Implementing Physical Unclonable Functions Using PCM Arrays

Enrico Piccinini, Massimo Rudan
"E. De Castro" Advanced Research Center on
Electronic Systems (ARCES) and Department DEI
University of Bologna, Viale Risorgimento 2, I-40136 Bologna, Italy
e-mail: enrico.piccinini@unibo.it, massimo.rudan@unibo.it

Rossella Brunetti
FIM Department,
University of Modena and Reggio Emilia
Via Campi 213/A, I-41125 Modena, Italy
e-mail: rossella.brunetti@unimore.it

***Abstract*—The stochastic nature of the switching mechanism of amorphous phase-change memory (PCM) arrays can fruitfully be exploited to implement primitives for hardware security. This paper tackles, by means of PCM, the feasibility of Reconfigurable Physical Unclonable Functions, that constitute one of the two building blocks of cryptographic applications.**

I. Introduction

Ovonic and phase-change materials have been selected by some leading electronic industries as semiconductors for innovative devices in the field of data storage, and proposed for beyond-von Neumann calculators and bio-inspired neuromorphic computing. Cross-point arrays of chalcogenide-based devices have been realized [1] and, quite later, commercial mass production has been announced.[1]

The stochastic nature of the switching mechanism of amorphous chalcogenides, either Ovonic or phase changing, is a drawback for the memory technology because it implies statistically dispersed threshold conditions. However, stochasticity can be given a turn for the better in other kinds of applications, e.g., it can fruitfully be exploited to implement primitives for hardware security.

By applying a set voltage pulse, whose amplitude corresponds to a switching probability of 50%, to a memory initially placed in the full-reset 0 state, half of the memory bits are statistically switched and programmed to state 1, whereas the remainder of the bits persist in state 0. In a recent paper [3] it has been shown that such a natural randomness can be exploited to create a True Random Number Generator (TRNG), which is one of the two building blocks of cryptographic applications.

The second building block, namely, the implementation of Physical Unclonable Functions (PUFs), is tackled in this paper. A PUF, in fact, converts the randomness into a secure primitive [4], [5]. Specifically, due to the stochastic programming of the physical bit, a *challenge* applied on a PUF gives origin to a unique *response*, that turns it into a digital random number (*challenge-response pairs*, CRPs). Natural statistical fluctuations in the amorphization process make these CRPs unique and, consequently, makes it impossible to clone the response or predict it, without altering the underlying physical substrate. Like in the case of the TRNG, the feasibility of a simple PUF by means of self-heating phase-change memory cells (PCM) coupled to Ovonic selectors in crossbar arrays (Fig. 1) is assessed and demonstrated through simulations based upon the Random Network Model [6], [7], [8].

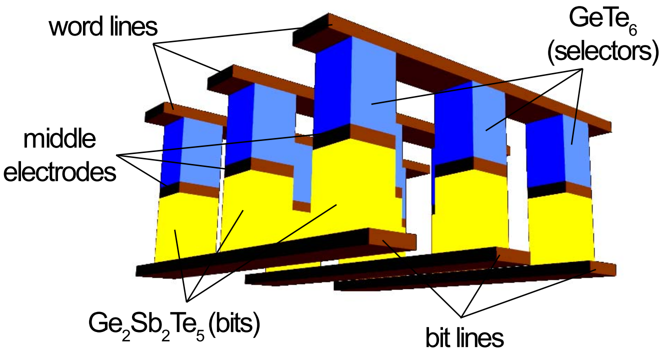

Fig. 1. Schematics of the crosspoint memory array with integrated Ovonic selectors. The GeTe$_6$ and Ge$_2$Sb$_2$Te$_5$ chalcogenides are template materials for Ovonic and phase-change switching.

II. Threshold Variability

The threshold variability in amorphous semiconductors is commonly due to two main sources, namely, *i)* intercell variability, that derives from the structural differences from a cell to another due to unavoidable process variations, and *ii)* intracell variability, due to the inherent stochastic nature of the amorphous phase.

