

lwig
Internet-Draft
Intended status: Informational
Expires: April 21, 2019

R. Struik
Struik Security Consultancy
October 18, 2018

Alternative Elliptic Curve Representations
draft-ietf-lwig-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 April 21, 2019.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents

(<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

- [1. Fostering Code Reuse with New Elliptic Curves](#) [3](#)
- [2. Specification of Wei25519](#) [3](#)
- [3. Example Uses](#) [3](#)
 - [3.1. ECDSA-SHA256-25519](#) [4](#)
 - [3.2. Other Uses](#) [4](#)
- [4. Security Considerations](#) [4](#)
- [5. IANA Considerations](#) [5](#)
- [6. Normative References](#) [5](#)
- [Appendix A. Some \(non-Binary\) Elliptic Curves](#) [6](#)
 - [A.1. Curves in short-Weierstrass Form](#) [6](#)
 - [A.2. Montgomery Curves](#) [6](#)
 - [A.3. Twisted Edwards Curves](#) [6](#)
- [Appendix B. Elliptic Curve Group Operations](#) [7](#)
 - [B.1. Group Law for Weierstrass Curves](#) [7](#)
 - [B.2. Group Law for Montgomery Curves](#) [7](#)
 - [B.3. Group Law for Twisted Edwards Curves](#) [8](#)
- [Appendix C. Relationship Between Curve Models](#) [8](#)
 - [C.1. Mapping between twisted Edwards Curves and Montgomery Curves](#) [8](#)
 - [C.2. Mapping between Montgomery Curves and Weierstrass Curves](#) [9](#)
 - [C.3. Mapping between twisted Edwards Curves and Weierstrass Curves](#) [10](#)
- [Appendix D. Curve25519 and Cousins](#) [10](#)
 - [D.1. Curve Definition and Alternative Representations](#) [10](#)
 - [D.2. Switching between Alternative Representations](#) [10](#)
 - [D.3. Domain Parameters](#) [12](#)
- [Appendix E. Further Mappings](#) [14](#)
 - [E.1. Isomorphic Mapping between Weierstrass Curves](#) [14](#)
 - [E.2. Isogeneous Mapping between Weierstrass Curves](#) [15](#)
- [Appendix F. Further Cousins of Curve25519](#) [16](#)
 - [F.1. Further Alternative Representations](#) [16](#)
 - [F.2. Further Switching](#) [16](#)
 - [F.3. Further Domain Parameters](#) [17](#)
- [Appendix G. Isogeny Details](#) [19](#)
 - [G.1. Isogeny Parameters](#) [19](#)
 - [G.1.1. Coefficients of u\(x\):](#) [19](#)
 - [G.1.2. Coefficients of v\(x\):](#) [21](#)
 - [G.1.3. Coefficients of w\(x\):](#) [24](#)

Struik

Expires April 21, 2019

[Page 2]

[G.2. Dual Isogeny Parameters](#) [25](#)
[G.2.1. Coefficients of \$u'\(x\)\$](#) : [25](#)
[G.2.2. Coefficients of \$v'\(x\)\$](#) : [27](#)
[G.2.3. Coefficients of \$w'\(x\)\$](#) : [30](#)
 Author's Address [31](#)

1. Fostering Code Reuse with New Elliptic Curves

It is well-known that elliptic curves can be represented using different curve models. Recently, IETF 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 of Curve25519, a so-called Montgomery curve, and of points of Edwards25519, a so-called twisted Edwards curve, which are both specified in [[RFC7748](#)], as points of a specific so-called "short" Weierstrass curve, called Wei25519. The draft also defines how to efficiently switch between these different representations.

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 [[SP-800-56a](#)], FIPS Pub 186-4 [[FIPS-186-4](#)], and ANSI X9.62-2005 [[ANSI-X9.62](#)] and fostering code reuse on platforms that already implement some of these schemes using elliptic curve arithmetic for curves in "short" Weierstrass form (see [Appendix B.1](#)).

2. Specification of Wei25519

For the specification of Wei25519 and its relationship to Curve25519 and Edwards25519, see [Appendix D](#). For further details and background information on elliptic curves, we refer to the other appendices.

The use of Wei25519 allows reuse of existing generic code that implements short-Weierstrass curves, such as the NIST curve P256, to also implement the CFRG curves Curve25519 and Ed25519. The draft also caters to reuse of existing code where some domain parameters may have been hardcoded, thereby widening the scope of applicability; see [Appendix F](#).

3. Example Uses

3.1. ECDSA-SHA256-25519

[RFC 8032](#) [[RFC8032](#)] specifies the use of EdDSA, a "full" Schnorr signature scheme, with instantiation by Edwards25519 and Ed448, two so-called twisted Edwards curves. These curves can also be used with the widely implemented signature scheme ECDSA [[FIPS-186-4](#)], by instantiating ECDSA with the curve Wei25519 and hash function SHA-256, where "under the hood" an implementation may carry out elliptic curve scalar multiplication routines using the corresponding representations of a point of the curve Wei25519 in Weierstrass form as a point of the Montgomery curve Curve25519 or of the twisted Edwards curve Edwards25519. (The corresponding ECDSA-SHA512-448 scheme arises if one were to specify a curve in short-Weierstrass form corresponding to Ed448 and use the hash function SHA512.) Note that, in either case, one can implement these schemes with the same representation conventions as used with existing NIST specifications, including bit/byte-ordering, compression functions, and the-like. This allows implementations of ECDSA with the hash function SHA-256 and with the NIST curve P-256 or with the curve Wei25519 specified in this draft to use the same implementation (instantiated with, respectively, the NIST P-256 elliptic curve domain parameters or with the domain parameters of curve Wei25519 specified in [Appendix D](#)).

3.2. Other Uses

Any existing specification of cryptographic schemes using elliptic curves in Weierstrass form and that allows introduction of a new elliptic curve (here: Wei25519) is amenable to similar constructs, thus spawning "offspring" protocols, simply by instantiating these using the new curve in "short" Weierstrass form, thereby allowing code and/or specifications reuse and, for implementations that so desire, carrying out curve computations "under the hood" on Montgomery curve and twisted Edwards curve cousins hereof (where these exist). This would simply require definition of a new object identifier for any such envisioned "offspring" protocol. This could significantly simplify standardization of schemes and help keeping the resource and maintenance cost of implementations supporting algorithm agility [[RFC7696](#)] at bay.

4. 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.

5. IANA Considerations

There is *currently* no IANA action required for this document. New object identifiers would be required in case one wishes to specify one or more of the "offspring" protocols exemplified in [Section 3](#).

6. 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.

[GECC]

D. Hankerson, A.J. Menezes, S.A. Vanstone, "Guide to Elliptic Curve Cryptography", New York: Springer-Verlag, 2004.

[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>>.

[RFC5639]

Lochter, M. and J. Merkle, "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation", [RFC 5639](#), DOI 10.17487/RFC5639, March 2010, <<https://www.rfc-editor.org/info/rfc5639>>.

[RFC7696]

Housley, R., "Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms", [BCP 201](#), [RFC 7696](#), DOI 10.17487/RFC7696, November 2015, <<https://www.rfc-editor.org/info/rfc7696>>.

[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 that 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 that 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 $a*x^2 + y^2 = 1 + d*x^2*y^2$, 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 that 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 of the Weierstrass curve $W_{\{a,b\}}$, the point at infinity 0 serves as identity element, i.e., $P + 0 = 0 + P = P$.

