探索LEW問題の整数計画問題への帰着とその実行例

白勢 政明[1,a)]

概要：$(A, \boldsymbol{t})$ を探索 LWE 問題のインスタンスとする．但し，A は行列，t はベクトルである．先行研究は，A と $\boldsymbol{t}$ を使って目的関数が 2 次関数，制約式が線形等式で与えられる整数計画問題を構成できることを示した [12]．本稿は，小さな探索 LWE 問題のインスタンスに対して整数計画問題を構成し，それを整数計画ソルバー SCIP を用いて解いた結果を報告する．

キーワード：探索 LWE 問題，整数計画問題，格子暗号, 整数計画ソルバー

Reduction of Search LWE Problem to Integer Optimization Problem and Its Implementation

Masaaki Shirase[1,a)]

Abstract: Let $(A, \boldsymbol{t})$ be an instance of the search LWE problem, where A is a matrix and $\boldsymbol{t}$ is a vector. The previous work shown that A and $\boldsymbol{t}$ can be used to construct an integer programming problem where the objective function is a quadratic function and the constraint equations are given by linear equations[12]. This manuscript constructs an integer programming problem for an instance of a small search LWE problem, and solve it with the integer programming solver SCIP.

Keywords: Search LWE problems, Integer programming problems, Lattice-based cryptography, Integer programming solver

1. まえがき

公開鍵暗号の誕生は暗号の鍵配送問題を解決し，更にディジタル署名のような様々な暗号プロトコルを誕生させた．現在よく使用されている公開鍵暗号は RSA 暗号と楕円曲線暗号である．しかしながら，大規模な量子ゲートタイプの量子計算機が実現すると，Shor のアルゴリズムにより RSA 暗号と楕円曲線暗号は多項式時間で攻撃可能となってしまう [13]．大規模な量子計算機が実現しても安全性が損なわれない公開鍵暗号は耐量子計算機暗号と呼ばれ，その候補の 1 つとして格子暗号がある．

格子は，ベクトル空間 $\mathbb{R}^m$ の一次独立な n 個のベクトル $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n$ の整数係数の線形結合の全体の集合である．格子に関する問題として，最短ベクトル問題，最近ベクトル問題，learning with errors(LWE) 問題[*1]があり，これらの困難性を利用した公開鍵暗号が提案されている．

Regev により LWE 問題の困難性を利用した公開鍵暗号が提案され [11]，本稿ではこれを Regev 暗号と呼ぶ．module-LWE 問題の困難性を利用した Regev 暗号は CRYSTLS-Kyber と呼ばれる．米国国立標準技術研究所 (NIST) は 2017 年に耐量子計算機暗号の標準化のためのコンテストを開始した．現在も選定作業は続いているが，2022 年に CRYSTALS-Kyber が選択された [10]．従って，暗号分野において (module-)LWE 問題の困難性をより正確に調査することは重要な課題の 1 つである．

LWE 問題を解く方法はいくつか存在し，[5] には Bounded Distance Decoding 問題に帰着させ Babai の最近接平面アルゴリズム [2] を用いる方法，最短ベクトル問題に帰着させ LLL アルゴリズム [9] のような基底簡約アルゴリズムを

[1] 公立はこだて未来大学
Future University Hakoate
[a)] shirase@fun.ac.jp

[*1] LWE 問題には，探索 LWE 問題と判定 LWE 問題がある．

使って最短ベクトルを求める方法，BKW アルゴリズム [4] を使う方法，非線形方程式系へ帰着させる方法 [1] が紹介されている．また 2023 年に最大独立集合問題に帰着させる方法が提案された [8]．同じく 2023 年に本稿の著者は整数最適問題へ帰着させる方法を提案した [12].

本稿は，探索 LWE 問題の小さな例題を整数最適問題へ帰着させる方法によって解いた結果を報告する．

1.1 記号と表記

本稿は以下の記号を用いる．

p : 素数
$\mathbb{R}^n$: n 次元 (行) 実ベクトル空間
$\mathbb{Z}^n (\subset \mathbb{R}^n)$: 整数成分の n 次元 (行) ベクトルの集合
$\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$, $\mathbb{Z}_p$は有限体をなす
$\mathbb{Z}_p^n$: $\mathbb{Z}_p$成分の n 次元 (行) ベクトル空間
$\mathbb{Z}_p^{n\times m}$: $\mathbb{Z}_p$成分の $n \times m$ 行列の集合
E_n : $n \times n$ 単位行列
$\boldsymbol{\epsilon}_i \in \mathbb{R}^n$: 第 i 成分が 1 の単位ベクトル
$N(0, \sigma^2)$: 平均値 0, 標準偏差σの $\mathbb{Z}_p$上離散 Gauss 分布
$\mathbf{0}_n \in \mathbb{R}^n$: n 次元零ベクトル
$\|\boldsymbol{x}\|$: $\boldsymbol{x}$ のノルム
$\lfloor \cdot \rfloor$: floor 関数 (小数点以下切り捨て)

合同関係の表記

本稿で扱う合同式は全て p を法とするため，「$a \equiv b \pmod p$」を「$a \equiv b$」と略記する．$\boldsymbol{v} = (v_1, v_2, \cdots, v_n), \boldsymbol{w} = (w_1, w_2, \cdots, w_n) \in \mathbb{Z}^n$ に対して，すべての i に対して $v_i \equiv w_i$ の時，$\boldsymbol{v} \equiv \boldsymbol{w}$ と表記する．行列 $A = (a_{i,j}), B = (b_{i,j}) \in \mathbb{Z}_p^{n\times m}$ に対して，すべての i, j に対して $a_{i,j} \equiv b_{i,j}$ の時，$A \equiv B$ と表記する．

