Cryptographic Pairings Based on Elliptic Nets

Naoki Ogura[1], Naoki Kanayama[2],
Shigenori Uchiyama[1], and Eiji Okamoto[2]

[1] Graduate School of Science and Engineering,
Tokyo Metropolitan University,
1-1, Minami-Ohsawa, Hachioji, Tokyo, 192-0397, Japan
ogura-naoki@ed.tmu.ac.jp, uchiyama-shigenori@tmu.ac.jp
[2] Faculty of Systems and Information Engineering,
University of Tsukuba,
1-1-1, Ten-nohdai, Tsukuba-shi, Ibaraki-ken, 305-8573 Japan
{kanayama,okamoto}@risk.tsukuba.ac.jp

Abstract. In 2007, Stange proposed a novel method for computing the Tate pairing on an elliptic curve over a finite field. This method is based on elliptic nets, which are maps from $\mathbb{Z}^n$ to a ring and satisfy a certain recurrence relation. In the present paper, we explicitly give formulae based on elliptic nets for computing the following variants of the Tate pairing: the Ate, Ate$_i$, R-Ate, and optimal pairings. We also discuss their efficiency by using some experimental results.

Keywords: Tate pairing, Ate pairing, R-Ate pairing, Optimal pairing, elliptic net, normalization.

1 Introduction

Recently, pairing-based cryptography have been one of the most attractive research topics in public-key cryptography since the proposals of some useful cryptographic schemes, such as the identity-based key agreement, the tripartite Diffie–Hellman key exchange, and the identity-based encryption schemes [3], [9], [15]. With respect to the efficient implementation of pairing-based cryptographic schemes, the computation of pairings, such as the Weil and Tate pairings, is the bottleneck. Currently, the most suitable pairing for the efficient implementation of pairing-based cryptographic schemes is the Tate pairing. Therefore, many algorithms for the efficient computation of the Tate pairing and some of its variants have been proposed, including the η_T [1], Duursma–Lee [6], Ate [8], Ate$_i$ [20], R-Ate [10], and optimal [21] pairings.

A standard algorithm for computing pairings is Miller's algorithm [11], [12]. A generic implementation of Miller's algorithm uses a classical double-and-add line-and-tangent method. Therefore, the time required using Miller's algorithm is linear with respect to the size of some input parameter r, as well as depending on the Hamming weight of r. Most improvements of pairing computation attempt to shorten the number of iterations of a loop in the algorithm, the so-called

T. Iwata and M. Nishigaki (Eds.): IWSEC 2011, LNCS 7038, pp. 65–78, 2011.

Miller loop. In fact, the Ate, Ate$_i$, R-Ate, and optimal pairings are truncated loop variants of the Tate pairing.

In 2007, Stange [18] defined elliptic nets and proposed an alternative method for the Tate pairing computation based on elliptic nets. Elliptic nets are a generalization of elliptic divisibility sequences, which are certain non-linear recurrence sequences related to elliptic functions. In 1948, Ward [22] first studied the arithmetic properties of elliptic divisibility sequences. As in the case of Miller's algorithm, a generic implementation of elliptic net algorithms proposed by Stange uses the double-and-add method, and so, as in the case of Miller's algorithm, the time required using the algorithm is linear with respect to the size of r. Both Miller's and elliptic net algorithms include two internal steps, referred to as Double and DoubleAdd [18]. In Miller's algorithm, the cost of DoubleAdd is about twice that of Double. In contrast, in the elliptic net algorithm, these two steps require almost the same amount of time. In particular, the running time is independent of the Hamming weight of r.

Because the efficiency of the algorithm is comparable to that of Miller's algorithm, by using further improvements and optimizations, we expect the elliptic net algorithm to be an efficient alternative to Miller's algorithm. Therefore, from both theoretical and practical points of view, it is important to investigate explicit formulae for computing some variants of the Tate pairing, based on elliptic nets.

In the present paper, we explicitly give formulae based on elliptic nets for computing the following variants of the Tate pairing: the Ate, Ate$_i$, R-Ate, and optimal pairings.

These pairings are defined as "point-evaluation" pairings, although the Tate pairing is originally "divisor-evaluation" pairing. These point-evaluation pairings are defined using normalized functions (see Section 2). Hence, we need to formulate a normalization of elliptic nets. In the present paper, we give a normalization of elliptic nets and then the formulae of the above-listed point-evaluation pairings. We also discuss their efficiency by using some experimental results.

The remainder of this paper is organized as follows. Section 2 gives a brief mathematical description of pairings and elliptic nets. Section 3 contains our main results concerning pairings described by elliptic nets. In Section 4, we will show our experimental results. We draw conclusions in Section 5.

2 Mathematical Preliminaries

2.1 Pairings

Let E be an elliptic curve over a finite field $\mathbb{F}_q$ with q elements. The set of $\mathbb{F}_q$-rational points of E is denoted as $E(\mathbb{F}_q)$. Let $E(\mathbb{F}_q)[r]$ denote the subgroup of r-torsion points in $E(\mathbb{F}_q)$. We write O for the point at infinity on E. Consider a large prime r such that $r \mid \#E(\mathbb{F}_q)$ and denote the embedding degree by k, which is the smallest positive integer such that r divides $q^k - 1$. Let π_q be the Frobenius endomorphism $\pi_q : E \to E : (x, y) \mapsto (x^q, y^q)$. We denote the trace of

Frobenius by t, i.e., $\#E(\mathbb{F}_q) = q + 1 - t$. Finally, let $\mu_r (\subset \mathbb{F}_{q^k}^{\times})$ be the group of r-th roots of unity.

