SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

May 2014, Vol. 57 052108:1–052108:10
doi: 10.1007/s11432-013-4840-7

Implementing optimized pairings with elliptic nets

TANG ChunMing[1,2], NI DongMei[2], XU MaoZhi[2], GUO BaoAn[3] & QI YanFeng[2,3]*

[1]*School of Mathematics and Information, China West Normal University, Nanchong* 637002*, China;*
[2]*LMAM, Chinese Ministry of Education, Peking University, and School of Mathematical Sciences, Peking University, Beijing* 100871*, China;*
[3]*Aisino Corporation Inc., Beijing* 100195*, China*

Received March 1, 2013; accepted May 6, 2013; published online June 28, 2013

Abstract In this paper, we use elliptic nets to implement the optimized Ate pairings and optimal pairings on the Barreto-Naehrig curves with embedding degree 12. In order to do the arithmetic of elliptic curves over finite fields with elliptic nets, we first give some basic properties of elliptic nets associated to elliptic curves over finite fields and the expression of Miller function in terms of elliptic nets. Then we give formulae to compute some optimized pairings with elliptic nets, which is a new method to implement pairings. This method with elliptic nets has time complexity comparable to Miller's algorithm and it can be optimized.

Keywords elliptic curves, elliptic nets, pairings, Miller's algorithm, pairing-based cryptography

Citation Tang C M, Ni D M, Xu M Z, et al. Implementing optimized pairings with elliptic nets. Sci China Inf Sci, 2014, 57: 052108(10), doi: 10.1007/s11432-013-4840-7

1 Introduction

Pairings on elliptic curves have been widely applied in the construction of cyptographic protocals, such as identity based encryption [1], the tripartite Diffie-Hellman protocol [2], short signatures [3], public key encryption with keyword search [4]. Consequently, pairing-base cryptography has developed rapidly [5–8]. The efficiency of pairing-based cryptography is dependent on the costly computation of pairings [9–11]. Miller's algorithm is often used as a polynomial time algorithm for implementing pairings. Stange [12] introduced another method to compute Tate pairing with elliptic nets.

An elliptic net is a function satisfying a certain recurrence relation and it is a generalization of elliptic divisibility sequences [13–15]. With elliptic nets, Stange [16] gave another view of the discrete logarithm problem on elliptic curves, Tate pairing and Weil pairing. Hence, it is a new approach. For elliptic nets $W(a,b)$ with two variables, Stange gave an elliptic net algorithm for calculating $W(a,0)$ and $W(a,1)$ with initial values and proposed an algorithm for computing Tate pairing and Weil pairing with $W(a,0)$ and $W(a,1)$. This new algorithm has the same loop length as Miller's algorithm and it is rapidly developing.

The computation of pairing is the bottleneck to efficient pairing-based cryptography. A main method to optimize the pairing computation is to construct pairing with short loop length [17–20]. Hess [18] proposed the Ate pairing with shorter loop length than Tate pairing. Moreover, some pairing friendly

*Corresponding author (email: qiyanfeng07@163.com)

elliptic curves [21,22] are used to construct pairing. In this paper, our main task is implementing these pairings with elliptic nets, thus offering another view of these pairings.

The remainder of the paper is organized as follows. In Section 2, we review some results of elliptic nets, pairings, Barreto-Naehrig curves and the methods of computing Tate pairing with elliptic nets. In Section 3, we give some properties of elliptic nets over finite fields and discuss how to compute Miller function with elliptic nets. Then we use elliptic nets to implement the optimized pairings. Section 4 concludes the paper.

2 Preliminary

2.1 Elliptic nets

Stange [12] introduced elliptic nets to pairing computation. In this subsection we give a review of some results of elliptic nets.

An elliptic net is a function satisfying a recurrence identity. Its definition is given below.

Definition 1. Let A be a finitely generated free Abelian group and R be an integral domain. An elliptic net is any map $W : A \to R$ such that the following recurrence holds for all p, q, r, $s \in A$:

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

From the definition of elliptic net, we can get $W(-p) = -W(p)$ for any $p \in A$. In particular, $W(0) = 0$.

Stange [12] constructed elliptic nets associated to elliptic curves over number fields, reduced them and got elliptic nets associated to elliptic curves over finite fields. We list the relevant notations here for the rest of the paper.

