The Tate Pairing via Elliptic Nets

Katherine E. Stange

Brown University
stange@math.brown.edu

Abstract. We derive a new algorithm for computing the Tate pairing on an elliptic curve over a finite field. The algorithm uses a generalisation of elliptic divisibility sequences known as elliptic nets, which are maps from $\mathbb{Z}^n$ to a ring that satisfy a certain recurrence relation. We explain how an elliptic net is associated to an elliptic curve and reflects its group structure. Then we give a formula for the Tate pairing in terms of values of the net. Using the recurrence relation we can calculate these values in linear time.
Computing the Tate pairing is the bottleneck to efficient pairing-based cryptography. The new algorithm has time complexity comparable to Miller's algorithm, and is should yield to further optimisation.

Keywords: Tate pairing, elliptic curve, elliptic divisibility sequence, elliptic net, Miller's algorithm, pairing-based cryptography.

1 Introduction

Pairing-based cryptography, since it was introduced in the mid-1990's, has had an ever-growing list of applications. Although it was originally suggested as a means of reducing the discrete logarithm problem on an elliptic curve to the discrete logarithm problem on a finite field [21, 15], considerable excitement and research has since been generated by public-key cryptographic applications such as Sakai, Ohgishi and Kasahara's key agreement and signature schemes [24], Joux's tri-partite Diffie-Hellman key exchange [19], and Boneh and Franklin's identity-based encryption scheme [7]. Good overviews include [12, 23], while a very up-to-date research bibliography can be found at [4].

The bottleneck to pairing-based cryptographic implementations is the costly computation of the pairing, which is most frequently the Tate or Weil pairing, the former being the most efficient. The only polynomial time algorithm currently in use for these computations was given by Victor Miller [22]. For an overview of the implemention of Miller's algorithm, see [11, 17].

In this paper, we propose a new method of computing of the Tate pairing, arising from the theory of elliptic nets. The theory of elliptic nets generalises that of elliptic divisibility sequences, which were first studied by Morgan Ward in 1948 [32]. For Ward, these were integer sequences $h_0, h_1, \ldots, h_n, \ldots$ satisfying the following two properties:

1. For all $n, m \in \mathbb{Z}^+$,
$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \ . \tag{1}$$
2. h_n divides h_m whenever n divides m.

Ward demonstrates that an elliptic divisibility sequence arises from any choice of elliptic curve and point on that curve. We denote by $\sigma(u; \Lambda)$ the Weierstrass sigma function of an elliptic curve.

Theorem 1 (M. Ward, 1948). *Suppose E is an elliptic curve represented by $\mathbb{C}/\Lambda$, and $u \in \mathbb{C}$. Then the sequence*
$$h_n := \frac{\sigma(nu; \Lambda)}{\sigma(u; \Lambda)^{n^2}}$$
forms an elliptic divisibility sequence.

Given a ring R and an abelian group A, an *elliptic net* is a map $W : A \to R$ satisfying the following recurrence relation for $p, q, r, s \in A$:

$$\begin{aligned} W(p+q+s)\,W(p-q)\,W(r+s)\,W(r) \\ + W(q+r+s)\,W(q-r)\,W(p+s)\,W(p) \\ + W(r+p+s)\,W(r-p)\,W(q+s)\,W(q) = 0 \end{aligned}$$

When $A = R = \mathbb{Z}$ and $W(1) = 1$, the positive terms of an elliptic net satisfy Ward's equation (1) above. Under the further conditions that $W(2)|W(4)$ and $W(0) = 0$, these terms form an elliptic divisibility sequence.

Theorem 3 in Section 2 relates elliptic nets over $R = \mathbb{C}$ to elliptic curves, generalising Theorem 1. However, for cryptographic applications it is desired to work over finite fields: Theorem 4 allows results over $\mathbb{C}$ to be carried over to the finite field case. Theorem 5 is the statement of the curve-net relationship over finite fields.

In Section 3, we will exploit these theorems to find a formula for the Tate pairing given by the terms of an elliptic net. The main result, stated here, uses notation found in Sections 2.3 and 2.4. In particular, W is an elliptic net $W : \hat{E}_K \to K$, where $\hat{E}_K$ is a finite-rank free abelian group with a quotient $\pi : \hat{E}_K \to E$.

Theorem 2. *Fix a positive $m \in \mathbb{Z}$. Let E be an elliptic curve defined over a finite field K containing the m-th roots of unity. Let P, $Q \in E(K)$, with $[m]P = \mathcal{O}$. Choose $S \in E(K)$ such that $S \notin \{\mathcal{O}, -Q\}$. Choose p, q, $s \in \hat{E}_K$ such that $\pi(p) = P$, $\pi(q) = Q$ and $\pi(s) = S$. Let $W \in \mathcal{W}_{\hat{E}_K}$. Then the quantity*

$$T_m(P,Q) = \frac{W(s+mp+q)W(s)}{W(s+mp)W(s+q)} \tag{2}$$

is a well-defined function $T_m : E(K)[m] \times E(K)/mE(K) \to K^*/(K^*)^m$. Further, $T_m(P,Q) = \tau_m(P,Q)$, the Tate pairing.

From Theorem 2, to calculate the Tate pairing only requires an efficient method of calculating the terms of an elliptic net. Rachel Shipsey's thesis [25] provides a double-and-add method of calculating the n-th term of an elliptic divisibility sequence in $\log n$ time. We generalise her algorithm to elliptic nets in Section 4. This Elliptic Net Algorithm is an example of doing arithmetic on elliptic curves via the arithmetic of elliptic nets. Rachel Shipsey's work made use of this approach to solve the elliptic curve discrete logarithm problem in certain cases. Her paradigm may well have many other fruitful applications.

The Elliptic Net Algorithm in its current form is of complexity comparable to Miller's algorithm, and has potential for efficient implementations. It should be noted that optimising Miller's algorithm has been a subject of research for decades, while this new algorithm is already of comparable – yet still somewhat worse – efficiency. The elliptic net algorithm is based on entirely new principles; therefore, as well as being subject to adaptations of many known optimisations for Tate pairing computation, it should be subject to entirely original improvements. This note should be considered a call to further research.

