London Mathematical Society ISSN 1461–1570

EASY DECISION DIFFIE–HELLMAN GROUPS

STEVEN D. GALBRAITH AND VICTOR ROTGER

Abstract

The decision Diffie–Hellman problem (DDH) is a central computational problem in cryptography. It is known that the Weil and Tate pairings can be used to solve many DDH problems on elliptic curves. Distortion maps are an important tool for solving DDH problems using pairings, and it is known that distortion maps exist for all supersingular elliptic curves. An algorithm is presented here to construct suitable distortion maps. The algorithm is efficient on the curves that are usable in practice, and hence all DDH problems on these curves are easy. The issue of which DDH problems on ordinary curves are easy is also discussed.

1. *Introduction*

It is well known that the Weil and Tate pairings make many decision Diffie–Hellman (DDH) problems on elliptic curves easy. This observation is behind exciting new developments in pairing-based cryptography. This paper studies the question of which DDH problems are easy, and which are not necessarily easy. First we recall some definitions.

Decision Diffie–Hellman problem (DDH). Let G be a cyclic group of prime order r, written additively. The DDH problem is to distinguish the following two distributions in G^4:

$$D_1 = \{(P, aP, bP, abP) : P \in G, 0 \leqslant a, b < r\};$$
$$D_2 = \{(P, aP, bP, cP) : P \in G, 0 \leqslant a, b, c < r\}.$$

Here, D_1 is the set of valid Diffie–Hellman-tuples and $D_2 = G^4$. By 'distinguish' we mean that there is an algorithm that takes as input an element of G^4, and outputs 'valid' or 'invalid', such that if the input is chosen with probability 1/2 from each of D_1 and $D_2 - D_1$, then the output is correct with probability significantly more than 1/2. (For precise definitions, see [**4**].) The DDH problem for a family of groups is said to be *hard* if there is no polynomial-time algorithm that distinguishes between the two distributions. A widely believed assumption in cryptography is that there exist families of groups for which the DDH problem is hard.

We now give a generalisation of the DDH problem, which – following Boneh, Lynn and Shacham [**6**] – we call *co-DDH*.

Generalised decision Diffie–Hellman problem (co-DDH). Let G_1 and G_2 be two cyclic groups of prime order r. The co-DDH problem is to distinguish the following two distributions in $G_1^2 \times G_2^2$:

$$\{(P, aP, Q, aQ) : P \in G_1, Q \in G_2, 0 \leqslant a < r\};$$
$$\{(P, aP, Q, cQ) : P \in G_1, Q \in G_2, 0 \leqslant a, c < r\}.$$

The first author thanks the Nuffield foundation grant NUFF NAL-02 for support.
Received 12 March 2004, revised 15 July 2004; *published* 27 August 2004.
2000 Mathematics Subject Classification 11G20 (primary), 11Y16, 14Q05, 14K02, 11G05, 14H52 (secondary).
© 2004, Steven D. Galbraith and Victor Rotger

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press
LMS J. Comput. Math. 7 (2004) 201–218

The goal of this paper is to determine which DDH and co-DDH problems on elliptic curves are made easy by using pairings. A common technique is to use distortion maps (endomorphisms that map certain subgroups of $E[r]$ to different subgroups) to ensure that the required pairing values are non-trivial. Theorem 5 of Verheul [**28**] states that a suitable distortion map always exists for subgroups of supersingular curves. This result alone does not imply that all DDH problems can be solved efficiently, since we require an explicit description of the map.

In Sections 2 and 3 we show that the trace map handles almost all cases. In Section 5 we give an alternative proof of [**28**, Theorem 5] (restricting to the remaining cases), which is more constructive. In Section 6 we show that a certain endomorphism $\sqrt{-d}$ suffices, and we give an algorithm to construct this distortion map. The complexity analysis of our algorithm proves that all DDH problems are easy on the supersingular elliptic curves that could potentially be used in practice. Sections 7 and 8 illustrate the theory in concrete situations. In particular, Section 7 lists some well-known examples and shows that they always suffice in practice. Section 8 gives examples of our method in the case where the distortion map cannot be an automorphism of the curve. Some of the examples in Sections 7 and 8 show that our algorithm is not optimal, in the sense that it does not necessarily produce an endomorphism of minimal degree.

Our results may have applications, as they mean that cryptographic protocols can use random points P and Q on a supersingular elliptic curve, and there is always a modified pairing so that $e(P, Q) \neq 1$.

In the case of ordinary elliptic curves, there are two hard DDH subgroups remaining. Understanding whether these are truly hard is a challenge to any interested person.

2. *Elliptic curves*

We will be concerned with elliptic curves E over finite fields $\mathbb{F}_q$ such that r is a large prime dividing $\#E(\mathbb{F}_q)$, and such that $\gcd(r, q) = 1$. The embedding degree is the smallest positive integer k such that $r \mid (q^k - 1)$. We restrict attention to elliptic curves such that k is not large (say, bounded by a fixed polynomial in $\log(q)$). Hence, one can efficiently compute in $E(\mathbb{F}_{q^k})$. We always assume that k is coprime to r (this is always true, since r is a large prime and k is small).

We will repeatedly make use of the following properties of the Weil pairing (see the work of Silverman [**25**, Section III.8]).

Lemma 2.1. *Let E be an elliptic curve over $\mathbb{F}_q$, let r be a positive integer, and let $P, Q \in E[r]$. Then the following statements hold.*

(1) $e_r(P, P) = 1$.

(2) *P and Q generate $E[r]$ if and only if $e_r(P, Q)$ is a primitive rth root of unity. In particular, if r is prime, then P and Q generate $E[r]$ if and only if $e_r(P, Q) \neq 1$.*

(3) *If $R \in E[r]$, then $R \in \langle P \rangle$ if and only if $e_r(P, R) = 1$.*

Proof. The first statement is the well-known alternating property of the Weil pairing.

Property (2) follows, since if $e_r(P, Q)$ is not primitive, then $e_r(P, aP + bQ)$ is not primitive for all $a, b \in \mathbb{Z}$, which contradicts the non-degeneracy of the Weil pairing. Conversely, if $e_r(P, Q)$ is a primitive rth root of unity, then P and Q have full order r, and by property (1) they are independent.

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press

Suppose that P and Q generate $E[r]$, and write $R = aP + bQ$. Then $e_r(P, R) = e_r(P, Q)^b$, and this is 1 if and only if $b \equiv 0 \pmod{r}$. This proves property (3). □

REMARK 2.1. Property (3) shows that the subgroup membership problem for any cyclic subgroup $G \subset E(\mathbb{F}_q)$ is easily solved using the Weil pairing if the embedding degree is small. Note that property (3) does not necessarily hold for the Tate pairing. (For details on the Tate pairing, see [**11**] or [**14**].)

The above properties clearly imply that all genuine co-DDH problems are easy. This result is already well known, but for emphasis we state it as a proposition.

PROPOSITION 2.2. *Let E be an elliptic curve over $\mathbb{F}_q$, and let r be a prime. Suppose that*

$$E[r] \subset E(\mathbb{F}_{q^k}), \qquad \textit{where } k \textit{ is polynomial in } \log(q).$$

Let G_1 and G_2 be cyclic subgroups of order r in $E(\mathbb{F}_{q^k})$, such that $G_1 \neq G_2$. Then all co-DDH problems in G_1, G_2 can be solved in polynomial time.

Proof. The fact $G_1 \neq G_2$ implies that $G_1 \cap G_2 = \{0_E\}$. Hence, for all $P \in G_1$, $Q \in G_2$, with $P, Q \neq 0_E$, we have $\{P, Q\}$ forming a basis for $E[r]$, and so by property (2), $e_r(P, Q) \neq 1$.

The co-DDH problem on a tuple (P_1, P_2, Q_1, Q_2) is therefore solved by testing whether

$$e_r(P_1, Q_2) \stackrel{?}{=} e_r(P_2, Q_1).$$ □

REMARK 2.2. As mentioned above, this result is not always true for the Tate pairing. However, in most practical cases the Tate pairing can be used, and will give a more efficient solution (see [**2, 15, 14**] for details).

For the remainder of the paper we will be concerned with solving DDH problems. Clearly, the Weil pairing cannot be used directly to solve these problems.

When $k = 1$ and $E(\mathbb{F}_q)[r]$ is a cyclic group of order r, then (due to the non-degeneracy of the Tate pairing) the DDH problem in this group can be solved in polynomial time. Note that if $r > (2\sqrt{q} + 2)$, then the curve is ordinary (since $r \mid \#E(\mathbb{F}_q) = (q + 1 - t)$ and $r \mid (q - 1)$, and so $r \mid (t - 2)$).

