Offre de thèse - PhD Thesis Offer

Generation of Masking Countermeasures Against Side-Channel Attacks

September 2023

Education:	Master's degree
Field:	Cryptography
Company:	CryptoExperts
Workplace:	41 boulevard des Capucines, 75002 Paris

1 Company Presentation

CryptoExperts is an SME providing outsourced R&D services in cryptography. The company has a team of experts from industry and academia, with PhDs in cryptography, and specialized in various fields. They include public key cryptography, symmetric cryptography, efficient and secure implementations, security protocols and proofs, side-channel attacks, and security of embedded systems. CryptoExperts develops innovative solutions for smart cards, payment and secure messaging services, and offers security auditing, certification support, and training services in cryptography. The company is also very active in the field of scientific research in cryptography, producing every year several publications in the main conferences in the field, and taking part in various academic and industrial projects on advanced research issues (white-box cryptography, homomorphic encryption, proven security against physical attacks, pairings, lattice-based cryptography, group signatures and anonymous accreditations, etc.).

2 Thesis Subject

Cryptography is everywhere in our daily life to ensure the confidentiality and authentication of our communications and the integrity of our records. Although there are strong expectations regarding the security of cryptographic schemes against black-box attackers whose knowledge is restricted to a few inputs or outputs, the security of their implementations is less challenged. However, once implemented on embedded devices, cryptographic schemes become vulnerable to powerful side-channel attacks. The latter additionally exploit the physical leakage (e.g., power consumption) released by the device to recover the manipulated secrets. With cheap equipment, side-channel attacks may yield tremendous damage (e.g., full key recovery) within seconds. Nevertheless, the current security level of countermeasures is not yet close to that achieved in the black-box model.

The community is divided on how to assess the security of cryptographic implementations. From practitioners' perspective, they need to be confronted with concrete side-channel attacks directly on embedded devices. Conversely, theorists consider that such an empirical approach is not portable and does not yield concrete security levels (e.g., not all attacks can be tested). Therefore, they instead investigate security proofs based on abstract leakage models, although the latter are often too far removed from reality to yield practical security.

The combination of both worlds with a toolbox to generate and verify cryptographic implementations with practical security is the topic of an ERC starting project that is hosted by CryptoExperts. As a member of this project, the candidate will work on the design of new compilers to turn any high-level algorithm into an efficient implementation proven secure for identified concrete devices.

2.1 State-Of-The-Art

Masking countermeasure. Of the many approaches investigated by the community to thwart side-channel attacks, the *masking* countermeasure is the most deployed in practice. It consists in applying a so-called secret sharing at the computation level to randomize the intermediate variables and mitigate the side-channel information leakage. Concretely, in a d^{th}-order masking, each sensitive variable is split into $d + 1$ random shares, among which any combination of d shares does not reveal any secret information. When the shares are combined by bitwise addition, the masking is said to be *Boolean*. In this setting, for linear operations, gadgets (as algorithms that operate on shared data) can be easily implemented by applying the operation to each share individually. However, non-linear gadgets require additional randomness to ensure that any set of at most d intermediate variables is still independent from the original secret.

Leakage models. To reason about the security of masked implementations against side-channel attacks, the community has introduced *leakage models* which aim to define the attacker's capabilities. The *t-probing model* introduced by Ishai, Sahai, and Wagner [16] assumes that an adversary is able to get the exact values of up to t intermediate variables and hence captures the difficulty of learning information from the combination of noisy variables. Despite its wide use by the community [19, 18, 10, 11, 12], the probing model fails to capture the huge amount of information resulting from the leakage of all manipulated data [3, 15]. For example, it typically ignores the repeated manipulation of sensitive intermediate variables which would average the noise and reduce the uncertainty on the secret variables (see horizontal attacks [3]). Conversely, the *noisy leakage model* [9, 17] offers an opposite trade-off. It captures well the reality of embedded devices by assuming that an attacker gets a noisy function of all the intermediate variables, but it is not convenient to build security proofs. To get the best of both worlds, Duc *et al.* proved that the noisy leakage security could be reduced to the probing security [13]. However, the reduction is not tight when considering a constant number of probes in the probing model as the security level decreases as the size of the circuit increases. The reduction of Duc *et al.* relies on an intermediate leakage model, the *p-random probing model*, in which each variable is disclosed to the adversary with a given probability p, related to the amount of noise in practice. The random probing model further encompasses the powerful horizontal attacks and also benefits from a tighter reduction with the noisy leakage model which becomes independent of the circuit size.

