Physically Unclonable Functions with multi-states and Machine Learning

Bertrand Cambou, and Fatemeh Afghah
Northern Arizona University, Flagstaff, Arizona, USA

Abstract

When subject to natural effects such as aging, temperature changes, bias voltages drifts, or electrostatic interferences, the profile of the Physically Unclonable Functions (PUF) Challenge-Response-Pairs (CRPs) error rates is made predictable when analyzed by multi-states and a Machine Learning Engine (MLE). With the error correction selected, physical drifts do not result in false negative authentications (FNA), while statistically abnormal CRPs are flagged without increasing the risk of false positive authentications (FPA). PUFs that are hard to uncover by side channel analysis that would be normally weak without this architecture become excellent candidates due to a favorable compromise unclonability-strength to authenticate.