論　文

2次ツイストを利用したSIDH

松尾　和人[†]

SIDH over Quadratic Twists

Kazuto MATSUO[†]

あらまし　Jao と De Feo によって提案された，超特異楕円曲線間の同種写像を求める問題の難しさに基づく Diffie-Hellman 鍵共有プロトコル (SIDH) は，量子計算に対する耐性を有するプロトコルとして注目され近年盛んに研究されている．しかし，超特異楕円曲線のとりうる位数が限定的なため利用可能な曲線が少ないことが課題の一つとして挙げられている．本論文では，超特異楕円曲線とその 2 次ツイストを同時に用いる SIDH の変形構成を提案する．提案構成はこれまでの SIDH と異なる曲線上でこれまでと同程度の効率の SIDH を実現可能であり，利用可能な効率的な曲線もこれまでの SIDH と同程度存在する．したがって，提案構成によってより豊富な SIDH を利用可能となる．また，提案構成はこれまでの SIDH よりも小さな有限体上で同程度の安全性を達成できる場合があり，より効率的な SIDH を構成できる可能性がある．

キーワード　SIDH，同種写像暗号，同種写像，2 次ツイスト，耐量子暗号

1. まえがき

有限体上の通常楕円曲線間の同種写像を求めることの困難性を用いた暗号プロトコル [1]～[3] は耐量子暗号として注目されていた．しかし，Childs と Jao [4] によって通常楕円曲線間の同種写像を求める問題の準指数時間計算量の量子計算アルゴリズムが提案されたため，この同種写像を用いた暗号は他の耐量子暗号と比較して優位性が認められなくなった．一方で，Jao と De Feo [5] が提案した，超特異楕円曲線間の同種写像を求めることの困難性を用いた Diffie-Hellman 鍵共有プロトコル (SIDH) は，超特異楕円曲線間の同種写像を求める問題に対し古典アルゴリズム，量子アルゴリズムともに指数時間計算量アルゴリズムしか知られていないため，耐量子暗号の候補として期待されている．そのため，SIDH に関する安全性に関する議論 [6]～[8] や効率的な実装方式 [9], [10] の研究が盛んに行われ，これらの成果として，SIDH を基に構成された鍵カプセル化方式 (SIKE) [11] が NIST の耐量子暗号コンペティションに提案されている．しかし，SIDH は利用可能な曲線が限定的であることが課題の一つとして挙げられている [12].

本論文では，2 次ツイストの 2 曲線それぞれの同種写像を利用することで，これまでとは異なるパラメータ設定の SIDH を構成可能であることを示す．また本論文で提案する構成は Jao と De Feo の SIDH と同程度の効率を実現可能であることを示す．これにより，Jao と De Feo の SIDH と本論文で提案する構成を併用することでより多くの SIDH を提供可能となる．本論文は [13] の拡張投稿版であるが，最近になって Costello [14] により本論文の提案と同様のアイディアの構成が独立に提案された．Costello は本論文のアイディアに加えて複数のねじれ群を利用することで，より効率的な構成ができる可能性を示している．

本論文の構成を以下に示す．まず，**2.** で超特異楕円曲線とその 2 次ツイストを定義し，本研究に必要な性質をまとめる．また，同種写像についてもまとめる．次に，**3.** で Jao と De Feo [5] が提案した SIDH を概説する．また，Jao と De Feo の SIDH に利用可能な曲線パラメータの具体例を挙げる．そして，**4.** で 2 次ツイストを利用した SIDH の変形を提案し，**5.** で提案構成の Montgomery 曲線を利用した効率的な構成を示す．**6.** では提案構成に利用可能な曲線パラメータ

[†] 神奈川大学，平塚市
Kanagawa University, Hiratsuka-shi, 259–1293 Japan

(注1)：本論文では，「だ円」を「楕円」と表記する．

の具体例を挙げるとともに，提案構成で利用可能な曲線パラメータに対応する Montgomery 曲線が存在することを示す．更に，**7.** では提案構成の具体的な数値例を示す．最後に **8.** でまとめる．

2. 超特異楕円曲線と同種写像

本章では，超特異楕円曲線とその 2 次ツイスト及びこれらに対して定義される同種写像を紹介し，本論文で必要となる性質をまとめる．

2.1 超特異楕円曲線とその 2 次ツイスト

p を奇素数，$q = p^2$ とし，E を $\mathbb{F}_q$ 上の超特異楕円曲線とする．E をモニック 3 次多項式 $F(X) \in \mathbb{F}_q[X]$ と $b \in \mathbb{F}_q^*$ によって

$$E : bY^2 = F(X) \tag{1}$$

と定義する．また，E の j 不変量を $j(E)$ と書く．E の $\mathbb{F}_q$ 有理点群 $E(\mathbb{F}_q)$ の位数は $\#E(\mathbb{F}_q) = p^2 + 1$, $\#E(\mathbb{F}_q) = p^2 \pm p + 1$, $\#E(\mathbb{F}_q) = (p \pm 1)^2$ のいずれかになることが知られている [15, Theorem 4.1]．以下では $\#E(\mathbb{F}_q) = (p \pm 1)^2$ であるとする．$\#E(\mathbb{F}_q) = (p+1)^2$ のとき $E(\mathbb{F}_q) \cong (\mathbb{Z}/(p+1)\mathbb{Z})^2$，$\#E(\mathbb{F}_q) = (p-1)^2$ のとき $E(\mathbb{F}_q) \cong (\mathbb{Z}/(p-1)\mathbb{Z})^2$ が成立する [16, 4.8]．

E の（非自明な）2 次ツイストを

$$E^t : \delta b Y^2 = F(X) \tag{2}$$

と定義する．ここで，$\delta \in \mathbb{F}_q^*$ は $\mathbb{F}_q$ 上平方非剰余である．E と E^t は $E(\mathbb{F}_q) \not\cong E^t(\mathbb{F}_q)$ かつ $E(\mathbb{F}_{q^2}) \cong E^t(\mathbb{F}_{q^2})$ を満足する．したがって，$E(\overline{\mathbb{F}_q}) \cong E^t(\overline{\mathbb{F}_q})$ であり，$j(E) = j(E^t)$ である．また，$\#E(\mathbb{F}_q) = (p+1)^2$ のとき $\#E^t(\mathbb{F}_q) = (p-1)^2$ であり，$\#E(\mathbb{F}_q) = (p-1)^2$ のとき $\#E^t(\mathbb{F}_q) = (p+1)^2$ である．$E(\overline{\mathbb{F}_q})$ から $E^t(\overline{\mathbb{F}_q})$ への同型写像 τ は

$$\begin{aligned} \tau : E(\overline{\mathbb{F}_q}) &\to E^t(\overline{\mathbb{F}_q}) \\ (x, y) &\mapsto (x, y/\sqrt{\delta}) \end{aligned} \tag{3}$$

で与えられる．

2.2 同種写像

楕円曲線 $E/\mathbb{F}_q$ から $E'/\mathbb{F}_q$ への非定数準同型写像

$$\phi : E(\overline{\mathbb{F}_q}) \to E'(\overline{\mathbb{F}_q})$$

が有理関数として式 (4) の形式で与えられるとき，ϕ を $\mathbb{F}_q$ 上の同種写像と呼ぶ [17, 12.2]．

$$\phi((x, y)) = \left(\frac{n_X(x)}{d_X(x)}, y\frac{n_Y(x)}{d_Y(x)} \right) \tag{4}$$

ここで，$n_X, d_X, n_Y, d_Y \in \mathbb{F}_q[X]$ である．ϕ が存在するとき，E と E' は同種であるという．ϕ の次数を $\deg \phi = \max(\deg n_X, \deg d_X)$ と定義し，次数 d の同種写像を d-同種写像と呼ぶ．$\mathrm{d}n_X(X)/\mathrm{d}X \neq 0$ のとき ϕ を分離同種写像と呼ぶ．本論文では $\mathbb{F}_q$ 上の分離同種写像のみを考慮し，以下ではこれを同種写像と略す．

$E(\mathbb{F}_q)$ の任意の部分群 $K \subset E(\mathbb{F}_q)$ に対して K を核とする $\#K$-同種写像 $\phi : E(\overline{\mathbb{F}_q}) \to E'(\overline{\mathbb{F}_q}) \cong E(\overline{\mathbb{F}_q})/K$ が存在する．Vélu [18] は，与えられた $E/\mathbb{F}_q$ と K に対して，同種写像 $\phi : E(\overline{\mathbb{F}_q}) \to E'(\overline{\mathbb{F}_q}) \cong E(\overline{\mathbb{F}_q})/K$ とその像 $E'/\mathbb{F}_q$ を与える公式を示した．Vélu の公式を用いて次数の小さい同種写像を効率的に計算可能である．SIDH は，次数が小さな素数の冪である同種写像に Vélu の公式を繰り返し適用することで，効率的に実現されている．

3. 超特異楕円曲線の同種写像を用いた DH 鍵共有プロトコル (SIDH)