For each affine point $P:=(x, y)$ of the Weierstrass curve $W_{\{a,b\}}$, the point $-P$ is the point $(x, -y)$ and one has $P + (-P) = 0$.

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

$$x + x1 + x2 = \lambda^2 \text{ and } y + y1 = \lambda(x1 - x), \text{ where } \lambda = (y2 - y1)/(x2 - x1).$$

Let $P:=(x1, y1)$ be an affine point of the Weierstrass curve $W_{\{a,b\}}$ and let $Q:=2P$, where Q is not the identity element. Then $Q:=(x, y)$, where

$$x + 2x1 = \lambda^2 \text{ and } y + y1 = \lambda(x1 - x), \text{ where } \lambda = (3x1^2 + a)/(2y1).$$

B.2. Group Law for Montgomery Curves

For each point P of the Montgomery curve $M_{\{A,B\}}$, the point at infinity 0 serves as identity element, i.e., $P + 0 = 0 + P = P$.

For each affine point $P:=(x, y)$ of the Montgomery curve $M_{\{A,B\}}$, the point $-P$ is the point $(x, -y)$ and one has $P + (-P) = 0$.

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

$$x + x1 + x2 = B\lambda^2 - A \text{ and } y + y1 = \lambda(x1 - x), \text{ where } \lambda = (y2 - y1)/(x2 - x1).$$

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

$$x + 2x1 = B\lambda^2 - A \text{ and } y + y1 = \lambda(x1 - x), \text{ where } \lambda = (3x1^2 + 2Ax1 + 1)/(2y1).$$

Alternative and more efficient group laws exist, e.g., when using the so-called Montgomery ladder. Details are out of scope.

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 formulae 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 of the twisted Edwards curve $E_{\{a,d\}}$, the point $0=(0,1)$ serves as identity element, i.e., $P + 0 = 0 + P = P$.

For each point $P:=(x, y)$ of the twisted Edwards curve $E_{\{a,d\}}$, the point $-P$ is the point $(-x, y)$ and one has $P + (-P) = 0$.

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

$$x = (x1*y2 + x2*y1)/(1 + d*x1*x2*y1*y2) \text{ and } y = (y1*y2 - a*x1*x2)/(1 - d*x1*x2*y1*y2).$$

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

$$x = (2*x1*y1)/(1 + d*x1^2*y1^2) \text{ and } y = (y1^2 - a*x1^2)/(1 - d*x1^2*y1^2).$$

Note that one can use the formulae for point addition to implement point doubling, taking inverses and adding the identity element as well (i.e., the point addition formulae are uniform and complete (subject to our Note above)).

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 of $M_{\{A,B\}}$ 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) of $M_{\{A,B\}}$ to the point $(x, y) := (u/v, (u-1)/(u+1))$ of $E_{\{a,d\}}$. 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 of $M_{\{A,B\}}$, 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 of the Montgomery curve $M_{\{A,B\}}$ to points of 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 of $M_{\{A,B\}}$ to the point at infinity O of $W_{\{a,b\}}$, while mapping each other point (u, v) of $M_{\{A,B\}}$ to the point $(x, y) := (u/(B+A/(3*B)), v/B)$ 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 h_1*n_1 , where $h_1=4$ and where n_1 is a prime number. For this curve, the base point is the point (G_u, G_v) , where $G_u=9$ and where G_v 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 point (G_x, G_y) , where parameters are as specified in [Appendix D.3](#). This curve is denoted as Edwards25519. 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 point $(G_{x'}, G_{y'})$, where parameters are as specified in [Appendix D.3](#). This curve is denoted as Wei25519.

[D.2.](#) Switching between Alternative Representations

Each affine 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 (G_u, G_v) of Curve25519 corresponds to the base point $(G_{x'}, G_{y'})$ of Wei25519. The inverse mapping maps the affine point (x,y) of Wei25519 to $(u,v):=(x - A/3,y)$ of Curve25519, while mapping the point

at infinity of Wei25519 to the point at infinity of 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 19298681539552699237261830834781317975544997444273427339909597
      334652188435537
```

```
(=0x2aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaad2
451)
```

The curve Edwards25519 is isomorphic to the curve Curve25519, where the base point (G_u, G_v) of Curve25519 corresponds to the base point (G_x, G_y) of Edwards25519 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 Edwards25519 and where each other point (u, v) of Curve25519 corresponds to the point $(c*u/v, (u-1)/(u+1))$ of Edwards25519, where c is the element of $GF(p)$ defined by

c sqrt(-(A+2))

