The “Rank Correction” Technique to Improve Side-Channel Attacks

Maxime Nassar[1,2], Youssef Souissi[1], Sylvain Guilley[1] and Jean-Luc Danger[1].

[1] Institut TELECOM / TELECOM ParisTech, CNRS LTCI (UMR 5141),
46 rue Barrault
75 634 Paris Cedex, France.
[2] Bull TrustWay
Rue Jean Jaurès, B.P. 68
78 340 Les Clayes-sous-Bois, France.

***Abstract*—Side-channel analysis (SCA) is a technique to recover secrets concealed in embedded systems. They exploit unintentional physical leakage, such as the power consumption or the radiated magnetic field. Since the initial publication of the differential power analysis in 1998, the theoretical tools to conduct SCAs have been much refined. Notably, through adequate evaluation frameworks (typically that of F.-X. Standaert et al. [10]), the attacks have been formally described in two independent steps.**

1) **A partitioning of the side-channel observations, which depends on the scenario (known/chosen plaintext/ciphertext), on the algorithm (to explore the internal rounds by guessing manageable parts of the secret), and on the implementation (whether it is software or hardware, pipelined or unrolled, protected or not, etc.)**
2) **A distinguisher that select the most relevant partitionings, amongst all the secret hypotheses. The distinguisher is basically a statistical tool, that aims at putting forward any bias. They can be for instance a difference of means [6], a covariance [4], a correlation (linear [1] or rank-based [5]), a mutual information [2] or a variance [7], [9].**

Some studies suggest that all distinguishers are equivalent asymptotically [8] (*i.e.* they are sound), and that they differ only by statistically artifacts that are data-dependent. However, in concrete operational cases, the goal is clearly to find some ways to accelerate the attack, taking into account that the scarce resource is the number of measurements. Some papers compare some distinguishers between them, and conclude about their difference of efficiency [9]. Interesting results [3] show that some distinguishers are better for the first order success rate and that others are better for the guessing entropy.

Nonetheless, few papers have tried to combine the distinguishers to improve the attack. In this paper, we explore the principle of taking advantage of the existence on various distinguishers. Our approach is deliberately partitioning-independent. Instead, we base our attack improvement on the fact that the plurality of sound distinguishers can be seen as redundant noisy estimates about the secret to recover. Thus we devise a rank correction attack methodology to boost the attack’s speed. One interesting point in our approach is that it is distinguisher agnostic, and that it works optimally when each unitary distinguishers performs about the same. Indeed, when one distinguisher is much better than the others, the proposed collaboration has less impact on the attack success. We illustrate our methodology on an unprotected implementation of DES using the first order success rate as a merit factor.

***Index Terms*—Side-channel analysis, distinguishers, comparison, success rate, rank correction.**

References

[1] É. Brier, C. Clavier, and F. 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] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel. Mutual information analysis. In *CHES, 10th International Workshop*, volume 5154 of *Lecture Notes in Computer Science*, pages 426–442. Springer, August 10-13 2008. Washington, D.C., USA.

[3] B. Gierlichs, E. De Mulder, B. Preneel, and I. Verbauwhede. Empirical comparison of side channel analysis distinguishers on DES in hardware. In IEEE, editor, *ECCTD. European Conference on Circuit Theory and Design*, pages 391–394, August 23-27 2009. Antalya, Turkey.

[4] S. Guilley, L. Sauvage, J.-L. Danger, N. Selmane, and R. Pacalet. Silicon-level solutions to counteract passive and active attacks. In *FDTC, 5th Workshop on Fault Detection and Tolerance in Cryptography, IEEE-CS*, pages 3–17, Washington DC, USA, aug 2008. (Up-to-date version on http://hal.archives-ouvertes.fr/HAL: http://hal.archives-ouvertes.fr/hal-00311431/en/).

[5] P. Karsmakers, B. Gierlichs, K. Pelckmans, K. D. Cock, J. Suykens, B. Preneel, and B. D. Moor. Side channel attacks on cryptographic devices as a classification problem. ftp://ftp.esat.kuleuven.ac.be/pub/SISTA/decock/reports/07-36.pdf.

[6] P. C. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In *Proceedings of CRYPTO’99*, volume 1666 of *LNCS*, pages 388–397. Springer-Verlag, 1999. (PDF).

[7] H. Maghrebi, J.-L. Danger, F. Flament, and S. Guilley. Evaluation of Countermeasures Implementation Based on Boolean Masking to Thwart First and Second Order Side-Channel Attacks. In *SCS*, IEEE, pages 1–6, November 6–8 2009. Jerba, Tunisia. Complete version online: http://hal.archives-ouvertes.fr/hal-00425523/en/. DOI: 10.1109/ICSCS.2009.5412597.

[8] S. Mangard, E. Oswald, and F.-X. Standaert. One for All - All for One: Unifying Standard DPA Attacks. Cryptology ePrint Archive, Report 2009/449, 2009. http://eprint.iacr.org/.

[9] F.-X. Standaert, B. Gierlichs, and I. Verbauwhede. Partition vs. Comparison Side-Channel Distinguishers: An Empirical Evaluation of Statistical Tests for Univariate Side-Channel Attacks against Two Unprotected CMOS Devices. In *ICISC*, volume 5461 of *LNCS*, pages 253–267. Springer, December 3-5 2008. Seoul, Korea.

[10] F.-X. Standaert, T. Malkin, and M. 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, April 26-30 2009. Cologne, Germany.