2. 準備

2.1 格子と探索 LWE 問題

格子 $L(\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n)$ は，ベクトル空間 $\mathbb{R}^m$ の一次独立な n 個の (行) ベクトル $\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n$ の整数係数の線形結合の集合

$$L(\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_n) = \left\{ \sum_{i=1}^{n} a_i \boldsymbol{b}_i \in \mathbb{R}^m : a_i \in \mathbb{Z} \right\}$$

である．

$A \in \mathbb{Z}_p^{n\times m}$ $(n < m)$，$\boldsymbol{s} \in \mathbb{Z}_p^n$，$\boldsymbol{e} \in \mathbb{Z}^m$，$\boldsymbol{t} \in \mathbb{Z}_p^m$ が

$$\boldsymbol{t} \equiv \boldsymbol{s}A + \boldsymbol{e} \tag{1}$$

を満たしているとする．但し，$\boldsymbol{e}$ の各成分は $N(0, \sigma^2)$ に従って選ばれるとする．この $\boldsymbol{e}$ はノイズベクトルまたは誤差ベクトルと呼ばれる．$(A, \boldsymbol{t})$ が与えられた時，$\boldsymbol{s}$ を求める問題を探索 LWE 問題と言う．

注意 1. $\boldsymbol{e}$ の各成分が $N(0, \sigma^2)$ に従って選ばれる時，$Pr[\|\boldsymbol{e}\| > 2\sqrt{m}\sigma] < 2^{-m+1}$ が成り立つ *[7]*．従って，$\|\boldsymbol{e}\|$ は大抵小さい値となる．*[5]* の *Lemma 1* や *Gauss* のヒューリスティックより，$\|\boldsymbol{e}\| \leq 2\sqrt{m}\sigma$ となる探索 *LWE* 問題のインスタンス $(A, \boldsymbol{t})$ が *2* つの解を持つ確率は無視できるほど小さい．

2.2 整数計画問題とソルバー

整数計画 (Integer Programming，IP) 問題は，与えられた制約式および整数条件のある変数に対して，目的関数の値を最適化 (最小化や最大化) する問題である．制約式は線形等式または線形不等式で与えられ，目的関数は線形関数または 2 次凸関数で与えられることが多い．IP 問題は一般には NP 困難であるが，効率的に解ける場合も多い．

IP 問題を解くソフトウェアを整数計画ソルバー (IP ソルバー) という．Zuse Institute Berlin により開発された SCIP は非商用 IP ソルバーの中で最速なソルバーの 1 つである [3]．本研究の実験は SCIP を用いている．

2.3 LP ファイル

本研究は IP 問題の記述に LP ファイルを用いている．ソルバーを利用するための IP 問題を記述するファイル形式は複数あるが，LP ファイルは文法が平易で可読性が高いという長所がある[*2]．

LP ファイルは，目的関数セクション，制約式セクション，上下限セクション，変数型セクション，end 宣言を記述する．

目的関数セクションでは，最大化問題の場合は「maximize」, 最小化問題の場合は「minimize」を記述し，それから目的関数を記述する．定数項があると動作しないソルバーがあるため，目的関数から定数項を除く方が望ましい．

制約式セクションでは，まず「subject to」を記述し，それから制約式を記述する．変数を含む項は等号不等号の左に，定数項は等号不等号の右にする．LP ファイルでは「>」と「>=」は同じ意味であり，同様に「<」は「<=」と同じ意味である．各制約式には「c1: ⋯」のように名前を付ける．

上下限セクションでは，自由変数（負の値も取りうる変数）に対して「変数 free」を記述する．不等号を用いて変数の範囲を指定することもできる．ここで記述しない変数は 0 以上の値を取る変数として扱われる．

変数型セクションでは，整数変数には「general」を，0-1 変数は「binary」を用いて宣言する．

最後に end 宣言を行う (「end」を記述する).

[*2] SCIP の使い方や LP ファイルの記述法については文献 [17] が大いに参考になった．但し，2 次式の目的関数の記述は [16] を参考にした．

3. 先行研究の手法 [12]

式 (1) を満たす行列 $A \in \mathbb{Z}_p^{n\times m}$, ベクトル $\boldsymbol{s} \in \mathbb{R}^n$, $\boldsymbol{e} \in \mathbb{Z}^m$, $\boldsymbol{t} \in \mathbb{R}^m$ に対して，$(A, \boldsymbol{t})$ を探索 LWE 問題のインスタンスとする．先行研究 [12] は，$(A, \boldsymbol{t})$ から $\boldsymbol{e}$ の成分が最適解となるような IP 問題を構成できることを示した．本節はその手法を紹介する．なお，3.2 節の注意 3 のように，$\boldsymbol{e}$(の一部) が得られれば探索 LWE 問題のインスタンスの解 $\boldsymbol{s}$ は簡単に計算できる．

3.1 行列とベクトルの分割

$A, \boldsymbol{t}, \boldsymbol{e}$ に対して，以下のように $A_0, A_1, \boldsymbol{t}_0, \boldsymbol{t}_1, \boldsymbol{e}_0, \boldsymbol{e}_1$ を定義する．

$A = (A_0\ A_1)$,
但し $\begin{cases} A_0 = A \text{ の左側の } n\times n \text{ 行列} \\ A_1 = A \text{ の右側の } n\times(m-n) \text{ 行列} \end{cases}$

$\boldsymbol{t} = (\boldsymbol{t}_0\ \boldsymbol{t}_1)$,
但し $\begin{cases} \boldsymbol{t}_0 = \boldsymbol{t} \text{ の左側の } n \text{ 次元ベクトル} \\ \boldsymbol{t}_1 = \boldsymbol{t} \text{ の右側の } (m-n) \text{ 次元ベクトル} \end{cases}$

