# 松尾研究室の紹介

松尾 和人

2012 年 6 月 20 日

# 松尾研究室の特徴

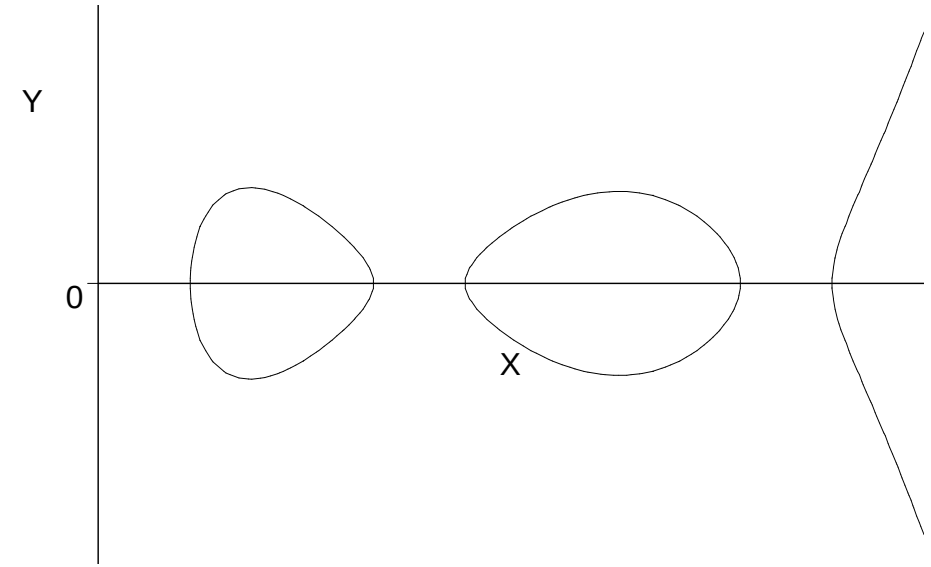
1. 新規研究室
2. 情報セキュリティ研究

# 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

# 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

# 楕円曲線暗号 ($g = 1$)

- RSA **暗号より安全性が高い**
  - **同一の安全性で、**
    **よりコンパクト・高速な実装が可能**
    **（本来、超楕円曲線暗号もそうであるはず。）**
- **標準**
  - RFC 5480, 5656, 4754, 5753
  - Advanced Access Control System (AACS)
  - Digital Transmission Content Protection (DTCP)
  - Wireless Transport Layer Security (WTLS)
  - Bluetooth
  - PKCS#13, IEEE P1363, ANSI X9.62, . . .

# 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

# 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
   - 学生論文賞受賞

# 研究室の研究テーマ

1. 暗号アルゴリズムの高速実装
   - 楕円・超楕円暗号
   - 多機能暗号
2. 暗号アルゴリズムに対する攻撃・構成手法
   - 楕円・超楕円暗号
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

# 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. 大学院に進学し研究に没頭したい

# 「情報科学ゼミナール」の予定

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 年のうちに全体を見渡しましょう。
2. 最近の論文の調査
   - 国内のセキュリティ専門シンポジウム
     - 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。