In Section 2, we give the necessary mathematical preliminaries concerning the Tate pairing and elliptic nets. In Section 3, we prove Theorem 2 and a corollary relating elliptic nets and the Tate pairing. In Section 4, we describe the algorithms necessary to compute elliptic nets, and therefore the Tate pairing, efficiently. In Section 5, we make some brief remarks on optimisation of the algorithms and the efficiency as compared with Miller's algorithm. Finally, we make some concluding remarks in Section 6.

2 Mathematical Preliminaries

2.1 Elliptic Functions $\Psi_{\mathbf{v}}$

We begin with some complex function theory which will be necessary for the definition of elliptic nets over $\mathbb{C}$. For a complex lattice Λ, define the Weierstrass sigma function $\sigma : \mathbb{C} \to \mathbb{C}$ by

$$\sigma(z;\Lambda) = z \prod_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(1 - \frac{z}{\omega}\right) e^{z/\omega + (1/2)(z/\omega)^2},$$

and the Weierstrass zeta function $\zeta : \mathbb{C} \to \mathbb{C}$ by

$$\zeta(z; \Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Recall that the quantity

$$\zeta(z+\omega; \Lambda) - \zeta(z; \Lambda)$$

is independent of z, and we call this $\eta(\omega)$. The map $\eta : \Lambda \to \mathbb{C}$ is called the quasi-period homomorphism. Define $\lambda : \Lambda \to \{\pm 1\}$ by

$$\lambda(\omega) = \begin{cases} 1 & \text{if } \omega \in 2\Lambda, \\ -1 & \text{if } \omega \notin 2\Lambda. \end{cases}$$

Recall that the Weierstrass sigma function $\sigma : \mathbb{C}/\Lambda \to \mathbb{C}$ satisfies the following transformation formula for all $z \in \mathbb{C}$ and $\omega \in \Lambda$:

$$\sigma(z+\omega; \Lambda) = \lambda(\omega) e^{\eta(\omega)(z+\frac{1}{2}\omega)} \sigma(z; \Lambda) \tag{3}$$

Definition 1. *Fix a lattice $\Lambda \in \mathbb{C}$ corresponding to an elliptic curve E. For $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{Z}^n$, define a function $\Psi_{\mathbf{v}}$ on $\mathbb{C}^n$ in variables $\mathbf{z} = (z_1, \dots, z_n)$ as follows:*

$$\Psi_{\mathbf{v}}(\mathbf{z}; \Lambda) = \frac{\sigma(v_1 z_1 + \ldots + v_n z_n; \Lambda)}{\prod_{i=1}^{n} \sigma(z_i; \Lambda)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{\substack{1 \leq k,j \leq n \\ k \neq j}} \sigma(z_i + z_j; \Lambda)^{v_i v_j}}$$

In particular, we have for each $n \in \mathbb{Z}$, a function Ψ_n on $\mathbb{C}$ in the variable z:

$$\Psi_n(z; \Lambda) = \frac{\sigma(nz; \Lambda)}{\sigma(z; \Lambda)^{n^2}}$$

and for each pair $(m, n) \in \mathbb{Z} \times \mathbb{Z}$, a function $\Psi_{n,m}$ on $\mathbb{C} \times \mathbb{C}$ in variables z and w:

$$\Psi_{m,n}(z, w; \Lambda) = \frac{\sigma(mz + nw; \Lambda)}{\sigma(z; \Lambda)^{m^2 - mn} \sigma(z+w; \Lambda)^{mn} \sigma(w; \Lambda)^{n^2 - mn}}$$

From the general theory of elliptic functions, the divisor of $\Psi_{\mathbf{v}}$ as a function of z_1 is

$$\left(-\sum_{j=2}^{n} [v_j] z_j \right) - \sum_{j=2}^{n} v_1 v_j (-z_j) - \left(v_1^2 - \sum_{j=2}^{n} v_1 v_j \right) (0) \tag{4}$$

Proposition 1. *Fix a lattice $\Lambda \in \mathbb{C}$ corresponding to an elliptic curve E. The functions $\Psi_{\mathbf{v}}$ are elliptic functions in each variable.*

Proof. Let $\omega \in \Lambda$. We show the function is elliptic in the first variable. Let $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{Z}^n$ and $\mathbf{z} = (z_1, \dots, z_n), \mathbf{w} = (\omega, 0, \dots, 0) \in \mathbb{C}^n$. Using (3), we calculate

$$F = \frac{\Psi_{\mathbf{v}}(\mathbf{z} + \mathbf{w}; \Lambda)}{\Psi_{\mathbf{v}}(\mathbf{z}; \Lambda)} = \frac{\lambda(v_1 \omega)}{\lambda(\omega)^{v_1^2}}$$

If $\omega, v_1\omega \notin 2\Lambda$, then v_1 is odd, and $F = 1$. If $\omega \notin 2\Lambda$ but $v_1\omega \in 2\Lambda$, then v_1 must be even, and so $F = 1$ again. Finally, if $\omega \in 2\Lambda$, then $v_1\omega \in 2\Lambda$, and $F = 1$. Thus $\Psi_{\mathbf{v}}$ is invariant under adding a period to the variable z_1. Similarly $\Psi_{\mathbf{v}}$ is elliptic in each variable on $(\mathbb{C}/\Lambda)^n$. $\square$

In view of this proposition, we will use the same notation $\Psi_{\mathbf{v}}$ for the associated map $E^n \to \mathbb{C}$, and write, for example, $\Psi_{m,n}(P_1, P_2; E)$.

Proposition 2. *Fix a lattice $\Lambda \in \mathbb{C}$. Let $\mathbf{v} \in \mathbb{Z}^n$ and $\mathbf{z} \in \mathbb{C}^n$. Let T be an $n \times n$ matrix with entries in $\mathbb{Z}$ and transpose T^{tr}. Then*

$$\Psi_{\mathbf{v}}(T^{tr}(\mathbf{z}); \Lambda) = \frac{\Psi_{T(\mathbf{v})}(\mathbf{z}; \Lambda)}{\prod_{i=1}^{n} \Psi_{T(\mathbf{e}_i)}(\mathbf{z}; \Lambda)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{\substack{1 \leq i,j \leq n \\ i \neq j}} \Psi_{T(\mathbf{e}_i + \mathbf{e}_j)}(\mathbf{z}; \Lambda)^{v_i v_j}}.$$

Proof. A straightforward calculation using (3). □

2.2 Some Notation

We set some notation for the remainder of the paper.

