Parameterization of Edwards curves on the rational field Q with given torsion subgroups

Tung Linh Vo

***Abstract*— Extending Harold Edwards's study of a new normal form of elliptic curves, Bernstein et al. generalized a family of curves, called the twisted Edwards curve, defined over a non-binary field k given by an equation $ax^2 + y^2 = 1 + dx^2y^2$, where $a, d \in k\backslash\{0\}, a \neq d$. The authors focused on the construction of efficient formulae of point adding on these curves in order to use them in the secure cryptographic schemes. Theoretically, the authors showed how to parameteries Edwards curves having torsion subgroup $\mathbb{Z}/12\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ over the rational field $\mathbb{Q}$. In the main result of this paper, we use the method which Bersntein et al. suggested to parameterise Edwards curves with the given torsion subgroups which are $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ over $\mathbb{Q}$.**

***Tóm tắt*— Để mở rộng nghiên cứu của Harold Edwards về một dạng chuẩn tắc mới cho các đường cong elliptic, Bernstein cùng cộng sự đã tổng quát hóa một lớp các đường cong, gọi là các đường cong Edwards cuộn, định nghĩa trên trường k có đặc số khác 2 cho bởi phương trình $ax^2 + y^2 = 1 + dx^2y^2$, trong đó $a, d \in k\backslash\{0\}, a \neq d$. Các tác giả đã tập trung vào việc xây dựng các công thức cộng điểm hiệu quả trên lớp đường cong này phục vụ cho mục tiêu sử dụng chúng trong các lược đồ mật mã an toàn. Về mặt lý thuyết, các tác giả đã chỉ ra cách tham số hóa các đường cong Edwards có nhóm con xoắn $\mathbb{Z}/12\mathbb{Z}$ hoặc $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ trên trường hữu tỉ $\mathbb{Q}$. Trong kết quả chính của bài báo này, chúng tôi sẽ sử dụng phương pháp của Bernstein và cộng sự để tham số hóa đường cong Edwards với nhóm con xoắn đã biết là $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, hoặc $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ trên trường $\mathbb{Q}$.**

***Keywords*: Edwards curve; twisted Edwards curve; torsion subgroup.**

***Từ khóa:* Đường cong Edwards; đường cong Edwards cuộn; nhóm con xoắn.**

I. INTRODUCTION

In 2007, Harold Edwards [5] proposed a new normal form for elliptic curves. By generalizing an example originally from Euler and Gauss, Edwards introduced a new addition law for the curves $x^2 + y^2 = c^2(1 + x^2y^2)$ defined over a non-binary field k. Although the paper of Edwards did not focus on applying this normal form of elliptic curves in cryptography, but gradually, with subsequent studies, this form has shown desirable and useful cryptographic properties by comparison with Weierstrass normal form.

Following this work, in [1, 2, 3, 4], Bernstein et al. generalized Edwards study to generalize curves given by an equation of the form $ax^2 + y^2 = 1 + dx^2y^2$, with $a \neq d, a, d \in k\backslash\{0\}$. They combined the Edwards idea of addition formula and dual addition law which was proposed by Hisil et al. in [6] to propose the unique formula for both addition and doubling laws. This is an essential proposal to result a group structure for a set of points on twisted Edwards curves in general, and Edwards curves in particular. This unique formula is a basic concept to use the normal form of Edwards in cryptography to be against channel attacks that exploits a power difference in computation between addition and doubling formulas.

The use of addition law, Bernstein et al. [2] showed a parameterization method of Edwards curves so that they have torsion subgroups given on the rational field $\mathbb{Q}$. However, authors only presented the parameterization for two case of torsion subgroups $\mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. In this paper, we present this method for remaining of torsion subgroups which are $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

The rest of paper is constructed as follow. The section II presents basic concepts of the normal form of Edwards curves, i.e. Edwards and twisted Edwards curves. The next section presents the parameterization of Edwards curves to have torsion subgroups given on $\mathbb{Q}$. In the section IV, we summarize the main results of paper.

This manuscript is received on December 12, 2017. It is commented on January 11, 2018 and is accepted on January 21, 2018 by the first reviewer. It is commented on , January 22, 2018 and is accepted on January 31, 2018 by the second reviewer.

II. EDWARDS NORMAL FORM

A. Definitions

In this section, we present Edwards curves and twisted Edwards curves from the general form of Bernstein et al. [1].