The case $k = 1$ and $E(\mathbb{F}_q)[r]$ non-cyclic is more interesting. The Weil and Tate pairings can have very different behaviour in this case (for example, there are cases where the Tate pairing gives non-trivial self-pairings for all non-zero points, and cases where the Tate pairing gives trivial self-pairings for all points). The ordinary case has been used by Joux and Nguyen [**18**] to generate examples where the DDH problem is easy and the CDH problem seems to be hard. We note that [**28**, Theorem 5] states that in the supersingular case, suitable distortion maps always exist; [**28**, Theorem 7] shows that in the ordinary case many DDH problems can be solved in this case, using the Weil pairing with a suitable distortion map.

In practice, the case $k > 1$ is of greater interest. Hence, for the remainder of the paper, we make the following assumption.

ASSUMPTION. The embedding degree is assumed to be $k \geqslant 2$.

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press

3. *Trace maps*

The trace map was proposed as a distortion map by Boneh *et al.*, in the full versions of [5] and [6]. Since $\mathbb{F}_{q^k}/\mathbb{F}_q$ is a Galois extension, we can define, for any point $P \in E(\mathbb{F}_{q^k})$,

$$\mathrm{Tr}(P) = \sum_{i=0}^{k-1} \pi^i(P),$$

where π is the q-power Frobenius map. Equivalently, if $P = (x, y)$, then

$$\mathrm{Tr}(P) = \sum_{i=0}^{k-1} \left(x^{q^i}, y^{q^i}\right).$$

The trace map is a group homomorphism, and if $P \in E(\mathbb{F}_q)$, then $\mathrm{Tr}(P) = kP$.

Let $P, Q \in E(\mathbb{F}_{q^k})[r]$. Define the function $e(P, Q)$ to be either the Weil pairing $e(P, Q) = e_r(P, Q)$ or the Tate pairing

$$e(P, Q) = \langle P, Q\rangle_r^{(q^k-1)/r}$$

(see, for example, [11] or [14]). If $P \in E(\mathbb{F}_q)$ and $k > 1$, then (since $\mathbb{F}_{q^k}$ is the extension of $\mathbb{F}_q$ of minimal degree that contains non-trivial rth roots of unity) it follows that $e(P, P) = 1$ for the Tate pairing as well as the Weil pairing.

If $r \mid \#E(\mathbb{F}_q)$, then the eigenvalues of π on $E(\overline{\mathbb{F}}_q)[r]$ are 1 and q. Hence there is a basis $\{P, Q\}$ for $E[r]$ such that $\pi(P) = P$ and $\pi(Q) = qQ$. Now, $\{P, Q\}$ forms a basis for the r-torsion and so, by the same arguments as those used to prove part (2) of Lemma 2.1, we see that $e(P, Q) \neq 1$ for both Weil and Tate pairings.

Boneh observed (see [3, 14]) that the eigenspace $\langle Q\rangle$ of points with eigenvalue q is equal to the set of all points $R \in E(\mathbb{F}_{q^k})[r]$ such that $\mathrm{Tr}(R) = 0_E$. Boneh has also shown that $e(Q, Q) = 1$ for the Tate pairing as well as the Weil pairing (see [14]). We call $\langle Q\rangle$ the *trace zero subgroup*, and we denote it by $\mathcal{T}$.

LEMMA 3.1. *Let E be an elliptic curve over $\mathbb{F}_q$. Let r be a large prime such that $r \mid \#E(\mathbb{F}_q)$ and $r \mid (q^k - 1)$. Define the basis $\{P, Q\}$ as the eigenbasis for Frobenius as above. Let $S = aP + bQ \in E(\mathbb{F}_{q^k})$ with $ab \neq 0$, and let $G = \langle S\rangle$. Then the DDH problem in G can be solved in polynomial time.*

Proof. Consider (S, uS, vS, wS). Since $\mathrm{Tr}(S) = kaP \neq 0_E$ and $b \neq 0$, we see that $e(S, \mathrm{Tr}(S)) \neq 1$. Hence, the DDH tuple (S, uS, vS, wS) gives rise to the co-DDH tuple

$$(S, uS, \mathrm{Tr}(vS) = v\mathrm{Tr}(S), \mathrm{Tr}(wS) = w\mathrm{Tr}(S))$$

and, as we have seen, all co-DDH problems can be solved using the Weil pairing. □

Hence, only two potentially hard DDH problems remain, namely the subgroup $\langle P\rangle$, which is the set of r-torsion points that are defined over the field $\mathbb{F}_q$, and the trace zero subgroup $\mathcal{T} \subset E(\mathbb{F}_{q^k})[r]$. Equivalently, these are the two eigenspaces in $E(\mathbb{F}_{q^k})[r]$ for the q-power Frobenius map. In the ordinary case, these problems seem to be hard. For the remainder of the paper, we consider the supersingular case.

4. *Review of quaternion algebras*

We devote this section to fixing the notation and briefly reviewing the theory of quaternion algebras that we need in the rest of the paper.

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press

A *quaternion algebra over a field* K is a central simple algebra of rank 4 over K. A quaternion algebra B is *division* if $B \not\simeq \mathrm{M}_2(K)$ or, equivalently, if $B^* = B \setminus \{0\}$. If $\mathrm{char}(K) \neq 2$, every quaternion algebra is of the form

$$B = \left(\frac{m, n}{K}\right) := K + Ki + Kj + Kij, \qquad i^2 = m,\ j^2 = n,\ ij = -ji$$

for some $m, n \in K^*$. The *conjugation map* on B is $\overline{a + bi + cj + dij} = a - bi - cj - dij$, and the *reduced trace* and *norm* on B are $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha}$ and $\mathrm{n}(\alpha) = \alpha \cdot \overline{\alpha}$ for any $\alpha \in B$, respectively.

We next present two different but equivalent versions of the Skolem–Noether theorem (see [29]).

PROPOSITION 4.1. *Let B be a quaternion algebra over a field K.*

(1) *Let $\sigma : B \longrightarrow B$ be an automorphism of B over K. Then $\sigma(\alpha) = \gamma^{-1}\alpha\gamma$ for some $\gamma \in B^*$.*

(2) *Let L/K be a quadratic field extension of K. Let $\phi, \psi : L \hookrightarrow B$ be two different immersions of L into B over K. Then there exists $\gamma \in B^*$ such that $\phi(\alpha) = \gamma^{-1}\psi(\alpha)\gamma$ for all $\alpha \in L$.*

Let R be a Dedekind ring, and let K be its field of fractions. Let B be a quaternion algebra over K. We say that a place $v \leqslant \infty$ of K *ramifies in* B if $B \otimes K_v$ is a division algebra over the completion K_v of K at v. A classical theorem (see [1] or [29, p. 74]) states that there is a finite and even number of places of K that ramify in B. Conversely, for any finite set $\{v_1, \ldots, v_{2r}\}$ of places of K of even cardinality, there exists a unique quaternion algebra up to isomorphism that ramifies exactly at the places v_i.

The reduced discriminant of B is defined to be the product $D_B = \prod \wp$ of all finite prime ideals of R ramifying in B.

An element α in B is *integral over* R if $\mathrm{Tr}(\alpha), \mathrm{n}(\alpha) \in R$. Unlike number fields, the set of integral elements in B is not a subring of B. (For an example, see [29, p. 20].)

An order $\mathcal{R}$ in B over R is a subring of B of rank 4 over R. We say that $\mathcal{R}$ is *maximal* if it is not properly contained in any other order of B. A *left projective ideal* I of a maximal order $\mathcal{R}$ is a locally principal sub-$\mathcal{R}$-module of B of rank 4 over R. Two projective left ideals I and J of $\mathcal{R}$ are *linearly equivalent* if $I = J \cdot \alpha$ for some $\alpha \in B^*$. We let $\mathrm{Pic}_R(\mathcal{R})$ denote the set of linear equivalence classes of left projective ideals of $\mathcal{R}$ over R. The set $\mathrm{Pic}_R(\mathcal{R})$ is finite, and its cardinality $h_R(B) = \#\mathrm{Pic}_R(\mathcal{R})$ is independent of the choice of $\mathcal{R}$. The *conjugation class* of an order $\mathcal{R}$ over R is the set of orders $[\mathcal{R}] = \{\gamma^{-1}\mathcal{R}\gamma : \gamma \in B^*\}$, which has infinite cardinality. There is, however, a finite number $t_R(B)$ of conjugation classes of maximal orders in B over R.

