情報保護學會論文誌
第17卷 第3號, 2007. 6

벡터 분해 문제의 어려움에 대한 분석

권 세 란,[1†] 이 향 숙[2]
[1]대림대학, [2]이화여자대학교

Analysis for the difficulty of the vector decomposition problem

Saeran Kwon,[1†] Hyang-Sook Lee[2]
[1]Daelim College, [2]Ewha Womans University

요 약

최근 M.Yoshida 등에 의해 2차원 벡터 공간상의 벡터 분해 문제 (vector decomposition problem 또는 VDP) 가 제안되었고, 그것은 어떤 특별한 조건하에서는 최소한 1차원 부분공간상의 계산적 Diffie-Hellman 문제 (CDHP) 보다 어렵다는 것이 증명되었다. 하지만 그들의 증명이, VDP를 암호학적 프로토콜 설계에 적용하려면 필요한 조건인 벡터 공간상의 주어진 기저에 관한 임의의 벡터의 벡터 분해 문제가 어렵다는 것을 보이는 것은 아니다. 본 논문에서는 비록 어떤 2차원 벡터 공간이 M.Yoshida 등이 제안한 특별한 조건을 만족한다 할지라도, 특정한 모양의 기저에 관해서는 벡터 분해 문제가 다항식 시간 안에 해결될 수 있다는 것을 보여준다. 또한 우리는 다른 구조를 갖는 어떠한 기저들에 대해서는 그 2차원 벡터 공간 상의 임의의 벡터에 대한 벡터 분해 문제가 적어도 CDHP 만큼 어렵다는 것을 증명한다. 그러므로 벡터 분해 문제를 기반이 되는 어려운 문제로 하는 암호학적인 프로토콜을 수행할 때는 기저를 주의하여 선택하여야 한다.

ABSTRACT

Recently, a new hard problem on a two dimensional vector space called vector decomposition problem (VDP) was proposed by M. Yoshida et al. and proved that it is at least as hard as the computational Diffie-Hellman problem (CDHP) on a one dimensional subspace under certain conditions. However, in this paper we present the VDP relative to a specific basis can be solved in polynomial time although the conditions proposed by M. Yoshida on the vector space are satisfied. We also suggest strong instances based on a certain type basis which make the VDP difficult for any random vector relative to the basis. Therefore, we need to choose the basis carefully so that the VDP can serve as the underlying intractable problem in the cryptographic protocols.

Keywords : *Vector Decomposition Problem, Weak Instances, Strong Instances, Computational Diffie-Hellman Problem*

I. 서 론

M.Yoshida 등은 유한체 $\mathbb{F}$상의 2차원 벡터 공간에서 정의되는 벡터 분해 문제(vector decomposition problem 또는 VDP)라고 불려지는 새로운 계산적으로 어려운 문제와 그 문제의 어려움에 기반한 inseparable

접수일: 2006년 11월 30일; 채택일: 2007년 3월 8일
* 저자[2]는 한국과학재단(R01-2005-000-10713-0) 및 2단계 BK21의 지원을 받아 이 연구를 수행하였습니다.
† 주저자 및 교신저자, sranie@ewhain.net

multiplex transmission (IMT) 스킴을 제안하였다 [1,2]. 그들은 IMT 스킴의 비분리성을 이용하여 암호학적 데이터(예를 들어 암호문, 서명, 암호학적 키 등)에 워터마크를 내장시키는 응용 기법을 제공하였다. 현재까지 계산적 Diffie-Hellman문제(Computational Diffie- Hellman problem 또는 CDHP)는 어려운 문제로 인정되고 있는데, Yoshida는 그의 논문[1,2]에서 2차원 벡터 공간상의 벡터 분해 문제가 어떤 특별한 조건하에서는 1차원 부분 공간상의 계산적 Diffie- Hellman 문제(Computational Diffie-Hellman problem)로 변환되는 것을 보였다.

