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 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.

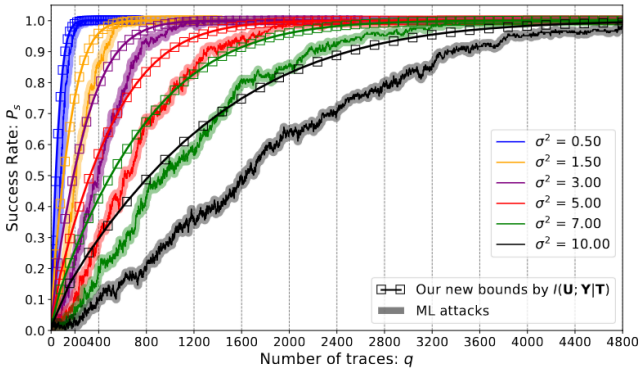

FIGURE 1 – Mutual Information Based Security Bound Extracted from [8]

Problem at Stake

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.

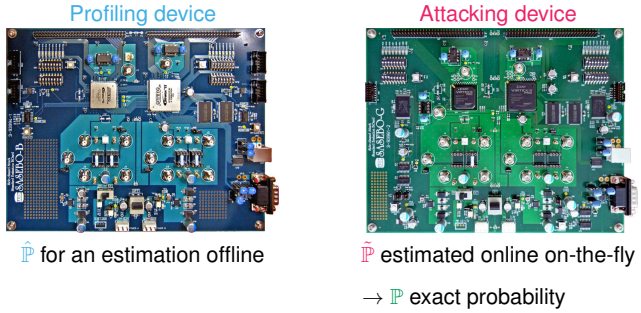

FIGURE 2 – Various Probabilistic Estimations in a Template Attack Setting

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.

Miscelaneous 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] Mathieu Renauld, François-Xavier Standaert, Nicolas Veyrat-Charvillon, Dina Kamel, and Denis Flandre. A formal study of power variability issues and side-channel attacks for nanoscale devices. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*, pages 109–128. Springer, 2011.

[10] Olivier Bronchain, Julien M. Hendrickx, Clément Massart, Alex Olshevsky, and François-Xavier Standaert. Leakage certification revisited : Bounding model errors in side-channel security evaluations. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part I*, volume 11692 of *Lecture Notes in Computer Science*, pages 713–737. Springer, 2019.

[11] Akira Ito, Rei Ueno, and Naofumi Homma. Perceived information revisited new metrics to evaluate success rate of side-channel attacks. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2022(4) :228–254, 2022.

[12] Loïc Masure, Gaëtan Cassiers, Julien M. Hendrickx, and François-Xavier Standaert. Information bounds and convergence rates for side-channel security evaluators. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2023(3) :522–569, 2023.