Curve Ed25519 in tchat

tworks@tutamail.com

March 1, 2025

Contents

1 Notes

tchat is a beginner project. The document contains only aspects of elliptic curves, security discussions and constant time implementations be missing. The cryptographic functions used in **tchat** are more complex [1]. If you find mistakes or bad code, please write an email or open an issue.

2 Some Basic Algebra

2.1 Groups

2.1 Definition (semigroup)**.**
Let G be a set. Let

$$\star : G \times G \to G, (g,h) \mapsto g \star h$$

be a map with the following conditions:

(S1) for all $f, g, h \in G$, $f \star (g \star h) = (f \star g) \star h$

(S2) there is a $e \in G$ such that for all $g \in G$, $e \star g = g$

[1] See crypto/src/lib.rs.

(S3) for all $g, h \in G$, $g \star h = h \star g$

Then the tupel $(G, \star)$ is called **semigroup**.

2.2 Lemma.

(a) Let $(G, \star)$ be a group. Let $e \in G$ such that for all $g \in G$, $e \star g = g$. Let $\tilde{e} \in G$ such that for all $g \in G$, $\tilde{e} \star g = g$. Then $\tilde{e} = e$.

(b) Let $(G, \star)$ be a group. Let $e \in G$ such that for all $g \in G$, $e \star g = g$. Let $g, h, \tilde{h} \in G$ with $h \star g = e$ and $\tilde{h} \star g = e$. Then $h = \tilde{h}$.

Proof.

(a) $\tilde{e} = e \star \tilde{e} = \tilde{e} \star e = e$

(b) $h = h \star e = h \star (g \star \tilde{h}) = (h \star g) \star \tilde{h} = e \star \tilde{h} = \tilde{h}$

□

2.3 Definition.
Let $(G, \star)$ be a semigroup. Let $e \in G$ such that for all $g \in G$, $e \star g = g$. Then $e_G := e$ is called the **identity element** of $(G, \star)$. Let $g, h \in G$ with $h \star g = e_G$ then $g^{-1} := h$ is called the **inverse** of g in $(G, \star)$.

2.4 Lemma.
Let $(G, \star)$ be a semigroup. Let $n \in \mathbb{N}$ with $n \geq 3$. Then for all $g_1, \ldots, g_n$ all brackets of the product $g_1 \star \ldots \star g_n$ give the same element.

Proof. Induction: $n = 3$ is (S1). Let $n > 3$. For $1 \leq i < j < n$, it is to show that

$$(g_1 \star \ldots \star g_i) \star (g_{i+1} \star \ldots \star g_n) = (g_1 \star \ldots \star g_j) \star (g_{j+1} \star \ldots \star g_n)$$

This follows by (S1):

$$\begin{aligned}(g_1 \star \ldots \star g_i) \star (g_{i+1} \star \ldots \star g_n) &= (g_1 \star \ldots \star g_i) \star ((g_{i+1} \star \ldots \star g_j) \star (g_{j+1} \star \ldots \star g_n)) \\ &= ((g_1 \star \ldots \star g_i) \star (g_{i+1} \star \ldots \star g_j)) \star (g_{j+1} \star \ldots \star g_n) \\ &= (g_1 \star \ldots \star g_j) \star (g_{j+1} \star \ldots \star g_n)\end{aligned}$$

□

2.5 Definition (group)**.**
Let G be a set. Let

$$\star : G \times G \to G, (g, h) \mapsto g \star h$$

be a map such that

(G1) $(G, \star)$ is a semigroup

(G2) for all $g \in G$, there exists the inverse of g in $(G, \star)$

Then the tupel $(G, \star)$ is called **group**.

2.6 Remark.
In Group Theory (S3) is not contained in the definition of a semigroup and group. All semigroups and groups in this paper satisfy (S3) so it is included in these definitions.

2.7 Corollary.
Let $(G, \star)$ be a semigroup. Set $G^* := \{g \in G \mid \text{there is } g^{-1} \in G\}$. Then

$$\bullet : G^* \times G^* \to G^*, (g, h) \mapsto g \star h$$

is well defined and $(G^*, \bullet)$ is a group with $e_{G^*} = e_G$ and for all $g \in G^*$, the inverse of g in $(G^*, \bullet)$ is the inverse of g in $(G, \star)$.

Proof. $G^* \times G^* \to G^*, (g,h) \mapsto g \star h$ is well defined:
For all $g, h \in G^*$, $g \star h$ is in G^*, since

$$(h^{-1} \star g^{-1}) \star (g \star h) = h^{-1} \star (g^{-1} \star (g \star h)) = h^{-1} \star ((g^{-1} \star g) \star h) = h^{-1} \star h = e_G.$$

So $g \star h \in G^*$.
$(G^*, \bullet)$ is a semigroup:

(S1) $f \bullet (g \bullet h) = f \star (g \star h) = (f \star g) \star h = (f \bullet g) \bullet h$

(S2) the identity element of G is in G^*, since ${e_G}^{-1} = e_G$. Then by definition of $\bullet$, $e_{G^*} = e_G$.

(S2) $g \bullet h = g \star h = h \star g = h \bullet g$.

$(G^*, \bullet)$ satisfies (G2), since for all $g \in G^*$, the inverse element of g in $(G^*, \bullet)$ is the inverse element of g in $(G, \star)$ by definition of $(G^*, \bullet)$. □

2.8 Definition (subgroup)**.**
Let $(G, \star)$ be a group. A non-empty set $H \subset G$ is called **subgroup** of $(G, \star)$, if the following hold.

(SG1) for all $g, h \in H$, $g \star h \in H$

(SG2) for all $h \in H$, $h^{-1} \in H$

2.9 Corollary.
Let H be a subgroup of $(G, \star)$. Then

$$\bullet : H \times H \to H, (g,h) \mapsto g \star h$$

is well defined and $(H, \bullet)$ is a group with $e_H = e_G$ and for all $h \in H$, the inverse of h in $(H, \bullet)$ is the inverse of h in $(G, \star)$.

Proof. From (SG1) follows $\bullet$ is well defined.
$(H, \bullet)$ satisfying conditions (G1) and (G2):
$(H, \bullet)$ is a semigroup:

(S1) $f \bullet (g \bullet h) = f \star (g \star h) = (f \star g) \star h = (f \bullet g) \bullet h$

(S2) Since H is non-empty, there exists $h \in H$. By (SG2) there exists $h^{-1} \in H$. With (SG1) follows $e_G = h^{-1} \star h \in H$. So for all $h \in H$, $e_G \bullet h = e_G \star h = h$. So $e_H = e_G$

(S3) $g \bullet h = g \star h = h \star g = h \bullet g$.

$(H, \bullet)$ satisfies (G2):
For all $h \in H$, there exists the inverse of h in $(H, \bullet)$:
By (SG2) for all $h \in H$, the inverse of h in $(G, \star)$ is an element of H. With $h^{-1} \bullet h = h^{-1} \star h = e_G = e_H$ follows h^{-1} is the inverse of h in $(H, \bullet)$. □

2.10 Definition.
Let $(G, \star)$ be a group. Set for all $n \in \mathbb{N}$,

$$g^n := g \star g^{n-1},$$
$$g^{-n} := (g^{-1})^n$$

and set

$$g^0 := e_G$$

2.11 Corollary.
Let $(G, \star)$ be a group. Then for all $n, m \in \mathbb{N}$,

$$g^m \star g^{-n} = g^{m-n}$$

and

$$(g^m)^n = g^{nm}.$$

Proof.
$$g^m \star g^{-n} = g^m \star (g^{-1})^n = g^{m-n}$$
□

2.1.1 Finite Groups

2.12 Definition (finite group)**.**
Let $(G, \star)$ be a group. $(G, \star)$ is called **finite** if G is a finite set.

2.13 Definition.
Let A be a non-empty finite set. Then $|A|$ is the number of elements in A.

2.14 Theorem (Fermat's little theorem)**.**
Let $(G, \star)$ be a finite group with $|G| = n$. Then for all $g \in G$, $g^{-1} = g^{n-1}$.

Proof. Let $g \in G$. The map $\phi : G \to G, h \mapsto g \star h$ is a bijection, since $G \to G, h \mapsto g^{-1} \star h$ is the inverse. Let $g_1, \ldots, g_n \in G$ such that $G = \{g_1, \ldots, g_n\}$. Since ϕ is a bijection, $\{g_1, \ldots, g_n\} = \{g \star g_1, \ldots, g \star g_n\}$. Then
$$h := g_n \star \ldots \star g_1 = (g \star g_n) \star \ldots \star (g \star g_1) = g^n \star g_n \star \ldots \star g_1 = g^n \star h.$$
This is equivalent to
$$g^{n-1} \star g = g^n = e_G$$
□

2.15 Corollary.
Let $(G, \star)$ be a finite group. Then for all $g \in G$, $g^{|G|} = e_G$.

2.16 Definition (order)**.**
Let $(G, \star)$ be a finite group. Then for all $g \in G$,
$$\mathrm{ord}_G(g) := \min\{n \in \mathbb{N} \mid g^n = e_G\}$$
is called **order** of g.

