



SG2024-11活動報告1

■ 輪講

青野良範・安田雅哉 [著] 『格子暗号解読のための数学的基礎』 (近代科学社)

第1章	格子の数学的基礎：Gram-Schmidt直交化など	下村(D1)、中森(M1)
第2章	LLL基底簡約とその改良	下村(D1)、勝岡(M2)、中森(M1)
第3章	さらなる格子基底簡約アルゴリズム	中森(M1)
第5章	近似版CVP解法とLWE問題への適用	下村(D1)、勝岡(M2)

耐量子計算機暗号の中で有望視されている格子暗号に関連する数理について学んだ

■ 暗号に関連する技術・製品・事件

- ・ 多要素認証：「記憶」「所持」「生体」の3種類の具体例と欠点
- ・ Time-based One-time Passwordのアプリ：Ente AuthとGoogle Authenticator
- ・ パスワード管理のアプリ：Bitwardenの製品紹介、End-to-end encryption
- ・ Facebookがユーザーのパスワードを平文で保存：ハッシュとソルト
- ・ KADOKAWAの個人情報漏洩事件：ランサムウェアへの対処法、復号ツール
- ・ 公衆無線LAN：HTTPS通信、VPN

SG2024-11活動報告2

■ MACSセミナー

安田 雅哉（立教大学理学研究科教授）	格子アルゴリズムと暗号解読への応用
古江 弘樹（NTT）	多変数多項式署名とその効率化手法について

■ 学会：2025年暗号と情報セキュリティシンポジウム(SCIS2025)

伊丹・伊藤・勝岡(M2)・大江(M2)・中森(M1)の5名でSCIS2025@小倉に参加
特に、大江(M2)は以下の口頭発表を行った

4B1-2 超特異QMアーベル曲面から構成される同種写像グラフのラマヌジャン性
©大江 優希(京都大学)、伊藤 哲史(京都大学)

Charlesらは超特異同種写像グラフのRamanujan 性を利用してハッシュ関数を構成した。このハッシュ関数の安全性は同種写像問題の計算量的困難性にに基づき、その後の同種写像暗号の発展の基礎となった。一方で、理論的興味によりCastryckらはCharlesらの構成を2次元の超特別アーベル多様体に拡張したが、超特別アーベル多様体の同種写像グラフにおいてはRamanujan 性を満たさない例がJordanらによって知られている。また、相川らによって任意次元の超特別アーベル多様体の同種写像グラフがエクスペンダー族であることが証明された。本論文では曲面の場合に適切な部分グラフがRamanujan 性を持つことを証明した。その証明には超特異QMアーベル曲面へのDeuring 対応の一般化が鍵になっている。この構成に基づく超特異QMアーベル曲面による新たな暗号方式設計の可能性についても考察を行う。

SG2024-11ポスタ一概要

■ 格子暗号の紹介 (勝岡)

- 公開鍵暗号方式の概要
- 耐量子計算機暗号の必要性といくつかの例
- 格子暗号
 - ❖ 格子の基礎と最短ベクトル問題
 - ❖ 格子基底簡約 (LLL簡約)
 - ❖ LWE問題とその解法

■ 来年度について

- 2024年度刊行の高木剛(著)『現代暗号理論』 (岩波書店) を輪講予定

【SG2024-11】 暗号理論の数理と社会実装

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) がある暗号方式
RSA暗号 (素因数分解) や楕円曲線暗号 (離散対数問題) が主流
・データの漏洩を防ぐ (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)

送信者: m:メッセージ → c:暗号文
受信者: c:暗号文 → m:メッセージ

耐量子計算機暗号

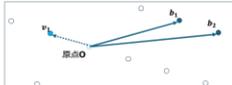
従来暗号方式の脆弱化

- 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開発
- 大規模な量子計算機の発現
- 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: 素数に一般化し格子点を扱うことの困難性を利用
CRYSTALS-Kyberが既に標準化
CRYSTALS-Dilithiumが標準化の途上
- 多変数多項式暗号: 多変数多項式方程式の求解問題を利用
OR-UV (NTT研究) など
- 同種写像暗号: 2つの有限群間の同型写像を利用
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 m 本のベクトル b_1, \dots, b_m の整数係数線形結合で表されるベクトルの集合
 Z^m に含まれる格子を整数格子という

