Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2015, Article ID 197097, 6 pages
http://dx.doi.org/10.1155/2015/197097

Research Article

Hyperelliptic Curves for the Vector Decomposition Problem over Fields of Even Characteristic

Seungkook Park

Department of Mathematics, Sookmyung Women's University, Cheongpa-ro 47-gil 100, Yongsan-gu, Seoul 140-742, Republic of Korea

Correspondence should be addressed to Seungkook Park; skpark@sookmyung.ac.kr

Received 26 August 2014; Accepted 11 February 2015

Academic Editor: Wei Wu

We present an infinite family of hyperelliptic curves of genus two over a finite field of even characteristic which are suitable for the vector decomposition problem.

1. Introduction

Intractable mathematical problems such as the integer factorization problem, the discrete logarithm problem (DLP), and the computational Diffie-Hellman problem (CDHP) are being used to provide secure protocols for cryptosystems. A new hard problem which is called the vector decomposition problem (VDP) was proposed by Yoshida et al. [1]. The VDP on a two-dimensional vector space can serve as the underlying intractable problem for cryptographic protocols. Galbraith and Verheul presented an application of trapdoor VDP where a trapdoor is used to construct a public key encryption scheme [2]. In 2009, Yoshida and Fujiwara introduced a new watermarking scheme designed for cryptographic data such as keys, ciphertexts, and signatures [3, 4]. The proposed scheme utilizes a two-dimensional vector space where one of the one-dimensional subspaces is used as the domain of cryptographic date and the other one-dimensional subspace is used to embed a watermark. The security of the scheme is based on the infeasibility of the VDP. In [5], Yoshida stated the conditions that are required for the VDP on a two-dimensional vector space to be at least as hard as the CDHP on a one-dimensional subspace and suggested a particular family of elliptic curves to be used for the VDP. Duursma and Kiyavash [6] showed that the family of elliptic curves chosen by Yoshida is not secure and moreover none of the elliptic curves have the property that is needed for the VDP to be a hard problem. In order to resolve this problem Duursma and Kiyavash introduced an infinite family of genus two hyperelliptic curves suitable for the VDP. Galbraith and Verheul analyzed the VDP and showed that the VDP on a two-dimensional vector space is equivalent to CDHP on a one-dimensional subspace for the Duursma-Kiyavash curves [2]. The family of hyperelliptic curves proposed by Duursma and Kiyavash are defined over a finite field of odd characteristic. Curve operations are performed using arithmetic operations in the underlying field. Hence the efficient implementation of finite field arithmetic is an important prerequisite in hyperelliptic curve systems. Smart showed that the general multiplication algorithm on the Jacobian for curves defined over odd characteristic fields ended up being around twice as slow as that for even characteristic fields, of an equivalent size, in genus two [7]. Thus curves defined over even characteristic fields have an advantage in computation time over curves defined over odd characteristic fields. Hence one would prefer curves defined over a finite field of even characteristic for the VDP. In this paper, we present an infinite family of hyperelliptic curves of genus two over a finite field of even characteristic and show that it satisfies all the conditions that are needed for the VDP to be a hard problem. The paper is organized as follows: The definitions of CDHP and VDP are given in Section 2. Also we state the conditions for the VDP to be a hard problem and describe the applications of the VDP given in [2–4]. In Section 3, we propose a family of hyperelliptic curves over fields of even characteristic such that the Jacobian of the curves is a product of two elliptic curves. In Section 4, we prove that the two elliptic curves found in Section 3 are 3-isogenous and we find the 3-isogeny. In Section 5, we give the setting of the VDP on the hyperelliptic curves given in Section 3 and show that the VDP defined on these curves can serve as an intractable problem in cryptographic protocols.

2. Vector Decomposition Problem

We state the definition of VDP and the conditions for the VDP on a two-dimensional vector space to be at least as hard as the CDHP on a one-dimensional subspace given by Yoshida [5].

Definition 1. The 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 $\mathcal{V}$, 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 CDHP on $\mathcal{V}'$ (a one-dimensional vector space over $\mathbb{F}$) is as follows: "given $e \in \mathcal{V}' \setminus \{0\}$ and $ae, be \in \langle e \rangle$, find $abe \in \langle e \rangle$."