```
51042569399160536130206135233146329284152202253034631822681833788
666877215207
```

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

(Here, we used the mapping of [Appendix C.1.](#)) The inverse mapping from Edwards25519 to Curve25519 is defined by mapping the point $(0, 1)$ and the point $(0, -1)$ of order two of Edwards25519 to, respectively, the point at infinity and the point $(0,0)$ of order two of Curve25519 and having each other point (x, y) of Edwards25519 correspond to the point $((1 + y)/(1 - y), c*(1 + y)/((1-y)*x))$.

The curve Edwards25519 is isomorphic to the Weierstrass curve Wei25519, where the base point (G_x, G_y) of Edwards25519 corresponds to the base point (G_x', G_y') of Wei25519 and where the identity element $(0,1)$ and the point $(0, -1)$ of order two of Edwards25519 correspond to, respectively, the point at infinity 0 and the point $(A/3, 0)$ of order two of Wei25519 and where each other point (x, y) of Edwards25519 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 Edwards25519 is defined by mapping the point at infinity 0 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

Edwards25519 and having each other point (x, y) of Wei25519 correspond to the point $(c*(3*x-A)/(3*y), (3*x-A-3)/(3*x-A+3))$.

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 the Montgomery curve Curve25519 and of the twisted Edwards curve Edwards25519 are as specified in [RFC 7748](#); the domain parameters of Wei25519 are "new".

General parameters (for all curve models):

p $2^{255}-19$

(=0x7ffffffff ffffffff ffffffff ffffffff ffffffff ffffffff
ffffffff ffffffff)

h 8

n 72370055773322622139731865630429942408571163593799076060019509382
85454250989

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

h1 4

n1 14474011154664524427946373126085988481603263447650325797860494125
407373907997

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

Montgomery curve-specific parameters (for Curve25519):

A 486662

B 1

Gu 9 (=0x9)

Gv 14781619447589544791020593568409986887264606134616475288964881837
755586237401

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

Twisted Edwards curve-specific parameters (for Edwards25519):

a -1 (-0x01)

d -121665/121666

(=370957059346694393431380835087545651895421138798432190163887855
33085940283555)

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

Gx 15112221349535400772501151409588531511454012693041857206046113283
949847762202

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

Gy 4/5

(=463168356949264781694283940034751631413079938662562256157830336
03165251855960)

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

Weierstrass curve-specific parameters (for Wei25519):

a 19298681539552699237261830834781317975544997444273427339909597334
573241639236

(=0x2aaaaaaaa aaaaaaaaa aaaaaaaaa aaaaaaaaa aaaaaaaaa aaaaaaaaa
aaaaaaaa98 4914a144)

b 55751746669818908907645289078257140818241103727901012315294400837
956729358436

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

Gx' 19298681539552699237261830834781317975544997444273427339909597334
652188435546

(=0x2aaaaaaaa aaaaaaaaa aaaaaaaaa aaaaaaaaa aaaaaaaaa aaaaaaaaa
aaaaaaaa aaad245a)

Gy' 14781619447589544791020593568409986887264606134616475288964881837
755586237401

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

Appendix E. Further Mappings

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. Within each curve model, further mappings exist that induce a mapping between elliptic curves within each curve model. This can be exploited to force some of the domain parameter to a value that allows a more efficient implementation of the addition formulae.

E.1. Isomorphic Mapping between Weierstrass Curves

One can map points of the Weierstrass curve $W_{\{a,b\}}$ to points of the Weierstrass curve $W_{\{a',b'\}}$, where $a:=a'*s^4$ and $b:=b'*s^6$ for some nonzero value u of the finite field $GF(q)$. This defines a one-to-one correspondence, which - in fact - is an isomorphism between $W_{\{a,b\}}$ and $W_{\{a',b'\}}$, thereby showing that, e.g., the discrete logarithm problem in either curve model is equally hard.

The mapping from $W_{\{a,b\}}$ to $W_{\{a',b'\}}$ is defined by mapping the point at infinity O of $W_{\{a,b\}}$ to the point at infinity O of $W_{\{a',b'\}}$, while mapping each other point (x, y) of $W_{\{a,b\}}$ to the point $(x', y') := (x*s^2, y*s^3)$ of $W_{\{a',b'\}}$. The inverse mapping from $W_{\{a',b'\}}$ to $W_{\{a,b\}}$ is defined by mapping the point at infinity O of $W_{\{a',b'\}}$ to the point at infinity O of $W_{\{a,b\}}$, while mapping each other point (x', y') of $W_{\{a',b'\}}$ to the point $(x, y) := (x/s^2, y/s^3)$ of $W_{\{a,b\}}$.

Implementations may take advantage of this mapping to carry out elliptic curve group operations originally defined for a Weierstrass curve with a generic domain parameter a on a corresponding isomorphic Weierstrass curve with domain parameter a' that has a special form, which is known to allow for more efficient implementations of addition laws, and translating the result back to the original curve. In particular, it is known that such efficiency improvements exist if $a' = -3 \pmod{p}$ and one uses so-called Jacobian coordinates with a particular projective version of the addition laws of [Appendix B.1](#). While not all Weierstrass curves can be put into this form, all traditional NIST curves have domain parameter $a = -3$, while all Brainpool curves [[RFC5639](#)] are isomorphic to a Weierstrass curve of this form. For details, we refer to Section 3.1.5 of [[GECC](#)].

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: this only holds if a'/a is a fourth power in $GF(q)$. However, even in this case, one can still express the curve $W_{\{a,b\}}$ in terms of a Weierstrass curve with a small a' domain parameter, thereby still allowing a more efficient implementation than with a general a value.

E.2. Isogeneous Mapping between Weierstrass Curves

One can still map points of the Weierstrass curve $W_{\{a,b\}}$ to points of the Weierstrass curve $W_{\{a',b'\}}$, where $a' = -3 \pmod{p}$, even if a'/a is not a fourth power in $GF(q)$. In that case, this mapping cannot be an isomorphism (see [Appendix E.1](#)) and, thereby, does not define a one-to-one correspondence. Instead, the mapping is a so-called isogeny (or homomorphism). Since most elliptic curve operations process points of prime order or use so-called "co-factor multiplication", in practice the resulting mapping has similar properties. In particular, one can still take advantage of this mapping to carry out elliptic curve group operations originally defined for a Weierstrass curve with domain parameter a unequal to $-3 \pmod{p}$ on a corresponding isogenous Weierstrass curve with domain parameter $a' = -3 \pmod{p}$ and translating the result back to the original curve.

In this case, the mapping from $W_{\{a,b\}}$ to $W_{\{a',b'\}}$ is defined by mapping the point at infinity O of $W_{\{a,b\}}$ to the point at infinity O of $W_{\{a',b'\}}$, while mapping each other point (x, y) of $W_{\{a,b\}}$ to the point $(x', y') := (u(x)/w(x)^2, y*v(x)/w(x)^3)$ of $W_{\{a',b'\}}$. Here, $u(x)$, $v(x)$, and $w(x)$ are polynomials that depend on the isogeny in question. The inverse mapping from $W_{\{a',b'\}}$ to $W_{\{a,b\}}$ is again an isogeny and defined by mapping the point at infinity O of $W_{\{a',b'\}}$ to the point at infinity O of $W_{\{a,b\}}$, while mapping each other point (x', y') of $W_{\{a',b'\}}$ to the point $(x, y) := (u'(x')/w'(x')^2, y'*v'(x')/w'(x')^3)$ of $W_{\{a,b\}}$, where -- again -- $u'(x')$, $v'(x')$, and $w'(x')$ are polynomials that depend on the isogeny in question. These mappings have the property that their composition is not the identity mapping (as is the case with the isomorphic mappings discussed in [Appendix E.1](#)), but rather a fixed multiple hereof: if this multiple is l then the isogeny is called an isogeny of degree l (or l -isogeny) and u , v , and w (and, similarly, u' , v' , and w') are polynomials of degrees l , $3(l-1)/2$, and $(l-1)/2$, respectively. Note that an isomorphism is simply an isogeny of degree $l=1$. Details of how to compute this mapping are outside scope of this document (for this, contact the author of this document).

Implementations may take advantage of this mapping to carry out elliptic curve group operations originally defined for a Weierstrass curve with a generic domain parameter a on a corresponding isogeneous Weierstrass curve with domain parameter $a' = -3 \pmod{p}$, where one can use so-called Jacobian coordinates with a particular projective version of the addition laws of [Appendix B.1](#). Since all traditional NIST curves have domain parameter $a = -3$, while all Brainpool curves [[RFC5639](#)] are isomorphic to a Weierstrass curve of this form, this allows taking advantage of existing generic implementations for these curves, provided one switches back and forth to this curve form using the isogeneous mapping in question.

Note that isogeneous mappings can be easily realized in projective coordinates and involves roughly 3×1 finite field multiplications, thus allowing switching between alternative representations at relative low incremental cost compared to that of elliptic curve scalar multiplications (provided the isogeny has low degree l). Note, however, that this does require storage of the polynomial coefficients of the isogeny and dual isogeny involved. This illustrates that low-degree isogenies are to be preferred, since an l -isogeny (usually) requires storing roughly $6 \times l$ elements of $\text{GF}(q)$. While there are many isogenies, we therefore only consider those with the desired property with lowest possible degree.

[Appendix F](#). Further Cousins of Curve25519

[F.1](#). Further Alternative Representations

The Weierstrass curve Wei25519 is isomorphic to the Weierstrass curve Wei25519.2 defined over $\text{GF}(p)$, with as base point the pair $(G1x, G1y)$, and isogeneous to the Weierstrass curve Wei25519.-3 defined over $\text{GF}(p)$, with as base point the pair $(G2x, G2y)$, where parameters are as specified in [Appendix F.3](#) and where the related mappings are as specified in [Appendix F.2](#).

[F.2](#). Further Switching

Each affine point (x, y) of Wei25519 corresponds to the point $(x', y') := (x \cdot s^2, y \cdot s^3)$ of Wei25519.2, where s is the element of $\text{GF}(p)$ defined by

```
s  20343593038935618591794247374137143598394058341193943326473831977
    39407761440
```

