The Vector Decomposition Problem for Elliptic and Hyperelliptic Curves

Iwan Duursma[1] and Negar Kiyavash[2]

[1] Coordinated Science Laboratory, Dept. of Mathematics,
University of Illinois at Urbana-Champaign
duursma@math.uiuc.edu,

[2] Coordinated Science Laboratory, Dept. of Electrical and Computer Engineering,
University of Illinois at Urbana-Champaign
kiyavash@uiuc.edu

Abstract. The group of m-torsion points on an elliptic curve, for a prime number m, forms a two-dimensional vector space. It was suggested and proven by Yoshida that under certain conditions the vector decomposition problem (VDP) on a two-dimensional vector space is at least as hard as the computational Diffie-Hellman problem (CDHP) on a one-dimensional subspace. In this work we show that even though this assessment is true, it applies to the VDP for m-torsion points on an elliptic curve only if the curve is supersingular. But in that case the CDHP on the one-dimensional subspace has a known sub-exponential solution. Furthermore, we present a family of hyperelliptic curves of genus two that are suitable for the VDP.

Key words. Elliptic curve cryptography, Curves of genus two.

1 Introduction

It is generally believed that the computational Diffie-Hellman problem (CDHP) is a mathematically hard problem. Yoshida et al. [YMF02], [YMF03] proposed a new hard problem; that of vector decomposition (VD). Yoshida [Yos03] proves sufficient conditions for which the VDP on a two-dimensional vector space is at least as hard as the CDHP on a one-dimensional subspace. We shall show that for every example on an elliptic curve that meets the condition, the Diffie-Hellman problem is weak. We then consider the vector decomposition problem for hyperelliptic curves. Precise definitions of CDHP and VDP are given in Section 2. We recite Theorem 2.21 from Yoshida [Yos03] that provides a set of sufficient conditions on a two-dimensional vector space such that its VDP is at least as hard as the CDHP on a one-dimensional subspace. Then under these conditions one can solve the CDHP in the underlying one-dimensional subspace by calling two instances of the VD problem. In Section 3 we prove that any elliptic curve for which the sufficient conditions in Section 2 hold is bound to be supersingular. In Section 4 we consider the classification of genus 2 curves according to their automorphism group [Igu60] and give a family of hyperelliptic curves of genus two that are suitable for the VDP. In Section 5 we prove that these curves satisfy the sufficient conditions of Section 2 and describe the VDP for such curves in details.

2 Vector Decomposition Problem

We formally define the vector decomposition problem (VDP) and the Computational Diffie-Hellman problem (CDHP). More importantly Theorem 2.21 of Yoshida [Yos03] is presented. This theorem states sufficient conditions on the two-dimensional vector space under which the VDP is at least as hard as the CDHP on the one-dimensional subspace. The proof of the sufficiency of these conditions can be found in Yoshida [Yos03].

Definition 1. *The Vector Decomposition Problem on $\mathcal{V}$ (a two-dimensional vector space over $\mathbb{F}$) is "Given $e_1, e_2, v \in \mathcal{V}$ such that $\{e_1, e_2\}$ is an $\mathbb{F}$-basis for $\mathcal{V}$, find the vector $u \in \mathcal{V}$ such that $u \in \langle e_1 \rangle$ and $v - u \in \langle e_2 \rangle$".*

Definition 2. *The computational Diffie-Hellman problem on $\mathcal{V}'$(a one-dimensional vector space over $\mathbb{F}$) is "Given $e \in \mathcal{V}' \setminus \{0\}$ and $ae, be \in \langle e \rangle$, find $abe \in \langle e \rangle$".*

Theorem 1. *(Yoshida [Yos03, Theorem 2.21])*

The Vector Decomposition Problem on $\mathcal{V}$ is at least as hard as the CDH problem on $\mathcal{V}' \subset \mathcal{V}$ if for any $e \in \mathcal{V}'$ there are linear isomorphisms $\phi_e, F_e : \mathcal{V} \to \mathcal{V}$ which satisfy the following three conditions:

(1) *For any $v \in \mathcal{V}$, $\phi_e(v)$ and $F_e(v)$ are effectively defined and can be computed in polynomial time.*

(2) *$\{e, \phi_e(e)\}$ is an $\mathbb{F}$-basis for $\mathcal{V}$.*

(3) *There are $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}$ with*

$$F_e(e) = \alpha_1 e,$$
$$F_e(\phi_e(e)) = \alpha_2 e + \alpha_3 \phi_e(e),$$

and $\alpha_1, \alpha_2, \alpha_3 \neq 0$. The elements $\alpha_1, \alpha_2, \alpha_3$ and their inverses can be computed in polynomial time.

To make the theorem clear, we will present a slight modification of the proof given by Yoshida [Yos03] here.

Proof. We will show that given (e, ae, be), the quantity abe can be computed by solving two instances of the VD problem. For the nontrivial case of $ae \neq 0$ we compute the following,

$$\begin{aligned} e_0 &= (\alpha_2^{-1}(\alpha_3 - \alpha_1)ae - \alpha_2^{-1}e) = \lambda e, \\ e_1 &= ae + \phi_e(e_0) = ae + \lambda\phi_e(e), \\ e_2 &= F_e(e_1) = (\alpha_3 a - 1)e + \alpha_3\lambda\phi_e(e). \end{aligned}$$

It is clear that $\alpha_3 e_1 - e_2 = e$ and the decomposition of be on the basis$\{e_1, e_2\}$ is $u = \alpha_3 be_1$. Furthermore decomposition of u on the basis $\{e, \phi_e(e)\}$ results in $u' = \alpha_3 abe$. The answer to the DHP is $\alpha_3^{-1}u' = abe$.

A key step in the above solution is that $\{e_1, e_2\}$ should form a $\mathbb{F}$-basis for $\mathcal{V}$. The condition (2) above implies that $\{e, \phi_e(e)\}$ is an $\mathbb{F}$-basis for $\mathcal{V}$. The condition for $\{e_1, e_2\}$ forming a basis is that the following matrix must be nonsingular,

$$\begin{bmatrix} a & \lambda \\ \alpha_3 a - 1 & \alpha_3\lambda \end{bmatrix}.$$

Clearly if $\lambda \neq 0$ then the matrix above is nonsingular. Now assume that $\lambda = 0$. Then $a = (\alpha_3 - \alpha_1)^{-1}$ and the desired quantity $abe = (\alpha_3 - \alpha_1)^{-1}be$. □

Next we shall show an example of applying VDP for solving CDHP. For reasons that will become clear, in analogy to the notation for a point on an algebraic curve, we shall represent an element of the vector space $\mathcal{V}'$ with letter P.

