The Weil pairing is just two applications of the Tate pairing

Tate pairing and Miller's algorithm

Sven Laur

08.04.2003

Elliptic curve over $\mathbb{F}_q$ is defined by *Weierstrass equation*

$$E: \; y^2 + a_1xy + a_3y = x^3 + a_2x_2 + a_4x + a_6, \qquad a_i \in \mathbb{F}_q.$$

Non-singular elliptic curves have no points, where all partial derivatives will vanish. All curve points are taken from the algebraic closure $\overline{K}$ of $\mathbb{F}_q$ except the infinity point $\mathcal{O}$.

All $\mathbb{F}_q$*-rational points* and all $\mathbb{F}_{q^k}$*-rational points*

$$E(\mathbb{F}_q) = \{(x,y) \in E \mid x, y \in \mathbb{F}_q\} \cup \{\mathcal{O}\}$$
$$E(\mathbb{F}_{q^k}) = \left\{(x,y) \in E \mid x, y \in \mathbb{F}_{q^k}\right\} \cup \{\mathcal{O}\}$$

form a sub-groups of E so that $E(\mathbb{F}_q) \subseteq E(\mathbb{F}_{q^k}) \subseteq E$.

Supersingular elliptic curves are all curves that satisfy

$$\#E(\mathbb{F}_q) \equiv 1 \mod p,$$

where p is the characteristic of $\mathbb{F}_q$.

The elements which order divides r form the r*-torsion sub-group*

$$E[r] = \{P \in E \mid rP = \mathcal{O}\}$$

If r and q are coprime numbers then the $E[r] \cong \mathbb{Z}_r \oplus \mathbb{Z}_r$.

If r is a prime number then for an arbitrary extension L of the field $\mathbb{F}_q$

$$E(L)[r] = E[r] \cap E(L)$$

is isomorphic to 0, $\mathbb{Z}_r$ or $\mathbb{Z}_r \oplus \mathbb{Z}_r$.

Exist a minimal sub-group $\mathbb{F}_{q^k}$ so that $E[r] \subseteq E(\mathbb{F}_{q^k})$ and $r \mid q^k - 1$ since the Weil pairing ensures existence of the primitive rth root.

For the Tate pairing we need subgroup $G_1 \subseteq E(\mathbb{F}_q)$ such that $r = \#G_1$.

We have two alternatives $G_1 \subsetneq E(\mathbb{F}_q)$ or $G_1 = E(\mathbb{F}_q)$ but both imply

$$r \mid \#E(\mathbb{F}_q).$$

The construction of Tate pairing favors following supersingular curves

Curve	Field	Order	k
$y^2 = x^3 + x$	$\mathbb{F}_p$	$p+1$	2
$y^2 + y = x^3 + x$	$\mathbb{F}_{2^m}$	$2^m + 1 + 2^{(m+1)/2}$	4
$y^2 + y = x^3 + x + 1$	$\mathbb{F}_{2^m}$	$2^m + 1 - 2^{(m+1)/2}$	4
$y^2 = x^3 - x + 1$	$\mathbb{F}_{3^m}$	$3^m + 1 + 3^{(m+1)/2}$	6
$y^2 = x^3 - x - 1$	$\mathbb{F}_{3^m}$	$3^m + 1 - 3^{(m+1)/2}$	6

The parameter k is the smallest exponent so that all rth roots of unity are in the field $\mathbb{F}_{q^k}$.

For the curves in the table the $E(\mathbb{F}_{q^k})$ contains entire r-torsion group, since there is a nontrival authomorphis $\phi : E(\mathbb{F}_{q^k}) \to E(\mathbb{F}_{q^k})$ that maps $E(\mathbb{F}_q)$ to a different subgroup.

All two-variate polynomials over the algebraic closure $\overline{K}$ form a ideal

$$I = I\big(E/\overline{K}\big) = \big\{ f \in \overline{K}[x,y] \mid \forall P \in E:\ f(P) = 0 \big\}\,.$$

Integral domain is a factor ring

$$\overline{K}[E] = \overline{K}[X]/I\big(E/\overline{K}\big)$$

and the *function field* is the quotinet field

$$\overline{K}(E) = \left\{ \frac{f_1(x,y)}{f_2(x,y)} + I \,\middle|\, f_1, f_2 \in \overline{K}[x,y],\ f_2 \notin I \right\}$$

The *order* $\operatorname{ord}_p(f)$ of a polynomial “counts” how many “zeros or poles of f” are at the point P.