L	number field contained in $\mathbb{C}$	$\delta : E_L \to E_{k_\mathfrak{p}}$	reduction map modulo $\mathfrak{p}$
E_L	elliptic curve defined over L	$\delta : R \to k_\mathfrak{p}$	reduction map modulo $\mathfrak{p}$
R	ring of integers of L	$q : \mathbb{C} \to E_L(\mathbb{C})$	complex uniformisation
$\mathfrak{p}$	prime of R of good reduction for E_L	Λ	lattice in $\mathbb{C}$ associated to E_L
$k_\mathfrak{p}$	residue field of $\mathfrak{p}$	$\hat{E}_L$	$q^{-1}(E_L(L))$
$E_{k_\mathfrak{p}}$	E_L reduced modulo $\mathfrak{p}$	$\hat{E}_{k_\mathfrak{p}}$	$q^{-1} \circ \delta^{-1}(E_{k_\mathfrak{p}}(k_\mathfrak{p}))$

For a finite field K, and elliptic curve E_K defined over K, there always exists a number field $L \subset \mathbb{C}$, prime $\mathfrak{p}$, and elliptic curve E_L such that $K = k_\mathfrak{p}$ and $E_K = \delta(E_L)$. Therefore, for any number field or finite field K, we may speak of $\hat{E}_K$. In either case, this is a free abelian group of finite rank with a quotient map $\pi : \hat{E}_K \to E_K(K)$.

2.3 Elliptic Nets

Since Ward's definition in 1948, elliptic divisibility sequences have been an active area of research (for an overview, see [13]). In her thesis in 2003 [30], Christine Swart studied a more general class of Somos-4 sequences arising from elliptic curves. Her work, and related work of van der Poorten [31] provided the clues that the following more general theory of nets existed. It has recently come to the author's attention that the possibility of such a definition was briefly discussed in correspondence by Noam Elkies, James Propp and Michael Somos in 2001 [3]. Several of the proofs in this section are omitted and can be found in [29].

Definition 2. *Let A be an abelian group, and R be a ring. An* elliptic net *is any map $W : A \to R$ such that the following recurrence holds for all p, q, r, $s \in A$.*

$$\begin{aligned} &W(p+q+s)\,W(p-q)\,W(r+s)\,W(r) \\ &\quad + W(q+r+s)\,W(q-r)\,W(p+s)\,W(p) \\ &\quad\quad + W(r+p+s)\,W(r-p)\,W(q+s)\,W(q) = 0 \end{aligned} \tag{5}$$

The set of such nets is denoted $\mathcal{EN}(A, R)$. If B is a subgroup of A, then W restricted to B is also an elliptic net and is called an elliptic subnet *of A.*

We will now see that $\Psi_{\mathbf{v}}$ forms an elliptic net as a function of $\mathbf{v} \in \mathbb{Z}^n$ when the lattice Λ and $\mathbf{z} \in \mathbb{C}^n$ are fixed. Let the standard basis of $\mathbb{Z}^n$ be denoted $\mathbf{e}_1, \ldots, \mathbf{e}_n$. As a means of fixing $\mathbf{z}$, we specify a homomorphism $\phi : \mathbb{Z}^n \to \hat{E}_L$.

Definition 3. *Suppose $\phi : \mathbb{Z}^n \to \hat{E}_L$ is a homomorphism such that the images of $\pm\mathbf{e}_i$ under $\pi \circ \phi$ are all distinct. Define $W_\phi : \mathbb{Z}^n \to \mathbb{C}$ by*

$$W_\phi(\mathbf{v}) = \Psi_{\mathbf{v}}(\phi(\mathbf{e}_1), \phi(\mathbf{e}_2), \ldots, \phi(\mathbf{e}_n); \Lambda)$$

Theorem 3. $W_\phi \in \mathcal{EN}(\mathbb{Z}^n, L)$.

Proof. The proof involves some lengthy calculations. See [29]. $\square$

In this way, we can associate an elliptic net to any choice of n points $P_i \in E(L)$ which, along with their negatives, are all distinct. We call $W_\phi \in \mathcal{EN}(\mathbb{Z}^n, L)$ the *elliptic net associated to* $E, P_1, \ldots, P_n$. Such an example net is shown in Figure 1. Let E be an elliptic curve defined over $\mathbb{Q}$, and $P \in E(\mathbb{Q})$. Then, for an

4335	5959	12016	-55287	23921	1587077	-7159461
94	479	919	-2591	13751	68428	424345
-31	53	-33	-350	493	6627	48191
-5	8	-19	-41	-151	989	-1466
1	3	-1	-13	-36	181	-1535
1	1	2	-5	7	89	-149
0	1	1	-3	11	38	249

$\uparrow$ Q, $P \rightarrow$

over $\mathbb{Q}$

0	4	4	3	1	2	4
4	4	4	4	1	3	0
4	3	2	0	3	2	1
0	3	1	4	4	4	4
1	3	4	2	4	1	0
1	1	2	0	2	4	1
0	1	1	2	1	3	4

$\uparrow$ Q, $P \rightarrow$

over $\mathbb{F}_5$

Fig. 1. A portion of the elliptic net of $E : y^2 + y = x^3 + x^2 - 2x$, $P = (0, 0)$, $Q = (1, 0)$.

appropriate choice of ϕ in the definition above, the positive terms of the elliptic net associated to E, P are integers and form an elliptic divisibility sequence as described by Ward. In particular, the recurrence relation (5) implies Ward's relation (1).

We wish to extend this idea to finite fields, but here we cannot use Weierstrass' sigma function to define appropriate functions. The following theorem allows us to push results on number fields L over to residue fields $k_\mathfrak{p}$. It says that we can find appropriate functions $f_\mathbf{v}$ for $E_{k_\mathfrak{p}}$ by simply considering (an appropriate normalisation of) the net $\Psi_\mathbf{v}$ modulo $\mathfrak{p}$. These $f_\mathbf{v}$ will also form an elliptic net. We will only need this theorem for $n \leq 3$.

