

# 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、耐量子計算機暗号や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:

- ・耐量子計算機暗号
  - 格子暗号、符号ベース暗号、同種写像暗号、...
- ・機械学習を用いた暗号解析
  - 強化学習と組み合わせ最適化問題、ニューラル識別器、量子回路学習、...
- ・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、...
- ・ほか

### 修了生修論タイトル(一部):

- 同種写像問題に基づくパスワードベース認証付き鍵共有に関する研究
- ゲームチート対策に対する準同型暗号の応用に関する研究
- 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

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

