TATE PAIRING

An extract of Elliptic Curve Cryptography, Winter term 2009/10

Michael Nüsken

August 5, 2010

Most of the following material is taken from Washington (2003).

1. Lift-off

Fix an elliptic curve E defined over a field $\mathbb{F}_q$ and a divisor p of the curve size $\#E(\mathbb{F}_q)$ which is coprime to the characteristic. Then (with point coordinates allowed from the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$)

$$E[p] \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

So we could define kind of a scalar product on $E[p]$ as follows. Fix a $\mathbb{Z}_p$-basis (T_1, T_2) of $E[p]$ and choose values for $e(T_i, T_j)$ in some appropriate group. Since we want e bilinear we then have $e(s_1T_1 + s_2T_2, t_1T_1 + t_2T_2) = \sum_{i,j} s_i e(T_i, T_j) t_j$. Actually, we want more: the pairing must also be non-degerenate, that is, if for all $T \in E[p]$ we have $e(S,T) = 0$ then we have $S = \mathcal{O}$, and also if for all $S \in E[p]$ we have $e(S,T) = 0$ then we have $T = \mathcal{O}$. We can grant this by requiring that the matrix $[e(T_i, T_j)]_{i,j}$ is invertible. All these things are now pairings on the p-torsion. However, we do not know anything about how to compute the pairing efficiently nor whether this is compatible with possible algebraic structures. In that light, it is only a minor complication to take a multiplicatively written group for the values: Let

$$\mu_p = \left\{ x \in \overline{k} \,\middle|\, x^p = 1 \right\}$$

be the group of pth roots of unity. Since p is coprime to the characteristic we have $\#\mu_p = p$ and so μ_p is a cyclic group of order p.

We will consider the (modified) Tate pairing τ_p which is slightly easier to compute than the Weil pairing e_p. The two are connected by a congruence of the form

$$e_p(S,T) \equiv \frac{\langle T, S\rangle_p}{\langle S, T\rangle_p}.$$

The Weil pairing is obviously antisymmetric, ie. $e_p(T,S) = e_p(S,T)^{-1}$. Actually, $e_p(S,S) = 1$ and so we cannot use it for cryptography in the symmetric setting although it has $G_1 = G_2 = E[p]$.

2. Divisors

Consider the simplest possible non-trivial function: a line $f = ax + by + c$. [By abuse of language we also call the function 'line', though strictly speaking the line is given by the solutions of $f = 0$.] Say, it passes through the points $P_1, P_2, P_3 \in E$. If $b \neq 0$ then the line does not pass through $\mathcal{O}$ and f has a triple pole there. We obtain

$$\operatorname{div}(ax + by + c) = [P_1] + [P_2] + [P_3] - 3[\mathcal{O}].$$

If $b = 0$ then the line passes through, say, $P_3 = (x_3, y_3)$, $-P_3 = (x_3, -y_3)$ and $\mathcal{O}$ and we find

$$\mathrm{div}(x - x_3) = [P_3] + [-P_3] - 2[\mathcal{O}].$$

Consequently, rewriting $P_3 = P_1 + P_2$,

$$\mathrm{div}\left(\frac{ax + by + c}{x - x_3}\right) = [P_1] + [P_2] - [P_1 + P_2] - [\mathcal{O}], \tag{1}$$

or

$$[P_1] + [P_2] = [P_1 + P_2] + [\mathcal{O}] + \mathrm{div}\left(\frac{ax + by + c}{x - x_3}\right).$$

This is related to the question which divisors are principal, ie. are divisors of a function. Since we can choose the line through any two given points $P_1, P_2 \in E$ we can replace a divisor $[P_1] + [P_2]$ with $[P_1 + P_2] + [\mathcal{O}]$ plus the divisor of some function g.

