PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 109(123) (2021), 125–141 DOI: https://doi.org/10.2298/PIM2123125H

CONSTRUCTION OF METRICS ON THE SET OF ELLIPTIC CURVES OVER A FINITE FIELD

Keisuke Hakuta

Abstract. We consider metrics on the set of elliptic curves in short Weierstrass form over a finite field of characteristic greater than three. The metrics have been first found by Mishra and Gupta (2008). Vetro (2011) constructs other metrics which are independent on the choice of a generator of the multiplicative group of the underlying finite field, whereas the metrics found by Mishra and Gupta, are dependent on the choice of a generator of the multiplicative group of the underlying finite field. Hakuta (2015, 2018) constructs metrics on the set of non-supersingular elliptic curves in short Weierstrass form over a finite field of characteristic two and three, respectively. The aim of this paper is to point out that the metric found by Mishra and Gupta is in fact not a metric. We also construct new metrics which are slightly modified versions of the metric found by Mishra and Gupta.

1. Introduction

The theory of elliptic curves is one of the important and major objects in number theory and algebraic geometry, and has received much attention. There is no doubt that the reason is mainly due to not only their own theoretical interests but also practical and/or computational applications of elliptic curves such as elliptic curve cryptography ([**8**], [**12**]), primality tests (cf. [**1**]), integer factorization (cf. [**9**]), and so on. In particular, elliptic-curve cryptography is widely used in the field of public-key cryptography. In elliptic-curve cryptography, point multiplication (or scalar multiplication) is the most time-consuming operation, namely computing a multiplication-by-d map $[d]P = P + \cdots + P$ (d times) for a given point P on an elliptic curve E and a given positive integer d. The security of elliptic curve cryptography depends on the hardness of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). The ECDLP is to find a positive integer d, if it exists, such that $Q = [d]P \in E$. Let $\mathbb{F}_q$ be a finite field with q elements, $q = p^m$, p a prime, and $m \geqslant 1$. We set $\#E(\mathbb{F}_q) = q + 1 - t$. By the Hasse bound, we have $|t| \leqslant 2\sqrt{q}$ (for

2010 *Mathematics Subject Classification:* Primary 14H52; Secondary 11G20,11T71, 14G50, 94A60.

Key words and phrases: elliptic curves, isomorphism, metric.

Communicated by Zoran Petrovic.

example, see [**10**, Theorem 2.8], [**16**, Chapter V, Theorem 1.1]). The elliptic curve $E/\mathbb{F}_q$ is called *supersingular* if p divides t. Otherwise, the curve $E/\mathbb{F}_q$ is called *ordinary* (or *non-supersingular*). It is well known that if $p = 2$ or $p = 3$, then $E/\mathbb{F}_q$ is ordinary if and only if $j(E) \neq 0$ (for example, see [**10**, page 24]), where $j(E)$ is the j-invariant of E (See Section 2). It is known that the MOV attack works effectively for the ECDLP on supersingular elliptic curves (See [**11**, Theorem 11 and Corollary 12], [**16**, Section XI.6]). In order to avoid the MOV attack, the two types of elliptic curves are commonly used in practice, namely, non-supersingular elliptic curves over prime fields and non-supersingular elliptic curves over finite fields of characteristic two [**14**, Appendix D]. Thus, we mainly focus on non-supersingular elliptic curves in this paper.

On the other hand, point multiplication requires the secret information as an input. Side channel attacks are exploit (whole or partial) secret information that leaks from a cryptographic device. The fixed table attack which was introduced in [**6**], is a kind of side channel attack to analyze the power consumption of the computation of elliptic curve additions during the computation of point multiplication. There are some countermeasures against the fixed table attack (cf. [**2**], [**6**], [**7**]). The pioneer work by Joye and Tymen [**7**] is to use isomorphisms on elliptic curves for computation of point multiplication in order to protect the secret information from side channel attacks. Afterwards, Mishra and Gupta in [**13**] and Vetro in [**17**] have found metrics on the set of elliptic curves in simplified Weierstrass form over a prime field of characteristic greater than three, respectively. The metrics in [**17**] are independent on the choice of a generator of the multiplicative group of the underlying finite field, whereas the metrics in [**13**] are dependent on the choice of a generator of the multiplicative group of the underlying finite field. Mishra and Gupta in [**13**] and Vetro in [**17**] have proposed potential applications of the metrics to the protection of fixed table attack. Similarly, Hakuta in [**3**] (resp. in [**5**]) constructs metrics on the set of non-supersingular elliptic curves in simplified Weierstrass form over a finite field of characteristic two (resp. characteristic three). Rishivarman and Parthasarathy in [**15**] construct a metric on the set of non-supersingular elliptic curves in the simplified Weierstrass form over $\mathbb{F}_{2^5}$, but Hakuta in [**4**] pointed out that the metric found by Rishivarman and Parthasarathy in [**15**] is in fact not a metric.

Let $\mathcal{EC}(q)$ be the set of elliptic curves in short Weierstrass form over $\mathbb{F}_q$ (See Equation (2.4)). In this paper, we shall point out that the metric $d_{g,q}$ defined by (3.1) (which is found by Mishra and Gupta in [**13**]) is in fact not a metric (See the precise definition of the map $d_{g,q}$ in (3.1)). Moreover, we construct a new metric $\widetilde{d_{g,q}}$ defined by (5.3) which is a slightly modified version of the map $d_{g,q}$ defined by (3.1). More precisely, the main results of this paper are:

MAIN THEOREM 1. *The map $d_{g,q}$ defined by* (3.1) *is not a metric on $\mathcal{EC}(q)$.*

MAIN THEOREM 2. *$(\mathcal{EC}(q), \widetilde{d_{g,q}})$ is a metric space.*

2. Mathematical Preliminaries

In this section we collect some basic facts on elliptic curves. We refer the reader to [**10**], [**16**] for details of the facts on elliptic curves. Let $\mathbb{F}_q^* := \mathbb{F}_q \smallsetminus \{0\}$ be the multiplicative group of $\mathbb{F}_q$. We denote by $p := \mathrm{char}(\mathbb{F}_q)$ the characteristic of $\mathbb{F}_q$. Throughout the paper, we assume that $p = \mathrm{char}(\mathbb{F}_q) \geqslant 5$. We denote by $\mathbb{N}_+ := \mathbb{N} \smallsetminus \{0\}$, $\mathbb{Z}$, and $\mathbb{R}$, the sets of positive integers, rational integers, and real numbers, respectively, For a group $\mathbb{G}$ and an element x of $\mathbb{G}$, we denote by $\mathrm{ord}_{\mathbb{G}}(x)$ the order of $x \in \mathbb{G}$. For a set S, we represent the cardinality of the set S by $\sharp S$. Let g be a generator of the multiplicative group $\mathbb{F}_q^*$. Recall that there always exists $g \in \mathbb{F}_q^*$ such that $\mathbb{F}_q^* = \langle g \rangle$ since $\mathbb{F}_q^*$ is a cyclic group. Thus, there exists an integer $a \in \{0, 1, \ldots, q-2\}$ such that $h = g^a$ for arbitrary $h \in \mathbb{F}_q^*$. The integer a is called the *discrete logarithm* of $h \in \mathbb{F}_q^*$ to the base g, and we reserve the symbol $\mathrm{Log}_g(h)$ for the discrete logarithm of $h \in \mathbb{F}_q^*$ to the base g satisfying that $\mathrm{Log}_g(h) \in \{0, 1, \ldots, q-2\}$. Set $\mathcal{S}_q := \{0, \pm 1, \ldots, \pm(q-5)/2, \pm(q-3)/2, (q-1)/2\} \subsetneq \mathbb{Z}$. Then one can see that

$$\mathbb{F}_q^* = \langle g \rangle = \{g^k \mid 0 \leqslant k \leqslant q-2\} = \{g^k \mid k \in \mathcal{S}_q\}. \tag{2.1}$$

The set $\mathcal{S}_q$ is called a *standard index set* of the generator g. We also reserve the symbol $\mathrm{Log}_g^{\mathcal{S}_q}(h)$ for the discrete logarithm of $h \in \mathbb{F}_q^*$ to the base g satisfying that $\mathrm{Log}_g^{\mathcal{S}_q}(h) \in \mathcal{S}_q$. For $n \in \mathbb{N}_+$, let $\boldsymbol{\mu}_n(\mathbb{F}_q) := \{u \in \mathbb{F}_q^* \mid u^n = 1\}$ be the group of the n-th roots of unity.

Let $E/\mathbb{F}_q$ be an elliptic curve. It can be written as the *short Weierstrass form* (or *the simplified Weierstrass form*), i.e.,

$$E/\mathbb{F}_q : y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{F}_q$ and $\Delta(E) := -16(4a^3 + 27b^2) \neq 0$ in $\mathbb{F}_q$. We define $j(E) := -1728(4a)^3/\Delta(E)$. The symbols $\Delta(E)$ and $j(E)$ are called the discriminant of $E/\mathbb{F}_q$ and the j-invariant of $E/\mathbb{F}_q$, respectively. For two elliptic curves $E_1/\mathbb{F}_q : y^2 = x^3 + a_1x + b_1$ and $E_2/\mathbb{F}_q : y^2 = x^3 + a_2x + b_2$, we say that $E_1/\mathbb{F}_q$ and $E_2/\mathbb{F}_q$ are isomorphic (or $\mathbb{F}_q$-isomorphic) if there exist two morphisms (as algebraic varieties) from $E_1/\mathbb{F}_q$ to $E_2/\mathbb{F}_q$ and from $E_2/\mathbb{F}_q$ to $E_1/\mathbb{F}_q$ which are inverses of each other, or equivalently, if there exists $u \in \mathbb{F}_q^*$ such that

$$a_2 = u^4 a_1 \text{ and } b_2 = u^6 b_1. \tag{2.2}$$

When the two elliptic curves $E_1/\mathbb{F}_q$ and $E_2/\mathbb{F}_q$ are isomorphic over $\mathbb{F}_q$ via the $\mathbb{F}_q$-isomorphism ϕ_u, then the $\mathbb{F}_q$-isomorphism ϕ_u is given by

$$\phi_u : E_1 \to E_2, \quad (x, y) \mapsto (u^2x, u^3y). \tag{2.3}$$

We denote the $\mathbb{F}_q$-isomorphism $\phi_u : E_1 \to E_2$ by $E_1/\mathbb{F}_q \overset{\phi_u}{\cong} E_2/\mathbb{F}_q$.

