Predictive Analysis of 3D ReRAM-based PUF for Securing the Internet of Things

Jeeson Kim
School of Engineering
RMIT University
Melbourne, Australia
jeeson.kim@rmit.edu.au

Hussein Nili
Electrical and Computer Engineering
University of California Santa Barbara
Santa Barbara, USA
hnili@ece.ucsb.edu

Gina C. Adam
Electrical and Computer Engineering
University of California Santa Barbara
Santa Barbara, USA
gina_adam@engineering.ucsb.edu

Nhan Duy Truong
School of Engineering
RMIT University
Melbourne, Australia
nhanduy.truong@rmit.edu.au

Dmitri B. Strukov
Electrical and Computer Engineering
University of California Santa Barbara
Santa Barbara, USA
strukov@ece.ucsb.edu

Omid Kavehei
Electrical and Information Engineering
The University of Sydney
Sydney, Australia
omid.kavehei@sydney.edu.au

***Abstract*—In recent years, an explosion of IoT devices and its use leads threats to the privacy and security concerns of individual users and merchandises. As one of promising solutions, physical unclonable function (PUF) has been extensively studied. This paper investigates quality of randomness in the first generation of 3D analog ReRAM PUF primitives using measured and gathered data from fabricated ReRAM 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 attack. Experimental results verify near perfect (50%) predictability. It confirms the PUFs potentials for large-scale, yet small and power efficient, implementation of hardware intrinsic security primitives.**

***Index Terms*—hardware-intrinsic security primitives, Internet of Things, resistive random access memories, machine learning attacks**

I. Introduction

Internet of Things (IoT) products from wearables and implants to smart supply chain have brought paramount benefits into near all aspects of our life over the past few decades. Since the interconnected objects may be remotely accessed from the Internet, the accelerated pace of IoT adoption poses increased privacy and security concerns of individual users and merchandises [1]. As the typical IoT devices possess a lack of sophisticated computing capabilities, securing sensitive information between lightweight devices or between IoT device and trust center is an important but yet a difficult challenge [2, 3]. Widely used traditional cryptographic solutions, for example, advanced encryption standard (AES) and elliptic curve cryptography (ECC), can be used for both the integrity and the authentication of exchanging data and messages.

IoT hardware anti-counterfeiting, integrated circuit (IC) trust and physical tampering are also critical tasks [4]. In 2014, defense advanced research projects agency (DARPA) launched the supply chain hardware integrity for electronics defense (SHIELD) program solicits hardware root-of-trust for IC authentication which aims to be low-cost, energy-efficient, tiny size, resilience to threats, and fully-fledged solutions. [5]. Hardware security primitives such as physical unclonable function (PUF) and true random number generation (TRNG) have emerged as promising low-overhead security applications based on the inherent physical constraint of IoT devices [6].

In particular, PUF is relatively new breed of cryptographic primitives that gain an advantage of otherwise disadvantageous variation in physical system manufacturing with the aim to produce secrets that are unclonable [7]. 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 [8, 9]. 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 resistive random access memory (ReRAM) 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 suggested experimentally verified ReRAM PUF based on monolithically integrated 3D analog crossbar arrays and showed its robust performance in a large-scale study [10]. 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 kbits. The test has a conventional part based on National Institute of Standards and Technology (NIST) statistical test suite, and more deliberate evaluation of the PUF resilience against various model-building attacks using advanced deep learning models.

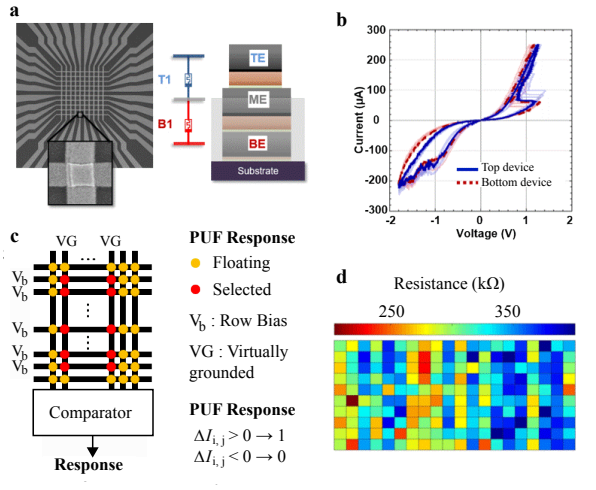

Fig. 1. (a) Top-view scanning electron microscopy (SEM) image, equivalent circuit and cross-sectional schematic of the 3D stacked crossbar. (b) Current-voltage (I–V) curves for all 2×10×10 devices with two representative curves being highlighted. (c) PUF primitive operation scheme. (d) Example of the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

