Leakage-Resilient Symmetric Cryptography

- Overview of the ERC Project CRASH, Part II -

(*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. The first solutions in this direction were typically aiming at reducing the amount of information leakage directly at the hardware level, and independent of the algorithm implemented. Over the years, a complementary approach (next denoted as leakage-resilience) emerged, trying to exploit the formalism of modern cryptography in order to design new constructions and security models in which the guarantees of provable security can be extended from mathematical objects towards physical ones. This naturally raises the question whether the formal results obtained in these models are practically relevant (both in terms of performance and security)?

The development of sound connections between the formal models of leakage-resilient (symmetric) cryptography and the practice of side-channel attacks 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. For this purpose, I will start with a separation result for the security of stateful and stateless primitives. I will then follow with a discussion of (*i*) pseudorandom building blocks together with the theoretical challenges they raise, and (*ii*) authentication, encryption and authenticated encryption schemes together with the practical challenges they raise. I will finally conclude by discussing emerging trends in the field of physically secure implementations. Quite naturally, a large number of researchers and teams have worked on similar directions. For most 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. The stateful vs. stateless separation. Leakage-resilient symmetric building blocks can be divided in two main categories. First stateful primitives for which the (secret) state can be modified via the public inputs, second stateless primitives for which the (secret) state is initialized only once. The first category is typically exemplified with *Pseudo-Random number Generators* (PRGs) / stream ciphers. The second category is typically exemplified with *Pseudom-Random Functions* (PRFs) and *Pseudo-Random Permutations* (PRPs) / *block ciphers.* The most natural constructions to improve the security of such primitives against side-channel attacks actually borrow from quite old proposals, namely the tree-based PRF introduced by Goldreich, Goldwasser and Micali (GGM) [33] (in 1984) and the forward-secure PRG of Bellare and Yee (in 2003) [15]. Intuitively, they reach this goal via key updates, or re-keying, which is achieved very similarly for PRGs/stream ciphers and PRFs/PRPs/block ciphers. Ideally, re-keying ensures that if the leakage of a single primitive execution is not too informative, the iteration of multiple executions remains safe. Yet, and despite the proofs of leakage-resilience are similar for all these constructions, their concrete relevance is very different. More precisely, while stateful primitives bound the number of measurements that can be made with each key (which prevents averaging the noise in the side-channel measurements obtained by the adversary), stateless primitives only bound the number of input/output pairs that can be measured (which still allows adversaries to query these primitives multiple times with the same challenges, and therefore to reduce the noise via averaging). In [13], we showed that as a result of this observations, quite powerful side-channel attacks can always be mounted against standard leakage resilient PRFs/PRPs such as the GGM tree. By contrast, the forward-secure PRG of Bellare and Yee provides good security guarantees. Typically, it ensures that if the leakage obtained from one execution of the PRG preserves the computational secrecy of its secret state, then this computational secrecy will be preserved with many executions.

2. PRGs / stream ciphers and theoretical challenges. Despite their security guarantees against many relevant (concrete) side-channel attacks, proving the security of leakage-resilient PRGs / stream ciphers turns out to be challenging for two main reasons. First, it requires to guarantee the independence between multiple executions of this primitive. Second, proving leakage-resilience in general requires to bound the information leakage provided by the target implementation in a way that can be quantified by hardware engineers. We next discuss how these issues relate to the difficulty of modeling physical objects.

A. Ensuring independence. When trying to prove the security of an implementation, the first problem is to find a way to capture the (time) complexity of the leakage function. In this respect, a natural idea is to consider it as a polynomial-time function of its inputs (e.g., the secret state in the case of PRGs/stream ciphers). Unfortunately, such a model leads to quite powerful ("precomputation" or "future computation") attacks [28]. For example, a polytime leakage function is able to compute many iterations of a PRG/stream cipher and to leak at time t about operations that will only be executed at time $t + \Delta$. While such attacks are obviously unrealistic [71], finding better ways to model the leakages is surprisingly hard. As a result, the first solutions proposed to deal with the problem were tweaking the designs in order to deal with this overly powerful (polytime) leakage function (e.g., with the alternating structure in [28, 63]).

Among the alternative solutions that we considered in order to improve the efficiency of leakage-resilient PRGs/stream ciphers, a first one was to model their iterations with a random oracle that the adversary can query but the leakage function cannot [71, 76]. While this solution is unsatisfying from the theoretical point-of-view (including random oracles to argue about implementation properties in indeed questionable), it directly leads to simple proofs for natural constructions (e.g., the forward-secure PRG of Bellare and Ye), since ruling out the precomputation attack by assumption (which is reminiscent of early attempts to prove the leakage-resilience of simple PRGs in specialized models [62]).

