Masterarbeit
Modulare, konfigurierbare und parallelisierte Basisreduktion

TECHNISCHE UNIVERSITÄT DARMSTADT

Institute for Scientific Computing

SCIENTIFIC COMPUTING

Dr. Michael Burger
Ansprechpartner

Alexanderstr. 2
64289 Darmstadt

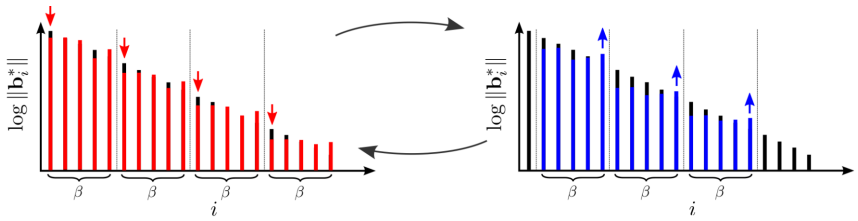
Tel.: +49 6151 16 - 76991
Fax: +49 6151 16 - 25345

michael.burger@tu-darmstadt.de

https://www.sc.informatik.tu-darmstadt.de/

Datum
7. Juli 2020

Im Bereich der Gitterbasierten Kryptographie spielen der BKZ-Algorithmus und seine Varianten [1] eine große Rolle, wenn es um das Reduzieren (=Verbessern) einer Basis geht. Dabei wird versucht die Basisvektoren kürzer und orthogonaler zu machen. Dazu verarbeitet BKZ die Vektoren in Blöcken der Größe β und läuft dabei iterativ in mehreren Runden (tours) in einem gleitenden Fenster über alle Basisvektoren. Ein Maß für die Qualität der Basis ist die Länge der Gram-Schmidt Vektoren $||\mathbf{b}_i^*||$, deren Betrag möglichst flach abfallen soll.



Gleitende Fenster der Breite β laufen über die Vektoren und glätten den Längenunterschied.

Bekannte Modifikationen von BKZ sind BKZ 2.0 [1] oder progressive BKZ [2]. Auch von Bedeutung sind das Prinzip der dualen Gitter und die Varianten Self-Dual BKZ oder Dual-DeepBKZ [3].

Im Rahmen dieser Masterarbeit soll ein Framework entwickelt werden, welches eine funktionsfähige, modulare BKZ-Implementierung beinhaltet. Modular in dem Sinn, dass benötigte Unterprozeduren (LLL-Algorithmus, SVP-oracle) einfach gegen andere Versionen ausgetauscht werden können. Nach Möglichkeit soll auch Parallelität ausgenutzt oder ihre Nutzung vorbereitet werden. Bereits vorhandene Building Blocks sollen integriert werden. Schnittstellen zu einigen bekannten Libraries sind zu designen und zu realisieren. Durch Literaturrecherche sind potentielle Verbesserungen und Modifikationen von BKZ zu identifizieren und in den Code zu integrieren oder die Nutzung durch das Design leicht integrierbar zu machen.

Empfohlene Vorkenntnisse:

- Gute Programmierkenntnisse in C++
- Erfahrung mit Software Engineering und bei Performance-Analyse und -Tuning (Intel VTune, Valgrind)
- Grundkenntnisse bezüglich Gitterproblemen von Vorteil, ansonsten die Bereitschaft der Einarbeitung in das Gebiet

[1] Yuanmi Chen and Phong Q. Nguyen. Bkz 2.0: Better lattice security estimates. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology – ASIACRYPT 2011*, pages 1–20, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[2] Yoshinori Aono, Yuntao Wang, Takuya Hayashi, and Tsuyoshi Takagi. Improved progressive bkz algorithms and their precise cost estimation by sharp simulator. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 789–819. Springer, 2016.

[3] Daniele Micciancio and Michael Walter. Practical, predictable lattice basis reduction. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 820–849. Springer, 2016.