Notes on bilinear pairings

Federico Barbacovi
f.barbacovi@nchain.com

January 29, 2025

Contents

1 Introduction

These notes are meant to be a companion to the Github repository zkscript. In the notes we present the material which is turned into code in the repository.

The notes are based on various references that are cited throughout. We also carry out some explicit calculations that we were not able to find in the literature. If you spot any mistake, please reach out to `f.barbacovi@nchain.com` or `research.enquiries@nchain.com`.

2 Recollections on elliptic curves

2.1 Torsion points and embedding degree

Let E be an elliptic curve over a field $\mathbb{F}_q$ of order $n = |E(\mathbb{F}_q)|$. Let r be a prime number, we define the group of r-torsion points on E as

$$E[r] := \{P \in E(\overline{\mathbb{F}_q}) : r \cdot P = \mathcal{O}\}$$

where $\mathcal{O}$ is the point at infinity.

If r is a prime divisor of n such that $\gcd(r, q) = 1$, then $E[r] \simeq (\mathbb{Z}/r\mathbb{Z})^2$ [CFA+12]. In general, $E[r]$ might be completely formed by points with coordinates in $\mathbb{F}_q$. However, this is not always the case, and to find $E[r]$ we often need to take an extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$.

Define the *embedding* degree of E to be the smallest k such that $r \nmid q^k - 1$. Then, under the assumption $r \nmid q - 1$ (i.e., $k > 1$), $\mathbb{F}_{q^k}$ is the smallest field such that $E[r] \subset E(\mathbb{F}_{q^k})$, [BK98, Thm. 1].

From now on, we assume the elliptic curve E has embedding degree $k > 1$.

2.2 Frobenius morphism

The Frobenius morphism for the curve E is defined as $\pi_q \colon E \to E, (x, y) \mapsto (x^q, y^q)$. Considering $\pi_q \in \mathrm{End}(E)$, its minimal polynomial is

$$\chi(X) = X^2 - tX + q$$

where t is called the *trace* of the Frobenius.[1]

Looking at the constant term of χ, we see that the eigenvalues of π_q are $1, q$. Indeed, $\pi_q|_{E(\mathbb{F}_q)} = \mathrm{id}$, and therefore the remaining eigenvalue is q.

We define

$$\mathbb{G}_1 = \ker(\pi_q - id) \cap E[r] \qquad \mathbb{G}_2 = \ker(\pi_q - q \cdot \mathrm{id}) \cap E[r]$$

Under the assumption that the embedding degree of E is $k > 1$, we have $\mathbb{G}_1, \mathbb{G}_2 \subset E(\mathbb{F}_{q^k})$.

[1] We have that $n = q - t + 1$ and that $|t| \leq 2\sqrt{q}$.

2.3 Line functions

Let E be an elliptic curve over a field $\mathbb{F}_{q^m}$. This means that $E \subset \mathbb{F}_q \times \mathbb{F}_{q^m}$.

For a couple of points $Q, T \in E$, let us consider the line $\ell_{Q,T}$ through Q and T (where $\ell_{Q,T}$ is the tangent line to Q if $Q = T$, and it is the vertical line through Q and T if $Q = -T$) and $\lambda_{Q,T}$ the gradient of this line. Then, we define the evaluation of $\ell_{Q,T}$ at $P \in E$ as follows:

- If $Q \neq -T$, $\ell_{Q,T}$ is given by the equation $y - y_Q = \lambda_{Q,T}(x - x_Q)$. Then
$$\mathrm{ev}_{\ell_{Q,T}}(P) := y_P - y_Q - \lambda_{Q,T}(x_P - x_Q) = y_P - y_T - \lambda_{Q,T}(x_P - x_T)$$
- If $Q = -T$, $\ell_{Q,T}$ is given by the equation $x = x_Q$. Then
$$\mathrm{ev}_{\ell_{Q,T}}(P) := x_P - x_Q = x_P - x_T$$

3 Bilinear pairings

For certain curves E and primes r, one can define an efficiently computable bilinear map
$$e \colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$$
Namely, a map such that
$$e(P + P', Q) = e(P, Q) \cdot e(P', Q) \qquad e(P, Q + Q') = e(P, Q) \cdot e(P, Q')$$

There exists various types of pairings (Weil's, Tate's, and (Optimal) Ate's [HSV06], [Ver08]), which differ for their definition and efficiency characteristics.

