Cryptographic Pairings Based on Elliptic Nets

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

[1] Tokyo Metropolitan University
[2] University of Tsukuba

Abstract. In 2007, Stange proposed a novel method of 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 that satisfy a certain recurrence relation. In this paper, we explicitly give formulae for computing some variants of the Tate pairing: Ate, Ate$_i$, R-Ate and Optimal pairings, based on elliptic nets. We also discuss their efficiency by using some experimental results.

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

1 Introduction

Recently, pairing-based cryptosystems 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 tri-partie Diffie-Hellman key exchange and the identity-based encryption schemes [3], [9], [14]. With respect to the efficient implementation of pairing-based cryptographic schemes, the computation of pairings such as the Weil and Tate pairings is to the bottleneck. Currently, the most suitable pairing for the efficient implementation of pairing-based cryptographic schemes is the Tate pairing. So, a lot of algorithms for the efficient computation of the Tate pairing and also some its variants such as η_T [1], Duursma-Lee method [6], Ate [8], Ate$_i$ [19], R-Ate [10] and Optimal pairings [20] have been proposed.

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. So, Miller's algorithm is linear time in the size of some input parameter r. Also it depends on the Hamming weight of r. Most improvements of pairing computation attempt to shorten the number of iterations of the loop, so-called Miller's loop, in

the algorithm. Actually, the Ate, Ate_i, R-Ate and Optimal pairings are truncated loop variants of the Tate pairing.

In 2007, Stange [17] 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 some non-linear recurrence sequences related to elliptic functions. In 1948, Ward [21] first studied some 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. Naturally, as in the case of Miller's algorithm, the algorithm is linear time in the size of r. In both Miller and elliptic net algorithms, we have two internal steps so-called Double and DoubleAdd [17]. In Miller's algorithm, the cost of DoubleAdd is about twice that of Double. On the other hand, in the elliptic net algorithm, these two steps take almost the same time. Namely, the running time of the algorithm would be independent of the Hamming weight of r. That is, elliptic net based Tate pairing is expected to be resistant against side channel attacks.

Since the efficiency of the algorithm is comparable to that of Miller's algorithm, by using further improvement and optimization, we would expect that elliptic net algorithm provides an efficient alternative to Miller's algorithm.

Therefore, from both theoretical and practical points of view, it would be important for us to investigate explicit formulae for computing some variants of the Tate pairing based on elliptic nets.

In this paper, we explicitly give formulae for computing some variants of the Tate pairing: Ate, Ate_i, R-Ate and Optimal pairings, based on elliptic nets. We also discuss their efficiency by using some experimental results.

This paper is organized as follows. Section 2 gives a brief mathematical description of pairings and elliptic nets. Section 3 contains our main results about 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, i.e. the smallest positive integer such that r divides $q^k - 1$. Let π_q be the Frobenius endomorphism, i.e. $\pi_q : E \to E : (x, y) \mapsto (x^q, y^q)$. We denote the trace of Frobenius with t, i.e. $\#E(\mathbb{F}_q) = q + 1 - t$. 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 which is 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 a choice of D_P and D_Q. Furthermore, the Weil pairing is bilinear and non-degenerate. Refer to [7] for more information on pairings.

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 is shown that $\langle P, Q\rangle_r$ has bilinearity and non-degeneracy.

For application to cryptography, it is convenient to define pairings whose outputs are unique values rather than equivalent classes. So, we usually 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.

Weil pairing and Tate pairing satisfy that

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

So, if cost of final exponentiation is sufficiently small, cost of computing Tate pairing is almost half of that of computing Weil pairing. Hence,

Tate pairing is widely used for cryptographic use and numerous improved versions of Tate pairing, such as Ate pairing and so on.

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

For cryptographic application, we usually consider that points P and Q are 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 $Q \in \mathbb{G}_2$.

Barret 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 $k > 1$.

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

Let $T = t - 1$. We set integers N by $N = \gcd(T^k - 1, q^k - 1)$ and L by $T^k - 1 = LN$. We assume that r^2 does not divide $q^k - 1$.

