lwip
Internet-Draft
Intended status: Informational
Expires: May 3, 2018

R. Struik
Struik Security Consultancy

October 30, 2017

Alternative Elliptic Curve Representations
draft-struik-lwip-curve-representations-00

Abstract

This document specifies how to represent Montgomery curves and (twisted) Edwards curves as curves in short-Weierstrass form and illustrates how this can be used to implement elliptic curve computations using existing implementations that already implement, e.g., ECDSA and ECDH using NIST prime curves.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 3, 2018.

Copyright Notice

Table of Contents

1. Fostering Code Reuse with New Elliptic Curves

It is well-known that elliptic curves can be represented using different curve models. Recently, IETF has standardized elliptic curves that are claimed to have better performance and improved robustness against "real world" attacks than curves represented in the traditional "short" Weierstrass model. This draft specifies an alternative representation of points on Curve25519, as specified in RFC 7748, and of points on Ed25519, as specified in RFC 8032, as points on a specific "short" Weierstrass curve, called Wei25519.

Use of Wei25519 allows easy definition of signature schemes and key agreement schemes already specified for traditional NIST prime curves, thereby allowing easy integration with existing

specifications, such as NIST SP 800-56a and FIPS Pub 186-4, and ANSI X9.63-2005, and fostering code reuse on platforms that already implement some of these schemes.

For details, we refer to the appendices.

2. Security Considerations

The different representations of elliptic curve points discussed in this draft are all obtained using a publicly known transformation. Since this transformation is an isomorphism, this transformation maps elliptic curve points to equivalent mathematical objects.

3. IANA Considerations

There is no IANA action required for this document.

4. Normative References

[ANSI-X9.62] ANSI X9.62-2005, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", American National Standard for Financial Services, Accredited Standards Committee X9, Inc Anapolis, MD, 2005.

[FIPS-186-4] FIPS 186-4, "Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4", US Department of Commerce/National Institute of Standards and Technology Gaithersburg, MD, July 2013.

[I-D.ietf-6lo-ap-nd] Sarikaya, B., Thubert, P., and M. Sethi, "Address Protected Neighbor Discovery for Low-power and Lossy Networks", draft-ietf-6lo-ap-nd-03 (work in progress), September 2017.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/info/rfc7748>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/info/rfc8032>.

[SP-800-56a] NIST SP 800-56a, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Log Cryptography, Revision 2", US Department of Commerce/National Institute of Standards and Technology Gaithersburg, MD, June 2013.

Appendix A. Some (non-Binary) Elliptic Curves

A.1. Curves in short-Weierstrass Form

Let GF(q) denote the finite field with q elements, where q is an odd prime power and where q is not divisible by three. Let W_{a,b} be the Weierstrass curve with defining equation y^2 = x^3 + a*x + b, where a and b are elements of GF(q) and where 4*a^3 + 27*b^2 is nonzero. The points of W_{a,b} are the ordered pairs (x, y) whose coordinates are elements of GF(q) and which satisfy the defining equation (the so-called affine points), together with the special point O (the so-called "point at infinity").This set forms a group under addition, via the so-called "chord-and-tangent" rule, where the point at infinity serves as the identity element. See Appendix B.1 for details of the group operation.

A.2. Montgomery Curves

Let GF(q) denote the finite field with q elements, where q is an odd prime power. Let M_{A,B} be the Montgomery curve with defining equation B*v^2 = u^3 + A*u^2 + u, where A and B are elements of GF(q) with A unequal to (+/-)2 and with B nonzero. The points of M_{A,B} are the ordered pairs (u, v) whose coordinates are elements of GF(q) and which satisfy the defining equation (the so-called affine points), together with the special point O (the so-called "point at infinity").This set forms a group under addition, via the so-called "chord-and-tangent" rule, where the point at infinity serves as the identity element. See Appendix B.2 for details of the group operation.

A.3. Twisted Edwards Curves

Let GF(q) denote the finite field with q elements, where q is an odd prime power. Let E_{a,d} be the twisted Edwards curve with defining equation a*x^2 + y^2 = 1+ d*x2*y2, where a and d are distinct nonzero elements of GF(q). The points of E_{a,d} are the ordered pairs (x, y) whose coordinates are elements of GF(q) and which satisfy the

defining equation (the so-called affine points). It can be shown that this set forms a group under addition if a is a square in GF(q), whereas d is not, where the point (0, 1) serves as the identity element. (Note that the identity element satisfies the defining equation.) See Appendix B.3 for details of the group operation. An Edwards curve is a twisted Edwards curve with a=1.

Appendix B. Elliptic Curve Group Operations

B.1. Group Law for Weierstrass Curves

For each point P on the Weierstrass curve W_{a,b}, the point at infinity O serves as identity element, i.e., P + O = O + P = P.