3.1 Structure of a pairing

Let $P \in \mathbb{G}_1, Q \in \mathbb{G}_2$, then pairings are we are interested in have the following form
$$e(P, Q) = f_{w,Q}(P)^{\frac{q^k-1}{r}}$$
where:

1. t is the trace of the Frobenius morphism
2. k is the embedding degree of E, i.e., the smallest positive k such that $r \mid q^k - 1$
3. r is the order of P and Q
4. $f_{w,Q}$ is the *Miller function* defined as the (unique up to scalar multiple) rational function on E with divisor $div(f_{w,Q}) = w[Q] - [wQ] - (w-1)[\mathcal{O}]$.

Remark 3.1. When $w = r$, we get the definition of the reduced Tate pairing, while for $w = t - 1$ we get the Ate pairing [HSV06, Thm. 1]

The computation of the pairing is divided in two parts: the computation of $f_{w,Q}(P)$, and the final exponentiation $f_{w,Q}(P) \mapsto f_{w,Q}(P)^{\frac{q^k-1}{r}}$.

3.2 The Miller loop

To compute $f_{w,Q}$, in [Mil04] Miller introduced a square-and-multiply algorithm that works as follows. Define $f_{0,Q} = 1$ and the functions $f_{i,Q}$, $i \geq 1$, as the unique ones, up to scalar multiple, that satisfy

$$div(f_{i,Q}) = i[Q] - [iQ] - (i-1)[\mathcal{O}]$$

Miller noticed that

$$f_{i+j,Q} = f_{i,Q} f_{j,Q} \frac{\ell_{iQ,jQ}}{\ell_{(i+j)Q,(i+j)Q}} \tag{1}$$

which can be used to compute $f_{w,Q}$ via square-and-multiply. Before describing the algorithm, let us notice that (1) passes on to the evaluations of the function. Hence, (1) can be used to directly compute $f_{w,Q}(P)$, see algorithm 1.

Algorithm 1 Miller's algorithm

Inputs: $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$, $w = \sum_{i=0}^{n} w_i 2^i$, $w_i \in \{-1, 0, 1\}$, $w_n \neq 0$
Output: $f_{w,Q}(P) \in \mathbb{G}_T$

$out \leftarrow 1$
if $w_n = 1$ **then**
  $T \leftarrow Q$
else
  $T \leftarrow -Q$
end if
for $i = n-1, \ldots, 0$ **do**
  $out \leftarrow out^2$
  $out \leftarrow out \cdot \frac{\mathrm{ev}_{\ell_{T,T}}(P)}{\mathrm{ev}_{\ell_{2T,2T}}(P)}$
  $T \leftarrow 2T$
  if $w_i = 1$ **then**
    $out \leftarrow out \cdot \frac{\mathrm{ev}_{\ell_{T,Q}}(P)}{\mathrm{ev}_{\ell_{T+Q,T+Q}}(P)}$
    $T \leftarrow T + Q$
  else
    $out \leftarrow out \cdot \frac{\mathrm{ev}_{\ell_{T,-Q}}(P)}{\mathrm{ev}_{\ell_{T-Q,T-Q}}(P)}$
    $T \leftarrow T - Q$
  end if
end for

3.3 Twists

The problem with using Miller's algorithm straightaway is that it requires P and Q to belong to $E(\mathbb{F}_{q^m})$ for the same m, which means that the cost to carry out the calculations might be high if m is large. In our case, we have $P, Q \in E(\mathbb{F}_{q^k})$.

To reduce the cost of the calculations in the Miller loop we use a twist of the elliptic curve E. That is, we find another elliptic curve E' such that:

- E' is defined over $\mathbb{F}_{q^{k/d}}$
- $E'(\mathbb{F}_{q^k}) \simeq E(\mathbb{F}_{q^k})$

Then, we carry out the computations of the Miller loop in $\mathbb{F}_{q^{k/d}}$, and we reduce their cost.

3.3.1 Types of twists and their equations

Below are the equation of E and E' in short Weierstrass

$$E : y^2 = x^3 + ax + b \qquad E' : y^2 = x^3 + \omega^4 ax + \omega^6 b$$

where $\omega \in \mathbb{F}_{q^k}$. The isomorphism between E and E' (over $\mathbb{F}_{q^k}$) is given by:

$$\Psi^{-1} \colon E' \to E : (x, y) \mapsto (\omega^2 x, \omega^3 y)$$

The twists differ depending on the characteristics of ω [Cos, Sec. 4.3]:

