九州大学学術情報リポジトリ
Kyushu University Institutional Repository

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

出版情報：九州大学, 2014, 博士（機能数理学）, 課程博士
バージョン：
権利関係：全文ファイル公表済

（様式３）

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)

区　　分　：　甲

論　文　内　容　の　要　旨

次世代公開鍵暗号として期待されるペアリング暗号は，従来の公開鍵暗号では実現が困難である ID ベース暗号や関数型暗号などの利便性の高い暗号システムが構築可能である. これまでにペアリング暗号の高速実装が多く報告されているが，現在最も高速な実装が提案されているペアリングの一つとして BN 曲線を用いた Optimal Ate ペアリングが知られている. Optimal Ate ペアリングの安全性は 12 次拡大体 GF(p^{12}) 上の離散対数問題の困難性によって保たれており，位数が 3072 ビットの拡大体 GF(p12) 上の離散対数問題の困難性は，128 ビットセキュリティレベルを満たすと考えられている.

ここで，素因数分解問題や素体 GF(p)上の離散対数問題の困難性は，500 ビットを超える大規模な計算機実験によって評価されているが，ペアリング暗号で用いられる n = 6 や n = 12 の拡大体 GF(p^n) 上の離散対数問題の計算機実験による困難性評価はまだ少なく，特に n = 12 の場合は計算機実験の報告はない．このため，ペアリング暗号の安全性評価の精度を高める上で，拡大体 GF(p^n) 上の離散対数問題の困難性を計算機実験により評価することは不可欠である.

素体 GF(p) 上の離散対数問題に対する漸近的に現在最速な解法として数体篩法(JL03-NFS)が知られているが，CRYPTO 2006 において Joux らは，JL03-NFS を拡大体 GF(p^n) 上に拡張した数体篩法(JLSV06-NFS)を提案した．JL03-NFS と，その拡張である JLSV06-NFS では，関係式の探索を行う関係探索ステップが大きく異なる. 関係探索ステップで用いられる手法として line sieve と lattice sieve が知られているが，一般に lattice sieve がより効率的であるとされている．このため，JL03-NFS や素因数分解での数体篩法では，2 次元篩領域上の lattice sieve が主流である．この lattice sieve では, ある基底により生成される格子点を篩領域内から探索する処理を含むが, 2 次元の lattice sieve においては Franke-Kleinjung 法を用いることで効率的かつ網羅的な格子点列挙を実現している．一方，n = 6 や n = 12 の拡大体 GF(p^n)上の数体篩法では，次元を拡張して 3 次元以上の多次元篩領域における lattice sieve を考慮しなければならない．しかし，一般次元の line sieve や Franke-Kleinjung 法を考慮しない lattice sieve が知られているものの，2 次元 Franke-Kleinjung 法の単純な一般次元への適用は難しく, 3 次元以上の Franke-Kleinjung 法が実現可能かはまだ知られていない.

本論文では始めに, 拡大体 GF(p^n)上の数体篩法で用いられる 2 次元篩領域での lattice sieve を自然に拡張することで得られた多次元篩領域における lattice sieve の実装を行った．次に，実装された lattice sieve を用いて 203 ビットの拡大体 GF(p^{12})上の離散対数問題を解いた．この実験の際，篩領域の次元や形状などの lattice sieve が高速となるようなパラメータを，見積り式を用いた数値実験により考察した．この結果から，実験では 7 次元の篩領域を用いて lattice sieve を行い，32241

個の関係式を得ることができた．これらの関係式から連立一次合同式を構成し，Lanczos 法を用いてこれを解いた．これにより，CPU コアを 16 個搭載した計算機 1 台により，位数 203 ビットの拡大体 GF(p^{12})上の離散対数問題を約 43 時間で計算することができた．

さらに本論文では，多次元篩領域上の lattice sieve の効率化を図るため，2 次元篩領域上の lattice sieve において用いられる格子点列挙法である Franke-Kleijung 法の 3 次元篩領域への拡張を行った．始めに，2 次元篩領域上の Franke-Kleinjung 法によって生成される基底が満たす条件を 3 次元篩領域上への拡張を行った．次に，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察した．具体的には，2 次元 Franke-Kleinjung 法の第 1 成分を，第 2 及び第 3 成分の 2 次元として拡張することで 3 次元篩領域への拡張を行った．そして，得られた 3 次元篩領域上の Franke-Kleinjung 法を実装し，篩領域のサイズを変化させてそれぞれ約 8000 個の基底の生成を行った．その結果，約 60%の基底に対して拡張した条件を満たすような基底を生成でき，網羅的に格子点を列挙できた．一方で，条件を満たさない約 40%の基底に関しても，約 70%程度の格子点を列挙できた．