Defining Perceived Information based on Shannon's Communication Theory

Eloi de Cherisey, Sylvain Guilley, Olivier Rioul and Annelie Heuser

Télécom ParisTech, LTCI, CNRS,
Université Paris-Saclay, 75 013 Paris, France.
Email: `firstname.lastname@telecom-paristech.fr`

In order to improve the characterization of a side-channel attack in keeping with Shannon's communication theory, we attempt to elaborate and conciliate several notions such as mutual information and perceived information by means of an optimal side-channel distinguisher.

We first establish a rigorous definition of perceived information based on the distinguisher that is used to carry out the side-channel attack. We show that the correct definition varies according to the leakage's knowledge. Furthermore, we formalize the communication channel as a Markov chain and use data-processing inequalities to lower bound the number of traces required to retrieve the secret. Finally, we establish a link between Shannon's capacity and side-channel attacks, leading to novel criteria that can be used to determine whether the attack can be be successful or not.