松尾研究室の紹介

松尾 和人

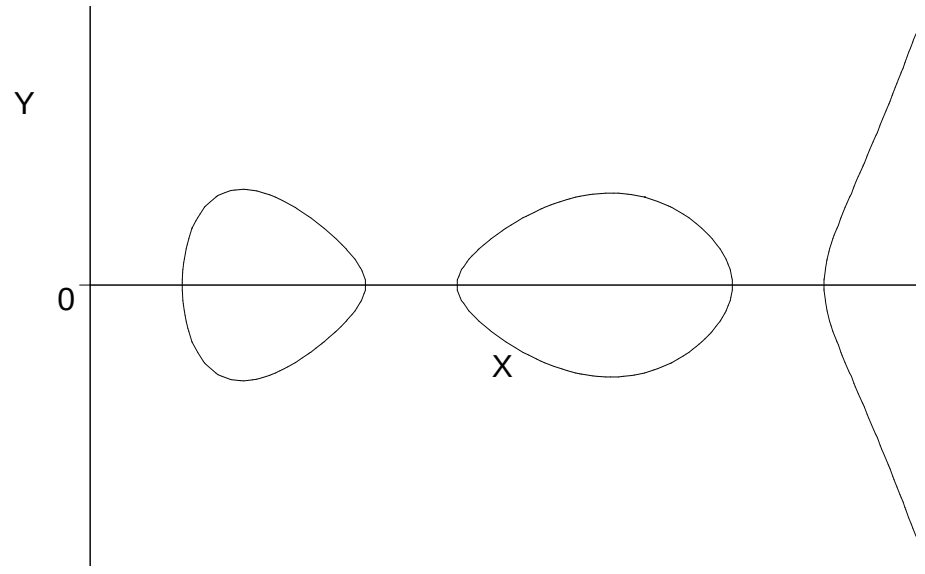
2023 年 5 月 24 日

指導教員のメインの研究内容

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

超楕円曲線暗号

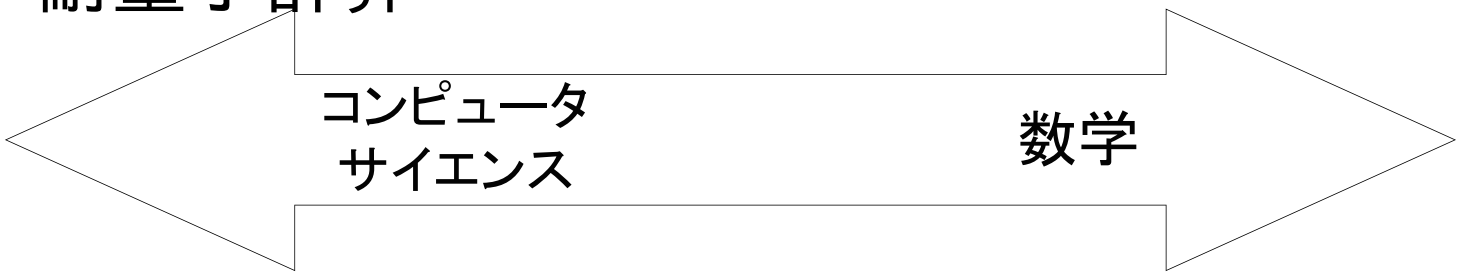
$$C : Y^2 = X^{2g+1} + f_{2g}X^{2g} + \cdots + f_1X + f_0 \in \mathbb{F}_p[X]$$



- 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
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

卒研生の研究テーマ (1/5)

	2015	2016
楕円暗号（実装） （構成） （攻撃）	○ ○	 ○
暗号系	古典暗号解読	パスワード暗号
数論アルゴリズム	Python 高速化 TwitterBot	素因数分解 素数判定 LWE 問題
プロトコル安全性	OAuth PW	TOR PW
プロトコル実装	秘密分散 ステガノグラフィ	OTP