- Quadratic twists: in this case $d = 2$, $\omega^2 \in \mathbb{F}_{q^{k/2}}$. Then, E' is defined over $\mathbb{F}_{q^{k/2}}$.
- Cubic twists: possible only when $a = 0$; in this case $d = 3$, $\omega^3 \in \mathbb{F}_{q^{k/3}}$, $\omega^2 \in \mathbb{F}_{q^k} \setminus \mathbb{F}_{q^{k/3}}$. Then, E' is defined over $\mathbb{F}_{q^{k/3}}$.
- Quartic twists: possible only when $b = 0$; in this case $d = 4$, $\omega^4 \in \mathbb{F}_{q^{k/4}}$, $\omega^2 \in \mathbb{F}_{q^{k/2}}$, $\omega^2 \in \mathbb{F}_{q^k} \setminus \mathbb{F}_{q^{k/2}}$. Then, E' is defined over $\mathbb{F}_{q^{k/4}}$.
- Sextic twists: possible only when $a = 0$; in this case $d = 6$, $\omega^6 \in \mathbb{F}_{q^{k/6}}$, $\omega^3 \in \mathbb{F}_{q^{k/3}}$, $\omega^2 \in \mathbb{F}_{q^{k/2}}$. Then, E' is defined over $\mathbb{F}_{q^{k/6}}$.

For any twist, the isomorphism Ψ maps:

$$E(\mathbb{F}_{q^k}) \supset \mathbb{G}_2 \xrightarrow{\Psi^{-1}} \Psi^{-1}(\mathbb{G}_2) \subset E'(\mathbb{F}_{q^{k/d}})$$

and therefore points of $\mathbb{G}_2$ can be thought as being defined over $\mathbb{F}_{q^{k/d}}$. From now on, we will conflate $\mathbb{G}_2$ and its image under Ψ^{-1}.

3.3.2 Using the twist in Miller's algorithm

Fix E and its twist E'. Then, $\mathbb{G}_1 \subset E(\mathbb{F}_q)$ and $\mathbb{G}_2 \subset E'(\mathbb{F}_{q^{k/d}})$, where d is the degree of the twist. To carry out the calculations of the Miller loop, we can proceed in two ways. Either we perform the computations in the twisted curve, or in the base curve. Namely, we either compute

$$\mathrm{ev}_{\ell_{T,Q}}(\Psi^{-1}(P))$$

or

$$\mathrm{ev}_{\ell_{\Psi(T),\Psi(Q)}}(P)$$

The fact that we obtain the same result in either case is a consequence of the following lemmas.

Lemma 3.1. *Ψ sends the line $\ell_{T,Q}$ to the line $\ell_{\Psi(T),\Psi(Q)}$.*

Proof. Assume $T \neq -Q$. If $(x, y) \in \ell_{T,Q}$, then $(x', y') = \Psi(x, y)$ satisfies

$$y' - \frac{y_Q}{\omega^3} = \frac{\lambda_{T,Q}}{\omega}\left(x' - \frac{x_Q}{\omega^2}\right)$$

An easy calculation shows $\lambda_{T,Q} = \omega \cdot \lambda_{\Psi(T),\Psi(Q)}$, and therefore $\Psi(x, y) \in \ell_{\Psi(Q),\Psi(T)}$.

If $T = -Q$, then $(x, y) \in \ell_{T,Q}$ means $x = x_T$, and therefore $x/\omega^2 = x_{\Psi(T)}$, which means $\Psi(x, y) \in \ell_{\Psi(T),\Psi(Q)}$. □

Lemma 3.2. *Let $P \in \mathbb{G}_1$. Then, we have*

$$\mathrm{ev}_{\ell_{T,Q}}(\Psi^{-1}(P)) = \omega^{3-\delta(T,-Q)}\mathrm{ev}_{\ell_{\Psi(T),\Psi(Q)}}(P)$$

where $\delta(T, -Q) = 1$ if $T = -Q$ and 0 otherwise.

Proof. We focus on the case $T \neq -Q$, the case $T = -Q$ is similar. From the above lemma, we know that $\ell_{\Psi(T),\Psi(Q)}$ has equation $y - y_Q/\omega^3 = \lambda_{TQ}/\omega \cdot (x - x_Q/\omega^3)$. Hence, we have

$$\mathrm{ev}_{\ell_{T,Q}}(\Psi^{-1}(P)) = y_P\omega^3 - y_Q - \lambda_{T,Q}(x_P\omega^2 - x_Q)$$

and

$$\mathrm{ev}_{\ell_{\Psi(T),\Psi(Q)}}(P) = y_P - y_Q/\omega^3 - \lambda_{T,Q}/\omega \cdot (x_P - x_Q/\omega^2)$$

□

Hence, when implementing Miller's algorithm, we are free to choose the curve that makes the computations more efficient: E or its twist E'. Below is the Miller's algorithm when Q is considered as a point in $E'(\mathbb{F}_{q^{k/d}})$ with the calculations carried out on the twisted curve

3.4 Denominator elimination

One drawback of Miller's algorithm as we have described it is that it requires dividing by $\mathrm{ev}_{\ell_{2T,2T}}(\Psi^{-1}(P))$ and $\mathrm{ev}_{\ell_{T\pm Q,T\pm Q}}(\Psi^{-1}(P))$. As dividing is an expensive operation, it would be nice if we could get rid of it.