PROPOSITION 4.2. *Let K be the field of fractions of a Dedekind ring R, and let B be a quaternion algebra over R. Then the following statements hold.*

(1) $h_R(B) \geqslant t_R(B)$.

(2) *If K is a local field, then $h_R(B) = t_R(B) = 1$.*

(3) *If K is a number field and $\mathfrak{M}$ is any ideal of K, there exists an integral ideal $\mathfrak{N}$ of R, $(\mathfrak{M}, \mathfrak{N}) = 1$, such that $h_{R[1/\mathfrak{N}]}(B) = t_{R[1/\mathfrak{N}]}(B) = 1$.*

Proof. The first two statements can be found in [29, p. 26], and [29, Chapter II], respectively. As for the third, let $\mathcal{R}$ be a maximal order of B, and let $\{I_1, \ldots, I_{h_R(B)}\}$ be a full set of

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press

representatives of the projective left ideals in $\mathrm{Pic}_R(\mathcal{R})$. It follows from [23, p. 5], that I_i can be chosen such that $\mathfrak{N} = \mathrm{n}(I_1) \cdot \ldots \cdot \mathrm{n}(I_{h_R(B)})$ is coprime to $\mathfrak{M}$. Since I_i are invertible in $\mathcal{R}[1/\mathfrak{N}]$, we see that $h_{R[1/\mathfrak{N}]}(B) = 1$. By (1) we also have $t_{R[1/\mathfrak{N}]}(B) = 1$. □

Let $B = (\frac{m,n}{K}) := K + Ki + Kj + Kij, i^2 = m, j^2 = n, ij = -ji$, and let $\mathcal{R}$ be a maximal order in B over R. Two questions that naturally arise in several contexts, and that we encounter in the proof of Theorem 5.2, are the following.

1. Do there exist elements $\pi, \psi \in \mathcal{R}$ such that $\pi^2 = m, \psi^2 = n, \pi\psi = -\psi\pi$?
2. Fix $\pi \in \mathcal{R}$ such that $\pi^2 = m$ (if there is any). Does there exist $\psi \in \mathcal{R}$ such that $\psi^2 = n, \pi\psi = -\psi\pi$?

These questions were considered in [24, appendix]. We state here a partial answer, which will suffice for our purposes.

Proposition 4.3. *Let the notation be as above.*

(1) *If $t_R(B) = 1$, then there exist $\pi, \psi \in \mathcal{R}$ such that $\pi^2 = m, \psi^2 = n, \pi\psi = -\psi\pi$.*

(2) *Fix $\pi \in \mathcal{R}$ such that $\pi^2 = m$. If $t_R(B) = 1$ and $\mathcal{O} = R[\sqrt{m}] \subset K(\sqrt{m})$ is locally a discrete valuation ring at the places $v \nmid D_B$ of class number $h(\mathcal{O}) = 1$, then there exists $\psi \in \mathcal{R}$ such that $\psi^2 = n, \pi\psi = -\psi\pi$.*

Proof. Part (1) follows from [24, Proposition 5.1]. As for (2), let $\mathcal{E}(m)$ denote the set of embeddings $i : R[\sqrt{m}] \hookrightarrow \mathcal{R}$ over R up to conjugation by elements in the normalizer group $\mathrm{Norm}_{B^*}(\mathcal{R})$. Since $\pi \in \mathcal{R}$, $\mathcal{E}(m)$ is non-empty. Eichler proved that $\mathcal{E}(m)$ is a finite set. More precisely, we have from our hypothesis and [29, Theorem 3.1 on p. 43 and Theorem 5.11 on p. 92], that in fact $\#\mathcal{E}(m) = 1$. It now follows from [24, Proposition 5.7 and its remark below], that there exists $\psi \in \mathcal{R}$ such that $\psi^2 = n, \pi\psi = -\psi\pi$. □

Let B be a quaternion algebra over $\mathbb{Q}$. We say that B is *definite* if ∞ ramifies in B: that is, if $B \otimes \mathbb{R} = \mathbb{H}$ is the algebra of real Hamilton quaternions. Equivalently, B is definite if and only if D_B is the product of an odd number of primes. Otherwise, $B \otimes \mathbb{R} = \mathrm{M}_2(\mathbb{R})$, and we say that B is *indefinite*.

If B is indefinite, then $h_{\mathbb{Z}}(B) = t_{\mathbb{Z}}(B) = 1$. Otherwise, $h_{\mathbb{Z}}(B)$ and $t_{\mathbb{Z}}(B)$ can be computed explicitly as in [29, p. 152]. When $D_B = p$ is prime, the class number $h_{\mathbb{Z}}(B)$ is the number of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, and $t_{\mathbb{Z}}(B)$ is the number of isomorphism classes of supersingular elliptic curves up to $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-conjugation.

Let $\mathbb{Q}_v$ be a local completion of $\mathbb{Q}$ at a place $v \leqslant \infty$. The Hilbert symbol over $\mathbb{Q}_v$ is a symmetric bilinear pairing

$$(\ , \ )_v : \mathbb{Q}_v^*/\mathbb{Q}_v^{*2} \times \mathbb{Q}_v^*/\mathbb{Q}_v^{*2} \longrightarrow \{\pm 1\},$$

which may be defined as $(m, n)_v = 1$ if the quaternion algebra $(\frac{m,n}{\mathbb{Q}_v}) \simeq \mathrm{M}_2(\mathbb{Q}_v)$, and $(m, n)_v = -1$ otherwise.

In practice, the Hilbert symbol is computed as follows. For $v = \infty$, we find that $(m, n)_\infty = -1$ if and only if $m < 0$ and $n < 0$. For any odd prime p, $(m, n)_p$ can be computed by using the multiplicative bilinearity of the pairing and the following three properties:

- $(-p, p)_p = 1$;
- $(m, n)_p = 1$ if $p \nmid 2mn$;
- $(m, p)_p = (\frac{m}{p})$ is the Legendre quadratic symbol for any $p \nmid m$.

Finally, the Hilbert symbol at 2 follows from the equality $\prod_v (m, n)_v = 1$.

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press

5. *Supersingular curves and distortion maps*

In the next sections we restrict attention to supersingular curves. As is known (see, for example, [25, Theorem V.3.1] and [17]), an elliptic curve E over a finite field $\mathbb{F}_q$ is *supersingular* if and only if $\mathrm{End}_{\overline{\mathbb{F}}_q}(E) \otimes \mathbb{Q}$ is a quaternion algebra over $\mathbb{Q}$ of reduced discriminant p.

Verheul [27] was the first to propose using non-rational endomorphisms to solve DDH problems. Let $P \in E(\mathbb{F}_{q^k})$ be a point of order r. If $\psi \in \mathrm{End}(E)$ is such that $\psi(P) \notin \langle P \rangle$, then $\{P, \psi(P)\}$ is a generating set for $E[r]$, and so $e_r(P, \psi(P)) \neq 1$. It follows that DDH problems in $\langle P \rangle$ can be solved. Verheul called such endomorphisms *distortion maps*.

Originally, distortion maps were exclusively used to map points defined over $\mathbb{F}_q$ to points defined over $\mathbb{F}_{q^k}$. In other words, the focus had been on the 1-eigenspace for the Frobenius map on $E[r]$. Verheul states [28, Theorem 5] that a suitable distortion map exists for every point $P \in E[r]$ when E is supersingular. The proof of [28, Theorem 5] is not constructive, and it seems difficult to obtain an algorithm for finding a distortion map using that approach.

In Theorem 5.2 below, we obtain an analogous result to that in [28], using completely different techniques. We can then give in Section 6 an algorithm for constructing a distortion map for any supersingular curve.

LEMMA 5.1. *Let E be a supersingular elliptic curve over $\mathbb{F}_q$, and let ψ be an endomorphism. Let P be an element of one of the eigenspaces of the q-power Frobenius map π. Then ψ maps P outside $\langle P \rangle$ if and only if*

$$P \notin \ker(\psi\pi - \pi\psi).$$

Proof. Suppose that $\pi(P) = [m]P$ for some m (indeed, either $m = 1$ or $m = q$). Now, $\psi(P)$ also in the eigenspace means that $\pi\psi(P) = [m]\psi(P) = \psi([m]P) = \psi\pi(P)$. In other words, $P \in \ker(\psi\pi - \pi\psi)$. The converse is similar. □

THEOREM 5.2. *Let E be a supersingular curve over $\mathbb{F}_q$, $q = p^a$. Suppose that $k > 1$, and let $r \mid \#E(\mathbb{F}_q)$, $r \neq p$, $r > 3$, be a prime. Let π be the q-power Frobenius map, and let $P \in E(\mathbb{F}_{q^k})$ be in a π-eigenspace. Then there exists a distortion map ψ on E that maps P outside $\langle P \rangle$.*

Proof. By Lemma 5.1, to prove the result it is enough to prove that there exists $\psi \in \mathrm{End}(E)$ such that $r \nmid \deg(\pi\psi - \psi\pi)$.

