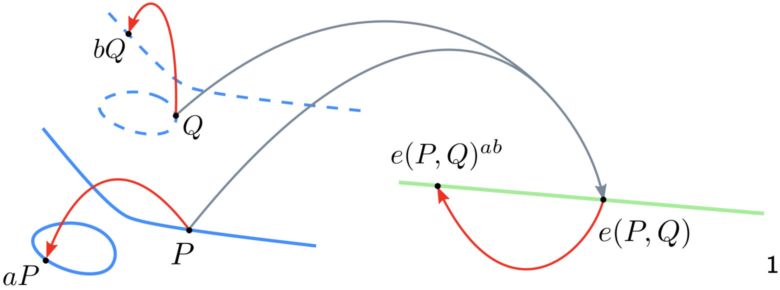
Elliptic Curve Optimizations. EC Pairing.

Distributed Lab

May 16, 2024



Plan

Preliminaries

Field

Definition

Field K is a set equipped with appropriate **addition** and **multiplication** operations with the corresponding well-defined inverses, where you can perform the basic arithmetic.

- $\mathbb{R}$ (real numbers) is a field.
- $\mathbb{Q}$ (rational numbers) is a field.
- $\mathbb{C}$ (complex numbers) is a field.
- $\mathbb{N}$ (natural numbers) is not a field: there is no additive inverse for 2 (-2 is not in $\mathbb{N}$).
- $\mathbb{Z}$ (integers) is not a field: additive inverse is defined, but the multiplicative is not (2^{-1} is not defined).

Finite Field

Definition

Finite field $\mathbb{F}_p$ is a set $\{0, 1, \ldots, p-1\}$ equipped with basic arithmetic ($+$ and $\times$) modulo p.

Example

$\mathbb{F}_5$ is a set with elements $\{0, 1, 2, 3, 4\}$. Examples of calculations:

1. $3 + 4 = 7 = 2$ (in $\mathbb{F}_5$);
2. $3 - 4 = -1 = 4$ (in $\mathbb{F}_5$);
3. $3 \times 4 = 12 = 2$ (in $\mathbb{F}_5$);
4. $3^{-1} = 2$ (since $3 \cdot 2 = 1$ in $\mathbb{F}_5$);
5. $2/3 = 2 \times 3^{-1} = 4$ in $\mathbb{F}_5$.

Typically, p is a large (e.g., 254-bit) **prime number**.

Finite Field Illustration

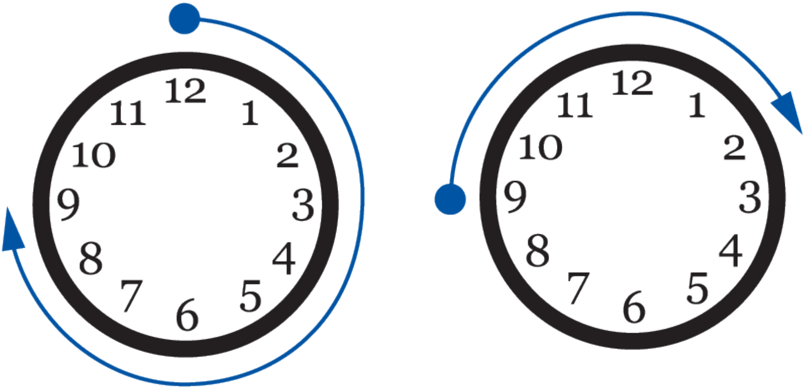


Figure: Illustration of performing addition in $\mathbb{Z}_{12}$ (not really a field, but the rules are identical besides inversion).

Elliptic Curve

Definition

Elliptic Curve $E(K)$ in short *Weierstraß form* over the field K is a set of coordinates (x, y) from K such that

$$y^2 = x^3 + ax + b, \quad (a, b \in K)$$

together with a "point at infinity" $\mathcal{O}$.