증명 과정을 구체적으로 설명해보면, 1차원 부분 공간상에서의 CDHP는, CDHP의 instance로 주어진 벡터를 이용하여 두 쌍의 기저를 생성한 다음, 주어진 벡터에 대해서 생성된 한 쌍의 기저에 대한 벡터 분해를 적용한 후 얻은 결과 벡터에 다시 나머지 쌍의 기저에 대한 벡터 분해를 적용하면 해결되는 것을 증명하였는데, 이것은 2차원 벡터공간상에서의 VDP가 쉽게 해결된다면 2번의 벡터 분해를 통하여 CDHP 문제가 해결됨을 의미하므로, VDP가 최소한 그것의 1차원 벡터 공간상에서의 CDHP보다 어렵다는 것을 의미한다고 말할 수 있다. 또한 Kiyavash와 Duursma는 그들의 논문[3,4]에서 VDP가 어려운 문제가 될 수 있는 특별한 조건을 만족하는 타원곡선은 supersingular 곡선만 가능하다는 것과, 또한 supersingular가 아닌 경우로써 그들이 찾아낸 genus 2인 일련의 초타원(hyperelliptic)곡선들이 VDP가 어려운 문제가 될 수 있는 특별한 조건을 만족시키는 것을 보였다. 그러나 우리는 본 논문에서 벡터분해문제가 어렵다는 사실에 반하는 예를 보여준다. 즉 타원곡선의 어떤 2차원 부분 공간 V 와 그것의 1차원 부분 공간 V'이 VDP에서 요구하는 특별한 조건을 만족한다 할지라도 V 에 속하는 벡터들이 V 의 어떤 특정 기저에 관해서는 다항식 시간 안에 분해 될 수 있다는 것을 보여준다. 이것은 VDP가 어떤 기저에 관한 임의의 벡터의 분해에 대해서는 어려운 문제가 될 수 없다는 것을 보여주는 실제 예가 된다. 사실 우리가 위에서 간단히 기술한, M.Yoshida 등[1,2]에 의해 VDP가 어렵다는 것을 보여주는 증명은 VDP를 어렵게 하는 instance의 존재성만을 보여주고 있다. 다시 말하면, 그들의 증명은, 암호학적인 프로토콜에 적용하기 위하여 필요한, 즉 임의로 주어진 기저에 대한 벡터 공간상의 임의의 벡터에 대한 벡터 분해 문제가 어렵게 된다는 사실을 보인 것은 아니기 때문에, 우리가 앞에서 얘기한 것과 같은 예를 찾을 수 있게 된 것이다. 그러나 Duursma와 Kiyavash는 그들의 논문[3]에서, 여기서 우리가 VDP가 어려운 문제라는 것에 대한 반례로 찾은 기저를 VDP를 어렵게 하는 기저로 이용하였다.

다음으로 우리는 주어진 기저에 관련해 임의의 벡터에 대한 VDP를 어렵게 하는 그와 같은 기저의 존재성을 찾아보고, 그와 같은 구조의 기저들에 대한 임의의 벡터의 분해는 적어도 CDHP 만큼 어렵다는 것을 증명한다. 즉 벡터 분해 문제가 쉽게 해결되는 기저가 존재하는 반면에 어떤 모양의 기저에 대해서는 VDP를 적어도 CDHP 만큼 어렵게 하는 그런 기저가 존재함을 증명하였다.

이 논문은 다음과 같이 구성된다. 단원 II에서는 논문[1,2]에서 정의된 VDP와 CDHP에 관한 정의와 관련된 결과를 정리한다. 단원 III에서는 어떤 2차원 벡터공간 V 가 M.Yoshida 등이 제안한 특별한 조건을 만족한다할지라도, 어떤 특정한 기저에 관해서는 V 에 속하는 임의의 벡터에 대하여 약간의 계산을 통하여 그 기저에 관한 벡터 분해가 다항식 시간 안에 해결 될 수 있다는 것을 증명한다. 또한 단원 IV에서는 VDP를 어렵게 하는 기저를 찾아보고 그와 같은 기저에 관련한 임의의 벡터들은 모두 VDP의 strong instance가 될 수 있음을 증명한다. 마지막으로 단원 V에서는 결론을 언급한다.

