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 α-information) can also be used in this perspective. Figure 1 illustrates the security bounds obtained with this approach.

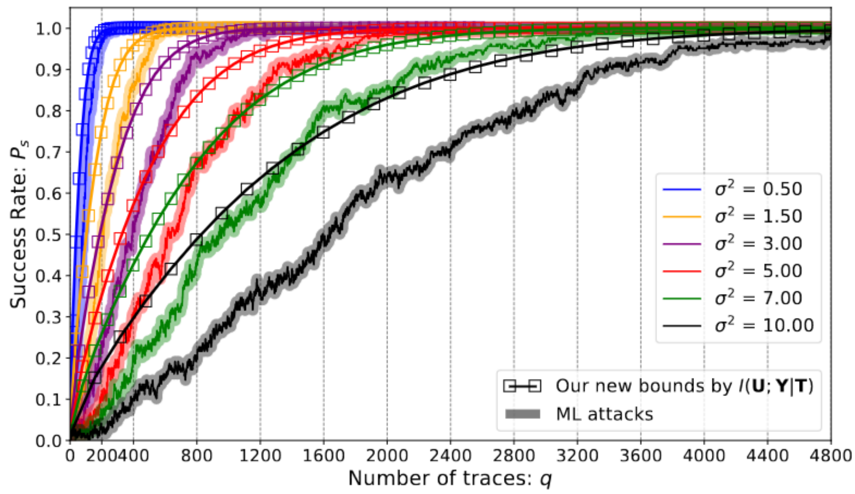

FIGURE 1 – Mutual Information Based Security Bound Extracted from [8]

Problem at Stake

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 ?

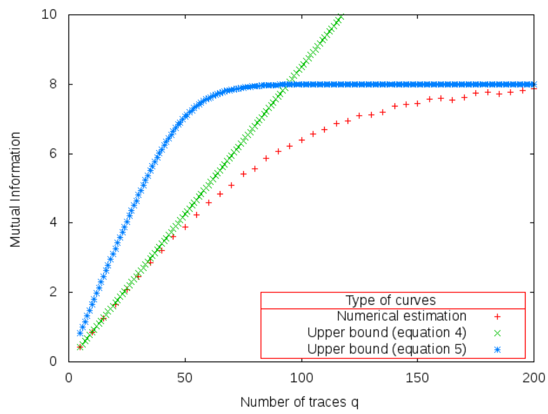

FIGURE 2 – De Chérisey Bounds on Mutual Information Extracted from [6]

De Chérisey [6] obtained a non-linear bound in the unprotected scenario (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

[1] Jean-François Dhem, François Koeune, Philippe-Alexandre Leroux, Patrick Mestré, Jean-Jacques Quisquater, and Jean-Louis Willems. A Practical Implementation of the Timing Attack. In Jean-Jacques Quisquater and Bruce Schneier, editors, *CARDIS*, volume 1820 of *Lecture Notes in Computer Science*, pages 167–182. Springer, 1998.

[2] Paul Kocher, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom. Spectre Attacks : Exploiting Speculative Execution. *CoRR*, abs/1801.01203, 2018.

[3] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi. The EM Side-Channel(s). In *CHES*, volume 2523 of *LNCS*, pages 29–45. Springer, 2002.

[4] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic Analysis : Concrete Results. In *CHES*, volume 2162 of *LNCS*, pages 251–261. Springer, May 14-16 2001. Paris, France.

[5] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In Michael J. Wiener, editor, *CRYPTO*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer, 1999.

[6] Éloi de Chérisey, Sylvain Guilley, Olivier Rioul, and Pablo Piantanida. Best Information is Most Successful — Mutual Information and Success Rate in Side-Channel Analysis. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2019(2) :49–79, 2019.

[7] Yi Liu, Wei Cheng, Sylvain Guilley, and Olivier Rioul. On conditional alpha-information and its application to side-channel analysis. In *IEEE Information Theory Workshop, ITW 2021, Kanazawa, Japan, October 17-21, 2021*, pages 1–6, 2021.

[8] Wei Cheng. *What can information guess ? : Towards information leakage quantification in side-channel analysis. (Qu'est ce que l'information permet de deviner ? : Vers une quantification des fuites d'informations dans l'analyse de canaux auxiliaires).* PhD thesis, Polytechnic Institute of Paris, France, 2021.

[9] Benjamin Wu, Aaron B. Wagner, G. Edward Suh, and Ibrahim Issa. Strong asymptotic composition theorems for sibson mutual information. In *IEEE International Symposium on Information Theory, ISIT 2020, Los Angeles, CA, USA, June 21-26, 2020*, pages 2222–2227. IEEE, 2020.