BN254 (or **BN256**/**BN128**) is the curve over $K = \mathbb{F}_p$ where:

$$y^2 = x^3 + 3 \qquad (a = 0, b = 3)$$

$$p = \text{0x30644e72e131a029b85045b68181585d97}\ldots$$

$$\ldots 816a916871ca8d3c208c16d87cfd47$$

Elliptic Curve on the Figure

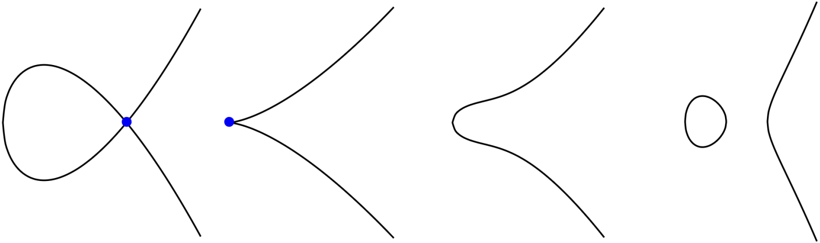


Figure 2.1: Singular curve $y^2 = x^3 - 3x + 2$ over $\mathbb{R}$.

Figure 2.2: Singular curve $y^2 = x^3$ over $\mathbb{R}$.

Figure 2.3: Smooth curve $y^2 = x^3 + x + 1$ over $\mathbb{R}$.

Figure 2.4: Smooth curve $y^2 = x^3 - x$ over $\mathbb{R}$.

Figure: Illustration of various elliptic curves over $\mathbb{R}$ (that is, $E(\mathbb{R})$).

Actually, these are Elliptic Curves...

But actual elliptic curves look more like that...

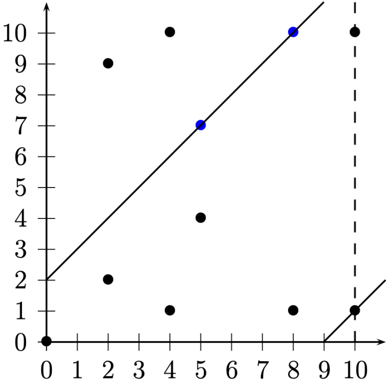


Figure 2.9: The points (excluding $\mathcal{O}$) on $E(\mathbb{F}_{11})$.

Figure: Illustration of an elliptic curve $E(\mathbb{F}_{11}) : y^2 = x^3 - 2x$.

Group structure

Definition

Group $(\mathbb{G}, \oplus)$ is just a set with defined operation $\oplus$, which has "nice" properties (e.g., closure).

Idea: A set of objects is useless unless we have practical relations between elements. For example, 7 and 13 are integers, but the structure is worthless without the ability to add/multiply them.

Theorem

$(E(\mathbb{F}_p), \oplus)$ is a group where operation $\oplus$ between points $P, Q \in E(\mathbb{F}_p)$ means drawing a line between P and Q (or tangent line if $P = Q$), finding intersection with $E(\mathbb{F}_p)$ and "reflecting around Ox axis" (negating y component). We denote the group order by $q := |E(\mathbb{F}_p)|$.

Also, we denote $[a]P = \underbrace{P \oplus P \oplus \cdots \oplus P}_{a \text{ times}}$ – scalar multiplication ($a \in \mathbb{F}_q$).

Illustration of addition

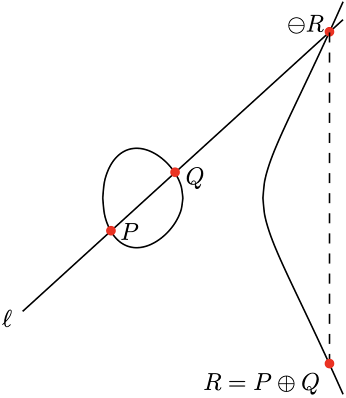


Figure 2.5: Elliptic curve addition.

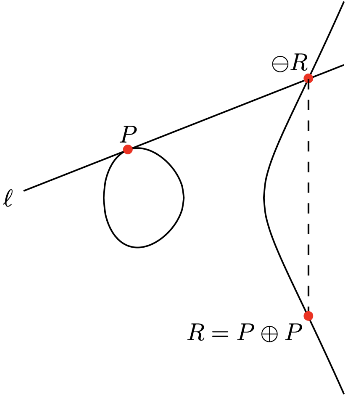


Figure 2.6: Elliptic curve doubling.

Figure: Illustration of operation $R = P \oplus Q$

Effective EC Point Addition

Classical Approach

Definition

Point $P \in E(\mathbb{F}_p)$, represented by coordinates (x_P, y_P) is called the **affine representation** of P.

So, how do we add $(x_R, y_R) = (x_P, y_P) \oplus (x_Q, y_Q)$ where (x_P, y_P) and (x_Q, y_Q) are affine representation of points $P, Q \in E(\mathbb{F}_p)$?

