On the Optimality of Mutual Information Analysis for Discrete Leakages

Eloi de Chérisey, Annelie Heuser,
Sylvain Guilley and Olivier Rioul
Telecom ParisTech

Abstract

Recent works investigated mutual information analysis (MIA) as a generic distinguisher for which the attack does not require specific information about the leakage model of the attacked device. We give a theoretical proof that MIA can be optimal in the absence of profiling, in the sense that it maximizes the empirical likelihood estimated on line from the data with a specific prediction function when no specific information about the model is known. We recover the earlier result that a non-injective prediction function is required for success. We also propose new strategies for estimating conditional entropy and mutual information using fast algorithms with shared cumulative data counts. Finally, we investigate discrete leakage models and identify various optimal exploitation strategies. In one of them, it is proved that MIA outperforms CPA. Similar schemes can be relevant in the real world, such as web side-channels where transmitted packets' sizes and arrival times leak information.