松尾研究室の紹介

松尾 和人

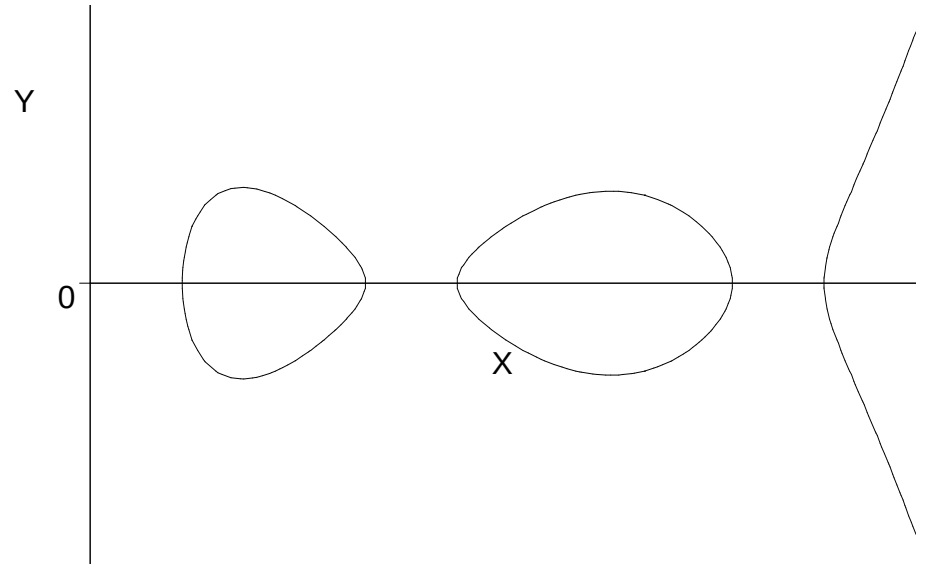
2016 年 6 月 22 日

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

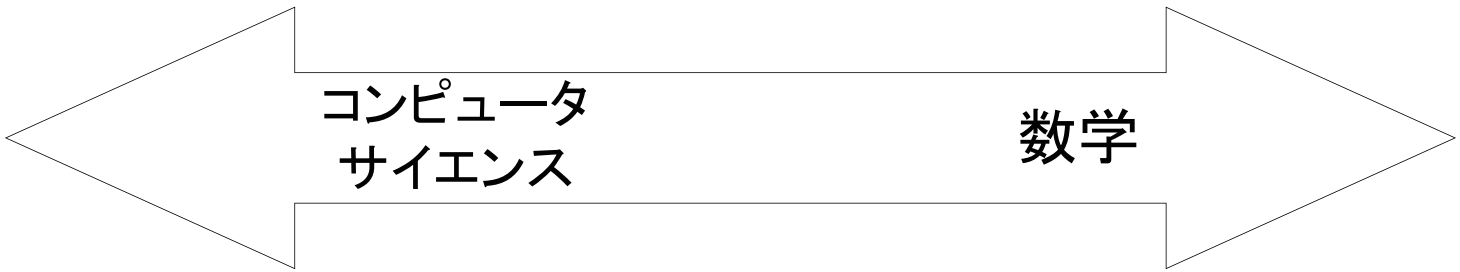
$$C : Y^2 = X^{2g+1} + f_{2g}X^{2g} + \cdots + f_1X + f_0 \in \mathbb{F}_p[X]$$



- 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



ナノ秒～ミリ秒

年～

分～月

研究室の研究テーマ

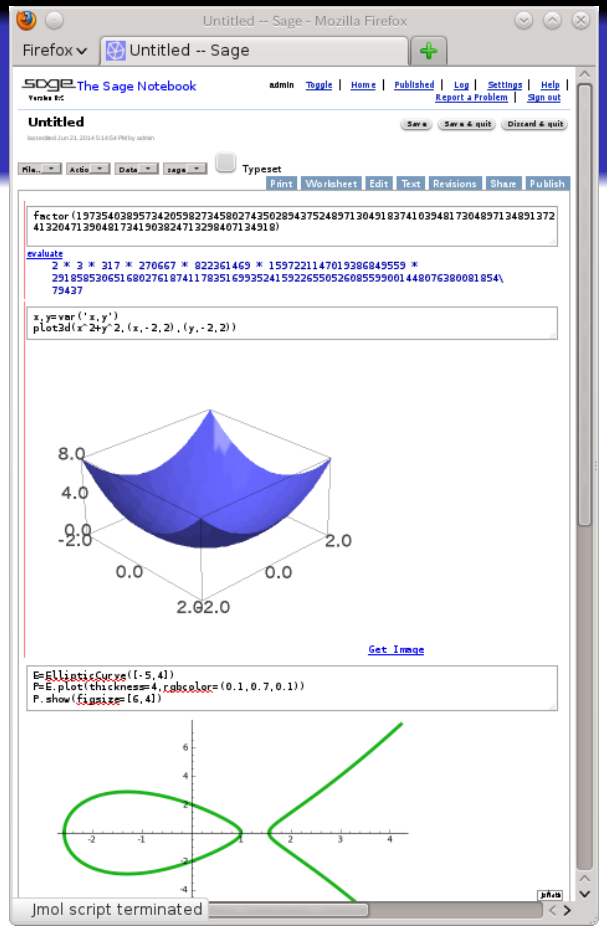
1. 暗号アルゴリズムに対する攻撃・構成手法
   - 楕円・超楕円曲線暗号
2. 暗号アルゴリズムの高速実装
   - 楕円・超楕円曲線暗号
   - 多機能暗号
3. 情報セキュリティ技術の安全性検証
   - モダンな認証プロトコル
4. その他、情報セキュリティ技術全般

卒研生の研究テーマ

	2013	2014	2015	2016
(超) 楕円暗号（実装） （構成） （攻撃）	○ ○ ○	○ ○	○ ○	 ○
暗号系	高機能暗号 暗号 AddOn	乱数生成	古典暗号解読	パスワード暗号
数論アルゴリズム		素因数分解	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	WLAN, TOR, OpenID	PW, SSL, BitCoin	OAuth	TOR PW
プロトコル実装			秘密分散 ステガノグラフィ	OTP
Web セキュリティ	XSS 攻撃			

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