# The Diffie-Hellman problem and generalization of Verheul's theorem

Dustin Moody

December 3, 2008

**Abstract**

Bilinear pairings on elliptic curves have been of much interest in cryptography recently. Most of the protocols involving pairings rely on the hardness of the bilinear Diffie-Hellman problem. In contrast to the discrete log (or Diffie-Hellman) problem in a finite field, the difficulty of this problem has not yet been much studied. In 2001, Verheul [66] proved that on a certain class of curves, the discrete log and Diffie-Hellman problems are unlikely to be provably equivalent to the same problems in a corresponding finite field unless both Diffie-Hellman problems are easy. In this paper we generalize Verheul's theorem and discuss the implications on the security of pairing based systems. We also include a large table of distortion maps.

## 1 Introduction

Throughout history, people have needed ways to transmit information in a secure manner. In the basic model for cryptography, entities $A$ (Alice) and $B$ (Bob) are communicating over a possibly insecure channel. It is assumed that an adversary $E$ (Eve), who desires to know what Alice and Bob are saying to each other, has access to the channel, as well as considerable computing power. If Alice and Bob are careful, they can use cryptography for many different objectives, including ensuring message confidentiality, creating digital signatures, or exchanging keys.

Since 1985, the theory of elliptic curves has been used in cryptography. Elliptic curve cryptosystems have some advantages over other systems. For one, there is a wide range of parameters for a user to choose from. Given a prime power $q = p^f$, ($p \neq 2$ or 3), we can define an elliptic curve over $\mathbb{F}_q$ by the equation

$$E : y^2 = x^3 + Ax + B,$$

where $A$ and $B$ in $\mathbb{F}_q$ are chosen so that $4A^3 + 27B^2 \neq 0$.

More importantly, elliptic curves offer the same level of security as other systems, but with a much shorter keylength. This has made elliptic curve cryptography an increasingly popular choice.

In the past few years, pairings on elliptic curves have been a very active area of research in cryptography. A pairing is a map from pairs of points on an elliptic curve into the multiplicative group of a finite field. The two pairings most commonly used, the Weil and Tate pairings, are also bilinear and non-degenerate. These properties have enabled the construction of new protocols for a variety of cryptographic applications.

The security for most of these protocols relies on the hardness of the bilinear Diffie-Hellman problem, or some related problem. In contrast to the discrete log (or Diffie-Hellman) problem in a finite field, the difficulty of this problem has not yet been much studied. It is known that the bilinear Diffie-Hellman problem is not harder than the discrete log or Diffie-Hellman problem in a finite field, but the precise relationship is not yet clear.

In 2001, Verheul [66] proved a theorem relating to the then new XTR cryptosystem. Using pairings, there is a computable homomorphism from certain supersingular elliptic curves to the group used in the XTR cryptosystem. At the Crypto 2000 rump session [47] it was pointed out that if this map could be efficiently inverted, the XTR system would be equivalent to a supersingular elliptic curve cryptosystem. As such, any attack on supersingular elliptic curve cryptography would yield an attack on the XTR system. Thus the security of XTR would be no greater than that of supersingular elliptic curve systems.

In response, Verheul proved that the construction of a computable inverse would yield an efficient algorithm to solve the Diffie-Hellman problem in certain finite fields. Since the Diffie-Hellman problem is widely believed to be difficult, this would seem to show that the XTR cryptosystem is not just an elliptic curve system in disguise.

The results in Verheul's paper were specifically geared at a certain class of finite fields and supersingular curves, but we generalize his result in this paper to arbitrary finite fields and associated supersingular curves. We show that for any finite field $\mathbb{F}_q$, we can construct supersingular elliptic curves which under the so called MOV embedding are isomorphic to the product of two cyclic groups of order $q-1$. If this embedding can be efficiently inverted, then we show that the Diffie-Hellman problem is efficiently solvable in $\mathbb{F}_q^*$, as well as on the curve.

Verheul established his result before the advent of pairing based cryptology, and it was intended solely to ensure confidence in the XTR system. It is now of interest because of the light it sheds on the relationship between Diffie-Hellman and discrete log type problems in different groups and especially because of certain implications for the security of pairing-based cryptography. Namely, our generalization of Verheul's theorem says that the security of pairing based systems depends on the infeasibility of constructing an inverse to the Menezes-Okamoto-Vanstone embedding. Moreover, Verheul's own interpretation of his theorem (see the title of [38]) would suggest that the groups used in pairing-based cryptography are less secure than subgroups of multiplicative groups of finite fields. We will examine these implications more closely.

The outline of this paper is as follows. In chapter 2 we will review some basic facts about elliptic curves. In chapter 3 we will discuss some of the mathematical problems upon which the security of many cryptosystems rely. In the

fourth chapter, we discuss in more detail the theorem of Verheul (including its generalization), and its consequences. We give the mathematical background and definitions of the Tate and Weil pairings in chapter 5. In chapter 6 we define distortion maps, a tool used in pairing based cryptography and a key part of the proof of the main result of this paper. We also study isogenies of elliptic curves over finite fields, which are used to create distortion maps. chapter 7 will look at some of the ways pairings have been utilized in cryptography. In chapter 8 we provide some algorithms needed for the generalization of Verheul's theorem, and determine their complexity. In chapter 9, we look at the special cases of our result when the characteristic of the finite field is 2. We give the proof of the main theorem in chapter 10, and some examples in chapter 11. Finally, in chapter 12 we look at future directions of research and open questions. We also include an appendix containing a table of explicit distortion maps.

# 2 Elliptic Curves

## 2.1 Group law

Let $K$ be a field. Consider the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in K.$$

Let $L$ be any field containing $K$, and $E(L)$ be the set of pairs $(x, y) \in L^2$ that satisfy the above equation, together with a "point at infinity" written $\infty$. If there is no point of $E(\overline{K})$ where the partial derivatives simultaneously vanish, then $E$ is called an *elliptic curve*. This condition makes the curve smooth.

For the purposes of this paper, $K$ will almost always be a finite field $\mathbb{F}_q$. We note that if the characteristic of $K$ is not 2 or 3, then by changing variables, we can write the equation of $E$ as

$$E : y^2 = x^3 + Ax + B, \text{ where } A, B \in K.$$

With this equation, the condition of smoothness becomes $4A^3 + 27B^2 \neq 0$. For elliptic curves defined over $\mathbb{Q}$, we use the following terminology. Let $y^2 = x^3+Ax+B$ be a *minimal model* for an elliptic curve $E$ defined over $\mathbb{Q}$. The term minimal model will be explained shortly. If $p$ is a prime such that $4A^3+27B^2 = 0$ in $\mathbb{F}_p$, then $p$ is known as a *bad prime* because the reduction of $E$ mod $p$ is not an elliptic curve. For a given curve $E$ defined over $\mathbb{Q}$, there are only a finite number of bad primes. A prime which isn't bad is called *good*. Throughout this paper, we will always assume that when we reduce a curve mod $p$ we exclude the bad primes.

Each element of $E(L)$ is called a *point*, and $E(L)$ can be made into an abelian group under a certain addition of points. We summarize how this is defined. For any $P, Q \in E(L)$,

i. $P + \infty = P = \infty + P$ (so $\infty$ is the identity element).

ii. $-\infty = \infty$, and for $P = (x, y) \neq \infty$, let $-P = (x, -y - a_1 x - a_3)$.

iii. $P + (-P) = \infty = (-P) + P$.

iv. For $P, Q \neq \infty$ and $Q \neq -P$, let $R$ be the third point of intersection (counting multiplicities) of the curve with the line $l = \overline{PQ}$ if $P \neq Q$, or with the tangent line to the curve at $P$ if $P = Q$. Then we set $P+Q = -R$.

This is visually depicted in Figure 1.

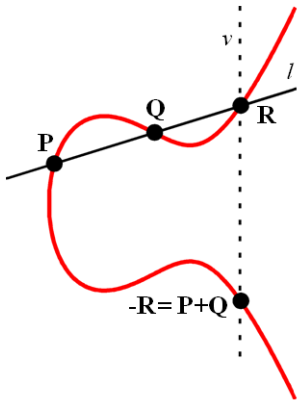


Figure 1: Addition of points on an elliptic curve

## 2.2 Elliptic curves over finite fields

Let $E$ be an elliptic curve defined over $\mathbb{F}_q$. The following facts are well-known. Since $\mathbb{F}_q$ is finite, it is clear that $E(\mathbb{F}_q)$ is a finite group. In fact, $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$ for some integers $n, n_1, n_2$ with $n_1 | n_2$.

If we know how many points are in $E(\mathbb{F}_q)$, then we can determine how many points there are over any extension of $\mathbb{F}_q$. Let $\#E(\mathbb{F}_q) = q + 1 - t$. The number $t$ is called the *trace* of $E$ over $\mathbb{F}_q$, and by Hasse's theorem, $|t| \leq 2\sqrt{q}$. If we write $X^2 - tX + q = (X - \alpha)(X - \overline{\alpha})$, then for all $k \geq 1$,

$$\#E(\mathbb{F}_{q^k}) = q^k + 1 - \alpha^k - \overline{\alpha}^k.$$

Note that $|\alpha| = \sqrt{q}$.

For odd $q$, if $E$ is given by $y^2 = x^3 + ax^2 + bx + c$, then the *twist of $E$ by $d$* is the curve $\tilde{E}$ given by $dy^2 = x^3 + ax^2 + bx + c$. It is easy to show that if $d$ is a square in $\mathbb{F}_q$, the number of points on $\tilde{E}$ is the same as on $E$, while if $d$ is not a square, then $\#\tilde{E}(\mathbb{F}_q) = q + 1 + t$. Similar notions and results hold when $q$ is a power of 2.

There is an important homomorphism we can define on $E(\mathbb{F}_q)$. Define the *Frobenius map* by

$$\phi_q : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$$
$$\phi_q(x, y) = (x^q, y^q).$$

The characteristic equation of $\phi_q$ is

$$\phi_q^2 - t\phi_q + q = 0,$$

meaning for any $P =\in E(\overline{\mathbb{F}}_q)$, we have

$$\phi_q^2(P) - [t]\phi_q(P) + [q]P = \infty.$$

The $t$ in this equation is the trace of $E$ over $\overline{\mathbb{F}}_q$, and is also the unique integer $a$ for which $\phi_q^2 - a\phi_q + q = 0$. $t$ is often referred to as the *trace of the Frobenius.*

The *j-invariant* of $E$ is an invariant which can be used to tell when two elliptic curves are isomorphic. If $E_1$ and $E_2$ are isomorphic over a field $K$, then $j(E_1) = j(E_2)$. If $K$ is algebraically closed, then the converse is also true. For curves given by the equation $E : y^2 = x^3 + Ax + B$, $j(E)$ can be calculated by

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

If we desire a curve with a given $j$-invariant, then we can use the curve

$$y^2 = x^3 + \frac{27j}{4(1728 - j)}x - \frac{27j}{4(1728 - j)},$$

which has $j$-invariant $j \neq 0, 1728$. If we desire a curve with $j$-invariant 0, we can use $y^2 = x^3 + B$ and any $B$. For $j$-invariant 1728, the curve $y^2 = x^3 + Ax$ will suffice with any $A$.

The *discriminant* of the curve $y^2 = x^3 + Ax + B$ is defined to be the discriminant of the polynomial $x^3 + Ax + B$, which is equal to $-16(4A^3 + 27B^2)$. Given an elliptic curve $E$ defined over the rationals, it is always possible (by changing variables) to find an equation for $E$ of the form $y^2 = x^3 + Ax + B$ with $A$ and $B$ in $\mathbb{Z}$, and the absolute value of the discriminant as small as possible. Such an equation is called a minimal model for $E$. The bad primes are exactly those primes which divide the minimal discriminant.

## 2.3 Torsion polynomials

For a given $n$, we now look at the points of order $n$ on an elliptic curve $E(\mathbb{F}_q)$. If $n$ and the characteristic of $\mathbb{F}_q$ are relatively prime, then

$$E[n] = \{P \in E(\overline{\mathbb{F}}_q) \mid [n]P = \infty\} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

$E[n]$ is the kernel of the multiplication-by-$n$ map, $[n] : E \to E$, where $[n](P) = [n]P$. Given a point $P = (x, y)$, we can derive explicit equations for the coordinates of $[n]P$ in terms of $x$ and $y$.

**Theorem 1** *Let $E$ be given by $y^2 = x^3 + Ax + B$, over a field whose characteristic is not 2. Then we can write*

$$[n]P = \left( \frac{\phi_n(x,y)}{\Phi_n^2(x,y)}, \frac{\omega_n(x,y)}{\Phi_n^3(x,y)} \right).$$

*The functions $\phi_n, \omega_n$, and $\Phi_n$ in $\mathbb{Z}[x,y]$ are defined recursively by*

$$\begin{aligned}
\Phi_0 &= 0 \\
\Phi_1 &= 1 \\
\Phi_2 &= 2y \\
\Phi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\Phi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
\Phi_{2n+1} &= \Phi_{n+2}\Phi_n^3 - \Phi_{n-1}\Phi_{n+1}^3 \text{ for } n \geq 2 \\
\Phi_{2n} &= \frac{\Phi_n}{2y}\left(\Phi_{n+2}\Phi_{n-1}^2 - \Phi_{n-2}\Phi_{n+1}^2\right) \text{ for } n \geq 2,
\end{aligned}$$

*and*

$$\begin{aligned}
\phi_n &= x\Phi_n^2 - \Phi_{n+1}\Phi_{n-1} \\
\omega_n &= \frac{1}{4y}\left(\Phi_{n+2}\Phi_{n-1}^2 - \Phi_{n-2}\Phi_{n+1}^2\right).
\end{aligned}$$

**Proof** These formulas are well-known. For example, see [67] for details. □

The polynomial $\Phi_n$ is called the *$n$-th torsion polynomial* of $E$. It can be shown that

$$\Phi_n(x,y) = \begin{cases} y(nx^{(n^2-4)/2} + ...) & \text{if } n \text{ is even,} \\ nx^{(n^2-1)/2} + ... & \text{if } n \text{ is odd.} \end{cases}$$

Notice that in both cases, we have $\Phi_n^2(x,y) = n^2x^{n^2-1} + ...$, is a function of $x$, since $y^2 = x^3 + Ax + B$.

Let

$$\Phi_n(x) = \Phi_n(x,1) = \begin{cases} \Phi_n(x,y)/y & \text{if } n \text{ is even,} \\ \Phi_n(x,y) & \text{if } n \text{ is odd.} \end{cases}$$

An immediate corollary is that a point $P = (x,y)$ is in $E[n]$ if and only if $\Phi_n(x) = 0$. We will use torsion polynomials in chapter 8 to prove the nondegeneracy of the Weil pairing.

## 2.4 Supersingular curves

Let $E$ be an elliptic curve defined over $\mathbb{F}_q$ where $q$ is a power of $p$. The curve $E$ is *supersingular* if $E$ satisfies one of three equivalent conditions (see [60]):

1. $\#E(\mathbb{F}_q) \equiv 1 \mod p$ or equivalently $\#E(\mathbb{F}_q) = q + 1 - t$ with $p|t$ ($t$ is the trace).

2. $E$ has no nontrivial points of order $p$ over $\overline{\mathbb{F}}_q$, i.e., $E[p] = \{\infty\}$.

3. The endomorphism ring of $E$ over $\overline{\mathbb{F}}_q$ is non-commutative, or more precisely, it is an order in a quaternion algebra.

For supersingular curves, if $E$ is defined over $\mathbb{F}_q$, where $q = p^f$, then it is known that $j(E) \in \mathbb{F}_{p^2}$. So every supersingular curve is isomorphic (over $\overline{\mathbb{F}}_p$) to one defined over $\mathbb{F}_{p^2}$.

If $E$ isn't supersingular, then $E$ is said to be *ordinary*. Supersingular curves can be classified according to their embedding degree $k$, which is at most 6 (see [19] or [44] for a proof). The *embedding degree of* $E$ is the smallest positive integer $k$ such that the order of every point of $E(\mathbb{F}_q)$ divides $q^k - 1$.

Table 1: Classification of supersingular curves by embedding degree (see [44])

| $k$ | Group structure of $E(\mathbb{F}_q)$ | Group structure of $E(\mathbb{F}_{q^k})$ | $t$ | $q$ |
|---|---|---|---|---|
| 1 | $(\mathbb{Z}/(\sqrt{q} \mp 1)\mathbb{Z})^2$ | $(\mathbb{Z}/(\sqrt{q} \mp 1)\mathbb{Z})^2$ | $\pm 2\sqrt{q}$ | $q = p^{2m}$ |
| 2 | $\mathbb{Z}/(q+1)\mathbb{Z}$ | $(\mathbb{Z}/(q+1)\mathbb{Z})^2$ | 0 | $q = p^{2m+1}$ |
| 2 | $\mathbb{Z}/(\frac{q+1}{2})\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ | $(\mathbb{Z}/(q+1)\mathbb{Z})^2$ | 0 | $q = p^{2m}, p \equiv 3 \bmod 4$ |
| 3 | $\mathbb{Z}/(q \mp \sqrt{q} + 1)\mathbb{Z}$ | $(\mathbb{Z}/(q^{\frac{3}{2}} \pm 1)\mathbb{Z})^2$ | $\pm\sqrt{q}$ | $q = p^{2m}$ |
| 4 | $\mathbb{Z}/(q \mp \sqrt{2q} + 1)\mathbb{Z}$ | $(\mathbb{Z}/(q^2+1)\mathbb{Z})^2$ | $\pm\sqrt{2q}$ | $q = 2^{2m+1}$ |
| 6 | $\mathbb{Z}/(q \mp \sqrt{3q} + 1)\mathbb{Z}$ | $(\mathbb{Z}/(q^3+1)\mathbb{Z})^2$ | $\pm\sqrt{3q}$ | $q = 3^{2m+1}$ |

# 3 Security

## 3.1 Hard problems

Public-key cryptosystems are based on one-way functions. In essence, a one-way function $f$ is one for which it is easy to compute $f(x)$ for a given input $x$, but given a $y$ in the image of $f$, it is hard to find an $x$ in the domain so that $f(x) = y$. One of the most important examples of a one-way function is the discrete logarithm problem (DLP). Let $G$ be a (multiplicatively written) cyclic group generated by $g$ of prime order $n$, i.e. $|G| = |\langle g \rangle| = n$. Given an integer $x < n$, it is relatively easy to compute $g^x$, but conversely given an element $y \in G$, it is sometimes difficult to determine $x$ such that $y = g^x$. The discrete log problem has been well-studied in groups such as finite fields and elliptic curves, and is believed to provide adequate security if parameters are carefully chosen.

A closely related problem is the Diffie-Hellman problem (DHP). Using the same group $G$ with generator $g$, the Diffie-Hellman problem asks one to determine $g^{xy}$ given $g, g^x$ and $g^y$. The decision Diffie-Hellman problem (DDHP) is: given $g$, $g^x$, and $g^y$, determine if another given element $h \in G$ is equal to $g^{xy}$. Clearly if you can solve the discrete log problem, then you can solve the

Diffie-Hellman problem, and if you can solve the Diffie-Hellman problem, you can solve the decision Diffie-Hellman problem.

Many of the protocols of elliptic curve cryptography use one of these problems, implemented in a prime order cyclic subgroup of the group of points on an elliptic curve.

Using bilinear pairings on elliptic curves, some related problems can be defined. Let $e : E(\mathbb{F}_q) \times E(\mathbb{F}_q) \to \mathbb{F}_{q^k}^*$ be a bilinear pairing. Bilinearity means that

$$e(P + R, Q) = e(P, Q)e(R, Q)$$

$$e(P, Q + R) = e(P, Q)e(P, R)$$

for all points $P, Q$ and $R$ on $E(\mathbb{F}_q)$. We also require $e$ to be nondegenerate, which means that for each point $P$, there is a point $Q$ such that $e(P, Q) \neq 1$ and similarly for each point $Q$ there is a point $P$ with $e(P, Q) \neq 1$. The bilinear Diffie-Hellman problem (BDHP) is: compute $e(P, P)^{abc}$, given $P, [a]P, [b]P$, and $[c]P$. If you can solve the DHP on the curve, you could find $[ab]P$, and compute $e([ab]P, [c]P) = e(P, P)^{abc}$, thus solving the bilinear Diffie-Hellman problem. Similarly, if we could solve the DHP in the finite field, we could apply the finite field DHP algorithm to $e(P, P), e([c]P, P)$, and $e([a]P, [b]P)$, which would solve the BDHP. We could also define the bilinear decision Diffie-Hellman problem (BDDHP), and similarly, solving the DDHP implies you can solve the bilinear decision Diffie-Hellman problem. The security of many pairing based protocols depend on the assumed hardness of these problems.

A problem $\mathcal{P}$ is said to reduce to another problem $\mathcal{Q}$, if given an algorithm that solves problem $\mathcal{Q}$ we can use it to efficiently solve problem $\mathcal{P}$. This means that problem $\mathcal{Q}$ is at least as hard as problem $\mathcal{P}$. So from what we said above, the BDHP reduces to the DHP, which reduces to the DLP. Similarly, the decision Diffie-Hellman and the bilinear Diffie-Hellman problems reduce to the DHP and BDHP respectively. If two problems reduce to each other, then the problems are said to be equivalent. Roughly speaking, this means that the two problems are equally hard.

We have a chain of reductions for the above problems, but could it be that some of these problems are equivalent? There is evidence that the Diffie-Hellman problem is actually equivalent to the discrete log problem (see [43]), and this has been proved in some cases (see [13]). But there is no strong evidence that any of the other problems are equivalent. For example, pairings can be used to show that on some curves, the DDHP is likely to be much easier than the DHP. We will show how this can be done in a later chapter.

We introduce one more problem which will be used in the proof of the main result in this paper. The *weak Diffie-Hellman problem* is the following. Given a cyclic group $\langle g \rangle$, we need to find another generator $h$ such that when presented with any $g^a$ and $g^b$ in $\langle g \rangle$, then we can compute $h^{ab}$. The generator $h$ should only depend on $g$, and not on $g^a$ or $g^b$. At first glance, this seems easier than the Diffie-Hellman problem, but the following lemma shows it is computationally equivalent to the Diffie-Hellman problem.

**Lemma 1** *If the weak Diffie-Hellman problem can be solved efficiently, then so can the Diffie-Hellman problem.*

**Proof** The following proof is from [66]. Let $\langle g \rangle$ be our cyclic group with generator $g$. Let $n$ be the order of $\langle g \rangle$. The order $n$ can be assumed to be prime, however the proof works for composite $n$, provided that we can factor $n$. Let $WDH$ be the function defined by $WDH(g^a, g^b) = h^{ab}$, for some generator $h$ which depends only on $g$. By hypothesis, $WDH$ can be efficiently computed.

We can write $h = g^s$, for some unknown $0 < s < n$. As $h$ is a generator, necessarily $(s, n) = 1$. We claim that we can efficiently find $g^{s^{\varphi(n)-3}}$. We're using $\varphi$ to denote the Euler-phi function. To see this, for any $i$ let

$$T(i) = (g^{s^{i-1}}, g^{s^i}).$$

Then $T(1) = (g, h)$, and

$$T(2i) = (g^{s^{2i-1}}, g^{s^{2i}}) = (h^{s^{2i-2}}, h^{s^{2i-1}}) = \left(WDH(g^{s^{i-1}}, g^{s^{i-1}}), WDH(g^{s^{i-1}}, g^{s^i})\right),$$

and

$$T(2i+1) = (g^{s^{2i}}, g^{s^{2i+1}}) = (h^{s^{2i-1}}, h^{s^{2i}}) = \left(WDH(g^{s^{i-1}}, g^{s^i}), WDH(g^{s^i}, g^{s^i})\right).$$

So given $i$, we can find $T(i)$ by repeated squarings and multiplications in $4 \log_2 i$ calls to the $WDH$ function. This means we can efficiently compute $T(\varphi(n)-3)$, and obtain $g^{s^{\varphi(n)-3}}$.

Now given $g^a$ and $g^b$, set

$$\begin{aligned} r = WDH\left(g^{s^{\varphi(n)-3}}, WDH(g^a, g^b)\right) &= WDH\left(g^{s^{\varphi(n)-3}}, h^{ab}\right) \\ &= WDH\left(g^{s^{\varphi(n)-3}}, g^{abs}\right) \\ &= h^{s^{\varphi(n)-3}abs} = h^{s^{\varphi(n)-2}ab} \\ &= (g^s)^{s^{\varphi(n)-2}ab} = g^{s^{\varphi(n)-1}ab} \\ &= g^{abs^{-1}}. \end{aligned}$$

The last equality follows by Euler's theorem, namely $s^{\varphi(n)} \equiv 1 \bmod n$ for any integer $s$ coprime to $n$.