2011 年に Jao と De Feo [5] によって同種写像を利用した耐量子 Diffie-Hellman 鍵共有プロトコル (SIDH) が提案され，2014 年に De Feo, Jao と Plût [9] がその改良を提案した．以下では，Alice と Bob が SIDH によって鍵共有を行う手順を「初期設定」,「鍵生成」,「鍵共有」のそれぞれについて紹介する．また，効率的な実装が可能な現実的なサイズの曲線パラメータの具体例を示す．

3.1 初期設定

ℓ_A, ℓ_B を互いに異なる小さな素数とする．効率を考慮し，これらを $\ell_A = 2$, $\ell_B = 3$ と設定するのが一般的である [5], [9]～[11]．p を ℓ_A, ℓ_B と異なる奇素数とし，e_A, e_B をそれぞれ $\ell_A^{e_A}\ell_B^{e_B} \mid p + 1$（または $\ell_A^{e_A}\ell_B^{e_B} \mid p - 1$）を満足する最大の非負整数とする．まず，$\#E(\mathbb{F}_q) = (p+1)^2$（または $\#E(\mathbb{F}_q) = (p-1)^2$）を満足する超特異楕円曲線 $E/\mathbb{F}_q$ を選択する．次に，$\langle P_A, Q_A \rangle = E[\ell_A^{e_A}]$ を満足する $P_A, Q_A \in E(\mathbb{F}_q)$ と $\langle P_B, Q_B \rangle = E[\ell_B^{e_B}]$ を満足する $P_B, Q_B \in E(\mathbb{F}_q)$ を選択する．そして，$p, \ell_A, \ell_B, e_A, e_B, E, P_A, Q_A, P_B, Q_B$ を公開パラメータとする．

3.2 鍵生成

a） Alice

Alice は秘密鍵 $s_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ を選択し，核が $K_A = \langle P_A + [s_A]Q_A \rangle$（注2）である $\ell_A^{e_A}$-同種写像 ϕ_A: $E \to E_A \cong E/K_A$ とその像 E_A を計算する．次に，

（注2）：効率を考慮し，核 K_A の定義は文献 [10] に従っている．

$\phi_A(P_B), \phi_A(Q_B) \in E_A(\mathbb{F}_q)$ を計算し，$E_A, \phi_A(P_B), \phi_A(Q_B)$ を Bob に送る．$\ell_A^{e_A}$-同種写像は Vélu の公式による ℓ_A-同種写像の計算を繰り返し適用することで効率的に計算される．$\ell_A^{e_A}$-同種写像計算の詳細については文献 [9, 4.2.2] を参照されたい．

b） Bob

Alice と同様に，Bob は選択した秘密鍵 $s_B \in \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$ に対し，核が $K_B = \langle P_B + [s_B]Q_B \rangle$ である $\ell_B^{e_B}$-同種写像 $\phi_B\colon E \to E_B \cong E/K_B$ と E_B を計算する．次に，$\phi_B(P_A), \phi_B(Q_A) \in E_B(\mathbb{F}_q)$ を計算し，$E_B, \phi_B(P_A), \phi_B(Q_A)$ を Alice に送る．

3.3 鍵 共 有

a） Alice

Bob から $E_B, \phi_B(P_A), \phi_B(Q_A)$ を受け取った Alice は，核が $K'_A = \langle \phi_B(P_A) + [s_A]\phi_B(Q_A) \rangle$ である $\ell_B^{e_B}$-同種写像 $\phi'_A\colon E_B \to E_{BA} \cong E_B/K'_A$ の像 E_{BA} を計算する．そして，E_{BA} の j 不変量 $j(E_{BA})$ を Bob との共有鍵とする．

b） Bob

Bob は核が $K'_B = \langle \phi_A(P_B) + [s_B]\phi_A(Q_B) \rangle$ である $\ell_A^{e_A}$-同種写像 $\phi'_B\colon E_A \to E_{AB} \cong E_A/K'_B$ の像 E_{AB} を計算し，j 不変量 $j(E_{AB})$ を Alice との共有鍵とする．

3.4 効率的なパラメータ

効率的な SIDH を得るためには，$\ell_A^{e_A} \approx \ell_B^{e_B}$ かつ $p \approx \ell_A^{e_A}\ell_B^{e_B}$ を満足する必要がある．そこで，パラメータの効率を表す指標として，$\rho = p/\min(\ell_A^{e_A}, \ell_B^{e_B})^2$ を考える．指標 ρ は $\rho > 1$ を満足し，$\rho = 1$ は $\ell_A^{e_A} = \ell_B^{e_B}$ かつ $p = \ell_A^{e_A}\ell_B^{e_B}$ に対応する．したがって，ρ が 1 に近いほど効率的な実装が可能であると考えられる．実際には CPU のワード長に適した構成を採用することなどで効率が変化するが，実装効率を一般的に議論するための指標としてこの ρ は妥当であると考えられる．

以下では，SIKE [11] で規定された曲線パラメータと $\ell_A = 2, \ell_B = 3$ の場合に対する Jao と De Feo の SIDH に利用可能な効率的な曲線パラメータの例を示す．

3.4.1 SIKE のパラメータ

Jao 等 [11] は NIST の耐量子暗号コンペティションに SIDH を応用した鍵カプセル化方式 “SIKE” を提案している．SIKE では $\#E(\mathbb{F}_q) = (p+1)^2$ を満足する曲線が利用され，$\ell_A = 2, \ell_B = 3, p = \ell_A^{e_A}\ell_B^{e_B} - 1$ とパラメータ設定されている．SIKE で規定されているパラメータを表 1 に示す．表 1 の第 1 行に `SIKEp503`，第 2 行に `SIKEp751`，第 3 行に `SIKEp964` のパラメータを示す．表 1 に現れる $\sqrt{\min(\ell_A^{e_A}, \ell_B^{e_B})}$ は SIDH の古典アルゴリズムによる解読に必要な計算量を表す．この値を 2/3 乗することで量子アルゴリズムによる計算量のビット長が得られる．

表 1 SIKE で規定された曲線パラメータ [11, Table 5.1]
Table 1 The curve parameters specified in [11, Table 5.1].

e_A	e_B	$\lceil \log_2 p \rceil$	$\sqrt{\min(\ell_A^{e_A}, \ell_B^{e_B})}$	ρ
250	159	503	$1.00 \cdot 2^{125}$	4.0
372	239	751	$1.00 \cdot 2^{186}$	111.9
486	301	964	$1.45 \cdot 2^{238}$	486.5

表 2 $\#E(\mathbb{F}_q) = (p+1)^2$ の場合の SIDH の効率的なパラメータ例
Table 2 Efficient parameters of SIDH for $\#E(\mathbb{F}_q) = (p+1)^2$.

e_A	e_B	f	$\lceil \log_2 p \rceil$	$\sqrt{\min(\ell_A^{e_A}, \ell_B^{e_B})}$	ρ
194	121	1	386	$1.85 \cdot 2^{95}$	4.7
193	122	5	389	$1.41 \cdot 2^{96}$	6.4
216	137	1	434	$1.00 \cdot 2^{108}$	2.2
227	143	5	456	$1.25 \cdot 2^{113}$	6.4
250	159	1	503	$1.00 \cdot 2^{125}$	4.0
273	172	1	546	$1.24 \cdot 2^{136}$	1.3
305	192	1	610	$1.11 \cdot 2^{152}$	1.6
445	279	1	888	$1.07 \cdot 2^{221}$	6.9
451	284	1	902	$1.05 \cdot 2^{225}$	1.8
464	293	1	929	$1.00 \cdot 2^{232}$	1.3
517	327	1	1036	$1.41 \cdot 2^{258}$	2.4
536	339	1	1074	$1.00 \cdot 2^{268}$	2.5

表 1 から，SIKE では ρ が比較的大きな曲線が選択されていることが分かる．これは，求められる安全性指標（攻撃耐性）（128bit, 192bit, 256bit）に合致したパラメータで ρ が小さな値のものがとれなかったためであると考えられるが，個別パラメータに対して実装効率を詳細に検討し，実際に高速実装が可能なパラメータを選択した結果，ρ が比較的大きくなってしまったものと思われる．これらは利用可能な曲線の選択肢が少ないことが一因である．

3.4.2 効率的なパラメータの具体例

ここでは，$\ell_A = 2, \ell_B = 3$ の場合に対して，Jao と De Feo の SIDH に利用可能な効率的なパラメータを示す．$2^{80} \le \sqrt{\min(\ell_A^{e_A}, \ell_B^{e_B})} < 2^{300}$ を満足するパラメータ，すなわち古典アルゴリズムに対して 80bit 安全性から 300bit 安全性をもつパラメータの中で効率指標 ρ が $\rho < 8.0$ を満足するものを全て示す．

表 2 に $\#E(\mathbb{F}_q) = (p+1)^2$ の場合，表 3 に $\#E(\mathbb{F}_q) = (p-1)^2$ の場合の曲線パラメータを示

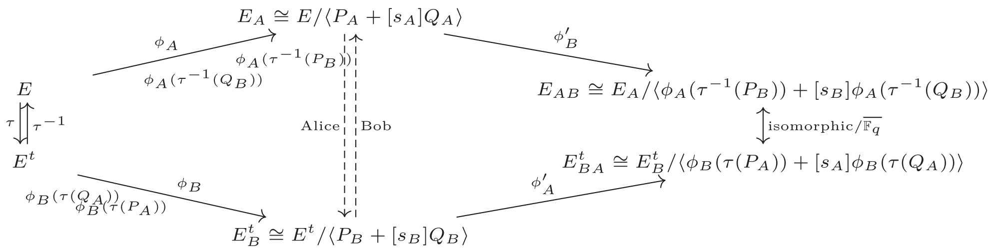

図 1　提案構成概要
Fig. 1　Overview of the Proposed Variant of SIDH.