Ⅱ. 벡터 분해 문제(The vector decomposition problem)

먼저 논문[1,2]에서 정의된 벡터 분해문제와 CDHP의 정의를 살펴 본 후, 관련된 몇 가지 성질과 논문[1,2]에서 보여준 증명을 살펴보기로 한다.

V 를 소수 위수 m을 갖는 유한체 $\mathbb{F}$상의 2차원 벡터 공간이라고 하고 V'을 V 의 1차원 부분 공간이라고 하자. 또한 벡터 $v \in V$에 대해 $<v>$는 $\{av \mid a \in \mathbb{F}\}$ 를 의미한다. 이 때 V상의 벡터분해문제는 다음과 같이 정의된다. :

- V상의 벡터분해문제(vector decomposition problem; VDP): $\{e_1, e_2\}$가 V에 대한 $\mathbb{F}$-기저이고, $e_1, e_2, v \in V$가 주어졌을 때, $u \in <e_1>$, $v - u \in <e_2>$를 만족하는 벡터 $u \in V$를 찾는 문제를 V 상의 벡터분해문제(VDP)로 정의한

다[1,2].

- V' 상의 계산적 Diffie-Hellman문제(Computational Diffie-Hellman problem; CDHP) : $a, b \in \mathbb{F}$ 에 대하여 $e \in V' / 0$ 와 $ae, be \in <e>$ 가 주어졌을 때 $abe \in <e>$ 를 찾는 문제를 말한다.

Yoshida 등이 논문[1,2]에서 주장한 "V상의 VDP가, 어떤 특별한 조건하에선, 적어도 1차원 부분 공간 V'상의 계산적 Diffie-Hellman 문제 (CDHP) 보다 어렵다" 에 관한 구체적 정리는 다음과 같다.

(정리1) 다음 세 가지 조건을 만족하는 선형 동형사상 (linear isomorphism) ψ_e, $\phi_e : V \rightarrow V$ 이 임의의 $e \in V'$에 대해 존재하면 V 상의 VDP는 적어도 $V'(\subset V)$상의 CDHP보다 어렵다[1].

(조건1) 어떤 $v \in V$에 대해 $\psi_e(v)$, $\phi_e(v)$ 는 효율적으로 정의되고 다항식 시간 내에 계산가능하다.

(조건2) $\{e, \psi_e(e)\}$ 는 v 에 대한 $\mathbb{F}$-기저이다.

(조건3) $\phi_e(e) = \alpha_1 e,$
$\phi_e(\psi_e(e)) = \alpha_2 e + \alpha_3 \psi_e(e),$
$\alpha_1 \cdot \alpha_2 \cdot \alpha_3 \neq 0$

을 만족하는 $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}$가 존재하고 이런 원소 $\alpha_1, \alpha_2, \alpha_3$ 와 각각의 역원들은 다항식 시간 내에 계산가능하다.

참조: 이후 우리는 위의 조건을 Yoshida 조건이라고 통칭한다.

(정리1)의 증명을 개략적으로 살펴보도록 하자. 우리는 일반성의 손실이 없으면서 증명을 단순화 하기 위해 CDHP 문제의 입력값인 (e, ae, be)에 대해 $(\alpha_3 - \alpha_1)a \neq 1$인 경우로 제한하여 증명을 살펴보기로 한다. 또한 여기서 벡터 분해를 제공해 주는 함수 이름을 VDP 라고 쓰기로 하자.

즉, $e_1, e_2, v \in V$ 에 대해 $\{e_1, e_2\}$ 가 만약 V 에 대한 $\mathbb{F}$-기저이면서, $u \in <e_1>$이고 $v - u \in <e_2>$이라면 $VDP((e_1, e_2), v) = u$ 가 됨을 의미한다.

