Bull. Korean Math. Soc. **46** (2009), No. 4, pp. 789–802
DOI 10.4134/BKMS.2009.46.4.789

AN ALGORITHM FOR COMPUTING A SEQUENCE OF RICHELOT ISOGENIES

Katsuyuki Takashima and Reo Yoshida

Abstract. We show that computation of a sequence of Richelot isogenies from specified supersingular Jacobians of genus-2 curves over $\mathbb{F}_p$ can be executed in $\mathbb{F}_{p^2}$ or $\mathbb{F}_{p^4}$. Based on this, we describe a practical algorithm for computing a Richelot isogeny sequence.

1. Introduction

Computing an isogeny between elliptic curves is used in some applications as a new basic cryptographic operation. One example of such an application was proposed in [5] in which a cryptographic hash function from expander graphs consists of computing an sequence of isogenies (see [6] as well). Moreover, there was an attempt to construct a new type of public key cryptosystem using such an operation (see [11]).

We proposed two simple algorithms for practically computing a sequence of 2-isogenies between supersingular elliptic curves [16]. These algorithms include several square root computations, then they might cause computation in a huge extension field. However, we [16] showed that, if the sequence starts at an appropriate elliptic curve (over $\mathbb{F}_{p^2}$), then all the computations of the sequence are performed in $\mathbb{F}_{p^2}$. This result implies that such computation is practical.

A Richelot isogeny is a natural generalization of 2-isogenies between elliptic curves to that in the genus-2 case (see [1, 2, 3, 12] etc). Then, we investigate and establish analogous results for a sequence of Richelot isogenies between supersingular Jacobian varieties of dimension 2.

Section 2 gives a summary of the results in the genus-1 case given in [16]. Section 3 explains the computation for a Richelot isogeny sequence. Section 4 gives a theoretical basis for the proposed algorithms. Section 5 proposes actually an algorithm for computing a sequence of Richelot isogenies.

Received December 15, 2008.
2000 *Mathematics Subject Classification.* 14Q05, 11Y16, 11T71, 14K02.
Key words and phrases. hyperelliptic curve, genus two, Richelot isogeny, isogeny graph, supersingular curve.

2. Previous result: Genus 1 case

Charles et al. [5] proposed an algorithm for computing a sequence of 2-isogenies between supersingular elliptic curves based on Vélu's formulas [14]. In [16], we described simple algorithms based on compact expressions of 2-isogenies, without some redundancy in the description in [5].

Let p be an odd prime > 3, $\mathbb{F}_p$ the finite field of order p, and $\overline{\mathbb{F}}_p$ an algebraic closure of $\mathbb{F}_p$. For $0 \le i \le n$, let $E_i/\overline{\mathbb{F}}_p$ be a supersingular elliptic curve given by the short Weierstrass normal form $Y^2 = f_i(X)$ with $\deg(f_i) = 3$. Let $(a_{i,0}, 0), (a_{i,1}, 0)$, and $(a_{i,2}, 0)$ be 2-torsion points on E_i. In [16], we considered the computation of the sequence of 2-isogenies ϕ_i associated to $(a_{i,0}, 0)$ without backtracking:

$$E_0 \xrightarrow{\phi_0} E_1 \xrightarrow{\phi_1} \cdots \xrightarrow{\phi_{n-2}} E_{n-1} \xrightarrow{\phi_{n-1}} E_n. \tag{1}$$

Here, we denote $(a_{i,1}, 0)$ as the 2-torsion point associated with the backtracking, i.e., the dual isogeny $\hat{\phi}_{i-1}$. Then, we obtained the following simple recurrence formulas between $(a_{i,0}, a_{i,1}, a_{i,2})$ and $(a_{i+1,0}, a_{i+1,1}, a_{i+1,2})$:

$$\begin{aligned} a_{i+1,1} &= -2a_{i,0} \quad \text{and} \\ a_{i+1,0}, a_{i+1,2} &= a_{i,0} \pm 2[(a_{i,0} - a_{i,1})(a_{i,0} - a_{i,2})]^{\frac{1}{2}}. \end{aligned} \tag{2}$$

Here, note that there is a square root term in the RHS of the second formula of (2).

Based on (2), we proposed two *simple* algorithms for a sequence (1). Moreover, we showed that when *appropriately* choosing a starting *supersingular* elliptic curve $E_0/\mathbb{F}_{p^2}$, all 2-torsions on E_i, i.e., $(a_{i,m}, 0)$, are defined in $\mathbb{F}_{p^2}$, and then *all* the computation of the proposed algorithms stays in $\mathbb{F}_{p^2}$.

3. Preliminaries

We give several basic facts and fix notations.

3.1. Hyperelliptic curves of genus 2 and their Jacobians

Let p be an odd prime > 5. Then, a hyperelliptic curve of genus 2 over $\overline{\mathbb{F}}_p$ is given by

$$C : Y^2 = f(X),$$

where $\deg(f(X)) = 5$ or 6 and $f(X)$ has no multiple zeros. Let the zeros of $f(X)$ be $(a_0, \ldots, a_4)$, or $(a_0, \ldots, a_5)$. Then, $P_m := (a_m, 0)$ for $0 \le m \le 4$ or 5 are called *Weierstrass points* (When $\deg(f) = 5$, the infinity point gives another Weierstrass point). Given a hyperelliptic curve C of genus 2, we can define a group variety J_C, the Jacobian. A point D on J_C is given by a divisor class of C of degree 0, which is a formal sum of points on C modulo linear equivalence. When $\deg(f(X)) = 5$, D is represented by a pair of polynomials, in other words, as a set,

$$J_C = J_C(\overline{\mathbb{F}}_p) = \{(u(X), v(X)) \in \overline{\mathbb{F}}_p[X]^2 \big| \ u(X) \mid v(X)^2 - f(X), u(X) : \text{monic}, \\ \deg(v(X)) < \deg(u(X)) \leq 2\},$$

where $\overline{\mathbb{F}}_p[X]$ is the polynomial ring whose coefficient field is $\overline{\mathbb{F}}_p$. When $\deg(f(X)) = 6$, a point in J_C is given by a pair $(u(X), v(X))$ s.t. $u(X) \mid v(X)^2 - f(X)$, $u(X)$: monic, and $\deg(v(X)) < \deg(u(X)) \leq 2$, and a (distance) parameter $m \in \mathbb{Z}$, where $0 \leq m \leq 2 - \deg(v(X))$. Such a representation is called Mumford representation. An addition of divisors naturally gives an algebraic addition law on J_C. For details, see [9, 10]. Jacobian J_C is called supersingular if it is isogenous (over $\overline{\mathbb{F}}_p$) to a product of two supersingular elliptic curves, and a curve C is called supersingular if J_C is supersingular.

