Proceedings of the 4th World Congress on New Technologies (NewTech'18)
Madrid, Spain – August 19 – 21, 2018
Paper No. ICNFA 117
DOI: 10.11159/icnfa18.117

Novel Multi-Level-Cell Resistive Random Access Memory based Reconfigurable Physical Unconable Functions Case

Gyo Sub Lee[1,2] and Hyunsu Ju[1,2]
[1]Post-Si Semiconductor Institute, Korea of Science and Technology (KIST)
Seoul, South Korea
[2]Nanomatarials Science and Engineering, Korea University of Science and Technology (UST)
Daejeon, South
H16502@kist.re.kr; Hyunsuju@kist.re.kr

Extended Abstract

Physical unclonable function (PUF) has been emerging as a commercialized technology in hardware security for highly secure systems and utilizes fabrication process variation and inherent randomness as a source of function. [1] Conventional complementary metal oxide semiconductor (CMOS) technology based PUFs have already been available on the market, but there are many obstacles to keep the system safe from various attacks due to their vulnerability toward model-and physical-attacks. [1-3] Therefore, to impede these attacks, various devices have been introduced so far - such as phase change memory (PCM), spin-transfer-torque magnetic random access memory (STT-MRAM), carbon-nanotube field effect transistors (CNFETs) and resistive random access memory (RRAM). [4] Especially, the RRAM based PUF is a promised device due to its strong stochastic behavior and intrinsic variability characteristics [5]. The various types of the RRAM PUF devices have been introduced to prove their feasibility for PUF application [4]. Those PUF devices demonstrated their capability enough to realize an ideal PUF and to prevent the attacks by presenting large challenge response pairs (CRPs) with relatively smaller area than CMOS PUF. Nevertheless, in order to obtain more sufficient and stronger CRPs, larger footprint is still required for the previously proposed RRAM based PUFs because they utilize the stored resistance states to create a single response bit. In addition, retention issue is critical to reliably maintain their CRP spaces under various environments such as ambient temperature variation. To overcome these problems, novel RRAM PUF is introduced to exploit the multi-level-cell (MLC) characteristic, one of the RRAM natures. Moreover, the MLC based RRAM PUF can enhance the tolerance toward the physical and model attacks as well due to its re-configurability. The MLC RRAM based PUF can maximize cycle-to-cycle and cell-to-cell variation to increase randomness of RRAM. The PUF proposed here can consequently increase the complexity in creation of CRPs and reduce the foot print of the PUF dramatically as well. The performance of PUF was evaluated by using uniqueness, randomness and bit error rate which satisfy ideally the expected value respectively.

References

[1] G. E. Suh, C. W. O'Donnell and S. Devadas, "AEGIS: A single-chip secure processor," *Information Security Technical Report*, vol. 10, no. 2, pp. 63-73, 2005.
[2] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson and S. Devadas, "PUF modeling attacks on simulated and silicon data," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1876-1891, 2013.
[3] C. Helfmeier, C. Boit, D. Nedospasov and J.-P. Seifert, "Cloning physically unclonable functions," in *Proc. IEEE Int. Symp. Hardw. Oriented Security Trust (HOST*), pp. 1-6, 2013.
[4] 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.
[5] S. Yu, X. Guan and H.-S. P. Wong, "Conduction mechanism of TiN/HfOx/Pt resistive switching memory: A trap assisted-tunneling model," *Applied Physics Letters*, vol. 99, p. 063507, 2011.