松尾研究室の紹介

松尾 和人

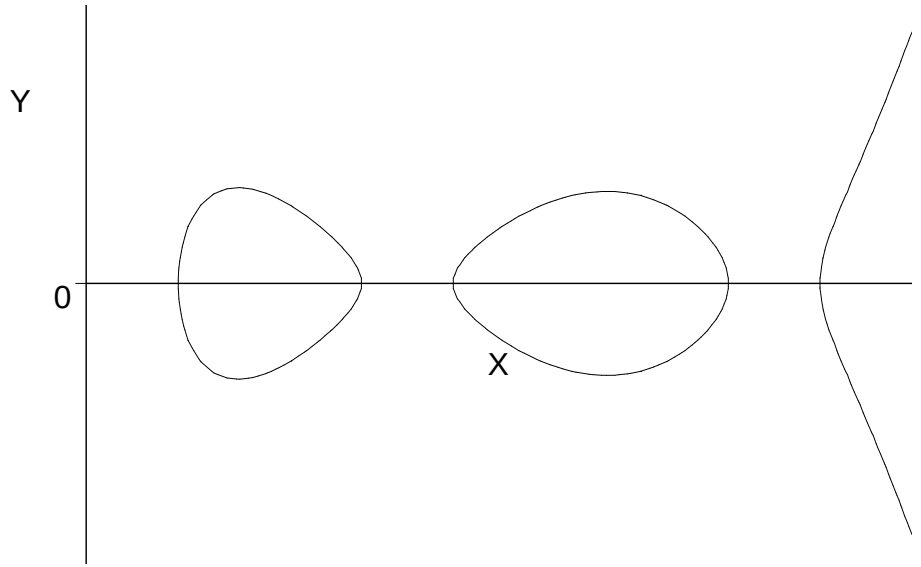
2013 年 6 月 19 日

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

超楕円曲線暗号

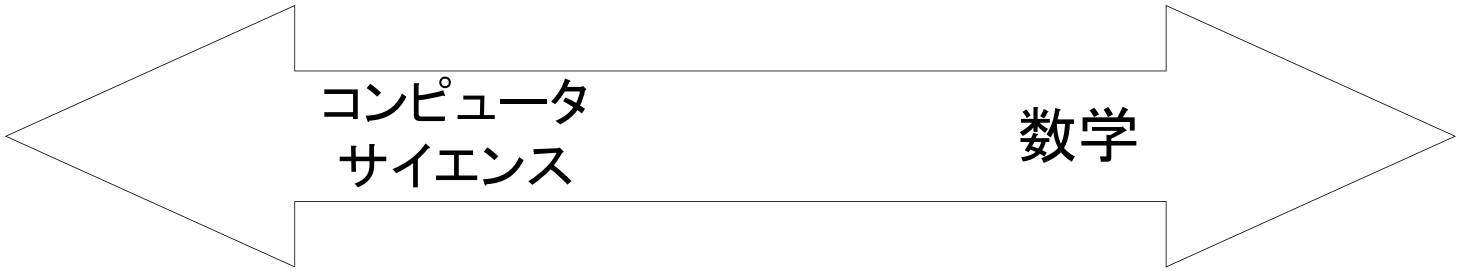
$$C : Y^2 = X^{2g+1} + f_{2g}X^{2g} + \cdots + f_1X + f_0 \in \mathbb{F}_p[X]$$



- 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

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

最近の研究: Bluethooth の安全性評価

1. Bluethooth
   1. 小型機器の通信方式
   2. セキュリティに気を使っている
   3. 中間者攻撃ができないとしている
2. 研究成果
   - 中間者攻撃を提案
   - 対策も同時に提案

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

現在の卒研生の研究テーマ

- 安全な楕円曲線の構成法
- 楕円曲線暗号に対する攻撃法
- 楕円曲線暗号の Android への実装
- 準同型暗号の実装と性能評価
- SSL 暗号強度表示 Firefox アドオン
- 匿名通信路 Tor の安全性評価
- OpenID プロトコルの安全性
- 無線 LAN セキュリティ機能の安全性
- XSS 攻撃に対する脆弱性統合検査ツール

こういう人に向いています

1. 情報セキュリティ技術に興味が有る
2. 高速プログラミングに興味が有る
3. 数学が好きです
4. 大学院に進学して研究したい

「情報科学ゼミナール」の予定

- 目的
  1. 「情報セキュリティ」を知る
  2. 研究テーマの選択
- 内容
  1. 教科書の輪読
     情報セキュリティは広範に渡る分野です。
     3 年生のうちに全体を見渡しましょう。
  2. 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
     合わせて年間 400 以上の発表が有ります。予稿を沢山読み、興味の湧く研究テーマを選びましょう。