The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems

Gerhard Frey, Michael Müller, Hans-Georg Rück
Institute for Experimental Mathematics
University of Essen
Ellernstr. 29, 45326 Essen (Germany)
{frey,mdm,rueck}@exp-math.uni-essen.de

October 7, 1998

1 The Tate–Lichtenbaum pairing

In the paper [F-R] it is shown how the Tate pairing on Abelian varieties in Lichtenbaum's version can be used to relate the discrete logarithm in the group $J_m(\mathbb{F}_q)$ of m–torsion points of the Mordell-Weil group of the Jacobian J of a curve over a finite field $\mathbb{F}_q$ to the discrete logarithm in $\mathbb{F}_q^*$ if $q-1$ is divisible by m.[1]

More precisely the main result of [F-R] can be stated as follows:

Theorem 1.1 *Let m be a natural number prime to q, and let $\mu_m(\mathbb{F}_q)$ be the group of roots of unity in $\mathbb{F}_q$ whose order divides m. We assume that $J(\mathbb{F}_q)$ contains a point of order m.*

1. *There is a surjective pairing*
$$\phi_m : J_m(\mathbb{F}_q) \times J(\mathbb{F}_q)/mJ(\mathbb{F}_q) \longrightarrow \mu_m(\mathbb{F}_q).$$
2. *ϕ_m is computable in $O(\log(q))$ steps, where one step is equivalent to the addition in J.*
3. *Given a cyclic subgroup C_m of order m in $J_m(\mathbb{F}_q)$ then the probability to find a point P' in $J(\mathbb{F}_q)$ with*
$$\{\phi_m(P,P'); P \in C_m\} = \mu_m(\mathbb{F}_q)$$
is positive (depending on $\dim(J)$ and m).

It may be useful for designers of discrete logarithm cryptosystems based on elliptic curves to have an explicit description of ϕ_m in the special case that J is an elliptic curve E. In addition it is helpful to know the probability finding a point P' as in the theorem.

We want to stress that a very similar procedure can be used to compute ϕ_m in the case that J is the Jacobian of a hyperelliptic curve or, more generally, in all cases in which an effective version of the theorem of Riemann–Roch is available.

[1] In [R] it is explained how to treat the case that m is a power of the characteristic of $\mathbb{F}_q$, in the case of elliptic curves see [Sem].

2 Application to elliptic curves

We assume now that E is an elliptic curve defined over $\mathbb{F}_q$. As above let m be prime to q and suppose that $E(\mathbb{F}_q)$ contains a point of order m.

Proposition 2.1 *If the trace of the Frobenius endomorphism of the elliptic curve E over $\mathbb{F}_q$ is congruent to 2 modulo m, then the discrete logarithm in $E_m(\mathbb{F}_q)$ can be reduced to the discrete logarithm in $\mathbb{F}_q^*$ "probabilistically" in polynomial time by using the Tate–Lichtenbaum pairing.*

Proof: We can apply Theorem 1.1 if and only if $\mathbb{F}_q$ contains the m-th roots of unity. The trace t of the Frobenius endomorphism and $\#E(\mathbb{F}_q)$, the number of $\mathbb{F}_q$-rational points on E are related by the well known formula

$$\#E(\mathbb{F}_q) = q + 1 - t.$$

Since $E(\mathbb{F}_q)$ contains a point of order m and since $t \equiv 2 \bmod m$, we see that $q-1$ is divisible by m. $\square$

Remark 2.2 The proposition clearly shows that the Tate–Lichtenbaum pairing can be applied in cases in which the Weil pairing does not work. Hence these two pairings should be distinguished carefully. In fact the fast algorithm used to compute the Weil pairing following V. Miller consists in a twofold computation of the Tate–Lichtenbaum pairing.

Remark 2.3 In some cases, which are the most important ones for cryptographic reasons, one can delete the word "probabilistically" in Proposition 2.1. This will be explained in the following examples.

We assume from now on that the conditions of Proposition 2.1 are satisfied, i.e. $E(\mathbb{F}_q)$ contains a point of order m and $q-1$ is divisible by m.

For a point $P \in E(\mathbb{F}_q)$ we denote by (P) the associated prime divisor of degree 1. Let ∞ be a fixed point on $E(\mathbb{F}_q)$ (usually when E is given in Weierstrass normal form, one chooses ∞ to be the point "at infinity").

It is well known ([Silv] Prop. 3.4 pp. 66) that the group $E(\mathbb{F}_q)$ is isomorphic to the class group of divisors of degree zero on E. By this isomorphism a point $P \in E(\mathbb{F}_q)$ is mapped to the class of $(P)-(\infty)$. Since it is an isomorphism of groups, one sees that for the points $r\cdot P$, $s\cdot P$ and $(r+s)\cdot P$ in $E(\mathbb{F}_q)$ the divisors $(r\cdot P)-(\infty)+(s\cdot P)-(\infty)$ and $((r+s)\cdot P)-(\infty)$ are in the same class.

