Edwards curves

Youssef El Housni

Edwards Curves

Youssef El Housni

EY Wavespace LAB - Paris

youssef.el.housni@fr.ey.com

November 28, 2018

Contents

Chapter 1

Introduction

In cryptography, Curve25519 is an elliptic curve offering 128 bits of security and designed for use with the elliptic curve Diffie–Hellman (ECDH) key agreement scheme and elliptic curve digital signature (ECDSA) scheme. It is one of the fastest ECC curves and is not covered by any known patents. It was first released by Daniel J. Bernstein in 2005 [1], but interest increased considerably after 2013 when it was discovered that the NSA had implemented a backdoor into Dual_EC_DRBG [6]. While not directly related, suspicious aspects of the NIST's P- curve constants led to concerns that the NSA had chosen values that gave them an advantage in factoring public keys.
Since then, Curve25519 has become the de facto alternative to P-256, and is used in a wide variety of applications. Starting in 2014, OpenSSH defaults to Curve25519-based ECDH. In 2017, NIST announced that Curve25519 and Curve448 (Ed448-Goldilocks) [8] would be added to Special Publication 800-186, which specifies approved elliptic curves for use by the US Federal Government. Both are described in RFC 7748 [10].

This document is organized as follows. The theory of Edwards elliptic curves is covered in section 2, the Curve25519 is then presented in section 3 and cryptographic protocols that use this curve are discussed in section 4.

Chapter 2

Edwards Curves

The normal form (Edwards form) for elliptic curves simplifies formulas in the theory of elliptic curves and functions. Its principal advantage is that it allows the addition law, the group law on the elliptic curve, to be stated explicitly. In this section we will look at the theory behind this from.

2.1 How it all began

In the bulletin of the american mathematical society 2007 [7], Harold Edwards introduced what he called at that time "A normal form for elliptic curves". He went back to the definition of an elliptic function (curve) given by Abel, Euler and Gauss to propose a new-not-new form with interesting group law formulas. In fact, Today an elliptic curve is realized as a cubic curve and when a point of the curve is chosen to serve as the identity of the group operation, the group structure can be described in terms of the sets of three points in which lines intersect the curve, a description that is now well known and widely taught. The connection between this now-familiar group structure and Euler's work is far from obvious, but in fact the two are aspects of the same phenomenon. Another approach to that phenomenon was developed by Abel, where he sketched a broad generalization of the group construction. Instead of intersecting a cubic curve with lines, he intersected an arbitrary curve with an arbitrary family of auxiliary curves. As the parameters in the defining equation of the auxiliary curve vary, the intersection points vary along the given curve. Abel discovered that, under suitable conditions, N intersection points move in this way with $N-g$ degrees of freedom, where g depends only on the given curve, not on N or on the family of auxiliary curves that is used, provided the family is sufficiently general. This g is the genus of the given curve. When that curve is a nonsingular cubic and the auxiliary curves are lines, there are $N = 3$ intersection points that move with $N - g = 2$ degrees of freedom because two of the intersection points can be chosen arbitrarily. Therefore, g is 1 in this case.
Harold Edwards presented in this bulletin a fourth view to this phenomenon that incorporates the the three that have been mentioned. He started from the

particular curve example $x^2+y^2+x^2y^2=1$ for which Euler suggested an explicit "addition formula" that had been stated by Gauss decades later, putting them in the form

$$S=\frac{s_1c_2+s_2c_1}{1-s_1s_2c_1c_2},\quad C=\frac{c_1c_2-s_1s_2}{1+s_1s_2c_1c_2} \tag{2.1.1}$$

(Gauss's choice of the letters s and c brings out the analogy with the addition laws for sines and cosines. (The numerators are the addition laws for sines and cosines))

These remarkable Euler-Gauss formulas apply only to the specific curve $s^2+c^2+s^2c^2=1$, but they are a special case of a formula that describes the group law of an arbitrary elliptic curve, as it was shown by Edwards in this bulletin, of the form

$$y^2+x^2=a^2(1+x^2y^2) \tag{2.1.2}$$

if a is a non-zero constant for which $a^5\neq a$, with the following addition law

$$X=\frac{x_1y_2+x_2y_1}{a(1+x_1x_2y_1y_2)},\quad Y=\frac{y_1y_2-x_1x_2}{a(1-x_1x_2y_1y_2)} \tag{2.1.3}$$

(formula 2.1.1 is the case $a=\sqrt{i}$, $x=s\sqrt{i}$ and $y=c\sqrt{i}$)
In fact a must be different from a^5 so that Eq.2.1.2 is an elliptic curve. In view of Abel's work, an elliptic curve is of the form $z^2=f(x)$ where f is a polynomial of degree 3 or 4 (of degree $2g-1$ or $2g-2$ where the genus g is 1) with distinct roots. Setting $z=(1-a^2x^2)$ puts Eq.2.1.2 in the form $z^2=(a^2-x^2)(1-a^2x^2)$. The polynomial in the right has degree 4, so the equation describes an elliptic curve provided this polynomial $(a^2-x^2)(1-a^2x^2)=a^2x^4-(a^4+1)x^2+a^2$ has distinct roots, which is true if and only if its discriminant is non-zero

$$\Delta=(a^4+1)^2-4a^4=(a^4-1)^2 \tag{2.1.4}$$

thus, $(a^4-1)^2$ must be non-zero or equivalently stated $a^5\neq a$.

What is more important to prove is how did Harold Edwards find these formulas (naughty Harold!).

2.2 Algebraic proof of the addition formula

Given two points (x_1,y_1) and (x_2,y_2) on the curve $x^2+y^2=a^2(1+x^2y^2)$, we want to prove that $(x_1,y_1)+(x_2,y_2)=(x_3,y_3)$ where

$$x_3=\frac{x_1y_2+x_2y_1}{a(1+x_1x_2y_1y_2)},\quad y_3=\frac{y_1y_2-x_1x_2}{a(1-x_1x_2y_1y_2)}$$

This point has to be on the curve, hence $x_3^2 + y_3^2 = a^2(1 + x_3^2 y_3^2)$. Let us use the letter T to abbreviate $x_1 x_2 y_1 y_1$ and multiply this equation by $a^2(1 - T^2)$

$$(x_3^2 + y_3^2 = a^2(1 + x_3^2 y_3^2)) \times a^2(1 - T^2)^2$$
$$(\frac{(x_1 y_2 + x_2 y_1)^2}{a^2(1 - T)^2} + \frac{(y_1 y_2 - x_1 x_2)^2}{a^2(1 + T)^2} = a^2(1 + \frac{(x_1 y_2 + x_2 y_1)^2 (y_1 y_2 - x_1 x_2)^2}{a^4(1 - T)^2(1 + T)^2})) \times a^2(1 - T^2)^2$$
$$(x_1 y_2 + x_2 y_1)^2(1 - T)^2 + (y_1 y_2 - x_1 x_2)^2(1 + T)^2 = a^4(1 - T)^4 + (x_1 y_2 + x_2 y_1)^2 (y_1 y_2 - x_1 x_2)^2$$

