Bull. Korean Math. Soc. **46** (2009), No. 2, pp. 245–253
DOI 10.4134/BKMS.2009.46.2.245

ANALYSIS OF THE STRONG INSTANCE FOR THE VECTOR DECOMPOSITION PROBLEM

Saeran Kwon and Hyang-Sook Lee

Abstract. A new hard problem called the vector decomposition problem (VDP) was recently proposed by Yoshida et al., and it was asserted that the VDP is at least as hard as the computational Diffie-Hellman problem (CDHP) under certain conditions. Kwon and Lee showed that the VDP can be solved in polynomial time in the length of the input for a certain basis even if it satisfies Yoshida's conditions. Extending our previous result, we provide the general condition of the weak instance for the VDP in this paper. However, when the VDP is practically used in cryptographic protocols, a basis of the vector space $\mathcal{V}$ is randomly chosen and publicly known assuming that the VDP with respect to the given basis is hard for a random vector. Thus we suggest the type of strong bases on which the VDP can serve as an intractable problem in cryptographic protocols, and prove that the VDP with respect to such bases is difficult for any random vector in $\mathcal{V}$.

1. Introduction

Yoshida et al. [7, 8] proposed a new computational hard problem on two dimensional vector space over a finite field so called the vector decomposition problem (VDP), and gave some applications including an inseparable multiplex transmission scheme. The computational Diffie-Hellman problem (CDHP) is generally believed to be a mathematically hard problem which can not be solved in polynomial time in the length of the input. In [7, 8], Yoshida showed that the VDP on two dimensional vector space over a finite field is at least as hard as the CDHP on its one dimensional subspace under some sufficient conditions. The existence of two dimensional vector space satisfying the sufficient conditions was illustrated over the full group of m-torsion points for a prime m on an elliptic curve, which is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Duursma and Kiyavash [1, 2] showed that if the group of m-torsion points on an elliptic curve is chosen as a

Received April 29, 2008.
2000 *Mathematics Subject Classification.* 94A60, 11T71.
Key words and phrases. vector decomposition problem, strong instance, computational Diffie-Hellman problem.
The second author was supported by Korea Research Foundation, grant number KRF-2006-0117.

vector space for the VDP satisfying the sufficient conditions, then the curve is bound to be supersingular. They also proposed a family of hyperelliptic curves of genus two satisfying the sufficient conditions, which are hence applicable for the VDP as non-supersingular curves.

Yoshida [7, 8] claimed the hardness of the VDP by showing that one can solve the CDHP for a random instance in the underlying one-dimensional subspace by calling the VDP oracle in twice where the VDP oracle is a simulator of an algorithm solving the VDP. Since the CDHP is believed to be hard until now, we can observe that the VDP for random instances is not always tractable, which shows the existence of a hard instance in VDP. However for the cryptographic system based on the VDP underlying a randomly chosen basis, it is not clear whether the VDP for any random vector under the chosen basis is hard. Accordingly, this result leads to the question when the VDP for a random instance chosen in the set of random bases and random vectors is intractable. In [5], we showed that even if the two-dimensional vector space satisfies the sufficient conditions, the VDP can be solved under some basis. In particular, the VDP under the chosen basis in Theorem 4 of [2], although it was asserted to be a hard VDP-instance, can be solved in polynomial time from the argument discussed in [5].

In this paper we provide the general condition of the weak instance for the VDP. When the VDP is practically used in cryptographic protocols, a basis of the vector space $\mathcal{V}$ is chosen and publicly known assuming that the VDP with respect to the given basis is hard for a random vector. Thus we propose the type of strong bases on which the VDP can serve as an intractable problem in useful cryptographic protocols, and prove that the VDP with respect to such bases is difficult for any random vector in $\mathcal{V}$.

Our paper is organized as follows. In Section 2, we review the properties of the vector decomposition problem. In Section 3, we provide the general condition of weak instances which makes the VDP feasible. In Section 4, we also suggest the type of strong bases of vector spaces on which the VDP can serve as a difficult problem in cryptographic protocols and prove that the VDP relative to such bases is hard for any random vector. Finally we give the conclusions in Section 5.

