Thesis subject: Formal leakage-free analysis and modelling of microarchitectural sources of leakage

Host team: LIP6 laboratory, ALSOC team

Director: Karine Heydemann karine.heydemann@lip6.fr
Co-supervisor: Quentin Meunier quentin.meunier@lip6.fr

Context

Physical attacks named side channel attacks (SCA) consist in measuring physical quantities of a computing system (power consumption, electromagnetic radiations) during the execution of a cryptographic algorithm, and using them in order to retrieve the encryption key [1, 2]. These attacks more specifically target embedded devices, such as payment cards, for which the encryption key must not be known to the user.

SCA have grown in popularity since the early 2000s. To limit their impact, two main hardening techniques have appeared: hiding [3] and masking [4]. The latter consists in breaking down the secret into several parts (shares) using masks (variables following a uniform random distribution between several executions), so that only the recomposition of the different shares makes it possible to deduce information on the original secret. The algorithm must be modified to apply an independent treatment to each of the shares.

Various works have studied how to automate the security proofs of such masking schemes [6, 7, 8, 9]: the goal of resulting tools is, from a description of the program, to verify for all the expressions manipulated by the program that their distributions are statistically independent of the secrets (typically the encryption key). Such security proofs are based on a leakage model (e.g value-based leakage model) that abstracts the real leakage. Moreover they are often applied on a high level representation of a masked program that is too far from the compiled code running on a given hardware target. To guarantee the absence of leakage when running a masked code, it is necessary to perform a leakage-free analysis on the assembly code (or binary) of the program with a sufficiently precise model of the processor [5], typically taking into account its micro-architecture and its sources of leakage.

Subject

The objective of the thesis is to study and design methods and tools to improve the security of masked software implementations by considering the execution of the binary code on a low-level description of the processor in order to account for micro-architectural effects.
Understanding the sources of leakage in processors will be an important aspect in order to propose a relevant and tractable model, or even a modelling methodology starting from an RTL description. Another important part will concern the design or extension of a formal leakage-free analysis.
The thesis will also include an experimental part in order to validate the different proposals (model and security analysis)

This thesis is funded by the ANR IDROMEL project that has started in 2021. The objectives of this project are to analyze the micro-architectural sources of leakage and to propose different methods and tools to strengthen the software and hardware security of embedded systems against SCA. The consortium brings together Arm France, CEA, IRISA, LAAS and LIP6. The PhD candidate will interact with all partners, in particular with Arm France.

We are looking for a candidate with some of the following skills:
– understanding of processor micro-architecture, side-channel attacks based on power consumption, HDL (Verilog)
– advanced programming level in at least one language such as Python, C, C++
– code analysis including assembly
– reasonable background in mathematics and statistical analysis

To apply please send a CV with a cover letter to karine.heydemann@lip6.fr and quentin.meunier@lip6.fr.

Note that depending on the candidate's profile and competency, the position can be adapted and transformed into a post-doc.

References

[1] S. Mangard, E. Oswald, and T. Popp. Power analysis attacks: Revealing the secrets of smart cards, Vol. 31. Springer Science & Business Media, 2008.

[2] Q. L. Meunier. FastCPA: Efficient Correlation Power Analysis Computation with a Large Number of Traces, in CS2'19, 2019, Valencia, Spain

[3] N. Belleville, D. Couroussé, K. Heydemann and H.-P. Charles. Automated software protection for the masses against side-channel attacks, ACM Transactions on Architecture and Code Optimization (TACO) 15.4 (2018): 47.

[4] Y. Ishai, A. Sahai, D. Wagner. Private circuits: Securing hardware against probing attacks, in Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 2003.

[5] D. Zoni, A. Barenghi, G. Pelosi, W. Fornaciari. A Comprehensive Side-Channel Information Leakage Analysis of an In-Order RISC CPU Microarchitecture, ACM Transactions on Design Automation of Electronic Systems (TODAES) 23.5 (2018): 57.

[6] G. Barthe, S. Belaïd, G. Cassiers, P.-A. Fouque, B. Grégoire, F.-X. Standaert. maskVerif: Automated Verification of Higher-Order Masking in Presence of Physical Defaults, European Symposium on Research in Computer Security. Springer, Cham, 2019.

[7] Q. L. Meunier, I. Ben El Ouahma, and K. Heydemann. SELA: a Symbolic Expression Leakage Analyzer. International Workshop on Security Proofs for Embedded Systems. 2020.

[8] I. Ben El Ouahma, Q. L. Meunier, K. Heydemann, E. Encrenaz. Side-channel robustness analysis of masked assembly codes using a symbolic approach, Journal of Cryptographic Engineering (JCEN), March 2019

[9] Pengfei, G., Hongyi, X., Sun, P., Zhang, J., Song, F., & Chen, T. (2020). Formal Verification of Masking Countermeasures for Arithmetic Programs. IEEE Transactions on Software Engineering.