Optimal CPA Attack

Michael Kasper[1] and Werner Schindler[2]

[1] Fraunhofer Institute for Secure Information Technology (SIT)
Rheinstraße 75
64295 Darmstadt, Germany
Michael.Kasper@sit.fraunhofer.de
[2] Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189
53175 Bonn, Germany
Werner.Schindler@bsi.bund.de

Abstract

The efficiency of a CPA attack depends on how the applied leakage model (e.g., the Hamming distance model) fits to the true leakage model of the targeted implementation.

We apply the stochastic approach to determine the optimal CPA for unprotected implementations with arbitrary leakage distributions. We provide both theoretical and experimental results. In our experiments we compare the attack efficiency of the optimal CPA attack with that of a 'standard' CPA attack. The standard CPA attack applies the Hamming distance model, which fits to the targeted implementations.

Our results quantify the advantage of the optimal CPA over standard CPA models. This advantage depends on the concrete implementation.