2. Definitions and analysis of the VDP

In this section, we review the definitions of the VDP, CDHP and some results on the VDP in [2, 8]. We note that $\mathbb{F}$ denotes a finite field, $\mathcal{V}$ a two-dimensional $\mathbb{F}$-vector space and $\mathcal{V}'$ a one-dimensional subspace of $\mathcal{V}$. For $v \in \mathcal{V}$, $\langle v \rangle$ denotes the set $\{av \mid a \in \mathbb{F}\}$.

Definition 2.1. *The vector decomposition problem* (VDP) *on* $\mathcal{V}$*,* a two-dimensional vector space over $\mathbb{F}$, is as follows: Given $e_1, e_2, v \in \mathcal{V}$ such that $\{e_1, e_2\}$ is an $\mathbb{F}$-basis for $\mathcal{V}$ and v is a randomly chosen vector in $\mathcal{V}$, find the vector $u \in \mathcal{V}$ such that $u \in \langle e_1 \rangle$ and $v - u \in \langle e_2 \rangle$.

If assuming a VDP oracle, a simulator of an algorithm solving the VDP, is given, we use the notation $VDP(e_1, e_2, v) = u$ to indicate that the VDP oracle gives an answer u for an instance (e_1, e_2, v). In particular, for the VDP relative to a chosen basis $\{e_1, e_2\}$, we may denote it by $VDP_{(e_1,e_2)}(v) = u$.

Definition 2.2. *The computational Diffie-Hellman problem* (CDHP) *on* $\mathcal{V}'$, a one-dimensional vector space over $\mathbb{F}$: Given $e \in \mathcal{V}'/\{0\}$ and $ae,\ be \in \langle e \rangle$ for a, b chosen at random in $\mathbb{F}$, find $abe \in \langle e \rangle$.

The following theorem in [7, 8] states that the CDHP is reducible to the VDP under certain conditions. We will call the conditions as Yoshida conditions.

Theorem 2.3 ([7, 8])**.** *The Vector Decomposition Problem on* $\mathcal{V}$ *is at least as hard as the computational Diffie-Hellman 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* $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}$ *such that* $\alpha_1 \cdot \alpha_2 \cdot \alpha_3 \neq 0$ *satisfying*

$$\begin{aligned} F_e(e) &= \alpha_1 e, \\ F_e(\phi_e(e)) &= \alpha_2 e + \alpha_3 \phi_e(e). \end{aligned} \tag{1}$$

The elements α_1, α_2, α_3 *and their inverses can be calculated in polynomial time.*

In order to show their proof briefly, we review the proof of the Theorem 2.3 only for the case $(\alpha_3 - \alpha_1)a \neq 1$ without loss of generality, given an input (e, ae, be) of the CDHP. For details, refer to [2, 7, 8].

Proof. For (e, ae, be), an input of the CDHP, abe can be computed by applying the VDP oracle twice as follows: Let

$$e_1 = ae + \phi_e\left({\alpha_2}^{-1}(\alpha_3 - \alpha_1)ae - {\alpha_2}^{-1}e\right) = ae + \lambda\phi_e(e),$$

where $\lambda = \alpha_2^{-1}(\alpha_3 - \alpha_1)a - {\alpha_2}^{-1}$. And let $e_2 = F_e(e_1)$, so that $e_2 = \alpha_1 ae + \lambda(\alpha_2 e + \alpha_3\phi_e(e)) = (\alpha_1 a + \lambda\alpha_2)e + \lambda\alpha_3\phi_e(e) = (\alpha_3 a - 1)e + \lambda\alpha_3\phi_e(e)$. Then $VDP(e_1, e_2,\ be)$ gives component $\alpha_3 be_1$ along e_1 of the vector be, since $\alpha_3 e_1 - e_2 = e$. Multiplying $\alpha_3 be_1$ by α_3^{-1}, then be_1 is obtained. Finally, $VDP(e, \phi_e(e),\ be_1)$ gives component abe along e of the vector be_1 since $e_1 = ae + \lambda\phi_e(e)$. □