Ate pairing is defined by $f_{T,Q}(P)(Q \in \mathbb{G}_2$ and $P \in \mathbb{G}_1)$. Ate pairing is also defined in On $\mathbb{G}_1 \times \mathbb{G}_2$ (See [8] for detail). However, we consider only the case of $\mathbb{G}_2 \times \mathbb{G}_1$ in this paper. We denote by $\alpha(Q, P)$ reduced Ate pairing: $\alpha(Q, P) := f_{T,Q}(P)^{(q^k-1)/r}$. Length of Miller's loop for computing Ate pairing $f_{T,Q}(P)$ is $\log_2 |T|$.

Ate$_i$ Pairing : The Ate$_i$ pairing is proposed by Zhao et al. [19]. Let $T_i := q^i \pmod r$ for $i = 1, 2, \cdots, k-1$. For each i, we define the following quantities as similar as Ate pairing: a_i be the smallest positive integer such that $T_i^{a_i} \equiv 1 \pmod r$. And $N_i := \gcd(T_i^{a_i} - 1, q^k - 1)$, L_i be the positive integer such that $T_i^{a_i} - 1 = L_i N_i$.

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 $P \in \mathbb{G}_1)$. As similar as the Ate pairing, we denote by $\alpha_i(Q, P)$ reduced Ate$_i$ pairing: $\alpha_i(Q, P) := f_{T_i,Q}(P)^{(q^k-1)/r}$. Length of Miller's loop for computing $f_{T_i,Q}(P)$ is $\log_2(T_i)$

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

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

$$R_{A,B}(Q,P) := f_{a,BQ}(P) \cdot f_{b,Q}(P) \cdot G_{aBQ,bQ}(P),$$

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. [10] 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 some 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 is proposed by Vercauteren [20]. 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 $\epsilon(k) \leq \log_2 k$).

Theorem 1 ([20] 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 $a_{[c_0,c_1,\cdots,c_l]}(Q,P)$ can be computed very efficiently if we can choose $c_0, c_1, \cdots, c_l$ very small.

2.2 Elliptic Nets

In 2007, Stange [17] defined elliptic nets which are maps from $\mathbb{Z}^n$ to a ring that satisfy a certain recurrence relation associated with elliptic curves. In general, Stange defined an elliptic net by the following: an elliptic net W

is a map from a finitely generated abelian group $\mathcal{A}$ to an integral domain $\mathcal{R}$, which satisfies 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. Actually, elliptic divisibility 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 main tools of Schoof's algorithm [15]. As we will see later, the division polynomials of an elliptic curve also play an important role in the computation of elliptic nets based pairings.

Stange gave elliptic nets associated to elliptic curves and described Tate pairing by using elliptic nets. In this section, we briefly review elliptic nets. See [17] for detail.

First, we consider a function, denoted by Ψ, associated to elliptic curves over $\mathbb{C}$ by using elliptic σ-function. We define an elliptic net W (in $\mathbb{C}$) using Ψ. Next we make Ψ to a function, denoted by Ω, defined in finite fields by reduction theorem (See Theorem 3 in [17]). So, we are able to consider W in finite fields and construct Tate pairing in finite fields.

To describe Tate pairing, Stange considered a function $\Omega_{1,v_2,v_3}(-S,P,Q)$ whose divisor on a variable S is $([v_2]P + [v_3]Q) - v_2(P) - v_3(Q) - (1 - v_2 - v_3)(O)$, where v_i are integers and P, Q are points on an elliptic curve over a finite field. Next, Stange showed that a function $f_{r,P}$ with $\mathrm{div}(f_P) = r(P) - r(O)$ can be expressed by $f_{r,P} = \dfrac{\Omega_{1,0,0,}(-S,P,Q)}{\Omega_{1,r,0}(-S,P,Q)}$. Then, Stange gave a formula of $f_{r,P}(D_Q)$, where D_Q is a divisor equivalent to $(-S) - (-S-Q)$, as a function in the variable S. Finally, Stange obtained the following result by putting $S = P$.