2.17 Corollary.
Let $(G, \star)$ be a finite group. Then for all $g \in G$,
$$\mathrm{ord}_G(g) \leq |G|.$$

2.18 Theorem.
Let $(G, \star)$ be a finite group. Then for all $g \in G$, $\mathrm{ord}_G(g)$ divides $|G|$, that is there is a $q \in \mathbb{N}$ such that
$$|G| = q \,\mathrm{ord}_G(g).$$

Proof. Assume there are $q, r \in \mathbb{N}$, $1 \leq r < \mathrm{ord}_G(g)$ such that
$$|G| = q \,\mathrm{ord}_G(g) + r$$
Then
$$g^r = g^{|G| - q \,\mathrm{ord}_G(g)} = g^{|G|} \star g^{-q \,\mathrm{ord}_G(g)} = g^{|G|} \star (g^{\mathrm{ord}_G(g)})^{-q} = e_G \star (e_G)^{-q} = e_G \star ({e_G}^{-1})^q = e_G.$$
This is a contradiction, since $r < \mathrm{ord}_G(g) = \min\{n \in \mathbb{N} \mid g^n = e_G\}$. □

2.19 Definition.
Let $(G, \star)$ be a finite group. Let $g \in G$. Set
$$\langle g \rangle := \{g, g^2, \ldots, g^{\mathrm{ord}_G(g)}\}$$

2.20 Corollary.
Let $(G, \star)$ be a finite group. Then for all $g \in G$, $\langle g \rangle \subset G$ is a subgroup.

Proof. $\langle g \rangle \subset G$ satisfies (SG1) and (SG2):

(SG1) Let $i, j \in \{1, \ldots, \operatorname{ord}_G(g)\}$. Case $i + j \leq \operatorname{ord}_G(g)$:

$$g^i \star g^j = g^{i+j} \in \langle g \rangle.$$

Case $\operatorname{ord}_G(g) < i + j \leq 2 \operatorname{ord}_G(g)$: $i + j = \operatorname{ord}_G(g) + k$ with $1 \leq k \leq \operatorname{ord}_G(g)$. Then

$$g^i \star g^j = g^{i+j} = g^{\operatorname{ord}_G(g)+k} = g^{\operatorname{ord}_G(g)} \star g^k = e_G \star g^k = g^k \in \langle g \rangle.$$

(SG2) Case $i = \operatorname{ord}_G(g)$: Then

$$g^i \star g^i = e_G \star e_G = e_G.$$

Case $i \in \{1, \ldots, \operatorname{ord}_G(g) - 1\}$: Then $1 < \operatorname{ord}_G(g) - i < \operatorname{ord}_G(g)$. So

$$g^{\operatorname{ord}_G(g)-i} \star g^i = g^{\operatorname{ord}_G(g)} = e_G.$$

□

2.21 Definition (cyclic group, generator)**.**
Let $(G, \star)$ be a finite group. $(G, \star)$ is called **cyclic**, if there is a $g \in G$ such that $G = \langle g \rangle$. Then g is called **generator** of G.

2.2 Rings

2.22 Definition (ring)**.**
Let R be a set. Let

$$+ : R \times R \to R$$

and

$$\cdot : R \times R \to R$$

be maps such that

(R1) $(R, +)$ is a group

(R2) $(R, \cdot)$ is a semigroup

(R3) for all $w, x, y \in R$, $w \cdot (x + y) = w \cdot x + w \cdot y$

Then the tripel $(R, +, \cdot)$ is called **ring**. The identity element of $(R, +)$ is denoted 0_R and for all $x \in R$ the inverse of x in $(R, +)$ is denoted $-x$. The identity element of $(R, \cdot)$ is denoted 1_R. If there are $x, y \in R$ with $x \cdot y = 1_R$ then y is denoted x^{-1}. Further set $R^* := \{x \in R \mid \text{There is } x^{-1} \in R\}$. Denote the map $R^* \times R^* \to R^*, (x, y) \mapsto x \cdot y$ with $\cdot$ again.

2.23 Corollary.
Let $(R, +, \cdot)$ be a ring. Then $(R^*, \cdot)$ is a group.

Proof. Corollary 2.7. □

2.24 Lemma.
Let $z \in \mathbb{Z}$ and let $q \in \mathbb{N}$. Then there are $r \in \mathbb{Z}$ and $0 \leq \varphi < q$ such that

$$z = rq + \varphi.$$

r and φ are uniquely determined by z and q.

Proof. Let $z = rq + \varphi = r'q + \varphi'$ with $\varphi' \leq \varphi$. Then $(r - r')q + \varphi - \varphi' = 0$. Assume $r - r' \neq 0$: Since $0 \leq \varphi - \varphi' < q$ this is a contradiction, so $r - r' = 0$. So $\varphi - \varphi' = 0$. $\square$

2.25 Definition.

(a) Let $q \in \mathbb{N}$ and let $z \in \mathbb{Z}$. You say q **divides** z and write $q|z$ if $z = rq$ for $r \in \mathbb{Z}$.

(b) For $q \in \mathbb{N}$ define the set
$$\mathbb{Z}_q := \{0, 1, \ldots, q-1\}$$

(c) For $q \in \mathbb{N}$ define the map
$$\varphi_q(z) : \mathbb{Z} \to \mathbb{Z}_q, z \mapsto z \mod q$$
by $z = rq + \varphi_q(z)$ with $r \in \mathbb{Z}$, and $0 \leq \varphi_q(z) < q$.

2.26 Corollary.
Let $q \in \mathbb{N}$.

(a) For all $x, y \in \mathbb{Z}$,
$$\varphi_q(x) = \varphi_q(y) \Leftrightarrow q \mid y - x.$$

(b) For all $x \in \mathbb{Z}$,
$$q|x - \varphi_q(x).$$

Proof. (a) "$\Rightarrow$": Write $x = rq + \varphi$ and $y = r'q + \varphi$ then $y - x = (r' - r)q$ so $q \mid y - x$.
"$\Leftarrow$": Write $x = rq + \varphi$ and $y = r'q_{\text{¸}} + \varphi'$. Without loss of generality $\varphi' - \varphi \geq 0$. So $0 \leq \varphi' - \varphi < q$ and
$$y - x = (r' - r)q + \varphi' - \varphi$$
Since $q \mid y - x$ and by Lemma 2.24 follows $\varphi = \varphi'$. $\square$

2.27 Definition and Lemma (ring of integers modulo q)**.**
Let $q \in \mathbb{N}$ with $q > 1$. Then $(\mathbb{Z}_q, +_q, \cdot_q)$ where
$$+_q : \mathbb{Z}_q \times \mathbb{Z}_q \to \mathbb{Z}_q, (x, y) \mapsto (x + y) \mod q$$
and
$$\cdot_q : \mathbb{Z}_q \times \mathbb{Z}_q \to \mathbb{Z}_q, (x, y) \mapsto (x \cdot y) \mod q$$
is a ring, which is called **ring of integers modulo** q.

Proof. $(\mathbb{Z}_q, +_q)$ is a group with identity element $0 \mod q$ and for all $x \in \mathbb{Z}_q$, $-x = -x \mod q$: $(\mathbb{Z}_q, +_q)$ satisfies (S1) follows from
$$(x +_q y) +_q z = ((x + y) \mod q + z) \mod q = \varphi_q(\varphi_q(x + y) + z) \overset{(*)}{=} \varphi_q(x + y + z) = (x + y + z) \mod q$$
Proof $(*)$: $q|x + y - \varphi_q(x + y) \Leftrightarrow q|x + y + z - (\varphi_q(x + y) + z)$
$(\mathbb{Z}_q, \cdot_q)$ is a semigroup with identity element 1: $(\mathbb{Z}_q, +_q)$ satisfies (S1) follows from
$$(x \cdot_q y) \cdot_q z = ((x \cdot y) \mod q \cdot z) \mod q = \varphi_q(\varphi_q(x \cdot y) \cdot z) \overset{(**)}{=} \varphi_q(x \cdot y \cdot z) = (x \cdot y \cdot z) \mod q$$
Proof $(**)$: $q|x \cdot y - \varphi_q(x \cdot y) \Leftrightarrow q|x \cdot y \cdot z - \varphi_q(x \cdot y) \cdot z$
$(\mathbb{Z}_q, +_q, \cdot_q)$ satisfies (R3):
$$x \cdot_q (y +_q z) = \varphi_q(x \cdot (y +_q z) \overset{(***)}{=} \varphi_q(x \cdot (y + z)) = \varphi_q(x \cdot y + x \cdot z) = \varphi_q(x \cdot y) +_q \varphi_q(x \cdot z) = x \cdot_q y +_q x \cdot_q z$$
Proof $(***)$: $q \mid y + z - \varphi_q(y + z) \Leftrightarrow q \mid x(y + z) - x \cdot \varphi_q(y + z)$ $\square$

2.3 Fields

2.28 Definition (field)**.**
Let $(R,+,\cdot)$ be a ring with $0_R \neq 1_R$ and $R^* = R \setminus \{0_R\}$. Then $(R,+,\cdot)$ is called **field**.

2.29 Theorem.
Let p be a prime number. Then $\mathbb{Z}_p{}^\star = \mathbb{Z}_p \setminus \{0\}$. So $(\mathbb{Z}_p,+,\cdot)$ is a field.

