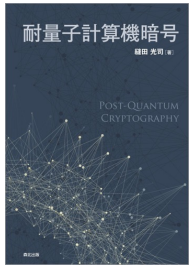
SG2023-11活動報告

■ **輪講**：縫田光司[著]『耐量子計算機暗号』(森北出版)



前期：具体例(エルガマル暗号)を通して公開鍵暗号の安全性証明
夏休みの宿題：好みの耐量子計算機暗号を1つ選んで勉強
後期：主要な3種類の耐量子計算機暗号の構成と攻撃方法

第1章	暗号技術の基礎：共通鍵暗号、公開鍵暗号 暗号技術の安全性証明：IND-CPA安全性	位田(B2)、西川(B3)、 勝岡(M1)、喬(B1)、下村(M2)
第2章前半	符号ベース暗号：誤り訂正符号、情報集合	角(M2)
第2章後半	多変数多項式暗号：UOV、グレブナー基底	勝岡(M1)
第3章	格子暗号：GSW方式、基底簡約アルゴリズム	横田(D1)、下村(M2)

■ **暗号技術を用いた技術・製品**

・Bitwarden：パスワード管理ソフトの仕組み・必要性・有用性
・Google Password Manager：Bitwardenとの違い
・ハッシュ関数：持つべき3つの性質・使い方・攻撃方法
・マイナンバーカード：電子署名・認証局・政府認証基盤
・Skiff(メール・カレンダー・文章・ストレージ)：全てを暗号化したGoogle(?)

SG2023-11活動報告

■ MACSセミナー

前期：情報セキュリティや暗号技術の基礎や楕円曲線を使った暗号について
後期：具体的な耐量子計算機暗号の構成・安全性・攻撃アルゴリズムについて

相川 勇輔（東京大学情報理工助教）	公開鍵暗号の発明から耐量子計算機暗号まで
縫田 光司（九州大学IMI教授）	耐量子計算機暗号に関するいくつかの研究事例

■ 学会発表：2024年暗号と情報セキュリティシンポジウム(SCIS2024)

勝岡(M1)：出島メッセ長崎で開催されたSCIS2024で口頭発表

4A1-2　Zhuang-Ziアルゴリズムを用いたLWE問題に対する代数的解法
◎勝岡 唯弘(京都大学)、伊丹 將人(京都大学)、伊藤 哲史(京都大学)

> Learning with Errors (LWE) 問題とは，Regevにより提案された誤差を含む線型方程式の解を求める問題であり，格子暗号において重要な役割を果たしている．LWE問題の代数的解法としては，有限体上の高次多変数連立方程式の求解問題に還元して解くArora-Geアルゴリズムや，グレブナー基底を用いて改良したAlbrecht-Cid-Faugere-Fitzpatrick-Perret の結果が知られている．一方，Zhuang-Ziアルゴリズムとは，有限体上の高次多変数連立方程式の求解問題を拡大体上の一変数方程式の求解問題に帰着させて解くアルゴリズムであり，Ding-Gower-Schmidt により提案された．本稿では，Zhuang-Ziアルゴリズムを用いたLWE問題の解法を提案し，実装評価を行う．

SG2023-11ポスター概要

■ 耐量子計算機暗号の紹介

- 共通鍵暗号方式と公開鍵暗号方式：バーナム暗号、RSA暗号
- 耐量子計算機暗号の必要性
- 耐量子計算機暗号の紹介
  - ❖ 符号ベース暗号：マクリース暗号
  - ❖ 多変数多項式暗号：Unbalanced Oil and Vinegar

■ 学会発表を行った研究の簡単な紹介

来年度は現時点で一番有望な格子暗号の数理を攻める予定