Tutorial of Twisted Edwards Curves in Elliptic Curve Cryptography

Emilie Menard Barnard

Abstract— **This is a tutorial of Twisted Edwards curves. I plan to introduce them in comparison to Edwards curves, and review standard group law operations. I will then relate Twisted Edwards curves and Montgomery curves. I will also introduce a projective and other popular coordinate systems for Twisted Edwards curves. In addition, I will compare and contrast Twisted Edwards curves with Edwards curves, and briefly discuss the EdDSA application of Twisted Edwards curves. Lastly, I will present the latest research regarding Twisted Edwards curves and their applications.**

I. Introduction

Edwards curves are a family of elliptic curves often used for cryptographic schemes. They exist over finite fields and are not only practically used in security measures, but also often studied for their mathematical properties.

Twisted Edwards curves are a generalization of the more popular Edwards curves. These generalized curves are used in important security schemes as well, and thus are also worth studying.

In this paper, I will introduce Twisted Edwards curves and provide sufficient background information so that one may apply them in their future studies.

II. Edwards Curves

Before discussing Twisted Edwards curves, I will briefly review the more commonly-known Edwards curves and their group law operations.

The original form of an Edwards curve, proposed by Harold Edwards in 2007, is as follows [7]:

$$x^2 + y^2 = c^2 + c^2x^2y^2$$

Bernstein and Lange then presented a simpler form given below [9]:

$$x^2 + y^2 = 1 + dx^2y^2 \tag{1}$$

where d is a quadratic non-residue, that is, the congruence

$$x^2 \equiv d \pmod{p}$$

for an integer $0 < x < p$ has no solution [15].

The zero or neutral element is $(0, 1)$, meaning $(x, y) \oplus (0, 1) = (x, y)$ for all x, y. The inverse of (x, y) is given by $(-x, y)$. The addition law for two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on an Edwards curve is as follows:

$$P \oplus Q = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

Note that the resulting point $P \oplus Q$ is also a point on the Edwards curve [9].

Author is with the Department of Computer Science, University of California, Santa Barbara, CA 93106. E-mail: `emilie@cs.ucsb.edu`

III. Twisted Edwards Curves

These Edwards curves are a specific kind of Twisted Edwards curves. That is, Twisted Edwards curves are a generalization of Edwards curves. Specifically, every Twisted Edwards curve is a *quadratic twist* of a corresponding Edwards curve[13]. A twist is defined as follows:

Definition 1: An elliptic curve E over field k has an associated quadratic twist when there is another elliptic curve which is isomorphic to E over an algebraic closure of k. Specifically, let E be an elliptic curve over a field k such that the field characteristic is not equal to 2 and E is of the following form:

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

Then, if $d \neq 0$, the *quadratic twist* of E is the curve E^d defined below:

$$y^2 = x^3 + da_2x^2 + d^2a_4x + d^3a_6$$

Moreover, the curves E and E^d are isomorphic over the field extension $k(\sqrt{d})$ [14].

In general, a Twisted Edwards curve over the field k (where the characteristic of k is no equal to 2) takes the following form:

$$ax^2 + y^2 = 1 + dx^2y^2 \tag{2}$$

with non-zeros $a \neq d$.

It can be shown that eq. (2) is a quadratic twist of the following Edwards curve:

$$\bar{x}^2 + \bar{y}^2 = 1 + (d/a)\bar{x}^2\bar{y}^2$$

where the map $(\bar{x}, \bar{y}) \to (x, y) = (\bar{x}\sqrt{a}, \bar{y})$ is an isomorphism over $k(\sqrt{a})$ [2].

Note further that a Twisted Edwards curve is just an Edwards curve with $a = 1$:

$$\begin{aligned} ax^2 + y^2 &= 1 + dx^2y^2 && \text{eq. (2)} \\ 1 \cdot x^2 + y^2 &= 1 + dx^2y^2 && (\text{let } a = 1) \\ x^2 + y^2 &= 1 + dx^2y^2 && \text{eq. (1)} \end{aligned}$$

IV. Group Law Operations

Just like with Edwards curves, the zero or neutral element on a Twisted Edwards curve is $(0, 1)$, and the inverse of point (x, y) is $(-x, y)$ [13].

