CORR 2001-07

Square-Root Algorithms for the Discrete Logarithm Problem (A Survey)

Edlyn Teske

Abstract The best algorithms to compute discrete logarithms in arbitrary groups (of prime order) are the baby-step giant-step method, the rho method and the kangaroo method. The first two have (expected) running time $O(\sqrt{n})$ group operations (n denoting the group order), thereby matching Shoup's lower bounds. While the baby-step giant-step method is deterministic but with large memory requirements, the rho and the kangaroo method are probabilistic but can be implemented very spece efficiently, and they can be parallelized with linear speed-up. In this paper, we present the state of the art in these methods.