表 3　$\#E(\mathbb{F}_q) = (p-1)^2$ の場合の SIDH の効率的なパラメータ例
Table 3　Efficient parameters of SIDH for $\#E(\mathbb{F}_q) = (p-1)^2$.

e_A	e_B	f	$\lceil \log_2 p \rceil$	$\sqrt{\min(\ell_A^{e_A}, \ell_B^{e_B})}$	ρ
160	101	5	323	$1.00 \cdot 2^{80}$	5.3
166	105	1	333	$1.00 \cdot 2^{83}$	1.3
188	119	5	379	$1.00 \cdot 2^{94}$	7.6
260	164	7	523	$1.95 \cdot 2^{129}$	7.3
265	168	1	532	$1.41 \cdot 2^{132}$	2.4
268	168	1	535	$1.10 \cdot 2^{133}$	3.3
336	211	1	671	$1.16 \cdot 2^{167}$	3.0
372	236	1	747	$1.00 \cdot 2^{186}$	4.1
374	236	5	751	$1.00 \cdot 2^{187}$	5.2

す．表 2 において $p = f\ell_A^{e_A}\ell_B^{e_B} - 1$ であり，表 3 において $p = f\ell_A^{e_A}\ell_B^{e_B} + 1$ である．ここで，f は正整数である．これらの曲線の具体的な生成については，例えば [19] を参照されたい．

SIDH に利用可能な超特異楕円曲線は $E[\ell_A^{e_A}] \subset E(\mathbb{F}_q)$ かつ $E[\ell_B^{e_B}] \subset E(\mathbb{F}_q)$ を満足する必要がある．したがって，$\ell_A^{e_A}\ell_B^{e_B} \mid p+1$ または $\ell_A^{e_A}\ell_B^{e_B} \mid p-1$ を満足する素数 p が必要となる．表 2, 3 から SIDH に利用可能なパラメータが限定的であることが分かる．

4.　2 次ツイストを利用した SIDH

3. で見たように，SIDH に利用可能な効率的な曲線は限定的である．しかし，実用上はできるだけ多くの曲線を利用できることが望ましい．本章では，SIDH に利用可能な曲線が少ないことを補うために，**3.** で紹介した Jao と De Feo の SIDH とは異なるパラメータを利用可能な SIDH の変形構成を提案する．この変形は Jao と De Feo の SIDH と同程度の効率を達成可能である．

本章で提案する SIDH の変形構成は超特異楕円曲線の 2 次ツイストを利用して構成される．提案構成は，「鍵生成」において超特異楕円曲線 E の $\ell_A^{e_A}$-ねじれ群と E の 2 次ツイスト曲線 E^t の $\ell_B^{e_B}$-ねじれ群を利用する．また，「鍵共有」においては，鍵生成において得られた，E の $\ell_A^{e_A}$-同種写像の像である超特異楕円曲線の $\mathbb{F}_{q^2}$-有理点からなる $\ell_B^{e_B}$-ねじれ群と，E^t の $\ell_B^{e_B}$-同種写像の像である超特異楕円曲線の $\mathbb{F}_{q^2}$-有理点からなる $\ell_A^{e_A}$-ねじれ群を利用する(注3)．これらの条件により，プロトコルに利用可能な素数 p の必要条件が $\ell_A^{e_A} \mid p+1$ かつ $\ell_B^{e_B} \mid p-1$ または $\ell_A^{e_A} \mid p-1$ かつ $\ell_B^{e_B} \mid p+1$ となり，通常の SIDH とは異なる p を利用可能となる．

本章では，提案構成の概要と正当性を示したのちに，その安全性について議論する．

4.1　提案構成の概要

以下では，Alice と Bob が提案構成によって鍵共有を行う手順を「初期設定」，「鍵生成」，「鍵共有」のそれぞれについて示す．また，図 1 に提案構成の概要をまとめる．図 1 の左半分は「鍵生成」，右半分は「鍵共有」に対応している．

4.1.1　初 期 設 定

ℓ_A, ℓ_B を互いに異なる小さな素数とし，p を ℓ_A, ℓ_B と異なる 5 以上の素数とする．e_A, e_B をそれぞれ $\ell_A^{e_A} \mid p+1$, $\ell_B^{e_B} \mid p-1$（または $\ell_A^{e_A} \mid p-1$, $\ell_B^{e_B} \mid p+1$）を満足する非負整数とする．

まず，$\#E(\mathbb{F}_q) = (p+1)^2$（または $\#E(\mathbb{F}_q) = (p-1)^2$）を満足し，式 (1) で与えられる超特異楕円曲線 $E/\mathbb{F}_q$ を選択する．また，$E^t/\mathbb{F}_q$ を式 (2) で与えられる $E/\mathbb{F}_q$ の 2 次ツイストとする．

次に，$\langle P_A, Q_A \rangle = E[\ell_A^{e_A}]$ を満足する P_A, $Q_A \in E(\mathbb{F}_q)$ と $\langle P_B, Q_B \rangle = E^t[\ell_B^{e_B}]$ を満足する P_B, $Q_B \in E^t(\mathbb{F}_q)$ を選択する．

そして，式 (3) で定義された τ と τ^{-1} を用いて，$\tau(P_A)$，$\tau(Q_A) \in E^t(\mathbb{F}_{q^2})$，$\tau^{-1}(P_B)$，$\tau^{-1}(Q_B) \in$

（注3）：鍵生成で利用するねじれ群は $\mathbb{F}_{q^2}$ 有理点群の部分群であるが $\mathbb{F}_q$ 有理点群の部分群ではないことに注意されたい．

$E(\mathbb{F}_{q^2})$ を計算し，p, ℓ_A, ℓ_B, e_A, e_B, E, E^t, P_A, Q_A, P_B, Q_B, $\tau(P_A)$, $\tau(Q_A)$, $\tau^{-1}(P_B)$, $\tau^{-1}(Q_B)$ を公開パラメータとする．

4.1.2　鍵　生　成

a）Alice

Alice は秘密鍵 $s_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ を選択し，核が $K_A = \langle P_A + [s_A]Q_A\rangle$ である $\ell_A^{e_A}$-同種写像 ϕ_A: $E \to E_A \cong E/K_A$ とその像 E_A を計算する．

次に，$\phi_A(\tau^{-1}(P_B)), \phi_A(\tau^{-1}(Q_B)) \in E_A(\mathbb{F}_{q^2})$ を計算し，$E_A, \phi_A(\tau^{-1}(P_B)), \phi_A(\tau^{-1}(Q_B))$ を Bob に送る．

b）Bob

Bob は秘密鍵 $s_B \in \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$ を選択し，核が $K_B = \langle P_B + [s_B]Q_B\rangle$ である $\ell_B^{e_B}$-同種写像 ϕ_B: $E^t \to E_B^t \cong E^t/K_B$ とその像 E_B^t を計算する．

次に，$\phi_B(\tau(P_A)), \phi_B(\tau(Q_A)) \in E_B^t(\mathbb{F}_{q^2})$ を計算し，$E_B^t, \phi_B(\tau(P_A)), \phi_B(\tau(Q_A))$ を Alice に送る．

4.1.3　鍵　共　有

a）Alice

Alice は核が $K_A' = \langle \phi_B(\tau(P_A)) + [s_A]\phi_B(\tau(Q_A))\rangle$ である $\ell_B^{e_B}$-同種写像 ϕ_A': $E_B^t \to E_{BA}^t \cong E_B^t/K_A'$ の像 E_{BA}^t を計算し，E_{BA}^t の j 不変量 $j(E_{BA}^t) \in \mathbb{F}_q$ を Bob との共有鍵とする．

b）Bob

Bob は核が $K_B' = \langle \phi_A(\tau^{-1}(P_B)) + [s_B]\phi_A(\tau^{-1}(Q_B))\rangle$ である $\ell_A^{e_A}$-同種写像 ϕ_B': $E_A \to E_{AB} \cong E_A/K_B'$ の像 E_{AB} を計算し，E_{AB} の j 不変量 $j(E_{AB}) \in \mathbb{F}_q$ を Alice との共有鍵とする．

4.2　正当性と安全性

Alice が得た E_{BA}^t は

$$\begin{aligned}
E_{BA}^t &= \phi_A'(\phi_B(E^t)) \\
&\cong \phi_A'(E^t/\langle P_B + [s_B]Q_B\rangle) \\
&\cong (E^t/\langle P_B + [s_B]Q_B\rangle)/ \\
&\quad \langle \phi_B(\tau(P_A)) + [s_A]\phi_B(\tau(Q_A))\rangle \\
&\cong (E^t/\langle P_B + [s_B]Q_B\rangle)/ \\
&\quad \langle \phi_B(\tau(P_A + [s_A]Q_A))\rangle \\
&\cong E^t/\langle \tau(P_A + [s_A]Q_A), P_B + [s_B]Q_B\rangle.
\end{aligned}$$

