同種写像暗号 CSIDH の Edwards 曲線による構成と超特異曲線の信頼できる生成法

数理情報学専攻 48186207　守谷 共起
指導教員　高木 剛 教授

1　はじめに

公開鍵暗号は通信の安全を保証する技術であり，現在のインターネット社会において欠かすことのできない技術となっている．公開鍵暗号としては，RSA 暗号 [13] と，楕円曲線暗号 [10, 7] が広く使われている．ところが，この二つの暗号方式には，量子コンピュータによって多項式時間で破られるという問題がある [14]．そのため，量子コンピュータに耐性のある公開鍵暗号（耐量子暗号）の開発が急務の課題となっている．これに際して，アメリカ国立標準技術研究所 (NIST) は 2016 年に耐量子暗号の標準化に向けて公募を宣言した [11]．

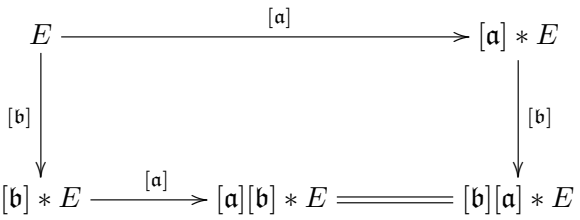
同種写像暗号は楕円曲線暗号をある意味で拡張した暗号方式であり，耐量子暗号の候補として考えられている．事実，同種写像暗号の鍵共有プロトコルである SIDH をカプセル化した SIKE[1] は，NIST の耐量子暗号の候補として残っている．同種写像暗号は同種写像問題と呼ばれる数学問題の計算量的困難性に安全性の根拠を置いている．

本研究では，Montgomery 曲線上でのみ考えられていた同種写像暗号の鍵共有プロトコル CSIDH を，Edwards 曲線上のアルゴリズムに拡張した．また，同種写像暗号において用いられる超特異楕円曲線の信頼できる生成法について提案を行った．

2　CSIDH の Edwards 曲線を用いた構成

2.1　研究背景

CSIDH[2] は有限可換群の超特異楕円曲線の同型類の集合への作用 [15] に基づいた同種写像暗号の鍵共有方式である．群作用における次の図式を作ることで鍵共有を実現する．



一般の楕円曲線については，この群作用の計算を効率的に行うのは困難である．CSIDH においては，Montgomery 型と呼ばれる楕円曲線（Montgomery 曲線）の性質を使い，効率的な作用計算を実現している．

一方で，楕円曲線には Montgomery 曲線以外の型の曲線が知られている．これは，楕円曲線暗号の効率化や安全性の向上という目的で考えられてきたものである．こうした Montgomery 曲線以外の曲線において，CSIDH のアルゴリズムを実行する方法は知られていない．

2.2　研究成果

本研究では，Edwards 曲線と呼ばれる楕円曲線の上で CSIDH を動かすアルゴリズムを提案した．アルゴリズムを実現するために，Edwards 曲線に関する新しい定理を 4 つ証明した．

また，提案アルゴリズムと従来の CSIDH のアルゴリズムの計算回数を，理論と実験両方で比較した．提案アルゴリズムは，理論的にも実験的にも，従来のものと比較して僅かながら高速なアルゴリズムとなった．

3　超特異楕円曲線の信頼できる生成法

3.1　研究背景

同種写像暗号は，超特異楕円曲線と呼ばれる特殊な楕円曲線を使って計算を行うように設計されている．ところが，超特異楕円曲線には信頼できる生成が困難であるという問題がある．

超特異楕円曲線は楕円曲線全体と比較すると，指数関数的に数が少なく，ランダムな楕円曲線は現実的なスケールでは超特異楕円曲線にはなり得ない．既に超特異楕円曲線だと知られている特殊な楕円曲線も存在しているが，これらの特殊な楕円曲線を使ったプロトコルは脆弱性があることがわかっている．したがって，脆弱性のないような超特異楕円曲線を生成する手法が求められている．そうした方法の一つとして，CGL ハッシュ関数 [4] を用いてランダムな超特異楕円曲線を生成するという方法がある．ところが，この方法では特定の人物のみが同種写像の情報を知ることができるという問題点があり，この手法で生成される超特異楕円曲線は信頼できる楕円曲線にはならない．信頼できる生成法として考えられるものに G-SIDH[6] がある．これはグ

ループ鍵共有方式であり，複数人の秘密鍵を合わせることで超特異楕円曲線が生成できるため，特定の人物が多くの情報を得ることができない．ところが，G-SIDH にも問題がある．G-SIDH は p のビット長を生成に関わる人数に比例したものを取る必要があるため，効率的な生成法にはならない．信頼できる方法で脆弱性のない超特異楕円曲線を効率的に生成することは，同種写像全体にかかわる重要な課題であるが，有用な解決法については提案がなされていない．

3.2 研究成果：G-CSIDH

初めに，CSIDH を複数人の鍵共有方式 G-CSIDH に拡張した．以下でプロトコルを述べる．パーティ $U_1, \ldots, U_u$ が共通の超特異楕円曲線を生成しようとしている．