Algorithm 1: Classical adding P and Q for $x_P \neq x_Q$

1. Calculate the slope $\lambda \leftarrow (y_P - y_Q)/(x_P - x_Q)$.
2. Set
$$x_R \leftarrow \lambda^2 - x_P - x_Q, \;\; y_R \leftarrow \lambda(x_P - x_R) - y_P.$$

Easy, right? What can go wrong?

Why this is bad?

Let

- **M** – cost of multiplication;
- **S** – cost of squaring;
- **I** – cost of inverse.

(all in $\mathbb{F}_p$)

Algorithm 1: Calculating $P \oplus Q$

$$\lambda \leftarrow (y_P - y_Q) \times (x_P - x_Q)^{-1}$$
$$x_R \leftarrow \lambda^2 - x_P - x_Q$$
$$y_R \leftarrow \lambda \times (x_P - x_R) - y_P$$

Then, calculating the aforementioned formula costs:

$$2\mathbf{M} + \mathbf{S} + \mathbf{I}$$

Well, just 4 operations... Easy right?

Main Problem!

Typically, $\mathbf{I} \approx 80\mathbf{M}$. So, the effective cost is roughly **80 operations**. Too bad.

Solution: Projective Coordinates

Definition

We now represent point $P \in E(\mathbb{F}_p)$ via three coordinates $(X_P : Y_P : Z_P)$. Such form is called **projective coordinates**. To convert this form to affine form, we use map $(X_P : Y_P : Z_P) \mapsto (X_P/Z_P, Y_P/Z_P)$, $(0 : Y_P : 0) \mapsto \mathcal{O}$.

Definition

If points $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ map to the same affine point, they are called **equivalent**. Formally, if exists $\lambda \in \mathbb{F}_p$ such that $(X_1 : Y_1 : Z_1) = (\lambda X_2 : \lambda Y_2 : \lambda Z_2)$.

Geometrical interpretation: two points $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ are equivalent if the line through them intersects $(0, 0, 0)$ in "3D space". The elliptic curve equation (or rather surface) is then:

$$\boxed{Y^2 Z = X^3 + aXZ^2 + bZ^3}$$

Elliptic Curve in Projective Form

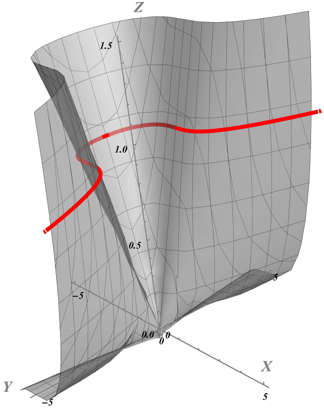


Figure: Elliptic Curve $Y^2Z = X^3 + 3Z^3$ visualized over reals $\mathbb{R}$ in 3D space. The "affine" curve is red, lying on a plane $z = 1$.

Equivalent points in projective form

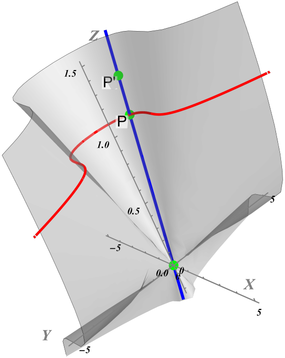


Figure: Points P and P' are equivalent ($P \sim P'$) since line PP' intersects $O = (0, 0, 0)$.

What does it give us?

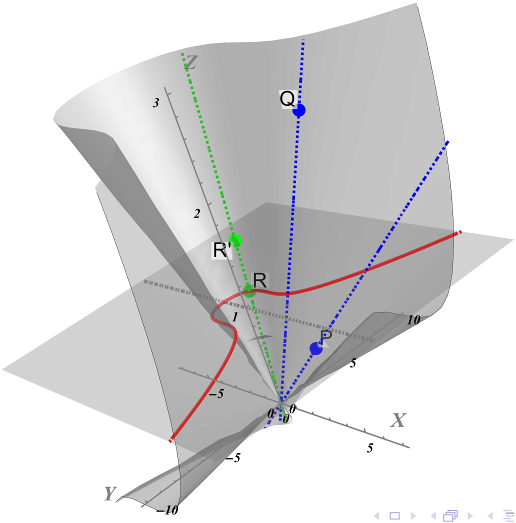
Now we have three instead of two coordinates... Why is it better? Because addition now looks like:

$$
\begin{aligned}
X_3 &= (X_1Y_2 + X_2Y_1)(Y_1Y_2 - 3bZ_1Z_2) \\
&\quad - 3b(Y_1Z_2 + Y_2Z_1)(X_1Z_2 + X_2Z_1), \\
Y_3 &= (Y_1Y_2 + 3bZ_1Z_2)(Y_1Y_2 - 3bZ_1Z_2) + 9bX_1X_2(X_1Z_2 + X_2Z_1), \\
Z_3 &= (Y_1Z_2 + Y_2Z_1)(Y_1Y_2 + 3bZ_1Z_2) + 3X_1X_2(X_1Y_2 + X_2Y_1),
\end{aligned}
$$

Figure: Elliptic Curve addition in projective form.

Although looks much more complicated, it takes only **14M** compared to **80M**.

Illustration of adding two points



General Strategy

1. Convert affine form (X_P, Y_P) to the projective $(X_P : Y_P : 1)$.
2. Make many additions, doubling, multiplications etc. in projective form, getting $(X_R : Y_R : Z_R)$ at the end.
3. Convert back to affine coordinates:

$$(X_R : Y_R : Z_R) \mapsto (X_R/Z_R, Y_R/Z_R)$$

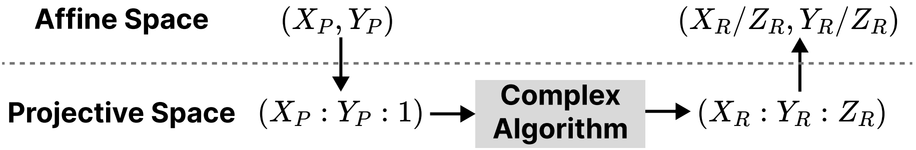


Figure: General strategy with EC operations.

EC Pairing

Definition

Definition

EC Pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a magical map satisfying the following property:

$$e([a]P, [b]Q) = e([ab]P, Q) = e(P, [ab]Q) = e(P, Q)^{ab}.$$

Pairing for BN254

For BN254, we have:

- $\mathbb{G}_1$ – "regular" points on the curve $E(\mathbb{F}_p)$.
- $\mathbb{G}_2$ – "good" points on the twisted curve $E'(\mathbb{F}_{p^2})$ over the field extension $\mathbb{F}_{p^2}$ ($y^2 = x^3 + b', b \neq b' \in \mathbb{F}_{p^2}$).
- $\mathbb{G}_T$ – multiplicative scalars from extension $\mathbb{F}_{p^{12}}$ *(namely, μ_r)*.

EC Pairing Illustration

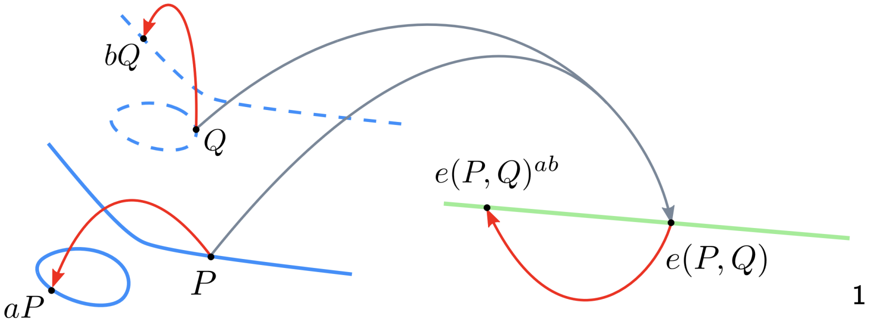


Figure: Pairing illustration. It does not matter what we do first: (a) compute $[a]P$ and $[b]Q$ and then compute $e([a]P,[b]Q)$ or (b) first calculate $e(P,Q)$ and then transform it to $e(P,Q)^{ab}$.

Example: BLS Signature

Suppose we have pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ (with generators G_1, G_2, respectively), and a hash function H, mapping message space $\mathcal{M}$ to $\mathbb{G}_1$.