Divisors are just formal sums of curve points

$$Div(E) = \left\{ D = \sum_{P \in E} n_P (P) \;\middle|\; \text{Number of nonzero terms is finite} \right\}.$$

The *degree* of divisor is just the sum of all coefficients

$$\deg D = \sum_{P \in E} n_P.$$

Every rational function $f \in \overline{K}(E)$ has a corresponding *divisor*

$$\operatorname{div}(f) = \sum_{P \in E} \operatorname{ord}_P(f)(P)$$

Divisor D is a *principal divisor* if exists a function $f \in \overline{K}(E)$ such that

$$D = \operatorname{div}(f).$$

Two divisors D_1 and D_2 are called *linearly equivalent* $D_1 \sim D_2$ iff $D_1 - D_2$ is a principal divisor.

Principal divisors form a subgroup of $Div(E)$ since

$$\mathrm{div}(f \cdot g) = \mathrm{div}(f) + \mathrm{div}(g).$$

The divisor$D$ is a principal divisor iff $\deg D = 0$ and non-formal sum of the divisor is $\mathcal{O}$.

All curve points that have nonzero coefficients form the *support of the divisor* denoted by $\mathrm{supp}(D)$.

The *support* $\mathrm{supp}(f)$ of the function f is $\mathrm{supp}\,\mathrm{div}(f)$.

If supports of divisors D and function f are disjoint we can *evaluatuate* the function at divisor

$$f(D) = \prod_{P \in E} f(P)^{n_P}.$$

Definition of Tate pairing

Let $G = E(\mathbb{F}_{q^k})$ such that $E[r] \subseteq G$.

The Tate pairing is a function $\widehat{e} : G[r] \times G/rG \to \mathbb{F}_{q^k}^*$ defined as follows:

- Given a point $P \in G[r]$, there exists function $f \in \mathbb{F}_{q^k}(E)$ such that

$$\operatorname{div}(f) = r(P) - r(\mathcal{O}).$$

- Let D be such a divisor that

$$D \sim (Q) - (\mathcal{O}) \qquad \text{and} \qquad \operatorname{supp}(D) \cap \operatorname{supp}(f) = \emptyset$$

- Then the value of Tate pairing is $\widehat{e}(P, Q) = f(D)^{(q^k-1)/l}$.

As the supports are disjoint the evaluation $f(D)$ exists.

The existance of the function $f \in \mathbb{F}_{q^k}(E)$ and the divisor D with $\mathbb{F}_{q^k}$-rational support follows from the Miller's algorithm.

Therefore at least the codomain is correct!

The value of $\widehat{e}(P,Q)$ does not depend on the function $f \in \mathbb{F}_{q^k}(E)$. If

$$\mathrm{div}(f_1) = \mathrm{div}(f_2) \qquad \Rightarrow \qquad f_1 = \alpha f_2, \qquad \alpha \in \mathbb{F}_{q^k}.$$

Now since D has a zero degree

$$f_1(D) = \prod_{\substack{P \in E \\ n_p \neq 0}} \alpha^{n_p} f_2(P)^{n_p} = \prod_{\substack{P \in E \\ n_p \neq 0}} f_2(P)^{n_p} = f_2(D).$$

The independece of $\widehat{e}(P,Q)$ from the choice of D is equivalent to the following condition.

For every principal divisor D_1 which support is in $E(\mathbb{F}_{q^k})$ and is disjoint from $r(P) - r(\mathcal{O})$ the evaluation $f(D_1)$ is $(q^k-1)/r$th root of unity.

The claim follows from the lineary of the evaluation map

$$f(D)^{(q^k-1)/l} f(D_1)^{(q^k-1)/l} = f(D+D_1)^{(q^k-1)/r} = \widehat{e}(P,Q) = f(D)^{(q^k-1)/r}.$$

Tate pairing is well defined

For all $P \in G[r]$ and all $Q \in G$:

- The equation $\widehat{e}(\mathcal{O}, Q) = 1$ holds since f must be a constant function.
- The equation and $\widehat{e}(P, rQ) = 1$ holds.

  We can decompose

  $$D_2 = (rQ) - \mathcal{O} = \underbrace{r(Q) - r(\mathcal{O})}_{rD} + \underbrace{(rQ) - r(Q) + (r-1)(\mathcal{O})}_{D_1}$$

  $$D_2 \sim r(Q) - r(\mathcal{O}) = rD$$

  and therefore

  $$f(D_2)^{(q^k-1)/r} = f(rD)^{(q^k-1)/r} = f(D)^{q^k-1} = 1.$$

Non-degerancy

For each point $P \in G[r] \setminus \mathcal{O}$ there exists $Q \in G$ such that

$$\widehat{e}(P, Q) \neq 1.$$

The corresponding proof is non-elementary. The proof can be found in the article by Gerhard Frey and Hans-Georg Rück

”A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves”

Mathematics of Computation, 62(206):865–874, 1994.