青: 数学不要 赤: プログラミング不要 緑: 両方不要

卒研生の研究テーマ (2/5)

	2017	2018
楕円暗号	攻撃	攻撃 × 2
数論アルゴリズム	素因数分解	
安全性評価	RSA 暗号 パスワード認証 BitCoin スマホアプリ スマホ広告ライブラリ プライベートブラウズ	RSA 暗号 匿名化技術 Web アプリ 公衆 WiFi DNS Web プロキシ
実装等	ステガノグラフィ カード秘密計算	秘密分散 検索可能暗号

卒研生の研究テーマ (3/5)

	2019	2020
楕円暗号	攻撃	対量子暗号実装 検索可能暗号
数論 Algo.	量子素因数分解	
安全性評価	RSA 暗号 DH 鍵共有 匿名化技術 Web キャッシュ	AI に対する攻撃 BitCoin ブラウザ PW 管理機能 経路情報交換プロトコル ブラウザフィンガープリント TCP リフレクション攻撃 なりすましメール対策
実装等	OTP システム	カード秘密計算 PW 管理ソフト

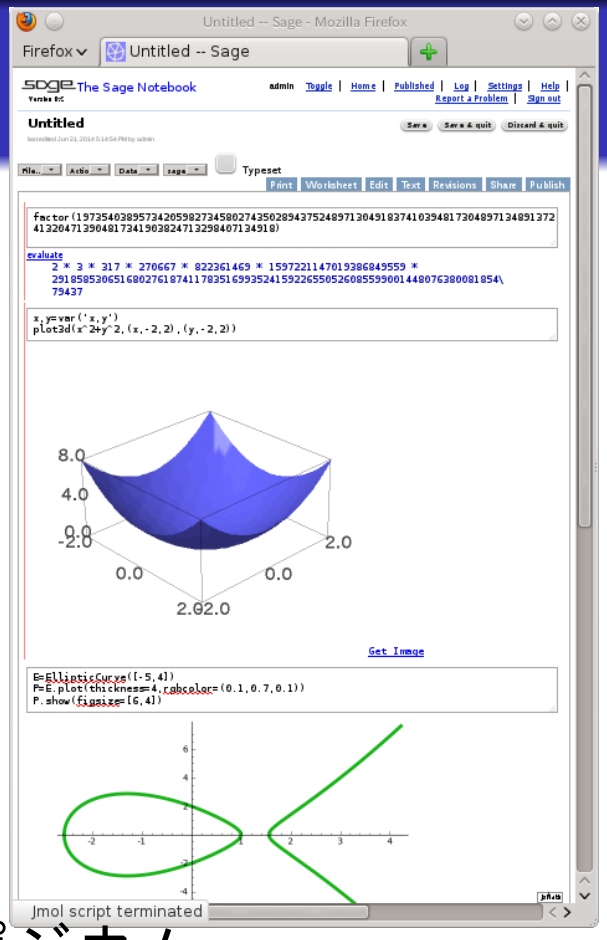
卒研生の研究テーマ (4/5)

	2021	2022
楕円暗号	検索可能暗号	耐量子計算暗号
安全性評価	耐量子計算暗号 パスワードリセット方式 TOR PDF Web キャッシュ DDos 攻撃	RSA AI × 2 QR コード パスワード認証 Bluethooth
実装等	耐量子計算暗号 ブロックチェーン認証	秘密分散 Phishing 検知 ブロックチェーン のゲーム利用

卒研生の研究テーマ (5/5)

	2023
楕円暗号	耐量子計算暗号
安全性評価	耐量子計算暗号 AI DDoS 悪性 Web サイト 2 要素認証
実装等	Python インタプリタの乗算高速化 視覚秘密分散 パスワード強度評価

「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
   - 高速プログラミングに興味が有る
   - 数学・計算が好き
2. 卒研は頑張る
3. 大学院に進学して研究を続けたい