Let $P(T) = T^2 - tT + q$ be the characteristic polynomial of the q-power Frobenius element π acting on E. Since $k > 1$, we know (see, for example, [30] or [14, Theorem I.20]) that $P(T)$ is irreducible, and so its roots generate a quadratic field of $\mathbb{Q}$.

The endomorphism ring $\mathcal{R} = \mathrm{End}(E)$ is a maximal order in the quaternion algebra $B_p = \mathrm{End}(E) \otimes \mathbb{Q}$, which ramifies exactly at p and ∞; see [17]. The ring $\mathrm{End}_{\mathbb{F}_q}(E)$ is an order in the quadratic field $\mathbb{Q}(\pi) = \mathrm{End}_{\mathbb{F}_q}(E) \otimes \mathbb{Q} \simeq \mathbb{Q}(\sqrt{t^2 - 4q})$, naturally embedded in $\mathcal{R}$. Let $\pi_0 = 2\pi - t \in \mathbb{Q}(\pi)$, which satisfies $\mathrm{Tr}(\pi_0) = 0$ and $\mathrm{n}(\pi_0) = -\pi_0^2 = 4q - t^2$.

There is a morphism of $\mathbb{Q}$-vector spaces

$$\begin{array}{rccc} c_\pi : & B_p & \longrightarrow & B_p \\ & \psi & \longmapsto & \pi\psi - \psi\pi \end{array}$$

with $\ker(c_\pi) = \mathbb{Q}(\pi)$.

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press

Let $s \in \mathbb{Z}$. We remark that there exists an element $\psi_0 \in B_p$ such that $\psi_0^2 = -s$ and $\pi_0\psi_0 = -\psi_0\pi_0$ if and only if

$$B_p \simeq \left(\frac{t^2 - 4q, -s}{\mathbb{Q}}\right). \tag{5.1}$$

Indeed, one direction is immediate. The other implication follows from the Skolem-Noether theorem: if

$$B_p = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij = \left(\frac{t^2 - 4q, -s}{\mathbb{Q}}\right),$$

there exists $\gamma \in B_p^*$ with $\pi_0 = \gamma^{-1} i \gamma$, and we may take $\psi_0 = \gamma^{-1} j \gamma$.

Note that since the discriminant of B_p is p, condition (5.1) for a given s can be checked by computing a finite number of local Hilbert symbols. Moreover, since $B_p \otimes \mathbb{R}$ is a division algebra, we necessarily have $s > 0$.

Let $s \in \mathbb{Z}$ be such that (5.1) holds. By Proposition 4.2(3), there exists an integer N_0 coprime to r such that $t_{\mathbb{Z}[1/N_0]}(B_p) = 1$. Similarly, there exists an integer N_1 coprime to r, such that $\mathbb{Z}[1/N_1, \sqrt{t^2 - 4q}]$ is locally a discrete valuation ring at all primes $\ell \neq p$ and $h(\mathbb{Z}[1/N_1, \sqrt{t^2 - 4q}]) = 1$. Indeed, this is accomplished by considering a system of representatives $J_1, \ldots, J_{h(\mathbb{Q}(\sqrt{t^2-4q}))}$ of classes of ideals in the quadratic field $\mathbb{Q}(\sqrt{t^2 - 4q})$ such that

$$r \nmid \mathrm{N}_{\mathbb{Q}\sqrt{t^2-4q})/\mathbb{Q}}(J_i)$$

and taking

$$N_1 = 2 \cdot \prod \mathrm{N}_{\mathbb{Q}(\sqrt{t^2-4q})/\mathbb{Q}}(J_i).$$

By Proposition 4.3, there exists $\psi_0 \in \mathcal{R}[1/(N_0 \cdot N_1)]$ such that $\psi_0^2 = -s$ and $\pi_0\psi_0 = -\psi_0\pi_0$. Hence $N\psi_0 \in \mathcal{R}$ for some integer N supported at the primes dividing $N_0 \cdot N_1$ and thus coprime to r. The endomorphism $N\psi_0$ will be the distortion map that we are looking for. (This is all assuming that condition (5.1) holds.)

Since

$$\pi\psi_0 - \psi_0\pi = 2\pi_0\psi_0$$

and

$$\pi(\pi_0\psi_0) - (\pi_0\psi_0)\pi = \left(\frac{\pi_0 - t}{2}\right)(\pi_0\psi_0) - (\pi_0\psi_0)\left(\frac{\pi_0 - t}{2}\right) = (t^2 - 4q)\psi_0,$$

it readily turns out that

$$\mathrm{Im}(c_\pi) = \mathbb{Q} \cdot \psi_0 + \mathbb{Q} \cdot \pi_0\psi_0$$

and

$$c_\pi(\mathcal{R}) \supseteq c_\pi(\mathbb{Z} + \mathbb{Z}\pi_0 + N\mathbb{Z}\psi_0 + N\mathbb{Z}\pi\psi_0) = (t^2 - 4q)N\mathbb{Z}\psi_0 + N\mathbb{Z}\pi_0\psi_0.$$

Moreover, the degree of the isogenies $(t^2 - 4q)N\psi_0$ and $N\pi_0\psi_0$ on E are computed in terms of the reduced norm in the quaternion algebra B_p as

$$\deg((t^2 - 4q)N\psi_0) = (t^2 - 4q)^2 N^2 \mathrm{n}(\psi_0) = (t^2 - 4q)^2 N^2 s$$

and

$$\deg(N\pi_0\psi_0) = N^2 \mathrm{n}(\pi_0)\mathrm{n}(\psi_0) = (4q - t^2)N^2 s.$$

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press

Hence

$$\deg(\pi(N\psi_0) - (N\psi_0)\pi) = N^2(4q - t^2)s$$

is coprime to r, as desired.

It remains to give choices of s for which (5.1) is satisfied. According to a theorem of Waterhouse [30], the possible values of the trace of the Frobenius endomorphism are

$$t = 0, \qquad t = \pm p^{a/2}, \qquad t = \pm 2p^{a/2} \qquad \text{and} \qquad t = \pm p^{(a+1)/2}.$$

Recall that we can exclude the value $t = \pm 2p^{a/2}$ because we are assuming that $k > 1$. Hence, the only possible prime factors of $4q - t^2$ are 2, 3 and p, and in order to prove the claim, it suffices to show that

$$B_p \simeq \left(\frac{t^2 - 4q, -s}{\mathbb{Q}}\right),$$

either for $s = 1$ or for some prime s, $s \neq r$.

The following table lists, for each of the possible values of t, a choice of s such that condition (5.1) holds.

$t = 0$, a is odd, $p \not\equiv 1 \pmod 4$	$s = 1$
$t = 0$, a is odd, $p \equiv 1 \pmod 4$	s is any prime $s \equiv 3 \pmod 4$ and split in $\mathbb{Q}(\sqrt{-p})$
$t = 0$, a is even	$s = p$
$t = \pm p^{(a+1)/2}$	$s = 1$
$t = \pm p^{a/2}$	$s = p$

This table can be checked by computing the relevant Hilbert symbols. We give details of the argument for the first two rows of the table. Assume that $t = 0$ and a is odd. We see that $(-4p^a, -s)_\ell = (-p, -s)_\ell$ for all primes ℓ and $(-p, -s)_\ell = 1$ for all finite primes $\ell \nmid 2p \cdot s$. Moreover, we have $(-p, -s)_\infty = -1$ if and only if $s > 0$.

If $p \not\equiv 1 \pmod 4$, $p \neq 2$, then $(-p, -1)_p = (p, -1)_p = (\frac{-1}{p}) = -1$. Since we know that p and ∞ ramify in $(\frac{-p,-1}{\mathbb{Q}})$ and the number of ramifying places must be even, we see that $(-p, -1)_2 = 1$. Hence $(\frac{-p,-1}{\mathbb{Q}})$ is the quaternion algebra of discriminant p and $B_p \simeq (\frac{-p,-1}{\mathbb{Q}})$.

Similarly, if $p = 2$, it holds that $B_2 \simeq (\frac{-2,-1}{\mathbb{Q}})$.

