# Reliability and Entropy of Delay PUFs: A Theoretical Analysis

Alexander Schaub  Jean-Luc Danger  Sylvain Guilley  Olivier Rioul

Silicon *physically unclonable functions* (PUF) are used in various applications requiring robust authentication. The expected reliability of the PUF is crucial because the cryptographic key or identifier generated by the PUF should remain steady over its life period. So far, reliability was assessed empirically for all the silicon PUFs and is relatively poor for bit error rates (BER) greater than 4%. Therefore, it is necessary to enhance reliability by a post-processing stage using error correcting codes. However, there was no *predictive* model to characterize the raw reliability level of PUFs. Such a formal knowledge would be particularly useful for the designer to calibrate the post-processing complexity and compare different PUF architectures without having recourse to a costly silicon run.

In this work, we develop a predictive framework which enables us to derive a closed-form expression of both entropy and reliability for several families of delay PUFs: the RO PUF, the RO sum PUF as well as the Loop PUF. Improving these delay PUFs with bit-filtering, we can provide an explicit trade-off between complexity, reliability and entropy. Error rates about $10^{-9}$ or even lower can be achieved by this method. The theoretical results are validated by experiments on Loop PUFs implemented in 65 nm CMOS ASIC technology and simulations (using the Loop PUF results) of the RO sum PUF as well as the RO PUF. Measurements also show that the Gaussian hypothesis about the noise model should be refined for very low BER.