Hessisches Kompetenzzentrum
für Hochleistungsrechnen

Cryptanalysis of SIDH Cryptosystem using Heterogeneous Hardware I

Project Manager
Giang Nam Nguyen

Principal Investigator
Prof. Dr. Christian Bischof

Project Term
2021 - 2022

Clusters
Lichtenberg Cluster Darmstadt

Additional Software
SageMath

Institute
Institute of Scientific Computing

University
Technische Universität Darmstadt

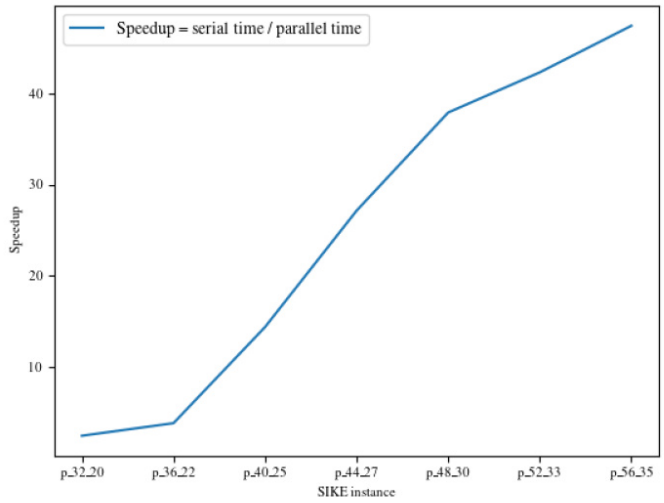

Figure 1: Speedup achieved with the parallel MiTM

Introduction

The project focuses on the cryptanalysis of the Computational Supersingular Isogeny (CSSI) problem which underlies the isogeny-based post-quantum cryptography. The attack against CSSI corresponds to the problem of finding a path connecting two nodes in a graph of exponentially many elliptic curves. The fastest known attack is based on the van Oorschot-Wiener (vOW) algorithm, a random walk collision-finding algorithm. In theory, vOW is perfectly parallelizable, while in practice, the parallelization aspect of vOW is not sufficiently studied regarding HPC.

Methods

Firstly, we aim to improve the node-level performance of the vOW attack by employing multithreading in a more efficient manner than the up-todate attack. Secondly, we plan to distribute the attack to many nodes on a HPC cluster. Making use of the large amount of memory aggregated from many compute nodes, this approach tackles the memory problem, which the existing attack so far faces, to solve larger CSSI instances. Thirdly, the collision finding by random walk is perfectly parallelizable by nature, making the use of massive parallelism on GPUs a promising approach to speed up the attack.

Results

The vOW attack inherently requires two points of a certain orders on each input elliptic curve. With this in regard, we developed a parallel application written in SageMath running in a Singularity container on the Lichtenberg cluster. The vOW attack consists of two steps: a precomputation and a random walk starting from the precomputed nodes. Regarding the parallelization of the vOW attack, we developed a parallel precomputation with OpenMP which achieves a speedup of an order of magnitude over the existing fastest attack.

Discussion

The container run-time Singularity on LB2 cluster provides HPC users a wide variety of options to develop applications in HPC environment without worrying about the incompatibility of the software stack. The containerization allows for smooth deployment of codes which require a different software stack than that currently available on the Lichtenberg cluster. This work demonstrates a manageable effort to employ container environment on HPC for an application written in a computer algebra system. The OpenMP parallelization of the precomputation in vOW shows a clear trade-off between memory and time to solution, i.e. having more memory is crucial to achieve faster time to solution. Given the fact that the precomputation can be accelerated significantly on a multi-core CPU, it is still an open question about the choice of the precomputation depth to reach an optimal speed up for the whole attack.

Last Update: 2023-03-16 02:07