If $p \equiv 1 \pmod 4$ and s is a prime $s \equiv 3 \pmod 4$ and split in $\mathbb{Q}(\sqrt{-p})$ (that is, $(\frac{-p}{s}) = 1$), then $(-p, -s)_p = (p, -s)_p = (\frac{-s}{p}) = -1$ and $(-p, -s)_s = (-p, s)_s = (\frac{-p}{s}) = 1$. Hence $B_p \simeq (\frac{-p,-s}{\mathbb{Q}})$.

Note that the theorem of Čebotarev implies there are infinitely many suitable primes s for line two of the table; hence we can always choose one that is not divisible by r.

We leave the checking of the remaining cases of the table above to the reader; remember that line three of the table applies only to $p = 2$ or $p \equiv 3 \pmod 4$, that line four of the table applies only to $p = 2, 3$, and that line five of the table applies only when $p = 3$ or $p \equiv 2 \pmod 3$.

This completes the proof. □

REMARK 5.1. It follows from the above proof that Theorem 5.2 is also valid for $r = 3$ unless $p = 3$ or $t = \pm p^{a/2}$. The statement is valid for $r = 2$ precisely when $p \neq 2$ and $t = \pm p^{a/2}$, or when $p = 3$ and $t = \pm p^{(a+1)/2}$.

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press

6. *An algorithm for constructing distortion maps*

The aim of this section is to derive from the proof of Theorem 5.2, an algorithm for constructing a distortion map on a supersingular curve over a field of characteristic p.

One might expect the first step of such an algorithm to involve computing a basis for the endomorphism ring using Kohel's algorithm [**19**] (which runs in exponential time). In fact, we argue that this is not required. Instead, we reflect upon how one would obtain a usable supersingular elliptic curve. It is known that for all finite fields $\mathbb{F}_q$ there is a supersingular elliptic curve E defined over $\mathbb{F}_q$ (and in general, there will be many non-$\mathbb{F}_q$-isomorphic such curves). We claim that all the curves that could potentially be used in practice arise as reductions of CM curves in characterstic zero of small class number.

To justify our claim, consider the following three candidate methods to find a supersingular curve over a finite field:

1. using the complex multiplication (CM) method;
2. constructing curves over fields of small characteristic (For example, $y^2 + y = f(x)$ over $\mathbb{F}_{2^m}$ is always supersingular.);
3. choosing random curves over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$ and counting points until a supersingular curve is found.

The third method method is not useful, as the probability of success is negligible. The number of isomorphism classes of supersingular curves over $\mathbb{F}_p$ is equal to $h_{-4p} + h_{-p}$ (where h_D is the class number of the order of discriminant D, and $h_{-p} = 0$ if $p \equiv 1 \pmod 4$; for details, see [**17**]). By the Brauer–Siegel theorem (more details below), this number is roughly $p^{1/2}$, and so the probability of a randomly chosen elliptic curve over $\mathbb{F}_p$ being supersingular is negligible. Similarly, the number of isomorphism classes of supersingular curves over $\mathbb{F}_{p^2}$ is $p/12$ (see [**25**, Theorem V.4.1 (c)]), and so the probability of a random curve over $\mathbb{F}_{p^2}$ being supersingular is negligible.

The second method restricts our attention to a very small number of isomorphism classes (and hence j-invariants). In the example given, the curves all have $j = 0$. Hence, all these curves can be treated as twists of reductions of curves in characteristic zero, and these curves can be chosen to be CM curves. Hence the second method is essentially a special case of the CM method.

The CM method works in the following setting. Let E be an elliptic curve over a number field F with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$. Let p be a rational prime that does not split in $\mathcal{O}$, and let $\mathfrak{p}$ be a prime of F above p. Then by the Deuring reduction theorem, $\tilde{E} = E \pmod{\mathfrak{p}}$ is a supersingular elliptic curve over the residue field k of F at $\mathfrak{p}$. The main step of the CM method is to construct the ring class polynomial of the order $\mathcal{O}$ (which has degree $h_{\mathcal{O}}$, the class number of the order), and to find a root of it in characteristic p. This process has exponential complexity in the class number $h_{\mathcal{O}}$, and can be applied in practice only when $h_{\mathcal{O}}$ is relatively small.

It would be very interesting to have an alternative construction for supersingular curves. This open problem is also raised in [**28**, Section 4.1].

Proposition 6.1. *Let E/F be an elliptic curve defined over a number field F with complex multiplication by an order $\mathcal{O}$ of discriminant D in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$. Assume that $K \not\subset F$. Let p be a prime for which E has good and supersingular reduction. Let $\mathfrak{p}$ be a prime ideal of F above p. Let $\tilde{E}$ over $k = \mathbb{F}_{p^m}$ be the reduction mod $\mathfrak{p}$ of E. Let π be the p^m-Frobenius map on $\tilde{E}$. Suppose that $r \mid \#\tilde{E}(\mathbb{F}_{p^m})$ is a prime such that $r > 3$ and $r \nmid pD$.*

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press

Let $d > 0$ be such that $\sqrt{-d} \in \mathcal{O}$. Let $\Psi \in \mathrm{End}(E)$ satisfy $\Psi^2 = -d$. Let $\psi \in \mathrm{End}_{\overline{\mathbb{F}}_p}(\tilde{E})$ be the reduction mod $\mathfrak{p}$ *of* Ψ.

Then ψ is a suitable distortion map for points $P \in \tilde{E}[r]$ that lie in a π-eigenspace.

Proof. Note that since $K \not\subset F$, $H = F \cdot K$ is a quadratic extension over F. We know by the theory of complex multiplication that the minimal field of definition of the endomorphisms of E is H; it follows that, if we let $\sigma \in \mathrm{Gal}(H/F)$ be a non-trivial element, then $\Psi^\sigma = -\Psi$. Let $\tilde{k}$ be the residue field of a prime ideal in H above $\mathfrak{p}$. The natural Galois action of $\mathrm{Gal}(H/F)$ on $\mathrm{End}_H(E) \otimes \mathbb{Q}$ descends to an action of $\mathrm{Gal}(\tilde{k}/k)$ on $\mathrm{End}_{\tilde{k}}(E) \otimes \mathbb{Q} \simeq B_p$. If we let $\tilde{\sigma}$ denote a generator of $\mathrm{Gal}(\tilde{k}/k)$, we find that $\psi^{\tilde{\sigma}} = -\psi$, due to the compatibility of the Galois action.

The Galois automorphism $\tilde{\sigma}$ acts on the quaternion algebra B_p as an automorphism $\tilde{\sigma} : B_p \longrightarrow B_p$. By the Skolem–Noether theorem, $\alpha^{\tilde{\sigma}} = \gamma\alpha\gamma^{-1}$ for some $\gamma \in B_p^*$, which is uniquely determined as an element of $B_p^*/\mathbb{Q}^*$. Since $\pi^{\tilde{\sigma}} = \gamma\pi\gamma^{-1} = \pi$ because $\pi \in \mathrm{End}_k(E)$, we deduce that $\gamma\pi = \pi\gamma$, and hence $\gamma \in \mathbb{Q}(\pi)$. Since $\psi^{\tilde{\sigma}} = \gamma\psi\gamma^{-1} = -\psi$, it follows that $\mathrm{Tr}(\gamma\psi) = \gamma\psi + \overline{\gamma\psi} = -\psi\gamma + \overline{\psi}\,\overline{\gamma} = \gamma\psi - \psi\overline{\gamma} = -\mathrm{Tr}(\gamma)\psi \in \mathbb{Z}$. Hence $\mathrm{Tr}(\gamma) = 0$ and $\gamma = \pi$ in $B_p^*/\mathbb{Q}^*$. Thus $\pi\psi = -\psi\pi$, and so $\psi\pi - \pi\psi = 2\psi\pi$ is an isogeny of degree $4p^m d$.

Now let $P \in \tilde{E}[r]$ be in a π-eigenspace. We apply arguments used in the proof of Theorem 5.2. Since $r > 3$ and $r \nmid pd$, we see that $P \notin \ker(\psi\pi - \pi\psi)$. Therefore $\psi(P)$ is independent of P. □

We can now present our algorithm. The input is a supersingular elliptic curve $\tilde{E}$ over a finite field $\mathbb{F}_q$, where $q = p^m$. We also assume that an order $\mathcal{O} \subset \mathrm{End}(\tilde{E})$ of class number $h_{\mathcal{O}}$ is specified. Note that by the Brauer–Siegel theorem, we find that the discriminant $D_{\mathcal{O}}$ of $\mathcal{O}$ is $O(h_{\mathcal{O}}^{2+\varepsilon})$ (see Lang's [**20**, Theorem XVI.5]; for non-maximal orders, see also [**21**, Theorem 8.7]). The notation $D_{\mathcal{O}} = O(h_{\mathcal{O}}^{2+\varepsilon})$ means that for every $\varepsilon > 0$ there is a constant c_ε, which depends on ε, such that $D_{\mathcal{O}} \leqslant c_\varepsilon h_{\mathcal{O}}^{2+\varepsilon}$ for all $\mathcal{O}$.

