On the modelling of processor micro-architecture for masked software verification

Karine Heydemann*[1]

[1]Thales – Thales (France) – France

Résumé

Masking is a popular countermeasure against side channel attacks exploiting consumption or electromagnetic emissions. A masked implementation can be formally proven secure with respect to a leakage model. However, its deployment at the software level remains tricky: the compiler and its optimizations can degrade the level of security proven at the source level; a proven secure assembly implementation can reveal leaks in practice due to the micro-architecture of the target platform. This presentation will explain the need to take into account the micro-architecture to formally verify the security of a masked software implementation and will present how we built a model of an SMT32 platform integrating a Cortex-M3 microcontroller to formally verify the absence of leaks in masked implementations. We will conclude by discussing the limitations of this approach and addressing current needs.

*Intervenant