A Formal Practice-Oriented Model For The Analysis of Side-Channel Attacks

François-Xavier Standaert[1,2], Tal G. Malkin[1], Moti Yung[1,3]

[1] Dept. of Computer Science, Columbia University.
[2] UCL Crypto Group, Université Catholique de Louvain.
[3] RSA Laboratories.

e-mails: fstandae@uclouvain.be, tal,moti@cs.columbia.edu

Abstract. Formal models that allow one to understand side-channel attacks and are also directly meaningful to practice have been an open question. Motivated by this challenge, this work proposes a practice oriented framework for the analysis of cryptographic implementations against such attacks. It is illustratively applied to block ciphers, although it could be used to analyze a larger class of cryptosystems. The model is based on weak and commonly accepted hypotheses about side-channels that computations give rise to. It allows us to quantify the effect of practically relevant leakage functions with a combination of security and information theoretic metrics. From a practical point of view, the model suggests a unified evaluation methodology for side-channel attacks. From a theoretical point of view, it is shown that the suggested evaluation criteria correspond to the formal notion of security against side-channel key recovery. This work finally allows discussing the fundamental tradeoffs in side-channel attacks, namely flexibility *vs.* efficiency and information *vs.* computation.