The solution is to use a technique known as *denominator elimination*. The idea is the following: if $\mathrm{ev}_{\ell_{2T,2T}}(\Psi^{-1}(P))$ and $\mathrm{ev}_{\ell_{T\pm Q,T\pm Q}}(\Psi^{-1}(P))$ belong to a subfield of $\mathbb{F}_{q^k}$ such that their $(q^k - 1)/r$-th power is 1, then we can avoid computing them, as they will be mapped to 1 by the final exponentiation and will not affect the value of the pairing.

The technique of denominator elimination has been described for all types of twists:

Algorithm 2 Miller's algorithm on twisted curve

Inputs: $P \in \mathbb{G}_1 \subset E(\mathbb{F}_q)$, $Q \in \mathbb{G}_2 \subset E'(\mathbb{F}_{q^{k/d}})$, $w = \sum_{i=0}^{n} w_i 2^i$, $w_i \in \{-1, 0, 1\}$, $w_n \neq 0$

Output: $f_{w,Q}(P) \in \mathbb{G}_T$

$out \leftarrow 1$
if $w_n = 1$ **then**
  $T \leftarrow Q$
else
  $T \leftarrow -Q$
end if
for $i = n-1, \ldots, 0$ **do**
  $out \leftarrow out^2$
  $out \leftarrow out \cdot \frac{\mathrm{ev}_{\ell_{T,T}}(\Psi^{-1}(P))}{\mathrm{ev}_{\ell_{2T,2T}}(\Psi^{-1}(P))}$
  $T \leftarrow 2T$
  if $w_i = 1$ **then**
    $out \leftarrow out \cdot \frac{\mathrm{ev}_{\ell_{T,Q}}(\Psi^{-1}(P))}{\mathrm{ev}_{\ell_{T+Q,T+Q}}(\Psi^{-1}(P))}$
    $T \leftarrow T + Q$
  else
    $out \leftarrow out \cdot \frac{\mathrm{ev}_{\ell_{T,-Q}}(\Psi^{-1}(P))}{\mathrm{ev}_{\ell_{T-Q,T-Q}}(\Psi^{-1}(P))}$
    $T \leftarrow T - Q$
  end if
end for

- Quadratic, quartic, sextic twists: $\omega^2 \in \mathbb{F}_{q^{k/2}}$; as $(k/2) \mid k$ and $r \nmid q^m - 1$ for $m < k$, $q^{k/2} - 1 \mid \frac{q^k-1}{r}$ (see also subsection 3.5). Hence[2]

$$\mathrm{ev}_{\ell_{T\pm Q,T\pm Q}}(\Psi^{-1}(P)) = x_{T\pm Q} - \omega^2 x_P \in \mathbb{F}_{q^{k/2}} \tag{2}$$

and

$$\mathrm{ev}_{\ell_{T\pm Q,T\pm Q}}(\Psi^{-1}(P))^{\frac{q^k-1}{r}} = \mathrm{ev}_{\ell_{T\pm Q,T\pm Q}}(\Psi^{-1}(P))^{(q^{k/2}-1)\frac{q^k-1}{(q^{k/2}-1)r}} = 1$$

- Cubic twists: see [LZZW07, Lem. 1].

Remark 3.2. Note that a similar calculation to (2) holds for $\mathrm{ev}_{\ell_{\Psi(T\pm Q),\Psi(T\pm Q)}}(P)$:

$$\mathrm{ev}_{\ell_{\Psi(T\pm Q),\Psi(T\pm Q)}}(P) = \frac{x_{T\pm Q}}{\omega^2} - x_P \in \mathbb{F}_{q^{k/2}}$$

Below is Miller's algorithm (3) on the twisted curve, leveraging denominator elimination for a quadratic, quartic or sextic twist.

