Research Internship Proposal

Understanding Perceived Information and Hypothetical Information for Side-Channel Attacks

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 leaks 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 countermeasures since it provides provable security guarantees. In a masked implementation, every sensitive variable is split into several shares on which the computations are performed. As a consequence, the adversary obtains leakages on each share 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.
Problem at Stake

To obtain practical security bounds, the informational metrics need to be estimated practically with real data that can be high dimensional. Renauld et al. [9] coined perceived information a plug-in estimator of mutual information for side-channel analysis. Because perceived information is usually a lower bound on mutual information, the resulting security bound can underestimate the required number of side-channel queries to recover a sensitive variable with a given level of confidence [10][11]. For this reason, Masure et al. [12] introduced the hypothetical information, an histogram-based estimator of mutual information that is guaranteed to upper bound mutual information. However, this estimator suffers from a curse of dimensionality making it unpractical in a high dimensional setting.

Therefore, an interesting open question is to find a mutual information estimator for side-channel analysis with a prescribed confidence that it does not underestimate the true value of mutual information. The link with the mutual information analysis, a mutual information-based distinguisher from the side-channel literature...
can also be made.

**Organization**

In this internship, the student will
1. establish a state of the art on perceived information and its variants;
2. find a positively biased estimator of mutual information with given confidence intervals;
3. benchmark the different estimators and compare them (neural evaluation, hypothetical information, perceived information,...) on real data.

**Miscellaneous Information**

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

**Références**