Finally,

$$WDH(r, g) = WDH\left(g^{abs^{-1}}, g\right) = h^{abs^{-1}} = (g^s)^{abs^{-1}} = g^{ab}.$$

We have efficiently solved the Diffie-Hellman problem in $\langle g \rangle$.

□

# 4 Verheul's theorem

Recall that the embedding degree of $E$ is the smallest positive integer $k$ such that the order of every point of $E(\mathbb{F}_q)$ divides $q^k - 1$. We'll soon see that the Weil pairing reduces the DLP (or DHP) on an elliptic curve with embedding degree $k$ to the same problems in $\mathbb{F}^*_{q^k}$. To ensure confidence in the security of pairing based cryptography, we would like to be able to show that the DLP on low-embedding degree curves is equivalent to (and not easier than) the DLP in $\mathbb{F}^*_{q^k}$, since this problem has been studied far more extensively in finite fields.

This is done using the MOV embedding, by which we mean the map

$$\hat{e} : \langle P \rangle \to \mathbb{F}_{q^k} \quad \text{where} \quad \hat{e}(Q) = e(Q, S),$$

where $P$ and $S$ are fixed points of order $n$ on $E(\mathbb{F}_{q^k})$. So a straightforward way to try to prove equivalence would be to find a homomorphism that goes from the finite field to the curve, i.e. a homomorphism that inverts the MOV embedding. Such a homomorphism might be interpreted as evidence for the security of pairing based cryptosystems. However, Verheul proved the following in [66].

**Theorem 2** *Let $p$ be a prime $p \equiv 2 \mod 3$, and $n$ a prime number such that $n|(p^2 + p - 1)$. Let $g$ be a generator of $\mu_n$, the group of $n^{th}$ roots of unity in $\mathbb{F}^*_{p^6}$. Let $P$ be a point of order $n$ on a supersingular curve $E$ defined over $\mathbb{F}_{p^2}$ with $\#E(\mathbb{F}_{p^2}) = p^2 - p + 1$.*

*If an efficiently computable homomorphism can be found from $\mu_n$ to $\langle P \rangle$, then the Diffie-Hellman problem can be efficiently solved in both $\mu_n$ and $\langle P \rangle$.*

The group $\mu_n$ in the theorem is called an XTR group. In 2000, A. Lenstra and Verheul created the XTR public key system. It is based on a new way to represent elements of a subgroup of the multiplicative group of certain finite fields [39]. Its security relies on the DHP in the finite field. At the Crypto 2000 rump session [47] it was pointed out that if an efficiently computable homomorphism inverting the MOV embedding for XTR groups could be found, the XTR system would be equivalent to certain supersingular elliptic curve cryptosystems. It was posed as an open problem to construct such a map. Wanting to show this was not likely, Verheul proved the above result. He concluded that this "provides evidence that the multiplicative group of a finite field provides essentially more...security than the group of points of a supersingular elliptic curve of comparable size." It should be noted, however, that one should be cautious about concluding that the finite field problems are harder than the problems on the supersingular curve just because one particular approach to proving equivalence seems unlikely to succeed. Verheul's theorem does provide some evidence, but opinions differ about how strong this evidence is.

Verheul's result also has implications for pairing based cryptography. Many people would hesitate to have confidence in pairing based systems unless some rigorous security guarantees can be given. For example, some of the applications in chapter 7 depend on the hardness of the DHP on the curve. It would provide

confidence if it could be shown the DHP on the curve is no easier than the DHP in the corresponding finite field. A natural way to try to prove this would be to construct an inverse MOV map.

Verheul's theorem was specifically aimed at certain finite fields and supersingular curves, but we generalize his result in this paper to arbitrary finite fields and associated supersingular curves. Since the DHP in finite fields has been extensively studied, and is generally regarded to be intractable, the generalized version of Verheul's theorem implies that if an efficiently computable inverse MOV homomorphism could be found, systems relying on the hardness of the DHP in $\mathbb{F}_q$ or in the corresponding elliptic curve group would be insecure. This would include almost all pairing based cryptosystems. This includes, for example, Joux's three party key distribution scheme, Boneh and Franklin's identity based encryption system, and Boneh, Lynn, and Schachem's short signature scheme, all of which we will discuss in chapter 7.

We emphasize that the absence of a map which inverts the MOV embedding does not mean that the DLP in the finite field isn't equivalent to the same problem on the curve. Nor does it mean that one problem is necessarily harder than the other. It just means that a certain avenue for proving equivalence does not work. There could be other, less direct methods to show their equivalence.

We also remark that even if it is the case that two problems are unlikely to be provably equivalent, they could still be equivalent in practice. That is, it is still possible that in practice no one will ever find a way to solve one of them without solving the other. For example, it is unlikely that the DDHP in a finite field is provably as hard as the DLP in a finite field. Yet currently there seems to be no way to solve the DDHP in a finite field without solving the DLP. So in practice, there is no gap between the two problems.

In [34], Koblitz and Menezes suggested how Verheul's theorem could be generalized. Let $\mathbb{F}_q$ be an arbitrary finite field, and suppose that we have a trace zero elliptic curve $E$ over $\mathbb{F}_q$. A trace zero curve means that $t = 0$, i.e., $\#E(\mathbb{F}_q) = q + 1$. Suppose that $E$ has equation $y^2 = f(x)$ for odd $q$ and $y^2 + y = f(x)$ for $q$ a power of 2. Let $\beta \in \mathbb{F}_{q^2}$ be a nonsquare in $\mathbb{F}_{q^2}$ for odd $q$ and an element of absolute trace 1 for $q$ a power of 2 (that is, $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(\beta) = 1$). Let $\tilde{E}$ be the twisted curve over $\mathbb{F}_{q^2}$ with equation $\beta y^2 = f(x)$ for odd $q$ and $y^2 + y + \beta = f(x)$ for $q$ a power of 2.

We have $\#E(\mathbb{F}_q) = q + 1 = q + 1 - \alpha - \bar{\alpha}$, and so $\alpha$ is purely imaginary. As $|\alpha| = \sqrt{q}$, we have $\alpha = \sqrt{q} \cdot i$. So $\#E(\mathbb{F}_{q^2}) = q^2 + 1 - \alpha^2 - \bar{\alpha}^2 = q^2 + 1 + 2q$, and $\#\tilde{E}(\mathbb{F}_{q^2}) = q^2 + 1 - 2q$. Then (using the classification of supersingular curves given in chapter 2) $\tilde{E}(\mathbb{F}_{q^2})$ is a product of two cyclic groups of order $q - 1$, each of which is isomorphic to the multiplicative group of $\mathbb{F}_q$ under the MOV embedding. If the theorem can be generalized to these curves, then an efficiently computable construction of a homomorphism that inverts the MOV embedding would make the Diffie-Hellman problem easily solvable in all finite fields.

When $q = p^{2m}$ and $p \not\equiv 3 \mod 4$, there is no trace zero curve over $\mathbb{F}_q$. However, we will show we can still construct a supersingular curve $E$, such that

$E(\mathbb{F}_{q^2})$ is a product of two cyclic groups of order $q-1$.

We now state the main theorem of this paper. The proof will be given in chapter 10.

**Theorem 3** *Let $\mathbb{F}_q$ be an arbitrary finite field. Then there is an elliptic curve $E$ over $\mathbb{F}_q$ such that $\tilde{E}(\mathbb{F}_{q^2})$ is a product of two cyclic groups of order $q-1$.*

*Given such a curve, let $P$ be a generator for one of the cyclic subgroups of order $q-1$. Under the MOV embedding, we have an isomorphism from $\langle P\rangle$ to $\mathbb{F}_q^*$. If an efficiently computable isomorphism can be found from $\mathbb{F}_q^*$ to $\langle P\rangle$, then the Diffie-Hellman problem can be efficiently solved in both $\mathbb{F}_q^*$ and $\langle P\rangle$.*

We note that the problem of inverting pairings is an area of active interest. See, for example, the papers [21], [22], [30], [51], [52], [53], or [54].

# 5 Pairings

Given an elliptic curve $E$ over $\mathbb{F}_q$ and a positive integer $n$ not divisible by the characteristic $p$ of $\mathbb{F}_q$, let

$$E[n] = \left\{P \in E(\overline{\mathbb{F}}_q) : [n]P = \infty\right\},$$

be the set of points of $E$ of order $n$ over $\overline{\mathbb{F}}_q$. Let $\mu_n$ be the set of $n^{\text{th}}$ roots of unity in $\overline{\mathbb{F}}_q$, $\mu_n = \{\zeta : \zeta^n = 1\} \subseteq \overline{\mathbb{F}}_q$. A *pairing* is a function

$$e : E[n] \times E[n] \to \mu_n.$$

We will be interested in pairings which are *bilinear* and *nondegenerate*. Bilinearity means for all $P, P_1, P_2, Q, Q_1$, and $Q_2$ in $E[n]$, we have

$$e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q) \text{ and } e(P, Q_1 + Q_2) = e(P, Q_1)e(P, Q_2).$$

Nondegeneracy means for all $P \neq \infty$ in $E[n]$, there is a $Q \in E[n]$ such that $e(P, Q) \neq 1$, and similarly, for all $Q \neq \infty$ in $E[n]$, there is a $P \in E[n]$ such that $e(P, Q) \neq 1$.

Some basic properties of pairings include the following:

**Lemma 2** *Let $e$ be a bilinear, nondegenerate pairing. Then for all $P, Q \in E[n]$, and any $a, b \in \mathbb{Z}$,*

1. $e(P, \infty) = e(\infty, Q) = 1$
2. $e(-P, Q) = e(P, -Q) = e(P, Q)^{-1}$
3. $e([a]P, Q) = e(P, Q)^a = e(P, [a]Q)$
4. $e([a]P, [b]Q) = e(P, Q)^{ab}$

**Proof** Everything easily follows from the bilinear property. □

The two most common pairings used, the Tate and Weil pairings, are bilinear and nondegenerate. Both pairings can also be efficiently computed. Before we can define them, we need to review the theory of divisors.

## 5.1 Divisors

All of the results given in this chapter are standard facts about divisors, and so we omit most proofs. Proofs can be found in [26] or [18]. Let $E$ be an elliptic curve defined over a field $K$. A divisor $D$ on $E$ is a formal sum

$$D = \sum_j c_j[P_j]$$

where each $P_j \in E(\overline{K})$ and $c_j \in \mathbb{Z}$, with only finitely many of the $c_j$ nonzero. We sometimes write alternatively

$$D = \sum_P c_P[P].$$

The *support* of $D$ is the set of all points $P_j$ where $c_j \neq 0$. The set of all divisors on $E$ is called $\mathrm{div}(E)$. It is an abelian group under addition with

$$\left(\sum_P c_P[P]\right) + \left(\sum_P d_P[P]\right) = \sum_P (c_P + d_P)[P]$$

We define the *degree* and *sum* of a divisor $D$ as follows:

$$\deg(D) = \deg\left(\sum_j c_j[P_j]\right) = \sum_j c_j \in \mathbb{Z}$$

$$\mathrm{sum}(D) = \mathrm{sum}\left(\sum_j c_j[P_j]\right) = \sum_j [c_j]P_j \in E(\overline{K}).$$

We also will define the divisor of a function on $E$. By a function on $E$, we mean a nonzero $f(x,y) \in \overline{K}(x,y)$. It is possible for functions to have more than one representation on a given curve. For example, if $E : y^2 = x^3 + x$, then on $E$ the function $f(x,y) = \frac{y}{x}$ could also be written as $g(x,y) = \frac{x^2+1}{y}$. It might seem that this could lead to confusion in evaluating $f(P)$, particularly when the numerator or denominator evaluates to 0. The following theorem ([18]) clarifies this.

**Theorem 4** *Given a point $P$ on an elliptic curve $E$, there is a function $U_P$ (called a* uniformizing parameter *for $P$) such that for any function $f$ on $E$, there is an integer $r$ and a function $g$ on $E$ such that*

$$f = U_P^r g,$$

*where $U_P(P) = 0$, and $g(P) \neq 0, \infty$. The number $r$ doesn't depend on the choice of $U_P$.*

For a given $P$, there are three possibilities for $f(P) = U_P^r g$. If $r = 0$, then $f(P) = g(P)$. If $r > 0$, then $f(P) = 0$, and $f$ has a zero at $P$ of order $r$. If $r < 0$, then $f$ has a pole of order $r$ at $P$. In all cases, define the *order of $f$ at $P$* to be the value of $r$, written $\mathrm{ord}_P(f) = r$. Then the divisor of $f$ is

$$\mathrm{div}(f) = \sum_{P \in E(\overline{K})} \mathrm{ord}_P(f)[P].$$

The sum in the definition of $\mathrm{div}(f)$ is actually a finite sum [18].

**Theorem 5** *Let $f$ be a function on $E$. Then*

1. *$f$ has only finitely many zeroes and poles.*
2. *The degree of div($f$) is 0.*
3. *If div($f$)=0, i.e., if $f$ has no zeroes or poles, then $f$ is constant.*

Given a function $f$ on $E$ and a divisor $D$, we can define $f(D)$ as follows. If $D = \sum_j c_j[P_j]$, then let

$$f(D) = \prod_j f(P_j)^{c_j}.$$

We will need a few more results about divisors before being able to define the Tate and Weil pairings.

**Lemma 3** *If $f$ and $g$ are two functions on $E$, then*

$$div(f) + div(g) = div\ (fg),$$

*and*

$$div(f) - div(g) = div\left(\frac{f}{g}\right).$$

A divisor $D$ is said to be *defined over* $\mathbb{F}_{q^k}$, when the $q^k$-th Frobenius map permutes the points in the support of $D$ so as not to change the formal expression of $D$.

**Theorem 6** *Let $D$ be a divisor of degree 0 on an elliptic curve $E$. There is a function $f$ on $E$ with div($f$)=$D$ if and only if sum($D$)=$\infty$. Furthermore, if sum($D$)=$\infty$ then we can choose $f$ so that it is defined over $\mathbb{F}_{q^k}$ when $D$ is defined over $\mathbb{F}_{q^k}$.*

**Proof** Following ([67]), we prove this theorem in one direction. For the other direction, see [18] or [26]. This part of the proof is worth giving in detail because the method can be used in computing pairings.

Suppose that sum($D$)=$\infty$ and deg($D$)=0. Let $P_1$ and $P_2$ be two points on $E$, with the equation of the line $l$ passing through them being $ax + by + c = 0$. By the way addition is defined on the curve, this line intersects the curve in a

third point, which is $-(P_1 + P_2)$. These are the only zeroes of the line on $E$. If $b \neq 0$, then the line also has a triple pole at $\infty$. Thus,

$$\text{div}(ax + by + c) = [P_1] + [P_2] + [-(P_1 + P_2)] - 3[\infty].$$

Also note that if $P_1 + P_2 = (x_3, y_3)$

$$\text{div}(x - x_3) = [P_1 + P_2] + [-(P_1 + P_2)] - 2[\infty].$$

We see that

$$\text{div}\left(\frac{ax + by + c}{x - x_3}\right) = [P_1] + [P_2] - [P_1 + P_2] - [\infty],$$

or

$$[P_1] + [P_2] = [P_1 + P_2] + [\infty] + \text{div}\left(\frac{ax + by + c}{x - x_3}\right).$$

Now

$$\text{sum}\left(\text{div}\left(\frac{ax + by + c}{x - x_3}\right)\right) = \text{sum}([P_1] + [P_2] - [P_1 + P_2] - [\infty]) = \infty.$$

In the special case when $P_1 + P_2 = \infty$, it is easy to see $[P_1] + [P_2] = 2[\infty] + \text{div}(x - x_0)$, where $x_0$ is the $x$-coordinate of $P_1$ and $P_2$.

In both cases, we see that we can replace $[P_1]+[P_2]$ by $[P_1+P_2]+[\infty]+\text{div}(g)$, for some function $g$ on $E$. So we can replace all the terms in $D$ with positive coefficients by $[P] + n_1[\infty] + \text{div}(g_1)$, for some point $P$ on $E$, some integer $n_1$, and some function $g_1$ on $E$. Likewise, for all the terms with negative coefficient we can replace them with $-[Q] - n_2[\infty] - \text{div}(g_2)$ for some $Q \in E(\overline{K}), n_2 \in \mathbb{Z}$, and function $g_2$ on $E$. Thus,

$$D = [P] - [Q] + n[\infty] + \text{div}(\frac{g_1}{g_2}).$$

Notice that both $g_1$ and $g_2$ are products of functions $g$ which satisfy $\text{sum}(\text{div}(g))=\infty$. We conclude that $\text{sum}(\text{div}(\frac{g_1}{g_2})) = \infty$. By Theorem 5.3, $0=\deg(\text{div}\left(\frac{g_1}{g_2}\right))$, so $0=\deg(D)=1\text{-}1+n$, so $n = 0$ and

$$D = [P] - [Q] + \text{div}\left(\frac{g_1}{g_2}\right).$$

Then as we're assuming $\text{sum}(D)=\infty$, we have

$$\infty = \text{sum}(D) = P - Q + \text{sum}(\text{div}\left(\frac{g_1}{g_2}\right)) = P - Q,$$

so $P = Q$, and $D$ is the divisor of a function $f$.

To see that we can choose $f$ to be defined over $\mathbb{F}_{q^k}$, note the following. A priori, $f$ is only defined over $\overline{\mathbb{F}}_{q^k}$. Let $\sigma$ be an element of the Galois group $G$

of $\overline{\mathbb{F}}_{q^k}/\mathbb{F}_{q^k}$. Then notice that $\sigma(D) = D$. So $f^\sigma$ (meaning $f$ with $\sigma$ applied to the coefficients) has the same divisor $D$, so $f^\sigma/f$ is a constant. Using Galois cohomology, the map $\sigma \to c_\sigma$ is a cocycle in $H^1(G, \overline{\mathbb{F}}^*_{q^k})$ which by Hilbert's theorem 90 is trivial. So there is a constant $c_1 \in \overline{\mathbb{F}}^*_{q^k}$ such that $c_\sigma = c_1^\sigma/c_1$ for all $\sigma \in G$. Then $f/c_1$ is fixed by all $\sigma$, so is defined over $\mathbb{F}_{q^k}$. Replacing $f$ by this, we can assume $f$ is defined over $\mathbb{F}_{q^k}$. □

We point out that the technique used in the proof shows us how to explicitly find a function $f$ such that div($f$)=$D$ when given a degree 0 divisor $D$ with sum $\infty$.

## 5.2 Weil pairing

We now define the Weil pairing and prove that it is a bilinear pairing. We'll also prove some additional properties the Weil pairing satisfies.

Let $n$ be an integer relatively prime to the characteristic of our field $K$. Let $Q$ be a point of order $n$ on $E$. Consider the divisor $D_1 = n[Q] - n[\infty]$. It has degree 0, and its sum is $\infty$. So by the results of the previous section, there is a function $f$ on $E$ with div($f$)=$n[Q] - n[\infty]$. Now find a point $Q' \in E[n^2]$ with $[n]Q' = Q$. Consider a second divisor,

$$D_2 = \sum_{R \in E[n]} \left([Q' + R] - [R]\right).$$

Then

$$\text{sum}(D_2) = \sum_{R \in E[n]} Q' = [n^2]Q' = [n]Q = \infty.$$

So as $D_2$ also has degree 0 and sums to $\infty$, there is a function $g$ on $E$ with div($g$)=$D_2$.

Since $D_2$ can also be written as

$$D_2 = \sum_{[n]Q''=Q} [Q''] - \sum_{R \in E[n]} [R],$$

we see that $D_2$ and hence $g$ do not depend on the choice of $Q'$.

We define the Weil pairing by

$$e_n : E[n] \times E[n] \to \mu_n$$

$$e_n(P, Q) = \frac{g(P + S)}{g(S)},$$

where $S$ is any point of $E(\overline{K})$ such that $g(P + S)$ and $g(S)$ are both defined and nonzero.

We must show this definition makes sense. Note that although $g$ is only determined up to a constant multiple, $e_n$ is independent of the choice of $g$. Recall that div($f$) = $n[Q] - n[\infty]$. Let $f \circ n : E \to \overline{K}$ be defined by

$$(f \circ n)(S) = f([n]S).$$

The zeroes of $f \circ n$ are the points $S$ such that $[n]S = Q$, so they are the points $Q' + R$, where $R \in E[n]$. Likewise the poles of $f \circ n$ are the points $P$ with $[n]P = \infty$, so they are just the set $E[n]$. Thus

$$\operatorname{div}(f \circ n) = n \sum_{R \in E[n]} [Q' + R] - n \sum_{R \in E[n]} [R].$$

But this is clearly equal to $\operatorname{div}(g^n)$. So

$$0 = \operatorname{div}(f \circ n) - \operatorname{div}(g^n) = \operatorname{div}\left(\frac{f \circ n}{g^n}\right),$$

so $\frac{f \circ n}{g^n}$ is constant. Multiplying $f \circ n$ by a constant doesn't change its divisor, so we can assume that $f$ is chosen so that $f \circ n = g^n$.

Then for $P \in E[n]$ and any $S$ on $E(\overline{K})$, we see that

$$g(P+S)^n = (f \circ n)(P+S) = f\left([n](P+S)\right) = f([n]S) = (f \circ n)(S) = g(S)^n.$$

So $\frac{g(P+S)}{g(S)}$ is an $n$-th root of unity, assuming both are nonzero.

For a fixed $P$, the map $\frac{g(P+S)}{g(S)}$ is a continuous map on $E(\overline{K})$ under the Zariski topology. Recall the Zariski topology has as closed sets the sets of points which are the zeroes of a polynomial. A map is continuous under this topology if the inverse image of a closed set is closed. Since $E$ is connected, the image of the map $\frac{g(P+S)}{g(S)}$ must also be connected. As $\mu_n$ is a finite discrete set, the map must actually be constant. This shows the definition of $e_n$ is independent of the choice of $S$, and so $e_n$ is well-defined.

**Theorem 7** *The Weil pairing $e_n$ satisfies the following properties:*

1. *$e_n$ is bilinear, i.e.*

   $$e_n(P_1 + P_2, Q) = e_n(P_1, Q)e_n(P_2, Q)$$

   *and*

   $$e_n(P, Q_1 + Q_2) = e_n(P, Q_1)e_n(P, Q_2).$$

2. *$e_n(P, P) = 1$*

3. *$e_n(P, Q) = e_n(Q, P)^{-1}$*

4. *$e_n$ is nondegenerate, i.e. if $e_n(P, Q) = 1$ for all $Q \in E[n]$ then $P = \infty$ and if $e_n(P, Q) = 1$ for all $P \in E[n]$ then $Q = \infty$.*

5. *$e_n$ is Galois invariant, i.e. if $\sigma$ is an automorphism of $\overline{K}$ that restricts to the identity on $K$, then*

   $$e_n(\sigma(P), \sigma(Q)) = \sigma(e_n(P, Q)).$$

   *Here we are using the notation that if $P = (x, y)$, then $\sigma(P) = (\sigma(x), \sigma(y))$.*

6. *If $P \in E[nn']$ and $Q \in E[n]$ then*

$$e_{nn'}(P,Q) = e_n([n']P, Q).$$

7. *If $E$ is considered over an extension field, the value of $e_n(P,Q)$ remains unchanged.*

**Proof** The following are standard arguments. See [67] or [60] for example. (1) Choose $S$ so that $g(P_1 + P_2 + S), g(P_2 + S)$, and $g(S)$ are all defined and nonzero. Then we have

$$\begin{aligned} e_n(P_1 + P_2, Q) &= \frac{g(P_1 + P_2 + S)}{g(S)} \\ &= \frac{g(P_1 + (P_2 + S))}{g(P_2 + S)} \frac{g(P_2 + S)}{g(S)} \\ &= e_n(P_1, Q) e_n(P_2, Q), \end{aligned}$$

since the definition of $e_n$ is independent of the choice of $S$. We have to work a little harder for linearity in the second variable. Let $Q_3 = Q_1 + Q_2$. In our definition of the Weil pairing above, given a point $Q$, we used functions $f$ and $g$. Let $f_i$ and $g_i$ be the corresponding functions for $Q_i$ for $i = 1, 2, 3$. Now the divisor $[Q_3] - [Q_1] - [Q_2] + [\infty]$ has degree 0 and sum $\infty$, so by Theorem 6, there is a function $h$ on $E$ with

$$\operatorname{div}(h) = [Q_3] - [Q_1] - [Q_2] + [\infty].$$

Now as $\operatorname{div}(f_i) = n[Q_i] - n[\infty]$, we have

$$\begin{aligned} \operatorname{div}\left(\frac{f_3}{f_1 f_2}\right) &= \operatorname{div}(f_3) - \operatorname{div}(f_1) - \operatorname{div}(f_2) \\ &= (n[Q_3] - n[\infty]) - (n[Q_1] - n[\infty]) - (n[Q_2] - n[\infty]) \\ &= n[Q_3] - n[Q_1] - n[Q_2] + n[\infty] \\ &= n \operatorname{div}(h) \\ &= \operatorname{div}(h^n). \end{aligned}$$

Thus $h^n$ is a constant multiple of $\frac{f_3}{f_1 f_2}$, and so there exists a $c$ such that $f_3 = c f_1 f_2 h^n$. By our choice of the $f_i$ and $g_i$, we have $f_i \circ n = g_i^n$. Substituting this in,

$$g_3^n = c g_1^n g_2^n (h \circ n)^n,$$

or

$$g_3 = c' g_1 g_2 (h \circ n).$$

From the definition

$$\begin{aligned} e_n(P, Q_1 + Q_2) = \frac{g_3(P + S)}{g_3(S)} &= \frac{g_1(P + S)}{g_1(S)} \frac{g_2(P + S)}{g_2(S)} \frac{h([n](P + S))}{h([n]S)} \\ &= e_n(P, Q_1) e_n(P, Q_2), \end{aligned}$$

as $[n]P = \infty$ so the last term is just $\frac{h([n]S)}{h([n]S)} = 1$. The point $S$ is chosen so that none of the above terms is 0 or $\infty$.

