Lessons From the Past, Challenges for the Future

The Eurocrypt 2009 Evaluation Framework in the Deep Learning Era

François-Xavier Standaert* Tal G. Malkin† Moti Yung‡

March 30, 2022

Two decades after the publication of the first Differential Power Analysis (DPA) by Kocher et al. [KJJ99], the evaluation of side-channel attacks remains a topic of intense discussion, somewhat torn between the two main different approaches that can be considered for this purpose.

On the one hand, current *certification schemes* emerged from the urgent need to mitigate DPA and its numerous extensions. Without good formal solutions to prevent them, the industry first reacted by combining countermeasures with a certain level of security by obscurity. As a result, certification schemes have been established in order to try characterizing the "practical security" of a product based on different rating factors.[1] Yet, defining the practicality of an adversary is hard because practicality is a somewhat subjective notion which tends to change over time.

On the other hand, and in parallel, various research works promoted *worst-case attacks* as a natural way to limit the subjective nature of such certification schemes. By worst-case, we mean attacks where the adversary has a complete knowledge of the implementation details, and is allowed to learn its leakage behavior in an offline profiling phase with full access to the device's internal values. The Eurocrypt 2009 evaluation framework formalized this worst-case approach by putting forward a methodology based on two types of metrics: information theoretic metrics aimed to characterize the implementation leakage independent of the adversarial strategy; security metrics aimed to compare adversarial strategies for a given implementation leakage [SMY09]. This methodological contribution outlined a broad research agenda aimed at the connection of these metrics, their efficient estimation in practice and their use in physical security proofs.

To a large extent, these two approaches have so far been seen as mostly competing ones.

In this talk, we will first survey how research progresses have addressed some of the challenges raised by the Eurocrypt 2009 evaluation framework. This will lead us to recall the interest of both information theoretic and security metrics, and to discuss the need of sound profiling tools, the problem of verifying that the leakage characterization used in an evaluation is good enough and optimal information processing strategies. We will next focus on two of the main remaining open problems for side-channel security evaluators. Namely, the gap between certification schemes and worst-case attacks, and the issue of estimating complex (higher-order and multivariate) distributions. For this purpose, we will illustrate how recent machine learning algorithms have the potential to deal with complex distributions in a quite generic manner and under minimum assumptions. Doing so, we will show that they are easy to integrate in the same methodological framework

* Crypto Group, ICTEAM Institute, UCLouvain, Belgium.
† Columbia University, New York City, NY, USA.
‡ Google and Columbia University, New York City, NY, USA.
[1] https://iacr.org/workshops/ches/ches2016/presentations/CHES16-Tutorial1.pdf

as former profiled side-channel attacks and, to a large extent, share the same goals. As a result, they are also good candidates to understand the gap between current certification schemes and worst-case attacks: the quantification of which being an important scope for further investigations. We will then conclude by putting forward how worst-case security evaluations could be combined with certification in the quest for cryptographic implementations that can withstand side-channel attacks: first as part of the backwards evaluations proposed in [ABB+20]; more generally as a shortcut in order to efficiently anticipate attack paths that could appear in the long term, and by using certification to verify that the integration of well studied building blocks remains secure: the instantiation of such a constructive interaction being an important topic of discussion as well.

Acknowledgments. François-Xavier Standaert is a senior research associate of the Belgian fund for scientific research (FNRS-F.R.S.). Work funded in parts by the ERC project SWORD.

References

[ABB+20] Melissa Azouaoui, Davide Bellizia, Ileana Buhan, Nicolas Debande, Sébastien Duval, Christophe Giraud, Éliane Jaulmes, François Koeune, Elisabeth Oswald, François-Xavier Standaert, and Carolyn Whitnall. A systematic appraisal of side channel evaluation strategies. In *SSR*, volume 12529 of *Lecture Notes in Computer Science*, pages 46–66. Springer, 2020.

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *CRYPTO*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer, 1999.

[SMY09] François-Xavier Standaert, Tal Malkin, and Moti Yung. A unified framework for the analysis of side-channel key recovery attacks. In *EUROCRYPT*, volume 5479 of *Lecture Notes in Computer Science*, pages 443–461. Springer, 2009.