L	A number field in $\mathbb{C}$
E_L	An elliptic curve defined over L
R	The ring of integers of L
$\mathfrak{P}$	The prime of R of good reduction for E_L
k	the residue field of $\mathfrak{P}$
$\delta : E_L(L) \longrightarrow E_k(k)$	The reduction map modulo $\mathfrak{P}$
$\delta : P^1(L) \longrightarrow P^1(k)$	The reduction map modulo $\mathfrak{P}$
$\overline{P} = \sigma(P)$	The reduction of a point$P$ on $E_L(L)$
$\mathcal{O}$	The infinite point for both $E_L(L)$ and $E_k(k)$

In order to define elliptic nets from elliptic curves, we begin with elliptic functions. Fix a complex lattice $\wedge$ corresponding to the elliptic curve E_L. The Weierstrass sigma function is defined by

$$\sigma(z;\wedge) = z \prod_{\omega\in\wedge,\omega\neq 0} \left(1 - \frac{z}{\omega}\right) \mathrm{e}^{-\frac{z}{\omega} - \frac{1}{2}(\frac{z}{\omega})^2}.$$

To obtain an elliptic net from an elliptic curve, we still need a function $\Psi_{\boldsymbol{v}}$. The function $\Psi_{\boldsymbol{v}}$ is defined by

$$\Psi_{\boldsymbol{v}}(\boldsymbol{z};\wedge) = \frac{\sigma(v_1 z_1 + \cdots + v_n z_n;\wedge)}{\prod_{i=1}^{n} \sigma(z_i;\wedge)^{2v_i^2 - v_i \sum_{j=1}^{n} v_j} \prod_{1\leqslant i<j\leqslant n} \sigma(z_i + z_j;\wedge)^{v_i v_j}}.$$

For notational simplicity, we omit the arguments $(\boldsymbol{z};\wedge)$ and write $\Psi_{\boldsymbol{v}}$ for $\Psi_{\boldsymbol{v}}(\boldsymbol{z};\wedge)$. An important property of $\Psi_{\boldsymbol{v}}$ is that it is an elliptic function in every variable z_i; that is, $\Psi_{\boldsymbol{v}}$ can be treated as a function over E^n. Then we use the same notation $\Psi_{\boldsymbol{v}}$ for $\Psi_{\boldsymbol{v}}(\boldsymbol{P};E)$, where $\boldsymbol{P} \in E^n$.

The following theorem describes the symmetry of variables $\boldsymbol{v}$ and $\boldsymbol{z}$, which is helpful for computation.

Theorem 1. Fix a lattice $\wedge \subset \mathbb{C}$ corresponding to an elliptic curve. Let $\boldsymbol{v} \in \mathbb{Z}^n$ and $\boldsymbol{z} \in \mathbb{C}^n$. Let $\boldsymbol{T}$ be an $n \times n$ matrix with entries in $\mathbb{Z}$ and transpose $\boldsymbol{T}^{\mathrm{T}}$. Then

$$\Psi_{\boldsymbol{v}}(\boldsymbol{T}^{\mathrm{T}}(\boldsymbol{z}); \wedge) = \frac{\Psi_{\boldsymbol{T}(\boldsymbol{v})}(\boldsymbol{z}; \wedge)}{\prod_{i=1}^{n} \Psi_{\boldsymbol{T}(\boldsymbol{e}_i)}(\boldsymbol{z}; \wedge)^{2v_i^2 - v_i \sum_{j=1}^{n} v_j} \prod_{1 \leqslant i < j \leqslant n} \Psi_{\boldsymbol{T}(\boldsymbol{e}_i + \boldsymbol{e}_j)}(\boldsymbol{z}; \wedge)^{v_i v_j}},$$

where $\boldsymbol{e}_i$ is a vector with the ith entry 1 and other entries 0.

We will see that under some conditions $\Psi_{\boldsymbol{v}}$ forms an elliptic net.

Theorem 2. Let $\mathcal{O}$ be the infinite point of E_L. Let $P_1, \ldots, P_n$ be n points in $E_L(L)$, where each P_i is distinct from $\mathcal{O}$. Then $\Psi_{\boldsymbol{v}}(P_1, \ldots, P_n)$ forms an elliptic net as a function of $\boldsymbol{v} \in \mathbb{Z}^n$.

To extend the relationship between elliptic nets and elliptic curves over finite fields, we should reduce $\Psi_{\boldsymbol{v}}$ and get elliptic nets from elliptic curve E_k.

Theorem 3. Let $P_1, \ldots, P_n \in E_L(L)$. Then for each $\boldsymbol{v} \in \mathbb{Z}^n$, there exists a function $\Omega_{\boldsymbol{v}}$ such that the following diagram commutes:

$$\begin{array}{ccc} E_L^n(L) & \xrightarrow{\Psi_{\boldsymbol{v}}} & P^1(L) \\ {\scriptstyle\delta}\downarrow & & \downarrow{\scriptstyle\delta} \\ E_k^n(k) & \xrightarrow{\Omega_{\boldsymbol{v}}} & P^1(k). \end{array}$$

Furthermore $\mathrm{div}(\Omega_{\boldsymbol{v}}) = \delta^*(\mathrm{div}(\Psi_{\boldsymbol{v}}))$.