Let $\mathcal{EC}(q)$ be the set of elliptic curves in the short Weierstrass form over $\mathbb{F}_q$, namely,

$$\mathcal{EC}(q) := \{E/\mathbb{F}_q : y^2 = x^3 + ax + b \mid a, b \in \mathbb{F}_q,\ \Delta(E) = -16(4a^3 + 27b^2) \neq 0\}. \tag{2.4}$$

We remark that there exist elliptic curves $E_1, E_2 \in \mathcal{EC}(q)$ such that $E_1 \neq E_2$ in $\mathcal{EC}(q)$ and $E_1/\mathbb{F}_q \cong E_2/\mathbb{F}_q$. Such an example is easily constructed. For example, pick up any $u \in \mathbb{F}_q^*$ such that $u^4 \neq 1$ or $u^6 \neq 1$. Such an element always exists since $p = \mathrm{char}(\mathbb{F}_q) \geqslant 5$. Then it satisfies $E_1 \neq E_2$ in $\mathcal{EC}(q)$ and $E_1/\mathbb{F}_q \cong E_2/\mathbb{F}_q$. There may exist several elements which define the same $\mathbb{F}_q$-isomorphism ϕ_u from E_1 to E_2. For two given $\mathbb{F}_q$-isomorphic elliptic curves $E_1/\mathbb{F}_q$ and $E_2/\mathbb{F}_q$, we define the set $\mathcal{U}(E_1, E_2)$ as $\mathcal{U}(E_1, E_2) := \{u \in \mathbb{F}_q^* \mid E_1/\mathbb{F}_q \overset{\phi_u}{\cong} E_2/\mathbb{F}_q\}$. The following theorem is the well known fact on the explicit description of the set $\mathcal{U}(E_1, E_2)$.

THEOREM 2.1 ([**10**, pp. 37–38]). *Let $E_i/\mathbb{F}_q : y^2 = x^3 + a_i x + b_i \in \mathcal{EC}(q)$ $(i = 1, 2)$ be two elliptic curves. Suppose that $p = \mathrm{char}(\mathbb{F}_q) \geqslant 5$, and $E_1/\mathbb{F}_q$ and $E_2/\mathbb{F}_q$ are isomorphic over $\mathbb{F}_q$ via the $\mathbb{F}_q$-isomorphism $\phi_u : E_1 \to E_2$, $(x, y) \mapsto (u^2 x, u^3 y)$ for some $u \in \mathbb{F}_q^*$. Then the followings hold.*

(1) *We assume that one of the following three conditions holds*:

(i) $a_1 \neq 0$ *and* $b_1 \neq 0$,

(ii) $a_1 = 0$, $b_1 \neq 0$, *and there does not exist* $\alpha \in \mathbb{F}_q^*$ *such that* $\mathrm{ord}_{\mathbb{F}_q^*}(\alpha) = 3$,

(iii) $a_1 \neq 0$, $b_1 = 0$, *and there does not exist* $\beta \in \mathbb{F}_q^*$ *such that* $\mathrm{ord}_{\mathbb{F}_q^*}(\beta) = 4$.

Then we have $\mathcal{U}(E_1, E_2) = \{\pm u\}$.

(2) *We assume that*

(iv) $a_1 = 0$, $b_1 \neq 0$, *and there exists* $\alpha \in \mathbb{F}_q^*$ *such that* $\mathrm{ord}_{\mathbb{F}_q^*}(\alpha) = 3$.

Then we have $\mathcal{U}(E_1, E_2) = \{\pm u, \pm \alpha u, \pm \alpha^2 u\}$.

(3) *We assume that*

(v) $a_1 \neq 0$, $b_1 = 0$, *and there exists* $\beta \in \mathbb{F}_q^*$ *such that* $\mathrm{ord}_{\mathbb{F}_q^*}(\beta) = 4$.

Then we have $\mathcal{U}(E_1, E_2) = \{u, \beta u, \beta^2 u, \beta^3 u\}$.

3. A map by Mishra and Gupta

In this section we briefly review the metric on $\mathcal{EC}(q)$ found by Mishra and Gupta in [**13**] [1]. Let $E_i/\mathbb{F}_q : y^2 = x^3 + a_i x + b_i \in \mathcal{EC}(q)$ $(i = 1, 2)$ be two elliptic curves. If $E_1/\mathbb{F}_q \cong E_2/\mathbb{F}_q$, then there exists $t \in \mathbb{F}_q^*$ such that $a_2 = t^4 a_1$ and $b_2 = t^6 b_1$. There exist several such elements which define the same $\mathbb{F}_q$-isomorphisms from E_1 to E_2. Let $\{t_1, \ldots, t_l\}$ be the subset of $\mathbb{F}_q^*$ of which the elements define the same $\mathbb{F}_q$-isomorphisms from E_1 to E_2. Set $t_i := g^{\gamma_i}$ for each i $(1 \leqslant i \leqslant l)$, where $\gamma_i \in \mathcal{S}_q$ $(1 \leqslant i \leqslant l)$. Take $r := \min\{\gamma_i \in \mathcal{S}_q \mid 1 \leqslant i \leqslant l\}$ and $t' := g^r$. We define the map $d_{g,q} : \mathcal{EC}(q) \times \mathcal{EC}(q) \to \mathbb{R} \cup \{\infty\}$ by

$$\begin{aligned} &(E_1, E_2) \mapsto |r|, \quad \text{if } E_1 \overset{\phi_{t'}}{\cong} E_2, \\ &(E_1, E_2) \mapsto \infty, \quad \text{otherwise}, \end{aligned} \tag{3.1}$$

where $\phi_{t'} : E_1 \to E_2$, $(x, y) \mapsto ({t'}^2 x, {t'}^3 y)$. Mishra and Gupta claimed to prove that the map $d_{g,q}$ is a metric on $\mathcal{EC}(q)$ [**13**, p. 1331].

[1] Originally, Mishra and Gupta in [**13**] proposed the metric on $\mathcal{EC}(p)$. Since the proposed metric can be naturally generalized to the metric on $\mathcal{EC}(q)$, we discuss in here the general case.

4. Remarks on the map $d_{g,q}$

The aim of this section is to give a proof of Main Theorem 1. In order to prove Main Theorem 1, we will show the following properties:

- The map $d_{g,q}$ does not satisfy the symmetry property for all $p = \mathrm{char}(\mathbb{F}_q) \geqslant 5$ and $m \in \mathbb{N}_+$ (Proposition 4.1).
- The map $d_{g,q}$ does not satisfy the non-degeneracy property for all $p = \mathrm{char}(\mathbb{F}_q) \geqslant 5$ and $m \in \mathbb{N}_+$ (Proposition 4.2).

By proving Proposition 4.1 and Proposition 4.2, we see that the map $d_{g,q}$ defined by (3.1) is in fact not a metric on $\mathcal{EC}(q)$ for all $p = \mathrm{char}(\mathbb{F}_q) \geqslant 5$ and $m \in \mathbb{N}_+$ (See Main Theorem 1). Throughout the section, we assume that $E_i/\mathbb{F}_q : y^2 = x^3 + a_i x + b_i \in \mathcal{EC}(q)$ $(i = 1, 2, 3)$ are elliptic curves over $\mathbb{F}_q$.

4.1. Some useful lemmas. Here we prove some useful lemmas which will be needed in Subection 4.2. Lemma 4.1 (resp. Lemma 4.2) allows us to obtain the concrete description of the set of 6-th roots of unity (resp. 4-th roots of unity).

LEMMA 4.1. *We have*

$$\boldsymbol{\mu}_6(\mathbb{F}_q) = \begin{cases} \{\pm 1, g^{\pm(q-1)/6}, g^{\pm(q-1)/3}\}, & \text{if } q \equiv 1 \bmod 3, \\ \{\pm 1\}, & \text{if } q \equiv 2 \bmod 3. \end{cases}$$

PROOF. It is obviously true that $\boldsymbol{\mu}_6(\mathbb{F}_q) \supset \{\pm 1\}$. If $\boldsymbol{\mu}_6(\mathbb{F}_q) \supsetneq \{\pm 1\}$ then it must satisfy $q \equiv 1 \bmod 3$, and hence we get the desired equation. □

LEMMA 4.2. *We have*

$$\boldsymbol{\mu}_4(\mathbb{F}_q) = \begin{cases} \{\pm 1, g^{\pm(q-1)/4}\}, & \text{if } q \equiv 1 \bmod 4, \\ \{\pm 1\}, & \text{if } q \equiv 3 \bmod 4. \end{cases}$$

PROOF. By the similar discussion as in the proof of Lemma 4.1, we can obtain the desired result. □

Lemma 4.3 shows that we can represent each element of $\mathcal{U}(E_1, E_2)$ explicitly as a power of the generator g of the multiplicative group $\mathbb{F}_q^*$ using an integer, say $\gamma \in \mathbb{Z}$. Recall that, from the assumption that $p = \mathrm{char}(\mathbb{F}_q) \neq 2, 3$, we have $\gcd(q, 6) = 1$. This yields that $q \equiv 1, 5, 7, 11 \bmod 12$. Thus, we have the followings (See [**10**, p. 38] for detailds):

- There exists an element $\alpha \in \mathbb{F}_q^*$ such that $\mathrm{ord}_{\mathbb{F}_q^*}(\alpha) = 3$ if and only if it satisfies that $q \equiv 1 \bmod 12$ or $q \equiv 7 \bmod 12$.
- There exists an element $\beta \in \mathbb{F}_q^*$ such that $\mathrm{ord}_{\mathbb{F}_q^*}(\beta) = 4$ if and only if it satisfies that $q \equiv 1 \bmod 12$ or $q \equiv 5 \bmod 12$.

