修士論文 要旨

ユニモジュラ行列を用いた格子基底のランダム化について

数理情報学専攻 48186220　青木 大地
指導教員　高木 剛 教授

1　はじめに

現在広く用いられている公開鍵暗号方式に RSA 暗号と楕円曲線暗号とがあるが，これらを高速に解くことが可能な量子アルゴリズムが発見されている [**?**]．量子コンピュータによる現代暗号の危殆化を懸念し耐量子計算機暗号の研究が盛んに行われている．

耐量子計算機暗号の有力な候補の一つに格子暗号がある．格子暗号は最短ベクトル問題 (SVP) などの格子問題の計算量的困難性を安全性の根拠としている．SVP の求解手法としては決定的アルゴリズムである数え上げアルゴリズム (enumeration) [6] や，確率的アルゴリズムである篩アルゴリズム (sieving) [1, 4] が知られている．また近似版 SVP の求解手法としては基底簡約アルゴリズムがある [7, 9, 2]．

これらのアルゴリズムで広く用いられる手法にユニモジュラ行列による格子基底のランダム化がある．ランダムユニモジュラ行列の生成方法はアプリケーションごとに差異があり，望ましい生成方法については十分に解析されていない．本研究では，ある方法で生成したユニモジュラ行列が特定のパラメータ範囲では格子基底をうまくランダム化できないことを示した．

2　既存研究

代表的な格子基底簡約アルゴリズムの 1 つである LLL アルゴリズム [7] を Algorithm 1 に示す．

代表的なアプリケーションにおいて用いられているランダムユニモジュラ行列の生成手順について紹介する．以下，n を格子の次元とする．

Magma [3] の RandomUnimodularMatrix 関数は対角成分が 1 で，その他の非対角成分を，R を正の整数として $\{-R, -R+1, \ldots, R\}$ から一様ランダムにとった下三角行列 $\mathbf{S}$，上三角行列 $\mathbf{T}$ の積 $\mathbf{ST}$ をランダムユニモジュラ行列として生成する．ランダムなユニモジュラ行列の生成方法としては最もシンプルで一般的な方法だと言える．他のランダムユニモジュラ行列の生成方法としては fpylll [5] ライブラリや，SageMath [8] ライブラリで用いられているものがある．

Algorithm 1 LLL 基底簡約アルゴリズム [7]

Input: n 次元格子 $\mathcal{L}$ の基底 $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$，簡約パラメータ $\frac{1}{4} < \alpha < 1$
Output: α-LLL 簡約基底 $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$

GSO ベクトル $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ および GSO 係数 $\mu_{i,j}$ $(1 \le j < i \le n)$ を計算
$k \leftarrow 2$
while $k \le n$ **do**
　for $j = k-1, \ldots, 1$ **do**
　　if $|\mu_{k,j}| > \frac{1}{2}$ **then**
　　$q \leftarrow \lfloor \mu_{k,j} \rceil$，$\mathbf{b}_k \leftarrow \mathbf{b}_k - q\mathbf{b}_j$
　　for $l = 1, \ldots, j$ **do**
　　$\mu_{k,l} \leftarrow \mu_{k,l} - q\mu_{j,l}$
　　end for
　　end if
　end for
　if $\|\mathbf{b}_k^*\|^2 \ge (\alpha - \mu_{k,k-1}^2)\|\mathbf{b}_{k-1}^*\|^2$ **then**
　　$k \leftarrow k+1$
　else
　　$\mathbf{b}_k, \mathbf{b}_{k-1}$ を交換
　　update GSO
　　$k \leftarrow \max\{k-1, 2\}$
　end if
end while

3　本研究の成果

Magma 型 のユニモジュラ行列についてパラメータ R によるランダム化格子基底の分布の変化を調べた．Magma 型は R が大きいときすべての基底が符号を除いて同一のものになることがわかった．他 2 つの型は Magma 型と異なり R を大きくしても分布のばらつきは失われないことがわかった．この結果を踏まえ本研究では次の主張が成り立つと予想する．

主張 1

n 次元格子 $\mathcal{L}$ の 0.99-LLL 簡約基底 $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ と，その基底行列 $\mathbf{B}$ が与えられたとする．ランダムユニモ

