公益財団法人九州先端科学技術研究所
Institute of Systems, Information Technologies and Nanotechnologies (ISIT)

情報セキュリティ研究室

研究員 奥村　伸也

研究概要 暗号は情報の機密性を確保するために欠かせない技術です。私は理論的・実験的に暗号の研究を行っています。特に、私は耐量子暗号の候補の一つである格子に関する計算困難な問題を利用した格子暗号の設計や安全性解析を中心に研究しています。現在広く普及しているRSA暗号や楕円曲線暗号は、量子コンピュータにより解読されてしまうことが分かっています。そこで、量子コンピュータでも解読が困難な暗号（耐量子暗号）の研究が必要となります。現在でも量子コンピュータは実現できていませんが、技術の進歩は目覚ましいため、早期から耐量子暗号の研究を行うことが重要です。また、準同型暗号や暗号学的多重線形写像等の高機能な暗号の研究も行っていきます。

研究キーワード

■ 耐量子暗号
- ・格子暗号
  - -NTRU, LWE, Ring-LWE
- ・ディオファントス問題の暗号利用
  - -公開鍵暗号（ディオファントス暗号）
  - -鍵交換

■ 高機能暗号
- ・完全準同型暗号
- ・暗号学的多重線形写像

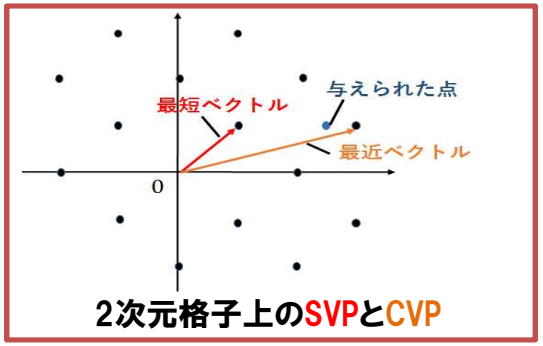
コンサルティング対応可能技術分野

公開鍵暗号，RSA暗号，楕円曲線暗号，
ペアリング暗号，格子暗号

連絡先 E-mail：okumra@isit.or.jp
TEL：092-852-3460
WEB：http://www.isit.or.jp/lab2/

参加プロジェクト

■ JST, CRESTのメンバー
課題「次世代暗号に向けたセキュリティ危殆化回避数理モデリング」研究代表者：高木剛（九大IMI）



2次元格子上のSVPとCVP

$$x^2 - Dy^2 = 1 \ (\sqrt{D} \notin \mathbb{Z})$$

ペル方程式

$$x^n + y^n = z^n \ (n > 3)$$

フェルマー方程式