3.2. Richelot isogeny

We explain an isogeny of a hyperelliptic curve of genus 2, called *Richelot isogeny* [1, 2, 3, 12] etc. First, we specify the notations hereafter.

Let $G_j(X) \in \overline{\mathbb{F}}_p[X]$ for $j = 0, 1, 2$ be 3 monic polynomials of $\deg(G_j) \leq 2$ such that $\prod_{j=0}^{2} G_j(X)$ is of degree 5 or 6 and squarefree. Then

$$C : Y^2 = f(X) = d \prod_{j=0}^{2} G_j(X), \tag{3}$$

where $d \in \overline{\mathbb{F}}_p^*$ is a curve of genus 2. By using coefficients $g_{j,k}$ of $G_j(X) = \sum_{k=0}^{2} g_{j,k} X^k$, let M be the matrix $(g_{j,k})_{0 \leq j,k \leq 2}$. Here, note that if $\deg(G_j) = 1$, then $g_{j,2} = 0$. If $\deg(G_j) = 2$, we denote the zeros of $G_j(X)$ by a_{2j} and a_{2j+1}, i.e., $G_j(X) = (X - a_{2j})(X - a_{2j+1})$. Hereafter, we consider permutations of $(a_0, \ldots, a_5)$ for the description of the Richelot isogeny. For that purpose, we use a special symbol "∞" to treat the case that $G_j(X)$ is linear, i.e., $G_j(X) = X - a$, where $a = a_{2j}$ or a_{2j+1}. Then, we consider that a and ∞ are the two zeros of $G_j(X)$, and treat permutations of 6 elements $(a_0, \ldots, a_5)$ including ∞.

Suppose that the determinant of $M = (g_{j,k})_{0 \leq j,k \leq 2}$ is non-zero. Hereafter, prime "$\prime$" means differentiation by the variable X. We then define the bracket product $[G_{j+1}(X), G_{j+2}(X)]$ and its transform to the monic one, $\tilde{G}_j(X)$, below.

$$[G_{j+1}(X), G_{j+2}(X)] := G'_{j+1}(X) G_{j+2}(X) - G'_{j+2}(X) G_{j+1}(X),$$
$$\tilde{G}_j(X) := c_j^{-1} [G_{j+1}(X), G_{j+2}(X)],$$

where c_j is the leading coefficient of $[G_{j+1}(X), G_{j+2}(X)]$. Here, and in similar places throughout this paper, we will take addition with respect to the index of G to mean addition modulo 3. Then, the degree of $\prod_{j=0}^{2} \tilde{G}_j(X)$ is 5 or 6 [12]. Let $\tilde{f}(X) := \tilde{d} \prod_{j=0}^{2} \tilde{G}_j(X)$, where $\tilde{d} := d \cdot c_0 c_1 c_2 \cdot \det(M)^{-1}$. Using $\tilde{f}(X)$, we then obtain a curve of genus 2

$$\tilde{C} : Y^2 = \tilde{f}(X) = \tilde{d} \prod_{j=0}^{2} \tilde{G}_j(X) \quad \text{with} \quad \tilde{d} := d \cdot c_0 c_1 c_2 \cdot \det(M)^{-1}. \tag{4}$$

The curve $\tilde{C}$ is called a *Richelot dual* of C. Here, we call the above correspondence *Richelot operator* $\mathcal{R}$ according to B. Smith [12].

$$\mathcal{R} : (G_0(X), G_1(X), G_2(X), d) \mapsto (\tilde{G}_0(X), \tilde{G}_1(X), \tilde{G}_2(X), \tilde{d}).$$

However, this $\mathcal{R}$ is slightly different from that in [12].

Associated with a Weierstrass point $P_0 = (a_0, 0)$, the *Richelot isogeny* is given by

$$\begin{gathered} \phi : J_C \to J_{\tilde{C}} \\ D = [(x, y) - P_0] \mapsto \phi(D) = [(z_1, t_1) - (z_2, -t_2)], \end{gathered} \tag{5}$$

where $[\cdot]$ means linear equivalence class, z_1 and z_2 are the zeros with respect to z of

$$U_x(z) = \sum_{k=0}^{2} U_{x,k} z^k := G_1(x)\tilde{G}_1(z) + G_2(x)\tilde{G}_2(z),$$

and t_ℓ satisfies

$$y t_\ell = \sum_{k=0}^{2} V_{x,k} z_\ell^k, \tag{6}$$

where $\sum_{k=0}^{2} V_{x,k} z_\ell^k := d G_1(x) \tilde{G}_1(z_\ell)(x - z_\ell)$ for $\ell = 1, 2$. We note that (z_1, t_1) and (z_2, t_2) are points on $\tilde{C}$. The kernel of ϕ is explicitly given by the Weierstrass points, and it is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. For details, see [1, 12].

3.3. A sequence of Richelot isogenies

Let C be given by (3). Richelot isogenies from J_C are determined by splitting $(G_0(X), G_1(X), G_2(X))$ of $f(X)$. This corresponds to a splitting of the zero-points of $f(X)$ into three pairs, i.e., $(a_0, a_1), (a_2, a_3)$, and (a_4, a_5). Therefore, the number of Richelot isogenies from C is $\binom{6}{2} \cdot \binom{4}{2}/3! = 15$. We consider computing a walk consisting of Richelot isogenies

$$J_0 \xrightarrow{\phi_0} J_1 \xrightarrow{\phi_1} \cdots \xrightarrow{\phi_{n-2}} J_{n-1} \xrightarrow{\phi_{n-1}} J_n \tag{7}$$

without backtracking, i.e., ϕ_{i+1} is not the dual of ϕ_i for $i = 0, \ldots, n-2$. Hence, at each step, there exist $14 = 15 - 1$ possible choices to go forward. In (7), J_i is the Jacobian of C_i, which is given below.

$$C_i/\overline{\mathbb{F}}_p : Y^2 = f_i(X) = d_i \prod_{j=0}^{2} G_{i,j}(X), \tag{8}$$

where

$$G_{i,j}(X) = \sum_{k=0}^{2} g_{i,j,k} X^k = \begin{cases} (X - a_{i,2j})(X - a_{i,2j+1}) & \text{if } \deg(G_{i,j}) = 2, \\ X - a_{i,2j} \text{ or } X - a_{i,2j+1} & \text{if } \deg(G_{i,j}) = 1, \end{cases}$$

where $d_i \neq 0$ and $\det(M_i) \neq 0$ for $M_i := (g_{i,j,k})_{0 \le j,k \le 2}$. For the Richelot dual $\tilde{C}_{i+1}$ (after applying ϕ_i to J_{C_i}), we use similar notation $\tilde{G}_{i+1,j}(X), \tilde{a}_{i+1,m}$, and $\tilde{d}_{i+1}$ for the corresponding ones, respectively.