Proof. Since $1 \in \mathbb{Z}_p{}^\star$ it is to show that for all $x \in \{2,\dots,p-1\}$ there is an inverse x^{-1} in $(\mathbb{Z}_p,\cdot_p)$:
For all $k \in \mathbb{N}_0$, $(x \mod p)^k = x^k \mod p \neq 0$ because $x^0 = 1$ by definition and for $k > 0$

$$x^k \mod p = 0 \Leftrightarrow x^k = rp \text{ for } r \in \mathbb{Z} \Rightarrow p|x^k \Rightarrow p|x \Rightarrow \text{ contradiction to } x < p$$

So $\{x^0 \mod p, \dots, x^{p-1} \mod p\}$ contains an element that occurs twice:

$$x^{k_1} \mod p = x^{k_2} \mod p, k_1 < k_2$$

So there is a $z \in \mathbb{Z}$ such that

$$x^{k_2} - x^{k_1} = pz \Leftrightarrow x^{k_1}x^{k_2-k_1} - x^{k_1} = pz \Leftrightarrow x^{k_2-k_1} = 1 + p\frac{z}{x^{k_1}}$$

$n := \frac{z}{x^{k_1}} \in \mathbb{N}$, since x^{k_1} divides pz and $x < p$. So

$$x^{k_2-k_1-1}x = 1 + np \Leftrightarrow x^{-1} = x^{k_2-k_1-1} \mod p.$$

□

2.30 Definition.
Let p be a prime number. Then set $\mathbb{F}_p := \mathbb{Z}_p$.

2.31 Lemma.
Let p be a prime number. Then for all $x \in \mathbb{F}_p{}^*$,

$$x^{-1} = x^{p-2} \mod p.$$

Proof. Lemma 2.14. □

2.32 Definition.
Let $p > 2$ be a prime number. Define

$$r_p : \mathbb{Z} \to \left\{-\frac{p-1}{2},\dots,\frac{p-1}{2}\right\}, z \mapsto \begin{cases} \varphi_p(z) & \text{for } 0 \leq \varphi_p(z) \leq \frac{p-1}{2} \\ \varphi_p(z) - p & \text{for } \frac{p+1}{2} \leq \varphi_p(z) \leq p-1 \end{cases}$$

2.33 Theorem (Gauss Lemma)**.**
Let $p > 2$ be a prime number. Let $\gcd(a,p) = 1$. Set

$$\mu := |\{1 \leq j \leq \frac{p-1}{2} \mid r_p(ja) < 0\}|.$$

Then

$$a^{\frac{p-1}{2}} \mod p = -1^\mu \mod p.$$

Proof. Set $P := \{1,\dots,\frac{p-1}{2}\}$ and $r := r_p$. Claim: The map $P \to P, j \mapsto |r(ja)|$ is injective and so bijective.
Proof of the claim: Let $i,j \in P$ with $|r(ia)| = |r(ja)|$. Then $r(ia) = r(ja)$ or $r(ia) = -r(ja)$. The latter is not possible, since

$$ia \mod p = r(ia) \mod p = -r(ja) \mod p = -ja \mod p$$

and so $(i+j)a \mod p = 0$. So $p|(i+j)a$ but $2 \leq i+j \leq p-1$ and $\gcd(a,p) = 1$.
With

$$ia \mod p = r(ia) \mod p = r(ja) \mod p = -ja \mod p$$

follows $(i-j)a \mod p = 0$. So $p|(i-j)a \Rightarrow p|(i-j) \Rightarrow i=j$. The last implication follows from $|i-j|<p$. Remark: If $r(ja)<0$ then $r(ja) = -|r(ja)|$ and if $r(ja)>0$ then $r(ja) = |r(ja)|$. Finally

$$\prod_{j=1}^{(p-1)/2} r(ja) = (-1)^\mu \prod_{j=1}^{(p-1)/2} |r(ja)| = (-1)^\mu \prod_{j=1}^{(p-1)/2} j$$

and

$$\left(\prod_{j=1}^{(p-1)/2} r(ja)\right) \mod p = \left(\prod_{j=1}^{(p-1)/2} ja\right) \mod p = \left(a^{\frac{p-1}{2}} \prod_{j=1}^{(p-1)/2} j\right) \mod p$$

It follows:

$$\left(a^{\frac{p-1}{2}} \prod_{j=1}^{(p-1)/2} j\right) \mod p = \left(\prod_{j=1}^{(p-1)/2} r(ja)\right) \mod p = \left((-1)^\mu \prod_{j=1}^{(p-1)/2} j\right) \mod p$$

The Gauss Lemma follows from

$$\left(\prod_{j=1}^{(p-1)/2} j\right) \mod p \in \mathbb{F}_p^*,$$

since $j \mod p \in \mathbb{F}_p^*$ □

2.34 Lemma.
Let p be a prime number with $p = 5+8k$ for $k \in \mathbb{N}$. Then $[2^{\frac{p-1}{2}}]_p = [-1]_p$.

Proof. By Gauss Lemma: $\left[2^{\frac{p-1}{2}}\right]_p = [(-1)^\mu]_p$. With $p = 5+8k$ for $k \in \mathbb{N}$ follows

$$\begin{aligned}\mu &= |\{1 \le j \le \frac{p-1}{2} \mid r(2j) < 0\}| = |\{1 \le j \le \frac{p-1}{2} \mid \frac{p+1}{2} \le 2j \le p-1\}| \\ &= |\{1 \le j \le \frac{p-1}{2} \mid \frac{p+1}{4} \le j \le \frac{p-1}{2}\}| = |\{1 \le j \le 2+4k \mid \frac{3}{2} + 2k \le j \le 2+4k\}| \\ &= |\{1 \le j \le 2+4k \mid 2+2k \le j \le 2+4k\}| = 2+4k-(1+2k) = 1+2k.\end{aligned}$$

So μ is odd. □

2.35 Lemma.
Let p be a prime number with $p \mod 8 = 5$. Let $a \in \mathbb{F}_p$ be a square. Let $I = 2^{(p-1)/4} \mod p$. Then either $a = x^2 \mod p$, where $x = \pm a^{(p+3)/8} \mod p$ or $a = x^2$, where $x = \pm I a^{(p+3)/8} \mod p$.

Proof. Let $z \in \mathbb{F}_p$ with $a = z^2 \mod p$ and let $p = 5+8k$ for $k \in \mathbb{N}$. Set $d := a^{(p-1)/4} \mod p$. Then $d^2 \mod p = a^{(p-1)/2} \mod p = z^{p-1} \mod p = 1$. So $d = 1$ or $d = -1 \mod p$.
Case $d = 1$:

$$1 = a^{(p-1)/4} \mod p = a^{2k+1} \mod p \Rightarrow a^{2k+2} \mod p = a \Rightarrow z = \pm a^{k+1} \mod p = \pm a^{(p+3)/8} \mod p$$

Case $d = -1 \mod p$:

$$\begin{aligned}-1 \mod p = a^{(p-1)/4} \mod p = a^{2k+1} \mod p &\Rightarrow a = -a^{2k+2} \mod p \\ &\Rightarrow z = \pm I a^{k+1} \mod p = \pm I a^{\frac{p+3}{8}} \mod p,\end{aligned}$$

where $I^2 = -1 \mod p$ by Lemma 2.34. □

2.36 Definition.

(a) Let $\mathbb{F}$ be a field. For all $v, w \in \mathbb{F}$ with $w \neq 0$ set

$$\frac{v}{w} := v \cdot w^{-1}.$$

(b) Let p be a prime number. For all $x, y \in \mathbb{Z}$ with $y \mod p \neq 0$. Set

$$\frac{x}{y} \mod p := (x \mod p) \cdot_p (y \mod p)^{-1}$$

2.37 Definition (square)**.**
Let $\mathbb{F}$ be a field. $v \in \mathbb{F}$ is called **square** if there is a $x \in \mathbb{F}$ with

$$v = x^2.$$

3 Cryptography

3.1 Twisted Edwards Curves

3.1 Definition.
Let $\mathbb{F}$ be a field. Let $a, d \in \mathbb{F}$. Then set

$$E_{a,d} := \{(x, y) \in \mathbb{F} \times \mathbb{F} \mid ax^2 + y^2 = 1 + dx^2y^2\} \tag{1}$$

$E_{a,d}$ is called (a, d)-**Twisted Edwards curve** over $\mathbb{F}$.

3.2 Theorem.
Let $\mathbb{F}$ be a field. Let $a \in \mathbb{F}$ be a square and let $d \in \mathbb{F}$ be no square. Then the map

$$\oplus : E_{a,d} \times E_{a,d} \to E_{a,d}$$

given by

$$(x_1, y_1) \oplus (x_2, y_2) := \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right)$$

is well defined. Further $(E_{a,d}, \oplus)$ is a group with identity element $(0, 1)$ and for all $(x, y) \in E_{a,d}$

$$(x, y)^{-1} = (-x, y).$$

Proof. Appendix □

3.1.1 Curve Ed25519

3.3 Lemma.
Let $p = 2^{255} - 19$. Then $a = -1 \mod p \in \mathbb{F}_p$ is a square and $d = -\frac{121665}{121666} \mod p \in \mathbb{F}_p$ is no square.

Proof. With $p - 5 = 2^{255} - 24 = 8 \cdot (2^{252} - 3)$ is $p = 5 + 8k$ for $k \in \mathbb{N}$.
a is a square: By Lemma 2.34

$$2^{2^{254}-10} \mod p = -1 \mod p.$$

So $-1 \mod p = v^2$ with $v = 2^{2^{253}-5} \mod p$.
d is no square: Let $b = d^{(p+3)/4}$. You can calculate (for example with python) that $d \neq b$ and $d \neq -b$. Then by Lemma 2.35 follows d is no square. □

3.4 Definition (Curve Ed25519)**.**
Let $p = 2^{255} - 19$, let $a = -1 \mod p \in \mathbb{F}_p$ and let $d = -\frac{121665}{121666} \mod p \in \mathbb{F}_p$. The (a, d)-Twistet Edwards curve over $\mathbb{F}_p$ is called **Curve Ed25519**. We set

$$E := E_{a,d}.$$

3.5 Definition.
Let $k \in \mathbb{N}$. Set $\mathrm{U}k := \{0, 1, \ldots, 2^k - 1\}$

3.6 Definition and Lemma (binary representation, binary expansion)**.**

(a) Let $n \in \mathrm{U}k$, then
$$n = \sum_{i=0}^{k-1} \varepsilon_i 2^i$$
with
$$(\varepsilon_0, \ldots, \varepsilon_{k-1}) \in \{0,1\}^k.$$
$(\varepsilon_0, \ldots, \varepsilon_{k-1})$ is called **binary representation** of n. Further the binary representation of n is unique.