Algorithm 3 Miller's algorithm on twisted curve with denominator elimination

Inputs: $P \in \mathbb{G}_1 \subset E(\mathbb{F}_q)$, $Q \in \mathbb{G}_2 \subset E'(\mathbb{F}_{q^{k/d}})$, $w = \sum_{i=0}^{n} w_i 2^i$, $w_i \in \{-1, 0, 1\}$, $w_n \neq 0$
Output: $f_{w,Q}(P) \in \mathbb{G}_T$

```
out ← 1
if w_n = 1 then
    T ← Q
else
    T ← −Q
end if
for i = n − 1, . . . , 0 do
    out ← out^2
    out ← out · ev_{ℓ_{T,T}}(Ψ^{−1}(P))
    T ← 2T
    if w_i = 1 then
        out ← out · ev_{ℓ_{T,Q}}(Ψ^{−1}(P))
        T ← T + Q
    else
        out ← out · ev_{ℓ_{T,−Q}}(Ψ^{−1}(P))
        T ← T − Q
    end if
end for
```

Now that we do not divide by $\mathrm{ev}_{\ell_{T+Q,T+Q}}(\Psi^{-1}(P))$, it is not clear whether Miller's algorithm can be carried out both on the base curve and on the twisted curve. The following lemma shows this is the case in the case of quadratic, quartic, and sextic twists.

[2] A similar calculation holds for $\mathrm{ev}_{\ell_{2T,2T}}(\Psi^{-1}(P))$.

Lemma 3.3. *Let $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$. Write* $\mathrm{miller}_{base}(-,-)$ *for Miller's algorithm with denominator elimination on the base curve, and* $\mathrm{miller}_{twisted}(-,-)$ *for the one on the twisted curve. Then,* $\mathrm{miller}_{twisted}(P,Q) = u \cdot \mathrm{miller}_{base}(P,Q)$ *for $u \in \mathbb{F}_{q^k}$ such that $u^{\frac{q^k-1}{r}} = 1$.*

Proof. We present the proof for the case of quadratic, quartic and sextic twists, but it easy to adapt it to the case of cubic twists using the results of [LZZW07].

Recall that by Lemma 3.2 evaluations on the base and twisted curve differ by a power of ω. Hence, $\mathrm{miller}_{twisted}(P,Q)$ and $\mathrm{miller}_{base}(P,Q)$ differ by a power of ω, and it is enough to show that such a power is mapped to 1 by the final exponentiation. As we are dealing with quadratic, quartic, or sextic twists, we have $\omega^2 \in \mathbb{F}_{q^{k/2}}$. Now, $(k/2) \mid k$ and $r \nmid q^m - 1$ for $m < k$, $q^{k/2} - 1 \mid \frac{q^k-1}{r}$ (see also subsection 3.5) imply

$$\omega^{\frac{q^k-1}{r}} = \left(\omega^2\right)^{\frac{(q^{k/2}-1)(q^{k/2}+1)}{2r}} = 1$$

□

Remark 3.3. It is easy to adapt the previous proof to the case of cubic twists with $q = 1 \mod 3$.

3.5 Final exponentiation

The last part of the computation of the pairing requires computing the $(q^k - 1)/r$-th power of the output of Miller's algorithm. We write $\Phi_n(x)$ for the n-cyclotomic polynomial. It holds that

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

Moreover, it is easy to show by induction that $\Phi_n(0) = 1$ for all $n > 1$ ($\Phi_1(x) = x - 1$).

As $r \mid q^k - 1$, and k is the smallest positive integer for which this relation holds, it follows that $r \mid \Phi_k(q)$. Indeed, if $r \mid \Phi_m(q)$ with $m < k$, then $r \mid q^m - 1$, which is in contrast with the definition of k.

Hence, the final exponentiation can be divided in two parts:

$$\frac{q^k - 1}{r} = \frac{q^k - 1}{\Phi_k(q)} \frac{\Phi_k(q)}{r}$$

The term

$$f_{w,Q}(P)^{\frac{q^k-1}{\Phi_k(q)}} \tag{3}$$

is easy to compute because $\frac{q^k-1}{\Phi_k(q)} + 1$ is a sum of powers of q, which can be easily computed using the Frobenius. The only difficult bit of (3) is that it requires the inversion of $f_{w,Q}(P)$ (this is because the polynomial $\frac{x^k-1}{\Phi_k(x)}$ has constant term equal to -1).

Once the easy part of the exponentiation has been computed, then one is left to compute the hard part:

$$\left(f_{w,Q}(P)^{\frac{q^k-1}{\Phi_k(q)}}\right)^{\frac{\Phi_k(q)}{r}}$$

Each curve has a different implementation of the hard exponentiation. The only characteristic that is common to all curves is that (3) lies in the cyclotomic subgroup, i.e., $(3)^{\Phi_k(q)} = 1$. This is helpful because, as $\Phi_k(x)$ has constant term equal to 1, it means that the inverse of (3) can be computed by means of the Frobenius morphism.