Theorem 2 ([17]) *Let E be an elliptic curve over a finite field K. For $P \in E(K)[r]$, $Q \in E(K)$,*

$$f_{r,P}(D_Q) = \frac{W_{P,Q}(r+1,1)W_{P,Q}(1,0)}{W_{P,Q}(r+1,0)W_{P,Q}(1,1)}, \tag{2}$$

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

[3] Note that we have $W_{P,Q}(1,0) = W_{P,Q}(1,1) = 1$.

Remark 1 *By using the theorem above and the equation (1), we can easily obtain the Weil pairing formula with 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 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 definition(see [17]): let $P = (x_1, y_1)$ 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 ([17])

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

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 recursive formulae of computing $W(2i-1, 0)$ and $W(2i-1, 0)$ is same as recursive formulae of division polynomials. So, if E is defined over K and $P \in E(K)$, $W_{P,Q}(i,0) \in K$ for all i and they vanish by final exponentiation.

See [17] for algorithms for computing elliptic nets.

3 The Main Results

3.1 Elliptic Net Based Pairings

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

First we explain the key lemma which connects various pairings with elliptic nets.

Lemma 1 *Assume that the function $f_{s,P}$ is well-defined over* $\bmod (\mathbb{F}_{q^k}{}^{\times})^r$. *Then, for an integer $s \in \mathbb{Z}$,*

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

Proof. Let $W_{-P,S}(s,\ 1) = \Omega_{s,1}(-P,\ S)$ be a rational function in variable S. As similar in [17], 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, $f_{s,P} \equiv W_{-P,Q}(s,1)^{-1} \pmod{(\mathbb{F}_{q^k}{}^{\times})^r}$. Finally, we obtain by putting $S = Q$.

Note that $f_{s,P}$ included in each pairing formula is well-defined over $(\mathbb{F}_{q^k}{}^{\times})^r$. This means that $(f_{s,P}(Q) \cdot W_{-P,Q}(s,1))^{(q^k-1)/r} = 1$.

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

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

$$A(P,\ Q) = \prod_{i=0}^{l} f_{c_i,P}^{d_i}(Q),$$

is bilinear, then

$$A(P,\ Q) = \prod_{i=0}^{l} W_{P,Q}^{d_i}(c_i,\ 1)\ .$$

Proof. Using Lemma1 and bilinearity of $A(P,\ Q)$,

$$\begin{aligned} A(P,\ Q) &= A(-P,\ Q)^{-1} \\ &= \prod_{i=0}^{l} f_{c_i,-P}^{-d_i}(Q) = \prod_{i=0}^{l} W_{P,Q}^{d_i}(c_i,\ 1)\ . \end{aligned}$$

□

We consider the case of optimal pairing. In this case, we need to compute scalar multiplications $[c_i q^i]Q (i = 0, 1, \cdots, l)$ by 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 [17], $W_{Q,P}(n, 0) = \psi_n(x_Q, y_Q)$. So, 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 $[c_i q^i]Q = \pi_q^i([c_i]Q) = (x_{[c_i]Q}^{q^i}, y_{[c_i]Q}^{q^i})$ by

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

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

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 $(r, q) = 1$. Also $T \equiv q \pmod r$ and $T_i \equiv q^i \pmod r$. Let $\lambda = \sum_{i=0}^{l} c_i q^i$ 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 $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})$,*

$$\tau_r(P, Q) = f_{r,P}(Q)^{\frac{q^k - 1}{r}} = W_{P,Q}(r, 1)^{\frac{q^k - 1}{r}}\ . \tag{3}$$

variants of 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*

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

– *Ate$_i$*

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

– *R-Ate*

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

where $A = aB + b$.

