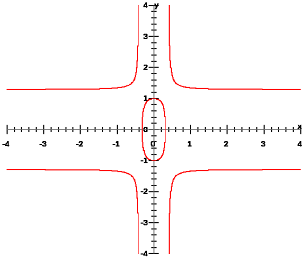
Twisted Edwards Curves

Emilie Menard Barnard
emilie@cs.ucsb.edu



Outline

- Edwards Curves Review
- Derivation of Twisted Edwards Curves
- Group Law Operations
- Montgomery Curves
- Projective Coordinate System
- Twisted Edwards Curves vs Edwards Curves
- EdDSA
- Latest Research

Edwards Curves Review

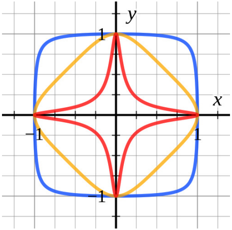
- Original Form of an Edwards Curve:

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

- Bernstein's and Lange's simpler form:

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

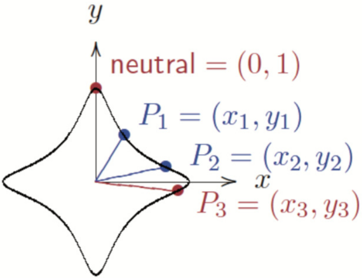
where d is a quadratic non-residue



Edwards Curves Review (slide credit to Professor Koç)

- The zero (neutral) element is (0,1)
- The inverse of (x, y) is $(-x, y)$
- The addition law is as follows:

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



Twisted Edwards Curves

- The Edwards Curves (ECs) we studied are a specific kind of **Twisted Edwards Curves** (TECs)
- Every TEC is a *twist* of a corresponding EC
  - 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

Quadratic Twists

- Let E be an elliptic curve over a field k ($char(k) \neq 2$) of the 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 as

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

- The curves E and E^d are isomorphic over the field extension $k(\sqrt{d})$

Derivation of TECs

- In general, a Twisted Edwards Curve in field k ($char(k) \neq 2$) of the form
$$ax^2 + y^2 = 1 + dx^2y^2$$
(where $a \neq d$ are non-zero)
is a quadratic twist of the Edwards Curve
$$\bar{x}^2 + \bar{y}^2 = 1 + (d/a)\bar{x}^2\bar{y}^2$$
- The map $(\bar{x}, \bar{y}) \to (x, y) = (\bar{x}/\sqrt{a}, \bar{y})$ is an isomorphism over $k(\sqrt{a})$

Twisted Edwards Curves

- Note that a TEC is just an EC with $a = 1$:

$$\begin{aligned} ax^2 + y^2 &= 1 + dx^2y^2 && \text{(TEC general form)} \\ 1 \cdot x^2 + y^2 &= 1 + dx^2y^2 && \text{(let } a = 1\text{)} \\ x^2 + y^2 &= 1 + dx^2y^2 && \text{(EC general form)} \end{aligned}$$

Neutral Element, Inverse, Addition

- The zero (neutral) element is (0,1)
- The inverse of (x, y) is $(-x, y)$
- Let $P = (x_1, y_1)$ and $Q = (x_2, y_1)$ be two points on a TEC. Then

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

Addition Example

- Given the TEC with $a = 3$ and $d = 2$:

$$3x^2 + y^2 = 1 + 2x^2y^2$$

- We can find $(1, \sqrt{2}) \oplus (1, -\sqrt{2})$:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} = \frac{1 \cdot (-\sqrt{2}) + 1 \cdot (\sqrt{2})}{1 + 2 \cdot 1 \cdot 1 \cdot \sqrt{2} \cdot (-\sqrt{2})} = \frac{0}{1 + 2 \cdot (-2)} = 0$$

$$y_3 = \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} = \frac{\sqrt{2} \cdot (-\sqrt{2}) - 3 \cdot 1 \cdot 1}{1 - 2 \cdot 1 \cdot 1 \cdot \sqrt{2} \cdot (-\sqrt{2})} = \frac{-2 - 3}{1 - 2 \cdot (-2)} = -1$$

$$\therefore (1, \sqrt{2}) \oplus (1, -\sqrt{2}) = (0, -1)$$

Doubling

- Can be derived from the addition formula
- Let $P = (x_1, y_1)$ be a point on a TEC. Then

$$[2]P = \left(\frac{2x_1y_1}{ax_1^2 + y_1^2}, \frac{y_1^2 - ax_1^2}{2 - ax_1^2 - y_1^2} \right)$$

Doubling Example

- Given the TEC with $a = 3$ and $d = 2$:

$$3x^2 + y^2 = 1 + 2x^2y^2$$

- We can find $[2](1, \sqrt{2})$:

$$x_3 = \frac{2x_1y_1}{ax_1^2 + y_1^2} = \frac{2 \cdot 1 \cdot \sqrt{2}}{3 \cdot 1^2 + \sqrt{2}^2} = \frac{2\sqrt{2}}{5}$$

$$y_2 = \frac{y_1^2 - ax_1^2}{2 - ax_1^2 - y_1^2} = \frac{\sqrt{2}^2 - 3 \cdot 1^2}{2 - 3 \cdot 1^2 - \sqrt{2}^2} = \frac{-1}{-3} = \frac{1}{3}$$

$$\therefore [2](1, \sqrt{2}) = \left(\tfrac{2\sqrt{2}}{5}, \tfrac{1}{3}\right)$$

Montgomery Curves

- Fix a field k with $char(k) \neq 2$, and certain $A, B \in k$. Then
$$By^2 = x^3 + Ax^2 + x$$
is a Montgomery curve.
- Every TEC over k is *birationally equivalent* (rational function fields are isomorphic) over k to a Montgomery curve
- Every Montgomery curve over k is birationally equivalent over k to a TEC
- $\therefore$ The set of Montgomery curves over k is equivalent to the set of TECs over k

Projective Coordinate System

- In the projective coordinate system, a point (x, y) on $ax^2 + y^2 = 1 + dx^2y^2$ is represented by X, Y, Z satisfying

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

- The corresponding projective TEC is of the form

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

- We avoid inversion costs using this system

TECs vs ECs

- Over fields F_p where $p \equiv 1 \pmod 4$, TECs cover more elliptic curves than ECs
- Even when a curve can be expressed in EC form, expressing it in TEC form often saves arithmetic time
  - If you are free to choose the curve, you can use this to your advantage

EdDSA

- Edwards-curve Digital Signature Algorithm (EdDSA) is based on TECs
- Designed for high performance while avoiding common security problems
- Ed25519 is a specific implementation using the TEC

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

over the field defined by $2^{255} - 19$

Latest Research

- (Jan.) The number of rational points on a TEC can be calculated using the Gaussian hypergeometric series
- (June) Microsoft's research group presented a new deterministic algorithm for generating TECs
- (Aug.) Bernstein et al. presented new speed records (8.77M per bit, on variables of size 256 bits) for arithmetic on curves with cofactor 3
- (Nov.) A special family of TECs named Optimal mixed Montgomery-Edwards (OME) curves were introduced

References (1/4)

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.

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.

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

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.

References (2/4)

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

"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.

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.

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.

References (3/4)

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.

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.

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

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.

References (4/4)

"Twisted Edwards curve" by Krishnavedala - Own work. Licensed under CC BY-SA 3.0 via Commons - https://commons.wikimedia.org/wiki/File:Twisted_Edwards_curve.svg#/media/File:Twisted_Edwards_curve.svg.

"Twists of Curves." Wikipedia. Wikimedia Foundation, 26 May 2015. Web. https://en.wikipedia.org/wiki/Twists_of_curves.

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