Then we can obtain elliptic nets from the elliptic curve E_k.

Theorem 4. Let $P_1, \ldots, P_n \in E_L(L)$, where each P_i is distinct from $\mathcal{O}$. Then $\Omega_{\boldsymbol{v}}(P_1, \ldots, P_n; E_k)$ is an elliptic net as a function of $\boldsymbol{v} \in \mathbb{Z}^n$.

In the rest of the paper, we often use $W_{P_1,\ldots,P_n}(\boldsymbol{v})$ to denote $\Psi_{\boldsymbol{v}}(P_1, \ldots, P_n)$ or $\Omega_{\boldsymbol{v}}(P_1, \ldots, P_n)$ and $W_{P_1,\ldots,P_n}(\boldsymbol{v})$ is the elliptic net proposed by Stange.

2.2 Pairings and Miller function

Let E be an elliptic curve defined over finite field $\mathbb{F}_q$, where q is a power of prime number p. Consider a large prime r such that $r|E(\mathbb{F}_q)$ and denote the embedding degree k, i.e., the smallest positive integer such that r divides $q^k - 1$. Let t be the trace of Frobenius map. Then $\#E(\mathbb{F}_q) = q + 1 - t$. Let $\mathcal{O}$ be the infinite point of E. Consider points $P, Q, R \in E(\overline{\mathbb{F}}_q)$ and an integer a. Then the Miller function $f_{a,P}$ is a rational function satisfying $\mathrm{div}(f_{a,P}) = a\langle P\rangle - \langle [a]P\rangle - (a-1)\langle\mathcal{O}\rangle$. We also define functions $l_{P,Q},\ v_R,\ g_{P,Q}$ such that

$$\begin{aligned} &\mathrm{div}(l_{P,Q}) = \langle P\rangle + \langle Q\rangle + \langle -P-Q\rangle - 3\langle\mathcal{O}\rangle, \\ &\mathrm{div}(v_P) = \langle R\rangle + \langle -R\rangle - 2\langle\mathcal{O}\rangle, \\ &\mathrm{div}(g_{P,Q}) = \langle P\rangle + \langle Q\rangle - \langle P+Q\rangle - \langle\mathcal{O}\rangle = \mathrm{div}\left(\frac{l_{P,Q}}{v_{P+Q}}\right). \end{aligned}$$

These functions are used to compute the Miller function.

Let $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_k)/rE(q^k)$. Then the Tate pairing [23] is defined by

$$\begin{aligned} \tau(\cdot,\cdot) : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) &\longrightarrow \mathbb{F}_{q^k}^{\times}/\left(\mathbb{F}_{q^k}^{\times}\right)^r, \\ (P,Q) &\longmapsto f_{r,P}(Q). \end{aligned}$$

The computation of Tate pairing is to compute the value of Miller function $f_{r,P}$ at Q. Miller's algorithm is often used to compute $f_{r,P}(Q)$ and the loop length is $\lfloor \log_2 r \rfloor$. We will introduce Ate pairing with shorter loop length.

Let ϕ be the Frobenius map of $E/\mathbb{F}_q$. Then

$$\begin{aligned}\phi: E &\longrightarrow E\\ (x,y) &\longmapsto (x^q, y^q).\end{aligned}$$

Consider $G_1 = E[r]\bigcap \ker(\phi-[1])$ and $G_2 = E[r]\bigcap \ker(\phi-[q])$. For $P \in G_1$ and $Q \in G_2$, the Ate pairing is defined by

$$\begin{aligned}\mathrm{Ate}(\cdot,\cdot): G_2\times G_1 &\longrightarrow \mathbb{F}_{q^k}^{\times}\\ (Q,P) &\longmapsto f_{T,Q}(P)^{\frac{q^k-1}{r}},\end{aligned}$$

where $T = t-1$.

The loop length of computing Ate pairing with Miller's algorithm is $\lfloor \log_2 |t-1| \rfloor$. The pairing with short loop length is what we need in pairing-based cryptography. The lower bound of the loop length is $\log_2 r/\varphi(k)$. For both security and efficiency, we should choose the right k, which is neither too big nor too small. The elliptic curves with the right embedding degree are called the pairing friendly elliptic curves. The Barreto-Naehrig curves [21] with embedding degree 12 are a family of elliptic curves getting much attraction. The parameters of Barreto-Naehrig curves are given by

$$p(x) = 36x^4 - 36x^3 + 24x^2 - 6x + 1, \quad t(x) = 6x^4 + 1,$$

where $p(x)$ is the size of the base field, $t(x)$ is the trace and x is an integer.

