jh190038-NAJ

照屋唯紀 (産業技術総合研究所・代表)、柏原賢二 (東京大学・副代表)、
池上努 (産業技術総合研究所)、松田源立 (成蹊大学)

大規模並列計算による格子の最短ベクトル探索の効率化に関する研究

背景

格子暗号は、格子の最短ベクトルを探索する問題(Shortest Vector Problem, SVP)の困難性をその安全性の根拠とする公開鍵暗号系の1つである。SVPは量子計算機を使用した効率的な解法が発見されていないため、耐量子計算機暗号の候補として注目を集めている。格子暗号の実用化のためには、実用上解読が困難なSVPの問題規模を明らかにする必要があり、そのためにはSVPを効率的に解くアルゴリズムの探求が重要な研究課題となっている。

目的

本研究では、大規模並列計算に適したSVP解法アルゴリズムを研究開発し、これを実装する。実際にSVPを解く実験を行うことを通じ、実用的で安全な格子暗号の設計に貢献する。

格子の最短ベクトル問題 (SVP)

正則な整数行列$\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$が基底として与えられた時に、基底ベクトルの整数結合$x = \sum_i u_i \mathbf{b}_i$で作られる点(ベクトル)の全体が格子$L$である。これら格子点のうち最も短い非ゼロの点を見つける問題が最短ベクトル問題(SVP)である。SVPは格子の次元数が上がると、解くことが極めて困難となる。

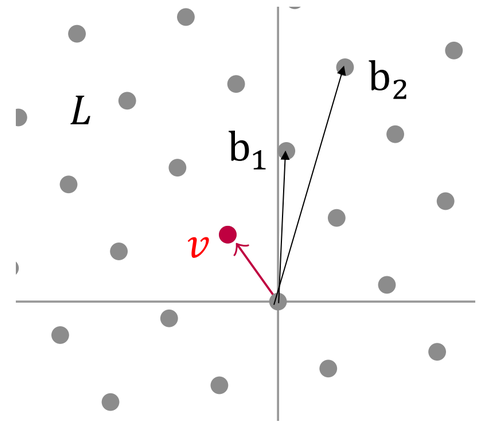

図1: 格子とSVP

これまでの研究・関連研究

ドイツのダルムシュタット大学によりSVP Challenge [1]が開設・運営されている。ここには各次元のSVPが具体的に与えられており、近似解のアップロードを通じて各種アルゴリズムの性能を比較・検討することができる。我々は、samplingと基底簡約を組み合わせた手法を用いて初めて150次元の近似SVPを解いた[2]。現在はsievingをさらに組み合わせた手法を用いた研究グループ[3]がより高次元の求解に成功している。

次元	長さ	解提出者	日付
157	3320	Ducas et al.	2019/05
155	3165	Albrecht et al.	2018/09
153	3192	Albrecht et al	2018/08
152	3217	柏原、照屋	2018/10

図2: SVP Challengeトップ4

解法アルゴリズム：基底簡約

Gram-Schmidt直交化した基底$\mathbf{B}^* = (\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*)$と書いた時、ノルムの列$(\|\mathbf{b}_1^*\|, \ldots, \|\mathbf{b}_n^*\|)$を基底$\mathbf{B}$のshapeと呼ぶ。基底簡約は、基底を入力に取り、そのshape が辞書式順序で小さい基底へと変換する。その結果として短い格子点を得る。基底以外の格子点を追加入力として取ることができ、短い格子点を与えれば、より小さいshapeの基底に変換され易くなる。