Theorem 4. *Let $0 < n \leq 3$. Consider points $P_1, \ldots, P_n$ defined over L such that the reductions modulo $\mathfrak{p}$ of the $\pm P_i$ are all distinct. Then there exists some $c \in L$ and quadratic form $f : \mathbb{Z}^n \rightarrow \mathbb{Z}$ such that the map $\Psi'_\mathbf{v} = c^{f(\mathbf{v})-1}\Psi_\mathbf{v} : E_L^n \rightarrow L$ takes values in R for all $\mathbf{v} \in \mathbb{Z}^n$. There exists a function $f_\mathbf{v} : E_{k_\mathfrak{p}}^n \rightarrow k_\mathfrak{p}$ such that the following diagram commutes.*

$$\begin{array}{ccc} E_L(R)^n & \xrightarrow{\Psi'_\mathbf{v}} & \mathbb{P}^1(R) \\ \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} \\ E_{k_\mathfrak{p}}(k_\mathfrak{p})^n & \xrightarrow{f_\mathbf{v}} & \mathbb{P}^1(k_\mathfrak{p}) \end{array}$$

Furthermore $\operatorname{div}(f_\mathbf{v}) = \delta^* \operatorname{div}(\Psi'_\mathbf{v})$.

Proof (Proof sketch.). Consider the scheme E_L^n over Spec R. Replacing E_L^n with its Néron model, a map to $\mathbb{P}^1$ on the generic fibre extends to a map over Spec R on the whole scheme. Let S be the set of primes of bad reduction for E together with primes such that the set of $\pm P_i$ are not distinct on the reduced curve. We must check that away from S, there are no vertical divisors in the fibres over 0 or ∞; this is a statement about the functions $\Psi'_\mathbf{v}$ which requires proof by multivariable induction. See [29] for details. $\square$

In light of this, we extend Definition 3 and state a fuller version of Theorem 3.

Definition 4. *Let $\phi : \mathbb{Z}^n \rightarrow \hat{E}_{k_\mathfrak{p}}$ be a homomorphism such that the images of $\pm\mathbf{e}_i$ under $\pi \circ \phi$ are all distinct. Let $f_\mathbf{v}$ be defined according to Theorem 4. Define $W_\phi : \mathbb{Z}^n \rightarrow k_\mathfrak{p}$ by*

$$W_\phi(\mathbf{v}) = f_\mathbf{v}(\phi(\mathbf{e}_1), \phi(\mathbf{e}_2), \ldots, \phi(\mathbf{e}_n))$$

Theorem 5. *Suppose K is either a number field or a finite field, and E is an elliptic curve defined over K. Then $W_\phi \in \mathcal{EN}(\mathbb{Z}^n, K)$.*

Proof. If K is a number field, this is Theorem 3. If K is a finite field, then this statement follows from Theorem 4: note that $\Psi'_{\mathbf{v}}$ still forms an elliptic net, and that an elliptic net postcomposed with a homomorphism is still an elliptic net. □

Figure 1 illustrates the relationship between an example elliptic net associated to E, P, Q over $\mathbb{Q}$ and the elliptic net associated to their reductions modulo 5.

2.4 Equivalence of Nets

In this section, K will denote a finite field.

Definition 5. *Let $W_1, W_2 \in \mathcal{EN}(A, K)$. Suppose $\alpha, \beta \in K^*$, and $f : A \to \mathbb{Z}$ is a quadratic form. If $W_1(\mathbf{v}) = \alpha\beta^{f(\mathbf{v})}W_2(\mathbf{v})$ for all $\mathbf{v}$, then we say W_1* is equivalent to *W_2 and write $W_1 \sim W_2$. If α and β lie in a subfield L of K, then we say further that W_1 and W_2 are* equivalent over *L.*

Clearly this definition gives an equivalence relation, and it is easily verified that an equivalence applied to an elliptic net gives another elliptic net. We write $\mathcal{EN}_0(A, K) = \mathcal{EN}(A, K)/\sim$. If W_1 is a subnet of W_2, then we may, by abuse of language, say that the equivalence class $[W_1]$ is a subnet of the equivalence class $[W_2]$, since then any $W'_1 \in [W_1]$ will be equivalent to some subnet of any $W'_2 \in [W_2]$.

For an m-torsion point $P \in E(K)$, the elliptic net associated to E, P does not necessarily satisfy $W_\phi(n + m) = W_\phi(n)$. So we cannot hope to consider W_ϕ as an elliptic net on the group $E(K)$ itself (nor should we wish to, as this subtlety is where the Tate pairing lives, as we shall see). On the other hand, we can consider it an elliptic net on $\hat{E}_K$ in a non-canonical fashion. If we consider the question only up to equivalence, however, the answer becomes canonical:

Theorem 6. *Let Γ be a subgroup of $\hat{E}_K$ of rank n. Let $\phi : \mathbb{Z}^n \to \Gamma$ be an isomorphism. Define $f_\phi : \Gamma \to K$ by $f_\phi(z) = W_\phi(\phi^{-1}(z))$. Then $f_\phi \in \mathcal{EN}(\Gamma, K)$ and the equivalence class of f_ϕ is independent of the choice of the isomorphism ϕ.*

Proof. Suppose $T : \mathbb{Z}^n \to \mathbb{Z}^n$ is a homomorphism. Then a restatement of Proposition 2 translated to finite fields via Theorem 4 is that $W_{\phi\circ T} \sim W_\phi \circ T$ (note that every finite field has a primitive element). Now choose another isomorphism $\phi' : \mathbb{Z}^n \to \Gamma$. Then there exists an isomorphism $T : \mathbb{Z}^n \to \mathbb{Z}^n$ such that $\phi \circ T = \phi'$. Then

$$f_{\phi'}(z) = W_{\phi'}(\phi'^{-1}(z)) = W_{\phi\circ T}(T^{-1}(\phi^{-1}(z))) \sim W_\phi(\phi^{-1}(z)) = f_\phi(z).$$

Note that this last equivalence is as a function of $\phi^{-1}(z) \in \mathbb{Z}^n$. But since ϕ^{-1} is linear, this implies equivalence as a function of z. The linearity of ϕ^{-1} also shows that f_ϕ is an elliptic net. So we have defined a unique class $[f_\phi] \in \mathcal{EN}_0(\Gamma, K)$. □

Definition 6. *Let $\mathcal{W}_{\hat{E}_K}$ denote the class $[f_\phi] \in \mathcal{EN}_0(\hat{E}_K, K)$ defined in Theorem 6.*

The importance of the preceeding theorem is as follows. There are many choices of basis for $\hat{E}_K$, and these may be specified either by choosing points $p_1, \ldots, p_n$ or by choosing an invertible $\phi : \mathbb{Z}^n \to \hat{E}_K$. In either case, the resulting elliptic net associated to $p_1, \ldots, p_n$ *considered as a function not of $\mathbb{Z}^n$ but of $\hat{E}_K$* always lies in the unique equivalence class $\mathcal{W}_{\hat{E}_K}$. However, to perform calculations, we must choose an isomorphism ϕ. Later, we will exploit this fact to allow ourselves freedom in choosing an appropriate ϕ for calculations.

