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 \(F_q\), then the group of \(m\)-torsion points on an elliptic curve \(E/F_q\), denoted \(E[m]\), is isomorphic to \((\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})\). Fix an elliptic curve \(E/F_q\) and a prime \(\ell\) that is not the characteristic of \(F_q\). Let \(P\) and \(Q\) generate the group \(E[\ell]\). A distortion map on \(E\) is an endomorphism \(\phi\) of \(E\) such that \(\phi(P) \notin (P)\). A distortion map can be used to solve the DDH problem on the group \((P)\) as follows: Given a triple \(R, S, T\) of points belonging to the group generated by \(P\), we check whether \(\epsilon_\ell(R, \phi(S)) = \epsilon_\ell(P, \phi(T))\), where \(\epsilon_\ell\) is the Weil pairing on the \(\ell\)-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 \(F_{q^k}\), where \(k\) is not large (say, bounded by a fixed polynomial in \(\log(q)\)), and that \(\phi\) can be computed in polynomial time, the DDH problem can be solved in 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 \(E(F_q)\) contains an \(\ell\)-torsion point and \(k > 1\), then \(E[\ell] \subseteq F_{q^k}\). 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 \(E(F_q)\) contains an \(\ell\)-torsion point, then there are two possibilities: either \(E[\ell](F_q)\) is cyclic or \(E[\ell] \subseteq E(F_q)\). 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 \(E[\ell] \subseteq E(F_q)\). In this article we characterize the existence of distortion maps for this case.

2. The Proof

Let \(k\) be a finite field, \(F_q \supseteq k\) and \(E/k\) be an ordinary elliptic curve. Suppose \(\ell\) is a prime such that \(E[\ell] \subseteq F_q\) but no point of exact order \(\ell\) is defined over a smaller field.

To study the existence of distortion maps, we study the reduction of the ring \(\text{End}(E)\) modulo \(\ell\). Our principal tool is the following observation: If \(\alpha \in \text{End}(E)\) has field polynomial \(f(x) \in \mathbb{Z}[x]\), then \(f \mod \ell\) is the characteristic equation of the action of \(\alpha\) on \(E[\ell]\).

Let \(\pi\) be the \(q\)-th power Frobenius endomorphism on \(E\) and let \(\phi^2 - t\phi + q = 0\) be its characteristic equation. We know that \(t \equiv 2 \mod \ell\) and \(q \equiv 1 \mod \ell\) as the full \(\ell\)-torsion is defined over \(F_q\).
Let \( O = \text{End}(E) \), \( K = O \otimes \mathbb{Q} \) and \( O_K \) the maximal order in \( K \). We have the inclusions \( \mathbb{Z}[\pi] \subseteq O \subseteq O_K \).

Since \( t^2 - 4q = 0 \mod \ell \) we have that \( \ell \) divides the product \( |O : \mathbb{Z}[\pi]| \) of \( O_K : O \) and \( \text{Disc}(K) \). The existence of distortion maps splits into cases depending on whether \( \ell ||O_K : O| \) or \( \ell ||\text{Disc}(K)\) \). Indeed, if \( \ell ||O_K : O| \) there are no distortion maps, since the reduction modulo \( \ell \) of every endomorphism is just multiplication by scalar.

In the following we assume that \( \ell \nmid |O_K : O| \) so that the conductor of \( O \) is prime to \( \ell \). Under this assumption we have that the residue class rings

\[
O_K/\ell \cong O/\ell.
\]

Suppose that \( \ell \nmid \text{Disc}(K) \) and that \( \ell \) is \textit{inert} in \( O_K \), then \( O/\ell \cong \mathbb{F}_{\ell^2} \). Let \( \alpha \in O \) be an endomorphism such that \( \alpha \mod (\ell) \) does not lie in \( \mathbb{F}_{\ell} \). Then the action of \( \alpha \) on \( E[\ell] \) is irreducible since its characteristic equation is irreducible over \( \mathbb{F}_{\ell} \). Now \( \alpha \) gives us a distortion map on \( E[\ell] \) since no subgroup of order \( \ell \) of \( E[\ell] \) is stabilized by \( \alpha \).

Now if \( \ell \nmid \text{Disc}(K) \) and \( \ell \) is \textit{split} in \( O_K \), then \( O/\ell \cong \mathbb{F}_{\ell}[X]/(X-a)(X-b) \cong (\mathbb{Z}/\ell\mathbb{Z})^2 \) (where \( a \neq b \)). The action of any \( \alpha \in O_K \), that corresponds to the image of \( X \) in \( \mathbb{F}_{\ell}[X]/(X-a)(X-b) \) under the isomorphism, is conjugate to \( \begin{pmatrix} \gamma & 0 \\ 0 & \delta \end{pmatrix} \). Thus, distortion maps exist for all but two of the subgroups of \( E[\ell] \).