Theorem 3 (Yoshida [5]). *The vector decomposition problem on $\mathcal{V}$ is at least as hard as the computational Diffe-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 $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}$ with*

$$F_e(e) = \alpha_1 e, \qquad F_e(\phi_e(e)) = \alpha_2 e + \alpha_3 \phi_e(e), \tag{1}$$

and $\alpha_1, \alpha_2, \alpha_3 \neq 0$. The elements α_1, α_2, α_3 and their inverses can be computed in polynomial time.

Proof. The proof is in [5] and is also included in [6]. □

The VDP is hard in general but for certain bases the VDP can be solved in polynomial time even if it satisfies Yoshida's conditions [2, 8]. In fact, the bases chosen by Duursma and Kiyavash are easy instances of the VDP. The fact that there are easy instances of VDP does not affect the VDP conjecture that the VDP should be hard for randomly chosen basis. In [8], Kwon and Lee provided criteria for choosing a basis such that the VDP can serve as an intractable problem in cryptographic protocols. In [2], Galbraith and Verheul showed that if $\{e_1, e_2\}$ is distortion eigenvector base for $\mathcal{V}$ then the VDP on a two-dimensional vector $\mathcal{V}$ is equivalent to the CDHP on one-dimensional vector space $\langle e_1 \rangle$.

We give the definition of eigenvector base and distortion eigenvector base.

Definition 4. Let $\mathcal{V}$ be a group of exponent m and order m^2. Let $F : \mathcal{V} \to \mathcal{V}$ be a group isomorphism computable in polynomial time. A pair of elements $e_1, e_2 \in \mathcal{V}$ is an eigenvector base with respect to F if $\mathcal{V} = \langle e_1, e_2 \rangle$; that is, each element $v \in \mathcal{V}$ can be uniquely written as a linear combination in e_1 and e_2 and if $F(e_1) = \alpha_1 e_1$ and $F(e_2) = \alpha_2 e_2$ for some distinct, nonzero $\alpha_1, \alpha_2 \in \mathbb{Z}/m\mathbb{Z}$.

Definition 5. An eigenvector base $\{e_1, e_2\}$ is said to be a distortion eigenvector base if there are group homomorphisms $\phi_1 : \langle e_1 \rangle \to \langle e_1 \rangle$ and $\phi_2 : \langle e_2 \rangle \to \langle e_1 \rangle$ computable in polynomial time and if an integer $d \not\equiv 0 \pmod{m}$ is given such that $\phi_2(\phi_1(e_1)) = de_1$.

Remark 6. The VDP with respect to an eigenvector base is solvable in polynomial time.

Two applications of the VDP are watermarking scheme designed for cryptographic date given in [3, 4] and public key encryption scheme given in [2]. In the watermarking scheme a cryptographic date which can be considered as a "vector" is watermarked by adding a linearly independent random vector. Embedding and removing a watermark correspond to adding a one-dimensional vector and decomposing a two-dimensional vector, respectively. Due to the infeasibility of the VDP, removing the watermark is hard unless one has some trapdoor information. The core idea of the public key encryption scheme given in [2] is that for certain bases the VDP is easy but for general bases the VDP is hard. Let $\mathcal{V}$ be a two-dimensional vector space isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ with a distortion eigenvector base $\{e_1, e_2\}$. If $u_1 = \alpha_{11}e_1 + \alpha_{12}e_2$ and $u_2 = \alpha_{21}e_1 + \alpha_{22}e_2$, where $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in \mathbb{Z}/m\mathbb{Z}$ and $\alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21} \not\equiv 0 \pmod{m}$, then for any $v \in \mathcal{V}$, if one knows the $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}$ then one can solve the VDP of v to the base $\{u_1, u_2\}$. Using α_{11}, α_{12}, α_{21}, α_{22} as a trapdoor we obtain a trapdoor VDP scheme. An application of the trapdoor VDP is the public key encryption scheme with public key $(e_1, v = \alpha_1 e_1 + \alpha_2 e_2)$ and private key (α_1, α_2). A message $m \in \langle e_1 \rangle$ is encrypted as $c = m + \beta v$ for a random β with $1 \leq \beta < m$.

