Towards Fair and Efficient Evaluations of Leaking Cryptographic Devices

- Overview of the ERC Project CRASH, Part I - (*Invited Talk*)

François-Xavier Standaert

ICTEAM Institute, Crypto Group,
Université catholique de Louvain, Belgium.

e-mail: fstandae@uclouvain.be

Extended abstract. Side-channel analysis is an important concern for the security of cryptographic implementations, and may lead to powerful key recovery attacks if no countermeasures are deployed. Therefore, various types of protection mechanisms have been proposed over the last 20 years. In view of the cost and performance overheads caused by these protections, their fair evaluation is a primary concern for hardware and software designers. Yet, the physical nature of side-channel analysis also renders the security evaluation of cryptographic implementations very different than the one of cryptographic algorithms against mathematical cryptanalysis. That is, while the latter can be quantified based on (well-defined) time, data and memory complexities, the evaluation of side-channel analysis additionally requires to quantify the informativeness and exploitability of the physical leakages. This implies that a part of these security evaluations is inherently heuristic and dependent on engineering expertise.

The development of sound tools allowing designers and evaluation laboratories to deal with this challenge was one of the main objectives of the CRASH project funded by the European Research Council. In this talk, I will survey a number of results we obtained in this direction, starting with concrete evaluation methodologies that are well-adapted to the investigation of current embedded devices, and following with emerging trends for future implementations. Quite naturally, a large number of researchers and teams have worked on similar directions. For each of the topics discussed, I will add a couple of references to publications that I found inspiring/relevant. The list is (obviously) incomplete and only reflects my personal interests. I apologize in advance for omissions.

1. Concrete evaluation methodologies. Side-channel analyses against cryptographic implementations can be viewed as a combination of several informal steps, next denoted as *measurement & pre-processing*, *prediction & modeling*, *exploitation* and *post-processing*. They can also be classified based on the adversarial capabilities. In particular, the literature generally suggests two important categories of attacks, namely *profiled attacks* (where the adversary can use a device he fully controls – meaning including the secret key and possibly randomness – in order to gain understanding of the target implementation leakages) and *non-profiled attacks* (where the adversary can only access a target device holding the secret key to recover). In this respect, our results are as follows.

A. The profiling separation. In practice, non-profiled attacks can be viewed as more realistic, since adversaries do not always have access to a profiling device. Therefore, a fundamental question regarding the evaluation of leaking devices is whether performing non-profiled attacks only is sufficient to state sound conclusions regarding susceptibility to side-channel analysis. We answered this question negatively in [69]. Defining a *generic strategy* as one which is able to recover secret information from side-channel leakages without any a-priori assumption about the target devices' physical characteristics, we showed that (strictly defined) such strategies cannot succeed in general. This implies that there exist devices (leakage characteristics) which can only be evaluated soundly by performing profiled attacks. Yet, we also showed that a minor relaxation of the strict definition of generic strategies, incorporating non-device-specific-intuitions, produces *generic-emulating strategies* able to succeed against a wide range of targets (an approach that we followed in [66]). Hence, these results suggest profiled attacks as the method of choice for side-channel security evaluations, since (*i*) they are strictly necessary, (*ii*) they lead to a better understanding of the leakage characteristics and (*iii*) they allow worst-case complexity estimates (which non-profiled adversaries can usually approach with generic-emulating strategies).

`Related works.` The COSADE 2014 paper by Reparaz et al. offers a critical view of this separation and discusses its impact in practical scenarios [55].

B. The heuristic vs. optimal separation. Based on the previous four (informal) steps, another important question regarding the evaluation of leaking devices is whether one can guarantee that (at least some of) these steps are optimal. Following the standard cryptographic approach, a perfectly sound evaluation indeed requires to determine the worst-case attack complexities, which implies to consider the most powerful adversaries (and again suggests profiled attacks are preferable for this purpose). But in view of the physical nature of the attacks, theoretical guarantees of optimality seem hard to reach. Interestingly, we could show that excepted for the measurement and pre-processing step of the attacks (which is indeed inherently heuristic), it is possible to guarantee that the other steps are "close enough to optimal" (or optimal), as we discuss next.