Theorem 2. *Consider an elliptic curve E and a divisor D. Then*

$$\exists f : D = \mathrm{div}(f)$$

iff

$$\mathrm{sum}(D) = \mathcal{O} \qquad \text{and} \qquad \deg(D) = 0.$$

3. Pairings

3.1. Tate pairing. Fix k such that $p \mid q^k - 1$. Given $P \in E(\mathbb{F}_q)[p]$ and $Q \in E(\mathbb{F}_{q^k})/pE(\mathbb{F}_{q^k})$. Assume f_P is a function with divisor $p[P + R] - p[R]$ for some R, and $Q_1 - Q_2 = Q$ such that $P + R, R, Q_1, Q_2$ are all different and non-zero. Then we define the *Tate-Lichtenbaum pairing* by

$$\langle \cdot, \cdot \rangle_p : \begin{array}{rcl} E(\mathbb{F}_q)[p] \times E(\mathbb{F}_{q^k})/pE(\mathbb{F}_{q^k}) & \longrightarrow & \mathbb{F}_{q^k}^\times / \left(\mathbb{F}_{q^k}^\times\right)^p, \\ (P, Q) & \longmapsto & \langle P, Q \rangle_p = \frac{f_P(Q_1)}{f_P(Q_2)}, \end{array}$$

and the *modified Tate-Lichtenbaum pairing*

$$\tau_p : \begin{array}{rcl} E(\mathbb{F}_q)[p] \times E(\mathbb{F}_{q^k})/pE(\mathbb{F}_{q^k}) & \longrightarrow & \mu_p \subseteq \mathbb{F}_{q^k}^\times, \\ (P, Q) & \longmapsto & \langle P, Q \rangle_p^{\frac{q^k - 1}{p}}. \end{array}$$

We should actually write $Q + pE(\mathbb{F}_{q^k})$ everywhere, however we can ignore it usually.

Side remark. *In practice, we will have $G_1 := E(\mathbb{F}_q)[p]$ be isomorphic to $\mathbb{Z}_p$ and map 'another' part of $E[p] \cong \mathbb{Z}_p \times \mathbb{Z}_p$ into $E(\mathbb{F}_{q^k})[p]$, so that we have a pairing defined on G_1 and another group G_2 both of order p.*

Back to our aim: given $P \in G_1 := E(\mathbb{F}_q)[p]$ and $Q \in G_2 := E(\mathbb{F}_{q^k})$ we want to compute

$$\tau_p(P, Q) = \left(\frac{f_P(Q_1)}{f_P(Q_2)}\right)^{\frac{q^k - 1}{p}}.$$

Since the final exponentiation does not pose serious problems we are left with the

Task 3. *Let $P, Q \in E$ (possibly subject to additional conditions) and assume* $\operatorname{div} f_P = p[P+R] - p[R]$ *with $R \in E$ and $Q = Q_1 - Q_2$ such that the divisor of f_P and the divisor $[Q_1] - [Q_2]$ are disjoint. Compute*

$$\frac{f_P(Q_1)}{f_P(Q_2)}.$$

3.2. Miller's algorithm. The tricky part is actually to find that function f_P. We break this down by successively solving the following, easier and slightly more complicated

Task(j). *Let $P, Q \in E$ (possibly subject to additional conditions) and assume*

$$\operatorname{div} f_j = D_j := j[P+R] - j[R] - [jP] + [\mathcal{O}]$$

with $R \in E$ such that the divisor of f_P and the divisor $D_Q = [Q_1] - [Q_2]$ with sum Q. Compute

$$\frac{f_j(Q_1)}{f_j(Q_2)}.$$

Assuming that Task(j) and Task(k) have been solved we want to derive a solution for task $j+k$. Let $\ell = ax + by + c$ be the line through jP and kP, and let $v = x + d$ be the vertical line trough $(j+k)P$. Then by (1) we have

$$\operatorname{div}\left(\frac{ax+by+c}{x+d}\right) = [jP] + [kP] - [(j+k)P] - [\mathcal{O}].$$

By assumption

$$\begin{aligned} \operatorname{div}(f_j) &= j[P+R] - j[R] - [jP] + [\mathcal{O}], \\ \operatorname{div}(f_k) &= k[P+R] - k[R] - [kP] + [\mathcal{O}]. \end{aligned}$$

Multiplying the functions we obtain

$$\operatorname{div}\left(f_j f_k \frac{ax+by+c}{x+d}\right) = (j+k)[P+R] - (j+k)[R] - [(j+k)P] + [\mathcal{O}] = D_{j+k}.$$