Consider a set of Q cells that have undergone P amorphization-crystallization cycles, and define $\overline{V}^s_{\rm th}$ and $\overline{V}_{\rm th}$ as:

$$\overline{V}^s_{\rm th} = \frac{1}{P}\sum_{k=1}^{P} V^{sk}_{\rm th}\,, \qquad \overline{V}_{\rm th} = \frac{1}{Q}\sum_{s=1}^{Q} \overline{V}^s_{\rm th}\,,$$

with $V^{sk}_{\rm th}$ the threshold voltage obtained from the k-th measurement on the s-th cell. By these definitions one is able to separate the effects of the process variation from those due to the stochastic nature of the amorphous phase; this is achieved

[1] In fact, the first commercial product incorporating a solid-state drive made of a 3D, cross-point non-volatile memory has been launched very recently [2]. As of today, the materials' nature and the exact operating principle of this memory cell have not been disclosed.

by calculating and separately storing the normalized intercell η and intracell ξ threshold voltages

$$\eta = \frac{\overline{V}_{\rm th}^{s}}{\overline{V}_{\rm th}} - 1\,, \qquad \xi = \frac{V_{\rm th}^{sk}}{\overline{V}_{\rm th}^{s}} - 1\,.$$

The relative weights of η and ξ depend on the manufacturing technology.

The mushroom and μ-trench architectures for PCM cells require the presence of an external heater connected in series to the chalcogenide layer to generate the thermal power necessary for the phase change. Since the intrinsic statistical nature of the electric response of amorphous materials is dominated by the heater-induced crystallization, such a solution provides a narrow dispersion of the intracell threshold voltage (ξ). The variability is therefore basically due only to unavoidable process variations, which are minimized as much as possible at the manufacturing stage. However, the heater enhances the possibility that interfacial atoms of an alien species diffuse into the chalcogenide layer and alter its conductive properties, and may hinder the miniaturization of the memory array.

These aspects are not present in self-heating cells, where the heater is missing. In self-heating cells, the phase change is solely due to the Joule heating produced by the current flux within the chalcogenide layer. The adoption of self-heating cells enlarges the variability window, as statistical effects connected to the thermodynamics of crystallization sums up with those linked to electrical transport, making the variability of the intercell threshold-voltage (η) variability dominating over its the intracell counterpart (ξ) variability. The enlarged window due to the stochastic nature of the threshold switching can better be exploited in the field of cryptography and on-chip data protection.

In order to simulate the intercell variability, we adopt the Random Network Model. This model naively describes the hot spots where the crystallization induced by Joule heating begins with the formation of conductive segments among clusters of traps, that have been demonstrated to populate the matrix [9]. Given the transition rate S_{ij} between two internal clusters i and j, with $(i,j) \in [1,N]$ (indices 0 and $N+1$ refer to the two contacts), the charge- and energy-balance equations are expressed as:

$$\frac{I}{-q}\delta_{0,j} + \sum_{j\neq i} n_j S_{ji} = n_i \sum_{j\neq i} S_{ij} + \frac{I}{-q}\delta_{N+1,j}\,, \tag{1}$$

$$\begin{aligned}\sum_{j\neq i} n_j S_{ji}\Big[e_j - q(\varphi_j - \varphi_i)\Big] + \frac{I}{-q}\, e_i \delta_{0,i} = \\ = e_i \left[n_i \sum_{j\neq i} S_{ij} + \frac{I}{-q}\delta_{N+1,i}\right] + n_i \frac{e_i - e_{i,\rm eq}}{\tau_R}\,,\end{aligned} \tag{2}$$

with q the elementary charge and τ_R an energy-relaxation time. In (1)-(2) n_i, e_i and φ_i are the carrier concentration and average energy, and the electrostatic potential of the i-th cluster, whereas subscript "eq" stands for equilibrium. The equations above are coupled to the Poisson and Fourier-heat equations:

$$\nabla \cdot (\varepsilon\, \nabla \varphi) + Q_i = 0\,, \tag{3}$$

$$\nabla \cdot (\kappa\, \nabla T) + W_{ij} = 0\,, \tag{4}$$

where T is the (local) lattice temperature, Q_i and W_{ij} are the charge of the i-th cluster and the heat generation along the segment connecting the i-th and the j-th clusters, respectively.