The main algorithm to compute Tate pairing is Miller's algorithm, which has polynomial time complexity. In the following subsection, we introduce another algorithm proposed by Stange to compute Tate pairing.

2.3 Computing Tate pairing with elliptic nets

Stange [12] gave a new approach to computing Tate pairing with elliptic nets.

Theorem 5. Let P be a r-torsion point in $E(\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_{q^k})$. Then the Tate pairing can be computed by the equation:

$$\tau(P,Q) = \frac{W_{P,Q}(r+1,1)W_{P,Q}(1,0)}{W_{P,Q}(r+1,0)W_{P,Q}(1,1)}.$$

Then the computation of Tate pairing is converted into the computation of elliptic nets, that is, the computation of $W_{P,Q}(a,b)$, where $a \in \mathbb{Z}$ and $b = 0$ or 1.

A double-and-add algorithm is given by Rachel Shipsey to compute terms of an elliptic divisibility sequence. The algorithm described here is a generalization of Shipsey's algorithm to compute $W_{P,Q}(a,b)$. Let E be an elliptic curve defined over K with the equation $E: y^2 = x^3 + Ax + B$, where the characteristic of K is distinct from 2 and 3. Consider points $P = (x_1, x_1)$ and $Q(x_2, y_2)$ in E, where $Q \neq \pm P$. For simplicity, we write $W(a,b)$ for $W_{P,Q}(a,b)$. The initial values are given below:

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

Before computing $W(a,b)$ with those initial values, we first introduce two basic algorithms.

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

Figure 1 A block centred on k.

Definition 2. A block centred on k (shown in Figure 1) of the elliptic net $W(a,b)$ consists of a first vector of eight consecutive terms of the sequence $W(i,0)$ centred on terms $W(k,0)$ and $W(k+1,0)$ and a second vector of three consecutive terms $W(i,1)$ centred on the term $W(k,1)$.

Definition 3. Given a block V centred on k, Double(V) is an algorithm that returns the block centred on $2k$.

Definition 4. Given a block V centred on k, DoubleAdd(V) is an algorithm that returns the block centred on $2k+1$.

With the definition of elliptic net $W(a,b)$, Double(V) and DoubleAdd(V) can be calculated by formulae below.

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

With Double(V) and DoubleAdd(V), we can compute $W(m,0)$ and $W(m,1)$ in elliptic nets. The algorithm for the computation is shown in Algorithm 1.

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 $W(0,1)=W(1,0)=1$ and integer $m=(d_k d_{k-1}\cdots d_1)_2$ with $d_k=1$

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

```
V ⟵ [[−a, −1, 0, 1, a, b, c, a^3 c − b^3]; [1, g, d]]
for i = k − 1 down to 1 do
    if d_i = 0 then
        V ⟵ Double(V)
    else
        V ⟵ DoubleAdd(V)
    end if
end for
return V[0, 3] and V[1, 1].
```

3 Computation of optimized pairings with elliptic nets

In this section, we will compute some optimized pairings with elliptic nets.

Theorem 6. Let $\boldsymbol{v}=(v_1,v_2,\ldots,v_n)$, where $v_1=1,\ v_2,\ldots,v_n\in\mathbb{Z}$, $\overline{P}_2,\overline{P}_3,\ldots,\overline{P}_n\in E_k(\overline{k})$ and $\pm\overline{P}_i$ are all distinct and nonzero. Consider $\Omega_{\boldsymbol{v}}(\overline{P},\overline{P}_2,\ldots,\overline{P}_n)$ as a function of $\overline{P}$. Then

$$\operatorname{div}(\Omega_{\boldsymbol{v}}) = \left\langle -\sum_{i=2}^{n}[v_i]\overline{P}_i\right\rangle - \sum_{i=2}^{n} v_i\langle -\overline{P}_i\rangle - \left(1-\sum_{i=2}^{n} v_i\right)\langle\mathcal{O}\rangle.$$

Proof. Let E_k be the reduction modulo $\mathfrak{P}$ and let P_i be the lifted point of $\overline{P_i}$. In Theorem 3, we get $\Psi_{\boldsymbol{v}} = \Psi(z, z_2, \ldots, z_n; \wedge)$, where $\wedge$ is the lattice corresponding to E_L and z_i is the complex number corresponding to P_i. Consider $\Psi_{\boldsymbol{v}}$ as a function of the first variable of z. In Theorem 3, we consider the projection of the first variable from E_L^n to E_k^n, and we still have the identity $\mathrm{div}(\Omega_{\boldsymbol{v}}) = \delta^*(\mathrm{div}(\Psi_{\boldsymbol{v}}))$. From the definition of $\Psi_{\boldsymbol{v}}$, we have

$$\Psi_{\boldsymbol{v}}(z, z_2, \ldots, z_n; \wedge) = \frac{\sigma(z + v_2 z_2 + \cdots + v_n z_n; \wedge)}{\sigma(z;\wedge)^{1-\sum_{i=2}^n v_i} \prod_{i=2}^n \sigma(z+z_i;\wedge)^{v_i} \prod_{i=2}^n \sigma(z_i;\wedge)^{2v_i^2 - \sum_{j=1}^n v_i v_j} \prod_{2\leqslant i<j\leqslant n} \sigma(z_i+z_j;\wedge)^{v_i v_j}}.$$