(2) We want to evaluate $e_n(P, P)$. Let $\tau_P$ be the map from $E$ to $E$ defined by translation by $P$:

$$\tau_P(R) = R + P.$$

The zeroes of the function $f \circ \tau_{[j]P}$ are the zeroes of $f$ translated by $-[j]P$, and similarly for the poles. So

$$\operatorname{div}(f \circ \tau_{[j]P}) = n[P - [j]P] - n[-[j]P].$$

Thus

$$\operatorname{div}\left(\prod_{j=0}^{n-1} f \circ \tau_{[j]P}\right) = n\sum_{j=0}^{n-1}([[1-j]P] - [-[j]P]).$$

Since $P \in E[n]$, both $\sum_{j=0}^{n-1}[[1-j]P]$ and $\sum_{j=0}^{n-1}[-[j]P]$ are equal to $\sum_{j=0}^{n-1}[[j]Q]$, so the last displayed sum equals 0. This implies that $\prod_{j=0}^{n-1}(f \circ \tau_{[j]Q})$ is constant. If $P'$ is a point such that $[n]P' = P$, then

$$\prod_{j=0}^{n-1} f \circ \tau_{[j]P} = \prod_{j=0}^{n-1} f \circ n \circ \tau_{[j]P'} = \left(\prod_{j=0}^{n-1} g \circ \tau_{[j]P'}\right)^n.$$

It follows that $\prod_{j=0}^{n-1} g \circ \tau_{[j]P'}$ is constant (again using the connectedness of $E$ in the Zariski topology). If we now evaluate this product at any point $S$ and at $S + P'$, then

$$\prod_{j=0}^{n-1} g \circ \tau_{[j]P'}(S) = \prod_{j=0}^{n-1} g \circ \tau_{[j]P'}(S + P'),$$

and so

$$\prod_{j=0}^{n-1} g(S + [j]P') = \prod_{j=0}^{n-1} g(S + [j+1]P').$$

Cancelling the common terms, we have

$$g(S) = g(S + [n]P') = g(S + P)$$

which means

$$e_n(P, P) = \frac{g(P+S)}{g(S)} = 1.$$

(3) easily follows from (1) and (2) using the calculation

$$\begin{aligned} 1 = e_n(P+Q, P+Q) &= e_n(P, P+Q)e_n(Q, P+Q) \\ &= e_n(P, P)e_n(P, Q)e_n(Q, P)e_n(Q, Q) = e_n(P, Q)e_n(Q, P). \end{aligned}$$

(4) Suppose that $e_n(P, Q) = 1$ for all $P \in E[n]$. Then $\frac{g(P+S)}{g(S)} = 1$ for all $P$ and we claim there is a function $h$ on $E$ with $g = h \circ n$. This is proved in

Lemma 4 at the end of this section. So $(h \circ n)^n = g^n = f \circ n$, and since the multiplication by $n$ map is surjective on $E(\overline{K})$, $f = h^n$. Thus

$$n \operatorname{div}(h) = \operatorname{div}(h^n) = \operatorname{div}(f) = n[Q] - n[\infty],$$

and hence $\operatorname{div}(h) = [Q] - [\infty]$. By Theorem 5.3, $Q = \infty$. Now suppose that $e_n(P, Q) = 1$ for all $Q \in E[n]$. Then $e_n(Q, P) = 1$ for all $Q$ and by the nondegeneracy in the second variable which we just showed, we must have $P = \infty$.

(5) Let $\sigma$ be an automorphism of $\overline{K}$ which is trivial on $K$. Let $\sigma(P) = (\sigma(x), \sigma(y)$ for $P = (x, y)$. Let $f^\sigma$ and $g^\sigma$ be the maps corresponding to $f$ and $g$ in the definition of the pairing of $e_n(\sigma(P), \sigma(Q))$. Note these are the same functions obtained by applying $\sigma$ to the coefficients of $f$ and $g$. Then

$$e_n(\sigma(P), \sigma(Q)) = \frac{g^\sigma(\sigma(P) + \sigma(S))}{g^\sigma(\sigma(S))} = \sigma\left(\frac{g(P+S)}{g(S)}\right) = \sigma(e_n(P, Q)).$$

(6) With $f$ and $g$ from the definition of the pairing, we have

$$\operatorname{div}(f^{n'}) = nn'[Q] - nn'[\infty],$$

and

$$(g \circ n')^n = (f \circ nn').$$

Thus

$$(g \circ n')^{nn'} = (f \circ nn')^{n'} = f^{n'} \circ nn'.$$

So we can use $f^{n'}$ and $g \circ n'$ in place of $f$ and $g$ in the definition of $e_{nn'}$. Then

$$e_{nn'}(P, Q) = \frac{(g \circ n')(S + P)}{(g \circ n')(S)} = \frac{g([n']S + [n']P)}{g([n']S)} = e_n([n']P, Q).$$

(7) In the definition of $e_n$, no reference was made to the field of definition of $E$. Everything was defined over $E(\overline{K})$.

□

Using the above properties of the Weil pairing, we have the following easy corollaries.

**Corollary 1** *There exist points $P, Q \in E[n]$ such that $e_n(P, Q)$ is a primitive $n$-th root of unity. In particular, if $\{P, Q\}$ is a basis for $E[n]$, then $e_n(P, Q)$ is a primitive $n$-th root of unity.*

**Proof** As $P$ and $Q$ vary over $E[n]$, the image of $e_n(P, Q)$ is a subgroup $\mu_d$ of $\mu_n$. Then by bilinearity,

$$1 = e_n(P, Q)^d = e_n([d]P, Q),$$

for all $P, Q \in E[n]$. By the nondegeneracy of the pairing, we must have $[d]P = \infty$ for all $P \in E[n]$. As $P$ was arbitrary, and $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$, it must be that $d = n$.

If $\{P, Q\}$ is a basis for $E[n]$, set $e_n(P, Q) = \zeta$, with $\zeta^d = 1$. The bilinearity of $e_n$ implies that $\zeta$ generates the whole image of $e_n$, which we just showed is $\mu_n$. Thus $d = n$ and $e_n(P, Q)$ is a primitive $n$-th root of unity. □

**Corollary 2** *If $E[n] \subset E(K)$, then $\mu_n \in K^*$.*

**Proof** Let $\sigma$ be any automorphism of $\overline{K}$ which is the identity on $K$. Then by the galois invariance property of the Weil pairing,

$$\sigma(e_n(P, Q)) = e_n(\sigma(P), \sigma(Q)) = e_n(P, Q)$$

for any $P, Q \in E[n]$. So we see that $e_n(P, Q) \in K^*$ for any $P, Q$. □

One consequence of this last corollary is that if $E$ is an elliptic curve defined over $\mathbb{Q}$, then for $n \geq 3$, $E[n] \not\subset E(\mathbb{Q})$.

**Lemma 4** *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over a field $K$. Suppose $g$ is a function on $E$ such that $g(P + S) = g(P)$ for all $P \in E(\overline{K})$ and all $S \in E[n]$, where $n \geq 1$ is not divisible by the characteristic of $K$. Then there is a function $h$ on $E$ satisfying $g(P) = h([n]P)$ for all $P$.*

**Proof** We follow the proof from [67]. The lemma is clearly true if $n = 1$, so we can assume $n > 1$. Given a point $S \in E[n]$, there are rational functions $T(x, y), U(x, y)$ (depending on $S$) so that

$$(x, y) + S = (T(x, y), U(x, y))$$

on $E$. Regard $\overline{K}(x, y)$ as the quadratic extension of $\overline{K}(x)$ obtained by adjoining the element $\sqrt{x^3 + Ax + B}$.

We define a map

$$\sigma_S : \overline{K}(x, y) \to \overline{K}(x, y)$$

$$\sigma_S(g(x, y)) = g(T(x, y), U(x, y)).$$

This makes sense as $(T, U)$ is on $E$. The map is easily seen to be a homomorphism. In fact, the inverse of $\sigma_S$ is $\sigma_{-S}$, so the map is actually an automorphism. We also note that because $(x, y) + S \neq (x, y) + S'$ unless $S = S'$, if $S \neq S'$ then $\sigma_S \neq \sigma_{S'}$.

Thus we have a group $G$ of $n^2$ automorphisms of $\overline{K}(x, y)$ as $S$ runs through $E[n]$. Let $F$ be the fixed field of $\overline{K}(x, y)$ corresponding to $G$. Note that if a function $g$ is fixed by one of these automorphisms, then $g(P + S) = g(S)$ for all $P$. So $F$ is actually the field of functions that satisfy the conditions of the lemma. It follows by basic Galois theory that

$$[\overline{K}(x, y) : F] = n^2.$$

Recall from Section 2.3, that there are rational functions $\phi_n(x), \Phi_n(x,y)$, and $\omega_n(x,y)$ such that

$$[n](x,y) = \left(\frac{\phi_n(x)}{\Phi_n^2(x)}, \frac{\omega_n(x,y)}{\Phi_n^3(x,y)}\right).$$

Notice that $\overline{K}\left(\frac{\phi_n(x)}{\Phi_n^2(x)}, \frac{\omega_n(x,y)}{\Phi_n^3(x,y)}\right) \subseteq F$, and moreover

$$\left[\overline{K}\left(\frac{\phi_n(x)}{\Phi_n^2(x)}, \frac{\omega_n(x,y)}{\Phi_n^3(x,y)}\right) : \overline{K}\left(\frac{\phi_n(x)}{\Phi_n^2(x)}\right)\right] \geq 2,$$

because $\frac{\omega_n(x,y)}{\Phi_n^3(x,y)} \notin \overline{K}\left(\frac{\phi_n(x)}{\Phi_n^2(x)}\right)$ as $\frac{\omega_n(x,y)}{\Phi_n^3(x,y)} = yH(x)$ for some function $H$. This implies

$$\left[\overline{K}(x,y) : \overline{K}\left(\frac{\phi_n(x)}{\Phi_n^2(x)}\right)\right] \geq 2n^2.$$

We now show we actually have equality. Let

$$P(X) = \phi_n(X) - \frac{\phi_n(x)}{\Phi_n^2(x)}\Phi_n^2(X)$$

which has $X = x$ as a root. The polynomial $\phi_n(X) = X^{n^2} + ...$, and $\Phi_n^2(X)$ has degree $n^2 - 1$, so $P(X) = X^{n^2-1} + ....$ It follows that $x$ is of degree at most $n^2$ over $\overline{K}\left(\frac{\phi_n(x)}{\Phi_n^2(x)}\right)$. As $[\overline{K}(x,y) : \overline{K}(x)] = 2$, then

$$\left[\overline{K}(x,y) : \overline{K}\left(\frac{\phi_n(x)}{\Phi_n^2(x)}\right)\right] \leq 2n^2.$$

As we have equality, then we must actually have

$$F = \overline{K}\left(\frac{\phi_n(x)}{\Phi_n^2(x)}, \frac{\omega_n(x,y)}{\Phi_n^3(x,y)}\right).$$

The functions in $F$ are those functions $g$ such that $g(P+S) = g(P)$, for all $P \in E(\overline{K})$ and $S \in E[n]$. The functions on the right are of the form $h([n]P)$, so this proves the lemma. □

## 5.3 The Tate pairing

The Tate pairing is also defined using divisors. Let $P \in E[n]$, so $P \in E(\mathbb{F}_{q^k})$ where $k$ is the embedding degree, the smallest positive integer such that $n|(q^k - 1)$. There is a function $f$ on $E$ such that

$$\text{div}(f) = n[P] - n[\infty].$$

Given another point $Q$ in $E[n]$, choose a point $R \in E[n]$ such that $R \notin \{\infty, P, -Q, P-Q\}$ so neither $R$ nor $Q+R$ is a pole or zero of $f$. Then we define

$$\tau_n(P,Q) = \left(\frac{f(Q+R)}{f(R)}\right)^{(q^k-1)/n}.$$

We need to verify that $\tau_n(P,Q)$ is an $n$-th root of unity, and that $\tau_n(P,Q)$ doesn't depend on the choice of $f$ or $R$.

If $f_1$ is another function on $E$ with divisor $n[P] - n[\infty]$, then by Theorem we must have $f_1 = cf$, for some constant $c$. Then

$$\frac{f_1(Q+R)}{f_1(R)} = \frac{cf(Q+R)}{cf(R)} = \frac{f(Q+R)}{f(R)},$$

so the value $\tau_n(P,Q)$ is independent of the choice of $f$.

Now let $S$ be another point of $E(\mathbb{F}_{q^k})[n]$, with $S \notin \{\infty, P, -Q, P-Q\}$. Note that the divisor $D = [Q+S] - [S] - [Q+R] + [R]$ has degree 0 and sum $\infty$, so there is a function $h$ on $E$ such that $\mathrm{div}(h) = D$. Then

$$\frac{f(Q+S)}{f(S)} = \frac{f(Q+R)}{f(R)}\frac{f(Q+S)f(R)}{f(S)f(Q+R)} = \frac{f(Q+R)}{f(R)}f(\mathrm{div}(h)).$$

We now need the Weil reciprocity theorem:

**Theorem 8** *Let $f$ and $h$ be two functions on $E$ with disjoint support. Then*

$$f(div(h)) = h(div(f)).$$

For a proof see [19]. Using this,

$$\frac{f(Q+S)}{f(S)} = \frac{f(Q+R)}{f(R)}h(\mathrm{div}(f)) = \frac{f(Q+R)}{f(R)}\left(\frac{h(P)}{h(\infty)}\right)^n.$$

By our choice of $R$ and $S$, neither $P$ nor $\infty$ is a zero or pole of $h$. If we raise both sides to the $(q^k-1)/n$ power, then the term with $h$ becomes 1.

Thus

$$\left(\frac{f(Q+S)}{f(S)}\right)^{(q^k-1)/n} = \left(\frac{f(Q+R)}{f(R)}\right)^{(q^k-1)/n},$$

and so $\tau_n(P,Q)$ doesn't depend on the choice of $R$.

By Theorem 6, we can take $f$ to be defined over $\mathbb{F}_{q^k}$. So the value $f(Q+R)/f(R)$ is in $\mathbb{F}_{q^k}^*$, hence so is $\tau_n(P,Q)$. Also, $\tau_n(P,Q)^n = \left(\frac{f(Q+R)}{f(R)}\right)^{q^k-1} = 1$, and we've shown $\tau_n(P,Q) \in \mu_n$.

Note that what we are calling the Tate pairing is a modified version of what is generally referred to as the Tate pairing. The image of a pair of points under the unmodified Tate pairing is a coset, rather than an element of $\mathbb{F}_{q^k}^*$. The modification we make is raising to the $(q^k-1)/n$-th power, which we do to simplify things as well as to make $\tau_n$ have the desired properties below.

**Theorem 9** *The Tate pairing*

$$\tau_n : E[n] \times E[n] \to \mu_n$$

*satisfies the following properties:*

1. *$\tau_n$ is bilinear*
2. *$\tau_n$ is nondegenerate*
3. *$\tau_n$ is Galois invariant*
4. *If $n|N$ and $N|(q^k - 1)$, then $\tau_N = \tau_n$*

**Proof** (1) Let $P_1, P_2 \in E[n]$. Then

$$D = ([P_1] - [\infty]) + ([P_2] - [\infty]) - ([P_1 + P_2] - [\infty])$$

is a divisor with sum $\infty$ and degree 0, so there is a function $f$ on $E$ defined over $\mathbb{F}_{q^k}$ with div($f$)=$D$. Let $f_i$ be a function on $E$ with divisor $n[P_i] - n[\infty]$ for $i = 1, 2$. Then

$$\text{div}(f_1 f_2 f^{-n}) = \text{div}(f_1) + \text{div}(f_2) - n\text{div}(f) = n[P_1 + P_2] - n[\infty].$$

So we can use $f_1 f_2 f^{-n}$ to compute the pairing for $\tau_n(P_1 + P_2, Q)$. Choose $R$ so that $R \notin \{\infty, P_1, P_2, P_1 + P_2, -Q, P_1 - Q, P_2 - Q, P_1 + P_2 - Q\}$. Then

$$\begin{aligned}\tau_n(P_1 + P_2, Q) &= \left(\frac{f_1(Q+R)}{f_1(R)}\frac{f_2(Q+R)}{f_2(R)}\frac{f(R)^n}{f(Q+R)^n}\right)^{(q^k-1)/n} \\ &= \tau_n(P_1, Q)\tau_n(P_2, Q).\end{aligned}$$

For bilinearity in the second variable, given $P, Q_1, Q_2 \in E[n]$, choose $R$ so that $R \notin \{\infty, P, -Q_1, -Q_2, -(Q_1 + Q_2), P - Q_1, P - Q_2, P - Q_1 - Q_2\}$. Then

$$\frac{f(Q_1 + Q_2 + R)}{f(R)} = \frac{f(Q_1 + Q_2 + R)}{f(Q_2 + R)}\frac{f(Q_2 + R)}{f(R)},$$

so

$$\begin{aligned}\tau_n(P, Q_1 + Q_2) &= \left(\frac{f(Q_1 + Q_2 + R)}{f(R)}\right)^{(q^k-1)/n} \\ &= \left(\frac{f(Q_1 + Q_2 + R)}{f(Q_2 + R)}\frac{f(Q_2 + R)}{f(R)}\right)^{(q^k-1)/n} \\ &= \tau_n(P, Q_1)\tau_n(P, Q_2).\end{aligned}$$

(2) Nondegeneracy will be proved at the end of this chapter using an alternative definition of the Tate pairing. A proof can also be found in [17].

(3) Let $\sigma$ be an element of the Galois group of $\overline{\mathbb{F}}_{q^k}$ over $\mathbb{F}_{q^k}$. Let $f^\sigma$ denote the function obtained by applying $\sigma$ to the coefficients of $f$. Then clearly $\sigma(f(P)) =$

$f^\sigma(\sigma(P))$. If $f$ is as in our definition of $\tau_n$, then $\mathrm{div}(f)=n[P]-n[\infty]$ and consequently $\mathrm{div}(f^\sigma)=n[\sigma(P)]-n[\infty]$. So

$$\begin{aligned}\tau_n(\sigma(P),\sigma(Q)) &= \left(\frac{f^\sigma(\sigma(Q+R))}{f^\sigma(\sigma(R))}\right)^{(q^k-1)/n}\\ &= \sigma\left(\frac{f(Q+R)}{f(R)}\right)^{(q^k-1)/n}\\ &= \sigma(\tau_n(P,Q)).\end{aligned}$$

(4) Write $N=mn$. If $f$ is a function on $E$ with $\mathrm{div}(f)=n[P]-n[\infty]$, then $\mathrm{div}(f^m)=N[P]-N[\infty]$. So we can use $f^m$ for $\tau_N$. It easily follows

$$\tau_N(P,Q)=\left(\frac{f(Q+R)^m}{f(Q)^m}\right)^{(q^k-1)/N}=\left(\frac{f(Q+R)}{f(Q)}\right)^{(q^k-1)/n}=\tau_n(P,Q).$$

□

The reader should be aware that if the same curve $E$, instead of being considered over $\mathbb{F}_q$, is considered over $\mathbb{F}_{q^j}$, (where $j$ is relatively prime to $k$), then the value of $\tau_n(P,Q)$ changes. It becomes the $\frac{q^{jk}-1}{q^k-1}$-th power of the value it had when $E$ was considered over $\mathbb{F}_q$. This is different than the Weil pairing, whose value didn't change when the same curve was regarded as a curve over a field extension.

Another difference with the Weil pairing, is that we need not have $\tau_n(P,P)=1$ when $k=1$. It can be shown if $k>1$ then $\tau_n(P,P)=1$.

One other difference between the two pairings is that for the Tate pairing, we work over the field $\mathbb{F}_q(\mu_n)=\mathbb{F}_{q^k}$, while for the Weil pairing, we work over the possibly bigger field $\mathbb{F}_q(E[n])$, which is the smallest field containing $\mathbb{F}_q$ and all the coordinates of the points of $E[n]$. The following theorem from [2] shows these fields are often the same.

**Theorem 10** *Let $E$ be an elliptic curve over $\mathbb{F}_q$. Suppose that $n$ is a prime dividing $\#E(\mathbb{F}_q)$ such that $n \not| \ (q-1)$. Then $E[n]\subseteq E(\mathbb{F}_{q^k})$ if and only if $q^k\equiv 1 \mod n$.*

**Proof** If $E[n]\subseteq E(\mathbb{F}_{q^k})$, then we already proved (Corollary 2) that $\mu_n\subseteq\mathbb{F}_{q^k}$, hence $q^k\equiv 1 \mod n$. Now suppose that $q^k\equiv 1 \mod n$, and let $P\in E(\mathbb{F}_q)$ be a point of order $n$. Let $Q$ be another point on $E(\overline{\mathbb{F}}_q)$ so that $\{P,Q\}$ is a basis for $E[n]$. Let $\phi_q$ be the Frobenius map where $\phi_q(x,y)=(x^q,y^q)$. As $P$ has coordinates in $\mathbb{F}_q$, $\phi_q(P)=P$. Let $\phi_q(Q)=[a]P+[b]Q$. Then $\phi_q$ acts on $E[n]$, with the action given by the matrix

$$(\phi_q)_n=\begin{pmatrix}1 & a\\ 0 & b\end{pmatrix}.$$

The trace $t$ of $\phi_q$ is given by $q+1-\#E(\mathbb{F}_q)$. So as $n$ divides $\#E(\mathbb{F}_q)$, $1+b \equiv q+1 \mod n$, so $b \equiv q \mod n$. We can thus replace $b$ by $q$ because $Q$ has order $n$, so$[b]Q = [q]Q$.

Now replace $Q$ by $Q' = Q + [c]P$, where $c \equiv a(q-1)^{-1} \mod n$ which makes sense as $q \not\equiv 1 \mod n$. Then $\{P, Q'\}$ is also a basis for $E[n]$. One easily sees that this change of basis diagonalizes the matrix of $\phi_q$ with respect to this basis, so without loss of generality we can assume that $a = 0$. It follows that the matrix of $\phi_q^k$ (with respect to this latter basis) is

$$\begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}^k = \begin{pmatrix} 1 & 0 \\ 0 & q^k \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod n.$$

So $\phi_q^k$ fixes $Q'$, hence $\phi_q^k$ fixes all points of $E[n]$. Given any $(x, y) \in E[n]$, we have that $(x^{q^k}, y^{q^k}) = (x, y)$, so both $x$ and $y$ are in $\mathbb{F}_{q^k}$. This shows that $E[n] \subseteq \mathbb{F}_{q^k}$.

We've seen that in order to prove $\tau_n$ gives a bilinear pairing, we need at least eight distinct points in $E(\mathbb{F}_{q^k}$ of order $n$. What if $\mathbb{F}_{q^k}$ is so small that this isn't possible? Although this is unlikely to be the case in a cryptographic setting, the situation can be remedied using the equivalent definition of the Tate pairing which we'll give in the next section. □

## 5.4 Computing pairings

There is another way to define the Weil pairing which is useful for computational purposes. It also shows a relationship with the Tate pairing.

Let $f_P$ be a function on $E$ such that $\mathrm{div}(f_P) = n[P] - n[\infty]$. Define

$$\langle P, Q \rangle_n = \frac{f_P(Q+R)}{f_P(R)}$$

for $P, Q \in E[n]$, and $R \in E(\mathbb{F}_{q^k})$ such that $R \notin \{\infty, P, -Q, P-Q\}$. In the last section we showed that this is independent of the choice of $f_P$, and up to $n$-th powers, it is independent of $R$. We also saw that

$$\tau_n(P, Q) = \langle P, Q \rangle_n^{(q^k-1)/n},$$

We now show how this can be used to define the Weil pairing.