を満足し，Bob が得た E_{AB} は

$$\begin{aligned}
E_{AB} &= \phi_B'(\phi_A(E)) \\
&\cong \phi_B'(E/\langle P_A + [s_A]Q_A\rangle) \\
&\cong (E/\langle P_A + [s_A]Q_A\rangle)/ \\
&\quad \langle \phi_A(\tau^{-1}(P_B)) + [s_B]\phi_B(\tau^{-1}(Q_B))\rangle \\
&\cong (E/\langle P_A + [s_A]Q_A\rangle)/ \\
&\quad \langle \phi_A(\tau^{-1}(P_B + [s_B]dQ_B))\rangle \\
&\cong E/\langle P_A + [s_A]Q_A, \tau^{-1}(P_B + [s_B]Q_B)\rangle.
\end{aligned}$$

を満足する．したがって，

$$\begin{aligned}
E_{BA}^t &\cong E^t/\langle \tau(P_A + [s_A]Q_A), P_B + [s_B]Q_B\rangle. \\
&\cong E/\langle P_A + [s_A]Q_A, \tau^{-1}(P_B + [s_B]Q_B)\rangle. \\
&\cong E_{AB}
\end{aligned}$$

であり，$j(E_{BA}^t) = j(E_{AB})$ を得る．

SIDH に対する既知の攻撃は $\ell_A^{e_A}$-同種写像 ϕ_A または $\ell_B^{e_B}$-同種写像 ϕ_B のどちらか一方を，古典計算を用いて中間一致攻撃で求めるか，クロー探索問題として量子計算を用いて求めるものである [5], [8], [9], [11], [20], [21]．この攻撃は本章で提案した SIDH の変形構成に対しても同一計算量で適用可能である．すなわち，古典計算に対して $O(\min(\ell_A^{e_A}, \ell_B^{e_B})^{1/2})$，量子計算に対して $O(\min(\ell_A^{e_A}, \ell_B^{e_B})^{1/3})$ の計算量が必要となる．

文献 [5]～[7], [9]～[11], [22], [23] では，SIDH に対する上述の攻撃以外の攻撃の可能性についても議論されている．これらの議論の結果から，上述の手法以外の攻撃は適切な設定により無効化できることが分かる．これらの議論は提案構成に対しても適用可能であり，これまでの SIDH と同様に提案構成も上述の手法以外の攻撃は適切な設定により無効化できると考えられる．更に，提案構成を通常の SIDH を $\mathbb{F}_{q^2}$ 上で実現したものと見做すことが可能であり，この視点からも通常の SIDH と異なる攻撃手法を得ることは困難であると考えられる．

5.　Montgomery 曲線の利用

4. で提案したツイストを利用した SIDH の変形構成は超特異楕円曲線の $\mathbb{F}_{q^2}$-有理点 $\tau(P_A)$, $\tau(Q_A)$, $\tau^{-1}(P_B)$, $\tau^{-1}(Q_B)$ を必要とし，これらを用いた整数倍算や同種写像計算を行う必要がある．したがって，提案構成の直接的な実装は，通常の SIDH を $\mathbb{F}_{q^2}$ 上で実現したことと同等になり，通常の SIDH と比較して効率が劣る．

本章では **4.** で提案した変形構成に対して Montgomery 曲線を用いた効率化手法を適用する．SIDH は提案当初より Montgomery 曲線を用いた効率化手法 [5], [9], [10] を用いているが，提案構成を Montgomery 曲線上で構成すると，通常の SIDH に対し

て Montgomery 曲線を利用した場合と同様の効果が得られるだけではなく，$\mathbb{F}_{q^2}$ 上の演算が不要となり Montgomery 曲線上で構成した通常の SIDH と同程度の効率が実現可能となる．

以下では，通常の SIDH と同様に $\ell_A = 2$, $\ell_B = 3$ とし，SIDH の実装 [5], [9], [10] や SIKE [11] と同様に e_A を偶数として 2-同種写像の代わりに 4-同種写像を用いる．

本章では，はじめに提案構成に必要となる Montgomery 曲線とその同種写像を導入し，次に Montgomery 曲線を利用した提案構成を示す．そして，提案構成を Montgomery 曲線上で構成した場合の効率について議論する．

5.1 Montgomery 曲線と同種写像

ここでは，提案構成の Montgomery 曲線上の構成に必要となる Montgomery 曲線とその同種写像を導入する．

5.1.1 Montgomey 曲線

$\mathbb{F}_q$ 上の Montgomery 曲線 $E_{(a,b)}$ を

$$E_{(a,b)} : bY^2 = X^3 + aX^2 + X, \tag{5}$$

と定義する．ここで，$a \in \mathbb{F}_q, b \in \mathbb{F}_q^*$ である [24]．また，$E_{(a,b)}$ の 2 次ツイスト曲線を $E^t_{(a,b)}$ と書く．式 (2) より，$\mathbb{F}_q$ 上平方非剰余数 $\delta \in \mathbb{F}_q^*$ を用いて $E^t_{(a,b)} = E_{(a,\delta b)}$ と書ける．Montgomery 曲線 $E_{(a,b)}$ の j 不変量 $j(E_{(a,b)})$ は

$$j(E_{(a,b)}) = \frac{256(a^2-3)^3}{a^2-4} \tag{6}$$

で与えられる [10]．

Montgomery 曲線上では，X 座標 $X(P), X(Q)$ が異なる 2 点 $P, Q \in E_{(a,b)}(\overline{\mathbb{F}_q})$ に対して，$X(P), X(Q)$, $X(Q-P)$ から $X(P+Q)$ が計算できることが知られている [24]．また，$X(P), a$ から $X([2]P)$ を計算できる [24]．更に，これらの演算を用いて，SIDH に必要な $P, Q \in E_{(a,b)}(\overline{\mathbb{F}_q})$, $s \in \mathbb{Z}_{\geq 0}$ に対する $X(P+[s]Q)$ を，$X(P), X(Q), X(Q-P), a$ から効率的に計算することができる [9, Algorithm 1]．

5.1.2 Montgomery 曲線に対する同種写像

ここでは，文献 [5], [9], [10] に従って Montgomery 曲線に対する 4-同種写像と 3-同種写像を与える．

a） 4-同種写像

$X(R) \neq \pm 1$ である $R \in E_{(a,b)}[4]$ に対して，$\langle R \rangle$ を核とする 4-同種写像 $\phi_4 : E_{(a,b)} \to E_{(a',b')} \cong E_{(a,b)}/\langle R \rangle$ の像は

$$(a', b') = \left(4X(R)^4 - 2, -\frac{X(R)(X(R)^2+1)b}{2}\right) \tag{7}$$

で与えられ，$P \in E_{(a,b)}(\overline{\mathbb{F}_q}) \setminus \langle R \rangle$ に対して

$$X(\phi_4(P)) = -\frac{X(P)X(R)^2 + X(P) - 2X(R)}{(X(P)-X(R))^2} \cdot \frac{X(P)(X(P)X(R)-1)^2}{2X(P)X(R) - X(R)^2 - 1} \tag{8}$$

が成立する [5], [9], [11]．

また，$X(R) = 1$ である $R \in E_{(a,b)}[4]$ に対して，$\phi_4 : E_{(a,b)} \to E_{(a',b')} \cong E_{(a,b)}/\langle R \rangle$ の像は

$$(a', b') = \left(2\frac{a+6}{a-2}, \frac{b}{2-a}\right) \tag{9}$$

で与えられ，$P \in E_{(a,b)}(\overline{\mathbb{F}_q}) \setminus \langle R \rangle$ に対して

$$X(\phi_4(P)) = \frac{(X(P)+1)^2(X(P)^2 + aX(P) + 1)}{(2-a)X(P)(X(P)-1)^2} \tag{10}$$

が成立する [5], [9]．同様に，$X(R) = -1$ である $R \in E_{(a,b)}[4]$ に対して，$\phi_4 : E_{(a,b)} \to E_{(a',b')} \cong E_{(a,b)}/\langle R \rangle$ の像は

$$(a', b') = \left(2\frac{6-a}{2+a}, \frac{b}{2+a}\right) \tag{11}$$

で与えられ，$P \in E_{(a,b)}(\overline{\mathbb{F}_q}) \setminus \langle R \rangle$ に対して

$$X(\phi_4(P)) = \frac{(X(P)+1)^2(X(P)^2 + aX(P) + 1)}{(2-a)X(P)(X(P)-1)^2} \tag{12}$$

が成立する．

b） 3-同種写像

$R \in E_{(a,b)}[3]$ に対して，$\langle R \rangle$ を核とする 3-同種写像 $\phi_3 : E_{(a,b)} \to E_{(a',b')} \cong E_{(a,b)}/\langle R \rangle$ の像は

$$(a', b') = ((aX(R) - 6X(R)^2 + 6)X(R), bX(R)^2) \tag{13}$$

で与えられ，$P \in E_{(a,b)}(\overline{\mathbb{F}_q}) \setminus \langle R \rangle$ に対して

$$X(\phi_3(P)) = \frac{X(P)(X(P)X(R)-1)^2}{(X(P)-X(R))^2} \tag{14}$$

が成立する [5], [9], [11].