Step 1. Measurement & pre-processing. This step typically includes the design of low-noise Printed Circuit Boards (PCBs) and probes, *filtering* the measurements, *dimensionality reduction* and the *detection of Points of Interest* (POIs) in leakage traces. As just mentioned, such tasks are essentially heuristic and highly depend on engineering skills. In this respect, it is important to note that even without guarantees of optimality, it is always possible to compare two solutions for the measurement and pre-processing of the leakages, using the other attack/evaluation steps described next. Public – ideally open source – measurement platforms are an interesting ingredient for this purpose. Quite naturally, the same holds for statistical signal processing and machine learning tools. As part of the CRASH project, we paid attention to filtering with Singular Spectrum Analysis [48], projection pursuits as an alternative to Principal Component Analysis (PCA [1]) and Linear Discriminant Analysis (LDA [59]) for dimension-

ality reduction / detection of POIs in side-channel attacks [22], improved *leakage detection tests* based on a simple partitioning of the side-channel measurements for fast (yet preliminary) security assessment [19], and the removal of random delays from software implementations using hidden Markov models [18].

`Related works.` [39, 58] for leakage detection, [11, 35, 2, 36] for concrete issues in the application of side-channel attacks and [10] for dimensionality reduction.

Step 2. Prediction & modeling. Given some public input X to the target device, a secret parameter K and the physical leakages L, most side-channel attacks require an estimation of the conditional probability distribution $\hat{\Pr}[K|X, L]$ (or a simplification of this distribution to some of its moments), usually denoted as the model. This is an essential step of the security evaluations that highly relates to the previously mentioned separation between non-profiled and profiled attacks. More precisely, fair evaluations ideally require exploiting a perfect leakage model (to extract all the available information). But since such perfect models are generally unknown, density estimation techniques have to be used to approximate the leakage distribution. This raises the fundamental problem that all security evaluations are potentially biased by both estimation and assumption errors. At Eurocrypt 2014, we proposed first *leakage certification tools* allowing evaluators to verify that their models are good enough [21]. That is, while knowing the distance between an estimated model and the optimal one is impossible in general, it is possible to verify that given number of leakages available for evaluation, any improvement of the (possibly imperfect) estimated model will be negligible. Technically, this requires checking that given this number of leakages, the model assumption errors are small enough in front of the model estimation errors, which amounts to test the hypothesis that the model is correct. At CHES 2016, we then described simpler leakage certification tools, which came at the cost of a couple of heuristic assumptions on the leakage distributions [20].

`Related works.` A complementary issue to leakage certification is templates portability / robust profiling [23, 12, 67]. Note that nothing prevents using certification tools to test a model built with one device against another device.

Step 3. Exploitation. Given a leakage model $\hat{\Pr}[K|X, L]$, most side-channel analyses are based on a divide-and-conquer strategy. In this context, the optimal solution is easy to implement and just corresponds to *maximizing the likelihood* of the key (bytes) given the observed leakages, which is the standard approach for profiled attacks. Interestingly, we could show that in the context of unprotected implementations, several of the published distinguishers are in fact equally efficient to perform key recovery attacks [37, 14]. By contrast, in the case of implementations protected with *masking* or *shuffling*, only the Bayesian (maximum likelihood) distinguisher guarantees optimal results [60, 64].

Besides, an alternative and (theoretically) more powerful strategy to perform key recoveries based on physical leakages is to consider *analytical attacks*. The first (algebraic) attempts in this direction were generally limited in their applicability because of their low tolerance to measurement noise [52, 53]. As part of the CRASH project, we developed new solutions to better deal with this

noise limitation, based on alternative descriptions of the key recovery problem as optimization or soft decoding problems [45, 63]. The latter one is particularly relevant to evaluation laboratories since it can deal with any level of noise, and exhibits a constant improvement over divide-and-conquer attacks [27].