**Theorem 11** *Let $P, Q \in E[n]$. Let $D_P$ be a divisor with sum $P$ and degree 0, and $D_Q$ a degree 0 divisor with sum $Q$ such that $D_P$ and $D_Q$ have disjoint support. If $f_P, f_Q$ are functions on $E$ such that $div(f_P) = nD_P$ and $div(f_Q) = nD_Q$, then*

$$e_n(P, Q) = \frac{f_Q(D_P)}{f_P(D_Q)}.$$

**Proof** This argument is due to [42]. We begin by showing that $\frac{f_Q(D_P)}{f_P(D_Q)}$ is independent of the particular choice of $D_P, D_Q, f_P$, or $f_Q$. Any function other than $f_P$ must be of the form $cf_P$ for some constant $c$. But then $(cf_P)(D_Q) = f_P(D_Q)$, because $D_Q$ is degree 0, and so the constant cancels out. Similarly, any other constant involved in the choice of $f_Q$ drops out.

Let $D_{Q'}$ be another degree zero divisor with sum $Q$ and support disjoint from $D_P$. Let $f_{Q'}$ be the corresponding function with $\mathrm{div}(f_{Q'}) = nD_{Q'}$. Note that $D_Q - D_{Q'} = \mathrm{div}(h)$ for some $h$, and that $\mathrm{div}(h^n) = n\mathrm{div}(h) = nD_Q - nD_{Q'} = \mathrm{div}(f_Q/f_{Q'})$. Thus $f_Q = cf_{Q'}h^n$ for some constant $c$. We then calculate

$$\begin{aligned}\frac{f_Q(D_P)}{f_P(D_Q)} &= \frac{cf_{Q'}(D_P)h(D_P)^n}{f_P(D_{Q'} + \mathrm{div}(h))} = \frac{f_{Q'}(D_P)h(nD_P)}{f_P(D_{Q'})f_P(\mathrm{div}(h))} \\ &= \frac{f_{Q'}(D_P)h(\mathrm{div}(f_P))}{f_P(D_{Q'})f_P(\mathrm{div}(h))} = \frac{f_{Q'}(D_P)}{f_P(D_{Q'})}.\end{aligned}$$

The constant $c$ cancels out because $D_P$ has degree 0, and the last equality follows by Weil reciprocity. An analogous argument can be used to show the same result if $D_{P'}$ is another degree 0 divisor with sum $P$.

Let $D_P$ and $D_Q$ be divisors as in the statement of the theorem. Let $\hat{D}_Q = [Q] - [\infty]$, and $\hat{f}_Q$ be a function such that $\mathrm{div}(\hat{f}_Q) = n\hat{D}_Q$. This is the same function we labeled as $f$ when we defined the Weil pairing $e_n(P, Q)$ at the start of Section 5.2. As $D_Q - \hat{D}_Q$ is a degree 0 divisor with sum $\infty$, we can write $D_Q = \hat{D}_Q + \mathrm{div}(h_Q)$ for some function $h_Q$.

Let $Q'$ be such that $[n]Q' = [Q]$. As we showed in the definition of the Weil pairing, there exists a function $\hat{g}_Q$ such that

$$\mathrm{div}(\hat{g}_Q) = \sum_{S \in E[n]} ([Q' + S] - [S]),$$

as well as $\hat{g}_Q^n = \hat{f}_Q \circ n$.

Let $P'$ be such that $[n]P' = P$ and let $X$ be a point on $E$ such that

$$D = (n-1)[P' + X] + [P' - P + X] - n[X]$$

has support disjoint from the support of $\hat{g}_Q$. We also require that $P + [n]X$ and $[n]X$ are not equal to either $Q$ or $\infty$. We can write $D_P = \hat{D}_P + \mathrm{div}(h_P)$, where $\hat{D}_P = [P + [n]X] - [[n]X]$, and there is an $\hat{f}_P$ with $\mathrm{div}(\hat{f}_P) = n\hat{D}_P$. Note that $\hat{D}_P$ and $\hat{D}_Q$ satisfy the conditions of our theorem. Its easy to see there is a function $\hat{g}_P$ such that

$$\mathrm{div}(\hat{g}_P) = \sum_{S \in E[n]} ([P' + X + S] - [X + S]),$$

which satisfies $\hat{g}_P^n = \hat{f}_P \circ n$.

Now $D$ has sum $\infty$ and degree 0, so there is a function $h$ with $\mathrm{div}(h) = D$. By Weil reciprocity, $h(\mathrm{div}(\hat{g}_Q)) = \hat{g}_Q(\mathrm{div}(h))$. We'll now evaluate each side of this equality and this will prove the result.

We have

$$\begin{aligned}\hat{g}_Q(\mathrm{div}(h)) &= \frac{\hat{g}_Q(P'+X)^{n-1}\hat{g}_Q(P'-P+X)}{\hat{g}_Q(X)^n} \\ &= \frac{\hat{g}_Q(P'+X)^n}{\hat{g}_Q(X)^n}\frac{\hat{g}_Q(P'-P+X)}{\hat{g}_Q(P'+X)} \\ &= \frac{\hat{f}_Q \circ n(P'+X)}{\hat{f}_Q \circ n(X)}\frac{\hat{g}_Q(P'')}{\hat{g}_Q(P''+P)} \\ &= \frac{\hat{f}_Q(P+[n]X)}{\hat{f}_Q([n]X)}\frac{1}{e_n(P,Q)},\end{aligned}$$

where $P'' = P' - P + X$.

Now we look at $h(\mathrm{div}(\hat{g}_Q) = \prod_{S\in E[n]} \frac{h(Q'+S)}{h(S)}$. Let $\tau_S(T) = T + S$, and

$$H(T) = \prod_{S\in E[n]} h(T+S) = \prod_{S\in E[n]} h \circ \tau_S(T).$$

Therefore,

$$\begin{aligned}\mathrm{div}(H) &= \sum_{S\in E[n]} \mathrm{div}(h\circ\tau_S) \\ &= \sum_{S\in E[n]} (n-1)[P'+X-S] + [P'-P+X-S] - n[X-S] \\ &= n\sum_{S\in E[n]}[P'+X-S] - \sum_{S\in E[n]}[P'+X-S] \\ &\quad + \sum_{S\in E[n]}[P'-P+X-S] - n\sum_{S\in E[n]}[X-S] \\ &= n\sum_{S\in E[n]}[P'+X-S] - n\sum_{S\in E[n]}[X-S] \\ &= n\sum_{s\in E[n]}[P'+X+S] - [X+S] \\ &= n\ \mathrm{div}(\hat{g}_P) \\ &= \mathrm{div}(\hat{g}_P^n).\end{aligned}$$

Thus $H = c\hat{g}_P^n = c\hat{f}_P \circ n$, so $H(T) = c\hat{f}_P([n]T)$.

So we have that $\prod_{S\in E[n]} h(Q'+S) = H(Q') = c\hat{f}_P(Q)$, and also $\prod_{S\in E[n]} h(S) = H(\infty) = c\hat{f}_P(\infty)$. Thus

$$h(\mathrm{div}(\hat{g}_Q) = \frac{\hat{f}_P(Q)}{\hat{f}_P(\infty)}.$$

When we combine this with our above results, we find

$$\frac{\hat{f}_P(Q)}{\hat{f}_P(\infty} = \frac{\hat{f}_Q(P+[n]X)}{\hat{f}_Q([n]X)}\frac{1}{e_n(P,Q)},$$

or

$$e_n(P,Q) = \frac{\hat{f}_Q(P+[n]X)}{\hat{f}_Q([n]X)}\frac{\hat{f}_P(\infty)}{\hat{f}_P(Q)}$$
$$= \frac{\hat{f}_Q(\hat{D}_P)}{\hat{f}_P(\hat{D}_Q)}.$$

By the independence of the choice of $D_P$ and $D_Q$, this is equivalent to

$$e_n(P,Q) = \frac{f_Q(D_P)}{f_P(D_Q)}.$$

□

We show how this relates to $\langle P,Q\rangle_n$. A natural choice of divisors in the statement of the theorem is $D_P = [P]-[\infty]$ and $D_Q = [Q+R]-[R]$, where $R \neq \infty, P, -Q, P-Q$. With this choice, we show the following.

**Corollary 3** *Up to $n$-th powers, we have*

$$e_n(P,Q) = \frac{\langle Q,P\rangle_n}{\langle P,Q\rangle_n}.$$

**Proof** Using $D_P = [P]-[\infty]$ and $D_Q = [Q+R]-[R]$, we have that

$$e_n(P,Q) = \frac{f_Q(D_P)}{f_P(D_Q)} = \frac{f_Q(D_P)}{\langle P,Q\rangle_n}.$$

So we need to verify that $f_Q(D_P) = \langle Q,P\rangle_n$, up to $n$-th powers.

Now let $S$ be any point of $E$ such that $S \notin \{\infty, Q, -P, Q-P\}$, and let $D_S = [P+S]-[S]$. Then $D_P - D_S = \mathrm{div}(h)$ for some function $f_S$. So

$$f_Q(D_P) = f_Q(D_S + \mathrm{div}(h)) = f_Q(D_S)f_Q(\mathrm{div}(h))$$
$$= f_Q(D_S)h(\mathrm{div}(f_Q)) = f_Q(D_S)h(nD_Q) = f_Q(D_S)h(D_Q)^n.$$

Furthermore, if $f$ is a function such that $\mathrm{div}(f) = n[Q]-n[\infty]$, then $\mathrm{div}(f_Q/f)$=$\mathrm{div}(f_Q)$-$\mathrm{div}(f) = n(D_Q-[Q]+[\infty]) = n\mathrm{div}(g) = \mathrm{div}(g^n)$ for some function $g$. It follows that $f_Q = cfg^n$ for some constant $c$. Then

$$f_Q(D_P) = f_Q(D_S)h(D_Q)^n = (cf)(D_S)g(D_S)^n h(D_Q)^n = f(D_S)$$

up to $n$-th powers. But $f(D_S) = \langle Q,P\rangle_n$ up to $n$-th powers, so we are done. □

We have seen that to compute $\langle P,Q\rangle_n$ (and thus $e_n(P,Q)$ and $\tau_n(P,Q)$) we have to find a function $f$ with $\mathrm{div}(f) = n[P]-n[\infty]$. The proof of Theorem 6 illustrated how we can do this. However, for large $n$, it is not efficient. V. Miller created an algorithm ([48],[49]) that finds $f$ in polynomial time.

The main idea is to use the double and add technique. Let $f_i$ be a function such that

$$\mathrm{div}(f_i) = i[P]-[[i]P]-(i-1)[\infty].$$

Such functions are determined up to a constant multiple. We seek to find $f_n$.

**Lemma 5** *The functions $f_i$ can be chosen so that:*

1. $f_1 = 1$.
2. *Let $l$ and $v$ be algebraic expressions for the straight lines used in the computation of $[i]P + [j]P = [i+j]P$. Then*

$$f_{i+j} = f_i f_j \frac{l}{v}.$$

**Proof** It is trivial that $f_1 = 1$ works. As in the proof of Theorem 6

$$\mathrm{div}(\frac{l}{v}) = [[i]P] + [[j]P] - [[i+j]P] - [\infty]$$

so

$$\begin{aligned}\mathrm{div}(f_i f_j \frac{l}{v}) &= \mathrm{div}(f_i) + \mathrm{div}(f_j) + \mathrm{div}(\frac{l}{v}) \\ &= i[P] - [[i]P] - (i-1)[\infty] + j[P] - [[j]P] - (j-1)[\infty] \\ &\qquad + [[i]P] + [[j]P] - [[i+j]P] - [\infty] \\ &= (i+j)[P] - [[i+j]P] - (i+j-1)[\infty].\end{aligned}$$

□

We double when $i = j$ and add when $j = 1$. The algorithm uses an addition chain for $[n]P$ to construct $f_n$. As we need to compute $f_n(D)$, where $D = [Q+R] - [R]$, we evaluate all intermediate $f_i$ at $D$. We now give his algorithm:

**Algorithm 1 - Miller's algorithm to evaluate $\langle P, Q \rangle_n$**

1. Given $P, Q \in E[n]$, choose $R \in E[n]$ with $R \notin \{\infty, P, -Q, P-Q\}$.
2. Write $n$ in binary as $n = (n_t, ..., n_1, n_0)$ with each $n_i \in \{0, 1\}$.
3. Set $f = 1$, $T = P$ and $i = t$.
4. If $i < 0$ then go to step 5. Else do the following:
   (a) Let $l$ be the tangent line to $E$ through $T$. Let $v$ be the vertical line through $2T$.
   (b) Set $T = 2T$.
   (c) Set $f = f^2 \frac{l(Q+R)}{v(Q+R)} \frac{v(R)}{l(R)}$.
   (d) If $n_i = 1$ then do the following:
      i. Let $l$ be the line through $T$ and $P$, and $v$ the vertical line through $T + P$.
      ii. Set $T = T + P$.
      iii. Set $f = f \frac{l(Q+R)}{v(Q+R)} \frac{v(R)}{l(R)}$.

(e) Set $i = i - 1$ and return to step 4

5. The desired value is $\langle P, Q \rangle_n = f$

This algorithm has been improved upon, and is efficient enough to be used to implement pairing based cryptography at current security levels.

## 5.5 An alternative definition of the Tate pairing

We first show another way the Tate pairing can be defined using the Weil pairing. We follow the exposition of Washington ([67]).

**Theorem 12** *Given points $P, Q \in E[n]$, choose $R \in E(\overline{\mathbb{F}}_q)$ such that $[n]R = Q$. Let $\phi$ be the Frobenius map, i.e., $\phi(x, y) = (x^{q^k}, y^{q^k})$. Then*

$$\tau_n(P, Q) = e_n(P, R - \phi(R)).$$

**Proof** Note that $[n](R - \phi(R)) = [n]R - [n]\phi(R) = Q - \phi(Q) = \infty$, so $e_n(P, R - \phi(R))$ is defined. We also need to verify that it is independent of the choice of $R$. Let $R'$ be another point such that $[n]R' = Q$. It's clear that $R' - R \in E[n]$. So

$$\begin{aligned} e_n(P, R' - \phi(R')) &= e_n(R - \phi(R) + (R' - R) - \phi(R' - R)) \\ &= \frac{e_n(P, R - \phi(R)) e_n(P, R' - R)}{e_n(P, \phi(R' - R))}, \end{aligned}$$

using the bilinearity of $e_n$. As $P \in E(\mathbb{F}_{q^k})$, then $\phi(P) = P$ and we see

$$e_n(P, \phi(R' - R)) = e_n(\phi(P), \phi(R' - R)) = \phi(e_n(P, R' - R)) = e_n(P, R' - R)$$

because $e_n(P, R' - R) \in \mathbb{F}_{q^k}$. This shows that

$$e_n(P, R' - \phi(R')) = e_n(P, R - \phi(R))$$

doesn't depend on the choice of $R$.

We now show this gives the same value as $\tau_n(P, Q)$. Let $T \in E[n]$ and choose a function $g$ with

$$\operatorname{div}(g) = n[R] - [Q + T] + [T] - n[\infty],$$

and let $g^\phi$ be the function obtained by applying $\phi$ to all the coefficients of $g$. Thus $\phi(g(X)) = g^\phi(\phi(X))$ for any point $X$. Looking at the divisor of $g^\phi$, we calculate

$$\operatorname{div}(g^\phi) = n[\phi(R)] - [Q + T] + [T] - n[\infty].$$

It follows that

$$\operatorname{div}(g/g^\phi) = n[R] - n[\phi(R)].$$

Now choose a degree 0 divisor $D_P$ such that $\operatorname{sum}(D_P) = P$, and $D_P$ has disjoint support from the support of $\operatorname{div}(g)$. We also require that $\phi(D_P) = D_P$, that is $\phi$ permutes the points in the support $D_P$ such that the formal expression

for $D_P$ is unchanged. There is always some choice which will work, by Lemma 11.9 of [67]. One possibility which will often work is $D_P = [P+S]-[S]$, where $S \in E(\mathbb{F}_{q^k})$ is chosen so $S \notin \{Q+T, R, T, \infty, Q+T-P, R-P, T-P, -P\}$.

As $[n]P = \infty$, then there is a function $f$ with $\mathrm{div}(f) = nD_P$, and by Theorem 6 we can assume that $f$ is defined over $\mathbb{F}_{q^k}$ so that $\phi(f(R)) = f(\phi(R))$. By Theorem 11 applied with $Q = R - \phi(R)$, $D_Q = [R] - [\phi(R)]$, $f_P = f$, and $f_Q = g/g^\phi$ we see

$$e_n(P, R-\phi(R)) = \frac{(g/g^\phi)(D_P)}{f([R]-[\phi(R)])}.$$

Rearranging this yields

$$e_n(P, R-\phi(R)) = \phi\left(\frac{f(R)}{g(D_P)}\right)\frac{g(D_P)}{f(R)} = \left(\frac{f(R)}{g(D_P)}\right)^{q^k-1},$$

since $\phi$ raises elements to the $q^k$-th power.

Notice that

$$g(D_P)^n = g(nD_P) = g(\mathrm{div}(f)) = f(\mathrm{div}(g)) = \frac{f(R)^n f(T)}{f(Q+T)f(\infty)^n}$$

by Weil reciprocity. So

$$\left(\frac{f(R)}{g(D_P}\right)^n = \frac{f(Q+T)}{f(T)} f(\infty)^n,$$

and raising both sides to the $(q^k-1)/n$-th power

$$\left(\frac{f(R)}{g(D_P}\right)^{q^k-1} = \left(\frac{f(Q+T)}{f(T)}\right)^{(q^k-1)/n} f(\infty)^{q^k-1}.$$

Since $f$ is defined over $\mathbb{F}_{q^k}$, then $f(\infty) \in \mathbb{F}_{q^k}$ and hence $f(\infty)^{q^k-1} = 1$. Combining the various pieces above, we see that

$$e_n(P, R-\phi(R)) = \left(\frac{f(Q+T)}{f(T)}\right)^{(q^k-1)/n}.$$

This is almost what we want, however in the definition of $\tau_n(P,Q)$, we need a function $F$ such that $\mathrm{div}(F) = n[P] - n[\infty]$, while we have $\mathrm{div}(f) = nD_P$. Note that $D_P - [P] + [\infty]$ is a degree 0 divisor with sum $\infty$, so is the divisor of a function $h$, which we can take to be defined over $\mathbb{F}_{q^k}$. A simple calculation shows that $h^n$ and $f/F$ have the same divisor, so $f = cFh^n$ for some constant $c$. We find

$$\begin{aligned}
\left(\frac{f(Q+T)}{f(T)}\right)^{(q^k-1)/n} &= \left(\frac{cF(Q+T)h(Q+T)^n}{cF(T)h(T)^n}\right)^{(q^k-1)/n} \\
&= \left(\frac{F(Q+T)}{F(T)}\right)^{(q^k-1)/n}\left(\frac{h(Q+T)}{h(T)}\right)^{q^k-1} \\
&= \left(\frac{F(Q+T)}{F(T)}\right)^{(q^k-1)/n},
\end{aligned}$$

since $\left(\frac{h(Q+T)}{h(T)}\right)^{q^k-1} = 1$.

Thus

$$e_n(P, R-\phi(R)) = \left(\frac{F(Q+T)}{F(T)}\right)^{(q^k-1)/n} = \tau_n(P,Q).$$

□

The properties of the Tate pairing in Theorem 9 can also be proved using this definition. For example, bilinearity easily follows from the bilinearity of $e_n$. We did not prove the nondegeneracy of $\tau_n$, which we can now do.

**Theorem 13** *If $n$ is a prime such that $n^3 \not| \#E(\mathbb{F}_{q^k})$, then the Tate pairing $\tau_n$ is nondegenerate.*

We'll establish a series of lemmas which will prove the result. The ideas are due to Washington ([67]).

**Lemma 6** *Let $G$ be a finite abelian group (written additively) such that $ng = 0$ for all $g \in G$. Letting $\mathrm{Hom}(G, \mu_n)$ denote the set of all homomorphisms from $G$ to $\mu_n$, then $|G| = \#\mathrm{Hom}(G, \mu_n)$.*

**Proof** We first prove the result for the special case when $G \cong \mathbb{Z}_m$, with $m|n$. Let $f$ be a homomorphism from $\mathbb{Z}_m$ to $\mu_n$. Then $f(1)^m = f(m) = 1$, so $f(1) \in \mu_m \subseteq \mu_n$. The value of $f(1)$ completely determines $f$, as $f(b) = f(1)^b$. There are clearly $m$ choices for $f(1)$, and each yields a different homomorphism, so $\#\mathrm{Hom}(G, \mu_n) = \#\mathrm{Hom}(\mathbb{Z}_m, \mu_n) = m = |G|$.

Now if $G$ is any finite abelian group, then we know

$$G \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_k}.$$

As $ng = 0$ for all $g$ in $G$, then we must have that $m_i|n$ for all $1 \leq i \leq k$. We claim there is a bijection

$$\Phi : \mathrm{Hom}(\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_k}, \mu_n) \to \mathrm{Hom}(\mathbb{Z}_{m_1}, \mu_n) \oplus \cdots \oplus \mathrm{Hom}(\mathbb{Z}_{m_k}, \mu_n).$$

Set $\Phi(f) = (f_1, ..., f_k)$, with $f_i$ defined by $f_i(b) = f(0, ..., 0, b, 0, ..., 0)$ where the $b$ is in the $i$-th entry. The inverse map sends $(f_1, ..., f_k)$ to $f$, where $f(b_1, ..., b_k) = f_1(b_1)f_2(b_2)\cdots f_k(b_k)$. The details are easy to verify. The result then follows as $|G| = m_1 m_2 \cdots m_k$. □

**Lemma 7** *The groups $E[n]$ and $H = \mathrm{Hom}(E[n], \mu_n)$ are isomorphic.*

**Proof** For each $T \in E[n]$, define a map $\psi_T : E[n] \to \mu_n$ by $\psi_T(S) = e_n(S, T)$. Clearly $\psi_T(S + S') = e_n(S + S', T) = e_n(S, T)e_n(S', T) = \psi_T(S)\psi_T(S')$, so $\psi_T \in H$. Let $T'$ be another point in $E[n]$. Then $\psi_{T+T'}$ is defined by

$$\psi_{T+T'}(S) = e_n(S, T + T') = e_n(S, T)e_n(S, T') = \psi_T(S)\psi_{T'}(S)$$

, so $\psi_{T+T'} = \psi_T \psi_{T'}$, which shows we have a homomorphism from $E[n]$ into $H$.

Suppose $\psi_T$ is the trivial homomorphism, so $\psi_T(S) = e_n(S,T) = 1$ for all $S$ in $E[n]$. By the nondegeneracy of the Weil pairing, $T = \infty$, which shows the homomorphism from $E[n]$ into $H$ is injective. By the previous lemma, the two groups have the same order which implies the injection is actually an isomorphism. □

Now, define the map $\psi$ by

$$\psi : E[n] \to \prod_{S \in E[n]} \mu_n$$

$$\psi(T) = (\cdots, e_n(S,T), \cdots).$$

It is clear that $\psi$ is a homomorphism.

**Lemma 8** *We have* $\#\psi(E[n]) = \#E[n]$.

**Proof** By Lemma 7, $E[n]$ and $\mathrm{Hom}(E[n], \mu_n)$ are isomorphic. The kernel of $\psi$ is

$$\ker \psi = \{T \in E[n] \mid e_n(S,T) = 1 \text{ for all } S \in E[n]\}.$$

Using the isomorphism, this is equivalently

$$\begin{aligned} \ker \psi &= \{f \in \mathrm{Hom}(E[n], \mu_n) \mid f(S) = 1 \text{ for all } S \in E[n]\} \\ &= \mathrm{Hom}(E[n]/E[n], \mu_n). \end{aligned}$$

Thus by Lemma 6, $\#\ker \psi = \#E[n]/\#E[n]$. From the first isomorphism theorem for groups, we know $\#E[n]/\#\ker \psi = \#\psi(E[n])$. Combining these last two equations gives the result. □

**Lemma 9** *The kernel of* $\psi$ *is* $(\phi - 1)E[n]$*, where* $\phi$ *is the Frobenius endomorphism of* $E(\mathbb{F}_{q^k})$.

**Proof** For any $T$ in $E[n]$, we see

$$\begin{aligned} \psi(\phi(T)) &= (\cdots, e_n(S, \phi(T)), \cdots) \\ &= (\cdots, e_n(\phi(S), \phi(T)), \cdots) \\ &= (\cdots, \phi(e_n(S,T)), \cdots) \\ &= (\cdots, e_n(S,T), \cdots) \\ &= \psi(T). \end{aligned}$$

This shows $(\phi - 1)E[n] \subseteq \ker \psi$.

