From Information Leakage to Rank Statistics in Side-Channel Attacks

Julien Béguinot and Olivier Rioul

Cryptarchi 2025

Abstract. In practical side-channel analysis, evaluators can estimate some key hypothesis rank statistics used as security indicators—e.g., arithmetic or geometric mean, median, α-marginal guesswork, or enumeration success rate. Yet, a direct estimation becomes time-consuming as security levels increase.

We provide new bounds on these figures of merit in terms of the mutual information between the secret and its side-channel leakages. These bounds provide theoretical insights on the evolution of the figures of merit in terms of noise level, computational complexity, and data complexity. Our results enable fast shortcut formulas for the certification laboratories, potentially enabling them to speed up the security evaluation process.

Joint work with Wei Cheng, Sylvain Guilley, Loïc Masure and François-Xavier Standaert.