For each point P:=(x, y) on the Weierstrass curve W_{a,b}, the point -P is the point (x, -y) and one has P + (-P) = O.

Let P1:=(x1, y1) and P2:=(x2, y2) be distinct points on the Weierstrass curve W{a,b} and let Q:=P1 + P2, where Q is not the identity element. Then Q:=(x, y), where

x + x1 + x2 = lambda^2 and y + y1 = lambda*(x1 - x), where lambda = (y2 - y1)/(x2 - x1).

Let P:= (x1, y1) be a point on the Weierstrass curve W{a,b} and let Q:=2P, where Q is not the identity element. Then Q:= (x, y), where

x + 2*x_1 = lambda^2 and y + y1 = lambda*(x1 - x), where lambda=(3*x1^2 + a)/(2*y1).

B.2. Group Law for Montgomery Curves

For each point P on the Montgomery curve M_{A,B}, the point at infinity O serves as identity element, i.e., P + O = O + P = P.

For each point P:=(x, y) on the Montgomery curve M_{A,B}, the point -P is the point (x, -y) and one has P + (-P) = O.

Let P1:=(x1, y1) and P2:=(x2, y2) be distinct points on the Montgomery curve M_{A,B} and let Q:=P1 + P2, where Q is not the identity element. Then Q:=(x, y), where

x + x1 + x2 = B*lambda^2 - A and y + y1 = lambda*(x1 - x), where lambda=(y2 - y1)/(x2 - x1).

Let P:= (x1, y1) be a point on the Montgomery curve M_{A,B} and let Q:=2P, where Q is not the identity element. Then Q:= (x, y), where

x + 2*x_1 = B*lambda^2 - A and y + y1 = lambda*(x1 - x), where lambda=(3*x1^2 + 2*A*x_1+1)/(2*y1).

B.3. Group Law for Twisted Edwards Curves

Note: The group laws below hold for twisted Edwards curves E_{a,d} where a is a square in GF(q), whereas d is not. In this case, the addition formula below are defined for each pair of points, without exceptions. Generalizations of this group law to other twisted Edwards curves are out of scope.

For each point P on the twisted Edwards curve E_{a,d}, the point O=(0,1) serves as identity element, i.e., P + O = O + P = P.

For each point P:=(x, y) on the twisted Edwards curve E_{a,d}, the point -P is the point (-x, y) and one has P + (-P) = O.

Let P1:=(x1, y1) and P2:=(x2, y2) be points on the twisted Edwards curve E_{a,d} and let Q:=P1 + P2. Then Q:=(x, y), where

x = (x1*y2 + x2*y1)/(1 + d*x1*x2*y1*y2) and y = (y1*y2 - a*x1*x2)/(1 - d*x1*x2*y1*y2).

Let P:=(x1, y1) be a point on the twisted Edwards curve E_{a,d} and let Q:=2P. Then Q:=(x, y), where

x = (2*x1*y1)/(1 + d*x1^2*y1^2) and y = (y1^2 - a*x1^2)/(1 - d*x1^2*y1^2).

Appendix C. Relationship Between Curve Models

The non-binary curves specified in Appendix A are expressed in different curve models, viz. as curves in short-Weierstrass form, as Montgomery curves, or as twisted Edwards curves. These curve models are related, as follows.

C.1. Mapping between twisted Edwards Curves and Montgomery Curves

One can map points of the Montgomery curve M_{A,B} to points of the twisted Edwards curve E_{a,d}, where a:=(A+2)/B and d:=(A-2)/B and, conversely, map points of the twisted Edwards curve E_{a,d} to points of the Montgomery curve M_{A,B}, where A:=2(a+d)/(a-d) and where B:=4/(a-d). For twisted Edwards curves we consider (i.e., those where a is a square in GF(q), whereas d is not), this defines a one-to-one correspondence, which - in fact - is an isomorphism between M_{A,B} and E_{a,d}, thereby showing that, e.g., the discrete logarithm problem in either curve model is equally hard.

For the Montgomery curves and twisted Edwards curves we consider, the mapping from M_{A,B} to E_{a,d} is defined by mapping the point at infinity O and the point (0, 0) of order two on M_{A,B} to, respectively, the point (0, 1) and the point (0, -1) of order two of E_{a,d}, while mapping each other point (u, v) on M_{A,B} to the point (x, y):=(u/v, (u-1)/(u+1)) on E_{a,d}. The inverse mapping from E_{a,d} to M_{A,B} is defined by mapping the point (0, 1) and the point (0, -1) of order two of E_{a,d} to, respectively, the point at infinity O and the point (0, 0) of order two on M_{A,B}, while each other point (x, y) of E_{a,d} is mapped to the point (u, v):=((1+y)/(1-y), (1+y)/((1-y)x)) of M_{A,B}.