Here, we note that, if $\det(M_i) = 0$, then J_{C_i} has an isogeny to a product of elliptic curves $E_1 \times E_2$ [12]. We do not consider such special cases in the presentation of sequence computation hereafter.

From the above, we have 14 possibilities to proceed to the next Jacobian at $i \ge 1$. When $i = 0$, we choose 14 possibilities from J_0 at the beginning. We then associate a walk data $\omega = b_0 b_1 \cdots b_{n-1} \in \mathcal{W} = \{0, \ldots, 13\}^n$ with a walk (7). Then, the correspondence is bijective as indicated below.

$$\mathcal{W} = \{0, \ldots, 13\}^n \longleftrightarrow \left\{ \begin{matrix} \text{a sequence (7) of Richelot isogenies } \phi_i \\ \text{starting from } J_0 \text{ without backtracking} \end{matrix} \right\},$$

where (7) starts from one of the candidate Jacobians chosen as above. The goal is to compute the C_n from C_0 and a walk data $\omega \in \mathcal{W} = \{0, \ldots, 13\}^n$.

For $i = 1, \ldots, n-1$, the i-th step in (7) for computing ϕ_i consists of the following 2 procedures

1: Permutation of the zero-points of $f_i(X)$,
2: Isogeny calculation by the Richelot operator, i.e.,

$$\tilde{G}_{i+1,j}(X) = c_{i,j}^{-1} [G_{i,j+1}(X), G_{i,j+2}(X)], \tag{9}$$

where $c_{i,j}$ is the leading coefficient of $[G_{i,j+1}(X), G_{i,j+2}(X)]$.

The flow of the computation is given below.

$$\begin{array}{cl}
\vdots & \\
\Downarrow & \text{Richelot op.} \\
\overbrace{\tilde{a}_{i,0}, \tilde{a}_{i,1}}^{\tilde{G}_{i,0}(X)}, \overbrace{\tilde{a}_{i,2}, \tilde{a}_{i,3}}^{\tilde{G}_{i,1}(X)}, \overbrace{\tilde{a}_{i,4}, \tilde{a}_{i,5}}^{\tilde{G}_{i,2}(X)} & \\
\Downarrow & \text{Perm.} \\
\overbrace{a_{i,0}, a_{i,1}}^{G_{i,0}(X)}, \overbrace{a_{i,2}, a_{i,3}}^{G_{i,1}(X)}, \overbrace{a_{i,4}, a_{i,5}}^{G_{i,2}(X)} & \\
\Downarrow & \text{Richelot op.} \\
\overbrace{\tilde{a}_{i+1,0}, \tilde{a}_{i+1,1}}^{\tilde{G}_{i+1,0}(X)}, \overbrace{\tilde{a}_{i+1,2}, \tilde{a}_{i+1,3}}^{\tilde{G}_{i+1,1}(X)}, \overbrace{\tilde{a}_{i+1,4}, \tilde{a}_{i+1,5}}^{\tilde{G}_{i+1,2}(X)} & \\
\Downarrow & \text{Perm.} \\
\vdots &
\end{array}$$

Here, one of $\{\tilde{a}_{i,m}\}$ and one of $\{a_{i,m}\}$ are ∞ when $\deg(\tilde{f}_i) = 5$ $(= \deg(f_i))$. Similarly, one of $\{\tilde{a}_{i+1,m}\}$ is ∞ when $\deg(\tilde{f}_{i+1}) = 5$ $(= \deg(f_{i+1}))$. We give an explicit expression of $\tilde{a}_{i+1,m}$ by $a_{i,0}, \ldots, a_{i,5}$ in Section 5.2.

To permute 6 zero-points of $\tilde{G}_{i,0}(X), \tilde{G}_{i,1}(X)$ and $\tilde{G}_{i,2}(X)$, we must solve the quadratic equations $\tilde{G}_{i,j}(X) = 0$ for $j = 0, 1, 2$. Hence, square root computations are the most time-consuming as in the genus 1 case. See Section 2 and [16].

4. Defining field of Weierstrass points

Since we take square roots at each step in (7), in the worst case, one might end up doing arithmetic in a prohibitively huge finite field, e.g., $\mathbb{F}_{p^{2^n}}$, even if we start at a curve over $\mathbb{F}_p$. However, here we show that if we choose a starting point appropriately, then all the computations for (7) stay in $\mathbb{F}_{p^2}$ or $\mathbb{F}_{p^4}$. Actually, we prove such computations are performed in $\mathbb{F}_{p^2}$ or $\mathbb{F}_{p^4}$ by starting a sequence at the following two types of hyperelliptic curves.

$$\text{(Type } I\text{) } C^I/\mathbb{F}_p : Y^2 = X^5 + \alpha \quad \text{for } p \equiv 4 \bmod 5,$$
$$\text{(Type } II\text{) } C^{II}/\mathbb{F}_p : Y^2 = X^5 + \alpha \quad \text{for } p \equiv 2, 3 \bmod 5.$$

Hereafter, we denote r to be 2 for Type I curves and 4 for Type II curves. We let q be p^r. Using this notation, Theorem 4.1 shows that all computations stay in $\mathbb{F}_q$ when we start at J_{C^I} or $J_{C^{II}}$.

4.1. The main theorem

Theorem 4.1. *If a sequence of Richelot isogenies* (7) *starts at* J_{C^I} *or* $J_{C^{II}}$*, then the following holds for all* i :

$$J_i(\mathbb{F}_q) \cong (\mathbb{Z}/(q^{\frac{1}{2}} + 1)\mathbb{Z})^4. \tag{10}$$

In particular, all Weierstrass points on C_i *are defined over* $\mathbb{F}_q$ *and all the computations of the sequence* (7) *are performed in* $\mathbb{F}_q$.