Trap clusters are generated as a result of an underlying dynamics, and mimic the properties of the amorphous matrix; in the absence of any further information, for simplicity, they are assumed to be uniformly distributed over the entire simulation domain. Given the current I, the solution of (1)-(4) allows one to check whether one segment reaches the phase-change condition (i.e., it has an average temperature above the glass transition temperature of the material under investigation) and initiates the phase-change process. The same model also applies to the investigation of OTS materials, with the only difference that the phase-change condition is never reached in the typical operating conditions, as testified by the absence of the very sharp transition in the current vs. voltage diagram shown by phase-changing chalcogenides (Fig. 2).

Finally, it should also be mentioned that the present form of the Random Network Model does not account for the forming effects, which are present in the first tens of amorphization cycles of real samples [10]. As a matter of fact, this is not a real problem because it can easily be fixed by the manufacturers before the final product is released.

III. PUF Implementation

We consider a very simple PUF, whose challenge is the address of a 16-bit sequence (word) and the response is the word itself, which is then post-processed into a fingerprint (like, e.g., 4 hex values). On the one side, if such a PUF is used as a fingerprint of a circuit or a device, or as a hash key, the stability of chalcogenide memories over time ensures its readability for more then 10 year; on the other side, when the information stored in the PUF does not need to be preserved after reading, the PUF can be reconfigured upon request a virtually-infinite number of times: it has been proven, in fact, that chalcogenide-based phase-change memories are stable up to 10^8 write cycles [11]. The PUF operation is summarized in Fig. 3.

By means of a protocol very similar to the one described in Ref. [3], we have generated 4800 bits, and have grouped them into 300 sequences of 16 bits each, as shown in Fig. 4. After having assessed (including also the parasitic effect of the series resistances) the true stochasticity of the sequence generation according to the NIST statistical test suite [12] (results are listed in table I), we have also checked these sequences as sources for the proposed PUF. Due to the relative small number of sequences, only 8 tests can be applied; following the NIST guidelines the following parameters have been set: *block frequency test: m=8; approximate entropy test: m=2; serial test: m=2*. Tests are passed if less than 3% of the sequences fails.

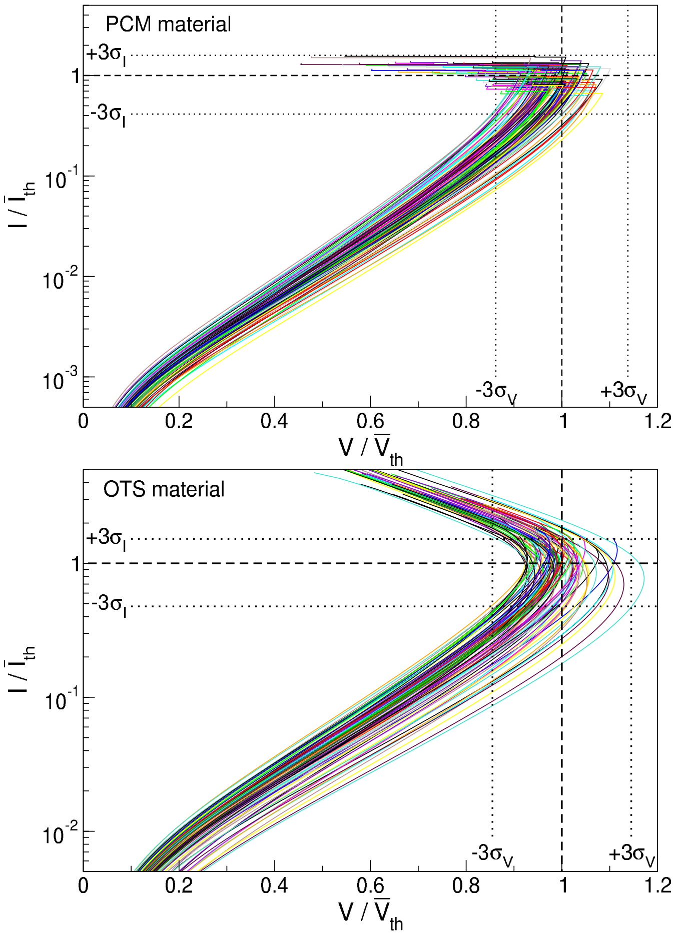

Fig. 2. Normalized current vs. voltage characteristics calculated by means of the Random Network Models with 100 current-driven simulations for a PCM cell (top) and an OTS selector (bottom). The switching region, marked by the dotted lines, is also shown for both cases.