Algorithm 1 (Construction of a distortion map on $\tilde{E}$).

1. Let $\mathcal{O}$ be an order in $\mathrm{End}(\tilde{E})$ of class number $h_{\mathcal{O}}$. Compute the discriminant D of $\mathcal{O}$. Hence compute an integer $d > 0$ of size $O(D)$ such that $\sqrt{-d} \in \mathcal{O}$ (for example, we can take $d = -D$). Denote $\sqrt{-d}$ by ψ, so that ψ is a d-isogeny.

2. Factor d as $\prod_{i=1}^n l_i$ (where l_i are not necessarily distinct primes). Then ψ is a composition $\psi_1 \ldots \psi_n$ of prime degree isogenies (and each ψ_i will be defined over $\mathbb{F}_{q^2}$).

3. Use Galbraith's algorithm [**12**] to construct a tree of prime degree isogenies between j-invariants of supersingular elliptic curves in characteristic p. The tree starts with vertex $j(\tilde{E})$, and the process terminates when this vertex is revisited by a non-trivial isogeny. Since we know there is a non-trivial isogeny ψ of degree d, we should select only the primes l_i as found in step 2.

4. Construct the isogeny ψ on $\tilde{E}$ explicitly as the composition of isogenies ψ_i. Each isogeny ψ_i can be computed from the j-invariants of the corresponding elliptic curves, using methods of Elkies [**10**] and Vélu [**26**]. Usually, it is also necessary to construct an additional isomorphism between the image of the final isogeny ψ_n and the elliptic curve $\tilde{E}$. All these calculations will be performed over $\mathbb{F}_{q^2}$.

By Proposition 6.1, the endomorphism ψ will be a suitable distortion map. Hence the algorithm is clearly correct.

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press

We now roughly analyse the complexity of the algorithm. We assume a unit cost for operations in the field of definition $\mathbb{F}_q$ of $\tilde{E}$. We express the complexity in terms of the class number $h = h_{\mathcal{O}}$. For further details of the complexity analysis of algorithms like this, see Elkies [**10**] and Galbraith [**12**].

1. Step 1 is essentially trivial. Since D is $O(h^{2+\varepsilon})$, the complexity of this step is $O(h^{2+\varepsilon})$.

2. Factorisation can be easily done in time $O(\sqrt{d})$, which is $O(h^{1+\varepsilon})$. The number n is $O(\log(h))$, while the primes themselves are $O(d) = O(\log(h^{2+\varepsilon}))$.

3. There are $n = O(\log(h))$ iterations of the process. Each step requires computing the lth modular polynomial $\Phi_l(x, y)$ (which has degree $l + 1$ in each variable, and takes $O(l^3)$ operations to compute) and finding the roots of $\Phi_l(j, y)$ in $\mathbb{F}_{q^2}$ (which takes $O(l \log(q))$ operations). The total cost of this stage in the worst case is therefore $O(\log(h)(h^{6+\varepsilon} + h^{2+\varepsilon} \log(q)))$. The space requirement for the tree is $O(\log(h))$.

4. Finding the path in the tree takes time $O(\log(h))$. For each l-isogeny in the composition, Elkies's algorithm requires $O(l^3)$ operations and Vélu's requires $O(l)$ operations. Computing the isomorphism is trivial. Hence the total cost of explicitly computing the isogeny ψ is $O(\log(h)h^{6+\varepsilon})$ operations.

To conclude, it is clear that step 3 is the dominant step. The total complexity of the algorithm is $O(\log(h)(h^{6+\varepsilon} + h^{2+\varepsilon} \log(q)))$. Since we can construct only curves for which h is bounded by a polynomial function, this is therefore a polynomial-time algorithm on families of curves that have been constructed in any practical setting.

7. *Standard examples*

In the previous sections, we showed the existence of non-rational endomorphisms ψ with a certain property (namely, that $\psi(\pi(Q)) \neq \pi(\psi(Q))$ for points of order r which are in a Frobenius eigenspace). In practice, there are a small number of examples of supersingular curves that are widely used, and popular distortion maps are already known in these cases. In this section we recall these familiar examples, and show that they satisfy the above property.

Table 1 gives the list of curves studied. These curves have been considered by several authors (for example, Verheul [**27**] and Galbraith [**13**]). Note that in all cases, we have $j(E) = 0$ or $j(E) = 1728$. This table does not list all possible variations of distortion maps. For instance, Barreto has suggested using

$$\psi(x, y) = (x + \zeta_3^2, y + \zeta_3 x + t),$$

where $t^2 + t = \zeta_3$ in the case of characteristic 2 and $k = 4$.

Proposition 7.1. *Let E be a supersingular curve over $\mathbb{F}_q$ from Table 1, where q is a power of $p > 3$. Let π be the q-power Frobenius. Suppose that $r \mid \#E(\mathbb{F}_q)$ and $r > 3$. Then the distortion map ψ listed in the table satisfies $r \nmid \deg(\pi\psi - \psi\pi)$.*

Proof. Consider first the case when E is the curve $y^2 = x^3 + ax$ over $\mathbb{F}_p$ with $k = 2$ and with the distortion map $\psi : (x, y) \longmapsto (-x, iy)$. Clearly, $\psi^2 = -1$ and this case is covered by Proposition 6.1. One can also give a direct proof.

Now consider the case $E : y^2 = x^3 + a$ with $k = 2$ over $\mathbb{F}_p$ ($p \equiv 2 \pmod 3$) and with the distortion map $\psi(x, y) = (\zeta_3 x, y)$. In this case we have $\psi^3 = 1$, and so Proposition 6.1 does not apply. A variant of Proposition 6.1 that handles this case can be proved, but instead we give the following direct argument. Let $Q = (x, y) \in E[r]$. Since $r > 3$, we have $x \neq 0$.

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press

Table 1: Popular distortion maps.

k	Elliptic curve data
2	$E : y^2 = x^3 + a$ over $\mathbb{F}_p$, where $p \equiv 2 \pmod 3$, $p > 2$; $\#E(\mathbb{F}_p) = p + 1$; distortion map $(x, y) \longmapsto (\zeta_3 x, y)$, where $\zeta_3^3 = 1$.
2	$y^2 = x^3 + ax$ over $\mathbb{F}_p$, where $p \equiv 3 \pmod 4$; $\#E(\mathbb{F}_p) = p + 1$; distortion map $(x, y) \longmapsto (-x, iy)$, where $i^2 = -1$.
3	$E : y^2 = x^3 + a$ over $\mathbb{F}_{p^2}$, where $p \equiv 5 \pmod 6$ and $a \in \mathbb{F}_{p^2}$, $a \notin \mathbb{F}_p$ is a square that is not a cube; $\#E(\mathbb{F}_{p^2}) = p^2 - p + 1$; distortion map $(x, y) \longmapsto (\gamma^2 x^p, by^p/b^p)$, where $a = b^2$ ($b \in \mathbb{F}_{p^2}$) and $\gamma \in \mathbb{F}_{p^6}$ satisfies $\gamma^3 = b/b^p$.
4	$y^2 + y = x^3 + x + b$ over $\mathbb{F}_2$; distortion map $(x, y) \longmapsto (\zeta_3 x + s^2, y + \zeta_3 sx + s)$, where $s \in \mathbb{F}_{2^4}$ satisfies $s^2 + \zeta_3 s + 1 = 0$.
6	$y^2 = x^3 + ax + b$ over $\mathbb{F}_3$; distortion map $(x, y) \longmapsto (\alpha - x, iy)$, where $i \in \mathbb{F}_{3^2}$ and $\alpha \in \mathbb{F}_{3^3}$ satisfy $i^2 = -1$ and $\alpha^3 + a\alpha - b = 0$.

We have $\pi\psi(Q) = \pi(\zeta_3 x, y) = (\zeta_3^2 \pi(x), \pi(y))$, while $\psi\pi(Q) = (\zeta_3 \pi(x), \pi(y)) \neq \pi\psi(Q)$. Clearly, $Q \notin \ker(\pi\psi - \psi\pi)$, and the result follows.