In order to obtain a proof in the standard model without relying on a random oracle assumption nor an alternating structure (which requires doubling the amount of key material), we proposed using alternating randomness in the PRG/stream cipher iterations [76]. Unfortunately, it was then showed by Faust et al. that this alternating randomness is not sufficient and that one needs (true) randomness in all the PRG/stream cipher iterations for the proof to hold [30]. In [75], we finally showed that this true randomness can be replaced by public pseudo-randomness in an idealized setting similar to *minicrypt*. More precisely, we showed that either it is possible to build a key exchange protocol using only symmetric cryptographic building blocks and their leakages, or the use of pseudo-randomness in leakage-resilient PRGs/stream ciphers is sound.

B. Bounding the leakage. Whenever trying to prove the security of an implementation against side-channel attacks, a minimum requirement is to assume that the secret key(s) is (are) not leaked in full in one execution of the target algorithm. But here as well, the problem of finding good restrictions on the informativeness of the leakage function is tricky. One simple abstraction, usually considered as a starting point, is to assume a leakage function with *bounded range*. Unfortunately, this hardly reflects the reality of actual measurement setups, where a single *observation* or *trace* can contain thousands of samples and have a much larger range than the actual security parameter. As a result, Dziembowski and Pietrzak introduced a milder requirement, namely that the secret parameter(s) should have high *HILL pseudoentropy* conditioned on the observed leakages [28]. But even this requirement does not provide a realistic solution to the problem [71]. On the one hand, enforcing high HILL pseudoentropy implies that some *indistinguishability* game is hard to break, which contradicts the early observations of Micali and Reyzin who showed that indistinguishability is general harder to reach than *unpredictability* for physical objects [54]. Second, concretely estimating the HILL pseudoentropy of a leaking device is a challenging problem as well (i.e., it is not clear how hardware engineers could estimate a value for the λ-bit leakage considered in proofs using such a leakage requirement).

Starting from the opposite direction of what are the leakage assumptions that are practically relevant, we face the complementary problem that they may not be sufficient to prove anything. For example, current evaluation methodologies (at best) focus on evaluating security against side-channel key recovery attacks [47, 69], which is unlikely to provide sound bases for theoretical analysis. In fact, the most promising solution would be to prove the leakage-resilience of a PRG based on an unpredictablity requirement, but for now the only solutions in this direction require an idealized (random oracle) assumption [76].

C. The simulatable leakage attempt. Digging into the previous limitations a bit more formally, one interesting observation is that bounding the computational complexity of a leakage function may not be possible at all. Indeed, physical leakage functions are in the same time highly elaborate and extremely simple. On the one hand, they solve Maxwell's equations for a complex implementation, which would require days of intensive computation if the same solution had to be found with a numerical integration software. (From this point-of-view, the leakage function of an AES implementation is certainly more complex than the AES itself). On the other hand, whenever accessing a physical device, performing a measurement provides an instantaneous solution to these Maxwell's equations. Based on this observation, and since mathematically modeling the leakages of an implementation may be hard, the solution we proposed at CRYPTO 2013 is simply to ignore the problem and to avoid modeling this function at all. For this purpose, we assumed that the leakages can be *simulated* using the same implementation as the target one (which is therefore considered as public knowledge) and without knowing the secret (key). The main interest of this assumption is that it is *empirically falsifiable* by hardware engineers and can be used to prove natural leakage-resilient constructions (e.g., the forward-secure PRG of Bellare and Ye) in the standard model. We also proposed a first instance of leakage simulator as a proof of concept and for further investigation, essentially building simulated traces by *concatenating* traces that are consistent with the public plaintext and ciphertext (generated with a random key) [70].

Interestingly, our instance of simulator has been analyzed (and falsified) in a work by Longo Galea et al. [46], who showed that it is in fact possible to detect simulated traces by looking at the correlation between successive samples in the measurements. In a following ASIACRYPT 2014 rump session talk, we then observed that this detection in fact mostly exploits the noise correlation (i.e., it is not based on the leakage of sensitive variables), and is therefore not in contradiction with the concrete security of a construction (while it of course contradicts its proof) [61]. As the authors of [46], we concluded that the definition of improved leakage simulator instances that withstand the correlation distinguisher is an interesting scope for further research, and that the simulatable leakage paradigm for now remains the only physically verifiable/falsifiable assumption available for the quantitative analysis of leakage-resilient constructions.

`Related works.` Remarkably, the STOC 2008 alternating structure is quite similar to the way threshold implementations deal with one concrete case of non-independent leakages at the block cipher S-box level (called glitches) [58]. This illustrates a case where theoretical and practical challenges in the field of side-channel security are well connected. Leakage-resilient PRFs and PRPs ignoring the concrete separation between stateful and stateless primitives of Section 1 (which is transparent from the proof point-of-view) can be found in [23]. Eventually, another attempt to bound the computational complexity of the leakage function can be found in [31], where it is modeled as an AC0 circuit.