In the three aforementioned leakage models, an observation relates only to one intermediate variable. But in practice, physical defaults might yield leakage on several intermediate variables at the same time. For instance, *glitches*, that occur when information does not propagate simultaneously throughout a run, are likely to leak information on an instruction and its predecessors (in the sense of dataflow analysis). The probing model has already been partially extended to consider such physical defaults [14, 7, 1]. Beyond that, more specific features of the target devices (*e.g.* the leaking operations or the dependencies between the leakage of specific instructions) could be revealed by a prior characterization. A first work in this direction, published in 2021 [2], designs a new approach to verify the implementations in a fine-grained probing model, but much remains to be done on the random probing and the noisy leakage models.

2.2 Objectives

Industrial cryptographers are expected to design efficient implementations that will resist both classical cryptanalysis and side-channel attacks when integrated on real devices. Although several compilers have been introduced in the past few years, they are still shunned because the resulting implementations do not properly match the reality of embedded devices. To automatically design cryptographic implementations so that they achieve measurable practical security, two main lacks need to be addressed: the practicality of the leakage models and the efficiency of the building blocks. In this PhD, the goals are three-fold:

(i) building more efficient compilers in the random probing model,

(ii) designing compilers in the noisy leakage model,

(iii) (in both cases) considering the device features as inputs for these compilers.

Namely, in addition to defining tighter composition rules, the candidate will design efficient building blocks for the main symmetric and asymmetric cryptographic algorithms that are secure in the increasingly realistic leakage models extended with device features. In particular, many operations are still left aside and practical security and efficiency (i.e., tolerated leakage, time and memory complexity) are far from being optimal.

Following the prior works on random probing compilers, the first task will be to mix the advantages of the expansion strategy exploited in [4, 5, 6] and the tight composition rules of [8] to improve the generated masked implementations. In addition to these more efficient composition rules, the idea will be to design more efficient gadgets for a wider range of operations with the best security features. In particular, many gadgets are still missing for common post-quantum algorithms. Moreover, the few existing designs are only valid when the leakage probability of each variable is very low (around 2^{-7}) or equivalently when the underlying device is very noisy. The analysis of upper bounds needs to be pushed forward and the candidate will aim to exhibit the best possible designs in this regard. When additionally considering the characteristics of the devices, composition rules will most likely be directly derived from the generic ones. Conversely, gadget variants will most likely require an increase in the number of shares, additional randomness in careful locations, or a smart choice of the order of the instructions based on the characteristics of the target device.

The only compiler in the noisy leakage model [17] relies on the existence of leak-free blocks that are meant to ensure the independence between the input and output sharings (when the secret is unknown) so that gadgets can be safely composed. The second task of this PhD thesis will be to investigate the possibility to get rid of them with additional randomness in careful locations. While the efficient gadgets in the random probing model are very likely to achieve their goals in the noisy leakage model, the main challenge will be to exhibit refresh gadgets (i.e., gadgets functionally equivalent to the identity function which aim to update a sharing with fresh randomness) which will minimize the mutual information between their input and output sharings. When additionally considering device features, the noisy leakage functions will have to be redefined to receive more inputs and varying noise, perhaps using previous designs.

3 Candidates

This PhD offer is for a student with a master's degree (or equivalent) who has a taste for cryptography and applied research. The candidate will have to demonstrate a solid background in mathematics and/or computer science with a specialization in cryptography. The technical background required for this PhD thesis combines skills in algebra (finite fields, polynomials, etc.) as well as ease in programming. The candidate will have to demonstrate autonomy and dynamism. A good level of English is also desired.

4 Contact

To apply for this PhD offer, please send your résumé to

Sonia Belaïd: `sonia.belaid@cryptoexperts.com`.

References

[1] Gilles Barthe, Sonia Belaïd, Gaëtan Cassiers, Pierre-Alain Fouque, Benjamin Grégoire, and François-Xavier Standaert. maskVerif: Automated verification of higher-order masking in presence of physical defaults. In Kazue Sako, Steve Schneider, and Peter Y. A. Ryan, editors, *ESORICS 2019, Part I*, volume 11735 of *LNCS*, pages 300–318. Springer, Heidelberg, September 2019.

[2] Gilles Barthe, Marc Gourjon, Benjamin Grégoire, Maximilian Orlt, Clara Paglialonga, and Lars Porth. Masking in fine-grained leakage models: Construction, implementation and verification. *IACR TCHES*, 2021(2):189–228, 2021. https://tches.iacr.org/index.php/TCHES/article/view/8792.