Definition

BLS Signature consists of the following algorithms:

- $\mathrm{Gen}(\cdot)$: Key generation. $\mathrm{sk} \xleftarrow{R} \mathbb{Z}_q, \mathrm{pk} \leftarrow [\mathrm{sk}]G_2 \in \mathbb{G}_2$.
- $\mathrm{Sign}(\mathrm{sk}, m)$. Signature is $\sigma \leftarrow [\mathrm{sk}]\mathrm{H}(m) \in \mathbb{G}_1$.
- $\mathrm{Verify}(\mathrm{pk}, m, \sigma)$. Check whether $e(\mathrm{H}(m), \mathrm{pk}) = e(\sigma, G_2)$.

Let us check the correctness:

$$e(\sigma, G_2) = e([\mathrm{sk}]\mathrm{H}(m), G_2) = e(\mathrm{H}(m), [\mathrm{sk}]G_2) = e(\mathrm{H}(m), \mathrm{pk})$$

Remark: $\mathbb{G}_1$ and $\mathbb{G}_2$ might be switched: public keys might live instead in $\mathbb{G}_1$ while signatures in $\mathbb{G}_2$.

What it takes to implement?

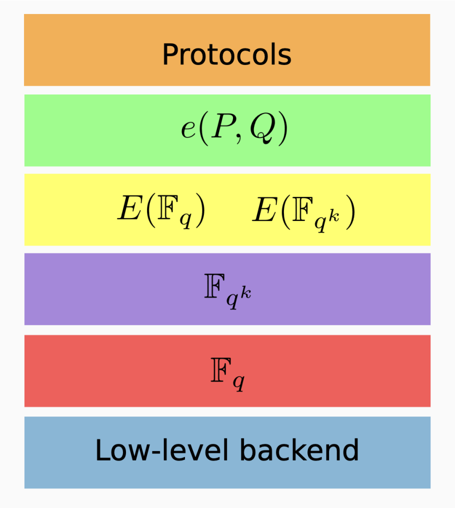


Figure: Various things under the hood.

What are field extensions?

These are "like" complex numbers $\mathbb{C}$. Recall that the complex number is $a + ib$ where $a, b \in \mathbb{R}$ and $i^2 = -1$. So that:

$$\begin{aligned}(a + ib)(c + id) &= ac + (ad)i + (bc)i + (bd)i^2 \\ &= (ac - bd) + (ad + bc)i\end{aligned}$$

Field extension $\mathbb{F}_{p^2}$ is $a + ib$ where $a, b \in \mathbb{F}_p$ and $i^2 = -1$. The same structure, essentially :)
Problems happen with $\mathbb{F}_{p^6}$ and $\mathbb{F}_{p^{12}}$ though since the intuition with complex numbers break...

Polynomials

Definition

Polynomial $K[X]$ is an expression

$$p(X) = c_0 + c_1 X + c_2 X^2 + \cdots + c_n X^n,\ c_i \in K$$

Definition

Polynomial $p \in K[X]$ is said to be irreducible if there are two non-constant polynomials $q, r \in K[X]$ such that $p = qr$.
Example: $X^2 + 4 \in \mathbb{R}[X]$ is irreducible.

Definition

Quotient group $K[X]/\langle p \rangle$ (which is a field) over irreducible polynomial p is polynomials from $K[X]$ modulo p.

Examples

Arithmetic in quotient group

Suppose $K = \mathbb{R}$ and $p(X) = X^2 + 1$ – irreducible over $\mathbb{R}$. Then, example elements are $1 + 2X, 2 + 3X \in \mathbb{R}[X]/\langle X^2 + 1\rangle$. You can do the regular arithmetic with them:

- **Addition:** $(1 + 2X) + (2 + 3X) = 3 + 5X$
- **Multiplication:** $(1 + 2X)(2 + 3X) = 2 + 7X + 6X^2$. But, we need to reduce mod $(X^2 + 1)$. So notice that

$$6X^2 + 7X + 2 = 6(X^2 + 1) + \underbrace{(-4 + 7X)}_{\text{result}}$$

- Division (except for by $0 + 0X$) and subtraction is also allowed.

Analogy!

In fact, $\mathbb{R}[X]/(X^2+1)$ is the same structure as complex numbers! (Formally, they are isomorphic $\mathbb{R}[X]/\langle X^2+1\rangle \cong \mathbb{C}$). For example, when we multiplied $(1+2X)(2+3X)$, we got $-4+7X$. But...

$$(1+2i)(2+3i) = 2+7i+\underbrace{6i^2}_{=-6} = -4+7i$$

Notice, that $\mathbb{R}[X]/(X^2+9)$ would have a similar structure and is also isomorphic to $\mathbb{C}$. Thus, the choice of $p(X)$ is **not unique**.