The performance of a PUF is usually controlled by specific metrics [13], among which the most important ones are *uniformity*, *uniqueness*, and *robustness*.

Uniformity (U_i) estimates how uniform the proportion of 1s and 0s is within the i-th response string r_i. It is defined as

$$U_i = \frac{100}{n} \sum_{l=1}^{n} r_{il}\,, \qquad i = 1, \ldots, N\,, \tag{5}$$

where index l spans over the n bit positions of the string. The expectation value for truly random sequences is 50%. After running the uniformity test, the mean uniformity found for the proposed PUF is $\mu(U_{PUF}) = \sum_{i=1}^{N} U_i/N = 51.2\%$, with a standard deviation $\sigma(U_{PUF}) = 12.4\%$ (Fig. 5). The relatively high standard deviation is coherent with the limited amount of tested PUFs.

Uniqueness (H) represents the ability of a PUF to uniquely distinguish a particular chip among a group of chips given the same challenge. Uniqueness is calculated by means of the Hamming distance $\mathcal{HD}$ of the responses r_i^p and r_j^q to the same challenge, of two strings belonging to chips p and q, averaged over k chips (inter-chip Hamming distance):

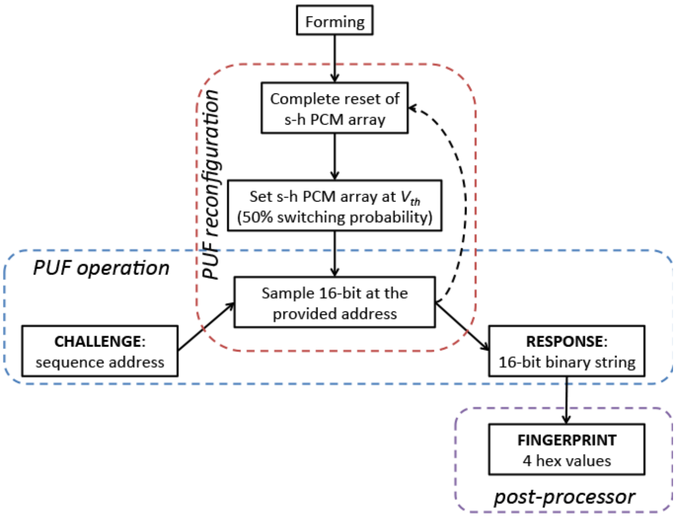
Forming
Complete reset of s-h PCM array
Set s-h PCM array at V_{th} (50% switching probability)
PUF reconfiguration
PUF operation
Sample 16-bit at the provided address
CHALLENGE: sequence address
RESPONSE: 16-bit binary string
FINGERPRINT 4 hex values
post-processor

Fig. 3. Flowchart or the proposed PUF ("s-h" stands for self-heating). The dashed arrow indicates an optional event for the case of PUF reconfiguration.

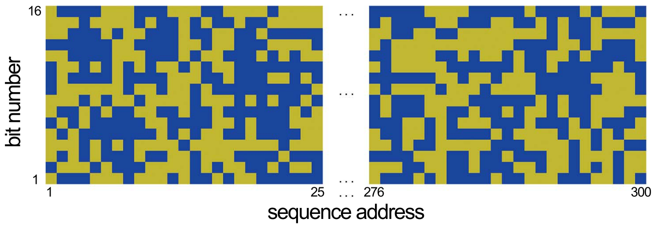

Fig. 4. Graphical representation of the 300 16-bit sequences under test. Bright and dark squares stand for '0' and '1' bits, respectively

$$H = \frac{100}{k\,(k-1)} \sum_{p=1}^{k-1} \sum_{q=p+1}^{k} \frac{\mathcal{HD}(r_i^p, r_i^q)}{n}\,. \tag{6}$$

The theoretical expectation value is again 50%. In order to perform this test we have grouped the 300 sequences of $n = 16$ bits in 10 batches of $k = 30$ chips each, using the address of the unique string coded into each chip as the common challenge. The uniqueness test provides results very close to ideality, with mean value $\mu(H_{PUF}) = 49.7\%$ and standard deviation $\sigma(H_{PUF}) = 1.5\%$.