3. Hyperelliptic Curves over Fields of Even Characteristic

By Theorem 3, the VDP is hard if the CDHP on a one-dimensional subspace is hard. Yoshida suggested to use the full group of m-torsion points on the elliptic curve $E : y^2 = x^3 + 1$ over $\mathbb{F}_p$ as the two-dimensional vector space $\mathcal{V} = E[m]$ and the subgroup of $\mathbb{F}_p$-rational m-torsion points as the one-dimensional subspace $\mathcal{V}' = E(\mathbb{F}_p) \cap E[m]$. The elliptic curve $E : y^2 = x^3 + 1$ given by Yoshida is supersingular. Thus the elliptic curve discrete logarithm problem (ECDLP), and hence the CDHP on the one-dimensional subspace, is vulnerable to the MOV attack. Duursma and Kiyavash [6] showed that any elliptic curve that satisfies the conditions of Theorem 3 is supersingular. Thus, using the VDP with the full m-torsion points on an elliptic curve introduces a vulnerability that needs to be compensated by choosing larger parameters. To avoid this, the VDP may be used with higher genus curves. Duursma and Kiyavash introduced an infinite family of genus two hyperelliptic curves suitable for the VDP defined over a finite field of odd characteristic.

In this section, we provide an infinite family of genus two hyperelliptic curves suitable for the VDP defined over a finite field of even characteristic. Unless specified otherwise all the fields will be of even characteristic and all the curves will be over fields of even characteristic. For our purpose, we need a hyperelliptic curve such that the Jacobian of the hyperelliptic curve decomposes into two isogenous elliptic curves. Let K be a finite field of even characteristic. We consider the following hyperelliptic curve of genus two over K:

$$C : y^2 + y = \frac{a}{x^3 + 1}, \tag{2}$$

where $a = \alpha^2 + \alpha$ for some $\alpha \in \overline{K}$. Let ω and $\overline{\omega}$ be the roots of $x^2 + x + 1 = 0$. The automorphism group of (2) is D_{12} and the automorphisms are

(1) $(x, y) \overset{\text{id}}{\mapsto} (x, y)$,

(2) $(x, y) \overset{\iota}{\mapsto} (x, y + 1)$,

(3) $(x, y) \overset{u}{\mapsto} (\omega/x, y + \alpha)$,

(4) $(x, y) \overset{\iota u}{\mapsto} (\omega/x, y + \alpha + 1)$,

(5) $(x, y) \overset{v}{\mapsto} (\omega x, y)$,

(6) $(x, y) \overset{\iota v}{\mapsto} (\omega x, y + 1)$,

(7) $(x, y) \overset{v^2}{\mapsto} (\overline{\omega} x, y)$,

(8) $(x, y) \overset{\iota v^2}{\mapsto} (\overline{\omega} x, y + 1)$,

(9) $(x, y) \overset{vu}{\mapsto} (\overline{\omega}/x, y + \alpha)$,

(10) $(x, y) \overset{\iota vu}{\mapsto} (\overline{\omega}/x, y + \alpha + 1)$,

(11) $(x, y) \overset{v^2 u}{\mapsto} (1/x, y + \alpha)$,

(12) $(x, y) \overset{\iota v^2 u}{\mapsto} (1/x, y + \alpha + 1)$.

We state a theorem given by Kani and Rosen [9] without proof which we use to show that the Jacobian of the hyperelliptic curve given by (2) decomposes into two isogenous elliptic curves.

Theorem 7 (Kani and Rosen [9]). *Given a curve C, let G be a finite subgroup of Aut(C) such that $G = H_1 \cup \cdots \cup H_t$ where the subgroups H_i of G satisfy $H_i \cap H_j = 1_G$ if $i \neq j$. Then one has the following isogeny relation:*

$$J_C^{t-1} \times J_{C/G}^{g} \sim J_{C/H_1}^{h_1} \times \cdots \times J_{C/H_t}^{h_t}, \tag{3}$$

where $g = |G|$ and $h_i = |H_i|$ and J^m means the product of J with itself m times.

Theorem 8. *The Jacobian of the hyperelliptic curve*

$$C : y^2 + y = \frac{a}{x^3 + 1} \quad \textit{where } a = \alpha^2 + \alpha \textit{ for some } \alpha \in \overline{K}, \tag{4}$$

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

$$\begin{aligned} E_1 &: y^2 + (\alpha + 1) y = \frac{\alpha^4 + \alpha^2}{x^3 + x}, \\ E_2 &: y^2 + \alpha y = \frac{\alpha^4 + \alpha^2}{x^3 + x}. \end{aligned} \tag{5}$$

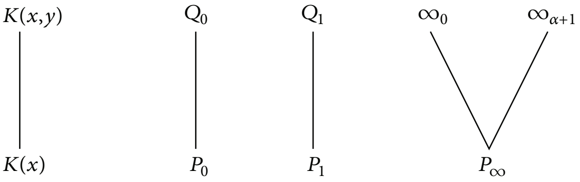

Figure 1: Elliptic function field.