Finally, consider the case $k = 3$ with $E : y^2 = x^3 + a$. Since $\gamma^2 \notin \mathbb{F}_{p^2}$, we have $\pi(\gamma^2) \neq \gamma^2$. The x-coordinate of $\psi\pi(Q)$ is $\gamma^2\pi(x)$, while the x-coordinate of $\pi\psi(Q)$ is $\pi(\gamma^2 x) = \pi(\gamma^2)\pi(x)$. Since $r > 3$, we have $x \neq 0$, and so the x-coordinates are not equal. The result follows. □

PROPOSITION 7.2. *Let E be a supersingular curve over $\mathbb{F}_q$ from Table 1, where q is a power of 2. Let π be the q-power Frobenius map. Suppose that $r \mid \#E(\mathbb{F}_q)$ is such that $r > 1$. Then the distortion map ψ listed in the table satisfies $r \nmid \deg(\pi\psi - \psi\pi)$.*

Proof. The relevant curve is $E : y^2 + y = x^3 + x + b$ with distortion map $\psi(x, y) = (\zeta_3 x + s^2, y + \zeta_3 sx + s)$, where $\zeta_3^3 = 1$ and $s^2 + \zeta_3 s + 1 = 0$. Since $\psi^3 = 1$, we cannot apply Proposition 6.1, so we give a direct argument.

If $\pi\psi(Q) = \psi\pi(Q)$, then $\pi^2\psi(Q) = \psi\pi^2(Q)$, so it is enough to prove that the latter equality does not hold. Suppose that $q = 2^m$, where m is odd (otherwise, $k < 4$). Clearly, π^2 fixes $\mathbb{F}_{q^2}$, and so $\pi^2(\zeta_3) = \zeta_3$. Now π^2 does not fix $s \in \mathbb{F}_{q^4}$ so, by inspection of the minimal polynomial, $\pi^2(s) = s + \zeta_3$.

Let $Q = (x, y) \in E[r]$. Then the x-coordinate of $\pi^2\psi(Q)$ is $\pi^2(\zeta_3 x + s^2) = \zeta_3\pi(x^2) + s^2 + \zeta_3^2$, while the x-coordinate of $\psi\pi^2(Q)$ is $\zeta_3\pi^2(x) + s^2$. The result follows. □

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press

PROPOSITION 7.3. *Let E be a supersingular curve over $\mathbb{F}_q$ from Table 1, where q is a power of 3. Let π be the q-power Frobenius map. Suppose that $r \mid \#E(\mathbb{F}_q)$ and $r > 1$. Then the distortion map ψ listed in the table satisfies $r \nmid \deg(\pi\psi - \psi\pi)$.*

Proof. Clearly, $\psi^2 = -1$, and Proposition 6.1 applies (take F to be a cubic extension of $\mathbb{Q}$). There is also an easy direct proof. □

8. *Distortion maps that are not isomorphisms*

By [25, Theorem III.10.1], there are non-trivial automorphisms only when $j(E) = 0$ or $j(E) = 1728$ (in particular, when the endomorphism ring has a subring isomorphic to either $\mathbb{Z}[i]$ or $\mathbb{Z}[\zeta_3]$, both of which are rings with non-trivial units). Hence, we cannot expect distortion maps to be automorphisms in all cases.

Even in the cases $j = 0$ and $j = 1728$, we see that the value $s = 1$ cannot always be taken in the proof of Theorem 5.2. This indicates why the $k = 3$ example in characteristic p (with $t = p^{a/2}$) does not admit a distortion map that is an automorphism.

The aim of this section is to give some examples of these distortion maps. For the first example, we use Algorithm 1. For the second example we use an ad-hoc technique that shows that Algorithm 1 is not optimal.

8.1. *Example: $D = -8$*

This example illustrates Algorithm 1 with the case $d = 2$. The ring $\mathbb{Z}[\sqrt{-2}]$ has discriminant $D = -8$. The elliptic curve

$$E : y^2 = x^3 + x^2 - 3x + 1$$

has j-invariant equal to 8000, and its endomorphism ring is isomorphic to $\mathbb{Z}[\sqrt{-2}]$.

We seek a 2-isogeny to a curve with j-invariant also equal to 8000. Consider the rational 2-isogeny whose kernel is generated by the 2-torsion point $(1, 0)$. The equations for this isogeny (found using [26]) are

$$(x, y) \longmapsto \left(\frac{3x^2 - 2x + 5}{3(x-1)}, y\frac{x^2 - 2x - 1}{(x-1)^2}\right),$$

and the image under this isogeny is the elliptic curve

$$E' : y^2 = x^3 - \frac{40x}{3} - \frac{448}{27}.$$

The curve E' has $j(E') = 8000$, but it is not isomorphic to E over $\mathbb{Q}$. There is an isomorphism from E' to E over $\mathbb{Q}(\sqrt{-2})$ given by

$$(x, y) \longmapsto \left(\frac{-x}{2} - \frac{1}{3}, \sqrt{-2}\frac{y}{4}\right).$$

The composition of the 2-isogeny and the isomorphism gives a distortion map $\psi : E \longrightarrow E$ which, by Proposition 6.1, is suitable for our application. This can be used for E over $\mathbb{F}_p$ whenever p is inert in $\mathbb{Q}(\sqrt{-2})$ (that is, $p \equiv 5, 7 \pmod 8$).

We note that nicer equations in this case are known; see [8, Section 14B], [16] or [22].

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press

8.2. *Example:* $D = -7$

We consider the CM curve with j-invariant -3375 and endomorphism ring $\mathbb{Z}[(1+\sqrt{-7})/2]$. The units of this ring are simply ± 1. We consider the following curve equation (obtained from Cremona's tables [9]):

$$E : y^2 + xy = x^3 - x^2 - 2x - 1.$$

By Deuring's reduction theorem (see [21, p. 182, Theorem 12]) this curve has supersingular reduction modulo p whenever $p = 7$ or $(\frac{-7}{p}) = -1$ (that is, $p \equiv 2, 5, 6 \pmod 7$). When E is supersingular modulo p, then $\#E(\mathbb{F}_p) = p + 1$, and the embedding degree is $k = 2$.

We seek a non-rational isogeny from E to itself. Since $\mathbb{Z}[(1+\sqrt{-7})/2]$ contains $\sqrt{-7}$, we could apply Algorithm 1 to get a 7-isogeny. Instead, we note that $\mathbb{Z}[(1+\sqrt{-7})/2]$ contains elements of norm 2, and so we should be able to find a 2-isogeny.

Since the kernel of a 2-isogeny is an element of order 2, we start by finding the 2-torsion on E in characteristic zero. Recall that a point $P = (x, y)$ has order 2 if $P = -P$ and in this case $-P = (x, -y - x)$; hence we require that $x = -2y$. One can easily check that

$$E[2] = \{0_E, (2, -1), (-2\alpha, \alpha), (-2\overline{\alpha}, \overline{\alpha})\},$$

where $\alpha = (5 + \sqrt{-7})/16$.

The isogeny coming from $(2, -1)$ is rational, and turns out not to be useful. Hence we apply Vélu's formulae [26] to construct an isogeny with kernel generated by the point $(-2\alpha, \alpha)$. Summarising the results, let

$$A_4 = \frac{-29 - 105\sqrt{-7}}{32} \qquad \text{and} \qquad A_6 = \frac{-849 + 595\sqrt{-7}}{128},$$

and define

$$X = x + \frac{-7 + 21\sqrt{-7}}{32x + 20 + 4\sqrt{-7}}$$

$$Y = y - \frac{\big(-7 + 21\sqrt{-7}\big)\big(2x + 2y + (5 + \sqrt{-7})/8\big)}{\big(8x + 5 + \sqrt{-7}\big)^2}.$$

Then the map $\psi_1(x, y) = (X, Y)$ is a 2-isogeny from E to

$$E' : Y^2 + XY = X^3 - X^2 + A_4 X + A_6,$$

where $j(E') = -3375$ too.

It remains to compute an isomorphism from E' to E. Let

$$u = \frac{-1 - \sqrt{-7}}{4};$$

$$r = \frac{11 - \sqrt{-7}}{32};$$

$$t = \frac{-11 + \sqrt{-7}}{64};$$

$$s = \frac{-5 - \sqrt{-7}}{8}.$$

Then the mapping $\psi_2(X, Y) = (u^2 X + r, u^3 Y + u^2 s X + t)$ is an isomorphism from E' to E.

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press

Defining $\psi(x, y) = \psi_2(\psi_1(x, y))$, we obtain our distortion map from E to E. In practice, it is easier to store the isogenies separately and to compute the distortion map by computing the composition.

