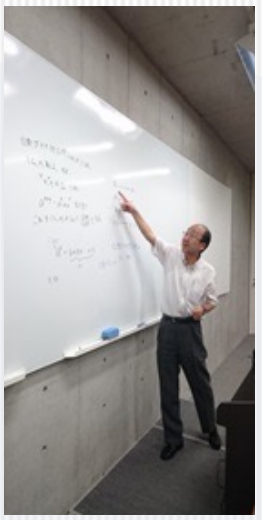
有田研究室

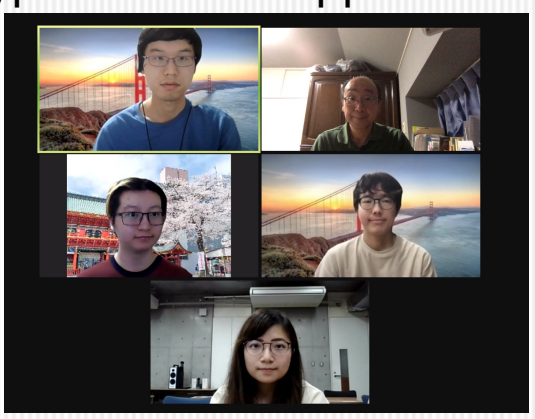
じっくりと
数の理論に向き合う



有田研究室は暗号理論や暗号技術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、機械学習を用いた暗号解析などを扱っています。暗号技術には数学的に興味深いトピックがたくさんあります。

研究テーマ:
・準同型暗号と応用
　　– 円分数、格子、準同型計算、ロジスティック回帰、クラスター分析、・・・
・耐量子計算機暗号
　　– 格子暗号、同種写像暗号、線形符号暗号、・・・
・機械学習を用いた暗号解析
　　– サイドチャネル攻撃への活用、ニューラル識別器、量子回路学習、・・・
・ほか

修了生修論タイトル(一部):
- デュプレックス構造に基づく軽量認証付き暗号に関する研究
- 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



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

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