$\boldsymbol{e} = (\boldsymbol{e}_0\ \boldsymbol{e}_1)$,
但し $\begin{cases} \boldsymbol{e}_0 = \boldsymbol{e} \text{ の左側の } n \text{ 次元ベクトル} \\ \boldsymbol{e}_1 = \boldsymbol{e} \text{ の右側の } (m-n) \text{ 次元ベクトル} \end{cases}$

例えば，$A = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 & 9 \end{pmatrix}$ とすると，$A_0 = \begin{pmatrix} 0 & 1 \\ 5 & 6 \end{pmatrix}$, $A_1 = \begin{pmatrix} 2 & 3 & 4 \\ 7 & 8 & 9 \end{pmatrix}$ であり，$\boldsymbol{t} = (0,1,2,3,4)$ とすると $\boldsymbol{t}_0 = (0,1)$, $\boldsymbol{t}_1 = (2,3,4)$ である．すると，式 (1) は

$$\begin{aligned} \boldsymbol{t}_0 &\equiv \boldsymbol{s}A_0 + \boldsymbol{e}_0 \\ \boldsymbol{t}_1 &\equiv \boldsymbol{s}A_1 + \boldsymbol{e}_1 \end{aligned} \tag{2}$$

と書ける．

3.2 写像 $\phi, \psi : \mathbb{R}^n \to \mathbb{R}^{m-n}$

行列 $A_0 \in \mathbb{Z}_p^{n\times n}$ は $\mathbb{Z}_p$ 上で正則である[*3]と仮定する．すると，

$$A_0 A_0^{-1} \equiv A_0^{-1} A_0 \equiv E_n$$

を満たす行列 $A_0^{-1} \in \mathbb{Z}_p^{n\times n}$ が存在する．実際に，有限体 $\mathbb{Z}_p$ 上で A_0 の逆行列を計算した結果が A_0^{-1} となる．A_0^{-1} の計算は PARI/GP[14] のような数学ソフトウェアを使えば簡単に行うことができる．A_0^{-1}, A_1, $\boldsymbol{t}_0$, $\boldsymbol{t}_1$ を使って，写像 $\phi : \mathbb{R}^n \to \mathbb{R}^{m-n}$ を次のように定義する．

$$\begin{array}{rccl} \phi: & \mathbb{R}^n & \to & \mathbb{R}^{m-n} \\ & \boldsymbol{v} & \mapsto & \boldsymbol{v}A_0^{-1}A_1 + \boldsymbol{t}_1 - \boldsymbol{t}_0 A_0^{-1} A_1 \end{array}$$

[*3] A の行列式が p の倍数でないことと同等である．

更に，別の写像 $\psi : \mathbb{R}^n \to \mathbb{R}^{m-n}$ を

$$\psi(\boldsymbol{v}) = \phi(\boldsymbol{v}) - \phi(\boldsymbol{0}_n)$$

と定義する．写像 ϕ と ψ は次の性質を持つ．

命題 2. *(a)* $\phi(\boldsymbol{e}_0) \equiv \boldsymbol{e}_1$
(b) $\boldsymbol{v}_0 \in \mathbb{R}^n$, $\boldsymbol{v}_1 \in \mathbb{R}^{m-n}$ が $\phi(\boldsymbol{v}_0) \equiv \boldsymbol{v}_1$ を満たすとする．$\hat{\boldsymbol{s}} \equiv (\boldsymbol{t}_0 - \boldsymbol{v}_0)A_0^{-1}$ とおくと，$(\boldsymbol{t}_0\ \boldsymbol{t}_1) = \hat{\boldsymbol{s}}(A_0\ A_1) + (\boldsymbol{v}_0\ \boldsymbol{v}_1)$ が成り立つ
(c) $\phi(\boldsymbol{0}_n) = \boldsymbol{t}_1 - \boldsymbol{t}_0 A_0^{-1} A_1$
(d) $\psi(\boldsymbol{v}) = \boldsymbol{v}A_0^{-1}A_1$ (つまりψは線形写像)
(e) $k_i \in \mathbb{Z}$ に対して，次が成り立つ．

$$\sum k_i(\phi(\boldsymbol{v}_i) - \phi(\boldsymbol{0}_n)) = \phi(\sum(k_i \boldsymbol{v}_i)) - \phi(\boldsymbol{0}_n)$$

Proof. [12] を参照. □

注意 3. 探索 *LWE* 問題のインスタンス $(A, \boldsymbol{t})$ が与えられた時，*3.1* 節のように A_0，$\boldsymbol{t}_0$，$\boldsymbol{e}_0$ を定める．A_0 は $\mathbb{Z}_p$ 上正則と仮定する．すると，式 *(2)* より

$$\boldsymbol{s} \equiv (\boldsymbol{t}_0 - \boldsymbol{e}_0)A_0^{-1}$$

が成り立つので，このインスタンスを解くには $\boldsymbol{e}_0$ を得れば十分である．

3.3 IP 問題の構成

$\boldsymbol{e} = (e_1, e_2, \cdots, e_m)$ $(e_i \in \mathbb{Z})$ とすると，$\boldsymbol{e}_0$ と $\boldsymbol{e}_1$ は

$$\begin{cases} \boldsymbol{e}_0 = (e_1, e_2, \cdots, e_n) \\ \boldsymbol{e}_1 = (e_{n+1}, e_{n+2}, \cdots, e_m) \end{cases} \tag{3}$$

と書ける．更に，$\boldsymbol{e}_0$ は各単位ベクトル $\boldsymbol{\epsilon}_i$ を使って，

$$\boldsymbol{e}_0 = e_1\boldsymbol{\epsilon}_1 + e_2\boldsymbol{\epsilon}_2 + \cdots + e_n\boldsymbol{\epsilon}_n \tag{4}$$