3. Authentication, encryption and practical challenges. Based on the previous leakage-resilient building blocks, the next step is to design authentication, encryption and authenticated encryption schemes that provide improved security against side-channel attacks, which we discuss in this section.

A. A pragmatic model. Our first contribution in this direction is a pragmatic answer to the separation result in Section 1. Namely, since leakage-resilience is hardly effective in the context of stateless primitives while such stateless primitives are in general necessary for the initialization/synchronization of symmetric cryptographic protocols, a solution is to consider a model in which an (expensive) stateful primitive that is protected by other countermeasures (see paragraph C in this section) is only used minimally and combined with a leakage-resilient mode of operation running with a (much cheaper and) less protected block cipher implementation. At CCS 2015, we showed that such a pragmatic model can be used to prove the leakage-resilience of authentication and encryption schemes [60].

In both cases, the proposed modes of operation provide strong security guarantees against side-channel key recovery attacks. In the case of authentication, since the unforgeability of a MAC is defined based on an unpredictability game, one also obtains security guarantees close to the ones expected in a black box setting (i.e., unforgeability with leakage). By contrast, in the case of encryption it remains that semantic security is impossible to achieve in a physical setting. Indeed, any single bit of information leaked about the plaintext (that has to be manipulated somehow by the leaking device) is enough to distinguish. More theoretical approaches (such as [56, 37]) were dealing with this problem by excluding the leakage during the challenge phase of the security definition (which is unrealistic, since there is no reason an adversary should not exploit this leakage). Our proposal is to consider a more realistic setting where we show that the security of multiple encryption rounds tightly reduces to the security of a single encryption round, independent of what can be guaranteed for it (e.g., certainly not semantic security). We leave as an interesting challenge to investigate alternative ways to define plaintext/ciphertex security with leakage.

B. Authenticated encryption. Leakage-resilient authentication and leakage-resilient encryption schemes can naturally be combined into leakage-resilient authenticated encryption schemes. Yet, one important problem remains that the security of the constructions in the previous paragraph strongly depends on the use of a fresh IV in order to generate ephemeral secrets. Hence, it also raises the question of what happens if one combines the exploitation of side-channel leakage and IV misuse. In [16], we showed that the security of some natural candidates for generic composition of authentication and encryption into authenticated encryption schemes strongly suffers from this combination. In fact, and based on a number of concrete attacks, we can even argue that full misuse-resistance with leakage seems impossible to achieve based on symmetric building blocks only. By contrast, we showed that the relaxed notion of *ciphertext integrity with misuse and leakage* is reachable and proposed first instances of constructions satisfying this new notion, that is the best that can be obtained currently.

Besides, we also observed that in the symmetric cryptographic setting, the fact that the decryption is deterministic usually allows an adversary accessing decryption leakages to bypass the ephemeral secrets corresponding to the IV. Hence, and despite our proposed construction satisfying ciphertext integrity with misuse and leakage mitigates a number of attacks, designing authenticated encryption schemes where attacks exploiting the decryption leakage are totally captured and prevented remains an important scope for further investigations.

C. Leak-free (stateless) component. Eventually, our pragmatic model implies the ability to design so-called leak-free implementations of a stateless cryptographic primitive (i.e., a PRF or a PRP/block cipher) based on other side-channel countermeasures. We next discuss three possible approaches for this purpose.

Example 1. Masking and bitslice ciphers. Quite naturally, a first solution is to build on established protection mechanisms such as masking (aka secret sharing) [17, 39, 67, 65, 24, 25] and shuffling [38, 74]. In view of the quite large overheads needed to implement masking securely for standard ciphers (such as the AES Rijndael), one interesting direction to reach this goal is to design ciphers dedicated to efficient masking. Intuitively, this implies reducing the amount of non-linear operations used in the cipher [64]. One solution we investigated is to reduce the number of non-linear S-boxes thanks to partial linear layers [32]. Another one is to reduce the multiplicative complexity of the S-boxes by taking advantage of bitslice ciphers (e.g., the LS-designs introduced in [34]).

Note that in both cases, such design approaches are inherently more risky than using standard ciphers such as the AES Rijndael. For example, partial linear layers have been cryptanalysed and improved in [5] and dense sets of weak keys have been put forward for some instances of (involutive) LS-designs in [45] (see also the recent work in [72]). Yet, and in general, no generic cryptanalysis made these new cipher structures invalid, and therefore they remain an interesting target for further investigations. Also, the eXtended LS-designs in [41] bring an interesting tradeoff, between the extreme simplicity of LS-designs and more conservative cipher structures exploiting the wide-trail strategy [19].