Example 1. We will illustrate the theorem for the values $\alpha_1 = 1, \alpha_2 = -1, \alpha_3 = -1$. Also we shall assume that the maps ϕ_P and F_P do not depend on P and thus the subscript P can be dropped,

$$\begin{aligned} F(P) &= P, \\ F(\phi(P)) &= -P - \phi(P). \end{aligned}$$

Let $P, A = aP, B = bP$ be given. Then abP can be computed from the VDP as follows. Let

$$\begin{aligned} S &= A + 2\phi(A) + \phi(P) \\ &= aP + (2a + 1)\phi(P). \end{aligned}$$

And let $T = F(S)$, so that

$$\begin{aligned} T &= A + 2(-A - \phi(A)) - P - \phi(P) \\ &= (-a-1)P - (2a+1)\phi(P). \end{aligned}$$

Then $S + T = -P$ and $VDP((S,T), -B)$ gives component bS on S. Finally, $VDP((P, \phi(P)), bS)$ gives component abP on P.

The conditions stated in the theorem are stronger than what is in fact necessary to prove the theorem. Indeed it is enough to have two linear endomorphisms that satisfy the condition stated above. The last condition and the fact that $\{e, \phi_e(e)\}$ is an $\mathbb{F}$-basis for $\mathcal{V}$, forces F_e to have an inverse, while ϕ_e is simply an endomorphism of the vector space that does not need to have an inverse. The significance of this becomes apparent in the case where $\mathcal{V}$ is chosen to be the vector space of m-torsion points of an elliptic curve. Then studying the endomorphism ring of the curve classifies all the possibilities for the linear endomorphisms $\phi_e, F_e : \mathcal{V} \to \mathcal{V}$.

The theorem above indeed seems quite strong. Basically, as long as the two-dimensional vector space $\mathcal{V}$ is equipped with the proper linear endomorphisms, then the VDP is at least as hard as the CDHP on the one-dimensional subspace.

The above theorem is an elegant result, but it is of no significance as long as one cannot find an example of the vector space $\mathcal{V}$ and a subspace $\mathcal{V}'$ satisfying the desired conditions.

3 Vector Decomposition Problem on Elliptic Curves

In this section we prove that an elliptic curve that meets the conditions of Theorem 1 has to be supersingular and thus not appropriate for cryptographic purposes.

Yoshida [Yos03] proposes to choose $\mathcal{V} = E[m]$, the full group of m-torsion points on an elliptic curve, and $\mathcal{V}' = E(\mathbb{F}_p) \cap E[m]$, the subgroup of $\mathbb{F}_p$-rational m-torsion points, where

Notation 1.

$$\begin{aligned} &p: \text{ a prime with } p \equiv 2 \pmod 3, \\ &E: \ y^2 = x^3 + 1, \text{ an elliptic curve over } \mathbb{F}_p, \\ &m: \text{ a prime such that } 6m = p + 1, \\ &E[m] = \{P \in E \mid mP = 0\} \subset E(\mathbb{F}_{p^2}). \end{aligned}$$

The map F is the Frobenius map, $F(x,y) = (x^p, y^p)$, and the map ϕ is chosen to be

$$\phi(x,y) = (\omega x, y), \quad \text{where } \omega^2 + \omega + 1 = 0.$$

Theorem 1 applies with $\alpha_1 = 1, \alpha_2 = -1, \alpha_3 = -1$, which is the special case illustrated in Example 1.

Unfortunately the proposed curve $E : y^2 = x^3 + 1$ is supersingular and thus susceptible to the MOV attack [MOV93]. This is not a mere incidence of a bad choice; we will show that under the conditions of Theorem 1, if $\mathcal{V}$ is chosen to be $E[m]$, the group of m-torsion points on an elliptic curve, then the curve is forced to be supersingular.

Theorem 2. *Any elliptic curve with the two linear endomorphisms $\phi_e, F_e : \mathcal{V} \to \mathcal{V}$ satisfying the conditions of Theorem 1, where $\mathcal{V}$ is chosen to be $E[m]$, the group of m-torsion points, is supersingular.*

Proof. $\mathrm{End}(E)$, the endomorphism ring of E, is of one of three types: the ring of integers Z, an order in an imaginary quadratic field, or an order in a quaternion algebra. Over a finite field only the last two occur, and the last type occurs if and only if the curve is supersingular [Sil99], [BSS00]. Now assume that the curve is not supersingular, then the endomorphism ring is of rank two and as vector space over $\mathbb{Q}$, $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} = \langle 1, \sigma \rangle$. Thus we have:

$$F = a + b\sigma \qquad \text{and} \qquad \phi = c + d\sigma.$$

The condition $F(e) = \alpha_1 e$ and the fact that $\{e, \phi(e)\}$ is an $\mathbb{F}$-basis implies that $b = 0$ and $a = \alpha_1$, and

$$F \circ \phi(e) = \alpha_1 \phi(e).$$

But $\{e, \phi(e)\}$ is a basis, thus

$$F \circ \phi(e) = \alpha_2 e + \alpha_3 \phi(e)$$

implies $\alpha_2 = 0$ (and $\alpha_1 = \alpha_3$). □

4 Curves of Genus Two

The difficulty of the vector decomposition problem is based on Theorem 1 [Yos03, Theorem 2.21]. Under the conditions of the theorem, the vector decomposition problem can be called to solve the underlying one-dimensional Diffie-Hellman problem. Thus the vector decomposition problem is hard if the Diffie-Hellman problem on a one-dimensional subspace is hard.