This is the consequence of the assumption that $x_1^2 + y_1^2 = a^2(1 + x_1^2 y_1^2)$ and $x_2^2 + y_2^2 = a^2(1 + x_2^2 y_2^2)$ yield $x_3^2 + y_3^2 = a^2(1 + x_3^2 y_3^2)$. In other words, it is to prove that

$$(x_1 y_2 + x_2 y_1)^2(1 - T)^2 + (y_1 y_2 - x_1 x_2)^2(1 + T)^2 = a^4(1 - T)^4 + (x_1 y_2 + x_2 y_1)^2 (y_1 y_2 + x_1 x_2)^2 + R_3$$

where R_3 is a linear combination of $R_1 = x_1^2 + y_1^2 - a^2(1 + x_1^2 y_1^2)$ and $R_2 = x_2^2 + y_2^2 - a^2(1 + x_2^2 y_2^2)$. Let's take a look at Eq.2.2

$$(x_1^2 y_2^2 + x_2^2 y_1^2 + 2T)^2(1 + T^2 - 2T)^2 + (y_1^2 y_2^2 + x_1^2 x_2^2 - 2T)^2(1 + T^2 + 2T)^2 =$$
$$(x_1^2 y_1^2 + y_1^2 x_2^2 + 2T)(y_1^2 y_2^2 + x_1^2 x_2^2 - 2T) + a^4(1 - T^2)^2 + R_3$$
$$(x_1^2 y_2^2 + 2T + y_1^2 x_2^2 + y_1^2 y_2^2 - 2T + x_1^2 x_2^2)(1 + T^2) + (-x_1^2 y_2^2 - 2T - y_1^2 x_2^2 + y_1^2 y_2^2 - 2T + x_1^2 x_2^2)(2T) =$$
$$(x_1^2 y_1^2 + y_1^2 x_2^2)(y_1^2 y_2^2 + x_1^2 x_2^2) + 2T(y_1^2 y_2^2 + x_1^2 x_2^2 - x_1^2 y_1^2 - y_1^2 x_2^2) - 4T^2 + a^4(1 - T^2)^2 + R_3$$
$$(x_1^2 + y_1^2)(x_2^2 + y_2^2)(1 + T^2) + ((x_1^2 - y_1^2)(x_2^2 - y_2^2) - 4T)(2T) =$$
$$x_1^2 y_1^2 y_2^4 + x_1^4 x_2^2 y_2^2 + y_1^4 x_2^2 y_2^2 + x_1^2 y_1^2 x_2^4 + 2T(x_1^2 - y_1^2)(x_2^2 - y_2^2) - 4T^2 + a^4(1 - T^2)^2 + R_3$$
$$(x_1^2 + y_1^2)(x_2^2 + y_2^2)(1 + T^2) + 2T(x_1^2 - y_1^2)(x_2^2 - y_2^2) - 8T^2 =$$
$$x_1^2 y_1^2 y_2^4 + x_1^4 x_2^2 y_2^2 + y_1^4 x_2^2 y_2^2 + x_1^2 y_1^2 x_2^4 + 2T(x_1^2 - y_1^2)(x_2^2 - y_2^2) - 4T^2 + a^4(1 - T^2)^2 + R_3$$

substracting $2T(x_1^2 - y_1^2)(x_2^2 - y_2^2) - 8T^2$ from both sides

$$\begin{aligned}(x_1^2 + y_1^2)(x_2^2 + y_2^2)(1 + T^2) &= x_1^2 y_1^2 y_2^4 + x_1^4 x_2^2 y_2^2 + y_1^4 x_2^2 y_2^2 + x_1^2 y_1^2 x_2^4 + 4T^2 + a^4(1 - T^2)^2 + R_3 \\ &= x_1^2 y_1^2 (y_2^4 + 2x_2^2 y_2^2 + x_2^4) + x_2^2 y_2^2 (y_1^4 + 2x_1^2 y_1^2 + x_1^4) + a^4(1 - T^2)^2 + R_3 \\ &= x_1^2 y_1^2 (y_2^2 + x_2^2)^2 + x_2^2 y_2^2 (y_1^2 + x_1^2)^2 + a^4(1 - T^2)^2 + R_3\end{aligned}$$

and writing $(1 - T^2)^2$ as

$$\begin{aligned}(1 - T^2)^2 &= (1 + T^2)^2 - 4T^2 \\ &= (1 + T^2)(1 + x_1^2 y_1^2 + x_2^2 y_2^2 + T^2) - (1 + T^2)(x_1^2 y_1^2 + x_2^2 y_2^2) - 4T^2 \\ &= (1 + T^2)(1 + x_1^2 y_1^2)(1 + x_2^2 y_2^2) - x_1^2 y_1^2 - x_2^2 y_2^2 - 2T^2 - 2T^2 - x_1^2 y_1^2 T^2 - x_2^2 y_2^2 T^2 \\ &= (1 + T^2)(1 + x_1^2 y_1^2)(1 + x_2^2 y_2^2) - x_1^2 y_1^2 (1 + 2x_2^2 y_2^2 + x_2^4 y_2^4) - x_2^2 y_2^2 (1 + 2x_1^2 y_1^2 + x_1^4 y_1^4) \\ &= (1 + T^2)(1 + x_1^2 y_1^2)(1 + x_2^2 y_2^2) - x_1^2 y_1^2 (1 + x_2^2 y_2^2)^2 - x_2^2 y_2^2 (1 + x_1^2 y_1^2)^2\end{aligned}$$

yields

$$R_3 = (1+T^2)[(x_1^2+y_1^2)(x_2^2+y_2^2) - a^2(1+x_1^2y_1^2)a^2(1+x_2^2y_2^2)]+$$
$$x_1^2y_1^2[a^4(1+x_2^2y_2^2)^2 - (x_2^2+y_2^2)^2] + x_2^2y_2^2[a^4(1+x_1^2y_1^2)^2 - (x_1^2+y_1^2)^2]$$
$$= (1+T^2)[R_1(x_2^2+y_2^2) + R_2(x_1^2+y_1^2)] - x_1^2y_1^2[R_2(2x_2^2+2y_2^2-R_2)] - x_2^2y_2^2[R_1(2x_1^2+2y_1^2-R_1)]$$

Which is a combination of R_1 and R_2. So if $R_1 = R_2 = 0$, then $R_3 = 0$ and thus the algebraic addition formula is correct.

I know that this proof is cumbersome; the algebra is straightforward but tedious however. So here is a way to "understand" this addition law for those who have Math anxiety (*I see you*):

Let $x^2 + y^2 = 1$ be the unit circle equation and $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ be points on this circle. We have (see Fig.2.1):

$$(x_1, y_1) = (sin(\alpha_1), cos(\alpha_1)), \quad (x_2, y_2) = (sin(\alpha_2), cos(\alpha_2))$$

and thus this addition is given by

$$\begin{aligned} x_3 &= sin(\alpha_1 + \alpha_2) \\ &= sin(\alpha_1)cos(\alpha_2) + cos(\alpha_1)sin(\alpha_2) \\ &= x_1y_2 + y_1x_2 \\ y_3 &= cos(\alpha_1 + \alpha_2) \\ &= cos(\alpha_1)cos(\alpha_2) - sin(\alpha_1)sin(\alpha_2) \\ &= y_1y_2 - x_1x_2 \end{aligned}$$

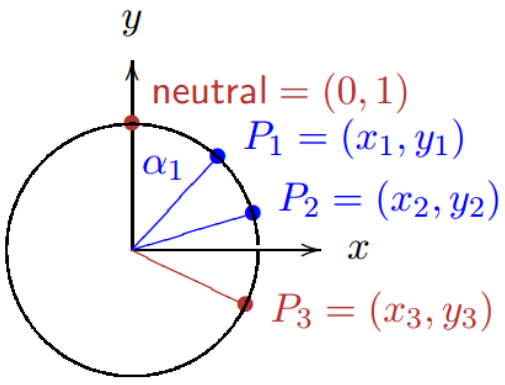

Figure 2.1: Addition law on a unit circle

Now take the Edwards curve $x^2 + y^2 = 1 + x^2y^2$ ($a = 1$) and the points $P_1(x_1, y_1)$, $P_2(x_2, y_2)$ on this curve (see Fig.2.2). The addition is given by

$$x_3 = \frac{x_1y_2 + x_2y_1}{1 + x_1x_2y_1y_2}$$
$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - x_1x_2y_1y_2}$$