`Related works.` Multi-target attacks can be viewed as an alternative between simple (single-target) divide-and-conquer attacks and anaytical ones [40].

Step 4. Post-processing. The outcome of a divide-and-conquer attack is typically shaped as lists of probabilities or scores for each of the target key bytes. If this outcome is such that the correct key byte is always rated first, then the attack is directly successful (which happens when a sufficient amount of measurements is available to the adversary). If not, the adversary can trade measurements for time and perform *key enumeration*, which allows testing whether the correct key is within reach given his computational power. Our first contribution in this direction was an optimal key enumeration algorithm published at SAC 2012 [61]. One possible limitation of key enumeration is that in case the result of the enumeration is negative (i.e., the key is not recovered), it does not provide any hint about the computational security of the key: is it close to computational reach (e.g., with rank 2^{45} while we performed enumeration up to rank 2^{40}) or close to a standard cryptographic key sizes (e.g., $2^{80} - 2^{100}$)? In order to deal with this issue, we introduced a first *key rank estimation* algorithm allowing "security evaluations beyond computing power" at Eurocrypt 2013 [62]. Following these initial works, we then proposed much simplified algorithms for both key enumeration and rank estimation. More precisely, in a FSE 2015 paper we showed that is it possible to estimate the rank of a block cipher key with very tight bounds (e.g., with less than one bit of accuracy) almost instantaneously, using simple tools such as histograms and convolutions [26]. In a CHES 2016 paper, we then extended the use of these tools to a key enumeration algorithm that is parallelizable and allows easy distribution of the key testing among various hardware and software computing platforms [47]. In a complementary line of work, we finally discussed the pros and cons of various approaches to rank estimation, together with the efficiency gains that can be obtained by replacing the previous approximations by simple(r) bounds based on easier-to-estimate metrics [46]. In the same paper, we again put forward the interest of a (profiled) probabilistic approach to allow the optimal post-processing of the attack outcomes.

`Related works.` [6] presents an alternative (similarly efficient) key ranking algorithm. [38] proposed the first parallel key enumeration algorithm.

Wrapping up & cautionary note. The previous separation results allow a better understanding of the necessary steps in side-channel security evaluations, together with a systematic view of the possible sources of sub-optimality which may lead evaluators to over-estimate the security of their implementations. For Steps 2, 3 and 4, we additionally provided tools allowing them to avoid such a false sense of security. These tools typically allow evaluators to estimate *security graphs* (i.e., plots of the attacks success rate in function of their measurement and time complexity) for any implementation. Yet, and despite these progresses, it is

important to note that all concrete security evaluations remain highly dependent on measurements and & pre-processing. That is, if an adversary/evaluator does a selection of POIs that ignores critical information, or does not filter a parasitic frequency and models it as noise, the next evaluation steps will not be able to correct this. Hence, and quite naturally, such a more established methodology has to be combined with continuous progresses in order to develop tools able to capture increasingly protected implementations, for which the exploitation of the leakages may require to deal with high-dimensional and high-order statistics. Finding solutions allowing adversaries/evaluators to deal with such complex settings is an important scope for further research on side-channel analysis.

`Related works.` [41, 5] illustrate that high-dimensions and high-order attacks become increasingly important as implementations become better protected.

2. Future trends. One emerging drawback of the concrete approaches to physical security evaluations is that they are essentially based on mounting attacks (or detecting biases). Yet, and as security levels increase, their direct evaluation with sufficient statistical confidence will soon become untractable. For example, think about an implementation that guarantees a computational security of 2^{80} after the observation of 2^{80} measurements. In order to evaluate its security, we foresee two trends that we illustrate with the masking countermeasure.

