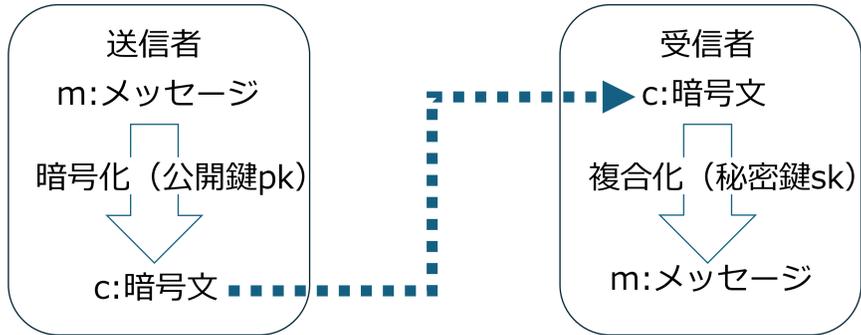


暗号と情報社会

公開鍵暗号

暗号化する鍵（公開鍵pk）と復号する鍵（秘密鍵sk）が異なる暗号方式
 RSA暗号（素因数分解）や楕円曲線暗号（離散対数問題）が主流
 ・データの盗聴を防ぐ（SSL/TLS）
 ・データが改竄されていないことを示す（マイナンバーカード）



耐量子計算機暗号

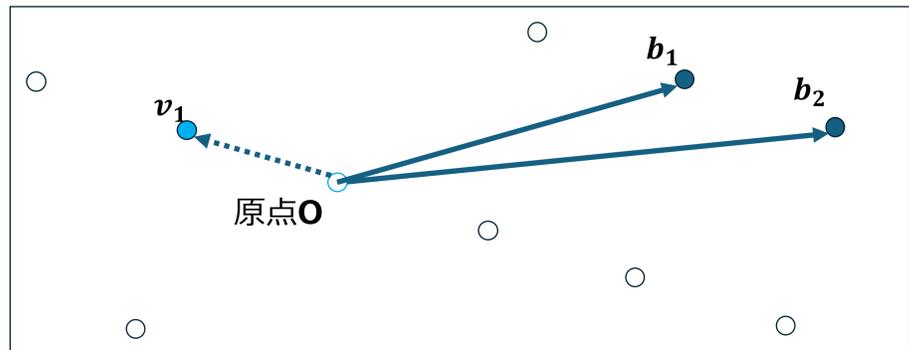
従来暗号方式の危殆化

・素因数分解や離散対数問題を高速で解く量子アルゴリズムの発見
 ・大規模な量子計算機の発展
 →量子計算機が実用化された社会でも安全な暗号方式の開発

主な耐量子計算機暗号

- ・格子暗号：原点が一番近い格子点を見つけることの困難性を利用
暗号化したまま計算が可能な準同型暗号の開発
CRYSTALS-Kyberが既に採択
- ・多変数多項式暗号：多変数連立2次方程式の求解問題を利用
QR-UOV (NTT研究所) など
- ・同種写像暗号：2つの楕円曲線間の代数的な写像を発見する
同種写像問題の困難性を利用
大江さんの研究：高次元化への理論的保証

格子暗号の基礎



格子：一次独立な \mathbb{R}^m のベクトルたちの整数係数線型結合で表されるベクトルの集合
 \mathbb{Z}^m に含まれる格子を整数格子という

$$L = \mathcal{L}(\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n) = \{ \sum_{i=1}^n a_i \mathbf{b}_i : a_i \in \mathbb{Z} \}$$

基底：格子を生成する一次独立なベクトルの組 $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$

基底行列：基底ベクトルを行ベクトルに持つ $n \times m$ 行列

$$B = \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_n \end{pmatrix} = \begin{pmatrix} b_{11} & \dots & b_{1m} \\ \vdots & \ddots & \vdots \\ b_{n1} & \dots & b_{nm} \end{pmatrix}$$

GSOベクトル： $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ にGram-Schmidtの直交化法を用いて得られるベクトルの組 $\{\mathbf{b}_1^*, \dots, \mathbf{b}_n^*\}$

GSO行列：GSOベクトルを行ベクトルとする $n \times m$ 行列を B^* として

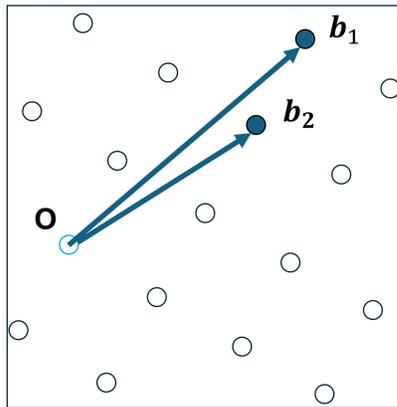
$$B = UB^* \text{をみたす } n \times n \text{ 行列 } U$$

$$U = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ \mu_{2,1} & 1 & 0 & \dots & 0 \\ \mu_{3,1} & \mu_{3,2} & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mu_{n,1} & \mu_{n,2} & \mu_{n,3} & \dots & 1 \end{pmatrix}$$