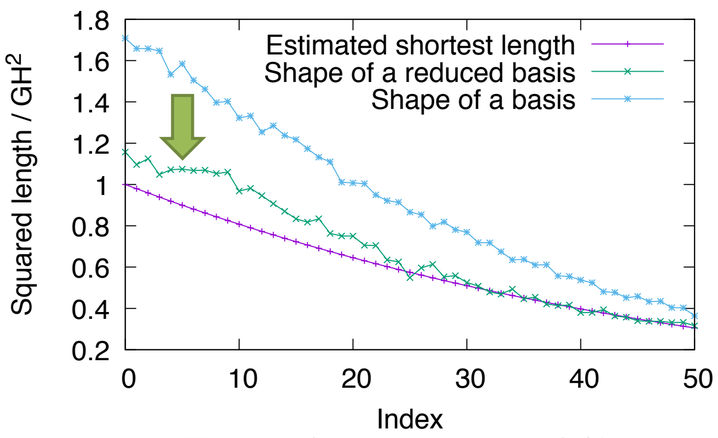

図3: 基底のshapeと基底簡約

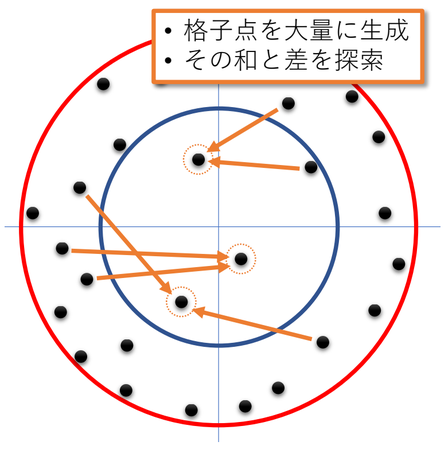

図4: Sieving

解法アルゴリズム：Sieving

格子点を大量に生成し、その和・差をbrute forceに探索する。高速に短い格子点を探索できるが、次元数に対して指数オーダーのメモリを要する。

研究開発の方針

基底簡約とsievingを組み合わせた効率的な解法について研究する。Sievingはその計算に膨大なメモリを要するため、これが並列化の障害となる可能性が高い。そこで、その削減に有用と考えられる下記の手法に注目し、大規模並列計算に適したより効率的なアルゴリズムを設計しながら、高速にSVPを解くプログラムの研究開発を行う:

1. 直交補空間への射影による次元削減[3][4]
2. 局所鋭敏ハッシュ(SimHash)を利用した高速化[3][4][5]

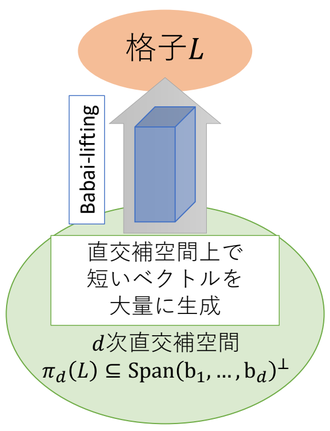

図5: 直交補空間への射影による次元削減

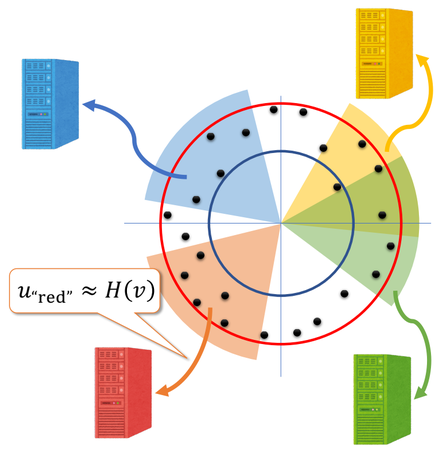

図6: 局所鋭敏ハッシュを利用した高速化

参考文献
[1] SVP Challenge, https://www.latticechallenge.org/svp-challenge/ (Accessed 2019-05-28)
[2] Teruya et al., Fast Lattice Basis Reduction Suitable for Massive Parallelization and Its Application to the Shortest Vector Problem, PKC 2018
[3] Albrecht et al., The General Sieve Kernel and New Records in Lattice Reduction, EUROCRYPT 2019
[4] Ducas, Shortest Vector from Lattice Sieving: A Few Dimensions for Free, EUROCRYPT 2018
[5] Becker et al., Speeding-up lattice sieving without increasing the memory, using sub-quadratic nearest neighbor search, IACR ePrint 2015/522