TABLE I
THE NUMBER OF DEPENDENT AND INDEPENDENT ERROR PATTERNS IN RANDOMLY GENERATED PATTERNS WITH A GIVEN NUMBER OF POINTS FROM THE HERMITIAN CURVE OVER $\mathbb{F}_{64}$

Points	Total Patterns	Dependent	Independent
2	10000	142	9858
5	10000	169	9831
10	10000	154	9846
20	10000	158	9842
50	10000	153	9847
100	10000	135	9865
150	10000	157	9843
200	10000	166	9834
250	10000	147	9853

The system of equations

$$\sum_{j=1}^{n} f_\ell(P_j)y_j = 0, \qquad \ell = 1, \cdots, \tau + i - 1$$

$$\sum_{j=1}^{n} f_{\tau+i}(P_j)y_j = 1$$

therefore, has a nonzero solution with $y_1 = \cdots = y_{\tau-\tau_0} = 0$ and $y_{\tau+i+1} = \cdots = y_n = 0$. But then $\underline{y} \in C_{\rho_{\tau+i-1}} \backslash C_{\rho_{\tau+i}}$ with a nonzero coordinate at a position greater than $\tau - \tau_0$ contradicting the definition of $\underline{a}$, therefore, we get that L has dimension $\tau - \tau_0 - 1$. □

We will now prove the theorem. For a fixed $\underline{e} \in (\mathbb{F}_q^*)^\tau$ we consider the map $\psi_{\underline{e}} : L \to \mathbb{F}_q^{\tau-\tau_0}$ defined by

$$\psi_{\underline{e}}(f) = (e_1 f(P_1), \cdots, e_{\tau-\tau_0} f(P_{\tau-\tau_0})).$$

This is injective since

$$\ker \psi_{\underline{e}} = \{f \in L | f(P_i) = 0, \quad 1 \le i \le \tau - \tau_0\}$$
$$= \{f \in L(\rho_{\tau-1}Q - (P_1 + \cdots + P_\tau))\} = \{0\}$$

so the dimension of its image is $\tau - \tau_0 - 1$ and the dimension of $\psi_{\underline{e}}^{-1}(\lambda \underline{a}, \lambda \in \mathbb{F}_q)$ is either 0 or 1. On the other hand, if $(e_1, \cdots, e_{\tau-\tau_0}) \neq (\hat{e}_1, \cdots, \hat{e}_{\tau-\tau_0})$ then

$$\psi_{\underline{e}}^{-1}(\lambda \underline{a}, \lambda \in \mathbb{F}_q) \cap \psi_{\underline{\hat{e}}}^{-1}(\lambda \underline{a}, \lambda \in \mathbb{F}_q) = 0$$

since, otherwise, we would have for some $f \in L$ that $e_i f(P_i) = \hat{e}_i f(P_i)$ for $i = 1, \cdots, \tau - \tau_0$ and, therefore, $e_i = \hat{e}_i$ since $f(P_i) = \mu a_i$, $i = 1, \cdots, \tau - \tau_0$.

This implies that the number of $\underline{e}$'s in $(\mathbb{F}_q^*)^\tau$ for which there exists an $f \in F_M$ with $\rho(f) \le \rho_{\tau-1}$ is at most $(q-1)^{\tau-\tau_0-1}(q-1)^{\tau_0}$, so the probability of getting such an $\underline{e}$ is at most

$$\frac{(q-1)^{\tau-1}}{(q-1)^\tau} = \frac{1}{q-1}.$$

Let us now consider the situation where $f \in F_M$, $\rho(f) = \rho_\tau$ but $f \notin F_r$. This implies that *span* $(f) > m - \rho_\tau = (m-1)/2 = \rho_{\tau-1}$, so *span* $(f) = \rho_{\tau+i}$. But we have just calculated the probability for this so $f \in F_r$ with probability $1 - (1/(q-1))$, this also concludes the proof of Theorem 8. □

Let us finally consider the situation where we have $f \in F_M$, $\rho(f) = \rho_\tau$, $f \in \Sigma_r$, and $\Delta_M \supseteq \{\rho_1, \cdots, \rho_{\tau-1}\}$. At Step 4 in the algorithm we get

$$\Gamma_{M+1} = \{\rho \in \Sigma_M | \rho \le m+1 \text{ and } m+1-\rho \in \Sigma_M\}.$$

Since $\rho_\tau = (m+1)/2$ we have $\rho_\tau \in \Gamma_{M+1}$ so f gives a (correct) vote, and this is the only one, so $\Delta_{M+1} = \Delta_M$ and $F_{M+1} = F_M$. At the next step we have

$$\Gamma_{M+2} = \{\rho \in \Sigma_{M+1} | \rho \le m+2 \text{ and } m+2-\rho \in \Sigma_{M+1}\}.$$

Here there are two possibilities.

If $\rho_{\tau+1} \in \Delta_{M+1} = \Delta_M$ then Γ_{M+2} is empty and there are no votes at all, but this situation corresponds to the situation we have analyzed above (with $i = 1$), so it happens in at most in a fraction of $1/(q-1)$ of the cases.

If $\rho_{\tau+1} \in \Sigma_{M+1}$ then $\Gamma_{M+2} = \{\rho_\tau, \rho_{\tau+1}\}$ and f gives a (correct) vote, but the function $h \in F_{M+1}$ with $\rho(h) = \rho_{\tau+1}$ also gives the correct vote since if not we would have *span* $(h) = m + 2 - \rho_{\tau+1} = \rho_\tau$, contradicting the fact that $\rho_\tau \notin \Delta_r$. Therefore, in this case the algorithm works correctly.