LEMMA 4.3. *There exists an integer $\gamma \in \mathbb{Z}$ such that we can represent each element of $\mathcal{U}(E_1, E_2)$ explicitly as a power of the generator g of the multiplicative group $\mathbb{F}_q^*$ using $\gamma \in \mathbb{Z}$. More precisely, the followings hold:*
(1) *If one of the three conditions* (i), (ii), (iii) *in Theorem* 2.1 *holds, then*

$$\mathcal{U}(E_1, E_2) = \{g^{\gamma}, g^{\gamma+(q-1)/2}\}.$$

(2) *If condition* (iv) *in Theorem* 2.1 *holds, then*

$$\mathcal{U}(E_1, E_2) = \{g^{\gamma}, g^{\gamma \pm (q-1)/6}, g^{\gamma \pm (q-1)/3}, g^{\gamma+(q-1)/2}\}.$$

(3) *If condition* (v) *in Theorem* 2.1 *holds, then*

$$\mathcal{U}(E_1, E_2) = \{g^{\gamma}, g^{\gamma \pm (q-1)/4}, g^{\gamma+(q-1)/2}\}.$$

PROOF. (1) From Theorem 2.1(1), we have $\mathcal{U}(E_1, E_2) = \{\pm u\}$ for some $u \in \mathbb{F}_q^*$. Set $\gamma := \mathrm{Log}_g(u) \in \{0, 1, \ldots, q-2\} \subsetneq \mathbb{Z}$. Since $-u = (-1) \cdot u = g^{(q-1)/2} \cdot g^{\gamma} = g^{\gamma+(q-1)/2}$, we obtain $\mathcal{U}(E_1, E_2) = \{g^{\gamma}, g^{\gamma+(q-1)/2}\}$.

(2) Let $\alpha \in \mathbb{F}_q^*$ be an element of order 3. From Theorem 2.1(2), we have $\mathcal{U}(E_1, E_2) = \{\pm u, \pm \alpha u, \pm \alpha^2 u\}$ for some $u \in \mathbb{F}_q^*$. Set $\gamma := \mathrm{Log}_g(u) \in \{0, 1, \ldots, q-2\} \subsetneq \mathbb{Z}$. Then by Lemma 4.1, it holds that $\{\alpha, \pm\alpha^2\} = \{g^{\pm(q-1)/6}, g^{\pm(q-1)/3}\}$. Remark that $q \equiv 1 \bmod 12$ or $q \equiv 7 \bmod 12$ since $q \equiv 1 \bmod 3$. Therefore, we have

$$\mathcal{U}(E_1, E_2) = \{g^{\gamma}, g^{\gamma \pm (q-1)/6}, g^{\gamma \pm (q-1)/3}, g^{\gamma+(q-1)/2}\}.$$

(3) Let $\beta \in \mathbb{F}_q^*$ be an element of order 4. From Theorem 2.1(3), we have $\mathcal{U}(E_1, E_2) = \{u,\ \beta u,\ \beta^2 u,\ \beta^3 u\}$ for some $u \in \mathbb{F}_q^*$. Set $\gamma := \mathrm{Log}_g(u) \in \{0, 1, \ldots, q-2\} \subsetneq \mathbb{Z}$. Then by Lemma 4.2, it holds that $\{\beta, \beta^2, \beta^3\} = \{g^{\pm(q-1)/4}, -1\} = \{g^{\pm(q-1)/4}, g^{(q-1)/2}\}$. Remark that $q \equiv 1 \bmod 12$ or $q \equiv 5 \bmod 12$ since $q \equiv 1 \bmod 4$. Therefore, we have $\mathcal{U}(E_1, E_2) = \{g^{\gamma}, g^{\gamma \pm (q-1)/4}, g^{\gamma+(q-1)/2}\}$. □

In Lemma 4.3, the discrete logarithm of each element of $\mathcal{U}(E_1, E_2)$ to the base g belongs to $\mathbb{Z}$. On the other hand, Lemma 4.4 shows that we can take the discrete logarithm of each element of $\mathcal{U}(E_1, E_2)$ to the base g belongs to the standard index set $\mathcal{S}_q$ by using Equation (2.1).

LEMMA 4.4. *There exists an integer $\gamma \in \mathcal{S}_q$ such that we can represent each element of $\mathcal{U}(E_1, E_2)$ explicitly as a power of the generator g of the multiplicative group $\mathbb{F}_q^*$ using $\gamma \in \mathcal{S}_q$. More precisely, the followings hold:*
(1) *If one of the three conditions* (i), (ii), (iii) *in Theorem* 2.1 *holds, then we have*

$$\mathcal{U}(E_1, E_2) = \{g^{\gamma}, g^{\gamma+(q-1)/2}\}$$

and $\gamma, \gamma + (q-1)/2 \in \mathcal{S}_q$.
(2) *If condition* (iv) *in Theorem* 2.1 *holds, then we have*

$$\mathcal{U}(E_1, E_2) = \{g^{\gamma}, g^{\gamma+(q-1)/6}, g^{\gamma+(q-1)/3}, g^{\gamma+(q-1)/2}, g^{\gamma+2(q-1)/3}, g^{\gamma+5(q-1)/6}\},$$

and $\gamma + i(q-1)/6 \in \mathcal{S}_q$ for $0 \leqslant i \leqslant 5$.
(3) *If condition* (v) *in Theorem* 2.1 *holds, then we have*

$$\mathcal{U}(E_1, E_2) = \{g^{\gamma}, g^{\gamma+(q-1)/4}, g^{\gamma+(q-1)/2}, g^{\gamma+3(q-1)/4}\},$$

and $\gamma + i(q-1)/4 \in \mathcal{S}_q$ for $0 \leqslant i \leqslant 3$.

PROOF. The proof of Lemma 4.4 is the exact word to word translation of the proof of Lemma 4.3. □

For two integers i, j satisfying $1 \leqslant i, j \leqslant 3$, we define

$$\mathcal{S}_{q,\mathcal{U}}^{(i,j)} := \{\mathrm{Log}_g^{\mathcal{S}_q}(t) \in \mathcal{S}_q \mid t \in \mathcal{U}(E_i, E_j)\} = \{k \in \mathcal{S}_q \mid g^k \in \mathcal{U}(E_i, E_j)\}.$$

Since $\mathcal{S}_q \subsetneq \mathbb{Z}$ is a finite set, so is $\mathcal{S}_{q,\mathcal{U}}^{(i,j)} \subsetneq \mathcal{S}_q$. Put $l := \sharp\mathcal{S}_{q,\mathcal{U}}^{(i,j)}$, and we rewrite $\mathcal{S}_{q,\mathcal{U}}^{(i,j)}$ as $\mathcal{S}_{q,\mathcal{U}}^{(i,j)} = \{k_1^{(i,j)}, \ldots, k_l^{(i,j)}\}$. Moreover, by changing the indices if necessary, we may assume that $k_1^{(i,j)} < k_2^{(i,j)} < \cdots < k_l^{(i,j)}$. Lemma 4.5 tells us that the subtraction of the two consecutive values $k_n^{(1,2)}$ and $k_{n+1}^{(1,2)}$ in $\mathcal{S}_{q,\mathcal{U}}^{(1,2)}$ is always constant for each n $(1 \leqslant n \leqslant l-1)$.

LEMMA 4.5. *For each n $(1 \leqslant n \leqslant l-1)$, we have*

$$k_{n+1}^{(1,2)} - k_n^{(1,2)} = |k_{n+1}^{(1,2)} - k_n^{(1,2)}| = (q-1)/\sharp\mathcal{S}_{q,\mathcal{U}}^{(1,2)}.$$

Here, $|\cdot|$ is the usual absolute value on $\mathbb{R}$.

PROOF. The statement is an immediate consequence of Lemma 4.4. □

We define four maps $\tau_1, \tau_2, \tau_3, \tau_4 : \mathcal{S}_q \to \mathcal{S}_q$, to prove Lemma 4.6 below, where the maps τ_2, τ_3 are defined if $q \equiv 1 \bmod 12$ or $q \equiv 7 \bmod 12$, and the map τ_4 is defined if $q \equiv 1 \bmod 12$ or $q \equiv 5 \bmod 12$. These four maps are useful to rewrite the statement of Lemma 4.4 in the form of Lemma 4.6, and are defined by

$$\tau_1 : \begin{cases} \gamma \mapsto \gamma + (q-1)/2, & \text{if } -(q-3)/2 \leqslant \gamma \leqslant 0, \\ \gamma \mapsto \gamma - (q-1)/2, & \text{otherwise,} \end{cases}$$

$$\tau_2 : \begin{cases} \gamma \mapsto \gamma + (q-1)/6, & \text{if } -(q-3)/2 \leqslant \gamma \leqslant (q-1)/3, \\ \gamma \mapsto \gamma - 5(q-1)/6, & \text{otherwise,} \end{cases}$$

$$\tau_3 : \begin{cases} \gamma \mapsto \gamma + (q-1)/3, & \text{if } -(q-3)/2 \leqslant \gamma \leqslant (q-1)/6, \\ \gamma \mapsto \gamma - 2(q-1)/3, & \text{otherwise,} \end{cases}$$

$$\tau_4 : \begin{cases} \gamma \mapsto \gamma + (q-1)/4, & \text{if } -(q-3)/2 \leqslant \gamma \leqslant (q-1)/4, \\ \gamma \mapsto \gamma - 3(q-1)/4, & \text{otherwise.} \end{cases}$$

Lemma 4.6 shows that the discrete logarithm of each element in $\mathcal{U}(E_1, E_2)$ to the base g can be represented using the maps τ_1, τ_2, τ_3, and τ_4.

LEMMA 4.6. *Let $\gamma := \min \mathcal{S}_{q,\mathcal{U}}^{(1,2)}$. Then each element in $\mathcal{U}(E_1, E_2)$ can be represented by $\gamma \in \mathcal{S}_{q,\mathcal{U}}^{(1,2)} \subsetneq \mathcal{S}_q$ and the four maps τ_1, τ_2, τ_3, and τ_4. More precisely, the followings hold:*

(1) *If one of the three conditions* (i), (ii), (iii) *in Theorem* 2.1 *holds, then we have*

$$\mathcal{U}(E_1, E_2) = \{g^\gamma, g^{\tau_1(\gamma)}\}.$$

(2) *If condition* (iv) *in Theorem* 2.1 *holds, then we have*

$$\mathcal{U}(E_1, E_2) = \{g^\gamma, g^{\tau_2(\gamma)}, g^{\tau_3(\gamma)}, g^{\tau_1(\gamma)}, g^{\tau_1(\tau_2(\gamma))}, g^{\tau_1(\tau_3(\gamma))}\}.$$

(3) *If condition* (v) *in Theorem* 2.1 *holds, then we have*

$$\mathcal{U}(E_1, E_2) = \{g^\gamma, g^{\tau_4(\gamma)}, g^{\tau_1(\gamma)}, g^{\tau_1(\tau_4(\gamma))}\}.$$

PROOF. It follows immediately from Lemma 4.4 and the definition of the maps τ_1, τ_2, τ_3, and τ_4. □

The following lemma is useful to prove that the map $d_{g,q}$ does not satisfy the symmetry property of the metric for all $p = \mathrm{char}(\mathbb{F}_q) \geqslant 5$ and $m \in \mathbb{N}_+$ (See Proposition 4.1).