5. 2　提案構成の Montgomery 曲線上の構成

ここでは **4. 1** で提案した SIDH の変形構成を Montgomery 曲線上で構成する.

5. 2. 1　初 期 設 定

$\ell_A = 2, \ell_B = 3$ とし，**4. 1. 1** に従って，p, e_A, e_B, $E = E_{(a,b)}, E^t = E^t_{(a,b)}$ を構成する．また，$P_A, Q_A \in E(\mathbb{F}_q)$, $P_B, Q_B \in E^t(\mathbb{F}_q)$ を **4. 1. 1** に従って定めるとともに，$Q_A - P_A \in E(\mathbb{F}_q)$, $Q_B - P_B \in E^t(\mathbb{F}_q)$ を計算し，p, ℓ_A, ℓ_B, e_A, e_B, a, $X(P_A)$, $X(Q_A)$, $X(Q_A - P_A)$, $X(P_B)$, $X(Q_B)$, $X(Q_B - P_B) \in \mathbb{F}_q$ を公開パラメータとする．鍵生成，鍵共有計算では，曲線パラメータ b 及び E^t を定める δ を必要としないことに注意されたい.

5. 2. 2　鍵　生　成

a）Alice

Alice は秘密鍵 $s_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ と $X(P_A)$, $X(Q_A)$, $X(Q_A - P_A)$ から $R_A = P_A + [s_A]Q_A$ の X 座標 $X(R_A) \in \mathbb{F}_q$ を文献 [9] の Algorithm 1 を用いて計算する．次に，式 (8), (10), (12) で与えられた 4-同種写像計算を繰り返し適用し，核が $K_A = \langle R_A \rangle$ である $\ell_A^{e_A}$-同種写像

$$\begin{aligned}\phi_A : E_{(a,b)} &\to E_A = E_{(a_A,b_A)} \cong E_{(a,b)}/K_A \\ (x,y) &\mapsto (\phi_{AX}(x), y\phi_{AY}(x))\end{aligned} \qquad (15)$$

の X 座標を与える関数 ϕ_{AX} を計算し，同時に式 (7), (9), (11) から E_A の係数 a_A を得る．また，$X(\phi_A(\tau^{-1}(P_B))) = \phi_{AX}(X(P_B)) \in \mathbb{F}_q$, $X(\phi_A(\tau^{-1}(Q_B))) = \phi_{AX}(X(Q_B)) \in \mathbb{F}_q$ 及び $X(\phi_A(\tau^{-1}(Q_B)) - \phi_A(\tau^{-1}(P_B))) = \phi_{AX}(X(Q_B - P_B)) \in \mathbb{F}_q$ を計算し，a_A, $X(\phi_A(\tau^{-1}(P_B)))$, $X(\phi_A(\tau^{-1}(Q_B))), X(\phi_A(\tau^{-1}(Q_B)) - \phi_A(\tau^{-1}(P_B)))$ を Bob に送る.

b）Bob

Alice と同様に Bob は，式 (14) で与えられた 3-同種写像計算を繰り返すことで，核が $K_B = \langle P_B + [s_B]Q_B \rangle$ である $\ell_B^{e_B}$-同種写像

$$\begin{aligned}\phi_B : E^t_{(a,b)} &\to E_B = E^t_{(a_B,b_B)} \cong E^t_{(a,b)}/K_B \\ (x,y) &\mapsto (\phi_{BX}(x), y\phi_{BY}(x))\end{aligned} \qquad (16)$$

の X 座標を与える関数 ϕ_{BX} を計算し，同時に式 (13) から E^t_B の係数 a_B を得る．更に，$X(\phi_B(\tau(P_A))) = \phi_{BX}(X(P_A)) \in \mathbb{F}_q$, $X(\phi_B(\tau(Q_A))) = \phi_{BX}(X(Q_A)) \in \mathbb{F}_q$, $X(\phi_B(\tau(Q_A)) - \phi_B(\tau(P_A))) = \phi_{BX}(X(Q_A - P_A)) \in \mathbb{F}_q$ を計算し，これらと a_B を Alice に送る.

5. 2. 3　鍵　共　有

a）Alice

Alice は，Bob から受け取った a_B, $X(\phi_B(\tau(P_A)))$, $X(\phi_B(\tau(Q_A)))$, $X(\phi_B(\tau(Q_A)) - \phi_B(\tau(P_A)))$ を用いて，$X(\phi_B(\tau(P_A)) + [s_A]\phi_B(\tau(Q_A))) \in \mathbb{F}_q$ を計算する．そして，鍵生成と同様の計算で，核が $K'_A = \langle \phi_B(\tau(P_A)) + [s_A]\phi_B(\tau(Q_A)) \rangle$ である $\ell_A^{e_A}$-同種写像 ϕ'_A: $E^t_B \to E^t_{BA} \cong E^t_B/K'_A$ の像 E^t_{BA}（の係数 $a \in \mathbb{F}_q$）を計算し，式 (6) から得られる E^t_{BA} の j 不変量 $j(E^t_{BA})$ を Bob との共有鍵とする.

b）Bob

Alice と同様に，Bob は $X(\phi_A(\tau^{-1}(P_B)))$, $X(\phi_A(\tau^{-1}(Q_B))), X(\phi_A(\tau^{-1}(Q_B)) - \phi_A(\tau^{-1}(P_B)))$ から,核が $K'_B = \langle \phi_A(\tau^{-1}(P_B)) + [s_B]\phi_A(\tau^{-1}(Q_B)) \rangle$ である $\ell_B^{e_B}$-同種写像 ϕ'_B: $E_A \to E_{AB} \cong E_A/K'_B$ の像 E_{AB} を計算し，E_{AB} の j 不変量 $j(E_{AB})$ を Alice との共有鍵とする.

5. 3　提案構成の効率

以上で見たように，提案構成を Montgomery 曲線上で構成した場合には，$\mathbb{F}_{q^2}$ 上の演算を必要とせず，全ての計算を $\mathbb{F}_q$ 上で行うことができる．また，ツイスト同型写像 τ は X 座標に対して恒等写像として作用するため，τ, τ^{-1} の計算は不要となる．したがって，実際には通常の SIDH と同一の計算手順を踏むことで提案構成を実現可能であり，提案構成は通常の SIDH 同程度の効率を達成できると考えられる.

ただし，SIDH の既存の実装 [9]〜[11] では $\mathbb{F}_p$ 上で定義可能な $\#E(\mathbb{F}_q) = (p+1)^2$ の曲線を選択しデータ量削減を行っているが，提案構成では，位数が $(p+1)^2$ の曲線のみならず $(p-1)^2$ の曲線も利用するため，曲線を $\mathbb{F}_p$ 上で定義し $\mathbb{F}_p$ 上の曲線を利用した既知の手法を適用可能であるが，位数が $(p-1)^2$ の曲線に対しては既存のデータ削減手法を適用できないことに注意されたい.

6.　効率的なパラメータ例

本章では，前章までに提案した変形 SIDH 構成で利用可能なパラメータの具体例を示す．また，提案構成に利用可能な曲線パラメータに対応する Montgomery 曲線が存在することを示す.

表 4 に $\ell_A^{e_A} \mid p+1$, $\ell_B^{e_B} \mid p-1$ の場合，表 5 に $\ell_A^{e_A} \mid p-1$, $\ell_B^{e_B} \mid p+1$ の場合の効率的なパラメータ

表 4　$\ell_A^{e_A} \mid p+1$, $\ell_B^{e_B} \mid p-1$ の場合の効率的なパラメータ例
Table 4　Efficient parameters of the proposed variant for $\ell_A^{e_A} \mid p+1$, $\ell_B^{e_B} \mid p-1$.

e_A	e_B	c	$\lceil \log_2 p \rceil$	$\sqrt{\min(\ell_A^{e_A}, \ell_B^{e_B})}$	ρ
170	107	0	334	$1.74 \cdot 2^{84}$	.03
180	113	3	362	$1.46 \cdot 2^{89}$	7.4
206	128	0	409	$1.35 \cdot 2^{101}$	5.2
240	150	1	479	$1.83 \cdot 2^{118}$	6.2
242	152	3	485	$1.37 \cdot 2^{120}$	7.3
260	163	0	518	$1.13 \cdot 2^{129}$	2.2
346	220	0	694	$1.00 \cdot 2^{173}$	2.2
348	220	0	696	$1.00 \cdot 2^{174}$	0.5
366	231	4	735	$1.00 \cdot 2^{183}$	4.7
410	259	3	823	$1.00 \cdot 2^{205}$	5.2
434	274	2	870	$1.00 \cdot 2^{217}$	2.5
586	369	0	1168	$1.34 \cdot 2^{292}$	0.2

表 5　$\ell_A^{e_A} \mid p-1$, $\ell_B^{e_B} \mid p+1$ の場合の効率的なパラメータ例
Table 5　Efficient parameters of the proposed variant for $\ell_A^{e_A} \mid p-1$, $\ell_B^{e_B} \mid p+1$.