We note one useful proposition.

Proposition 3. *Let $W \in \mathcal{W}_{\hat{E}_K}$. Then $W(p) = 0$ implies $\pi(p) = \mathcal{O}$.*

Proof. This follows from the definitions. □

2.5 The Tate Pairing

Choose $m \in \mathbb{Z}^+$. Let E be an elliptic curve defined over a field K containing the m-th roots of unity. Suppose $P \in E(K)[m]$ and $Q \in E(K)/mE(K)$. Since P is an m-torsion point, $m(P) - m(\mathcal{O})$ is a principal divisor, say $\mathrm{div}(f_P)$. Choose another divisor D_Q defined over K such that $D_Q \sim (Q) - (\mathcal{O})$ and with support disjoint from $\mathrm{div}(f_P)$. Then, we may define the Tate pairing

$$\tau_m : E(K)[m] \times E(K)/mE(K) \to K^*/(K^*)^m$$

by

$$\tau_m(P, Q) = f_P(D_Q)$$

This pairing is well-defined, bilinear and Galois invariant. For cryptographic applications, the Tate pairing is usually considered over finite fields, where it is non-degenerate. For details, see [10, 16].

3 Tate Pairing Using Elliptic Nets

Proof (Proof of Theorem 2). By the assumptions on the choice of S and Proposition 3, any W in the equivalence class of $\mathcal{W}$ is non-vanishing at the four arguments in (2). To verify that T_m is independent of choice of representative of $\mathcal{W}$, suppose that W_1 and W_2 are in the equivalence class of $\mathcal{W}$. Then $W_2(\mathbf{v}) = \alpha\beta^{f(\mathbf{v})}W_1(\mathbf{v})$ for some $\alpha, \beta \in K^*$ and quadratic form f. Then

$$\begin{aligned}
&\frac{W_1(s+mp-q)W_1(s)W_2(s+mp)W_2(s-q)}{W_1(s+mp)W_1(s-q)W_2(s+mp-q)W_2(s)} \\
&= \beta^{f(s+mp)+f(s-q)-f(s+mp-q)-f(s)} \\
&= \beta^{f(mp+q)-f(mp)-f(q)} = \beta^{m[f(p+q)-f(p)-f(q)]} \in (K^*)^m.
\end{aligned}$$

Let $\Gamma \subset \hat{E}_K$ be the subgroup generated by s, p, and q. Let

$$f_P = \frac{\Psi_{1,0,0}(s,p,q)}{\Psi_{1,m,0}(s,p,q)},$$

which is a function in $S = \pi(s)$, $P = \pi(p)$ and $Q = \pi(q)$, by Theorem 4.

Therefore, we may compute the divisor of f_P as a function of S (by equation (4)):

$$(f_P) = -([-m]P) + (1-m)(\mathcal{O}) + m(P) = m(P) - m(\mathcal{O}).$$

Let D_Q be the divisor $(Q+S) - (S)$.

Then, using Proposition 2 and Theorem 4,

$$f_P(D_Q) = \frac{\Psi_{1,0,0}(s+q,p,q)\Psi_{1,m,0}(s,p,q)}{\Psi_{1,m,0}(s+q,p,q)\Psi_{1,0,0}(s,p,q)} = \frac{\Psi_{1,0,1}(s,p,q)\Psi_{1,m,0}(s,p,q)}{\Psi_{1,m,1}(s,p,q)\Psi_{1,0,0}(s,p,q)}. \tag{6}$$

By a choice of $\phi : \mathbb{Z}^3 \to \Gamma$ such that $\phi(1,0,0) = s$, $\phi(0,1,0) = p$, and $\phi(0,0,1) = q$, we have $W_\phi(\mathbf{v}) = \Psi_{\mathbf{v}}(s,p,q) \in \mathcal{EN}(\mathbb{Z}^3, K)$. Therefore the equation (6) is just $T_m(P,Q)$ by Theorem 6. So $T_m(P,Q) = \tau_m(P,Q)$. $\square$

Corollary 1. *Let E be an elliptic curve defined over a finite field K, m a positive integer, $P \in E(K)[m]$ and $Q \in E(K)$. If W is the elliptic net associated to E, P, then we have*

$$\tau_m(P,P) = \frac{W(m+2)W(1)}{W(m+1)W(2)} \tag{7}$$

Further, if W is the elliptic net associated to E, P, Q, then we have

$$\tau_m(P,Q) = \frac{W(m+1,1)W(1,0)}{W(m+1,0)W(1,1)} \tag{8}$$

Proof. For the first formula, taking $q = p$ and $s = 2p$, we obtain $T_m(P,P) = \dfrac{\mathcal{W}((m+2)p)\mathcal{W}(p)}{\mathcal{W}((m+1)p)\mathcal{W}(2p)}$. For the second, take $s = p$, obtaining $T_m(P,Q) = \dfrac{\mathcal{W}((m+1)p+q)\mathcal{W}(p)}{\mathcal{W}((m+1)p)\mathcal{W}(p+q)}$. □

4 Tate Pairing Computation

4.1 Computing the Values of an Elliptic Net

In her thesis [25], Rachel Shipsey gives a double-and-add algorithm for computing terms of an elliptic divisibility sequence. In the case of interest to us now, given the initial values of an elliptic divisibility sequence, the algorithm computes the n-th term of a sequence in $\log(n)$ time. Shipsey applied her more general algorithm (which allows beginning elsewhere in the sequence) to give a solution to the elliptic curve discrete logarithm problem in certain cases.