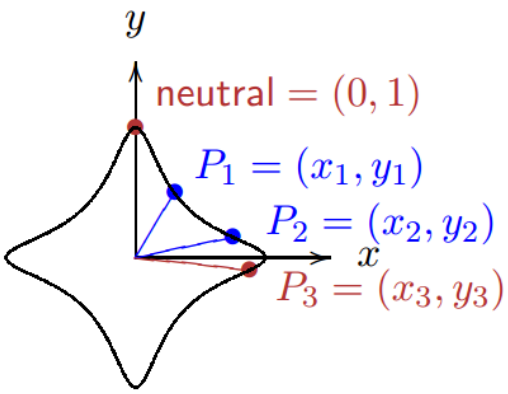

Figure 2.2: Addition law on a unit edwards curve

Furthermore, given the formulas of Eq.2.1.3, the neutral element (the zero on the curve) is $(0, a)$ and the inverse of (x_1, y_1) is $(-x_1, y_1)$.

Proof. Let $P(x_1, y_1)$ be a point on the curve $x^2 + y^2 = a^2(1 + x^2y^2)$, we have:

$$\frac{x_1a + 0.y_1}{a(1 + x_1.0.y_1a)} = x_1, \quad \frac{y_1a - x_1.0}{a(1 - x_1.0.y_1a)} = y_1$$

and

$$\frac{x_1y_1 - x_1.y_1}{a(1 + x_1^2.y_1^2)} = 0$$
$$\frac{y_1^2 + x_1^2}{a(1 - x_1^2y_1^2)} = a$$

Given the uniqueness of the neutral element and inverse element the proof is complete. □

Claim 1. *The addition law is strongly unified, i.e., it can be also used for doubling operation.*

$$2(x_1, y_2) = \left(\frac{2x_1y_1}{a(1 + x_1^2y_1^2)}, \frac{y_1^2 - x_1^2}{a(1 - x_1^2y_1^2)}\right)$$

2.3 A larger class of Edwards curves

First, Edwards curves (E) : $x^2 + y^2 = a^2(1 + x^2y^2)$ are defined over non-binary fields ($char \neq 2$) as to be non singular. In fact, the partial derivatives are:

$$\frac{\partial E}{\partial x} = 2x(1 - a^2y^2), \quad \frac{\partial E}{\partial y} = 2x(1 - a^2x^2)$$

Thus, for binary fields, $\frac{\partial E}{\partial x} = \frac{\partial E}{\partial y} = 0$ in all points. Hence, the curve is singular. From now on, the field over which an Edwards curve is defined is a non-binary

field ($char \neq 2$).

Harold Edwards in [7] showed that all elliptic curves over non-binary fields can be transformed to Edwards form. Some elliptic curves require a field extension for the transformation, but some have transformations defined over the original finite field. To capture a larger class of elliptic curves over the original field, Bernstein and Lange in [5] expanded the notion of Edwards form to include curves $x^2 + y^2 = a^2(1 + dx^2y^2)$ where $cd(1 - dc^4) \neq 0$ (the proof is the same as in 2.1.4). Thus, the addition law becomes:

$$(x_1, y_1) + (x_2, y_2) \mapsto (\frac{x_1y_2 + x_2y_1}{a(1 + dx_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{a(1 - dx_1x_2y_1y_2)}) \tag{2.3.1}$$

Claim 2. *If d is a non-square the addition law is complete, i.e., it works for all input pairs with no exceptions.*

Proof. Let (x_1, y_1) and (x_2, y_2) be on the curve and $\epsilon = dx_1x_2y_1y_2$. The addition would be complete if the denominator can't be 0. Let d be a non-square and suppose that $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and

$$\begin{aligned} dx_1^2y_1^2(x_2^2 + y_2^2) &= dx_1^2y_1^2(1 + dx_2^2y_2^2) \\ &= dx_1^2y_1^2 + \epsilon^2 \\ &= dx_1^2y_1^2 + 1 \\ &= x_1^2 + y_1^2 \end{aligned}$$

it follows that

$$\begin{aligned} (x_1 + \epsilon y_1)^2 &= x_1^2 + y_1^2 + 2\epsilon x_1y_1 \\ &= dx_1^2y_1^2(x_2^2 + y_2^2) + 2dx_1^2y_1^2x_2y_2 \\ &= dx_1^2y_1^2(x_2^2 + 2x_2y_2 + y_2^2) \\ &= dx_1^2y_1^2(x_2 + y_2)^2 \end{aligned}$$

So if

- $x_2 + y_2 \neq 0 \implies d = (\frac{x_1 + \epsilon y_1}{x_1y_1(x_2 + y_2)})^2 \implies d$ is a square (contradiction)
- $x_2 - y_2 \neq 0 \implies d = (\frac{x_1 - \epsilon y_1}{x_1y_1(x_2 - y_2)})^2 \implies d$ is a square (contradiction)
- $x_2 + y_2 = 0$ and $x_2 - y_2 = 0 \implies x_2 = y_2 = 0$ (contradiction)

□

Every Edwards curve can be easily transformed to an isomorphic Edwards curve over the same field having $a = 1$ and thus, in the subsequent, we will note an Edwards curve one of the form:

$$(E) : x^2 + y^2 = 1 + dx^2y^2 \tag{2.3.2}$$

Proof. Let $\overline{x}^2+\overline{y}^2 = \overline{c}^2(1+\overline{d}\overline{x}^2\overline{y}^2)$ be an Edwards curve. Define $\overline{x} = \overline{c}x$ and $\overline{y} = \overline{c}y$, then

$$\overline{x}^2 + \overline{y}^2 = \overline{c}^2(1 + \overline{d}\overline{x}^2\overline{y}^2) \implies x^2 + y^2 = 1 + \overline{d}\overline{c}^4x^2y$$

with $d = \overline{d}\overline{c}^4$. □

Next, we will show that Edwards curves of equation 2.3.2 defined over non-binary fields that has an element of order 4 are bi-rationally equivalent to elliptic curves of Weierstrass form. Note that every Edwards curve has a point of order 4 (the points $(\pm 1, 0)$), so it is natural to consider elliptic curves of order 4. For the other way round, that is to map a Weierstrass curve that hasn't a an element of order 4 to an Edwards curve, we construct an extension field such as the group of point defined over the extension has an element of order 4. Therefore, some twisted curve will be bi-rationally equivalent to Edwards curve over the extension field.

- *Emmanuel Macron: Wait, what is a bi-rational equivalence?*
- *Youssef: First of all, bi-rational equivalence is a geometric notion. Given two geometric objects, elliptic curves for instance, we want to define what it means to be "the same". The usual terminology is that given two curves E_1 and E_2, they are "the same" when they are isomorphic. There is another way to equate objects, and that is by saying that they are "almost the same". This is what a bi-rational equivalence does: two curves E_1 and E_2 are bi-rationally equivalent when there is a map $\phi : E_1 \to E_2$ between them which is defined at every point of E_1 except a small set of exceptions and there is an inverse map $\phi^{-1} : E_2 \to E_1$ which is defined at every point of E_2 except a small set of exceptions. This definition is very close to that of an isomorphism, except for the fact that we allow some exceptions.*
  To make this more concrete, on one hand, you could think of an isomorphism as a tuple of polynomials $\Phi : E_1 \to E_2$, $(x, y) \mapsto (f(x, y), g(x, y))$ where f, g are polynomials in x, y. The inverse is also defined in terms of polynomials. On the other hand, a bi-rational map can be thought of as a tuple of fractions of polynomials $\phi : E_1 \to E_2$, $(x, y) \mapsto (\frac{f_1(x,y)}{f_2(x,y)}, \frac{g_1(x,y)}{g_2(x,y)})$. This map is defined at all points x, y except for the ones where $f_2(x, y) = 0$ or $g_2(x, y) = 0$. The inverse map is also a fraction of polynomials, and thus can be undefined at some points.