A. Exploiting (tight) proofs. The (measurement) security of a masked implementation theoretically increases exponentially with the number of shares, given that the leakage of each share is sufficiently noisy and independent. In practice, it means that if a designer is able to quantify this noise condition and guarantee independence, he can evaluate the security of a masked implementation by evaluating the leakage of a single share (which is roughly as easy as evaluating an unprotected implementation) rather than that of their combination (a task for which the complexity is exponential in the number of shares). A seed result in this direction was published at Eurocrypt 2015 [16, 17]. We believe that evaluations based on tight proofs will be increasingly relevant in the future.

`Related works.` Models to analyze masked implementations include the probing model and the noisy leakage model [31, 51]. In a very important piece of work, Duc et al. showed probing security implies noisy leakage security (under some conditions discussed in the paper) [15]. Simplified tools allowing faster security evaluations but specialized to certain popular distinguishers include [13, 34].

B. Security without obscurity. A positive artifact of masked (serial) implementations is that the number of POIs that have to be identified by an adversary also increases exponentially with the number shares. Yet, contrary to the noise condition that guarantees high measurement complexity, these POIs are typically a long-term secret that depend on the adversarial knowledge about the implementation. A single leak of this secret (e.g., the implementation source code) may completely annihilate its impact. In this respect, it is naturally advisable to design security mechanisms that are not based on such hard to quantify secrets, but only on a sound combination of reproducible (empirically verifiable) physical

assumptions and mathematical amplification. Since security without obscurity is also the best (and probably only) setting in which security proofs can be established, we believe it will also become increasingly relevant in the future.

Other results. For completeness, we list a number of other results related to the fair evaluation of side-channel attacks obtained during the CRASH project. First, we used our tools and methodology to evaluate the impact of technology scaling on the side-channel resistance of cryptographic implementations, e.g., variability [54] and static leakages [49]. Second, we analyzed (pseudo) generic distinguishers in [3, 65], which are typical candidate tools to manipulate high-dimension and high-order leakages. Third, we investigated collision attacks as an alternative path between divide-and-conquer and analytical attacks [24].

`Other related works.` The exploitability of static leakages in side-channel analysis was first put forward in [42]. The Kolmogorov-Smirnov test has been studied in [68] as an alternative (pseudo) generic distinguisher. There is a wide literature on side-channel collision attacks. Recent examples include [43, 7]. Finally, and in a recent line of papers, standard side-channel distinguishers have been revisited thanks to a theoretical framework where the leakage function is fixed (i.e., in a so-called simulated attack setting). This brings a complementary view to the concrete setting where most of the efforts are put on finding the right leakage model, and a maximum likelihood strategy is applied afterwards. The authors showed that as long as the assumed leakage function is close to the ones observed in practice, the standard distinguishers / dimensionality reductions previously proposed in the literature are indeed close to optimal [29, 9, 8].

Acknowledgements. François-Xavier Standaert is a research associate of the Belgian Fund for Scientific Research (F.R.S.-FNRS). This work has been funded in part by the European Commission through the ERC project 280141. The author is highly grateful to the SPACE 2016 organizers for inviting him to give this talk, and allowing him to amortize the load of his final project report.

References

1. Cédric Archambeau, Eric Peeters, François-Xavier Standaert, and Jean-Jacques Quisquater. Template attacks in principal subspaces. In Louis Goubin and Mitsuru Matsui, editors, *Cryptographic Hardware and Embedded Systems - CHES 2006, 8th International Workshop, Yokohama, Japan, October 10-13, 2006, Proceedings*, volume 4249 of *Lecture Notes in Computer Science*, pages 1–14. Springer, 2006.
2. Josep Balasch, Benedikt Gierlichs, Oscar Reparaz, and Ingrid Verbauwhede. DPA, bitslicing and masking at 1 GHz. In Güneysu and Handschuh [28], pages 599–619.
3. Lejla Batina, Benedikt Gierlichs, Emmanuel Prouff, Matthieu Rivain, François-Xavier Standaert, and Nicolas Veyrat-Charvillon. Mutual information analysis: a comprehensive study. *J. Cryptology*, 24(2):269–291, 2011.
4. Lejla Batina and Matthew Robshaw, editors. *Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings*, volume 8731 of *Lecture Notes in Computer Science*. Springer, 2014.