(b) Let
$$(\varepsilon_0, \ldots, \varepsilon_{k-1}) \in \{0,1\}^k.$$
Then
$$\sum_{i=0}^{k-1} \varepsilon_i 2^i \in \mathrm{U}k.$$
$\sum_{i=0}^{k-1} \varepsilon_i 2^i$ is called **binary expansion** from $(\varepsilon_0, \ldots, \varepsilon_{k-1})$

3.7 Definition.

(a) Set
$$\mathrm{bit}_{\min} : \mathbb{N} \to \{0,1\}, n \mapsto n \mod 2.$$

(b) For all $k \in \mathbb{N}$ set
$$\mathrm{bit}_{\max}^k : \mathrm{U}k \to \{0,1\}, \sum_{i=0}^{k-1} \varepsilon_i 2^i \mapsto \varepsilon_{k-1},$$
with $(\varepsilon_0, \ldots, \varepsilon_{k-1}) \in \{0,1\}^k$.

Protocol 1 Scalarmult

Inputs. $n \in \mathbb{N}_0$, $P \in E$.

The protocol:

1. If $n = 0$ return $(0,1) \in E$.
2. Compute $Q = \mathsf{Scalarmult}((n - \mathrm{bit}_{\min}(n))/2, P)$.
3. Compute $R = Q \oplus Q$.
4. If $\mathrm{bit}_{\min}(n) = 0$ return $S = R$, else return $S = P \oplus R$.

Outputs. $S \in E$

3.8 Lemma.
Let $n \in \mathbb{N}_0$ and let $P \in E$. Then,
$$\mathsf{Scalarmult}(n, P) = P^n =: nP$$
Further the recursive protocol needs $\lfloor \log_2(n) \rfloor + 1$ cycles.

Proof. Let $k \in \mathbb{N}$ such that $n = \sum_{i=0}^{k-1} \varepsilon_i 2^i$ with $\varepsilon_i \in \{0,1\}$ for all $0 \le i < k$. Set $S_0 := \mathsf{Scalarmult}(n, P)$, then
$$\begin{aligned}
S_0 &= \varepsilon_0 P \oplus 2S_1, \text{ with } S_1 := \mathsf{Scalarmult}\left(\sum_{i=1}^{k-1} \varepsilon_i 2^{i-1}, P\right), \\
S_1 &= \varepsilon_1 P \oplus 2S_2, \text{ with } S_2 := \mathsf{Scalarmult}\left(\sum_{i=2}^{k-1} \varepsilon_i 2^{i-2}, P\right), \\
&\vdots \\
S_{k-2} &= \varepsilon_{k-2} P \oplus 2S_{k-1}, \text{ with } S_{k-1} := \mathsf{Scalarmult}(\varepsilon_{k-1}, P), \\
S_{k-1} &= \varepsilon_{k-1} P \oplus 2S_k, \text{ with } S_k := \mathsf{Scalarmult}(0, P) = (0,1)
\end{aligned}$$

Now you can recursivly determine S_0:

$$\begin{aligned}
S_{k-1} &= \varepsilon_{k-1}P, \\
S_{k-2} &= \varepsilon_{k-2}P \oplus 2S_{k-1} = (\varepsilon_{k-2} + 2\varepsilon_{k-1})P, \\
&\vdots \\
S_1 &= \varepsilon_1 P \oplus 2S_2 = \left(\sum_{i=1}^{k-1} \varepsilon_i 2^{i-1}\right) P, \\
S_0 &= \varepsilon_0 P \oplus 2S_1 = \left(\sum_{i=0}^{k-1} \varepsilon_i 2^{i}\right) P = nP
\end{aligned}$$

□

3.9 Remark.
tchat uses a different elliptic curve math to compute nP. The protocol $\mathsf{Scalarmult}$ is an example how to compute nP faster then by induction 2.10: $n-1$ cycles by induction and $\lfloor \log_2(n) \rfloor + 1$ cycles with $\mathsf{Scalarmult}$. The implementation in **tchat** uses for example precomputated powers of $\mathcal{G}$, to compute $n\mathcal{G}$.

Protocol 2 Compress

Inputs. $(x, y) \in E$

The protocol:

1. Compute $b = \mathrm{bit}_{\min}(x)$.
2. Compute $y' = b \cdot 2^{255} + y$.

Outputs. $y' \in \mathrm{U256}$

Protocol 3 Decompress

Inputs. $y' \in \mathrm{U256}$

The protocol:

1. Compute $b = \mathrm{bit}^{256}_{\max}(y')$.
2. Compute $y = y' - b \cdot 2^{255}$.
3. Set $u := y^2 - 1 \mod p$ and $v = dy^2 + 1 \mod p$ and compute $z = uv^3(uv^7)^{(p-5)/8} \mod p$. Then either
   (a) If $u = vz^2 \mod p$ then $x' := z$.
   (b) If $u = -vz^2 \mod p$ then compute $x' = 2^{(p-1)/4} z \mod p$.
   (c) If $u \neq z^2 v \mod p$ and $u \neq -z^2 v \mod p$ return error.
4. If $b = \mathrm{bit}_{\min}(x')$ then $x = x'$, else $x = -x' \mod p$.

Outputs. $(x, y) \in E$ or error.

3.10 Theorem.
For all $(x, y) \in E$,

$$(x, y) = \mathsf{Decompress} \circ \mathsf{Compress}(x, y).$$

and for all $y' \in \mathrm{U256}$,

$$\mathsf{Compress}(y') = \text{error} \Leftrightarrow \text{there is no } x \in \mathbb{F}_p \text{ such that } (x, y) \in E,$$

where $y = y' - b \cdot 2^{255}$ with $b := \mathrm{bit}^{256}_{\max}(y')$.

Proof. Let $(x, y) \in E$. Since $-1 \mod p$ is a square and d is no square. Equation (1) implies with the notation from $\mathsf{Decompress}$ protocol:

$$x^2 \mod p = \frac{y^2 - 1}{dy^2 + 1} \mod p = \frac{u}{v}$$

Set

$$z := \left(\frac{u}{v}\right)^{(p+3)/8} \mod p$$

With Lemma 2.31 we can calculate

$$\begin{aligned} z &= \left(u \cdot v^{p-2}\right)^{(p+3)/8} \mod p = uv^{p-2}\left(u \cdot v^{p-2}\right)^{(p-5)/8} \mod p \\ &= uv^{3+8(p-5)/8}\left(u \cdot v^{p-2}\right)^{(p-5)/8} \mod p \\ &= uv^3\left(u \cdot v^8 \cdot v^{p-2}\right)^{(p-5)/8} \mod p \\ &= uv^3\left(u \cdot v^7\right)^{(p-5)/8} \mod p \end{aligned}$$

By Lemma 2.35 there are two cases:

(a) $x' := z = \pm x \mod p \Leftrightarrow z^2 \mod p = x^2 \mod p = \frac{u}{v} \Leftrightarrow u = z^2 v \mod p$

(b) $x' := Iz \mod p = \pm x \mod p$, where $I := 2^{(p-1)/4} \mod p$ with $I^2 \mod p = -1 \mod p$ is equivalent to

$$-z^2 \mod p = x^2 \mod p = \frac{u}{v} \Leftrightarrow u = -z^2 v \mod p$$

If $x' = 0 \Rightarrow x = 0$. If $x' \neq 0$ then you need $b := \mathrm{bit}_{\min}(x)$ to choose the right sign: For all $w \in \mathbb{F}_p \setminus \{0\}$, $\mathrm{bit}_{\min}(w) \neq \mathrm{bit}_{\min}(p - w)$, since p is odd. So if $b = \mathrm{bit}_{\min}(x')$ then $x = x'$, else $x = p - x'$.

If $u \neq z^2 v \mod p$ and $u \neq -z^2 v \mod p \Leftrightarrow \frac{u}{v}$ is no square $\Leftrightarrow$ there is no $x \in \mathbb{F}_p$ such that $(x, y) \in E$

□

3.11 Definition.
Let $y' := \frac{4}{5} \mod p \in \mathrm{U}256$. Then define $\mathcal{G} := \mathsf{Decompress}(y')$. Set $l := \mathrm{ord}_E(\mathcal{G})$.

3.12 Remark.
l is the prime number $2^{252} + 27742317777372353535851937790883648493$. It is valid: $l < p$.

4 tchat

We use in tchat the SHA-256 hash function, which we denote by $\mathcal{H}$ and interpret by

$$\mathcal{H} : \bigcup_{k \in \mathbb{N}} \mathrm{U}8k \to \mathrm{U}256.$$

4.1 Definition.
Let $k, r \in \mathbb{N}$. Let

$$(\alpha_0, \ldots, \alpha_{k-1}) \in \{0, 1\}^k$$

be the binary representation from $n \in \mathrm{U}k$. Let

$$(\beta_0, \ldots, \beta_{r-1}) \in \{0, 1\}^r$$

be the binary representation from $m \in \mathrm{U}r$. Then define

$$n \| m \in \mathrm{U}(k + r)$$

by the binary expansion from $(\alpha_0, \ldots, \alpha_{k-1}, \beta_0, \ldots, \beta_{k-1}) \in \{0, 1\}^{k+r}$.

4.2 Definition (secret key, public key, key pair)**.**
A **secret key** is a number $k \in \mathbb{F}_l$. The corresponding **public key** is $K := \mathsf{Scalarmult}(k, \mathcal{G})$. The pair (k, K) is called **key pair**.

4.1 Client Authentication

Protocol 4 Sign

Inputs. $k \in \mathbb{F}_l$, $\mathcal{R} \in$ U256.

The protocol:

1. Compute $\alpha = \mathcal{H}(\mathcal{H}(k')\|\mathcal{R}) \mod l$, with $k = k' \in$ U256.
2. Compute $\beta = \mathsf{Compress}(\mathsf{Scalarmult}(\alpha, \mathcal{G}))$.
3. Compute $c = \mathcal{H}(\beta\|\mathsf{Compress}(\mathsf{Scalarmult}(k, \mathcal{G}))\|\mathcal{R}) \mod l$.
4. Compute $r = (\alpha + c \cdot k) \mod l$.

Outputs. $\beta \in$ U256, $r \in \mathbb{F}_l$.

Protocol 5 Verify

Inputs. $\beta \in$ U256, $r \in \mathbb{F}_l$, $\kappa \in$ U256, $\mathcal{R} \in$ U256.