Theorem 1. *Let $\mathbb{K}$ be a field where $char(\mathbb{K}) \neq 2$. Let $\mathcal{E}$ be an elliptic curve of Weierstrass form such that the group $\mathcal{E}(\mathbb{K})$ has an element of order 4. Then*

1. *There exists $d \in \mathbb{K}-\{0, 1\}$ such that the curve $x^2+y^2 = 1+dx^2y^2$ is bi-rationally equivalent over $\mathbb{K}$ to a quadratic twist of $\mathcal{E}$,*
2. *if $\mathcal{E}(\mathbb{K})$ has a unique element of order 2, then there is a non-square $d \in \mathbb{K}$ such that the curve $x^2+y^2 = 1+dx^2y^2$ is bi-rationally equivalent over $\mathbb{K}$ to a quadratic twist of $\mathcal{E}$ and*

3. *if $\mathbb{K}$ is a finite field and $\mathcal{E}(\mathbb{K})$ has a unique element of order 2 then there is a non-quare $d \in \mathbb{K}$ such that the curve $x^2 + y^2 = 1 + dx^2y^2$ is bi-rationally equivalent over $\mathbb{K}$ to $\mathcal{E}$*

Proof. Refer to ([5], Theorem 2.1). However, here is a sketch of the proof: Define $\mathcal{E}$ in long Weierstrass form then reduce it without loss of generality to the Montgomery form $y^2 = x^3+a_2x^2+a_4x$ and then show, under the presumed conditions, that $x^2+y^2 = 1+dx^2y^2$ is bi-rationally equivalent to $\frac{1}{1-d}v^2 = u^3+2\frac{1+d}{1-d}u^2+u$. The rational map $(u, v) \mapsto (x, y)$ is defined by $x = \frac{2u}{v}$ and $y = \frac{u-1}{u+1}$; there are only few exceptional points with $v(u + 1) = 0$ (see Christophe's definition). The inverse rational map $(x, y) \mapsto (u, v)$ is defined by $u = \frac{1+y}{1-y}$ and $v = \frac{2(1+y)}{x(1-y)}$; there are only few exceptional points with $x(1 - y) = 0$.

□

Now we have (*almost*) all the necessary background to define the Curve25519 in its Edwards form.

Chapter 3

Curve25519

Curve25519 was introduced in 2006 [1] as an elliptic-curve-Diffie-Hellman function but it is known today as the underlying elliptic curve designed for use with ECDH key agreement scheme (X25519) or with ECDSA signature (Ed25519). It was first introduced in its Montgomery form

$$E_1 : v^2 = u^3 + 486662u^2 + u \tag{3.0.1}$$

over the prime field defined by the the pseudo-Mersenne prime number $p = 2^{255} - 19$. This curve is, as we have shown in Sec. 2.3, bi-rationally equivalent to the Edwards curve

$$E_2 : x^2 + y^2 = 1 + \frac{121665}{121666}x^2y^2 \tag{3.0.2}$$

The bi-rational equivalence is given by the map

$$\begin{aligned} \phi : \quad & E_1 \to E_2 \\ & (u, v) \mapsto \left(\frac{\sqrt{486664}u}{v}, \frac{u-1}{u+1} \right) \end{aligned}$$

Notice that it is undefined for $v = 0$ or $u = -1$, and therefore it is not an isomorphism; it is a bi-rational equivalence (Christophe's answer to Emmanuel Macron). The inverse map is defined by

$$\begin{aligned} \phi^{-1} : \quad & E_2 \to E_1 \\ & (x, y) \mapsto \left(\frac{1+y}{1-y}, \frac{\sqrt{486664}u}{x} \right) \end{aligned}$$

It is undefined for $y = 1$ or $x = 0$.
Note that 486664 is a square modulo p and that $d = \frac{121665}{121666}$ is not a square modulo p.
To avoid exceptional points, consider the twisted Edwards curve

$$E_3 : -x^2 + y^2 = 1 - \frac{121665}{121666}x^2y^2 \tag{3.0.3}$$

There is a map $\chi : E_2 \to E_3$ defined by $\chi(x, y) = (ix, y)$, assuming that i is a square root of -1. This is clearly defined everywhere, and is an isomorphism

- **The choice of the field:**
  The field is a prime finite field with $p = 2^{255} - 19$ elements to assure a 128-bit security level as the fastest known attack on the discrete logarithm problem (Pollard's ρ combined with Pohlig-Hellman) has complexity $\mathcal{O}(\sqrt{\ell})$ where ℓ is the cyclic subgroup order. Since ℓ is related to the order of the elliptic curve group N by Lagrange's theorem $h = N/\ell$ where h the cofactor is taken small to avoid Pohlig-Hellman attack, it is natural to consider that the complexity is $\approx \mathcal{O}(\sqrt{N})$ and since the gap between N and p is at most $2\sqrt{p}$ according to Hasse's theorem, the complexity is $\approx \mathcal{O}(\sqrt{p})$. Thus, since p has 256 bits the curve offers a 128-bit security level. Bernstein chose a pseudo-Mersenne prime number pf the form $p = 2^m - \alpha$ to perform modular arithmetic efficiently; a product to be reduced modulo p is split into a lower and higher part, with the lower part of length m bits. The top part is multiplied by c and added to the lower part. Finally the small excess beyond m bits is extracted, multiplied by c and added to the total.

- **The choice of the constant:**
  Let us note the constant A. Montgomery suggested to take $(A-2)/4$ as a small integer to speed up the multiplication by $(A-2)/4$; this has no effect on the conjectured security level. Furthermore, to protect against various attacks discussed in ([1], Section 3), Bernstein rejected choices of A whose curve and twist orders were not $\{4.\text{prime}, 8.\text{prime}\}$. The smallest positive choices for A are 358990, 464586 and 486662. He rejected $A = 358990$ because one of its primes is slightly smaller than 2^{252}, raising the question of how standards and implementations should handle the theoretical possibility of a user's secret key matching the prime; discussing this question is more difficult than switching to another A. He rejected 464586 for the same reason. So he ended up with $A = 486662$.

Chapter 4

X25519 and Ed25519 protocols

The Curve25519 can be used in an Elliptic Curve Diffie-Hellman (ECDH) protocol or an Elliptic Curve Digital Signature Algorithm (ECDSA). These protocols are named respectively X25519 and Ed25519.

4.1 X25519

The X25519 function [1] can be used in an Elliptic Curve Diffie-Hellman (ECDH) protocol using the Curve25519 with the base point $x = 9$. This base point has order $2^{252} + 27742317777372353535851937790883648493$. The protocol is as follows:

Alice generates 32 random bytes in $a[0]$ to $a[31]$ and transmits $K_A = \text{X25519}(a, 9)$ to Bob, where 9 is the x-coordinate of the base point and is encoded as a byte with value 9, followed by 31 zero bytes.
Bob similarly generates 32 random bytes in $b[0]$ to $b[31]$, computes $K_B = \text{X25519}(b, 9)$, and transmits it to Alice.
Using their generated values and the received input, Alice computes $\text{X25519}(a, K_B)$ and Bob computes $\text{X25519}(b, K_A)$. Both now share $K = \text{X25519}(a, \text{X25519}(b, 9)) = \text{X25519}(b, \text{X25519}(a, 9))$ as a shared secret.