Definition 1 ([1]). *Let k be a field whose characteristic is not 2, and an element $d \in k\backslash\{0,1\}$. The Edwards curve with coefficient d, called $E_{E,d}$, is a curve given by an equation:*

$$E_{E,d}: x^2 + y^2 = 1 + dx^2y^2. \quad (1)$$

A Twisted Edwards curve with coefficients a, d, called $E_{E,a,d}$, is a curve given by an equation:

$$E_{E,a,d}: ax^2 + y^2 = 1 + dx^2y^2, \quad (2)$$

where $a, d \in k\backslash\{0\}, a \neq d$.

Definition 2 ([1]). *Assuming that E is a curve over k. A quadratic twist of E is a curve E' that is isomorphic to E on the Galois field K/k with $[K:k] = 2$.*

It can be easily seen that the twisted Edwards curve $E_{E,a,d}: ax^2 + y^2 = 1 + dx^2y^2$ is a quadratic twist of the Edwards curve $E_{E,d/a}: X^2 + Y^2 = 1 + (d/a)X^2Y^2$. The map $(x, y) \mapsto \left(x\sqrt{a}, y\right) = (X, Y)$ is an isomorphism from $E_{E,a,d}$ to $E_{E,d/a}$ over the Galois field $k\left(\sqrt{a}\right)$. Therefore, if a is a square in k then $E_{E,a,d}$ is isomorphic to $E_{E,d/a}$ on k.

Here is a definition of Montgomery elliptic curve that is necessary for results represented in next sections.

Definition 3 ([1]). *The Montgomery curve, $E_{M,A,B}$, defined over a field k is a curve given by an equation:*

$$E_{M,A,B}: Bv^2 = u^3 + Au^2 + u, \quad (3)$$

where $A \in k\backslash\{-2,2\}$ and $B \in k\backslash\{0\}$.

Due to $B \in k\backslash\{0\}$, we can divide two sides of this equations by B^3, and get:

$$\left(\frac{v}{B}\right)^2 = \left(\frac{u}{B}\right)^3 + \frac{A}{B}\left(\frac{u}{B}\right)^2 + \frac{1}{B^2}\left(\frac{u}{B}\right). \quad (4)$$

Set $X = \frac{u}{B}, Y = \frac{v}{B}$, we get an equation of Weierstrass form:

$$Y^2 = X^3 + \frac{A}{B}X^2 + \frac{1}{B^2}X. \quad (5)$$

Therefore, a map $(u, v) \mapsto \left(\frac{u}{B}, \frac{v}{B}\right)$ transforms a curve of Montgomery to a Weierstrass form. In other words, a Montgomery curve is a particular case of elliptic curves with general Weierstrass form.

The next lemma gives a relationship between a twisted Edward curve and a Montgomery curve.

Lemma 1 ([1]). *Every twisted Edwards curve $E_{E,a,d}$ over k is birationally equivalent to a Montgomery curve $E_{M,A,B}: Bv^2 = u^3 + Au^2 + u$, where $A = 2(a + d)/(a - d)$ and $B = 4/(a - d)$.*

B. Addition Law

Bernstein et al. [1] constructed the addition law on twisted Edwards curve which is a generality of the addition formula of Edwards presented in [5].

Definition 4 ([1]). *Let k be a field with $char(k) \neq 2$, and $E_{E,a,d}: ax^2 + y^2 = 1 + dx^2y^2$, with $a, d \in k\backslash\{0\}, a \neq d$ is a twisted Edwards curve over k. Let $(x_1, y_1), (x_2, y_2)$ be two points on $E_{E,a,d}$. Then the sum of these points over $E_{E,a,d}$ is defined by*

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right). \quad (6)$$

The neutral element is $(0,1)$, and the negative of (x_1, y_1) is $(-x_1, y_1)$.

As it was shown by authors in [1], the addition law in Definition 5 is correct and complete if a is a square in k and d is a nonsquare in k, i.e. the addition law is well-defined on every pair of points on twisted Edwards curve $E_{E,a,d}$. Moreover, this law works for doubling, i.e. the case in which $(x_1, y_1) = (x_2, y_2)$. However, there is a case in which this addition is not well-defined, i.e. denominators in the above formula equal 0, in other words $dx_1x_2y_1y_2 \in \{-1,1\}$. The following lemma shows particular cases of the exception.