LEMMA 4.7. *Let* $\gamma := \min \mathcal{S}_{q,\mathcal{U}}^{(1,2)}$. *Then the followings hold:*
(1) *If one of the three conditions* (i), (ii), (iii) *in Theorem* 2.1 *holds, then we have*

$$\min \mathcal{S}_{q,\mathcal{U}}^{(2,1)} = \begin{cases} 0, & \text{if } \gamma = \min \mathcal{S}_{q,\mathcal{U}}^{(1,2)} = 0, \\ -\tau_1(\gamma), & \text{otherwise.} \end{cases} \tag{4.1}$$

(2) *If condition* (iv) *in Theorem* 2.1 *holds, then we have*

$$\min \mathcal{S}_{q,\mathcal{U}}^{(2,1)} = \begin{cases} -(q-1)/3, & \text{if } \gamma = \min \mathcal{S}_{q,\mathcal{U}}^{(1,2)} = -(q-1)/3, \\ -\tau_1(\tau_3(\gamma)), & \text{otherwise.} \end{cases} \tag{4.2}$$

(3) *If condition* (v) *in Theorem* 2.1 *holds, then we have*

$$\min \mathcal{S}_{q,\mathcal{U}}^{(2,1)} = \begin{cases} -(q-1)/4, & \text{if } \gamma = \min \mathcal{S}_{q,\mathcal{U}}^{(1,2)} = -(q-1)/4, \\ -\tau_1(\tau_4(\gamma)), & \text{otherwise.} \end{cases} \tag{4.3}$$

PROOF. We remark that $-(q-1)/2 \equiv (q-1)/2 \bmod (q-1)$ and $(q-1)/2 \in \mathcal{S}_q$. We also remark that from $\gamma = \min \mathcal{S}_{q,\mathcal{U}}^{(1,2)}$, Lemma 4.5, and Lemma 4.7, $\gamma \neq (q-1)/2$ holds.
(1) By applying Lemma 4.6(1), we have $\mathcal{S}_{q,\mathcal{U}}^{(1,2)} = \{\gamma, \tau_1(\gamma)\}$. If $\gamma = 0$, then $\mathcal{S}_{q,\mathcal{U}}^{(1,2)} = \{0, (q-1)/2\} = \mathcal{S}_{q,\mathcal{U}}^{(2,1)}$. Therefore, $\min \mathcal{S}_{q,\mathcal{U}}^{(2,1)} = 0$. Next, we assume that $\gamma \neq 0$. Then by Lemma 4.5, the inequalities $-(q-3)/2 \leqslant \gamma < 0$ and $0 < -\tau_1(\gamma) < (q-1)/2$ hold, or equivalently, the inequalities $0 < -\gamma \leqslant (q-3)/2$ and $-(q-1)/2 < \tau_1(\gamma) < 0$ hold. This implies that $\mathcal{S}_{q,\mathcal{U}}^{(2,1)} = \{-\tau_1(\gamma), -\gamma\} \subset \mathcal{S}_q$ and $\min \mathcal{S}_{q,\mathcal{U}}^{(2,1)} = -\tau_1(\gamma)$ when $\gamma \neq 0$. Thus, we obtain Equation (4.1).

(2) By Lemma 4.6(2), we have $\mathcal{S}_{q,\mathcal{U}}^{(1,2)} = \{\gamma, \tau_2(\gamma), \tau_3(\gamma), \tau_1(\gamma), \tau_1(\tau_2(\gamma)), \tau_1(\tau_3(\gamma))\}$. Since $\gamma = \min \mathcal{S}_{q,\mathcal{U}}^{(1,2)}$, it is easy to verify that

$$\gamma < \tau_2(\gamma) < \tau_3(\gamma) < \tau_1(\gamma) < \tau_1(\tau_2(\gamma)) < \tau_1(\tau_3(\gamma)).$$

If $\gamma = -(q-1)/3$, then $\mathcal{S}_{q,\mathcal{U}}^{(1,2)} = \{0, \pm(q-1)/6, \pm(q-1)/3, (q-1)/2\} = \mathcal{S}_{q,\mathcal{U}}^{(2,1)}$. Hence, we have $\min \mathcal{S}_{q,\mathcal{U}}^{(2,1)} = -(q-1)/3$. Next, we assume that $\gamma \neq -(q-1)/3$. Then by Lemma 4.5, the following inequalities hold

$$\begin{gathered} -(q-3)/2 \leqslant \gamma < -(q-1)/3, \quad -(q-1)/3 \leqslant \tau_2(\gamma) < -(q-1)/6, \\ -(q-1)/6 \leqslant \tau_3(\gamma) < 0, \quad 0 \leqslant \tau_1(\gamma) < (q-1)/6, \\ (q-1)/6 \leqslant \tau_1(\tau_2(\gamma)) < (q-1)/3, \quad (q-1)/3 \leqslant \tau_1(\tau_3(\gamma)) < (q-1)/2. \end{gathered}$$

In other words, we have the inequalities

$$-(q-1)/2 < -\tau_1(\tau_3(\gamma)) \leqslant -(q-1)/3, \quad -(q-1)/3 < -\tau_1(\tau_2(\gamma)) \leqslant -(q-1)/6,$$
$$-(q-1)/6 < -\tau_1(\gamma) \leqslant 0, \quad 0 < -\tau_3(\gamma) \leqslant (q-1)/6,$$
$$(q-1)/6 \leqslant -\tau_2(\gamma) \leqslant (q-1)/3, \quad (q-1)/3 \leqslant -\gamma \leqslant (q-3)/2,$$
$$-\tau_1(\tau_3(\gamma)) < -\tau_1(\tau_2(\gamma)) < -\tau_1(\gamma) < -\tau_3(\gamma) < -\tau_2(\gamma) < -\gamma.$$

This shows that $\mathcal{S}^{(2,1)}_{q,\mathcal{U}} = \{-\gamma, -\tau_2(\gamma), -\tau_3(\gamma), -\tau_1(\gamma), -\tau_1(\tau_2(\gamma)), -\tau_1(\tau_3(\gamma))\} \subset \mathcal{S}_q$ and $\min \mathcal{S}^{(2,1)}_{q,\mathcal{U}} = -\tau_1(\tau_3(\gamma))$. Finally, we obtain Equation (4.2).

(3) By Lemma 4.6(3), we have $\mathcal{S}^{(1,2)}_{q,\mathcal{U}} = \{\gamma, \tau_4(\gamma), \tau_1(\gamma), \tau_1(\tau_4(\gamma))\}$. Since $\gamma = \min \mathcal{S}^{(1,2)}_{q,\mathcal{U}}$, it is easy to verify that $\gamma < \tau_4(\gamma) < \tau_1(\gamma) < \tau_1(\tau_4(\gamma))$. If $\gamma = -(q-1)/4$, then $\mathcal{S}^{(1,2)}_{q,\mathcal{U}} = \{0, \pm(q-1)/4, (q-1)/2\} = \mathcal{S}^{(2,1)}_{q,\mathcal{U}}$. Hence, we have $\min \mathcal{S}^{(2,1)}_{q,\mathcal{U}} = -(q-1)/4$. Next, we assume that $\gamma \neq -(q-1)/4$. Then by Lemma 4.5, the following inequalities hold

$$-(q-3)/2 \leqslant \gamma < -(q-1)/4, \quad -(q-1)/4 \leqslant \tau_4(\gamma) < 0,$$
$$0 \leqslant \tau_1(\gamma) < (q-1)/4, \quad (q-1)/4 \leqslant \tau_1(\tau_4(\gamma)) < (q-1)/2.$$

In other words, we have the inequalities

$$-(q-1)/2 < -\tau_1(\tau_4(\gamma)) \leqslant -(q-1)/4, \quad -(q-1)/4 < -\tau_1(\gamma) \leqslant 0,$$
$$0 < -\tau_4(\gamma) \leqslant (q-1)/4, \quad (q-1)/4 < -\gamma \leqslant (q-3)/2,$$
$$-\tau_1(\tau_4(\gamma)) < -\tau_1(\gamma) < -\tau_4(\gamma) < -\gamma.$$

This shows that $\mathcal{S}^{(2,1)}_{q,\mathcal{U}} = \{-\gamma, -\tau_4(\gamma), -\tau_1(\gamma), -\tau_1(\tau_4(\gamma))\} \subset \mathcal{S}_q$ and $\min \mathcal{S}^{(2,1)}_{q,\mathcal{U}} = -\tau_1(\tau_4(\gamma))$. Thus, we obtain Equation (4.3).
This completes the proof of Lemma 4.7. □

4.2. Remarks on the map $d_{g,q}$. Here we prove Proposition 4.1 and Proposition 4.2. We first remark that the map $d_{g,q} : \mathcal{EC}(q) \times \mathcal{EC}(q) \to \mathbb{R} \cup \{\infty\}$ defined by (3.1) can be rewritten as

$$(E_1, E_2) \mapsto r, \quad \text{if } E_1 \overset{\phi_u}{\cong} E_2,$$
$$(E_1, E_2) \mapsto \infty, \quad \text{otherwise},$$

where $r := \min \mathcal{S}^{(1,2)}_{q,\mathcal{U}}$ and $u := g^r \in \mathcal{U}(E_1, E_2)$. As described in Lemma 4.8, the symmetry property of the map $d_{g,q}$ holds only under very restrictive conditions.

LEMMA 4.8. *Suppose that $p = \mathrm{char}(\mathbb{F}_q) \geqslant 5$. Let $E_1/\mathbb{F}_q$, $E_2/\mathbb{F}_q$ be elliptic curves, and let $\gamma := \min \mathcal{S}^{(1,2)}_{q,\mathcal{U}}$.*

1. *We assume that one of the three conditions* (i), (ii), (iii) *in Theorem* 2.1 *holds. If $\gamma \neq 0$ and $\gamma \neq -(q-1)/4$ then we have $d_{g,q}(E_1, E_2) \neq d_{g,q}(E_2, E_1)$.*
2. *We assume that condition* (iv) *in Theorem* 2.1 *holds. If $\gamma \neq -(q-1)/3$ and $\gamma \neq -5(q-1)/12$ then we have $d_{g,q}(E_1, E_2) \neq d_{g,q}(E_2, E_1)$.*

(3) *We assume that condition* (v) *in Theorem* 2.1 *holds. If* $\gamma \neq -(q-1)/4$ *and* $\gamma \neq -3(q-1)/8$ *then we have* $d_{g,q}(E_1, E_2) \neq d_{g,q}(E_2, E_1)$.