Proof. First, note that if (10) holds for all i, then $J_i(\mathbb{F}_q)[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$ because p is an odd prime. From Lemma 4.2, then all the computation of (7) are performed in $\mathbb{F}_q$.

Therefore, we must show the group structure (10) of $J_i(\mathbb{F}_q)$. We show this by induction. The following Lemma 4.3 shows that (10) holds at the starting point $J_0 = J_{C^I}$ or $J_{C^{II}}$. In addition, Lemma 4.4 shows that (10) holds for *all* i inductively. □

Lemma 4.2. *If* $J_i(\mathbb{F}_q)[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$*, the Richelot isogeny* ϕ_i *in* (7) *is defined over* $\mathbb{F}_q$.

Lemma 4.3. *For the curves* C^I *and* C^{II}*,*

$$J_{C^I}(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/(p+1)\mathbb{Z})^4 \quad \text{and} \tag{11}$$
$$J_{C^{II}}(\mathbb{F}_{p^4}) \cong (\mathbb{Z}/(p^2+1)\mathbb{Z})^4. \tag{12}$$

Lemma 4.4. *If* (10) *holds for* J_i *in* (7)*, then* $J_i(\mathbb{F}_q) \cong J_{i+1}(\mathbb{F}_q)$ *as a group.*

We next prove Lemmas 4.2, 4.3 and 4.4.

4.2. Proofs of Lemmas 4.2, 4.3 and 4.4

Proof of Lemma 4.2. All Weierstrass points $(a_{i,m}, 0)$ of C_i, where $m = 0, \dots, 5$, are defined in $\mathbb{F}_q$ from the assumption of Lemma 4.2. Therefore, all the coefficients of $G_{i,j}(X)$ and $\tilde{G}_{i+1,j}(X)$, which are defined in Section 3.3, are in $\mathbb{F}_q$. Therefore, all coefficients $U_{x,k}$ in (6) and $V_{x,k}$ in (6) for $k = 0, 1, 2$, are in $\mathbb{F}_q[x]$.

Because z_1 and z_2 are two zeros of U_x in (6), the u-polynomial of the Mumford representation of $\phi(D)$ in (5) is equal to U_x up to a constant multiple, and it is defined over $\mathbb{F}_q$. Let $V(z) := \sum_{k=0}^{2} (V_{x,k}/y)\, z^k$. Then, from (6), $t_\ell = V(z_\ell) \in \mathbb{F}_q(y)[x]$ for $\ell = 1, 2$. The v-polynomial of the Mumford representation of $\phi(D)$ in (5) is given by the remainder of $V(z)$ by the u-polynomial, which is defined over $\mathbb{F}_q$. Hence, all the coefficients of the v-polynomial are also in $\mathbb{F}_q(x, y)$.

This means that the isogeny ϕ_i is defined over $\mathbb{F}_q$. □

We denote the characteristic polynomial of the p^r-th power Frobenius on a Jacobian $J/\mathbb{F}_p$ by $h_r(T)$. Let the characteristic polynomial $h_1(T)$ be given by $h_1(T) = \prod_{\ell=1}^{2} (T - \pi_\ell)(T - \overline{\pi}_\ell)$.

Lemma 4.3 follows from the following Facts 4.5, 4.6 and 4.7. Fact 4.5 gives $h_1(T)$ for $J_{C^I}/\mathbb{F}_p$ and $J_{C^{II}}/\mathbb{F}_p$. Fact 4.6 gives a fundamental relation between $h_1(T)$ and $h_r(T)$. Fact 4.7 determines the group structure of $\mathbb{F}_q$-rational points of Jacobians from the characteristic polynomials $h_r(T)$.

Proof of Lemma 4.3. We first show (11) for J_{C^I}. Without loss of generality, we let $\pi_1 = \pi_2 = \sqrt{-p} \in \mathbb{C}$ from (13) in Fact 4.5. Then, all $\pi_1^2 = \pi_2^2 = \overline{\pi}_1^2 = \overline{\pi}_2^2 = -p$, i.e., $h_2(T) = (T + p)^4$ from Fact 4.6. Fact 4.7 shows that the group structure is $J_{C^I}(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/(p+1)\mathbb{Z})^4$.

We next show (12) for $J_{C^{II}}$. Without loss of generality, we let $\pi_1 = \zeta_8 \sqrt{p}$ and $\pi_2 = \zeta_8^3 \sqrt{p} \in \mathbb{C}$, where ζ_8 is a primitive 8-th root of unity, from (14) in Fact 4.5. Then, all $\pi_1^4 = \pi_2^4 = \overline{\pi}_1^4 = \overline{\pi}_2^4 = -p^2$, i.e., $h_4(T) = (T + p^2)^4$ from Fact 4.6, and $J_{C^{II}}(\mathbb{F}_{p^4}) \cong (\mathbb{Z}/(p^2+1)\mathbb{Z})^4$ from Fact 4.7. □

Fact 4.5 ([8, Prop. 1.13], [7, Example 5.1])**.** *Two curves* C^I *and* C^{II} *are supersingular, and* $h_1(T)$ *for each curve is given by*

$$(I)\ h_1(T) = (T^2 + p)^2 \ \text{and} \tag{13}$$

$$(II)\ h_1(T) = T^4 + p^2, \tag{14}$$

respectively.

Fact 4.6 ([4, Ch.14 Theorem 14.17]). *Let the characteristic polynomial $h_1(T)$ be given by the following*:

$$h_1(T) = \prod_{\ell=1}^{2}(T - \pi_\ell)(T - \overline{\pi}_\ell),$$

where π_ℓ in $\mathbb{C}$ for $\ell = 1, 2$ s.t. $|\pi_\ell| = \sqrt{p}$. Then, the characteristic polynomials $h_r(T)$ are given by

$$h_r(T) = \prod_{\ell=1}^{2}(T - \pi_\ell^r)(T - \overline{\pi}_\ell^r).$$

Fact 4.7 ([15, Theorem 2]). *Let q be p^r, A a supersingular abelian surface over $\mathbb{F}_q$, and $h_r(T)$ the characteristic polynomial of $A/\mathbb{F}_q$. Suppose that $h_r(T)$ has the decomposition $h_r(T) = \prod_{\ell=1}^{\eta} w_\ell(T)^{e_\ell}$, where $w_\ell(T)$ is $\mathbb{Q}$-irreducible for $\ell = 1, \ldots, \eta$. Then,*

$$A(\mathbb{F}_q) \cong \bigoplus_{\ell=1}^{\eta} (\mathbb{Z}/|w_\ell(1)|\mathbb{Z})^{e_\ell}$$

except for A in the following cases:

(i) $h_r(T) = (T^2 - q)^2$,
(ii) *r is odd and* $h_r(T) = (T^2 + q)^2$.