```
(=0x047f6814 6d568b44 7e4552ea a5ed633d 02d62964 a2b0a120
5e7941e9 375de020),
```


while the point at infinity of Wei25519 corresponds to the point at infinity of Wei25519.2. (Here, we used the mapping of [Appendix E.1.](#)) Under this mapping, the base point (Gx', Gy') of Wei25519 corresponds to the base point $(G1x', G1y')$ of Wei25519.2. The inverse mapping maps the affine point (x', y') of Wei25519.2 to $(x, y) := (x'/s^2, y'/s^3)$ of Wei25519, while mapping the point at infinity of Wei25519.2 to the point at infinity of Wei25519. Note that this mapping (and its inverse) involves a modular multiplication of both coordinates with fixed constants s^2 and s^3 (respectively, $1/s^2$ and $1/s^3$), which can be precomputed.

Each affine point (x, y) of Wei25519 corresponds to the point $(x', y') := (x1/t^2, y1/t^3)$ of Wei25519.-3, where $(x1, y1) = (u(x)/w(x)^2, y*v(x)/w(x)^3)$, where u , v , and w are the polynomials with coefficients in $GF(p)$ as defined in [Appendix G](#) and where t is the element of $GF(p)$ defined by

```
t  26012855558634277483276064234565597076862996895623795164528458073
   435568115620
```

