Extended Abstracts of the 2017 International Conference on Solid State Devices and Materials, Sendai, 2017, pp589-590

M-2-04

Predictive Analysis of Randomness in 3D RRAM-based Physically Unclonable Security Primitive

Jeeson Kim[1], Hussein Nili[2], Gina C. Adam[2,3], Dmitri Strukov[2] and Omid Kavehei [1§]

[1] School of Engineering, RMIT University, Melbourne, VIC 3000, Australia
Phone: +61-3-9925-2450 E-mail: [§]omid.kavehei@rmit.edu.au
[2] University of California Santa Barbara, Santa Barbara, CA 93106-9560, U.S.A.
[3]National Institute for R&D in Microtechnologies, Romania

Abstract

This paper investigates quality of randomness in the first generation of 3D analog RRAM Physically Unclonable Function (PUF) primitives using measured and gathered data from fabricated RRAM crossbars. This study is significant as the randomness quality of a PUF directly relates to its resilience against various model-building attacks, including machine learning. Experimental result verifies near perfect (50%) predictability. It confirms the PUF's potentials for large-scale, yet small and power efficient, implementation of hardware intrinsic security primitives.

1. Introduction

Physically Unclonable Functions (PUFs) are relatively new breed of cryptographic primitives that gain advantage of otherwise disadvantageous variation in physical system manufacturing with the aim to produce secrets that are unclonable [1]. While their role in security hierarchy is still under study, they eliminate the need to explicitly store secrets in memory (e.g. EEPROM) and therefore are expected to significantly improve security. A PUF is, in its mathematical form, a hardware implementation of a one-way function that maps an input (challenge) to an ideally unique and unpredictable output (response). A PUF should ideally be unclonable against a wide range of adversarial attacks including: modeling, random guessing, man-in-the-middle, wide variety of side-channels and machine learning attacks. Recently, there has been an increased focus on implementing hardware-intrinsic security primitives based on inherent randomness in emerging electronic memory technologies.

Memory hardware such as RRAM (resistive random access memory) crossbars are among the most promising alternatives for large scale memory class, due to their relative low-cost fabrication, simple operation (yet rich switching dynamics), and a major intrinsic, layout-independent, variations in their switching characteristics. We have recently proposed a high-performance RRAM-based PUF architecture based on monolithically integrated 3D analog crossbar arrays and experimentally verified its robust performance in a large-scale study [2]. Our results indicate the immense potential of state tuning and harnessing conductance nonlinearity in analog crossbars for reconfigurable and secure security primitives. Herein, we present a test on true randomness generation of these PUFs entirely based on experimentally gathered response string of length of 352 kb. The test has a conventional part based on NIST's statistical test suite, and more deliberate evaluation of the PUF resilience against various model-building attacks using advanced deep learning models.

2. Analog RRAM-based PUF operation

A fully passive and monolithically integrated 2×10×10 TiO_{2-x} analog crossbars with an active device area of 350×350 nm^2 was employed for the RRAM-based PUF design (Fig. 1a). The top and bottom crossbars share a middle electrode. Full details on fabrication process can be found in [3]. Individual devices show a large dynamic range of resistance and an excellent *I-V* nonlinearity. While the analog crossbars show excellent uniformity in their switching and performance characteristics (Fig. 1b), the small spatial variations in resistance across the array can be used as an effective source of randomness.

To this end, our proposed PUF architecture (Fig. 1c) employs a selection scheme that generates 1-bit response based on differential comparison between currents passed through two sets of selected rows/columns, each includes sneak-path currents component through neighboring unselected devices. The aim is to implement an effective one-way function that incorporates array-scaled random spatial variations, thereby complicating many side-channel probing attacks, therefore

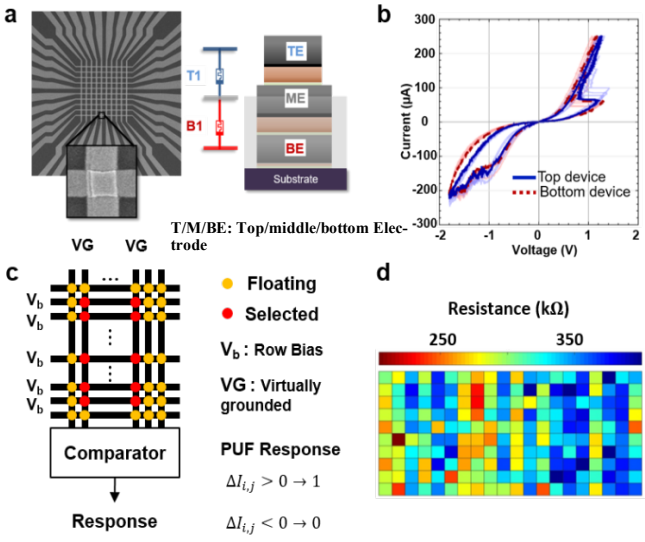

Fig 1. (a) Top-view scanning electron microscopy (SEM) image, equivalent circuit and cross-sectional schematic of the 3D stacked crossbar. (b) I-V curves for all 2×10×10 devices with two representative curves being highlighted. (c) PUF primitive operation scheme. (d) Example of the tuned crossbar.

Table I Machine learning test configuration and predictability.