e_A	e_B	c	$\lceil \log_2 p \rceil$	$\sqrt{\min(\ell_A^{e_A}, \ell_B^{e_B})}$	ρ
168	108	0	338	$1.00 \cdot 2^{84}$	2.8
224	141	0	448	$1.67 \cdot 2^{111}$	1.3
228	144	1	457	$1.00 \cdot 2^{114}$	1.5
360	226	0	716	$1.07 \cdot 2^{179}$	0.5
390	246	0	780	$1.93 \cdot 2^{194}$	1.0
446	283	0	893	$1.00 \cdot 2^{223}$	1.3
458	293	0	919	$1.00 \cdot 2^{229}$	6.4
462	291	4	926	$1.53 \cdot 2^{230}$	7.2
488	308	2	978	$1.00 \cdot 2^{244}$	2.7

の例を示す．

表 4 に示したパラメータの導出手順を以下に示す：まず，中国式剰余定理を用いて $\ell_A^{e_A} \mid m+1$, $\ell_B^{e_B} \mid m-1$ を満足する $0 < m < \ell_A^{e_A}\ell_B^{e_B}$ を求めた．次に m に対して $p = m + c\ell_A^{e_A}\ell_B^{e_B}$ が素数となる最小の $c \in \mathbb{Z}_{\geq 0}$ を計算し p を定めた．表 5 のパラメータも同様の手順で導出した．

表中の効率指標 ρ は **3.4** と同じ定義である．また，**3.4** と同様に古典アルゴリズムに対して 80bit 安全性から 300bit 安全性をもつ位数，すなわち $2^{80} \leq \sqrt{\min(\ell_A^{e_A}, \ell_B^{e_B})} < 2^{300}$ を満足する位数の中で，効率指標 ρ が $\rho < 8.0$ を満足するものを示した．ただし，Montgomery 曲線の利用が前提となるため $2 \mid e_A$ を満足するパラメータのみを示した．

提案構成における素数 p の漸近的な大きさは通常の SIDH と同一の $p = O(\ell_A^{e_A}\ell_B^{e_B})$ であることが p の構成手順から分かる．したがって，効率的な曲線も通常の SIDH と同程度存在することが期待される．実際に表 4, 5 と表 2, 3 を比較すると，提案構成の利用により，通常の SIDH と同程度に効率的なパラメータをこれまでと同程度の数提供できると考えられる．一方で，提案構成では，通常の SIDH では達成できない，$\rho \leq 1$ となるパラメータが存在し，このようなパラメータでは提案構成は通常の SIDH より小さな有限体上で同一安全性を達成可能である．

表 4, 5 は効率的なパラメータを示しているが，そのパラメータに対応した Montgomery 曲線の存在を示す必要がある．一般に任意の楕円曲線と $\mathbb{F}_q$ 上同型な Montgomery 曲線が存在するとは限らないことが知られている [25]．しかし，以下に示す定理 1 から E が超特異かつ $E[2] \subset E(\mathbb{F}_q)$ の場合には任意の曲線と同型な Montgomery 曲線が存在する．

［定理 1］　$E[2] \subset E(\mathbb{F}_q)$ を満足する超特異楕円曲線 $E/\mathbb{F}_q$ と $\mathbb{F}_q$ 上同型な Montgomery 曲線が存在する．

証明　$E[2] \subset E(\mathbb{F}_q)$ より，$e_1 \neq e_2 \neq e_3 \neq e_1$ を満足する $e_1, e_2, e_3 \in \mathbb{F}_q$ によって E を

$$E : Y^2 = (X - e_1)(X - e_2)(X - e_3)$$

と書ける．

この E と $\overline{\mathbb{F}_q}$ 上同型な Legendre 曲線が

$$E_\lambda : Y^2 = X(X - 1)(X - \lambda)$$

で与えられる [26, Prop. 1.7]．ここで，$\lambda = \frac{e_3 - e_1}{e_2 - e_1} \in \mathbb{F}_q^*$ である．また，E_λ は超特異なので，$\sqrt{\lambda} \in \mathbb{F}_q^*$ である [27, Prop. 3.1]．そこで，$b = \sqrt{\lambda}$ と置いて，$(x, y) \mapsto (x/b, y/b^2)$ により E_λ を同型変換すると，E と $\overline{\mathbb{F}_q}$ 上同型な Montgomery 曲線

$$E_{(-(b^2+1)/b, b)} : bY^2 = X^3 - \frac{b^2+1}{b}X^2 + X$$

が得られる．この $E_{(-(b^2+1)/b, b)}$ が E と $\mathbb{F}_q$ 上非同型な場合は，$\mathbb{F}_q$ 上平方非剰余な $\delta \in \mathbb{F}_q^*$ により E と $\mathbb{F}_q$ 上同型な Montgomery 曲線 $E_{(-(b^2+1)/b, \delta b)}$ が得られる．　□

$E(\mathbb{F}_q) \cong (\mathbb{Z}/(p \pm 1)\mathbb{Z})^2$ より，提案構成の具体的な構成において $\ell_A = 2$（または，$\ell_B = 2$）とした場合には定理 1 の仮定を満足する．したがって，表 4, 5 に挙げた曲線パラメータをはじめとする効率的なパラメータに対応した Montgomery 曲線が存在し，その

パラメータを用いた提案構成を実現可能である．

7. 具体的な構成例

本章では提案構成の具体的な構成例を $\ell_A = 2$, $\ell_B = 3$ の場合に対して示す．以降では `0x` で始まる数値は 16 進記法の非負整数を表す．

7.1 初期設定

表 4 より $e_A = 260, e_B = 163$ と設定し，$\ell_A^{e_A} \mid p+1$, $\ell_B^{e_B} \mid p-1$ を満足する 518 ビット素数

$p =$ 0x39B393879221253930D9A0E4E30D498DCD1333D6737614AD2B88
CDA054BB866E2FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFF

を得る．

ここで，$q = p^2$, $\mathbb{F}_q = \mathbb{F}_p(\alpha)$, $\alpha = \sqrt{-1}$ とし，$\mathbb{F}_q$ 上で提案構成を実現する．$E = E_{(1,1)}/\mathbb{F}_q$，すなわち

$$E : Y^2 = X^3 + X.$$

とする．この E は条件 $\#E(\mathbb{F}_q) = (p+1)^2$ を満足する．また，E の 2 次ツイスト E^t を $E^t = E_{(\delta,1)}$ で与える．ここで，$\delta = \alpha + 10$ は $\mathbb{F}_q$ 上平方非剰余である．

以下で与える $P_A, Q_A \in E(\mathbb{F}_q)$ を $E[\ell_A^{e_A}]$ の基底として用いる：

$P_A =$ (0x851AB4D360DCB4939A87DA552A1C6A40CEBA27030D0AA1301
9B24D6736327A6D91776E0D0D1DBC0FE0AEC078F1CDCF6DB883B
11BC566587D6DBCA84DCD010932F, 0x2D0F06066C6EC1F91F9C3
373DCCBFD4820DD91C96DE21608410A581299AF0F2AFD5830BBA
F690FE5F090EFF4BCFB55A994F56F0892F8E6E0AD3DF473C89F8
B0CC7),

$Q_A =$ (0x3161E83A5C1359EFF731233F906B82E9C027916642A56A9A2
9EDA8C9E1585EC756E8891F2F2E243F01F513F870E323092477C
4EE43A99A782924357B232FEF6CD0, 0x2D0F06066C6EC1F91F9C
3373DCCBFD4820DD91C96DE21608410A581299AF0F2AFD5830BB
AF690FE5F090EFF4BCFB55A994F56F0892F8E6E0AD3DF473C89F
8B0CC7α).

また，P_A, Q_A から

$X(Q_A - P_A)$
$=$ 0xC114AFB8DE61A924A87AD83FC2F8E6794D6342A7C495860938118
EBA68461D150AC402BABBF85174D6963265BA9B3EE1D4B0E8ABE6E3
4C76D10A28EB001720571α

を計算する．更に，以下で与える $P_B, Q_B \in E^t(\mathbb{F}_q)$ を $E^t[\ell_B^{e_B}]$ の基底として用いる：

$P_B =$ (0x287355D8C93D2C1AC8B5F9C91CFB5F5D8A23EAFFF978F4E18
5AEC2721471ACC8778F0B7A9567793265CE7B6D18C58984820F3
6CF1AE69D9F1822283C662D6118D0α + 0x1A7B1B6F6992E61E0
DF0935BF303548EADC5127E1506B5CEEC3075BEE66E15BC26F15
1A0B0863E2517EAC5765854EC1C4F76715898C426DB36AF6D09B
2C96AC066, 0x481E63C49BF0D3216DAEE1F84C981359CBA54A04
E58A1F0A84511071C42768D2653B8B806D3FB918EC7C4158E4F9
B50B0BDCE753A3478EEC60124513E13FEC663α + 0x2DDF51D75
94CA8C822806CEF974FAC27CC706CAE35811B6D92AB873054533
418986DA3EABBE6F1AA86F80B8CEFE41D9FEFE008A042B56C5ED
3163452E6DD2A131D),

$Q_B =$ (0x17FBF897E8C5422829690B744E789F44D2619B7F1EA0035FA
CC9A95EE4398C8135AEC4B3B8DA53CAC92BBEBAEABF3D2D1F619
BFA74E0C6B2BD4DF83537CD34C054α + 0x28170E7843034AD69
2E9285FEE55B999DCEA25E28DE252DEF71E1C83014F95B9B73DD
1E7E4F02F9D4EA890DEA7BBCB5705DDE3966D1E50B63A4F5CB7C
01B0C1B83, 0x1B1021781A99D193D9DEA951BCE1895CAFF91ECB
62B6E523E5F0BC575CF0EF7C498E8342F6F0132BECE5A3F7EF03
D2A6FFACA7A58AC14292C9312E2D44AB0EE6BEα + 0x118FDC76
1FF26A9C09D8921D1ECA15832E9679B40CF9E677C4DF55640AD1
F3D79C7C5B29A9CC6A81D5E2D1F2DDF073A7CF8C8B02CC8E3F5D
2A73109023D8FC5437).

