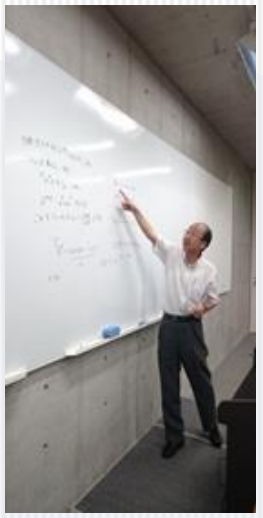
有田研究室

じっくりと
数の理論に向き合う



有田研究室では、暗号理論や暗号技術全般をテーマにしています。最近はとくに、準同型暗号や耐量子計算機暗号を扱っています。格子や代数的整数あるいは楕円曲線間の同種写像など数学的に興味深い構成がたくさんあります。

研究テーマ:
- 準同型暗号と機械学習
  - 円分数、格子、準同型計算、ブートストラップ、ロジスティック回帰、・・・
- 量子計算と耐量子計算機暗号
  - ショア／サイモンのアルゴリズム、隠れ部分群問題、格子、同種写像、・・・
- 軽量暗号とその実装評価
  - PRINCE, ChaCha20, NISTプロジェクト、・・・
- ほか

修了生修論タイトル(一部):
- Recent Progress of Authenticated Encryption
- 量子計算機を前提とした攻撃に対する共通鍵暗号の安全性評価に関する調査
- Enigmaプラットフォームにおけるブロックチェーンを用いたマルチパーティ計算に関する調査
- 準同型暗号における大小比較
- 完全準同型暗号のパラメータ導出に関する一考察
- ストレージ証明とその動向について
- A Study of CCA-secure Attribute-Based Encryption and Its Applications
- Two Applications of Multilinear Maps: Group Key Exchange and Witness Encryption

If you are interested in cryptography
Please come and join us !

http://lab.iisec.ac.jp/~arita/