Robustness (R) assesses the efficiency of a PUF to reproduce the response string under different conditions. It is calculated by means of the Hamming distance of the response to the same challenge in the same chip at different times, temperatures or fluctuations of the reading voltage (intra-chip Hamming distance):

$$R = \frac{100}{m} \sum_{i=1}^{m} \frac{\mathcal{HD}(r_i, r_i')}{n}\,. \tag{7}$$

The ideal value for robustness is 0%. On the basis of the switching probability reported in [3], fluctuations up to 2.7 V of the reading voltage do not influence at all the probability of

TABLE I
RESULTS OF 8 TESTS FROM THE NIST STATISTICAL SUITE

Test name	Failure rate	Result
Frequency	1.00%	PASS
Block Frequency	1.67%	PASS
Cumulative Sums (forward)	1.00%	PASS
Cumulative Sums (reverse)	1.00%	PASS
Runs	0.67%	PASS
Longest Run of 1's	0.00%	PASS
FFT	0.33%	PASS
Approximate Entropy	0.33%	PASS
Serial (P-value$_1$)	1.33%	PASS
Serial (P-value$_2$)	0.00%	PASS

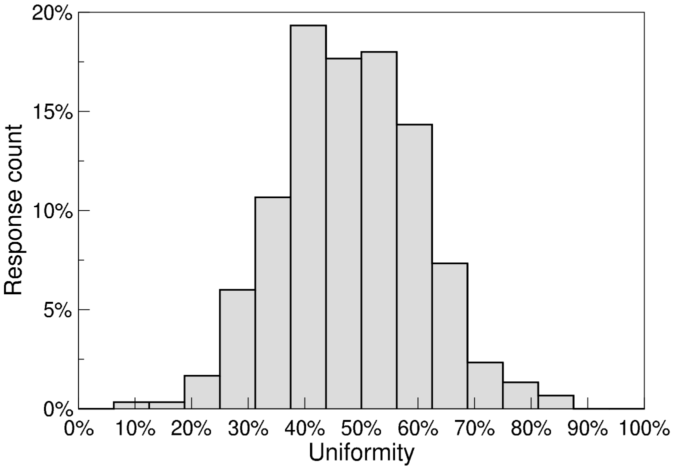

Fig. 5. Distribution of the uniformity test run over 300 response strings.

switching, since the lower boundary of the switching windows was determined to be about 3.2 V. Moreover, as already mentioned before, the data-retention time at room temperature in phase-change memories is larger than 10 years, which makes the response very stable in time.

As far as operating temperatures are concerned, two aspects deserve attention: the glass transition temperature of the material, by which the phase change sets in, and the reduction of the threshold voltage due to the activation energy of conduction. They both limit the operating conditions for a given reading voltage. Calculations show that the reduction of the threshold voltage to values close to the reading voltage of the proposed PUF requires operating temperatures near or above the glass transition temperature [14]. Furthermore, the drift with time of the resistance of the amorphous phase [15], [16] is not an issue, since it enforces the stability of the high-resistance state. On the basis of these considerations, we conclude that the intra-chip Hamming distance is essentially 0%.

IV. CONCLUSIONS

The simulation of a small demonstrator for reconfigurable PUFs has been carried out by means of the Random Network Model using a crossbar memory array made of self-heating memory cells and Ovonic selectors, taking care also of the parasitic losses due to line resistance. The true stochasticity of sequences of bits has successfully been checked by means of the benchmarks proposed in the NIST statistical test suite. The performances of the tested PUF have been tested in terms of uniformity, uniqueness and robustness. For all the above metrics, the envisaged implementation has been found close to ideality.

