An Experiment of The Number Field Sieve for Discrete Logarithm Problem over GF(pn)

早坂, 健一郎

https://doi.org/10.15017/1500512

（様式６－２）

氏　　名	早坂　健一郎
論　文　名	An Experiment of The Number Field Sieve for Discrete Logarithm Problem over GF(p^n) (拡大体 GF(p^n)上の離散対数問題に対する数体篩法の計算機実験)
論文調査委員	主査　九州大学　教授　髙木　剛 副査　九州大学　教授　藤澤 克樹 副査　九州大学　教授　岡田 勘三 副査　九州大学　准教授　田口 雄一郎

論　文　審　査　の　結　果　の　要　旨

本論文では，数体篩法の計算機実験によりペアリング暗号の安全性に関する考察を行っている．ペアリング暗号は，大きな標数 p の n 次拡大体 GF(p^n) 上の離散対数問題の困難性を安全性の根拠にしている．本稿では，2 次元格子篩法で用いられていた効率的な格子巡回法を 3 次元以上の空間上において拡張し，高速に実装可能な多次元格子篩法を考察した．

Joux 等は CRYPTO2006 において，有限体 GF(p^n) 上の離散対数問題に対する数体篩法として，共役な関係にある 2 個の n 次代数体 F_1 と F_2 を用いる手法を提案した．数体篩法は，1. 多項式選択ステップ，2. 関係式探索ステップ，3. 線形代数ステップの三段階から構成される．数体篩法の多項式選択では，代数体 F_1, F_2 を定義する多項式 f_1, f_2 として，f_1 が GF(p) 上で既約，$f_2 = f_1 \pm p$，$\deg(f_1) = \deg(f_2) = n$ の 3 条件を満たすものを探す．関係式探索ステップでは，終結式の組 $\mathrm{Res}(f_1, f_s)$ と $\mathrm{Res}(f_2, f_s)$ が同時に smooth となる整数係数の多項式の f_s を大量に求める必要がある．多項式 f_s を効率的に集める方法として線篩と格子篩が知られており，一般的に位数が 300 ビット以上の有限体に対する NFS 法では格子篩法の方が高速となる．線形代数ステップでは，巨大な線形方程式を解く必要があり Lanczos 法などの共役勾配法が用いられている．既に実用化され国際標準化が進んでいるペアリング暗号では，拡大次数として n=2, 6, 12 などが利用されている．また，2006 年に Joux 等が 394 ビットの 3 次拡大体 GF(p^3)，2008 年に Zajac が 242 ビットの 6 次拡大体 GF(p^6) の実装を報告している．

本博士論文では，関係式探索ステップの高速化に関する研究を行った．通常の数体篩法では 2 次元格子篩法を用いるが，拡大体 GF(p^n) の場合は 2 次元では十分な関係式を集めることができない．そのため，多次元の格子篩法を考察する必要があるが，従来の格子篩法は 2 次元，Zajac は 3 次元線篩法の実装に留まっている．本稿では，2 次元格子篩法で用いられていた効率的な格子巡回法を 3 次元以上の空間上において拡張し，高速に実装可能な多次元格子篩法を考察した．具体的には，3 次元篩領域上の格子点を効率的かつ網羅的に列挙できる基底の条件を既知の 2 次元 Franke-Kleinjung 法を基に拡張し，それらの条件を満たすような基底を生成するアルゴリズムを考案した．また，3 次元 Franke-Kleinjung 法における条件を満たした基底を用いた場合，3 次元領域内の全ての格子点が計算できることを証明した．

最後に基底を加算することにより逐次的に格子点を計算できること，領域の 1 つの次元に対して単調非減少な格子点計算ができることを示した．さらに，この 3 次元へ拡張した提案 Franke-Kleinjung 法を計算機により実装し，約 80000 個の基底を生成した結果，効率的かつ網羅的な条件を満たすような基底を生成でき，実際に格子点数の見積もり値とほぼ同数の格子点を列挙できることを検証した．

本博士論文の結果は，Number Theory and Cryptography 2013, Springer LNCS 8260, pp. 108-120, 2013 および JSIAM Letters, Vol.6, pp.53-56, 2014 として公表済である．この結果は，数体篩法を用いてペアリング暗号の安全性解析を詳細に考察しており，暗号理論の分野において学術的に価値のある業績である．

よって，本研究者は博士（機能数理学）の学位を受ける資格があるものと認める．