と書ける．$i = 1, 2, \cdots, n$ に対して，$\boldsymbol{w}_i$ を

$$\boldsymbol{w}_i = \phi(\boldsymbol{\epsilon}_i) - \phi(\boldsymbol{0}_n) (= \psi(\boldsymbol{\epsilon}_i)) \in \mathbb{R}^{m-n} \tag{5}$$

と定義し，その成分を

$$\boldsymbol{w}_i = (w_{i,1}, w_{i,2}, \cdots, w_{i,m-n})\ (w_{i,j} \in \mathbb{Z}_p) \tag{6}$$

とする．加えて，

$$\phi(\boldsymbol{0}_n) = (u_1, u_2, \cdots, u_{m-n})\ (u_i \in \mathbb{Z}_p) \tag{7}$$

とする．すると，次の計算が得られる．

$$\begin{aligned} &\boldsymbol{e}_1 \\ \equiv &\phi(\boldsymbol{e}_0) && \text{命題 2(a) より} \\ = &\phi(e_1\boldsymbol{\epsilon}_1 + e_2\boldsymbol{\epsilon}_2 + \cdots + e_n\boldsymbol{\epsilon}_n) && \text{(4) より} \\ = &\sum_{i=1}^{n}(e_i(\phi(\boldsymbol{\epsilon}_i) - \phi(\boldsymbol{0}_n)) + \phi(\boldsymbol{0}_n)) && \text{命題 2(e) より} \\ = &e_1\boldsymbol{w}_1 + e_2\boldsymbol{w}_2 + \cdots + e_n\boldsymbol{w}_n + \phi(\boldsymbol{0}_n) && \text{(5) より} \end{aligned} \tag{8}$$

よって，$i = 1, 2, \cdots, m-n$ に対して，式 (3)，(6)，(7)，(8) より

$$e_{n+i} \equiv w_{1,i}e_1 + w_{2,i}e_2 + \cdots + w_{n,i}e_n + u_i \tag{9}$$

と書ける．従って，次の $x_1, x_2, \cdots, x_m$ を変数とする $\mathbb{Z}_p$ 上線形方程式系は解 $(x_1, x_2, \cdots, x_m) = (e_1, e_2, \cdots, e_m)$ を持つ．

$$\begin{cases} w_{1,1}x_1 + w_{2,1}x_2 + \cdots + w_{n,1}x_n + u_1 = x_{n+1} \\ w_{1,2}x_1 + w_{2,2}x_2 + \cdots + w_{n,2}x_n + u_2 = x_{n+2} \\ \qquad\qquad\qquad\qquad \vdots \\ w_{1,m-n}x_1 + w_{2,m-n}x_2 + \cdots + w_{n,m-n}x_n + u_{m-n} = x_m \end{cases}$$

しかし，

$$m(\text{ 変数の個数 }) > m - n(\text{ 式の個数 })$$

であるため，この方程式系の解は一意ではない．そこで，この方程式系を IP 問題へ改変する．合同式 (9) は，ある $f_i \in \mathbb{Z}$ を用いて，整数の等式

$$w_{1,i}e_1 + w_{2,i}e_2 + \cdots + w_{n,i}e_n - e_{n+i} + pf_i = -u_i \tag{10}$$

に書き換えることができる．

次に $\boldsymbol{e}$ の成分 e_i と f_i の範囲を考える．e_i は $N(0, \sigma^2)$ に従って選ばれるので，高い確率で

$$-t \le e_i \le t \ (i = 1, 2, \cdots, m)$$

を満たす $t \in \mathbb{N}$ を選ぶことができる．すると，$0 \le w_{i,j} \le p-1$ であることと式 (10) より f_i の範囲

$$-\left\lfloor \frac{t(np-n+1)+p-1}{p} \right\rfloor \le f_i \le \left\lfloor \frac{t(np-n+1)}{p} \right\rfloor$$
$$(i = 1, 2, \cdots, m-n)$$

が得られる．また，注意 1 より $\|\boldsymbol{e}\|$ は十分小さい値になる．

次の補題は，$w_{i,j}$ と u_i の効率的な計算法を与える．

補題 4. 探索 *LWE* 問題のインスタンス $(A, \boldsymbol{t})$ が与えられているとする．ここで，$A \in \mathbb{Z}_p^{n\times m}$ $(n < m)$, $\boldsymbol{t} \in \mathbb{R}^m$ とする．A_0 と $\boldsymbol{t}_0$ を *3.1* 節のようにセットする．A_0 は $\mathbb{Z}_p$ 上正則であると仮定する．

(a) 式 *(6)* で与えられる $w_{i,j}$ を使って，$n \times (n-m)$ 行列 W を $W = (w_{i,j})$ と定義する．すると，$W \equiv A_0^{-1}A_1$ である．

(b) 式 *(7)* で与えられる u_i に対して，次が成り立つ．

$$(u_1, u_2, \cdots, u_{m-n}) = \boldsymbol{t}_1 - \boldsymbol{t}_0 A_0^{-1} A_1$$

Proof. [12] を参照. □

命題 5. 式 *(1)* を満たす探索 *LWE* 問題のインスタンス $(A, \boldsymbol{t})$ が与えられているとする．ここで，$A \in \mathbb{Z}_p^{n\times m}$ $(n < m)$, $\boldsymbol{t} \in \mathbb{R}^m$ とする．A_0 と $\boldsymbol{t}_0$ を *3.1* 節のようにセットする．A_0 は $\mathbb{Z}_p$ 上正則であると仮定する．$w_{i,j}, u_i$ $(i = 0, 1, \cdots, n,\ j = 1, 2, \cdots, m-n)$ を補題 *4* のように計算し，$t \in \mathbb{N}$ を選ぶ．x_i, y_j を変数とする次のような *IP* 問題を構成する．