また，P_B, Q_B から

$X(Q_B - P_B)$
$=$ 0x8D4B223F2628CD66B989634414F0C08DC9214F8327D7234990B4F
630922B1B1D520F52DC8AD685E89889FC6C8F9477104062AFF3CB5A
BDDC995E36F072374C64Bα + 0x2D0476AD3629AFF5A3F5475391520
4292F7DF99B90F204C69446D204E445BFE0B8FD5D48BC3131A2D9E0
9AD66EB53BD5E9428B065391C58D7B9F8AB9E5FA8452F1

を計算する．

7.2 鍵生成

a) Alice

Alice は秘密鍵

$s_A =$ 0x9A1A79C74BAB6212DE568C315B05E9CD20633C36597950EB02
70530E4FE4D0612

をランダムに生成し，同種写像の核の生成元 $P_A + [s_A]Q_A$ の X 座標

$X(P_A + [s_A]Q_A)$
$=$ 0x1B1B01231417B0889F83DF237FD5894298B3E0FC0F1B4978CCBA9
DFD0376C7A0E117DDF02477FA94BA42EEE7F3D010574C08AA651245
1511D9F3DD6F8A8B6F4C46α + 0xC6203554ECF1A002B63007AA6E0
6233643DB4CA47F5A18E088970D68FB5F6859F2176252CEFEE4AE80
FFC60AE77EDE845A1685722EA3737D14D1854BE36DDA942.

を計算する．次に，$\ell_A^{e_A}$ 同種写像 ϕ_A の像 $E_A =$

$E_{(a_A,b_A)} \cong E/\langle P_A + [s_A]Q_A \rangle$ の係数

a_A = 0x263923E5E4F02B9F69E0308D147962F6743F500D0E3EAFDA80
C6A77937E3E44C2C4103723B28C3261B243B8879030C70CC5D8B
B0ABD8210D67AD7AB4D3496D29C8α + 0x1D8E00B4C9729B80D03
AFECCA61B37D763F9697A7F6614B1EB9570D1E22BB86DF77178
D7867B36EF5E5B1B29C9CB7406C31799271F058598C9E7E54A7
B523EC83A

と

$X(\phi_A(\tau^{-1}(P_B))) = \phi_{AX}(X(P_B))$
= 0x27AC53D45FC0771D273AD6BFE9BA672E8C0A6AFA110FE74C67DC9
72A9C8FE3CA98186E86EBCB6D64B60FABD5C30AFF6147B312037F4B
0DD670C580E17217A91465α + 0x37BF976FCF8332166F0EB4CF903
92557E44FCE6DFDD8D1C80DDFC78668049A11DBD64AF28B76199055
EA908E02AC41EEE614204F05DB87867A8A3160B81172EBFD,
$X(\phi_A(\tau^{-1}(Q_B))) = \phi_{AX}(X(Q_B))$
= 0x2D132B4BAAC411FE90A780E4050C1024681DEA11DD25B27571988
0779B8E8972D758AF76B17F5249B694BB5B4F0868FC4B5D02E642B6
6C03AED5CFDFD65E0553E3α + 0x3D216A8A05CAD37EE480AE426CB
BC1C3B59BE0BBFDC113712A439C9594B9C344006F5531B7BCDA1FF4
039A512C250E9E445A5A8DCA158B95FF9E04CC852E4CED5,
$X(\phi_A(\tau^{-1}(Q_B)) - \phi_A(\tau^{-1}(P_B))) = \phi_{AX}(X(Q_B - P_B))$
= AC1CD801384EC95DD92040412835BB782D3B1668BBCB86CC9558BE9
33EB82E99519A442A6CFF5D65516B9EFBD4DBDF5555A0E713635BEC
B574EC9256E12006541α + 3010BCA68369389850F44C99646655C7
FD06208BF8EFCC8A5D92B039B5C9A7D691A58EE3C8396245ED5ABB1
6BAA58B938D235906DA4C8E3933C815E140C43B59D5

を同種写像計算によって計算する．そしてこれらを Bob に送る．ここで，ϕ_{AX} は式 (15) で与えられた関数である．

b） Bob

同様に，ランダムに選択した秘密鍵

s_B = 0x47D794E6AC190BF99FFA08719F7C87BDB6CDDC7548F809D46E0
DE740D25CCF311

から，Bob は $\ell_B^{e_B}$ 同種写像 ϕ_B の像 $E_B^t = E_{(a_B,b_B)} \cong E^t/\langle P_B + [s_B]Q_B \rangle$ の係数

a_B = 0x2A41ABD50038C97E156248A24249C09A06BECFFCE218E327F
23787147C8854B000C640156B4CFBA31986B32B74DFBE3A30AE
8DC98AB83672742197645FC943C2BFα + 0x2E87F7DC3751B62
8CCFDFA8DCBE7B9BDABEE6E488DE2BADC08E96C49B2E68A4ED5
9BE3973C1DD3353D0E8A43B2E029B1986052A839A847323C678
441FAC234303D

と

$X(\phi_B(\tau(P_A))) = \phi_{BX}(X(P_A))$
= 0x19C46CC0C3C4C94DFA377271460DFFBF55F2F5E449D7F59A31473
D194B9A1A73AFB83F63C0127F150BDD899C3F3BBFCA97868443AF2E
CFA22EB48CF8E56A5954D5α + 0x2989EE2487431EBD66E95A86364
108185869A269C427BAA2AC64488DC3B5CBEBA8559FFE7C3665A9D2
0E7003D6CB420A2C957691753A8362295D2926623B12986A,
$X(\phi_B(\tau(Q_A))) = \phi_{BX}(X(Q_A))$
= 0x2BEBDBB6D334F2F7535A1973FE5D5AC9CC99BB924E4725E95691E
FF0DEC8BA542ACFE725D43D5C3F7E4E2D146984966E8AF22E3BA9C1
D88A3AB00A839C5BC11B9Fα + 0x2BD2092FE8E2ECD78E1CB255401
1D18170DF2F1674CC25D0127C618BC9FE6D28E71E4880FB77B720A0
CDB53B258FD70531350D71C38AD15F5BAF8F41A916D82066,
$X(\phi_B(\tau(Q_A)) - \phi_B(\tau(P_A))) = \phi_{BX}(X(Q_A - P_A))$
= 0x2B3CF6243FF0CD87D18C62DDA70BF2923974ABC6E1A4FEAA98025
377EE833E76A518D43A8A651125461A123B7AD2F1A5052CDB680EB7
A80CCD4404550F937C4DA5α + 0xF683EEF96DFD3A31D0C9B3D2B9D
EB6CAFF0F954241A2627084CCFDA4CCFC7E2486F1FBFFB191A6CBE3
5D09308A3FA2DBDA13F295F0D8AC16DEC2A045681FEDE99

を計算し，Alice に送る．ここで，ϕ_{BX} は式 (16) で与えられた関数である．

7.3 鍵 共 有

a） Alice

Alice は Bob から受け取った値から

$X(\phi_B(\tau(P_A)) + [s_A]\phi_B(\tau(Q_A)))$
= 0x32252714B43BCACD707DEABB8D9FD2C7668EC62349A4A82222F84
D0D64325A30251D12B8A4D9AFCD071046BB2BC843B4A18DDBA02929
D27990EEBD7D17A83857C2α + 0x100BC5CC3809D20E972C8A0FE8F
669BB536C3FB067DC087704236174A5825B313A7BD38F7C6D7E1B89
DC55A1192E5A2F8B7B633DE9BF928C0BE5E72E98E0848251

を計算し，$\ell_A^{e_A}$ 同種写像 ϕ'_A の像 $E_{BA}^t = E_{(a_{BA},b_{BA})} \cong E_B^t/\langle \phi_B(\tau(P_A)) + [s_A]\phi_B(\tau(Q_A)) \rangle$ の係数

a_{BA} = 0x141E16D3C5D6D98DE9AD01220579CDCF69AFB2D646A0B2EEE
705AC2538048E386B667A23CDBFE56E7A3F8CB5749BD6B612AB
5223C6C2FF5FE91A6EC03B29362308α + 0x22D8C48B40D1A5E
0DE2A692488D47CBDF301D3E888687CBF56EEF3553E1AE7C6B
5E99A7226A4835EA6478F7606E24BBC84B02777427AF8DFAAC
C0984016458EEE5.