Implementations may take advantage of this mapping to carry out elliptic curve group operations originally defined for a twisted Edwards curve on the corresponding Montgomery curve, or vice-versa, and translating the result back to the original curve, thereby potentially allowing code reuse.

C.2. Mapping between Montgomery Curves and Weierstrass Curves

One can map points on the Montgomery curve M_{A,B} to points on the Weierstrass curve W_{a,b}, where a:=(3-A^2)/(3*B^2) and b:=(2*A^3-9*A)/(27*B^3). This defines a one-to-one correspondence, which - in fact - is an isomorphism between M_{A,B} and W_{a,b}, thereby showing that, e.g., the discrete logarithm problem in either curve model is equally hard.

The mapping from M_{A,B} to W_{a,b} is defined by mapping the point at infinity O on M_{A,B} to the point at infinity O on W_{a,b}, while mapping each other point (u, v) of M_{A,B} to the point (x, y):=(u/B+A/3B, v/B) of W_{a,b}. Note that not all Weierstrass curves can be injectively mapped to Montgomery curves, since the latter have a point of order two and the former may not. In particular, if a Weierstrass curve has prime order, such as is the case with the so-called "NIST curves", this inverse mapping is not defined.

This mapping can be used to implement elliptic curve group operations originally defined for a twisted Edwards curve or for a Montgomery curve using group operations on the corresponding elliptic curve in short-Weierstrass form and translating the result back to the original curve, thereby potentially allowing code reuse. Note that implementations for elliptic curves with short-Weierstrass form that hard-code the domain parameter a to a= -3 (which value is known to allow more efficient implementations) cannot always be used this way, since the curve W_{a,b} may not always be expressed in terms of a Weierstrass curve with a=-3 via a coordinate transformation.

C.3. Mapping between twisted Edwards Curves and Weierstrass Curves

One can map points of the twisted Edwards curve E_{a,d} to points of the Weierstrass curve W_{a,b}, via function composition, where one uses the isomorphic mapping between twisted Edwards curve and Montgomery curves of Appendix C.1 and the one between Montgomery and Weierstrass curves of Appendix C.2. Obviously, one can use function composition (now using the respective inverses) to realize the inverse of this mapping.

Appendix D. Curve25519 and Cousins

D.1. Curve Definition and Alternative Representations

The elliptic curve Curve25519 is the Montgomery curve M_{A,B} defined over the prime field GF(p), with p:=2^{255}-19, where A:=486662 and B:=1. This curve has order h*n, where h=8 and where n is a prime number. For this curve, A^2-4 is not a square in GF(p), whereas A+2 is. The quadratic twist of this curve has order h1*n1, where h1=4 and where n1 is a prime number. For this curve, the base point is defined to be the ordered pair (Gu,Gv) of elements of GF(p), where Gu=9 and where Gv is an odd integer in the interval [0, p-1].

This curve has the same group structure as (is "isomorphic" to) the twisted Edwards curve E_{a,d} defined over GF(p), with as base point the ordered pair (Gx,Gy) of elements of GF(p), where parameters are as specified in Appendix D.3. This curve is denoted as Ed25519. For this curve, the parameter a is a square in GF(p), whereas d is not, so the group laws of Appendix B.3 apply.

The curve is also isomorphic to the elliptic curve W_{a,b} in short-Weierstrass form defined over GF(p), with as base point the ordered pair (Gx’,Gy’) of elements, where parameters are as specified in Appendix D.3. This curve is denoted as Wei25519.

D.2. Switching between Alternative Representations

Each point (u,v) of Curve25519 corresponds to the point (x,y):=(u + A/3,y) of Wei25519, while the point at infinity of Curve25519 corresponds to the point at infinity of Wei25519. (Here, we used the mapping of Appendix C.2.) Under this mapping, the base point (Gu,Gv) of Curve25519 corresponds to the base point (Gx’,Gy’) of Wei25519. The inverse mapping maps the point (x,y) on Wei25519 to (u,v):=(x - A/3,y) on Curve25519, while mapping the point at infinity of Wei25519 to the point at infinity on Curve25519. Note that this mapping involves a simple shift of the first coordinate and can be implemented via integer-only arithmetic as a shift of (p+A)/3 for the

isomorphic mapping and a shift of -(p+A)/3 for its inverse, where delta=(p+A)/3 is the element of GF(p) defined by

delta 19298681539552699237261830834781317975544997444273427339909597334652188435537

(=0x2aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaad2451)