Proof. Let $\sigma := v^2 u$ and $\tau := \iota v^2 u$ be automorphisms. We compute $C/\langle\sigma\rangle$ and $C/\langle\tau\rangle$. Since $x + x^{-1}$ and $y^2 + \alpha y$ are invariants under σ, we set $x + x^{-1} = s$, $y^2 + \alpha y = t$ and find the relation between s and t. We have

$$t^2 + (\alpha + 1) t = \frac{\alpha^4 + \alpha^2}{s^3 + s}. \tag{6}$$

Thus $C/\langle\sigma\rangle$ is

$$t^2 + (\alpha + 1) t = \frac{\alpha^4 + \alpha^2}{s^3 + s}. \tag{7}$$

By Hurwitz genus formula, (7) is a genus 1 curve. Similarly, we can compute $C/\langle\tau\rangle$. Since $x + x^{-1}$ and $y^2 + (\alpha + 1)y$ are invariants under τ, to compute $C/\langle\tau\rangle$ we plug in $\alpha + 1$ instead of α in (7) to get

$$t^2 + \alpha t = \frac{\alpha^4 + \alpha^2}{s^3 + s} \tag{8}$$

which is also a genus 1 curve. By applying Theorem 7 with $\text{Aut}(C) = D_{12}$, $G = \langle\iota\rangle \cup \langle\sigma\rangle \cup \langle\tau\rangle$, and $g = 4$, we have

$$\text{Jac}(C)^2 \times \text{Jac}\left(\mathbb{P}^1\right)^4 \sim \text{Jac}\left(\mathbb{P}^1\right)^2 \times E_1^2 \times E_2^2. \tag{9}$$

By applying Poincaré's complete reducibility theorem, we conclude that Jac(C) is isogenous to the product of the two elliptic curves (7) and (8). □

For ease of computation we transform the elliptic curves E_1 and E_2 into Weierstrass form. First, we consider

$$E_1 : y^2 + (\alpha + 1) y = \frac{\alpha^4 + \alpha^2}{x^3 + x} \tag{10}$$

with elliptic function field as in Figure 1.

In Figure 1, P_i is the zero of $x - i$ and P_∞ is the pole of x in $K(x)$. Q_i is the extension of P_i and ∞_0, $\infty_{\alpha+1}$ are extensions of P_∞. Since

$$\begin{aligned} \text{div}\left(\frac{1}{(x + 1) y}\right) &= -2\infty_0 + \infty_{\alpha+1} + Q_0 \in L\left(2\infty_0\right), \\ \text{div}\left(\frac{1}{y}\right) &= -3\infty_0 + Q_0 + 2Q_1 \in L\left(3\infty_0\right), \end{aligned} \tag{11}$$

we set

$$\frac{1}{(x+1)\,y} = X, \qquad \frac{1}{y} = Y \tag{12}$$

or

$$x = \frac{Y}{X} + 1, \qquad y = \frac{1}{Y}. \tag{13}$$

By plugging in x and y into E_1, we get

$$Y^2 + XY + \frac{1}{\alpha+1}Y = \alpha^2(\alpha+1)X^3 + \frac{1}{\alpha+1}X. \tag{14}$$

By the transformation

$$(X,Y) \longmapsto \left(\frac{X}{\alpha^2(\alpha+1)}, \frac{Y}{\alpha^2(\alpha+1)}\right), \tag{15}$$

the curve given by (14) is transformed into

$$Y^2 + XY + \alpha^2 Y = X^3 + \alpha^2 X. \tag{16}$$

By the transformation

$$(X,Y) \longmapsto \left(X + \alpha^2, Y + \alpha^2 + \alpha^4\right), \tag{17}$$

the curve given by (16) is transformed into

$$Y^2 + XY = X^3 + \alpha^2 X^2 + \alpha^8 + \alpha^6. \tag{18}$$

By the above transformations, we have the elliptic curve

$$E_3 : y^2 + xy = x^3 + \alpha^2 x^2 + \alpha^8 + \alpha^6 \tag{19}$$

which is isomorphic to E_1 with j-invariant $j = (\alpha^8 + \alpha^6)^{-1}$. We plug in $\alpha + 1$ into α in (19) to obtain the elliptic curve

$$E_4 : y^2 + xy = x^3 + (\alpha+1)^2 x^2 + \alpha^8 + \alpha^6 + \alpha^4 + \alpha^2 \tag{20}$$