Then according to basic properties of σ function, we get $\mathrm{div}(\sigma(z;\wedge)) = \langle \wedge \rangle$. Hence

$$\mathrm{div}(\Psi_{\boldsymbol{v}}) = \left\langle -\sum_{i=2}^n [v_i] z_i + \wedge \right\rangle - \sum_{i=2}^n v_i \langle -z_i + \wedge \rangle - \left(1 - \sum_{i=2}^n v_i\right) \langle \mathcal{O} \rangle.$$

$\Psi_{\boldsymbol{v}}$ is an elliptic function of z. Then we express divisors of the above equation as divisors of E_L and get

$$\mathrm{div}(\Psi_{\boldsymbol{v}}) = \left\langle -\sum_{i=2}^n [v_i] P_i \right\rangle - \sum_{i=2}^n v_i \langle -P_i \rangle - \left(1 - \sum_{i=2}^n v_i\right) \langle \mathcal{O} \rangle.$$

Reducing this equation modulo $\mathfrak{P}$, we have

$$\mathrm{div}(\Omega_{\boldsymbol{v}}) = \left\langle -\sum_{i=2}^n [v_i] \overline{P}_i \right\rangle - \sum_{i=2}^n v_i \langle -\overline{P}_i \rangle - \left(1 - \sum_{i=2}^n v_i\right) \langle \mathcal{O} \rangle,$$

which finishes the proof.

From this theorem and some properties of elliptic nets, we can get the following corollary.

Corollary 1. Let $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$, where $v_1 = 1,\ v_2, \ldots, v_n \in \mathbb{Z}$, $\overline{P}_2, \ldots, \overline{P}_n \in E_k(k)$ and $\pm\overline{P}_i$ are all distinct and nonzero. Consider $\Omega_{\boldsymbol{v}}(-\overline{P}, \overline{P}_2, \ldots, \overline{P}_n)$ as a function of $\overline{P}$. Then

(1) $\mathrm{div}(\Omega_{\boldsymbol{v}}(-\overline{P}, \overline{P}_2, \ldots, \overline{P}_n)) = \langle \sum_{i=2}^n [v_i]\overline{P}_i \rangle - \sum_{i=2}^n v_i \langle \overline{P}_i \rangle - (1 - \sum_{i=2}^n v_i)\langle \mathcal{O} \rangle$.

(2) $\mathrm{div}(\Omega_{1,a,b}(-\overline{P}, \overline{P}_1, \overline{P}_2)) = \langle [a]\overline{P}_1 + [b]\overline{P}_2 \rangle - a\langle \overline{P}_1 \rangle - b\langle \overline{P}_2 \rangle - (1-a-b)\langle \mathcal{O} \rangle$, where $a, b \in \mathbb{Z}$.

(3) When $\overline{P}_2$ is a m-torsion point, we have

$$\mathrm{div}\left(\frac{1}{\Omega_{1,m,0}(-\overline{P}, \overline{P}_1, \overline{P}_2)}\right) = m\langle \overline{P}_2 \rangle - m\langle \mathcal{O} \rangle.$$

Proof. (1) can be directly obtained from Theorem 6; in (1), by setting $n = 3$, $v_2 = a$ and $v_3 = b$, we get (2) immediately; (3) can be got from (2).

Theorem 7. Let $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$, $v_i \in \mathbb{Z}$ and $\boldsymbol{P} = (\overline{P}_1, \overline{P}_2, \ldots, \overline{P}_n)$, where $v_i \in \mathbb{Z}$ and $P_i \in E_k(\overline{k})$. Then

$$\Omega_{\boldsymbol{v}}(\boldsymbol{T}^{\mathrm{T}}(\boldsymbol{P})) = \frac{\Omega_{\boldsymbol{T}(\boldsymbol{v})}(\boldsymbol{P})}{\prod_{i=1}^n \Omega_{\boldsymbol{T}(\boldsymbol{e}_i)}(\boldsymbol{P})^{2v_i^2 - v_i \sum_{j=1}^n v_j} \prod_{1\leqslant i<j\leqslant n} \Omega_{\boldsymbol{T}(\boldsymbol{e}_i+\boldsymbol{e}_j)}(\boldsymbol{P})^{v_i v_j}},$$

where $\boldsymbol{e}_i$ is a vector with the ith entry 1 and other entries 0.