The algorithm described here is an adaptation and generalisation of Shipsey's algorithm to calculate terms $W(m,0)$ and $W(m,1)$ of an elliptic net. We define a *block centred on k* (shown in Figure 2) to consist of a first vector of eight consecutive terms of the sequence $W(n,0)$ centred on terms $W(k,0)$ and $W(k+1,0)$ and a second vector of three consecutive terms $W(n,1)$ centred on the term $W(k,1)$. We define two functions:

		(k-1,1)	(k,1)	(k+1,1)			
(k-3,0)	(k-2,0)	(k-1,0)	(k,0)	(k+1,0)	(k+2,0)	(k+3,0)	(k+4,0)

Fig. 2. A block centred on k.

1. **Double**(V)**:** Given a block V centred on k, returns the block centred on $2k$.
2. **DoubleAdd**(V)**:** Given a block V centred on k, returns the block centred on $2k+1$.

We assume the elliptic net satisfies $W(1,0) = W(0,1) = 1$. The first vectors of Double(V) and DoubleAdd(V) are calculated according to the following special cases of (5) (or (1)).

$$W(2i-1,0) = W(i+1,0)W(i-1,0)^3 - W(i-2,0)W(i,0)^3 \tag{9}$$
$$W(2i,0) = (W(i,0)W(i+2,0)W(i-1,0)^2 - W(i,0)W(i-2,0)W(i+1,0)^2)/W(2,0) \tag{10}$$

The formulæ needed for the computations of the second vectors are instances of (5) [1].

$$\begin{aligned} W(2k-1,1) &= (W(k+1,1)W(k-1,1)W(k-1,0)^2 \\ &\qquad - W(k,0)W(k-2,0)W(k,1)^2)/W(1,1) \qquad (11) \\ W(2k,1) &= W(k-1,1)W(k+1,1)W(k,0)^2 - W(k-1,0)W(k+1,0)W(k,1)^2 \qquad (12) \\ W(2k+1,1) &= (W(k-1,1)W(k+1,1)W(k+1,0)^2 \\ &\qquad - W(k,0)W(k+2,0)W(k,1)^2)/W(-1,1) \qquad (13) \\ W(2k+2,1) &= (W(k+1,0)W(k+3,0)W(k,1)^2 \\ &\qquad - W(k-1,1)W(k+1,1)W(k+2,0)^2)/W(2,-1) \qquad (14) \end{aligned}$$

Equations (9) and (10), applied for $i = k-1, \ldots, k+3$, allow calculation of the first vectors of Double(V) and DoubleAdd(V) in terms of $W(2,0)$ and the terms of V. Equations (11)–(14) allow calculation of the second vectors in terms of $W(1,1)$, $W(-1,1)$, $W(2,-1)$ and the terms of V.

The algorithm to calculate $W(m,1)$ and $W(m,0)$ for any positive integer m is shown in Algorithm 1. The last term of the first vector of V in line 1 is calculated using (1). Note also that elliptic nets satisfy $W(-n,-m) = -W(n,m)$. In Section 5.1 we will consider possible optimisations.

Algorithm 1 Elliptic Net Algorithm

Input: Initial terms $a = W(2,0), b = W(3,0), c = W(4,0), d = W(2,1), e = W(-1,1), f = W(2,-1), g = W(1,1)$ of an elliptic net satisfying $W(1,0) = W(0,1) = 1$ and integer $m = (d_k d_{k-1} \ldots d_1)_2$ with $d_k = 1$

Output: Elliptic net elements $W(m,0)$ and $W(m,1)$

1: $V \leftarrow [[-a, -1, 0, 1, a, b, c, a^3c - b^3]; [1, g, d]]$
2: **for** $i = k-1$ down to 1 **do**
3:   **if** $d_i = 0$ **then**
4:     $V \leftarrow$ Double(V)
5:   **else**
6:     $V \leftarrow$ DoubleAdd(V)
7:   **end if**
8: **end for**
9: **return** $V[0,3]$ and $V[1,1]$ // terms $W(m,0)$ and $W(m,1)$ respectively

4.2 Computation of the Tate Pairing

We can now compute the Tate pairing via Corollary 1. Consider an elliptic curve E over a finite field $\mathbb{F}_q$ of characteristic not 2 or 3, in Weierstrass form

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

and points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on $E(\mathbb{F}_q)$ with $Q \neq \pm P$. We must calculate the values a, b, c, d, e, f, g required as input for the Elliptic Net Algorithm. These are terms of the elliptic net associated to E, P, Q. The necessary formulæ are given by the functions $\Psi_{n,m}$. In the case that $m = 0$, these are called *division*

[1] The values p, q, r, s substituted into (5) to obtain equations (11) - (14) are $[p, q, r, s] = [(k,0), (k-1,0), (1,0), (0,1)]$, $[(k+1,0), (k,0), (1,0), (-1,1)]$, $[(k+1,0), (k,0), (-1,0), (0,1)]$, and $[(k+2,0), (k,1), (1,0), (0,0)]$ respectively.

polynomials (see [26, p.105] and [27, p.477]). We have

$$W(1,0) = 1 \tag{15}$$
$$W(2,0) = 2y_1 \tag{16}$$
$$W(3,0) = 3x_1^4 + 6Ax_1^2 + 12Bx_1 - A^2 \tag{17}$$
$$W(4,0) = 4y_1(x_1^6 + 5Ax_1^4 + 20Bx_1^3 - 5A^2x_1^2 - 4ABx_1 - 8B^2 - A^3) \tag{18}$$

For the formulæ in case of characteristic 2 or 3, or the more general Weierstrass form, see [14, p.80]. Also using classical formulæ (see for example [8]), we have

$$W(0,1) = W(1,1) = 1 \tag{19}$$
$$W(2,1) = 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 \tag{20}$$
$$W(-1,1) = x_1 - x_2 \tag{21}$$
$$W(2,-1) = (y_1 + y_2)^2 - (2x_1 + x_2)(x_1 - x_2)^2 \tag{22}$$

Suppose that P has order m. Then we use the Elliptic Net Algorithm, with input $m+1$ and a, b, c, d, e, f, g given by (16)–(22). The output is used to evaluate formula (8) of Corollary 1, giving the Tate pairing.

