CORR 2001-01

# Computing discrete Logarithms with the Parallelized Kangaroo Method

Edlyn Teske

**Abstract** The Pollard kangaroo method computes discrete logarithms in arbitrary cyclic groups. It is applied if the discrete logarithm is known to lie in a certain interval, say $[a, b]$, and then has expected running time $O(\sqrt{b-a})$ group operations. In its serial version it uses very little storage. It can be parallelized with linear speed-up, and in its parallelized version its storage requirements can be efficiently monitored. This makes the kangaroo method the most powerful method to solve the discrete logarithm problem in this situation. In this paper, we discuss various experimental and theoretical aspects of the method that are important for its most effective application.