(정리1)의 개략적 증명[1] : CDHP 문제의 입력값인 (e, ae, be)에 대해 abe 는 VDP 함수를 다음처럼 두 번 적용하는 것에 의해 계산되어 질 수 있다. 먼저 다음처럼 정의된 V의 기저 $\{e_1, e_2\}$를 선택한다.

$e_1 = ae + \psi_e(\alpha_2^{-1}(\alpha_3 - \alpha_1)ae - \alpha_2^{-1}e)$
$= ae + \lambda\psi_e(e)$ 로 정의하고

(여기서 λ 는 $\lambda = \alpha_2^{-1}(\alpha_3 - \alpha_1)a - \alpha_2^{-1}$ 를 표시), $e_2 = \phi_e(e_1)$ 로 정의한다. 이 때 e_2 에 대해 좀 더 계산을 해보면 다음 결과를 이끌어 낼 수 있다. 즉,

$e_2 = \alpha_1 ae + \lambda(\alpha_2 e + \alpha_3\psi_e(e)) = (\alpha_1 a + \lambda\alpha_2)e + \lambda\alpha_3\psi_e(e) = (\alpha_3 a - 1)e + \lambda\alpha_3\psi_e(e)$ 임을 알 수 있다. 이 때 벡터 be 와 기저 $\{e_1, e_2\}$에 대해 다음처럼 VDP 함수를 적용하면, $\alpha_3 e_1 - e_2 = e$ 이므로, $VDP((e_1, e_2), be) = \alpha_3 be_1$가 됨을 알 수 있다. 즉 기저 $\{e_1, e_2\}$에 대해 벡터 be의 e_1에 대한 성분 $\alpha_3 be_1$ 이 주어진다. 이 때 이 벡터 $\alpha_3 be_1$에 α_3^{-1}배의 스칼라 곱을 하게 되면 우리는 벡터 be_1을 얻게 된다. 마지막으로 이 벡터 be_1에 기저 $\{e, \psi_e(e)\}$와 함께 벡터 분해 함수 VDP를 다시 적용하여 $VDP((e, \psi_e(e)), be_1)$ 를 구해보면, $e_1 = ae + \lambda\psi_e(e)$ 이므로, 벡터 be_1 의 기저 e 에 대한 성분인 abe을 구할 수 있다. □

하지만 위의 증명은, 만약 우리가 CDHP를 어려운 문제라 받아들인다면 $VDP((e_1, e_2), be)$와 $VDP((e, \psi_e(e)), be_1)$ 중 적어도 한 문제는 어려운 문제임을 증명한 것 이라 할 수 있다. 이것은 VDP에 관한 정리의 증명[1]이, Yoshida 조건을 만족하는 환경에서 임의의 기저가 주어지면 그 기저에 대한 임의의 벡터를 분해하는 것이 어려운 문제라는 것을 증명하기 보다는, VDP 가 어려운 문제가 되는 instance 의 존재성만을 보인 것 이라 할 수 있다. 사실 Ⅲ 절에서 우리는 Yoshida 조건을 만족하는 어떤 구체적 곡선 상에서 $VDP((e, \psi_e(e)), be_1)$ 가 다항식 시간에 해결 될 수 있다는 것을 보여주므로, 이 증명에서는 $VDP((e_1, e_2), be)$가 VDP가 어려운 instance 라고 말할 수 있다.