[3] Alberto Battistello, Jean-Sébastien Coron, Emmanuel Prouff, and Rina Zeitoun. Horizontal side-channel attacks and countermeasures on the ISW masking scheme. In Benedikt Gierlichs and Axel Y. Poschmann, editors, *CHES 2016*, volume 9813 of *LNCS*, pages 23–39. Springer, Heidelberg, August 2016.

[4] Sonia Belaïd, Jean-Sébastien Coron, Emmanuel Prouff, Matthieu Rivain, and Abdul Rahman Taleb. Random probing security: Verification, composition, expansion and new constructions. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part I*, volume 12170 of *LNCS*, pages 339–368. Springer, Heidelberg, August 2020.

[5] Sonia Belaïd, Matthieu Rivain, and Abdul Rahman Taleb. On the power of expansion: More efficient constructions in the random probing model. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 313–343. Springer, Heidelberg, October 2021.

[6] Sonia Belaïd, Matthieu Rivain, Abdul Rahman Taleb, and Damien Vergnaud. Dynamic random probing expansion with quasi linear asymptotic complexity. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part II*, volume 13091 of *LNCS*, pages 157–188. Springer, Heidelberg, December 2021.

[7] Roderick Bloem, Hannes Groß, Rinat Iusupov, Bettina Könighofer, Stefan Mangard, and Johannes Winter. Formal verification of masked hardware implementations in the presence of glitches. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part II*, volume 10821 of *LNCS*, pages 321–353. Springer, Heidelberg, April / May 2018.

[8] Gaëtan Cassiers, Sebastian Faust, Maximilian Orlt, and François-Xavier Standaert. Towards tight random probing security. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part III*, volume 12827 of *LNCS*, pages 185–214, Virtual Event, August 2021. Springer, Heidelberg.

[9] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards sound approaches to counteract power-analysis attacks. In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 398–412. Springer, Heidelberg, August 1999.

[10] Jean-Sébastien Coron, Emmanuel Prouff, Matthieu Rivain, and Thomas Roche. Higher-order side channel security and mask refreshing. In Shiho Moriai, editor, *FSE 2013*, volume 8424 of *LNCS*, pages 410–424. Springer, Heidelberg, March 2014.

[11] Jean-Sébastien Coron, Franck Rondepierre, and Rina Zeitoun. High order masking of look-up tables with common shares. *IACR TCHES*, 2018(1):40–72, 2018. https://tches.iacr.org/index.php/TCHES/article/view/832.

[12] Jean-Sébastien Coron and Lorenzo Spignoli. Secure wire shuffling in the probing model. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part III*, volume 12827 of *LNCS*, pages 215–244, Virtual Event, August 2021. Springer, Heidelberg.

[13] Alexandre Duc, Stefan Dziembowski, and Sebastian Faust. Unifying leakage models: From probing attacks to noisy leakage. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 423–440. Springer, Heidelberg, May 2014.

[14] Sebastian Faust, Vincent Grosso, Santos Merino Del Pozo, Clara Paglialonga, and François-Xavier Standaert. Composable masking schemes in the presence of physical defaults & the robust probing model. *IACR TCHES*, 2018(3):89–120, 2018. https://tches.iacr.org/index.php/TCHES/article/view/7270.

[15] Hannes Groß, Ko Stoffelen, Lauren De Meyer, Martin Krenn, and Stefan Mangard. First-order masking with only two random bits. In Begül Bilgin, Svetla Petkova-Nikova, and Vincent Rijmen, editors, *Proceedings of ACM Workshop on Theory of Implementation Security, TIS@CCS 2019, London, UK, November 11, 2019*, pages 10–23. ACM, 2019.

[16] Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 463–481. Springer, Heidelberg, August 2003.

[17] Emmanuel Prouff and Matthieu Rivain. Masking against side-channel attacks: A formal security proof. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 142–159. Springer, Heidelberg, May 2013.

[18] Matthieu Rivain and Emmanuel Prouff. Provably secure higher-order masking of AES. In Stefan Mangard and François-Xavier Standaert, editors, *CHES 2010*, volume 6225 of *LNCS*, pages 413–427. Springer, Heidelberg, August 2010.

[19] Kai Schramm and Christof Paar. Higher order masking of the AES. In David Pointcheval, editor, *CT-RSA 2006*, volume 3860 of *LNCS*, pages 208–225. Springer, Heidelberg, February 2006.