The protocol:

1. Compute $c = \mathcal{H}(\beta\|\kappa\|\mathcal{R}) \mod l$.
2. If $\mathsf{Scalarmult}(r, \mathcal{G}) = \mathsf{Decompress}(\beta) \oplus \mathsf{Scalarmult}(c, \mathsf{Decompress}(\kappa))$ return true, else false.

Outputs. true or false.

4.3 Lemma.
Let (k, K) be a key pair. Let $\mathcal{R} \in$ U256 then

$$\mathsf{Verify}(\mathsf{Sign}(k, \mathcal{R}), \mathsf{Compress}(K), \mathcal{R}) = \text{true}.$$

Proof. Set $(\beta, r) := \mathsf{Sign}(k, \mathcal{R})$. Then

$$c := \mathcal{H}(\beta\|\mathsf{Compress}(\mathsf{Scalarmult}(k, \mathcal{G}))\|\mathcal{R}) \mod l = \mathcal{H}(\beta\|\mathsf{Compress}(K)\|\mathcal{R}) \mod l$$

and so

$$\begin{aligned}\mathsf{Scalarmult}(r, \mathcal{G}) &= \mathsf{Scalarmult}((\alpha + c \cdot k) \mod l, \mathcal{G}) = \mathsf{Scalarmult}((\alpha + c \cdot k), \mathcal{G}) \\ &= \mathsf{Scalarmult}(\alpha, \mathcal{G}) \oplus \mathsf{Scalarmult}(c \cdot k, \mathcal{G}) = \mathsf{Decompress}(\beta) \oplus \mathsf{Scalarmult}(c \cdot k, \mathcal{G}) \\ &= \mathsf{Decompress}(\beta) \oplus \mathsf{Scalarmult}(c, \mathsf{Scalarmult}(k, \mathcal{G})) = \mathsf{Decompress}(\beta) \oplus \mathsf{Scalarmult}(c, K) \\ &= \mathsf{Decompress}(\beta) \oplus \mathsf{Scalarmult}(c, \mathsf{Decompress}(\mathsf{Compress}(K)))\end{aligned}$$

□

Protocol 6 ClientAuthentication

The interactive protocol:

1. Client sends $\kappa \in$ U256 to server.
2. Server generates a random number $\mathcal{R} \in$ U256 and sends $\mathcal{R}$ to the client.
3. Client computes $(\beta, r) = \mathsf{Sign}(k, \mathcal{R})$ and sends s to the server.
4. Server computes $v = \mathsf{Verify}(\beta, r, \kappa, \mathcal{R})$. If v is true the server accept the client, else the server does not accept the client.

4.2 Client-Message Encryption and Decryption

Protocol 7 SharedSecret

Inputs. $k \in \mathbb{F}_l$, $K \in \langle \mathcal{G} \rangle$.

The protocol: Compute $S = \mathsf{Scalarmult}(k, K)$.

Outputs. $S \in \langle \mathcal{G} \rangle$

4.4 Lemma.
Let $(k_a, K_a), (k_b, K_b)$ be key pairs, then

$$\mathsf{SharedSecret}(k_a, K_b) = \mathsf{SharedSecret}(k_b, K_a)$$

Proof.

$$\mathsf{SharedSecret}(k_a, K_b) = \mathsf{Scalarmult}(k_a, K_b) = \mathsf{Scalarmult}(k_a, \mathsf{Scalarmult}(k_b, \mathcal{G})) = \mathsf{Scalarmult}(k_a k_b, \mathcal{G})$$

and analogues

$$\mathsf{SharedSecret}(k_b, K_a) = \mathsf{Scalarmult}(k_a k_b, \mathcal{G})$$

□

4.5 Definition.
Denote U256 vectors in arbitrary length by U256*, i.e.

$$\text{U256}^* := \bigcup_{i \in \mathbb{N}} \text{U256}^i$$

We cover only modular arithmetic and elliptic curves in the protocols shown here[2].

Protocol 8 Encrypt

Inputs. $(u_1, u_2, \ldots, u_I) \in \text{U256}^*$, $k_a \in \mathbb{F}_l$, $K_b \in \langle \mathcal{G} \rangle$.

The protocol:

1. Generate a random number $\mathcal{R} \in \text{U256}$.
2. Compute $s = \mathsf{Compress}(\mathsf{SharedSecret}(k_a, K_b))$.
3. Compute $o = \mathcal{H}(\mathcal{R} \| s)$.
4. Compute $v_j = u_j + o \mod 2^{256}$ for $j = 1, 2, \ldots, I$.

Outputs. $(v_1, v_2, \ldots, v_I) \in \text{U256}^*$, $\mathcal{R} \in \text{U256}$.

Protocol 9 Decrypt

Inputs. $(v_1, \ldots, v_I) \in \text{U256}^*$, $\mathcal{R} \in \text{U256}$, $k_b \in \mathbb{F}_l$, $K_a \in \langle \mathcal{G} \rangle$.

The protocol:

1. Compute $s = \mathsf{Compress}(\mathsf{SharedSecret}(k_b, K_a))$.
2. Compute $o = \mathcal{H}(\mathcal{R} \| s)$.
3. Compute $u_j = v_j - o \mod 2^{256}$ for $j = 1, 2, \ldots, I$.

Outputs. $(u_1, u_2, \ldots, u_I) \in \text{U256}^*$

4.6 Lemma.
Let $(u_1, u_2, \ldots, u_I) \in \text{U256}^*$. Let $(k_a, K_a), (k_b, K_b)$ be key pairs. Then

$$\mathsf{Decrypt}(\mathsf{Encrypt}((u_1, u_2, \ldots, u_I), k_a, K_b), k_b, K_a) = (u_1, \ldots, u_I).$$

[2]For more details such as converting messages to U256*, see the Rust functions decrypt and encrypt in crypto/src/lib.rs.

5 Appendix

5.1 Definition (ring homomorphism)**.**
Let R, S be rings. A map $\phi : R \to S$ with the properties

(a) For all $r, h \in R$,
$$\phi(r + h) = \phi(r) + \phi(h)$$
and
$$\phi(r \cdot h) = \phi(r) \cdot \phi(h).$$

(b) $\phi(1_R) = 1_S$

is called **ring homomorphism**.

5.2 Definition and Lemma.
Let R be a ring. Then the map defined by
$$\mathrm{unit}^R : \mathbb{Z} \to R, z \mapsto \begin{cases} z \cdot 1_R, & \text{for } z \geq 0 \\ -z \cdot (-1_R), & \text{for } z < 0 \end{cases}$$
is a ring homomorphism.

5.3 Lemma.
Let R, S, T be rings. Let $\phi : R \to S$ and $\psi : S \to T$ be ring homomorphisms. Then $\psi \circ \phi : R \to T$ is a ring homomorphism.

5.4 Lemma (kernel property)**.**
Let R, S be rings. Let $\phi : R \to S$ be a ring homomorphism. Let $r_1, \ldots, r_n, e_1, \ldots, e_n \in R$ with $\phi(e_1) = \ldots = \phi(e_n) = 0$. Set $r = r_1 \cdot e_1 + \ldots + r_n \cdot e_n$. Then $\phi(r) = 0$.

Proof.
$$\phi(r) = \phi(r_1 \cdot e_1 + \ldots + r_n \cdot e_n) = \phi(r_1 \cdot e_1) + \ldots + \phi(r_n \cdot e_n) = \phi(r_1) \cdot \phi(e_1) + \ldots + \phi(r_n) \cdot \phi(e_n) = 0$$
□

5.1 Multivariate Polynomials

5.5 Definition (multi-index)**.**
Let $n \in \mathbb{N}$. Set $\mathbb{N}_0^n := \underbrace{\mathbb{N}_0 \times \ldots \times \mathbb{N}_0}_{n\text{-times}}$. An element of $\mathbb{N}_0^n$ is called **multi-index**. Let $\nu \in \mathbb{N}_0^n$. Then for all $i = 1, \ldots, n$, $\nu_i \in \mathbb{N}_0^n$ is defined by
$$\nu =: (\nu_1, \ldots, \nu_n).$$

5.6 Definition and Lemma.
Let R be a ring. A **polynom** in the variables $X_1, \ldots, X_n$ is a term
$$\sum_{\nu \in \mathbb{N}_0^n} r_\nu X^\nu,$$
where $r_\nu \in R$, $r_\nu \neq 0$ for a finte number of $\nu \in \mathbb{N}_0^n$ and $X^\nu := X_1^{\nu_1} \cdot \ldots \cdot X_n^{\nu_n}$. The set of all polynoms in the variables $x_1, \ldots, x_n$ is denoted by $R[x_1, \ldots, x_n]$. Define
$$+ : R[X_1, \ldots, X_n] \times R[X_1, \ldots, X_n] \to R[X_1, \ldots, X_n], (\sum_{\nu \in \mathbb{N}_0^n} r_\nu X^\nu, \sum_{\nu \in \mathbb{N}_0^n} h_\nu X^\nu) \mapsto \sum_{\nu \in \mathbb{N}_0^n} (r_\nu + h_\nu) X^\nu$$
and
$$\cdot : R[X_1, \ldots, X_n] \times R[X_1, \ldots, X_n] \to R[X_1, \ldots, X_n], (\sum_{\nu \in \mathbb{N}_0^n} r_\nu X^\nu, \sum_{\nu \in \mathbb{N}_0^n} h_\nu X^\nu) \mapsto \sum_{\nu \in \mathbb{N}_0^n} (\sum_{\nu = \mu + \kappa} r_\mu h_\kappa) X^\nu.$$
Then $(R[X_1, \ldots, X_n], +, \cdot)$ is a ring.