Lemma 2. *Let $E_{E,a,d}$ be a twisted Edwards curve over k. Assuming there exists $\alpha, \beta \in k$ such that $\alpha^2 = a, \beta^2 = d$. Given two arbitrary points $(x_1, y_1), (x_2, y_2)$ on the curve. Then, $dx_1x_2y_1y_2 \in \{-1,1\}$ if and only if $(x_2, y_2) \in S$ in which S is a set of points $\left(\frac{1}{\beta y_1}, \frac{-1}{\beta x_1}\right)$, $\left(\frac{-1}{\beta y_1}, \frac{1}{\beta x_1}\right)$, $\left(\frac{1}{\beta y_1}, \frac{1}{\beta x_1}\right)$, $\left(\frac{-1}{\beta y_1}, \frac{-1}{\beta x_1}\right)$, $\left(\frac{1}{\alpha\beta x_1}, \frac{\alpha}{\beta y_1}\right)$, $\left(\frac{-1}{\alpha\beta x_1}, \frac{-\alpha}{\beta y_1}\right)$, $\left(\frac{1}{\alpha\beta x_1}, \frac{-\alpha}{\beta y_1}\right)$, $\left(\frac{-1}{\alpha\beta x_1}, \frac{\alpha}{\beta y_1}\right)$.*

Proof. Necessity: Assume that $dx_1x_2y_1y_2 \in \{1, -1\}$. Then, $x_1, x_2, y_1, y_2 \neq 0$, and if we fix

x_1, y_1, then x_2, y_2 are roots of the system of equations

$$\begin{cases} (1 - dx_1x_2y_1y_2)(1 + dx_1x_2y_1y_2) = 0 \\ ax_2^2 + y_2^2 = 1 + dx_2^2y_2^2. \end{cases} \quad (7)$$

By solving the system of equations above, we get (x_2, y_2) being points given by the statement of the lemma.

Sufficiency: Conversely, by substituting the points of S for (x_2, y_2), we compute and get directly results from the lemma.

It can be easily seen that the addition law in Definition 5 contains two coefficients a, d of the curve. By a requirement to reduce a dependence on these coefficients when computing the addition law, Hisil, Carter, Wong, and Dawson in [6] built a new addition law, called Dual Addition as follows:

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_1 + x_2y_2}{y_1y_2 + ax_1x_2}, \frac{x_1y_1 - x_2y_2}{x_1y_2 - y_1x_2}\right).$$

This addition formula only depends on a unique coefficient a of the curve. The authors in [6] have shown that, this formula and the addition law in Definition 5 have the same results when the both are defined. However, there is a weakness of the Dual Addition that it does not work for doubling computation: if $(x_1, y_1) = (x_2, y_2)$ the computation of second coordinate $(x_1y_1 - x_2y_2)/(x_1y_2 - x_2y_1)$ results $0/0$. Despite of this weakness, the well-defined of dual addition have advantages on an efficient of computation [6].

Similar to the addition in Definition 5, we indicate exception cases of the dual addition on the twisted Edwards curve when a, d are squares on k.

Lemma 3 ([6]) . *With an assumption similar to Lemma 2, then* $(y_1y_2 + ax_1x_2)(x_1y_2 - y_1x_2) = 0$ *if and only if* $(x_2, y_2) \in S'$ *, where* S' *is a set containing points* (x_1, y_1), $(-x_1, -y_1)$, $\left(\frac{y_1}{\alpha}, -x_1\alpha\right)$, $\left(\frac{-y_1}{\alpha}, x_1\alpha\right)$, $\left(\frac{1}{\beta y_1}, \frac{1}{\beta x_1}\right)$, $\left(\frac{-1}{\beta y_1}, \frac{-1}{\beta x_1}\right)$, $\left(\frac{1}{\alpha\beta x_1}, \frac{-\alpha}{\beta y_1}\right)$, $\left(\frac{-1}{\alpha\beta x_1}, \frac{\alpha}{\beta y_1}\right)$ *if they are well-defined.*

C. A complete addition formula

In the previous subsection, we represent two addition formulas on the twisted Edwards curve. However, as seen on Lemmas 6 and 7, both of these formulas have drawbacks that exists exception cases to not make the addition work. It means that they are not a well-defined operation on a set of points, called $E_{E,a,d}(k)$, of twisted Edwards curve $E_{E,a,d}$ with $a, d \in k\backslash\{0\}$, $a \neq d$ arbitrary. To overcome this drawback and construct a binary operation on the whole set of points of the twisted Edwards curves, D.J. Bernstein and T. Lange [4] provide a solution as follows. They embed the set of twisted Edwards curve $E_{E,a,d}$ into in $\mathbb{P}^1 \times \mathbb{P}^1$, and indicate cases in which the addition law in Definition 5 does not work to use the formulae of Dual Addition and vice versa. Then the addition law is really a binary operation on the whole set of points of the twisted Edwards curves.