Example 2. PRFs with non-standard assumptions. As an alternative to masking, we introduced a specialized leakage-resilient PRF construction taking advantage of (hardware) parallelism at CHES 2012 [52]. The security of this construction essentially relies on a careful selection of plaintexts that makes standard divide-and-conquer side-channel attacks hardly applicable. More precisely, by ensuring that each plaintext byte is always the same, one can guarantee that the key-dependent predictions of the leakages used in such attacks will be the same for all key bytes, so that the only thing an adversary can obtain from the leakages is some joint information about all these key bytes at once. In other words, such a construction creates hard(er) to exploit *key-dependent algorithmic noise.* Its main advantage are that (i) it does not require any fresh randomness (contrary to masking, which has high randomness requirements) and (ii) hardware parallelism can be emulated in software thanks to shuffling [35]. Its main drawbacks are that (i) it relies on a new hardware assumptions that the

S-boxes leak according to a similar model and (*ii*) advanced attacks can reduce the impact of key-dependent algorithmic noise (see [14], which also proposed new cipher structures to deal with the requirements of the CHES 2012 PRF).

In order to mitigate these limitations, we then introduced an alternative leakage-resilient PRF construction relying on a combination of (hardware) parallelism and unknown inputs generated thanks to a leakage-resilient PRG at ASIACRYPT 2016 [53]. The latter construction is an interesting target for external analysis since it maintains the advantages of the CHES 2012 PRF proposal while significantly redusing/simplifying its hardware assumptions.

Example 3. Key-homomorphism and fresh re-keying. Yet another approach to make masking more efficient is to consider key-homomorphic building blocks, so that the complexity of the protected implementations scales only linearly (hence optimally) in the number of shares. A typical approach to exploit such properties is *fresh re-keying*, for which the first instances were exploiting non-cryptographic (heuristic) and key-homomorphic re-keying functions [51, 50], and could only guarantee birthday security [20]. Such first attempts also left as an open problem to protect the interaction between the block cipher and the re-keying function, which has been analyzed in [12, 11, 36]. We contributed on these issues in two directions. First we showed in [22] how to design fresh re-keying schemes with beyond birthday (black box) security. Second, we proposed new instances of cryptographically strong re-keying functions based on the Learning Parity with Noise (LPN) and Learning With Errors (LWR) problems [27].

`Related works.` The problem of leakage-resilient encryption (thanks to a PRF) has been tackled by Belaid et al. in [1] (although their use of a leakage-resilient PRF also ignores the stateful vs. stateless separation of Section 1, which limits its practical relevance). Leakage-resilient authenticated encryption in the symmetric setting has been considered independently in [21], where the authors describe a sponge-based construction which provides a nice heuristic connection between the amount of leakage that can be tolerated and the capacity of the sponge. Eventually, another way to deal with the problem of leakage resilient authentication and encryption is to rely directly on asymmetric cryptography, of which the richer algebraic structure allows easier formal treatment [44, 49]

4. Wrapping up and emerging trends. The main conclusion of the previous sections is that we now have a number of well understood building blocks, working both as internal protection for any primitive (e.g., masking, shuffling) as as modes for authentication, encryption and authenticated encryption. So an important challenge for future cryptographic implementations is to establish sound and efficient ways to combine these building blocks. In this respect, and as a conclusion of this overview, I next list a few trends that I believe relevant for further progresses in the field of side-channel secure design.

Trend 1. Tools and formal methods. In view of the difficulty of establishing the security of an implementation, exploiting tools for better and earlier security assessments of side-channel leakages appears as an important direction. Early attempts in this direction include the compiler-assisted masking tool in [55] or the automatic application of side-channel countermeasures that we studied in [10]. Even more relevant for the future is the exploitation of formal methods for proving the security of an implementation [29, 6] and the exploitation of composable gadgets to efficiently analyze the security of large systems [7].

Trend 2. Lazy engineering and security against physical defaults. One consistent limitation of masking is that its secure implementation is not only expensive but also highly dependent on physical defaults. For examples, glitches in hardware implementations [48], or memory transitions in software implementations [18] are well-known issues that can reduce the security guarantees of masking. In general, solutions that inherently reduce the security risks due to such physical defaults, or systematic approaches to deal with them (such as the threshold implementations in [58] and lazy engineering in [4]) are certainly an important ingredient to develop for emerging secure technologies.

Trend 3. Advanced attacks and more elaborate masking schemes. Since side-channel countermeasures generally imply performance overheads (e.g., masking implies a quadratic increase of the operations to perform), it also means that a protected implementation offers more and more target leakages to the adversaries, which is potentially exploitable with advanced techniques such as [73, 9]. Hence, masking schemes that better cope with this increase of exploitable leakages, such as the circuit compiler in [2] or the parallel implementations in [8] (which reduce the cycle count) are an important research direction.