ジュラ行列 $\mathbf{U}$ を

$$\mathbf{U} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ r_{2,1} & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & 0 \\ r_{n,1} & r_{n,2} & \dots & 1 \end{pmatrix} \begin{pmatrix} 1 & r_{1,2} & \dots & r_{1,n} \\ 0 & 1 & \dots & r_{2,n} \\ \vdots & \vdots & \ddots & r_{n-1,n} \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

と定める．ただし，正の整数 R に対し各非対角成分 r_{ij} は $\{-R, -R+1, \dots, R-1, R\}$ からそれぞれ一様ランダムにサンプルされるとする．行列 $\mathbf{C} = \mathbf{UB}$ とする．このとき R が十分大きいならば，基底行列 $\mathbf{C}$ の α-LLL 簡約基底行列は $\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ のみによって各行ベクトルの符号を除いて一意に定まる．

本研究では主張 1 において，非対角成分 $r_{ij} = r$ とした特殊な場合が格子次元 $n = 3$ において成り立つことを証明した．

また，パラメータ R によってランダム化格子基底の分布がどのように変化するかを調べることにより，主張 1 が成り立つことを実験的に確かめた．図 1 はランダム化格子基底を 1 万個生成し，そこに含まれる各行ベクトルの符号を除いて同一である基底行列の割合を示したグラフである．グラフからパラメータ R を大きくするほど同一基底の割合が増加することがわかる．生成したランダム化格子基底の 9 割が同一の基底行列となるようなパラメータ R の値を推定すると $R = O(n^{2.39})$ が得られた．

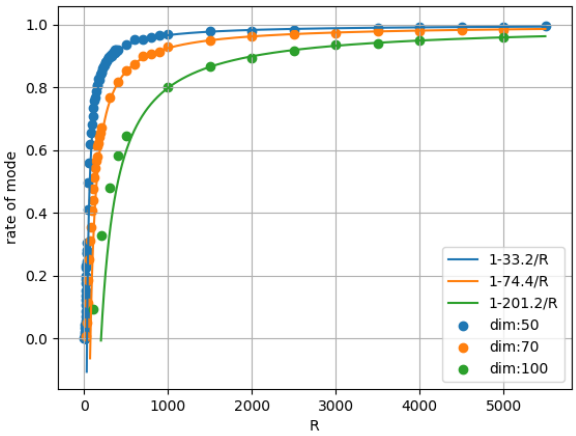

図 1: ランダム化格子基底の同一基底の生成確率．

参考文献

[1] Miklós Ajtai, Ravi Kumar and Dandapani Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing*, pages 601–610. ACM, 2001.

[2] Yoshinori Aono, Yuntao Wang, Takuya Hayashi, and Tsuyoshi Takagi. Improved progressive BKZ algorithms and their precise cost estimation by sharp simulator. In *Adcances in Cryptology – EUROCRYPT 2016, LNCS*, volume 9665, pages 789–819. Springer, 2016.

[3] John Cannon, Wieb Bosma, Claus Fieker, and Allan Steel (Eds.). Handbook of Magma Functions, Edition 2.22 (2016).

[4] Léo Ducas. Shortest vector from lattice sieving: A few dimensions for free. In *Advances in Cryptology – EUROCRYPT 2018, LNCS*, volume 10820, pages 125–145. Springer, 2018.

[5] The FPLLL development team. Fplll, a lattice reduction library. Available: `https://github.com/fplll/fplll`, 2016.

[6] Nicolas Gama, Phong Q. Nguyen, and Oded Regev. Lattice enumeration using extreme pruning. In *Advances in Cryptology – EUROCRYPT 2010, LNCS*, volume 6110, pages 257–278. Springer, 2010.

[7] Arjen Klaas Lenstra, Hendrik Willem Lenstra and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.

[8] The SageMath Developers. SageMath mathematics software (version 8.2), 2018, available: `http://www.sagemath.org/`

[9] Claus Peter Schnorr and Martin Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Journal of Mathematical Programming*, 66(1-3):181–199, 1994.