SCIS 2019 2019 Symposium on
Cryptography and Information Security
Shiga, Japan, Jan. 22 - 25, 2019
The Institute of Electronics,
Information and Communication Engineers

ツイストを利用したSIDH
SIDH over quadratic twists

松尾 和人 *

あらまし Jao と 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 の変形を提案する。提案プロトコルはこれまでの 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、提案プロトコルによってより豊富な SIDH を利用可能となる。また、提案プロトコルはこれまでの 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 はじめに

有限体上の通常の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 [Cou06, RS06, Sto10] は耐量子暗号として注目されていた。しかし、Childs と Jao [CJS14] によって通常の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め、この同種写像を用いた暗号は耐量子暗号としての優位性が認められなくなった。一方で、Jao と Feo [JF11] 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 [GPST16, GV18, ACVCD+18] や効率的な実装方式 [FJP14, CLN16] 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) [JAC+17] が NIST の耐量子暗号コンペティションに提案されている。SIDH では通常 2 次と 3 次の同種写像を繰り返し用いる。しかし、この構成で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。より多くの曲線を利用可能にするために、Costello ら [CH17] は高次同種写像の効率的な計算アルゴリズムを提案している。

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 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、2 次、3 次の同種写像を用いた場合においても、Jao と Feo の SIDH とは異なるパラメータの SIDH を構成可能となり、Jao と Feo の SIDH と併用することでより多くの SIDH を提供可能となる。さらに、提案プロトコルでは Jao と Feo 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。

本論文の構成を以下に示す。まず、2 節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 節で Jao と Feo [JF11] が提案した SIDH を概説する。また、Jao と 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 節で 2 次ツイストを利用した SIDH の変形を提案し、5 節で提案プロトコルの Montgomery 曲線を利用した効率的な構成を示す。6 節では提案プロトコルに利用可能な曲線パラメータの具体例を挙げるとともに、提案プロトコルを構成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。最後に 7 節でまとめる。

2 超特異楕円曲線と同種写像

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 monic 3 次多項式 $F(X) \in \mathbb{F}_q[X]$ と $b \in$

* 神奈川大学理学部情報科学科, 〒 259-1293 神奈川県平塚市土屋 2946, Dept. of Information Sciences, Faculty of Science, Kanagawa University, 2946, Tsuchiya, Hiratsuka-shi, Kanagawa 259-1293, Japan

$\mathbb{F}_q^*$ 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。$E(\mathbb{F}_q)$ の位数は $\#E(\mathbb{F}_q) = p^2 + 1$, $\#E(\mathbb{F}_q) = p^2 \pm p + 1$, $\#E(\mathbb{F}_q) = (p\pm1)^2$ のいずれかになることが知られている [Wat69, Theorem 4.1]。以下では $\#E(\mathbb{F}_q) = (p+1)^2$ または $\#E(\mathbb{F}_q) = (p-1)^2$ 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 [Sch87, 4.8]。

E の（非自明な）2 次ツイストを

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

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 $E(\mathbb{F}_q) \ncong E^t(\mathbb{F}_q)$ かつ $E(\mathbb{F}_{q^2}) \cong E^t(\mathbb{F}_{q^2})$ を満足する。したがって、$j(E) = j(E^t)$ 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 $E_1/\mathbb{F}_q$ から $E_2/\mathbb{F}_q$ への非定数準同型写像

$$\phi : E_1(\overline{\mathbb{F}_q}) \to E_2(\overline{\mathbb{F}_q})$$

を同種写像と呼び、ϕ が存在するとき、E_1 と E_2 は同種であるという。同種写像 ϕ は有理関数として式 (4) の形式で与えられる [Was08, 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 の次数を $\deg\phi = \max(\deg n_X, \deg d_X)$ と定義する。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。本論文では分離同種写像のみを考慮の対象とし、以下では「同種写像」は分離同種写像のことを指す。

$E_1(\mathbb{F}_q)$ の有限部分群 $K \subset E_1(\mathbb{F}_q)$ に対して K を核とする同種写像 $\phi : E_1(\overline{\mathbb{F}_q}) \to E_2(\overline{\mathbb{F}_q}) \cong E_1(\overline{\mathbb{F}_q})/K$ が存在する。ϕ は $\#K$-同種写像となる。与えられた $E_1/\mathbb{F}_q$ と $K \subset E_1(\mathbb{F}_q)$ に対して、K を核とする同種写像 $\phi : E_1(\overline{\mathbb{F}_q}) \to E_2(\overline{\mathbb{F}_q}) \cong E_1(\overline{\mathbb{F}_q})/K$ とその像 $E_2/\mathbb{F}_q$ を与える公式が Vélu [Vél71] によって示された。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実現されている。