Fixed a twisted Edwards curve, $E_{E,a,d}$, defined by an equation

$$E_{E,a,d}: ax^2 + y^2 = 1 + dx^2y^2 \quad (8)$$

over the field k whose characteristic is not 2, $a, d \in k\backslash\{0\}$, $a \neq d$. The projective closure of $E_{E,a,d}$ in $\mathbb{P}_k^1 \times \mathbb{P}_k^1$ is

$$\bar{E}_{E,a,d}(k) = \left\{ \begin{matrix} ((X:Z),(Y:T)) \in \mathbb{P}_k^1 \times \mathbb{P}_k^1: \\ aX^2T^2 + Y^2Z^2 = Z^2T^2 + dX^2Y^2 \end{matrix} \right\}. \quad (9)$$

Each point (x, y) on affine curve $E_{E,a,d}$, embedded as usual into $\mathbb{P}_k^1 \times \mathbb{P}_k^1$ by $(x, y) \mapsto ((x:1),(y:1))$. Conversely, a point $((X:Z),(Y:T)) \in \bar{E}_{E,a,d}(k)$ with $ZT \neq 0$ is corresponding to a point of coordinate $(X/Z, Y/T)$ on affine curve $E_{E,a,d}$.

For $ZT = 0$, we consider two cases $(X:Z) = (1:0)$ or $(Y:T) = (1:0)$.

If $(X:Z) = (1:0)$ the equation of the curve becomes $aT^2 = dY^2$. Then, we have two points $((X:Z),(Y:T)) = \left((1:0),\left(\pm\sqrt{a/d}:1\right)\right)$, and these points are defined over the extension field $k\left(\sqrt{a/d}\right)$. The authors in [4] show that these points correspond to $(1:0:0)$ in projective closure of $E_{E,a,d}$ in $\mathbb{P}^2$.

If $(Y:T) = (1:0)$, then the equation of the curve becomes $Z^2 = dX^2$. Then, we also have two points $((X:Z),(Y:T)) = \left(\left(1:\pm\sqrt{d}\right),(1:0)\right)$, and these points are defined over the extension field $k\left(\sqrt{d}\right)$.

The authors in [4] also show that these points correspond to $(0:1:0)$ in projective closure of $E_{E,a,d}$ in $\mathbb{P}^2$. By using the represent of coordinating points, the authors [4] proved the following results to construct a complete addition law over twisted Edwards curves.

Theorem 1 ([4]). *Let $E_{E,a,d}$ be a twisted Edwards curve defined over k. Assuming $P_1, P_2 \in \bar{E}_{E,a,d}(k)$ with $P_1 = \big((X_1:Z_1),(Y_1:T_1)\big)$ and $P_2 = \big((X_2:Z_2),(Y_2:T_2)\big)$. We define*

$$X_3 = X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2$$
$$Z_3 = Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2$$
$$Y_3 = Y_1Y_2Z_1Z_2 - aX_1X_2T_1T_2$$
$$T_3 = Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2;$$

and

$$X_3' = X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1$$
$$Z_3' = aX_1X_2T_1T_2 + Y_1Y_2Z_1Z_2$$
$$Y_3' = X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1$$
$$T_3' = X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2.$$

Then, $X_3Z_3' = X_3'Z_3$ and $Y_3T_3' = Y_3'T_3$. Moreover, at least one of following case are hold:

- $(X_3, Z_3) \neq (0,0)$ *and* $(Y_3, T_3) \neq (0,0)$,
- $(X_3', Z_3') \neq (0,0)$ *and* $(Y_3', T_3') \neq (0,0)$.

By the above theorem, an addition law over twisted Edwards curve is constructed as follow.

Theorem 2 ([4]). *Let $E_{E,a,d}$ be a twisted Edwards curve and define $P_1, P_2, X_3, Y_3, Z_3, T_3, X_3', Y_3', Z_3', T_3'$ as in Theorem 1. Define $P_3 = P_1 + P_2$ as follow:*

- $P_3 = \big((X_3:Z_3),(Y_3:T_3)\big)$ *if* $(X_3, Z_3) \neq (0,0)$ *and* $(Y_3, T_3) \neq (0,0)$*;*
- $P_3 = \big((X_3':Z_3'),(Y_3':T_3')\big)$ *if* $(X_3', Z_3') \neq (0,0)$ *and* $(Y_3', T_3') \neq (0,0)$*;*
- *If both cases are applicable, then P_3 is defined arbitrarily by one of the above definitions.*

Then $P_3 \in \bar{E}_{E,a,d}(k)$.

Then, we have a fact on the set of points over twisted Edwards curve.

