Practical vs. theoretical evaluation of DPA and CPA

Annelie Heuser, Sylvain Guilley and Olivier Rioul

TELECOM-ParisTech

Extended Abstract

Different side-channel distinguishers may have different efficiencies, however, their fair comparison is a difficult task, since many factors come into play. In particular, their intrinsic statistical properties and the quality of their estimation are significant factors. Apart from formulating a framework that can be carried out for various distinguishers [8, 10], several works concentrated on the evaluation of the efficiency of certain attacks individually.

More precisely, first works concentrated on finding a link between the Signal-to-noise ratio (SNR) of the power measurements and the effectiveness of the attack. E.g. in [5] the author presents a statistical model for CPA [1], finding an approximation of the success rate. An extension of this work has been given in [9]. While these works only focused on the correct key guess, Rivain first determined the exact success rate of CPA in [6] assuming an uniform setting in terms of the leakage model.

Recently, Fei et al. introduced a new methodology to evaluate side-channel distinguishers [2] giving the example of DPA [4]. Their approach consists in estimating the success rate of DPA due to the characterization of the physical implementation as well as the cryptographic algorithm. In particular, the authors provided an estimation of the success rate depending on the relationship between the correct and incorrect key hypothesis (named as *confusion*), the number of measurements and the SNR.

In this talk, we generalize the idea of [2], that has been restricted to the application of one-bit DPA, to any additive distinguishers and show an application to CPA. Moreover, given the generalized estimation results, we further highlight a new framework to classify distinguishers, which may close the gap between purely practical and purely theoretical evaluations.

References

1. Éric Brier, Christophe Clavier, and Francis Olivier. Correlation Power Analysis with a Leakage Model. In *CHES*, volume 3156 of *LNCS*, pages 16–29. Springer, August 11–13 2004. Cambridge, MA, USA.
2. Yunsi Fei, Qiasi Luo, and A. Adam Ding. A Statistical Model for DPA with Novel Algorithmic Confusion Analysis. In Emmanuel Prouff and Patrick Schaumont, editors, *CHES*, volume 7428 of *Lecture Notes in Computer Science*, pages 233–250. Springer, 2012.

3. Benedikt Gierlichs, Kerstin Lemke-Rust, and Christof Paar. Templates vs. Stochastic Methods. In *CHES*, volume 4249 of *LNCS*, pages 15–29. Springer, October 10-13 2006. Yokohama, Japan.
4. 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.
5. Stefan Mangard. Hardware Countermeasures against DPA – A Statistical Analysis of Their Effectiveness. In *CT-RSA*, volume 2964 of *Lecture Notes in Computer Science*, pages 222–235. Springer, 2004. San Francisco, CA, USA.
6. Matthieu Rivain. On the Exact Success Rate of Side Channel Analysis in the Gaussian Model. In *Selected Areas in Cryptography*, volume 5381 of *LNCS*, pages 165–183. Springer, August 14-15 2008. Sackville, New Brunswick, Canada.
7. François-Xavier Standaert, Philippe Bulens, Giacomo de Meulenaer, and Nicolas Veyrat-Charvillon. Improving the Rules of the DPA Contest. Cryptology ePrint Archive, Report 2008/517, December 8 2008. `http://eprint.iacr.org/2008/517`.
8. 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 *LNCS*, pages 443–461. Springer, April 26-30 2009. Cologne, Germany.
9. François-Xavier Standaert, Éric Peeters, Gaël Rouvroy, and Jean-Jacques Quisquater. An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays. *Proceedings of the IEEE*, 94(2):383–394, February 2006. (Invited Paper).
10. Carolyn Whitnall and Elisabeth Oswald. A Fair Evaluation Framework for Comparing Side-Channel Distinguishers. *J. Cryptographic Engineering*, 1(2):145–160, 2011.