Proof. This theorem can be obtained by Theorems 1 and 3.

Corollary 2. Let $S, P, Q \in E_k(\overline{k})$, where $S + Q \neq \mathcal{O}$. Let a be an integer. Then

$$\Omega_{1,a,0}(S+Q, P, Q) = \frac{\Omega_{1,a,1}(S, P, Q)}{\Omega_{1,0,1}(S,P,Q)^{1-a}\Omega_{0,1,0}(S,P,Q)^{a^2-a}\Omega_{1,1,1}(S,P,Q)^{a}}.$$

Proof. Consider

$$\boldsymbol{T} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad \boldsymbol{P} = (S, P, Q), \quad \boldsymbol{v} = (1, a, 0).$$

This corollary follows from Theorem 7.

Theorem 8. Let $a, b \in \mathbb{Z}$, $z_1, z_2, z_3 \in \mathbb{C}$ and $z_1, z_2, z_1 + z_2 \notin \wedge$. Then

(1) $\Psi_{a,0}(z_1, z_2) = \Psi_a(z_1)$;

(2) $\Psi_{1,a,0}(z_1, z_2, z_3) = \Psi_{1,a}(z_1, z_2)$;

(3) $\Psi_{1,a,1}(z_1, z_1, z_2) = \frac{\Psi_{1+a,1}(z_1,z_2)}{\Psi_2(z_1)^a}$;

(4) $\Psi_{a,b}(z_1, z_1) = \frac{\Psi_{a+b}(z_1)}{\Psi_2(z_1)^{ab}}$.

Proof. (1) and (2) can be obtained from the definition of $\Psi_{\boldsymbol{v}}(\boldsymbol{z})$;

$$\begin{aligned}\Psi_{1,a,1}(z_1, z_1, z_2) =& \frac{\sigma((1+a)z_1 + z_2)}{\sigma(z_1)^{a^3-3a}\sigma(z_2)^{-a}\sigma(2z_1)^a\sigma(z_1+z_2)^{1+a}} \\ =& \frac{\sigma((1+a)z_1 + z_2)}{\sigma(z_1)^{2(1+a)^2-(1+a)(a+2)}\sigma(z_2)^{2-(a+2)}\sigma(z_1+z_2)^{1+a}} \frac{1}{\sigma(2z_1)^a\sigma(z_1)^{-4a}} = \frac{\Psi_{1+a,1}(z_1, z_2)}{\Psi_2(z_1)^2},\end{aligned}$$

which gives (3);

$$\begin{aligned}\Psi_{a,b}(z_1, z_1) =& \frac{\sigma((a+b)z_1)}{\sigma(z_1)^{2a^2-a(a+b)+2b^2-b(a+b)}\sigma(2, z_1)^{ab}} = \frac{\sigma((a+b)z_1)}{\sigma(z_1)^{a^2-2ab+b^2}\sigma(2z_1)^{ab}} \\ =& \frac{\sigma((a+b)z_1)}{\sigma(z_1)^{2(a+b)^2-(a+b)^2}} \frac{1}{[\sigma(2z_1)/\sigma(z_1)^{2^2}]^{ab}} = \frac{\Psi_{a+b}(z_1)}{\Psi_2(z_1)^{ab}},\end{aligned}$$

which gives (4).

Corollary 3. Let $a \in \mathbb{Z}$ and $P_1, P_2, P_3 \in E_k(\overline{k})$, where P_1, P_2 and $P_1 + P_2$ are all distinct from $\mathcal{O}$. Then

(1) $\Omega_{a,0}(P_1, P_2) = \Omega_a(P_1)$;

(2) $\Omega_{1,a,0}(P_1, P_2, P_3) = \Omega_{1,a}(P_1, P_2)$;

(3) $\Omega_{1,a,1}(P_1, P_1, P_2) = \dfrac{\Omega_{1+a,1}(P_1, P_2)}{\Omega_2(P_1)^2}$;

(4) $\Omega_{a,b}(P_1, P_1) = \dfrac{\Omega_{a+b}(P_1)}{\Omega_2(P_1)^{ab}}$.

Proof. This corollary can be obtained by Theorem 3 and 8.