3 Jao と Feo の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

2011 年に Jao と Feo [JF11] が超特異楕円曲線の同種写像を利用した耐量子 Diffie-Hellman 鍵共有プロトコル (SIDH) を提案し、2014 年に Feo, Jao と Plût [FJP14] 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。（通常は $\ell_A = 2$, $\ell_B = 3$ とする [JF11, FJP14, CLN16, JAC+17]。）p を ℓ_A, ℓ_B と異なる 5 以上の素数とし、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, ℓ_A, ℓ_B, ℓ_A, ℓ_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

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、$\phi_A(P_B)$, $\phi_A(Q_B) \in E_A(\mathbb{F}_q)$ 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。この同種写像計算の詳細については、文献 [FJP14, 4.2.2] を参照されたい。また、効率を考慮し、核 K_A の定義は文献 [CLN16] にしたがっていることに注意されたい。

Bob Bob は Alice と同様の計算を行い、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 ϕ_B: $E \to E_B \cong E/K_B$ 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

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 ϕ'_A: $E_B \to E_{BA} \cong E_B/K'_A$ と E_{BA} を計算する。そして、E_{BA} の j 不変量 $j(E_{BA})$ を共有鍵とする。

Bob Alice と同様に 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 ϕ'_B: $E_A \to E_{AB} \cong E_A/K'_B$ と E_{AB} を計算し、j 不変量 $j(E_{AB})$ を共有鍵とする。

3.4 プロトコルの正当性

Alice が得た E_{BA} は $E_{BA} \cong E/\langle P_A + [s_A]Q_A, P_B + [s_B]Q_B\rangle$ を満足し、Bob が得た E_{AB} は $E_{AB} \cong E/\langle P_A + [s_A]Q_A, P_B + [s_B]Q_B\rangle$ を満足する。したがって、Alice の得た E_{BA} と Bob の得た E_{AB} は同型であり、$j(E_{BA}) = j(E_{AB})$ となる。

3.5 効率的な実装が可能な曲線

ここでは、Jao と Feo の SIDH に利用可能な効率的な曲線の例を示す。SIDH が効率的であるためには、$\ell_A^{e_A} \approx \ell_B^{e_B}$ 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、曲線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。Jao と Feo の SIDH では、$\rho > 1$ であり、$\rho = 1$ は $\ell_A^{e_A} = \ell_B^{e_B}$ かつ $p = \ell_A^{e_A}\ell_B^{e_B}$ の場合に対応する。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 [JAC+17] で規定された曲線パラメータ及び一般的な設定である $\ell_A = 2$, $\ell_B = 3$ の場合に対する Jao と Feo の SIDH に利用可能な効率的な曲線パラメータを示す。

3.5.1 SIKE のパラメータ

Jao 等 [JAC+17] 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。表中の $\left\lceil \log_2 \sqrt{\min(\ell_A^{e_A}, \ell_B^{e_B})} \right\rceil$ は古典アルゴリズムによる SIDH の解読に必要な計算量のビット長を表す。この値を 2/3 倍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 [JAC+17] で規定された曲線パラメータ

e_A	e_B	$\lceil \log_2 p \rceil$	$\left\lceil \log_2 \sqrt{\min(\ell_A^{e_A}, \ell_B^{e_B})} \right\rceil$	ρ
250	159	503	126	4.0
372	239	751	187	111.9
486	301	964	240	486.5

表 1 から、SIKE では本論文で定義した 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。逆に、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であるとも思われる。いずれも利用可能な曲線の選択肢が少ないことが一因になっている。