Theorem 3 ([4]). *By the addition law defined as in the Theorem 2, the set of points $\bar{E}_{E,a,d}(k)$ is an Abel group whose neutral element is $\big((0:1),(1:1)\big)$ and the negative of $P_1 = \big((X_1:Z_1),(Y_1:T_1)\big)$ is $\big((-X_1:Z_1),(Y_1:T_1)\big)$. Moreover, the group $\bar{E}_{E,a,d}(k)$ is isomorphic to $\bar{E}_{M,A,B}(k)$, where*

$$\bar{E}_{M,A,B}(k) = \left\{ \begin{matrix} (U:V:W) \in \mathbb{P}_k^2: \\ BV^2W = U^3 + AU^2W + UW^2 \end{matrix} \right\}$$

is the projective closure in $\mathbb{P}_k^2$ of the Montgomery curve

$$E_{M,A,B}: Bv^2 = u^3 + Au^2 + u,$$

with $A = 2(a+d)/(a-d)$ and $B = 4/(a-d)$.

By a directive way of computation, we can determine particular points of low order in the group $\bar{E}_{E,a,d}(k)$ of a twisted Edwards curve.

Theorem 4 ([2]). *Assume that $E_{E,a,d}: aX^2 + Y^2 = 1 + dX^2Y^2$ is a twisted Edwards curve over k whose $char(k) \neq 2$. Then:*

1. *The point of order 1 or the neutral element in $\bar{E}_{E,a,d}(k)$ is $\big((0:1),(1:1)\big)$.*
2. *The points of order 2 in $\bar{E}_{E,a,d}(k)$ are:*
   - $\big((0:1),(-1:1)\big)$.
   - $\Big((1:0),\big(\pm\sqrt{a/d}:1\big)\Big)$ *if* $a/d = s^2, s \in k$.
3. *The points of order 4 in $\bar{E}_{E,a,d}(k)$ are:*
   - $\Big(\big(1:\pm\sqrt{a}\big),(0:1)\Big)$ *if* $a = r^2, r \in k$.
   - $\Big(\big(1:\pm\sqrt{d}\big),(1:0)\Big)$ *if* $d = t^2, t \in k$.
   - $\Big(\big(\pm\sqrt{-s/a}:1\big),\big(\pm\sqrt{s}:1\big)\Big)$ *if* $a/d = s^2$, *s and $-s/a$ are squares in k, where the signs may be chosen independently.*
4. *The points of order 8 in $\bar{E}_{E,a,d}(k)$ doubling to $\Big(\big(1:\pm\sqrt{a}\big),(1:0)\Big)$ are:*
   - $\big((X:1),(\pm rX:1)\big)$ *with* $r^2 = a$, $X \in k$, *satisfied* $adX^4 - 2aX^2 + 1 = 0$.
5. *The points of order 8 in $\bar{E}_{E,a,d}(k)$ doubling to $\Big(\big(1:\pm\sqrt{d}\big),(1:0)\Big)$ are:*

- $\big((X:1),(1:\pm sX)\big)$ *with* $s^2 = d$, $X \in k$ *satisfied* $adX^4 - 2dX^2 + 1 = 0$.

6. *The points of order* 3 *in* $\bar{E}_{E,a,d}(k)$ *are:*

$\big((X:1),(Y:1)\big)$ *with* $X, Y \in k\backslash\{0\}$ *satisfied* $aX^2 + Y^2 = 1 + dX^2Y^2 = -2Y$.

III. PARAMETERIZATION OF EDWARDS CURVES WITH TORSION SUBGROUPS GIVEN OVER RATIONAL FIELD $\mathbb{Q}$

Assuming that $\mathcal{E}$ is an elliptic curve over the rational field $\mathbb{Q}$, and notate $\mathcal{E}(\mathbb{Q})$ be a group of points of this curve. According to the Mordell-Weil theorem ([7, Theo.8.17]), we have $\mathcal{E}(\mathbb{Q})$ to be a finitely generated abelian group. In particular, using the theorem on structure of a finitely generated abelian group ([7, Theo.B.4]), it can be shown that

$$\mathcal{E}(\mathbb{Q}) \cong \mathcal{E}_{\text{tor}}(\mathbb{Q}) \oplus \mathbb{Z}^r,$$

in which $\mathcal{E}_{\text{tor}}(\mathbb{Q})$ notates a finite subgroup, called torsion subgroup of the elliptic curve $\mathcal{E}$ over $\mathbb{Q}$, and $r \geq 0$ is an integer, called the rank of $\mathcal{E}(\mathbb{Q})$. In a simple way, it can be called that $\mathcal{E}_{\text{tor}}(\mathbb{Q})$ is the torsion part and $\mathbb{Z}^r$ is the free part of the group of points on elliptic curve $\mathcal{E}(\mathbb{Q})$. Therefore, to determine the group of points of elliptic curves over $\mathbb{Q}$, we must identify the torsion subgroup $\mathcal{E}_{\text{tor}}(\mathbb{Q})$ and the free rank r. In this section, we consider the torsion subgroup of curves of Edwards forms.