Suppose that \( \ell \mid \text{Disc}(K) \) so that \( \ell \) is \textit{ramified} in \( O_K \), then \( O/\ell \cong \mathbb{F}_{\ell}[X]/(X-a)^2 \). Consider the map \( \alpha \in O \) that corresponds to the image of \( X \) in the ring \( \mathbb{F}_{\ell}[X]/(X-a)^2 \). The action of \( \alpha \) on \( E[\ell] \) is conjugate to \( \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \). Note that \( \beta 
eq 0 \), for if \( \beta = 0 \) then \( O/\ell \cong \mathbb{Z}/\ell\mathbb{Z} \), but we know that \( O \) is rank 2 over \( \mathbb{Z}/\ell\mathbb{Z} \) since \( \ell \) is ramified in \( O_K \) and does not divide the conductor of \( O \). Thus, distortion maps exist for all but one subgroup of \( E[\ell] \).

In summary, we have:

\textbf{Theorem 2.1.} Let \( k \) be a finite field, \( \mathbb{F}_q \supseteq k \) and \( E/k \) be an ordinary elliptic curve whose endomorphism ring is \( O \), an order in an imaginary quadratic field \( \mathbb{O} \). Suppose \( \ell \) is a prime such that \( E[\ell] \subseteq \mathbb{F}_q \) but no point of exact order \( \ell \) is defined over a smaller field.

\begin{enumerate}
    \item If \( \ell \mid |O_K : O| \) there are no distortion maps.
    \item If \( \ell \nmid |O_K : O| \text{Disc}(K) \) and
        \begin{enumerate}
            \item \( \ell \) is \textit{inert} in \( O_K \), then there are distortion maps for every (order \( \ell \)) subgroup of \( E[\ell] \);
            \item \( \ell \) is \textit{split} in \( O_K \), then all but two subgroups of \( E[\ell] \) have distortion maps.
        \end{enumerate}
    \item If \( \ell \mid |O_K : O| \) and \( \ell \mid \text{Disc}(K) \) so that \( \ell \) is ramified in \( O_K \), then all (except one) subgroups of \( E[\ell] \) have distortion maps.
\end{enumerate}

3. Examples

In this section, we give examples to illustrate that all the cases in Theorem 2.1 do occur.

\textbf{Example 3.1.} Consider the elliptic curve \( E : y^2 = x^3 + x \) over \( \mathbb{Q} \). \( E \) has complex multiplication by \( \mathbb{Z}[i] \) and has good reduction at all odd primes. Let \( p \) be a prime such that \( p \equiv 1 \mod 4 \), \( E \) be the reduction of \( E \) modulo \( p \), and let \( t^2 = -1 \mod p \). Then \( E[2] \subseteq E(\mathbb{F}_p) \) and \( E[2] = \{0_E,(0,0),((1,0),(-1,0),(-i,0)) \} \) where \( 0_E \) is the identity element. The map \([i]\) is an endomorphism that sends \((x,y) \mapsto (-x,iy)\). It is easy to see that the map \([i]\) preserves the subgroup \( \langle (0,0) \rangle \) and interchanges the remaining two subgroups, of order 2, of \( E[2] \). Note, that Deuring’s reduction theorem tells us that \( \text{End}(E) \cong \mathbb{Z}[i] \). Furthermore, in this case the subring \( \mathbb{Z}[\pi] \) generated by the Frobenius is usually a smaller ring. Indeed, if \( t \) is the trace of Frobenius and \( t^2 - 4p = -4b^2 \), then the conductor of the order \( \mathbb{Z}[\pi] \) is \( b \). Now \( b \) is at least 2, since \( t \equiv 2 \mod 4 \), so \( (t/2) \) is odd and we must have \( p = (t/2)^2 + b^2 \). Thus, case (3) of Theorem 2.1 applies and matches with what we observe for the 2-torsion.