4.2 Ed25519

Ed25519 is the Edwards-curve Digital Signature Algorithm (EdDSA)[2] using SHA-512/256 and the twisted Curve25519 of equation 3.0.3. EdDSA is a digital signature scheme using a variant of Schnorr signature based on Twisted Edwards curves. It is designed to be faster than existing digital signature schemes without sacrificing security. It was developed by a team including Bernstein, Duif, Lange, Schwabe, Yang. In fact Elliptic Curve Digiral Signature Algortihm (ECDSA) is notably known because of the PlayStation 3 hack (Sony's mistake) in which private key would be retrieved because ECDSA wasn't properly randomized. Researchers then have asked themselves how could data be signed without relying on a random generator, hence avoiding randomness-failure of this sort. A few answers came out, with -most notably- RFC6979 [11], which

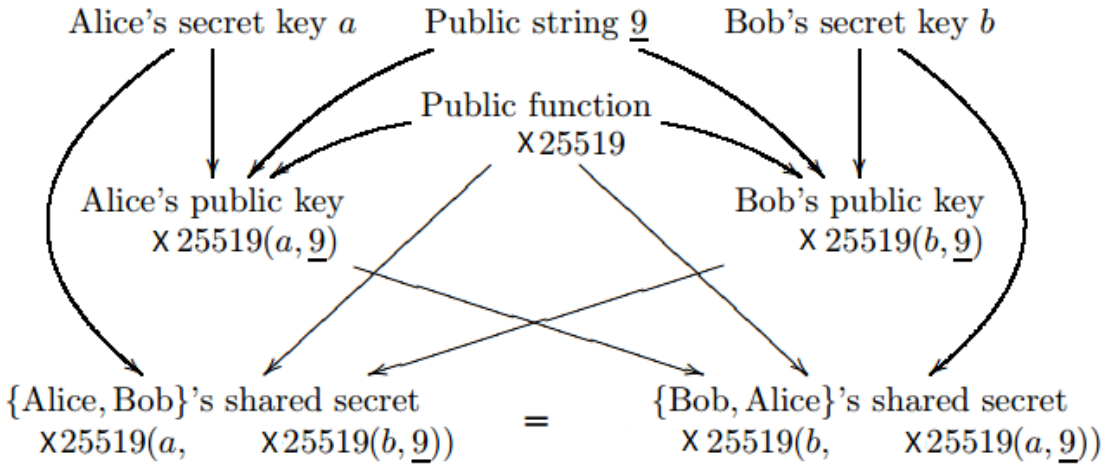

Figure 4.1: X25519 protocol

introduced a deterministic version of ECDSA to avoid those problems. EdDSA is another deterministic elliptic curve signature scheme, described in RFC8032 [9] and originally introduced in [3] and generalized for more curves in [4].
An EdDSA signature scheme is a choice

- of finite field $\mathbb{F}_q$ over odd prime power q,
- of elliptic curve E $\mathbb{F}_q$ whose group $E(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points has order $\#E(\mathbb{F}_q) = 2^c\ell$, where ℓ is a large prime and 2^c the cofactor,
- of base point $B \in E(\mathbb{F}_q)$ with order ℓ and
- of target-collision-resistant hash function H with $2b$-bit outputs, where $2^{b-1} > q$ so that elements of $\mathbb{F}_q$ and curve points in $E(\mathbb{F}_q)$ can be represented by strings of b bits.

Within an EdDSA signature scheme,
Public key
An EdDSA public key is a curve point $A \in E(\mathbb{F}_q)$, encoded in b bits.

Signature An EdDSA signature on a message M by public key A is the pair (R, S), encoded in $2b$ bits, of a curve point $R \in E(\mathbb{F}_q)$ and an integer $0 < S < \ell$ satisfying the verification equation$2^cSB = 2^cR + 2^cH(R, A, M)A$.

Private key An EdDSA private key is a b-bit string k which should be chosen uniformly at random. The corresponding public key is $A = sB$, where $s = H_{0,\ldots,b-1}(k)$ is the least significant b bits of $H(k)$ interpreted as an integer in little-endian. The signature on a message M is (R, S) where $R = rB$ for $r = H(H_{b,\ldots,2b-1}(k), M)$, and $S \equiv r + H(R, A, M)s \pmod{\ell}$.

This clearly satisfies the verification equation:

$$\begin{aligned} 2^c SB &= 2^c(r + H(R, A, M)s)B \\ &= 2^c rB + 2^c H(R, A, M)sB \\ &= 2^c R + 2^c H(R, A, M)A. \end{aligned}$$

For Ed25519 the parameters are:

- $q = 2^{255} - 19$,
- $E/\mathbb{F}_q$ is the twisted Edwards curve $-x^2 + y^2 = 1 - \frac{121665}{121666}x^2y^2$,
- B is the unique point in $E(\mathbb{F}_q)$ whose y coordinate is $4/5$ and whose x Coordinate is positive, and
- H is SHA-512, with $b = 256$.

Arithmetic modulo $q = 2^{255} - 19$ can be implemented efficiently and securely. For instance, inversion modulo q can be carried using the identity $x^{-1} \equiv x^{q-2} \pmod{q}$ (because $x^q \equiv x \pmod{q}$ in $GF(q)$). For point decoding or "decompression", square roots modulo q are needed. They can be computed using the Tonelli-Shanks algorithm or the special case for $q \equiv 5 \pmod{8}$. To find a square root of a, first compute the candidate root $x \equiv a^{\frac{q+3}{8}} \pmod{q}$. Then there are three cases:

- $x^2 \equiv a \pmod{q}$. Then x is a square root.
- $x^2 \equiv -a \pmod{q}$. Then $2^{\frac{q-1}{4}} \times x$ is a square root.
- a is not a square modulo q.

Proof. see appendix D □

Bibliography

[1] D. J. Bernstein. Curve25519: New diffie-hellman speed records. In *Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA, April 24-26, 2006, Proceedings*, pages 207–228, 2006.

[2] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B. Yang. High-speed high-security signatures. *J. Cryptographic Engineering*, 2(2):77–89, 2012.

[3] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B. Yang. High-speed high-security signatures. *J. Cryptographic Engineering*, 2(2):77–89, 2012.

[4] D. J. Bernstein, S. Josefsson, T. Lange, P. Schwabe, and B. Yang. Eddsa for more curves. *IACR Cryptology ePrint Archive*, 2015:677, 2015.

[5] D. J. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. In *Advances in Cryptology - ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, December 2-6, 2007, Proceedings*, pages 29–50, 2007.

[6] D. J. Bernstein, T. Lange, and R. Niederhagen. Dual EC: A standardized back door. In *The New Codebreakers - Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*, pages 256–281, 2016.

[7] H. M. Edwards. A normal form for elliptic curves. In *Bulletin of the American Mathematical Society*, pages 393–422.

[8] M. Hamburg. Ed448-goldilocks, a new elliptic curve. *IACR Cryptology ePrint Archive*, 2015:625, 2015.

[9] S. Josefsson and I. Liusvaara. Edwards-Curve Digital Signature Algorithm (EdDSA). RFC 8032, Jan. 2017.

[10] A. Langley, M. Hamburg, and S. Turner. Elliptic Curves for Security. RFC 7748, Jan. 2016.

[11] T. Pornin. Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA). RFC 6979, Aug. 2013.

Appendix A

Explicit-Formulas database

A.1 Montgomery Curves

Given the elliptic curve in Montgomery form (E_m): $by^2 = x^3 + ax^2 + x$, we give the affine formulas for the addition law, then we establish projective formulas.