A. *Addition*

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on a Twisted Edwards curve. Then the addition law is given below [2]:

$$P \oplus Q = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - a x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right) \tag{3}$$

For example, consider the following Twisted Edwards curve with $a = 3$ and $d = 2$:

$$3x^2 + y^2 = 1 + 2x^2 y^2 \tag{4}$$

Note that the point $(1, \sqrt{2})$ is on the curve. We can verify this by plugging the x and y values into eq (4):

$$\begin{aligned} 3x^2 + y^2 &= 1 + 2x^2y^2 \\ 3(1)^2 + (\sqrt{2})^2 &\overset{?}{=} 1 + 2(1)^2(\sqrt{2})^2 \\ 3 \cdot 1 + 2 &\overset{?}{=} 1 + 2 \cdot 1 \cdot 2 \\ 5 &= 5 \qquad \checkmark \end{aligned}$$

Similarly, we can also very that the point $(1, -\sqrt{2})$ is on the same curve:

$$\begin{aligned} 3x^2 + y^2 &= 1 + 2x^2y^2 \\ 3(1)^2 + (-\sqrt{2})^2 &\overset{?}{=} 1 + 2(1)^2(-\sqrt{2})^2 \\ 3 \cdot 1 + 2 &\overset{?}{=} 1 + 2 \cdot 1 \cdot 2 \\ 5 &= 5 \qquad \checkmark \end{aligned}$$

Thus, we can use eq. (3) to find $(1, \sqrt{2}) \oplus (1, -\sqrt{2})$:

$$\begin{aligned} (1, \sqrt{2}) \oplus (1, -\sqrt{2}) &= \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - a x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right) \\ &= (x_3, y_3) \\ &\implies \\ x_3 &= \frac{1 \cdot (-\sqrt{2}) + 1 \cdot (\sqrt{2})}{1 + 2 \cdot 1 \cdot 1 \cdot \sqrt{2} \cdot (-\sqrt{2})} \\ &= \frac{0}{1 + 2 \cdot (-2)} \\ &= 0 \\ y_3 &= \frac{\sqrt{2} \cdot (-\sqrt{2}) - 3 \cdot 1 \cdot 1}{1 - 2 \cdot 1 \cdot 1 \cdot \sqrt{2} \cdot (-\sqrt{2})} \\ &= \frac{-2 - 3}{1 - 2 \cdot (-2)} \\ &= -1 \end{aligned}$$

Therefore, $(1, \sqrt{2}) \oplus (1, -\sqrt{2}) = (0, -1)$. We can also check that this point is on our curve given by eq. (4):

$$\begin{aligned} 3x^2 + y^2 &= 1 + 2x^2y^2 \\ 3(0)^2 + (-1)^2 &\overset{?}{=} 1 + 2(0)^2(-1)^2 \\ 1 &= 1 \qquad \checkmark \end{aligned}$$

B. *Doubling*

We can derive a doubling formula for $[2]P = (x_1, y_1) \oplus (x_1, y_1)$ from the addition formula given by eq (3):

$$\begin{aligned} P \oplus Q &= \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - a x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right) \\ 2[P] &= \left(\frac{x_1 y_1 + y_1 x_1}{1 + d x_1 x_1 y_1 y_1}, \frac{y_1 y_1 - a x_1 x_1}{1 - d x_1 x_1 y_1 y_1} \right) \\ &= \left(\frac{2 x_1 y_1}{1 + d x_1^2 y_1^2}, \frac{y_1^2 - a x_1^2}{1 - d x_1^2 y_1^2} \right) \end{aligned}$$

This is equivalent to the following:

$$2[P] = \left(\frac{2 x_1 y_1}{a x_1^2 + y_1^2}, \frac{y_1^2 - a x_1^2}{2 - a x_1^2 - y_1^2} \right) \tag{5}$$

For example, consider doubling the point $(1, \sqrt{2})$ on the curve given in eq. (4):

$$\begin{aligned} 2[P] &= \left(\frac{2 x_1 y_1}{a x_1^2 + y_1^2}, \frac{y_1^2 - a x_1^2}{2 - a x_1^2 - y_1^2} \right) \\ &= (x_3, y_3) \\ &\implies \\ x_3 &= \frac{2 x_1 y_1}{a x_1^2 + y_1^2} \\ &= \frac{2 \cdot 1 \cdot \sqrt{2}}{3 \cdot 1^2 + \sqrt{2}^2} \\ &= \frac{2\sqrt{2}}{5} \\ y_2 &= \frac{y_1^2 - a x_1^2}{2 - a x_1^2 - y_1^2} \\ &= \frac{\sqrt{2}^2 - 3 \cdot 1^2}{2 - 3 \cdot 1^2 - \sqrt{2}^2} \\ &= \frac{-1}{-3} \\ &= \frac{1}{3} \end{aligned}$$

