Towards an Open Approach to Secure Cryptographic Implementations

François-Xavier Standaert*

UCL Crypto Group, Université Catholique de Louvain, Belgium

Abstract. In this talk, I will discuss how recent advances in side-channel analysis and leakage-resilience could lead to both stronger security properties and improved confidence in cryptographic implementations. For this purpose, I will start by describing how side-channel attacks exploit physical leakages such as an implementation's power consumption or electromagnetic radiation. I will then discuss the definitional challenges that these attacks raise, and argue why heuristic hardware-level countermeasures are unlikely to solve the problem convincingly. Based on these premises, and focusing on the symmetric setting, securing cryptographic implementations can be viewed as a tradeoff between the design of modes of operation, underlying primitives and countermeasures.

Regarding modes of operation, I will describe a general design strategy for leakage-resilient authenticated encryption, propose models and assumptions on which security proofs can be based, and show how this design strategy encourages so-called leveled implementations, where only a part of the computation needs strong (hence expensive) protections against side-channel attacks.

Regarding underlying primitives and countermeasures, I will first emphasize the formal and practically-relevant guarantees that can be obtained thanks to masking (i.e., secret sharing at the circuit level), and how considering the implementation of such countermeasures as an algorithmic design goal (e.g., for block ciphers) can lead to improved performances. I will then describe how limiting the leakage of the less protected parts in a leveled implementations can be combined with excellent performances, for instance with respect to the energy cost.

I will conclude by putting forward the importance of sound evaluation practices in order to empirically validate (by lack of falsification) the assumptions needed both for leakage-resilient modes of operation and countermeasures like masking, and motivate the need of an open approach for this purpose. That is, by allowing adversaries and evaluators to know implementation details, we can expect to enable a better understanding of the fundamentals of physical security, therefore leading to improved security and efficiency in the long term.

* The author is a Senior Research Associate of the Belgian Fund for Scientific Research (FNRS-F.R.S.). This work has been funded in part by the ERC Project 724725.