5. Alberto Battistello, Jean-Sébastien Coron, Emmanuel Prouff, and Rina Zeitoun. Horizontal side-channel attacks and countermeasures on the ISW masking scheme. In Gierlichs and Poschmann [25], pages 23–39.
6. Daniel J. Bernstein, Tanja Lange, and Christine van Vredendaal. Tighter, faster, simpler side-channel security evaluations beyond computing power. *IACR Cryptology ePrint Archive*, 2015:221, 2015.
7. Andrey Bogdanov and Ilya Kizhvatov. Beyond the limits of DPA: combined side-channel collision attacks. *IEEE Trans. Computers*, 61(8):1153–1164, 2012.
8. Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, Damien Marion, and Olivier Rioul. Less is more - dimensionality reduction from a theoretical perspective. In Güneysu and Handschuh [28], pages 22–41.
9. Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, and Olivier Rioul. Masks will fall off - higher-order optimal distinguishers. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II*, volume 8874 of *Lecture Notes in Computer Science*, pages 344–365. Springer, 2014.
10. Eleonora Cagli, Cécile Dumas, and Emmanuel Prouff. Enhancing dimensionality reduction methods for side-channel attacks. In Homma and Medwed [30], pages 15–33.
11. Omar Choudary and Markus G. Kuhn. Efficient template attacks. In Aurélien Francillon and Pankaj Rohatgi, editors, *Smart Card Research and Advanced Applications - 12th International Conference, CARDIS 2013, Berlin, Germany, November 27-29, 2013. Revised Selected Papers*, volume 8419 of *Lecture Notes in Computer Science*, pages 253–270. Springer, 2013.
12. Omar Choudary and Markus G. Kuhn. Template attacks on different devices. In Prouff [50], pages 179–198.
13. A. Adam Ding, Liwei Zhang, Yunsi Fei, and Pei Luo. A statistical model for higher order DPA on masked devices. In Batina and Robshaw [4], pages 147–169.
14. Julien Doget, Emmanuel Prouff, Matthieu Rivain, and François-Xavier Standaert. Univariate side channel attacks and leakage modeling. *J. Cryptographic Engineering*, 1(2):123–144, 2011.
15. Alexandre Duc, Stefan Dziembowski, and Sebastian Faust. Unifying leakage models: From probing attacks to noisy leakage. In Nguyen and Oswald [44], pages 423–440.
16. Alexandre Duc, Sebastian Faust, and François-Xavier Standaert. Making masking security proofs concrete - or how to evaluate the security of any leaking device. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 401–429. Springer, 2015.
17. Alexandre Duc, Sebastian Faust, and François-Xavier Standaert. Making masking security proofs concrete or how to evaluate the security of any leaking device (extended version). *IACR Cryptology ePrint Archive*, 2015:119, 2015.
18. François Durvaux, Mathieu Renauld, François-Xavier Standaert, Loïc van Oldeneel tot Oldenzeel, and Nicolas Veyrat-Charvillon. Efficient removal of random delays from embedded software implementations using hidden markov models. In Stefan Mangard, editor, *Smart Card Research and Advanced Applications - 11th International Conference, CARDIS 2012, Graz, Austria, November 28-30, 2012, Revised Selected Papers*, volume 7771 of *Lecture Notes in Computer Science*, pages 123–140. Springer, 2012.