3.5.2 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 Feo の SIDH に利用可能な効率的なパラメータを示す。古典アルゴリズムに対して 80bit 安全性から 300bit 安全性を持つ位数、すなわち $80 \le \left\lceil \log_2^{\frac{1}{2}} \min(\ell_A^{e_A}, \ell_B^{e_B}) \right\rceil \le 300$ を満足する位数の中で、効率性指標 ρ が $\rho < 8.0$ を満足するものを示す。表 2 に $\#E(\mathbb{F}_q) = (p+1)^2$ の場合の曲線パラメータを示す。表 2 において $p = c\ell_A^{e_A}\ell_B^{e_B} - 1$ である。ここで、c は正整数である。また、表 3 に $\#E(\mathbb{F}_q) = (p-1)^2$ の場合の曲線パラメータを示す。表 3 において $p = c\ell_A^{e_A}\ell_B^{e_B} + 1$ である。これまでに知られた SIDH の実装では Montgmery 曲線を利用した高速化のために $2 \mid e_A$ を満足するパラメータを利用しているが、ここでは $2 \nmid e_A$ の場合も含めて示した。これらの曲線の具体的な生成については、例えば [Brö09] を参照されたい。

表 2: $\#E(\mathbb{F}_q) = (p+1)^2$ の場合の SIDH の効率的な曲線パラメータ例

e_A	e_B	c	$\lceil \log_2 p \rceil$	$\left\lceil \log_2 \sqrt{\min(\ell_A^{e_A}, \ell_B^{e_B})} \right\rceil$	ρ
194	121	1	386	96	4.7
193	122	5	389	97	6.4
216	137	1	434	108	2.2
227	143	5	456	114	6.4
250	159	1	503	125	4.0
273	172	1	546	137	1.3
305	192	1	610	153	1.6
445	279	1	888	222	6.9
451	284	1	902	226	1.8
464	293	1	929	232	1.3
517	327	1	1036	259	2.4
536	339	1	1074	268	2.5

表 3: $\#E(\mathbb{F}_q) = (p-1)^2$ の場合の SIDH の効率的な曲線パラメータ例

e_A	e_B	c	$\lceil \log_2 p \rceil$	$\left\lceil \log_2 \sqrt{\min(\ell_A^{e_A}, \ell_B^{e_B})} \right\rceil$	ρ
160	101	5	323	80	5.3
166	105	1	333	83	1.3
188	119	5	379	94	7.6
260	164	7	523	130	7.3
265	168	1	532	133	2.4
268	168	1	535	134	3.3
336	211	1	671	168	3.0
372	236	1	747	186	4.1
374	236	5	751	187	5.2

表 2, 3 から SIDH に利用可能な曲線が限定的であることが分かる。SIKE のパラメータ程度の ρ 値を許せばよ

り多くの曲線を利用可能となるが、効率的な実装が可能な曲線を豊富に提供することは難しい。

4 2次ツイストを利用したSIDH

前節で見たように、JaoとFeoのSIDHに利用可能な効率的な曲線は限られている。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。本節では、SIDHに利用可能な曲線が少ないことを補うために、JaoとFeoのSIDHと同程度の効率を持つが異なる曲線を利用可能なSIDHの変形を提案する。この変形には2次ツイストを利用する。

JaoとFeoのSIDHで利用可能な超特異楕円曲線 E は、$E[\ell_A^{e_A}] \subset E(\mathbb{F}_q)$ かつ $E[\ell_B^{e_B}] \subset E(\mathbb{F}_q)$ であるため、$E[\ell_A^{e_A}\ell_B^{e_B}] \subset E(\mathbb{F}_q)$ 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 p が必要であるが、このような p は少ない。本節で提案するSIDHの変形プロトコルは、「鍵生成」において超特異楕円曲線 E の $\ell_A^{e_A}$-ねじれ群のみを利用し、$\ell_B^{e_B}$ に対しては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、超特異楕円曲線の $\mathbb{F}_{q^2}$-有理点からなる $\ell_A^{e_A}$-ねじれ群と、それとは異なる超特異楕円曲線の $\mathbb{F}_{q^2}$-有理点からなる $\ell_B^{e_B}$-ねじれ群を利用する。これにより、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、JaoとFeoのSIDHとは異なる p に対応する有限体 $\mathbb{F}_q$ 上の超特異楕円曲線を利用可能となる。したがって、提案プロトコルをJaoとFeoのSIDHと併用することでより多くのSIDHを提供できるようになる。さらに、提案プロトコルではこれまでのSIDHでは不可能であった $p < \ell_A^{e_A}\ell_B^{e_B} - 1$ を満足する超特異楕円曲線を利用できる場合があり、同一安全性を持つプロトコルをより小さな定義体上で構成できる可能性がある。