Affine coordinates

Given the points (x_1, y_1), $(x_2, y_2) \in E_m$, let the point $(x_1, y_1) + (x_2, y_2) \mapsto (x_3, y_3)$ be the result addition point.

$$x_3 = b\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a - x_1 - x_2 \tag{A.1.1}$$

$$y_3 = (2x_1 + x_2 + a)\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - b\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^3 - y_1 \tag{A.1.2}$$

Proof. Let $(L) : y = mx + n$ be the line passing through (x_1, y_1) and (x_2, y_2) where $m = \frac{y_2 - y_1}{x_2 - x_1}$ and $n = y_1 - mx_1 = y_2 - mx_2$. The point (x_3, y_3) is x-axis symmetric point defined by the intersection between (E_m) anad (L). That is to say,

$$\begin{aligned} b(mx + n)^2 &= x^3 + ax^2 + x \\ x^3 + (a - bm^2)x^2 + (1 - bmn)x - bn^2 &= 0 \end{aligned}$$

This equation has 3 roots, namely x_1, x_2 and x_3. According to Vieta's formulas the sum of the roots verify $x_1 + x_2 + x_3 = bm^2 - a$. Hence

$$x_3 = bm^2 - a - x_1 - x_2$$

and

$$\begin{aligned} -y_3 &= mx_3 + n \\ -y_3 &= m(bm^2 - a - x_1 - x_2) + y_1 - mx_1 \\ y_3 &= (2x_1 + x_2 + a)m - bm^3 - y_1 \end{aligned}$$

□

For doubling, the result the point $2(x_1y_1) \mapsto (x_3y_3)$ is

$$x_3 = b\left(\frac{3x_1^2 + 2ax_1 + 1}{2by_1}\right)^2 - a - x_1 - x_2 \tag{A.1.3}$$

$$y_3 = (2x_1 + x_2 + a)\left(\frac{3x_1^2 + 2ax_1 + 1}{2by_1}\right) - b\left(\frac{3x_1^2 + 2ax_1 + 1}{2by_1}\right)^3 - y_1 \tag{A.1.4}$$

Proof. The line (L) is the tangent of equation $f'(x_1)(x - x_1) + f(x_1)$ where $f(x) = \pm\sqrt{(x^3 + ax^2 + x)/b}$. Given that

$$f'(x) = \frac{3x^2 + 2ax + 1}{2by}$$

we have $f'(x_1) = \frac{3x_1^2+2ax_1+1}{2by_1}$ and $f(x_1) = y_1$. Thus we can write (L) as $mx + n$ where

$$m = f'(x_1) = \frac{3x_1^2 + 2ax_1 + 1}{2by_1}$$
$$n = f(x_1) - x_1f'(x_1) = y_1 - mx_1$$

Then the formulas can be obtained following the same proof as for the addition law, with the apropriate m. □

Projective coordinates

Montgomery proposed an efficient method to compute the x-coordinate of $k \times (x_1, y_1)$ given only the x-coordinate of (x_1, y_1). For this, we use the projective representation $(X : Z)$ with $x = X/Z$. Let $a_{24} = (a + 2)/4$ *(For Curve25519* $a_{24} = 121666 =$ *0x1DB42)*, we have

$$A = (X_1 + Z_1)^2;\ B = (X_1 - Z_1)^2;\ C = A - B$$
$$X_3 = A \times B$$
$$Z_3 = C \times (B + a_{24} \times C)$$

A.2 Edwards Curves

Given the elliptic curve (E_e): $x^2 + y^2 = 1 + dx^2y^2$, we start by recalling the affine formulas for the addition law, then we establish projective and inverted formulas. A comparison, in terms of operations counts, is carried afterwards.

Affine coordinates

Given the points (x_1, y_1), $(x_2, y_2) \in E_e$, let the point $(x_1, y_1) + (x_2, y_2) \mapsto (x_3, y_3)$ be the result addition point.

$$x_3 = \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2} \tag{A.2.1}$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \tag{A.2.2}$$

Remark: This formula are unified for doubling and adding operation (see. Claim 1). If d is not a square, then the formula are complete (see. Claim 2).

Projective coordinates

Given the set of projective points $(X : Y : Z)$ where $Z \neq 0$ corresponds to the set of affine points $(X/Z, Y/Z)$, the equation of (E) becomes

$$(E_Z) : \ Z^2(X^2 + Y^2) = Z^4 + dX^2Y^2$$

The neutral element is $(0 : 1 : 1)$ and the inverse of $(X : Y : Z)$ is $(-X : Y : Z)$. Given the points $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ on the curve (E_Z) let the point $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) \mapsto (X_3 : Y_3 : Z_3)$ be the result addition point. Thus,

$$\begin{aligned}
&A = Z_1Z_2;\ B = A^2;\ C = X_1X_2 \\
&D = Y_1Y_2;\ E = dCD;\ F = B - E;\ G = B + E \\
&X_3 = AF((X_1 + Y_1)(X_2 + Y_2) - C - D) && \text{(A.2.3)} \\
&Y_3 = AG(D - C) && \text{(A.2.4)} \\
&Z_3 = GF && \text{(A.2.5)}
\end{aligned}$$

Proof. According to A.2.1 and A.2.2 we have

$$\frac{X_3}{Z_3} = \frac{\frac{X_1}{Z_1}\frac{Y_2}{Z_2} + \frac{X_2}{Z_2}\frac{Y_1}{Z_1}}{1 + d\frac{X_1X_2Y_1Y_2}{Z_1^2Z_2^2}}, \quad \frac{Y_3}{Z_3} = \frac{\frac{Y_1}{Z_1}\frac{Y_2}{Z_2} - \frac{X_1}{Z_1}\frac{X_2}{Z_2}}{1 - d\frac{X_1X_2Y_1Y_2}{Z_1^2Z_2^2}}$$

$$\frac{X_3}{Z_3} = \frac{Z_1Z_2(X_1Y_2 + X_2Y_1)}{Z_1^2Z_2^2 + dX_1X_2Y_1Y_2}, \quad \frac{Y_3}{Z_3} = \frac{Z_1Z_2(Y_1Y_2 - X_1X_2)}{Z_1^2Z_2^2 - dX_1X_2Y_1Y_2}$$

We take

$$\begin{aligned}
Z_3 &= (Z_1^2Z_2^2 + dX_1X_2Y_1Y_2)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2) \\
&= Z_1^4Z_2^4 - d^2X_1^2X_2^2Y_1^2Y_2^2 \\
&= GF
\end{aligned}$$

and then we have

$$\begin{aligned}
X_3 &= Z_1Z_2(X_1Y_2 + X_2Y_1)(Z_1^2Z_2^2 - dX_1X_2Y_1Y_2) \\
&= AF((X_1 + Y_1)(X_2 + Y_2) - C - D)
\end{aligned}$$

and

$$\begin{aligned} Y_3 &= Z_1Z_2(Y_1Y_2 - X_1X_2)(Z_1^2Z_2^2 + dX_1X_2Y_1Y_2) \\ &= AG(D - C) \end{aligned}$$

□

Remark: This formula are unified for doubling and adding operation (see. Claim 1). If d is not a square, then the formula are complete (see. Claim 2).

Mixed addition: This refers to the case where $Z_2 = 1$. In this case, the multiplication $A = Z_1Z_2$ can be eliminated. **Doubling:** If doubling and adding operation are different, then the formula of doubling could be

$$\begin{aligned} B = (X1 + Y1)^2;\ C = X1^2;\ D = Y1^2 \\ E = C + D;\ H = Z1^2;\ J = E - 2H \\ X3 = B - E \\ Y3 = E(C - D) \\ Z3 = EJ \end{aligned}$$

with only 3 multiplications, 4 squares, 5 additions over $\mathbb{F}_p$.