4 Optimisations

4.1 Parallel execution of multiple Miller loops

When computing $\prod f_{w,Q_j}(P_j)$ for many couples (P_j, Q_j), the most efficient thing to do is to compute the Miller loops[3] in parallel. Indeed, as the Miller loop is a square-and-multiply loop, by executing various loops in parallel we can reuse the squarings. Algorithm 4 is the description of a multi Miller loop on the twisted curve with denominator elimination for a quadratic, quartic or sextic twist.

As noted by [Sco19], the parallel execution of various Miller loops permits leveraging the structure of line evaluations. Indeed, line evaluations live in $\mathbb{F}_{q^k}$, but it is not necessarily true that all the coefficients in their representation are non-zero. It is often the case that the elements $\mathrm{ev}_{\ell_{T,T}}(\Psi^{-1}(P))$ and $\mathrm{ev}_{\ell_{T,Q}}(\Psi^{-1}(P))$ are sparse (they have many zero coefficients) and therefore computing the products

$$\prod_j \mathrm{ev}_{\ell_{T_j,T_j}}(\Psi^{-1}(P_j))$$

is more efficient than computing products between elements in $\mathbb{F}_{q^k}$ (because it requires fewer operations).

4.2 Removing the final exponentiation

It is often the case that the heaviest part of the calculation of a pairing is the final exponentiation. In [NE24], the authors explain how to get rid of the final exponentiation when the goal is to verify an equality of the from

$$\prod_j e(P_j, Q_j) = 1$$

rather than an explicit calculation of the pairings $e(P_j, Q_j)$.

The idea is the following. The final exponentiation in the definition of a pairing is required to make the value of the pairing unambiguous. Namely,

[3] With the term Miller loop we refer to the loop in Miller's algorithm.

Algorithm 4 Multi Miller's algorithm on twisted curve with denominator elimination

Inputs: $P_j \in \mathbb{G}_1$, $Q_j \in \mathbb{G}_2$, $j = 1, \ldots, m$, $w = \sum_{i=0}^{n} w_i 2^i$, $w_i \in \{-1, 0, 1\}$, $w_n \neq 0$

Output: $\prod_j f_{w,Q_j}(P_j) \in \mathbb{G}_T$

$out \leftarrow 1$
if $w_n = 1$ **then**
  $T_j \leftarrow Q_j$
else
  $T_j \leftarrow -Q_j$
end if
for $i = n-1, \ldots, 0$ **do**
  $out \leftarrow out^2$
  $out \leftarrow out \cdot \prod_j \mathrm{ev}_{\ell_{T_j,T_j}}(\Psi^{-1}(P_j))$
  $T_j \leftarrow 2T_j$
  if $w_i = 1$ **then**
    $out \leftarrow out \cdot \prod_j \mathrm{ev}_{\ell_{T_j,Q_j}}(\Psi^{-1}(P_j))$
    $T_j \leftarrow T_j + Q_j$
  else
    $out \leftarrow out \cdot \prod_j \mathrm{ev}_{\ell_{T_j,-Q_j}}(\Psi^{-1}(P_j))$
    $T_j \leftarrow T_j - Q_j$
  end if
end for

the value of the pairing is only defined in $f_{w,Q}(P) \in \mathbb{F}_{q^k}/(\mathbb{F}_{q^k}^*)^r$, and to avoid considering equivalence classes, we remove ambiguity by raising the output of the Miller loop to $(q^k - 1)/r$. However, if our goal is to show $e(P, Q) = 1$, then it is enough to produce a value $c \in \mathbb{F}_{q^k}$ such that

$$f_{w,Q}(P) = c^r \implies e(P, Q) = (c^r)^{\frac{q^k-1}{r}} = 1$$

The story is not so easy because computing the r-th power of c is not much more efficient than computing the $\frac{q^k-1}{r}$-th power of $f_{w,Q}(P)$. To address this inefficiency, the authors of [NE24] employ Optimal Ate pairings [Ver08]. In a nutshell, they replace w with a multiple λ of r for which $f_{\lambda,Q}(P)$ is efficient to compute and for which one can embed the calculation of c^λ inside the Miller loop. We refer to [NE24] for more details.

Presently, we do not implement the removal of the final exponentiation in the zkscript codebase.

4.3 Verifying instead of computing

As our goal is to implement bilinear pairings on-chain to verify a Groth16 proof, we do not need to carry out all the computations on-chain. We can delegate some computations off-chain, as long as we *verify* on-chain that the data we use is correct.