本節では、提案プロトコルの概要と正当性示し、5節で提案プロトコルのMontgomery曲線を利用した効率的な構成を示す。

4.1 提案プロトコルの概要

以下では、AliceとBobが提案プロトコル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に提案プロトコルの概要をまとめる。

4.1.1 初期設定

ℓ_A, ℓ_B を互いに異なる小さな素数とする。p を ℓ_A, ℓ_B と異なる5以上の素数とし、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、$\mathbb{F}_q$ 上の平方非剰余数 δ を選択し、$E^t/\mathbb{F}_q$ 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 p, ℓ_A, ℓ_B, e_A, e_B, E, E^t, P_A, Q_A, P_B, Q_B を公開パラメータとする。また、式(3)で定義された τ と τ^{-1} を用いて、$\tau(P_A), \tau(Q_A) \in E^t(\mathbb{F}_{q^2})$, $\tau^{-1}(P_B), \tau^{-1}(Q_B) \in E(\mathbb{F}_{q^2})$ を計算し公開パラメータとする。

4.1.2 鍵生成

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 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。

Bob Bobは Aliceと同様の計算を行い、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 ϕ_B: $E^t \to E_B^t \cong E^t/K_B$ と 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

Alice Bobから E_B^t, $\phi_B(\tau(P_A))$, $\phi_B(\tau(Q_A)$ を受け取った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: $E_B^t \to E_{BA}^t \cong E_B^t/K'_A$ と E_{BA}^t を計算し、E_{BA}^t の j 不変量 $j(E_{BA}^t) \in \mathbb{F}_q$ を共有鍵とする。

Bob Aliceと同様に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: $E_A \to E_{AB} \cong E_A/K'_B$ と E_{AB} を計算し、E_{AB} の j 不変量 $j(E_{AB}) \in \mathbb{F}_q$ を共有鍵とする。

4.2 提案プロトコルの正当性

Aliceが得た E_{BA}^t は

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

を満足する。また、Bobが得た E_{AB} は

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

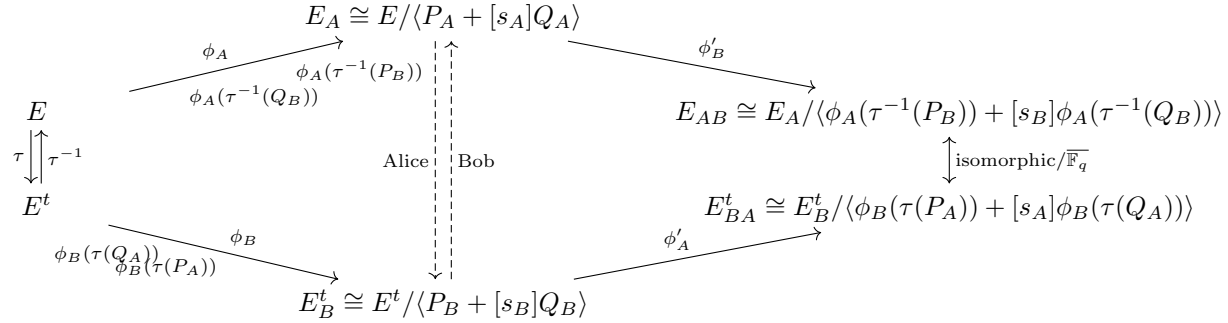

図 1: 提案プロトコル概要

を満足する。したがって、Alice の得た E^t_{BA} と Bob の得た E_{AB} は $\overline{\mathbb{F}_q}$ 上同型であり、$j(E^t_{BA}) = j(E_{AB})$ を得る。

5 Montgomery 曲線の利用

前節で提案した SIDH の変形プロトコルは超特異楕円曲線の $\mathbb{F}_{q^2}$-有理点 $\tau(P_A), \tau(Q_A), \tau^{-1}(P_B), \tau^{-1}(Q_B)$ を必要とする。また、これらを用いて $\mathbb{F}_{q^2}$-有理点の整数倍算や同種写像計算を行う必要がある。したがって、前節の構成の素直な実装は、Jao と Feo の SIDH を $\mathbb{F}_{q^2}$ 上で実現したことと同等になり、Jao と Feo の SIDH と比較して効率が劣ると考えられる。そこで、本節では前節で提案したツイストを利用した SIDH に対して Montgomery 曲線を用いた効率化手法を適用する。Jao と Feo の SIDH [JF11, FJP14, CLN16] は提案当初より Montgomery 曲線を用いた効率化手法を用いているが、前節で提案した変形プロトコルを Montgomery 曲線上で構成すると、Jao と Feo の SIDH に対して Montgomery 曲線を利用する効果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 Jao と Feo の SIDH と同程度の効率の SIDH を実現可能となる。