Related to the structure of torsion subgroups on elliptic curves over the field $\mathbb{Q}$, the following classical theorem, called Mazur Theorem, indicates that:

Theorem 5 (Mazur Theorem [7]). *Let* $\mathcal{E}$ *be an elliptic curve defined over* $\mathbb{Q}$. *Then the torsion subgroup,* $\mathcal{E}_{tor}(\mathbb{Q})$, *of* $\mathcal{E}(\mathbb{Q})$ *is isomorphic to one of the following:*

$$\mathcal{E}_{tor}(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/m\mathbb{Z}, with\ 1 \leq m \leq 10\ or\ m = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z},\ with\ 1 \leq m \leq 4. \end{cases}$$

Now, we consider a case of Edwards E defined over the field $k = \mathbb{Q}$ with $d \in \mathbb{Q}\backslash\{0,1\}$. We consider following note.

Note 1. Asssume that $E: x^2 + y^2 = 1 + dx^2y^2$ is an Edwards curve defined over $\mathbb{Q}$ with $d \neq 0,1$.

Then, from Theorem 3, the point group of E is isomorphic to the point group of the elliptic curve :

$$E_{M,A,B}: Bv^2 = u^3 + Au^2 + u,$$

where $A = 2(1+d)/(1-d)$ and $B = 4/(1-d)$. The map $(u,v) \mapsto (X,Y) = \left(\frac{u}{B}, \frac{v}{B}\right)$ transform $E_{M,A,B}$ into an elliptic curve of Weierstrass form.

$$\mathcal{E}: Y^2 = X^3 + \frac{A}{B}X^2 + \frac{1}{B^2}X,$$

or

$$\mathcal{E}: Y^2 = X^3 + \frac{1+d}{2}X^2 + \frac{(1-d)^2}{16}X.$$

Then, we have an isomorphism

$$E_{\text{tor}}(\mathbb{Q}) \cong \mathcal{E}_{\text{tor}}(\mathbb{Q}).$$

According to the case 3 of Theorem 4, the Edwards curve E always has a point of order 4 that is $(1,0)$, in other words, it is $\big((1:1),(0:1)\big)$, so from Mazur's Theorem, it follows that, the torsion subgroup $E_{\text{tor}}(\mathbb{Q})$ of E can only be isomorphic to one of groups $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

Mazur's Theorem and Note 1 give us the possibility of torsion subgroup $E_{\text{tor}}(\mathbb{Q})$ of Edwards curve defined over $\mathbb{Q}$ without knowing of what parameters to provide that torsion subgroup. To solve this, in [2] the authors point out the parameterization of Edwards curves whose torsion subgroups are $\mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, respectively. The following theorems provides of particular results.

Theorem 6 ([2]). *The Edwards curve* $E: x^2 + y^2 = 1 + dx^2y^2$ *defined over* $\mathbb{Q}$ *has a point of order* 3, *or equivalently, the torsion subgroup* $E_{tor}(\mathbb{Q})$ *of* E *is isomorphic to* $\mathbb{Z}/12\mathbb{Z}$ *if and only if*

$$d = \frac{(1+t^2)^3(1-4t+t^2)}{(1-t)^6(1+t)^2}, \quad \forall t \in \mathbb{Q}\backslash\{0,\pm 1\}.$$

Theorem 7 ([2]). *The Edwards curve* $E: x^2 + y^2 = 1 + dx^2y^2$ *defined over* $\mathbb{Q}$ *has torsion subgroup* $E_{tor}(\mathbb{Q})$ *isomorphic to* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ *and has points of order* 8 *doubling to* $(\pm 1,0)$ *if and only if*

$$d = \frac{(t^2-2)^2(t^2+4t+2)^2}{(t^2+2t+2)^4}, \forall t \in \mathbb{Q}\backslash\{-2,-1,0\}.$$

For the remaining of paper, we present the parameterization of Edwards curves defined over $\mathbb{Q}$ whose torsion subgroups are $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, respectively.

