Abstract

Abstract

This work deals with the parallelization of the LUP triangular matrix decomposition over a finite field Z/pZ. This computation is motivated by numerous applications, including algebraic attacks with polynomial system solving, index calculus attacks on the discrete logarithm, etc. We first describe different possible implementations of matrix factorization over a finite field. Then we focus on the implementation of the tiled LU decomposition in C++ using the FFLAS-FFPACK library. This decomposition consists in factorizing the initial matrix into a lower triangular L, an upper triangular U and a permutation matrix P. When the matrix is rank deficient, the lower triangular matrix can be replaced by a matrix in column echelon form, which defines the CUP decomposition.

In order to take advantage of the parallel architecture of processing units, the implementation is adapted to multithreaded computation. We use KAAPI which is a C++ library that allows to execute fine/medium grain multithreaded computation with dynamic data flow synchronizations. We then compare performances of our algorithm using OpenMP and KAAPI.