Evaluation of Side-Channel Attacks Using Alpha-Information

Yi Liu[1], Wei Cheng[2], Sylvain Guilley[1,2], and Olivier Rioul[1]

[1]Télécom Paris, Institut Polytechnique de Paris, France
[2]Secure-IC, France

Mutual information as an information-theoretic tool has been frequently used in many security analyses. Chérisey et al. used Shannon information-theoretic tools to establish some universal inequalities between the probability of success of a side-channel attack and the minimum number of queries to reach a given success rate. α-information theory is a generalization of classic information-theoretic tools which seems more persuasive in a side-channel context. Such metrics include Rényi's α-entropy, α-divergence, Arimoto's conditional α-entropy, Sibson's α-information, etc.

In this work, we aim at extending the work of Chérisey et al. to α-information quantities depending on a parameter α. A conditional version of Sibson's α-information is defined using a simple closed-form expression. Our definition of conditional α-information satisfies important properties such as consistency, uniform expansion, and data processing inequalities, while other previous proposals do not satisfy all of these properties. Based on our proposal and a generalized Fano inequality, we extend the case $\alpha = 1$ of previous works to any $\alpha > 0$, and obtain sharp universal upper bounds for the probability of success of any type of side-channel attack. It turns out the bound is improved as α increases, and it is already very tight when $\alpha = 2$.