Theorem 9. Let $a \in \mathbb{Z}$, $P, Q \in E_k(\overline{k})$ and $D_P = \langle -Q \rangle - \langle -Q - P \rangle$. Then

$$f_{a,Q}(D_P) = \frac{W_{Q,P}(1+a,1)}{W_{Q,P}(1+a,0)} \frac{W_{Q,P}(1,0)^{1+a-a^2}W_{Q,P}(2,0)^a}{W_{Q,P}(1,1)^{1-a}W_{Q,P}(2,1)^a}.$$

Proof. From Corollary 1, we have

$$\mathrm{div}\left(\frac{1}{\Omega_{1,a,0}(-S,Q,P)}\right) = a\langle Q \rangle - \langle aQ \rangle - (a-1)\langle \mathcal{O} \rangle,$$

Consider $\Omega_{1,a,0}(-S, Q, P)$ as an elliptic function of S. Then

$$\mathrm{div}\left(\frac{\Omega_{1,0,0}(-S,Q,P)}{\Omega_{1,a,0}(-S,Q,P)}\right) = a\langle Q \rangle - \langle aQ \rangle - (a-1)\langle \mathcal{O} \rangle.$$

Consider $f_{a,Q}(S)$ such that

$$f_{a,Q}(S) = \frac{\Omega_{1,0,0}(-S,Q,P)}{\Omega_{1,a,0}(-S,Q,P)}.$$

Compute the value of $f_{a,Q}$ at $\langle -S\rangle - \langle -S-P\rangle$,

$$\frac{f_{a,Q}(-S)}{f_{a,Q}(-S-P)} = \frac{\Omega_{1,0,0}(S,Q,P)\Omega_{1,a,0}(S+P,Q,P)}{\Omega_{1,a,0}(S,Q,P)\Omega_{1,0,0}(S+P,Q,P)}.$$

From Corollary 1, we have

$$\frac{f_{a,Q}(-S)}{f_{a,Q}(-S-P)} = \frac{\Omega_{1,0,0}(S,Q,P)\Omega_{1,a,1}(S,Q,P)}{\Omega_{1,a,0}(S,Q,P)\Omega_{1,0,1}(S,Q,P)^{1-a}\Omega_{0,1,0}(S,Q,P)^{a^2-a}\Omega_{1,b,1}(S,Q,P)^a},$$

Let $S=Q$. Then

$$f_{a,Q}(D_P) = \frac{\Omega_{1,0,0}(Q,Q,P)\Omega_{1,a,1}(Q,Q,P)}{\Omega_{1,a,0}(Q,Q,P)\Omega_{1,0,1}(Q,Q,P)^{1-a}\Omega_{0,1,0}(Q,Q,P)^{a^2-a}\Omega_{1,b,1}(Q,Q,P)^a},$$

From Corollary 3, we have

$$\begin{aligned} f_{a,Q}(D_P) =& \frac{\Omega_1(Q)\Omega_{1+a,1}(Q,P)/\Omega_2(Q)^a}{\Omega_{1,a}(Q,Q)[\Omega_{1,1}(Q,P)/\Omega_2(Q)^a]^{1-a}\Omega_{0,1}(Q,Q)^{a^2-a}[\Omega_{2,1}(Q,P)/\Omega_2(Q)^2]^a} \\ =& \frac{\Omega_1(Q)\Omega_{1+a,1}(Q,P)}{\Omega_{1,a}(Q,Q)\Omega_{1,1}(Q,P)^{1-a}\Omega_{0,1}(Q,Q)^{a^2-a}\Omega_{2,1}(Q,P)^a} \\ =& \frac{\Omega_1(Q)\Omega_{1+a,1}(Q,P)}{[\Omega_{1+a}(Q)/\Omega_2(Q)^a]\Omega_{1,1}(Q,P)^{1-a}[\Omega_1(Q)/\Omega_2(Q)^a]^{a^2-a}\Omega_{2,1}(Q,P)^a} \\ =& \frac{\Omega_1(Q)^{1+a-a^2}\Omega_{1+a,1}(Q,P)\Omega_2(Q)^a}{\Omega_{1+a}(Q)\Omega_{1,1}(Q,P)^{1-a}\Omega_{2,1}(Q,P)^a} = \frac{\Omega_{1+a,1}(Q,P)}{\Omega_{1+a}(Q)}\frac{\Omega_1(Q)^{1+a-a^2}\Omega_2(Q)^a}{\Omega_{1,1}(Q,P)^{1-a}\Omega_{2,1}(Q,P)^a}. \end{aligned}$$

Hence

$$f_{a,Q}(D_P) = \frac{W_{Q,P}(1+a,1)}{W_{Q,P}(1+a,0)}\frac{W_{Q,P}(1,0)^{1+a-a^2}W_{Q,P}(2,0)^a}{W_{Q,P}(1,1)^{1-a}W_{Q,P}(2,1)^a},$$

which completes the proof.

