Factoring integers with ECM on the Kalray MPPA-256 processor

Jérémie Detrey*[1]

[1]INRIA, LORIA – - – France

Résumé

The Kalray MPPA-256 is a recent low-power chip which embeds 256 32-bit cores. As such, it can be used as an efficient co-processor for accelerating computations, bridging the gap between usual CPUs and the more throughput-oriented GPUs, all the while consuming far less power.

In this talk, we will present a fast and energy-efficient implementation of the Elliptic Curve Method (ECM, an algorithm for factoring integers) on this platform. After a brief presentation of the ECM and of its important role in cryptanalysis, especially in the context of factoring RSA keys, we will glance at some of the key architectural features of the MPPA-256. We will then present an optimized library for multiprecision modular arithmetic, on top of which the ECM implementation was built, before concluding with a few benchmarks and comparisons with the state of the art.

This is a joint work with Masahiro Ishii, Pierrick Gaudry, Atsuo Inomata, and Kazutoshi Fujikawa.

*Intervenant