Besides, masking schemes with a more elaborate algebraic structure, potentially secure in stronger model than the probing model of Ishai et al. [39] are another interesting scope for further investigation. In this respect, inner product masking appears as a promising candidate [26]. Yet, we note that its higher security guarantees would only materialize if applied in large fields, and it is still unclear how this could be efficiently applied to standard cryptographic primitives (e.g., in [3] the application to the AES Rijndael is running in $\mathsf{GF}(2^8)$).

Trend 4. Security without obscurity. Finally, we mention that both for the application of tools and formal methods to concrete systems (e.g., microcontrollers, cryptographic co-processors) and for the mitigation of physical defaults, the knowledge of the implementation details is critical. So we believe that open designs and (physical) security without obscurity will become increasingly relevant in the future. They are indeed generally needed for security proofs to apply, and for security evaluations to guarantee high security levels.

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 INDOCRYPT 2016 organizers for inviting him to give this talk, and allowing him to amortize the load of his final project report.

References

1. Michel Abdalla, Sonia Belaïd, and Pierre-Alain Fouque. Leakage-resilient symmetric encryption via re-keying. *IACR Cryptology ePrint Archive*, 2015:204, 2015.
2. Marcin Andrychowicz, Stefan Dziembowski, and Sebastian Faust. Circuit compilers with o(1/\log (n)) leakage rate. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*, volume 9666 of *Lecture Notes in Computer Science*, pages 586–615. Springer, 2016.
3. Josep Balasch, Sebastian Faust, and Benedikt Gierlichs. Inner product masking revisited. In Oswald and Fischlin [59], pages 486–510.
4. Josep Balasch, Benedikt Gierlichs, Vincent Grosso, Oscar Reparaz, and François-Xavier Standaert. On the cost of lazy engineering for masked software implementations. In Joye and Moradi [43], pages 64–81.
5. Achiya Bar-On, Itai Dinur, Orr Dunkelman, Virginie Lallemand, Nathan Keller, and Boaz Tsaban. Cryptanalysis of SP networks with partial non-linear layers. In Oswald and Fischlin [59], pages 315–342.
6. Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, and Pierre-Yves Strub. Verified proofs of higher-order masking. In Oswald and Fischlin [59], pages 457–485.
7. Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, Pierre-Yves Strub, and Rébecca Zucchini. Strong non-interference and type-directed higher-order masking. In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, pages 116–129. ACM, 2016.
8. Gilles Barthe, François Dupressoir, Sebastian Faust, Benjamin Grgoire, Franois-Xavier Standaert, and Pierre-Yves Strub. Parallel implementations of masking schemes and the bounded moment leakage model. Cryptology ePrint Archive, Report 2016/912, 2016. `http://eprint.iacr.org/2016/912`.
9. Alberto Battistello, Jean-Sébastien Coron, Emmanuel Prouff, and Rina Zeitoun. Horizontal side-channel attacks and countermeasures on the ISW masking scheme. In *Cryptographic Hardware and Embedded Systems - CHES 2016 - 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings*, pages 23–39, 2016.
10. Ali Galip Bayrak, Francesco Regazzoni, David Novo, Philip Brisk, François-Xavier Standaert, and Paolo Ienne. Automatic application of power analysis countermeasures. *IEEE Trans. Computers*, 64(2):329–341, 2015.
11. Sonia Belaïd, Jean-Sébastien Coron, Pierre-Alain Fouque, Benoît Gérard, Jean-Gabriel Kammerer, and Emmanuel Prouff. Improved side-channel analysis of finite-field multiplication. In *Cryptographic Hardware and Embedded Systems - CHES 2015 - 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings*, pages 395–415, 2015.
12. Sonia Belaïd, Pierre-Alain Fouque, and Benoît Gérard. Side-channel analysis of multiplications in GF(2128) - application to AES-GCM. In *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*, pages 306–325, 2014.