Theorem 8. *The Edwards curve* $E: x^2 + y^2 = 1 + dx^2y^2$, $d \in \mathbb{Q}\backslash\{0,1\}$ *has torsion subgroup* $E_{tor}(\mathbb{Q})$ *isomorphic to* $\mathbb{Z}/8\mathbb{Z}$ *if and only if* d *is not square in* $\mathbb{Q}$ *and* $d = (2\alpha^2-1)/\alpha^4$ *where* $\alpha \in \mathbb{Q}\backslash\{0, \pm 1\}$.

Proof. Necessity: Assume that an Edwards curve $E: x^2 + y^2 = 1 + dx^2y^2$ defined over $\mathbb{Q}$ such that

$$E_{\text{tor}}(\mathbb{Q}) \cong \mathbb{Z}/8\mathbb{Z}.$$

Due to $\mathbb{Z}/8\mathbb{Z}$ has only a point of order 2, so the group of points of E are the same. By the second case of Theorem 4, E has a point of order 2 which is $(0,-1)$, it means the point $\big((0:1),(-1:1)\big)$, and it is a unique point of order 2 on E if and only if d is not a square. In addition, with this value of d, E has only two points of order 4 by the third case of Theorem 4 which are $(1,0)$ and $(-1,0)$. Now, we assume P be a point of order 8 of E. Following the fourth case of Theorem 4, we have $P = (\alpha, \pm\alpha)$ where $\alpha \in \mathbb{Q}\backslash\{0\}$ satisfying the equation $dx^4 - 2x^2 + 1 = 0$. Due to P is a point on E, so we must have $\alpha \neq \pm 1$, because if it is not, it leads to $d = 1$, that is against the assumption of $d \neq 1$. Moreover, the curve equation results to $d = (2\alpha^2-1)/\alpha^4$ and $d\alpha^2 + \frac{1}{\alpha^2} = 2$. We rewrite $dx^4 - 2x^2 + 1 = dx^4 - \left(d\alpha^2 + \frac{1}{\alpha^2}\right)x^2 + 1 = dx^2(x-\alpha)(x+\alpha) - \frac{(x-\alpha)(x+\alpha)}{\alpha^2} = (x-\alpha)(x+\alpha)\left(dx^2 - \frac{1}{\alpha^2}\right)$. Because d is not a square, so that $dx^2 - \frac{1}{\alpha^2} \neq 0$ in $\mathbb{Q}$. So, the equation $dx^4 - 2x^2 + 1 = 0$ has only two roots α and $-\alpha$, and by the Theorem 4, E has only four points of order 8: (α,α), $(\alpha,-\alpha)$, $(-\alpha,-\alpha)$ and $(-\alpha,\alpha)$.

Therefore, if $E_{\text{tor}}(\mathbb{Q}) \cong \mathbb{Z}/8\mathbb{Z}$, d must satisfy to be not a square in $\mathbb{Q}$ and $d = (2\alpha^2-1)/\alpha^4$ with $\alpha \in \mathbb{Q}\backslash\{0, \pm 1\}$.

Sufficiency: Conversely, if $d = (2\alpha^2-1)/\alpha^4$ for $\alpha \in \mathbb{Q}\backslash\{0, \pm 1\}$ and d is not a square. So $d \neq 0,1$.

Then the Edwards curve defined over $\mathbb{Q}$

$$E: x^2 + y^2 = 1 + dx^2y^2$$

has only a point of order 2 and two points of order 4 because of Theorem 4. Moreover, by assumption $d = (2\alpha^2-1)/\alpha^4$ leads to α satisfies the equation $dx^4 - 2x^2 + 1 = 0$ so, by the Theorem 4, it implies that $(\alpha, \pm\alpha)$ are points of order 8 on E. Due to d is not a square, the equation $dx^4 - 2x^2 + 1 = 0$ has only two roots of α and $-\alpha$ in $\mathbb{Q}$. Therefore, all of points of order 8 of E are (α,α), $(-\alpha,-\alpha)$, $(\alpha,-\alpha)$, and $(-\alpha,\alpha)$. Lastly, we use the Mazur's theorem to get

$$E_{\text{tor}}(\mathbb{Q}) \cong \mathbb{Z}/8\mathbb{Z}.$$

Theorem 9. *The Edwards curve* $E: x^2 + y^2 = 1 + dx^2y^2$ *defined over* $\mathbb{Q}$ *has the torsion subgroup* $E_{tor}(\mathbb{Q})$ *isomorphic to* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ *if and only if* $d = s^2$ *where* $s \in \mathbb{Q}\backslash\{0\}$ *such as* $(s^2x^4 - 2x^2 + 1)(s^2x^4 - 2s^2x^2 + 1) \neq 0$ *for all* $x \in \mathbb{Q}$.