II. Analog ReRAM-based PUF Operation

A fully passive and monolithically integrated $2\times10\times10$ TiO_{2-x} nm^2 was employed for the ReRAM-based PUF design (Fig. 1(a)). The top and bottom crossbars are accessible using top electrode (TE) and bottom electrode (BE), respectively, by sharing a middle electrode (ME). Full details on fabrication process can be found in Reference [11]. 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. 1(b), 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. 1(c)) 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 [12]. In this work, the PUF uses a selection scheme with 5 rows and 2 columns.

The aim is to implement an effective one-way function that incorporates array-scaled random spatial variations (Fig. 1(d)), thereby complicating many side-channel probing attacks, therefore, allows for more dependable operation. The significant difference between our ReRAM PUF and a conventional CMOS-based PUF is the additional layout-independent variation in ReRAMs. We extract this feature by varying applied bias, V_b of the lowest at 0.2 V to the highest at 0.6 V, which employs device nonlinearity as an additional source of entropy [10]. 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.

III. Evaluation of Randomness

In Reference [10], randomness and stability of the analog ReRAM-based PUF against key PUF metrics

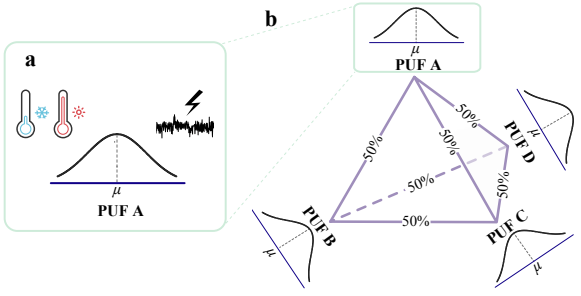

Fig. 2. Traditional PUF performance evaluations metrics. (a) represents intra-Hamming distance (HD) measuring stability of a PUF instance. (b) represents inter-HD showing PUF randomness measured across multiple PUF instances.

TABLE I
MACHINE LEARNING TESTS 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%

are exhaustively evaluated. The stability measures the robustness of a PUF against spatio-temporal variation which will ideally be represented as 0% (Fig. 2(a)), while ideal 50% randomness is the highest level of stochasticity across PUF instances (Fig. 2(b). 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 kbits $\times$ 5 for 5 different biases included in the network challenge). The PUF response sequence is subjected to two randomness evaluations including machine learning and statistical randomness tests.

A. 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 [13, 14]. In this work, we used three different LSTM network configurations tested on random number 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 across the output. The results show almost ideal level of unpredictability using three conditions for training sequence length and output dimension.

B. Statistical tests

The NIST statistical randomness test suite is employed to further evaluate the random quality of the PUF response string. NIST statistical test suit is an important measure for randomness analysis that is often adapted for formal randomness testing for various applications. The test suite includes 15 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 [15]. If the significance level α is too high or too low, then the test may result in *Type I* or *Type II* error, therefore, it is important to carefully design the significance level for the appropriate test setup.

The computed p-values and successful test results are shown in Fig. 3(a). With the significance level α at 0.01 (dotted red line), a PUF response sequence passes all 15 test (total 118 sub-tests).

We also statistically quantify the degree of randomness using 200×10 kbits response sequences. The empirical results then can be interpreted with two methods; (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 (the lowest) from test number 15, linear complexity test, and 1.00 (the highest) from test number 2, block frequency test. The distribution of p-values assessment is to ensure a uniformity, p-value$_{\mathrm{T}}$. For p-value$_{\mathrm{T}}$, 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. 3(b)-(e) demonstrate the histograms for the distributions of p-values, illustrating the successful uniformity results obtained for the device.