This will be the case for example if the one-dimensional subspace is a cyclic subgroup $\mathbb{Z}/m\mathbb{Z}$ of large prime order in the group of points of a general elliptic curve. Assume that the full m-torsion of the elliptic curve is defined over a small extension of the original base field so that we can choose as our two-dimensional vector space the group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ of all m-torsion points on the elliptic curve. Then, the Weil-pairing is non-degenerate over the extension field and the MOV attack applies to reduce the one-dimensional Diffie-Helman problem to a problem in the multiplicative group of the extension field, where it has a sub-exponential solution. More seriously, as shown by Theorem 2, the conditions of Theorem 1 hold for the group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ of m-torsion points only if the elliptic curve is of supersingular type. And in that case the MOV attack applies with small degree (at most six) of the extension field. Altogether, this means that the full m-torsion of an elliptic curve is not a suitable vector space for the two-dimensional VDP.

If we choose the group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ as a subgroup of the m-torsion points in the Jacobian of a higher genus curve then we can avoid the MOV attack and the Frey-Rück attack [FR94], [FMR99] and we can satisfy the conditions of Theorem 1 for curves that are not supersingular.

In this section we consider curves of higher genus. We can indeed find curves with m-torsion of rank two among families of hyperelliptic curves with non-trivial automorphisms. Such families have been classified for curves of genus two. In the next section we recall these results and present a family of genus 2 curves that is suitable for the vector decomposition problem.

4.1 A Suitable Class of Genus 2 Curves

Igusa's classification of genus 2 curves according to their automorphism group [Igu60, Section 8, Hyperelliptic curves with many automorphisms] lists three infinite families and three special curves. The more recent publications [CGLR99], [CQ02], [GS01], [SV04] describe these families in more detail and add further properties. We give the classification and some important properties. In the next section, we focus on one of the infinite families.

Ignoring the case of even characteristic, a hyperelliptic curve of genus two is birationally equivalent to a curve in Rosenhain normal form

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu). \tag{1}$$

The moduli space $\mathcal{M}_2$ of genus 2 curves is an affine variety of dimension three whose coordinate ring is generated by the classical invariants J_2, J_4, J_6, J_{10} of a binary sextic [Igu60]. Let G denote the full automorphism group of a curve and $e_0 \in G$ the canonical involution. Igusa classifies curves with non-trivial reduced automorphism group $\bar{G} = G/\langle e_0 \rangle$ according to their Rosenhain form. For the special choice $\nu = \lambda(1-\mu)/(1-\lambda)$, the three factors $x-\lambda$, $x(x-\mu)$ and $(x-1)(x-\nu)$ become linearly dependent and the curve has a nontrivial involution that acts on the roots of the Rosenhain form as $(\infty\,\lambda)(0\,\mu)(1\,\nu)$. The same family is described in Jacobi normal form by an equation

$$y^2 = x(x-1)(x-a)(x-b)(x-ab). \tag{2}$$

The choice $c = ab$ makes the factors x, $(x-a)(x-b)$ and $(x-1)(x-c)$ linearly dependent and corresponds to a nontrivial involution that acts on the roots of the Jacobi form as $(\infty\,0)(a\,b)(1\,ab)$. Cassels and Flynn [CF96] describe a straightforward procedure to bring a curve with given non-trivial involution in the form

$$C : y^2 = c_3x^6 + c_2x^4 + c_1x^2 + c_0. \tag{3}$$

So that the non-trivial involutions $e_1 = (x, y) \mapsto (-x, y)$ and $e_2 = (x, y) \mapsto (-x, -y)$ act on the roots via $x \mapsto -x$. The quotients $E_1 = C/\langle e_1 \rangle$ and $E_2 = C/\langle e_2 \rangle$ are the elliptic curves

$$\begin{aligned} &E_1 : y^2 = c_3x^3 + c_2x^2 + c_1x + c_0, \quad C \longrightarrow E_1 : (x, y) \mapsto (x^2, y),\\ &E_2 : y^2 = c_0x^3 + c_1x^2 + c_2x + c_3, \quad C \longrightarrow E_2 : (x, y) \mapsto (1/x^2, y/x^3). \end{aligned}$$

The Jacobian J of C decomposes up to isogeny as $J \sim E_1 \times E_2$. Existence of the isogeny is immediate with the techniques from [KR89]. The isogeny is induced by the product of the quotient maps and has kernel of type $Z_2 \times Z_2$ with non-trivial elements $(e, 0) - (-e, 0)$, for $(e, 0) \in C$.

After scaling, (3) becomes

$$y^2 = x^6 - s_1x^4 + s_2x^2 - 1. \tag{4}$$

Following [SV04], let

$$u = s_1s_2 = \frac{c_2c_1}{c_3c_0}, \quad v = s_1^3 + s_2^3 = \frac{c_2^3c_0 + c_1^3c_3}{c_3^2c_0^2}.$$

Observe that, for $y^2 = f(x)$,

$$u = (\sum_{f(z)=0} z^2)(\sum_{f(z)=0} z^{-2}), \quad u^2 + 4u - 2v = (\sum_{f(z)=0} z^4)(\sum_{f(z)=0} z^{-4}).$$

The following theorem by Shaska and Völklein shows that u, v parameterize the moduli space of genus 2 curves together with the image of an elliptic involution in the reduced automorphism group. In other words, a point in this moduli space represents the isomorphism class of a Galois cover $C/\mathbb{P}^1$ of type $Z_2 \times Z_2 = \{1, e_0, e_1, e_2\}$, such that e_0 is the canonical involution and the quotients $C/\langle e_1 \rangle = E_1$ and $C/\langle e_2 \rangle = E_2$ are elliptic curves.

Theorem 3. *[SV04, Lemma 1] For $(s_1, s_2) \in k^2$ with $\Delta(x^6 - s_1x^4 + s_2x^2 - 1) \neq 0$, Equation (4) defines a genus 2 field K_{s_1,s_2}. Its reduced automorphism group contains the elliptic involution $\epsilon_{s_1,s_2} : x \mapsto -x$. Two such pairs $(K_{s_1,s_2}, \epsilon_{s_1,s_2})$ and $(K_{s_1',s_2'}, \epsilon_{s_1',s_2'})$ are isomorphic if and only if $(u, v) = (u', v')$, where*

$$(u, v) = (s_1s_2, s_1^3 + s_2^3)$$

Remark 1. Formulas to compute the Igusa invariants J_2, J_4, J_6, J_{10} and thus the absolute invariants i_2, i_4, i_{10} from (u, v) can be found in [SV04]. There one can also find formulas for the $j-$invariants of the elliptic curves E_1 and E_2 in terms of u, v.