Proof. From Lemma 4.4 (or Lemma 4.5), it is easy to see that $\gamma \leqslant 0$. Moreover, if condition (iv) or condition (v) in Theorem 2.1 holds, then we have $\gamma < 0$.

(1) We remark that if $\gamma = 0$, then we have $d_{g,q}(E_1, E_2) = d_{g,q}(E_2, E_1)$ since $E_1 = E_2$. We next assume that $\gamma \neq 0$. By Lemma 4.4(1) and $\gamma < 0$, we have $d_{g,q}(E_1, E_2) = -\gamma$ and $d_{g,q}(E_2, E_1) = \gamma + (q-1)/2$. If $d_{g,q}(E_1, E_2) = d_{g,q}(E_2, E_1)$ holds, then we have $\gamma = -(q-1)/4$. Thus, $d_{g,q}(E_1, E_2) \neq d_{g,q}(E_2, E_1)$ holds except for $\gamma = 0$ and $\gamma = -(q-1)/4$.

(2) It is easy to verify that $E_1 = E_2$ when $\gamma = -(q-1)/3$. Assume that $\gamma \neq -(q-1)/3$. From Lemma 4.4(2), the equations $d_{g,q}(E_1, E_2) = -\gamma$ and $d_{g,q}(E_2, E_1) = \gamma + 5(q-1)/6$ hold. When $d_{g,q}(E_1, E_2) = d_{g,q}(E_2, E_1)$, then it must satisfy that $\gamma = -5(q-1)/12$. Note that $-5(q-1)/12 \in \mathcal{S}_q$ if and only if $q \equiv 1 \bmod 12$. Hence, $d_{g,q}(E_1, E_2) \neq d_{g,q}(E_2, E_1)$ holds except for $\gamma = -(q-1)/3$ and $\gamma = -5(q-1)/12$.

(3) When $\gamma = -(q-1)/4$, we have $E_1 = E_2$. Suppose that $\gamma \neq -(q-1)/4$. By Lemma 4.4(3), we obtain the two equations $d_{g,q}(E_1, E_2) = -\gamma$ and $d_{g,q}(E_2, E_1) = \gamma + 3(q-1)/4$. This implies that $d_{g,q}(E_1, E_2) = d_{g,q}(E_2, E_1)$ holds for the case $-3(q-1)/8$. Remark that $-3(q-1)/8 \in \mathcal{S}_q$ if and only if $q \equiv 1 \bmod 8$. Therefore, $d_{g,q}(E_1, E_2) \neq d_{g,q}(E_2, E_1)$ holds except for $\gamma = -(q-1)/4$ and $\gamma = -3(q-1)/8$. □

By Lemma 4.8, one can obtain that the symmetry property of the map $d_{g,q}$ *does not* hold.

Proposition 4.1. *Suppose that* $p = \mathrm{char}(\mathbb{F}_q) \geqslant 5$. *Then there exist elliptic curves* E_1, E_2 *over* $\mathbb{F}_q$ *such that* $d_{g,q}(E_1, E_2) \neq d_{g,q}(E_2, E_1)$. *In other words, the map* $d_{g,q}$ *defined by* (3.1) *does not hold the symmetry property of the map* $d_{g,q}$.

Proof. It fillows immediately from Lemma 4.8. □

As said in Proposition 4.2, the non-degeneracy property of the map $d_{g,q}$ *does not* hold.

Proposition 4.2. *Suppose that* $p = \mathrm{char}(\mathbb{F}_q) \geqslant 5$. *Then there exists an elliptic curve* E *over* $\mathbb{F}_q$ *such that* $d_{g,q}(E, E) \neq 0$. *In other words, the map* $d_{g,q}$ *defined by* (3.1) *does not hold the non-degeneracy property.*

Proof. Suppose that $q \not\equiv 11 \bmod 12$. Let $E/\mathbb{F}_q \in \mathcal{EC}(q)$ be an elliptic curve defined by the equation $y^2 = x^3 + ax + b$ $(a, b \in \mathbb{F}_q)$. By $E/\mathbb{F}_q \cong E/\mathbb{F}_q$ and by Equation (2.2), we have $a = u^4 a = a$ and $b = u^6 b = b$, namely, $a(u^4 - 1) = 0$ and $b(u^6 - 1) = 0$. Then the four cases may occur:

$$\begin{aligned} &\text{(A)}\ \ a = 0,\ \ b = 0, && \text{(C)}\ \ u^4 - 1 = 0,\ \ b = 0, \\ &\text{(B)}\ \ a = 0,\ \ u^6 - 1 = 0, && \text{(D)}\ \ u^4 - 1 = 0,\ \ u^6 - 1 = 0. \end{aligned}$$

If $a = 0$ and $b = 0$, then it is obvious that E is not an elliptic curve. Therefore, case (A) does not occur. If $u^4 - 1 = 0$ and $u^6 - 1 = 0$, then we have $u^4 - 1 =$

$(u-1)(u+1)(u^2+1)=0$ and $u^6-1=(u-1)(u+1)(u^2+u+1)(u^2-u+1)=0$. Since $u\in\mathbb{F}_q^*$, the two equations $u^2+1=0$ and $u^2+u+1=0$ do not have any common root in $\mathbb{F}_q^*$. Similarly, the two equations $u^2+1=0$ and $u^2-u+1=0$ do not have any common root in $\mathbb{F}_q^*$. Hence, the two equations $u^4-1=0$ and $u^6-1=0$ have two common roots $u=\pm 1$. In this case, by the definition of the map $d_{g,q}$ defined by (3.1), we have $d_{g,q}(E,E)=0$. This yields that there is nothing to prove in case (D). Thus, it suffices to consider only case (B) and case (C).

Case 1. $a=0$ and $u^6-1=0$. We further assume that $q\not\equiv 5 \bmod 12$. Let $u_1\in\mathbb{F}_q^*$ be a solution of the equation $u^6-1=0$. Since $\gcd(q,6)=1$, $q\not\equiv 11 \bmod 12$, and $q\not\equiv 5 \bmod 12$, we have $q\equiv 1 \bmod 12$ or $q\equiv 7 \bmod 12$. For both cases $q\equiv 1 \bmod 12$ and $q\equiv 7 \bmod 12$, we have $q\equiv 1 \bmod 3$. By Theorem 2.1(2) and Lemma 4.1, it is easy to see that

$$u_1\in\boldsymbol{\mu}_6(\mathbb{F}_q)=\mathcal{U}(E,E)=\{\pm 1, g^{\pm(q-1)/6}, g^{\pm(q-1)/3}\}. \tag{4.4}$$

By Equation (4.4) and the definition of the map $d_{g,q}$ defined by (3.1), we obtain $d_{g,q}(E,E)=|\min \mathcal{S}^{(1,2)}_{q,\,\mathcal{U}}|=|-(q-1)/3|=(q-1)/3\neq 0$.

Case 2. $u^4-1=0$ and $b=0$. We further assume that $q\not\equiv 7 \bmod 12$. Let $u_2\in\mathbb{F}_q^*$ be a solution of the equation $u^4-1=0$. Since $\gcd(q,6)=1$, $q\not\equiv 11 \bmod 12$, and $q\not\equiv 7 \bmod 12$, we have $q\equiv 1 \bmod 12$ or $q\equiv 5 \bmod 12$. For both cases $q\equiv 1 \bmod 12$ and $q\equiv 5 \bmod 12$, we have $q\equiv 1 \bmod 4$. By Theorem 2.1(3) and Lemma 4.2, it is easy to see that

$$u_2\in\boldsymbol{\mu}_4(\mathbb{F}_q)=\mathcal{U}(E,E)=\{\pm 1, g^{\pm(q-1)/4}\}. \tag{4.5}$$

By Equation (4.5) and the definition of the map $d_{g,q}$ defined by (3.1), we obtain $d_{g,q}(E,E)=|\min \mathcal{S}^{(1,2)}_{q,\,\mathcal{U}}|=|-(q-1)/4|=(q-1)/4\neq 0$. □

Corollary 4.1. *Suppose that* $p=\mathrm{char}(\mathbb{F}_q)\geqslant 5$.

(1) *If an elliptic curve* $E/\mathbb{F}_q$ *has* j*-invariant* 0 *or* 1728*, then it always satisfies that* $d_{g,q}(E,E)\neq 0$,
(2) *If an elliptic curve* $E/\mathbb{F}_q$ *has* $\sharp\,\mathrm{Aut}(E)=4$ *or* $\sharp\,\mathrm{Aut}(E)=6$*, then it always satisfies that* $d_{g,q}(E,E)\neq 0$*, where* $\mathrm{Aut}(E)$ *is the automorphism group of* E.

Proof. It is immediately from the proof of Proposition 4.2 and [**16**, Chapter 3, Theorem 10.1]. □

By Proposition 4.1 (or Lemma 4.8) and Proposition 4.2 (or Corollary 4.1), we have Main Theorem 1.

Main Theorem 1. *The map* $d_{g,q}$ *defined by* (3.1) *is not a metric on* $\mathcal{EC}(q)$.

Proof. This is a direct consequence of Proposition 4.1 or Proposition 4.2. □

Remark 4.1. In order to prove Main Theorem 1, it is enough only to prove Proposition 4.1 or Proposition 4.2. However, in Section 5, one can see that the proof of Proposition 4.1 is useful for our new construction of metrics on $\mathcal{EC}(q)$ based on the map $d_{g,q}$.

REMARK 4.2. As we mentioned above, by Propositions 4.1, 4.2, and Main Theorem 1, one can see that the map $d_{g,p}$ defined by (3.1) is *not* a metric on $\mathcal{EC}(p)$.

EXAMPLE 4.1. We demonstrate Proposition 4.1 and Proposition 4.2 on the following three examples.