Now we want to evaluate the Tate–Lichtenbaum pairing ϕ_m of points $P \in E_m(\mathbb{F}_q)$ and $P' \in E(\mathbb{F}_q)$. Let D_P and $D_{P'}$ be coprime divisors in the class of $(P)-(\infty)$ and $(P')-(\infty)$ respectively. Since $m \cdot P = 0_E$, we see that $m \cdot D_P$ is the divisor of a function F_{D_P} on E. Then the Tate–Lichtenbaum pairing is given by

$$\phi_m : (P, P') \longmapsto (F_{D_P}(D_{P'}))^{(q-1)/m} \in \mu_m(\mathbb{F}_q).$$

The above remarks show that we can choose D_P to be equal to $(k\cdot P)-((k-1)\cdot P)$ for any $k \in \mathbb{Z}$.

In order to get the pairing we have at first to find the function F_{D_P} and then to evaluate its value at $D_{P'}$. Doing these steps separately has a big disadvantage: One has to evaluate and to compute a function of a huge degree.

Instead of this we consider the following group structure:
We choose $D_P = (P) - (\infty)$. At first we assume that the divisor $D_{P'}$ is prime to all prime divisors $(r \cdot P)$ for $0 \le r < m$. We define on the set $\{r \cdot P\,;\, 0 \le r < m\} \times \mathbb{F}_q^*$ the following group law:

$$(r_1 \cdot P, a_1) \oplus (r_2 \cdot P, a_2) := ((r_1 + r_2) \cdot P, a_1 a_2 h(D_{P'})),$$

where h is a function whose divisor satisfies

$$(h) = (r_1 \cdot P) + (r_2 \cdot P) - ((r_1 + r_2) \cdot P) - (\infty)$$

This function h can be evaluated using the addition formulas on the elliptic curve. One can show that this defines indeed a group structure. And by induction we get easily the following rule:

$$m \odot (P, 1) = (0_E, F_{D_P}(D_{P'})). \tag{1}$$

Hence in this group by repeated doubling one can evaluate $F_{D_P}(D_{P'})$ in $O(\log m)$ steps.

In addition it is clear that for evaluating $F_{D_P}(D_{P'})$ we need not the whole group. Hence the divisor $D_{P'}$ has not to be prime to all prime divisors $(r \cdot P)$, but only to those which occur in the repeated doubling process. Let $S(m)$ be the set of those integers i such that $(i \cdot P)$ occurs in this process. The set $S(m)$ has size $O(\log m)$ and can be computed without knowing $D_{P'}$. So we can precompute $S(m)$ at first and then choose the divisor $D_{P'}$ appropriately.

If for example $P' = P$, we just take any k such that $k, k-1 \notin S(m)$ (such a k always exists if m is large enough) and choose $D_{P'} = (k \cdot P) - ((k-1) \cdot P)$. Then

$$\phi_m(P, P) = (F_{D_P}(D_{P'}))^{(q-1)/m} \tag{2}$$

Remark 2.4 In contrast to the Weil pairing $\langle\,,\rangle_m$, where the value $\langle P, P\rangle_m$ is always trival, the value of the Tate–Lichtenbaum pairing $\phi_m(P, P)$ can be nontrival. Hence it can play an important role in the computation of discrete logarithms, as will be seen in the next steps.

We look at the following special case: Let $m = p^k$, where p is an odd prime number and let p^l be the exact p-power dividing $\#E(\mathbb{F}_q)$. We assume that $E_{p^l}(\mathbb{F}_q)$ is cyclic. Let P be a point of order p^k and let Q be a multiple of P, we want to evaluate the integer n with $Q = n \cdot P$. We consider two different cases.

In the first case let $k = l$. Then we choose $P' = P$. So in this case the word "probabilistic" can be dropped in Theorem 1.1. We evaluate $\phi_{p^k}(P, P)$ according to (1) and (2). In this case $\phi_{p^k}(P, P)$ is a primitive p^k-th root of unity. Furthermore we try to compute $\phi_{p^k}(Q, P)$ with the divisors $D_Q = (Q) - (\infty)$ and $D_P = (2 \cdot P) - (P)$. Either we succeed in this attempt, then we reduced the calculation of n to the discrete logarithm problem $\phi_{p^k}(Q, P) = \phi_{p^k}(P, P)^n$ in $\mathbb{F}_q^*$. Or we have no success, but then in our calculations we reach explicitly an integer i such that P or $2 \cdot P$ equals $i \cdot Q$.

In the second case let $k < l$. Then we choose any point $P' \in E(\mathbb{F}_q)$ of order p^l randomly. Then $\phi_{p^k}(P, P')$ is a primitive p^k-th root of unity. The probability to find such a P' is $1 - \frac{1}{p}$ (see below). Now we calculate $\phi_{p^k}(P, P')$ and $\phi_{p^k}(Q, P')$ with the divisors $D_P = (P) - (\infty)$, $D_Q = (Q) - (\infty)$ and $D_{P'} = (2 \cdot P') - (P')$. Here $2 \cdot P'$ or P' can never be $i \cdot P$ or $j \cdot Q$, so we can calculate the pairings without any problems and get as above the discrete logarithm $\phi_{p^k}(Q, P') = \phi_{p^k}(P, P')^n$ in $\mathbb{F}_q^*$.

