有田研究室

じっくりと
数の理論に向き合う

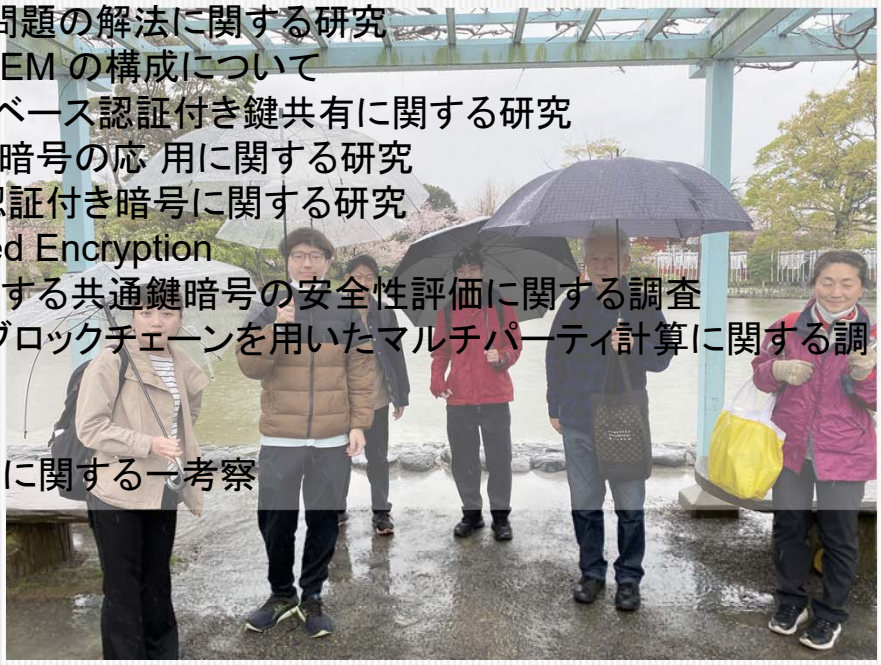
有田研究室は暗号理論や暗号技術をテーマにしています。最近はとくに、（耐）量子計算機暗号、ゼロ知識証明、準同型暗号などを扱っています。暗号技術には数学的に興味深いトピックがたくさんあります。

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、量子ランダムオラクル、Pseudorandom Quantum States、・・・
・ゼロ知識証明
  – SNARK、再帰的証明、増分検証、・・・
・準同型暗号と応用
  – LWE、準同型計算、マルチパーティ計算、・・・
・ほか

修了生修論タイトル(一部):

- 深層強化学習によるナップサック問題の解法に関する研究
- 符号ベースのマルチレシーバー KEM の構成について
- 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 !