松尾研究室の紹介

https://kazutomatsuo.github.io/lab/

松尾 和人

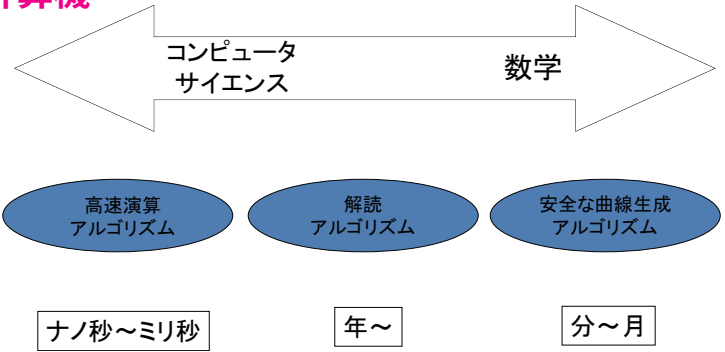
2026 年 6 月 3 日

松尾の主な研究テーマ

1. 情報セキュリティ技術 $\supset$
2. 暗号技術 $\supset$
3. 公開鍵暗号 $\supset$
4. 超楕円曲線暗号 $\subset$
5. 数論アルゴリズム・計算代数

楕円・超楕円曲線曲線暗号の研究課題

1. 高速アルゴリズムとそのソフト実装
2. 安全な曲線の構成法とそのソフト実装
3. 安全性評価
4. 多様なプロトコル
5. 耐量子計算機



卒研テーマ

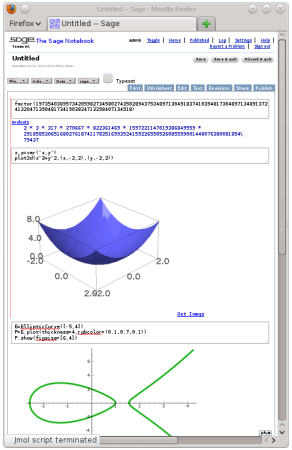
1. 暗号アルゴリズムに対する攻撃・構成手法
   - 楕円・超楕円曲線暗号
   - 耐量子計算機暗号
2. 暗号アルゴリズムの高速実装
   - 楕円・超楕円曲線暗号
   - 多機能暗号
3. 情報セキュリティ技術の安全性検証
   - モダンな認証プロトコル
   - Web セキュリティ
4. その他、数論アルゴリズムを含む情報セキュリティ技術全般
   - AI セキュリティ、AI 利用セキュリティ

メンバーが興味のあるテーマを相談しながら選びます

2025 年度卒業論文一覧

- **楕円曲線離散対数問題に対する Diem 攻撃の実装** 楕円 攻撃 実装
- **同種写像暗号に対する中間一致攻撃の実装比較** 楕円 対量子 攻撃 実装
- **ナップザック暗号に対する攻撃の有効性について** 対量子 攻撃 実装
- **耐量子署名 SPHINCS+の Rust 実装** 対量子 構成 実装
- **RSA 合成数を利用した SSL 証明書の脆弱性調査** インターネット プロトコル 攻撃
- **WPA2-PSK の盗聴に対する安全性検証** プロトコル 攻撃 実験
- **認可 API の CSRF 攻撃に対する安全性検証** インターネット プロトコル 攻撃
- **使わなくなったドメイン名放棄の課題と対策** インターネット 管理
- **(2,3) 視覚暗号方式の実装** 実装
- **パスフレーズポリシーの安全性評価** 管理 実装
- **フィッシングサイト検知性能分析** インターネット AI 応用
- **Slowloris 攻撃に対する防御設定の実験的評価** インターネット 攻撃 実験
- **機械学習を用いたスパムメールの検出実験** インターネット AI 応用
- **アカウント ID 使い回しの安全性** インターネット 管理

「情報ゼミナール」の予定



- 目的
  1. 研究テーマの選択
  2. ベースツール入門

- 内容
  1. 最近の論文の調査
     - 暗号と情報セキュリティシンポジウム
     - コンピュータセキュリティシンポジウム

     年間 400 以上の研究発表が有ります。論文を沢山読み、興味の湧く研究テーマを選びましょう。
  2. 数学統合ソフト Sage の演習

こういう人に向いています

- 情報セキュリティ技術に興味が有る
- 数学・計算が好き
- 高速プログラミングに興味が有る
- 卒業研究にも本気で取り組みたい

お待ちしております