The main idea of the proof of Theorem 2.3 is as follows: The CDHP for a random instance (e, ae, be) in the underlying one-dimensional subspace can be solved in polynomial time by calling twice the VDP oracle for the instances $(e_1, e_2,\ be)$, $(e, \phi_e(e),\ be_1)$ sequentially, if both $VDP(e_1, e_2,\ be)$ and $VDP(e, \phi_e(e),\ be_1)$ are computed in polynomial time. In fact, the CDHP is known to be a hard problem. Thus we can observe that at least one of $VDP(e_1, e_2,\ be)$ and $VDP(e, \phi_e(e),\ be_1)$ is not computed in polynomial time.

This result does not show that the VDP is hard for any random basis and any random vector as described in the definition of the VDP. In fact, over the following curve satisfying the sufficient conditions provided in [7, 8], $(e, \phi_e(e),\ be_1)$ is actually a weak instance for the VDP, that is, $VDP(e, \phi_e(e),\ be_1)$ can be computed in polynomial time [5].

Yoshida et al. [7, 8] proposed an elliptic curve $E : y^2 = x^3 - a,\ a \in \mathbb{F}_p,\ p \equiv 2 \pmod 3$ as an example of a two-dimensional vector space $\mathcal{V}$ over $\mathbb{F}_p$ and a one-dimensional subspace $\mathcal{V}'$ of $\mathcal{V}$, choosing $\mathcal{V} = E[m]$, the group of m-torsion points on E, and $\mathcal{V}' = E(\mathbb{F}_p) \cap E[m]$, where m is a prime such that $6m = p + 1$. The linear maps defined on $\mathcal{V}$: the map $\phi(x,\ y) = (\xi x,\ y)$, where $\xi^2 + \xi + 1 = 0$, and the Frobenius map $F(x,\ y) = (x^p,\ y^p)$, satisfy the Yoshida conditions. That is, for any $e \in \mathcal{V}'$,

(i) $\phi(e) \in E[m],\ \ \phi(e) \notin \langle e \rangle$,
(ii) $F(e) = e \quad \text{and} \quad F(\phi(e)) = -e - \phi(e)$,

which says that the set $\{e,\ \phi(e)\}$ is an $\mathbb{F}_p$-basis of $\mathcal{V}$, and $\alpha_1 = 1, \alpha_2 = \alpha_3 = -1$.

Duursma and Kibayashi [2] showed elliptic curves satisfying the Yoshida conditions should be supersingular. Since the CDHP defined over supersingular curves has been known as a subexponential problem by either MOV attack [6] or Frey-Rück attack [4], they suggested two ordinary hyperelliptic curves, $C_1 : y^2 = x^6 - ax^3 + 1$ and $C_2 : y^2 = x^6 - ax^3 - 3$ defined over $\mathbb{F}_p, p \equiv 2 \pmod 3$, choosing 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 each of the curves C_1, C_2 over the field $\mathbb{F}_{p^2}$, and as one-dimensional subspace $\mathcal{V}'$ the subspace $\mathbb{Z}/m\mathbb{Z}$ of $\mathcal{V}$ that is rational over $\mathbb{F}_p$. On the two-dimensional vector space $\mathcal{V}$ of these curves, they also defined the isomorphisms F and ϕ as $F(x, y) = (x^p, y^p)$ and $\phi(x, y) = (\omega x, y)$, where ω is a primitive third root of unity, and these isomorphisms satisfy the Yoshida conditions:

$$F(e) = e \ \text{ and } \ F(\phi(e)) = -e - \phi(e) \quad \text{for any element } e \in \mathcal{V}'.$$

In addition, on the curves C_1 and C_2, the relation $\phi^2(e) = -e - \phi(e)$ is satisfied for any $e \in \mathcal{V}'$. Theorem 4 and Theorem 5 in [2] respectively describe that the VDP on C_1 and the VDP on C_2 with respect to the basis $\{e, \phi(e)\}$ are as hard as the CDHP.