以下では、一般的な SIDH と同様に $\ell_A = 2$, $\ell_B = 3$ とする。また、$\ell_A = 2$ に対して、e_A が奇数のとき Montgomery 曲線の $\ell_A^{e_A}$-同種は Montgomery 曲線ではないので [JF11]、Jao と Feo の SIDH の実装 [JF11, FJP14, CLN16] や SIKE[JAC+17] 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。

本節では、はじめに提案プロトコルの構成に必要となる Montgmery 曲線とその同種写像を導入し、次に提案プロトコルの Montgmery 曲線上の構成を示す。そして、提案プロトコルを Montgmery 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、提案プロトコルの構成に必要となる Montgmery 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。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 $E^t_{(a,b)} = E_{(a,\delta b)}$ である。ここで、$\delta \in \mathbb{F}_q^*$ は式 (2) に現れた $\mathbb{F}_q$ 上平方非剰余数である。Montgomery 曲線の j 不変量は

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

で与えられる [CLN16]。

Montgomery 曲線上の加算は X 座標のみを用いて実現可能であることが知られている。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 [Mon87]。また、$X(P)$, a から $X([2]P)$ を計算できる [Mon87]。さらに、これらの結果から、$P, Q \in E_{(a,b)}(\overline{\mathbb{F}_q})$ に対して $X(P)$, $X(Q)$, $X(Q-P)$, a が与えられると、$s \in \mathbb{Z}_{\geq 0}$ に対して、SIDH に必要な $X(P+[s]Q)$ を効率的に計算することができる [FJP14, Algorithm 1]。

5.1.2 同種写像

ここでは、文献 [JF11, FJP14, CLN16] にしたがって Montgomery 曲線に対する 4-同種写像と 3-同種写像を与える。5.1.1 節で述べたように、Montgomery 曲線上の群演算を X 座標のみを用いて進めることができる。また、式 (4) より、ある点を同種写像で写した先の点の X 座標は元の点の X 座標のみから決定される。そこで、本節では同種写像の X 座標に対する作用のみを示す。

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 $\phi_4 : E_{(a,b)} \to E_{(a',b')}$ 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

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

が成立する [JF11, FJP14, JAC+17]。

また、$X(R)=1$ 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 $\phi_4 : E_{(a,b)} \to E_{(a',b')}$ 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 [JF11, FJP14]。

同様に、$X(R)=-1$ 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 $\phi_4 : E_{(a,b)} \to E_{(a',b')}$ 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。

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

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

が成立する [JF11, FJP14, JAC+17]。

5.2　提案プロトコルの Montgomery 曲線上の構成

ここでは 4.1 節で提案した 2 次ツイストを利用した SIDH の変形を Montgomery 曲線上で構成する。以下では「初期設定」「鍵生成」「鍵共有」のそれぞれの Montgomery 曲線上での構成の詳細を示す。

5.2.1　初期設定

4.1.1 節にしたがって構成した、p, ℓ_A, ℓ_B, e_A, e_B, $E = E_{(a,b)}$ の係数 $a \in \mathbb{F}_q$ 及び $E^t = E^t_{(a,b)}$ を規定する平方非剰余数 $\delta \in \mathbb{F}_q^*$ を公開パラメータとする。ただし、$2|e_A$ とする。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 節にしたが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、$X(P_A)$, $X(Q_A)$, $X(Q_A - P_A)$, $X(P_B)$, $X(Q_B)$, $X(Q_B - P_B) \in \mathbb{F}_q$ を公開パラメータとする。