Proposition 6.1 does not apply to this map, so we give a direct proof that it is suitable. Consider a point Q on the reduction of E over $\mathbb{F}_{p^m}$ (m odd) where p is inert in $\mathbb{Q}(\sqrt{-7})$. Let π be the p^m-power Frobenius. If $Q \notin \ker(\psi)$, then we show that $\pi\psi(Q) \neq \psi\pi(Q)$. The x-coordinate of the composition of the isogeny and the isomorphism is

$$\frac{-3+\sqrt{-7}}{8}x + \frac{\left(-63-35\sqrt{-7}\right)/16}{8x+5+\sqrt{-7}} + \frac{11-\sqrt{-7}}{32}.$$

Since π maps $\sqrt{-7} \in \mathbb{F}_{q^2}$ to $-\sqrt{-7}$, it is clear that we cannot have $\pi\psi(Q) = \psi\pi(Q)$ for any point Q except the points in the kernel of ψ.

As noted above, this example shows that Algorithm 1 does not necessarily provide an endomorphism of minimal degree. Finally, we note that nicer equations in this case are known; see [**7**, Section 7.2.3], [**16**] or [**22**].

9. *Remaining hard problems*

In the ordinary case, Verheul [**27**] has shown that there are no non-rational endomorphisms. In this case it seems that DDH is hard in both eigenspaces for the Frobenius map.

To solve the DDH problem in the small field, one might try to invert the trace map. In fact, it is trivial to find pre-images under the trace map (for example, given $R \in E(\mathbb{F}_q)$, a pre-image would be $k^{-1}R$), but it seems to be difficult to find pre-images in a coherent way without using some kind of non-rational group homomorphism.

It remains an open problem either to show that DDH is easy on ordinary elliptic curves in all cases, or to give evidence that the problem is hard in the remaining two cases (that is, the two eigenspaces of Frobenius).

The generalisation of these results to the case of abelian varieties of higher dimension seems to be hard. In particular, our algorithm relies on modular equations to compute isogenies, and it is a well-known open problem to extend these techniques to the higher-dimensional case.

Acknowledgements. We are grateful to Paulo Barreto, Florian Hess, Takakazu Satoh, Alice Silverberg and Eric Verheul for comments on an earlier version of the paper.

References

1. M. Alsina and P. Bayer, *Quaternion orders, quadratic forms, and Shimura curves*, CRM Monogr. Ser. 22 (Amer. Math. Soc., Providence, RI, 2004). 205

2. P. S. L. M. Barreto, H. Y. Kim, B. Lynn and M. Scott, 'Efficient implementation of pairing-based cryptosystems', *CRYPTO* 2002, Lecture Notes in Comput. Sci. 2442 (ed. M. Yung, Springer, New York, 2002) 354–368. 203

3. P. S. L. M. Barreto, B. Lynn and M. Scott, 'On the selection of pairing-friendly groups', *SAC* 2003, Lecture Notes in Comput. Sci. 3006 (ed. M. Matsui and R. Zuccherato, Springer, New York, 2004) 17–25. 204

4. D. Boneh, 'The decision Diffie–Hellman problem', *ANTS* III, Lecture Notes in Comput. Sci. 1423 (ed. J. Buhler, Springer, New York, 1998) 48–63. 201

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press

5. D. Boneh and M. Franklin, 'Identity-based encryption from the Weil pairing', (full version) *SIAM J. Comp.* 32 (2003) 586–615. 204

6. D. Boneh, B. Lynn and H. Shacham, 'Short signatures from the Weil pairing', *ASIACRYPT* 2001, Lecture Notes in Comput. Sci. 2248 (ed. C. Boyd, Springer, New York, 2001) 514–532. 201, 204

7. H. Cohen, *A course in computational algebraic number theory*, Grad. Texts in Math. 138 (Springer, New York, 1993). 216

8. D. A. Cox, *Primes of the form* $x^2 + ny^2$ (Wiley, 1989). 214

9. J. Cremona, *Algorithms for modular elliptic curves* (Cambridge Univ. Press, 1992). 215

10. N. Elkies, 'Elliptic and modular curves over finite fields and related computational issues', *Computational perspectives on number theory* (ed. D. A. Buell and J. T. Teitelbaum, Amer. Math. Soc., 1997) 21–76. 211, 212

11. G. Frey and H.-G. Rück, 'A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves', *Math. Comp.* 52 (1994) 865–874. 203, 204

12. S. D. Galbraith, 'Constructing isogenies between elliptic curves over finite fields', *LMS J. Comput. Math.* 2 (1999) 118–138. 211, 212

13. S. D. Galbraith, 'Supersingular curves in cryptography', *ASIACRYPT* 2001, Lecture Notes in Comput. Sci. 2248 (ed. C. Boyd, Springer, New York, 2001) 495–513. 212

14. S. Galbraith, 'Pairings', *Advances in elliptic curve cryptography*, (ed. I. Blake, G. Seroussi and N. P. Smart, Cambridge Univ. Press, to appear) Chapter IX. 203, 204, 207

15. S. D. Galbraith, K. Harrison and D. Soldera, 'Implementing the Tate pairing', *ANTS*-V, Lecture Notes in Comput. Sci. 2369 (ed. C. Fieker and D. Kohel, Springer, New York, 2002) 324–337. 203

16. R. P. Gallant, R. J. Lambert and S. A. Vanstone, 'Faster point multiplication on elliptic curves with efficient endomorphisms', *CRYPTO* 2001, Lecture Notes in Comput. Sci. 2193 (ed. J. Kilian, Springer, New York, 2001) 190–200. 214, 216

17. B. H. Gross, *Heights and special values of L-series*, CMS Conf. Proc. 7 (Amer. Math. Soc., Providence, RI, 1986) 115–187. 207, 210

18. A. Joux and K. Nguyen, 'Separating decision Diffie–Hellman from computational Diffie–Hellman in cryptographic groups', *J. Cryptology* 16 (2003) 239–247 . 203

19. D. Kohel, 'Endomorphism rings of elliptic curves over finite fields', PhD thesis, Berkeley, 1996. 210

20. S. Lang, *Algebraic number theory*, Grad. Texts in Math. 110 (Springer, New York, 1986). 211

21. S. Lang, *Elliptic functions*, Grad. Texts in Math. 112 (Springer, New York, 1987). 211, 215

22. A. G. Rostovtsev and E. B. Makhovenko, 'Elliptic curve point multiplication', *MMM-ACNS* 2003, Lecture Notes in Comput. Sci. 2776 (ed. V. Gorodetsky *et al.*, Springer, New York, 2003) 328–336. 214, 216

23. V. Rotger, 'Quaternions, polarizations and class numbers', *J. Reine Angew. Math.* 561 (2003) 177–197. 206

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press

24. V. Rotger, 'The field of moduli of quaternionic multiplication on abelian varieties', *Int. J. Math. Math. Sci.*, to appear. 206

25. J. H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts in Math. 106 (Springer, New York, 1986). 202, 207, 210, 214

26. J. Vélu, 'Isogénies entre courbes elliptiques', *C.R. Acad. Sci. Paris, Sér. A* 273 (1971) 238–241. 211, 214, 215

27. E. R. Verheul, 'Evidence that XTR is more secure than supersingular elliptic curve cryptosystems', *EUROCRYPT* 2001, Lecture Notes in Comput. Sci. 2045 (ed. B. Pfitzmann, Springer, New York, 2001) 195–210. 207, 212, 216

28. E. R. Verheul, 'Evidence that XTR is more secure than supersingular elliptic curve cryptosystems' (full version), *J. Cryptology*, to appear. 202, 203, 207, 210

29. M. F. Vignéras, *Arithmetic of quaternion algebras*, Lecture Notes in Math. 800 (Springer, New York, 1980). 205, 206

30. E. Waterhouse, 'Abelian varieties over finite fields', *Ann. Sci. École Norm. Sup.* (4) 2 (1969) 521–560. 207, 209

Steven D. Galbraith `Steven.Galbraith@rhul.ac.uk`
`http://www.isg.rhul.ac.uk/~sdg/`

Mathematics Department
Royal Holloway University of London
Egham, Surrey TW20 0EX
United Kingdom

Victor Rotger `vrotger@mat.upc.es`

Universitat Politècnica de Catalunya
Departament de Matemàtica Aplicada IV (EUPVG)
Av. Victor Balaguer s/n
08800 Vilanova i la Geltrú
Spain

https://doi.org/10.1112/S1461157000001108 Published online by Cambridge University Press