を得る．そして，Bob との共有鍵である E_{BA}^t の j 不変量を式 (6) を用いて

$j(E_{BA}^t)$ = 0x114D98C5BBFFC4601C1F15419B6C23E32F44F8DB65B73C
10FCD5AF7E9F96C8CBF1D58C69D62CEB1CA890557387ADCC
A4E0713222BFB664182344F258172444571Eα + 0xA0E2AD8

$$\texttt{17785BD2AA7103A48B9D190F5DFB1194E3FC8BCE203DF7A}$$
$$\texttt{CAFF61EED448F79970D269C7C8388BFAAC2E5A69095CDA8}$$
$$\texttt{C347338699F713A4EEB496449ABC}.$$

を得る．

b） Bob

同様に Bob は

$$\begin{aligned}
&X(\phi_B(\tau(P_A)) + [s_B]\phi_B(\tau(Q_A))) \\
&= \texttt{0x2F4EC437DA2C460B00223BBA6DC472220638470B7545B4B1CC6B2} \\
&\quad \texttt{1D0083104C26DF8EAD6F03EC4675936890259B700042895EBE79200} \\
&\quad \texttt{8BCDDF12D6068333C7052B}\alpha + \texttt{0x2619419BEC29C6D8A782510E610} \\
&\quad \texttt{005EFFA0018648A291E4EBDB524E196247F0B2A7538E5E86EF4A2A3} \\
&\quad \texttt{FC90426B29536938C819997A8558FE7A56EA26E7F3FA0A98}
\end{aligned}$$

を計算し，$\ell_B^{e_B}$ 同種写像 ϕ'_B の像 $E_{AB} = E_{(a_{AB}, b_{AB})} \cong E_A/\langle \phi_A(\tau^{-1}(P_B)) + [s_B]\phi_A(\tau^{-1}(Q_B)) \rangle$ の係数 $a_{AB} = a_{BA}$ を得る．そして，E_{AB} の j 不変量 $j(E_{AB}) = j(E_{BA}^t)$ を Alice との共有鍵とする．

本章で利用したプログラムは SIDH Library [28] に添付された Magma プログラムを修正して作成した．計算には Xeon E5-2699 2.3GHz 上の Magma 2.23 [29] を使用した．Alice の鍵生成は 79.4ms，鍵共有は 72.5ms，Bob の鍵生成は 97.6ms，鍵共有は 81.8ms で計算された．

8. む す び

本論文では，2 次ツイストを利用した，SIDH の変形構成を提案した．提案構成は Montgomery 曲線を利用することで通常の SIDH と同程度の効率を実現可能である．また通常の SIDH とは異なる条件の曲線パラメータを利用可能なため，通常の SIDH とともに用いることでより多くの SIDH を提供可能とする．また，提案構成では通常の SIDH よりも小さな有限体上で同程度の安全性を達成できる場合があり，より効率的な SIDH を構成できる可能性がある．

位数が $(p-1)^2$ である曲線上のデータ削減手法と文献 [12] に示された高次同種写像の利用は今後の課題である．

謝辞 適切なご指摘を頂いた担当査読委員に感謝致します．

文 献

[1] J.-M. Couveignes, “Hard homogeneous spaces,” Cryptology ePrint Archive, Report 2006/291, 2006. https://eprint.iacr.org/2006/291

[2] A. Rostovtsev and A. Stolbunov, “Public-key cryptosystem based on isogenies,” Cryptology ePrint Archive, Report 2006/145, 2006. https://eprint.iacr.org/2006/145

[3] A. Stolbunov, “Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves,” Advances in Mathematics of Communications, vol.4, pp.215–235, 2010.

[4] A.M. Childs, D. Jao, and V. Soukharev, “Constructing elliptic curve isogenies in quantum subexponential time,” J. Mathematical Cryptology, vol.8, no.1, pp.1–29, 2014.

[5] D. Jao and L.D. Feo, “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies,” Proc. PQCrypto 2011, pp.19–34, 2011.

[6] S.D. Galbraith, C. Petit, B. Shani, and Y.B. Ti, “On the security of supersingular isogeny cryptosystems,” Advances in Cryptology – ASIACRYPT 2016, LNCS10031, pp.63–91, Springer, 2016.

[7] S.D. Galbraith and F. Vercauteren, “Computational problems in supersingular elliptic curve isogenies,” Quantum Information Processing, vol.17, no.10, p.265, 2018.

[8] G. Adj, D. Cervantes-Vázquez, J.-J. Chi-Domínguez, A. Menezes, and F. Rodríguez-Henríquez, “On the cost of computing isogenies between supersingular elliptic curves,” Selected Areas in Cryptography – SAC 2018, LNCS11349, pp.322–343, Springer, 2019.

[9] L.D. Feo, D. Jao, and J. Plût, “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies,” Mathematical Cryptology, vol.8, no.3, pp.209–247, 2014.

[10] C. Costello, P. Longa, and M. Naehrig, “Efficient algorithms for supersingular isogeny Diffie-Hellman,” Advances in Cryptology – CRYPTO 2016, Part I, LNCS59814, pp.572–601, Springer, 2016.

[11] D. Jao, R. Azrderakhsh, M. Campagna, C. Costello, L.D. Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, and D. Urbanik, “Supersingular isogeny key encapsulation,” Round 1 submission, NIST Post-Quantum Cryptography Standardization, 2017. https://sike.org/files/SIKE.zip

[12] C. Costello and H. Hisil, “A simple and compact algorithm for SIDH with arbitrary degree isogenies,” Advances in Cryptology – ASIACRYPT 2017, LNCS10625, pp.303–329, Springer, 2017.

[13] 松尾和人，“ツイストを利用した SIDH,” 2019 年暗号と情報セキュリティシンポジウム (SCIS2019)，3B3-1, 電子情報通信学会，2019.

[14] C. Costello, “B-SIDH: Supersingular isogeny Diffie-Hellman using twisted torsion,” Cryptology ePrint Archive, Report 2019/1145, 2019. https://eprint.iacr.org/2019/1145

[15] W.C. Waterhouse, “Abelian varieties over finite

fields,” Ann. Scient. É.N.S., 4th series, vol.2, no.4, pp.521–560, 1969.

[16] R. Schoof, “Nonsingular plane cubic curves over finite fields,” J. Combinatorial Theory, Series A, vol.46, no.2, pp.183–211, 1987.

[17] L.C. Washington, Elliptic curves: Number theory and cryptography, 2nd edition, Chapman & Hall/CRC, 2008.

[18] J. Vélu, “Isogénies entre courbes elliptiques,” C. R. Acad. Sci. Paris Sér. A-B, vol.273, pp.A238–A241, 1971.

[19] R. Bröker, “Constructing supersingular elliptic curves,” J. Comb. Number Theory, vol.1, no.3, pp.269–273, 2009.

[20] S. Jaques and J. Schanck, “Quantum cryptanalysis in the RAM model: Claw-finding attacks on SIKE,” Advances in Cryptology – CRYPTO 2019, LNCS11692, pp.32–61, Springer, 2019.

[21] C. Costello, P. Longa, M. Naehrig, J. Renes, and F. Virdia, “Improved classical cryptanalysis of the computational supersingular isogeny problem,” Cryptology ePrint Archive, Report 2019/298, 2019. https://eprint.iacr.org/2019/298

[22] A. Gélin and B. Wesolowski, “Loop-abort faults on supersingular isogeny cryptosystems,” Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26–28, 2017, pp.93–106, 2017.

[23] C. Petit, “Faster algorithms for isogeny problems using torsion point images,” Advances in Cryptology – ASIACRYPT 2017, Part II, LNCS10625, pp.330–353, Springer, 2017.

[24] P.L. Montgomery, “Speeding the Pollard and elliptic curve methods of factorization,” Math. Comp., vol.48, no.177, pp.243–264, 1987.

[25] K. Okeya, H. Kurumatani, and K. Sakurai, “Elliptic curves with the Montgomery-form and their cryptographic applications,” Public Key Cryptography, Third International Workshop on Practice and Theory in Public Key Cryptography, PKC 2000, LNCS1751, pp.238–257, Springer, 2000.

[26] J.H. Silverman, The Arithmetic of Elliptic Curves, 2nd edition, Graduate Texts in Mathematics, vol.106, Springer, 2009.

[27] R. Auer and J. Top, “Legendre elliptic curves over finite fields,” J. Number Theory, vol.95, pp.303–312, 2002.

[28] C. Costello, P. Longa, and M. Naehrig, “SIDH library,” 2016. http://research.microsoft.com/en-us/downloads/bd5fd4cd-61b6-458a-bd94-b1f406a3f33f/

[29] W. Bosma, J. Cannon, and C. Playoust, “The Magma algebra system. I. The user language,” J. Symbolic Comput., vol.24, no.3-4, pp.235–265, 1997.

（2019 年 10 月 26 日受付，2020 年 1 月 7 日再受付）

松尾　和人　（正員）

1986 中央大学理工学部卒．1988 同大大学院博前修了．1988 東洋通信機（株）入社．2001 中央大学大学院理工学研究科博後修了．博士（工学）．2002 中央大学研究開発機構機構助教授．2003 同機構教授．2004 情報セキュリティ大学院大学教授．2012 神奈川大学教授．