Weil Pairing. The Weil pairing $e_r(\cdot, \cdot)$ is defined by

$$\begin{aligned} e_r(\cdot, \cdot) : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})[r] &\to \mu_r, \\ (P, Q) &\mapsto e_r(P, Q) := f_{r,P}(D_Q)/f_{r,Q}(D_P), \end{aligned}$$

where D_P is a divisor equivalent to $(P) - (O)$ and $f_{s,P}$ is a rational function on E such that $\mathrm{div}(f_{s,P}) = rD_P$. Similarly, $\mathrm{div}(f_{s,Q}) = rD_Q$, where D_Q is equivalent to $(Q) - (O)$. We assume that D_P and D_Q are chosen with disjoint supports.

Note that the Weil pairing does not depend on the choice of D_P and D_Q. Furthermore, the Weil pairing is bilinear and non-degenerate.

Tate Pairing. Let $P \in E(\mathbb{F}_{q^k})[r]$ and $Q \in E(\mathbb{F}_{q^k})$. Choose a point $R \in E(\mathbb{F}_{q^k})$ such that the support of $\mathrm{div}(f_{r,P}) = r(P) - r(O)$ and $D_Q := (Q + R) - (R)$ are disjoint. Then, the Tate pairing is defined by

$$\begin{aligned} \langle \cdot, \cdot \rangle_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) &\to \mathbb{F}_{q^k}^{\times}/(\mathbb{F}_{q^k}^{\times})^r, \\ (P, Q) &\mapsto \langle P, Q \rangle_r := f_{r,P}(D_Q) \mod (\mathbb{F}_{q^k}^{\times})^r \ . \end{aligned}$$

It has been shown that $\langle P, Q \rangle_r$ is bilinear and non-degenerate.

For cryptography applications, it is convenient to define pairings whose outputs are unique values rather than equivalence classes. Thus, herein, we consider the reduced Tate pairing defined by

$$\begin{aligned} \tau_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) &\to \mu_r, \\ \tau_r(P, Q) &= \langle P, Q \rangle_r^{(q^k-1)/r}. \end{aligned}$$

We call the operation $z \mapsto z^{(q^k-1)/r}$ final exponentiation.

The Weil Tate pairings satisfy that

$$e_r(P, Q) = \frac{\langle P, Q \rangle_r}{\langle Q, P \rangle_r} \text{ up to } r\text{-th powers.} \tag{1}$$

Thus, if the cost of final exponentiation is sufficiently small, the cost of computing the Tate pairing is almost half of that of computing the Weil pairing. Because of this, the Tate pairing is widely used in cryptography and there are numerous improved versions, such as the Ate pairing.

As mentioned in Section 1, a classical and currently standard algorithm for computing pairings is Miller's algorithm [11], [12]. One of the efficiency benchmarks of pairing computation is based on the Miller loop. The length of the Miller loop is $\log_2(r)$ in the case of the Tate pairing $\langle \cdot, \cdot \rangle_r$. Most improvements of pairing computation attempt to shorten the Miller loop.

Barreto et al. [2] pointed out that $\tau_r(P,Q)$ can be computed by $\tau_r(P,Q) = f_{r,P}(Q)^{(q^k-1)/r}$ if $P \in E(\mathbb{F}_q)[r]$ and $k > 1$.

For cryptographic applications, it is usually assumed that points P and Q are respectively elements in the following groups:

$$\mathbb{G}_1 = E(\mathbb{F}_q)[r] = E(\mathbb{F}_{q^k})[r] \cap \mathrm{Ker}(\pi_q - 1),$$
$$\mathbb{G}_2 = E(\mathbb{F}_{q^k})[r] \cap \mathrm{Ker}(\pi_q - q)$$

Hereafter, we assume that $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$.

We give a brief review of the following variants of the Tate pairing: the Ate [8], Ate$_i$ [20], R-Ate [10], and optimal [21] pairings. These pairings are defined on $\mathbb{G}_2 \times \mathbb{G}_1$ and $\mathbb{G}_1 \times \mathbb{G}_2$. In the present paper, we consider the case of $\mathbb{G}_2 \times \mathbb{G}_1$. See the appropriate papers cited above for the case of $\mathbb{G}_1 \times \mathbb{G}_2$. We use normalized functions to define the above pairings on $\mathbb{G}_2 \times \mathbb{G}_1$; therefore, we will first define this normalization as follows.

Normalization of Rational Functions. For $s \in \mathbb{Z}$, we define $f_{s,Q}$ as the rational function satisfying the equation $\mathrm{div}(f_{s,Q}) = s(Q) - (sQ) - (s-1)(O)$. This function $f_{s,Q}$ is determined uniquely up to multiplication by a constant. Uniqueness is obtained by normalization. We will denote the normalized form of $f_{s,R}$ by $f_{s,R}^{\mathrm{norm}}$ and refer to the latter as the normalized function.