```
(=0x3982c126 59ad1749 ab8bc495 bb1a9d64 c9deffc5 e7b8e601
  a5651992 07d48fa4),
```

while the point at infinity of Wei25519 corresponds to the point at infinity of Wei25519.-3. (Here, we used the isogeneous mapping of [Appendix E.2.](#)) Under this isogeneous mapping, the base point (Gx', Gy') of Wei25519 corresponds to the base point $(G2x', G2y')$ of Wei25519.-3. The dual isogeny maps the affine point (x', y') of Wei25519.-3 to $(x, y) := (u'(x1)/w'(x1)^2, y1*v'(x1)/w'(x1)^3)$ of Wei25519, where $(x1, y1) = (x'*t^2, y'*t^3)$ and where u' , v' , and w' are the polynomials with coefficients in $GF(p)$ as defined in [Appendix G](#), while mapping the point at infinity of Wei25519.-3 to the point at infinity of Wei25519. Under this dual isogeneous mapping, the base point $(G2x', G2y')$ of Wei25519.-3 corresponds to a multiple of the base point (Gx', Gy') of Wei25519, where this multiple is $l=47$ (the degree of the isogeny; see the description in [Appendix E.1](#)). Note that this isogenous map (and its dual) primarily involves the evaluation of three fixed polynomials involving the x -coordinate, which takes roughly 140 modular multiplications (or less than 5% relative incremental cost compared to the cost of an elliptic curve scalar multiplication).

[F.3.](#) Further Domain Parameters

The parameters of the Weierstrass curve with $a=2$ that is isomorphic with Wei25519 and the parameters of the Weierstrass curve with $a=-3$ that is isogeneous with Wei25519 are as indicated below. Both domain

parameter sets can be exploited directly to derive more efficient point addition formulae, should an implementation facilitate this.

Weierstrass curve-specific parameters (for Wei25519.2, i.e., with a=2):

a 2 (=0x02)

b 12102640281269758552371076649779977768474709596484288167752775713
178787220689

(=0x1ac1da05 b55bc146 33bd39e4 7f94302e f19843dc f669916f
6a5dfd01 65538cd1)

G1x' 107705531383684005184170201967961611367923681983263378231495026
81097436401658

(=0x17cfeac3 78aed661 318e8634 582275b6 d9ad4def 072ea193
5ee3c4e8 7a940ffa)

G1y' 544305758615084056530986689844575286168071033325025775211614397
7388639873869

(=0x0c08a952 c55dfad6 2c4f13f1 a8f68dca dc5c331d 297a37b6
f0d7fdcc 51e16b4d)

Weierstrass curve-specific parameters (for Wei25519.-3, i.e., with a=-3):

a -3

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

b 29689592517550930188872794512874050362622433571298029721775200646
451501277098

(=0x41a3b6bf c668778e be2954a4 b1df36d1 485ecef1 ea614295
796e1022 40891faa)

G2x' 538371792299408724349427232574807773704511272123391981336972078
46219400243292

(=0x7706c37b 5a84128a 3884a5d7 1811f1b5 5da3230f fb17a8ab
0b32e48d 31a6685c)

G2y' 695480730911001844144020555292799703925148674228551417730708041
8460388229929

(=0x0f60480c 7a5c0e11 40340adc 79d6a2bf 0cb57ad0 49d025dc
38d80c77 985f0329)

Appendix G. Isogeny Details

The isogeny and dual isogeny are both isogenies with degree $l=47$. Both are specified by a triple of polynomials u , v , and w (resp. u' , v' , and w') of degree 47, 69, and 23, respectively, with coefficients in $GF(p)$. The coefficients of each of these polynomials are specified in [Appendix G.1](#) (for the isogeny) and in [Appendix G.2](#) (for the dual isogeny). For each polynomial in variable x , the coefficients are tabulated as sequence of coefficients of x^0 , x^1 , x^2 , ..., in hexadecimal format.

G.1. Isogeny Parameters

G.1.1. Coefficients of $u(x)$:

0 0x670ed14828b6f1791ceb3a9cc0edfe127dee8729c5a72ddf77bb1abaebbbba1e8
1 0x1135ca8bd5383cb3545402c8bce2ced14b45c29b241e4751b035f27524a9f932
2 0x3223806ff5f669c430efd74df8389f058d180e2fcffa5cdef3eacecdd2c34771
3 0x31b8fecf3f17a819c228517f6cd9814466c8c8bea2efccc47a29bfc14c364266
4 0x2541305c958c5a326f44efad2bec284e7abee840fadb08f2d994cd382fd8ce42
5 0x6e6f9c5792f3ff497f860f44a9c469cec42bd711526b733e10915be5b2dbd8c6
6 0x3e9ad2e5f594b9ce6b06d4565891d28a1be8790000b396ef0bf59215d6cabfde
7 0x278448895d236403bbc161347d19c913e7df5f372732a823ed807ee1d30206be
8 0x42f9d171ea8dc2f4a14ea46cc0ee54967175ecfe83a975137b753cb127c35060
9 0x128e40efa2d3ccb51567e73bae91e7c31eac45700fa13ce5781cbe5ddc985648
10 0x450e5086c065430b496d88952dd2d5f2c5102bc27074d4d1e98bfa47413e0645
11 0x487ef93da70dfd44a4db8cb41542e33d1aa32237bdca3a59b3ce1c59585f253d
12 0x33d209270026b1d2db96efb36cc2fa0a49be1307f49689022eab1892b010b785
13 0x4732b5996a20ebc4d5c5e2375d3b6c4b700c681bd9904343a14a0555ef0ecd48
14 0x64dc9e8272b9f5c6ad3470db543238386f42b18cb1c592cc6caf7893141b2107

15 0x52bbacd1f85c61ef7eafd8da27260fa2821f7a961867ed449b283036508ac5c5
16 0x320447ed91210985e2c401cfe1a93db1379424cf748f92fd61ab5cc356bc89a2
17 0x23d23a49bbcdf8cf4c4ce8a4ff7dd87d1ad1970317686254d5b4d2ec050d019f
18 0x1601fca063f0bbbf15f198b3c20e474c2170294fa981f73365732d2372b40cd4
19 0x7bf3f93840035e9688cfff402cee204a17c0de9779fc33503537dd78021bf4c4
20 0x311998ce59fb7e1cd6af591ece3e84dfcb1c330cbcf28c0349e37b9581452853
21 0x7ae5e41acfd28a9add2216dfed34756575a19b16984c1f3847b694326dad7f99
22 0x704957e279244a5b107a6c57bd0ab9afe5227b7c0be2052cd3513772a40efee7
23 0x56b918b5a0c583cb763550f8f71481e57c13bdcef2e5cfc8091d0821266f233b
24 0x677073fed43ab291e496f798fbcf217bac3f014e35d0c2fa07f041ae746a04d7
25 0x22225388e76f9688c7d4053b50ba41d0d8b71a2f21da8353d98472243ef50170
26 0x66930b3dfdd3995a2502cef790d78b091c875192d8074bb5d5639f736400555
27 0x79eb677c5e36971e8d64d56ebc0dedb4e9b7dd2d7b01343ebbd4d358d376e490
28 0x48a204c2ca6d8636e9994842605bd648b91b637844e38d6c7dd707edce8256e2
29 0xfb3529b0d4b9ce2d70760f33e8ce997a58999718e9277caf48623d27ae6a788
30 0x4352604bffd0c7d7a9ed898a2c6e7cf2512ffb89407271ba1f2c2d0ead8cc5aa
31 0x6667697b29785fb6f0bd5e04d828991a5fe525370216f347ec767a26e7aac936
32 0x9fc950b083c56dbd989badf9887255e203c879f123a7cb28901e50aea6d64dc
33 0x41e51b51b5caadd1c15436bbf37596a1d7288a5f495d6b5b1ae66f8b2942b31d