However, in the next section, we show that $\mathrm{VDP}_{(e,\phi(e))}(v)$ for any $v \in \mathcal{V}$ is solvable in polynomial time on the above curves C_1 and C_2 by the similar method with the argument in [5]. Especially, we show that $(e, \phi(e), v)$ for any $v \in \mathcal{V}$ is a weak instance under more general conditions for $\alpha_1, \alpha_2, \alpha_3$ and the characteristic polynomial of ϕ.

3. Weak instances

Theorem 2.3 shows that there exists an instance which makes the VDP as hard as the CDHP. However, this does not imply the VDP for a random vector relative to a chosen basis is difficult. In [5], we showed that the VDP for the instance $(e, \phi(e), v)$ with a random vector $v \in \mathcal{V}$ is solved in polynomial time on

the vector space $\mathcal{V} = \langle e, \phi(e)\rangle$ defined over curves which have been suggested in [7, 8]. We generalize this result to the Jacobian of an algebraic curve.

Proposition 3.1. *Let J_C be the Jacobian of an algebraic curve C with genus g over a finite field $\mathbb{F}_q$ whose characteristic is a prime p. Let $\mathcal{V}$ be a two-dimensional subspace of m-torsion divisors of J_C over $\mathbb{F}_{p^2}$, where m is a prime with $m > 3$, $\gcd(q, m) = 1$, and $\mathcal{V}'$ a one-dimensional subspace of $\mathcal{V}$ that is rational over $\mathbb{F}_p$. If linear isomorphisms on $\mathcal{V}$, F and ϕ, satisfy Yoshida conditions as followings*:

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

for any $e \in \mathcal{V}'$, and also the characteristic polynomial of ϕ is given by $\phi(\phi(e)) = -e - \phi(e)$, then the vector decomposition problem of $\mathcal{V}$ with respect to the basis $\{e, \phi(e)\}$ is solvable in polynomial time.

Proof. Given a random vector $v \in \mathcal{V}$, we can write v as $v = A + \phi(B)$ for some $A, B \in \langle e\rangle$, since $\{e, \phi(e)\}$ is a basis of $\mathcal{V}$. Then we show how to find A which is the projection of v along e as follows:

Since $F(\phi(B)) = \phi^2(B) = -B - \phi(B)$ and $F(A) = A$,

$$F(v) - \phi(v) = F(A + \phi(B)) - \phi(A + \phi(B)) = A - \phi(A). \tag{2}$$

Applying the morphism F to both sides of Eq. (2),

$$F(F(v) - \phi(v)) = F(A - \phi(A)) = 2A + \phi(A). \tag{3}$$

Multiplying the addition of (2) and (3) by 3^{-1}, we obtain for a random vector $v = A + \phi(B)$ the projection of v along e:

$$3^{-1} \cdot [F(v) - \phi(v) + F(F(v) - \phi(v))] = A.$$

Therefore, we can find the vector $A \in \mathcal{V}$ such that $A \in \langle e\rangle$ and $v - A \in \langle \phi(e)\rangle$ for given a random vector $v \in \mathcal{V}$ and a basis $\{e,\ \phi(e)\}$ for $\mathcal{V}$. □

In the example given by Yoshida et al. [7, 8] which is also mentioned in Section 2, the map ϕ is defined as $\phi(x, y) = (\xi x, y)$, where $\xi^2 + \xi + 1 = 0$. Then we can easily check the characteristic polynomial of ϕ as well satisfying the condition in Proposition 3.1: $\phi(\phi(e)) = -e - \phi(e)$.

The following theorem provides general sufficient conditions for which the VDP with respect to the basis $\{e, \phi_e(e)\}$ of the Theorem 2.3 is solvable in polynomial time. In particular, the characteristic polynomials of ϕ for examples in [2, 7, 8] are the special case of $t_1 = t_2 = -1$ in the following theorem.