Let u_O be a uniformizer of E on O. We may choose as this uniformizer $u_O = -\frac{x}{y}$. Then the normalized function $f_{s,R}^{\mathrm{norm}}$ is defined by

$$f_{s,R}^{\mathrm{norm}} = f_{s,R}/c, \quad \text{where} \quad c = (u_O^{s-1} f_{s,R})(O). \tag{2}$$

From now on, we may assume that all rational functions on elliptic curves are normalized.

Ate Pairing. The Ate pairing, proposed by Hess et al. [8], is a generalization of the η_T pairing [1]. The Ate pairing can be applied to not only supersingular but also ordinary elliptic curves.

Let $T = t-1$. We choose integers N and L such that $N = \gcd(T^k - 1, q^k - 1)$ and $T^k - 1 = LN$. We assume that r^2 does not divide $q^k - 1$. Then the Ate pairing is defined by $f_{T,Q}(P)(Q \in \mathbb{G}_2$ and $P \in \mathbb{G}_1)$. We denote by $\alpha(Q,P)$ the reduced Ate pairing: $\alpha(Q,P) := f_{T,Q}(P)^{(q^k-1)/r}$. The length of the Miller loop for computing the Ate pairing $f_{T,Q}(P)$ is $\log_2 |T|$.

Ate$_i$ Pairing. The Ate$_i$ pairing was proposed by Zhao et al. [20]. Let $T_i := q^i \pmod r$ for $i = 1, 2, \cdots, k-1$. For each i, we define the following quantities similarly to those for the Ate pairing: a_i is the smallest positive integer such that $T_i^{a_i} \equiv 1 \pmod r$, $N_i := \gcd(T_i^{a_i} - 1, q^k - 1)$, and L_i is the positive integer such that $T_i^{a_i} - 1 = L_i N_i$.

The Ate$_i$ pairing on $\mathbb{G}_2 \times \mathbb{G}_1$ is defined by $f_{T_i,Q}(P)(Q \in \mathbb{G}_2$ and $P \in \mathbb{G}_1)$. Analogous to the case for Ate pairing, we denote by $\alpha_i(Q,P)$ the reduced Ate$_i$

pairing: $\alpha_i(Q,P) := f_{T_i,Q}(P)^{(q^k-1)/r}$. The length of the Miller loop for computing $f_{T_i,Q}(P)$ is $\log_2(T_i)$.

If $T_n := \min\{T_i : i = 1, 2, \cdots, k-1, 0 \le T_i \le r-1\}$, then $f_{T_n,Q}(P)$ can be computed faster than the Ate pairing $f_{T,Q}(P)$.

R-Ate Pairing. The R-Ate pairing was proposed by Lee et al. [10] Let A, B, a, b be integers such that $A = aB + b$. We define the R-Ate pairing to be

$$R_{A,B}(Q,P) := f_{a,[B]Q}(P) \cdot f_{b,Q}(P) \cdot G_{[aB]Q,[b]Q}(P),$$

where G_{P_1,P_2} is a rational function on E such that $\mathrm{div}(G_{P_1,P_2}) = (P_1) + (P_2) - (P_3) - (O)$ $(P_3 = P_1 + P_2)$.

Lee et al. showed that $R_{A,B}(Q,P)$ is bilinear and non-degenerate under some conditions (see Theorem III.2 of [10]). Furthermore, they also gave the following examples in which $R_{A,B}(Q,P)$ is bilinear and non-degenerate: $(A,B) = (q^i, r)$, $(A,B) = (q, T_1)$ where $q > T_1$, $(A,B) = (T_i, T_j)$, and $(A,B) = (r, T_j)$. See Corollary III.3. in [10].

Optimal Pairing. Optimal pairing was proposed by Vercauteren [21]. Optimal pairing can be computed in $\log_2 r/\phi(k) + \epsilon(k)$ Miller loop iterations ($\phi(k)$ is the Euler function of k and $\epsilon(k) \le \log_2 k$).

Theorem 1 ([21] Theorem 1). *Let λ be an integer such that $r|\lambda$ and $r^2 \nmid \lambda$. We express λ as $\lambda = \sum_{i=0}^{l} c_i q^i$. Then*

$$\begin{aligned} &a_{[c_0,c_1,\cdots,c_l]} : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r \\ &(Q,P) \mapsto \Big(\prod_{i=0}^{l} f_{c_i,Q}^{q^i}(P) \cdot \prod_{i=0}^{l-1} \frac{l_{[s_{i+1}]Q,[c_i q^i]Q}(P)}{v_{[s_i]Q}(P)} \Big)^{\frac{q^k-1}{r}} \end{aligned}$$

(where $s_i = \sum_{j=i}^{l} c_j q^j$) defines a bilinear map. Furthermore, if

$$\frac{\lambda}{r} k q^{k-1} \not\equiv \frac{q^k-1}{r} \sum_{i=0}^{l} i c_i q^{i-1} \pmod{r},$$

$a_{[c_0,c_1,\cdots,c_l]}(Q,P)$ is non-degenerate.

Note that we may consider $l = \phi(k) - 1$ because $r \mid \Phi_k(q)$, where $\Phi_k(X)$ is the k-th cyclotomic polynomial. The pairing $a_{[c_0,c_1,\cdots,c_l]}(Q,P)$ is called the optimal pairing because it can be computed very efficiently if $c_0, c_1, \cdots, c_l$ can be chosen very small.