Thus, $[2](1, \sqrt{2}) = \left(\frac{2\sqrt{2}}{5}, \frac{1}{3} \right)$. Let's confirm that $[2]P$ is indeed on the Twisted Edwards curve:

$$\begin{aligned} 3x^2 + y^2 &= 1 + 2x^2y^2 \\ 3\left(\frac{2\sqrt{2}}{5}\right)^2 + \left(\frac{1}{3}\right)^2 &\overset{?}{=} 1 + 2\left(\frac{2\sqrt{2}}{5}\right)^2 \left(\frac{1}{3}\right)^2 \\ 3\left(\frac{4 \cdot 2}{25}\right) + \frac{1}{9} &\overset{?}{=} 1 + 2\left(\frac{4 \cdot 2}{25}\right)\left(\frac{1}{9}\right) \\ \frac{24}{25} + \frac{1}{9} &\overset{?}{=} \frac{225}{225} + \frac{16}{255} \\ \frac{216}{225} + \frac{25}{225} &\overset{?}{=} \frac{241}{225} \\ \frac{241}{225} &= \frac{241}{255} \qquad \checkmark \end{aligned}$$

Therefore $[2]P$ is on the Twisted Edwards curve, as expected.

V. Twisted Edwards Curves and Montgomery Curves

Twisted Edwards curves and Montgomery curves are closely related. First, I will provide a brief introduction to Montgomery curves.

Fix a field k with characteristic of k not equal to 2. Fix specific $A, B \in k$. Then the following:

$$By^2 = x^3 + Ax^2 + x$$

is a Montgomery curve [11].

It can be shown that every Twisted Edwards curve over a field k is *birationally equivalent* over k to a Montgomery curve [2]. A birational equivalence is defined as follows:

Definition 2: Two varieties are said to be birationally equivalent if there exits a birational map between them, or an isomorphism of their function fields as extensions of the base field.
In the case of Twisted Edwards curves and Montgomery curves, their rational function fields are isomorphic. Similarly, every Montgomery curve over k is birationally equivalent over k to a Twisted Edwards curve. Thus, the set of Montgomery curves over k is equivalent to the set of Twisted Edwards curves over k [2].

VI. Alternate Coordinate Systems

There are various alternate coordinate systems in which one can work with coordinates on a given Twisted Edwards curve. They are worth studying not only for their pure mathematical properties, but also for their advantages in certain application settings.

A. Extended Coordinate Systems

In extended coordinate systems, a point (x, y) on $ax^2 + y^2 = 1 + dx^2y^2$ is represented by X, Y, Z and T satisfying the following equations:

$$x = X/Z$$
$$y = Y/Z$$
$$xy = T/Z$$

In extended coordinate systems, $(0 : 1 : 1 : 0$ is the identity element, and the negative of point $(X : Y : Z : T)$ is $(-X : Y : Z : -T)$ [13].

There is a specific extended coordinate system where
$a = -1$ [3].

B. Inverted Coordinate System

In the inverted coordinate system, a point (x, y) is represented by X, Y and Z as follows:

$$x = Z/X$$
$$y = Z/Y$$

where X, Y and Z are non-zero. The general form of the corresponding curve is given below:

$$(X^2 + aY^2)Z^2 = X^2Y^2 + dZ^4$$

When $a = 1$, addition operations take less time [13].

C. Projective Coordinate System

An affine point (x, y) can also be considered in the projective coordinate system. X, Y and Z represent the x and y coordinates using the following rules:

$$x = X/Z$$
$$y = Y/Z$$

The corresponding projective Twisted Edwards curve is of the form below:

$$(aX^2 + Y^2)Z = Z^4 + dX^2Y^2$$

where $Z \neq 0$ [3].

Using the projective coordinate system, inversion costs can be avoided [13].

VII. Twisted Edwards Curves versus Edwards Curves

In some cases, there are advantages to using Twisted Edwards curves over Edwards curves. Even when a curve can be expressed in the form of an Edwards curve, expressing it as a Twisted Edwards curve oven saves arithmetic time. If you are free to choose the curve in your application, you can use this knowledge to your advantage to save time [2].

Twisted Edwards curves also cover more elliptic curves than Edwards curves over fields over prime p where
$p \equiv 1 \pmod 4$. Specifically, there are approximately 1.67 times more Twisted Edwards curves than Edwards curves in this case [2].

VIII. EdDSA

The Edwards-curve Digital Signature Algorithm (EdDSA) is the likely the most significant cryptographic application based on Twisted Edwards curves. The algorithm is designed for high performance and avoids common security issues that are common in alternative digital signature algorithms [5].

