# Evaluation Tools for Side-Channel Attacks: An Overview

François-Xavier Standaert*

UCL Crypto Group, Université catholique de Louvain.
Place du Levant 3, B-1348, Louvain-la-Neuve, Belgium.
e-mails: {fstandae}@uclouvain.be

Side-channel attacks are an important concern for the security of cryptographic implementations and their fair evaluation is a challenge for the certification of cryptographic products. In this survey, I will tackle the question of the best methods and tools for the objective evaluation of leaking devices, and discuss their limitations. For this purpose, I will first attempt to define a side-channel adversary in function of different ingredients, e.g.

1. *Measurement context*, i.e. can the adversary characterize the leakage distribution of his target device (in a profiled attack) or not (in a non-profiled attack)?
2. *I/O control of the device*, i.e. are the target device's inputs and outputs unknown to the adversary, known to the adversary or chosen by the adversary.
3. *Adversarial power*, i.e. what are the data complexity, time complexity, memory complexity and number of measurements that can be exploited to perform the attack?

Second, I will identify a number of target implementations according to two main criteria:

1. *Type of design*, e.g. unprotected implementation, implementation protected with data randomizations (aka masking), implementations protected with time randomizations (including shuffling of the operations and random process interrupts), implementations protected with hiding based on dual-rail logic styles, ...
2. *Type of leakage function*, according to the following features:
   (a) *Linearity*, i.e. does the leakage function's deterministic part have dominating linear dependencies in the manipulated data (or strong non-linear dependencies)?
   (b) *Noise distribution*, i.e. does the leakage function's non deterministic part follow a known (e.g. normal or multivariate normal) distribution?
   (c) *Variability*, i.e. do cryptographic devices designed in the same technology, from the same manufacturer, have identical leakage functions?

Taking the implementations of the AES Rijndael as a case study, I will then discuss which evaluation tools and metrics are best suited for the evaluation of different leaking devices. Doing so, I will also emphasize the relatively good understanding of so-called "univariate side-channel attacks" (in which the evaluation tools essentially exploit univariate statistics), and the more challenging nature of multivariate side-channel attacks, in particular in a non-profiled adversarial scenario. I will end this survey with general observations and recommendations, about (i) the need of profiled attacks in security evaluations, (ii) the importance of considering adversaries with sufficient time complexities, and (iii) the asymptotic equivalence (hence redundancy) of certain evaluation tools. Finally, and as a conclusion, a few open problems for the evaluation of side-channel attacks and their combination with classical cryptanalysis methods will additionally be spot.

* Associate researcher of the Belgian Fund for Scientific Research (FNRS-F.R.S.).