Tower of Extensions

We are ready to define $\mathbb{F}_{p^{12}}$. So,

Tower of Extensions

To define $\mathbb{F}_{p^{12}}$, we use the following objects with $\beta = -1 \in \mathbb{F}_p, \xi = 9 + u \in \mathbb{F}_{p^2}$:

$$\mathbb{F}_{p^2} = \mathbb{F}_p[u]/\langle u^2 - \beta \rangle$$
$$\mathbb{F}_{p^6} = \mathbb{F}_{p^2}[v]/\langle v^3 - \xi \rangle$$
$$\mathbb{F}_{p^{12}} = \mathbb{F}_{p^6}[w]/\langle w^2 - v \rangle$$

Visualization (sort of)

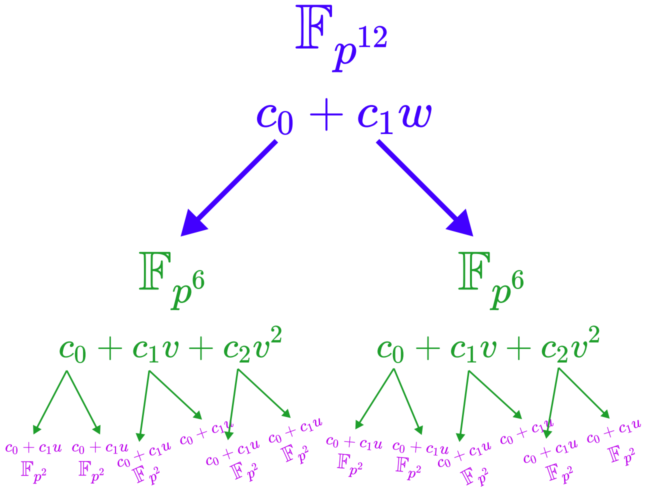


Figure: Tower of extensions visualized

Formulating more simply

More simply:

- $\mathbb{F}_{p^2}$ is a number $a + bu$ where $a, b \in \mathbb{F}_p$ and $u^2 = -1$.
- $\mathbb{F}_{p^6}$ is a number $a + bv + cv^2$ where $a, b, c \in \mathbb{F}_{p^2}$ and $v^3 = 9 + u$.
- $\mathbb{F}_{p^{12}}$ is a number $a + bw$ where $a, b \in \mathbb{F}_{p^6}$ and $w^2 = v$.

Intuition

You should regard an element from $\mathbb{F}_{p^k}$ as a regular number, but composed of k scalars from $\mathbb{F}_p$ in a "special" way.

Curves used

As mentioned, $\mathbb{G}_1$ is a regular curve $y^2 = x^3 + 3$.
However, $\mathbb{G}_2$ is a curve (called **twisted curve**):

$$y^2 = x^3 + \frac{3}{9+u}, \text{ where } x, y \in \mathbb{F}_{p^2}$$

So the element in $\mathbb{G}_2$ is described using four scalars from $\mathbb{F}_p$:

$$(a + bu, c + du), \quad a, b, c, d \in \mathbb{F}_p$$

To conclude:

- $\mathbb{G}_1$ is a group of points on the curve $y^2 = x^3 + 3$ over $\mathbb{F}_p$.
- $\mathbb{G}_2$ is a group of points on the curve $y^2 = x^3 + \frac{3}{9+u}$ over the field extension $\mathbb{F}_{p^2}$.
- $\mathbb{G}_T$ "$=$" $\mathbb{F}_{p^{12}}^{\star}$ is a multiplicative subgroup of scalars from $\mathbb{F}_{p^{12}}$.

What it takes to implement?

Calculating pairing $e(P, Q)$

1. $x \leftarrow \text{MillerLoop}(P, Q) \in \mathbb{F}_{p^{12}}$.
2. $f \leftarrow \text{FinalExp}(x) = x^{(p^{12}-1)/q} \in \mathbb{F}_{p^{12}}$.
3. **return** f.

So, one needs to:

1. Implement MillerLoop that outputs the scalar f in $\mathbb{F}_{p^{12}}$, also called a *Tate pairing*.
2. Implement final exponentiation (FinalExp) that raises f to the power of $(p^{12} - 1)/q$ – this ensures there are no equivalence classes in the output (called *Reduced Tate pairing* or simply *ate pairing*).