19. François Durvaux and François-Xavier Standaert. From improved leakage detection to the detection of points of interests in leakage traces. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I*, volume 9665 of *Lecture Notes in Computer Science*, pages 240–262. Springer, 2016.
20. François Durvaux, François-Xavier Standaert, and Santos Merino Del Pozo. Towards easy leakage certification. In Gierlichs and Poschmann [25], pages 40–60.
21. François Durvaux, François-Xavier Standaert, and Nicolas Veyrat-Charvillon. How to certify the leakage of a chip? In Nguyen and Oswald [44], pages 459–476.
22. François Durvaux, François-Xavier Standaert, Nicolas Veyrat-Charvillon, Jean-Baptiste Mairy, and Yves Deville. Efficient selection of time samples for higher-order DPA with projection pursuits. In Stefan Mangard and Axel Y. Poschmann, editors, *Constructive Side-Channel Analysis and Secure Design - 6th International Workshop, COSADE 2015, Berlin, Germany, April 13-14, 2015. Revised Selected Papers*, volume 9064 of *Lecture Notes in Computer Science*, pages 34–50. Springer, 2015.
23. M. Abdelaziz Elaabid and Sylvain Guilley. Portability of templates. *J. Cryptographic Engineering*, 2(1):63–74, 2012.
24. Benoît Gérard and François-Xavier Standaert. Unified and optimized linear collision attacks and their application in a non-profiled setting: extended version. *J. Cryptographic Engineering*, 3(1):45–58, 2013.
25. Benedikt Gierlichs and Axel Y. Poschmann, editors. *Cryptographic Hardware and Embedded Systems - CHES 2016 - 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings*, volume 9813 of *Lecture Notes in Computer Science*. Springer, 2016.
26. Cezary Glowacz, Vincent Grosso, Romain Poussier, Joachim Schüth, and François-Xavier Standaert. Simpler and more efficient rank estimation for side-channel security assessment. In Gregor Leander, editor, *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, volume 9054 of *Lecture Notes in Computer Science*, pages 117–129. Springer, 2015.
27. Vincent Grosso and François-Xavier Standaert. Asca, SASCA and DPA with enumeration: Which one beats the other and when? In Iwata and Cheon [32], pages 291–312.
28. Tim Güneysu and Helena Handschuh, editors. *Cryptographic Hardware and Embedded Systems - CHES 2015 - 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings*, volume 9293 of *Lecture Notes in Computer Science*. Springer, 2015.
29. Annelie Heuser, Olivier Rioul, and Sylvain Guilley. Good is not good enough - deriving optimal distinguishers from communication theory. In Batina and Robshaw [4], pages 55–74.
30. Naofumi Homma and Marcel Medwed, editors. *Smart Card Research and Advanced Applications - 14th International Conference, CARDIS 2015, Bochum, Germany, November 4-6, 2015. Revised Selected Papers*, volume 9514 of *Lecture Notes in Computer Science*. Springer, 2016.
31. Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In Dan Boneh, editor, *CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 463–481. Springer, 2003.