M.Yoshida 등은 V와 V' 의 예로, 논문[5]의 암호 시스템과 마찬가지 환경으로, 타원곡선의 m-torsion point의 군(group)인 $E[m]$ 와 그것의 부분군 $E(\mathbb{F}_p) \cap E[m]$ 를 각각 택하였는데 여기서의 시스템 매개변수들은 다음과 같이 정의되어 있다.

p : $p \equiv 2 \pmod 3$ 를 만족하는 소수
$\mathbb{F}_p$: 위수가 p인 유한체
E : $y^2 = x^3 + 1$, $\mathbb{F}_p$ 위에서의 타원곡선
m : $6m = p + 1$ 의 관계를 만족하는 소수

$E(\mathbb{F}_p)$:x, y $\in \mathbb{F}_p$ 인 E 위에서의 점 (x, y)의 집합

$E[m]$: $\{P \mid mP = 0\} \subset E(\mathbb{F}_{p^2})$.

또한 선형 동형사상 $\psi_e, \phi_e : V \to V$ 는 $\psi(x, y) = (\xi x, y)$ 와 Frobenius map $\phi(x, y) = (x^p, y^p)$ 으로 선택하였다. 여기서 $\xi \in \mathbb{F}_{p^2}$ 는 $\xi^2 + \xi + 1 = 0$ 을 만족시키는 값이다. 이 때 임의의 $P \in V'$ 에 대해 우리는 다음관계가 만족 됨을 알 수 있다.

$$\phi(P) = P \ , \ \phi(\psi(P)) = -P - \psi(P) \ .$$

또한 Kiyavash와 Duursma는 그들의 논문[3,4]에서 VDP가 어려운 문제가 될 수 있는 특별한 조건을 만족하는 타원곡선은 supersingular 곡선만 가능하다는 것과, 또한 supersingular가 아닌 경우로써 그들이 찾아낸 체 $\mathbb{F}_p$ (여기서 $p \equiv 2 \ (mod\ 3)$) 위에 정의된 genus 2인 일련의 초타원(hyperelliptic)곡선들 $C_1 : y^2 = x^6 - ax^3 + 1$과 $C_2 : y^2 = x^6 - ax^3 - 3$가 VDP가 어려운 문제가 될 수 있는 Yoshida 조건을 만족시키는 것을 보였다. 즉 이 곡선들 C_1, C_2 상에서 동형사상 $\psi, \phi : V \to V$ 를 $\psi(x, y) = (\xi x, y)$ 와 Frobenius map $\phi(x, y) = (x^p, y^p)$ 으로 선택하면 이 곡선 상에서도 역시 $\phi(P) = P$, $\phi(\psi(P)) = -P - \psi(P)$ 로서 Yoshida 조건을 만족시키는 것을 보였다.

Ⅲ. 정리1의 반례

이 단원에서는 M.Yoshida 등이 앞 단원에서 제안한 VDP의 특별한 조건을 만족시키는 위의 벡터공간들에서의 벡터들이 실제로는 어떤 기저에 관해서 약간의 계산을 통하여 분해 될 수 있다는 것을 증명하고자 한다. 먼저 우리의 증명을 도와주는 보조정리를 보여줌으로써 증명을 시작하고자 한다.

(보조정리 2) 모든 $Q \in E[m]$ 에 대해
$\psi(\psi(Q)) = -Q - \psi(Q)$.

증명) 만약 $Q \in E[m]$ 의 좌표를 $Q = (x, y)$ 로 표시한다면, 그때 $\psi(Q) = (\xi x, y)$ 이다. 또한 $Q + \psi(Q)$ 의 좌표를 (x', y') 로 표시하면,

$$x' = \left(\frac{y - y}{\xi x - x}\right)^2 - x - \xi x = -x - \xi x$$

$$y' = \left(\frac{y - y}{\xi x - x}\right)^2 (x - x') - y = -y$$

가 됨 을 알 수 있다. 그러므로 다음이 성립한다.

$$\psi(\psi(Q)) = (\xi^2 x, y) = (-x - \xi x, y)$$
$$= (x', -y') = -(x', y') = -Q - \psi(Q).$$