2.2 Elliptic Nets

In 2007, Stange [18] defined elliptic nets as maps from $\mathbb{Z}^n$ to a ring and they satisfy a certain recurrence relation associated with elliptic curves. In general, an elliptic net W is a map from a finitely generated abelian group $\mathcal{A}$ to an integral domain $\mathcal{R}$ such that

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

for $p, q, r, s \in \mathcal{A}$. Elliptic divisibility sequences arise from an elliptic curve defined over the rational numbers and a rational point of that curve. These sequences are strongly related to elliptic functions and the division polynomials of an elliptic curve. For cryptographic applications, the division polynomials of an elliptic curve are the main tools of Schoof's algorithm [16]. As we will see later, the division polynomials of an elliptic curve also play an important role in the computation of elliptic net-based pairings.

Stange introduced the concept of elliptic nets associated with elliptic curves and described Tate pairing by using elliptic nets. In this section, we briefly review elliptic nets. See [18] for detail.

First, we consider a function, denoted by Ψ, associated with elliptic curves over $\mathbb{C}$ by using an elliptic σ-function. We define an elliptic net W (in $\mathbb{C}$) using Ψ. Next, we construct a function associated with Ψ, denoted by Ω, that is defined in finite fields by applying a reduction theorem (see Theorem 3 in [18]). Thus, we are able to consider W in finite fields and construct the Tate pairing in finite fields.

To describe the Tate pairing $f_{r,P}(D_Q)$ by using elliptic nets, Stange showed a formula for a function $f_{r,P}$ with $\mathrm{div}(f_P) = r(P) - r(O)$ as $f_{r,P} = \dfrac{\Omega_{1,0,0,}(-S,P,Q)}{\Omega_{1,r,0}(-S,P,Q)}$, where $\Omega_{1,v_2,v_3}(-S,P,Q)(v_i \in \mathbb{Z})$ is a function in S and the divisor of $\Omega_{1,v_2,v_3}(-S,P,Q)$ on a variable S is $([v_2]P + [v_3]Q) - v_2(P) - v_3(Q) - (1 - v_2 - v_3)(O)$. Then a formula for $f_{r,P}(D_Q)$, where D_Q is a divisor equivalent to $(-S) - (-S - Q)$, as a function in variable S is computed. The following result is obtained by setting $S = P$ the formula of $f_{r,P}(D_Q)$.

Theorem 2 ([18]). *Let E be an elliptic curve over a finite field K. For $P \in E(K)[r]$, $Q \in E(K)$,*

$$f_{r,P}(D_Q) = \frac{W_{P,Q}(r+1,1)W_{P,Q}(1,0)}{W_{P,Q}(r+1,0)W_{P,Q}(1,1)}, \tag{3}$$

where $W_{P,Q}(r+1,i) = \Omega_{1,r,i}(-S,P,Q)|_{S=P}$.

Remark 1. *By using the above theorem and the equation (1), we can easily obtain the Weil pairing formula using elliptic nets as the following. For $P, Q \in E(\mathbb{F}_{q^k})[r]$,*

$$e_r(P,Q) = \frac{W_{P,Q}(r+1,1)W_{Q,P}(r+1,0)}{W_{P,Q}(r+1,0)W_{Q,P}(r+1,1)} \quad \textit{up to } r\textit{-th powers.}$$

Here, we assume that an elliptic curve E has a Weierstrass equation of the form $Y^2 = X^3 + AX + B$. Let $\psi_n(x,y)$ denote the n-th division polynomial of an elliptic curve. For simplicity, we write $W_{P,Q}(i,j) = W(i,j)$. Initial values of elliptic nets $W(i,0)$ and $W(i,1)$ are obtained by the following definition (see [18]): if $P=(x_1,y_1)$ and $Q=(x_2,y_2)$, then

$$\begin{aligned}
&W(1,0)=1,\\
&W(2,0)=2y_1,\\
&W(3,0)=3x_1^3+6Ax_1^2+12Bx_1-A^2,\\
&W(4,0)=4y_1(x_1^6+5Ax_1^4+20Bx_1^3-5A^2x_1^2-4ABx_1-8B^2-A^3),\\
&W(0,1)=W(1,1)=1,\\
&W(2,1)=2x_1+x_2-(\frac{y_2-y_1}{x_2-x_1})^2,\\
&W(-1,1)=x_1-x_2,\\
&W(2,-1)=(y_1+y_2)^2-(2x_1+x_2)(x_1-x_2)^2.
\end{aligned}$$

Elliptic nets $W(i,0)$ and $W(j,1)$ can be computed by the following recursive formulae.

Proposition 1 ([18])

$$\begin{aligned}
W(2i-1,0)&=W(i+1,0)W(i-1,0)^3-W(i-2,0)W(i,0)^3,\\
W(2i,0)&=\frac{W(i,0)W(i+2,0)W(i-1,0)^2-W(i,0)W(i-2,0)W(i+1,0)^2}{W(2,0)},\\
W(2i-1,1)&=\frac{W(i+1,1)W(i-1,1)W(i-1,0)^2-W(i,0)W(i-2,0)W(i,1)^2}{W(1,1)},\\
W(2i,1)&=W(i-1,1)W(i+1,1)W(k,0)^2-W(i-1,0)W(i+1,0)W(i,1)^2,\\
W(2i+1,1)&=\frac{W(i-1,1)W(i+1,1)W(i+1,0)^2-W(i,0)W(i+2,0)W(i,1)^2}{W(-1,1)},\\
W(2i+2,1)&=\frac{W(i+1,0)W(i+3,0)W(i,1)^2-W(i-1,1)W(i+1,1)W(i+2,0)^2}{W(2,-1)}.
\end{aligned}$$

