修士論文 要旨

同種写像暗号 CSIDH における秘密鍵空間の最適化

数理情報学専攻 48196221　中川 皓平
指導教員　高木 剛教授

1　はじめに

公開鍵暗号はインターネット上で安全に通信するための重要な基盤技術である．現在主に用いられている公開鍵暗号には RSA 暗号 [8] と楕円曲線暗号 [3, 6] があるが，これらの暗号方式はいずれも Shor の量子アルゴリズム [9] を用いることによって破られることが知られている．そのため，量子コンピュータを用いても破られることのない耐量子暗号の開発が急務である．

同種写像暗号は，同種写像問題の困難性をその安全性の根拠とした暗号方式であり，耐量子暗号の候補として考えられている．同種写像暗号は，他の耐量子暗号の候補と比べて計算に時間がかかるが，鍵のサイズが小さいという利点がある．同種写像を用いた鍵共有プロトコルの一つに CSIDH [1] がある．

CSIDH では秘密鍵として，L_∞ ノルム球などの空間から一様にサンプルした整数ベクトルを用い，その秘密鍵に対応するイデアル類を楕円曲線に作用させることで公開鍵を得る．このイデアル類による作用の計算アルゴリズムを高速化することは CSIDH そのものの高速化に繋がるため重要な課題であり，近年盛んに研究されている．作用の計算量は秘密鍵の値に依存するため，秘密鍵空間を適切に変えることにより平均計算量を小さくすることができる．実際に，秘密鍵空間を重み付きの L_∞ ノルム球にすることで CSIDH を高速化できるということが [2, 4] でも示されている．

本研究では，秘密鍵と作用の計算量との関係性を精査し，その結果を用いることで平均計算量を最小化する最適な秘密鍵空間を提案する．また，この最適な秘密鍵空間は複雑であり，整数ベクトルを一様にサンプルすることが困難であるので，この秘密鍵空間をいくつかの簡単なノルム球で近似し，そのノルム球から整数ベクトルを一様にサンプルするアルゴリズムを提案する．

2　鍵空間の最適化

2.1　研究背景

CSIDH はイデアル類群の $\mathbb{F}_p$ 上定義された超特異楕円曲線の $\mathbb{F}_p$ 同型類の集合への群作用に基づいた鍵共有方式である．鍵共有の際は，作用計算のしやすい n 個のイデアル類 $I_1, \ldots, I_n$ と，ある秘密鍵空間 $\mathcal{A}$ $(\subset \mathbb{Z}^n)$ から一様ランダムに選ばれた秘密鍵 $\mathbf{e} = (e_1, \ldots, e_n)$ を用いて，$I^{\mathbf{e}} := \prod_{i=1}^n I_i^{e_i}$ という形で表されるイデアル類を用いる．CSIDH による Alice と Bob の鍵共有は鍵共有は以下の図のようにして行われる．

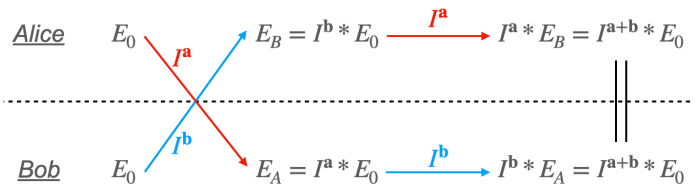

図 1. CSIDH による Alice と Bob の鍵共有の様子．

イデアル類 $I^{\mathbf{e}}$ の作用の計算量は秘密鍵 $\mathbf{e} \in \mathcal{A}$ の値に依存するため，秘密鍵をランダムに選んだ際の計算量の期待値は，秘密鍵空間 $\mathcal{A}$ に依存する．既存の研究では $\mathcal{A}$ として重み付き L_∞ ノルム球を採用し，その重みを変化させることにより計算量の期待値を減少させていたが，その多くはアドホックなものである上，重み付き L_∞ ノルム球以外の空間についての考察はされてこなかった．

2.2　研究成果

本研究では，$I^{\mathbf{e}}$ の作用の計算量を $T(\mathbf{e})$，鍵空間を $\mathcal{A}$ として $T(\mathbf{e})$ の期待値を最小化する次の問題を考える:

$$\begin{aligned} \min \quad & \mathbb{E}_{\mathbf{e}\in\mathcal{A}}[T(\mathbf{e})] \\ \text{subject to} \quad & \#\mathcal{A} \geq \sqrt{p}. \end{aligned}$$

ここで，条件 $\#\mathcal{A} \geq \sqrt{p}$ は安全性のために必要な条件である．最適な鍵空間 $\mathcal{A}_{\mathrm{opt}}$ はある実数 r を用いて次のように表される:

$$\mathcal{A}_{\mathrm{opt}} = \{\mathbf{e} \in \mathbb{Z}^n \mid T(\mathbf{e}) \leq r\}.$$

本研究では，$T(\mathbf{e})$ を $\mathbf{e}$ の式で与え，その上界 r の推定値を与えるアルゴリズムを提案した．さらに，これらの結果を用いて，CSIDH-512 というパラメータ設定下での最適な鍵空間 $\mathcal{A}_{\mathrm{opt}}^{512}$ と，その時の平均計算量 T_{opt} を求めた．