5 Analysis

5.1 Some Implementation Considerations

For an integer m and finite field $\mathbb{F}_q$, we define the *embedding degree* k to be the least integer such that $m|(q^k - 1)$, thus ensuring the m-th roots of unity are contained in $\mathbb{F}_{q^k}^*$. In cryptographic applications of the Tate pairing, it is usual to use a curve defined over $\mathbb{F}_q$ of embedding degree $k > 1$, and points $P \in E(\mathbb{F}_q)$, $Q \in E(\mathbb{F}_{q^k})$: throughout what follows we make this assumption.

First, note that no inversions are actually needed in equations (9)–(14), since the inverses of $W(2,0)$, $W(2,1)$, $W(-1,1)$ and $W(2,-1)$ may be precomputed before the double-and-add loop is begun. Therefore these inversions are replaced by multiplications.

Now we consider optimisations in the functions Double and DoubleAdd. The largest savings can be gained by first computing a number of products which appear frequently in the formulæ:

$$W(i,0)^2 \text{ and } W(i-1,0)W(i+1,0) \quad \text{for } i = k-2, \ldots, k+3$$
$$W(k,1)^2 \text{ and } W(k-1,1)W(k+1,1)$$

With these 14 computations, each term of the 11 to be calculated requires only two multiplications and an addition (plus multiplications by $W(2,0)^{-1}$, $W(2,-1)^{-1}$, $W(1,1)^{-1}$ and $W(-1,1)^{-1}$).

Finally, we may try to avoid some of these extra multiplications by $W(2,0)^{-1}$, $W(1,1)^{-1}$, $W(2,1)^{-1}$ and $W(2,-1)^{-1}$ entirely. Recall that by Theorem 2, applying an equivalence to the net will not alter the Tate pairing result. Let $\eta = W(-1,1)$. Apply the equivalence given by $\alpha = 1$, $\beta = \eta$ and $f(n,m) = mn$. Clearly, this preserves the conditions[2] that $W(1,0) = W(0,1) = 1$ (and leaves terms $W(n,0)$ unchanged, so they are still in $\mathbb{F}_q$), but changes $W(-1,1)$ to 1, which saves one multiplication in $\mathbb{F}_{q^k}$ per iteration. If $W(2,0)$ has a cube root ν in $\mathbb{F}_q$, then the equivalence $\alpha = \nu^{-1}, \beta = \nu$ and $f(n,m) = m^2 + n^2 + mn$ will change $W(2,0)$ to 1, while preserving $W(1,0) = W(0,1) = W(-1,1) = 1$, saving four $\mathbb{F}_q$ multiplications per iteration.

Finally, we consider the applicability of some of the usual optimisations of Miller's algorithm. In Miller's algorithm, a final exponentiation is applied, in order to compute a unique value for the Tate pairing; the same exponentiation must be applied here. In the case of Miller's, this exponentiation eliminates multiplicative

[2] These were needed to derive formulæ (9)–(14).

factors living in the base field $\mathbb{F}_q$. In our case, the $\mathbb{F}_q$ computations do not give rise to strictly multiplicative factors (the algorithm requires much addition and subtraction), and so we cannot use this final exponentiation as a justification for the saving of $\mathbb{F}_q$ computations. Windowing methods (as in [6] and [18]) may lead to improvement. A triple-and-add adaptation (as in [17] and [5]) does not seem promising, by the nature of the recurrence relation. However, efficiency improvements are likely to be found by studying the characteristic 2 and 3 cases.

5.2 Complexity

Since the algorithm involves a fixed number of precomputations, and a double-and-add loop with a fixed number of computations per step, the algorithm is linear time in the size of m, as is Miller's algorithm. Miller's algorithm also consists of a double-and-add loop, and we call the two internal steps Double and DoubleAdd, as for the Elliptic Net Algorithm. In Miller's algorithm the cost of DoubleAdd is almost twice that of Double. By contrast, in the Elliptic Net Algorithm these steps take the same time, so the complexity is independent of Hamming weight. This makes the choice of appropriate curves for cryptographical implementations somewhat easier [12].

Denote squaring and multiplication in $\mathbb{F}_q$ by S and M. Denote squaring and multiplication in $\mathbb{F}_{q^k}$ by S_k and M_k. Assume that multiplying an element of $\mathbb{F}_q$ by one of $\mathbb{F}_{q^k}$ takes k multiplications in $\mathbb{F}_q$. Recall that E is defined over $\mathbb{F}_q$, $P \in E(\mathbb{F}_q)$, and $Q \in E(\mathbb{F}_{q^k})$. Then any term $W(n,0)$, being a term in the elliptic divisibility sequence associated to E, P, has a value in $\mathbb{F}_q$. Under the optimisations discussed in Section 5.1, each Double or DoubleAdd step requires $6S + (6k+26)M + S_k + 2M_k$. Furthermore, under the condition that $2y_P \in \mathbb{F}_q$ is a cube, then precomputing its cube root will save four multiplications in $\mathbb{F}_q$ per step.

The Elliptic Net Algorithm requires no inversions. Miller's algorithm in affine coordinates requires one or two $\mathbb{F}_q$ inversion per step. In situations where inversions are costly (depending on implementation, they may cost anywhere from approximately 4 to 80 multiplications [9]), one may implement Miller's algorithm in homogeneous coordinates.

For the purpose of comparison, we consider an optimised implementation of Miller's algorithm in Jacobian coordinates analysed by Neal Koblitz and Alfred Menezes [20]. In their implementation, they assume $Q \in E(\mathbb{F}_{q^{k/2}})$ (this is possible by using a twist of the curve). Applying this additional assumption to the elliptic net algorithm, $W(1,1)$ will be an element of $\mathbb{F}_{q^{k/2}}$, reducing one of the multiplications in Double to one half the time. The comparison is summarised in Tables 1 and 2. In the latter, a squaring is assumed to be comparable to a multiplication (although it is more usually assumed to be 0.8 times as fast), and a multiplication in $\mathbb{F}_{q^k}$ is assumed to take $k^{1.5}$ multiplications in $\mathbb{F}_q$ (see [20]). The number of steps constitutes a range because the Double and DoubleAdd steps may differ in cost.