Remark 2.5 This first case is the "usual" case for elliptic curve cryptosystems, mostly one has $k = l = 1$.

Now we show how we find a point P' of order p^l randomly of probability $1 - \frac{1}{p}$. Let the elliptic curve E be give in Weierstrass form

$$E : Y^2 = f(X).$$

We choose $x \in \mathbb{F}_q$ randomly. Then there are two possibilities:

If $f(x)$ is a square in $\mathbb{F}_q$, then we can compute $y \in \mathbb{F}_q$ with $y^2 = f(x)$ in polynomial time by the Schoof algorithm or by the probabilistic Shanks algorithm (see [Co] pp. 33). We define $P'' := (x, y)$, then

$$P' := \frac{\#E(\mathbb{F}_q)}{p^l} \cdot P''$$

is a point of order p^j in $E(\mathbb{F}_q)$ with $j \leq l$.

If $f(x)$ is not a square in $\mathbb{F}_q$, then the point $P'' := (x, \sqrt{f(x)})$ is an element of $E(\mathbb{F}_{q^2})$. Since

$$\#E(\mathbb{F}_{q^2}) = \#E(\mathbb{F}_q)\,(-\#E(\mathbb{F}_q) + 2(q-1) + 4)\,,$$

the p–primary parts of $E(\mathbb{F}_q)$ and $E(\mathbb{F}_{q^2})$ are the same. Then again

$$P' = \frac{\#E(\mathbb{F}_{q^2})}{p^l} \cdot P''$$

is a point in $E(\mathbb{F}_q)$ of order p^j with $j \leq l$.

Hence for every choice of $x \in \mathbb{F}_q$ we find a point of order p^j with $j \leq l$. And the probability to find a generator of the cyclic group $E_{p^l}(\mathbb{F}_q)$ is equal to

$$\frac{p^l - p^{l-1}}{p^l} = 1 - \frac{1}{p}.$$

3 An example

With a simple `Maple` program, we can calculate the Tate–Lichtenbaum pairing (and the Weil pairing c.f. Remark 2.2). All the computations where done on a Linux PC with a (nowadays slow) Pentium 133 processor in a few seconds.

Example 3.1 Consider the elliptic curve

$$E : Y^2 + Y = X^3 - X^2 - 10X - 7$$

defined over the finite field $\mathbb{F}_q$ with $q = 1609667$ elements. By counting points on E we find that $\#E(\mathbb{F}_q) = q - 1 = 2 \cdot 804833$, therefore the trace of the Frobenius endomorphism is equal to 2. This implies that for $m = p = 804833$ the m-th roots of unity are in $\mathbb{F}_q$. So we can use the Tate–Lichtenbaum pairing to reduce the discrete logarithm problem for elliptic curves to a discrete logarithm problem in $\mathbb{F}_q^*$. Since $E(\mathbb{F}_q)$ does not contain all points of order p, we cannot use the Weil pairing. The point

$$P = (x, y) := (797482, 1369997) \in E(\mathbb{F}_q) \text{ has exact order } p = 804833.$$

We choose $Q := n \cdot P = (822050, 1036146) \in E(\mathbb{F}_q)$ with $n = 89865$. The points $5 \cdot P$ and $6 \cdot P$ do not occur in the calculation of $p \cdot P$ (i.e. $5, 6 \notin S(p)$). In our example we have $k = l = 1$ (see above) we calculate $\phi_p(P, P)$ with the divisors $D_p = (P) - (\infty)$ and $D_{P'} = (6 \cdot P) - (5 \cdot P)$, and $\phi_p(Q, P)$ as above. We get

$$\phi_q(P, P) = 822530^{(q-1)/p} = 1293131 \in \mu_m(\mathbb{F}_q),$$
$$\phi_q(Q, P) = 824368^{(q-1)/p} = 508028 \in \mu_m(\mathbb{F}_q).$$

Hence in order to compute n, we have to solve the discrete logarithm problem

$$1293131^n \equiv 508028 \bmod q. \tag{3}$$

(Of course we can check in this example that $n = 89865$ is a solution of (3).)

References

[Co] H. Cohen. A Course in Computational Algebraic Number Theory, GTM 138, Springer–Verlag, Heidelberg, 1993.

[F-R] G. Frey and H. G. Rück. A Remark Concerning m–Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves. *Math. of Comp.*, 62:865–874, 1994.

[R] H. G. Rück. On the discrete logarithm in the Divisor Class Group of Curves, (to appear in *Math. of. Comp.*).

[Sem] I. A. Semaev. Evaluation of discrete logarithms in a group of p–torsion points of an elliptic curve in characteristic p. *Math. of Comp.*, 67:353–356, 1998.

[Silv] J. H. Silverman. Arithmetic of Elliptic Curves, GTM 106, Springer–Verlag, Heidelberg, 1986.