しかし，ここで求めた最適な鍵空間は複雑な空間であり，秘密鍵を一様ランダムにサンプルすることが困難である．そこで，$T(\mathbf{e})$ を $\|\mathbf{e}\|_1$ や $\|\mathbf{e}\|_1 + \|\mathbf{e}\|_\infty$ などのノルムで近似することを考え，L_1 ノルム球 $\{\mathbf{e} \in$

$\mathbb{Z}^n \mid \|\mathbf{e}\|_1 \leq r\}$ と (L_1+L_∞) ノルム球 $\{\mathbf{e} \in \mathbb{Z}^n \mid \|\mathbf{e}\|_1 + \|\mathbf{e}\|_\infty \leq r\}$ から秘密鍵を一様サンプルするアルゴリズムを提案した．なお, ここで提案したアルゴリズムは, 事前に計算した値をデータテーブルに保存しておく必要があり, 既存の L_∞ ノルム球を用いる場合と比べて, 追加のメモリが必要である．

最後に, CSIDH-512 の設定下で, 提案したノルム球を鍵空間として用いた場合の計算量と既存の鍵空間を用いた場合の計算量とを比較する実験を行なった．その結果を表 1 に示す．

表 1. 各ノルム球に対する計算量 ($\mathbb{F}_p$ 乗算回数)

ノルム	半径	計算量 T	T/T_{opt}
$\|\mathbf{e}\|_\infty$ [1, 5]	5	454,034	1.37
$\|\mathbf{e}\|_\infty$ (weighted) [7]	–	442,977	1.33
$\|\mathbf{e}\|_1$	152	355,804	1.08
$\|\mathbf{e}\|_1 + \|\mathbf{e}\|_\infty$	162	350,068	1.05

表 1 からわかる通り, L_1 ノルム球を用いることで, 従来の L_∞ ノルム球を用いた場合に比べて, 計算量が約 20% 削減された．また, この時の計算量は本研究で求めた最適値のわずか 1.08 倍であった．さらに, $(L_1 + L_\infty)$ ノルム球を用いた場合は, 従来の L_∞ ノルム球を用いた場合に比べて, 計算量が約 23% 削減され, 最適値のわずか 1.05 倍となった．なお, 秘密鍵を一様ランダムにサンプルするために用いたデータテーブルのサイズは L_1 ノルムで約 160Kbytes, $(L_1 + L_\infty)$ ノルムで約 11Mbytes だった．

3 定時間実装の場合

3.1 研究背景

暗号化処理にかかる時間が秘密鍵に依存するような場合, サイドチャネル攻撃により秘密鍵の情報の一部が漏れてしまう恐れがある．そのため, 処理時間が秘密鍵によらず一定になるような実装 (定時間実装) が必要である．

CSIDH の作用計算アルゴリズムの定時間実装は [4] で提案され, その計算量の削減について [2, 7] などで研究がなされてきた．

3.2 研究成果

本研究では, 定時間実装した場合の作用計算について簡単なモデルを考え, その計算量を最小化する秘密鍵空間を求める問題を考えた．そして, その緩和問題の最適解を求めることで, 近似解を導出した．

また, その結果を CSIDH-512 の設定下で用いることで, 計算量が [4] に比べて約 11% 減少することを実験的に確認した．

4 今後の課題

本研究では, 計算量の評価を簡単にするため, 作用計算アルゴリズムの一部を簡略化したモデルを用いた．より厳密な計算量評価を与えることは今後の課題である．また, $\mathcal{A}_{\mathrm{opt}}$ のより良い近似を求めることや, $(L_1 + L_\infty)$ ノルム球からのサンプリングで必要になる事前計算のデータ量を削減することも重要な課題である．

定時間実装に関する研究では, 緩和問題を考えることで近似解を与えたが, より厳密な解を求めることは今後の課題である．

参考文献

[1] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings, Part I*, pages 395–427. Springer, 2018.

[2] Aaron Hutchinson, Jason LeGrow, Brian Koziel, and Reza Azarderakhsh. Further optimizations of csidh: A systematic approach to efficient strategies, permutations, and bound vectors. In *International Conference on Applied Cryptography and Network Security*, pages 481–501. Springer, 2020.

[3] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.

[4] Michael Meyer, Fabio Campos, and Steffen Reith. On lions and elligators: An efficient constant-time implementation of CSIDH. In *International Conference on Post-Quantum Cryptography*, pages 307–325. Springer, 2019.

[5] Michael Meyer and Steffen Reith. A faster way to the CSIDH. In *International Conference on Cryptology in India*, pages 137–152. Springer, 2018.

[6] Victor S Miller. Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*, pages 417–426. Springer, 1985.

[7] Hiroshi Onuki, Yusuke Aikawa, Tsutomu Yamazaki, and Tsuyoshi Takagi. A faster constant-time algorithm of CSIDH keeping two points. In *International Workshop on Security*, pages 23–33. Springer, 2019.

[8] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[9] Peter W Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.