

# The Ristretto and Cortado elliptic curve groups

Mike Hamburg\*

January 14, 2018

**Abstract**

## 1 Introduction

## 2 Definitions and notation

Let the symbol  $\perp$  denote failure.

### 2.1 Field elements

Let  $\mathbb{F}$  be a finite field of prime order  $p$ . For an element  $x \in \mathbb{F}$ , let  $\text{res}(x)$  be the integer representative of  $x \in [0, p-1]$ . We call an element  $x \in \mathbb{F}$  *negative* if  $\text{res}(x)$  is odd. Call an element in  $\mathbb{F}$  *square* if it is a quadratic residue, i.e. if there exists  $\sqrt{x} \in \mathbb{F}$  such that  $\sqrt{x}^2 = x$ . There will in general be two such square roots; let the notation  $\sqrt{x}$  mean the unique non-negative square root of  $x$ . If  $p \equiv 1 \pmod{4}$ , then  $\mathbb{F}$  contains an element  $i := \sqrt{-1}$ .

Let  $\ell := \lceil \log_2 p \rceil$ . Each  $x \in \mathbb{F}$  has a unique *little-endian byte representation*, namely the sequence

$$\mathbb{F}\text{\_to\_bytes}(x) := \llbracket b_i \rrbracket_{i=0}^{\ell-1} \text{ where } b_i \in [0, 255] \text{ and } \sum_{i=0}^{\ell-1} 2^{8i} \cdot b_i = \text{res}(x)$$

**[[TODO: bytes to  $\mathbb{F}$ ]]**

---

\*Rambus Security Division

## 2.2 Groups

For an abelian group  $\mathbb{G}$  with identity  $O$ , let  $n\mathbb{G}$  denote the subgroup of  $\mathbb{G}$  which are of the form  $n \cdot g$  for some  $g \in \mathbb{G}$ . Let  $\mathbb{G}_n$  denote the  $n$ -torsion group of  $\mathbb{G}$ , namely the subgroup  $\{g \in \mathbb{G} : n \cdot g = O\}$ .

## 2.3 Edwards curves

We will work with twisted Edwards elliptic curves of the form

$$E_{a,d} : y^2 + a \cdot x^2 = 1 + d \cdot x^2 \cdot y^2$$

where  $x, y \in \mathbb{F}$ . Twisted Edwards curves have a group law

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

with identity point  $O := (0, 1)$  and group inverse operation

$$-(x, y) = (-x, y)$$

The group law is called *complete* if it produces the correct answer (rather than e.g.  $0/0$ ) for all points on the curve. The above formulas are complete when  $d$  and  $ad$  are nonsquare in  $\mathbb{F}$ , which implies that  $a$  is square. When these conditions hold, we also say that the curve itself is complete.

Let the number of points on the curve be

$$\#E_{a,d} = h \cdot q$$

where  $q$  is prime and  $h \in \{4, 8\}$ . We call  $h$  the *cofactor*.

For  $P = (x, y) \in E$ , we can define the *projective homogeneous form* of  $P$  as  $(X, Y, Z)$  with  $Z \neq 0$  and

$$(x, y) = (X/Z, Y/Z)$$

and the *extended homogeneous form* as  $(X, Y, Z, T)$  where additionally  $XY = ZT$ . Extended homogeneous form is popular because it supports simple and efficient complete addition formulas [?].

## 2.4 Montgomery curves

When  $a - d$  is square in  $\mathbb{F}$ , the twisted Edwards curve  $E_{a,d}$  is isomorphic to the Montgomery curve

$$v^2 = u \cdot \left( u^2 + 2 \cdot \frac{a+d}{a-d} \cdot u + 1 \right)$$

by the map

$$(u, v) = \left( \frac{1+y}{1-y}, \frac{1+y}{1-y} \cdot \frac{1}{x} \cdot \frac{2}{\sqrt{a-d}} \right)$$

with inverse

$$(x, y) = \left( \frac{u}{v} \cdot \frac{\sqrt{a-d}}{2}, \frac{u-1}{u+1} \right)$$

If  $M = (u, v)$  is a point on the Montgomery curve, then the  $u$ -coordinate of  $2M$  is  $(u^2 - 1)^2 / (4v^2)$  is necessarily square. It follows that if  $(x, y)$  is a point on  $E_{a,d}$ , and  $a - d$  is square, then  $(1+y)/(1-y)$  is also square.

Likewise, when  $d - a$  is square in  $\mathbb{F}$ ,  $E_{a,d}$  is isomorphic to the Montgomery curve

$$v^2 = u \cdot \left( u^2 - 2 \cdot \frac{a+d}{a-d} \cdot u + 1 \right)$$

by the map

$$(u, v) = \left( \frac{y+1}{y-1}, \frac{y+1}{y-1} \cdot \frac{1}{x} \cdot \frac{2}{\sqrt{d-a}} \right)$$

with inverse

$$(x, y) = \left( \frac{u}{v} \cdot \frac{\sqrt{d-a}}{2}, \frac{1+u}{1-u} \right)$$

## 3 Lemmas

First, we characterize the 2-torsion and 4-torsion groups.