$$\begin{cases} \textbf{目的関数} \\ x_1^2 + x_2^2 + \cdots + x_m^2 \to \text{最小} \\ \textbf{制約式} \\ w_{1,1}x_1 + w_{2,1}x_2 + \cdots + w_{n,1}x_n - x_{n+1} + py_1 = -u_1 \\ w_{1,2}x_1 + w_{2,2}x_2 + \cdots + w_{n,2}x_n - x_{n+2} + py_2 = -u_2 \\ \qquad\qquad\qquad\qquad \vdots \\ w_{1,m-n}x_1 + w_{2,m-n}x_2 + \cdots + w_{n,m-n}x_n - x_m + py_{m-n} = -u_{m-n} \\ -t \le x_i \le t \\ -\lfloor (t(np-n+1)+p-1)/p \rfloor \le y_i \le \lfloor (t(np-n+1)/p \rfloor \\ x_i, y_j \in \mathbb{Z} \quad (i = 0, 1, \cdots, n,\ j = 1, 2, \cdots, m-n) \end{cases}$$

IP ソルバーにより出力されるこの問題の最適解またはノルムが小さい暫定解 $(x_1, x_2, \cdots, x_m) = (\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_m)$ に対して，$\hat{\boldsymbol{x}}_0 = (\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_n) \in \mathbb{R}^n$ とおく．すると，

$$\hat{\boldsymbol{s}} = (\boldsymbol{t}_0 - \boldsymbol{x}_0)A_0^{-1}$$

は高い確率で探索 *LWE* 問題のインスタンス $(A, \boldsymbol{t})$ の解である．

Proof. [12] を参照. □

4. 探索 LWE 問題の解決例

本節は本稿の主結果である．

4.1 IP 問題の構成

適切なサイズと思われるので，文献 [15] の例 5.2.5 の探索 LWE 問題のインスタンス $(A, \boldsymbol{t})$ を例題として命題 5 を使って解いてみる．ここで，A は図 1 で与えられ，$\boldsymbol{t} =$ (50,41,53,64,24,28,2,22,43,32,25,16,2,30,96,53,66,89,87,29) である．なお，この例題のノイズベクトル $\boldsymbol{e}$ は

$$\boldsymbol{e} = (-1, -2, 0, 5, 0, 1, -1, 0, 1, -1, 1, 1, 2, -2, 0, -1, 3, 0, 1) \tag{11}$$

であり，解 $\boldsymbol{s}$ は $\boldsymbol{s} = (7, 16, 45, 45, 64, 70, 79, 82, 65, 36)$ である．すると，3.1 節で定義した $A_0, A_1, \boldsymbol{t}_0, \boldsymbol{t}_1$ は次のようになる．

$$A_0 = \begin{pmatrix} 88 & 53 & 93 & 66 & 39 & 46 & 47 & 26 & 10 & 54 \\ 3 & 1 & 49 & 82 & 42 & 18 & 45 & 94 & 67 & 83 \\ 2 & 25 & 56 & 83 & 96 & 79 & 27 & 45 & 83 & 77 \\ 1 & 22 & 89 & 58 & 76 & 64 & 83 & 87 & 55 & 79 \\ 80 & 68 & 78 & 95 & 64 & 11 & 79 & 67 & 5 & 4 \\ 68 & 17 & 24 & 15 & 40 & 31 & 14 & 36 & 94 & 53 \\ 18 & 52 & 29 & 45 & 42 & 82 & 5 & 95 & 42 & 38 \\ 12 & 19 & 55 & 59 & 72 & 50 & 75 & 50 & 73 & 37 \\ 52 & 6 & 78 & 98 & 59 & 87 & 32 & 24 & 26 & 26 \\ 63 & 99 & 44 & 9 & 34 & 43 & 50 & 48 & 20 & 44 \end{pmatrix}$$

$$A = \begin{pmatrix} 88 & 53 & 93 & 66 & 39 & 46 & 47 & 26 & 10 & 54 & 41 & 23 & 37 & 60 & 39 & 39 & 2 & 9 & 19 & 83 \\ 3 & 1 & 49 & 82 & 42 & 18 & 45 & 94 & 67 & 83 & 66 & 93 & 96 & 29 & 72 & 1 & 68 & 68 & 34 & 24 \\ 62 & 25 & 56 & 83 & 96 & 79 & 27 & 45 & 83 & 77 & 64 & 90 & 87 & 18 & 34 & 99 & 50 & 47 & 71 & 13 \\ 1 & 22 & 89 & 58 & 76 & 64 & 83 & 87 & 55 & 79 & 18 & 86 & 48 & 17 & 57 & 35 & 37 & 22 & 40 & 40 \\ 80 & 68 & 78 & 95 & 64 & 11 & 79 & 67 & 5 & 4 & 61 & 67 & 52 & 3 & 11 & 42 & 0 & 2 & 97 & 65 \\ 68 & 17 & 24 & 15 & 40 & 31 & 14 & 36 & 94 & 53 & 76 & 19 & 84 & 10 & 8 & 50 & 97 & 76 & 76 & 96 \\ 18 & 52 & 29 & 45 & 42 & 82 & 5 & 95 & 42 & 38 & 95 & 31 & 0 & 83 & 19 & 72 & 14 & 81 & 17 & 37 \\ 12 & 19 & 55 & 59 & 72 & 50 & 75 & 50 & 73 & 37 & 73 & 19 & 3 & 31 & 34 & 76 & 67 & 19 & 66 & 75 \\ 52 & 6 & 78 & 98 & 59 & 87 & 32 & 24 & 26 & 26 & 23 & 99 & 56 & 12 & 97 & 49 & 67 & 65 & 98 & 2 \\ 63 & 99 & 44 & 9 & 34 & 43 & 50 & 48 & 20 & 44 & 74 & 8 & 37 & 68 & 28 & 61 & 71 & 27 & 75 & 60 \end{pmatrix}$$