Again, understanding the construction requires ton of theory (in particular, from abstract geometry), but the algorithms are quite concrete.

Some excerpts from papers...

Algorithm 1 Optimal ate pairing over Barreto–Naehrig curves.

Input: $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$.

Output: $a_{\text{opt}}(Q, P)$.

Write $s = 6t + 2$ as $s = \sum_{i=0}^{L-1} s_i 2^i$, where $s_i \in \{-1, 0, 1\}$;
$T \leftarrow Q$, $f \leftarrow 1$;
for $i = L - 2$ to 0 **do**
    $f \leftarrow f^2 \cdot l_{T,T}(P)$; $T \leftarrow 2T$;
    if $s_i = -1$ **then**
        $f \leftarrow f \cdot l_{T,-Q}(P)$; $T \leftarrow T - Q$;
    else if $s_i = 1$ **then**
        $f \leftarrow f \cdot l_{T,Q}(P)$; $T \leftarrow T + Q$;
    end if
end for
$Q_1 \leftarrow \pi_p(Q)$; $Q_2 \leftarrow \pi_{p^2}(Q)$;
$f \leftarrow f \cdot l_{T,Q_1}(P)$; $T \leftarrow T + Q_1$;
$f \leftarrow f \cdot l_{T,-Q_2}(P)$; $T \leftarrow T - Q_2$;
$f \leftarrow f^{(p^{12}-1)/r}$;
return f;

Figure: Miller Loop algorithm formalized.

Some excerpts from papers...

Algorithm 31 Final Exponentiation

Require: $f \in \mathbb{F}_{p^{12}} = \mathbb{F}_{p^6}[w]/(w^2 - \gamma)$, where $f = g + hw$.

Ensure: $f^{(p^{12}-1)/r} \in \mathbb{F}_{p^{12}}$.

$f_1 \leftarrow \bar{f}$;
$f_2 \leftarrow f^{-1}$;
$f \leftarrow f_1 \cdot f_2$;
$f \leftarrow f^{p^2} \cdot f$; {Algorithm 29}
$ft_1 \leftarrow f^t$; {Algorithm 25}
$ft_2 \leftarrow f^{t^2}$;
$ft_3 \leftarrow f^{t^3}$;
$fp_1 \leftarrow f^p$; {Algorithm 28}
$fp_2 \leftarrow f^{p^2}$; {Algorithm 29}
$fp_3 \leftarrow f^{p^3}$; {Algorithm 30}
$y_0 \leftarrow fp_1 \cdot fp_2 \cdot fp_3$;
$y_1 \leftarrow f_1$;
$y_2 \leftarrow (ft_2)^{p^2}$; {Algorithm 29}
$y_3 \leftarrow (ft_1)^p$; {Algorithm 28}
$y_3 \leftarrow \bar{y_3}$;
$y_4 \leftarrow (ft_2)^p \cdot ft_1$; {Algorithm 28}
$y_4 \leftarrow \bar{y_4}$;
$y_5 \leftarrow \bar{ft_2}$;
$y_6 \leftarrow (ft_3)^p \cdot ft_3$; {Algorithm 28}
$y_6 \leftarrow \bar{y_6}$;
$t_0 \leftarrow y_6^2 \cdot y_4 \cdot y_5$; {Algorithm 24 for squaring}
$t_1 \leftarrow y_3 \cdot y_5 \cdot t_0$;
$t_0 \leftarrow t_0 \cdot y_2$;
$t_1 \leftarrow (t_1^2 \cdot t_0)^2$; {Algorithm 24 for squaring}
$t_0 \leftarrow t_1 \cdot y_1$;
$t_1 \leftarrow t_1 \cdot y_0$;
$t_0 \leftarrow t_0^2$; {Algorithm 24}
$f \leftarrow t_1 \cdot t_0$;
return f;

Figure: Final Exponentiation formalized.

So many are still uncovered...

1. Useful curve endomorphisms (Kobitz curves) for **ecmul**.
2. GLV decomposition.
3. Arithmetics over NonNativeFields.
4. Divisors and line function evaluations.
5. Embedding degree and what r-torsion subgroups are.
6. Torus $\mathbb{T}_2$ compression.
7. ...

Thanks for your attention!