同種写像暗号 CSIDH におけるランダム自己帰着に基づいた効率的な認証鍵共有

数理情報学専攻 48-196211　川島智紀
指導教員　高木剛 教授

1　研究背景

現在広く用いられている公開鍵暗号の多くは，量子計算機と呼ばれる計算機を用いて，解読できることが知られている [8]．現状では大きなメモリを持つ量子計算機は実現されていないため，直ちに大きな問題があるわけではないが，量子計算機の出現に備えて，量子計算機でも破られない耐量子計算機暗号の研究が重要である．

耐量子計算機暗号の一つの例として，同種写像暗号と呼ばれるクラスの暗号がある．これは，楕円曲線の間の準同型写像である同種写像の計算が，量子計算機を用いても困難であると考えられていることを基にした暗号プロトコルの総称であり，SIDH [4] や CSIDH [2] といった具体的な鍵共有プロトコルが提案されている．鍵共有プロトコルとは，通信が公開される状況で，二者の間で秘密の値 (鍵) を共有するプロトコルである．SIDH や CSIDH は，現在広く用いられている Diffie–Hellman 鍵共有 [5] と同様の構造を持つ．Diffie–Hellman 鍵共有は耐量子性を持たないことに注意が必要である．

2　ランダム自己帰着性についての比較

本研究では，ランダム自己帰着性と呼ばれる性質に着目して，SIDH や CSIDH を Diffie–Hellman 鍵共有と比較した．ここで，問題 P がランダム自己帰着性を持つとは，その問題をマルチ化した問題 (複数個のインスタンスから一つを選んで解く問題) にタイトに帰着できることを指し，この性質はユーザーが複数いる状況での安全性証明で有用な性質である．Diffie–Hellman においては，計算問題，判定問題とギャップ問題のいずれもランダム自己帰着性を持つ一方で，SIDH は計算問題と判定問題のいずれもランダム自己帰着性が示されておらず，かつ暗号学上適切なギャップ問題が見つかっていない．そのなかで本研究では，CSIDH の計算問題とギャップ問題がランダム自己帰着性を持つことを示した (図 1)．なお，ギャップ問題とは対応する判定問題を解くオラクルへのアクセスが与えられたもとで計算問題を解く問題のことで，認証鍵共有での安全性証明において有用である．

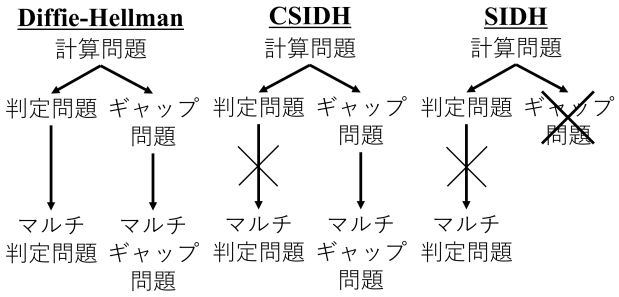

図 1. Diffie-Hellman, CSIDH, SIDH のランダム自己帰着性に関する比較.

また，CSIDH の判定問題がランダム自己帰着性を持たないことの一つの根拠として，「代数的」な計算方法のみで CSIDH の判定問題のランダム自己帰着性を示すことができる場合，その判定問題が容易であるということを示した．CSIDH においては，計算問題だけでなく判定問題も困難であると考えられているため，これは CSIDH の判定問題がランダム自己帰着性を持たないことの一つの根拠といえる．CSIDH は有限群の有限集合への群作用を用いて鍵共有を実現するが，このときアルゴリズムが代数的であるとは，この群の演算と群作用のみを用いて計算されるアルゴリズムを指す．この「代数的」という言葉は，群における問題の困難性などを示す際に用いられてきた [6] が，本研究でこれを CSIDH へと拡張した．また，本研究でこのモデルの下では，群作用の逆作用を計算することと，鍵共有の安全性を破ることが等価であることを示した．

3　CSIDH におけるランダム自己帰着に基づいた効率的な認証鍵共有

本研究の第二の貢献は，CSIDH のギャップ問題がランダム自己帰着性を持つことの応用例として，耐量子性を持ち，かつ最適タイトな認証鍵共有 Π_{CSIDH} を提案したことである (図 2)．この構成は Cohn-Gordon ら [3] の構成に基づいており，ユーザー数に比例したセキュリティロスを持つ．ここで，セキュリティロスとは，暗号プロトコルの安全性と，困難性を仮定する問題の困難性の間の差のことで，セキュリティロスが大きいと，ある安全性を達成するために用いられるパラメータの大き