Theorem 3.2. *For $e \in \mathcal{V}'$, let F_e, ϕ_e be isomorphisms on $\mathcal{V}$ satisfying Yoshida conditions with α_1, α_2 and α_3, and let $\phi_e^2 = t_1 + t_2\phi_e$ be the characteristic polynomial of ϕ_e. If α_i's and t_1, t_2 can be computed in polynomial time and satisfy*

$$\alpha_1\alpha_3 - \alpha_1^2 \pm \alpha_2 = 0 \text{ or } (\alpha_2 \mp t_1)(\alpha_3 - \alpha_1) - \alpha_2(\alpha_3 \mp t_2) = 0$$

but both are not zero, then the VDP with respect to the $\{e, \phi_e(e)\}$ *is solvable in polynomial time.*

Proof. As the proof of Proposition 3.1 for $v = A + \phi_e(B)$, we want to find $A \in \langle e \rangle$. Apply F_e and ϕ_e to v.

$$F_e(v) = \alpha_1 A + \alpha_2 B + \alpha_3 \phi_e(B), \tag{4}$$

$$\phi_e(v) = \phi_e(A) + t_1 B + t_2 \phi_e(B). \tag{5}$$

Subtracting or adding (5) from (4) yields

$$F_e(v) \mp \phi_e(v) = \alpha_1 A \mp \phi_e(A) + (\alpha_2 \mp t_1)B + (\alpha_3 \mp t_2)\phi_e(B). \tag{6}$$

Applying F_e to (6), we obtain

$$\begin{aligned} &\mathbb{F}_e(F_e(v) \mp \phi_e(v)) \\ &= (\alpha_1^2 \mp \alpha_2)A \mp \alpha_3 \phi_e(A) + \alpha_1(\alpha_2 \mp t_1)B + (\alpha_3 \mp t_2)[\alpha_2 B + \alpha_3 \phi_e(B)]. \end{aligned} \tag{7}$$

By eliminating $\phi_e(A)$ from (6) and (7), we obtain the equation

$$\begin{aligned} &\alpha_3(F_e(v) \mp \phi_e(v)) - F_e(F_e(v) \mp \phi_e(v)) \\ &= (\alpha_1\alpha_3 - \alpha_1^2 \pm \alpha_2)A + [(\alpha_2 \mp t_1)(\alpha_3 - \alpha_1) - \alpha_2(\alpha_3 \mp t_2)]\, B. \end{aligned}$$

Therefore, we can compute A or B if the given condition is satisfied. For example, if $\alpha_1\alpha_3 - \alpha_1^2 + \alpha_2 = 0$ and $(\alpha_2 - t_1)(\alpha_3 - \alpha_1) - \alpha_2(\alpha_3 - t_2) \neq 0$, we can compute B by

$$B = [(\alpha_2 - t_1)(\alpha_3 - \alpha_1) - \alpha_2(\alpha_3 - t_2)]^{-1} \left[\alpha_3(F_e(v) - \phi_e(v)) - F_e(F_e(v) - \phi_e(v))\right].$$

□

4. Analysis of the strong instance for the VDP

The VDP is first proposed by Yoshida et al. [7, 8]. Observing their proof to show the difficulty of the VDP, we agree on the point that $VDP(e_1, e_2,\ be)$ for such a vector be whose type is an element of the subspace $\langle e \rangle$ of $\mathcal{V}$ relative to the basis $\{e_1, e_2\}$ is hard to compute in polynomial time, since the VDP relative to the basis $\{e, \phi(e)\}$ is tractable for every vector of $\mathcal{V}$ over some curves by Proposition 3.1. When we use the VDP practically in the cryptographic protocols [3, 7, 8], a basis of $\mathcal{V}$ is ahead set and publicly known assuming that the VDP for a random vector of $\mathcal{V}$ under the given basis is hard. Thus we need to generalize their result by providing requisites for random bases serving as strong instances along with random vectors of any type in $\mathcal{V}$ for the VDP.