– *Optimal*

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

Remark 2 *We explain differences between (2) and (3). In [17], Stange gave a general formula of the Tate pairing with a parameter S by using the divisor D_Q. We obtain (2) 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 $W_{P,Q}(r,1) \equiv W_{P,Q}(r+1,1) \pmod{(F_{q^k}^{\times})^r}$ since $f_{r,P}(Q) = f_{r+1,P}(Q)$ if $[r]P = O$. 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 (3) would be a special case of (2). However, (3) is sufficient and efficient for cryptographic use.*

3.2 Some Remarks

We describe some useful propositions for computing elliptic nets.

Proposition 2 *For an integer $e \in \mathbb{Z}$,*

$$W_{P,Q}(s,1) = \frac{W_{P,Q-eP}(s+e,1)}{W_{P,Q}(e,1)^{1-s} \cdot W_{P,Q}(1+e,1)^s} \ .$$

Proof. The proposition 2 of [17] derives the proposition with the following parameters.

– z_1, z_2 corresponding to P, $Q - eP$, respectively.
– $v_1 = s,\ v_2 = 1$.
– $T = \begin{pmatrix} 1 & e \\ 0 & 1 \end{pmatrix}$.

We can prove immediately the following formula.

Corollary 1 *For an integer $e \in \mathbb{Z}$,*

$$W_{P,Q}(s,1) = \frac{W_{P,Q-eP}(s+e,1)}{W_{P,Q}(e,1)} \cdot \Big(\frac{W_{P,Q}(-1,1)^e}{W_{P,Q}(e,1) \cdot W_{P,P+Q}(e,1)}\Big)^s .$$

Especially, we apply the corollary in the case that e is a power of 2. If the Hamming weight of s is small, we may compute $W_{P,Q}(s,1)$ by using the corollary repeatedly.

4 Implementation

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

We used the computer whose CPU is 2GHz AMD Opteron 246, memory is 4GB, and hard disk is 160GB. Magma [22] was used as a software for writing the program.

We used the following elliptic curves for our experiments.

1 $y^2 = x^3 + 4$ [4]
$k = 12$, $q = 234980175259684736902960831138646770636883178734845136410201584254 47$ (224 bit), $r = 17064817657290063780567158346925100943102388 33$ (151 bit), $T = T_n = 203247593908$.

2 $y^2 = x^3 + 3$ [5]
$k = 12$, $q = 14615016244967902651454485899207854937172588908 19$ (160 bit),
$r = 14615016244967902651454473809949711884993000276 13$ (160 bit), $T = T_n = 120892581430521795886320 6$.

3 $y^2 = x^3+2x+25575441317520594647996278509327595814781177583607486825447 5\backslash$
$5542022504589304559812663114754842137$ [13]
$k = 10$, $q = 2691656114049822988376675914574795422806785455749627181432 97\backslash$
$9627630878236096516081595057133066956 9$ (324 bit),
$r = 11849726599065014363894088691306325568842217481310656896 1$ (187 bit),
$T = -12131133023075412575000611486055266851595610191692815$,$T_n = 104334294221056$.

The Table 1, 2 shows experimental results of our implementations. The column "EN" means a computation with elliptic nets. The column "miller" means a computation with miller's algorithm. Note that we did not use

built-in functions in Magma (such as "ReducedTatePairing") but rewrite miller's algorithm by using Magma's language.

The column "R-Ate (i)" corresponding to the index i in the Corollary 3.3 of [10]. Note that the parenthetic values in some cells mean that these values are corresponding to values in other cells. For example, the Ate_i pairing may equal to the Ate pairing.

Our experimental results show that pairing computations with elliptic nets is comparable the ones with miller's algorithm on the efficiency. However, our implementations are not optimized, so we have to study these algorithms in detail and optimize implementations of computations of various pairings.

Table 1. Experimental Results for Tate, Ate, 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, 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 formulae for computing some variants of the Tate pairing: Ate, Ate_i, R-Ate and Optimal pairings, based on elliptic nets. We also discussed their efficiency by using some experimental results. Further improvement and optimization of the elliptic net based algorithms are expected.

