Cryptology ePrint Archive: Report 2011/416

Efficient Parallelization of Lanczos Type Algorithms

Ilya Popovyan

Abstract: We propose a new parallelization technique for Lanczos type algorithms for solving large sparse linear systems over finite fields on mesh cluster architecture. The algorithm computation time scales as P^{-1} on $P processors, and the communcation times scales as $P^{-1/2}$ for reasonable choice of P.

Category / Keywords: number field sieve, parallel sparse linear system solver

Date: received 2 Aug 2011

Contact author: poilyard at gmail com

Available formats: PDF | BibTeX Citation

Version: 20110805:134555 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]