Tate-Lichtenbaum pairing on EC

For elliptic curves use isomorphism

$$\mathrm{Pic}^0_E(\mathbb{F}_{q^k}) \cong E(\mathbb{F}_{q^k})$$

to define pairing on points $T_\ell(P,Q)$, with

$$D_1 = P - P_\infty, D_2 = (Q+R) - R$$

for some R.

Build F iteratively by Miller's algorithm (double-and-add).

Often

$$T_\ell : E(\mathbb{F}_{q})[\ell] \times E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \to \mathbb{F}^*_{q^k}/\mathbb{F}^{*\ell}_{q^k}.$$

Miller's algorithm

In: $\ell = \sum_{i=0}^{n-1} \ell_i 2^i$, $P, Q+R, R$
Out: $T_\ell(P,Q)$

1. $T \leftarrow P$, $F \leftarrow 1$
2. for $i = n-2$ downto 0 do
   (a) Calculate lines l and v in doubling
   $T \leftarrow 2T$
   $F \leftarrow F^2 \cdot l(Q+R)v(R)/(l(R)v(Q+R))$
   (b) if $\ell_i = 1$ then
   Calculate lines l and v in addition $T+P$
   $T \leftarrow T+P$
   $F \leftarrow F \cdot l(Q+R)v(R)/(l(R)v(Q+R))$
3. return F

Weil pairing

For an elliptic curve E define

$$\begin{aligned} W_\ell : E(\overline{\mathbb{F}}_q)[\ell] \times E(\overline{\mathbb{F}}_q)[\ell] &\rightarrow \mu_\ell \\ (P, Q) &\mapsto \frac{F_{P-P_\infty}(D_Q)}{F_{Q-P_\infty}(D_P)} \end{aligned}$$

where μ_ℓ is the multiplicative groups of the ℓ-th roots of unity in the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$.
Obviously, $W_\ell(P, P) = 1$.

Weil pairings can be seen as two-fold application of the Tate-Lichtenbaum pairing, note $Q \in E(\mathbb{F}_{q^k})$.

Needs full group of order ℓ in $E(\mathbb{F}_{q^k})$, if $k = 1$ then the Weil pairing is trivial & one needs to use larger field.

Efficient computation

k minimal

Observation:
k is minimal with $\ell \mid q^k - 1$, so final exponentiation $T_\ell(\bar{D}_1, \bar{D}_2)^{(q^k-1)/\ell}$ removes all terms from subfields.

- Choose $R \in E(\mathbb{F}_q)$, computation of $l(R)$ and $v(R)$ not needed.
- Choose $R = P_\infty$,

$$\tilde{T}_\ell(P, Q) = F_{P-P_\infty}(Q)^{(q^k-1)/\ell}.$$

- If protocol allows, choose $Q = (x_Q, y_Q) \in \mathbb{F}_{q^k}$ with x in subfield, this avoids computation of $v(Q)$. This means no extra division!

Improvements to Miller

Observation:
Let $N = c\ell$ for some c, then

$$\tilde{T}_\ell(P,Q) = T_\ell(P,Q)^{(q^k-1)/\ell} = T_N(P,Q)^{(q^k-1)/N}.$$

- Other addition chains can be used in Miller's algorithm, e.g. NAF.
  Other bases might be good depending on characteristic of the field.
- Use multiple N with low Hamming weight (in p-adic representation).
  For supersingular curves choosing N as number of points gives fast final exponentiation.

Special curves

Duursma-Lee and Barreto-Galbraith-O hEigeartaigh-Scott obtain further speed-up by choosing supersingular curves of genus $(p-1)/2$ over $\mathbb{F}_{p^r}$.

Main ideas are to use p as basis in addition chain $\Rightarrow$ much shorter chain and take into account that each order divides $p^r + 1$.

Key words are “eta-pairing” and “eta-T-pairing”.

Supersingular and ordinary

Definition

Let E be an elliptic curve defined over $\mathbb{F}_q, q = p^r$.
E is supersingular if

- $E[p^s](\overline{\mathbb{F}}_q) = \{P_\infty\}$.
- $t \equiv 0 \bmod p$.
- End_E is order in quaternion algebra.

Otherwise it is ordinary and one has $E[p^s](\overline{\mathbb{F}}_q) = \mathbb{Z}/p^s\mathbb{Z}$.
These statements hold for all s if they hold for one.

Example:

$$y^2 + y = x^3 + a_4 x + a_6 \text{ over } \mathbb{F}_{2^r}$$

is supersingular, as a point of order 2 would satisfy

$$y_P = y_P + 1$$

which is impossible.

Distortion map I

For supersingular curves it is possible to find maps $\phi : E(\mathbb{F}_q) \to E(\mathbb{F}_{q^k})$ that map to a linearly independent subgroup, i.e.

$$T'_\ell(P,P) \neq 1 \text{ for } T'_\ell(P,P) = T_\ell(P,\phi(P)).$$

(This needs that there are independent endomorphisms, so no chance for ordinary curves).
Examples:

- $y^2 = x^3 + a_4 x$, for $p \equiv 3 \pmod 4$.
  Distortion map $(x,y) \mapsto (-x, iy)$ with $i^2 = -1$
- $y^2 = x^3 + a_6$, for $p \equiv 2 \pmod 3$.
  Distortion map $(x,y) \mapsto (jx, y)$ with $j^3 = 1, j \neq 1$,

In both cases, $\#E(\mathbb{F}_p) = p + 1$, $k = 2$.

Distortion maps II

- Over $\mathbb{F}_{2^d}$ consider
$$y^2 + y = x^3 + x + a_6, \text{ with } a_6 = 0 \text{ or } 1$$
and distortion map
$$(x, y) \mapsto (x+s^2, y+sx+t),\ s, t \in \mathbb{F}_{2^{4d}},\ s^4+s = 0,\ t^2+t+s^6+s^2 = 0.$$
$$\#E(\mathbb{F}_{2^d}) = 2^d + 1 \pm 2^{(d+1)/2},\ k = 4.$$
- Over $\mathbb{F}_{3^d}$ consider
$$y^2 = x^3 + x + a_6, \quad \text{with} \quad a_6 = \pm 1$$
and distortion map
$$(x, y) \mapsto (-x + s, iy) \quad \text{with} \quad s^3 + 2s + 2a_6 = 0 \quad \text{and} \quad i^2 = -1.$$
$$\#E(\mathbb{F}_{3^d}) = 3^d + 1 \pm 3^{(d+1)/2},\ k = 6.$$

Application of distortion maps

- Distortion maps allow to state the protocols as using bilinear map
$$G_1 \times G_1 \to G.$$
- Scalar multiplications of input point can be performed over $\mathbb{F}_q$ and then mapped into $E(\mathbb{F}_{q^k})$, this saves computation time
$\Rightarrow$ obvious computational savings in the above protocols.
- Can be used to map on points with x-coordinate in subfield.
- Systems are easier to state.