松尾研究室の紹介

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

松尾 和人

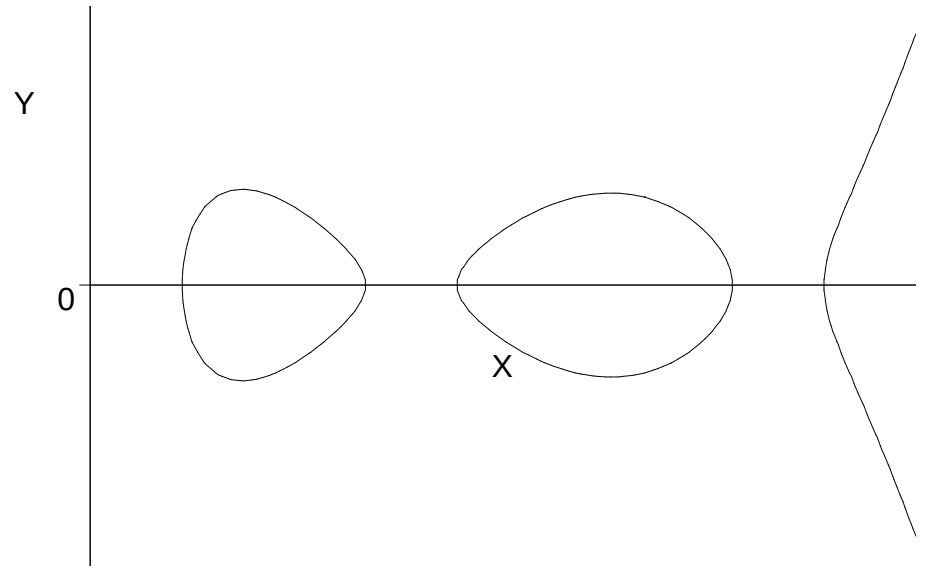
2024 年 6 月 5 日

指導教員のメインの研究内容

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

超楕円曲線暗号

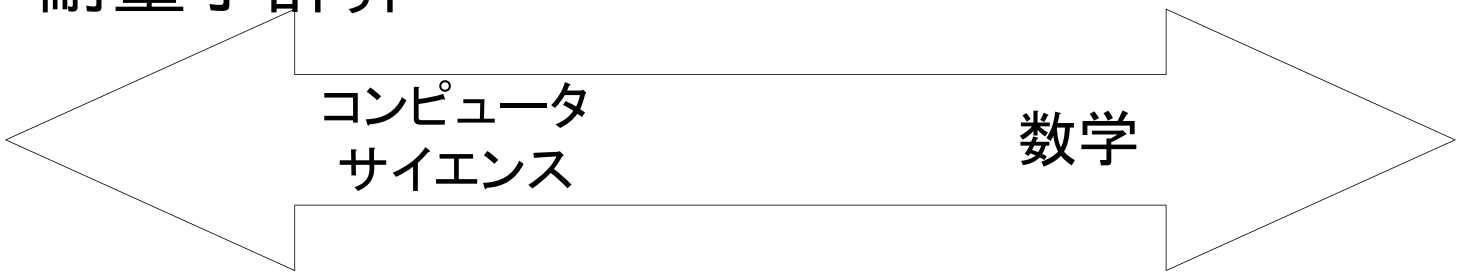
$$C : Y^2 = X^{2g+1} + f_{2g}X^{2g} + \cdots + f_1X + f_0 \in \mathbb{F}_p[X]$$



- g 個以下の点の組が有限可換群を成す
  $\Rightarrow$ 離散対数問題ベースの公開鍵暗号
- $g = 1$: 楕円曲線（公開鍵暗号の新主流）

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



ナノ秒～ミリ秒

年～

分～月

研究室の研究テーマ

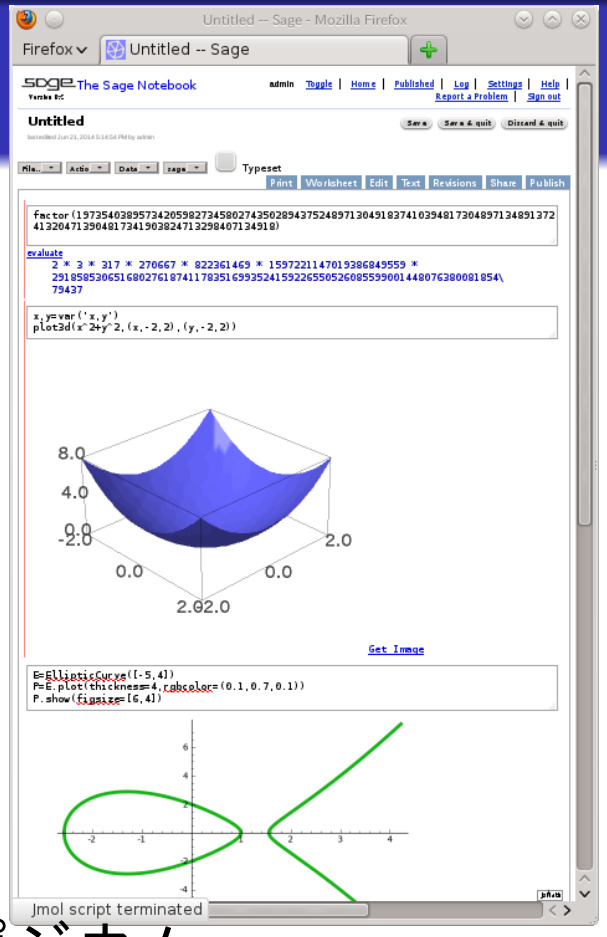
1. 暗号アルゴリズムに対する攻撃・構成手法
   - 楕円・超楕円曲線暗号
   - 耐量子計算機暗号
2. 暗号アルゴリズムの高速実装
   - 楕円・超楕円曲線暗号
   - 多機能暗号
3. 情報セキュリティ技術の安全性検証
   - モダンな認証プロトコル
4. その他、数論アルゴリズムを含む情報セキュリティ技術全般

各自が興味のあるテーマを
教員と相談しながら選択・決定

2023年度卒業論文題名一覧

- SIDHに対するCastryck-Decru攻撃の研究
- 多変数多項式署名方式Rainbowへの攻撃
- CPythonへのToom-Cook乗算の実装
- CNNに対するBadnets攻撃
- QUICに対するDDoS攻撃の調査
- Google Safe Browsingを用いた悪性Webサイトの検出
- 二要素認証の安全性
- パスワードポリシーの比較と策定
- 視覚復号型秘密分散法の実装

「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

1. 次のどれかに当てはまる
   - 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
2. 卒業研究にはまじめに取り組みたい
3. 大学院に進学して研究を続けたい

配属希望者

WebClass のメッセージ機能で連絡します