Lemma 4.4 follows from Facts 4.7, 4.8 and Lemma 4.2. Fact 4.8 is (a part of) a famous classification theorem given by Tate [13].

Proof of Lemma 4.4. Since ϕ_i are defined over $\mathbb{F}_q$ from Lemma 4.2, the characteristic polynomials of the q-th power Frobenius, $h_r(T)$, are the same for J_i and J_{i+1}. Because the polynomial $h_r(T)$ is $(T + q^{\frac{1}{2}})^4$, we conclude that $J_{i+1}(\mathbb{F}_q) \cong J_i(\mathbb{F}_q)$ from Fact 4.7. □

Fact 4.8 ([13, Theorem 1, a part of (c)]). *Let A and B be abelian varieties over a finite field $\mathbb{F}$, and let h_A and h_B be characteristic polynomials of their Frobenius endomorphisms relative to $\mathbb{F}$. Then, the following statements equivalent*:

(i) *A and B are $\mathbb{F}$-isogenous.*
(ii) $h_A = h_B$.

5. Algorithm for computing a sequence

In this section, we propose an algorithm for computing a sequence of Richelot isogenies (Algorithms 1 and 2). We give some notations for that. Using the notation (8), let ξ_i be a tuple of 6 $a_{i,m}$'s, namely, $\xi_i = (a_{i,0}, \ldots, a_{i,5})$ (possibly including ∞) and let S_i be the data consisting of ξ_i and the mulplicative factor d_i, which determines the defining equation of C_i, that is,

$$S_i := (\xi_i, d_i) = ((a_{i,0}, \ldots, a_{i,5}), d_i).$$

We use a similar notation,

$$\tilde{S}_i := (\tilde{\xi}_i, \tilde{d}_i) = ((\tilde{a}_{i,0}, \ldots, \tilde{a}_{i,5}), \tilde{d}_i)$$

as well. Since the starting curve C_0 is C^I or C^{II}, we let $\tilde{\xi}_0$ consist of 5 zero-points $\tilde{a}_0, \ldots, \tilde{a}_4$ of $f(X)$ for C_0 and ∞. Then, $\tilde{S}_0 = (\tilde{\xi}_0, 1)$, and, computing a sequence of Richelot isogenies (7) is represented by computing the following sequence consisting of S_i and $\tilde{S}_i$.

$$\tag{15} \begin{aligned} \tilde{S}_0 \overset{\mathtt{Perm}_0}{\longrightarrow} S_0 \overset{\phi_0}{\longrightarrow} \tilde{S}_1 \overset{\mathtt{Perm}_1}{\longrightarrow} S_1 \overset{\phi_1}{\longrightarrow} \tilde{S}_2 \overset{\mathtt{Perm}_2}{\longrightarrow} \\ \cdots \overset{\phi_{n-2}}{\longrightarrow} \tilde{S}_{n-1} \overset{\mathtt{Perm}_{n-1}}{\longrightarrow} S_{n-1} \overset{\phi_{n-1}}{\longrightarrow} \tilde{S}_n, \end{aligned}$$

where $\mathtt{Perm}_i$ for $i = 0, \ldots, n-1$ are permutations of the Weierstrass points determined by the i-th bit b_i of a walk data $\omega = b_0 \cdots b_{n-1}$, and ϕ_i are Richelot operators. $\mathtt{Perm}_i$ does not change the multiplicative factor $\tilde{d}_i$. Hence, $\tilde{d}_i = d_i$ for $i = 0, \ldots, n-1$, where d_i and $\tilde{d}_i$ are a component of S_i and $\tilde{S}_i$ in (15), respectively.

5.1. Permutation function

Here, we give function `Perm` to permute the Weierstrass points. In Section 3.2, we observed that a splitting $(G_0(X), G_1(X), G_2(X))$ of $f(X)$ in (3) leads to a Richelot isogeny ϕ. Let $\mathfrak{S}_6$ be the symmetric group of degree 6, acting on $\{0, \ldots, 5\}$. Then, the above splitting is given by some permutation $\sigma \in \mathfrak{S}_6$ of the zeros $\{a_0, \ldots, a_5\}$ of f, i.e., then, the splitting is given by $(a_{\sigma(0)}, a_{\sigma(1)})$, $\ldots, (a_{\sigma(4)}, a_{\sigma(5)})$. Smith [12] showed that the following set H of permutations gives all representatives, which give 14 non-isomorphic Jacobians. See Table 9.1 in [12].

$$\begin{aligned} H :=\{&(0,1,3,5,2,4), (1,3,5,2,4), (0,3,1,5,4,2), (0,5,1), (0,2)(1,5,4,3), \\ &(0,5), (0,1,2,3,4,5), (1,2,3,4,5), (0,2,5,3)(1,4), (0,2,5,3,1,4), \\ &(0,4,3,2,1), (0,3,2)(1,5,4), (0,4,2,1), (0,4,2)\}. \end{aligned}$$

Hereafter, the elements in H are ordered as above.

`Perm` takes as input an ordered tuple $(a_0, \ldots, a_5)$ and $b \in \{0, \ldots, 13\}$, and outputs the ordered tuple $(a_{\sigma(0)}, \ldots, a_{\sigma(5)})$, where $\sigma \in \mathfrak{S}_6$ is the b-th element in H. It is easy to see that the identity permutation gives the backtracking isogeny.

5.2. Richelot operator computation: Formulas for Weierstrass points

We give explicit formulas for $\tilde{a}_{2j}$, $\tilde{a}_{2j+1}$, and $\tilde{d}$ obtained by applying the Richelot operator $\mathcal{R}$. The following cases occur according to $\deg(G_{i,j+1})$, $\deg(G_{i,j+2})$, and $\deg(\tilde{G}_{i+1,j})$, where $j = 0, 1, 2$.

From (4), in the Richelot operator computation, d is multiplied by $\prod_{j=0}^{2} c_j$ and $(\det(g_{j,k}))^{-1}$. The former factor is from the leading coefficients of the brackets $[G_{i,j+1}(X), G_{i,j+2}(X)]$, then we describe the effect in Section 5.2. We treat the update of $\tilde{d}$ using the latter factor in Section 5.3.