Note that $W(i,0)=W_{P,Q}(i,0)$ is equal to $\psi_i(x_1,y_1)$ because $W_{P,Q}(i,0)=\psi_i(x_1,y_1)$ for $i=1,2,3,4$ and the recursive formulae for computing $W(2i-1,0)$ and $W(2i-1,0)$ are the same as the recursive formulae for division polynomials. Therefore, if E is defined over K and $P\in E(K)$, $W_{P,Q}(i,0)\in K$ for all i and they are killed by final exponentiation.

See [18] for algorithms for computing elliptic nets.

3 The Main Results

In this section, we describe variants of the Tate pairing, the Ate, Ate$_i$, R-Ate, and optimal pairings by using elliptic nets.

As seen in Section 2, these pairings are point-evaluation pairings and are defined by using normalized functions. Therefore, we need to formulate a normalization of elliptic nets in order to describe the formulae of the above-listed point-evaluation pairings.

3.1 Normalization of Elliptic Nets

First, we present the following lemma, which can be proved by using a straight forward calculation.

Lemma 1. *Let* $\wp(z;\Lambda) := \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}}(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2})$ *be the Weierstrass* $\wp$ *function and* $\sigma(z;\Lambda) := z\prod_{\omega\in\Lambda\setminus\{0\}}(1-\frac{z}{\omega})e^{z/\omega+(1/2)(z/\omega)^2}$ *be the Weierstrass* σ *function on* $\mathbb{C}$*; then*

$$\left(\frac{\wp(z;\Lambda)}{\wp'(z;\Lambda)\sigma(z;\Lambda)}\right)(0) = -\frac{1}{2} \ .$$

Next, we show the following equation corresponding to equation (2) in Section 2.1.

Proposition 2. *Let* $\Lambda \in \mathbb{C}$ *be a lattice corresponding to the elliptic curve* E*. Fix* $w \in \mathbb{C} \ \setminus \{0\}$*. For* $s \in \mathbb{Z}$*,*

$$(-\wp(z;\Lambda)/\wp'(z;\Lambda))^{1-s}\Psi_{s,1}(w,\ z)|_{z=0} = 2^{s-1}\Psi_{s,0}(w,\ z) \ .$$

Proof. The proposition follows from Lemma 1 and the following fact:

$$\Psi_{s,1}(w,\ z) = \frac{\sigma(sw+z)}{\sigma(w)^{s^2-s}\sigma(w+z)^s\sigma(z)^{1-s}} \ .$$

The uniformizer $u_O = -\frac{x}{y}$ corresponds to $-\frac{\wp(z)}{\wp'(z)}$. Thus, we have the following proposition, which gives the normalization of elliptic nets.

Proposition 3. $\tilde{W}_{P,Q}(s,\ 1)$ *denotes the normalization (by* $-\frac{x}{y}$*) for the elliptic net* $W_{P,Q}(s,\ 1)$*. For* $s \in \mathbb{Z}$*, assume* $[s]P \neq O$*. Then*

$$\tilde{W}_{P,Q}(s,1) = \frac{W_{P,Q}(s,1)}{2^{s-1}W_{P,Q}(s,0)} \ .$$

For practical uses of pairings, we can assume $k > 1$. In this case, $2^{(q^k-1)/r} = 1$, and so we have

$$\tilde{W}_{P,Q}(s,1)^{\frac{q^k-1}{r}} = \left(\frac{W_{P,Q}(s,1)}{W_{P,Q}(s,0)}\right)^{\frac{q^k-1}{r}} \ .$$

3.2 Elliptic Net-Based Pairings

We explain the key lemma which connects various pairings with elliptic nets. We use $\tilde{W}_{P,S}(s,\ 1)$ to denote the normalization for $W_{P,S}(s,\ 1)$, where $W_{P,S}(s,\ 1)$ is a function in S and P is a fixed point on E.

Lemma 2. *For* $s \in \mathbb{Z}$*, we assume that the point* Q *is neither a zero nor a pole of* $f_{s,P}$*. Then*

$$f_{s,P}(Q) = \tilde{W}_{-P,Q}(s,1)^{-1}.$$

Proof. Let $W_{-P,S}(s,\ 1) = \Omega_{s,1}(-P,\ S)$ be a rational function in variable S. Similar to in [18], the divisor of $W_{-P,S}(s,\ 1)$ in S is

$$\begin{aligned}\mathrm{div}_S(\Omega_{s,1}(-P,\ S)) &= ([-s](-P)) - s(P) - (1-s)(O) \\ &= -\{s(P) - ([s]P) - (s-1)(O)\} \\ &= -\mathrm{div}_S(f_{s,P})\ .\end{aligned}$$

Hence, $f_{s,P} = \tilde{W}_{-P,S}(s,1)^{-1}$ from the uniqueness of the normalized function. Finally, we obtain the desired result by taking $S = Q$.

The following theorem derives formulae for elliptic net-based pairings.