which is isomorphic to E_2 with j-invariant $j = (\alpha^8 + \alpha^6 + \alpha^4 + \alpha^2)^{-1}$. From now on we consider the two elliptic curves

$$E_3 : y^2 + xy = x^3 + \alpha^2 x^2 + \alpha^8 + \alpha^6 \tag{21}$$

with $j_1 = (\alpha^8 + \alpha^6)^{-1}$ and

$$E_4 : y^2 + xy = x^3 + (\alpha+1)^2 x^2 + \alpha^8 + \alpha^6 + \alpha^4 + \alpha^2 \tag{22}$$

with $j_2 = (\alpha^8 + \alpha^6 + \alpha^4 + \alpha^2)^{-1}$.

4. Three-Isogeny of E_3 and E_4

The modular equation of level three is

$$\Phi_3(x,y) = x^4 + x^3y^3 + y^4 \tag{23}$$

which is the modular curve reduced modulo 2. Since $\Phi_3(j_1, j_2) = 0$, E_3 and E_4 are 3-isogenous. In this section we find a 3-isogeny from E_3 to E_4. We use the following theorem in [10] to find an isogeny.

Theorem 9 (Lercier [10]). *Let F be a subgroup (of odd order) of an elliptic curve E_a. If $b = a + \Sigma_{(X_s,Y_s)\in F^*} Y_s + Y_s^2$, then there exist isogenies between E_a and E_b of kernel F. One of these isogenies is given by*

$$(X,Y) \longmapsto \left(X + \sum_{S\in F^*} X_{P+S}, Y + \sum_{S\in F^*} Y_{P+S}\right), \tag{24}$$

where $E_a : y^2 + xy = x^3 + a$, $a \in \mathbb{F}_{2^n}^*$.

In order to find a 3-isogeny using Theorem 9 we first find the 3-torsion points of the elliptic curve E_3. Let $P = (x,y)$ be a point of the elliptic curve $E : y^2 + xy = x^3 + a_2x^2 + a_6$ over a field of even characteristic with a point $\mathcal{O}$ at infinity. Then $-P = (x, x+y)$ and the formula for doubling a point $P = (x,y)$ is

$$2P = \left(x^2 + \frac{a_6}{x^2}, \left(x + \frac{y}{x}\right)\left(x^2 + \frac{a_6}{x^2}\right) + \frac{a_6}{x^2}\right). \tag{25}$$

$P = (x,y)$ is a 3-torsion point if and only if $3P = \mathcal{O}$; that is, $2P = -P$. To find the 3-torsion points we set $x^2 + a_6(x^2)^{-1} = x$ or $x^4 + x^3 + a_6 = 0$. If the equation $x^4 + x^3 + a_6 = 0$ has four roots, say, x_1, x_2, x_3, and x_4, then

$$E[3] = \{\mathcal{O}, (x_1, \pm y_1), (x_2, \pm y_2), (x_3, \pm y_3), (x_4, \pm y_4)\}, \tag{26}$$

where $y_i^2 + x_iy_i = x_i^3 + a_2x_i^2 + a_6$. Now we find two of the 3-torsion points of E_3. Since α^2 is a root for $x^4 + x^3 + \alpha^8 + \alpha^6$ we plug in $x = \alpha^2$ in E_3 and solve for y to get $y = \alpha^4$ or $\alpha^2 + \alpha^4$. The two points $R_1 = (\alpha^2, \alpha^4)$ and $Q_1 = (\alpha^2, \alpha^2 + \alpha^4)$ are 3-torsion points of $E_3 : y^2 + xy = x^3 + \alpha^2x^2 + \alpha^8 + \alpha^6$. Let $F = \{\mathcal{O}, R_1, Q_1\}$ be a subgroup of the elliptic curve E_3 and let

$$\begin{aligned} E_3' &: y^2 + xy = x^3 + \alpha^8 + \alpha^6, \\ E_4' &: y^2 + xy = x^3 + \alpha^8 + \alpha^6 + \alpha^4 + \alpha^2 \end{aligned} \tag{27}$$

be two elliptic curves. There exists an isomorphism $\varphi_1 : E_3 \rightarrow E_3'$ defined by $\varphi_1(x,y) = (x, y + sx)$, where $s^2 + s = \alpha^2$. Then

$$\begin{aligned} \varphi_1(R_1) &= R_1' = \left(\alpha^2, \alpha^4 + s\alpha^2\right), \\ \varphi_1(Q_1) &= Q_1' = \left(\alpha^2, \alpha^2 + \alpha^4 + s\alpha^2\right), \\ \varphi_1(\mathcal{O}) &= \mathcal{O}. \end{aligned} \tag{28}$$