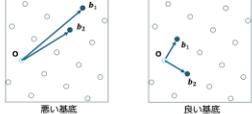
$$L = \{ \sum_{i=1}^m z_i b_i \mid z_i \in \mathbb{Z} \}$$

基底: 格子を生成する一次独立ベクトルの組 (b_1, \dots, b_m)
基底行列: 基底ベクトルを行ベクトルにした $m \times m$ 行列
 $B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = \begin{pmatrix} b_{11} & \dots & b_{1m} \\ \vdots & \ddots & \vdots \\ b_{m1} & \dots & b_{mm} \end{pmatrix}$

GSOベクトル: (b_1, \dots, b_m) にGram-Schmidtの直交化法を用いて得られるベクトルの組 $(\hat{b}_1, \dots, \hat{b}_m)$
GSO行列: GSOベクトルを行ベクトルとする $m \times m$ 行列 \hat{B} として
 $\hat{B} = U B^{-1} B^T U^{-1}$

最短ベクトル問題 (Shortest Vector Problem)
 N 次元格子の基底 (b_1, \dots, b_m) が与えられたとき
格子上の最短の非零ベクトル l を見つける問題
上の解では $l = b_1 = b_2$ が最短ベクトル

格子基底簡約



悪い基底: 格子基底簡約: 各基底ベクトルが短く、互いに直交に近い
良い基底: 各基底ベクトルが長く、互いに直交に近い

基礎理論: 各基底ベクトル b_i の成分が $|b_{ij}| \leq \frac{1}{2}$ を満たす
サイズ基底簡約: $|b_i| \leq 2^{\frac{i-1}{2}}$ を満たすように基底を足し引きする操作

基礎理論が直交に近いGSO行列の成分が $|b_{ij}| \leq \frac{1}{2}$ を満たす
サイズ基底簡約: $|b_i| \leq 2^{\frac{i-1}{2}}$ を満たすように基底を足し引きする

各基底ベクトルが短いGSOベクトルがLovasz条件を満たす
Lovasz条件: $\delta < \delta < 1$ を満たす簡約パラメータ δ を固定して
任意の $1 \leq i \leq m$ に対して次が成り立つ
則が成り立つ

LLL簡約: Lovasz条件を満たさないとき、基底を交換
その操作が基底簡約を行う
多変数暗号で停止する

LLL簡約の復習

LLL簡約: 一次独立な m 本の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
多変数暗号で停止する

LWE問題とその解法

LWE問題

誤差付きの線形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
有限群 \mathbb{Z}_q 上の基底ベクトル e を固定
一様ランダムに選ばれたベクトル $a_i \in \mathbb{Z}_q^n$ ($1 \leq i \leq m$)
ランダムかつ均一に小さい誤差ベクトル $e \in \mathbb{Z}_q^m$

$$A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \equiv \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} \pmod{q}$$

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

LWE問題の解法

\mathbb{Z}_q をの部分集合 \mathcal{S} のみならず \mathbb{Z}_q の整数に帰属
 $\text{mod } q$ の情報を取り入れるための多次元生活行列 X を考える

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

目標ベクトル $b = sA^T + e + qz$ ($z \in \mathbb{Z}^n$)
に最近 \mathbb{Z}^m で生成される格子 L 上の $(x, z) = (x, z)$ を見つける
問題のみならず \mathbb{Z}_q を考慮する問題への帰属
 $\rightarrow e$ が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簡約して得られる基底行列 \hat{X} とする

各LLL簡約することで基底ベクトル $(e, 1)$ が基底
探索のない一次元方程式を復元
探索なしに最短基底ベクトル $e \in \mathbb{Z}_q^n$ を復元できる