다음에서 체 $\mathbb{Z}_m$ 위의 2차원 벡터공간 V와 V의 1차원 부분 공간 V' 은 각각 단원 Ⅱ에서 정의된 $E[m]$ 과 $E(\mathbb{F}_p) \cap E[m]$ 을 의미한다. 먼저 임의의 점 $P \in V'$ 를 택한다. 이때 $\psi(P)$ 는 벡터공간 $E[m]$에는 속하지만 $E(\mathbb{F}_p)$에는 속하지 않으므로, P와 $\psi(P)$는 V에서 선형독립 관계이다. 그러므로 $\{P, \psi(P)\}$는 2차원 벡터공간 V에 대한 체 $\mathbb{Z}_m$-기저가 될 수 있음을 알 수 있고 결과적으로 임의의 벡터 $v \in V$ 에 대해 다음 식을 만족하는 체 $\mathbb{Z}_m$에 속하는 원소 a, b가 존재함을 알 수 있다. 즉, $v = aP + b\psi(P) = aP + \psi(bP) = A + \psi(B)$. (여기서 $A = aP$ 그리고 $B = bP$를 표시한다.) 그러면, $X = A$ 또는 B에 대해 $\phi(X) = X$이고 $\phi(\psi(X)) = -X - \psi(X)$ 이므로 우리는 다음 관계식이 성립함을 볼 수 있다.

$$\phi(v) = \phi(A + \psi(B)) = A - B - \psi(B) \tag{1}$$

또한 같은 벡터 $v = A + \psi(B)$에 선형사상 ψ를 양변에 적용한 후 식에서 나타나는 값 $\psi(\psi(B))$ 대신에 보조정리 2의 결과를 이용하여 $-B - \psi(B)$를 대입하면 다음 등식이 얻어진다.

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

등식 (2) 좌우 변에서 등식 (1)의 좌우 변을 각각 빼게 되면 다음 관계식을 얻을 수 있다.

$$\phi(v) - \psi(v) = A - \psi(A) \tag{3}$$

다시 등식 (3)의 좌우 변에 선형 사상 ϕ을 적용하면 아래 등식 (4)를 얻을 수 있다.

$$\phi(\phi(v) - \psi(v)) = \phi(A - \psi(A))$$
$$= A - (-A - \psi(A)) = 2A + \psi(A) \tag{4}$$

등식(3)과 등식(4)의 좌우 변을 각각 더한 후 얻어진 관계식의 좌우 변을 다시 3^{-1} 배 스칼라 곱을 하게 되면, 임의로 주어진 벡터 $v = A + \psi(B)$ 에 대해서 다음 등식 (5) 가 성립함을 알 수 있다.

$$3^{-1} \cdot [\phi(v) - \psi(v) + \phi(\phi(v) - \psi(v))] = A \tag{5}$$

그러므로 우리는 벡터공간 V의 체 $\mathbb{Z}_m$-기저 $\{P, \psi(P)\}$에 대해 임의의 벡터 $v \in V$가 주어졌을 때 $A \in < P >$이고 $v - A \in < \psi(P) >$를 만족하는 벡터 A를, 선형사상 ϕ, ψ 및 타원곡선상의 한 번의 뺄셈, 한 번의 덧셈, 그리고 한 번의 스칼라 곱을 사용하여 다항식 시간 안에 분해할 수 있다는 것을 증명하였다.

Ⅳ. VDP가 어려운 문제가 될 수 있는 기저

이 단원에서는 VDP를 어렵게 하는 기저를 찾아보고 그와 같은 기저에 관련한 임의의 벡터들은 모두 VDP의 strong instance가 될 수 있음을 증명한다. 그러므로 이와 같은 기저들은 벡터 분해 문제를 기반이 되는 어려운 문제로 하는 암호학적인 프로토콜을 수행하기에 적합한 기저가 될 수 있을 것이다.

(보조정리 3) $ae, be, ce \in V' = \langle e \rangle$인 (e, ae, be. ce)가 주어질 때, V' 상에서 CDHP가 어려운 문제라면, $(ac - b(2a+1))e$를 계산하는 것은 어려운 문제이다.

