

Investigation of Entropy Space Affecting on Novel MLC-ReRAM Based PUF and System Level Optimization

Gyo Sub Lee^{1,2} and Hyunsu Ju^{1,2}

¹Post-Si Semiconductor Institute, Korea of Science and Technology (KIST)
Seoul, South Korea

²Nanomaterials Science and Engineering, Korea University of Science and Technology (UST)
Daejeon, South Korea

H16502@kist.re.kr; Hyunsuju@kist.re.kr

Extended Abstract

Resistive random access memory (RRAM) is a promising device for various applications such as memory, neuromorphic, random number generation and hardware security devices [1-4]. Especially, RRAM-based physical unclonable function (PUF) for hardware security application has been introduced in various literatures to overcome vulnerabilities [3]. The stochastic behaviour of the RRAM devices intrinsically offer excellent characteristics to realize the PUF during the conduction path formation and disconnection [5]. This stochastic variation leads to higher order randomness in each device than other conventional complementary metal oxide (CMOS) IC-based PUFs [6]. However, those RRAM-based PUFs still require large footprint to afford as numerous challenge response pairs (CRPs) as possible. Our novel reconfigurable multi-level cell (MLC) RRAM-based PUF is demonstrated by using a Pt/HfO₂/Ta/TiN device to overcome the limits mentioned earlier. The novel PUF basically utilizes quantization levels of the RRAM cell current distribution in advantage of the MLC characteristic. It can fully draw and utilize essential randomness of the RRAM devices due to maximization of cell-to-cell and cycle-to-cycle variation. Moreover, bit shuffling can enhance the randomness to improve the operation of the RRAM-based PUFs, which consequently enable to bring the uniqueness and the randomness of the PUFs to the ideal. Additionally, by these properties, our PUFs significantly increase complexity and a single RRAM cell can independently perform complete hardware security functions as a PUF device in our platform. In other words, an array of the RRAM-based PUF presented here can be considered a cluster of small PUF devices. Therefore, our PUF not only has large CRPs but also has less-footprint than other fingerprint method RRAM PUF consequently. In this paper, followed by prior study, the detailed investigation was performed on individual PUF cell to thoroughly disclose the characteristics and the advantages of the novel PUF system. We categorized 3 different RRAM cells with variant current distribution in each another and the difference and variance were evaluated by conversion to entropy space for quantitative analysis. As a result, we analysed the impact of entropy space on the uniqueness and the randomness of our PUFs. Moreover, we investigated the relationship between system parameters such as quantization level and response length and performance parameter such as uniqueness and randomness to optimize the PUF regardless of individual cell's entropy space.

Acknowledgments

This research was financially supported by Korea National Research Foundation Program, NRF-2017R1E1A1A01077484.

References

- [1] H.-S. P. Wong, et.al., "Metal-oxide RRAM," *Proceedings of the IEEE*, 2012, vol. 100, pp. 1951-1970.
- [2] L. Gao, et al, "Fully parallel write/read in resistive synaptic array for accelerating on-chip learning," *Nanotechnology*, vol. 26, p. 455204, 2015.
- [3] Y. Pang, H. Wu, B. Gao, N. Deng, D. Wu, R. Liu, S. Yu, A. Chen and H. Qian, "Optimization of RRAM-based physical unclonable function with a novel differential read-out method," *IEEE Electron Device Letters*, vol. 38, pp. 168-171, 2017.

- [4] S. Balatti, et al., "Physical unbiased generation of random numbers with coupled resistive switching devices," *IEEE Trans. Electron Devices*, vol. 63, no. 5, pp. 2029–2035, 2016.
- [5] S. Yu, X. Guan and H.-S. P. Wong, "Conduction mechanism of TiN/HfO_x/Pt resistive switching memory: A trap-assisted-tunneling model," *Applied Physics Letters*, vol. 99, p. 063507, 2011.
- [6] 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.