Offre de stage - Internship Offer

*Generation of Masking Countermeasures Against Side-Channel Attacks*

2023-2024

<table>
<thead>
<tr>
<th>Education:</th>
<th>Master’s degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field:</td>
<td>Cryptography</td>
</tr>
<tr>
<td>Company:</td>
<td>CryptoExperts</td>
</tr>
<tr>
<td>Workplace:</td>
<td>41 boulevard des Capucines, 75002 Paris</td>
</tr>
</tbody>
</table>
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 cryptographic solutions for various applications, and offers security auditing, custom conception of cryptographic protocols and implementation of cryptographic libraries. 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 (such as white-box cryptography, homomorphic encryption, proven security against physical attacks, post-quantum cryptography and zero-knowledge proofs).

2 Internship 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 model.

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. Therefore this internship will specifically focus on the construction of more efficient compilers in the (practical) random probing model. 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 random probing model. 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 \cite{4,5,6} and the tight composition rules of \cite{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.

3 Candidates

This internship 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 internship 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 will also be a plus.
4 Contact

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

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