32. Tetsu Iwata and Jung Hee Cheon, editors. *ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, volume 9453 of *Lecture Notes in Computer Science*. Springer, 2015.
33. Thomas Johansson and Phong Q. Nguyen, editors. *EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*. Springer, 2013.
34. Victor Lomné, Emmanuel Prouff, Matthieu Rivain, Thomas Roche, and Adrian Thillard. How to estimate the success rate of higher-order side-channel attacks. In Batina and Robshaw [4], pages 35–54.
35. Victor Lomné, Emmanuel Prouff, and Thomas Roche. Behind the scene of side channel attacks. In Sako and Sarkar [56], pages 506–525.
36. Jake Longo, Elke De Mulder, Dan Page, and Michael Tunstall. SoC it to EM: electromagnetic side-channel attacks on a complex system-on-chip. In Güneysu and Handschuh [28], pages 620–640.
37. Stefan Mangard, Elisabeth Oswald, and François-Xavier Standaert. One for all - all for one: unifying standard differential power analysis attacks. *IET Information Security*, 5(2):100–110, 2011.
38. Daniel P. Martin, Jonathan F. O'Connell, Elisabeth Oswald, and Martijn Stam. Counting keys in parallel after a side channel attack. In Iwata and Cheon [32], pages 313–337.
39. Luke Mather, Elisabeth Oswald, Joe Bandenburg, and Marcin Wójcik. Does my device leak information? an a priori statistical power analysis of leakage detection tests. In Sako and Sarkar [56], pages 486–505.
40. Luke Mather, Elisabeth Oswald, and Carolyn Whitnall. Multi-target DPA attacks: Pushing DPA beyond the limits of a desktop computer. In Sarkar and Iwata [57], pages 243–261.
41. Amir Moradi. Statistical tools flavor side-channel collision attacks. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*, pages 428–445. Springer, 2012.
42. Amir Moradi. Side-channel leakage through static power - should we care about in practice? In Batina and Robshaw [4], pages 562–579.
43. Amir Moradi, Oliver Mischke, and Thomas Eisenbarth. Correlation-enhanced power analysis collision attack. In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hardware and Embedded Systems, CHES 2010, 12th International Workshop, Santa Barbara, CA, USA, August 17-20, 2010. Proceedings*, volume 6225 of *Lecture Notes in Computer Science*, pages 125–139. Springer, 2010.
44. Phong Q. Nguyen and Elisabeth Oswald, editors. *EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014*, volume 8441 of *Lecture Notes in Computer Science*. Springer, 2014.
45. Yossef Oren, Mathieu Renauld, François-Xavier Standaert, and Avishai Wool. Algebraic side-channel attacks beyond the hamming weight leakage model. In Emmanuel Prouff and Patrick Schaumont, editors, *Cryptographic Hardware and Embedded Systems - CHES 2012 - 14th International Workshop, Leuven, Belgium, September 9-12, 2012*, volume 7428 of *Lecture Notes in Computer Science*, pages 140–154. Springer, 2012.

46. Romain Poussier, Vincent Grosso, and François-Xavier Standaert. Comparing approaches to rank estimation for side-channel security evaluations. In Homma and Medwed [30], pages 125–142.
47. Romain Poussier, François-Xavier Standaert, and Vincent Grosso. Simple key enumeration (and rank estimation) using histograms: An integrated approach. In Gierlichs and Poschmann [25], pages 61–81.
48. Santos Merino Del Pozo and François-Xavier Standaert. Blind source separation from single measurements using singular spectrum analysis. In Güneysu and Handschuh [28], pages 42–59.
49. Santos Merino Del Pozo, François-Xavier Standaert, Dina Kamel, and Amir Moradi. Side-channel attacks from static power: when should we care? In Wolfgang Nebel and David Atienza, editors, *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition, DATE 2015, Grenoble, France, March 9-13, 2015*, pages 145–150. ACM, 2015.
50. Emmanuel Prouff, editor. *Constructive Side-Channel Analysis and Secure Design - 5th International Workshop, COSADE 2014, Paris, France, April 13-15, 2014. Revised Selected Papers*, volume 8622 of *Lecture Notes in Computer Science*. Springer, 2014.
51. Emmanuel Prouff and Matthieu Rivain. Masking against side-channel attacks: A formal security proof. In Johansson and Nguyen [33], pages 142–159.
52. Mathieu Renauld and François-Xavier Standaert. Algebraic side-channel attacks. In Feng Bao, Moti Yung, Dongdai Lin, and Jiwu Jing, editors, *Information Security and Cryptology - 5th International Conference, Inscrypt 2009, Beijing, China, December 12-15, 2009. Revised Selected Papers*, volume 6151 of *Lecture Notes in Computer Science*, pages 393–410. Springer, 2009.
53. Mathieu Renauld, François-Xavier Standaert, and Nicolas Veyrat-Charvillon. Algebraic side-channel attacks on the AES: why time also matters in DPA. In Christophe Clavier and Kris Gaj, editors, *Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, September 6-9, 2009, Proceedings*, volume 5747 of *Lecture Notes in Computer Science*, pages 97–111. Springer, 2009.
54. 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, *EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 109–128. Springer, 2011.
55. Oscar Reparaz, Benedikt Gierlichs, and Ingrid Verbauwhede. Generic DPA attacks: Curse or blessing? In Prouff [50], pages 98–111.
56. Kazue Sako and Palash Sarkar, editors. *ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I*, volume 8269 of *Lecture Notes in Computer Science*. Springer, 2013.
57. Palash Sarkar and Tetsu Iwata, editors. *ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Part I*, volume 8873 of *Lecture Notes in Computer Science*. Springer, 2014.
58. Tobias Schneider and Amir Moradi. Leakage assessment methodology - extended version. *J. Cryptographic Engineering*, 6(2):85–99, 2016.

