An Improved Architecture of a Hardware Accelerator for Factoring Integers with Elliptic Curve Method

Michał Andrzejczak
Military University of Technology
Warsaw, Poland

Abstract: Elliptic Curve Method (ECM) is a well-known method for factoring integers, which is usually used in the Number Field Sieve algorithm as a subroutine for factoring smaller integers than the targeted one. ECM is called many times and can be executed in parallel for different inputs. This method mainly consist of simple operations on elliptic curves. Thus, ECM is suitable for hardware implementations that can efficiently reduce computational time. This work describes a new, improved FPGA-based hardware accelerator for ECM, designed for large scale computations. Our accelerator can operate with an onboard ARM processor or with an external host computer and is equipped with a small instruction set. This design can factor several numbers at once and can be easily ported to various FPGA boards. Different methods for improving results (e.g. the use of DSP blocks, cache-registers, reorganizing instruction order) are described and their performance is analyzed. As a result, one of the fastest hardware ECM units is achieved.