5.2.2　鍵生成

Alice　Alice は秘密鍵 $s_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ を定め、[FJP14, Algorithm 1] を用いて s_A, $X(P_A)$, $X(Q_A)$, $X(Q_A - P_A)$ から $R_A = P_A + [s_A]Q_A$ の X 座標 $X(R_A) \in \mathbb{F}_q$ を計算する。次に、5.1.2 節で与えられた 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 ϕ_A: $E \to E_A \cong E/K_A$ を計算する。式 (7), (9), (11) を繰り返し適用することで、$\mathbb{F}_q$ 上で定義された Montgomery 曲線 E_A（の係数 a）が得られる。ϕ_A の X 座標への作用は $X(R_A)$, a から、式 (8), (10), (12) を用いて計算可能である。また、$X(\phi_A(\tau^{-1}(P_B))) = X(\phi_A(P_B)) \in \mathbb{F}_q$, $X(\phi_A(\tau^{-1}(Q_B))) = X(\phi_A(Q_B)) \in \mathbb{F}_q$ 及び $X(\phi_A(\tau^{-1}(Q_B)) - \phi_A(\tau^{-1}(P_B))) = X(\phi_A(Q_B - P_B)) \in \mathbb{F}_q$ を計算し、E_A, $\phi_A(\tau^{-1}(P_B))$, $\phi_A(\tau^{-1}(Q_B))$, $X(\phi_A(\tau^{-1}(Q_B)) - \phi_A(\tau^{-1}(P_B)))$ を Bob に送る。

Bob　Alice と同様に Bob は、5.1.2 節の式 (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 ϕ_B: $E^t \to E^t_B \cong E^t/K_B$ を計算する。このとき、式 (13) より $\mathbb{F}_q$ 上で定義された Montgomery 曲線として E^t_B が得られる。さらに、$X(\phi_B(\tau(P_A))) = X(\phi_B(P_A)) \in \mathbb{F}_q$, $X(\phi_B(\tau(Q_A))) = X(\phi_B(Q_A)) \in \mathbb{F}_q$, $X(\phi_B(\tau(Q_A)) - \phi_B(\tau(P_A))) = X(\phi_B(Q_A - P_A)) \in \mathbb{F}_q$ を計算し、これらと E^t_B を Alice に送る。

5.2.3　鍵共有

Alice　Alice は s_A, $X(\phi_B(\tau(P_A)))$, $X(\phi_B(\tau(Q_A)))$, $X(\phi_B(\tau(Q_A)) - \phi_B(\tau(P_A)))$ から、$X(\phi_B(\tau(P_A)) + [s_A]\phi_B(\tau(Q_A))) \in \mathbb{F}_q$ を計算する。そして、5.1.2 節の 3-同種写像計算を繰り返し適用し、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: $E^t_B \to E^t_{BA} \cong E^t_B/K'_A$ の像 E^t_{BA}（の係数 $a \in \mathbb{F}_q$）を計算する。そして、E^t_{BA} の j 不変量 $j(E^t_{BA})$ を式 (6) にしたがって計算し共有鍵とする。

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 $\ell_A^{e_A}$-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 $j(E_{AB})$ を共有鍵とする。

5.3　提案プロトコルの効率

以上で見たように、提案プロトコルを Montogomery 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、すべての計算を $\mathbb{F}_q$ 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、実際には τ, τ^{-1} の計算を必要としない。したがって、実際には Jao と Feo の SIDH と同じ計算手順を踏むことで提案プロトコルを実現可能であり、提案プロトコルは Jao と Feo の SIDH 同程度の効率を達成できると考えられる。ただし、Jao と Feo の SIDH の現実的な実装では、$\#E(\mathbb{F}_q) = (p+1)^2$ の曲線を選択し、$\mathbb{F}_p$ 上で定義された曲線を利用することでより一層の効率化やデータ量削減を行っている。一方で提案プロトコルでは、E または E^t のどちらか一方は位数が $(p+1)^2$ であり曲線を $\mathbb{F}_p$ 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、他方は位数が $(p-1)^2$ であり $\mathbb{F}_q$ 上の曲線となるため $\mathbb{F}_p$ 上の曲線を利用した既知の手法を適用できないことに注意が必要である。

6 提案プロトコルに利用可能な曲線

本節では前節までに提案した 2 次ツイストを利用した SIDH の変形に利用可能なパラメータの例を示す。また、提案プロトコル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 $\ell_A^{e_A} \mid p-1, \ell_B^{e_B} \mid p+1$ の場合の効率的な曲線のパラメータを示す。

