同種写像問題に基づく暗号技術

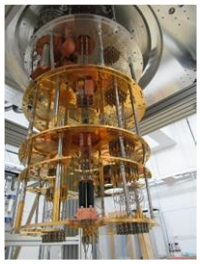
Cryptographic Techniques Based on the Isogeny Problem

松浦栄亮・システム分科会・情報セキュリティ大学院大学

Abstruct : In recent years, research and development in quantum computing have advanced significantly, leading to the introduction of quantum algorithms that pose a threat to existing cryptographic systems. If large-scale, general-purpose quantum computers are realized, cryptographic schemes based on the hardness of integer factorization and the discrete logarithm problem, such as RSA and elliptic curve cryptography (ECC), are likely to be broken. Consequently, the development of post-quantum cryptography (PQC) that can withstand attacks from quantum computers has become an urgent task.Currently, the U.S. National Institute of Standards and Technology (NIST) is conducting the selection process for post-quantum cryptographic standards, and isogeny-based cryptography is among the candidates. Isogeny-based cryptography is a cryptographic scheme that uses two elliptic curves as a public key and an isogeny between them as a private key. It has the smallest key size among PQC candidates but is computationally intensive.In this report, we investigate the fundamental concepts and key exchange protocols based on the isogeny problem as part of efforts to accelerate computational processing. Additionally, we outline future directions based on our findings.

1. 背景・目的

耐量子計算機暗号は、量子コンピュータの発展に伴い、従来の公開鍵暗号（RSA、ECCなど）が破られる可能性があることから、新たな安全な暗号方式を確立するために研究されている分野である。Shorのアルゴリズムに代表される量子アルゴリズムに対して耐性を持つ暗号方式が求められ、その中でも 同種写像暗号は、楕円曲線同種写像を基にした耐量子暗号の一つであり、研究が進められている。



理研の超電導量子コンピュータ

Peter Williston Shor (1959 -)

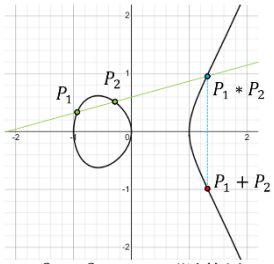
2. 同種写像暗号とは

2-1. 有限体上の楕円曲線

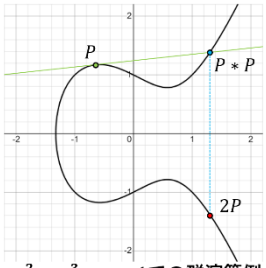
有限体上の楕円曲線は、次のような形で定義される:

$$E : y^2 = x^3 + ax + b$$

この曲線の上で定義された点の集合は、加法群を形成し、暗号アルゴリズムに利用される。



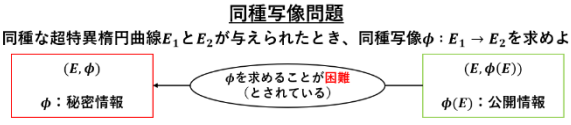
$y^2 = x^3 - x$での群演算例
（$P_1 \neq P_2$のとき）



$y^2 = x^3 - x + 1$での群演算例
（$P_1 = P_2$のとき）

2-2. 楕円曲線間の同種写像

楕円曲線E_1からE_1への同種写像とは、加法構造を保つ準同型写像であり、核を持つ。同種写像が難しい理由は、特定の楕円曲線から別の楕円曲線への同種写像を求める計算が難しいためである。



3. 同種写像題に基づいた鍵共有

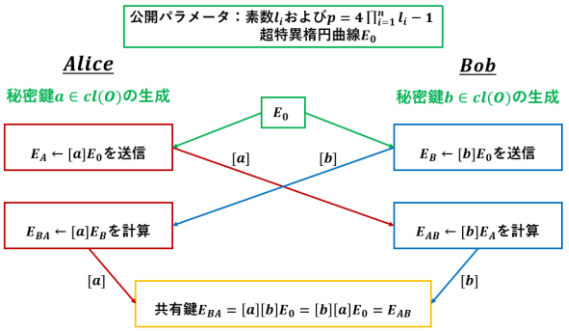
3-1. イデアル類群の作用

CSIDHでは、虚二次体上の整環におけるイデアル類群$cl(\mathcal{O})$の作用を楕円曲線の集合上に定義する。具体的には:

- イデアル類群$cl(\mathcal{O})$の要素が同種写像を決定する。
- CSIDHの秘密鍵は、イデアル類群の元として扱われ、対応する同種写像を計算することで公開鍵が得られる。
- イデアル類群の作用が計算困難であるため、安全性が保証される。このクラス群の作用により、鍵共有プロトコルが実現される。

3-2. CSIDHのプロトコル

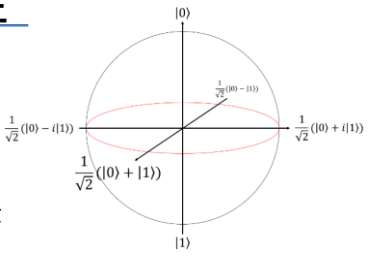
CSIDHの具体的なプロトコルは以下になる。



4. 研究の方向性

4-1. 量子マネーとは

量子マネーとは、量子力学の複製不可能性を利用し、偽造を防ぐデジタル通貨である。量子状態を銀行券とし、秘密鍵または公開鍵で検証可能な仕組みを持つ。



量子状態イメージ

4-2. 量子技術を用いた同種写像暗号

ASIACRYPT2024で発表されたMontgomery&Sharifの研究では、CSIDHと同じくイデアル類群の作用を利用した方式であり、その上で、量子マネーの設計をするという新たな応用を示した。具体的にはイデアル類群の作用を利用して量子マネーを構築し、その際に楕円曲線の同種類を一様な重ね合わせで表現する方法を提案した。これは、量子暗号とイデアル類群の作用を用いた暗号手法の発展に大きく貢献する可能性があり、新しい暗号技術としての発展が見込める。