Remark 2. A pair (u, v) describes a pair $(K, \{1, e_0, e_1, e_2\})$. Thus the quotients $C \longrightarrow E_1$ and $C \longrightarrow E_2$ of C correspond to the same point (u, v) in the moduli space, although E_1 and E_2 need not be isomorphic. And to find the number of nonisomorphic quotients $C \longrightarrow E$, for a given curve C, a point in the moduli space may need to be counted with multiplicity two. In addition, some curves C may correspond to more than one point (u, v) in the moduli space. This happens for example for $(u, v) = (0, 0)$ and $(u, v) = (15^2, 2 \cdot 15^3)$ that represent nonisomorphic $Z_2 \times Z_2$ quotients of the same curve. The involution $w \mapsto -w$ on $z^2 = w^6 + 1$ is the unique central involution in the reduced automorphism group D_{12}. Under the isomorphism from $y^2 = 2x^6 + 30x^4 + 30x^2 + 2$ to $z^2 = w^6 + 1$ given by $w = (x + 1)/(x - 1), z = y/(x - 1)^3$ the elliptic involution $x \mapsto -x$ corresponds to $w \mapsto 1/w$ which is contained in a subgroup S_3 of D_{12}.

Igusa's classification of genus two curves with many (more than two) automorphisms contains the three infinite families (1), (2) and (3) and

Table 1. Igusa's Classification of Genus 2 Curves.

Family	$\bar{G} = G/\langle e_o \rangle$	G	(λ, μ, ν)	Comment
(1)	Z_2	V_4	$\nu = \lambda(1-\mu)/(1-\lambda)$	$(\infty\,\lambda)(0\,\mu)(1\,\nu) \in \bar{G}$
(2)	S_3	D_{12}	$\mu = -1/\lambda + 1, \nu = 1/(1-\lambda)$	$(\infty\,1\,0)(\lambda\,\mu\,\nu) \in \bar{G}$
(3)	V_4	D_8	$\mu = 1/\lambda, \nu = -1$	$(\infty\,0)(\lambda\,\mu) \in \bar{G}$
(3')	V_4	D_8	$\mu = 1/(2-\lambda), \nu = \lambda/(2-\lambda)$	$(\infty\,\mu)(0\,\lambda) \in \bar{G}$
(4)=(2) $\cap$ (3)	D_{12}	$Z_3 \rtimes D_8$	$(2, 1/2, -1)$	$\simeq y^2 = x^6 + 1$
(5)=(2) $\cap$ (3')	S_4	$GL_2(3)$	$(1+i, (1+i)/2, i)$	$\simeq y^2 = x^5 - x$
(6)	Z_5	Z_{10}		$\simeq y^2 = x^5 - 1$

the three special curves (4), (5) and (6). Table 1 depicts their reduced automorphism group, full automorphism group and Rosenhain form. For the family (3), we add an equivalent description (3').

In each case a curve belongs to a family whenever its reduced automorphism group contains the particular permutation given in the last column. Conversely, a curve in a family can always be represented such that it has a reduced automorphism of the given form.

The families (2) and (3) ($\simeq$(3')) are one-dimensional subfamilies of the two-dimensional family (1). They intersect in the two special curves (4) and (5). In [CGLR99], [CQ02], it is erroneously claimed that only (4) lies in the intersection of (2) and (3). The last column provides generators for the reduced automorphism group. For any given family, the reduced automorphism group is obtained by adding the generator in the last column to the group generated by the parent families.

For each family, the number of subgroups of type $Z_2 \times Z_2$ are listed in Table 2. In the same table, we list the number of these subgroups up to conjugacy and the resulting number of nonisomorphic elliptic quotients [CGLR99], [CQ02], [SV04]. For each family, all the numbers in Table 2 follow immediately from the properties of the group G. The upper bound 2 for the number of nonisomorphic elliptic quotients is established in a different way in [GS01]. There all elliptic quotients for a given Rosenhain form are computed and compared. The proof of [GS01, Theorem 11] misrepresents the involution τ_1 which is confusing but does not harm

Table 2. Enumeration of Subgroups of Type $Z_2 \times Z_2$.

Family	G	Number of Subgps	Number of Subgps up to conjugacy	Number of nonisomorphic elliptic quotients
(1)	V_4	1	1	2
(2)	D_{12}	3	1	2
(3)	D_8	2	2	2
(4)	$Z_3 \rtimes D_8$	4	2	2
(5)	$GL_2(3)$	6	1	1
(6)	Z_{10}	0	0	0

the main point of the proof (a choice such that $\{1, \tau_1, \tau_2, \tau_3, \rho_1, \rho_2\} = S_3$ would lead to $\Lambda_1 = \Lambda_2 = \Lambda_3$, whereas the proof arrives at $\Lambda_1 \neq \Lambda_2 = \Lambda_3$).

To each pair of a curve and a subgroup $Z_2 \times Z_2$ up to conjugacy corresponds a unique pair of invariants (u, v) (Theorem 3). The moduli spaces of invariants (u, v) associated to each family are [SV04]:

(1) $\{(u, v) : \Delta = u^2 - 4v + 18u - 27 \neq 0\}$.
(2) $\{(u, v) : \Delta \neq 0$ and $4v - u^2 + 110u - 1125 = 0\}$.
(3) $\{(u, v) : \Delta \neq 0$ and $v^2 = 4u^3\}$.
(4) $\{(0, 0), (15^2, 2 \cdot 15^3)\}$.
(5) $\{(5^2, -2 \cdot 5^3)\}$.
(6) the curve has no elliptic involutions

For a curve in family (1) or (2) there is a unique pair (u, v), that corresponds to a decomposition of the Jacobian $J \sim E_1 \times E_2$. For a curve in family (2) the two elliptic quotients E_1 and E_2 are 3-isogenous [GS01]. For a curve in family (3) or (4) there are two pairs (u, v) that give decompositions of the Jacobian $J \sim E_1^2$ and $J \sim E_2^2$, respectively. The two elliptic quotients E_1 and E_2 are $2-$isogenous [Gey74]. For the curve (4), the point $(15^2, 2 \cdot 15^3)$ corresponds to a subgroup $Z_2 \times Z_2$ of both D_8 and D_{12} whereas $(0, 0)$ corresponds to a subgroup of D_8 but not of D_{12} (see also Remark 2). The curve (5) has up to conjugacy a single subgroup $Z_2 \times Z_2$ that is therefore contained in both D_8 and D_{12}.