(1) Set $q = 13$. Then we have $\mathcal{S}_{13} = \{0, \pm 1, \ldots, \pm 5, 6\}$. It is easy to verify that $g = 2$ is a generator of the multiplicative group $\mathbb{F}_{13}^*$. Let $E_1/\mathbb{F}_{13} : y^2 = x^3 + x + 1$, $E_2/\mathbb{F}_{13} : y^2 = x^3 + 9x - 1$, $E_3/\mathbb{F}_{13} : y^2 = x^3 + x - 1$ be elliptic curves. These curves are $\mathbb{F}_{13}$-isomorphic to each other, by the isomorphisms $\phi_4 : E_1 \to E_2$, $\phi_8 : E_1 \to E_3$, and $\phi_2 : E_2 \to E_3$ (See the definition of the map (2.3)). Since $\mathcal{U}(E_1, E_2) = \{4, 9\} = \{g^2, g^8\} = \{g^{-4}, g^2\}$, one can derive $\mathcal{S}^{(1,2)}_{13,\,\mathcal{U}} = \{-4, 2\}$ and $\mathcal{S}^{(2,1)}_{13,\,\mathcal{U}} = \{-2, 4\}$. Thus, from

$$d_{2,13}(E_1, E_2) = |\min \mathcal{S}^{(1,2)}_{13,\,\mathcal{U}}| = |-4| = 4,$$
$$d_{2,13}(E_2, E_1) = |\min \mathcal{S}^{(2,1)}_{13,\,\mathcal{U}}| = |-2| = 2,$$

we obtain $d_{2,13}(E_1, E_2) \neq d_{2,13}(E_2, E_1)$ (Proposition 4.1). Similarly, we can show that (Proposition 4.1)

$$\mathcal{U}(E_1, E_3) = \{5, 8\} = \{g^3, g^9\} = \{g^{\pm 3}\}, \quad \mathcal{S}^{(1,3)}_{13,\,\mathcal{U}} = \{\pm 3\} = \mathcal{S}^{(3,1)}_{13,\,\mathcal{U}},$$
$$d_{2,13}(E_1, E_3) = |\min \mathcal{S}^{(1,3)}_{13,\,\mathcal{U}}| = |\min \mathcal{S}^{(3,1)}_{13,\,\mathcal{U}}| = d_{2,13}(E_3, E_1).$$

(2) Set $q = 37$. Then we have $\mathcal{S}_{37} = \{0, \pm 1, \ldots, \pm 17, 18\}$. It is easy to verify that $g = 2$ is a generator of the multiplicative group $\mathbb{F}_{37}^*$. Let $E_1/\mathbb{F}_{37} : y^2 = x^3 + 1$, $E_2/\mathbb{F}_{37} : y^2 = x^3 + 26$, $E_3/\mathbb{F}_{37} : y^2 = x^3 - 1$ be elliptic curves. These curves are $\mathbb{F}_{37}$-isomorphic to each other, by the isomorphisms $\phi_4 : E_1 \to E_2$, $\phi_8 : E_1 \to E_3$, and $\phi_2 : E_2 \to E_3$ (See the definition of the map (2.3)). Since $\mathcal{U}(E_1, E_2) = \{3, 4, 7, 30, 33, 34\} = \{g^2, g^8, g^{14}, g^{20}, g^{26}, g^{32}\} = \{g^{-16}, g^{-10}, g^{-4}, g^2, g^8, g^{14}\}$, one can derive $\mathcal{S}^{(1,2)}_{37,\,\mathcal{U}} = \{-16, -10, -4, 2, 8, 14\}$ and $\mathcal{S}^{(2,1)}_{37,\,\mathcal{U}} = \{-14, -8, -2, 4, 10, 16\}$. Thus, from

$$d_{2,37}(E_1, E_2) = |\min \mathcal{S}^{(1,2)}_{37,\,\mathcal{U}}| = |-16| = 16$$
$$d_{2,37}(E_2, E_1) = |\min \mathcal{S}^{(2,1)}_{37,\,\mathcal{U}}| = |-14| = 14,$$

we obtain $d_{2,37}(E_1, E_2) \neq d_{2,37}(E_2, E_1)$ (Proposition 4.1). Similarly, we can show that (Proposition 4.1)

$$\mathcal{U}(E_1, E_3) = \{6, 8, 14, 23, 29, 31\} = \{g^3, g^9, g^{15}, g^{21}, g^{27}, g^{33}\} = \{g^{\pm 3}, g^{\pm 9}, g^{\pm 15}\},$$
$$\mathcal{S}^{(1,3)}_{37,\,\mathcal{U}} = \{\pm 3, \pm 9, \pm 15\} = \mathcal{S}^{(3,1)}_{13,\,\mathcal{U}},$$
$$d_{2,37}(E_1, E_3) = |\min \mathcal{S}^{(1,3)}_{37,\,\mathcal{U}}| = |\min \mathcal{S}^{(3,1)}_{37,\,\mathcal{U}}| = d_{2,13}(E_3, E_1).$$

Furthermore, since

$$\mathcal{U}(E_1, E_1) = \{1, 10, 11, 26, 27, 36\} = \{g^0, g^{\pm 6}, g^{\pm 12}, g^{18}\},$$

we have $\mathcal{S}^{(1,1)}_{37,\,\mathcal{U}} = \{0, \pm 6, \pm 12, 18\}$. This yields that $d_{2,37}(E_1, E_1) = |\min \mathcal{S}^{(1,1)}_{37,\,\mathcal{U}}| = |-12| = 12 \neq 0$ (Proposition 4.2).

(3) Set $q = 17$. Then we have $\mathcal{S}_{17} = \{0, \pm 1, \ldots, \pm 7, 8\}$. It is easy to verify that $g = 3$ is a generator of the multiplicative group $\mathbb{F}_{17}^*$. Let $E_1/\mathbb{F}_{17} : y^2 = x^3 + x$, $E_2/\mathbb{F}_{17} : y^2 = x^3 + 13x$, $E_3/\mathbb{F}_{17} : y^2 = x^3 - x$ be elliptic curves. These curves are $\mathbb{F}_{17}$-isomorphic to each other, by the isomorphisms $\phi_3 : E_1 \to E_2$, $\phi_9 : E_1 \to E_3$, and $\phi_3 : E_2 \to E_3$ (See the definition of the map (2.3)). Since $\mathcal{U}(E_1, E_2) = \{3, 5, 12, 14\} = \{g^1, g^5, g^9, g^{13}\} = \{g^{-7}, g^{-3}, g^1, g^5\}$, one can derive $\mathcal{S}_{17,\,\mathcal{U}}^{(1,2)} = \{-7, -3, 1, 5\}$ and $\mathcal{S}_{17,\,\mathcal{U}}^{(2,1)} = \{-5, -1, 3, 7\}$. Thus, from

$$d_{3,17}(E_1, E_2) = |\min \mathcal{S}_{17,\,\mathcal{U}}^{(1,2)}| = |-7| = 7,$$
$$d_{3,17}(E_2, E_1) = |\min \mathcal{S}_{17,\,\mathcal{U}}^{(2,1)}| = |-5| = 5,$$

we obtain $d_{3,17}(E_1, E_2) \neq d_{3,17}(E_2, E_1)$ (Proposition 4.1). Similarly, we can show that $\mathcal{U}(E_1, E_3) = \{2, 8, 9, 15\} = \{g^2, g^6, g^{10}, g^{14}\} = \{g^{\pm 2}, g^{\pm 6}\}$, $\mathcal{S}_{17,\,\mathcal{U}}^{(1,3)} = \{\pm 2, \pm 6\} = \mathcal{S}_{17,\,\mathcal{U}}^{(3,1)}$, and $d_{3,17}(E_1, E_3) = |\min \mathcal{S}_{17,\,\mathcal{U}}^{(1,3)}| = |\min \mathcal{S}_{17,\,\mathcal{U}}^{(3,1)}| = d_{3,17}(E_3, E_1)$ (Proposition 4.1). Furthermore, since $\mathcal{U}(E_1, E_1) = \{1, 4, 13, 16\} = \{g^0, g^{\pm 4}, g^8\}$, we have $\mathcal{S}_{17,\,\mathcal{U}}^{(1,1)} = \{0, \pm 4, 8\}$. This yields that $d_{3,17}(E_1, E_1) = |\min \mathcal{S}_{17,\,\mathcal{U}}^{(1,1)}| = |-4| = 4 \neq 0$ (Proposition 4.2).

5. Our construction of metrics based on the map $d_{g,q}$

In this section we construct new metrics on $\mathcal{EC}(q)$ which are slightly modified versions of the map $d_{g,q}$ defined by (3.1). Let $E_i/\mathbb{F}_q : y^2 = x^3 + a_i x + b_i \in \mathcal{EC}(q)$ $(i = 1, 2, 3)$ be elliptic curves defined over $\mathbb{F}_q$. In Section 4, we pointed out that the map $d_{g,q}$ defined by (3.1) is in fact not a metric (Main Theorem 1). As one can see in Proposition 4.1 and Proposition 4.2, the main problem concerning the map $d_{g,q}$ is in handling the two values $\min \mathcal{S}_{q,\,\mathcal{U}}^{(1,2)}$ and $\min \mathcal{S}_{q,\,\mathcal{U}}^{(2,1)}$. Unfortunately, $\min \mathcal{S}_{q,\,\mathcal{U}}^{(i,j)} \neq \min \mathcal{S}_{q,\,\mathcal{U}}^{(j,i)}$ holds in general. However, by defining

$$\widetilde{\mathcal{S}_{q,\,\mathcal{U}}^{(i,j)}} := \{|\mathrm{Log}_g^{\mathcal{S}_q}(t)| \in \mathcal{S}_q \mid t \in \mathcal{U}(E_i, E_j)\} = \{|k| \in \mathcal{S}_q \mid g^k \in \mathcal{U}(E_i, E_j)\}, \tag{5.1}$$

we have

$$\min \widetilde{\mathcal{S}_{q,\,\mathcal{U}}^{(i,j)}} = \min \widetilde{\mathcal{S}_{q,\,\mathcal{U}}^{(j,i)}} \tag{5.2}$$

for $1 \leqslant i, j \leqslant 3$ $(i \neq j)$. From this observation, one can naturally construct the map $\widetilde{d_{g,q}} : \mathcal{EC}(q) \times \mathcal{EC}(q) \to \mathbb{R} \cup \{\infty\}$ as follows:

$$\begin{aligned} &(E_1, E_2) \mapsto r, \quad \text{if } E_1 \overset{\phi_u}{\cong} E_2, \\ &(E_1, E_2) \mapsto \infty, \quad \text{otherwise,} \end{aligned} \tag{5.3}$$

where $r := \min \widetilde{\mathcal{S}_{q,\,\mathcal{U}}^{(1,2)}} \geqslant 0$ and $u := g^r \in \mathcal{U}(E_1, E_2)$. One can easily see that the map $\widetilde{d_{g,q}}$ is slightly modified version of the map $d_{g,q}$. Main Theorem 2 states that the map $\widetilde{d_{g,q}}$ is a metric on $\mathcal{EC}(q)$.