5.7 Definition.
Let R, S be rings. Let $\phi : R \to S$ be a ring homomorphism. Define

$$\phi_{(X_1,\ldots,X_n)} : R[X_1,\ldots,X_n] \to S[X_1,\ldots,X_n],\ \sum_{\nu\in\mathbb{N}_0^n} r_\nu X^\nu \mapsto \sum_{\nu\in\mathbb{N}_0^n} \phi(r_\nu) X^\nu.$$

5.8 Lemma.
Let R, S be rings. Let $\phi : R \to S$ be a ring homomorphism. Then $\phi_{(x_1,\ldots,x_n)} : R[x_1,\ldots,x_n] \to S[x_1,\ldots,x_n]$ is a ring homomorphism.

Proof. Set $\phi_X := \phi_{(X_1,\ldots,X_n)}$.

$$\begin{aligned}\phi_X(\sum_{\nu\in\mathbb{N}_0^n} r_\nu X^\nu + \sum_{\nu\in\mathbb{N}_0^n} h_\nu X^\nu) &= \phi_X(\sum_{\nu\in\mathbb{N}_0^n} (r_\nu + h_\nu) X^\nu) = \sum_{\nu\in\mathbb{N}_0^n} \phi(r_\nu + h_\nu) X^\nu = \sum_{\nu\in\mathbb{N}_0^n} (\phi(r_\nu) + \phi(h_\nu)) X^\nu \\ &= \sum_{\nu\in\mathbb{N}_0^n} \phi(r_\nu) X^\nu + \sum_{\nu\in\mathbb{N}_0^n} \phi(h_\nu) X^\nu = \phi_X(\sum_{\nu\in\mathbb{N}_0^n} r_\nu X^\nu) + \phi_X(\sum_{\nu\in\mathbb{N}_0^n} h_\nu X^\nu)\end{aligned}$$

and

$$\begin{aligned}\phi_X(\sum_{\nu\in\mathbb{N}_0^n} r_\nu X^\nu \cdot \sum_{\nu\in\mathbb{N}_0^n} h_\nu X^\nu) &= \phi_X(\sum_{\nu\in\mathbb{N}_0^n} (\sum_{\nu=\mu+\kappa} r_\mu h_\kappa) X^\nu) = \sum_{\nu\in\mathbb{N}_0^n} \phi(\sum_{\nu=\mu+\kappa} r_\mu h_\kappa) X^\nu \\ &= \sum_{\nu\in\mathbb{N}_0^n} (\sum_{\nu=\mu+\kappa} \phi(r_\mu)\phi(h_\kappa)) X^\nu = \sum_{\nu\in\mathbb{N}_0^n} \phi(r_\nu) X^\nu \cdot \sum_{\nu\in\mathbb{N}_0^n} \phi(h_\nu) X^\nu \\ &= \phi_X(\sum_{\nu\in\mathbb{N}_0^n} r_\nu X^\nu) \cdot \phi_X(\sum_{\nu\in\mathbb{N}_0^n} h_\nu X^\nu)\end{aligned}$$

□

5.9 Definition and Lemma.
Let R be a ring. Let $x_1,\ldots,x_n \in R$. For all $\nu \in \mathbb{N}_0^n$ set $x^\nu := x_1^{\nu_1} \cdot \ldots \cdot x_n^{\nu_n}$. Then define

$$\mathrm{eval}^R_{(x_1,\ldots,x_n)} : R[X_1,\ldots,X_n] \to R,\ \sum_{\nu\in\mathbb{N}_0^n} r_\nu X^\nu \mapsto \sum_{\nu\in\mathbb{N}_0^n} r_\nu x^\nu$$

Then $\mathrm{eval}^R_{(x_1,\ldots,x_n)}$ is a ring homomorphism.

Proof. Set $\psi := \mathrm{eval}^R_{(x_1,\ldots,x_n)}$.

$$\begin{aligned}\psi(\sum_{\nu\in\mathbb{N}_0^n} r_\nu X^\nu + \sum_{\nu\in\mathbb{N}_0^n} h_\nu X^\nu) &= \psi(\sum_{\nu\in\mathbb{N}_0^n} (r_\nu + h_\nu) X^\nu) = \sum_{\nu\in\mathbb{N}_0^n} (r_\nu + h_\nu) x^\nu \\ &= \sum_{\nu\in\mathbb{N}_0^n} r_\nu x^\nu + \sum_{\nu\in\mathbb{N}_0^n} h_\nu x^\nu = \psi(\sum_{\nu\in\mathbb{N}_0^n} r_\nu X^\nu) + \psi(\sum_{\nu\in\mathbb{N}_0^n} h_\nu X^\nu)\end{aligned}$$

and

$$\begin{aligned}\psi(\sum_{\nu\in\mathbb{N}_0^n} r_\nu X^\nu \cdot \sum_{\nu\in\mathbb{N}_0^n} h_\nu X^\nu) &= \psi(\sum_{\nu\in\mathbb{N}_0^n} (\sum_{\nu=\mu+\kappa} r_\mu h_\kappa) X^\nu) = \sum_{\nu\in\mathbb{N}_0^n} (\sum_{\nu=\mu+\kappa} r_\mu h_\kappa) x^\nu \\ &= \sum_{\nu\in\mathbb{N}_0^n} r_\nu x^\nu \cdot \sum_{\nu\in\mathbb{N}_0^n} h_\nu x^\nu = \psi(\sum_{\nu\in\mathbb{N}_0^n} r_\nu X^\nu) \cdot \psi(\sum_{\nu\in\mathbb{N}_0^n} h_\nu X^\nu)\end{aligned}$$

□

5.2 Localization

5.10 Definition (multiplicatively closed, zero-divisor, integral domain)**.**
Let R be a ring.

(a) $S \subset R$ is called **multiplicatively closed** if $1_R \in S$ and for all $a, b \in S$, $a \cdot b \in S$.

(b) A $x \in R$ is called **zero-divisor** if there is a $y \in R \setminus \{0\}$ with $x \cdot y = 0$.

(c) R is called **integral domain** if $1_R \neq 0_R$ and 0_R is the only zero-divisor.

5.11 Definition and Lemma.
Let R be a ring. Let $S \subset R$ be multiplicatively closed with no zero-divisors. Then

$$(r, s) \sim (r', s') :\Leftrightarrow rs' = r's \tag{2}$$

is a equivalence relation on on $R \times S$. Denote the equivalence classes of $(r, s) \in R \times S$ by $\frac{r}{s}$. The set

$$S^{-1}R := (R \times S)/\sim = \left\{ \frac{r}{s} \mid r \in R, s \in S \right\}$$

is called **localization** of R at S. The maps

$$+ : S^{-1}R \times S^{-1}R \to S^{-1}R, \left(\frac{r}{s}, \frac{r'}{s'} \right) \mapsto \frac{rs' + r's}{ss'}$$

and

$$\cdot : S^{-1}R \times S^{-1}R \to S^{-1}R, \left(\frac{r}{s}, \frac{r'}{s'} \right) \mapsto \frac{rr'}{ss'}$$

are well defined. $(S^{-1}R, +, \cdot)$ is a ring.

Proof. $\sim$ is a equivalence relation:

- $(r, s) \sim (r, s)$, since $rs = rs$.
- $(r, s) \sim (r', s') \Rightarrow (r', s') \sim (r, s)$, since $rs' = r's \Leftrightarrow r's = rs'$.
- $(r, s) \sim (r', s')$ and $(r', s') \sim (\tilde{r}, \tilde{s}) \Rightarrow (r, s) \sim (\tilde{r}, \tilde{s})$, since $s'(r\tilde{s} - \tilde{r}s) = \tilde{s}(rs' - r's) + s(r'\tilde{s} - \tilde{r}s') = 0$ and s' is no zero-divisor. So $r\tilde{s} - \tilde{r}s = 0$.

$+$ and $\cdot$ are well defined: Let $\frac{r}{s} = \frac{\tilde{r}}{\tilde{s}}$, then with $r\tilde{s} = \tilde{r}s$,

$$(rs' + r's)(\tilde{s}s') - (\tilde{r}s' + r'\tilde{s})(ss') = (r\tilde{s} - \tilde{r}s)(s')^2 = 0$$

and

$$(rr')(\tilde{s}s') - (\tilde{r}r')(ss') = r's'(r\tilde{s} - \tilde{r}s) = 0$$

so

$$\frac{rs' + r's}{ss'} = \frac{\tilde{r}s' + r'\tilde{s}}{\tilde{s}s'}$$

and

$$\frac{rr'}{ss'} = \frac{\tilde{r}r'}{\tilde{s}s'}$$

$(S^{-1}R, +, \cdot)$ is a ring: $1_{S^{-1}R} = \frac{1}{1}$ □

5.12 Definition and Lemma.
Let R be a ring. Let $S \subset R$ be multiplicatively closed with no zero-divisors. Let $\phi : R \to T$ be a ring homomorphism with $\phi(S) \subset T^*$. Then the map

$$\phi' : S^{-1}R \to T, \frac{r}{s} \mapsto \frac{\phi(r)}{\phi(s)} := \phi(r)\phi(s)^{-1}$$

is a well defined ring homomorphism.