4.2 A Suitable Class of Genus Two Curves

The curves belonging to the family (2) in Igusa's classification are characterized by a reduced automorphism $x \mapsto -1/x+1$ of order three acting as $(\infty 10)(\lambda\mu\nu)$ on the Weierstrass points. After a suitable fractional transformation, the action on the Weierstrass points diagonilizes and a curve in family (2) can be written as

$$y^2 = x^6 - ax^3 + 1, \quad \text{for} \quad a^2 = \frac{(1+\lambda)^2\,(2-\lambda)^2\,(1-2\,\lambda)^2}{\left(1-\lambda+\lambda^2\right)^3}. \tag{5}$$

With j the $j-$invariant of the elliptic curve $y^2 = x(x-1)(x-\lambda)$ in Legendre form, we can write $a^2 = 4(j-1728)/j$. Curves of the given form arise if we scale

$$y^2 = (x^3 - r^2)(x^3 - s^2), \tag{6}$$

over a field containing a cube root of rs, to

$$y^2 = (x^3 - r/s)(x^3 - s/r) = x^6 - ax^3 + 1, \quad \text{for} \quad a = \frac{r^2+s^2}{rs}.$$

In [CGLR99], curves in the family (2) have a normalized form $y^2 = x^6 + x^3 + t$ where t is uniquely determined by the isomorphism class of the curve. The curves in (5) have $t = 1/a^2$. To apply results obtained in [SV04] for the model

$$y^2 = c_3x^6 + c_2x^4 + c_1x^2 + c_0,$$

we use a substitution $x = (x+1)/(x-1), y = y/(x-1)^3$ to transform (5) into

$$y^2 = (2-a)x^6 + (30+3a)x^4 + (30-3a)x^2 + (2+a).$$

This yields a parametrization

$$u = \frac{c_2c_1}{c_3c_0} = 9\frac{a^2-100}{a^2-4}, \quad v = \frac{c_2^3c_0 + c_1^3c_3}{c_3^2c_0^2} = 54\frac{a^4+360a^2+2000}{(a^2-4)^2},$$

for the equation $4v - u^2 + 110u - 1125 = 0$ of the moduli (u,v) in family (2).

The elliptic quotients of a curve in family (2) are $3-$isogenous. We determine the $3-$isogeny explicitly when the curve is of the from (5). In general, an elliptic curve with a stable torsion subgroup of order three has a model over the base field

$$E : y^2 = x^3 + d(3ax + b)^2. \tag{7}$$

The line $x = 0$ intersects the curve in a stable $3-$torsion subgroup $T = \{\mathcal{O}, (0, +b\sqrt{d}), (0, -b\sqrt{d})\}$. An isogeny defined on E preserves the differential dx/y and is of the form $(x, y) \mapsto (R(x), cR'(x)y)$ [Sil94]. The $3-$isogeny $\phi : E \longrightarrow E_0$ with kernel T onto an elliptic curve E_0 of the form (7) is easily and uniquely determined by requiring that $R(x)$ vanishes on the full $3-$torsion, that is on the zeros of the Hessian of the curve. We find that

$$\phi = (x(y^2 + 3d(ax + b)^2) : y(y^2 - 9d(ax + b)^2) : x^3),$$
$$E_0 : y^2 = x^3 - 3d(3ax + 3b - 12a^3d)^2.$$

Over a field containing $\sqrt{d}$, the model for E scales to $d = 1, a = 1, b = b/(da^3)$. Over a field containing $\sqrt{-3d}$, we can write E_0 as in (7) with $d_0 = 1, a_0 = 1, b_0 = (3b - 12a^3d)/(-3da^3) = 4 - b/(da^3)$.

In particular, we see that the two elliptic curves

$$E_1 : y^2 = x^3 + (3x + 2 + a)^2, \quad E_2 : y^2 = x^3 + (3x + 2 - a)^2$$

are $3-$isogenous over a field containing $\sqrt{-3}$. They are quotients of the curve $y^2 = x^6 - ax^3 + 1$ for the involutions $(x, y) \mapsto (1/x, y/x^3)$ and $(x, y) \mapsto (1/x, -y/x^3)$, respectively. The corresponding quotient maps are given by

$$(x, y) \mapsto \left(-\frac{(2 + a)x}{(x + 1)^2}, \frac{(2 + a)y}{(x + 1)^3}\right) \in E_1,$$
$$(x, y) \mapsto \left(\frac{(2 - a)x}{(x - 1)^2}, \frac{(2 - a)y}{(x - 1)^3}\right) \in E_2.$$

For the various representations of the hyperelliptic curves in the family (2), one can find expressions for the $j-$invariants of the elliptic quotients in [CGLR99], [CQ02], [GS01], [SV04]. In each case, verification that the elliptic quotients are $3-$isogenous is straightforward. The modular equation $\Phi_3(j, j_0)$ vanishes if and only if j and j_0 are $3-$isogenous. Klein [Kle21] gives a useful description of the modular equation of level three using resolvents. Let $\psi : X_0(3) \longrightarrow X(1)$,

$$j = \psi(\eta) = 27\frac{\eta(\eta + 8)^3}{(\eta - 1)^3}.$$

Then $j = \psi(\eta)$ and $j_0 = \psi(\eta_0)$ are 3−isogenous whenever $(\eta - 1)(\eta_0 - 1) = 1$ [Coh94]. In fact, for η, η_0 such that $(\eta - 1)(\eta_0 - 1) = 1$, the curves

$$E : y^2 = x^3 + (3x + 4/\eta)^2 \quad \text{and} \qquad E_0 : y^2 = x^3 + (3x + 4/\eta_0)^2$$

are 3−isogenous and have j−invariants $j = \psi(\eta)$ and $j_0 = \psi(\eta_0)$.