表 4: $\ell_A^{e_A} \mid p+1, \ell_B^{e_B} \mid p-1$ の場合の提案プロトコルの効率的な曲線パラメータ例

e_A	e_B	c	$\lceil \log_2 p \rceil$	$\left\lceil \log_2 \sqrt{\min(\ell_A^{e_A}, \ell_B^{e_B})} \right\rceil$	ρ
170	107	0	334	85	.03
180	113	3	362	90	7.4
206	128	0	409	102	5.2
240	150	1	479	119	6.2
242	152	3	485	121	7.3
260	163	0	518	130	2.2
346	220	0	694	173	2.2
348	220	0	696	174	0.5
366	231	4	735	183	4.7
410	259	3	823	205	5.2
434	274	2	870	217	2.5
586	369	0	1168	293	0.2

表 5: $\ell_A^{e_A} \mid p-1, \ell_B^{e_B} \mid p+1$ の場合の提案プロトコルの効率的な曲線パラメータ例

e_A	e_B	c	$\lceil \log_2 p \rceil$	$\left\lceil \log_2 \sqrt{\min(\ell_A^{e_A}, \ell_B^{e_B})} \right\rceil$	ρ
168	108	0	338	84	2.8
228	144	1	457	114	1.5
360	226	0	716	180	0.5
390	246	0	780	195	1.0
446	283	0	893	223	1.3
458	293	0	919	229	6.4
462	291	4	926	231	7.2
488	308	2	978	244	2.7

表 4 に示したパラメータの導出は、$\ell_A^{e_A} \mid m+1, \ell_B^{e_B} \mid m-1$ を満足する $0 < m < \ell_A^{e_A}\ell_B^{e_B}$ を求め、次に m に対して $m + c\ell_A^{e_A}\ell_B^{e_B}$ が素数となる最小の $c \in \mathbb{Z}_{\leq 0}$ を定め、$p = m + c\ell_A^{e_A}\ell_B^{e_B}$ とした。表 5 に掲載したパラメータも同様の手法で導出した。

表中の ρ は 3.5 節と同じ定義である。また、3.5 節と同様に古典アルゴリズムに対して 80bit 安全性から 300bit 安全性を持つ位数、すなわち $80 \leq \left\lceil \log_2 \sqrt{\min(\ell_A^{e_A}, \ell_B^{e_B})} \right\rceil \leq 300$ 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。

提案プロトコルにおける素数 p と $\ell_A^{e_A}, \ell_B^{e_B}$ の関係は Jao と Feo の SIDH と同一の $p = O(\ell_A^{e_A}\ell_B^{e_B})$ であることが位数の構成手順から分かる。したがって、効率的な曲線も Jao と Feo 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、提案プロトコルの利用により、これまでの SIDH と異なるパラメータの効率的な曲線をこれまでと同程度提供できると考えられる。一方で、Jao と Feo の SIDH では $\rho > 1$ であるが、本論文の構成では $\rho < 1$ となることがあり、より効率的な構成ができる可能性がある。

表 4, 5 は効率的な位数の一覧であり、その位数の曲線の存在が課題として残る。特に提案構成では効率的な位数に対応する Montgomery 曲線の存在が必要であるが、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 [OKS00]。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 Mongomery 曲線が存在する。

Theorem 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。

Proof. $E[2] \subset E(\mathbb{F}_q)$ より、E を

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

と書ける。ここで、$e_1, e_2, e_3 \in \mathbb{F}_q$ かつ、$e_1 \neq e_2, e_1 \neq e_3, e_2 \neq e_3$ である。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 [Sil09, 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 [AT02, 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、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。この曲線が E と $\mathbb{F}_q$ 上非同型な 2 次ツイストの場合は、$\mathbb{F}_q$ 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。 □

定理 1 より、提案手法の具体的な構成において $\ell_A = 2$ とした場合には、定理の仮定を満足する。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曲線パラメータに対応した Montgomery 曲線が存在し、その曲線パラメータを用いた提案プロトコルを構成可能である。