セットアップ: CSIDH と同じ設定とする．

鍵生成: パーティ U_j の秘密鍵を $[\mathfrak{a}_j]$ とする．

- **ステップ 1**: U_j は $[\mathfrak{a}_j]$ の E_0 への作用を計算し，超特異楕円曲線 $E_{A_1^{(j)}} = [\mathfrak{a}_j] * E_0$ を得る．U_j はこの曲線を U_{j+1} に送る．
- **ステップ k $(2 \leq k \leq u-1)$**: U_j は $[\mathfrak{a}_j]$ の $E_{A_{k-1}^{(j-1)}}$ への作用を計算し，超特異楕円曲線 $E_{A_k^{(j)}} = [\mathfrak{a}_j] * E_{A_{k-1}^{(j-1)}}$ を得る．U_j はこの曲線を U_{j+1} に送る．

鍵共有: U_j は $[\mathfrak{a}_j]$ の $E_{A_{u-1}^{(j-1)}}$ への作用を計算し，超特異楕円曲線 $E_{A^{(j)}} = [\mathfrak{a}_j] * E_{A_{u-1}^{(j-1)}}$ を得る．この曲線を共有鍵とする．

このプロトコルにより，$U_1, \ldots, U_u$ は $[\mathfrak{a}_1] \cdots [\mathfrak{a}_u] * E_0$ を共有する．

さらに，G-CSIDH の安全性が CSSDDH 仮定に帰着されることを証明した．CSSDDH 仮定は，CSIDH の安全性を保証する仮定である．

3.3 研究成果：信頼できる超特異楕円曲線の生成法

秘密分散のアイディアを利用し，信頼できる超特異楕円曲線の生成法の定義を行った．具体的には，超特異楕円曲線の生成に関わった u 人のうち $u-1$ 人が共謀しても超特異楕円曲線の情報が割れないとき，この生成法を信頼できる生成法と呼ぶ．

この定義の下で，G-CSIDH が安全ならば，G-CSIDH が信頼できる超特異楕円曲線の生成法になっていることを証明した．

4 今後の課題

一つ目の研究では，単純な CSIDH のアルゴリズムを Edwards 曲線を用いたアルゴリズムに拡張した．一方で，CSIDH は秘密鍵によって計算時間が異なるため，アルゴリズムの実行時間を計測することで秘密鍵の情報が漏れてしまう．そのため，定時間の CSIDH のアルゴリズムを考えることは重要な課題である．現在知られている定時間アルゴリズムを Edwards 曲線に拡張することが今後の課題である．

また，最近，Hessian 曲線の同種写像の計算公式が新たに提案された [5, 8]．この曲線の上で CSIDH アルゴリズムを動かす手法は発見されていない．この曲線に CSIDH アルゴリズムを拡張することも今後の課題である．

二つ目の研究では，情報を分散させることで信頼できる超特異楕円曲線を生成する手法を提案した．一方で，現実的な要求を考慮に入れると，純粋に超特異楕円曲線をランダムに生成する方が望ましい．このような手法は現在発見されておらず，このような手法の提案も今後の課題である．

参考文献

[1] Reza Azarderakhsh, Matthew Campagna, Craig Costello, LD Feo, Basil Hess, A Jalali, D Jao, B Koziel, B LaMacchia, P Longa, et al. Supersingular isogeny key encapsulation. *Submission to the NIST Post-Quantum Standardization project*, 2017.

[2] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In *International Conference on the Theory and Application of Cryptology and Information Security–ASIACRYPT 2018*, pages 395–427. Springer, 2018.

[3] Daniel Cervantes-Vázquez, Mathilde Chenu, Jesús-Javier Chi-Domínguez, Luca De Feo, Francisco Rodríguez-Henríquez, and Benjamin Smith. Stronger and faster side-channel protections for csidh. In *International Conference on Cryptology and Information Security in Latin America–LATINCRYPT 2019*, pages 173–193. Springer, 2019.

[4] Denis X Charles, Kristin E Lauter, and Eyal Z Goren. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113, 2009.

[5] Thinh Dang and Dustin Moody. Twisted hessian isogenies. *IACR Cryptology ePrint Archive*, 2019:1003, 2019. https://ia.cr/2019/1003.

[6] Satoshi Furukawa, Noboru Kunihiro, and Katsuyuki Takashima. Multiparty key exchange protocols from supersingular isogenies. In *International Symposium on Information Theory and Its Applications–ISITA 2018*, pages 208–212. IEEE, 2018.

[7] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, pages 203–209, 1987.

[8] Perez Broon Fouazou Lontouo and Emmanuel Fouotsa. Analogue of Vélu's formulas for computing isogenies over Hessian model of elliptic curves.

[9] 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–PQCrypto 2018*, pages 307–325. Springer, 2019.

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

[11] National Institute of Standards and Technology. Post–quantum cryptography standardization, December 2016. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization.

[12] Hiroshi Onuki, Yusuke Aikawa, Tsutomu Yamazaki, and Tsuyoshi Takagi. A Faster Constant-time Algorithm of CSIDH keeping Two Points. In *Advances in Information and Computer Security–IWSEC 2019*, pages 23–33. Springer, 2019.

[13] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, pages 120–126, 1978.

[14] 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.

[15] William C Waterhouse. Abelian varieties over finite fields. In *Annales scientifiques de l'École Normale Supérieure*, pages 521–560, 1969.