Lemma 1. *The Jacobian of the hyperelliptic curve*

$$C : y^2 = x^6 - ax^3 + 1$$

is isogenous to a product of elliptic curves E_1 and E_2,

$$\begin{aligned} E_1 &: y^2 = x^3 + (3x + 2 + a)^2, \\ E_2 &: y^2 = x^3 + (3x + 2 - a)^2, \end{aligned}$$

with j-invariants

$$\begin{aligned} j_1 &= \psi(\frac{4}{2+a}) = 4 \cdot 1728 \, \frac{(5 + 2a)^3}{(2 + a)(2 - a)^3}, \\ j_2 &= \psi(\frac{4}{2-a}) = 4 \cdot 1728 \, \frac{(5 - 2a)^3}{(2 - a)(2 + a)^3}. \end{aligned}$$

5 Vector Decomposition Problem on Genus Two Curves

In this section we will show that the genus two curves of Lemma 1 are indeed suitable for VDP. We consider the curves over a field of characteristic $p \equiv 2 \pmod 3$ and we assume that $a^2 \in \mathbb{F}_p$. First we consider the case that E_1 and E_2 are defined over $\mathbb{F}_p$ ($a \in \mathbb{F}_p$), then separately the case that E_1 and E_2 are defined over $\mathbb{F}_{p^2}$ but conjugate over $\mathbb{F}_p$ ($a \notin \mathbb{F}_p$). In the latter case, choosing -3 as a fixed nonresidue in $\mathbb{F}_p$, the curves have an equation $C' : y^2 = x^6 - (a/\sqrt{-3})x^3 + 1$ over $\mathbb{F}_{p^2}$, and a model $C : y^2 = x^6 - ax^3 - 3$ over $\mathbb{F}_p$.

5.1 Vector Decomposition Problem on Curves of the form $C : y^2 = x^6 - ax^3 + 1$

Lemma 1 of Section 4 describes the Jacobian of the curves up to isogeny as a product of two elliptic curves E_1 and E_2. The elliptic curves E_1 and E_2 are 3−isogenous over an extension field that contains the third roots of unity. Over the extension field, both E_1 and E_2 have the same number of points. The setup for the VDP is now as follows.

We choose $C : y^2 = X^6 - ax^3 + 1$ such that E_1 has a large cyclic subgroup $\mathbb{Z}/m\mathbb{Z}$ of rational points over $\mathbb{F}_p$, for $p \equiv 2 \pmod 3$. Then we choose as two-dimensional vector space $\mathcal{V}$ the m-torsion $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ in the Jacobian of the hyperelliptic curve C over the extension field $\mathbb{F}_{p^2}$. And we choose as one-dimensional subspace $\mathcal{V}'$ the subspace $\mathbb{Z}/m\mathbb{Z}$ of $\mathcal{V}$ that is rational over $\mathbb{F}_p$.

Notation 2.

$$\begin{aligned} &p : \text{ a prime with } p \equiv 2 \pmod 3,\\ &C : \ y^2 = x^6 - ax^3 + 1, \text{ a curve with } a \in \mathbb{F}_p,\\ &\mathrm{Jac}(C) : \text{ Jacobian of the curve C},\\ &\mathcal{V} = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \subset \mathrm{Jac}(C)(\mathbb{F}_{p^2}),\\ &\mathcal{V}' = \mathbb{Z}/m\mathbb{Z} \subset \mathrm{Jac}(C)(\mathbb{F}_p). \end{aligned}$$

Let $\omega, \bar{\omega}$ be primitive third roots of unity, and let

$$\begin{aligned} &\phi : (x, y) \mapsto (\omega x, y), \quad \bar{\phi} : (x, y) \mapsto (\bar{\omega} x, y),\\ &F : (x, y) \mapsto (x^p, y^p),\\ &\sigma : (x, y) \mapsto (x^{-1}, yx^{-3}). \end{aligned}$$

Lemma 2. *For any element $e \in Jac(C)(\overline{\mathbb{F}}_p)$,*

$$\phi(\phi(e)) = -e - \phi(e),$$

and

$$F(\phi(e)) = -F(e) - \phi(F(e)).$$

Proof. The map $\phi^2 + \phi + 1$ is the trace map onto the Jacobian of the quotient curve $C/\langle\phi\rangle$. But $C/\langle\phi\rangle$ is the curve $y^2 = x^2 - ax + 1$ which has trivial Jacobian. Thus $\phi^2 + \phi + 1$ is the zero map.
For the second claim, we need that $\phi^2 \circ F = F \circ \phi$. But this is clear, since for $p \equiv 2 \pmod 3$ both sides map $(x, y) \mapsto (\omega^2 x^p, y^p)$.

Lemma 3. *For an element $e \in Jac(C)(\mathbb{F}_p)$ of prime order $m > 3$,*

$$\langle e, \phi(e)\rangle \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Proof. Since ϕ is an automorphism of C, the elements e and $\phi(e)$ have the same order in the Jacobian of C. And it suffices to show that $\phi(e) \notin \langle e\rangle$. Assume to the contrary that $\phi(e) = \lambda e$, and thus in particular $\phi(e) \in \mathrm{Jac}(C)(\mathbb{F}_p)$. The previous lemma yields $\lambda^2 e = -e - \lambda e$ and $\lambda e = -e - \lambda e$. But then $0 = (2\lambda + 1)(2\lambda + 1)e = (-4 - 4\lambda + 4\lambda + 1)e = -3e$, which contradicts $m > 3$.

The family of the curves $C : y^2 = x^6 - ax^3 + 1$ with the linear maps F and ϕ of Notation 2 fulfill the requirement of Theorem 1.

Theorem 4. *Let $C : y^2 = x^6 - ax^3 + 1$ be a hyperelliptic curve, and let $\mathcal{V}$ and $\mathcal{V}'$ be vector spaces of dimensions two and one, respectively, as in Notation 2. For any $e \in \mathcal{V}'$ with $3e \neq 0$, the two-dimensional vector space $\mathcal{V}$ has a basis $\{e, \phi(e)\}$ such that the following holds,*

$$F(e) = e,$$

$$F(\phi(e)) = -e - \phi(e).$$

The VDP on $\mathcal{V}$, with respect to the basis $\{e, \psi(e)\}$, is at least as hard as the computational Diffie-Hellman problem in $\mathcal{V}'$: given (e, ae, be) compute abe. If $\mathcal{V}'$ is chosen to be of prime order then it can be identified with a subgroup of $E_1(\mathbb{F}_p)$ or $E_2(\mathbb{F}_p)$.

