2次元の同種写像を用いた耐量子安全なコミットメントスキームの構成に関する研究

A Study on Construction of Post-Quantum Commitment Schemes Using Two-dimensional Isogenies

松浦 栄亮・ネットワーク分科会・情報セキュリティ大学院大学

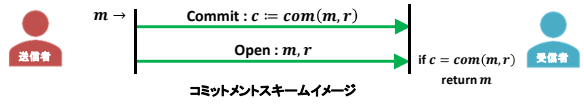
Abstract：Looking ahead to a future in which advances in quantum computing will undermine the security of RSA and elliptic-curve cryptography, we propose a post-quantum com mitment scheme based on isogenies. A commitment scheme is a cryptographic primi tive used in applications such as electronic voting and blockchains. As prior work on isogeny-based commitments, schemes using the CGL hash function have been proposed. However, in such schemes, the number of isogeny evaluations grows proportionally to the message length, and generating the starting curve requires a trusted setup, or al ternatively imposes constraints such as selecting specific curves to reduce the likelihood of collisions. In this study, we leverage two-dimensional isogenies derived from Kani’ s lemma, which enables efficient representation and evaluation even for non-smooth degrees, and we design the protocol so that the message is embedded into the degree of an endomorphism via the Deuring correspondence. To satisfy the required security properties, we further refine the protocol by using torsion points. As a result, we con struct a new isogeny-based commitment scheme that does not require a trusted setup, even when the starting curve has a known endomorphism ring.

本研究の貢献

- メッセージを同種写像の次数に埋め込む新たなコミットメントスキームの構成を提案
- 先行研究で必要とされた，開始曲線のセットアップ過程を必要としない方式を実現

背景

- コミットメントスキームはZKP，電子投票等で活用される暗号プロトコル
- PQC時代に備え，耐量子性を持つコミットメントスキームの開発が必要
- 同種写像問題は量子計算機でも困難とされ，同種写像暗号はPQC候補



コミットメントスキームイメージ

コミットメントスキームの安全性に必要な条件

- 秘匿性：コミットメント情報 c からは，メッセージ m が分からない．
- 束縛性：一度コミットした後に，異なるメッセージ $m \neq m'$ を同一のコミットメント情報 c に対応させて開示することができない．

同種写像

同種写像の定義

- E, E'を楕円曲線とする．有理式で表せる群準同型写像 ϕ が $\phi : E \to E'$ で $\phi(O_E) = O_{E'}$ を満たすとき，ϕ を同種写像という．

同種写像問題 ：楕円曲線 E, E' から同種写像 $\phi : E \to E'$ を求めよ．
→ ϕの次数が高い場合，同種写像問題は量子計算機でも困難

2次元の同種写像（ Kani の補題 ）

次の条件を満足する写像を考える．

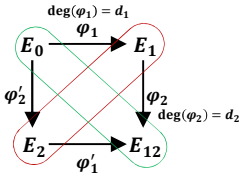
- $\varphi_2 \circ \varphi_1 = \varphi_1' \circ \varphi_2'$
- $\deg(\varphi_1) = d_1,\ \deg(\varphi_2) = d_2$
- $d \coloneqq d_1 + d_2$
- d_1およびd_2は正の互いに素な整数

このとき，次の写像は (d,d)-同種写像である．

$$\Phi = \begin{pmatrix} \varphi_1 & \widehat{\varphi_2} \\ -\varphi_2' & \widehat{\varphi_1'} \end{pmatrix} : E_0 \times E_{12} \to E_1 \times E_2$$

さらに，同種写像Φの核は次のように表される．

$$\mathrm{Ker}(\Phi) = \{([d_1]P, \varphi_2 \circ \varphi_1(P)) \mid P \in E_0[d]\}.$$



提案コミットメントスキーム

2次元同種写像を用いて入力メッセージを同種写像の次数に埋め込む構成

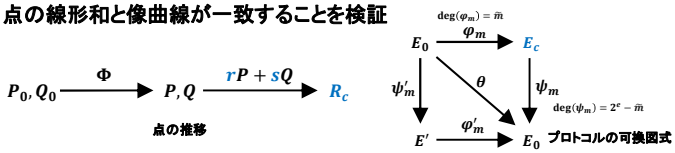
コミットメント情報：(E_c, r, s, R_c)　オープン情報：$(m,\ \theta)$

コミットフェーズの流れ（入力：m　出力：(E_c, r, s, R_c)，$(m,\ \theta)$）

① メッセージ m をパディングして $\tilde{m}$ を作る
② $\deg(\theta) = \tilde{m}(2^e - \tilde{m})$ を満たす自己準同型 $\theta \in End(E_0)$ をサンプル
③ 2次元同種写像 $\Phi : E_0 \times E_0 \to E_c \times E'$ の像 $P = \varphi_m(P_0), Q = \varphi_m(Q_0)$ を計算
④ 乱数 r, s を選び，ランダム線形和 $R_c = rP + sQ$ を計算

オープンフェーズの流れ（入力：(E_c, r, s, R_c)，$(m,\ \theta)$ 出力：m or $\perp$）

受信者はコミットフェーズと同様の手順で Φ を再構成，$rP + sQ$ を再計算し，点の線形和と像曲線が一致することを検証



提案コミットメントスキームの安全性

秘匿性：任意の m_0, m_1 で C_{m_0}, C_{m_1} は計算量的に識別不能

① m が十分に大きいとき，E_c は $\mathbb{F}_p$ 上の超特異曲線上一様に分布する
② 乱数 r, s の効果より，R_c は$E_c[2^e]$上一様に分布する
③ 仮定：$R_c = \varphi(rP_0 + sQ_0), r, s, E_c$から，$\varphi : E_0 \to E_c$を求めることは困難
→ よって，$m = \deg(\varphi)$ を求めることは困難

以上より，m が十分に大きいとき，コミットメント情報 $c = (E_c, r, s, R_c)$ は m とは独立に分布すると期待できる．

束縛性：同じコミットメント c から異なる $m \neq m'$ を開示できない

- c から $m \neq m'$ を開示できると仮定
→ 検証で再構成される点が一致し，$\varphi(R_0) = \varphi'(R_0)$ が出る
$\psi = \varphi - \varphi'$ とおくと
上界：$\deg(\psi) < (m + m')$ かつ $m, m' < 2^{e-2}$ ⇒ $\deg(\psi) < 2^e$
下界：$R_0(|R_0| = 2^e)$ が $\ker(\psi)$ に含まれる ⇒ $deg(\psi) \geq 2^e$
上下界が矛盾 ⇒ 開示は一意

先行研究との比較

	先行研究①	先行研究②	本研究提案方式
Trusted setup	✕ 必要	○ 不要	○ 不要
開始曲線の制約	✕ 開始曲線は自己準同型環を秘密にする必要がある	✕ CGLハッシュ関数の衝突が起きない開始曲線を選ぶ必要がある	○ 自己準同型環が既知の楕円曲線 $E_0 : y^2 = x^3 + x$でよい
同種写像計算	△ 多数回の1次元同種写像	△ 多数回の1次元同種写像	△ 少数回の2次元同種写像

※ Φ の計算には Kummer surface を使用できるため，恐らく先行研究より計算が速いと考えられる