When optimal means optimal

Finding optimal distinguishers from the mathematical theory of communication

Annelie Heuser[1], Olivier Rioul[1], Sylvain Guilley[1,2]

[1] TELECOM-ParisTech, COMELEC, Paris, FRANCE
[3] Secure-IC S.A.S., Rennes, FRANCE

We find mathematically optimal distinguishers in the context of side-channel key recovery for various scenarios through the modeling as a communication channel. Our methodology can be adapted to any given scenario (device, signal-to-noise ratio, noise distributions, leakage models, etc.). In the scenarios we investigated, all optimal distinguishers are novel, different from previous ones (Pearson correlation, mutual information, Kolmogorov-Smirnov test, etc.) even for Gaussian noise distributions, and empirically outperform all contestants. For example, for mono-bit leakage models, our optimal distinguisher outperforms the classical difference of means. When the model is known and the noise is Gaussian, the optimal distinguisher outperforms CPA and covariance. Moreover, we consider the scenario, when the model is imperfectly known, i.e., an unevenly weighted sum of the sensitive variable bits. In this case, our optimal distinguisher performs better than the classical linear regression analysis, which was known to be the best distinguisher so far in this scenario.