References

1. P.S.L.M. Barreto, S. Galbraith, C. ÓhÉigeartaigh, and M. Scott, "Efficient pairing computation on supersingular abelian varieties," *Designs, Codes and Cryptography*, Vol.42, No.3, pp.239-271, Springer, 2007.
2. P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott, "Efficient Algorithms for Pairing-Based Cryptosystems," *CRYPTO 2002*, LNCS 2442, pp. 354-369, 2002.
3. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *CRYPTO 2001*, LNCS 2139, pp. 213–369, 2001.
4. P.S.L.M. Barreto, B. Lynn, and M. Scott, "Constructing elliptic curves with prescribed embedding degrees," *SCN 2002*, LNCS 2576, pp. 263–273, 2002.
5. P.S.L.M. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order," *SAC 2005*, LNCS 3897, pp. 319–331, 2006.
6. I. Duursma and H.S. Lee, "Tate Pairing Implementation for Hyperelliptic Curves $y^2 = x^p - x + d$," *Advances in Cryptology–ASIACRYPT 2003*, LNCS 2894, pp. 111–123, Springer-Verlag, 2003.
7. S. D. Galbraith, Pairings, Chapter IX of book Advances in elliptic curve cryptography, edited by I. Blake, G. Seroussi and N. Smart, Cambridge University Press, 2005.
8. F. Hess, N.P. Smart and F. Vercauteren, "The Eta pairing Revisited," *IEEE Transaction on Information Theory*, vol.52, NO. 10, pp. 4595–4602, OCTOBER 2006.
9. A. Joux, "A one round protocol for tripartite Diffie-Hellman," *ANTS IV*, LNCS 1838, pp. 385–3393, 2000.
10. E. Lee, H.S. Lee, and C. M. Park, "Efficient and Generalized pairing Computation on Abelian Varieties," *Cryptology ePrint Archive*, Report 2008/040, 2008. `http://eprint.iacr.org/2008/040.pdf`.
11. V.S. Miller, "Short Programs for functions on Curves," 1986. `http://crypto.stanford.edu/miller/miller.pdf`.
12. V.S. Miller. "The Weil pairing and its efficient calculation," *Journal of Cryptology*, Vol. 17, No. 4, pp. 235–261, 2004.
13. A. Murphy, N. Fitzpatrick, " Elliptic Curves for Pairing Applications," *Cryptology ePrint Archive*, Report 2005/302, 2005. `http://eprint.iacr.org/2005/302.pdf`.
14. R. Sakai, K. Ohgshi and M. Kasahara, "Cryptosystems based on pairings," *Symposium on Cryptography and Information Security 2000*, SCIS2000, 2000.
15. R.Schoof, "Elliptic Curves over Finite Fields and Computation of Square Roots mod p," *Math. Comp.*, **44**, pp.483–494, 1985.
16. J. H. Silverman, "The arithmetic of elliptic curves," *Graduate Texts in Mathematics*, 106. Springer-Verlag, New York, 1986
17. K. E. Stange, "The Tate Pairing Via Elliptic Nets," *Pairing Conference 2007*, LNCS 4575, pp. 329–348, 2007.
18. G. Taylor, "Stange's Algorithm for Elliptic Nets." `http://maths.straylight.co.uk/archives/102`.
19. C.-A. Zhao, F. Zhang and J. Huang "A Note on the Ate pairing," *International Journal of Information Security*, Vol. 6, No. 7, pp. 379–382, 2008. *Cryptology ePrint Archive*, Report 2007/247, 2007. `http://eprint.iacr.org/2007/247`.
20. F. Vercauteren, "Optimal pairings," *IEEE Transactions on Information Theory*, Vol. 56, No. 1, pp. 455–461, 2010. *Cryptology ePrint Archive*, Report 2008/096,

2008.
http://eprint.iacr.org/2008/096.pdf.
21. M. Ward, "Memoir on elliptic divisibility sequence," *American Journal of Mathematics*, 70, pp.31–74, 1948.
22. MAGMA group, Magma.
http://magma.maths.usyd.edu.au/magma/.