Dummy rounds DPA countermeasure

Stanislav Jerabek, Martin Novotny
Czech Technical University, Prague, Czech republic

Abstract

This presentation describes novel Dummy rounds method which is DPA countermeasure for FPGA round cipher implementations. This countermeasure principle is inspired by several well–known countermeasures used in hardware but also in software implementations. The method especially combines hiding of power consumption with hiding in time and is also inspired by dynamic architecture reconfiguration. In this work are also discussed several ways of random number generator usage. RNG is crucial for the countermeasure method itself, but working with the numbers in a slightly different way could make the whole countermeasure much more efficient. Unfortunately, there are still no experimental results of the countermeasure method.