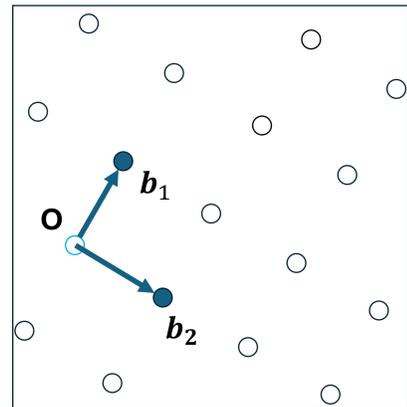
最短ベクトル問題(Shortest Vector Problem)

N次元格子Lの基底 $\{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n\}$ が与えられたとき、格子上の最短の非零ベクトル $\mathbf{v} \in L$ を見つける問題
 上の例では $\mathbf{v} = \mathbf{b}_1 - \mathbf{b}_2$ が最短ベクトル

格子基底簡約



悪い基底



良い基底

格子基底簡約：各基底ベクトルが短く、互いに直交に近い
 同じ格子の基底へ変換する操作

基底同士が直交に近い \Leftrightarrow GSO行列の成分が $|\mu_{i,j}| \leq \frac{1}{2}$ をみたく
 サイズ基底簡約： $|\mu_{i,j}| \leq \frac{1}{2}$ をみたくように基底を足し引きする

各基底ベクトルが短い \Leftrightarrow GSOベクトルがLovasz条件をみたく
 Lovasz条件： $\frac{1}{4} < \delta < 1$ をみたく簡約パラメータ δ を固定して
 任意の $2 \leq k \leq n$ に対して次が成り立つ

$$\|\mathbf{b}_k^*\|^2 \geq (\delta - \mu_{k,k-1}^2) \|\mathbf{b}_{k-1}^*\|^2$$

LLL簡約：Lovasz条件を満たさないとき、基底を交換
 その後サイズ基底簡約を行う
 多項式時間で停止する

LLL簡約の変種

MLLL簡約：一次従属なベクトルの組に適用可能なLLL簡約
 DeepLLL簡約：より自由度の高い基底の入れ替えを行うことで
 より短い基底ベクトルを得るLLL簡約
 多項式時間での停止性は保証されていない

LWE問題とその解法

LWE問題

誤差付きの連立一次方程式を解く問題
 CRYSTALS-Kyber が安全性の根拠としている

LWE問題の定式化

m ：サンプルの個数、 n ：正の整数、 q ：奇素数
 有限体 \mathbb{F}_q 上の秘密ベクトル $\mathbf{s} \in \mathbb{F}_q^n$ を固定
 一様ランダムに選ばれるベクトル $\mathbf{a}_i \in \mathbb{F}_q^n$ ($1 \leq i \leq m$)
 ランダムかつノルムが小さい誤差ベクトル $\mathbf{e} \in \mathbb{F}_q^m$

$$A = \begin{pmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \vdots \\ \mathbf{a}_m \end{pmatrix} \in \mathbb{F}_q^{m \times n}, \quad \mathbf{b} \equiv \mathbf{s}A^T + \mathbf{e} \pmod{q}$$

公開鍵の組 $(A, \mathbf{b}) \in \mathbb{F}_q^{m \times n} \times \mathbb{F}_q^m$ から秘密鍵 $\mathbf{s} \in \mathbb{F}_q^n$ を復号する問題

LWE問題の解法

\mathbb{F}_q を \mathbb{Z} の部分集合とみなすことで整数格子上の問題に帰着
 $\text{mod } q$ の情報を取り入れるため次の生成行列 X を考える

$$X = \begin{pmatrix} A^T \\ qI_m \end{pmatrix}$$

目標ベクトル $\mathbf{b} = \mathbf{s}A^T + \mathbf{e} + q\mathbf{z}$ ($\exists \mathbf{z} \in \mathbb{Z}^m$)
 に最も近い X で生成される格子上の点(= $\mathbf{s}A^T + q\mathbf{z}$)を見つける
 問題とみなすことで、 \mathbf{e} を特定する問題へ帰着
 → \mathbf{e} を最短ベクトルとする新たな格子におけるSVPを考える
 X をLLL簡約して得られた基底行列を B とする

$$\begin{pmatrix} B & \mathbf{0}^T \\ \mathbf{b} & 1 \end{pmatrix}$$

をLLL簡約することで最短ベクトル $(\mathbf{e}, 1)$ が復元
 誤差のない一次連立方程式を復元
 掃き出し法によって秘密ベクトル $\mathbf{s} \in \mathbb{F}_q^n$ を復元できる