Then $F' = \{\mathcal{O}, R_1', Q_1'\}$ is a subgroup of an elliptic curve E_3'. We can apply Theorem 9 to E_3' and E_4' with subgroup F' to get a 3-isogeny $\varphi_2 : E_3' \rightarrow E_4'$ defined as

$$\begin{aligned} \varphi_2(x,y) = \Bigg(& x + \frac{\alpha^2}{x+\alpha^2} + \frac{\alpha^4}{(x+\alpha^2)^2}, \\ & y + \frac{\alpha^4}{x+\alpha^2} + \frac{\alpha^2y^2 + \alpha^4y + \alpha^{10} + \alpha^6}{(x+\alpha^2)^3}\Bigg). \end{aligned} \tag{29}$$

Define $\varphi_3 : E_4' \to E_4$ by

$$\varphi_3(x, y) = (x, y + (s + \omega)x). \tag{30}$$

Then φ_3 is an isomorphism from E_4' to E_4.

Let $\varphi = \varphi_3 \circ \varphi_2 \circ \varphi_1 : E_3 \to E_4$. Then

$$\begin{aligned}\varphi(x, y) = \Bigg(& x + \frac{\alpha^2}{x + \alpha^2} + \frac{\alpha^4}{(x + \alpha^2)^2}, \\ & y + \omega x + \frac{\alpha^4}{x + \alpha^2} \\ & + \frac{\alpha^2(y + sx)^2 + \alpha^4(y + sx) + \alpha^{10} + \alpha^6}{(x + \alpha^2)^3}\Bigg),\end{aligned} \tag{31}$$

where $s^2 + s = \alpha^2$ is a 3-isogeny over the extension field of K. Thus we have proved the following theorem.

Theorem 10. *Let E and E' be two elliptic curves defined over $\mathbb{F}_{2^n}$ by*

$$\begin{aligned} E &: y^2 + xy = x^3 + \alpha^2 x^2 + \alpha^8 + \alpha^6 \quad \textit{with } j = (\alpha^8 + \alpha^6)^{-1}, \\ E' &: y^2 + xy = x^3 + (\alpha + 1)^2 x^2 + \alpha^8 + \alpha^6 + \alpha^4 + \alpha^2 \\ &\qquad \textit{with } j = (\alpha^8 + \alpha^6 + \alpha^4 + \alpha^2)^{-1}. \end{aligned} \tag{32}$$

Then

$$\begin{aligned}\varphi(x, y) = \Bigg(& x + \frac{\alpha^2}{x + \alpha^2} + \frac{\alpha^4}{(x + \alpha^2)^2}, \\ & y + \omega x + \frac{\alpha^4}{x + \alpha^2} \\ & + \frac{\alpha^2(y + sx)^2 + \alpha^4(y + sx) + \alpha^{10} + \alpha^6}{(x + \alpha^2)^3}\Bigg),\end{aligned} \tag{33}$$

where ω is a primitive third root of unity and $s^2 + s = \alpha^2$ is a 3-isogeny over the extension field of $\mathbb{F}_{2^n}$.

5. VDP on Hyperelliptic Curves over Fields of Even Characteristic

In this section, we set up the VDP on the hyperelliptic curve C and prove that the VDP defined on the hyperelliptic curve C is hard in general by showing the existence of a distortion eigenvector base. We have shown that the Jacobian of

$$C : y^2 + y = \frac{a}{x^3 + 1} \tag{34}$$

decomposes into a product of two elliptic curves E_3 and E_4 which are 3-isogenous over the extension field that contains the third roots of unity and s, where $s^2 + s = \alpha^2$. E_3 and E_4 have the same number of points over the extension field. We set up the VDP on C as follows.

Choose

$$C : y^2 + y = \frac{a}{x^3 + 1} \tag{35}$$

such that E_3 has a large cyclic subgroup $\mathbb{Z}/m\mathbb{Z}$ of rational points over $\mathbb{F}_q$, where $q = 2^n$, n is odd, and m is a prime greater than 3. Then we choose as two-dimensional vector space $\mathcal{V}$ the m-torsion points $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ in the Jacobian of the hyperelliptic curve C over the extension field $\mathbb{F}_{q^2}$ and choose as one-dimensional subspace $\mathcal{V}'$ the subspace $\mathbb{Z}/m\mathbb{Z}$ of $\mathcal{V}$ that is rational over $\mathbb{F}_q$.