Main Theorem 2. *$(\mathcal{EC}(q), \widetilde{d_{g,q}})$ is a metric space.*

PROOF. Let $E_i/\mathbb{F}_q : y^2 = x^3 + a_i x + b_i \in \mathcal{EC}(q)$ $(i = 1, 2, 3)$ be elliptic curves. We prove that $\widetilde{d_{g,q}}$ is a metric on $\mathcal{EC}(q)$.

Non-negativity: By the definition (5.3) of $\widetilde{d_{g,q}}$, we have $\widetilde{d_{g,q}}(E_1, E_2) \geqslant 0$ for all $E_1, E_2 \in \mathcal{EC}(q)$.

Non-degeneracy: We assume that $\widetilde{d_{g,q}}(E_1, E_2) = 0$, and prove that $E_1 = E_2$. We first recall that $\widetilde{d_{g,q}}(E_1, E_2) = \min \widetilde{\mathcal{S}_{q,\mathcal{U}}^{(1,2)}}$. Then we have $0 \in \widetilde{\mathcal{S}_{q,\mathcal{U}}^{(1,2)}}$. This indicates that $E_1 = E_2$. Conversely, if $E_1 = E_2$, then it is obvious that $0 \in \widetilde{\mathcal{S}_{q,\mathcal{U}}^{(1,2)}}$. Then, by the definition of the set $\widetilde{\mathcal{S}_{q,\mathcal{U}}^{(1,2)}}$, $\min \widetilde{\mathcal{S}_{q,\mathcal{U}}^{(1,2)}}$ equals to zero. Thus, we obtain $\widetilde{d_{g,q}}(E_1, E_2) = 0$.

Symmetry: When $E_1/\mathbb{F}_q \ncong E_2/\mathbb{F}_q$, we obviously have $\widetilde{d_{g,q}}(E_1, E_2) = \widetilde{d_{g,q}}(E_2, E_1) = \infty$. If $E_1/\mathbb{F}_q \cong E_2/\mathbb{F}_q$ then it follows immediately from Equation (5.2) that $\widetilde{d_{g,q}}(E_1, E_2) = \widetilde{d_{g,q}}(E_2, E_1)$. Thus, $\widetilde{d_{g,q}}(E_1, E_2) = \widetilde{d_{g,q}}(E_2, E_1)$ for all $E_1, E_2 \in \mathcal{EC}(q)$.

Triangular inequality: We claim that $\widetilde{d_{g,q}}(E_1, E_3) \leqslant \widetilde{d_{g,q}}(E_1, E_2) + \widetilde{d_{g,q}}(E_2, E_3)$ for all $E_1, E_2, E_3 \in \mathcal{EC}(q)$. There are two cases to consider:

Case 1. $E_1/\mathbb{F}_q \ncong E_3/\mathbb{F}_q$. In this case, we have $\widetilde{d_{g,q}}(E_1, E_3) = \infty$. It follows immediately from $E_1/\mathbb{F}_q \ncong E_3/\mathbb{F}_q$ that $E_1/\mathbb{F}_q \ncong E_2/\mathbb{F}_q$ or $E_2/\mathbb{F}_q \ncong E_3/\mathbb{F}_q$. This indicates that $\widetilde{d_{g,q}}(E_1, E_2) = \infty$ or $\widetilde{d_{g,q}}(E_2, E_3) = \infty$. Thus, we obtain the triangular inequality for (Case 1).

Case 2. $E_1/\mathbb{F}_q \cong E_3/\mathbb{F}_q$. There are two possibilities: $E_1/\mathbb{F}_q \ncong E_2/\mathbb{F}_q$ and $E_1/\mathbb{F}_q \cong E_2/\mathbb{F}_q$. The former case gives $\widetilde{d_{g,q}}(E_1, E_2) = \infty$, which shows the triangular inequality. Next, we consider the latter case. In the latter case, the two elliptic curves $E_1/\mathbb{F}_q$ and $E_3/\mathbb{F}_q$ are $\mathbb{F}_q$-isomorphic. Set $\widetilde{d_{g,q}}(E_1, E_2) = r_1$, $\widetilde{d_{g,q}}(E_2, E_3) = r_2$, and $\widetilde{d_{g,q}}(E_1, E_3) = r_3$. From $r_1 \in \widetilde{\mathcal{S}_{q,\mathcal{U}}^{(1,2)}}$, $r_1 = |r_1|$ holds. Similarly, we get $r_2 = |r_2|$ and $r_3 = |r_3|$. Put $r := r_1 + r_2$. Since $0 \leqslant r_i \leqslant (q-1)/2$ for $1 \leqslant i \leqslant 3$, the inequality $0 \leqslant r = r_1 + r_2 \leqslant q - 1$ holds. We further divide into two subcases:

Subcase 2-1. $E_1/\mathbb{F}_q \cong E_3/\mathbb{F}_q$ and $0 \leqslant r \leqslant (q-1)/2$. In this subcase, it is easy to see that $r, r_3 \in \mathcal{S}_{q,\mathcal{U}}^{(1,3)}$. Then by $r_3 = \min \widetilde{\mathcal{S}_{q,\mathcal{U}}^{(1,3)}}$, we obtain

$$\widetilde{d_{g,q}}(E_1, E_3) = r_3 \leqslant r = r_1 + r_2 = \widetilde{d_{g,q}}(E_1, E_2) + \widetilde{d_{g,q}}(E_2, E_3).$$

Subcase 2-2. $E_1/\mathbb{F}_q \cong E_3/\mathbb{F}_q$ and $(q-1)/2 < r \leqslant q - 1$. In this case, we have $-(q-1)/2 < r - (q-1) \leqslant 0$. Then we can see that $r - (q-1), r_3 \in \mathcal{S}_{q,\mathcal{U}}^{(1,3)}$. By the same argument as in (Case 2-1), we obtain

$$\widetilde{d_{g,q}}(E_1, E_3) = r_3 \leqslant r - (q-1) < r = r_1 + r_2 = \widetilde{d_{g,q}}(E_1, E_2) + \widetilde{d_{g,q}}(E_2, E_3).$$

Hence the triangular inequality $\widetilde{d_{g,q}}(E_1, E_3) \leqslant \widetilde{d_{g,q}}(E_1, E_2) + \widetilde{d_{g,q}}(E_2, E_3)$ holds for all $E_1, E_2, E_3 \in \mathcal{EC}(q)$. □

EXAMPLE 5.1. We demonstrate Main Theorem 2 on the three examples in Example 4.1.
(1) Let $E_1/\mathbb{F}_{13} : y^2 = x^3+x+1$, $E_2/\mathbb{F}_{13} : y^2 = x^3+9x-1$, $E_3/\mathbb{F}_{13} : y^2 = x^3+x-1$ be elliptic curves. Then we have

$$\widetilde{d_{2,13}}(E_1, E_2) = \min \widetilde{\mathcal{S}^{(1,2)}_{13,\,\mathcal{U}}} = \min\{2, 4\} = 2 = \widetilde{d_{2,13}}(E_2, E_1),$$
$$\widetilde{d_{2,13}}(E_2, E_3) = \min \widetilde{\mathcal{S}^{(2,3)}_{13,\,\mathcal{U}}} = \min\{3\} = 3 = \widetilde{d_{2,13}}(E_3, E_2).$$

(2) Let $E_1/\mathbb{F}_{37} : y^2 = x^3+1$, $E_2/\mathbb{F}_{37} : y^2 = x^3+26$, $E_3/\mathbb{F}_{37} : y^2 = x^3-1$ be elliptic curves. Then we have

$$\widetilde{d_{2,37}}(E_1, E_2) = \min \widetilde{\mathcal{S}^{(1,2)}_{37,\,\mathcal{U}}} = \min\{2, 4, 8, 10, 14, 16\} = 2 = \widetilde{d_{2,37}}(E_2, E_1),$$
$$\widetilde{d_{2,37}}(E_2, E_3) = \min \widetilde{\mathcal{S}^{(2,3)}_{37,\,\mathcal{U}}} = \min\{3, 9, 15\} = 3 = \widetilde{d_{2,37}}(E_3, E_2),$$
$$\widetilde{d_{2,37}}(E_1, E_1) = \min \widetilde{\mathcal{S}^{(1,1)}_{37,\,\mathcal{U}}} = \min\{0, 6, 12, 18\} = 0.$$

(3) Let $E_1/\mathbb{F}_{17} : y^2 = x^3 + x$, $E_2/\mathbb{F}_{17} : y^2 = x^3 + 13x$, $E_3/\mathbb{F}_{17} : y^2 = x^3 - x$ be elliptic curves. Then we have

$$\widetilde{d_{3,17}}(E_1, E_2) = \min \widetilde{\mathcal{S}^{(1,2)}_{17,\,\mathcal{U}}} = \min\{1, 3, 5, 7\} = 1 = \widetilde{d_{3,17}}(E_2, E_1),$$
$$\widetilde{d_{3,17}}(E_2, E_3) = \min \widetilde{\mathcal{S}^{(2,3)}_{17,\,\mathcal{U}}} = \min\{2, 6\} = 2 = \widetilde{d_{3,17}}(E_3, E_2),$$
$$\widetilde{d_{3,17}}(E_1, E_1) = \min \widetilde{\mathcal{S}^{(1,1)}_{17,\,\mathcal{U}}} = \min\{0, 4, 8\} = 0.$$

In a similar manner to [**3**, Corollary 1] and [**5**, Corollary 5.1.1], one can construct different metrics on $\mathcal{EC}(q)$. We need Lemma 5.1 for our proof of Corollary 5.1.

LEMMA 5.1. *If $E_1, E_2 \in \mathcal{EC}(q)$ and $E_1/\mathbb{F}_q \cong E_2/\mathbb{F}_q$, then the following inequality holds*:

$$0 \leqslant \widetilde{d_{g,q}}(E_1, E_2) \leqslant (q - (q \bmod (2 \cdot \sharp\widetilde{\mathcal{S}^{(1,2)}_{q,\,\mathcal{U}}})))/(2 \cdot \sharp\widetilde{\mathcal{S}^{(1,2)}_{q,\,\mathcal{U}}}). \tag{5.4}$$

In particular, the inequality

$$0 \leqslant \widetilde{d_{g,q}}(E_1, E_2) \leqslant (q - (q \bmod 4))/4 \tag{5.5}$$

holds for $E_1, E_2 \in \mathcal{EC}(q)$ satisfying $E_1/\mathbb{F}_q \cong E_2/\mathbb{F}_q$.