Proof. Let $\frac{r}{s} = \frac{\tilde{r}}{\tilde{s}}$. Then with $r\tilde{s} = \tilde{r}s$,

$$\phi(r)\phi(\tilde{s}) = \phi(r\tilde{s}) = \phi(\tilde{r}s) = \phi(\tilde{r})\phi(s) \Leftrightarrow \phi(r)\phi(s)^{-1} = \phi(\tilde{r})\phi(\tilde{s})^{-1}.$$

ϕ' is a ring homomorphism:

$$\begin{aligned}\phi'\left(\frac{r}{s} + \frac{\tilde{r}}{\tilde{s}}\right) &= \phi'\left(\frac{r\tilde{s} + \tilde{r}s}{s\tilde{s}}\right) = \phi(r\tilde{s} + \tilde{r}s)\phi(s\tilde{s})^{-1} = \phi(r\tilde{s})\phi(s\tilde{s})^{-1} + \phi(\tilde{r}s)\phi(s\tilde{s})^{-1} \\ &= \phi(r)\phi(s)^{-1} + \phi(\tilde{r})\phi(\tilde{s})^{-1} = \phi'\left(\frac{r}{s}\right) + \phi'\left(\frac{\tilde{r}}{\tilde{s}}\right)\end{aligned}$$

and

$$\phi'\left(\frac{r}{s} \cdot \frac{\tilde{r}}{\tilde{s}}\right) = \phi'\left(\frac{r\tilde{r}}{s\tilde{s}}\right) = \phi(r\tilde{r})\phi(s\tilde{s})^{-1} = \phi(r)\phi(s)^{-1}\phi(\tilde{r})\phi(\tilde{s})^{-1} = \phi'\left(\frac{r}{s}\right)\phi'\left(\frac{\tilde{r}}{\tilde{s}}\right)$$

□

5.13 Definition and Lemma.
Let R be a ring. Let $\delta \in R$ be no zero-divisor. Then the set $S_\delta := \{1_R, \delta, \delta^2, \ldots\}$ is multiplicatively closed with no zero-divisors. Then set

$$S_\delta{}^{-1}R := R\langle\delta\rangle.$$

Proof. 1_R is no zero divisor: Let $x \in R \setminus \{0\}$. Then $1_R \cdot x = x \neq 0_R$.
For all $n \in \mathbb{N}$, δ^n is no zero-divisor: Proof this by induction. Let $\delta^{n+1}x = 0$. So

$$\delta(\delta^n x) = 0 \Rightarrow \delta^n x = 0 \Rightarrow x = 0.$$

□

5.3 Proof of Twisted Edward Curves Theorem

5.14 Definition.
Set $R_n := \mathbb{Z}[A, D, X_1, Y_1, X_2, Y_2, \ldots, X_n, Y_n]$. Define for all $i, j = 1, \ldots, n$, $\delta_{ij}^{\pm} \in R_n$ by

$$\delta_{ij}^{\pm} = 1 \pm DX_iX_jY_iY_j$$

and $\delta_{ij} := \delta_{ij}^{+}\delta_{ij}^{-}$.
Set $\delta^+ := \delta_{12}^{+} \in R_2$, $\delta^- := \delta_{12}^{-} \in R_2$ and $\delta := \delta_{12} \in R_2$. $\delta \in R_2$ is no zero-divisor. Define $(X_i, Y_i) \oplus (X_j, Y_j) \in R_n\langle\delta_{ij}\rangle \times R_n\langle\delta_{ij}\rangle$ by

$$(X_i, Y_i) \oplus (X_j, Y_j) := \left(\frac{(X_1Y_2 + X_2Y_1)\delta_{ij}^{-}}{\delta_{ij}}, \frac{(Y_1Y_2 - AX_1X_2)\delta_{ij}^{+}}{\delta_{ij}}\right).$$

Define for all $i = 1, \ldots, n$, $e_i \in R_n$ by

$$e_i := AX_i^2 + Y_i^2 - 1 - DX_i^2Y_i^2.$$

Define the map

$$e : R_n\langle\delta_{ij}\rangle \times R_n\langle\delta_{ij}\rangle \to R_n\langle\delta_{ij}\rangle, (x, y) \mapsto Ax^2 + y^2 - 1 - Dx^2y^2.$$

Let S be a ring. Let $a, d, x_1, y_1, x_2, y_2, \ldots, x_n, yy_n \in S$. Define $\phi_n : R_n \to S$, by

$$\phi_n := \mathrm{eval}^S_{(a,d,x_1,y_1,x_2,y_2,\ldots,x_n,y_n)} \circ \mathrm{unit}^S_{(A,D,X_1,Y_1,X_2,Y_2,\ldots,X_n,Y_n)}$$

Let $i, j = 1, \ldots, n$. If $\phi_n(\delta_{ij}) \in S^*$. Define $(x_i, y_i) \oplus (x_j, y_j) \in S \times S$ by

$$(x_i, y_i) \oplus (x_j, y_j) := \phi_n'((X_i, Y_i) \oplus (X_j, Y_j)).$$

5.15 Lemma.

(a) Let $\phi_2(\delta) \in S^*$. Then

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

(b) $(X_1, Y_1) \oplus (X_2, Y_2) = (X_2, Y_2) \oplus (X_1, Y_1)$

(c) Let $(x_1, y_1) := (0, 1)$. Then

$$(x_1, y_1) \oplus (x_2, y_2) = (x_2, y_2).$$

(d) Let $\phi_2(\delta) \in S^*$ with $(x_2, y_2) := (-x_1, y_1)$ and $\phi_2(e_1) = 0$. Then

$$(x_1, y_1) \oplus (x_2, y_2) = (0, 1).$$

Proof. (a)

$$\begin{aligned}
\phi_2'((X_1, Y_1) \oplus (X_2, Y_2)) &= \left(\frac{\phi_2((X_1Y_2 + X_2Y_1)\delta^-)}{\phi_2(\delta)}, \frac{\phi_2((X_1Y_2 - AX_1X_2)\delta^+)}{\phi_2(\delta)} \right) \\
&= \left(\frac{\phi_2(X_1Y_2 + X_2Y_1))}{\phi_2(\delta^+)}, \frac{\phi_2(X_1Y_2 - AX_1X_2)}{\phi_2(\delta^-)} \right) \\
&= \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right)
\end{aligned}$$

(d) With $ax_1^2 + y_1^2 - 1 - dx_1^2y_1^2 = \phi_2(e_1) = 0 \Leftrightarrow 1 + dx_1^2y_1^2 = ax_1^2 + y_1^2$ follows

$$(x_1, y_1) \oplus (-x_1, y_1) = \left(\frac{0}{1 - dx_1^2y_1^2}, \frac{ax_1^2 + y_1^2}{1 + dx_1^2y_1^2} \right) = \left(0, \frac{1 + dx_1^2y_1^2}{1 + dx_1^2y_1^2} \right) = (0, 1).$$

□

5.16 Theorem.
Let $\phi_2(\delta) \in S^*$ and $\phi_2(e_1) = \phi_2(e_2) = 0$. Set $(x, y) := (x_1, y_1) \oplus (x_2, y_2)$ Then

$$ax^2 + y^2 - 1 - dx^2y^2 = 0$$

Proof. Calculate

$$e((X_1, Y_1) \oplus (X_2, Y_2)) = \frac{r}{\delta^2},$$

where

$$r = \delta^2 - A(X_1Y_2 + Y_1X_2)^2(\delta^-)^2 - (Y_1Y_2 - AX_1X_2)(\delta^+)^2 + D(X_1Y_2 + Y_1X_2)^2(Y_1Y_2 - AX_1X_2)^2 \in R_2.$$

So

$$ax^2 + y^2 - 1 - dx^2y^2 = \phi_2'(e((X_1, Y_1) \oplus (X_2, Y_2))) = \frac{\phi_2(r)}{\phi_2(\delta^2)}.$$

So it is enough to show that $\phi_2(r) = 0$. There are $r_1, r_2 \in R_2$ such that $r = r_1e_1 + r_2e_2$. You can verify this result by a computer algebra programm like *Mathematica* (use *PolynomialReduce*). Then by kernel property (Lemma 5.4):

$$\phi_2(r) = 0.$$

□

5.17 Definition.
Define

$$(X_3', Y_3') := (X_1, Y_1) \oplus (X_2, Y_2) = \left(\frac{(X_1Y_2 + X_2Y_1)\delta_{12}^-}{\delta_{12}}, \frac{(Y_1Y_2 - AX_1X_2)\delta_{12}^+}{\delta_{12}} \right) \in R_3\langle\delta_{12}\rangle \times R_3\langle\delta_{12}\rangle$$

and

$$(X_1', Y_1') := (X_2, Y_2) \oplus (X_3, Y_3) = \left(\frac{(X_2Y_3 + X_3Y_2)\delta_{23}^-}{\delta_{23}}, \frac{(Y_2Y_3 - AX_2X_3)\delta_{23}^+}{\delta_{23}} \right) \in R_3\langle\delta_{23}\rangle \times R_3\langle\delta_{23}\rangle$$

Then set

$$\delta^{\pm}(X_3', Y_3', X_3, Y_3) := 1 \pm DX_3'Y_3'X_3Y_3 \in R_3\langle\delta_{12}\rangle$$

and

$$\delta^{\pm}(X_1, Y_1, X_1', Y_1') := 1 \pm DX_1Y_1X_1'Y_1' \in R_3\langle\delta_{23}\rangle$$

$$\Delta^{\pm} := \delta_{12}\delta_{23}\delta^{\pm}(X_3', Y_3', X_3, Y_3)\delta^{\pm}(X_1, Y_1, X_1', Y_1') \in R_3$$

Set

$$\Delta := \Delta^+\Delta^- \in R_3$$

and then

$$\begin{aligned}
(X_3', Y_3') \oplus (X_3, Y_3) &:= \left(\frac{p_x}{\Delta}, \frac{p_y}{\Delta}\right) \in R_3\langle\Delta\rangle \times R_3\langle\Delta\rangle \\
(X_1, Y_1) \oplus (X_1', Y_1') &:= \left(\frac{q_x}{\Delta}, \frac{q_y}{\Delta}\right) \in R_3\langle\Delta\rangle \times R_3\langle\Delta\rangle
\end{aligned}$$

with

$$\begin{aligned}
p_x &:= ((X_1Y_2 + X_2Y_1)\delta_{12}^-Y_3 + X_3(Y_1Y_2 - AX_1X_2)\delta_{12}^+)\delta_{23}\delta^+(X_1, Y_1, X_1', Y_1')\Delta^- \\
p_y &:= ((Y_1Y_2 - AX_1X_2)\delta_{12}^+Y_3 - A(X_1Y_2 + X_2Y_1)\delta_{12}^-X_3)\delta_{23}\delta^-(X_1, Y_1, X_1', Y_1')\Delta^+ \\
q_x &:= (X_1(Y_2Y_3 - AX_2X_3)\delta_{23}^+ + (X_2Y_3 + X_3Y_2)\delta_{23}^-y_1)\delta_{12}\delta^+(X_3', Y_3', X_3, Y_3)\Delta^- \\
q_y &:= (Y_1(Y_2Y_3 - AX_2X_3)\delta_{23}^+ - AX_1(X_2Y_3 + X_3Y_2)\delta_{23}^-)\delta_{12}\delta^-(X_3', Y_3', X_3, Y_3)\Delta^+
\end{aligned}$$