In this section we prove that the vector decomposition problem is hard for a random vector with respect to a random basis in $\mathcal{V}$ under some conditions. In following theorem, we consider a family of such bases $\{e_1, e_2\}$ as $e_1,\ e_2 \notin \langle e \rangle \cup \langle \phi(e) \rangle$. We denote it by $\mathcal{S}$.

Theorem 4.1. *Let* $\mathcal{V}$ *be a two-dimensional vector space over a finite field* $\mathbb{F}$ *and* $\mathcal{V}'$ *a one dimensional subspace of* $\mathcal{V}$*. Then the VDP relative to bases in* $\mathcal{S}$ *is at least as hard as the CDHP on* $\mathcal{V}'$ *except the negligible case if there exist*

$\mathbb{F}$-linear isomorphisms $F, \phi : \mathcal{V} \to \mathcal{V}$ which are computable in polynomial time respectively such that

(i) $\phi^2 + \phi + 1 = 0$ *on* $\mathcal{V}$;

(ii) *for any* $e \in \mathcal{V}'$, $F(e) = e$, $F(\phi(e)) = -e - \phi(e)$, *and* $\{e, \phi(e)\}$ *is a basis for* $\mathcal{V}$.

Proof. We denote by $VDP_{(e_1,e_2)}(v) \in \langle e_1 \rangle$ that the VDP oracle solves the VDP for the vector $v \in \mathcal{V}$ with respect to the basis $\{e_1, e_2\}$ in $\mathcal{S}$, which means the oracle provides a component of v along e_1. We claim that for a nontrivial arbitrary vector $v \in \mathcal{V}$, if the VDP on $\mathcal{V}$ relative to the basis in $\mathcal{S}$ is solvable, then the CDHP on $\mathcal{V}'$ is solvable. In other words, given an oracle which solves the VDP relative to the basis in $\mathcal{S}$, we can construct an algorithm $\mathcal{B}$ which solves the CDHP. For a random vector $v \in \mathcal{V}$, v is one of the three types of vectors in $\mathcal{V}$ as follows: $v \in \langle \phi(e) \rangle$, $v \in \langle e \rangle$ or $v \notin \langle e \rangle \cup \langle \phi(e) \rangle$. We show $\mathcal{B}$ solves the CDHP for each case. This implies the VDP is hard for any random vector relative to the basis in $\mathcal{S}$. We recall the VDP relative to the basis $\{e, \phi(e)\}$ is solvable from Proposition 3.1.

(Case i) Suppose that the VDP for the vector in $\langle \phi(e) \rangle$ is solvable relative to the basis in $\mathcal{S}$. Let (e, ae, be) be an instance for the CDHP on $\mathcal{V}'$. We may assume each of ae, be is not 0. If the instance is given to the algorithm $\mathcal{B}$, then $\mathcal{B}$ chooses nonzero $x, y, z, w \in \mathbb{F}$ uniformly at random satisfying $xw - yz \neq 0$ and computes $e_1 = xae + y\phi(e), e_2 = zae + w\phi(e)$. Then $\{e_1, e_2\}$ is a basis for $\mathcal{V}$ in $\mathcal{S}$. For $\phi(be) \in \mathcal{V}$, there exist $s, t \in \mathbb{F}$ such that $\phi(be) = se_1 + te_2$. Since

$$\phi(be) = se_1 + te_2 = (sx + tz)ae + (sy + tw)\phi(e),$$

we must have $sx + tz = 0, sy + tw = b$ by the hypothesis $\{e, \phi(e)\}$ is a basis for $\mathcal{V}$. Since $D = xw - yz \neq 0$, s and t can be determined by

$$\begin{pmatrix} s \\ t \end{pmatrix} = D^{-1} \begin{pmatrix} w & -z \\ -y & x \end{pmatrix} \begin{pmatrix} 0 \\ b \end{pmatrix} = \begin{pmatrix} -D^{-1}zb \\ D^{-1}xb \end{pmatrix}.$$

