CRYPTOEXPERTS

WE INNOVATE TO SECURE YOUR BUSINESS

Offre de Stage - Internship Offer

Efficient and Proven Method to Verify
Cryptographic Implementations against Side-Channel Attacks

November 2018

Type of internship:	Master 2 or last year engineer student (6 months)
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 about five experts from industry and the academy, all with a Ph.D. 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, pay-TV, 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 of 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, lattices-based cryptography, group signatures and anonymous accreditations, etc.).

2 Internship description

Most of widely used cryptosystems are secure in the black-box model when the adversary is limited to the observation of the inputs and outputs. However, this model does not faithfully reflect the reality of embedded devices. Introduced in the nineties, a more realistic model in which the attacker can observe the physical leakage of the device has revealed a new class of attacks referred to as *side-channel attacks*. These attacks exploit the dependence between sensitive values of an algorithm and the physical leakage of the device (time, power consumption, electromagnetic radiation, ...).

The most deployed countermeasure against side-channel attacks is currently what we call *masking*. In a nutshell, the idea of masking is to split the information of each sensitive data x into $t+1$ shares $x_0, x_1, \ldots, x_t$ such that $x = x_0 \star ... \star x_t$ where $\star$ is a group law (when $\star = \oplus$, the masking is said to be Boolean) to break its dependency with the leakage. Concretely, t shares are uniformly generated at random:

$$\forall \;\; 1 \leq i \leq t, \quad x_i \leftarrow \$$$

while the last one is built from the sensitive data and the t previously generated shares:

$$x_0 = x \star^{-1} x_1 \star^{-1} x_2 \star^{-1} \cdots \star^{-1} x_t.$$

Given this countermeasure, the knowledge of at most t shares does not reveal any information on the sensitive variable and an attacker has to combine the leakage of $t+1$ variables to recover the sensitive data. As leakage come with noise, the combination of shares has been shown to be exponential in the number of data to combine, that is in the masking order t [2].

While it can be very challenging to design cryptographic functions that are properly masked at a generic order t (such that combining t variables cannot reveal anything), combining such masked functions without inducing any flaw is also a difficult task.

As part of its research activities, CryptoExperts has developed a method for analyzing countermeasures against side-channel attacks. Given an algorithm consisting of state of-the-art functions masked at a generic order t, this automatic and proven method makes it possible to determine whether the global implementation is secure in a tried and tested model, the probing model. This method will appear in the proceedings of Asiacrypt 2018 [1] and already comes with a dedicated tool.

While the current method was only implemented to assemble simple cryptographic functions: additions, multiplications as designed by Ishai, Sahai, and Wagner in [3], and strong refreshing algorithms, the first idea of this internship will be to extend it to other linear functions and to integrate these changes to the tool (which is currently implemented in Python).

Then, the internee will be asked to adapt the method to other state-of-the-art (non linear) multiplications which do not fulfill the same security properties. This will require a modification of the existing proofs, and a modification of the tool as well.

Finally and optionally, the current method determines whether or not an implementation is secure in the probing model for any masking order t. If an implementation proves to be flawed, then a usual method is to add refreshing blocks at carefully chosen locations. But the choice of these locations is not trivial and a deep analysis was left as future work. If there is enough time, an important step will be to exhibit such a (hopefully optimal) method.

3 Candidates

This internship offer is for a Master 2 or final year engineer student 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 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 internship offer, please send your résumé to Sonia Belaïd:
sonia.belaid@cryptoexperts.com

References

[1] Sonia Belaïd, Dahmun Goudarzi, and Matthieu Rivain. Tight private circuits: Achieving probing security with the least refreshing. Cryptology ePrint Archive, Report 2018/439, 2018. https://eprint.iacr.org/2018/439.

[2] 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.

[3] 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.