TMU ISEC Lab

東京都立大学大学院 理学研究科 数理科学専攻

暗号数理研究室

内山 成憲

uchiyama-shigenori@tmu.ac.jp

研究テーマ

Information Security Laboratory

計算困難な問題の解法アルゴリズムの解析と
その暗号理論への応用：
数論，代数幾何学，組合せ論，離散数学，
量子コンピュータの基礎数理等

計算困難な問題の解法アルゴリズムの解析を行い，
それに基づく暗号・署名方式等の安全性評価及び
新しい方式の提案

主要なキーワード

Information Security Laboratory

- 素数判定問題，素因数分解問題
- 有限体上の離散対数問題
- 楕円曲線（位数，離散対数問題，同種写像，ペアリング等）
- 多変数連代数方程式の解法（グレブナー基底等）
- 格子に関する問題（LLLアルゴリズム等）
- 量子計算

最近の研究成果例

耐量子計算機暗号安全性評価で世界記録更新

Information Security Laboratory

Fukuoka MQ Challenge

多変数２次連立方程式を解く国際コンテスト

（暗号を解読することに相当）

https://www.mqchallenge.org/

多変数非線形連立方程式は計算困難問題の一つ。

Type Ⅱ，Ⅲでの世界記録（耐量子計算機暗号の安全性評価の世界記録）：37変数74個の連立方程式をそれぞれ約76日間，５６日間で解いた（19/4/10、6/27）報道発表19/6/27

国際会議 IWSEC2019 Best Paper Award 受賞!

研究室メンバー

Information Security Laboratory

2021年度研究室構成メンバー：

- 大学院生　D3：１名
  M2：2名
  M1：２名
- 卒研生　　B4：４名

博士・修士論文のタイトル

Information Security Laboratory

博論：2011:On Multivariate Public-Key Cryptosystems
2016: Faster Explicit Formulae and Parallelization for Computation of Pairings Using Elliptic Nets

修論：2008: 非Wieferich素数とその公開鍵暗号への応用, 二次形式を基礎とする公開鍵暗号, 楕円曲線を用いた秘密分散共有法
2009: Elliptic netを用いたペアリングの計算とそのIDベース暗号への応用
2010: 代数曲面暗号に対するリダクション攻撃法の考察, 公開鍵暗号NICEへの2次形式を用いた攻撃法について
2011: Dickson多項式とその暗号への応用
2012: Elliptic Divisibility Sequence を用いた素因数分解アルゴリズム
2013: 素数判定アルゴリズムの高速化, Twisted Edwards curve を用いたスカラー倍算について, 関数体篩を用いた有限体上の離散対数問題計算アルゴリズム, 楕円DH問題と計算量的に等価な問題
2014: Dickson多項式を用いた暗号方式に対する秘密鍵が小さい場合の攻撃法
2015: 楕円曲線を用いたMulti-Secret Sharing Schemeについて, EDS-DH問題に基づく公開鍵暗号方式
2016: F4アルゴリズムを用いた2次多変数連立方程式の求解の高速化
2017: F4アルゴリズムの高速実装についての注意
2018: Nemecらの素因数分解法について, 有限体上の2次連立代数方程式に対するF4アルゴリズムの高速実装について, 多項式 x^2 + 5x + 5 関する2次Frobenius擬素数について
2019: Edwards曲線を用いた3者間SIDHについて, 2次強Frobeniusテストを用いた素数判定法について, グレブナー基底計算における多項式選択について
2020: F4アルゴリズムにおける多項式選択について, 2次強Frobeniusテストとその判定効率について