From the above assumption for the vector $\phi(be) \in \langle \phi(e) \rangle$ relative to the basis in $\mathcal{S}$, $\mathcal{B}$ can obtain $VDP_{(e_1,e_2)}(\phi(be)) = se_1 = -D^{-1}zbe_1$ in polynomial time. Since the VDP relative to the basis $\{e, \phi(e)\}$ is solvable by Proposition 3.1 and $e_1 = xae + y\phi(e)$, $\mathcal{B}$ can easily obtain the vector $-D^{-1}zxabe$, say it R, from $-D^{-1}zbe_1$. Hence $abe = -D \cdot (zx)^{-1} \cdot R$.

(Case ii) Suppose that the VDP for the vector in $\langle e \rangle$ is solvable relative to the basis in $\mathcal{S}$. Let (e, ae, be) be an instance for the CDHP on $\mathcal{V}'$. We may assume each of ae, be is not 0. If the instance is given to the algorithm $\mathcal{B}$, then $\mathcal{B}$ chooses nonzero $x, y, z, w \in \mathbb{F}$ uniformly at random satisfying $xw - yz \neq 0$ and computes $e_1 = xe + y\phi(ae), e_2 = ze + w\phi(ae)$. Now $\{e_1, e_2\}$ is a basis for $\mathcal{V}$ in $\mathcal{S}$. For $be \in \mathcal{V}$, $be = se_1 + te_2$ for some $s, t \in \mathbb{F}$. Since

$$be = se_1 + te_2 = (sx + tz)e + (sy + tw)\phi(ae),$$

we have $sx + tz = b, sy + tw = 0$. Then we can determine s and t by

$$\begin{pmatrix} s \\ t \end{pmatrix} = D^{-1} \begin{pmatrix} w & -z \\ -y & x \end{pmatrix} \begin{pmatrix} b \\ 0 \end{pmatrix} = \begin{pmatrix} D^{-1}wb \\ -D^{-1}yb \end{pmatrix},$$

where $D = xw - yz$. From the assumption for the vector $be \in \langle e \rangle$ relative to the basis in $\mathcal{S}$, $\mathcal{B}$ obtains $VDP_{(e_1,e_2)}(be) = se_1 = D^{-1}wb(xe + y\phi(ae))$ in polynomial time. Since the VDP relative to the basis $\{e, \phi(e)\}$ is solvable by Proposition 3.1, $D^{-1}wby\phi(ae)$, say it R, is easily obtained from se_1. Since $wy \neq 0$, $\phi(abe) = D \cdot (wy)^{-1} \cdot R$. On the other hand, from the condition $\phi^2 + \phi + 1 = 0$,

$$\begin{aligned} abe &= -(\phi + 1)(\phi(abe)) = -(\phi + 1)(D(wy)^{-1}R) \\ &= -D(wy)^{-1}(\phi + 1)(R). \end{aligned}$$

(Case iii) Suppose that the VDP for the vector v in $\mathcal{V}$ such that $v \notin \langle e \rangle \cup \langle \phi(e) \rangle$ is solvable relative to the basis in $\mathcal{S}$. Let (e, ae, be) be an instance for the CDHP on $\mathcal{V}'$ such that $ae \neq 0, be \neq 0$, which is given to the algorithm $\mathcal{B}$. Then $\mathcal{B}$ chooses a random $k \neq 0 \in \mathbb{F}$, and computes $e' = e + k\phi(e) \in \mathcal{V}$. Then $\{e, e'\}$ is a basis for $\mathcal{V}$. $\mathcal{B}$ chooses at random nonzero $x, y, z, w \in \mathbb{F}$ such that $xw - yz \neq 0$, $xae \neq -ye$ and $zae \neq -we$, and computes $e_1 = xae + ye', e_2 = zae + we'$. Now

$$\begin{aligned} e_1 &= (xa + y)e + yk\phi(e), \\ e_2 &= (za + w)e + wk\phi(e). \end{aligned}$$

