Research Internship Proposal
Towards a Nonlinear Bound of Mutual Information Leakage for Additive-Masked Implementations

2024

Olivier RIoul
Télécom Paris, Institut Polytechnique de Paris

olivier.rioul@telecom-paris.fr

State of the Art

Cryptographic algorithms may leak some side information about the sensitive variables it manipulates through the so called side-channels. These leak can be of different natures, typically leakages includes timing leakages [1], micro-architectural leakages [2], electromagnetic leakages [3, 4] or even power consumption leakages [5]. The corresponding side-channel attacks can be very powerful and compromise the security of most cryptographic primitives if the proper countermeasures are not implemented.

The masking countermeasure is one of the main countermeasure since it provides provable security guarantees. In a masked implementations, every sensitive variable is split into several shares on which the computations are performed. As a consequence, the adversary obtains leakages on each shares independently. The adversary needs to recombine the leakages to recover the secret sensitive variable.

De Chérisey et al. [6] showed how the mutual information can be used to bound the number of measures required by a side-channel adversary to recover a targeted sensitive variable with a given level of confidence. Liu et al. [7] further showed that generalized version of mutual information (Sibson’s $\alpha$-information) can also be used in this perspective. Figure 1 illustrates the security bounds obtained with this approach.
Both De Chérisey et al. and Liu et al. rely on a "linear bound" where the informational metric grows linearly with the number of measurements. This process is called tensorization or single-letterization in information theory. This approach cannot be tight for a large number of measures because the informational metrics are bounded by the entropy of the secret. Hence the question: How can we improve the tensorization of the informational metrics in the side-channel evaluation setting?

De Chérisey [6] obtained a non-linear bound in the unprotected scenario (Fi-
Figure [2] which can serve a starting point. A first step will be to re-derive a similar non-linear bound in the protected scenario. Issa et al. [9] also improved the asymptotic tensorization of the informational metrics by connecting it to the Chernov exponent. Their results cannot be used as his since it applies at the limit, however their ideas could be used to improve further the non-linear tensorization of informational metrics.

**Organization**

In this internship, the student will:

1. establish a state of the art on tensorization of informational metric for side-channel analysis;
2. improve existing bounds to obtain a nonlinear bound of the informational leakage in terms of number of measurements;
3. validate numerically its approach and compare to the state of the art bounds.

**Miscellaneous Information**

— **Theme**: Side-Channel Analysis, Information Theory
— **Laboratoire**: LTCI, Télécom Paris, 91120 Palaiseau
— **Research Group**: Olivier Rioul and Julien Béguinot (PhD Student)

**Références**