Table 1. Comparison of Operations for Double and DoubleAdd steps

Algorithm	Double	DoubleAdd
Optimised Miller's [20]	$4S + (k+7)M + S_k + M_k$	$7S + (2k+19)M + S_k + 2M_k$
Elliptic Net Algorithm	$6S + (6k+26)M + S_k + \frac{3}{2}M_k$	$6S + (6k+26)M + S_k + 2M_k$

5.3 A Remark on Implementations

The elliptic net algorithm has been implemented by the author for PARI/GP (see [2]) and is available at [28]. It has also been implemented in C++ by Michael Scott and Augusto Dun Devigili for a pairing-friendly curve of degree 2. The implementation by Ben Lynn in the Pairing Based Cryptography Library [1] is applicable to

Table 2. $\mathbb{F}_q$ Multiplications per Step

Embedding degree	2	4	6	8	10	12
Optimised Miller's	18-38	31-58	46-82	64-109	84-140	106-174
Elliptic Net	51-52	76-80	104-112	136-147	171-186	207-228

curves of various sizes and embedding degrees and includes a program to compare the Elliptic Net algorithm with Miller's. Preliminary data agree with the complexity analysis above.

6 Conclusions

The Elliptic Net Algorithm has no significant restrictions on the points, curves or finite fields to which it applies, and requires no inversions. The efficiency of the algorithm is comparable to Miller's algorithm. One expects that the Elliptic Net Algorithm will yield to many further optimisations, and provide an efficient alternative to Miller's algorithm in many cases.

Acknowledgements. The author would like to thank Rafe Jones, Anna Lysyanskaya, Michelle Manes, Michael Scott, Joseph Silverman and Jonathan Wise for helpful discussions and editorial comments. This work was supported by NSERC Award PGS D2 331379-2006.

References

[1] The pairing-based cryptography library. http://crypto.stanford.edu/pbc/.
[2] Pari/gp development headquarters. http://pari.math.u-bordeaux.fr/.
[3] Robbins forum. http://www.math.wisc.edu/~propp/about-robbins.
[4] Paulo S. L. M. Barreto. The pairing-based crypto lounge. http://planeta.terra.com.br/informatica/paulbarreto/pblounge.html.
[5] Paulo S. L. M. Barreto, Hae Y. Kim, Ben Lynn, and Michael Scott. Efficient algorithms for pairing-based cryptosystems. In *Advances in cryptology—CRYPTO 2002*, volume 2442 of *Lecture Notes in Comput. Sci.*, pages 354–368. Springer, Berlin, 2002.
[6] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic curves in cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000. Reprint of the 1999 original.
[7] Dan Boneh and Matt Franklin. Identity-based encryption from the Weil pairing. In *Advances in cryptology—CRYPTO 2001 (Santa Barbara, CA)*, volume 2139 of *Lecture Notes in Comput. Sci.*, pages 213–229. Springer, Berlin, 2001.
[8] K. Chandrasekharan. *Elliptic functions*, volume 281 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1985.
[9] Mathieu Ciet, Marc Joye, Kristin Lauter, and Peter L. Montgomery. Trading inversions for multiplications in elliptic curve cryptography. *Des. Codes Cryptogr.*, 39(2):189–206, 2006.
[10] Sylvain Duquesne and Gerhard Frey. Background on pairings. In *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Math. Appl. (Boca Raton), pages 115–124. Chapman & Hall/CRC, Boca Raton, FL, 2006.
[11] Sylvain Duquesne and Gerhard Frey. Implementation of pairings. In *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Math. Appl. (Boca Raton), pages 389–404. Chapman & Hall/CRC, Boca Raton, FL, 2006.
[12] Sylvain Duquesne and Tanja Lange. Pairing-based cryptography. In *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Math. Appl. (Boca Raton), pages 573–590. Chapman & Hall/CRC, Boca Raton, FL, 2006.
[13] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. *Elliptic Divisibility Sequences*, pages 163–175. American Mathematical Society, Providence, 2003.

[14] Gerhard Frey and Tanja Lange. Background on curves and Jacobians. In *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Math. Appl. (Boca Raton), pages 45–85. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[15] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62(206):865–874, 1994.

[16] S. Galbraith. Pairings. In *Advances in elliptic curve cryptography*, volume 317 of *London Math. Soc. Lecture Note Ser.*, pages 183–213. Cambridge Univ. Press, Cambridge, 2005.

[17] Steven D. Galbraith, Keith Harrison, and David Soldera. Implementing the Tate pairing. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 324–337. Springer, Berlin, 2002.

[18] Darrel Hankerson, Julio López Hernandez, and Alfred Menezes. Software implementation of elliptic curve cryptography over binary fields. In *Proceedings of CHES 2000*, volume 1965 of *Lecture Notes in Comput. Sci.*, pages 1–24. Springer, Berlin, 2000.

[19] Antoine Joux. A one round protocol for tripartite Diffie-Hellman. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 385–393. Springer, Berlin, 2000.

[20] Neal Koblitz and Alfred Menezes. Pairing-based cryptography at high security levels. Cryptology ePrint Archive, Report 2005/076, 2005. http://eprint.iacr.org/.

[21] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39(5):1639–1646, 1993.

[22] Victor Miller. Short programs for functions on curves. 1986.

[23] K. G. Paterson. Cryptography from pairings. In *Advances in elliptic curve cryptography*, volume 317 of *London Math. Soc. Lecture Note Ser.*, pages 215–251. Cambridge Univ. Press, Cambridge, 2005.

[24] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. In *Symposium on Cryptography and Information Security*. Okinawa, Japan, 2000.

[25] Rachel Shipsey. *Elliptic Divibility Sequences*. PhD thesis, Goldsmiths, University of London, 2001.

[26] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[27] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[28] Katherine E. Stange. Pari/gp scripts for tate pairing via elliptic nets. http://www.math.brown.edu/∼stange/tatepairing/.

[29] Katherine E. Stange. *Elliptic Nets*. PhD thesis, Brown University, in preparation.

[30] Christine Swart. *Elliptic curves and related sequences*. PhD thesis, Royal Holloway and Bedford New College, University of London, 2003.

[31] Alfred J. van der Poorten. Elliptic curves and continued fractions. *J. Integer Seq.*, 8(2):Article 05.2.5, 19 pp. (electronic), 2005.

[32] Morgan Ward. Memoir on elliptic divisibility sequences. *Amer. J. Math.*, 70:31–74, 1948.