증명) (e, ae, be.)가 V'상에서 CDHP의 임의의 instance라고 하자. 이때 만약 우리가 ce=be로 둔 경우에 $(ac - b(2a+1))e$를 다항식 시간 안에 얻을 수 있다면 우리는

$$X = (ac - b(2a+1))e = (ab - b(2a+1))e$$
$$= -abe - be$$

를 다항식 시간 안에 얻을 수 있고 $-X - be = abe$의 해 CDHP의 임의의 instance (e, ae, be)에 대한 abe를 다항식 시간 안에 얻을 수 있게 된다.

다음 정리는 위의 (보조 정리 3)을 이용하여 벡터 공간 V의 임의의 벡터 $v \in V$에 대해 VDP를 어렵게 하는 기저를 제공해 준다.

(정리 4) $V' = \langle e \rangle$을 일차원 부분 공간으로 갖는, 유한 체 $\mathbb{F}$위의 $\{e, \psi(e)\}$ 에 의해 생성되는 2차원 벡터 공간 V에서 (정리1)의 $\alpha_1 = 1, \alpha_2 = -1$, $\alpha_3 = -1$인 경우의 Yoshida 조건을 만족하는 선형 동형사상 $\psi, \phi : V \to V$ 가 있을 때, 특히 이때 ψ는 모든 $v \in V$ 에 대해 $\psi(\psi(v)) = -v - \psi(v)$를 만족하며 ψ^{-1}도 다항식 시간 내에 계산 가능한 사상일 때, $2ae + e \neq 0$ (여기서 0은 V의 zero vector를 의미)인 임의의 벡터 $ae \in < e >$에 대해 아래의 두 벡터 $\{e_1, e_2\}$ 는 V 의 기저가 되며,

$$e_1 = ae + \psi(2ae + e)$$
$$e_2 = \phi(e_1)$$

이 기저에 대한 V 상의 임의의 벡터에 대한 VDP 는 적어도 V' 상의 CDHP 만큼 어렵다.

증명) 표현의 간편성을 위해 $2a+1$을 λ로 표시하자. 이때 $e_1 = ae + \lambda\psi(e)$ 로 표시되고 $e_2 = (-a-1)e - \lambda\psi(e)$ 가 되며 특히 $\lambda \neq 0$ 이므로 $\{e_1, e_2\}$ 는 V의 또 다른 기저가 된다. 그러므로 V의 모든 벡터는 기저 $\{e_1, e_2\}$ 의 선형 조합으로 표현될 수 있고 따라서 아래 식을 만족하는 $s, t \in \mathbb{F}$ 가 존재한다.

$$\psi(e) = se_1 + te_2 = (sa + t(-a-1))e + (s\lambda - t\lambda)\psi(e) \quad (5)$$

여기서 우리는 $\{e, \psi(e)\}$ 또한 V의 기저이기 때문에

$$sa + t(-a-1) = 0,\ s\lambda - t\lambda = 1 \quad (6)$$

이 되어야 함을 알 수 있고 $\lambda \neq 0$ 이므로 식 (6)으로부터 결국 s, t 는 $\begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} \lambda^{-1}(1+a) \\ \lambda^{-1}a \end{pmatrix}$ 의 값을 갖게 됨을 알 수 있다. 이제 우리는 be,ce 가 $V' = < e >$에 속하는 임의의 벡터일 때, V 상의 임의의 벡터 $v = be + \psi(ce)$ 에 대해 $VDP(e_1, e_2, v)$를 다항식 시간 내에 풀 수 있다면 $CDHP(e, ae, be)$ 또한 다항식 시간 내에 풀 수 있음을 보이고자 한다. $-e_1 - e_2 = e$ 이고 (5)에서 $\psi(e) = \lambda^{-1}(1+a)e_1 + \lambda^{-1}ae_2$ 로 표현되므로 우리는 기저 $\{e_1, e_2\}$ 에 관하여 v를 다음과 같이 쓸 수 있다.