5.2.1. Case that $\deg(G_{i,j+1}) = \deg(G_{i,j+2}) = 2$. From (9), zeros $\tilde{a}_{2j}$ and $\tilde{a}_{2j+1}$ of $\tilde{G}_{i+1,j}(X)$ are related to zeros $a_{2(j+1)}, a_{2(j+1)+1}, a_{2(j+2)}$, and $a_{2(j+2)+1}$ of $G_{i,j+1}(X), G_{i,j+2}(X)$ as follows:

$$\begin{aligned}(16)\quad [G_{i,j+1}(X), G_{i,j+2}(X)] &= G'_{i,j+1}(X)G_{i,j+2}(X) - G'_{i,j+2}(X)G_{i,j+1}(X)\\ &= (a_{2(j+1)} + a_{2(j+1)+1} - a_{2(j+2)} - a_{2(j+2)+1})X^2\\ &\quad - 2(a_{2(j+1)}a_{2(j+1)+1} - a_{2(j+2)}a_{2(j+2)+1})X\\ &\quad + a_{2(j+1)}a_{2(j+1)+1}(a_{2(j+2)} + a_{2(j+2)+1})\\ &\quad - a_{2(j+2)}a_{2(j+2)+1}(a_{2(j+1)} + a_{2(j+1)+1}).\end{aligned}$$

Let $\vartheta_j := a_{2(j+1)} + a_{2(j+1)+1} - a_{2(j+2)} - a_{2(j+2)+1}$, $\lambda_{j+1} := a_{2(j+1)}a_{2(j+1)+1}$, and $\lambda_{j+2} := a_{2(j+2)}a_{2(j+2)+1}$.

Subcase that $\deg(\tilde{G}_{i+1,j}) = 2$. If $\vartheta_j \neq 0$, $\deg(\tilde{G}_{i+1,j}) = 2$ and then (16) is equal to

$$\vartheta_j \tilde{G}_{i+1,j}(X) = \vartheta_j (X - \tilde{a}_{2j})(X - \tilde{a}_{2j+1}).$$

A quarter of the discriminant of the quadratic $[G_{i,j+1}(X), G_{i,j+2}(X)]$ is

$$\begin{aligned}\delta_j = &(a_{2(j+1)} - a_{2(j+2)})(a_{2(j+1)} - a_{2(j+2)+1})\\ &(a_{2(j+1)+1} - a_{2(j+2)})(a_{2(j+1)+1} - a_{2(j+2)+1}).\end{aligned}$$

That is, δ_j is given by the product of the differences between the zero-points of $G_{i,j+1}(X)$, i.e., $a_{2(j+1)}$ and $a_{2(j+1)+1}$, and the zero-points of $G_{i,j+2}(X)$, i.e., $a_{2(j+2)}$ and $a_{2(j+2)+1}$.

Hence, $\tilde{a}_{2j}$ and $\tilde{a}_{2j+1}$ are given by

$$\tilde{a}_{2j}, \tilde{a}_{2j+1} = \frac{\lambda_{j+1} - \lambda_{j+2} \pm \delta_j^{\frac{1}{2}}}{\vartheta_j}.$$

The multiplicative factor $\tilde{d}$ is updated to $\tilde{d} \cdot \vartheta_j$.

Subcase that $\deg(\tilde{G}_{i+1,j}) = 1$. If $\vartheta_j = 0$, (16) is linear, i.e., $\deg(\tilde{G}_{i+1,j}) = 1$. Then, the root of $\tilde{G}_{i+1,j}(X) = 0$, $\tilde{a}_{2j}$, is given by

$$\tilde{a}_{2j} = \frac{a_{2(j+1)} + a_{2(j+1)+1}}{2}$$

since $a_{2(j+1)} + a_{2(j+1)+1} = a_{2(j+2)} + a_{2(j+2)+1}$.

The leading coefficient of $\tilde{G}_{i+1,j}(X)$ is $-2(\lambda_{j+1} - \lambda_{j+2})$. Then $\tilde{d}$ is updated to $-2(\lambda_{j+1} - \lambda_{j+2}) \cdot \tilde{d}$.

5.2.2. Case that $\deg(G_{i,j+1}) = 1$ or $\deg(G_{i,j+2}) = 1$. First, we consider the case that $\deg(G_{i,j+1}) = 1$, i.e., $G_{i,j+1}(X)$ is linear. We obtain formulas for $\tilde{a}_{2j}$, $\tilde{a}_{2j+1}$ as follows: Let $G_{i,j+1}(X) = X - a_{2(j+1)}$, $G_{i,j+2}(X) = (X - a_{2(j+2)})(X - a_{2(j+2)+1})$. Then,

$$\begin{aligned} & [G_{i,j+1}(X), G_{i,j+2}(X)] \\ = & -\tilde{G}_{i+1,j}(X) \\ = & -[X^2 - 2a_{2(j+1)}X + (a_{2(j+2)} + a_{2(j+2)+1})a_{2(j+1)} - a_{2(j+2)}a_{2(j+2)+1}]. \end{aligned}$$

Let $\delta_j := (a_{2(j+1)} - a_{2(j+2)})(a_{2(j+1)} - a_{2(j+2)+1})$. Then, we obtain

$$\tilde{a}_{2j}, \tilde{a}_{2j+1} = a_{2(j+1)} \pm \delta_j^{\frac{1}{2}}.$$

Next, we consider the case that $\deg(G_{i,j+2}) = 1$. Let $G_{i,j+1}(X) = (X - a_{2(j+1)})(X - a_{2(j+1)+1})$, $G_{i,j+2}(X) = X - a_{2(j+2)}$. Then,

$$\begin{aligned} & [G_{i,j+1}(X), G_{i,j+2}(X)] \\ & = \tilde{G}_{i+1,j}(X) \\ & = X^2 - 2a_{2(j+2)}X + (a_{2(j+1)} + a_{2(j+1)+1})a_{2(j+2)} - a_{2(j+1)}a_{2(j+1)+1}. \end{aligned}$$

Let $\delta_j := (a_{2(j+2)} - a_{2(j+1)})(a_{2(j+2)} - a_{2(j+1)+1})$. Then, we obtain

$$\tilde{a}_{2j}, \tilde{a}_{2j+1} = a_{2(j+2)} \pm \delta_j^{\frac{1}{2}}.$$

For the former case, $\tilde{d}$ is updated to $-\tilde{d}$ and for the latter case, $\tilde{d}$ remains unchanged.