4.3.1 Inverse of the Miller output

As we remarked in subsection 3.5, the final exponentiation can be split in two parts. The most cumbersome bit of the easy part is the fact that we need the inverse of $f_{w,Q}(P)$. Instead of computing the inverse on-chain, we get it as an input z' and on-chain we verify $z' \cdot f_{w,Q}(P) = 1 \in \mathbb{F}_{q^k}$, to ensure $z' = f_{w,Q}(P)^{-1}$.

4.3.2 Gradients

To calculate $f_{w,Q}(P)$, we must calculate wQ. Each step in the calculation of wQ requires computing the gradient of the line between two points in $E'(\mathbb{F}_{q^{k/d}})$, which in turn requires inverting an element in $\mathbb{F}_{q^{k/d}}$. Instead of computing the gradients, we get them as input and we verify their correctness. The verification can take two forms according to whether Q is fixed or not:

- If Q is not fixed, given the gradient, we verify that is correct by replacing the inversion with a multiplication (similarly to what we did in subsubsection 4.3.1)
- If Q is fixed, as suggested in [NE24], we construct a commitment to all the gradients needed for the calculation of wQ, and check that the gradients given as input reconstruct the commitment.[4]

5 Examples

5.1 BLS12

For BLS12 curves, see [BLS02], [FST06], and BLS12-381 for the rest of us.

BLS12 curves are defined by equations of the form $y^2 = x^3 + b$ where b is a parameter of the specific BLS12 curve, and

$$q = \frac{(u-1)^2(u^4 - u^2 + 1)}{3} + u$$

is a prime dependent on a seed u.

BLS12 curves have trace $t = u+1$, embedding degree 12, and $r = u^4 - u^2 + 1$. The Ate pairing for these curves is defined by:

$$e(P, Q) := f_{u,Q}(P)^{\frac{(q^{12}-1)}{r}}$$

Remark 5.1. In zkscript, we have implemented the bilinear pairing for the BLS12-381 curve, whose parameters are:

$$u = -(2^{63} + 2^{62} + 2^{60} + 2^{57} + 2^{48} + 2^{16}) \qquad b = 4$$

[4] This way of verifying the correctness of the gradients has not yet been implemented in zkscript.

5.2 Field extensions

Take $u = 3 \mod 8$. Then, the field extensions for BLS12 curves are defined as follows:

$$\begin{aligned}
\mathbb{F}_{q^2} &= \mathbb{F}_q[u]/(u^2+1) \\
\mathbb{F}_{q^4} &= \mathbb{F}_{q^2}[s]/(s^2-\xi) \\
\mathbb{F}_{q^6} &= \mathbb{F}_{q^2}[v]/(v^2-\xi) \\
\mathbb{F}_{q^{12}} &= \mathbb{F}_{q^6}[w]/(w^2-v) = \mathbb{F}_{q^4}[r]/(r^3-s)
\end{aligned}$$

where $\xi = 1 + u$.

Note we have an isomorphism

$$\varphi \colon \mathbb{F}_{q^6}[w]/(w^2-v) \to \mathbb{F}_{q^4}[r]/(r^3-s)$$

mapping $\varphi(w) = r$.

5.2.1 Twists

Each BLS12 curve admits a sextic twists, but the twist can be of two types: a D-twist or an M-twist. A D-twist is defined by

$$E'_D : y^2 = x^3 + \omega^6 b \qquad \omega^{-1} = w$$

while an M-twist is defined by

$$E'_M : y^2 = x^3 + \omega^6 b \qquad \omega = w$$

Lemma 5.1. *Let E be a BLS12 curve with equation $y^2 = x^3 + b$ and $u = 3 \mod 8$. Then, if E admits a D-twist E'_D, we have*

$$\mathrm{ev}_{\ell_{\Psi(T)\Psi(Q)}}(P) = y_P + (\lambda_{T,Q}x_Q - y_Q)s + r(-\lambda_{T,Q}x_P) \in \mathbb{F}_{q^{12}} = \mathbb{F}_{q^4}[r]/(r^3-s)$$

while if E admits an M-twist E'_M we have

$$\mathrm{ev}_{\ell_{TQ}}(\Psi^{-1}(P)) = -y_Q + \lambda_{T,Q}x_Q + y_P s + r^2(-\lambda_{T,Q}x_P) \in \mathbb{F}_{q^{12}} = \mathbb{F}_{q^4}[r]/(r^3-s)$$

