A Machine Learning Attack Resilient True Random Number Generator Based on Stochastic Programming of Atomically Thin Transistors

A. Wali[1], H. Ravichandran[2] & S. Das[2,3,4,*]

[1] Electrical Engineering, Penn State University, University Park, PA 16802

[2] Engineering Science and Mechanics, Penn State University, University Park, PA 16802

[3] Materials Science and Engineering, Penn State University, University Park, PA 16802

[4]Materials Research Institute, Pennsylvania State University, University Park, PA 16802

Abstract:

A true random number generator (TRNG) is a critical hardware component that has become increasingly important in the era of Internet of Things (IoT) and mobile computing for ensuring secure communication and authentication schemes. While recent years have seen an upsurge in TRNGs based on nanoscale materials and devices, their resilience against machine learning (ML) attacks remain unexamined. In this article, we demonstrate a ML attack resilient, low-power, and low-cost TRNG by exploiting stochastic programmability of floating gate (FG) field effect transistors (FETs) with atomically thin channel materials. The origin of stochasticity is attributed to the probabilistic nature of charge trapping and detrapping phenomena in the FG. Our TRNG also satisfies other requirements, which include high entropy, uniformity, uniqueness, and unclonability. Furthermore, the generated bit-streams pass NIST randomness tests without any post-processing. Our findings are important in the context of hardware security of resource constrained IoT edge devices, which are becoming increasingly vulnerable to ML attacks.