The following is a summary of the VDP setting:

$$C : y^2 + y = \frac{a}{x^3 + 1}, \quad a = \alpha^2 + \alpha. \tag{36}$$

Jac(C) is Jacobian of the curve C, as

$$\mathcal{V} = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}} \subset \operatorname{Jac}(C)(\mathbb{F}_{q^2}), \tag{37}$$

where $q = 2^n$, n is odd, and m is a prime greater than 3. Consider

$$\mathcal{V}' = \frac{\mathbb{Z}}{m\mathbb{Z}} \subset \operatorname{Jac}(C)(\mathbb{F}_q). \tag{38}$$

Let ω be a primitive third root of unity and let

$$\begin{aligned}\phi &: (x, y) \longmapsto (\omega x, y), \\ F &: (x, y) \longmapsto (x^q, y^q).\end{aligned} \tag{39}$$

Let $e \in \operatorname{Jac}(C)(\mathbb{F}_q)$ and let $l = 2^{-1} \pmod m$. We will show that $(e, \phi'(e))$ is a distortion eigenvector base, where $\phi' = l + \phi$.

Lemma 11. *For any element $e \in Jac(C)(\mathbb{F}_q)$, $q = 2^n$,*

$$\phi(\phi(e)) = -e - \phi(e), \tag{40}$$

and if n is odd then

$$F(\phi(e)) = -F(e) - \phi(F(e)) = -e - \phi(e). \tag{41}$$

Proof. Let P be a point in C. Since $\phi(\phi^2(P) + \phi(P) + P) = P + \phi^2(P) + \phi(P)$, $\phi^2(P) + \phi(P) + P$ is fixed by ϕ. Thus $\phi^2(P) + \phi(P) + P \in C/\langle\phi\rangle$. Since $\phi(x^3) = x^3$, $C/\langle\phi\rangle$ is

$$y^2 + y = \frac{a}{x + 1}. \tag{42}$$

Equation (42) has genus 0. Therefore the class number of the Jacobian of (42) is 1 and hence $\phi^2 + \phi + 1 = 0$. We have proved (40).

We need to show that $\phi^2 \circ F = F \circ \phi$:

$$\begin{aligned}(\phi^2 \circ F)(x, y) &= (\omega^2 x^q, y^q), \\ (F \circ \phi)(x, y) &= (\omega^q x^q, y^q).\end{aligned} \tag{43}$$

If n is odd, then $2 \equiv 2^n \pmod 3$ and hence $\phi^2 \circ F = F \circ \phi$. □

Theorem 12. *For an element $e \in Jac(C)(\mathbb{F}_q)$ of prime order $m > 3$, $\{e, \phi'(e)\}$ is a distortion eigenvector base for $\mathscr{V}$.*

Proof. We begin by showing that $\{e, \phi'(e)\}$ is an eigenvector base for $\mathscr{V}$. Suppose that $le + \phi(e) = \phi'(e) \in \langle e \rangle$; that is, $\phi(e) = \beta e$ for some $\beta \in \mathbb{Z}/m\mathbb{Z}$. Thus $\phi(e) \in \mathrm{Jac}(C)(\mathbb{F}_q)$. By (40) of Lemma 11, we have $\beta^2 e = -e - \beta e$; that is, $\beta^2 = -1 - \beta$. By (41) of Lemma 11, we have $\beta e = -e - \beta e$; that is, $(2\beta + 1)e = 0$. Thus

$$\begin{aligned} 0 &= (2\beta + 1)(2\beta + 1)e = \left(4\beta^2 + 4\beta + 1\right) \\ &= \left(-4 - 4\beta + 4\beta + 1\right)e = -3e. \end{aligned} \tag{44}$$

This is a contradiction to the assumption $m > 3$. Hence $\{e, \phi'(e)\}$ is a basis for $\mathscr{V}$. Note that $F(e) = e$. By Lemma 11, we have

$$\begin{aligned} F\left(\phi'(e)\right) &= F\left(le + \phi(e)\right) \\ &= le - e - \phi(e) \\ &= le - e + le - \phi'(e) \\ &= \phi'(e). \end{aligned} \tag{45}$$

