

最強の解読法で作る安全な暗号技術

研究課題名：大規模並列計算に適した高速な 格子基底簡約アルゴリズムの開発

照屋唯紀 産業技術総合研究所 サイバーフィジカルセキュリティ研究センター
研究員

目的：安全な格子暗号の実現

- 格子暗号は耐量子計算機暗号の候補
- 格子の**最短ベクトル**を探索する問題(Shortest Vector Problem, SVP)の困難性が安全性の根拠
- 完全準同型暗号や関数暗号が構成可能

- 高次元のSVPは求解困難
 - 量子計算機を利用しても理論上困難

- 次元数を大きくすると、**困難性(安全性)が高まる**
- 次元数が大きすぎると、**実用性が失われる**

解決したい問題：

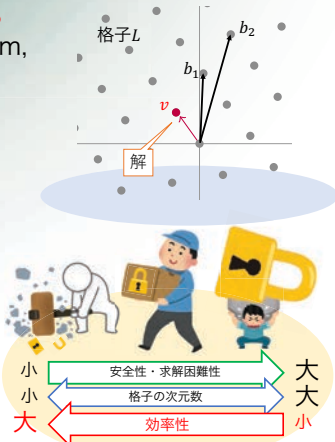
- 安全性と実用性を両立する
「**丁度良い次元数**」を明らかにしたい！

アプローチ：

- 最強の解読法の開発
 - まず最速の求解法＝最強の矛を作る！
- 求解計算量の推定方法の開発
 - 丁度良い次元数を求めて安全な盾を作る！

実用的な量子計算機が登場しても安全な暗号技術の提供が可能に
・情報システムやサービスの安全性の確保
・プライバシーの保護・配慮したサービスの構築

入力：格子の基底 $B = (b_1, b_2)$



成果：求解計算量推定法を提案

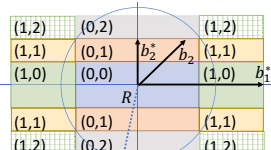
- 格子点サンプリングが出力する格子点の長さの分布を推定する方法を提案^[1]
- 推定した分布から求解計算量を推定可能

格子点サンプリングの入力：

- 格子の基底
- 探索空間(＝超直方体の集合)

出力：

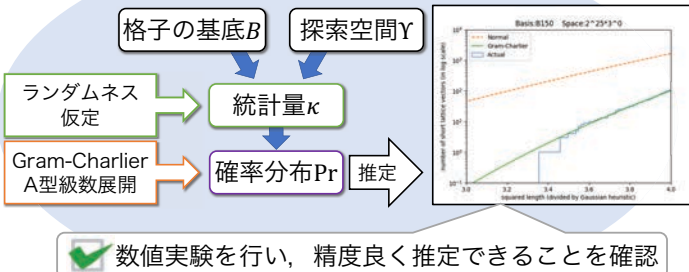
- 探索空間内の格子点の集合



短い格子点は
いくつあるのか？

モデル化

ある半径の超球と交わる
超直方体の体積はいくら？



提案法の応用例：

- 格子点列挙・Babaiの最近平面アルゴリズム・射影格子ふるいの求解計算量推定
- 基底の良さの評価

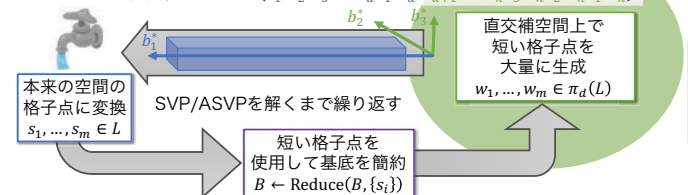
[1] Matsuda, Teruya, Kashiwabara: Efficient Estimation of Number of Short Lattice Vectors in Search Space under Randomness Assumption, APKC 2019 doi:10.1145/3327958.3329543

高速な格子基底簡約アルゴリズムの開発に向けて

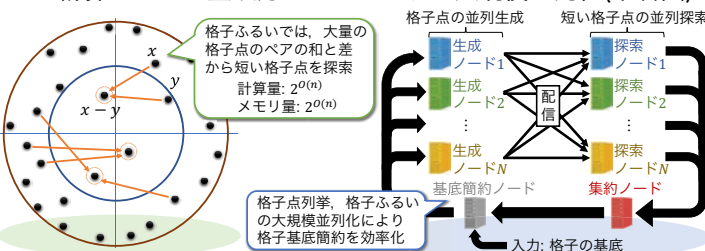
サンプリングリダクションの概要

入力：基底 $B = (b_1, \dots, b_n)$

Gram-Schmidt直交化基底 $B^* = (b_1^*, b_2^*, b_3^*, \dots, b_{d-1}^*, b_d^*, b_{d+1}^*, \dots, b_{n-3}^*, b_{n-2}^*, b_{n-1}^*, b_n^*)$

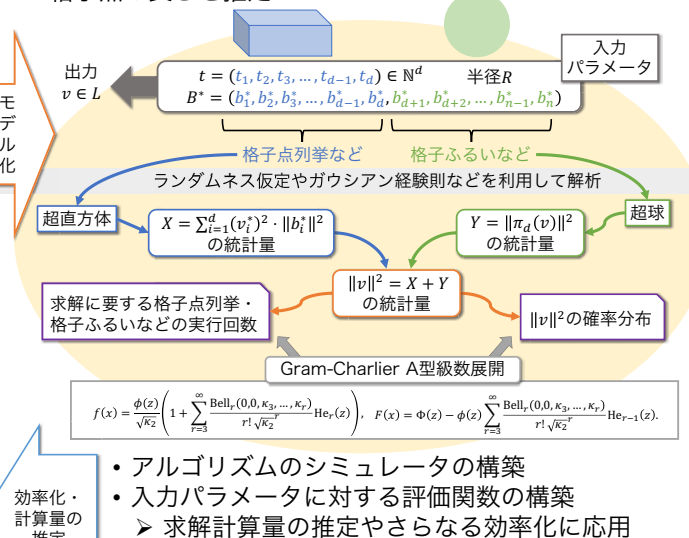


- サンプリングリダクション(上図)を拡張
- 新たに格子ふるい(下左図)を導入して格子点生成を高速化
 - 膨大なメモリ使用量がボトルネック
 - 計算・メモリ量双方でスケールする大規模並列化(下右図)



精密な求解計算量推定法の構築に向けて

- 利用するアルゴリズムに適した確率モデルの導入
- Gram-Charlier A型級数展開を応用し出力される格子点の長さを推定



- アルゴリズムのシミュレータの構築
- 入力パラメータに対する評価関数の構築
 - 求解計算量の推定やさらなる効率化に応用