5.3. Final update of the multiplicative factor

5.3.1. Case that $\deg(f_i) = 6$. In this case, $\tilde{d}$ is updated to $\tilde{d} \cdot \det(M_i)^{-1}$, where

$$M_i := \begin{pmatrix} a_0a_1 & -(a_0 + a_1) & 1 \\ a_2a_3 & -(a_2 + a_3) & 1 \\ a_4a_5 & -(a_4 + a_5) & 1 \end{pmatrix}.$$

Then, $\det(M_i)$ is equal to the determinant of the following 2×2 matrix:

$$M_i^0 := \begin{pmatrix} \lambda_1 - \lambda_0 & \vartheta_2 \\ \lambda_2 - \lambda_0 & -\vartheta_1 \end{pmatrix}.$$

We see that $\vartheta_1 + \vartheta_2 = -\vartheta_0$ by direct calculation. Hence, $\det(M_i^0) = -\sum_{j=1}^2 \vartheta_j (\lambda_j - \lambda_0) = -\sum_{j=1}^2 \vartheta_j\lambda_j + (\vartheta_1 + \vartheta_2)\lambda_0 = -\sum_{j=1}^2 \vartheta_j\lambda_j - \vartheta_0\lambda_0 = -\sum_{j=0}^2 \lambda_j\vartheta_j$. That is,

$$\det(M_i) = -\sum_{j=0}^{2} \lambda_j\vartheta_j. \tag{17}$$

5.3.2. Case that $\deg(f_i) = 5$. Assume that $\deg(G_{i,j_0}) = 1$, a_{m_0} is the zero of $G_{i,j_0}(X)$, and $a_{m_1} = \infty$. Let $\lambda_{j_0+1} := a_{2(j_0+1)}a_{2(j_0+1)+1}$, $\lambda_{j_0+2} := a_{2(j_0+2)}a_{2(j_0+2)+1}$, and $\vartheta_{j_0} := a_{2(j_0+1)}+a_{2(j_0+1)+1}-a_{2(j_0+2)}-a_{2(j_0+2)+1}$. Then, $\tilde{d}$ is updated to $\tilde{d}\cdot\det(M_i)^{-1}$, where M_i is constructed from the coefficients of $G_{i,0}(X), G_{i,1}(X)$, and $G_{i,2}(X)$. Here, since $G_{i,j_0}(X)$ is linear, the quadratic coefficient of it is 0. From direct computation,

$$\det(M_i) = a_{m_0}\vartheta_{j_0} - \lambda_{j_0+1} + \lambda_{j_0+2}.$$

Then, if we let $\lambda_{j_0} := -a_{m_0}$, $\vartheta_{j_0+1} := 1$ and $\vartheta_{j_0+2} := -1$, we see that (17) holds similar to the case that $\deg(f_i) = 6$.

5.4. Description of the algorithm

Algorithm 1 gives the computation of a Richelot isogeny sequence, and Algorithm 2 gives the computation of a Richelot isogeny. Algorithm 2 computes $\tilde{S}_{i+1}$ from S_i according to the explicit formulas for $\tilde{a}_0, \dots, \tilde{a}_5$ and $\tilde{d}$ given in Sections 5.2 and 5.3.

Algorithm 1 iterates Algorithm 2 n-times, and uses the `Perm` function to choose the next edge according to ω. Step 3 of Algorithm 1 checks whether $\tilde{d}_i = \perp$ or not, and if so, then Algorithm 1 also returns $\perp$ (See Section 3.3). We observed that such split cases rarely occur when starting at J_{C^I} or $J_{C^{II}}$ and $p \geq 2^{160}$.

We fix a branch of square roots, $\delta^{\frac{1}{2}}$, in Algorithm 2 as follows: Fix $\tau \in \mathbb{F}_q$ s.t. $\mathbb{F}_q = \mathbb{F}_p[\tau] = \oplus_{\ell=0}^{r-1}\mathbb{F}_p\tau^\ell \cong (\mathbb{F}_p)^r$ as an $\mathbb{F}_p$-vector space. Then, $\delta^{\frac{1}{2}}$ is defined as the max of the two branches using a natural lexicographic order of $\mathbb{F}_q \cong (\mathbb{F}_p)^r$.

5.5. Cost of a Richelot operator computation

We give the cost of the computation of *one* Richelot isogeny, and we explain the cost of the dominant case that all $G_j(X)$ and $\tilde{G}_j(X)$ are quadratics. Then, we see that from Algorithm 2, the total cost is 25 multiplications, 4 inversions, and 3 square root computations in $\mathbb{F}_q$.

Algorithm 1 `RIsogSeq` : Computing a sequence of Richelot isogenies

Input : $\tilde{S}_0$ and walk data $\omega = b_0 \cdots b_{n-1}$.
Output : $\tilde{S}_n$ or $\perp$ if split case.
1: **for** $i \leftarrow 0$ to $n-1$ **do**
2: $(\tilde{\xi}_i, \tilde{d}_i) \leftarrow \tilde{S}_i$, $\xi_i \leftarrow$ `Perm`$(\tilde{\xi}_i, b_i)$. {/* `Perm`$_i(\tilde{\xi}_i)$ */}
3: **if** $\tilde{d}_i = \perp$ **then** {/* split case */}
4: `return` $\perp$.
5: **end if**
6: $S_i \leftarrow (\xi_i, \tilde{d}_i)$, $\tilde{S}_{i+1} \leftarrow$ `RIsog`(S_i).
7: **end for**
8: `return` $\tilde{S}_n$.

Algorithm 2 `RIsog` : Computing a Richelot isogeny

Input : $S_i = ((a_0, a_1, a_2, a_3, a_4, a_5), d)$.
Output : $\tilde{S}_{i+1} = ((\tilde{a}_0, \tilde{a}_1, \tilde{a}_2, \tilde{a}_3, \tilde{a}_4, \tilde{a}_5), \tilde{d})$.