13. Sonia Belaïd, Vincent Grosso, and François-Xavier Standaert. Masking and leakage-resilient primitives: One, the other(s) or both? *Cryptography and Communications*, 7(1):163–184, 2015.
14. Sonia Belaïd, Fabrizio De Santis, Johann Heyszl, Stefan Mangard, Marcel Medwed, Jörn-Marc Schmidt, François-Xavier Standaert, and Stefan Tillich. Towards fresh re-keying with leakage-resilient PRFs: cipher design principles and analysis. *J. Cryptographic Engineering*, 4(3):157–171, 2014.
15. Mihir Bellare and Bennet S. Yee. Forward-security in private-key cryptography. In Marc Joye, editor, *Topics in Cryptology - CT-RSA 2003, The Cryptographers' Track at the RSA Conference 2003, San Francisco, CA, USA, April 13-17, 2003, Proceedings*, volume 2612 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2003.
16. Francesco Berti, François Koeune, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. Leakage-resilient and misuse-resistant authenticated encryption. Cryptology ePrint Archive, Report 2016/996, 2016. `http://eprint.iacr.org/2016/996`.
17. Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards sound approaches to counteract power-analysis attacks. In Michael J. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 398–412. Springer, 1999.
18. Jean-Sébastien Coron, Christophe Giraud, Emmanuel Prouff, Soline Renner, Matthieu Rivain, and Praveen Kumar Vadnala. Conversion of security proofs from one leakage model to another: A new issue. In Werner Schindler and Sorin A. Huss, editors, *Constructive Side-Channel Analysis and Secure Design - Third International Workshop, COSADE 2012, Darmstadt, Germany, May 3-4, 2012. Proceedings*, volume 7275 of *Lecture Notes in Computer Science*, pages 69–81. Springer, 2012.
19. Joan Daemen and Vincent Rijmen. The wide trail design strategy. In Bahram Honary, editor, *Cryptography and Coding, 8th IMA International Conference, Cirencester, UK, December 17-19, 2001, Proceedings*, volume 2260 of *Lecture Notes in Computer Science*, pages 222–238. Springer, 2001.
20. Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, and Florian Mendel. On the security of fresh re-keying to counteract side-channel and fault attacks. In Joye and Moradi [43], pages 233–244.
21. Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel, and Thomas Unterluggauer. ISAP – authenticated encryption inherently secure against passive side-channel attacks. Cryptology ePrint Archive, Report 2016/952, 2016. `http://eprint.iacr.org/2016/952`.
22. Christoph Dobraunig, François Koeune, Stefan Mangard, Florian Mendel, and François-Xavier Standaert. Towards fresh and hybrid re-keying schemes with beyond birthday security. In *Smart Card Research and Advanced Applications - 14th International Conference, CARDIS 2015, Bochum, Germany, November 4-6, 2015. Revised Selected Papers*, pages 225–241, 2015.
23. Yevgeniy Dodis and Krzysztof Pietrzak. Leakage-resilient pseudorandom functions and side-channel attacks on Feistel networks. In Tal Rabin, editor, *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*, volume 6223 of *Lecture Notes in Computer Science*, pages 21–40. Springer, 2010.

24. Alexandre Duc, Stefan Dziembowski, and Sebastian Faust. Unifying leakage models: From probing attacks to noisy leakage. In Nguyen and Oswald [57], pages 423–440.
25. Alexandre Duc, Sebastian Faust, and François-Xavier Standaert. Making masking security proofs concrete - or how to evaluate the security of any leaking device. In Oswald and Fischlin [59], pages 401–429.
26. Stefan Dziembowski and Sebastian Faust. Leakage-resilient cryptography from the inner-product extractor. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 702–721. Springer, 2011.
27. Stefan Dziembowski, Sebastian Faust, Gottfried Herold, Anthony Journault, Daniel Masny, and François-Xavier Standaert. Towards sound fresh re-keying with hard (physical) learning problems. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 272–301. Springer, 2016.
28. Stefan Dziembowski and Krzysztof Pietrzak. Leakage-resilient cryptography. In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 293–302. IEEE Computer Society, 2008.
29. Hassan Eldib, Chao Wang, and Patrick Schaumont. Formal verification of software countermeasures against side-channel attacks. *ACM Trans. Softw. Eng. Methodol.*, 24(2):11:1–11:24, 2014.
30. Sebastian Faust, Krzysztof Pietrzak, and Joachim Schipper. Practical leakage-resilient symmetric cryptography. In Prouff and Schaumont [66], pages 213–232.
31. Sebastian Faust, Tal Rabin, Leonid Reyzin, Eran Tromer, and Vinod Vaikuntanathan. Protecting circuits from leakage: the computationally-bounded and noisy cases. In Henri Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings*, volume 6110 of *Lecture Notes in Computer Science*, pages 135–156. Springer, 2010.
32. Benoît Gérard, Vincent Grosso, María Naya-Plasencia, and François-Xavier Standaert. Block ciphers that are easier to mask: How far can we go? In Guido Bertoni and Jean-Sébastien Coron, editors, *Cryptographic Hardware and Embedded Systems - CHES 2013 - 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings*, volume 8086 of *Lecture Notes in Computer Science*, pages 383–399. Springer, 2013.
33. Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions (extended abstract). In *25th Annual Symposium on Foundations of Computer Science, West Palm Beach, Florida, USA, 24-26 October 1984*, pages 464–479. IEEE Computer Society, 1984.
34. Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, and Kerem Varici. LS-Designs: Bitslice encryption for efficient masked software implementations. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, volume 8540 of *Lecture Notes in Computer Science*, pages 18–37. Springer, 2014.