5.18 Lemma.

(a) Let $\phi_3(\delta_{12}), \phi_3(\Delta) \in S^*$. Then

$$((x_1, y_1) \oplus (x_2, y_2)) \oplus (x_3, y_3) = \left(\frac{\phi_3(p_x)}{\phi_3(\Delta)}, \frac{\phi_3(p_y)}{\phi_3(\Delta)}\right)$$

(b) Let $\phi_3(\delta_{23}), \phi_3(\Delta) \in S^*$. Then

$$(x_1, y_1) \oplus ((x_2, y_2) \oplus (x_3, y_3)) = \left(\frac{\phi_3(q_x)}{\phi_3(\Delta)}, \frac{\phi_3(q_y)}{\phi_3(\Delta)}\right).$$

Proof. Set $(\alpha, \beta) := (x_1, y_1) \oplus (x_2, y_2)$. Then calculate

$$\begin{aligned}
\frac{\phi_3(p_x)}{\phi_3(\Delta)} &= \frac{\phi_3(((X_1Y_2 + X_2Y_1)\delta_{12}^-Y_3 + X_3(Y_1Y_2 - AX_1X_2)\delta_{12}^+)\delta_{23}\delta^+(X_1, Y_1, X_1', Y_1'))}{\phi_3(\Delta^+)} \\
&= \frac{\phi_3(((X_1Y_2 + X_2Y_1)\delta_{12}^-Y_3 + X_3(Y_1y_2 - AX_1X_2)\delta_{12}^+)\delta_{23}\delta^+(X_1, Y_1, X_1', Y_1'))}{\phi_3(\delta_{12}\delta_{23}\delta^+(X_3', Y_3', X_3, Y_3)\delta^+(X_1, Y_1, X_1', Y_1'))} \\
&= \frac{\phi_3((X_1Y_2 + X_2Y_1)\delta_{12}^-Y_3 + X_3(Y_1Y_2 - AX_1X_2)\delta_{12}^+)}{\phi_3(\delta_{12}\delta^+(X_3', Y_3', X_3, Y_3))} \\
&= \frac{\phi_3((X_1Y_2 + X_2Y_1)\delta_{12}^-)y_3 + x_3\phi_3((Y_1Y_2 - AX_1X_2)\delta_{12}^+)}{\phi_3(\delta_{12})(1 + d\frac{\phi_3((X_1Y_2+X_2Y_1)(Y_1Y_2-AX_1X_2))}{\phi_3(\delta_{12})}x_3y_3)} \\
&= \frac{\alpha y_3 + x_3\beta}{1 + d\alpha\beta x_3y_3}
\end{aligned}$$

□

5.19 Theorem.
Let $\phi_3(\Delta) \in S^*$ and $\phi_3(e_1) = \phi_3(e_2) = \phi_3(e_3) = 0$. Then

$$((x_1, y_1) \oplus (x_2, y_2)) \oplus (x_3, y_3) = (x_1, y_1) \oplus ((x_2, y_2) \oplus (x_3, y_3)).$$

Proof. There are $r_1, r_2, r_3 \in R_3$ such that $p_x - q_x = r_1 e_1 + r_2 e_2 + r_3 e_3$. You can verify this result by a computer algebra programm like *Mathematica* (use *PolynomialReduce* again). So

$$\frac{\phi_3(p_x)}{\phi_3(\Delta)} - \frac{\phi_3(q_x)}{\phi_3(\Delta)} = \frac{\phi_3(p_x) - \phi_3(q_x)}{\phi_3(\Delta)} = \frac{\phi_3(p_x - q_x)}{\phi_3(\Delta)} = 0$$

The last equation follows again by kernel property (Lemma 5.4). □

Now we consider the map $\phi_n : R_n \to \mathbb{F}$, where $\mathbb{F}$ is a field.

5.20 Lemma.
Let $\mathbb{F}$ be a field. Then

$$\phi_2(\delta) = \phi_2(e_1) = \phi_2(e_2) = 0 \Rightarrow d \text{ or } ad \text{ is a nonzero square in } \mathbb{F}$$

Proof. Define $r \in R_2$ by $r := (1 - ADX_1^2 X_2^2)(1 - DX_1^2 Y_2^2)$.

$$r = (1 - DX_1^2)\delta + D^2 X_1^2 X_2^2 Y_2^2 e_1 - DX_1^2 e_2$$

So $\phi(r) = 0$. Then

$$\phi(r) = 0 \Leftrightarrow 1 - adx_1^2 x_2^2 = 0 \text{ or } 1 - dx_1^2 y_2^2 = 0 \Leftrightarrow ad = \left(\frac{1}{x_1 x_2}\right)^2 \text{ or } d = \left(\frac{1}{x_1 y_2}\right)^2$$

□

Now we have the tools to prove Theorem 3.2. For better readability we repeat the Theorem:

5.21 Theorem.
Let $\mathbb{F}$ be a field. Let $a \in \mathbb{F}$ be a square and let $d \in \mathbb{F}$ be no square. Then the map

$$\oplus : E_{a,d} \times E_{a,d} \to E_{a,d}$$

given by

$$(x_1, y_1) \oplus (x_2, y_2) := \left(\frac{x_1 y_2 + x_2 y_1}{1 + dx_1 x_2 y_1 y_2}, \frac{y_1 y_2 - ax_1 x_2}{1 - dx_1 x_2 y_1 y_2}\right)$$

is well defined. Further $(E_{a,d}, \oplus)$ is a group with identity element $(0, 1)$ and for all $(x, y) \in E_{a,d}$

$$-(x, y) := (x, y)^{-1} = (-x, y).$$

Proof. $\oplus$ is well defined: Let $(x_1, y_1), (x_2, y_2) \in E_{a,d}$. Then $\phi_2(e_1) = \phi_2(e_2) = 0$. By Lemma 5.20,

$$\begin{aligned} a \in \mathbb{F} \text{ is a square and } d \in \mathbb{F} \text{ is no square} &\Rightarrow \neg(d \text{ or } ad \text{ is a nonzero square in } \mathbb{F}) \\ &\Rightarrow \neg(\phi_2(\delta) = \phi_2(e_1) = \phi_2(e_2) = 0) \\ &\Rightarrow \phi_2(\delta) \neq 0. \end{aligned}$$

So $1 + dx_1 x_2 y_1 y_2 \neq 0$ and $1 - dx_1 x_2 y_1 y_2 \neq 0$ and, by Theorem 5.16, $(x_1, y_1) \oplus (x_2, y_2) \in E_{a,d}$.
$(E_{a,d}, \oplus)$ is a semigroup:

(S1) Let $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in E_{a,d}$. Then $\phi_3(e_1) = \phi_3(e_2) = \phi_3(e_3) = 0$. Let $(\alpha, \beta) := (x_1, y_1) \oplus (x_2, y_2)$. Then

$$1 \pm d\alpha\beta x_3 y_3 \neq 0$$

So, by proof of Lemma 5.18,

$$\phi(\delta_{12}\delta^+(X_3', Y_3', X_3, Y_3)\delta_{12}\delta^-(X_3', Y_3', X_3, Y_3)) = (1 + d\alpha\beta x_3 y_3)(1 - d\alpha\beta x_3 y_3) \neq 0$$

With the same argument follows $\phi(\delta_{23}\delta^+(X_1, Y_1, X_1', Y_1')\delta_{23}\delta^-(X_1, Y_1, X_1', Y_1')) \neq 0$. So finally $\phi(\Delta) \neq 0$. Then by Theorem 5.19

$$((x_1, y_1) \oplus (x_2, y_2)) \oplus (x_3, y_3) = (x_1, y_1) \oplus ((x_2, y_2) \oplus (x_3, y_3)).$$

(S2) Let $(x_1, y_1), (x_2, y_2) \in E_{a,d}$ with $(x_1, y_1) := (0, 1)$. (x_1, y_1) is well defined, since $\phi_2(e_1) = 0$. Then, by Lemma 5.15 (c),

$$(x_1, y_1) \oplus (x_2, y_2) = (x_2, y_2).$$

(S3) By Definition of $\oplus$ or Lemma 5.15 (b),

$$(x_1, y_1) \oplus (x_2, y_2) = (x_2, y_2) \oplus (x_1, y_1).$$

$(E_{a,d}, \oplus)$ satisfies (G2):

(G2) Let $(x_1, y_1), (x_2, y_2) \in E_{a,d}$ with $(x_2, y_2) := (-x_1, y_1)$. (x_2, y_2) is well defined, since $\phi_2(e_2) = 0$. By definition $\phi_2(e_1) = 0$. Then by Lemma 5.15 (d),

$$(x_1, y_1) \oplus (x_2, y_2) = (0, 1).$$

□

References

[1] *Zero to Monero: Second Edition.* `https://www.getmonero.org/library/Zero-to-Monero-2-0-0.pdf`.

[2] *Formal Proof of the Group Law for Edwards Elliptic Curves.* `https://pmc.ncbi.nlm.nih.gov/articles/PMC7324045/pdf/978-3-030-51054-1_Chapter_15.pdf`

[3] *RFC 8032: Edwards-Curve Digital Signature Algorithm (EdDSA).* `https://www.rfc-editor.org/rfc/rfc8032`