Linearity by the first term

For any integer n the following equality holds

$$\widehat{e}(P,Q)^n = \widehat{e}(nP,Q).$$

We can decompose

$$D_{nP} = r(nP) - r(\mathcal{O}) = \underbrace{rn(P) - rn(\mathcal{O})}_{nD_1} + \underbrace{r(nP) - rn(P) + r(n-1)(\mathcal{O})}_{rD_2}.$$

Let $\mathrm{div}(f) = D_{nP}$, $\mathrm{div}(f_1) = r(P) - r(\mathcal{O})$ and $\mathrm{div}(g) = D_2$. Then

$$f = g^r f_1^n \qquad \Rightarrow \qquad g^r \in E(\mathbb{F}_{q^k}) \qquad \Rightarrow \qquad g \in E(\mathbb{F}_{q^k})$$

and therefore

$$\widehat{e}(nP,Q) = f(D)^{(q^k-1)/r} = f_1(D)^{n(q^k-1)/r} = \widehat{e}(P,Q)^n.$$

Linearity by the second term

For any integer n the following equality holds

$$\widehat{e}(P,Q)^n = \widehat{e}(P,nQ).$$

Let $[n]$ denote multiplication function $[n] : E \to E$ st. $[n](P) = nP$.

As the divisor corresponding to nQ decomposes

$$[n](D) = nD + [n](D) - nD \sim nD$$

since $[n](D) - nD$ is a principal divisor then

$$\widehat{e}(P,nQ) = f(nD)^{(q^k-1)/l} = f(D)^{n(q^k-1)/l} = \widehat{e}(P,Q)^n$$

If S and T are taken from the cyclic group G_2

$$\widehat{e}(P,S+T) = \widehat{e}(P,S)\widehat{e}(P,T).$$

Divisors of stright lines

The third intersection point of a line l_{P_1,P_2} is the curve point $(-P_1 - P_2)$.

The divisor of a stright line $l_{P,Q}$ is

$$\mathrm{div}(l_{P_1,p_2}) = (P_1) + (P_2) + (-P_1 - P_2) - 3(\mathcal{O}).$$

If the straight line is tangent

$$\mathrm{div}(l_{P,P}) = 2(P) + (-2P) - 3\mathcal{O}.$$

If the straight line is vertical

$$\mathrm{div}(l_{P,\mathcal{O}}) = (P) + (-P) - 2\mathcal{O}.$$

The working principle of Miller's algorithm

- We can construct lines through curve points.
- We start from point P and use the square-and-multiple algorithm to construct term $r(P)$ of the divisor
- All other manipulations elliminate "trash" from divisor.
  - Multiplication adds terms.
  - Division substracts terms.
  - Elliminating one term produces a new term.
- We succeed since $rP = \mathcal{O}$ and the trash will vanish in the last step.
- We evaluate the f during the construction.
- In principle we must evaluate f at $(Q + S) - (S) \sim (Q) - (\mathcal{O})$.

Square-and-multiple algorithm

Input: The r-torsion point $P \in G[r]$ and $R \in G$

Output: The value $f(R)$, where $\mathrm{div}(f) = r(P) - r(\mathcal{O})$.

$n \leftarrow \lfloor \log r \rfloor$ *** $r = \overline{r_0 \ldots r_n}$ ***

$V \leftarrow P; f \leftarrow 1$

for $i = 1$ ***to*** n **do**

$\quad f \leftarrow f^2 \cdot l_{V,V}(R)/l_{2V,\mathcal{O}}(R)$

$\quad V \leftarrow 2V$

$\quad$ **if** $r_i = 1$ **then**

$\quad\quad f \leftarrow f \cdot l_{V,P}(x,y)/l_{V+P,\mathcal{O}}(R)$

$\quad\quad V \leftarrow V + P$

return f

Correctness

First of all

$$\operatorname{div}(l_{V,V}/l_{2V,\mathcal{O}}) = 2(V) - (2V) - \mathcal{O},$$
$$\operatorname{div}(l_{V,P}/l_{V+P,\mathcal{O}}) = (V) + (P) - (V+P) - \mathcal{O}.$$