図 1 探索 LWE 問題の例題の A

$$A_1 = \begin{pmatrix} 41 & 23 & 37 & 60 & 39 & 39 & 2 & 9 & 19 & 83 \\ 66 & 93 & 96 & 29 & 72 & 1 & 68 & 68 & 34 & 24 \\ 64 & 90 & 87 & 18 & 34 & 99 & 50 & 47 & 71 & 13 \\ 18 & 86 & 48 & 17 & 57 & 35 & 37 & 22 & 40 & 40 \\ 61 & 67 & 52 & 3 & 11 & 42 & 0 & 2 & 97 & 65 \\ 76 & 19 & 84 & 10 & 8 & 50 & 97 & 76 & 76 & 96 \\ 95 & 31 & 0 & 83 & 19 & 72 & 14 & 81 & 17 & 37 \\ 73 & 19 & 3 & 31 & 34 & 76 & 67 & 19 & 66 & 75 \\ 23 & 99 & 56 & 12 & 97 & 49 & 67 & 65 & 98 & 2 \\ 74 & 8 & 37 & 68 & 28 & 61 & 71 & 27 & 75 & 60 \end{pmatrix}$$

$\boldsymbol{t}_0 = (50, 41, 53, 64, 24, 28, 2, 22, 43, 32)$

$\boldsymbol{t}_1 = (25, 16, 2, 30, 96, 53, 66, 89, 87, 29)$

また，A_0^{-1} は次のようになる．

$$A_0^{-1} = \begin{pmatrix} 27 & 15 & 96 & 67 & 91 & 92 & 49 & 61 & 80 & 95 \\ 38 & 48 & 9 & 45 & 20 & 94 & 33 & 18 & 99 & 100 \\ 90 & 82 & 55 & 85 & 40 & 52 & 69 & 93 & 39 & 60 \\ 96 & 39 & 12 & 43 & 91 & 29 & 59 & 3 & 79 & 95 \\ 69 & 90 & 90 & 96 & 86 & 53 & 45 & 18 & 25 & 58 \\ 8 & 58 & 10 & 14 & 88 & 64 & 23 & 100 & 51 & 0 \\ 93 & 6 & 1 & 43 & 43 & 44 & 45 & 46 & 0 & 33 \\ 65 & 95 & 58 & 36 & 29 & 6 & 100 & 56 & 19 & 47 \\ 69 & 8 & 5 & 89 & 54 & 88 & 46 & 46 & 93 & 98 \\ 9 & 59 & 13 & 32 & 9 & 53 & 9 & 56 & 24 & 54 \end{pmatrix}$$

補題 4 のように W と $\boldsymbol{t}_1 - \boldsymbol{t}_0 A_0^{-1} A_1$ を計算すると

$$W = \begin{pmatrix} 73 & 69 & 2 & 0 & 37 & 30 & 17 & 46 & 5 & 93 \\ 19 & 62 & 22 & 17 & 1 & 92 & 78 & 12 & 3 & 66 \\ 37 & 36 & 90 & 74 & 55 & 64 & 61 & 23 & 19 & 11 \\ 77 & 54 & 68 & 94 & 71 & 34 & 6 & 51 & 97 & 71 \\ 31 & 85 & 98 & 36 & 46 & 81 & 12 & 19 & 71 & 22 \\ 82 & 34 & 11 & 15 & 33 & 99 & 11 & 45 & 99 & 35 \\ 81 & 9 & 26 & 34 & 6 & 14 & 34 & 69 & 80 & 76 \\ 97 & 56 & 52 & 1 & 24 & 43 & 57 & 20 & 37 & 60 \\ 60 & 39 & 31 & 43 & 74 & 20 & 83 & 13 & 33 & 97 \\ 44 & 25 & 25 & 30 & 72 & 69 & 24 & 24 & 39 & 37 \end{pmatrix}$$

$\boldsymbol{t}_1 - \boldsymbol{t}_0 A_0^{-1} A_1 = (88, 20, 49, 59, 64, 49, 84, 0, 37, 17)$

となる．命題 5 で構成される IP 問題は図 3 のようになる．

```
SCIP> display solution

objective value:                                28
x1                                              -1   (obj:0)
x2                                              -2   (obj:0)
x4                                               5   (obj:0)
x6                                               1   (obj:0)
x7                                              -1   (obj:0)
x8                                               1   (obj:0)
x10                                              1   (obj:0)
y1                                               5   (obj:0)
y2                                               2   (obj:0)
y3                                               4   (obj:0)
y4                                               5   (obj:0)
y5                                               5   (obj:0)
y6                                               2   (obj:0)
y8                                               2   (obj:0)
y9                                               6   (obj:0)
y10                                              2   (obj:0)
quadobjvar                                      28   (obj:1)
x11                                             -1   (obj:0)
x12                                              1   (obj:0)
x13                                              1   (obj:0)
x14                                              2   (obj:0)
x15                                             -2   (obj:0)
x17                                             -1   (obj:0)
x18                                              3   (obj:0)
x20                                              1   (obj:0)
```

図 2 SCIP の出力

4.2 IP ソルバーによる解決

図 3 の IP 問題の LP ファイルは図 4 のようになる．なお，この LP ファイルでは変数 x_{10} から x_{20} は整数変数の宣言をしておらず，y_1 から y_{10} は制限を与えず自由変数宣言のみを行っている．その理由はこうした方が SCIP の実行時間が短くなるからである．

IP ソルバー SCIP にこの LP ファイルを読み込ませ最適化処理を実行すると，図 2 のような暫定解が得られる[*4]．これは

$$\begin{array}{lllll} x_1 = -1, & x_2 = 2, & x_3 = 0, & x_4 = 5, & x_5 = 0, \\ x_6 = 1, & x_7 = -1, & x_8 = 1, & x_9 = 0, & x_{10} = 1, \\ x_{11} = -1, & x_{12} = 1, & x_{13} = 1, & x_{14} = 2, & x_{15} = -2, \\ x_{16} = 0, & x_{17} = -1, & x_{18} = 3, & x_{19} = 0, & x_{20} = 1 \end{array}$$