Theorem 3. *If the following function on P and Q,*

$$A(P,\ Q) = \prod_{i=0}^{l_1} f_{t_i,P}^{\alpha_i}(Q) \prod_{j=0}^{l_2} G_{[u_j]P,[v_j]P}^{\beta_j}(Q),$$

is bilinear, then

$$A(P,\ Q) = \prod_{i=0}^{l_1} \tilde{W}_{P,Q}^{\alpha_i}(t_i,\ 1) \prod_{j=0}^{l_2} G_{[-u_j]P,[-v_j]P}^{-\beta_j}(Q)\ .$$

Proof. Using Lemma 2 and the bilinearity of $A(P,\ Q)$,

$$\begin{aligned}A(P,\ Q) &= A(-P,\ Q)^{-1} \\ &= \prod_{i=0}^{l_1} f_{t_i,-P}^{-\alpha_i}(Q) \prod_{j=0}^{l_2} G_{[-u_j]P,[-v_j]P}^{-\beta_j}(Q) \\ &= \prod_{i=0}^{l_1} \tilde{W}_{P,Q}^{\alpha_i}(t_i,\ 1) \prod_{j=0}^{l_2} G_{[-u_j]P,[-v_j]P}^{-\beta_j}(Q)\ .\end{aligned}$$

□

We consider the case of the optimal pairing. In this case, we need to compute scalar multiplications $[c_i q^i]Q (i = 0, 1, \cdots, l)$ using elliptic nets.

Note that $Q := (x_Q, y_Q)$ satisfies $[c_i q^i]Q = [q^i]([c_i]Q) = \pi_q^i([c_i]Q)$ because $Q \in E(\mathbb{F}_{q^k})[r] \cap \mathrm{Ker}(\pi_q - q)$.

Furthermore, as seen in Section 2 of [18], $W_{Q,P}(n, 0) = \psi_n(x_Q, y_Q)$. Thus, we are able to express $[n]Q$ in terms of elliptic nets by using the following famous multiplication formula:

$$[n](x,y) = \left(x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}(x,y), \frac{\psi_{n-1}^2\psi_{n+2} - \psi_{n+1}^2\psi_{n-2}}{4y\psi_n^3}(x,y)\right).$$

Hence, we obtain $[c_i q^i]Q = \pi_q^i([c_i]Q) = (x_{[c_i]Q}^{q^i}, y_{[c_i]Q}^{q^i})$, where

$$x_{[c_i]Q}^{q^i} = \left(x_Q - \frac{W_{Q,P}(c_i - 1, 0)W_{Q,P}(c_i + 1, 0)}{W_{Q,P}(c_i, 0)^2}\right)^{q^i},$$

$$y_{[c_i]Q}^{q^i} = \left(\frac{W_{Q,P}(c_i - 1, 0)^2 W_{Q,P}(c_i + 2, 0) - W_{Q,P}(c_i + 1, 0)^2 W_{Q,P}(c_i - 2, 0)}{2W_{Q,P}(2, 0)W_{Q,P}(c_i, 0)^3}\right)^{q^i}$$

To summarize, we show formulae of cryptographic pairings:

Theorem 4. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ and $\pi_q : (x, y) \mapsto (x^q, y^q)$ the q-Frobenius endomorphism on E. We assume that the embedding degree $k > 1$. Let r be a large prime number with $r | \#E(\mathbb{F}_q)$ and $(r, q) = 1$, and also $T \equiv q \pmod{r}$ and $T_i \equiv q^i \pmod{r}$. Let $\lambda = \sum_{i=0}^{l} c_i q^i$ be such that $r | \lambda$ and $r^2 \nmid \lambda$. We define $s_i = \sum_{j=i}^{l} c_j q^j$.*

Then, we have the following.

Tate Pairing: *For $P \in E(\mathbb{F}_{q^k})[r]$ and $Q \in E(\mathbb{F}_{q^k})$,*

$$\tau_r(P, Q) = f_{r,P}(Q)^{\frac{q^k-1}{r}} = \tilde{W}_{P,Q}(r+1, 1)^{\frac{q^k-1}{r}} \ .$$

Variants of the Tate Pairing: *For $P \in \mathbb{G}_1 = E(\mathbb{F}_{q^k})[r] \cap \mathrm{Ker}(\pi_q - 1)$ and $Q \in \mathbb{G}_2 = E(\mathbb{F}_{q^k})[r] \cap \mathrm{Ker}(\pi_q - q)$,*

- *Ate*

$$\alpha(Q, P) = f_{T,Q}(P)^{\frac{q^k-1}{r}} = \tilde{W}_{Q,P}(T, 1)^{\frac{q^k-1}{r}} \ ;$$

- *Ate$_i$*

$$\alpha_i(Q, P) = f_{T_i,Q}(P)^{\frac{q^k-1}{r}} = \tilde{W}_{Q,P}(T_i, 1)^{\frac{q^k-1}{r}} \ ;$$