Let $a_i = \overline{r_0 r_1 \ldots r_i}$. Then at the end of the cycle

$$\begin{aligned} r_i = 0: \ \operatorname{div}(f_i) &= \operatorname{div}(f_{i-1}^2 \cdot l_{V,V}/l_{2V,\mathcal{O}}) \\ &= 2\operatorname{div}(f_{i-1}) + 2(a_{i-1}P) - (a_i P) - \mathcal{O}, \\ r_i = 1: \ \operatorname{div}(f_i) &= \operatorname{div}(f_{i-1}^2 \cdot l_{V,V}/l_{2V,\mathcal{O}} \cdot l_{2V,P}/l_{2V+P,\mathcal{O}}) \\ &= 2\operatorname{div}(f_{i-1}) + 2(a_{i-1}P) + (P) - (a_i P) - 2\mathcal{O}. \end{aligned}$$

Simple induction gives $\operatorname{div}(f_i) = a_i(P) - (a_i P) - (a_i - 1)(\mathcal{O})$.

Therefore $\operatorname{div}(f_n) = l(P) - l(\mathcal{O})$.

Why to use the cube-and-multiply algorithm?

- The supersingular curves $E : y^2 = x^3 - x \pm 1$ over $\mathbb{F}_{3^m}$ favor the tripling.
- The calculation of $3P$ does not contain divisions!
- The cubing an element $\alpha \in \mathbb{F}_{q^k}$ requires $2q$ operations in $\mathbb{F}_q$.
- The nessasary stright lines $l_{V,V}$ and $l_{V,2V}$ require only one division!
- Finally $\log_3 r < \log_2 r$.
- Additional optimization is possible!

Cube-and-multiply algorithm

Input: The r-torsion point $P \in G[r]$ and $R \in G$

Output: The value $f(R)$, where $\mathrm{div}(f) = r(P) - r(\mathcal{O})$.

$n \leftarrow \lfloor \log_3 r \rfloor$

$V \leftarrow P$; $f \leftarrow 1$

$g \leftarrow 1/(x - x_P)(R)$ $*** \ \mathrm{div}(g) = -(P) - (-P) + 2\mathcal{O} \ ***$

for $i = 1$ ***to*** n **do**

  $f \leftarrow f^3 \cdot l_{V,V}/l_{2V,\mathcal{O}} \cdot l_{V,2V}/l_{3V,\mathcal{O}}(R)$

  $V \leftarrow 3V$

  if $r_i = 1$ **then**

    $f \leftarrow f \cdot l_{V,P}/l_{V+P,\mathcal{O}}(R)$

    $V \leftarrow V + P$

  else if $r_i = -1$ **then**

    $f \leftarrow fg \cdot l_{V,-P}/l_{V-P,\mathcal{O}}(R)$

    $V \leftarrow V - P$

return f

Correctness

Let a_i be the truncated number $a_i = \overline{r_0 \ldots r_i}$ in trinary representation. Then

$$\begin{aligned}
\operatorname{div}(f_i) &= 3\operatorname{div}(f_{i-1}) + 3(a_{i-1}P) - (a_iP) - 2\mathcal{O}, && r_i = 0,\\
\operatorname{div}(f_i) &= 3\operatorname{div}(f_{i-1}) + 3(a_{i-1}P) + (P) - (a_iP) - 3\mathcal{O}, && r_i = 1,\\
\operatorname{div}(f_i) &= 3\operatorname{div}(f_{i-1}) + 3(a_{i-1}P) - (P) - (a_iP) - 3\mathcal{O}, && r_i = -1.
\end{aligned}$$

and induction gives $\operatorname{div}(f_i) = a_i(P) - (a_iP) - (a_i - 1)(\mathcal{O})$.

Note that if $R \notin E(\mathbb{F}_q)$ then algorithm can never fail since the supports of the intermediate divisors are from $E(\mathbb{F}_q)$.

For calculatting $\widehat{e}(P,Q)$ we must

- Take $S \in E(\mathbb{F}_q^k)$ such that $S \neq -Q$ and $S \notin \langle P \rangle$.
- Calculate $s_1 = f(Q+S)$.
- Calculate $s_2 = f(S)$.
- As $(Q+S)-(S) \sim (Q)-(\mathcal{O})$ we can express

$$\widehat{e}(P,Q) = (s_1 s_2^{-1})^{(q^k-1)/r}.$$

- Half of these calculations can be skipped.