Table II shows the proportion analysis and uniformity analysis on the collected data with three different bias

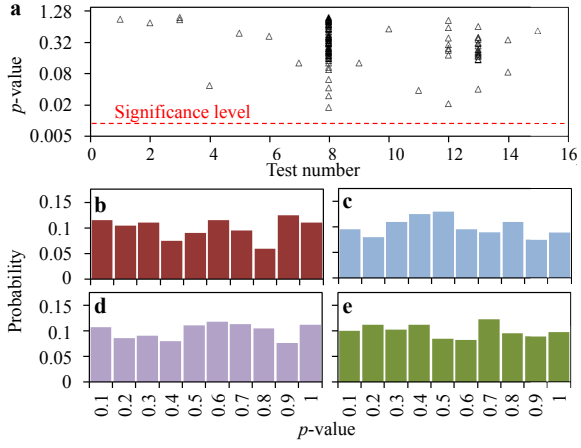

Fig. 3. NIST statistical test results. (a) shows a single sequence p-values of total 15 tests including different numbers of sub-tests, which are all greater than the selected significance level (α=0.01). Histograms showing the uniformity of p-values obtained from (b) block-frequency, (c) longest run, (d) non-overlapping templates and (e) serial sub-tests.

TABLE II
NIST STATISTICAL TEST RESULTS OF A PUF WITH THREE DIFFERENT BIAS VOLTAGES AT 0.2 V, 0.4 V AND 0.6 V.

	Bias voltage (V_b)		
	0.2 V	**0.4 V**	**0.6 V**
Mean rate of passing sequences	97.95%	98.04%	98.35%
Mean of uniformity (p-value$_T$)	0.16	0.19	0.19

voltages. In particular, the results show that increasing the bias voltage from 0.2 V to 0.6 V by 0.2 V increment improves the mean of passing rate from already high 97.95% to nearly ideal 98.35%. In another analysis, mean of uniformity (p-value$_T$) is well above 0.0001 for all cases. The slightly lower mean uniformity is found at lowest bias voltage of 0.2 V. The result indicates that the stronger I–V nonlinearity in the device attributes to the better PUF randomness at higher bias voltages. The feature could be beneficial since the bias voltage could be used as one of the independent challenge parameters and it also very useful against power monitoring attacks [10].

IV. CONCLUSION

In summary, we have investigated and verified randomness of our proposed analog 3D-ReRAM PUF using two standard and advanced tests, machine learning test and statistical test. Hence, we 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.

REFERENCES

[1] J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, 2014.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] C. M. Medaglia and A. Serbanati, "An overview of privacy and security issues in the Internet of Things," in *The Internet of Things*, 2010, pp. 389–395.

[4] K. Yang, D. Forte, and M. M. Tehranipoor, "Protecting endpoint devices in IoT supply chain," in *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2015, pp. 351–356.

[5] Defense Advanced Research Projects Agency (DARPA), Microsystems Technology Office/MTO Broad Agency Announcement, "Supply chain hardware integrity for electronics defense (SHIELD)," 2014.

[6] A. P. Johnson, R. S. Chakraborty, and D. Mukhopadhyay, "A PUF-enabled secure architecture for FPGA-based IoT applications," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 110–122, 2015.

[7] 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*, 2002, pp. 148–160.

[8] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proceedings of the 44th Annual Design Automation Conference*, 2007, pp. 9–14.

[9] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola *et al.*, "Design and implementation of PUF-based 'unclonable' RFID ICs for anti-counterfeiting and security applications," in *IEEE International Conference on RFID*, 2008, pp. 58–64.

[10] H. Nili, G. C. Adam, B. Hoskins, M. Prezioso, J. Kim *et al.*, "Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors," *Nature Electronics*, vol. 1, no. 3, pp. 197–202, 2018.

[11] G. Adam, H. Nili, J. Kim, B. Hoskins, O. Kavehei *et al.*, "Utilizing IV non-linearity and analog state variations in ReRAM-based security primitives," in *47th European Solid-State Device Research Conference (ESSDERC)*, 2017, pp. 74–77.

[12] J. Kim, T. Ahmed, H. Nili, J. Yang, D. S. Jeong *et al.*, "A physical unclonable function with redox-based nanoionic resistive memory," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 437–448, 2018.

[13] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[14] N. Srivastava, E. Mansimov, and R. Salakhutdinov, "Unsupervised learning of video representations using LSTMs," in *32nd International Conference on Machine Learning (ICML)*, 2015, pp. 843–852.

[15] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid *et al.*, "SP 800-22 Rev. 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications," Gaithersburg, MD, United States, Tech. Rep., 2010.