greg S. Snider. Spike-timing-dependent learning in memristive nanodevices. In *Nanoscale Architectures, 2008. NANOARCH 2008. IEEE International Symposium on*, pages 85–92, June 2008.

[13] Dmitri B. Strukov, Gregory S. Snider, Duncan R. Stewart, and R. Stanley Williams. The missing memristor found. *Nature*, 453(7191):80–83, May 2008.

[14] Wei Wang, Tom T. Jing, and Brian Butcher. Fpga based on integration of memristors and cmos devices. In *ISCAS*, pages 1963–1966, 2010.

[15] Joshua J. Yang, Matthew D. Pickett, Xuema Li, Douglas A. A. Ohlberg, Duncan R. Stewart, and R. Stanley Williams. Memristive switching mechanism for metal/oxide/metal nanodevices. *Nature NanoTechnology*, 3(7):429–433, July 2008.