59. François-Xavier Standaert and Cédric Archambeau. Using subspace-based template attacks to compare and combine power and electromagnetic information leakages. In Elisabeth Oswald and Pankaj Rohatgi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2008, 10th International Workshop, Washington, D.C., USA, August 10-13, 2008*, volume 5154 of *Lecture Notes in Computer Science*, pages 411–425. Springer, 2008.
60. François-Xavier Standaert, Nicolas Veyrat-Charvillon, Elisabeth Oswald, Benedikt Gierlichs, Marcel Medwed, Markus Kasper, and Stefan Mangard. The world is not enough: Another look on second-order DPA. In Masayuki Abe, editor, *ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 112–129. Springer, 2010.
61. Nicolas Veyrat-Charvillon, Benoît Gérard, Mathieu Renauld, and François-Xavier Standaert. An optimal key enumeration algorithm and its application to side-channel attacks. In Lars R. Knudsen and Huapeng Wu, editors, *Selected Areas in Cryptography, 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers*, volume 7707 of *Lecture Notes in Computer Science*, pages 390–406. Springer, 2012.
62. Nicolas Veyrat-Charvillon, Benoît Gérard, and François-Xavier Standaert. Security evaluations beyond computing power. In Johansson and Nguyen [33], pages 126–141.
63. Nicolas Veyrat-Charvillon, Benoît Gérard, and François-Xavier Standaert. Soft analytical side-channel attacks. In Sarkar and Iwata [57], pages 282–296.
64. Nicolas Veyrat-Charvillon, Marcel Medwed, Stéphanie Kerckhof, and François-Xavier Standaert. Shuffling against side-channel attacks: A comprehensive study with cautionary note. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 740–757. Springer, 2012.
65. Nicolas Veyrat-Charvillon and François-Xavier Standaert. Generic side-channel distinguishers: Improvements and limitations. In Phillip Rogaway, editor, *CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 354–372. Springer, 2011.
66. Weijia Wang, Yu Yu, Junrong Liu, Zheng Guo, François-Xavier Standaert, Dawu Gu, Sen Xu, and Rong Fu. Evaluation and improvement of generic-emulating DPA attacks. In Güneysu and Handschuh [28], pages 416–432.
67. Carolyn Whitnall and Elisabeth Oswald. Robust profiling for DPA-style attacks. In Güneysu and Handschuh [28], pages 3–21.
68. Carolyn Whitnall, Elisabeth Oswald, and Luke Mather. An exploration of the Kolmogorov-Smirnov test as a competitor to mutual information analysis. In Emmanuel Prouff, editor, *Smart Card Research and Advanced Applications, CARDIS 2011, Leuven, Belgium, September 14-16, 2011, Revised Selected Papers*, volume 7079 of *Lecture Notes in Computer Science*, pages 234–251. Springer, 2011.
69. Carolyn Whitnall, Elisabeth Oswald, and François-Xavier Standaert. The myth of generic DPA... and the magic of learning. In Josh Benaloh, editor, *Topics in Cryptology - CT-RSA 2014, San Francisco, CA, USA, February 25-28, 2014*, volume 8366 of *Lecture Notes in Computer Science*, pages 183–205. Springer, 2014.