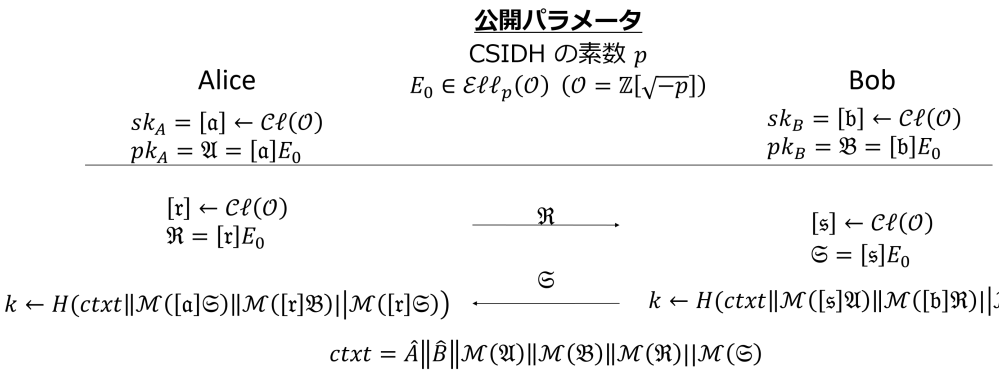

図 2. 本研究で提案した認証鍵共有 Π_{CSIDH}.

さが大きくなるため，結果的にプロトコルが遅くなる．

さらに，本研究では既存の CSIDH を基にした認証鍵共有 [7] と効率性の比較を行い，110 ビットの安全性を目指した際に，提案プロトコルの方が高速であることを示した (表 1)．この際，ユーザー数と，各ユーザーの鍵共有の最大回数はそれぞれ 2^{16} として，クロックサイクル数の評価には，論文 [1] の結果を用いた．「群作用」は，一回の鍵共有で各ユーザーが何回の群作用評価を行うかを指し，「クロックサイクル数」は一回の鍵共有で一人のユーザーが行う計算の計算時間の期待値を指す．特に，CSIDH UM と比べた際に，CSIDH UM の方が一回の鍵共有あたりの群作用の計算回数は少ないものの提案プロトコルの Π_{CSIDH} の方が高速であるのは，Π_{CSIDH} の方が小さなパラメータを用いることができるためで，これは Π_{CSIDH} がセキュリティロスを小さくすることを意識して構成されたことの一つの利点となっている．

表 1. CSIDH を基にした認証鍵共有の計算時間の比較.

プロトコル	群作用	クロックサイクル数
CSIDH UM	3	$719\mathrm{M} \times 3 = 2,157\mathrm{M}$
CSIDH Biclique	5	$120\mathrm{M} \times 5 = 600\mathrm{M}$
Π_{CSIDH}	4	$120\mathrm{M} \times 4 = 480\mathrm{M}$

4 今後の課題

CSIDH のランダム自己帰着性についての今後の課題としては，代数的でない方法でランダム自己帰着性を示すことが挙げられる．ランダム自己帰着性は様々な暗号プロトコルの安全性証明で有用であるため，これを示すことができれば大きな貢献となる．また，今回提案した認証鍵共有については，より強い安全性モデルの下で安全な認証鍵共有を構成することが課題として挙げられる．

参考文献

[1] Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. Faster computation of isogenies of large prime degree. Cryptology ePrint Archive, Report 2020/341, 2020. `https://eprint.iacr.org/2020/341`.

[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*, pages 395–427. Springer, 2018.

[3] Katriel Cohn-Gordon, Cas Cremers, Kristian Gjøsteen, Håkon Jacobsen, and Tibor Jager. Highly Efficient Key Exchange Protocols with Optimal Tightness. In *Advances in Cryptology – CRYPTO 2019*, pages 767–797, Cham, 2019. Springer International Publishing.

[4] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014.

[5] W. Diffie and M. Hellman. New Directions in Cryptography. *IEEE Trans. Inf. Theor.*, 22(6):644–654, 1976.

[6] Georg Fuchsbauer, Eike Kiltz, and Julian Loss. The Algebraic Group Model and its Applications. In *Advances in Cryptology – CRYPTO 2018*, pages 33–62, Cham, 2018. Springer International Publishing.

[7] Atsushi Fujioka, Katsuyuki Takashima, and Kazuki Yoneyama. One-Round Authenticated Group Key Exchange from Isogenies. In *ProvSec 2019*, pages 330–338, 2019.

[8] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.