Leakage Squeezing Countermeasure Against High Order Attacks

Houssem Maghrebi, Jean-Luc Danger and Sylvain Guilley

Abstract

In the recent years, DPA attacks have been widely investigated. In particular, second order DPA (2O-DPA) have been improved and successfully applied to break many masked implementations. In this context we propose a new concept to hinder attacks of all order: instead of injecting more entropy, we make the most of a single-mask entropy. With specially crafted bijections instantiated on the mask path, we manage to reduce the inter-class variance (method we call "leakage squeezing") so that the leakage distributions become almost independent from the processed data. We decline this countermeasure in two implementation options. The first one is based on a recoded memory with a size squared w.r.t. the unprotected requirement, whilst the second one is an enhancement alleviating the requirement for a large memory. We theoretically prove the robustness of those implementations and practically evaluate their security improvements. This is attested by an 2O-DPA attack metric and robustness evaluation based on an information theoretic framework. As opposed to software-oriented 3O-DPA-proof countermeasure that seriously impact the performances, our is hardware-oriented and keeps a complexity similar to that of a standard 2O-DPA countermeasure with an almost untouched throughput, which is a predominant feature in computing-intensive applications.