Specifically, Ed25519 (a particular implementation of EdDSA) uses the following Twisted Edwards curve:

$$-x^2 + y^2 = 1 - \frac{121665}{121666}x^2y^2$$

where $a = -1$ and $d = 121665/121666$ over the field defined by the prime number $2^{255} - 19$. It is birationally equivalent (see section V.) to the Montgomery curve $Curve25519$ with the following equivalence [5]:

$$x = \sqrt{-486664}u/v$$
$$y = \frac{u-1}{u+1}$$

IX. Latest Research

Because Twisted Edwards curves were only recently introduced, there has been significant recent research. Just this year, over 3000 papers that discuss these curves have been published, according to Google Scholar.[1]

[1] https://scholar.google.com/

In January of this year, a short article that shows that the number of rational points on a Twisted Edwards curve can be calculated using the Gaussian hypergeometic series was published [12]. In June, Microsoft's research group presented a new deterministic algorithm for generating Twisted Edwards curves [4]. A paper published in August presented new speed records (8.77M per bit on variables of size 256 bits) for arithmetic on curves with cofactor 3 [1]. And just last month, a special family of Twisted Edwards curves named Optimal mixed Montgomery-Edwards (OME) curves were introduced [10].

New research supporting the significance of Twisted Edwards curves is presented daily. Hopefully this brief tutorial of these elliptic curves will inspire, or at least facilitate, more.

Acknowledgements

Thank you to Professor Çetin Kaya Koç, Professor of Computer Science at the University of California, Santa Barbara.

References

[1] Bernstein, Daniel J., Chitchanok Chuengsatiansup, David Kohel, and Tana Lange. "Twisted Hessian Curves." Springer Link. Progress in Cryptology – LATINCRYPT 2015, 15 Aug. 2015. Web. http://link.springer.com/chapter/10.1007/978-3-319-22174-8_15.

[2] Bernstein, Daniel J., Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. "Twisted Edwards Curves."Cryptology EPrint Archive (2008): Web. http://eprint.iacr.org/2008/013.pdf.

[3] Bernstein, Daniel J., and Tanja Lange. "Twisted Edwards Curves." Explicit-Formulas Database. Hyperelliptic.org. Web. http://hyperelliptic.org/EFD/g1p/auto-twisted.html.

[4] Costello, Craig, Patrick Longa, and Michael Naehrig. "A Brief Discussion on Selecting New Elliptic Curves." Microsoft Research. Microsoft, 8 June 2015. Web. http://research.microsoft.com/pubs/246915/NIST.pdf.

[5] "EdDSA." Wikipedia. Wikimedia Foundation, 15 Oct. 2015. Web.https://en.wikipedia.org/wiki/EdDSA.

[6] "Edward-curves" by Georg-Johann - Own work coordinates from this vector image includes elements that have been taken or adapted from this: Lemniscate-of-Gerono.svg. Licensed under CC BY-SA 3.0 via Commons - https://commons.wikimedia.org/wiki/File:Edward-curves.svg#/media/File:Edward-curves.svg.

[7] Edwards, Harold M. "A Normal Form for Elliptic Curves." American Mathematical Society 44.3 (2007): 393-422. Web. http://www.ams.org/journals/bull/2007-44-03/S0273-0979-07-01153-6/S0273-0979-07-01153-6.pdf.

[8] Hisil, Huseyin, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. "Twisted Edwards Curves Revisited." Advances in Cryptology - ASIACRYPT 2008 Lecture Notes in Computer Science (2008): 326-43. Web. http://eprint.iacr.org/2008/522.pdf.

[9] Koç, Çetin Kaya. "Edwards Curves." ECC Fundamentals. University of California, Santa Barbara: CS290G, 9 Nov. 2015. Web. http://cs.ucsb.edu/~koc/ecc/docx/10edwards.pdf.

[10] Liu, Zhe, Zhi Hu, and Wei Hu. "Elliptic Curve with Optimal Mixed Montgomery-Edwards Model for Low-end." Springer Link. Science China Information Sciences, Nov. 2015. Web. http://link.springer.com/article/10.1007/s11432-015-5410-y.

[11] "Montgomery Curve." Wikipedia. Wikimedia Foundation, 30 Oct. 2015. Web. https://en.wikipedia.org/wiki/Montgomery_curve#Equivalence_with_twisted_Edwards_curves.

[12] Sadek, Mohammad, and Nermine El-Sissi. "Edwards Curves and Gaussian Hypergeometric Series." Number Theory. Cornell University Library, 14 Jan. 2015. Web. http://arxiv.org/abs/1501.03526.

[13] "Twisted Edwards Curves." Wikipedia. Wikimedia Foundation, 26 May 2015. Web. https://en.wikipedia.org/wiki/Twisted_edwards_curve.

[14] "Twists of Curves." Wikipedia. Wikimedia Foundation, 15 Sept. 2015. Web. https://en.wikipedia.org/wiki/Twists_of_curves.

[15] Weisstein, Eric W. "Quadratic Nonresidue." From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/QuadraticNonresidue.html