\textbf{Example 3.2.} (Suggested by anonymous reviewer). Let \( E \) be the curve over \( \mathbb{F}_{701} \) given by the equation \( y^2 = x^3 - 35x + 98 \). Then \( \text{End}(E) = \mathbb{Z}[1+\sqrt{-7}] \) which is the maximal order in \( \mathbb{Q}(\sqrt{-7}) \). The order \( \mathbb{Z}[\pi] \)
has conductor 10 in \(\text{End}(E)\). The 5-torsion is \(\mathbb{F}_{701}\) rational, and moreover, 5 is inert in \(\text{End}(E)\). Theorem 2.1 (2a) shows that every subgroup of \(E[5]\) admits a distortion map. Indeed, the map corresponding to multiplication by \(\alpha = \frac{1+\sqrt{-7}}{2}\) is given by \((\text{Sil94} \text{ Chapter II, Proposition 2.3.1 (iii)})\)

\[
[\alpha](x,y) = \left(\alpha^{-2} \left(x - \frac{7(1-\alpha)^4}{x + \alpha^2 - 2}\right), \alpha^{-3}y \left(1 + \frac{7(1-\alpha)^4}{x + \alpha^2 - 2}\right)\right).
\]

Let us check this for the group generated by the 5-torsion point \(P\) (with affine coordinates) \(P = (224, 31)\). Since \(\alpha = 386 \in \mathbb{F}_{701}\), this tells us that \([\alpha](P) = (173, 194)\). One checks that the Weil pairing \(e_5(P, [\alpha](P)) = 464 \neq 1\). Thus, \([\alpha]\) works as a distortion map for the group generated by \(P\).

Now the 5-torsion of \(E\) is generated by \(P\) and the point \(Q = (573, 450)\). A similar computation shows that \([\alpha](Q) = (463, 495)\). Also, \(e_5(Q, [\alpha]Q) = 89 \neq 1\). Again, this shows that \([\alpha]\) works as a distortion map.

Given these calculations it is not hard to find the matrix of the action of \([\alpha]\) on \(E[5]\) relative to the basis \(P, Q\)

\[
[\alpha] = \begin{pmatrix} 0 & -1 \\ 2 & 1 \end{pmatrix}.
\]

The characteristic polynomial of this matrix is irreducible modulo 5 and thus the action on \(E[5]\) is irreducible.

**Example 3.3.** One can use the elliptic curve \(E\) from Example 3.2 to illustrate case (2b) of Theorem 2.1. This time we look at \(E[2]\) (also contained in \(\mathbb{F}_{701}\)) which is generated by the points \(P = (319, 0)\) and \(Q = (389, 0)\). The prime 2 splits completely in \(\text{End}(E)\). The proof of Theorem 2.1 tells us that the characteristic polynomial of the action of the endomorphism \([\alpha]\) has two distinct roots and would work as a distortion map for all but two subgroups of \(E[2]\). Now the minimal polynomial \(\alpha\) is \(x^2 - x + 2\) and modulo 2 this splits as \(x(x+1)\).

Thus the action of \([\alpha]\) on \(E[2]\) will have two eigenvectors, with eigenvalues 0 and 1 respectively. It is easy to check given the formula for \([\alpha]\) that indeed \([\alpha](P) = 0_E\) and \([\alpha](Q) = Q\).

**Example 3.4.** In this example we illustrate that case (1) of Theorem 2.1 also occurs. Consider the curve \(E/\mathbb{Q}\) given by the Weierstrass equation

\[
y^2 = x^3 - \frac{3375}{121}x + \frac{6750}{121}.
\]

The \(j\)-invariant of \(E\) is \(2^43^75^3\) and the conductor of \(E\) is 108900. \(E\) has CM by the order of conductor 2 in \(\mathbb{Q}(\sqrt{-3})\). Thus \(\text{End}(E) \cong \mathbb{Z} + 2\mathcal{O}_K\) where \(\mathcal{O}_K = \mathbb{Z} + \frac{1}{2}(1 + \sqrt{-3})\mathbb{Z}\). \(E\) has good reduction at the prime 13 and one sees that the reduction \(\tilde{E}\) has \(\mathbb{F}_{13}\)-rational 2-torsion. Now \(\text{End}(\tilde{E}) \cong \text{End}(E)\) by the Deuring reduction theorem \((\text{Lan87} \text{ Chapter 13 §4, Theorem 12})\), but \(\text{End}(\tilde{E}) \mod 2 \cong (\mathbb{Z}/2\mathbb{Z})\) and so there are no distortion maps.

**References**

[BK98] Balasubramanian, R.; Kobliitz, 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.

[Lan87] Lang, S.; *Elliptic Functions*, 2nd ed., Graduate Texts in Math., vol. 112, Springer-Verlag, 1987.

[Sil94] Silverman, J.; *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Math. Vol. 151, Springer-Verlag, 1994.

[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.