ON THE EXISTENCE OF DISTORTION MAPS ON ORDINARY ELLIPTIC CURVES

DENIS CHARLES

1. Introduction

An important problem in cryptography is the so called Decision Diffie-Hellman problem (henceforth abbreviated DDH). The problem is to distinguish triples of the form (g^a, g^b, g^{ab}) from arbitrary triples from a cyclic group $G = \langle g \rangle$. It turns out that for (cyclic subgroups of) the group of m-torsion points on an elliptic curve over a finite field, the DDH problem admits an efficient solution if there exists a suitable endomorphism called a distortion map (which can be efficiently computed) on the elliptic curve.

Suppose m is relatively prime to the characteristic of a finite field $\mathbb{F}_q$, then the group of m-torsion points on an elliptic curve $E/\mathbb{F}_q$, denoted $E[m]$, is isomorphic to $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$. Fix an elliptic curve $E/\mathbb{F}_q$ and a prime ℓ that is not the characteristic of $\mathbb{F}_q$. Let P and Q generate the group $E[\ell]$. A *distortion map* on E is an endomorphism ϕ of E such that $\phi(P) \notin \langle P \rangle$. A distortion map can be used to solve the DDH problem as follows: Given a triple R, S, T of points belonging to the group generated by P, we check whether $\mathbf{e}_\ell(R, \phi(S)) = \mathbf{e}_\ell(P, \phi(T))$, where $\mathbf{e}_\ell$ is the Weil pairing on the ℓ-torsion points. It follows from well known properties of the Weil pairing that this check succeeds if and only if $R = aP$, $S = bP$ and $T = abP$. Under the assumptions that P and Q are both defined over $\mathbb{F}_{q^k}$, where k is not large (say, bounded by a fixed polynomial in $\log(q)$), and that ϕ can be computed in polynomial time, the DDH problem can be solved in (randomized) polynomial time using this idea. If P and Q are not eigenvectors for the Frobenius map, then in many cases one can use the trace map as a distortion map (see [GR04]). For this reason, we will concentrate only on the subgroups that are Frobenius eigenspaces.

It is known that distortion maps exist on supersingular elliptic curves ([Ver01, GR04]), and that distortion maps that do not commute with the Frobenius do not exist on ordinary elliptic curves (see [Ver01] or [Ver04] Theorem 6). The latter implies that distortion maps *do not* exist for ordinary elliptic curves with embedding degree > 1. The embedding degree, (say) k, is the order of q in the group $(\mathbb{Z}/\ell\mathbb{Z})^*$. A theorem of Balasubramanian and Koblitz ([BK98] Theorem 1) says that if $E(\mathbb{F}_q)$ contains an ℓ-torsion point and $k > 1$, then $E[\ell] \subseteq \mathbb{F}_{q^k}$. Thus, the only remaining cases where the existence of Distortion maps is not known are the cases when the embedding degree k is 1. If the embedding degree is 1 and $E(\mathbb{F}_q)$ contains an ℓ-torsion point, then there are two possibilities: either $E[\ell](\mathbb{F}_q)$ is cyclic or $E[\ell] \subseteq E(\mathbb{F}_q)$. In the former situation there are no distortion maps (by [Ver04] Theorem 6). However, the Tate pairing can be used to solve DDH efficiently in this case (see the comments in [GR04] following Remark 2.2). Thus, the only case in which the question of the existence of a distortion map remains open is when $E[\ell] \subseteq E(\mathbb{F}_q)$. In this article we show that there are no distortion maps for the Frobenius eigenspaces in this case.

2. The Proof

Theorem 2.1. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve and let ℓ be a prime different from the characteristic of the field. Suppose $E[\ell] \subseteq E(\mathbb{F}_q)$, but no ℓ-torsion points (apart from the identity) are defined over a proper subfield of $\mathbb{F}_q$, then there are no distortion maps for the Frobenius eigenspaces on E.*

Proof : The idea behind the proof is to use Tate's theorem ([Tat66])to show that no distortion maps exist.