Proof. Necessity: Assume an Edwards curve E has a torsion subgroup $E_{\text{tor}}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Then, due to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ has only three points of order 2, four of order 4, and no points of order 8, it is the same for E. According to Theorem 4, this case appears if and only if $d \neq 0$ is a square in $\mathbb{Q}$, i.e $d = s^2$ with $s \in \mathbb{Q}\backslash\{0\}$. Moreover, due to E does not have a point of order 8, so the equation $(s^2x^4 - 2x^2 + 1)(s^2x^4 - 2s^2x^2 + 1) = 0$ does not have any roots on $\mathbb{Q}$ by Theorem 4.

Sufficiency: Conversely, we have an Edwards curve $E: x^2 + y^2 = 1 + dx^2y^2$ defined over $\mathbb{Q}$ in which d satisfies conditions from the theorem. Then, use of Theorem 4 to compute directly, we conclude the Edwards curve E to contain only three points of order 2, four of order 4, and no point of order 8. Therefore, by the theorem of Mazur, we obtain

$$E_{\text{tor}}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

From the above results, we have a consequence on parameterization of Edwards curve over $\mathbb{Q}$ with given torsion subgroups.

Corollary 1. *Given* $d \in \mathbb{Q}\backslash\{0,1\}$. *An Edwards curve* E *defined over* $\mathbb{Q}$ *by an equation*

$$E: x^2 + y^2 = 1 + dx^2y^2$$

has a torsion subgroup $E_{tor}(\mathbb{Q})$ which is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ if and only if d does not held any conditions shown in above Theorems 6, 7, 8, 9.

Proof. We conclude the corollary by the use of Note 1 and Theorems 6, 7, 8, 9.

IV. CONCLUSION

In this paper, we represented basic concepts on the generality of Edwards curves called twisted Edwards curve, and the addition law from the set of their points. The paper focuses on the parameterization of Edwards curves having the given torsion subgroup over the rational field Q. The main results are presented in the Theorems 16, 17 and Corollary 18.

Studying the parameterization of Edwards curves to be useful in construction a family of Edwards curves which are suitable to cryptographic applications. In [2], the authors use the parameterization of Edwards curves to construct the suitable curves for applying in the Elliptic Curve Method (ECM) to factor in factorization of integer numbers.

However, the parameterization in this paper is considered only for the Edwards curves, not for the case of twisted Edwards curves. The ability in cryptography application from these curves are also not mentioned. These problems are clearly interesting with many practical meanings that needs to further investigations.

ACKNOWLEDGMENT

First of all, we would like to thank the Editors, the critics who contributed deep, valuable comments to complete the scientific content as well as presentation form of the article. We would also like to thank the colleagues for their helping to the article.

REFERENCES

[1]. D.J. Bernstein, P. Birkner, M. Joye, T. Lange, C. Peters, "Twisted Edwards curves", In Africacrypt 2008, vol. 5023 of Lecture Notes in Computer Science, pp. 389-405, 2008.

[2]. D.J. Bernstein, P. Birkner, T. Lange, C. Peters, "ECM using Edwards curves", Mathematics of Computation, vol. 82, pp. 1139-1179, AMS, 2013.

[3]. D.J. Bernstein, T. Lange, "Faster addition and doubling on elliptic curves", In Asiacrypt 2007, vol. 4833 of Lecture Notes in Computer Sciene, pp. 29-50, Springer, 2007.

[4]. D.J. Bernstein, T. Lange, "A complete set of addition laws for incomplete Edwards curves", Journal of Number Theory, vol. 131, pp. 858-872, 2011.

[5]. H.M. Edwards, "A normal form of elliptic curves", Bullentin of the American Mathematical Society, vol. 44, pp. 393-422, 2007.

[6]. H. Hisil, K.K-H. Wong, G. Carter, E. Dawson, "Twisted Edwards curves revisited", In Asiacrypt 2008, vol. 5350 of Lecture Notes in Computer Science, pp. 326-343, Springer, Heidelberg, 2008.

[7]. L.C. Washington, *"Elliptic Curve: Number Theory and Cryptography"*, CRC Press, Boca Raton, 2008.

ABOUT THE AUTHOR

MS. Tung Linh Vo

Workplace: Institute of Cryptography Science and Technology.

Email: vtlinh@gmail.com

The education process: has received a mathematical bachelor degree in Hanoi University of Science, in 2005, and has received a mathematical master degree in Hanoi University of Science, in 2014.

Research today: elliptic curve cryptography; public key cryptography.