The curve Ed25519 is isomorphic to the curve Curve25519, where the base point (Gu,Gv) of Curve25519 corresponds to the base point (Gx,Gy) of Ed25519 and where the point at infinity and the point (0,0) of order two of Curve25519 correspond to, respectively, the point (0, 1) and the point (0, -1) of order two of Ed25519 and where each other point (u, v) of Curve25519 corresponds to the point (c*u/v, (u-1)/(u+1)) of Ed25519, where c is the element of GF(p) defined by

c sqrt(-(A+2))

5104256939916053613020613523314632928415220225303463182268183378866687721520 7

(=0x70d9120b 9f5ff944 2d84f723 fc03b081 3a5e2c2e b482e57d 3391fb55 00ba81e7)

(Here, we used the mapping of Appendix C.1.) The inverse mapping from Ed25519 to Curve25519 is defined by mapping the point (0, 1) and the point (0, -1) of order two of Ed25519 to, respectively, the point at infinity and the point (0,0) of order two of Curve25519 and having each other point (x, y) of Ed25519 correspond to the point ((1 + y)/(1 - y), c(1 + y)/((1-y)x)).

The curve Ed25519 is isomorphic to the Weierstrass curve Wei25519, where the base point (Gx,Gy) of Ed25519 corresponds to the base point (Gx’,Gy’) of Wei25519 and where the identity element (0,1) and the point (0,-1) of order two of Ed25519 correspond to, respectively, the point at infinity O and the point (A/3, 0) of order two of Wei25519 and where each other point (x, y) of Ed25519 corresponds to the point (x’, y’):=((1+y)/(1-y)+A/3, c(1+y)/((1-y)*x)) of Wei25519, where c was defined before. (Here, we used the mapping of Appendix C.3.) The inverse mapping from Wei25519 to Ed25519 is defined by mapping the point at infinity O and the point (A/3, 0) of order two of Wei25519 to, respectively, the identity element (0,1) and the point (0,-1)) of order two of Ed25519 and having each other point (x, y) of Wei25519 correspond to the point (c*(3*x+A)/(3*y), (x+A-3)/(x+A+3)).

Note that these mappings can be easily realized in projective coordinates, using a few field multiplications only, thus allowing switching between alternative representations with negligible relative incremental cost.

D.3. Domain Parameters

The parameters of the Montgomery curve and the corresponding isomorphic curves in twisted Edwards curve and short-Weierstrass form are as indicated below. Here, the domain parameters of Curve25519 and Ed25519 are as specified in RFC 7748; the domain parameters of Wei25519 are "new".

General parameters:

p 2^{255}-19

(=0x7fffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff ffffffed)

h 8

n 7237005577332262213973186563042994240857116359379907606001950938285454250989

(=2^{252} + 0x14def9de a2f79cd6 5812631a 5cf5d3ed)

h1 4

n1 1447401115466452442794637312608598848160326344765032579786049412540737390799 7

(=2^{253} - 0x29bdf3bd 45ef39ac b024c634 b9eba7e3)

Montgomery curve-specific parameters:

A 486662

B 1

Gu 9 (=0x9)

Gv 1478161944758954479102059356840998688726460613461647528896488183775558623740 1

(=0x20ae19a1 b8a086b4 e01edd2c 7748d14c 923d4d7e 6d7c61b2 29e9c5a2 7eced3d9)

Twisted Edwards curve-specific parameters:

a -1 (-0x01)

d -121665/121666

(=37095705934669439343138083508754565189542113879843219016388785533085940283555)

(=0x52036cee 2b6ffe73 8cc74079 7779e898 00700a4d 4141d8ab 75eb4dca 135978a3)

Gx 15112221349535400772501151409588531511454012693041857206046113283949847762202

(=0x216936d3 cd6e53fe c0a4e231 fdd6dc5c 692cc760 9525a7b2 c9562d60 8f25d51a)

Gy 4/5

(=46316835694926478169428394003475163141307993866256225615783033603165251855960)

(=0x66666666 66666666 66666666 66666666 66666666 66666666 66666666 66666658)

Weierstrass curve-specific parameters:

a 19298681539552699237261830834781317975544997444273427339909597334573241639236

(=0x2aaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaa98 4914a144)

b 55751746669818908907645289078257140818241103727901012315294400837956729358436

(=0x7b425ed0 97b425ed 097b425e d097b425 ed097b42 5ed097b4 260b5e9c 7710c864)

Gx’ 19298681539552699237261830834781317975544997444273427339909597334652188435546

(=0x2aaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaad245a)

Gy’ 14781619447589544791020593568409986887264606134616475288964881837755586237401

(=0x20ae19a1 b8a086b4 e01edd2c 7748d14c 923d4d7e 6d7c61b2
29e9c5a2 7eced3d9)

Author’s Address

Rene Struik
Struik Security Consultancy

Email: rstruik.ext@gmail.com