7 まとめ

本論文では、2 次ツイストを利用した、SIDH の変形プロトコルを提案した。提案プロトコルは Montgomery 曲線を利用することで Jao と Feo の SIDH と同程度の効率を実現可能である。また Jao と Feo 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、より多くの SIDH の提供を可能とする。また、提案プロトコルでは Jao と Feo 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。Jao と Feo の SIDH と同様に位数が $(p-1)^2$ である曲線上の効率的な実装については今後の課題である。また、文献 [CH17] に示された高次同種写像の利用も今後の課題である。

参考文献

[ACVCD+18] Gora Adj, Daniel Cervantes-Vázquez, Jesús-Javier Chi-Domínguez, Alfred Menezes, and Francisco Rodríguez-Henríquez. On the cost of computing isogenies between supersingular elliptic curves. Cryptology ePrint Archive, Report 2018/313, 2018. `https://eprint.iacr.org/2018/313`.

[AT02] Roland Auer and Jaap Top. Legendre elliptic curves over finite fields. *J. of Number Theory*, Vol. 95, pp. 303–312, 2002.

[BL17] Joppe W. Bos and Arjen K. Lenstra, editors. *Topic in Computational Number Theory Inspired by Peter L. Montgomery*. Cambridge U. P., 2017.

[Brö09] Reinier Bröker. Constructing supersingular elliptic curves. *J. Comb. Number Theory*, Vol. 1, No. 3, pp. 269–273, 2009.

[CH17] Craig Costello and Huseyin Hisil. A simple and compact algorithm for SIDH with arbitrary degree isogenies. In *Advances in Cryptology – ASIACRYPT 2017*, LNCS10625, pp. 303–329. Springer, 2017.

[CJS14] Andrew M. Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *J. Mathematical Cryptology*, Vol. 8, No. 1, pp. 1–29, 2014.

[CLN16] Craig Costello, Patrick Longa, and Michael Naehrig. Efficient algorithms for supersingular isogeny Diffie-Hellman. In *Advances in Cryptology – CRYPTO 2016, Proceedings, Part I*, LNCS9814, pp. 572–601. Springer, 2016.

[Cou06] Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006. `https://eprint.iacr.org/2006/291`.

[Feo17] Luca De Feo. Mathematics of isogeny based cryptography. `http://defeo.lu/ema2017/poly.pdf`, 2017.

[FJP14] Luca De Feo, David Jao, and Jèrôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Mathmatical Cryptology*, Vol. 8, No. 3, pp. 209–247, 2014.

[GPST16] Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti. On the security of supersingular isogeny cryptosystems. In *Advances in Cryptology – ASIACRYPT 2016*, LNCS10031, pp. 63–91. Springer, 2016. `http://eprint.iacr.org/2016/859`.

[GV18] Steven D. Galbraith and Frederik Vercauteren. Computational problems in supersingular elliptic curve isogenies. *Quantum Information Processing*, Vol. 17, No. 10, p. 265, 2018.

[Hus86] Dale Husemöller. *Elliptic Curves*. GTM111. Springer, 1986.

[JAC+17] David Jao, Reza Azrderakhsh, Mathew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, and David Urbanik. Supersinglar isogeny key encapsulation. Round 1 submission, NIST Post-Quantum Cryptography Standrdization, 2017. `https://sike.org/files/SIKE.zip`.

[JF11] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *Proc. of PQCrypto 2011*, pp. 19–34, 2011.

[Mon87] Peter L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Math. Comp.*, Vol. 48, No. 177, pp. 243–264, 1987.

[OKS00] Katsuyuki Okeya, Hiroyuki Kurumatani, and Kouichi Sakurai. Elliptic curves with the montgomery-form and their cryptographic applications. In *Public Key Cryptography, Third International Workshop on Practice and Theory in Public Key Cryptography, PKC 2000*, LNCS1751, pp. 238–257. Springer, 2000.

[RS06] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Report 2006/145, 2006. `https://eprint.iacr.org/2006/145`.

[Sch87] René. Schoof. Nonsingular plane cubic curves over finite fields. *J. Combinatorial Theory*, Vol. A 46, pp. 183–211, 1987.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. GTM106. Springer, 2nd ed., 2009.

[Sto10] Anton 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.

[Vél71] Jean Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, Vol. 273, pp. A238–A241, 1971.

[Was08] Lawrence C. Washington. *Elliptic curves: number theory and cryptography*. Chapman & Hall/CRC, 2nd ed., 2008.

[Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Ann. scient. É.N.S.*, Vol. 4^o t. 2, pp. 521–560, 1969.