High-Performance Integer Factoring with Reconfigurable Devices

Ralf Zimmermann
Ruhr-University Bochum, Germany

Abstract

We present a novel FPGA-based implementation of the Elliptic Curve Method (ECM) for the factorization of medium-sized composite integers. More precisely, we demonstrate an ECM implementation capable to determine prime factors of up to 2,424 151-bit integers per second using a single Xilinx Virtex-4 SX35 FPGA.

To provide this vast number of integer factorizations per FPGA, we make use of the available DSP blocks on each FPGA device to accelerate low-level arithmetic computations. This methodology allows the development of a time-area efficient design that runs 24 ECM cores in parallel, implementing both phase 1 and phase 2 of the ECM. Moreover, our design is fully scalable and and can be optimized for composite integers in the range from 66 to 236 bits without any significant modifications to the hardware.