For elliptic curves $E : y^2 = x^3 - x \pm 1$ the tripling and doubling is easy

$$P = (x_1, y_1), \quad 2P = (\lambda_1^2 + x_1, -\lambda_1^3 - y_1), \quad 3P = (x_1 + y_1^2 + y_1^6, -y_1^9),$$

where $\lambda_1 = 1/y_1$. We can skip $2P$ and calculate $3P$.

It takes: 2M, 3F, 2A, and 1N in $\mathbb{F}_q$.

Next the algorithm evaluates lines

$$\begin{aligned} l_{VV} &: y - \lambda_1 x + (\lambda_1 x_1 - y_1) = 0 & \qquad l_{2V,\mathcal{O}} &: x - x_2 = 0 \\ l_{V,2V} &: y - \lambda_2 x + (\lambda_2 x_1 - y_1) = 0 & \qquad l_{3V,\mathcal{O}} &: x - x_3 = 0 \end{aligned}$$

where $\lambda_2 = y_1^3 - \lambda_1$. This takes:

l_{VV} and $l_{V,2V}$: 2M, 2A, 2S in $\mathbb{F}_{q^k}$, and 2M and 2S in $\mathbb{F}_q$;

$l_{2V,\mathcal{O}}$ and $l_{3V,\mathcal{O}}$: 2S in $\mathbb{F}_{q^k}$ and 1M and 1A in $\mathbb{F}_q$;

λ_2: 1F and 1S in $\mathbb{F}_q$.

Additionally we must do 1F, 2M and 2D in $\mathbb{F}_{q^k}$.

Additional $r_i = \pm 1$ round requres less operations

$$P = (x_1, y_1), \qquad V = (x_2, y_2)$$

$$P + V = (\lambda_1^2 - x_1 - x_2, \lambda(x_2 - x_3) - y_2),$$

where $\lambda_1 = (y_2 - y_1)/(x_2 - x_1)$.

This requires 6A, 2M and 1D in $\mathbb{F}_q$.

Next the algorithm evaluates lines

$$l_{VP} : y - \lambda_1 x + (\lambda_1 x_1 - y_1) = 0 \qquad l_{P+V\mathcal{O}} : x - x_2 = 0$$

This takes:

l_{VP}: 1M, 2A in $\mathbb{F}_{q^k}$, and 1M and 1A $\mathbb{F}_q$;

$l_{V+P,\mathcal{O}}$: 1A in $\mathbb{F}_{q^k}$.

Additionally we must do (1+1)M and 1D in $\mathbb{F}_{q^k}$.

The value $g(R)$ can be precalculated.

BKLS-optimizations

If the curve is supersingular then $\widehat{e}(P,Q) = f(Q)^{(q^k-1)/r}$ as long the parameter $k > 1$.

Theorem 1. *Let P be from an r-element sub-group $G_1 \subseteq E(\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_{q^k})$ where curve parameter $k > 1$. Then*

$$\widehat{e}(P,Q) = f(Q)^{(q^k-1)/r},$$

where $\mathrm{div}(f) = r(P) - r(Q)$.

To take the subgroup $G_2 = \phi(G_1)$ such that ϕ is a special automorphism of $E(\mathbb{F}_{q^k})$. Then all the denominators can be discarded. Since their order divides $(q^k-1)/r$. However, the automorphism itself has simple form.

Primes with low weight

The basic Miller's algorithm does an additional multiplication if $r_i = 1$. Therefore it is natural to seek primes r with low Hamming weight.

The supersingular curves from the table have this property, since group orders $2^m \pm 2^{(m+1)/2+1}$ and $3^m \pm 3^{(m+1)/2} + 1$ have very low Hamming weight. The number of multiplications drops significantly.

Moreover, in the article [DL03] closed formula of the Tate pairing for supersingular curve $y^2 = x^3 - x \pm 1$ over $\mathbb{F}_{3^m}$ was obtained.

Cycle was unrolled. Last multiplication $l_{V,P} = l_{-P,P}$ was dropped and more efficient polynomial for $l_{V,V}/l_{2V,\mathcal{O}} \cdot l_{V,2V}/l_{3V,\mathcal{O}}$ was proposed.

Weil pairing

The Weil pairing $e_r : E[r] \times E[r] \to \mathbb{F}_{q^k}$ is usually computed by two applications of Tate pairing

$$e_r(P, Q) = f(D_1)/g(D_2)$$

where $\mathrm{div}(f) = (P) - (\mathcal{O})$ and $\mathrm{div}(g) = (Q) - (\mathcal{O})$.

However if $P \in E(\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_{q^k-1})$ the calculation of the denominator requires more time since $V \notin E(\mathbb{F}_q)$ in the Miller's agorithm.