$$v = be + \psi(ce)$$
$$= b(-e_1 - e_2) + c\lambda^{-1}(1+a)e_1 + c\lambda^{-1}ae_2 \quad (7)$$
$$= (-b + c\lambda^{-1}(1+a))e_1 + (-b + c\lambda^{-1}a)e_2.$$

만약 $VDP((e_1, e_2), v)$가 다항식 시간에 해결된다면, 우리는 식 (7)로부터 다항식 시간에 $v - VDP((e_1, e_2), v)$

$=(-b+c\lambda^{-1}a)e_2$를 얻을 수 있다. 다시 여기서 기저 $\{e,\psi(e)\}$에 관해

$$(-b+c\lambda^{-1}a)e_2$$
$$=(-b+c\lambda^{-1}a)\{(-a-1)e-\lambda\psi(e)\}$$

로 표현될 수 있고 Ⅲ절에서 증명한 것처럼 기저 $\{e,\psi(e)\}$ 에 관해 VDP 는 다항식 시간에 해결 될 수 있으므로 다음 벡터를 얻을 수 있다.

$$(-b+c\lambda^{-1}a)e_2-$$
$$VDP((e,\psi(e)),(-b+c\lambda^{-1}a)e_2) \quad (8)$$
$$=-(-b+c\lambda^{-1}a)\lambda\psi(e)$$

또한 동형사상 ψ^{-1} 도 다항식 시간 내에 계산 될 수 있으므로 식 (8)의 결과에 ψ^{-1}를 적용하여 부호를 변화시키면 다항식 시간 안에 $(ac-b\lambda)e$를 얻을 수 있다. 그런데 우리는 (보조 정리3)에서 instance $(e,ae,be.ce)$에 대해 다항식 시간 안에 $(ac-b\lambda)e$를 얻을 수 있다면 이 오라클을 이용하여 CDHP를 다항식 시간 내에 구할 수 있다는 것을 보였다.

V. 결 론

본 논문에서 우리는 M.Yoshida 등이 제안한 특별한 조건[1,2]을 만족하는 벡터 공간이라 할지라도 벡터들이 어떤 특정한 종류의 기저에 관해서는 다항식 시간 안에 분해 될 수 있다는 것을 보여주었다. 또한 그와 다른 형태를 갖는 어떤 모양의 기저에 대해서는 임의의 벡터에 대해 VDP가 어려운 문제가 되는 strong instance들이 된다는 것을 증명하였다. 그러므로 VDP가 어려운 문제가 되기 위해서는 기저를 선택함에 있어 주의를 기울어야 할 것이다.

참고문헌

[1] 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

[2] M. Yoshida, S. Mitsunari, and T. Fujiwara, "Vector decomposition problem and the trapdoor inseparablemultiplex transmission scheme based the problem", Proc. of the 2003 Symposium on Cryptography and Information Security (SCIS), 7B-1, 2003.

[3] I. Duursma and N. Kiyavash, "The Vector Decomposition Problem for Elliptic and Hyperelliptic Curves", J. Ramanujan Math. Soc., 20, No. 1, pp. 59-76, 2005.

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

[5] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", Proc. of Advances in Cryptology, Crypto 2001, LNCS 2139, pp. 213-229, 2001.

〈著者紹介〉

권 세 란 (Saeran Kwon) 정회원
서울대학교 수학과 졸업
이화여자대학교 컴퓨터공학과 석 박사통합과정 수료
대림대학 컴퓨터정보학과 교수
<관심분야> 암호이론, 정보보호

이 향 숙 (Hyang-Sook Lee) 정회원
학사: 이화여자대학교 수학과
석사: 이화여자대학교 수학과
Ph. D.: 노스웨스턴 대학교 수학과
1995년 3월 - 현재: 이화여자대학교 수학과 교수
<관심분야> 암호이론, 정보보호