Proof. Lemma 3 gives that $\{e, \phi(e)\}$ forms a basis. The other properties follow from Lemma 2 and the fact that e is $\mathbb{F}_p$-rational. The claim that these curves are indeed suitable for VDP follows from Theorem 1, in particular from the special case treated in Example 1. To investigate the one-dimensional vector space $\mathcal{V}'$, let $E_1 = \mathrm{Jac}(C)/\langle\sigma\rangle$, $E_2 = \mathrm{Jac}(C)/\langle-\sigma\rangle$. Multiplication by 2 on $\mathrm{Jac}(C)$ factors as

$$\begin{array}{ll} \mathrm{Jac}(C) \longrightarrow E_1 \times E_2, & P \mapsto (P_1, P_2) = (P + \sigma P, P - \sigma P). \\ E_1 \times E_2 \longrightarrow \mathrm{Jac}(C), & (P_1, P_2) \mapsto (P_1 + P_2) = 2P. \end{array} \tag{8}$$

Since both morphisms are defined over $\mathbb{F}_p$, it is clear that a subgroup of prime order in $\mathrm{Jac}(\mathbb{F}_p)$ can be identified with a subgroup of $E_1(\mathbb{F}_p)$ or $E_2(\mathbb{F}_p)$. □

The factorization in the proof of Theorem 4 extends to a commutative diagram of subgroups of $\mathrm{Jac}(\mathbb{F}_p^2)$.

$$\begin{tikzcd}
\mathrm{Jac}(\mathbb{F}_p) \arrow[r] \arrow[d] & E_1(\mathbb{F}_p) \times E_2(\mathbb{F}_p) \arrow[r] \arrow[d] & \mathrm{Jac}(\mathbb{F}_p) \arrow[d] \\
E_1(\mathbb{F}_{p^2}) \arrow[r] & E_1(\mathbb{F}_p) \times E_2(\mathbb{F}_p) \arrow[r] & \mathrm{Jac}(\mathbb{F}_p)
\end{tikzcd}$$

$$\begin{tikzcd}
P \arrow[r] \arrow[d] & (P_1, P_2) \arrow[r] \arrow[d] & 2P \arrow[d] \\
Q \arrow[r] & (Q_1, Q_2) \arrow[r] & -6P
\end{tikzcd}$$

For $P \in \mathrm{Jac}(C)(\mathbb{F}_p)$, let $Q = \phi P + \sigma\phi P \in E_1(\mathbb{F}_{p^2})$, and let

$$\begin{aligned} Q_1 &= Q + F(Q), \\ Q_2 &= (\phi - \bar{\phi})Q + F((\phi - \bar{\phi})Q). \end{aligned}$$

It follows from

$$F(\phi P) = \bar{\phi} P, \qquad F(\sigma\phi P) = \phi\sigma P,$$

and Lemma 2 that

$$\begin{aligned} Q_1 &= -P - \sigma(P) = -P_1 \in E_1(\mathbb{F}_p), \\ Q_2 &= -3P + 3\sigma P = -3P_2 \in E_2(\mathbb{F}_p). \end{aligned}$$

And the diagram commutes.

We have shown that genus two curves of the form $y^2 = x^6 - ax^3 + 1$ satisfy the requirements of Theorem 1 and can be considered for the vector decomposition problem. The implication of Theorem 1 is that the VDP in the Jacobian of such a curve is at least as hard as the CDHP on the elliptic curve E_1 that appears in its decomposition $\mathrm{Jac}(C) \sim E_1 \times E_2$. However, we saw that $\mathcal{V}'$ is a subgroup of $E_1(\mathbb{F}_p)$ and we do not benefit from the full size of $\mathrm{Jac}(\mathbb{F}_p)$. This is of course undesirable because even though we pay the price of computing in $\mathrm{Jac}(\mathbb{F}_p)$, the security is only proportional to the size of the points on $E_1(\mathbb{F}_p)$.

5.2 Vector Decomposition Problem on Curves of the form $C : y^2 = x^6 - ax^3 - 3$

In section 5.1 we saw that although the curves of form $C : y^2 = x^6 - ax^3 + 1$ are suitable for VDP, the computations for VDP are done in $\mathrm{Jac}(\mathbb{F}_p)$ while they are only as secure as the CDHP on the elliptic curve $E_1(\mathbb{F}_p)$. In this section we consider another class of genus two curves that do not have this problem. For $p \equiv 2 \pmod 3$, let $-3 \in \mathbb{F}_p$ be a fixed nonsquare. Any curve with equation $y^2 = x^6 + Ax^3 + B$ over $\mathbb{F}_p$, with B a nonsquare, is isomorphic over $\mathbb{F}_p$ to a curve $C : y^2 = x^6 - ax^3 - 3$ and isomorphic over $\mathbb{F}_{p^2}$ to a curve $C' : y^2 = x^6 - (a/\sqrt{-3})x^3 + 1$.