We now prove these two sets have the same order, which gives equality.

$$\begin{aligned}
\#E[n] &= \#\ker\,(\phi-1)|_{E[n]} && (\text{as } \ker(\phi-1)=\mathbb{F}_{q^k})\\
&= \#E[n]/\#((\phi-1)E[n]) && (\text{1st isomorphism theorem})\\
&\geq \#E[n]/\#\ker\,\psi && (\text{as } (\phi-1)E[n]\subseteq \ker\,\psi\\
&= \#\psi(E[n]) && (\text{by the 1st isomorphism theorem})\\
&= \#E[n] && (\text{by Lemma 8}).
\end{aligned}$$

So there must be equality throughout, and $\#(\phi-1)E[n] = \#\ker\,\psi$. □

**Lemma 10** *Suppose we have a bilinear pairing $\langle,\rangle : E[n]\times E[n]\to\mu_n$ which is nondegenerate in the first variable (that is, if $\langle S,T\rangle = 1$ for all $S\in E[n]$ then $T=\infty$). Then the pairing is nondegenerate in the second variable also.*

**Proof** Let

$$\mathcal{S} = \{S\in E[n] | \langle S,T\rangle = 1 \text{ for all } T\in E[n]\}.$$

For any $T$ in $E[n]$, we can define a homomorphism $f_T : E[n]/\mathcal{S}\to\mu_n$ where $f_T(S+\mathcal{S}) = \langle S,T\rangle$. By the definition of $\mathcal{S}$, these homomorphisms are well-defined.

Now suppose that $f_T$ is the trivial homomorphism for some $T$. Then $\langle S,T\rangle = 1$ for all $S\in E[n]$. By the nondegeneracy in the first variable, we must have that $T=\infty$. This means we have an injection from $E[n]$ into $\mathrm{Hom}(E[n]/\mathcal{S},\mu_n)$. By Lemma 6, $\#\mathrm{Hom}(E[n]/\mathcal{S},\mu_n) = \#E[n]/|\mathcal{S}|$. The injection implies that $|\mathcal{S}|=1$, thus $\mathcal{S}=\{\infty\}$. This is exactly what nondegeneracy in the second variable means. □

We can now prove the nondegeneracy of $\tau_n$. Suppose $\tau_n(P,Q)=1$ for all $P\in E[n]$. Let $R$ be such that $[n]R=Q$, so $e_n(P,R-\phi(R))=1$ for any $P$ in $E[n]$. This means that $R-\phi(R)$ is in the kernel of $\psi$, which is the same as $(\phi-1)E[n]$. So there exists a $T\in E[n]$ such that $\phi(T)-T = R-\phi(R)$, or $R+T=\phi(R+T)$. The fixed field of $\phi$ is $\mathbb{F}_{q^k}$, so $R+T\in E(\mathbb{F}_{q^k})$. We can thus write $Q=[n]R=[n](R+T)$, and $[n^2](R+T)=[n]Q=\infty$. By our assumption that $n^3\not|\,\#E(\mathbb{F}_{q^k})$, then $n\not|\,\#E(\mathbb{F}_{q^k})/n^2$, and $R+T$ can't have order $n^2$. As $n$ is prime, $R+T$ has order 1 or $n$, and either way $Q=\infty$, and we have shown nondegeneracy in the first variable. Lemma 10 shows that $\tau_n$ is nondegenerate in the second variable as well.

# 6 Distortion Maps

## 6.1 Endomorphisms, isogenies, and distortion maps

Let $E: y^2 = x^3+Ax+B$ be an elliptic curve defined over $\mathbb{F}_q$. An *endomorphism* of $E$ is a homomorphism from $E(\overline{\mathbb{F}}_q)$ to itself given by rational functions. The

simplest endomorphisms are just those given by multiplication by an integer $[n] : E \to E$ where $[n](P) = [n]P$. This shows that $\mathbb{Z} \subseteq \text{End}(E)$, the ring of all endomorphisms of $E$. But there are more endomorphisms, as the following theorem shows. For a proof, see [66].

**Theorem 14** *If $E$ is ordinary, then End($E$) is an order in an imaginary quadratic field. If $E$ is supersingular, then End($E$) is an order in a quaternion algebra.*

A *quaternion algebra* is an algebra of the form

$$\mathbb{H} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta,$$

where $\alpha$ and $\beta$ satisfy

$$\alpha^2, \beta^2 \in \mathbb{Q},\ \alpha^2 < 0,\ \beta^2 < 0,\ \beta\alpha = -\alpha\beta.$$

Note that $\mathbb{H}$ is non-commutative. D. Kohel has created an algorithm (see [36]) that determines End($E$).

Now let $n$ be a prime, and let $K$ be the smallest extension of $\mathbb{F}_q$ for which $E[n] \subseteq K$. If the embedding degree satisfies $k > 1$, then $K = \mathbb{F}_{q^k}$ by Theorem 10. A *distortion map* $H$ with respect to a cyclic subgroup $\langle P \rangle$ of order $n$ is an endomorphism of the curve (defined over $K$) that maps any nonzero point $Q \in \langle P \rangle$ to a point $H(Q)$ linearly independent from $Q$. That is, $H(Q) \notin \langle P \rangle$. Since $H$ is a group homomorphism, $H(Q)$ is a non-trivial element of order $n$ on the curve. It follows from Corollary 1 of Theorem 7 that the value $e_n(Q, H(Q)) \neq 1$. As we will show in chapter 10, Verheul's argument can readily be generalized, provided that an efficiently computable $H$ can be found.

We illustrate with a few simple examples. Suppose $q = p^f$, with $p$ a prime where $p \equiv 2 \mod 3$. Then the curve defined by $y^2 = x^3 - 1$ is supersingular. The map

$$(x, y) \to (\zeta x, y)$$

where $\zeta \in \mathbb{F}_{p^2}$ with $\zeta^3 = 1, \zeta \neq 1$ is a distortion map. Similarly, if $p \equiv 3 \mod 4$, the curve $y^2 = x^3 + x$ is also supersingular. The map

$$(x, y) \to (-x, iy)$$

with $i \in \mathbb{F}_{p^2}, i^2 = -1$ is a distortion map.

Verheul proved that distortion maps exist for all supersingular curves. Finding an *efficiently computable* distortion map for *all* supersingular curves is more difficult. One way to create distortion maps is to use $l$-isogenies. An *isogeny* is a nonconstant homomorphism from $E(\overline{\mathbb{F}}_q)$ to another curve $E_1(\overline{\mathbb{F}}_q)$ given by rational functions. If the kernel has order $l$, then it is called an $l$-isogeny. Given a curve $E$ for which we wish to construct a distortion map, the image of an $l$-isogeny $\phi$ from $E$ is usually not $E$. However, we can construct an isomorphism $\psi$ from the image back to $E$, and the map $\psi \circ \phi$ will be a distortion map. Which $l$ we use depends on the elliptic curve. We will always assume that $l$ is prime, as if $l$ is composite, we can factor $l$ into a product of primes $l = p_1 \cdots p_r$. Then the $l$-isogeny can be obtained by using a composition of $p_i$-isogenies.

In the examples given above, the distortion maps are not only isogenies, but actually are automorphisms of the curve. In fact, these maps and their inverses are the only non-trivial automorphisms of elliptic curves when the characteristic of $\mathbb{F}_q$ is greater than 3 (Theorem III.10.1 of [60]). Note that the endomorphism rings of these curves are isomorphic to either $\mathbb{Z}[i]$ or $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, which are the only imaginary quadratic number rings with non-trivial units.

We now describe how to find isogenies.

## 6.2 Vélu's formulae

In [64], Vélu showed how to find an isogeny explicitly. Let $l$ be an odd (not necessarily prime) number. For simplicity, we'll assume the characteristic of $\mathbb{F}_q$ is greater than 3. Let $F$ be a subgroup of $E$ of order $l$, which we desire to be the kernel of our isogeny.

We define $\phi$ in the following way. For $P = (x_P, y_P) \notin F$, let

$$\phi(P) = \left( x_P + \sum_{Q \in F - \{\infty\}} (x_{P+Q} - x_Q), y_P + \sum_{Q \in F - \{\infty\}} (y_{P+Q} - y_Q) \right).$$

The points of $F$ cause some difficulty, as $x_\infty$ and $y_\infty$ don't make sense. To get around this, we could use projective coordinates. We omit the details, because the basic idea is clear. For any point $P \in F$, we set $\phi(P) = \infty$. It is easy to see that $\phi$ is invariant under translation by elements of $F$, and that the kernel of $\phi$ is $F$. Using the group law on the curve, we also see that $\phi$ can be written in terms of rational functions. It necessarily follows by the following theorem that $\phi$ is an isogeny.

**Theorem 15** *Let $E$ and $E_1$ be two elliptic curves defined over a field $K$, and $\alpha : E(\overline{K}) \to E_1(\overline{K})$ be a nonconstant map given by rational functions. If $\alpha(\infty) = \infty$, then $\alpha$ is an isogeny.*

For a proof see [60] or [67]. So $\phi$ is an $l$-isogeny with kernel $F$, as desired.

We would like to have an easier way of computing $\phi$. If we set $\phi(x, y) = (X, Y)$ then using the formula for addition on $E$,

$$X = x + \sum_{Q \in F - \{\infty\}} \left( \left( \frac{y - y_Q}{x - x_Q} \right)^2 - x - 2x_Q \right),$$

and a similar expression for $Y$. Using the fact that $Q$ lies on $E$ and some straightforward algebra we can simplify the expression for $X$:

$$X = x + \sum_{Q \in F - \{\infty\}} \left( \frac{3x_Q^2 + A}{x - x_Q} + 2\frac{x_Q^3 + Ax_Q + B}{(x - x_Q)^2} \right).$$

This equation can be further rewritten. In what follows, when we use derivatives, we mean the formal derivative of a polynomial defined by the familiar

$\frac{\partial}{\partial x}x^n = nx^{n-1}$. We extend this to derivatives of rational functions by using the quotient rule. Let

$$D(x) = \prod_{Q \in F - \{\infty\}} (x - x_Q),$$

and define $\sigma$ by

$$D(x) = x^{l-1} - \sigma x^{l-2} + ...$$

As $F$ is a subgroup, whenever a point $Q = (x, y) \in F$, then necessarily $-Q = (x, -y) \in F$, so $D(x)$ will be a square, $D(x) = g(x)^2$. Note also that $\frac{D'(x)}{D(x)} = 2\sum_{Q \in F - \{\infty\}} \frac{1}{x - x_Q}$ and $\left(\frac{D'(x)}{D(x)}\right)' = -2\sum_{Q \in R} \frac{1}{(x-x_Q)^2}$. Some more algebra shows that

$$X = x + \sum_{Q \in F - \{\infty\}} \left( (x - x_Q) - \frac{3x^2 + A}{x - x_Q} + 2\frac{x^3 + Ax + B}{(x - x_Q)^2} \right).$$

Thus

$$X = lx - \sigma - (3x^2 + A)\frac{D'(x)}{D(x)} - 2(x^3 + Ax + B)\left(\frac{D'(x)}{D(x)}\right)'.$$

Up until now, we have been ignoring $Y$. There is a good reason to do so. Any isogeny can be written as $I(x, y) = (I(x), cyI'(x))$ for some constant $c$ (see [61]). In our case it can be checked that $c = 1$, and so $Y = y\frac{\partial X}{\partial x}$, so the formula for $X$ determines the formula for $Y$. If the image of $E$ under the isogeny is $y^2 = x^3 + \tilde{A}x + \tilde{B}$, then we have

$$(x^3 + Ax + B)(I'(x))^2 = I(x)^3 + \tilde{A}I(x) + \tilde{B}.$$

Differentiating this, we find

$$(3x^2 + A)I'(x) + 2(x^3 + Ax + B)I''(x) = 3I(x)^2 + \tilde{A}.$$

Note the similarity of the left hand side of the equation for $X$ above. The similarities become even more apparent if we make the substitution $I(x) = -\log D(x)$.

This shows that $\phi$ can be written as

$$\phi(x, y) = \left( \frac{N(x)}{D(x)}, y\left(\frac{N(x)}{D(x)}\right)' \right)$$

where $N(x)$ is related to $D(x)$ by

$$\frac{N(x)}{D(x)} = lx - \sigma - (3x^2 + A)\frac{D'(x)}{D(x)} - 2(x^3 + Ax + B)\left(\frac{D'(x)}{D(x)}\right)'.$$

We can also determine the Weierstrass equation of the image $\tilde{E}$ of $E$. Let

$$D(x) = x^{l-1} - \sigma x^{l-2} + \sigma_2 x^{l-3} - \sigma_3 x^{l-4} + ...$$

and set $t = A(l-1)+3(\sigma^2-2\sigma_2)$ and $w = 3A\sigma+2B(l-1)+5(\sigma^3-3\sigma\sigma_2+3\sigma_3)$. Then the isogenous curve is $\tilde{E} : y^2 = x^3 + (A-5t)x + (B-7w)$. All the above computations are done in $\mathbb{F}_q$.

More generally, Vélu's paper does not require that $l$ be odd, although the equations are easier in this case. In our applications $l$ is odd and prime.

Observe that along with the coefficients $A$ and $B$ in the equation of $E$, the polynomial $D(x)$ is enough to determine the $l$-isogeny. As a consequence, we will often display only $D(x)$, and not the explicit equations for the image $(X, Y)$ of the isogeny. We will show how to find $D(x)$ in Algorithm 2 of chapter 8.

As an illustration of Vélu's formulae, let's take $E$ to be the curve $y^2 = x^3 + 9x + 4$ over $\mathbb{F}_{13}$. A simple calculation finds that $E$ has 14 points over $\mathbb{F}_{13}$. The point $P = (0, 2)$ has order 7, with $[2]P = (1, 12)$ and $[3]P = (8, 9)$. Using these points, we can find a 7-isogeny. Since we know the kernel explicitly, we easily see

$$D(x) = (x-0)^2(x-1)^2(x-8)^2 = x^6 + 8x^5 + 6x^4 + 12x^3 + 12x^2,$$

and hence $\sigma = 5$. We then compute

$$\begin{aligned}\frac{N(x)}{D(x)} &= 7x - 5 - (3x^2+9)\frac{6x^5+x^4+11x^3+10x^2+11x}{x^6+8x^5+6x^4+12x^3+12x^2} \\ &\qquad - 2(x^3+9x+4)\left(\frac{6x^5+x^4+11x^3+10x^2+11x}{x^6+8x^5+6x^4+12x^3+12x^2}\right)' \\ &= \frac{x^7+8x^6+8x^5+11x^4+9x^3+x^2+5x+10}{(x^3+4x^2+8x)^2}.\end{aligned}$$

Then by Vélu, the 7-isogeny with kernel $\{P, [2]P, [3]P, [4]P, [5]P, [6]P, \infty\}$ is

$$\begin{aligned}\phi(x,y) = \Bigg(&\frac{x^7+8x^6+8x^5+11x^4+9x^3+x^2+5x+10}{(x^3+4x^2+8x)^2}, \\ &y\frac{x^9+12x^8+5x^7+6x^6+9x^5+6x^4+10x^2+8x+9}{(x^3+4x^2+8x)^3}\Bigg).\end{aligned}$$

To find the image of $E$ under $\phi$, we observe that $\sigma_2 = 6$ and $\sigma_3 = 1$. So $t = 9(7-1)+3(4\cdot9^2-2\cdot6) = 2$ and $w = 6\cdot9\cdot9+2\cdot4(7-1)+5(8\cdot9^3-6\cdot9\cdot6+3\cdot1) = 9$. This means the image is $\tilde{E} : y^2 = x^3 + 12x + 6$.

Let's do an example where we have to use an extension of $\mathbb{F}_{13}$. Suppose we want an 11-isogeny. As $11|(13^{10}-1)$, we'll work over $\mathbb{F}_{13^{10}}$. We'll represent this field as $\mathbb{F}_{13}(\theta)$, where $\theta$ is a root of $x^{10}+7x^5+5x^4+8x^3+x^2+x+2$. Then $E(\mathbb{F}_{13^{10}})$ has $137859234436 = 2^2 \cdot 7^2 \cdot 11^2 \cdot 2411^2$ points. The point $P = (7\theta^9+2\theta^8+\theta^7+5\theta^6+2\theta^5+12\theta^4+12\theta^3+4\theta^2+6\theta+10, 3\theta^9+10\theta^8+8\theta^7+3\theta^6+10\theta^5+5\theta^3+9\theta^2+5)$ has order 11. Then if we take the x-coordinates of $P, [2]P, [3]P, [4]P$, and $[5]P$,

we get the degree 5 polynomial

$$\begin{aligned} g(x) = (x^5 &+ (12\theta^9 + 9\theta^8 + 11\theta^7 + 3\theta^6 + 9\theta^5 + 2\theta^4 + 2\theta^3 + 5\theta^2 + \theta + 6)x^4 \\ &+ (2\theta^9 + 6\theta^8 + 6\theta^7 + 9\theta^6 + 7\theta^5 + 11\theta^4 + \theta^3 + 9\theta + 7)x^3 \\ &+ (4\theta^9 + 8\theta^8 + 8\theta^7 + 11\theta^6 + \theta^5 + 9\theta^4 + 4\theta^3 + 7\theta^2 + \theta + 9)x^2 \\ &+ (11\theta^9 + 11\theta^8 + 3\theta^7 + 5\theta^6 + 5\theta^5 + 2\theta^3 + 10\theta^2 + \theta)x \\ &+ 7\theta^9 + 6\theta^8 + \theta^7 + 8\theta^6 + 3\theta^5 + 8\theta^4 + 9\theta^3 + 3\theta^2 + 6\theta + 9)^2, \end{aligned}$$

and $D(x) = g(x)^2$. As mentioned before, $D(x)$ explicitly determines the isogeny. We do not display the complete equations for $(X, Y)$ here for reasons of space.

# 7 Pairing Based Cryptography

Since 2000, pairings have been used in a variety of contexts in cryptography. Here we list a few of the many ways pairings have been utilized. For several of these, we need a point to have non-trivial pairing with itself, so we first need to show how we can modify our pairings to accommodate this.

Let $E(\mathbb{F}_q)$ be an elliptic curve. The examples we give, as well as most cryptographic protocols, require us to work in a cyclic subgroup $\langle P \rangle$ of $E(\mathbb{F}_q)$, where $P$ has large prime order $n$. Let $D$ be a distortion map for $P$, so $D(P) \notin \langle P \rangle$. By the nondegeneracy of the pairings, $e_n(P, D(P)) \neq 1$ and when $\tau_n(P, P) = 1$ (which is the case when $k > 1$) then $\tau_n(P, D(P)) \neq 1$ also. Several possible elliptic curves with corresponding distortion maps are given in the appendix.

For the remainder of this chapter, let $e(P, Q) = e_n(P, D(Q))$ or $e(P, Q) = \tau_n(P, D(Q))$ depending on whether we wish to use the Weil or Tate pairing. Note that $e$ is still a bilinear pairing, and satisfies $e(P, P) \neq 1$.

## 7.1 MOV/Frey-Rück attack

Both the Tate pairing and the Weil pairing ([46],[17]) can transform an instance of the elliptic curve discrete logarithm problem into an instance of a finite field discrete logarithm problem. There are sub-exponential algorithms to solve the discrete log problem in finite fields, while no such algorithms are known for general elliptic curves. Let $\hat{e}$ be either the Tate or Weil pairing. Note that $\hat{e}$ is different than $e$.

Suppose $P$ is a point of prime order $n$ on an elliptic curve $E(\mathbb{F}_q)$, with $n$ and $q$ relatively prime. Let $Q = [a]P$ for some unknown $a$. We will work in the field $\mathbb{F}_{q^k}$, where $k$ is the embedding degree. If $k > 1$, this is the smallest field in which the curve has a full set of $n^2$ points of order $n$. We then find an $S \in E[n]$ such that $\hat{e}(P, S) \neq 1$. Note that $S$ cannot be found in $E(\mathbb{F}_q)$, since $E(\mathbb{F}_q)[n] = \langle P \rangle$. We are guaranteed such an $S$ exists by nondegeneracy, and with high probability a random choice of $S$ will work. Now compute $\zeta_P = \hat{e}(P, S)$ and $\zeta_Q = \hat{e}(Q, S)$ both in $\mathbb{F}_{q^k}$. Then

$$\zeta_Q = \hat{e}(Q, S) = \hat{e}([a]P, S) = \hat{e}(P, S)^a = \zeta_P^a.$$

We have transformed our discrete logarithm from the elliptic curve $E$ to the finite field $\mathbb{F}_{q^k}$, and the solution of the finite field problem is also the solution to the elliptic curve DLP.

The best discrete log algorithms for $\mathbb{F}_{q^k}$ are subexponential in $\log(q^k)$, but not in $\log(q)$, unless $k$ is very small. So this attack will be computationally helpful only if $k$ is small. For supersingular curves, we have $k \leq 6$, so supersingular curves are vulnerable to this attack.

## 7.2 Three party key distribution

Suppose we wished to create a common key between three parties Alice, Bob, and Charles. One way to do this is to extend the Diffie-Hellman key exchange. Given a point $P$ on an elliptic curve $E(\mathbb{F}_q)$, Alice chooses a secret number $a$, Bob chooses secret $b$, and Charles chooses secret $c$. In the first round, Alice sends $[a]P$ to Bob. Bob sends $[b]P$ to Charles, and Charles sends $[c]P$ to Alice. In the second round, Alice computes and sends $[a]([c]P) = [ac]P$ to Bob. Bob likewise sends $[ab]P$ to Charles, and Charles sends $[bc]P$ to Alice. All three users can now find the common key $[abc]P$. It is natural to wonder if there is a one round tripartite key exchange.

In 2001, Joux [29] found a way to do exactly this using pairings. In the first round, Alice sends $[a]P$ to both Bob and Charles. Bob sends $[b]P$ to Alice and Charles, and Charles sends $[c]P$ to Alice and Bob. Then all three parties can compute the key $e(P,P)^{abc}$. For example, Alice can compute

$$e([b]P, [c]P)^a = e(P,P)^{abc}.$$

An attacker who wished to find the key would need to find $e(P,P)^{abc}$, given $P, [a]P, [b]P$, and $[c]P$. This is what's known as the *bilinear Diffie-Hellman problem*. Most pairing based cryptosystems rely on this or some similar problem for security.

This simple three party key exchange was one of the first applications of bilinear pairings to cryptography, and stimulated a lot of interest in the area.

## 7.3 Separating DH from DDH

Given points $P, [a]P$, and $[b]P$ on an elliptic curve $E$ defined over a finite field, the *Diffie-Hellman problem*(DH) is to compute $[ab]P$.

Let $P_1, P_2, P_3$, and $P_4$ be points in the subgroup $\langle P_1 \rangle$ of $E(\mathbb{F}_q)$, with $P_2 = [a]P_1$ for some $a$. The *decision Diffie-Hellman problem*(DDH) is to determine if $P_4 = [a]P_3$. If one can solve the Diffie-Hellman problem (which is sometimes called the *computational Diffie-Hellman problem* to distinguish it from the DDH), then one can solve the decision Diffie-Hellman problem as follows. Solve the Diffie-Hellman problem for the triple $P_1, P_2 = [a]P_1, P_3 = [b]P_1$, to get $[ab]P_1$. Note that $[ab]P_1 = [a]([b]P_1) = [a]P_3$. So $P_4 = [a]P_3$ if and only if $P_4 = [ab]P_1$, and we have solved the decision problem. This shows that the decision Diffie-Hellman problem is no harder than the computational Diffie-Hellman

problem. Can we find an example of a group where the decision Diffie-Hellman problem appears (based on known algorithms) to be strictly easier than the Diffie-Hellman problem?

Joux and Nguyen [31] used pairings to find such a group. Both the Tate and Weil pairing will work (when combined with a distortion map), as the key feature needed is bilinearity. If $e(P_1, P_3) \neq 1$, then we compute $e(P_1, P_4)$ and $e(P_2, P_3)$. If these values agree, then $e(P_2, P_3) = e([a]P_1, P_3) = e(P_1, [a]P_3)$, and if $n$ is prime this implies $P_4 = [a]P_3$. Conversely, if $P_4 = [a]P_3$, then clearly $e(P_1, P_4) = e(P_1, [a]P_3) = e([a]P_1, P_3) = e(P_2, P_3)$. Joux and Nguyen showed how to construct elliptic curves where the decisional Diffie-Hellman problem can be solved in polynomial time using pairings, but the computational Diffie-Hellman is provably as hard as the discrete logarithm problem on the curve.

Using Algorithms 2 and 3 of chapter 8, we can construct more examples of curves for which the DDH is "easy", as the following theorem shows.