Consequently, $f_{j+k} = \gamma f_j f_k \frac{ax+by+c}{x+d}$ for any non-zero constant γ is 'the' function needed in Task($j+k$). Actually, we only need the evaluation of this function at D_Q:

$$\frac{f_{j+k}(Q_1)}{f_{j+k}(Q_2)} = \frac{f_j(Q_1)}{f_j(Q_2)} \cdot \frac{f_k(Q_1)}{f_k(Q_2)} \cdot \frac{\left.\frac{ax+by+c}{x+d}\right|_{(x,y)=Q_1}}{\left.\frac{ax+by+c}{x+d}\right|_{(x,y)=Q_2}} \tag{4}$$

now describes the value of f_{j+k} at D_Q. All we need are the values of f_j and f_k at D_Q, the points jP and kP. Performing the addition $jP + kP$ gives the point $(j+k)P$ and the function $\frac{ax+by+c}{x+d}$, evaluating at D_Q and then multiplying with the values of f_j and f_k at D_Q yields the desired value of f_{j+k} at D_Q along with the point $(j+k)P$.

If now $P \in E[p]$ then $pP = \mathcal{O}$. Thus solving Task(p) yields with $\mathrm{div}(f_p) = p[P+R] - p[R] - [\mathcal{O}] + [\mathcal{O}] = \mathrm{div}(f_P)$ the desired value

$$\frac{f_P(Q_1)}{f_P(Q_2)} = \frac{f_p(Q_1)}{f_p(Q_2)}.$$

Notice that Task(0) is trivial: $D_0 = 0$, so $f_0 = 1$. Also Task(1) is easy: $D_0 = [P+R] - [R] - [P] + [\mathcal{O}]$, so $f_1 = \frac{x+d}{ax+by+c}$ where $\ell = ax+by+c$ is the line through P and R and $v = x+d$ is the vertical line through $P+R$. Thus

$$\frac{f_1(Q_1)}{f_1(Q_2)} = \frac{\left.\frac{ax+by+c}{x+d}\right|_{(x,y)=Q_1}}{\left.\frac{ax+by+c}{x+d}\right|_{(x,y)=Q_2}}$$

Miller's algorithm now simply follows an addition chain for pP and performs point addition and point doublings along with multiplying the corresponding values of f_j. If we simply use add and double we obtain

Algorithm 5. Miller's algorithm.
Input: Points $P, R, Q_1, Q_2 \in E$, the desired index p.
Output: The value $\frac{f_P(Q_1)}{f_P(Q_2)}$ where $\mathrm{div}\, f_P = p[P+R] - p[R] - [pP] + [\mathcal{O}]$.

1. Compute $P+R$, the line $\ell = ax+by+c$ through P and R, the vertical line $v = x+d$ through $P+R$ and let $g \leftarrow \frac{\left.\frac{ax+by+c}{x+d}\right|_{(x,y)=Q_1}}{\left.\frac{ax+by+c}{x+d}\right|_{(x,y)=Q_2}}$.
2. Let $f \leftarrow g$, $J \leftarrow P$, $j \leftarrow 1$.
3. Write $p = (p_{r-1}, \ldots, p_1, p_0)$ in base 2.
4. For $i = r-2$ down to 0 do 5–15
5. Let $\ell = ax+by+c$ be the tangent at J.
6. $S \leftarrow 2J$.
7. Let $v = x+d$ be the vertical line through S.
8. Let $f \leftarrow f^2 \cdot \left.\frac{\ell}{v}\right|_{Q_1} \cdot \left.\frac{v}{\ell}\right|_{Q_2}$.
9. $J \leftarrow S$, $j \leftarrow 2j$.
10. If $p_i = 1$ then
11. Let $\ell = ax+by+c$ be the line through J and P.
12. $S \leftarrow J+P$.
13. Let $v = x+d$ be the vertical line trough S.
14. Let $f \leftarrow f \cdot g \cdot \left.\frac{\ell}{v}\right|_{Q_1} \cdot \left.\frac{v}{\ell}\right|_{Q_2}$.
15. $J \leftarrow S$, $j \leftarrow j+1$.
16. Return f.

As a consequence computing a pairing is only a constant factor slower than a scalar multiplication by p. (Exercise!)

References

Lawrence C. Washington (2003). *Elliptic Curves — Number Theory and Cryptography*. Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, USA. ISBN 1-58488-365-0.