- *R-Ate*

$$\begin{aligned} R_{A,B}(Q, P)^{\frac{q^k-1}{r}} &= \left\{ f_{a,[B]Q}(P) \cdot f_{b,Q}(P) \cdot G_{[aB]Q,[b]Q}(P) \right\}^{\frac{q^k-1}{r}} \\ &= \left\{ \tilde{W}_{[B]Q,P}(a, 1) \cdot \tilde{W}_{Q,P}(b, 1) \cdot {G_{[-aB]Q,[-b]Q}}^{-1}(P) \right\}^{\frac{q^k-1}{r}} \ , \end{aligned}$$

  where $A = aB + b$;
- *optimal*

$$\begin{aligned} a_{[c_0,c_1,\ldots,c_l]}(Q, P) &= \left\{ \prod_{i=0}^{l} f_{c_i,Q}(P)^{q^i} \cdot \prod_{i=0}^{l-1} G_{[s_{i+1}]Q,[c_i q^i]Q}(P) \right\}^{\frac{q^k-1}{r}} \\ &= \left\{ \prod_{i=0}^{l} \tilde{W}_{Q,P}(c_i, 1)^{q^i} \cdot \prod_{i=0}^{l-1} {G_{[-s_{i+1}]Q,[-c_i q^i]Q}}^{-1}(P) \right\}^{\frac{q^k-1}{r}} \ . \end{aligned}$$

For Tate pairings, we have the following stronger result.

Theorem 5. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. We assume that the embedding degree $k > 1$. Let r be a large prime number with $r | \#E(\mathbb{F}_q)$ and $(r, q) = 1$. Then, for $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})$,*

$$\tau_r(P, Q) = f_{r,P}(Q)^{\frac{q^k-1}{r}} = W_{P,Q}(r, 1)^{\frac{q^k-1}{r}} \ . \tag{4}$$

Proof. Note that Tate pairing $f_{r,P}(Q)$ is uniquely defined over $\pmod{(\mathbb{F}_{q^k}^\times)^r}$ even though $f_{r,P}$ is not normalized since $P \in E(\mathbb{F}_q)[r]$. Then, just as in the proof of the Lemma 2,

$$f_{r,P}(Q) \equiv W_{-P,Q}(r,1)^{-1} \mod (\mathbb{F}_{q^k}^\times)^r .$$

Therefore, from the bilinearity of $\tau_r(P,Q) = f_{r,P}(Q)^{\frac{q^k-1}{r}}$,

$$\tau_r(P,Q) = \tau_r(-P,Q)^{-1} = W_{P,Q}(r,1)^{\frac{q^k-1}{r}} .$$

Remark 2. *The differences between (3) in Theorem 2 (see p.7) and (4) are explained as follows. In [18], Stange gave a general formula of the Tate pairing with a parameter S by using the divisor D_Q. We obtain (3) by putting $S = P$. On the other hand, we need to compute only $W_{P,Q}(r,1)$ because we evaluate the function f_P at the point Q. We can verify $W_{P,Q}(r,1) \equiv W_{P,Q}(r+1,1)$ $\pmod{(F_{q^k}^\times)^r}$ because $f_{r,P}(Q) = f_{r+1,P}(Q)$ if $[r]P = O$. (Here we note that $f_{r,P}$, $f_{r+1,P}$ are normalized.) Since we assume that P is an $\mathbb{F}_q$ rational point on E, we can compute the Tate pairing $\langle P,Q\rangle_r$ by evaluating $f_{r,P}$ at Q. Thus, the equation (4) is a special case of (3). However, (4) is sufficient and efficient for cryptographic use.*

4 Implementation

In this section, we will show some experimental results for implementations of various pairings using elliptic nets.

The computer specifications are the following: CPU, a 2 GHz AMD Opteron 246; memory, 4 GB; and hard disk, 160 GB. Magma [23] was used as the software for writing the program.

We used the following elliptic curves for our experiments.

1 $y^2 = x^3 + 4$ [4]
$k = 12$,
$q = 23498017525968473690296083113864677063688317873484513641020158425447$ (224 bit),
$r = 1706481765729006378056715834692510094310238833$ (151 bit),
$T = T_n = 203247593908$.

2 $y^2 = x^3 + 3$ [5]
$k = 12$,
$q = 1461501624496790265145448589920785493717258890819$ (160 bit),
$r = 1461501624496790265145447380994971188499300027613$ (160 bit),
$T = T_n = 1208925814305217958863206$.

3 $y^2 = x^3+2x+25575441317520594647996278509327595814781177583607486825447\backslash$
$5542022504589304559812663114754842137$ [13]
$k = 10$,
$q = 26916561140498229883766759145747954228067854557496271814329 7\backslash$

$96276308782360965160815950571330669569$ (324 bit),
$r = 1184972659906501436389408869130632556884221748131065689 61$ (187 bit),
$T = -121311330230754125750006114860552668515956101916928 15,$
$T_n = 104334294221056.$

The Tables 1 and 2 show the experimental results of our implementations. The column "EN" indicates a computation using elliptic nets. The column "Miller" indicates a computation using Miller's algorithm. Note that we did not use built-in functions in Magma (such as "ReducedTatePairing") but rewrote Miller's algorithm by using the Magma language.

The column "R-Ate (i)" corresponds to the index i in Corollary 3.3 of [10]. Note that showing values in some cells parenthetically indicates that those values correspond to values in other cells. For example, the calculation of the Ate$_i$ pairing is sometimes equivalent to that of the Ate pairing.

Our experimental results show that pairing computations using elliptic nets is comparable to those using Miller algorithm in terms of efficiency. However, our implementations were not optimized, and so we need to study these algorithms in detail and optimize their implementations of various pairings.