**Lemma 1.** *Let  $E_{a,d}$  be a complete Edwards curve. Its 2-torsion subgroup is generated by  $(0, -1)$ . The 4-torsion subgroup is generated by  $(1/\sqrt{a}, 0)$ .*

*Adding the 2-torsion generator to  $(x, y)$  produces  $(-x, -y)$ . Adding the 4-torsion generator  $(1/\sqrt{a}, 0)$  produces  $(y/\sqrt{a}, -x \cdot \sqrt{a})$*

*Proof.* Inspection. □

**Lemma 2.** *Let  $E_{a,d}$  be a complete twisted Edwards curve over  $\mathbb{F}$ , and  $P_1 = (x_1, y_1)$  be any point on it. Then there are exactly two points  $P_2 = (x_2, y_2)$  satisfying  $x_1y_2 = x_2y_1$ , namely  $P_1$  itself and  $(-x_1, -y_1)$ . That is, there are either 0 or 2 points on any line through the origin.*

*Proof.* Plugging into the group operation gives

$$x_1y_2 = x_2y_1 \iff P_1 - P_2 = (0, y_3)$$

for some  $y_3$ . Plugging  $x = 0$  into the curve equation gives  $y = \pm 1$ , the 2-torsion points. Adding back, we have  $P_2 = P_1 + (0, \pm 1) = (\pm x_1, \pm y_1)$  as claimed. □

**Lemma 3.** *If  $E_{a,d}$  is a complete Edwards curve, then  $a^2 - ad$  is square in  $\mathbb{F}$  (and thus  $a - d$  is square in  $\mathbb{F}$ ) if and only if the cofactor of  $E_{a,d}$  is divisible by 8.*

*Proof.* Doubling an 8-torsion generator  $(x, y)$  should produce a 4-torsion generator, i.e. a point with  $y = 0$ . From the doubling formula, this happens precisely when  $y^2 = ax^2$ , or  $2ax^2 = 1 + adx^4$ . This has roots in  $\mathbb{F}$  if and only if its discriminant  $4a^2 - 4ad$  is square, so that  $a^2 - ad$  is square. □

**Lemma 4.** *If  $(x_2, y_2) = 2 \cdot (x_1, y_1)$  is an even point in  $E_{a,d}$ , then  $(1 - ax_2^2)$  is a quadratic residue in  $\mathbb{F}$ . [TODO:  $(y_2^2 - 1)$ ]*

*Proof.* The doubling formula has

$$x_2 = \frac{2x_1y_1}{y_1^2 + ax_1^2}$$

so that

$$1 - ax_2^2 = \left( \frac{y_1^2 - ax_1^2}{y_1^2 + ax_1^2} \right)^2$$

is a quadratic residue. Now for any point  $(x, y) \in E_{a,d}$ , we have

$$(y^2 - 1) \cdot (1 - ax^2) = y^2 + ax^2 - 1 - ax^2y^2 = (d - a)x^2y^2$$

which is a quadratic residue by Lemma 3. □

## 4 The Espresso groups

Let  $E$  be a complete twisted Edwards curve with  $a \in \{\pm 1\}$  and cofactor 4 or 8. We describe the *Espresso* group  $\mathbb{G}(E)$  as

$$\text{Espresso}(E) := 2E/E_{h/2}$$

This group has prime order  $q$ .

### 4.1 Group law

The group law on  $\text{Espresso}(E)$  is the same as that on  $E$ .

### 4.2 Equality

Two elements  $P_1 := (x_1, y_1)$  and  $P_2 := (x_2, y_2)$  in  $\text{Espresso}(E)$  are equal if they differ by an element of  $E_{h/2}$ .

If  $h = 4$ , the points are equal if  $P_1 - P_2 \in E_2$ . By Lemma 2, this is equivalent to

$$x_1y_2 = x_2y_1$$

If  $h = 8$ , the points are equal if  $P_1 - P_2 \in E_4$ . By Lemmas 1 and 2, this is equivalent to

$$x_1y_2 = x_2y_1 \quad \text{or} \quad x_1x_2 = -ay_1y_2$$

These equations are homogeneous, so they may be evaluated in projective homogeneous form with  $X_i$  and  $Y_i$  in place of  $x_i$  and  $y_i$

### 4.3 Encoding

We now describe how to encode a point  $P = (x, y)$  to bytes. The requirements of encoding are that

- Any point  $P \in 2E$  can be encoded.
- Two points  $P, Q$  have the same encoding if and only if  $P - Q \in E_{h/2}$ .

When  $h = 4$ , we encode a point as  $\sqrt{a(y-1)/(y+1)}$