**Theorem 16** *Let $E$ be an elliptic curve constructed using Algorithm 1, or one of the curves in the appendix. Let $P \in E(\mathbb{F}_q)$ have prime order $n$. Then the decision Diffie-Hellman problem in $\langle P \rangle$ is efficiently solvable.*

The proof was outlined in the paragraphs preceding the statement of the theorem.

## 7.4 Determining group structure

If we know the number of points $N$ of an elliptic curve $E$ over $\mathbb{F}_q$, we can use pairings to determine the group structure. The following theorem from [67] tells us the possibilities.

**Theorem 17** *Let $E(\mathbb{F}_q)$ be an elliptic curve. Then*

$$E(\mathbb{F}_q) \equiv \mathbb{Z}_N \text{ or } \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

*for some integers $n_1, n_2$ with $n_1 n_2 = N$ and $n_1 | n_2$.*

V. Miller has created a random polynomial time algorithm which finds the group structure using the Weil pairing [48].

## 7.5 Identity based encryption

In 1984, Shamir [57] introduced the notion of identity based cryptography. With public key cryptography, if a user Bob wishes to send a message to Alice, he needs to know Alice's public key. How can Bob be sure he has Alice's key, and not that substituted by some malicious attacker? One answer lies in the use of certificates. Some trusted authority can issue a certificate with some form of Alice's identification, along with her public key. Bob can check the trusted authority's signature on the certificate to be confident he knows Alice's key.

Shamir came up with the idea of using some form of Alice's identification for her public key, thereby avoiding the need for a certificate. This could be

her email address, for example. Anyone sending a message to Alice would then know Alice's public key. The notion of identity based encryption extends to identity based signature schemes, identity based key exchanges, etc. It wasn't until 2001 that a practical identity based encryption scheme was created by Boneh and Franklin [4]. We will illustrate a basic version of their scheme.

We need two hash functions,

$$H_1 : \{0,1\}^m \to \langle P \rangle$$

$$H_2 : \mathbb{F}_{q^k} \to \{0,1\}^m$$

where $P$ is a point on an elliptic curve $E(\mathbb{F}_q)$, and $k$ is the embedding degree. If we represent Alice's identification as $ID_A$, then her public key is $K_A = (ID_A)$. A trusted authority with master secret key $s$ gives Alice her private deciphering key $D_A = [s]H_1(K_A)$. The trusted authority has public key $S = [s]P$.

To send her a message $M \in \{0,1\}^m$, Bob computes $Q = H_1(K_A)$ and selects a random integer $r$. He also computes $R = [r]P$ and $c = M \oplus H_2(e(Q,S)^r)$. He sends Alice the pair $(R, c)$.

To decrypt, Alice uses her private key $D_A$ to calculate $c \oplus H_2(e(D_A, R))$. This is equal to

$$c \oplus H_2(e([s]Q, [r]P)) = c \oplus H_2(e(Q,S)^r) = M.$$

Anyone other than Alice wishing to decrypt the message $M$ from $(R, c)$ needs to be able to compute $e(Q,S)^r = e(Q,P)^{rs}$ given $P, Q, S$, and $R$. This requires solving the bilinear Diffie-Hellman problem.

### 7.6 Short signatures

Boneh, Lynn and Shachem ([5]) used pairings to construct a signature scheme with much shorter lengths than other signature schemes. Let $H_1$ be the hash function from the previous section. Alice's private key is a secret integer $r$, and her public key is $R = [r]P$. To sign a message $M$, Alice computes $S = [r]H_1(M)$. Her signature is $S$. Anyone wishing to verify her signature can check if $e(P,S) = e(R, H_1(M))$. This equality holds for a valid signature

$$e(P,S) = e(P, [r]H_1(M)) = e([r]P, H_1(M)) = e(R, H_1(M)).$$

Somebody wishing to forge a signature on $M$ needs to be able to find $S = [r]H_1(M)$, given $P, R$, and $H_1(M)$, which is a Diffie-Hellman problem in $\langle P \rangle$.

## 8 The algorithms

### 8.1 Theory

Recall that to generalize Verheul's theorem, we need an algorithm to create trace zero supersingular curves, as well as an algorithm to find distortion maps. In this section we provide algorithms which do this.

An elliptic curve is said to have *complex multiplication* if its endomorphism ring is larger than $\mathbb{Z}$. Theorem 14 states that elliptic curves over finite fields always have complex multiplication. We will use curves with complex multiplication to obtain supersingular curves.

The key result needed is the Deuring reduction theorem ([14]).

**Theorem 18** *Let $E$ be an elliptic curve defined over a number field with complex multiplication by an order $O$ contained in the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. If $p$ is a good prime which doesn't split in $\mathbb{Q}(\sqrt{-d})$, then the reduction of $E$ mod $p$ is a supersingular curve. If $p$ splits then the reduction of $E$ mod $p$ is ordinary.*

For example, the curve $E : y^2 = x^3 + x$ defined over $\mathbb{Q}$ has complex multiplication because the map

$$(x, y) \rightarrow (-x, iy)$$

is an endomorphism over $\mathbb{Q}(\sqrt{-1})$. A prime $p$ splits in $\mathbb{Q}(\sqrt{-1})$ iff $p \equiv 1 \mod 4$, so we see that $E$ is a supersingular curve over $\mathbb{F}_p$ for any prime $p \equiv 3 \mod 4$. Similarly, by looking at which primes split in $\mathbb{Q}(\sqrt{-3})$ we see that the curve $y^2 = x^3 - 1$ is a supersingular curve over $\mathbb{F}_p$ whenever $p \equiv -1 \mod 6$.

It is well-known that there are 9 imaginary quadratic fields with class number one. These are $\mathbb{Q}(\sqrt{-d})$ for $d$=1, 2, 3, 7, 11, 19, 43, 67, and 163. Since roughly half of all primes split in each $\mathbb{Q}(\sqrt{-d})$, we can use one of these quadratic imaginary fields to create supersingular curves over $\mathbb{F}_p$ for all but a fraction $(\frac{1}{2^9})$ of the primes. In [61], Silverman has a table of elliptic curves defined over $\mathbb{Q}$ with complex multiplication in each of these nine fields. So for a given prime $p$, if we are looking to find a supersingular curve over $\mathbb{F}_p$, then with high probability, we can use one of these curves. Note that if $p > 3$, then the curve will have trace zero by Hasse's theorem.

This doesn't work for all primes, and we would also like to find supersingular curves over arbitrary $\mathbb{F}_q$, not just prime fields. The algorithm of R. Bröker in [7] allows us to find a supersingular curve over a prime field. This curve can then be twisted to get a supersingular curve over an extension field. The input to this algorithm is a finite field $\mathbb{F}_q$, of characteristic $p$. The output is a supersingular curve $\tilde{E}$ such that $\tilde{E}(\mathbb{F}_{q^2})$ is isomorphic to $\mathbb{F}_q^* \times \mathbb{F}_q^*$. For $p = 2$ see chapter 9.

**Algorithm 2 – Finding the Curve**

1. (optional) If $p$ is inert in any of the nine class number one fields, then get $E$ from the appendix. Go to step 6.
2. If $p = 3$ then let $E$ be the curve $y^2 = x^3 + x$. Go to step 6.
3. Find the smallest prime $l \equiv 3 \mod 4$ such that $(\frac{-l}{p}) = -1$.
4. Construct the Hilbert class polynomial $P_K(x) \bmod p$, where $K = \mathbb{Q}(\sqrt{-l})$.
5. Find a root $j$ of $P_K(x)$ in $\mathbb{F}_p$. Then $j$ is the $j$-invariant of our desired $E$, and if we set $a = \frac{27j}{4(1728-j)}$, then $E : y^2 = x^3 + ax - a$ has $j(E) = j$.

6. a) If $f = [\mathbb{F}_q : \mathbb{F}_p]$ is odd, twist $E$ by a quadratic nonresidue $\beta$ in $\mathbb{F}_{p^2}$. That is, $\tilde{E}(\mathbb{F}_{q^2}) : y^2 = x^3 + a\beta^2 x - a\beta^3$.

   b) If $f$ is even, let $\tilde{E}$ be $E$ considered as a curve over $\mathbb{F}_{q^2}$.

We now explain the algorithm and why it is correct. Let $E$ be an elliptic curve over $\mathbb{C}$ with complex multiplication by the maximal order in the field $K = \mathbb{Q}(\sqrt{-l})$. Let $H$ be the Hilbert class field of $K$, which is the maximal abelian unramified extension of $K$. Then $[H : K]$ is the class number $h_K$ of $K$, and $H = K[x]/(P_K(x))$, where $P_K(x)$ is the *Hilbert class polynomial* of $K$. The polynomial $P_K(x)$ is the minimal polynomial for the modular function $j$ of $E$ (see Section 6.3), and is a monic polynomial with integer coefficients.

If we take a prime $p$ that doesn't split in $K$, then the roots of $P_K \bmod p$ are the $j$-invariants of supersingular curves by Deuring's reduction theorem. By Lemma 2.3 of [7], if $d$ is prime, and $d \equiv 3 \mod 4$, then $P_K$ has a root in $\mathbb{F}_p$. This shows that the elliptic curve $E$ we obtain in step 5 of Algorithm 2 is a supersingular curve over $\mathbb{F}_p$.

The choice of $l$ to be the smallest such prime is important. For the purpose of just finding a non-residue in provably polynomial expected run time, one just tries random $l < p$. However, the run times of Algorithms 2 and 3 depend crucially on the size of $l$, so we choose it to be as small as possible. An alternative choice could be to choose $l$ so that the class number of $\mathbb{Q}(\sqrt{-l})$ is minimal.

From the classification of supersingular curves given in chapter 2, we see that if $f = [\mathbb{F}_q : \mathbb{F}_p]$ is odd then the trace of $E$ over $\mathbb{F}_q$ is 0. Then as described in chapter 4, the twisted curve over $\mathbb{F}_{q^2}$ is isomorphic to two copies of the multiplicative group of $\mathbb{F}_q^*$. If instead $f$ is even, then first recall that $E(\mathbb{F}_p)$ has trace 0. When we consider $E$ as a curve over $\mathbb{F}_q$, the trace is then $\pm 2\sqrt{q}$, and considered over $\mathbb{F}_{q^2}$ the trace is $-2q$. Thus the output of the algorithm is as desired.

Our second algorithm finds a distortion map for supersingular curves, assuming we know the imaginary quadratic field where they have complex multiplication. In particular, this holds for the curves returned by algorithm 1. If the field of complex multiplication is unknown, Kohel's algorithm [36] could be used to find it, but the algorithm runs in exponential time.

The following algorithm is adapted from an algorithm of Stark [62]. The input is a supersingular elliptic curve $E(\mathbb{F}_q)$, $q = p^f$, with complex multiplication by $\mathbb{Q}(\sqrt{-l})$. We need $l$ coprime to $p$, and we'll assume $l$ is odd, though $l$ need not be prime. The output is a distortion map for the subgroup $\langle P \rangle$, where $P$ is any point of prime order $r$, with $r \nmid pl$.

Associated to each elliptic curve over $\mathbb{C}$, there is a function known as the Weierstrass $\wp$ function. For background information on $\wp$, see [33] or [67]. Algorithm 3 uses the power series expansion of $\wp(z)$ to find $D(x)$. All computations are done mod $p$.

**Algorithm 3 – Computing the Distortion Map**

1. Find the series expansion of $\wp(z)$ up to precision $z^{4l}$.

2. Let $T(z) = \wp(-lz)$ up to precision $z^{4l}$.

3. Set $n = -1$, $q_{-2} = 1$, and $q_{-1} = 0$.

4. While the degree of $q_n$ is less than $l - 1$ do:
   a) Define $r$ and $t_{2r}$ by $T(z) = \frac{t_{2r}}{z^{2r}} + ...t_0 + t_2 z^2 + ...$
   b) Let $n = n + 1$ and $a_n = 0$.
   c) While $r \geq 0$ do:
      i) Set $a_n = a_n + t_{2r} z^r$.
      ii) Let $T(z) = T(z) - t_{2r} \wp(z)^r \mod z^{4l}$.
      iii) Re-define $r$ and $t_{2r}$ by $T(z) = \frac{t_{2r}}{z^{2r}} + ... + t_0 + t_2 z^2 + ...$
   d) Let $q_n = a_n q_{n-1} + q_{n-2}$.
   e) If $n = l - 1$ then go to step 5.
   f) Let $T(z) = 1/T(z) \mod z^{4l}$

5. Let $D(x)$ be the polynomial $q_n(x)$

6. Use Vélu's formulae on the polynomial $D(x)$. This gives us an explicit $l$-isogeny $\phi$ (defined over $\mathbb{F}_q$) from $E$ to an isogenous curve $E_1$.

7. Construct an isomorphism $\psi$ from $E_1$ back to $E$. The distortion map is $H = \psi \circ \phi$.

It is well-known that we can compute the expansion of $\wp(z)$ in the following way (see [6]). If the equation for our curve $E$ is $y^2 = x^3 + Ax + B$, then let $c_1 = -A/5$ and $c_2 = -B/7$. We define $c_k$ for $k \geq 3$ by

$$c_k = \frac{3}{(k-2)(2k+3)} \sum_{i=1}^{k-2} c_i c_{k-1-i}.$$

Then

$$\wp(z) = \frac{1}{z^2} + \sum_{i=1}^{\infty} c_i z^{2i}.$$

Algorithm 3 relies on the following theorem. A proof can be found in [11].

**Theorem 19** *Let $E$ be an elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-l})$. Then the weierstrass $\wp$ function satisfies*

$$\wp(\sqrt{-l}z) = \frac{N(\wp(z))}{D(\wp(z))}$$

*where $N(x)$ and $D(x)$ are relatively prime polynomials with the degree of $A(x)$ being equal to $l + 1$, and the degree of $B(x)$ is $l$.*

The polynomial $D(x)$ is computed by using a classical continued fraction expansion algorithm. The rational function $\frac{N(x)}{D(x)}$ is the same as that arising from Vélu's formula in section 5.2, and as shown there, the polynomial $D(x)$ allows us to easily compute $\frac{N(x)}{D(x)}$.

The isomorphism from $E_1$ back to $E$ is easily computed from the coefficients in the equations of the curves. Indeed, if $E$ is the curve $y^2 = x^3 + Ax + B$, and $E_1$ is given by $y^2 = x^3 + A_1x + B_1$, then the isomorphism $\psi : E_1 \to E$ is given by

$$\psi(x, y) \to (\mu^2 x, \mu^3 y),$$

where $\mu$ satisfies

$$\begin{aligned} \mu^4 &= A/A_1 && \text{if } A_1 \neq 0 \\ \mu^6 &= B/B_1 && \text{if } B_1 \neq 0. \end{aligned}$$

When $\mu \notin \mathbb{F}_q$ then given $P \in E(\mathbb{F}_q)$, we see $H(P) \notin \langle P \rangle \subseteq E(\mathbb{F}_q)$. So it is easy to verify that $H$ is a distortion map for $P$ in this case. Even if $\mu \in \mathbb{F}_q$, we can still show $H$ is a distortion map. We'll need the Deuring lifting theorem [14].

**Theorem 20** *Given an elliptic curve $E$ defined over a finite field, and an endomorphism $\alpha$ of $E$, then there exists an elliptic curve $\tilde{E}$ defined over a finite extension $K$ of $\mathbb{Q}$ and an endomorphism $\tilde{\alpha}$ of $\tilde{E}$ such that $E$ is the reduction of $\tilde{E}$ by some prime ideal of the ring of integers of $K$, and $\alpha$ is the reduction of $\tilde{\alpha}$.*

By our construction in Algorithm 3, $\tilde{E}$ has complex multiplication by an order $O \subseteq \mathbb{Q}(\sqrt{-l})$. If $\alpha$ is an element of $O$, then the size of the kernel of $\alpha$ is equal to $N(\alpha)$. Note the only elements in $O$ with norm $l$ are $\pm\sqrt{-l}$. From this it follows that since our map $H$ has a kernel of size $l$, that on $E$ we have $H^2 = -l$. That is, $H(H(P)) = [-l]P$, for all points $P$ on $E$. For $H$ to be a distortion map, we need a point $P \in E(\mathbb{F}_q)$ such that $H(P) \notin \langle P \rangle$. Theorem 6.1 of [23] proves that as long as $P$ has prime order $r > 3$ such that $r \nmid pl$, then $H$ is a distortion map for $P$.

We remark that there is are other ways to find the polynomial $D(x)$. In [15], Elkies describes a way to compute $D(x)$ by parameterizing modular curves. Elkies' methods are not organized into an actual algorithm. To use his ideas, one also needs a nice parameterization of the modular curve $\mathrm{X}_0(l)$, which may not be easy to find. Elkies estimates that the complexity of his technique is roughly $\tilde{O}(l^4)$ bit operations, although he emphasizes that no rigorous analysis has been done. In comparison, the algorithm given in this paper to find $D(x)$ is also $\tilde{0}(l^4)$ bit operations, but is much easier to implement.

Another way is to use torsion polynomials. If we wish to find an $l$-isogeny, we first compute $\Phi_l$, the $l$-th torsion polynomial of $E$. The factorization of $\Phi_l$ will usually yield an irreducible factor $g(x)$ of degree $\frac{l-1}{2}$. Then $D(x) = g(x)^2$. This method is less efficient than Algorithm 3, but when $l$ is small the difference is negligible. It also has the advantage that finding torsion polynomials and factoring polynomials are both standard computations already programmed in

most computer software packages. We also note that we can use this method to sometimes find simpler distortion maps. This is possible when there are elements of norm smaller than $l$ in the ring of integers of $\mathbb{Q}(\sqrt{-l})$. An element with norm $m < l$ will yield an $m$-isogeny, which by Vélu will have a simpler equation than the distortion map we get from algorithm 3. For example, when $l = 11$, the element $\alpha = \frac{1+\sqrt{-11}}{2}$ has norm 3, so we can find a 3-isogeny. Instead of factoring the torsion polynomial $\Phi_{11}(x)$, we would instead factor $\Phi_3(x)$, to obtain $g(x)$, which would be a degree 1 polynomial, rather than a degree 5 polynomial. This factor $g(x)$ will typically be defined over an extension field.

In chapter 11, we'll give examples using both algorithms. We also applied Algorithm 2 to the curves with complex multiplication in a quadratic imaginary field of class number one. This gives 9 explicit curves with distortion maps. If $p$ is the characteristic of $\mathbb{F}_q$, then unless $p$ splits in all nine fields, we can use these curves with their distortion maps. The distortion maps are listed in the appendix. We can use these for all but a small fraction of primes $p$.

We could carry this approach further, obtaining explicit curves and distortion maps for the twenty fields with class number 2. This is possible as the Hilbert class polynomial $P_K$ is a quadratic, and we can find the roots of $P_K$. We give an example of how to do this in chapter 11. However the equations become more complicated as the class number rises. For imaginary quadratic fields $K$ with class numbers higher than 2, one either needs a root of the Hilbert class polynomial (which has degree 3 or more), or an equation of an elliptic curve defined over a number field which has complex multiplication in $K$. Both problems seem to be difficult, and this technique would only be needed for the primes which split in all twenty nine of the fields with class numbers 1 and 2. For such a prime one can use Algorithms 2 and 3 to find a curve and distortion map.

## 8.2 Complexity analysis

Let us analyze the complexity of our algorithms. We will use $\tilde{O}$-notation, which means that terms which are of logarithmic size in the main terms are ignored. We start with the algorithm to construct supersingular curves. We are assuming that the characteristic $p$ of our field satisfies $p > 2$. For $p = 2$ see chapter 9.

Step 3 requires the computation of a quadratic non-residue mod $p$. Assuming the generalized Riemann Hypothesis (GRH), we can find a prime $l$ congruent to 3 mod 4 with $\left(\frac{-l}{p}\right) = -1$ with $l \leq 2(\log p)^2$, see [37], [1]. Without the GRH, the best bound is due to Burgess ([8]), who proved that there is an $l$ with $l \leq p^{\frac{1}{4\sqrt{e}}}(\log p)^2$. Heuristically, we expect roughly one half of the primes to be non-residues, so in practice we expect $l$ to be very low for most primes $p$. As there are 24 primes less than 200 congruent to 3 mod 4, we could expect that for roughly all but $\frac{1}{2^{24}}$ of the primes, we will have $l < 200$.

If one is not content with an estimate for $l$ that heuristically holds for all but a very small proportion of primes (namely, a constant bound on $l$), then one can get a bound on $l$ heuristically that holds for any $p$. This bound is no

longer constant, but it's better than the provable bound using the GRH.

For large $x$ and some constant $c$, consider the set

$$\left\{\text{primes } p < x \quad \middle| \quad \left(\frac{-j}{p}\right) = 1 \text{ for all primes } j \equiv 3 \bmod 4 \text{ with } j < c \log x \log\log x\right\}.$$

Heuristically, this set should have cardinality approximately $\pi(x)\frac{1}{2^{\pi(c\log x \log\log x)/2}}$, and if we take $c > \frac{2}{\log 2}$, then for large $x$, this is asymptotically $\ll 1$. This follows as $\pi(c \log x \log\log x)$ is easily seen to be asymptotic to $c \log x$. Hence, for large $x$, there is a high probability the set is empty. Thus heuristically we expect $l$ to be bounded by $O(\log p \log\log p) = \tilde{O}(\log p)$. The remainder of the complexity analysis relies heavily on which estimate we use for $l$.

We next examine the cost of computing the Hilbert class polynomial $P_K$, where $K = \mathbb{Q}(\sqrt{-l})$. By [3], $P_K$ can be computed in $\tilde{O}(l)$ bit operations. Assuming the GRH, $l = O((\log p)^2)$, and the complexity is $\tilde{O}((\log p)^2)$ bit operations. Again, as $l$ will typically be small, $P_K$ could be computed and stored in a table, say, for all $l < 200$, and this would be sufficient for most primes. In fact, such a table exists for all $l < 10^7$ [35].

Step 5 requires us to find a root of $P_K$ in $\mathbb{F}_p$, which it has by construction. Root finding is a special case of factoring polynomials over $\mathbb{F}_p$, and we will discuss how we get the complexity estimate when we discuss our third algorithm. If $h$ is the class number of $K$, the root $j$ can be found probabilistically with an expected run time of $\tilde{O}(h(\log p)^3)$ bit operations with a chance of failure less than $\frac{1}{2^r}$, where $r$ is the number of roots in $\mathbb{F}_p$. We can run the algorithm $k$ times so that the failure probability is less than $\frac{1}{2^{rk}}$. If $\delta > 0$ is given, then if we run the algorithm $\frac{-\log\delta}{r\log 2}$ times, then the chance of failure is less than $\delta$. The Brauer-Siegel theorem tells us that $h = O(\sqrt{\text{disc}(K)}) = O(\sqrt{l})$. So under the GRH, $h = O(\log p)$, and the complexity is $\tilde{O}((\log p)^4)$ bit operations.

Finally, if we need to twist the curve produced to get another trace, then this can be done by simple field arithmetic. The cost of this is negligible when compared with the rest of the algorithm.

If we do not assume the GRH, then we have an exponential algorithm. With the GRH assumption, the total algorithm has an expected run time of $\tilde{O}((\log q)^4)$ bit operations . Under heuristic assumptions, our non-residue $l$ will be even smaller, and the algorithm will be very quick.

We next look at the algorithm to compute distortion maps. In step 1 we find the series expansion of $\wp(z) = \frac{1}{z^2} + \sum_{i=1}^{\infty} c_i z^{2i}$. Using the recurrence given, we can find $c_1$ through $c_l$ in $O(l^2(\log q)^2)$ bit operations. The time for steps 2 and 3 are certainly less than this. Step 4 is the dominant part of the algorithm, and part f) is the most time consuming step. Inverting $T(z) \bmod z^{2l}$ can be done in time $O(l^2(\log q)^2)$, so the total time for this step is $O(l^3(\log q)^2)$ bit operations. The multiplications in part d) are also $O(l^3)$. Part c) requires calculating $\wp(z)^r$, where $r$ is bounded by $2l - 2$. Thus the complexity of this part is at most $O(l^3(\log q)^2)$ bit operations. All of these computations with power series can be done by standard algorithms (see [24] or [58]). Assuming the GRH, step 4 requires $O((\log q)^8)$ bit operations.

The remaining steps in computing the distortion map involve performing arithmetic with polynomials in $\mathbb{F}_q[x]$ or $\mathbb{F}_{q^2}[x]$, which can be done in time $\tilde{O}(l^2(\log q)^2)$. Under the GRH, this is $\tilde{O}((\log q)^6)$.