PROOF. We define the function $f : \mathbb{R} \to \mathbb{R}$ as $f(x) := (q - (q \bmod (2x)))/(2x)$. Since

$$\begin{aligned} f(2) - f(4) &= \tfrac{1}{4}\big(q - (q \bmod 4)\big) - \tfrac{1}{8}\big(q - (q \bmod 8)\big) \\ &= \tfrac{1}{8}\big((q - (q \bmod 4)) + ((q \bmod 8) - (q \bmod 4))\big) \geqslant 0, \\ f(2) - f(6) &= \tfrac{1}{4}\big(q - (q \bmod 4)\big) - \tfrac{1}{12}\big(q - (q \bmod 12)\big) \\ &= \tfrac{1}{12}\big(2(q - (q \bmod 4)) + ((q \bmod 12) - (q \bmod 4))\big) \geqslant 0, \end{aligned}$$

we have $f(4) \leqslant f(2)$ and $f(6) \leqslant f(2)$. By $f(2) = (q-(q \bmod 4))/4$, Inequality (5.5) follows from Inequality (5.4) and $\widetilde{\mathcal{S}^{(1,2)}_{q,\mathcal{U}}} = 2, 4$, or 6. Thus it is enough to show the right-hand side of Inequality (5.4). Set $r := \widetilde{d_{g,q}}(E_1, E_2)$ and $l := \sharp\widetilde{\mathcal{S}^{(1,2)}_{q,\mathcal{U}}}$. Let us assume that there exist $\mathbb{F}_q$-isomorphic elliptic curves $E_1, E_2 \in \mathcal{EC}(q)$ such that

$$\begin{aligned} r = \widetilde{d_{g,q}}(E_1, E_2) &> (q - (q \bmod (2 \cdot \sharp\widetilde{\mathcal{S}^{(1,2)}_{q,\mathcal{U}}})))/(2 \cdot \sharp\widetilde{\mathcal{S}^{(1,2)}_{q,\mathcal{U}}}) \\ &= (q - (q \bmod 2l))/(2l) \end{aligned}$$

and seek a contradiction. From $r = \min \widetilde{\mathcal{S}^{(1,2)}_{q,\mathcal{U}}} \geqslant 0$, we have $r \in \mathcal{S}^{(1,2)}_{q,\mathcal{U}}$ or $-r \in \mathcal{S}^{(1,2)}_{q,\mathcal{U}}$. We first assume that $r \in \mathcal{S}^{(1,2)}_{q,\mathcal{U}}$. Combining $\sharp\widetilde{\mathcal{S}^{(1,2)}_{q,\mathcal{U}}} = \sharp\mathcal{S}^{(1,2)}_{q,\mathcal{U}}$ and Lemma 4.5 yield that $r-(q-1)/l \in \mathcal{S}^{(1,2)}_{q,\mathcal{U}}$ and $r-(q-1)/l < 0$. By the minimality of r, we have $r < |r-(q-1)/l| = (q-1)/l - r$. Thus, the inequality $r \leqslant (q-(q \bmod 2l))/(2l)$ follows from $r < (q-1)/(2l)$ and $r \in \mathcal{S}_q$. This is a contradiction. In the same way as in the case of $r \in \mathcal{S}^{(1,2)}_{q,\mathcal{U}}$, we can also derive a contradiction in the case $-r \in \mathcal{S}^{(1,2)}_{q,\mathcal{U}}$. Hence, Inequality (5.4) holds. □

Corollary 5.1 (Other metrics on $\mathcal{EC}(q)$). *Set* $\delta := ((q-(q \bmod 4))/4) + 1$, $\mathcal{N}_{q,\delta} := \{\delta, \delta+1, \delta+2, \ldots\} \subseteq \mathbb{N}_+$, $\widehat{\mathcal{N}}_{q,\delta} := \{\delta, \delta+1, \delta+2, \ldots\} \cup \{\infty\} = \mathcal{N}_{q,\delta} \cup \{\infty\}$, *and* $\mathbb{R}_{>0} := \{c \in \mathbb{R} \mid c > 0\}$. *Let* $\mathcal{S} \subsetneq \widehat{\mathcal{N}}_{q,\delta}$ *be a finite subset.*

(1) *For any integer* $\ell \in \mathcal{N}_{q,\delta}$, *we define the map* $\widetilde{d^{(\ell)}_{g,q}} : \mathcal{EC}(q) \times \mathcal{EC}(q) \to \mathbb{R}$ *by*

$$\begin{aligned} &(E_1, E_2) \mapsto r := \min \widetilde{\mathcal{S}^{(1,2)}_{q,\mathcal{U}}}, && \text{if } E_1/\mathbb{F}_q \cong E_2/\mathbb{F}_q, \\ &(E_1, E_2) \mapsto \ell, && \text{otherwise.} \end{aligned}$$

Then $(\mathcal{EC}(q), \widetilde{d^{(\ell)}_{g,q}})$ *is a metric space for each* $\ell \in \mathcal{N}_{q,\delta}$.

(2) *The map*

$$\sum_{\ell \in \mathcal{S}} \widetilde{d^{(\ell)}_{g,q}} : \mathcal{EC}(q) \times \mathcal{EC}(q) \to \mathbb{R} \cup \{\infty\}, \quad (E_1, E_2) \mapsto \sum_{\ell \in \mathcal{S}} \widetilde{d^{(\ell)}_{g,q}}(E_1, E_2)$$

is also a metric on $\mathcal{EC}(q)$.

(3) *For each* $\ell \in \mathcal{S}$, *we take* $c^{(\ell)} \in \mathbb{R}_{>0}$. *Then one can define the metric*

$$\sum_{\ell \in \mathcal{S}} c^{(\ell)} \cdot \widetilde{d^{(\ell)}_{g,q}} : \mathcal{EC}(q) \times \mathcal{EC}(q) \to \mathbb{R} \cup \{\infty\}, \quad (E_1, E_2) \mapsto \sum_{\ell \in \mathcal{S}} c^{(\ell)} \cdot \widetilde{d^{(\ell)}_{g,q}}(E_1, E_2)$$

on $\mathcal{EC}(q)$.

Proof. We first prove (1). The non-negativity property, the non-degeneracy property, and the symmetry property of $\widetilde{d^{(\ell)}_{g,q}}$ are obvious from Theorem 2 and the definition of the map $\widetilde{d^{(\ell)}_{g,q}}$. The triangular inequality of $\widetilde{d^{(\ell)}_{g,q}}$ follows from Main Theorem 2 and Lemma 5.1. (2) and (3) follow from (1) and Main Theorem 2. □

Acknowledgement. The author would like to thank the anonymous referees for their valuable comments.

References

1. A. O. L. Atkin, F. Morain, *Elliptic curves and primality proving*, Math. Comp. **61**(203) (1993), 29–68.
2. O. Billet, M. Joye, *The jacobi model of an elliptic curve and side-channel analysis*, in: M. Fossorier, T. Hoholdt, A. Poli (eds.), Proceedings of Applied Algebra, Algebraic Algorithms and Error-Correcting Codes–AAECC 2003, Lect. Notes Comput. Sci. 2643 (2003), 34–42, Springer, Berlin, Heidelberg.
3. K. Hakuta, *Metrics on the sets of nonsupersingular elliptic curves in simplified Weierstrass form over finite fields of characteristic two*, Int. J. Math. Math. Sci. **2015** (2015), 597849:1–597849:5.
4. ———, *Some remarks on a distance between two ordinary elliptic curves over the finite field* $\mathbb{F}_{2^5}$, Int. J. Pure Appl. Math. **89**(4) (2016), 801–807.
5. ———, *Distance functions on the sets of ordinary elliptic curves in short Weierstrass form over finite fields of characteristic three*, Math. Slovaca **68**(4) (2018), 1–18.
6. T. Izu, B. Möller, T. Takagi, *Improved elliptic curve multiplication methods resistant against side channel attacks*, In: A. Menezes, P. Sarkar (eds.), Proceedings of Progress in Cryptology–INDOCRYPT 2002, Lect. Notes Comput. Sci. 2551 (2002), 296–313, Springer, Berlin, Heidelberg.
7. M. Joye, C. Tymen, *Protections against differential analysis for elliptic curve cryptography: An algebraic approach*, In: Ç. K. Koç, D. Naccache, C. Paar (eds.), Proceedings of Cryptographic Hardware and Embedded Systems–CHES 2001, Lect. Notes Comput. Sci. 2162 (2001), 377–390, Springer, Berlin, Heidelberg.
8. N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48**(177) (1987), 203–209.
9. H. W. Lenstra. Jr., *Factoring integers with elliptic curves*, Ann. of Math. **126**(3) (1987), 649–673.
10. A. J. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer, Boston, 1993.
11. A. J. Menezes, T. Okamoto, S. A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Trans. Inform. Theory **39**(5) (1993), 1639–1646.
12. V. Miller, *Use of elliptic curves in cryptography*, In: H. C. Williams (ed.), Proceedings of Advances in Cryptology–CRYPTO '85, Lect. Notes Comput. Sci. 218 (1986), 417–426, Springer, Berlin, Heidelberg.
13. P. K. Mishra, K. C. Gupta, *A metric on the set of elliptic curves over* $\mathbb{F}_p$, Appl. Math. Lett. **21**(12) (2008), 1330–1332.
14. National Institute of Standards and Technology, Digital Signature Standard (DSS), Fed. Inf. Process. Stand. Publ. 186-4, July, 2013.
15. A. R. Rishivarman, B. Parthasarathy, *An elliptic curve metric on the fundamental group over* $GF(2^5)$, Int. J. Pure Appl. Math. **89**(4) (2013), 547–552.
16. J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts Math. 106, Springer-Verlag, 2009.
17. F. Vetro, *Metrics on the set of elliptic curves over* $\mathbb{F}_p$, Int. J. Contemp. Math. Sci. **1**(1) (2011), 22–24.

Institute of Science and Engineering, Academic Assembly
Shimane University
Matsue, Shimane
Japan
hakuta@cis.shimane-u.ac.jp

(Received 15 12 2018)
(Revised 19 12 2020)