Since $(xa + y)w - (za + w)y = (xw - zy)a \neq 0$, $xae \neq -ye$, $zae \neq -we$, and $yk, wk \neq 0$, the set $\{e_1, e_2\}$ is a basis for $\mathcal{V}$ in $\mathcal{S}$. For the random vector $v = be + k\phi(be) = be'$ of the type $v \notin \langle e \rangle \cup \langle \phi(e) \rangle$, there exist $s, t \in \mathbb{F}$ such that

$$\begin{aligned} be' &= se_1 + te_2 \\ &= (sx + tz)ae + (sy + tw)e'. \end{aligned}$$

Then since $\{e, e'\}$ is a basis of $\mathcal{V}$, we have $sx + tz = 0, sy + tw = b$, and accordingly $s = -D^{-1}zb$, $t = D^{-1}xb$, where $D = xw - yz$. From the assumption for the vector $be' \notin \langle e \rangle \cup \langle \phi(e) \rangle$ relative to the basis in $\mathcal{S}$, $\mathcal{B}$ obtains $VDP_{(e_1,e_2)}(be') = se_1 = -D^{-1}zbe_1$ in polynomial time. Now

$$\begin{aligned} -D^{-1}zbe_1 &= -D^{-1}zb\{(xa + y)e + yk\phi(e)\} \\ &= -D^{-1}zb(xa + y)e - D^{-1}zbyk\phi(e). \end{aligned}$$

Then $\mathcal{B}$ easily obtains $-D^{-1}zb(xa + y)e$ by the VDP relative to the basis $\{e, \phi(e)\}$, say it R. Since $z \neq 0$, $b(xa + y)e = -Dz^{-1}R$ and $xabe = -Dz^{-1}R - ybe$. Therefore $\mathcal{B}$ obtains $abe = x^{-1}(-Dz^{-1}R - ybe)$. □

5. Conclusion

In this paper, we give weak instances which show the VDP can be solved for a certain basis even if Yoshida condition is satisfied. We also suggest requisites for strong instances which make the VDP difficult for any random vector relative

to the given basis. Therefore, we can choose the basis uniformly at random and the random vector so that the VDP can serve as the underlying intractable problem in the cryptographic protocols.

References

[1] I. Duursma and N. Kiyavash, *On the vector decomposition problem for m-torsion points on an elliptic curve*, Proc. IEEE International Symposium on Information Theory (ISIT) **27** (2004), 545–545.

[2] ———, *The vector decomposition problem for elliptic and hyperelliptic curves*, J. Ramanujan Math. Soc. **20** (2005), no. 1, 59–76.

[3] I. Duursma and S. K. Park, *ElGamal type signature schemes for n-dimensional vector spaces*, Cryptology ePrint Archive, Report 2006/312.

[4] G. Frey and H. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Math. Comp. **62** (1994), no. 206, 865–874.

[5] S. Kwon and H.-S. Lee, *Analysis for the difficulty of the vector decomposition problem*, Journal of KIISC **17** (2007), no. 3, 27–33.

[6] A. Menezes, T. Okamoto, and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Trans. Inform. Theory **39** (1993), no. 5, 1639–1646.

[7] M. Yoshida, *Inseparable multiplex transmission using the pairing on elliptic curves and its application to watermarking*, Proc. Fifth Conference on Algebraic Geometry, Number Theory, Coding Theory and Cryptography, University of Tokyo, 2003. Available from: http://www.math.uiuc.edu/∼duursma/pub/yoshida_paper.pdf.

[8] M. Yoshida, S. Mitsunari, and T. Fujiwara, *Vector decomposition problem and the trapdoor inseparable multiplex transmission scheme based the problem*, Proc. of the 2003 Symposium on Cryptography and Information Security (SCIS), 2003.

Saeran Kwon
Department of Computer Science
Daelim University College
Keungki-Do 431-715, Korea
E-mail address: srkwon@daelim.ac.kr

Hyang-Sook Lee
Department of Mathematics
Ewha Womans University
Seoul 120-750, Korea
E-mail address: hsl@ewha.ac.kr