を意味する．これは式 (11) と同じであるため，正しくノイズベクトルが得られたことが分かる．注意 3 よりノイズベクトルから探索 LWE 問題のインスタンスの解がすぐに得られる．

[*4] SCIP は解が 0 の場合は出力しない．

目的関数

$x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2 + x_9^2 + x_{10}^2 + x_{11}^2 + x_{12}^2 + x_{13}^2 + x_{14}^2 + x_{15}^2 + x_{16}^2 + x_{17}^2 + x_{18}^2 + x_{19}^2 + x_{20}^2 \rightarrow$ 最小

制約式

$73x_1 + 19x_2 + 37x_3 + 77x_4 + 31x_5 + 82x_6 + 81x_7 + 97x_8 + 60x_9 + 44x_{10} - x_{11} - 101y_1 = -88$

$69x_1 + 62x_2 + 36x_3 + 54x_4 + 85x_5 + 34x_6 + 9x_7 + 56x_8 + 39x_9 + 25x_{10} - x_{12} - 101y_2 = -20$

$2x_1 + 22x_2 + 90x_3 + 68x_4 + 98x_5 + 11x_6 + 26x_7 + 52x_8 + 31x_9 + 25x_{10} - x_{13} - 101y_3 = -49$

$0x_1 + 17x_2 + 74x_3 + 94x_4 + 36x_5 + 15x_6 + 34x_7 + 1x_8 + 43x_9 + 30x_{10} - x_{14} - 101y_4 = -59$

$37x_1 + 1x_2 + 55x_3 + 71x_4 + 46x_5 + 33x_6 + 6x_7 + 24x_8 + 74x_9 + 72x_{10} - x_{15} - 101y_5 = -64$

$30x_1 + 92x_2 + 64x_3 + 34x_4 + 81x_5 + 99x_6 + 14x_7 + 43x_8 + 20x_9 + 69x_{10} - x_{16} - 101y_6 = -49$

$17x_1 + 78x_2 + 61x_3 + 6x_4 + 12x_5 + 11x_6 + 34x_7 + 57x_8 + 83x_9 + 24x_{10} - x_{17} - 101y_7 = -84$

$46x_1 + 12x_2 + 23x_3 + 51x_4 + 19x_5 + 45x_6 + 69x_7 + 20x_8 + 13x_9 + 24x_{10} - x_{18} - 101y_8 = 0$

$5x_1 + 3x_2 + 19x_3 + 97x_4 + 71x_5 + 99x_6 + 80x_7 + 37x_8 + 33x_9 + 39x_{10} - x_{19} - 101y_9 = -37$

$93x_1 + 66x_2 + 11x_3 + 71x_4 + 22x_5 + 35x_6 + 76x_7 + 60x_8 + 97x_9 + 37x_{10} - x_{20} - 101y_{10} = -17$

(各変数の範囲は省略)

図 3 構成した IP 問題

本稿の計算機環境は次の通りである．

プロセッサ	Intel(R) Core(TM) i3-8145U 2.10GHz
RAM	8.00 GB
OS	Windows 11 Home ver.22H2

結果が得られるのに要した時間は正確には計測していないが，10 分以上 1 時間未満であった．(SCIP の実行開始から停止までの時間でなく，正解と等しい暫定解を出力するまでの時間である．) なお，この時 PC は他の作業にも用いていた．この例題では $y_i \geq 0$ であるため各 y_i の free 宣言が無くても正しい結果が得られる．最初は各 y_i の free 宣言無しで実行してしまったのだが，その時は数分程度で結果が得られた．もし何らかの方法で y_i の正負を知ることができれば，この手法に要する時間を短くすることができそうである．

A が 40×1600 行列であるような探索 LWE 問題のインスタンスが 2 秒で解けたという例がある [6]．従って，既存の手法と比較して提案手法は高速であるとは言えない．

4.3 考察と課題

著者が知る限り，暗号攻撃と IP 問題 (より広く数理計画問題) は関係するとは思われてこなかった．そのため著者は IP 問題の知識がなく IP 問題を解く設備を有しておらず，図 3 のような IP 問題を解くにあたり，非商用 IP ソルバー SCIP を利用する手段しかなかった．

現時点で以下のような課題があると考える．1) もし商用 IP ソルバーを用いれば, 提案手法はどのくらい高速になるのか．2) 探索 LWE 問題から得られる IP 問題を解くには既存の IP ソルバーに頼るのではなく，解法を自ら探るべきなのか．また，より簡単な課題として，3) $\mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$ の代わりに $\mathbb{Z}_p = \{-(p-1)/2, -(p-3)/2, \cdots, (p-1)/2\}$ とすると，IP ソルバーの実行時間に変化が起こるか, 4) 目的関数を「$x_1^2+x_2^2+\cdots+x_m^2 \rightarrow$ 最小」の代わりに「$|x_1|+|x_2|+\cdots+|x_m| \rightarrow$ 最小」とすると IP ソルバーの実行時間に変化が起こるか, が挙げられる．

5. まとめと今後の課題

本稿は探索 LWE 問題を IP 問題に帰着させる先行研究を紹介し，その手法を使って探索 LWE 問題の小さな例題を解いた．現時点では実行時間に関して，この手法は既存の探索 LWE 問題を解く手法の代替にはならないようであるが，今後の改良に期待したい．4.3 節の課題の解決を今後の課題としたい．

参考文献

[1] Sanjeev Arora and Rong Ge. New algorithms for learning in presence of errors. In *International Colloquium on Automata, Languages, and Programming*, pages 403–415. Springer, 2011.

