

松尾研究室の紹介

松尾 和人

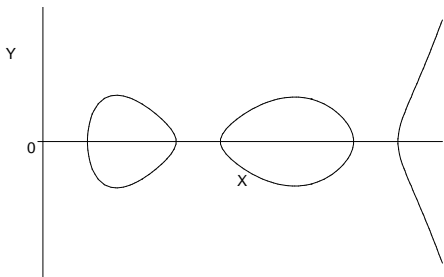
2019年6月26日

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

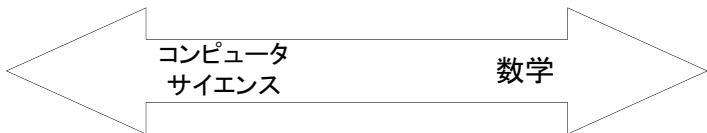
$$C : Y^2 = X^{2g+1} + f_{2g}X^{2g} + \cdots + f_1X + f_0 \in \mathbb{F}_p[X]$$



- g 個以下の点の組が有限可換群を成す
⇒ 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



高速演算
アルゴリズム

解読
アルゴリズム

安全な曲線生成
アルゴリズム

ナノ秒～ミリ秒

年～

分～月

卒研究生の研究テーマ

	2018	2019
(超) 楕円暗号	攻撃	攻撃
数論 Algo.		量子素因数分解
安全性評価	RSA 暗号 匿名化技術 DNS Web キャッシュ Web アプリ スマホ広告ライブラリ 公衆 WiFi	RSA 暗号 DH 鍵共有 匿名化技術 Web キャッシュ BitCoin
実装等	秘密分散 検索可能暗号	PW 管理ソフト OTP システム カード秘密計算

青: 数学不要 赤: プログラミング不要 緑: 両方不要

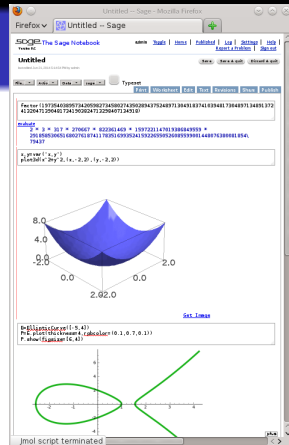
「情報ゼミナール」の予定

● 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 以上の研究発表があります。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ある
 - 高速プログラミングに興味がある
 - 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

注意

希望者が定員に達しないときも面談を行います

お待ちしております