34 0x73b59fec709aa1cabd429e981c6284822a8b7b07620c831ab41fd31d5cf7430
35 0x67e9b88e9a1bfbcb2554107d67d814986f1b09c3107a060cba21c019a2d5dc848
36 0x6881494a1066ca176c5e174713786040affb4268b19d2abf28ef4293429f89c1
37 0x5f4d30502ff1e1ccd624e6f506569454ab771869d7483e26afc09dea0c5ccd3d
38 0x2a814cfc5859bca51e539c159955cbe729a58978b52329575d09bc6c3bf97ad

39 0x1313c8aaae20d6f4397f0d8b19e52cfcdf8d8e10fba144aec1778fd10ddf4e9c
40 0x7008d38f434b98953a996d4cc79fcbe9502411dcdf92005f725cea7ce82ad47
41 0x5a74d1296aaaa245ffb848f434531fa3ba9e5cb9098a7091d36c2777d4cf5a13
42 0x4bd3b700606397083f8038177bdaa1ac6edbba0447537582723cae0fd29341a9
43 0x573453fb2b093016f3368356c786519d54ed05f5372c01723b4da520597ec217
44 0x77f5c605bdb3a30d7d9c8840fce38650910d4418eed707a212c8927f41c2c812
45 0x16d6b9f7ff57ca32350057de1204cc6d69d4ef1b255dfef8080118e2fef6ace3
46 0x34e8595832a4021f8b5744014c6b4f7da7df0d0329e8b6b4d44c8fadad6513b7
47 0x1

G.1.2. Coefficients of $v(x)$:

0 0xf9f5eb7134e6f8dafa30c45afa58d7bfc6d4e3ccbb5de87b562fd77403972b2
1 0x36c2dcd9e88f0d2d517a15fc453a098bbbb5a05eb6e8da906fae418a4e1a13f7
2 0xb40078302c24fa394a834880d5bf46732ca1b4894172fb7f775821276f558b3
3 0x53dd8e2234573f7f3f7df11e90a7bdd7b75d807f9712f521d4fb18af59aa5f26
4 0x6d4d7bb08de9061988a8cf6ff3beb10e933d4d2fbb8872d256a38c74c8c2ceda
5 0x71bfe5831b30e28cd0fbe1e9916ab2291c6beacc5af08e2c9165c632e61dd2f5
6 0x7c524f4d17ff2ee88463da012fc12a5b67d7fb5bd0ab59f4bbf162d76be1c89c
7 0x758183d5e07878d3364e3fd4c863a5dc1fe723f48c4ab4273fc034f5454d59a4
8 0x1eb41ef2479444ecdccbc200f64bde53f434a02b6c3f485d32f14da6aa7700e1
9 0x1490f3851f016cc3cf8a1e3c16a53317253d232ed425297531b560d70770315c
10 0x9bc43131964e46d905c3489c9d465c3abbd26eab9371c10e429b36d4b86469c
11 0x5f27c173d94c7a413a288348d3fc88daa0bcf5af8f436a47262050f240e9be3b
12 0x1d20010ec741aaa393cd19f0133b35f067adab0d105babe75fe45c8ba2732ceb
13 0x1b3c669ae49b86be2f0c946a9ff6c48e44740d7d9804146915747c3c025996a

14 0x24c6090f79ec13e3ae454d8f0f98e0c30a8938180595f79602f2ba013b3c10db
15 0x4650c5b5648c6c43ac75a2042048c699e44437929268661726e7182a31b1532f
16 0x957a835fb8bac3360b5008790e4c1f3389589ba74c8e8bf648b856ba7f22ba5
17 0x1cd1300bc534880f95c7885d8df04a82bd54ed3e904b0749e0e3f8cb3240c7c7
18 0x760b486e0d3c6ee0833b34b64b7ebc846055d4d1e0beeb6aedd5132399ada0ea
19 0x1c666846c63965ef7edf519d6ada738f2b676ae38ff1f4621533373931b3220e
20 0x365055118b38d4bc0df86648044affea2ef33e9a392ad336444e7d15e45585d1
21 0x736487bde4b555abfccd3ea7ddcda98eda0d7c879664117dee906a88bc551194
22 0x70de05ab9520222a37c7a84c61eedff71cb50c5f6647fc2a5d6e0ff2305cea37
23 0x59053f6cdf6517ab3fe4bd9c9271d1892f8cf353d8041b98409e1e341a01f8b5
24 0x375db54ed12fe8df9a198ea40200e812c2660b7022681d7932d89fafefc6e88d
25 0x2a070c31d1c1a064daf56c79a044bd1cd6d13f1ddb0ff039b03a6469aaa9ed77
26 0x41482351e7f69a756a5a2c0b3fa0681c03c550341d0ca0f76c5b394db9d2de8d
27 0x747ac1109c9e9368d94a302cb5a1d23fcc7f0fd8a574efb7ddcaa738297c407a
28 0x45682f1f2aab6358247e364834e2181ad0448bb815c587675fb2fee5a2119064
29 0x148c5bf44870dfd307317f0a0e4a8c163940bee1d2f01455a2e658aa92c13620
30 0x6add1361e56ffa2d2fbbddba284b35be5845aec8069fc28af009d53290a705ce
31 0x6631614c617400dc00f2c55357f67a94268e7b5369b02e55d5db46c935be3af5
32 0x17cffb496c64bb89d91c8c082f4c288c3c87feabd6b08591fe5a92216c094637
33 0x648ff88155969f54c955a1834ad227b93062bb191170dd8c4d759f79ad5da250
34 0x73e50900b89e5f295052b97f9d0c9edb0fc7d97b7fa5e3cfeefe33dd6a9cb223
35 0x6afcb2f2ffe6c08508477aa4956cbd3dc864257f5059685adf2c68d4f2338f00
36 0x372fd49701954c1b8f00926a8cb4b157d4165b75d53fa0476716554bf101b74c
37 0x334ed41325f3724ff8becbf2b3443fea6d30fa543d1ca13188aceb2bdaf5f4e

38 0x70e629c95a94e8e1b3974acb25e18ba42f8d5991786f0931f650c283adfe82fd
39 0x738a625f4c62d3d645f1274e09ab344e72d441f3c0e82989d3e21e19212f23f3
40 0x7093737294b29f21522f5664a9941c9b476f75d443b647bd2c777040bcd12a6a
41 0xa996bad5863d821ccb8b89fa329ddbe5317a46bcb32552db396bea933765436
42 0x2da237e3741b75dd0264836e7ef634fc0bc36ab187ebc790591a77c257b06f53
43 0x1902f3daa86fa4f430b57212924fdc9e40f09e809f3991a0b3a10ab186c50ee5
44 0x12baffec1bf20c921afd3cdf67a7f1d87c00d5326a3e5c83841593c214dadcb1
45 0x6460f5a68123cb9e7bc1289cd5023c0c9ccd2d98eea24484fb3825b59dcd09aa
46 0x2c7d63a868ffc9f0fd034f821d84736c5bc33325ce98aba5f0d95fef6f230ec8
47 0x756e0063349a702db7406984c285a9b6bfba48177950d4361d8efa77408dc860
48 0x37f3e30032b21e0279738e0a2b689625447831a2ccf15c638672da9aa7255ae
49 0x1107c0dbe15d6ca9e790768317a40bcf23c80f1841f03ca79dd3e3ef4ea1ae30
50 0x61ff7f25721d6206041c59a788316b09e05135a2aad94d539c65daa68b302cc2
51 0x5dbfe346cbd0d61b9a3b5c42ec0518d3ae81cabcc32245060d7b0cd982b8d071
52 0x4b6595e8501e9ec3e75f46107d2fd76511764efca179f69196eb45c0aa6fade3
53 0x72d17a5aa7bd8a2540aa9b02d9605f2a714f44abfb4c35d518b7abc39b477870
54 0x658d8c134bac37729ec40d27d50b637201abbf1ab4157316358953548c49cf22
55 0x36ac53b9118581ace574d5a08f9647e6a916f92dda684a4dbc405e2646b0243f
56 0x1917a98f387d1e323e84a0f02d53307b1dd949e1a27b0de14514f89d9c0ef4b6
57 0x21573434fde7ce56e8777c79539479441942dba535ade8ecb77763f7eb05d797
58 0xe0bf482dc40884719bea5503422b603f3a8edb582f52838caa6eaab6eeac7ef
59 0x3b0471eb53bd83e14fbc13928fe1691820349a963be8f7e9815848a53d03f5eb
60 0x1e92cb067b24a729c42d3abb7a1179c577970f0ab3e6b0ce8d66c5b8f7001262
61 0x74ea885c1ebed6f74964262402432ef184c42884fceb2f8dba3a9d67a1344dd7

62 0x433ebce2ce9b0dc314425cfc2b234614d3c34f2c9da9fff4fdddd1ce242d035b
63 0x33ac69e6be858dde7b83a9ff6f11de443128b39cec6e410e8d3b570e405ff896
64 0xdab71e2ae94e6530a501ed8cf3df26731dd1d41cd81578341e12dca3cb71aa3
65 0x537f58d52d18ce5b1d5a6bd3a420e796e64173491ad43dd4d1083a7dcc7dd201
66 0x49c2f6afa93fdcc4e0f8128a8b06da4c75049be14edf3e103821ab604c60f8ae
67 0x10a333eabd6135aeaa3f5f5f7e73d102e4fd7e4bf0902fc55b00da235fa1ad08
68 0xf5c86044bf6032f5102e601f2a0f73c7bce9384bedd120f3e72d78484179d9c
69 0x1

G.1.3. Coefficients of $w(x)$:

0 0x3da24d42421264f30939ff00203880f2b017eb3fecf8933ae61e18df8c8ba116
1 0x457f20bc393cdc9a66848ce174e2fa41d77e6dbae05a317a1fb6e3ae78760f8
2 0x7f608a2285c480d5c9592c435431fae94695beef79d770bb6d029c1d10a53295
3 0x3832accc520a485100a0a1695792465142a5572bed1b2e50e1f8f662ac7289bb
4 0x2df1b0559e31b328eb34beedd5e537c3f4d7b9befb0749f75d6d0d866d26fbaa
5 0x25396820381d04015a9f655ddd41c74303ded05d54a7750e2f58006659adda28
6 0x6fa070a70ca2bc6d4d0795fb28d4990b2cc80cd72d48b603a8ac8c8268bef6a6
7 0x27f488578357388b20fbc7503328e1d10de602b082b3c7b8ceb33c29fea7a0d2
8 0x15776851a7cabcf84c632118306915c0c15c75068a47021968c7438d46076e6
9 0x101565b08a9af015c172fb194b940a4df25c4fb1d85f72d153efc79131d45e8f
10 0x196b0ffbf92f3229fea1dac0d74591b905ccaab6b83f905ee813ee8449f8a62c
11 0x1f55784691719f765f04ee9051ec95d5deb42ae45405a9d87833855a6d95a94
12 0x628858f79cca86305739d084d365d5a9e56e51a4485d253ae3f2e4a379fa8aff
13 0x4a842dcd943a80d1e6e1dab3622a8c4d390da1592d1e56d1c14c4d3f72dd01a5
14 0xf3bfc9cb17a1125f94766a4097d0f1018963bc11cb7bc0c7a1d94d65e282477

15 0x1c4bd70488c4882846500691fa7543b7ef694446d9c3e3b4707ea2c99383e53c
16 0x2d7017e47b24b89b0528932c4ade43f09091b91db0072e6ebdc5e777cb215e35
17 0x781d69243b6c86f59416f91f7decaca93eab9cdc36a184191810c56ed85e0fdc
18 0x5f20526f4177357da40a18da054731d442ad2a5a4727322ba8ed10d32eca24fb
19 0x33e4cab64ed8a00d8012104fe8f928e6173c428eff95bbbe569ea46126a4f3cd
20 0x50555b6f07e308d33776922b6566829d122e19b25b7bbacbb0a4b1a7dc40192
21 0x533fa4bf1e2a2aae2f979065fdbb5b667ede2f85543fddbba146aa3a4ef2d281
22 0x5a742cac1952010fc5aba200a635a7bed3ef868194f45b5a6a2647d6d6b289d2
23 0x1

G.2. Dual Isogeny Parameters

G.2.1. Coefficients of $u'(x)$:

0 0xf0eddb584a20aaac8f1419efdd02a5cca77b21e4cfae78c49b5127d98bc5882
1 0x7115e60d44a58630417df33dd45b8a546fa00b79fea3b2bdc449694bade87c0a
2 0xb3f3a6f3c445c7dc1f91121275414e88c32ff3f367ba0edad4d75b7e7b94b65
3 0x1eb31bb333d7048b87f2b3d4ec76d69035927b41c30274368649c87c52e1ab30
4 0x552c886c2044153e280832264066cce2a7da1127dc9720e2a380e9d37049ac64
5 0x4504f27908db2e1f5840b74ae42445298755d9493141f5417c02f04d47797dda
6 0x82c242cce1eb19698a4fa30b5affe64e5051c04ae8b52cb68d89ee85222e628
7 0x480473406add76cf1d77661b3ff506c038d9cdd5ad6e1ea41969430bb876d223
8 0x25f47bb506fba80c79d1763365fa9076d4c4cb6644f73ed37918074397e88588
9 0x10f13ed36eab593fa20817f6bb70cac292e18d300498f6642e35cbdf772f0855
10 0x7d28329d695fb3305620f83a58df1531e89a43c7b3151d16f3b60a8246c36ade
11 0x2c5ec8c42b16dc6409bdd2c7b4ffe9d65d7209e886badbd5f865dec35e4ab4a
12 0x7f4f33cd50255537e6cde15a4a327a5790c37e081802654b56c956434354e133

13 0x7d30431a121d9240c761998cf83d228237e80c3ef5c7191ec9617208e0ab8cec
14 0x4d2a7d6609610c1deed56425a4615b92f70a507e1079b2681d96a2b874cf0630
15 0x74676df60a9906901d1dc316c639ff6ae0fcdb02b5571d4b83fc2eedcd2936a8
16 0x22f8212219aca01410f06eb234ed53bd5b8fbe7c08652b8002bcd1ea3cdae387
17 0x7edb04449565d7c566b934a87fadade5515f23bda1ce25daa19fff0c6a5ccc2f
18 0x106ef71aa3aa34e8ecf4c07a67d03f0949d7d015ef2c1e32eb698dd3bec5a18c
19 0x17913eb705db126ac3172447bcd811a62744d505ad0eea94cfcfdde5ca7428
20 0x2cc793e6d3b592dcf5472057a991ff1a5ab43b4680bb34c0f5fafc5307827c1
21 0x6dafcc0b16f98300cddb5e0a7d7ff04a0e73ca558c54461781d5a5ccb1ea0122
22 0x7e418891cf222c021b0ae5f5232b9c0dc8270d4925a13174a0f0ac5e7a4c8045
23 0x76553bd26fecb019ead31142684789fea7754c2dc9ab9197c623f45d60749058
24 0x693efb3f81086043656d81840902b6f3a9a4b0e8f2a5a5edf5ce1c7f50a3898e
25 0x46c630eac2b86d36f18a061882b756917718a359f44752a5caf41be506788921
26 0x1dcfa01773628753bc6f448ac11be8a3bffa0011b9284967629b827e064f614
27 0x8430b5b97d49b0938d1f66ecb9d2043025c6eec624f8f02042b9621b2b5cb19
28 0x66f66a6669272d47d3ec1efea36ee01d4a54ed50e9ec84475f668a5a9850f9be
29 0x539128823b5ef3e87e901ab22f06d518a9bad15f5d375b49fe1e893ab38b1345
30 0x2bd01c49d6fff22c213a8688924c10bf29269388a69a08d7f326695b3c213931
31 0x3f7bea1baeccea3980201dc40d67c26db0e3b15b5a19b6cdac6de477aa717ac1
32 0x6e0a72d94867807f7150fcb1233062f911b46e2ad11a3eac3c6c4c91e0f4a3fa
33 0x5963f3cc262253f56fc103e50217e7e5b823ae8e1617f9e11f4c9c595fbb5bf6
34 0x41440b6fe787777bc7b63afac9f4a38ddadcebc3d72f8fc73835247ba05f3a1d
35 0x66d185401c1d2d0b84fcf6758a6a985bf9695651271c08f4b69ce89175fb7b34
36 0x2673fb8c65bc4fe41905381093429a2601c46a309c03077ca229bac7d6ccf239

37 0x1ce4d895ee601918a080de353633c82b75a3f61e8247763767d146554dd2f862
38 0x18efa6c72fa908347547a89028a44f79f22542baa588601f2b3ed25a5e56d27c
39 0x53de362e2f8ff220f8921620a71e8faa1aa57f8886fcbb6808fa3a5560570543
40 0xdc29a73b97f08aa8774911474e651130ed364e8d8cffd4a80dee633aacecc47
41 0x4e7eb8584ae4de525389d1e9300fc4480b3d9c8a5a45ecfbe33311029d8f6b99
42 0x6c3cba4aa9229550fa82e1cfaee4b02f2c0cb86f79e0d412b8e32b00b7959d80
43 0x5a9d104ae585b94af68eeb16b1349776b601f97b7ce716701645b1a75b68dcf3
44 0x754e014b5e87af035b3d5fe6fb49f4631e32549f6341c6693c5172a6388e273e
45 0x6710d8265118e22eaceba09566c86f642ab42da58c435083a353eaa12d866c39
46 0x6e88ac659ce146c369f8b24c3a49f8dca547827250cf7963a455851cfc4f8d22
47 0x971eb5f253356cd1fde9fb21f4a4902aa5b8d804a2b57ba775dc130181ae2e8

G.2.2. Coefficients of $v'(x)$:

0 0x43c9b67cc5b16e167b55f190db61e44d48d813a7112910f10e3fd8da85d61d3
1 0x72046db07e0e7882ff3f0f38b54b45ca84153be47a7fd1dd8f6402e17c47966f
2 0x1593d97b65a070b6b3f879fe3dc4d1ef03c0e781c997111d5c1748f956f1ffc0
3 0x54e5fec076b8779338432bdc5a449e36823a0a7c905fd37f232330b026a143a0
4 0x46328dd9bc336e0873abd453db472468393333fbf2010c6ac283933216e98038
5 0x25d0c64de1dfe1c6d5f5f2d98ab637d8b39bcf0d886a23dabac18c80d7eb03ce
6 0x3a175c46b2cd8e2b313dde2d5f3097b78114a6295f283cf58a33844b0c8d8b34
7 0x5cf4e6f745bdd61181a7d1b4db31dc4c30c84957f63cdf163bee5e466a7a8d38
8 0x639071c39b723eea51cfd870478331d60396b31f39a593ebdd9b1eb543875283
9 0x7ea8f895dcd85fc6cb2b58793789bd9246e62fa7a8c7116936876f4d8dff869b
10 0x503818acb535bcaacf8ad44a83c213a9ce83af7c937dc9b3e5b6efedc0a7428c
11 0xe815373920ec3cbf3f8cae20d4389d367dc4398e01691244af90edc3e6d42b8