V. CONCLUSIONS AND OPEN PROBLEMS

We have shown that the decoding algorithm fails if the error points are independent, except for high rates where it performs quite well. We believe, and experiments support this (see Table I), that this is indeed the typical situation, but we have no proofs. From the analysis we also see that in the cases where the true minimum distance exceeds the Feng–Rao distance the current decoding algorithms do not correct up to half the minimum distance.

REFERENCES

[1] M. E. O'Sullivan, "Decoding Hermitian codes beyond $(d_{\min}-1)/2$," in *Proc. 1997 IEEE Int. Symp. Information Theory* (Ulm, Germany, June 20–July 4, 1997).

[2] ——, "Decoding of codes defined by a single point on a curve," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1709–1719, Nov. 1995.

[3] M. A. Shokrollahi and H. Wassermann, "Decoding algebraic-geometric codes beyond the error-correction bound," Univ. Berkeley, Berkeley, CA, Aug. 1997, preprint.

[4] M. Sudan, "Decoding of Reed Solomon codes beyond the error-correction bound," *J. Complexity*, vol. 13, pp. 180–193, 1997.

[5] S. Sakata, H. Elbrønd Jensen, and T. Høholdt, "Generalized Berlekamp–Massey decoding of algebraic-geometric codes up to half the Feng–Rao bound," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1762–1768, Nov. 1995.

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

Gerhard Frey, Michael Müller, and Hans-Georg Rück

***Abstract*—The Tate pairing is used to reduce the discrete logarithm (DL) problem on certain elliptic curves to the DL in the multiplicative group of finite fields.**

***Index Terms*—Cryptography, discrete logarithm, elliptic curves, Tate pairing.**

I. THE TATE–LICHTENBAUM PAIRING

In [2] 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

Manuscript received October 1, 1998; revised November 30, 1998.

The authors are with the Institute for Experimental Mathematics, University of Essen, 45326 Essen, Germany.

Communicated by I. Blake, Associate Editor for Coding Theory.
Publisher Item Identifier S 0018-9448(99)04733-1.

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 [2] 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
$$\phi_m\colon\ J_m(\mathbb{F}_q) \times J(\mathbb{F}_q)/mJ(\mathbb{F}_q) \to \mu_m(\mathbb{F}_q).$$
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 of finding a point P' in $J(\mathbb{F}_q)$ with
$$\{\phi_m(P,\, P');\ P \in C_m\} = \mu_m(\mathbb{F}_q)$$
is positive (and depends 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 of 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.

II. 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 mth 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 $t \equiv 2 \mod m$, we see that $q-1$ is divisible by m. □

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 Miller [4] consists of a twofold computation of the Tate–Lichtenbaum pairing (cf. Menezes, Okamoto, and Vanstone [3]).

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 later.

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 [7, Proposition 3.4, p. 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
$$\phi_m\colon (P,\, P') \mapsto (F_{D_P}(D_{P'}))^{(q-1)/m} \in \mu_m(\mathbb{F}_q).$$
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 evaluate it at $D_{P'}$. Doing these steps separately has a big disadvantage, because F_{D_P} is a function whose degree is approximately m.

Instead, 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 indeed defines a group structure. And by induction we easily get the following rule:
$$m \odot (P,\, 1) = (0_E,\, F_{D_P}(D_{P'})). \tag{1}$$
Hence in this group by repeated doubling and adding 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 do not need the whole group. Hence the divisor $D_{P'}$ does not have 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 trivial, the value of the Tate–Lichtenbaum pairing $\phi_m(P,\, P)$ can be nontrivial. 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.

[1] In [5] it is explained how to treat the case when m is a power of the characteristic of $\mathbb{F}_q$, in the case of elliptic curves see [6].

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^kth 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, in which case we reduce 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 explicitly obtain 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^kth root of unity. The probability of finding 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 with probability $1 - \frac{1}{p}$. Let the elliptic curve E be given in Weierstrass form

$$E\colon Y^2 = f(X).$$

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 $y^2 = f(x)$ by the probabilistic Shanks algorithm (see [1, pp. 33]) in polynomial time. 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 of finding a generator of the cyclic group $E_{p^l}(\mathbb{F}_q)$ is equal to

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

III. 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 were done on a Linux PC with a Pentium 133 processor (which is slow by today's standards) in a few seconds.

Example 3.1: Consider the elliptic curve

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

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 mth 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, where $k = l = 1$ (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 we calculate $\phi_p(Q, P)$ in the same way as in our earlier general description of the case $k = l$. We get

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

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

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

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

References

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM 138. Heidelberg, Germany: Springer-Verlag, 1993.

[2] G. Frey and H. G. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves," *Math. Comput.*, vol. 62, pp. 865–874, 1994.

[3] A. Menezes, T. Okamoto, and S. A. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1639–1646, 1993.

[4] V. Miller, "Short programs for function on curves," unpublished, 1996.

[5] H. G. Rück, "On the discrete logarithm in the divisor class group of curves," *Math. Comput.*, to be published.

[6] I. A. Semaev, "Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p," *Math. Comput.*, vol. 67, pp. 353–356, 1998.

[7] J. H. Silverman, *Arithmetic of Elliptic Curves*, GTM 106. Heidelberg, Germany: Springer-Verlag, 1986.