Notation 3.

$$\begin{aligned}
&p: \text{ a prime with } p \equiv 2 \pmod 3,\\
&C:\ y^2 = x^6 - ax^3 - 3, \text{ a curve with } a \in \mathbb{F}_p,\\
&\mathrm{Jac}(C): \text{ Jacobian of the curve C},\\
&\mathcal{V} = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \subset \mathrm{Jac}(C)(\mathbb{F}_{p^2}),\\
&\mathcal{V}' = \mathbb{Z}/m\mathbb{Z} \subset \mathrm{Jac}(C)(\mathbb{F}_p).
\end{aligned}$$

Define morphisms $\phi, \bar{\phi}, F$ as before. In particular Lemma 2 and Lemma 3 still hold. But, for $\beta^6 = -3, \beta^2 \in \mathbb{F}_p$, define

$$\begin{aligned}
&\phi : (x, y) \mapsto (\omega x, y), \quad \bar{\phi} : (x, y) \mapsto (\bar{\omega} x, y),\\
&F : (x, y) \mapsto (x^p, y^p),\\
&\sigma : (x, y) \mapsto (\frac{\beta^2}{x}, \frac{\beta^3 y}{x^3}).
\end{aligned}$$

Theorem 5. *Let $C : y^2 = x^6 - ax^3 - 3$ be a hyperelliptic curve, and let $\mathcal{V}$ and $\mathcal{V}'$ be vector spaces of dimensions two and one, respectively, as in Notation 3. For any $e \in \mathcal{V}'$ with $3e \neq 0$, the two-dimensional vector space $\mathcal{V}$ has a basis $\{e, \phi(e)\}$ such that the following holds,*

$$F(e) = e,$$

$$F(\phi(e)) = -e - \phi(e).$$

The VDP on $\mathcal{V}$, with respect to the basis $\{e, \phi(e)\}$, is at least as hard as the computational Diffie-Hellman problem in $\mathcal{V}'$: given (e, ae, be) compute abe.

Proof. The proof of theorem 4 still holds.

Note that $\mathcal{V}'$ in general is not a subgroup of $E_1(\mathbb{F}_p)$. With $E_1 = \mathrm{Jac}(C)/\langle\sigma\rangle$ and $E_2 = \mathrm{Jac}(C)/\langle-\sigma\rangle$, multiplication by 2 on $\mathrm{Jac}(C)$ factors as in (8). The quotients E_1 and E_2 are in general defined over $\mathbb{F}_{p^2}$ but not over $\mathbb{F}_p$. For $P \in \mathrm{Jac}(C)(\mathbb{F}_p)$, let $Q = \phi P + \sigma\phi P \in E_1(\mathbb{F}_{p^2})$. We have

$$F(\phi P) = \bar{\phi} P, \qquad F(\sigma\phi P) = -\phi\sigma P.$$

Thus, for $\bar{Q} = F(Q)$,

$$Q = \phi P + \bar{\phi}\sigma P, \quad \bar{Q} = \bar{\phi} P - \phi\sigma P.$$

Finally, with Lemma 2, $P = -\phi Q - \bar{\phi}\bar{Q}$. So that the groups $\mathrm{Jac}(C)(\mathbb{F}_p)$ and $E_1(\mathbb{F}_{p^2})$ are isomorphic.

$$\begin{tikzcd}
\mathrm{Jac}(\mathbb{F}_p) \arrow[r] & E_1(\mathbb{F}_{p^2}) \arrow[r] & \mathrm{Jac}(\mathbb{F}_p) \\
P \arrow[r] & Q \arrow[r] & (-\phi Q - \bar{\phi} F Q) = P
\end{tikzcd}$$

Since E_1 is in general not defined over $\mathbb{F}_p$, it is possible for a suitable choice of curve $C:\ y^2 = x^6 - ax^3 - 3$, to find $\mathcal{V}'$ of large prime order and of small index in $E_1(\mathbb{F}_{p^2})$.

6 Conclusion

Yoshida proved Theorem 1 that guarantees the intractability of the vector decomposition problem for a two-dimensional vector space. In this work we prove that if the group of m-torsion points on an elliptic curve is chosen as the two-dimensional vector space, then the conditions of the theorem force the curve to be supersingular.

Moreover, we consider the VDP on the Jacobian variety of curves of higher genus, for which the conditions of the theorem turn out to be less restrictive. We introduce a family of hyperelliptic curves of genus two for which the VDP is at least as hard as the Diffie-Hellman problem on a general elliptic curve.

References

[BSS00] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic curves in cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000. Reprint of the 1999 original.

[CF96] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus* 2, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.

[CGLR99] G. Cardona, J. González, J. C. Lario, and A. Rio. On curves of genus 2 with Jacobian of GL_2-type. *Manuscripta Math.*, 98(1):37–54, 1999.

[Coh94] Harvey Cohn. *Introduction to the construction of class fields*. Dover Publications Inc., New York, 1994. Corrected reprint of the 1985 original.

[CQ02] G. Cardona and J. Quer. Curves of genus 2 with group of automorphisms isomorphic to d8 or d12. February 2002. Preprint.

[FMR99] G. Frey, M. Müller, and H. Rück. The tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. *IEEE Trans. Info. Theory*, 45:203–209, 1999.

[FR94] G. Frey and H. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp*, 62:865–874, 1994.

[Gey74] W. D. Geyer. Invarianten binärer Formen. In *Classification of algebraic varieties and compact complex manifolds*, pages 36–69. Lecture Notes in Math., Vol. 412. Springer, Berlin, 1974.

[GS01] P. Gaudry and É. Schost. On the invariants of the quotients of the Jacobian of a curve of genus 2. In *Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001)*, volume 2227 of *Lecture Notes in Comput. Sci.*, pages 373–386. Springer, Berlin, 2001.

[Igu60] Jun-ichi Igusa. Arithmetic variety of moduli for genus two. *Ann. of Math. (2)*, 72:612–649, 1960.

[Kle21] F. Klein. *Gesammelte mathematische Abhandlungen*, volume 3. Springer, 1921.

[KR89] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Math. Ann.*, 284(2):307–327, 1989.

[MOV93] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39(5):1639–1646, 1993.

[Sil99] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 199? Corrected reprint of the 1986 original.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[SV04] Tanush Shaska and Helmut Völklein. Elliptic subfields and automorphisms of genus 2 function fields. In *Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000)*, pages 703–723. Springer, Berlin, 2004.

[YMF02] M. Yoshida, S. Mitsunari, and T. Fujiwara. Inseprable multiplex transmision scheme using the pairing on elliptic curves. In *ISEC 2002*. 2002.

[YMF03] M. Yoshida, S. Mitsunari, and T. Fujiwara. Vector decomposition problem and the trapdoor inseparable multiplex transmission scheme based the problem. In *SCIC'03*. 2003.

[Yos03] M. Yoshida. Inseprable multiplex transmision using the pairing on elliptic curves and its application to watermarking. In *Fourth Conference on Algebraic Geometry, Number Theory, Coding Theory and Cryptography*. Graduate School of Mathematical Sciences, University of Tokyo, 2003.