12 0x7e4b23e1e0b739087f77910cc635a92a3dc184a791400cbceae056c19c853815
13 0x145322201db4b5ec0a643229e07c0ab7c36e4274745689be2c19cfa8a702129d
14 0xfde79514935d9b40f52e33429621a200acc092f6e5dec14b49e73f2f59c780d
15 0x37517ac5c04dc48145a9d6e14803b8ce9cb6a5d01c6f0ad1b04ff3353d02d815
16 0x58ae96b8eefe9e80f24d3b886932fe3c27aeea810fa189c702f93987c8c97854
17 0x6f6402c90fa379096d5f436035bec9d29302126e9b117887abfa7d4b3c5709a
18 0x1dbdf2b9ec09a8defeb485cc16ea98d0d45c5b9877ff16bd04c0110d2f64961
19 0x53c51706af523ab5b32291de6c6b1ee7c5cbd0a5b317218f917b12ff38421452
20 0x1b1051c7aec7d37a349208e3950b679d14e39f979db4fcd7b50d7d27dc918650
21 0x1547e8d36262d5434cfb029cdd29385353124c3c35b1423c6cca1f87910b305b
22 0x198efe984efc817835e28f704d41e4583a1e2398f7ce14045c4575d0445c6ce7
23 0x492276dfe9588ee5cd9f553d990f377935d721822ecd0333ce2eb1d4324d539c
24 0x77bad5319bacd5ed99e1905ce2ae89294efa7ee1f74314e4095c618a4e580c9b
25 0x2cb3d532b8eac41c61b683f7b02feb9c2761f8b4286a54c3c4b60dd8081a312e
26 0x37d189ea60443e2fee9b7ba8a34ed79ff3883dcefc06592836d2a9dd2ee3656e
27 0x79a80f9a0e6b8ded17a3d6ccf71eb565e3704c3543b77d70bca854345e880aba
28 0x47718530ef8e8c75f069acb2d9925c5537908e220b28c8a2859b856f46d5f8db
29 0x7dc518f82b55a36b4fa084b05bf21e3efce481d278a9f5c6a49701e56dac01ec
30 0x340a318dad4b8d348a0838659672792a0f00b7105881e6080a340f708a9c7f94
31 0x55f04d9d8891636d4e9c808a1fa95ad0dae7a8492257b20448023aad3203278e
32 0x39dc465d58259f9f70bb430d27e2f0ab384a550e1259655443e14bdecba85530
33 0x757385464cff265379a1adfadfd6f6a03fa8a2278761d4889ab097eff4d1ac28
34 0x4d575654dbe39778857f4e688cc657416ce524d54864ebe8995ba766efa7ca2b
35 0x47adb6aecc1949f2dc9f01206cc23eb4a0c29585d475dd24dc463c5087809298

36 0x30d39e8b0c451a8fcf3d2abab4b86ffa374265abbe77c5903db4c1be8cec7672
37 0x28cf47b39112297f0daeaa621f8e777875adc26f35dec0ba475c2ee148562b41
38 0x36199723cc59867e2e309fe9941cd33722c807bb2d0a06eeb41de93f1b93f2f5
39 0x5cdeb1f2ee1c7d694bdd884cb1c5c22de206684e1cafb8d3adb9a33cb85e19a2
40 0xf6e6b3fc54c2d25871011b1499bb0ef015c6d0da802ae7eccf1d8c3fb73856c
41 0xc1422c98b672414344a9c05492b926f473f05033b9f85b8788b4bb9a080053c
42 0x19a8527de35d4faacb00184e0423962247319703a815eecf355f143c2c18f17f
43 0x7812dc3313e6cf093da4617f06062e8e8969d648dfe6b5c331bccd58eb428383
44 0x61e537180c84c79e1fd2d4f9d386e1c4f0442247605b8d8904d122ee7ef9f7be
45 0x544d8621d05540576cfc9b58a3dab19145332b88eb0b86f4c15567c37205adf9
46 0x11be3ef96e6e07556356b51e2479436d9966b7b083892b390caec22a117aa48e
47 0x205cda31289cf75ab0759c14c43cb30f7287969ea3dc0d5286a3853a4d403187
48 0x48d8fc6934f4f0a99f0f2cc59010389e2a0b20d6909bfcf8d7d0249f360acdc
49 0x42cecc6d9bdca6d382e97fcea46a79c3eda2853091a8f399a2252115bf9a1454
50 0x117d41b24f2f69cb3270b359c181607931f62c56d070bbd14dc9e3f9ab1432e
51 0x7c51564c66f68e2ad4ce6ea0d68f920fafa375376709c606c88a0ed44207aa1e
52 0x48f25191fc8ac7d9f21adf6df23b76ccbca9cb02b815acdbefafa3f4eddc71b34
53 0x4fc21a62c4688de70e28ad3d5956633fc9833bc7be09dc7bc500b7fae1e1c9a8
54 0x1f23f25be0912173c3ef98e1c9990205a69d0bf2303d201d27a5499247f06789
55 0x3131495618a0ac4cb11a702f3f8bab66c4fa1066d0a741af3c92d5c246edd579
56 0xd93fe40faa53913638e497328a1b47603cb062c7afc9e96278603f29fd11fd4
57 0x6b348bc59e984c91d696d1e3c3cfae44021f06f74798c787c355437fb696093d
58 0x65af00e73043edcb479620c8b48098b89809d577a4071c8e33e8678829138b8a
59 0x5e62ffb032b2ddb06591f86a46a18effd5d6ecf3f129bb2bacfd51a3739a98b6

60 0x62c974ef3593fc86f7d78883b8727a2f7359a282cbc0196948e7a793e60ce1a1
61 0x204d708e3f500aad64283f753e7d9bab976aa42a4ca1ce5e9d2264639e8b1110
62 0xa90f0059da81a012e9d0a756809fab2ce61cb45965d4d1513a06227783ee4ea
63 0x39fa55971c9e833f61139c39e243d40869fd7e8a1417ee4e7719dd2dd242766f
64 0x22677c1e659caa324f0c74a013921facf62d0d78f273563145cc1ddccfcc4421
65 0x3468cf6df7e93f7ff1fe1dd7e180a89dec3ed4f72843b4ea8a8d780011a245b2
66 0x68f75a0e2210f52a90704ed5f511918d1f6bcfcd26b462cc4975252369db6e9d
67 0x6220c0699696e9bcab0fe3a80d437519bd2bdf3caef665e106b2dd47585ddd9f
68 0x553ad47b129fb347992b576479b0a89f8d71f1196f83e5eaab5f533a1dd6f6d7
69 0x239aef387e116ec8730fa15af053485ca707650d9f8917a75f22acf6213197df

G.2.3. Coefficients of $w'(x)$:

0 0x6bd7f1fc5dd51b7d832848c180f019bcbdb101d4b3435230a79cc4f95c35e15e
1 0x17413bb3ee505184a504e14419b8d7c8517a0d268f65b0d7f5b0ba68d6166dd0
2 0x47f4471beed06e5e2b6d5569c20e30346bdba2921d9676603c58e55431572f90
3 0x2af7eaafd04f6910a5b01cdb0c27dca09487f1cd1116b38db34563e7b0b414eb
4 0x57f0a593459732eef11d2e2f7085bf9adf534879ba56f7afd17c4a40d3d3477b
5 0x4da04e912f145c8d1e5957e0a9e44cca83e74345b38583b70840bdfdbd0288ed
6 0x7cc9c3a51a3767d9d37c6652c349adc09bfe477d99f249a2a7bc803c1c5f39ed
7 0x425d7e58b8adf87eebf445b424ba308ee7880228921651995a7eab548180ad49
8 0x48156db5c99248234c09f43fedf509005943d3d5f5d7422621617467b06d314f
9 0xd837dbbd1af32d04e2699cb026399c1928472aa1a7f0a1d3afd24bc9923456a
10 0x5b8806e0f924e67c1f207464a9d025758c078b43ddc0ea9afe9993641e5650be
11 0x29c91284e5d14939a6c9bc848908bd9df1f8346c259bbd40f3ed65182f3a2f39
12 0x25550b0f3bceef18a6bf4a46c45bf1b92f22a76d456bdfdf19d07398c80b0f946

- 13 0x495d289b1db16229d7d4630cb65d52500256547401f121a9b09fb8e82cf01953
- 14 0x718c8c610ea7048a370eabfd9888c633ee31dd70f8bcc58361962bb08619963e
- 15 0x55d8a5ceef588ab52a07fa6047d6045550a5c52c91cc8b6b82eeb033c8ca557d
- 16 0x620b5a4974cc3395f96b2a0fa9e6454202ef2c00d82b0e6c534b3b1d20f9a572
- 17 0x4991b763929b00241a1a9a68e00e90c5df087f90b3352c0f4d8094a51429524e
- 18 0x18b6b49c5650fb82e36e25fd4eb6decfdd40b46c37425e6597c7444a1b6afb4e
- 19 0x6868305b4f40654460aad63af3cb9151ab67c775eaac5e5df90d3aea58dee141
- 20 0x16bc90219a36063a22889db810730a8b719c267d538cd28fa7c0d04f124c8580
- 21 0x3628f9cf1fbe3eb559854e3b1c06a4cd6a26906b4e2d2e70616a493bba2dc574
- 22 0x64abcc6759f1ce1ab57d41e17c2633f717064e35a7233a6682f8cf8e9538afec
- 23 0x1

Author's Address

Rene Struik
Struik Security Consultancy

Email: rstruik.ext@gmail.com