Inverted coordinates

Given the set of projective points $(X : Y : Z)$ where $XYZ \neq 0$ corresponds to the set of affine points $(Z/X, Z/Y)$, the equation of (E) becomes

$$(E'_Z) :\ Z^2(X^2 + Y^2) = dZ^4 + X^2Y^2$$

The result addition point is

$$\begin{aligned} A = Z_1Z_2;\ B = dA^2;\ C = X_1X_2;\ D = Y_1Y_2;\ E = CD; \\ F = C - D;\ G = (X_1 + Y_1)(X_2 + Y_2) - C - D; \\ X_3 = (E + B)F \qquad \text{(A.2.6)} \\ Y_3 = (E - B)G \qquad \text{(A.2.7)} \\ Z_3 = AFG \qquad \text{(A.2.8)} \end{aligned}$$

Proof. According to A.2.1 and A.2.2 we have

$$\begin{aligned} \frac{Z_3}{X_3} &= \frac{Z_1Z_2(X_2Y_1 + X_1Y_2)}{X_1X_2Y_1Y_2 + dZ_1^2Z_2^2}, \quad \frac{Z_3}{Y_3} = \frac{Z_1Z_2(X_1X_2 - Y_1Y_2)}{X_1X_2Y_1Y_2 - dZ_1^2Z_2^2} \\ \frac{X_3}{Z_3} &= \frac{X_1X_2Y_1Y_2 + dZ_1^2Z_2^2}{Z_1Z_2(X_2Y_1 + X_1Y_2)}, \quad \frac{Y_3}{Z_3} = \frac{X_1X_2Y_1Y_2 - dZ_1^2Z_2^2}{Z_1Z_2(X_1X_2 - Y_1Y_2)} \end{aligned}$$

we take

$$\begin{aligned} Z_3 &= Z_1Z_2(X_1X_2 - Y_1Y_2)(X_1Y_2 + X_2Y_1) \\ &= AFG \end{aligned}$$

and then we have

$$\begin{aligned} X_3 &= (X_1X_2 - Y_1Y_2)(X_1X_2Y_1Y_2 + dZ_1^2Z_2^2) \\ &= (E + B)F \end{aligned}$$

and

$$\begin{aligned} Y_3 &= (X_1Y_2 + X_2Y_1)(X_1X_2Y_1Y_2 - dZ_1^2Z_2^2) \\ &= (E - B)G \end{aligned}$$

□

Note that the requirement $XYZ \neq 0$ means that we can't represent in inverted coordinates points (x, y) such that $xy = 0$. There 4 points satisfying this condition: The neutral element $(0, 1)$, the point of order 2 $(0, -1)$ and the points of order 4 $(\pm 1, 0)$. Additions that involve these points must be handled separately.
Mixed addition: This refers to the case where $Z_2 = 1$. In this case, the multiplication $A = Z_1Z_2$ can be eliminated.

Remark: In order to compute the inverted coordinates from affine coordinates. The cost is 2 modular inversions for $Z = 1$. For a Z in $\mathbb{F}_p$, the cost is 2 modular inversion and 2 modular multiplications. To reduce the 2 inversions up to 1 inversion and 3 modular multiplications, the elegant idea from Youssef is compute the product of X and Y, make the inversion of the product and after multiply by X the Y and vice versa.

Count of operations

Here we denote

- **M**: Field multiplication.
- **S**: Field squaring.
- **m**: Multiplication by a constant d.
- **A**: Field addition.
- **I**: Field inversion.

From the explicit formulas, one can readily count

Coordinates / Operations	**M**	**S**	**m**	**A**	**I**
Affine	5	0	1	4	2
Projective	10	1	1	7	0
Inverted	9	1	1	7	0

Table A.1: Count of operations for addition

In mixed addition, $A = Z_1 Z_2$ is eliminated and thus one 1**M** is saved for each addition. The resulting count of operation for a mixed addition is

- In projective coordinates: 9**M**, 1**S**, 1**m** and 7**A**.
- In inverted coordinates: 8**M**, 1**S**, 1**m** and 6**A**.

Since the addition law is strongly unified, we use it as well for the doubling count

Coordinates / Operations	**M**	**S**	**m**	**A**	**I**
Affine	2	2	1	4	2
Projective	3	4	1	7	0
Inverted	3	4	1	7	0

Table A.2: Count of operations for doubling

A.3 Twisted Edwards curves

For the twisted Edwards curve $\mathbf{a}x^2 + y^2 = 1 + dx^2y^2$, the formulas are:

Affine coordinates

Affine coordinates:

$$x_3 = \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \quad y_3 = \frac{y_1y_2 - \mathbf{a}x_1x_2}{1 - dx_1x_2y_1y_2}$$

Projective coordinates

$$\begin{aligned} &A = Z_1Z_2;\ B = A^2;\ C = X_1X_2 \\ &D = Y_1Y_2;\ E = dCD;\ F = B - E;\ G = B + E \\ &X_3 = AF((X_1 + Y_1)(X_2 + Y_2) - C - D) && \text{(A.3.1)} \\ &Y_3 = AG(D - \mathbf{a}C) && \text{(A.3.2)} \\ &Z_3 = GF && \text{(A.3.3)} \end{aligned}$$

Inverted coordinates:

$$\begin{aligned} &A = Z_1Z_2;\ B = dA^2;\ C = X_1X_2;\ D = Y_1Y_2;\ E = CD; \\ &F = C - \mathbf{a}D;\ G = (X_1 + Y_1)(X_2 + Y_2) - C - D; \\ &X_3 = (E + B)F && \text{(A.3.4)} \\ &Y_3 = (E - B)G && \text{(A.3.5)} \\ &Z_3 = AFG && \text{(A.3.6)} \end{aligned}$$

Count of operations

Note that the formulas are almost the same as in a normal Edwards curve. Hence, the operations count (Tables A.1 and A.2) is the same, plus a multiplication by the constant **a** in case of a twisted curve.

Appendix B

The Edwards-Weierstrass race

[1]