$\tilde{d} \leftarrow d$.
for $j \leftarrow 0$ to 2 **do** {/* calc. of λ_j */}
  if $a_{2j} = \infty$ **then**
    $\lambda_j \leftarrow -a_{2j+1}$.
  else if $a_{2j+1} = \infty$ **then**
    $\lambda_j \leftarrow -a_{2j}$.
  else
    $\lambda_j \leftarrow a_{2j}a_{2j+1}$.
  end if
end for
for $j \leftarrow 0$ to 2 **do** {/* calc. of $\tilde{a}_{2j}, \tilde{a}_{2j+1}, \tilde{d}$ */}
  if $\infty \notin \{a_{2(j+1)},\ a_{2(j+1)+1},\ a_{2(j+2)},\ a_{2(j+2)+1}\}$ **then** {/* case that $\deg(G_{i,j+1}) = \deg(G_{i,j+2}) = 2$ */}
    $\rho_0 \leftarrow a_{2(j+1)} - a_{2(j+2)}$, $\rho_1 \leftarrow a_{2(j+1)+1} - a_{2(j+2)+1}$,
    $\rho_2 \leftarrow a_{2(j+1)} - a_{2(j+2)+1}$, $\rho_3 \leftarrow a_{2(j+1)+1} - a_{2(j+2)}$,
    $\vartheta_j \leftarrow \rho_0 + \rho_1$, $\nu \leftarrow \lambda_{j+1} - \lambda_{j+2}$.
    if $\vartheta_j \neq 0$ **then** {/* case that $\deg(\tilde{G}_{i+1,j}) = 2$ */}
      $\delta \leftarrow \rho_0\rho_1\rho_2\rho_3$, $\kappa \leftarrow \delta^{\frac{1}{2}}$, $\mu \leftarrow \vartheta_j^{-1}$,
      $\tilde{a}_{2j} \leftarrow (\nu + \kappa)\mu$, $\tilde{a}_{2j+1} \leftarrow (\nu - \kappa)\mu$, $\tilde{d} \leftarrow \vartheta_j \tilde{d}$.
    else {/* case that $\deg(\tilde{G}_{i+1,j}) = 1$ */}
      $\tilde{a}_{2j} \leftarrow (a_{2(j+1)} + a_{2(j+1)+1})/2$, $\tilde{a}_{2j+1} \leftarrow \infty$, $\tilde{d} \leftarrow -2\nu \cdot \tilde{d}$.
    end if
  else {/* case that $\deg(G_{i,j+1})$ or $\deg(G_{i,j+2}) = 1$ */}
    if $\infty \in \{a_{2(j+1)}, a_{2(j+1)+1}\}$ **then**
      $j_0 \leftarrow j+1$, $j_1 \leftarrow j+2$, $\vartheta_j \leftarrow -1$. {/* $j = j_0 + 2$ */}
    else
      $j_0 \leftarrow j+2$, $j_1 \leftarrow j+1$, $\vartheta_j \leftarrow 1$. {/* $j = j_0 + 1$ */}
    end if
    Set (m_0, m_1) such that a_{m_0} is the zero of $G_{j_0}(X)$ and $a_{m_1} = \infty$.
    $\rho_0 \leftarrow a_{m_0} - a_{2j_1}$, $\rho_1 \leftarrow a_{m_0} - a_{2j_1+1}$, $\delta \leftarrow \rho_0\rho_1$,
    $\kappa \leftarrow \delta^{\frac{1}{2}}$, $\tilde{a}_{2j} \leftarrow a_{m_0} + \kappa$, $\tilde{a}_{2j+1} \leftarrow a_{m_0} - \kappa$, $\tilde{d} \leftarrow \vartheta_j \tilde{d}$.
  end if
end for
$\chi \leftarrow -\sum_{j=0}^{2} \lambda_j \vartheta_j$.
if $\chi = 0$ **then** {/* case that $\det(M_i) = 0$ */}
  $\tilde{d} \leftarrow \perp$.
else {/* case that $\det(M_i) \neq 0$. final update of $\tilde{d}$ */}
  $\tilde{d} \leftarrow \tilde{d} \cdot \chi^{-1}$.
end if
$\tilde{S}_{i+1} \leftarrow ((\tilde{a}_0, \ldots, \tilde{a}_5), \tilde{d})$.
`return` $\tilde{S}_{i+1}$.

References

[1] P. R. Bending, *Curves of genus 2 with $\sqrt{2}$ multiplication*, Ph. D. Thesis, University of Oxford, 1998.

[2] J.-B. Bost and J.-F. Mestre, *Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2*, Gaz. Math. No. **38** (1988), 36–64.

[3] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2, London Mathematical Society Lecture Note Series, 230. Cambridge University Press, Cambridge, 1996.

[4] H. Cohen and G. Frey et al., *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman & Hall, 2006.

[5] D. X. Charles, E. Z. Goren, and K. E. Lauter, *Cryptographic hash functions from expander graphs*, to appear in Journal of Cryptology.

[6] ———, *Families of Ramanujan graphs and quaternion algebras*, to appear in AMS-CRM volume "Groups and Symmetries" in honor of John McKay.

[7] Y. J. Choie, E. K. Jeong, and E. J. Lee, *Supersingular hyperelliptic curves of genus 2 over finite fields*, Appl. Math. Comput. **163** (2005), no. 2, 565–576.

[8] T. Ibukiyama, T. Katsura, and F. Oort, *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), no. 2, 127–152.

[9] S. Paulus and H.-G. Rück, *Real and imaginary quadratic representations of hyperelliptic function fields*, Math. Comp. **68** (1999), no. 227, 1233–1241.

[10] S. Paulus and A. Stein, *Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves*, Algorithmic number theory (Portland, OR, 1998), 576–591, Lecture Notes in Comput. Sci., 1423, Springer, Berlin, 1998.

[11] A. Rostovtsev and A. Stolbunov, *Public-key cryptosystem based on isogenies*, preprint, IACR ePrint 2006/145.

[12] B. Smith, *Explicit endomorphisms and correspondences*, Ph. D. Thesis, The Univ. of Sydney, 2005.

[13] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

[14] J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241.

[15] C. Xing, *On supersingular abelian varieties of dimension two over finite fields*, Finite Fields Appl. **2** (1996), no. 4, 407–421.

[16] R. Yoshida and K. Takashima, *Simple algorithms for computing a sequence of 2-isogenies*, ICISC 2008, LNCS No. 5461, pp. 52–65, Springer Verlag, 2009.

Katsuyuki Takashima
Information Technology R&D Center
Mitsubishi Electric
Kamakura-shi, Kanagawa 247-8501, Japan
E-mail address: Takashima.Katsuyuki@aj.MitsubishiElectric.co.jp

Reo Yoshida
Department of Social Informatics
Graduate School of Informatics
Kyoto University
Sakyo-ku, Kyoto 606-8501, Japan
E-mail address: yoshida@ai.soc.i.kyoto-u.ac.jp