REFERENCES

[1] D. Kau, S. Tang, I. Karpov, R. Dodge, B. Klehn, J. Kalb, J. Strand, A. Diaz, N. Leung, J. Wu, S. Lee, T. Langtry, K. wei Chang, C. Papagianni, J. Lee, J. Hirst, S. Erra, E. Flores, N. Righos, H. Castro, and G. Spadini, "A stackable cross point phase change memory," in *IEEE International Electron Devices Meeting (IEDM)*, 2009, pp. 617–620.

[2] March 2017, http://www.anandtech.com/show/11208.

[3] E. Piccinini, R. Brunetti, and M. Rudan, "Self-Heating Phase-Change Memory-Array Demonstrator for True Random Number Generation," *IEEE Trans. Electron Devices*, vol. 64, no. 5, pp. 2185–2192, 2017.

[4] C. Herder, M. D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug 2014.

[5] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Emerging physical unclonable functions with nanotechnology," *IEEE Access*, vol. 4, pp. 61–80, 2016.

[6] A. Cappelli, E. Piccinini, F. Xiong, A. Behnam, R. Brunetti, M. Rudan, E. Pop, and C. Jacoboni, "Conductive preferential paths of hot carriers in amorphous phase-change materials," *Appl. Phys. Lett.*, vol. 103, no. 8, 2013.

[7] A. Cappelli, R. Brunetti, C. Jacoboni, E. Piccinini, F. Xiong, A. Behnam, and E. Pop, "3D-nHD: A hydrodynamic model for trap-limited conduction in a 3D network," in *IEEE International Conference on Simulation of Semiconductor Processes and Devices (SISPAD)*, Sept 2013, pp. 436–439.

[8] E. Piccinini, A. Cappelli, F. Xiong, A. Behnam, F. Buscemi, R. Brunetti, M. Rudan, E. Pop, and C. Jacoboni, "Novel 3D random-network model for threshold switching of phase-change memories," in *IEEE International Electron Devices Meeting (IEDM)*, Dec 2013, pp. 22.6.1–22.6.4.

[9] A. Pirovano, A. Lacaita, A. Benvenuti, F. Pellizzer, and R. Bez, "Electronic switching in phase-change memories," *IEEE Trans. Electron Devices*, vol. 51, no. 3, pp. 452–459, 2004.

[10] F. Xiong, M.-H. Bae, Y. Dai, A. D. Liao, A. Behnam, E. A. Carrion, S. Hong, D. Ielmini, and E. Pop, "Self-aligned nanotube–nanowire phase change memory," *Nano Lett.*, vol. 13, no. 2, pp. 464–469, 2013.

[11] A. L. Lacaita and A. Redaelli, "The race of phase change memories to nanoscale storage and applications," *Microelectron. Eng.*, vol. 109, pp. 351–356, 2013.

[12] *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, NIST Special Publication 800-22rev1a, Apr 2010. [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/rng/index.html

[13] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," in *Embedded System Design with FPGAs*. Springer-Verlag, NY, USA, 2012, pp. 245–267.

[14] E. Piccinini, A. Cappelli, F. Buscemi, R. Brunetti, D. Ielmini, M. Rudan, and C. Jacoboni, "Hot-carrier trap-limited transport in switching chalcogenides," *J. Appl. Phys.*, vol. 112, no. 8, p. 083722, 2012.

[15] A. Pirovano, A. L. Lacaita, F. Pellizzer, S. A. Kostylev, A. Benvenuti, and R. Bez, "Low-field amorphous state resistance and threshold voltage drift in chalcogenide materials," *IEEE Trans. Electron Devices*, vol. 51, no. 5, pp. 714–719, May 2004.

[16] D. Ielmini, A. L. Lacaita, and D. Mantegazza, "Recovery and drift dynamics of resistance and threshold voltages in phase-change memories," *IEEE Trans. Electron Devices*, vol. 54, no. 2, pp. 308–315, Feb 2007.