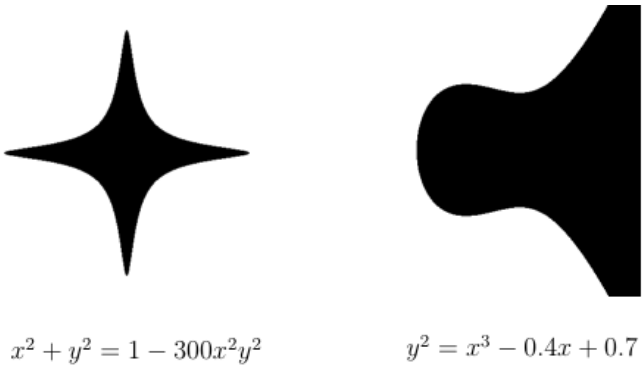

Figure B.1: Silhouttes of the competitors

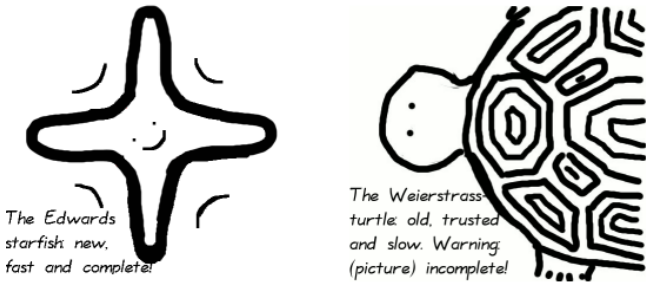

Figure B.2: Portraits of the competitors

[1] http://cr.yp.to/talks/2008.05.12/zoo.html

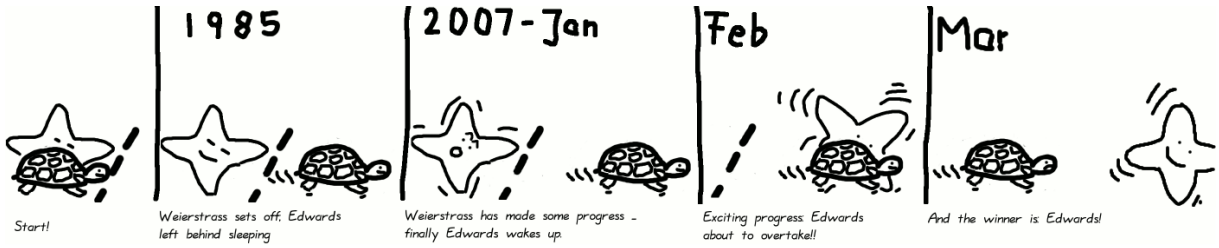

Figure B.3: The Edwards-Weierstrass race

Appendix C

Curves parameters

For Curve25519 in Montgomery form is $E : v^2 = u^3 + Au^2 + u$ (see. [10]):
The elliptic curve domain parameters are:

- $p = 2^{255} - 19$
- $A = 48662$
- $n = 2^{252} + 27742317777372353535851937790883648493$
- $h = 8$
- $u_G = 9$
- $v_G = 14781619447589544791020593568409986887264606134$
  $616475288964881837755586237401$

In hexadecimal format, the parameters are :

- $p =$0x7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFED
- $A =$0x76D06
- $n =$ 0x1000000000000000000000000000000014DEF9DEA2F79CD65812631A5CF5D3ED
- $h =$0x8
- $u_G =$ 0x9
- $v_G =$ 0x20AE19A1B8A086B4E01EDD2C7748D14C923D4D7E6D7C61B229E9C5A27ECED3D9

For the bi-rational mapping:

$$(u, v) = (\frac{1+y}{1-y}, \frac{\sqrt{-486664}u}{x})$$
$$(x, y) = (\frac{\sqrt{-486664}u}{v}, \frac{u-1}{u+1})$$

For the bi-rational mapping ϕ the $s = \sqrt{48664}$ is :

For Curve25519 in Edwards form : $E : x^2 + y^2 = 1 + dx^2y^2$
The elliptic curve domain parameters are:

- $p = 2^{255} - 19$
- $d = 37095705934669439343138083508754565189542113879843219016388785533085940283555$
- $n = 2^{252} + 27742317777372353535851937790883648493$
- $h = 8$
- $x_G = 15112221349535400772501151409588531511454012693041857206046113283949847762202$
- $y_G = 46316835694926478169428394003475163141307993866256225615783033603165251855960$

In hexadecimal format, the parameters are :

- $p =$0x7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFED
- $d =$0x2DFC9311D490018C7338BF8688861767FF8FF5B2BEBE27548A14B235ECA6874A
- $n =$ 0x1000000000000000000000000000000014DEF9DEA2F79CD65812631A5CF5D3ED
- $h =$0x8
- $x_G =$ 0x9
- $y_G =$ 0x20AE19A1B8A086B4E01EDD2C7748D14C923D4D7E6D7C61B229E9C5A27ECED3D9

For twisted Curve25519 in twisted Edwards form : $E : ax^2 + y^2 = 1 + dx^2y^2$

- $p =$0x7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFED
- $a =$ 0x7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEC
- $d =$ 0x52036CEE2B6FFE738CC740797779E89800700A4D4141D8AB75EB4DCA135978A3

Appendix D

Tonelli-Shanks algorithm

Theorem 2 (Euler's criterion)**.** *Let q be an odd prime and a an integer coprime to q. Then*

$$a^{\frac{q-1}{2}} \equiv \begin{cases} \quad 1 \pmod{q} \implies a \text{ is a square root} \\ -1 \pmod{q} \implies a \text{ is not a square root} \end{cases}$$

Proof. Since a is coprime to q, Fermat's little theorem implies that

$$\begin{aligned} a^{q-1} &\equiv 1 \pmod{q} \\ (a^{\frac{q-1}{2}} - 1)(a^{\frac{q-1}{2}} + 1) &\equiv 0 \pmod{q} \end{aligned}$$

hence, q divides $a^{\frac{q-1}{2}} - 1$ or q divides $a^{\frac{q-1}{2}} + 1$ (not both, otherwise q divides 2). If a is a square root, $\exists x / \, a \equiv x^2 \pmod{q}$, and then

$$\begin{aligned} a^{\frac{q-1}{2}} &\equiv x^{q-1} \pmod{q} \\ a^{\frac{q-1}{2}} &\equiv 1 \pmod{q} \quad \text{(Fermat's little theorem)} \end{aligned}$$

and thus q divides $a^{\frac{q-1}{2}} - 1$. □

The Tonelli–Shanks algorithm is used within modular arithmetic to solve for a congruence x of the form $x^2 \equiv a \pmod{q}$, where q is an odd prime. Since q id odd we can write $q - 1 = 2^s Q$ where Q is odd.
Let $R \equiv x^{\frac{Q+1}{2}} \pmod{q}$, we have then

$$R^2 \equiv x \times \underbrace{x^Q}_{t} \pmod{q}$$

if $t \equiv 1 \pmod{q}$ then we found R such that $x \equiv R^2 \pmod{q}$, otherwise:

$$\begin{cases} R^2 \equiv xt \pmod{q} \text{ and} \\ t \text{ is the } 2^{s-1}\text{-th root of } 1 \end{cases}$$

because $t^{2^{s-1}} \equiv x^{Q2^{s-1}} \equiv x^{\frac{q-1}{2}} \equiv 1 \pmod{q}$ according to Euler's criterion.
So taking successively the sqaure roots of t implies $t \equiv 1 \pmod{q}$ or otherwise $\exists k / t^{2^{s-k}} \equiv -1 \pmod{q}$. In the former case, we do not need to do anything as the same choice of R and t works. In latter case, we need to find a new pair (R, t); we can multiply R by a factor b, to be determined and t must be then multiplied by b^2 to keep $R^2 \equiv xt \pmod{q}$. Let for instance $t^{2^{s-2}} \equiv -1 \pmod{q}$, we need to find a factor b^2 so that tb^2 is a 2^{s-2}-th root of 1, i.e. $(tb^2)^{2^{s-2}} \equiv 1 \pmod{q}$ or equivalently $(b^2)^{2^{s-2}} \equiv -1 \pmod{q}$ since we said $t^{2^{s-2}} \equiv -1 \pmod{q}$. The trick here is to choose a known z which is not a square modulo q (e.g. $z = 2$) and apply Euler's criterion. Thus, $z^{\frac{q-1}{2}} \equiv (z^{\frac{Q}{2}})^{2^{s-2}} \equiv -1 \pmod{q}$ and hence $b \equiv z^Q \pmod{q}$.

Appendix E

Protocols and software using X25519 and Ed25519

- A list of protocols and software that use or support the superfast, super secure Curve25519 ECDH function from Dan Bernstein can be found in this page: `https://ianix.com/pub/curve25519-deployment.html`. Note that Curve25519 ECDH should be referred to as X25519.

- A list of protocols and software that use or support the Ed25519 public-key signature system from Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang can be found in this page: `https://ianix.com/pub/ed25519-deployment.html`.

These pages are divided by Protocols, Networks, Operating Systems, Hardware, Software, TLS Libraries, NaCl Crypto Libraries, Libraries, Miscellaneous, Timeline notes, and Support coming soon.