[2] László Babai. On lovász' lattice reduction and the nearest lattice point problem. *Combinatorica*, 6:1–13, 1986.

[3] Zuse Institute Berlin. Scip (solving constraint integer programs), 2023. `https://scipopt.org/`.

[4] Avrim Blum, Adam Kalai, and Hal Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model. *Journal of the ACM (JACM)*, 50(4):506–519, 2003.

[5] Johannes Buchmann, Niklas Büscher, Florian Göpfert, Stefan Katzenbeisser, Juliane Krämer, Daniele Micciancio, Sander Siim, Christine van Vredendaal, and Michael Walter. Creating cryptographic challenges using multi-party computation: The LWE challenge. In *Proceedings of the 3rd ACM International Workshop on ASIA Public-Key Cryptography*, pages 11–20, 2016.

[6] T. U. Darmstadt. LWE challenge. `https://www.latticechallenge.org/lwe_challenge/challenge.php`, 最終アクセス 2023/08/21.

[7] Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky. Lattice signatures and bimodal gaussians. In *Annual Cryptology Conference*, pages 40–56. Springer, 2013.

[8] Yasuhito Kawano. A reduction from an LWE problem to maximum independent set problems. *Scientific Reports*, 13(1):7130, 2023.

```
minimize
[x1^2 + x2^2 + x3^2 +x4^2 + x5^2 + x6^2 + x7^2 + x8^2 + x9^2 + x10^2 + x11^2 + x12^2 + x13^2 + x14^2
+ x15^2 + x16^2 + x17^2 + x18^2 + x19^2 + x20^2]/ 2
subject to
c1: 73 x1 + 19 x2 + 37 x3 + 77 x4 + 31 x5 + 82 x6 + 81 x7 + 97 x8 + 60 x9 + 44 x10 - x11 - 101 y1 = - 88
c2: 69 x1 + 62 x2 + 36 x3 + 54 x4 + 85 x5 + 34 x6 +  9 x7 + 56 x8 + 39 x9 + 25 x10 - x12 - 101 y2 = - 20
c3: 2  x1 + 22 x2 + 90 x3 + 68 x4 + 98 x5 + 11 x6 + 26 x7 + 52 x8 + 31 x9 + 25 x10 - x13 - 101 y3 = - 49
c4:  0 x1 + 17 x2 + 74 x3 + 94 x4 + 36 x5 + 15 x6 + 34 x7 +  1 x8 + 43 x9 + 30 x10 - x14 - 101 y4 = - 59
c5: 37 x1 +  1 x2 + 55 x3 + 71 x4 + 46 x5 + 33 x6 +  6 x7 + 24 x8 + 74 x9 + 72 x10 - x15 - 101 y5 = - 64
c6: 30 x1 + 92 x2 + 64 x3 + 34 x4 + 81 x5 + 99 x6 + 14 x7 + 43 x8 + 20 x9 + 69 x10 - x16 - 101 y6 = - 49
c7: 17 x1 + 78 x2 + 61 x3 +  6 x4 + 12 x5 + 11 x6 + 34 x7 + 57 x8 + 83 x9 + 24 x10 - x17 - 101 y7 = - 84
c8: 46 x1 + 12 x2 + 23 x3 + 51 x4 + 19 x5 + 45 x6 + 69 x7 + 20 x8 + 13 x9 + 24 x10 - x18 - 101 y8 = 0
c9:  5 x1 +  3 x2 + 19 x3 + 97 x4 + 71 x5 + 99 x6 + 80 x7 + 37 x8 + 33 x9 + 39 x10 - x19 - 101 y9 = - 37
c10: 93 x1 + 66 x2 + 11 x3 + 71 x4 + 22 x5 + 35 x6 + 76 x7 + 60 x8 + 97 x9 + 37 x10 - x20 - 101 y10 = - 17
bounds
-5 < x1 < 5
-5 < x2 < 5
-5 < x3 < 5
-5 < x4 < 5
-5 < x5 < 5
-5 < x6 < 5
-5 < x7 < 5
-5 < x8 < 5
-5 < x9 < 5
-5 < x10 < 5
-5 < x11 < 5
-5 < x12 < 5
-5 < x13 < 5
-5 < x14 < 5
-5 < x15 < 5
-5 < x16 < 5
-5 < x17 < 5
-5 < x18 < 5
-5 < x19 < 5
-5 < x20 < 5
y1 free
y2 free
y3 free
y4 free
y5 free
y6 free
y7 free
y8 free
y9 free
y10 free
general
x1 x2 x3 x4 x5 x6 x7 x8 x9 x10 y1 y2 y3 y4 y5 y6 y7 y8 y9 y10
end
```

図 4　IP 問題の LP ファイルの記述

[9] Arjen K Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische annalen*, 261(ARTICLE):515–534, 1982.

[10] NIST. Post-quantum cryptography. https://csrc.nist.gov/projects/post-quantum-cryptography, 最終アクセス 2023/08/21.

[11] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):1–40, 2009.

[12] Masaaki Shirase. Reduction of search-lwe problem to integer programming problem. Cryptology ePrint Archive, Paper 2023/1162, 2023. https://eprint.iacr.org/2023/1162, 最終アクセス 2023/08/21.

[13] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[14] The PARI Development Team. Pari/gp. http://pari.math.u-bordeaux.fr/, 最終アクセス 2023/08/21.

[15] 青野良範, 安田雅哉. 格子暗号解読のための数学的基礎: 格子基底簡約アルゴリズム入門. 近代科学社, 2019.

[16] 宮代隆平. 整数計画法メモ. https://web.tuat.ac.jp/~miya/ipmemo.html, 最終アクセス 2023/08/21.

[17] 宮代隆平. 整数計画ソルバー入門. オペレーションズ・リサーチ, 57(4):183–189, 2012.