Let π denote the (q-th power) Frobenius map on the Tate module $T_\ell(E) = \varprojlim E[\ell^n]$. The characteristic polynomial of the Frobenius is $f(x) = x^2 - tx + q$. We claim that $f(x)$ factors over $\mathbb{Z}_\ell[x]$ with two distinct

Date: 28 March 2006.

roots. We begin by noting that the discriminant of this polynomial is $t^2 - 4q < 0$ since the curve is not supersingular. The polynomial has non-zero discriminant in $\mathbb{Z}_\ell$ and thus has distinct roots in the algebraic closure of $\mathbb{Z}_\ell$. One way to see that f is not irreducible in $\mathbb{Q}_\ell[x]$ is as follows: Suppose f is irreducible, then the 2-dimensional $\mathbb{Q}_\ell$ vector space $V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ has a basis of the form $P, \pi(P)$. This is a special case of the linear algebra fact that if a linear operator L acting on a finite dimensional vector space has minimal polynomial equal to its characteristic polynomial, then it has a cyclic basis: i.e., there is a vector v such that the vectors $v, L(v), L(L(v)), \cdots$ span the space (a Corollary to §7.2 Theorem 3 of [HK71]). With respect to this basis the action of π on T_ℓ is given by

$$M_\pi = \begin{pmatrix} 0 & 1 \\ -q & t \end{pmatrix}$$

since $\pi(\pi(P)) = \pi^2(P) = t\pi(P) - q\pi(P)$ from the characteristic equation of π. The action of π on $E[\ell]$ is given by the reduction of this matrix $\mod \ell$. But we know that the action of π on $E[\ell]$ is the identity matrix, but the reduction of $M_\pi \mod \ell$ is not (conjugate to) the identity matrix since $q \equiv 1 \mod \ell$ and $t \equiv 2 \mod \ell$. This is a contradiction and hence f has two distinct roots over $\mathbb{Z}_\ell$ and our claim is proven.

We have shown that the action of π on $T_\ell(E)$ is conjugate to

$$M_\pi = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \text{ with } \alpha \neq \beta \in \mathbb{Z}_\ell.$$

In fact, the matrix M_π takes the above form with respect to the Frobenius eigenbasis of $V_\ell(E)$. Tate's theorem tells us that $\mathrm{End}_{\mathbb{F}_q}(T_\ell(E)) \cong \mathrm{End}_{\mathbb{F}_q}(E) \otimes \mathbb{Z}_\ell$. In other words, a matrix with entries in $\mathbb{Z}_\ell$ arises from a map on the curve (in the sense that it belongs to the right hand side of the isomorphism) iff it commutes with the action of Frobenius given by M_π. But the commutant of the matrix M_π are again matrices of the form

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}.$$

Therefore, no map of the curve can send points in one eigenspace outside that eigenspace. Thus, there are no distortion maps. □

Remark 2.2. We note that if E is *supersingular* and embedding degree $k = 1$, then Theorem 2.1 gives a simple proof of the existence of distortion maps. Indeed, under these assumptions one has that $f(x) = (x - a)^2$ where a is an integer and that π, the Frobenius map, acts as multiplication by scalar on E. Since any matrix commutes with this action, Tate's theorem implies the existence of distortion maps. If $k > 1$ a more complicated argument (still using Tate's theorem) works (see [Ver04] Theorem 7).

Acknowledgements: I would like to thank Bjorn Poonen and Kristin Lauter for pointing out an error in a previous version of the theorem. I would also like to thank Steven Galbraith for very useful discussions.

References

[BK98] Balasubramanian, R.; Koblitz, N.; *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone Algorithm*, Journal of Cryptology, **Vol. 11**, No. 2, 141-145, 1998.

[GR04] Galbraith, S.; Rotger. V.; *Easy decision Diffie-Hellman groups*, LMS J. Comput. Math., **7**, 201-218, 2004.

[HK71] Hoffman, K.; Kunze, R.; *Linear algebra*, Prentice-Hall, Englewood Cliffs, NJ., 1971.

[Tat66] Tate, John; *Endomorphisms of abelian varieties over finite fields*, Invent. Math., **2**, 134-144, 1966.

[Ver01] Verheul, E., R.; *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*, EUROCRYPT 2001, Lecture Notes in Computer Science, **2045**, Springer-Verlag, 195-201, 2001.

[Ver04] Verheul, E., R.; *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems (Journal version)*, Journal of Cryptology, **Vol. 17**, No. 4, 277-296, 2004.

Microsoft Research, One Microsoft Way, Redmond WA 98052
E-mail address: cdx@microsoft.com