Thus $\{e, \phi'(e)\}$ is an eigenvector base. Now we show that $\{e, \phi'(e)\}$ is a distortion eigenvector base by showing the existence of a homomorphism ϕ'' and an integer $d \not\equiv 0 \pmod{m}$ with the property $\phi''\phi' = d$ on $\langle e \rangle$. Let $\phi'' = l + \phi^2$ and let $d = l^2 - l + 1$. Since the dual isogeny $\widehat{\phi}$ of ϕ is $\widehat{\phi} = \phi^2$, we have

$$\begin{aligned} \phi''\phi' &= \left(l + \phi^2\right)\left(l + \phi\right) = l^2 + l\left(\phi^2 + \phi\right) + \phi^2\phi \\ &= l^2 - l + 1 = d. \end{aligned} \tag{46}$$

□

We have shown that the basis $\{e, \phi'(e)\}$ is a distortion eigenvector base and hence proved that the VDP for the proposed family of hyperelliptic curves is hard in general. It is permitted that the VDP be easy for some bases. In fact, for the bases $\{e, \phi(e)\}$ and $\{e, \phi'(e)\}$ the VDP can be solved easily. Using the criteria for strong bases for the VDP given in [8], we may choose $\{e_1, e_2\}$ with $e_1, e_2 \notin \langle e \rangle \cup \langle \phi(e) \rangle$ as our basis for the VDP, for example, $e_1 = \alpha_{11}e + \alpha_{12}\phi(e)$ and $e_2 = \alpha_{21}e + \alpha_{22}\phi(e)$, where $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in \mathbb{Z}/m\mathbb{Z}$ are nonzero and $\alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21} \not\equiv 0 \pmod{m}$.

6. Conclusion

Yoshida and Fujiwara introduced a new watermarking scheme for cryptographic data which is based on VDP. Duursma and Kiyavash showed that elliptic curves are not suitable for VDP and presented an infinite family of genus two hyperelliptic curves suitable for the VDP defined over a finite field of odd characteristic. In this paper, we introduce an infinite family of genus two hyperelliptic curves suitable for the VDP defined over a finite field of even characteristic.

Conflict of Interests

The author declares that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This research was supported by the Sookmyung Women's University Research Grants (1-1103-0682).

References

[1] M. Yoshida, S. Mitsunari, and T. Fujiwara, "Vector decomposition problem and the trapdoor inseparable multiplex transmission scheme based problem," in *Proceedings of the Symposium on Cryptography and Information Security (SCIS '03)*, 2003.

[2] S. D. Galbraith and E. R. Verheul, "An analysis of the vector decomposition problem," in *Public Key Cryptography—PKC 2008*, vol. 4939 of *Lecture Notes in Computer Science*, pp. 308–327, Springer, Berlin, Germany, 2008.

[3] M. Yoshida and T. Fujiwara, "Toward digital watermarking for cryptographic data," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E94-A, no. 1, pp. 270–272, 2011.

[4] M. Yoshida and T. Fujiwara, "Watermarking cryptographic data," in *Proceedings of the 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IH-MSP '09)*, pp. 40–43, September 2009.

[5] M. Yoshida, "Inseparable multiplex transmission using the pairing on elliptic curves and its application to watermarking," in *Proceedings of 5th Conference on Algebraic Geometry, Number Theory, Coding Theory and Cryptography, Graduate School of Mathematical Sciences, University of Tokyo*, 2003.

[6] I. Duursma and N. Kiyavash, "The vector decomposition problem for elliptic and hyperelliptic curves," *Journal of the Ramanujan Mathematical Society*, vol. 20, no. 1, pp. 59–76, 2005.

[7] N. P. Smart, "On the performance of hyperelliptic cryptosystems," in *Advances in Cryptology—EUROCRYPT '99*, vol. 1592 of *Lecture Notes in Computer Science*, pp. 165–175, Springer, Berlin, Germany, 1999.

[8] S. Kwon and H.-S. Lee, "Analysis of the strong instance for the vector decomposition problem," *Bulletin of the Korean Mathematical Society*, vol. 46, no. 2, pp. 245–253, 2009.

[9] E. Kani and M. Rosen, "Idempotent relations and factors of Jacobians," *Mathematische Annalen*, vol. 284, no. 2, pp. 307–327, 1989.

[10] R. Lercier, "Computing isogenies in F_{2^n}," in *Algorithmic Number Theory*, vol. 1122 of *Lecture Notes in Computer Science*, pp. 197–212, Springer, Berlin, Germany, 1996.