Heuristically, the algorithm to construct distortion maps should be efficient. This is because everything depends on the quadratic non-residue $l$ we find in the first algorithm. As explained before, we expect $l$ to be small. It should also be noted that our estimates are based on the simple quadratic-time algorithms for both multiplying polynomials and field operations. Using faster multiplication techniques would obviously give even lower complexity bounds.

Overall, we find that we can construct a suitable elliptic curve and distortion map in an expected run time of $\tilde{O}((\log q)^8)$ bit operations, assuming the GRH. Heuristically we also expect the run time to be much lower than the given bound. Indeed, if $l = O(\log q)$ (or $l = O(1)$), then the algorithm should run in about $\tilde{O}((\log q)^5)$ (or $\tilde{O}(\log q)^2$) bit operations.

## 8.3 Timings

Overall, we find that we can construct a suitable elliptic curve and distortion map in an expected run time of $\tilde{O}((\log q)^{10})$ bit operations, assuming the GRH. Recall that we need to use these algorithms only if our explicit ones do not work. Roughly speaking, the 9 examples from class number 1 imaginary quadratic fields should work for all but $\frac{1}{2^9}$ of the primes. Using the same technique, we can construct 20 more examples from class number 2 imaginary quadratic fields, which would cover all but roughly $\frac{1}{2^{20}}$ of the remaining primes. Heuristically we also expect the run time to be much lower than the given bound. Indeed, if $l = O(\log q)$ (or $l = O(1)$), then the algorithm should run in about $\tilde{O}((\log q)^6)$ (or $\tilde{O}(\log q)^3$) bit operations.

Using V. Shoup's ntl library in SAGE (see [63]), we time some computations involving our algorithms. This was done on a 64 bit Dual Core AMD Opteran Processor 865, with clock cycle 1.8 GHz. We do not count the time needed to initialize the finite fields. We can assume that anybody who is interested in solving the discrete log or Diffie-Hellman problem in $\mathbb{F}_p$ has already done so. The time needed to run Algorithm 2 is very small. Indeed, for $p$ as large as $10^{600}$, the algorithm took around 0.1 seconds on average. The potential bottleneck is computing the Hilbert class polynomial $P_K$, and finding a root. When the non-residue $l$ is small, this is very fast.

For Algorithm 3, we include a table of run-times to find $D(x)$, which is the most time consuming step. The parameters are the degree $l$ of the isogeny, and the prime $p$, where the supersingular curve is defined over $\mathbb{F}_p$.

Note that the algorithm appears to run in time $O(l^2)$ for a fixed $p$. For comparison purposes, we also look at the time required to find the distortion map by factoring the $l$-th torsion polynomial, $\Phi_l$. The most time consuming step is in factoring $\Phi_l$, and we include the results in Table 3. We see that for small $l$, this technique is faster than Algorithm 3.

Table 2: Run times to find $D(x)$ using Algorithm 3

| | $p \approx 10^{50}$ | $p \approx 10^{100}$ | $p \approx 10^{200}$ | $p \approx 10^{400}$ |
|---|---|---|---|---|
| $l = 10$ | .8 s | .85 s | .94 s | 1.11 s |
| $l = 20$ | 3.07 s | 3.28 s | 3.65 s | 4.44 |
| $l = 40$ | 12.6 s | 13.2 s | 14.8 s | 18.0 s |
| $l = 80$ | 51 s | 54 s | 61 s | 75 s |
| $l = 160$ | 220 s | 242 s | 283 s | 358 s |

Table 3: Run times to factor torsion polynomials

| | $p \approx 10^{10}$ | $p \approx 10^{20}$ | $p \approx 10^{30}$ | $p \approx 10^{40}$ |
|---|---|---|---|---|
| $l = 10$ | .02 s | .05 s | .07 s | .12s |
| $l = 20$ | .4 s | .5 s | .8 s | 1.1 s |
| $l = 30$ | 3.5 s | 3.5 s | 5 s | 7 s |
| $l = 40$ | 18 s | 19 s | 25 s | 31 s |
| $l = 50$ | 63 s | 67 s | 89 s | 107 s |

# 9 The Characteristic 2 case

When our finite field is of characteristic 2, we can find explicit equations for supersingular curves, as well as for their distortion maps.

Note that over $\mathbb{F}_2$, we can easily count the number of points on the curves:

1. $y^2 + y = x^3$
2. $y^2 + y = x^3 + x$
3. $y^2 + y = x^3 + x + 1$.

The first curve has 3 points, the second 5 points, and the third has only the point at infinity. All three of these curves are thus supersingular over $\mathbb{F}_2$. The traces of the three curves are 0,$-2$, and 2 respectively. It's easy to calculate that over $\mathbb{F}_{2^m}$, these curves have traces 0, $(-1+i)^m+(-1-i)^m$, and $(1+i)^m+(1-i)^m$. In fact, up to isomorphism, these are the only 3 supersingular curves over $\mathbb{F}_{2^m}$ when $m$ is odd. For curves over $\mathbb{F}_{2^m}$, with $m$ even, there are 7 different curves up to isomorphism. For a proof of these statements, see [44]. We list the results in the table below, writing $\mathbb{F}_q = \mathbb{F}_{2^m}$.

Here (for $m$ even) we need $\gamma$ a non-cube in $\mathbb{F}_{2^m}$, $\alpha, \beta, \delta, \omega \in \mathbb{F}_{2^m}$ such that $\mathrm{Tr}(\frac{\alpha}{\gamma^2}) = 1$, $\mathrm{Tr}(\frac{\beta}{\gamma^4}) = 1$, $\mathrm{Tr}(\omega) = 1$, and $\mathrm{Te}(\delta) \neq 0$, where

$$\mathrm{Te} : \mathbb{F}_{2^m} \to \mathbb{F}_4$$

and

$$\mathrm{Te}(x) = x + x^{2^2} + x^{2^4} + ... + x^{2^{m-2}}.$$

Table 4: Isomorphism class representatives of supersingular curves over $\mathbb{F}_{2^m}$ (see [44])

| Curve $E$ | $m$ | $\#E(\mathbb{F}_q)$ | Group Structure of $E(\mathbb{F}_q)$ | $k$ |
|---|---|---|---|---|
| $y^2+y=x^3$ | $m \equiv 1,3,5,7 \mod 8$ | $q+1$ | cyclic | 2 |
| $y^2+y=x^3+x$ | $m \equiv 1,7 \mod 8$ | $q+1+\sqrt{2q}$ | cyclic | 4 |
| | $m \equiv 3,5 \mod 8$ | $q+1-\sqrt{2q}$ | cyclic | 4 |
| $y^2+y=x^3+x+1$ | $m \equiv 1,7 \mod 8$ | $q+1-\sqrt{2q}$ | cyclic | 4 |
| | $m \equiv 3,5 \mod 8$ | $q+1+\sqrt{2q}$ | cyclic | 4 |
| $y^2+y=x^3+\delta x$ | $m \equiv 0,2 \mod 4$ | $q+1$ | cyclic | 2 |
| $y^2+y=x^3$ | $m \equiv 0 \mod 4$ | $q+1-2\sqrt{q}$ | $(\mathbb{Z}/(\sqrt{q}-1)\mathbb{Z})^2$ | 1 |
| | $m \equiv 2 \mod 4$ | $q+1+2\sqrt{q}$ | $(\mathbb{Z}/(\sqrt{q}+1)\mathbb{Z})^2$ | 1 |
| $y^2+y=x^3+\omega$ | $m \equiv 0 \mod 4$ | $q+1+2\sqrt{q}$ | $(\mathbb{Z}/(\sqrt{q}+1)\mathbb{Z})^2$ | 1 |
| | $m \equiv 2 \mod 4$ | $q+1-2\sqrt{q}$ | $(\mathbb{Z}/(\sqrt{q}-1)\mathbb{Z})^2$ | 1 |
| $y^2+\gamma y=x^3$ | $m \equiv 0 \mod 4$ | $q+1+\sqrt{q}$ | cyclic | 3 |
| | $m \equiv 2 \mod 4$ | $q+1-\sqrt{q}$ | cyclic | 3 |
| $y^2+\gamma y=x^3+\alpha$ | $m \equiv 0 \mod 4$ | $q+1-\sqrt{q}$ | cyclic | 3 |
| | $m \equiv 2 \mod 4$ | $q+1+\sqrt{q}$ | cyclic | 3 |
| $y^2+\gamma^2 y=x^3$ | $m \equiv 0 \mod 4$ | $q+1+\sqrt{q}$ | cyclic | 3 |
| | $m \equiv 2 \mod 4$ | $q+1-\sqrt{q}$ | cyclic | 3 |
| $y^2+\gamma^2 y=x^3+\beta$ | $m \equiv 0 \mod 4$ | $q+1-\sqrt{q}$ | cyclic | 3 |
| | $m \equiv 2 \mod 4$ | $q+1+\sqrt{q}$ | cyclic | 3 |

The map Tr is the absolute trace down to $\mathbb{F}_2$.

It is therefore simple to find trace 0 supersingular curves over $\mathbb{F}_{2^m}$. If $m$ is odd, then $y^2+y=x^3$ will suffice. If $m$ is even, then if we find a $\delta$ with $\mathrm{Te}(\delta) \neq 0$, the curve $y^2+y=x^3+\delta x$ works. For a random choice of an element $x$ in $\mathbb{F}_{2^m}$, we have $\mathrm{Te}(x) \neq 0$ three quarters of the time, so finding an appropriate $\delta$ will not be hard.

When the characteristic is two, the curves we need distortion maps for are of the form

$$y^2+y=x^3+B,$$

where $B$ is an element of $\mathbb{F}_{2^m}$, possibly zero. A distortion map is given by

$$H(x,y)=(x+s+1, y+sx+s)$$

where $s$ satisfies $s^2+s+1=0$.

# 10 Proof of the Main Theorem

We end with the proof of the generalized version of Verheul's theorem:

**Theorem 21** *Let $\mathbb{F}_q$ be an arbitrary finite field. Then there is an elliptic curve such that $\tilde{E}(\mathbb{F}_{q^2})$ is a product of two cyclic groups of order $q-1$.*

*Given such a curve, let $P$ be a generator for one of the cyclic subgroups of order $q-1$. Under the MOV embedding, we have an isomorphism from $\langle P\rangle$ to $\mathbb{F}_q^*$. If an efficiently computable isomorphism can be found from $\mathbb{F}_q^*$ to $\langle P\rangle$, then the Diffie-Hellman problem can be efficiently solved in both $\mathbb{F}_q^*$ and $\langle P\rangle$.*

**Proof** If the characteristic $p$ of $\mathbb{F}_q$ is greater than 2, then using Algorithm 2 in section 8, we can find $E$ as desired. If $p = 2$ then we can find $E$ as described in section 9. The fact that $\tilde{E}(\mathbb{F}_{q^2})$ is a product of two cyclic groups of order $q-1$ follows from the classification of supersingular curves given in Section 2. Let $S$ be any point that together with $P$ generates the whole group. Then we can define the MOV embedding by

$$\hat{e} : \langle P\rangle \to \mathbb{F}_q^* \text{ where } \hat{e}(Q) = e_{q-1}(Q, S),$$

where $e_{q-1}$ is the Weil pairing. By Corollary 1 of Section 5, $\zeta = \hat{e}(P)$ is a generator for $\mathbb{F}_q^*$, so $\hat{e}$ is onto. The fact that $\hat{e}$ is a homomorphism follows from the bilinearity of $e_{q-1}$. As $\hat{e}$ is thus a surjective homomorphism between two finite groups of the same order, we have that $\hat{e}$ is an isomorphism.

Let $I$ be an efficiently computable isomorphism from $\mathbb{F}_q^*$ to $\langle P\rangle$. Let $H$ be a distortion map on $\tilde{E}$, which we can find efficiently using Algorithm 3 (see Section 8). A distortion map means that for any point $Q$, $Q$ and $H(Q)$ are linearly independent. Set

$$\gamma = e_{q-1}(I(\zeta), H(I(\zeta))),$$

from which it follows that $\gamma$ is a generator for $\mathbb{F}_q^*$. Now suppose we are given $\zeta, \zeta^a$, and $\zeta^b$. We calculate

$$e_{q-1}(I(\zeta^a), H(I(\zeta^b))) = e_{q-1}([a]I(\zeta), [b]H(I(\zeta))) = e_{q-1}(I(\zeta), H(I(\zeta)))^{ab} = \gamma^{ab}.$$

We have solved the weak Diffie-Hellman problem. Thus, by Lemma 1, we can efficiently find $\zeta^{ab}$, solving the Diffie-Hellman problem.

Given that we can efficiently solve the DHP in $\mathbb{F}_q^*$, we can also efficiently solve the DHP in $\langle P\rangle$. Given $[a]P$ and $[b]P$, notice that $\hat{e}(P), \hat{e}([a]P)$, and $\hat{e}([b]P)$ are the input for a DHP in $\mathbb{F}_q^*$. By what we just showed, we can find $\hat{e}([ab]P)$. Then note that $I(\hat{e}(P))$ is a generator of $\langle P\rangle$, and we can compute $[ab]I(\hat{e}(P)) = I(\hat{e}([ab]P))$. This solves the weak Diffie-Hellman problem in $\langle P\rangle$, and so by Lemma 1, we can efficiently solve the DHP in $\langle P\rangle$ also. □

# 11 Examples

## 11.1 Using the algorithms to create supersingular curves and distortion maps

Let's first try various random primes $p$, and come up with supersingular curves over $\mathbb{F}_p$ with computable distortion maps. This shows that if a homomorphism

inverting the MOV embedding existed, then the Diffie-Hellman problem in $\mathbb{F}_p$ would be efficiently solvable.

Let's take $p = 9013$. We first check our 9 explicit curves and see if $p$ satisfies any of the conditions. It actually satisfies three of them, $(\frac{2}{p}) = (\frac{43}{p}) = (\frac{163}{p}) = -1$. So there are three curves we could use.

The first is $E := y^2 = x^3 - \frac{10}{3}x - \frac{56}{27}$, or over $\mathbb{F}_{9013}$ we have

$$E : y^2 = x^3 + 3001x + 1667$$

Working in our finite field, we also have:

$$\phi : (x, y) \to (X, Y) = (\frac{x^2 + 6010x + 2}{x + 6010}, y\frac{x^2 + 3007x + 5007}{(x + 6010)^2})$$

$$\psi : (X, Y) \to= (-\frac{X}{2}, -\frac{Y}{2\sqrt{-2}}).$$

Combining these two, we have the distortion map $H = \psi \circ \phi$, or

$$D(x, y) = (4506\frac{x^2 + 6010x + 2}{x + 6010}, y\frac{4506}{\sqrt{-2}}\frac{x^2 + 3007x + 5007}{(x + 6010)^2}).$$

This distortion map comes from a 2-isogeny.

If instead we use Algorithm 2, then we find we can use $l = 23$. The Hilbert class polynomial for $K = \mathbb{Q}(\sqrt{-23})$ is $P_K(x) = x^3 + 3719 * x^2 + 2158 * x + 7102$. A root is $j = 6673$, and the elliptic curve is $E := y^2 = x^3 + 7713x + 1300$. $E$ is a supersingular curve over $\mathbb{F}_{9013}$ with trace 0.

We now use Algorithm 3 to create a distortion map for $E := y^2 = x^3 + 7713x + 1300$. We calculate

$$\wp(z) = z^{-2} + 260z^2 + 3677z^4 + 1503z^6 + 6730z^8 + 8879z^{10} + ...$$

and

$$\wp(\sqrt{-23}z) = z^{-2} + 260z^2 + 3677z^4 + 1503z^6 + 6730z^8 + 8879z^{10} + ...$$

Using the continued fraction expansion algorithm we find

$$\begin{aligned} D(x) = x^{22} &+ 1573x^{21} + 3278x^{20} + 3448x^{19} + 3210x^{18} + 2608x^{17} + 5255x^{16} \\ &+ 2652x^{15} + 3072x^{14} + 2934x^{13} + 2613x^{12} + 4240x^{11} + 6711x^{10} \\ &+ 7484x^9 + 1305x^8 + 5411x^7 + 3488x^6 + 4304x^5 + 857x^4 \\ &+ 7613x^3 + 7184x^2 + 455x + 534. \end{aligned}$$

Using Vélu's formulae, this defines an isogeny to the curve $E_1 := y^2 = x^3 + 6301x + 715$. We can construct an isomorphism back to $E$ using $\mu = \sqrt{3135}$.

## 11.2 Example of constructing a distortion map by factoring torsion polynomials

Let $p = 18313$. We use our algorithm to first construct a supersingular elliptic curve over the finite field with 18313 elements. The first prime $l$ congruent to 3 mod 4 such that $\left(\frac{-l}{18313}\right) = -1$ is $l = 23$. The Hilbert polynomial for $K = \mathbb{Q}(\sqrt{-23})$ reduced mod $p$ is $P_K = x^3 + 12280x^2 + 3521x + 14225$, which has a root $j = 12735$. Then setting $a = \frac{27j}{4(1728-j)} = 3964$, the elliptic curve is

$$E : y^2 = x^3 + 3964x - 3964$$

which is supersingular over $\mathbb{F}_{18313}$. We now want to find a 23-isogeny. So we compute the division polynomial $\Phi_{23}$, and find a degree 11 factor

$$\begin{aligned} g(x) = x^{11} &+ 6810x^{10} + 14200x^9 + 4046x^8 + 14378x^7 + 1604x^6 + 9479x^5 \\ &+ 631x^4 + 7787x^3 + 13918x^2 + 2644x + 9822. \end{aligned}$$

The roots of the polynomial $g(x)$ are the $x$-coordinates of 22 points of $E$ (2 points for each x-value), which, along with the point at infinity, give us the kernel of a 23-isogeny.

Let's try some finite fields of prime power order. Let's say we want to run our algorithms over $\mathbb{F}_{541^5}$. The only possible trace for a supersingular curve is $t = 0$. We first use Algorithm 2 to create a supersingular curve over $\mathbb{F}_{541}$. We see that we have $l = 11$, and our curve is $E : y^2 = x^3 + 105x + 436$. Considered over $\mathbb{F}_{541^5}$, this curve has a trace of 0. We can represent $\mathbb{F}_{541^5}$ by $\mathbb{F}_{541}(\theta)$, where $\theta^5 + 3\theta - 2 = 0$. We find a degree 5 factor of $\Phi_{11}(x)$

$$g(x) = x^5 + 225x^4 + 183x^3 + 121x^2 + 165x + 170.$$

By Vélu's formula, $g$ determines an 11-isogeny.

Now let's try an extension of even degree. Let's keep $p = 541$, and work over $\mathbb{F}_{541^4}$. We use Algorithm 2 to create a supersingular elliptic curve with trace $t = -2 * 541^2 = -585362$. We'll represent $\mathbb{F}_{541^4}$ as $\mathbb{F}_{541}(\theta)$, where $\theta^4 + 6\theta^2 + 333\theta + 2 = 0$. Then we have

$$E : y^2 = x^3 + 105\theta^2 x + 436\theta^3.$$

Then we again want a degree 5 factor of $\Phi_{11}(x)$

$$\begin{aligned} g(x) = x^5 &+ (144\theta^3 + 369\theta^2 + 429\theta + 369)x^4 + (494\theta^3 + 422\theta^2 + 400\theta + 261)x^3 \\ &+ (461\theta^3 + 373\theta^2 + 494\theta + 429)x^2 + (473\theta^3 + 81\theta^2 + 257\theta + 467)x \\ &+ 387\theta^3 + 518\theta^2 + 388\theta + 450 \end{aligned} .$$

Vélu's formula can be used to explicitly write down the isogeny by performing some simple calculations.

## 11.3 Example of constructing an explicit curve and distortion map from an imaginary quadratic field with class number 2

The field $K = \mathbb{Q}(\sqrt{-5})$ has class number 2. The Hilbert class polynomial is

$$P_K = x^2 - 1264000x - 681472000$$

It has roots $632000 \pm 282880\sqrt{5}$. If we let $a = \frac{27j}{4(1728-j)}$ for one of the roots $j$, then $E : y^2 = x^3 + ax - a$ is a supersingular elliptic curve over $\mathbb{F}_p$, with complex multiplication in $K$, whenever $\left(\frac{-5}{p}\right) = -1$. The desired curve is:

$$E : y^2 = x^3 - (\frac{1461375}{349448} + \frac{805545}{698896}\sqrt{5})x + (\frac{1461375}{349448} + \frac{805545}{698896}\sqrt{5})$$

.

For example, $(\frac{-5}{31}) = -1$ and $(\frac{5}{31}) = 1$. Then $E$ over $\mathbb{F}_{31}$ reduces to be $y^2 = x^3 + 25x - 25$, and has trace zero.

If we try this with $p = 37$, where both 5 and -5 are non-residues, then we find that $E$ becomes $y^2 = x^3 + (34 + 31\sqrt{5})x - (34 + 31\sqrt{5})$, which is supersingular over $\mathbb{F}_{37^2}$ with trace -74.

We could also twist $E$ to make its equation a bit simpler. The twisted curve is $\widetilde{E} : y^2 = x^3 + au^2x - au^3$, where $u$ is in $\mathbb{Q}(\sqrt{5})$. Taking $u = 836/3$, we get $\widetilde{E} : y^2 = x^3 - (324750 + 24942060\sqrt{5})x + (324750 + 24942060\sqrt{5})$.

We can create a distortion map for $E$. Using Algorithm 3, we find $D(x)$. For reasons of space, we only list $g(x)$, where $D(x) = g(x)^2$. Since $K = \mathbb{Q}(\sqrt{-5})$, we look at the 5-torsion polynomial of $E$.

$$\begin{aligned}
g(x) = x^{12} &+ \left(-309281544\sqrt{5} - 4026900\right)x^{10} + \left(1895596560\sqrt{5} + 24681000\right)x^9 \\
&+ \left(-340197227370000\sqrt{5} - 65323382203390500\right)x^8 \\
&+ \left(-777593662560000\sqrt{5} - 149310587893464000\right)x^7 \\
&+ \left(4655457705992367657240000\sqrt{5} + 1818280411323606090360000\right)x^6 \\
&+ \left(-10800661879706310261936000\sqrt{5} - 4218414018276405258000000\right)x^5 \\
&+ \left(-25195658409010904492768032800000\sqrt{5} - 24193440548356635395964659025000\right)x^4 \\
&+ \left(16125163778236953775050144000000\sqrt{5} + 15483801928450038555943220400000\right)x^3 \\
&+ \left(24140642852996814231741259840419900000000\sqrt{5} + 15711462595865985153678434414922300000\right)x^2 \\
&+ \left(-48281285673742804324853223334865400000000\sqrt{5} - 31422894224127919457209951131667800000\right)x \\
&+ 94056372835102842500597474786589600012000000\sqrt{5} + 60221941999119898057627340028132504241962000
\end{aligned}$$

which determines a 25-isogeny. We can make it explicit using Vélu's formulae, but we do not display it here. We also can easily find an isomorphism back

to $E$ to create the distortion map. These equations simplify over a finite field. For example, working over $\mathbb{F}_{31}$, we get that $g(x) = x^2 + 5x + 8$. By Vélu, we determine that the isogeny is

$$D = \psi \circ \phi$$

with

$$\phi(x,y) = \left( \frac{x^5 + 10x^4 + 9x^3 + 24x + 3}{(x^2+5x+8)^2}, y\frac{x^6 + 15x^5 + 7x^4 + 24x^3 + 20x^2 + 23x + 7}{(x^2+5x+8)^3} \right).$$

and

$$\psi(x,y) = \left(\mu^2 x, \mu^3 y\right),$$

with $\mu = 11 + \sqrt{3}$.

In general, over a class number 2 field $\mathbb{Q}(\sqrt{d})$, if we desire the supersingular curve to be defined over $\mathbb{F}_p$ for some prime $p$, then roughly one fourth of all primes will work. This is because the Hilbert class polynomial will be a quadratic polynomial, so we can get an explicit equation for a curve $E$ defined over some quadratic field $\mathbb{Q}(\sqrt{k})$ with complex multiplication in $\mathbb{Q}(\sqrt{d})$. The condition that $E$ is supersingular and defined over $\mathbb{F}_p$ means we need $(\frac{-d}{p}) = -1$ and $(\frac{k}{p}) = 1$, which happens for roughly a quarter of all primes.

## 11.4 Example of constructing a simpler distortion map by using an element of small norm

At the end of section 8.1, we remarked that in some cases we can find a simpler distortion map. We now provide an example of this. Let $E$ be the curve $y^2 = x^3 - \frac{22}{3}x + \frac{847}{108}$. This curve has complex multiplication by $\mathbb{Q}(\sqrt{-11})$, and is listed in the appendix. If we choose a prime $p$ such that $(\frac{-11}{p}) = -1$, then $E$ will be a supersingular curve mod $p$.