35. Vincent Grosso, Romain Poussier, François-Xavier Standaert, and Lubos Gaspar. Combining leakage-resilient PRFs and shuffling - towards bounded security for small embedded devices. In Joye and Moradi [43], pages 122–136.
36. Qian Guo and Thomas Johansson. A new birthday-type algorithm for attacking the fresh re-keying countermeasure. *IACR Cryptology ePrint Archive*, 2016:225, 2016.
37. Carmit Hazay, Adriana López-Alt, Hoeteck Wee, and Daniel Wichs. Leakage-resilient cryptography from minimal assumptions. In Johansson and Nguyen [40], pages 160–176.
38. Christoph Herbst, Elisabeth Oswald, and Stefan Mangard. An AES smart card implementation resistant to power analysis attacks. In Jianying Zhou, Moti Yung, and Feng Bao, editors, *Applied Cryptography and Network Security, 4th International Conference, ACNS 2006, Singapore, June 6-9, 2006, Proceedings*, volume 3989 of *Lecture Notes in Computer Science*, pages 239–252, 2006.
39. 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.
40. 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.
41. Anthony Journault, François-Xavier Standaert, and Kerem Varici. Improving the security and efficiency of block ciphers based on LS-Designs. Designs, Codes and Cryptography, to appear.
42. Antoine Joux, editor. *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, volume 5479 of *Lecture Notes in Computer Science*. Springer, 2009.
43. Marc Joye and Amir Moradi, editors. *Smart Card Research and Advanced Applications - 13th International Conference, CARDIS 2014, Paris, France, November 5-7, 2014. Revised Selected Papers*, volume 8968 of *Lecture Notes in Computer Science*. Springer, 2015.
44. Eike Kiltz and Krzysztof Pietrzak. Leakage resilient elgamal encryption. In *Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings*, pages 595–612, 2010.
45. Gregor Leander, Brice Minaud, and Sondre Rønjom. A generic approach to invariant subspace attacks: Cryptanalysis of robin, iscream and zorro. In Oswald and Fischlin [59], pages 254–283.
46. Jake Longo, Daniel P. Martin, Elisabeth Oswald, Daniel Page, Martijn Stam, and Michael Tunstall. Simulatable leakage: Analysis, pitfalls, and new constructions. In Sarkar and Iwata [68], pages 223–242.
47. Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power analysis attacks - revealing the secrets of smart cards*. Springer, 2007.
48. Stefan Mangard, Thomas Popp, and Berndt M. Gammel. Side-channel leakage of masked CMOS gates. In Alfred Menezes, editor, *Topics in Cryptology - CT-RSA 2005, The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005, Proceedings*, volume 3376 of *Lecture Notes in Computer Science*, pages 351–365. Springer, 2005.

49. Daniel P. Martin, Elisabeth Oswald, Martijn Stam, and Marcin Wójcik. A leakage resilient MAC. In Jens Groth, editor, *Cryptography and Coding - 15th IMA International Conference, IMACC 2015, Oxford, UK, December 15-17, 2015. Proceedings*, volume 9496 of *Lecture Notes in Computer Science*, pages 295–310. Springer, 2015.
50. Marcel Medwed, Christophe Petit, Francesco Regazzoni, Mathieu Renauld, and François-Xavier Standaert. Fresh re-keying II: securing multiple parties against side-channel and fault attacks. In *Smart Card Research and Advanced Applications - 10th IFIP WG 8.8/11.2 International Conference, CARDIS 2011, Leuven, Belgium, September 14-16, 2011, Revised Selected Papers*, pages 115–132, 2011.
51. Marcel Medwed, François-Xavier Standaert, Johann Großschädl, and Francesco Regazzoni. Fresh re-keying: Security against side-channel and fault attacks for low-cost devices. In Daniel J. Bernstein and Tanja Lange, editors, *Progress in Cryptology - AFRICACRYPT 2010, Third International Conference on Cryptology in Africa, Stellenbosch, South Africa, May 3-6, 2010. Proceedings*, volume 6055 of *Lecture Notes in Computer Science*, pages 279–296. Springer, 2010.
52. Marcel Medwed, François-Xavier Standaert, and Antoine Joux. Towards super-exponential side-channel security with efficient leakage-resilient PRFs. In Prouff and Schaumont [66], pages 193–212.
53. Marcel Medwed, François-Xavier Standaert, Ventzislav Nikov, and Martin Feldhofer. Unknown-input attacks in the parallel setting: Improving the security of the CHES 2012 leakage-resilient PRF. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I*, volume 10031 of *Lecture Notes in Computer Science*, pages 602–623, 2016.
54. Silvio Micali and Leonid Reyzin. Physically observable cryptography (extended abstract). In Moni Naor, editor, *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, volume 2951 of *Lecture Notes in Computer Science*, pages 278–296. Springer, 2004.
55. Andrew Moss, Elisabeth Oswald, Dan Page, and Michael Tunstall. Compiler assisted masking. In Prouff and Schaumont [66], pages 58–75.
56. Moni Naor and Gil Segev. Public-key cryptosystems resilient to key leakage. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, volume 5677 of *Lecture Notes in Computer Science*, pages 18–35. Springer, 2009.
57. 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.
58. Svetla Nikova, Vincent Rijmen, and Martin Schläffer. Secure hardware implementation of nonlinear functions in the presence of glitches. *J. Cryptology*, 24(2):292–321, 2011.
59. 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*. Springer, 2015.
60. Olivier Pereira, François-Xavier Standaert, and Srinivas Vivek. Leakage-resilient authentication and encryption from symmetric cryptographic primitives. In Indrajit Ray, Ninghui Li, and Christopher Kruegel, editors, *Proceedings of the 22nd*

ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015, pages 96–108. ACM, 2015.

61. Peter Pessl, François-Xavier Standaert, Stefan Mangard, and François Durvaux. Towards leakage simulators that withstand the correlation distinguisher. *ASIACRYPT 2014 rump session.*
62. Christophe Petit, François-Xavier Standaert, Olivier Pereira, Tal Malkin, and Moti Yung. A block cipher based pseudo random number generator secure against side-channel key recovery. In Masayuki Abe and Virgil D. Gligor, editors, *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2008, Tokyo, Japan, March 18-20, 2008*, pages 56–65. ACM, 2008.
63. Krzysztof Pietrzak. A leakage-resilient mode of operation. In Joux [42], pages 462–482.
64. Gilles Piret, Thomas Roche, and Claude Carlet. PICARO - A block cipher allowing efficient higher-order side-channel resistance. In Feng Bao, Pierangela Samarati, and Jianying Zhou, editors, *Applied Cryptography and Network Security - 10th International Conference, ACNS 2012, Singapore, June 26-29, 2012. Proceedings*, volume 7341 of *Lecture Notes in Computer Science*, pages 311–328. Springer, 2012.
65. Emmanuel Prouff and Matthieu Rivain. Masking against side-channel attacks: A formal security proof. In Johansson and Nguyen [40], pages 142–159.
66. 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*. Springer, 2012.
67. Matthieu Rivain and Emmanuel Prouff. Provably secure higher-order masking of AES. In *Cryptographic Hardware and Embedded Systems, CHES 2010, 12th International Workshop, Santa Barbara, CA, USA, August 17-20, 2010. Proceedings*, pages 413–427, 2010.
68. 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.
69. François-Xavier Standaert, Tal Malkin, and Moti Yung. A unified framework for the analysis of side-channel key recovery attacks. In Joux [42], pages 443–461.
70. François-Xavier Standaert, Olivier Pereira, and Yu Yu. Leakage-resilient symmetric cryptography under empirically verifiable assumptions. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, volume 8042 of *Lecture Notes in Computer Science*, pages 335–352. Springer, 2013.
71. François-Xavier Standaert, Olivier Pereira, Yu Yu, Jean-Jacques Quisquater, Moti Yung, and Elisabeth Oswald. Leakage resilient cryptography in practice. In Ahmad-Reza Sadeghi and David Naccache, editors, *Towards Hardware-Intrinsic Security - Foundations and Practice*, Information Security and Cryptography, pages 99–134. Springer, 2010.
72. Yosuke Todo, Gregor Leander, and Yu Sasaki. Nonlinear invariant attack - practical attack on full SCREAM, iSCREAM, and Midori64. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II*, volume 10032 of *Lecture Notes in Computer Science*, pages 3–33, 2016.

73. Nicolas Veyrat-Charvillon, Benoît Gérard, and François-Xavier Standaert. Soft analytical side-channel attacks. In Sarkar and Iwata [68], pages 282–296.
74. 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.
75. Yu Yu and François-Xavier Standaert. Practical leakage-resilient pseudorandom objects with minimum public randomness. In Ed Dawson, editor, *Topics in Cryptology - CT-RSA 2013 - The Cryptographers' Track at the RSA Conference 2013, San Francisco,CA, USA, February 25-March 1, 2013. Proceedings*, volume 7779 of *Lecture Notes in Computer Science*, pages 223–238. Springer, 2013.
76. Yu Yu, François-Xavier Standaert, Olivier Pereira, and Moti Yung. Practical leakage-resilient pseudorandom generators. In Ehab Al-Shaer, Angelos D. Keromytis, and Vitaly Shmatikov, editors, *Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, October 4-8, 2010*, pages 141–151. ACM, 2010.