Secure Computation

Institution: Department of Computer science and department of Mathematics, UVSQ
Teaching hours: CM: 12h TD: 12h Total: 30h (Eq. TD)
ECTS: 3
Semester: 2
Faculty members: Louis Goubin
Location: UVSQ
Nature: Compulsory
Specializations: Applied Algebra, Computer Science
Evaluation: Midterm and final exam
Prerequisite: Cryptography course (M1 MINT, first semester)

Description:
Traditionally, in cryptography, we try to ensure the confidentiality, integrity and authenticity of messages, which are static objects (stored or transmitted as such over unsecured communication channels). However we do not consider the security of cryptographic algorithms and protocols themselves (which are usually programs that are running, and so are dynamic objects). For example we do not consider the confidentiality of programs (the principle Kerckhoffs assumes they are known to everyone), or their integrity (it is assumed that Alice and Bob perform these algorithms/protocols/programs properly without any change/error/bug), or their authenticity (it is assumed that the algorithms/protocols/programs run by Alice and Bob have been installed by a trusted authority). The course "Secure Computation" for M1 students in computer science or mathematics, aims at showing that in reality it is very important to also secure the calculations (in the sense of algorithms/protocols/programs).

Contents:
- The course covers the practical aspects of these vulnerabilities (buffer overflow, reverse engineering code, side-channel attacks, fault injection, ...).
- It is also an opportunity to deepen more theoretical issues (modeling the concept of computing, Turing machines, garbled circuits, self-modifying programs, code obfuscation, ...), showing how these concepts can be used to prevent software vulnerabilities.
- The course will be illustrated by numerous examples, particularly from smart card security, computer virology and emerging applications in the "cloud computing".