Proof. We show the calculation for M-twists, the one for D-twists being similar. We have

$$\begin{aligned}
\mathrm{ev}_{\ell_{T,Q}}(\Psi^{-1}(P)) &= y_P\omega^3 - y_Q - \lambda_{T,Q}(x_P\omega^2 - x_Q) \\
&= y_P w^3 - y_Q - \lambda_{T,Q}(x_P w^2 - x_Q) \\
&\overset{\varphi}{\mapsto} -y_Q + \lambda_{T,Q}x_Q + y_P s + r^2(-\lambda_{T,Q}x_P)
\end{aligned}$$

where we used $\varphi(\omega) = \varphi(w) = r$ and $\varphi(\omega^3) = r^3 = s$. □

Note that the line evaluations in Lemma 5.1 are sparse elements (only five $\mathbb{F}_q$ elements are required to represent them, not 12). Therefore, calculations in the Miller loop can be optimised by taking into account the structure of the line evaluations. This is what we do in out implementation.

5.3 MNT4

For MNT4 curves, see [MNT].

MNT4 curves E are defined by a seed u for which E is defined over $\mathbb{F}_q$ with $q = u^2 + u + 1$. The trace of the Frobenius can either be $t = -u$ or $t = u + 1$, while the embedding degree is 4.

5.3.1 MNT4-753

The MNT4-753 curve is defined by the seed u found here (arkworks) and has trace $t = u + 1$, $r = u^2 + 1$. The curve equation is $E : y^2 = x^3 + ax + b$, with $a = 2$ coefficient b found here (arkworks).

Twists MNT4-753 admits a quadratic twists E' defined over

$$\mathbb{F}_{q^2} = \mathbb{F}_q[u]/(u^2 - 13)$$

whose equation is $E' : y^2 = x^3 + Ax + B$, where

$$A = a \cdot 13 \in \mathbb{F}_{q^2} \qquad B = (b \cdot 13)u \in \mathbb{F}_{q^2}$$

E and E' are isomorphic over $\mathbb{F}_{q^4} = \mathbb{F}_{q^2}[r]/(r^2 - u)$. Note that the element ω for which E' has equation $y^2 = x^3 + a\omega^4 x + b\omega^6$ is $\omega = r$.

Line functions The formula for line evaluations in MNT4-753 is given below.

Lemma 5.2. *For MNT4-753, we have*

$$\mathrm{ev}_{\ell_{T,Q}}(\Psi^{-1}(P)) = -y_Q + \lambda_{T,Q} \cdot (x_Q - x_P \cdot u) + y_P \cdot ru \in \mathbb{F}_{q^4}$$

Proof.

$$\begin{aligned}\mathrm{ev}_{\ell_{T,Q}}(\Psi^{-1}(P)) &= y_P\omega^3 - y_Q - \lambda_{T,Q}(x_P\omega^2 - x_Q) \\ &= y_P r^3 - y_Q - \lambda_{T,Q}(x_P r^2 - x_Q) \\ &= -y_Q + \lambda_{T,Q} \cdot (x_Q - x_P \cdot u) + y_P \cdot ru\end{aligned}$$

where we used $r^2 = u$, $r^3 = ru$. □

References

[BK98] R. Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the menezes—okamoto—vanstone algorithm. *Journal of Cryptology*, 11(2):141–145, 1998.

[BLS02] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. Constructing elliptic curves with prescribed embedding degrees. Cryptology ePrint Archive, Paper 2002/088, 2002.

[CFA+12] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography, Second Edition.* Chapman & Hall/CRC, 2nd edition, 2012.

[Cos] C. Costello. Pairings for beginners.

[FST06] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. Cryptology ePrint Archive, Paper 2006/372, 2006.

[HSV06] F. Hess, N. P. Smart, and F. Vercauteren. The eta pairing revisited. Cryptology ePrint Archive, Paper 2006/110, 2006.

[LZZW07] Xibin Lin, Chang-An Zhao, Fangguo Zhang, and Yanming Wang. Computing the ate pairing on elliptic curves with embedding degree $k = 9$. Cryptology ePrint Archive, Paper 2007/434, 2007.

[Mil04] Victor S. Miller. The weil pairing, and its efficient calculation. *Journal of Cryptology*, 17(4):235–261, 2004.

[MNT] Atsuko Miyaji, Masaki Nakabayashi, and Shunzou Takano. New explicit conditions of elliptic curve traces for FR-reduction. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science.

[NE24] Andrija Novakovic and Liam Eagen. On proving pairings. Cryptology ePrint Archive, Paper 2024/640, 2024.

[Sco19] Michael Scott. Pairing implementation revisited. Cryptology ePrint Archive, Paper 2019/077, 2019.

[Ver08] F. Vercauteren. Optimal pairings. Cryptology ePrint Archive, Paper 2008/096, 2008.