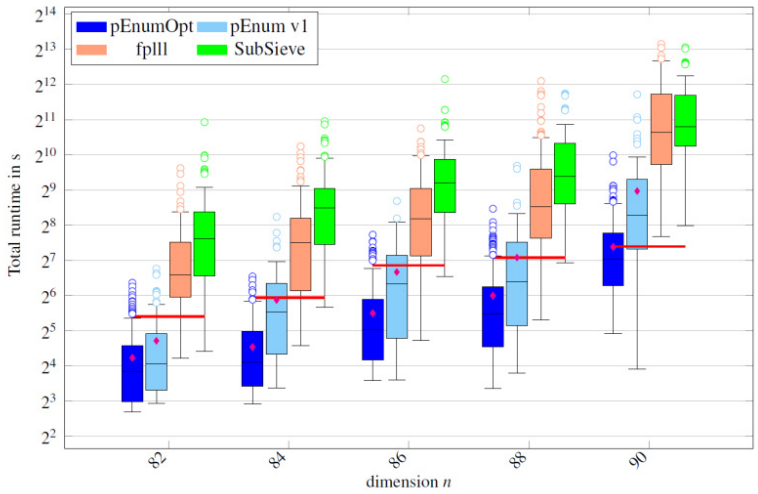
p3Enum: A Parallel, Parameterizable Open-Source Framework for Enumeration with Extreme Pruning



Project Manager
Dr. Michael Burger

Principal Investigator
Dr. Michael Burger

Project Term
2018 - 2019

Clusters
Lichtenberg Cluster Darmstadt

Additional Software
boost, fplll, gmp , Intel VTune, NTL library

Institute
Institute of Scientific Computing

University
Technische Universität Darmstadt

Introduction

In our project, we investigate the hardness of various instances of the shortest vector problem (SVP) which are the bases of novel schemes for quantum-safe cryptography. To that end, we employ our open-source software *p3*Enum which was developed, tested and optimized within this project. Our package is based on a parallelized implementation of the enumeration algorithm with extreme pruning which searches the coefficients of the shortest vector in a heuristically pruned tree. The SVP is known to be NP-hard and the required runtime to solve it grows exponentially with the dimension of the lattice in which the search is processed. Additionally, the random nature of the algorithm results in highly varying runtimes for different runs to solvethe same problem instance, requiring many repetitions in order to understand its behavior in detail. Investigating problems of dimensions higher than 100 may require many hours of runtime although our software is efficiently parallelized.

Methods

The p3Enum-software is written in C++-11 and parallelized with OpenMP. It automatically increases the workload during the search in a pruned search-tree by relaxing the pruning strategy, meaning that more nodes are left in the tree. If appropriately parametrized, a parallel run of our enumeration takes about the same runtime as the standard serial enumeration but visits much more nodes in the tree and thus increases the success probability. Synchronization between threads is minimized by

JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN
TECHNISCHE UNIVERSITÄT DARMSTADT
UNIKASSEL VERSITÄT
Philipps Universität Marburg

new thread-safe and shared data structures. The single-core performance was also optimized based on profiled runs.

Results

We performed a detailed performance comparison with other state-of-the-art frameworks and demonstrated that *p3*Enum is the fastest SVP solver for dimensions ≤ 92 due to its parallelization. The parallel efficiency is still near 0.7 when employing 24 cores on the dual core Haswell systems of the HHLR, although parts of the parallel solution process are memory bound. Additionally, we highlighted that *p3*Enum provides relatively stable runtimes for the solution of the problems, in contrast to the other software packages considered.

Discussion

The fast runtimes combined with their stability and reproducibility make *p3*Enum a good candidate as SVP oracle in lattice reduction frameworks, since during the basis reduction many SVP instances in smaller dimensions have to be solved. Additionally, the data gathered allows a better understanding of the runtime behavior of enumeration with extreme pruning and will help us to develop models to predict the runtime of higher lattice dimension which are needed in order to set appropriate parameters for quantum-safe cryptography.

Figures

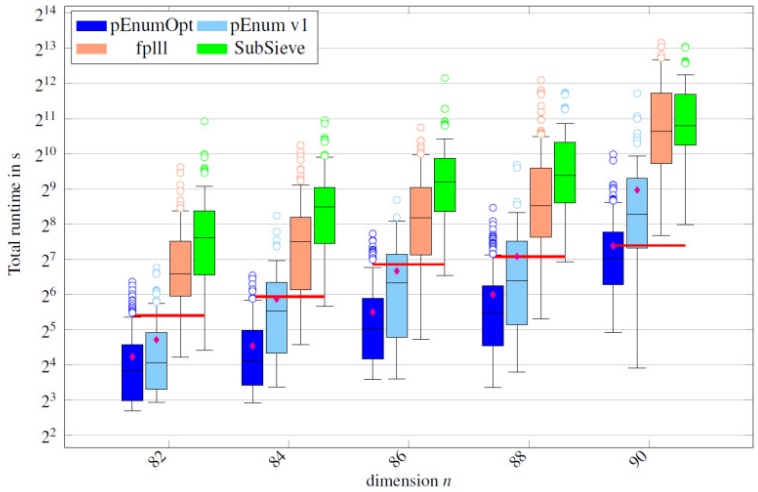


Figure 1: Runtime comparison of the recent p3Enum-version (pEnumOpt) with its predecessor and with the state-of-the-art fplll-library based on pruned enumeration and SubSieve as a sieving based solution.

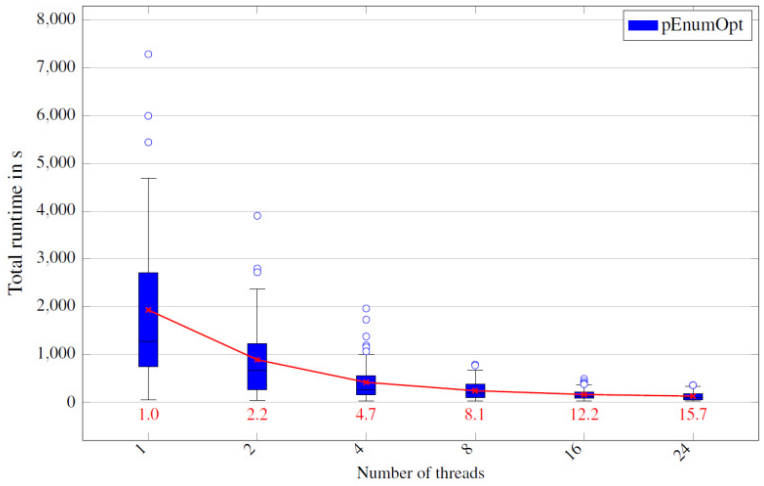


Figure 2: Speedup when increasing the number of threads for 88-dimensional lattices. Based on 360 measurement points. Red line connects the averages.

Publications

Burger, M., Bischof, C., Krämer, J.: p3Enum: A New Parameterizable and Shared-Memory Parallelized Shortest Vector Problem Solver. In: ICCS 2019, 535-542 June 2019, Faro. [Conference or Workshop Item], 2019
https://tubiblio.ulb.tu-darmstadt.de/112554/

Burger, M., Bischof, C., Krämer, J.: A new Parallelization for p3Enum and Parallelized Generation of Optimized Pruning Functions. In: HPCS 2019, N/A June 2019, Dublin. [Conference or Workshop Item], 2019
https://tubiblio.ulb.tu-darmstadt.de/115537/

Last Update: 2023-03-16 01:30