Cryptology ePrint Archive: Report 2011/657

A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions

Abhranil Maiti and Vikash Gunreddy and Patrick Schaumont

Abstract: In this work, we propose a systematic method to evaluate and compare the performance of Physical Unclonable Functions (PUFs). The need for such a method is justified by the fact that various types of PUFs have been proposed so far. However, there is no common method that can fairly compare them in terms of their performances. We first propose three generic dimensions of PUF measurements. We then define several parameters to quantify the performance of a PUF along these dimensions. We also analyze existing parameters proposed by other researchers. Based on our analysis, we propose a compact set of parameters that will be used as a tool to evaluate as well as compare the performance of different PUFs. To make the method independent of the underlying PUF technique, we focus on the statistical properties of the binary PUF responses. Finally, we show a detailed comparison analysis between two PUFs: ring-oscillator-based PUF (RO PUF) and Arbiter-based PUF (APUF) using measured PUF data.

Category / Keywords: Physical Unclonable Function, Challenge, Response, Ring Oscillator, Arbiter, Parameter, Performance

Date: received 4 Dec 2011

Contact author: abhranil at vt edu