Configuration	Training sequence length	Output dimension of	Predictability (%)
LSTM-Dropout-LSTM-Dense-Dense-Softmax	301	LSTM: 128, Dense: 128, 2	50.41
	101	LSTM: 128, Dense: 128, 2	50.52
	64	LSTM: 256, Dense: 256, 2	50.28

allows for more dependable operation. The significant difference between our RRAM PUF and a conventional CMOS-based PUF is the additional layout-independent variation in RRAMs. We extract this feature by varying applied bias, readout voltage, which employs device nonlinearity as an additional source of entropy [2]. To effectively combine the contribution of variation sources to the overall transfer function and avoid unintentional systematic biases, all devices in the array are programmed in a tight highly nonlinear range.

3. Evaluation of randomness

In Ref. [2], we have exhaustively evaluated the analog RRAM-based PUF against key PUF metrics of randomness and stability. Here, we investigate the degree of predictability and statistical randomness of the PUF response, utilizing a relatively large subset of the 1-bit responses at different biases (350 kb×5 for 5 different biases included in the network challenge).

Machine Learning Tests

We run predictive machine learning tests using long short-term memory (LSTM) architecture, a special case of recurrent neural network (RNN), capable of handling long-range dependencies in general purpose sequence modeling tasks [4, 5]. We have used three LSTM network configurations to test response sequences generated from the proposed PUF as shown in Table I. Dense is a fully connected layer which all nodes are connected to all output nodes of the previous layers, therefore, "Dense-Dense" configuration uses two dense layers. Dropout randomly chooses 50% of the previous layer's output nodes. Softmax here is the final layer of the network to obtain a vector of normalized probabilities

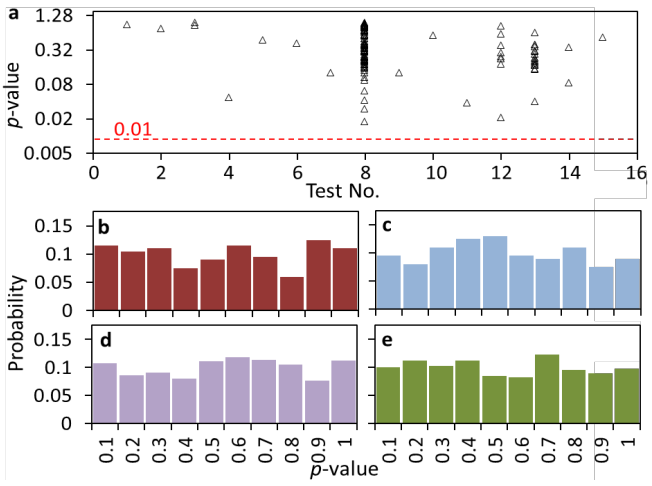

Fig 2. Histograms showing the uniformity of p-values obtained from (a) block-frequency, (b) longest run, (c) non-overlapping templates and (d) serial sub-tests.

across the output. The results show almost ideal level of unpredictability using three conditions for training sequence length and output dimension.

Statistical Tests

The NIST statistical randomness test suite is employed to further evaluate the random quality of the PUF response string. The test suite includes 17 different tests including two similar tests running on different directions of bit sequence. In each test, the sequence is interpreted as random if p-value is greater than significance level (α=0.01) [6]. The computed p-values and successful test results are shown in Fig. 2a. We statistically quantify the degree of randomness using 200×10 kb response sequences. Results then can be interpreted with (1) the proportion of sequences that pass the statistical test (proportion analysis) and (2) the distribution of p-values for uniformity (uniformity analysis). The proportion analysis results show the passing rate at 0.975 (lowest) from test number 15, Linear Complexity test, and 1.00 (highest) from test number 2, Block Frequency test. The distribution of p-values assessment is to ensure a uniformity, p-value$_T$. For p-value$_T$, if it is smaller than 0.0001, which is the significance level recommended for a uniformity test by NIST, p-values are considered as non-uniform. Figs. 2b-e demonstrate the histograms for the distributions of p-values, illustrating the successful uniformity results obtained for the device. Due to the space limitation, only 4 out of 15 results are demonstrated here.

4. Conclusions

We have investigated and verified randomness of our proposed analog 3D-RRAM PUF using two standard and advanced tests, and hence, demonstrated its resilience against a range of model building and machine learning attacks. We demonstrated near ideal unpredictability in our deep learning test using three different networks architectures and successful statistical evaluation using NIST statistical test suite with near uniform distribution of all p-values.

Acknowledgements

This work was supported by NSF CCF-1528250 and Australian Research Council (ARC) DP140103448.

References

[1] B. Gassend, et al., *Proc. ACM CCS'02* (2002) 148-160.

[2] H. Nili *et al.*, *arXiv preprints 1611.07946* (2016).

[3] G. C. Adam *et al.*, *46th European Solid-State Device Research Conference (ESSDERC)* (2016) 436-439.

[4] S. Hochreiter and J. Schmidhuber, *Neural Computation*, 9.8 (1997) 1735–1780.

[5] N. Srivastava *et al.*, *32nd International Conference on Machine Learning (ICML)* (2015) 843–852.

[6] L.E. Bassham III, *et al.*, Tech. Rep. (2010).