Let's take $p = 19$, and reducing mod $p$ we have $E : y^2 = x^3 + 18x + 14$. We seek an 11-isogeny, and using Algorithm 3 we find $D(x)$:

$$D(x) = x^{10} + 17x^9 + 9x^8 + 9x^7 + 17x^6 + 4x^5 + 5x^4 + 7x^3 + 13x^2 + 4x + 16.$$

By Vélu, the 11-isogeny is then

$$\phi(x,y) = \left( \frac{x^{11} + 17\,x^{10} + 14\,x^9 + 3\,x^8 + 7\,x^7 + 6\,x^6 + 11\,x^5 + 14\,x^4 + 10\,x^3 + 8\,x^2 + 14\,x + 13}{\left(x^5 + 18\,x^4 + 4\,x^3 + 18\,x^2 + 9\,x + 15\right)^2}, \right.$$
$$\left. y\frac{x^{15} + 16\,x^{14} + 10\,x^{13} + 17\,x^{12} + 12\,x^{11} + 15\,x^{10} + 4\,x^9 + 4\,x^8 + 16\,x^7 + 16\,x^6 + 12\,x^5 + 15\,x^4 + 10\,x^3 + 9\,x^2 +}{\left(x^5 + 18\,x^4 + 4\,x^3 + 18\,x^2 + 9\,x + 15\right)^3} \right)$$

The image of $E$ is the curve $y^2 = x^3 + 12x + 5$. Then an isomorphism back to $E$ is given by

$$\psi(x,y) = \left(\mu^2 x, \mu^3 y\right),$$

with $\mu = 2\sqrt{3}$.

To simplify the distortion map $D = \psi \circ \phi$, we note that $\mathbb{Q}(\sqrt{-11})$ has an element of norm 3, namely $\alpha = \frac{1-\sqrt{-11}}{2}$. The 3-torsion polynomial factors as

$$\Phi_3(x) = 3(x^2 + 9x + 10)(x^2 + 10x + 12)$$

over $\mathbb{F}_{19}[x]$. Over $\mathbb{F}_{19^2}[x]$, then a degree 1 factor is

$$g(x) = x + 5 + 3\sqrt{-11}.$$

Using Vélu's formulae, it is easy to check

$$\phi(x,y) = \left( \frac{x^3 + (10 + 6\sqrt{-11})x^2 + (12 + \sqrt{-11})x + 6 + 14\sqrt{-11}}{(x + 5 + 3\sqrt{-11})^2}, \right.$$
$$\left. y\frac{x^3 + \left(15 + 9\sqrt{-11}\right)x^2 + \left(15 + 5\sqrt{-11}\right)x + 15 + 13\sqrt{-11}}{(x + 5 + 3\sqrt{-11})^3} \right),$$

which is much simpler than the earlier $\phi$. The isomorphism $\psi$ is the same as above, with $\mu = \alpha$.

# 12 Future work

An open question is to generalize some form of Verheul's theorem to ordinary curves with low embedding degree. This would require new methods, since Verheul proved that distortion maps for ordinary curves exist only when $k = 1$, and even then only under certain conditions. It would be interesting to find a way to construct distortion maps efficiently for ordinary curves with $k = 1$.

Another area of further research would be to see how these results can be extended to genus 2 curves. There are pairings defined for genus 2 curves, and this would seem to be a good area for exploration.

# 13 Acknowledgements

The author would like to thank Neal Koblitz for suggesting this problem and for many helpful conversations and advice. The author would also like to thank Francois Morain and the anonymous referees for their suggestions which greatly improved this paper.

# A Tables of distortion maps

In this section we give examples of distortion maps. $E$ is the equation of the curve defined over $\mathbb{F}_q$, and the distortion map is $H$.

$q = 2^d$
$E : y^2 + y = x^3 + x$
$H : (x, y) \to (x + s^2, y + sx + t)$ with $s^2 + s + 1 = 0$ and $t^2 + t + s = 0$
$\#E(\mathbb{F}_{2^d}) = 2^d + 1 \pm 2^{(d+1)/2}$
$k = 4$

$q = 3^d$
$E : y^2 = x^3 + x + 1$
$H : (x, y) \to (-x + s, iy)$ with $s^3 + 2s + 2 = 0$ and $i^2 = -1$
$\#E(\mathbb{F}_{3^d}) = 3^d + 1 \pm 3^{(d+1)/2}$
$k = 6$

The following supersingular curves and distortion maps correspond to the nine quadratic imaginary fields $\mathbb{Q}(\sqrt{-d})$ with class number 1. Here $E$ is defined over $\mathbb{F}_p$, where $p$ is a prime satisfying the given congruence.

$d = 1$
$p \equiv 3 \mod 4$
$E : y^2 = x^3 + x$
$H : (x, y) \to (-x, \sqrt{-1}y)$

$d = 2$
$p \equiv 5, 7 \mod 8$
$E : y^2 = x^3 - \frac{10}{3}x - \frac{56}{27}$
$\phi : (x, y) \to (X, Y) = (\frac{x^2 + \frac{4}{3}x + 2}{x + 4/3}, y\frac{x^2 + \frac{8}{3}x - \frac{2}{9}}{(x + \frac{4}{3})^2})$
$\psi : (X, Y) \to (-\frac{X}{2}, -\frac{Y}{2\sqrt{-2}})$
$H = \psi \circ \phi$

$d = 3$
$p \equiv 2 \mod 3$
$E : y^2 = x^3 - 1$
$H : (x, y) \to ((\frac{1}{2} + \frac{\sqrt{-3}}{2})x, y)$

For the remaining examples, we will use the following notation. Each curve $E$ is written in the form $y^2 = x^3 + ax + b$. The distortion map $H$ is given by

$H = \psi \circ \phi$, with

$$\phi : (x, y) \to (X, Y) = \left( \frac{N(x)}{D(x)}, y \left( \frac{N(x)}{D(x)} \right)' \right),$$

and

$$\psi : (X, Y) \to \left( \mu^2 X, \mu^3 Y \right).$$

The constant $\mu$ and a degree $(l-1)/2$ polynomial $g(x)$ will be given, with $D(x) = g(x)^2$. Let $\sigma$ be the negative coefficient of $x^{(l-1)/2-1}$. That is,

$$D(x) = x^{l-1} - \sigma x^{l-2} + ...$$

Then $\frac{N(x)}{D(x)}$ is determined by $D(x)$:

$$\frac{N(x)}{D(x)} = lx - \sigma - (3x^2 + a)\frac{D'(x)}{D(x)} - 2(x^3 + ax + b)\left( \frac{D'(x)}{D(x)} \right)'.$$

To save space, we will list $g(x)$ in place of $D(x)$. We also include an alternate polynomial $\tilde{g}$ defined over $\mathbb{Q}(\sqrt{-d})$, which can be used in place of $g(x)$. This polynomial was obtained by using an element of norm less than $d$.

$d = 7$
$\left(\frac{p}{7}\right) = -1$
$E : y^2 = x^3 - \frac{35}{16}x + \frac{49}{32}$
$g(x) = x^3 - \frac{7}{4}x^2 - \frac{21}{16}x + \frac{91}{64}$
$\mu = \frac{1}{\sqrt{-7}}$

$d = 11$
$\left(\frac{p}{11}\right) = -1$
$E : y^2 = x^3 - \frac{22}{3}x + \frac{847}{108}$
$g(x) = x^5 - \frac{22}{3}x^4 + \frac{55}{9}x^3 + \frac{847}{27}x^2 - \frac{4477}{81}x + \frac{5203}{243}$
$\tilde{g}(x) = x - \frac{11+\sqrt{-11}}{6}$
$\mu = \frac{1}{\sqrt{-11}}$ or $\frac{1+\sqrt{-11}}{6}$ respectively

$d = 19$
$\left(\frac{p}{19}\right) = -1$
$E : y^2 = x^3 - 38x + \frac{361}{4}$
$g(x) = x^9 - 38x^8 + 437x^7 - 1444x^6 - 7942x^5 + 82308x^4 - 274360x^3$
$\quad + 390963x^2 - 130321x - 130321$
$\tilde{g}(x) = x^2 + (-\frac{1}{2}\sqrt{-19} - \frac{19}{2})x + \frac{19}{10}\sqrt{-19} + \frac{209}{10}$
$\mu = \frac{1}{\sqrt{-19}}$ or $\frac{1+\sqrt{-19}}{10}$ respectively

$d = 43$

$\left(\frac{p}{43}\right) = -1$
$E : y^2 = x^3 - 860x + \frac{38829}{4}$
$$\begin{aligned} g(x) = x^{21} &- 516x^{20} + 103630x^{19} - 11413877x^{18} + 778748877x^{17} \\ &- 33769644166x^{16} + 833870847126x^{15} - 2000870379255x^{14} \\ &- 736993488833148x^{13} + 3291127628790512 5x^{12} - 80658135964755 7814x^{11} \\ &+ 12154326008097154232x^{10} - 85488636774415066268x^{9} \\ &- 81946043770446376945x^{8} + 33045266965480421066927x^{7} \\ &- 50722665314356575399414 9x^{6} + 49504436839890318397967 50x^{5} \\ &- 33086781074272853256290845x^{4} + 15040315550259349682403 9509x^{3} \\ &- 43847870157515071061546 6845x^{2} + 71328981520602970654477 4271x \\ &- 44607635619331184098463 0959 \end{aligned}$$
$$\begin{aligned} \tilde{g}(x) = x^5 &+ (-3\sqrt{-43} - 129)x^4 + (\frac{473}{2}\sqrt{-43} + \frac{11997}{2})x^3 \\ &+ (-6880\sqrt{-43} - 131279)x^2 + (\frac{175655}{2}\sqrt{-43} + \frac{2760557}{2})x \\ &- \frac{9154399}{22}\sqrt{-43} - \frac{124110427}{22} \end{aligned}$$
$\mu = \frac{1}{\sqrt{-43}}$ or $\frac{1+\sqrt{-43}}{22}$ respectively

$d = 67$
$\left(\frac{p}{67}\right) = -1$
$E : y^2 = x^3 - 7370x + \frac{974113}{4}$

$$
\begin{aligned}
g(x) = x^{33} &- 2546x^{32} + 2649247x^{31} - 1595291842x^{30} \\
&+ 640348896539x^{29} - 184253611923904x^{28} + 39510232802557718x^{27} \\
&- 6410867835187893127x^{26} + 777889689833250785627x^{25} \\
&- 657536172358628745623 63x^{24} + 266537676456620575513 1386x^{23} \\
&+ 22462467412647317451870 1681x^{22} - 57499834498241686961815567932x^{21} \\
&+ 64983400042084287258120748 14882x^{20} \\
&- 49462429358928875105129828901 7859x^{19} \\
&+ 25957216907649962515771432250558117x^{18} \\
&- 73730093212317336893609169296412 0779x^{17} \\
&- 18673465964555838152080088863869343413x^{16} \\
&+ 39822262567247293696577268580459699345 18x^{15} \\
&- 29724115971114589458520822585423757383 9212x^{14} \\
&+ 15302398104577546280070801623351769789679589x^{13} \\
&- 60382188074868776859266693797499382952229 1592x^{12} \\
&+ 18746518151806629074828169624747001744170025840x^{11} \\
&- 45404918714526646495895792488825297263593927 2305x^{10} \\
&+ 81588998863695736375163976386107961305850153954 62x^{9} \\
&- 90518122926725311334202042278153526052702720644243x^{8} \\
&- 88602715854562730530381942532238574486674897032159x^{7} \\
&+ 29538089522615801104551289493626919072944395256348431x^{6} \\
&- 72919492118884335720520795776832632176695843273183 1809x^{5} \\
&+ 10829332229673947961792361795296021760140934355272515866x^{4} \\
&- 10905266832981050603500128135146509707523453660689925585 5x^{3} \\
&+ 73580371728067420493815509046583947022542551805678830 4413x^{2} \\
&- 30290741823927864373034541413837478303315616546601763899 89x \\
&+ 57808636403559518035412517255829208318210781320700312698 09
\end{aligned}
$$

$$
\begin{aligned}
\tilde{g}(x) = x^8 &+ (-\frac{19}{2}\sqrt{-67} - \frac{1273}{2})x^7 + (4020\sqrt{-67} + 158455)x^6 \\
&+ (-\frac{1424621}{2}\sqrt{-67} - \frac{42237001}{2})x^5 + (\frac{137771899}{2}\sqrt{-67} + \frac{3369394021}{2})x^4 \\
&+ (-\frac{7882598709}{2}\sqrt{-67} - \frac{166760150691}{2})x^3 \\
&+ (133762539672\sqrt{-67} + 2519056747702)x^2 \\
&+ (-\frac{4996435864205}{2}\sqrt{-67} - \frac{85372823611109}{2})x \\
&+ \frac{337215206417115}{17}\sqrt{-67} + \frac{5299018657203644}{17}
\end{aligned}
$$

$\mu = \frac{1}{\sqrt{-67}}$ or $\frac{1+\sqrt{-67}}{34}$ respectively

$d = 163$
$\left(\frac{p}{163}\right) = -1$
$E : y^2 = x^3 - 2174420x + \frac{4936546769}{4}$

$$\begin{aligned}
\bar{g}(x) = x^{20} &+ (-181\sqrt{-163} - 29503)x^{19} + (\frac{7744619}{2}\sqrt{-163} + \frac{734730487}{2})x^{18} \\
&+ (-37930957217\sqrt{-163} - 2692457531821)x^{17} \\
&+ (228093679624065\sqrt{-163} + 13327099062294002)x^{16} \\
&+ (-94931257491871989 3\sqrt{-163} - 47969958126555042793)x^{15} \\
&+ (2916633081409821170837\sqrt{-163} + 131333948208755892888788)x^{14} \\
&+ (-\frac{13758057532173014129076119}{2}\sqrt{-163} - \frac{563173356960855925776027973}{2})x^{13} \\
&+ (127718758202367680929619665 90\sqrt{-163} + 48203367204794161061437928 4385)x^{12} \\
&+ (-189727559127386106701286247294 61\sqrt{-163} - 66721770235134648188885235885 1432)x^{11} \\
&+ (22777652737830346424672334885165592\sqrt{-163} + 75247305901152839663292966739973 8718)x^{10} \\
&+ (-\frac{444269027280961498593730220999187 43847}{2}\sqrt{-163} - \frac{138762855349875014531138294341930286 9489}{2})x^{9} \\
&+ (\frac{352238356606533484875661381272225305565 83}{2}\sqrt{-163} \\
&\quad + \frac{104563684752677818142025930175304158221 5333}{2})x^{8} \\
&+ (-\frac{226263243194245193233352892432104824642282 85}{2}\sqrt{-163} \\
&\quad - \frac{641139938510026569750171049518954935923272679}{2})x^{7} \\
&+ (58395844205944716282708778857316968809169566 40\sqrt{-163} \\
&\quad + 15852265151177367676316706055831528766108073 8015)x^{6} \\
&+ (-23879893566466458071700816748733586204616526688 78\sqrt{-163} \\
&\quad - 62294936670810816183045963066318920456146464461422)x^{5} \\
&+ (\frac{15126265378882432349197122140885137511639392013537 89}{2}\sqrt{-163} \\
&\quad + \frac{38020351834146587883244350917151535539095986603424115}{2})x^{4} \\
&+ (-17895781771816123179687273662756274362927769778268095 3\sqrt{-163} \\
&\quad - 43441109754333769656258352382226681875397339988134048 92)x^{3} \\
&+ (\frac{59568312510665006849348831822837101964968589780156064893}{2}\sqrt{-163} \\
&\quad + \frac{13992948322658187401645787385779671238904603878707717879 17}{2})x^{2} \\
&+ (-\frac{62216676185609786001788785256246541367489215635595080303 31}{2}\sqrt{-163} \\
&\quad - \frac{14168362340657260409202862013382376267161559529490666029993 9}{2})x \\
&+ \frac{12581930240043493641072765695324996911884245555598783194049991}{82}\sqrt{-163} \\
&\quad + \frac{27820714799103429431810282340106979018248989818726906527958428 3}{82}
\end{aligned}$$

$\mu = \frac{1+\sqrt{-163}}{82}$

# References


[1] E. Bach, *Explicit bounds for primality testing and other related problems*, Math. Comp., **55** (1990), 355–380.

[2] R. Balasubramanian and N. Koblitz, *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm*, J. Cryptology, **11** (1998), 141–145.

[3] J. Belding, R. Bröker, A. Enge, and K. Lauter, *Computing Hilbert Class Polynomials*, To appear; 2007.

[4] D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, Advances in Cryptology – CRYPTO 2001, LNCS **2139** (2001), 213–229.

[5] D. Boneh, B. Lynn, and H. Shacham, *Short signatures from the Weil pairing*, Advances in Cryptology – ASIACRYPT 2001, LNCS **2248** (2001), 514–532.

[6] A. Bostan, F. Morain, B. Salvy and É. Schost, *Fast algorithms for computing isogenies between elliptic curves*, Mathematics of Computation, 2006.

[7] R. Bröker, *Constructing supersingular elliptic curves*, Manuscript, 2007.

[8] D. Burgess, *A note on the distribution of residues and non-residues*, J. London Math. Soc., **38** (1963), 253–256.

[9] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.

[10] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, *Handbook of elliptic and hyperelliptic curve cryptography*, Chapman & Hall/CRC press, 2006.

[11] D. Cox, Primes of the form $x^2 + ny^2$, Wiley, (1989).

[12] I. Damgard and G. Frandsen, *Efficient Algorithms for GCD and cubic residuosity in the ring of Eisenstein integers*, FCT '03, LNCS **2751** (2003), 109–117.

[13] B. den Boer, *Diffie-Hellman is as strong as discrete log for certain primes*, Advances in Cryptology '88, LNCS **403** (1989), 530–539.

[14] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer funktionenkörper*, Abh. Math. Sem. Univ. Hamburg., **14** (1941), 197–272.

[15] N. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, Computational perspectives on number theory: proceedings of a conference in honor of AOL Atkin (eds. D.A. Buell and J.T. Teitelbaum), 1997, 21–76.

[16] A. Enge, *The complexity of class polynomial computation via floating point approximations*, HAL-INRIA 1040 and ArXiv cs.CC/0601104, INRIA, 2006. Available at http://hal.inria.fr/inria-00001040.

[17] G. Frey and H. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Math. Comp., **62** (1994), 865–874.

[18] W. Fulton *Algebraic Curves*, W. A. Benjamin, Inc., 1969.

[19] S. Galbraith, *Constructing isogenies between elliptic curves over finite fields*, Manuscript, 2003.

[20] S. Galbraith, *Pairings*, Ch. IX of I. Advances in elliptic curve cryptography Vol. 2, (eds. Blake, Seroussi, and Smart), Cambridge University Press, 2005.

[21] S. Galbraith, F. Hess, and F. Vercauteren, *Aspects of pairing inversion*, To appear, 2007.

[22] S. Galbriath, C. o hEigeartaigh, and C. Sheedy, Simplified pairing computation and security implications, J. Math. Crypto, **1**, pp. 267–281, (2007).

[23] S. Galbraith and V. Rotger, *Easy decision Diffie-Hellman groups*, Journal of Computation and Mathematics, **7** (2004), 201–218.

[24] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra, 2nd. ed.*, Cambridge University Press, 2003.

[25] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, 2004.

[26] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, Graduate Texts in Mathematics, **52** (1977).

[27] E. Howe, *Supersingular genus-two curves over fields of characteristic three*, available at http://arXiv:math/0604413v1, 2006.

[28] M. Huang and D. Ierardi, *Counting points on curves over finite fields*, J. Symbolic Computation, **25** (1998), 1–21.

[29] A. Joux, *A one round protocol for tri-partite Diffie-Hellman*, J. Cryptology, **17** (2004), 263–276.

[30] A. Joux, The Weil and Tate pairings as building blocks for public key cryptosystems (survey), Algorithm Number Theory Symposium – ANTS-V, LNCS **2369**, Springer-Verlag, pp. 20–32 (2002).

[31] A. Joux, and K. Nguyen, *Separating Decision Diffie-Hellman from Computational Diffie-Hellman in cryptographic groups*, J. Cryptology, **16** (2003), 239–247.

[32] N. Koblitz, *Algebraic Aspects of Cryptography*, Springer-Verlag, 1998.

[33] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms 2nd ed.*, Springer-Verlag, 1993.

[34] N. Koblitz and A. Menezes, *Pairing-based cryptography at high security levels*, In: N. Smart (ed.) Cryptography and Coding, LNCS, **3796** (2005), 13–36.

[35] D. Kohel, *ECHIDNA: Algorithms for Algebra and Geometry Experimentation*, http://echidna.maths.usyd.edu.au/kohel/alg/index.html.

[36] D. Kohel, *Endomorphism Rings of Elliptic Curves over Finite Fields*, PhD thesis, University of California at Berkeley, 1996.

[37] J.C. Lagarias, and A.M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic Number Fields, ed. A. Fröhlich, Academic Press, 1977, 409–465.

[38] S. Lang, *Abelian varieties*, Springer-Verlag, New York, 1983.

[39] A. Lenstra, and E. Verheul, *The XTR public key system*, Advances in Cryptology-CRYPTO 2000, LNCS **1880**, Springer-Verlag 2000, 1–19.

[40] R. Lercier, D. Lubicz, and F. Vercauteren, *Point counting on elliptic and hyperelliptic curves*, in Handbook of elliptic and hyperelliptic curve cryptography, Chapman & Hall/CRC press, **ch. 17** (2006), 407–453.

[41] R. Lidl and H. Niederreiter, *Finite Fields 2nd ed.*, Cambridge University Press, 1997.

[42] M. Maas, *Pairing-Based Cryptography*, Master's Thesis, Technische Universiteit Eindhoven, 2004.

[43] U. Maurer, and S. Wolf, *The Diffie-Hellman protocol*, Designs, Codes, and Cryptography, **19** (2000), 147–171.

[44] A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, 1993.

[45] A. Menezes, *An introduction to pairing-based cryptography*, Notes from lectures given in Santander, Spain, 2005.

[46] A. Menezes, T. Okamoto, and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in finite fields*, IEEE Trans. Inform. Theory, **IT-39** (1993), 1639–1646.

[47] A. Menezes, and S. Vanstone, *ECSTR (XTR): Elliptic Curve Singular Trace Representation*, Rump Session of Crypto 2000.

[48] V. Miller, *Short programs for functions on curves*, Unpublished manuscript, 1986. Available at http://crypto.stanford.edu/miller/miller.pdf.

[49] V. Miller, *The Weil pairing, and its efficient calculation*, J. Cryptology, **17** (2004), 235–261.

[50] D. Morales, Cheon's algorithm, pairing inversion and the discrete logarithm problem, IACR e-print report 2008/300, (2008).

[51] T. Satoh, On pairing inversion problems, Pairing Conference 2007, LNCS **4575**, pp. 317-328, (2007).

[52] T. Satoh, Closed formulae for the Weil pairing inversion, Finite fields and their appl., **14**, pp. 743–765, (2008).

[53] T. Satoh, On degrees of polynomial interpolations related to elliptic curves, International workshop, WCC 2005, Bergen, Norway, March 2005, Revised and selected papers, LNCS **3969**, pp. 155-163, (2006).

[54] T. Satoh, On polynomial interpolations related to Verheul homomorphisms, LMS J. Comput. Math. **9**, pp. 135–158, (2006).

[55] R. Schoof, *Counting points on elliptic curves over finite fields*, J. Théor. Nombres Bordeaux, **44** (1995).

[56] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp., **44** (1985), 483–494.

[57] A. Shamir, *Identity-based cryptosystems and signature schemes*, Advances in Cryptology–Proceedings of CRYPTO 84, LNCS, **196** (1985), 277-296.

[58] V. Shoup, *A computational introduction to number theory and algebra*, Cambridge University Press, 2005.

[59] I. Shparlinski, *Finite Fields: Theory and Computation*, Kluwer Academic Publishers, 1999.

[60] J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 1986.

[61] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, 1994.

[62] H. M. Stark, Class numbers of complex quadratic fields, in Modular Functions of One Variable I, Lecture Notes in Math. **320**, Springer-Verlag, pp. 153–174, (1973).

[63] W. Stein, *SAGE: Software for Algebra and Geometry Experimentation*, http://www.sagemath.org/sage/, http://sage.scipy.org/.

[64] J. Vélu, *Isogénies entre courbes elliptiques*, C.R. Acad. Sc. Paris, Série A., **273** (1971), 238–241.

[65] H. Verdure, *Factorisation patterns of division polynomials*, Proceedings of the Japan Academy, **80**, Ser. A, No. 5 (2004).

[66] E. Verheul, *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*, J. Cryptology, **17** (2004), 277–296.

[67] L. Washington, *Elliptic curves (Number theory and cryptography), 2nd edition*, Chapman & Hall, 2008.

[68] E. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. 4th series, **2** (1969), 521–560.