Table 1. Experimental Results for Tate, Ate, and Ate$_i$ Pairings

	Tate		Ate		Ate$_i$	
curve	EN[s]	Miller[s]	EN[s]	Miller[s]	EN[s]	Miller[s]
1	0.19	0.26	0.22	0.19	(0.22)	(0.19)
2	0.13	0.21	0.24	0.21	(0.24)	(0.21)
3	0.21	0.31	0.39	0.37	0.23	0.22

Table 2. Experimental Results for R-Ate and Optimal Pairings

	R-Ate (2)		R-Ate (3)		R-Ate (4)		Optimal	
curve	EN[s]	Miller[s]	EN[s]	Miller[s]	EN[s]	Miller[s]	EN[s]	Miller[s]
1	0.65	0.51	0.38	0.31	0.39	0.32	0.98	0.76
2	0.34	0.27	0.33	0.27	0.34	0.26	0.74	0.56
3	0.73	0.67	0.36	0.34	0.40	0.38	1.07	0.94

5 Conclusion

In this paper, we explicitly gave a normalization of elliptic nets and gave formulae based on elliptic nets for computing some variants of the Tate pairing: the Ate, Ate$_i$, R-Ate, and optimal pairings. We also discussed their efficiency by using some experimental results. Further improvement and optimization of these elliptic net-based algorithms are expected in future work.

Acknowledgment. The authors would like to thank the anonymous referees for various improvements. This work was supported Grants-in-Aid for Scientific Research 20540125, 22500005 and 22300002.

References

1. Barreto, P.S.L.M., Galbraith, S.D., ÓhÉigeartaigh, C., Scott, M.: Efficient pairing computation on supersingular abelian varieties. Designs, Codes and Cryptography 42(3), 239–271 (2007)
2. Barreto, P.S.L.M., Kim, H.Y., Lynn, B., Scott, M.: Efficient algorithms for pairing-based cryptosystems. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 354–369. Springer, Heidelberg (2002)
3. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–369. Springer, Heidelberg (2001)
4. Barreto, P.S.L.M., Lynn, B., Scott, M.: Constructing elliptic curves with prescribed embedding degrees. In: Cimato, S., Galdi, C., Persiano, G. (eds.) SCN 2002. LNCS, vol. 2576, pp. 257–267. Springer, Heidelberg (2003)
5. Barreto, P.S.L.M., Naehrig, M.: Pairing-friendly elliptic curves of prime order. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 319–331. Springer, Heidelberg (2006)
6. Duursma, I., Lee, H.-S.: Tate Pairing Implementation for Hyperelliptic Curves $y^2 = x^p - x + d$. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 111–123. Springer, Heidelberg (2003)
7. Galbraith, S.D.: Pairings. In: Blake, I., Seroussi, G., Smart, N. (eds.) Advances in Elliptic Curve Cryptography, Ch. IX, Cambridge University Press, Cambridge (2005)
8. Hess, F., Smart, N.P., Vercauteren, F.: The Eta pairing revisited. IEEE Transaction on Information Theory 52(10), 4595–4602 (2006)
9. Joux, A.: A one round protocol for tripartite Diffie–Hellman. In: Bosma, W. (ed.) ANTS 2000 Part IV. LNCS, vol. 1838, pp. 385–393. Springer, Heidelberg (2000)
10. Lee, E., Lee, H.S., Park, C.M.: Efficient and generalized pairing computation on abelian varieties. IEEE Transactions on Information Theory 55(4), 1793–1803 (2009)
11. Miller, V.S.: Short programs for functions on curves (1986), `http://crypto.stanford.edu/miller/miller.pdf`
12. Miller, V.S.: The Weil pairing and its efficient calculation. Journal of Cryptology 17(4), 235–261 (2004)
13. Murphy, A., Fitzpatrick, N.: Elliptic Curves for Pairing Applications. Cryptology ePrint Archive, Report 2005/302 (2005), `http://eprint.iacr.org/2005/302.pdf`
14. Ogura, N., Uchiyama, S., Kanayama, N., Okamoto, E.: A note on the pairing computation using normalized Miller functions, to appear in IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences
15. Sakai, R., Ohgshi, K., Kasahara, M.: Cryptosystems based on pairings. In: Symposium on Cryptography and Information Security 2000, SCIS (2000)
16. Schoof, R.: Elliptic curves over finite fields and computation of square roots mod p. Math. Comp. 44, 483–494 (1985)
17. Silverman, J.H.: The arithmetic of elliptic curves. Graduate Texts in Mathematics, vol. 106. Springer, Heidelberg (1986)

18. Stange, K.E.: The tate pairing via elliptic nets. In: Takagi, T., Okamoto, T., Okamoto, E., Okamoto, T. (eds.) Pairing 2007. LNCS, vol. 4575, pp. 329–348. Springer, Heidelberg (2007)
19. Taylor, G.: Stange's algorithm for elliptic nets, `http://maths.straylight.co.uk/archives/102`
20. Zhao, C.-A., Zhang, F., Huang, J.: A note on the Ate pairing. International Journal of Information Security 6(7), 379–382 (2008)
21. Vercauteren, F.: Optimal pairings. IEEE Transactions on Information Theory 56(1), 455–461 (2010)
22. Ward, M.: Memoir on elliptic divisibility sequence. American Journal of Mathematics 70, 31–74 (1948)
23. MAGMA group, Magma, `http://magma.maths.usyd.edu.au/magma/`