Template Attacks, Optimal Distinguishers and the Perceived Information Metric

Sylvain Guilley [1], Annelie Heuser [1],
Olivier Rioul [1], and François-Xavier Standaert [2]

[1] Telecom ParisTech

[2] Université catholique de Louvain

Abstract

Side-channel analysis is long known as a real threat on unprotected and even protected devices. While template attacks are admittedly the most powerful ones, most practical attacks are of a different kind, such as Kocher's difference of mean or correlation power analysis. It is the imprecision of the a priori leakage model that accounts for the discrepancy between theory and practice. A closer look into the mathematical expression of template attacks reveals conditions under which practical distinguishers may approach optimality. A metric aiming at quantifying the amount of leakage in an information-theoretic context has been recently put forward as the perceived information. We show that this metric also corresponds to the likelihood computed by a template attack using an imperfect model. We thus consolidate the published literature about optimal (template) attacks and optimal distinguishers by clarifying the state-of-the-art about the strongest side-channel adversarial strategies, with emphasis on the importance of the initial knowledge of the system under attack, which is typically accessed through profiling.