松尾研究室の紹介

松尾 和人

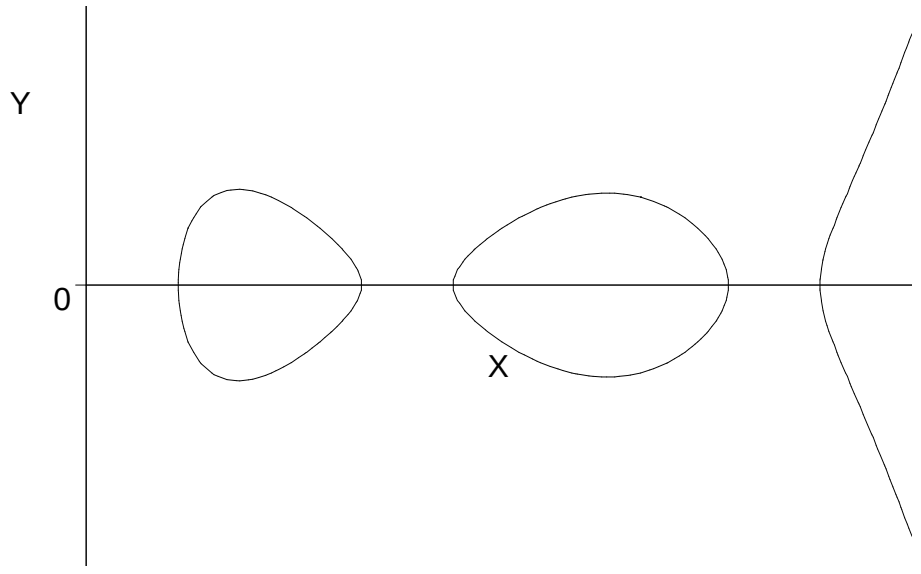
2020 年 6 月 24 日

指導教員のメインの研究内容

1. 情報セキュリティ技術 $\supset$
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

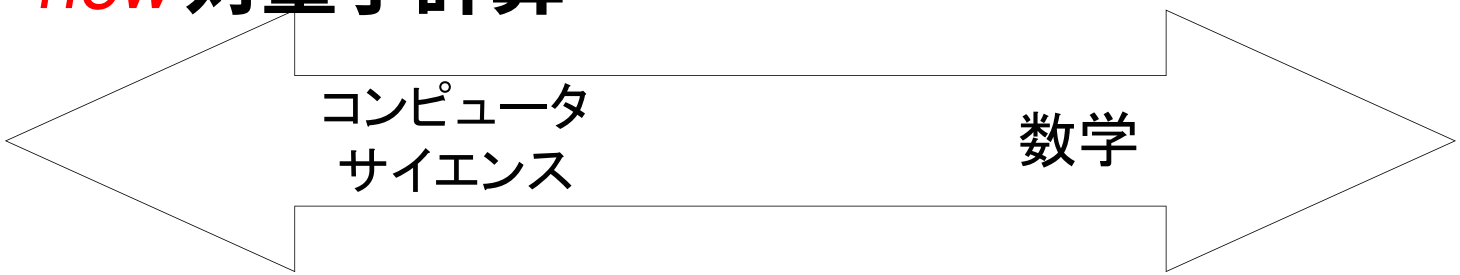
$$C : Y^2 = X^{2g+1} + f_{2g}X^{2g} + \cdots + f_1X + f_0 \in \mathbb{F}_p[X]$$



- 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. *new* 対量子計算



ナノ秒～ミリ秒

年～

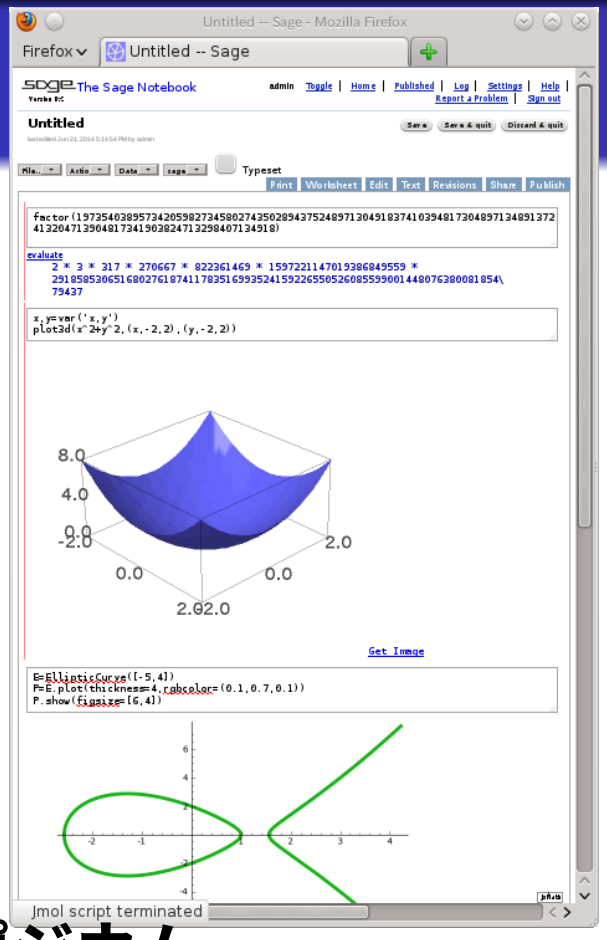
分～月

卒研生の研究テーマ

	2019	2020
(超) 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

青: 数学不要 赤: プログラミング不要 緑: 両方不要

「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・計算が好きです
2. 卒研も（は）一生懸命やるつもり
3. 大学院に進学して研究を続けたい

お待ちしております