Theorem 10. Let E be an elliptic curve defined over $\mathbb{F}_q$ and $T=t-1$. Then we have a bilinear pairing:

$$\begin{aligned} &\mathrm{Ate}_T(\cdot,\cdot) : G_2 \times G_1 \longrightarrow \mathbb{F}_{q^k}^\times \\ &\qquad (Q,P) \longmapsto \left\{\frac{W_{Q,P}(1+T,1)}{W_{Q,P}(1+T,0)}\frac{W_{Q,P}(1,0)^{1+q-q^2}W_{Q,P}(2,0)^q}{W_{Q,P}(1,1)^{1-q}W_{Q,P}(2,1)^q}\right\}^{\frac{q^k-1}{r}}. \end{aligned}$$

Proof. From [18] and Theorem 9, we have a pairing:

$$(Q,P) \longmapsto \left\{\frac{W_{Q,P}(1+T,1)}{W_{Q,P}(1+T,0)}\frac{W_{Q,P}(1,0)^{1+T-T^2}W_{Q,P}(2,0)^T}{W_{Q,P}(1,1)^{1-T}W_{Q,P}(2,1)^T}\right\}^{\frac{q^k-1}{r}}.$$

Note that $T \equiv q \mod r$ and $W_{Q,P}(1,0), W_{Q,P}(2,0), W_{Q,P}(1,1), W_{Q,P}(2,1) \in \mathbb{F}_{q^k}^\times$. Hence $\mathrm{Ate}_T(\cdot,\cdot)$ is a bilinear pairing.

Theorem 11. Let S be an integer such that $S \equiv q \mod r$. Let $N = \gcd(s^k-1, q^k-1) > 0$, $L = (s^k-1)/N$ and $C_S \equiv \sum_{i=0}^{k-1} S^{k-1-i}q^i \mod N$. Then we have a bilinear pairing:

$$\begin{aligned} &\mathrm{Ate}_S(\cdot,\cdot) : G_2 \times G_1 \longrightarrow \mathbb{F}_{q^k}^\times \\ &\qquad (Q,P) \longmapsto \left\{\frac{W_{Q,P}(1+S,1)}{W_{Q,P}(1+S,0)}\frac{W_{Q,P}(1,0)^{1+q-q^2}W_{Q,P}(2,0)^q}{W_{Q,P}(1,1)^{1-q}W_{Q,P}(2,1)^q}\right\}^{C_S\frac{q^k-1}{N}}. \end{aligned}$$

If $k|\#\mathrm{Aut}(E)$, then

$$Ate_S^{\mathrm{twist}}(\cdot,\cdot) : G_1 \times G_2 \longrightarrow \mathbb{F}_{q^k}^\times$$

$$(P,Q) \longmapsto \left\{ \frac{W_{P,Q}(1+S,1)}{W_{P,Q}(1+S,0)} \frac{W_{P,Q}(1,1)^{q-1}}{W_{P,Q}(2,1)^q} \right\}^{C_S \frac{q^k-1}{N}}.$$

For $r \nmid L$, both $\mathrm{Ate}_S(\cdot,\cdot)$ and $\mathrm{Ate}_S^{\mathrm{twist}}(\cdot,\cdot)$ are nondegenerate.

Proof. From [19] and Theorem 9, we have

$$(Q,P) \longmapsto \left\{ \frac{W_{Q,P}(1+S,1)}{W_{Q,P}(1+S,0)} \frac{W_{Q,P}(1,0)^{1+S-S^2} W_{Q,P}(2,0)^S}{W_{Q,P}(1,1)^{1-S} W_{Q,P}(2,1)^S} \right\}^{C_S \frac{q^k-1}{N}}.$$

Note that $S \equiv q \mod r$. The above equation still holds by substituting q for S. Therefore $\mathrm{Ate}_S(\cdot,\cdot)$ is a bilinear pairing. If $k|\#\mathrm{Aut}(E)$, then from [19] we have

$$(P,Q) \longmapsto \left\{ \frac{W_{P,Q}(1+S,1)}{W_{P,Q}(1+S,0)} \frac{W_{P,Q}(1,0)^{1+S-S^2} W_{P,Q}(2,0)^S}{W_{P,Q}(1,1)^{1-S} W_{P,Q}(2,1)^S} \right\}^{C_S \frac{q^k-1}{N}}$$

is a bilinear pairing. Note that $W_{P,Q}(1,0), W_{P,Q}(2,0) \in \mathbb{F}_q^\times$ and $S \equiv q \mod r$. Elements in $\mathbb{F}_q^\times$ and $(\mathbb{F}_q^\times)^r$ contribute nothing to the value of the pairing. Hence the above pairing can be simplified. We have

$$(P,Q) \longmapsto \left\{ \frac{W_{P,Q}(1+S,1)}{W_{P,Q}(1+S,0)} \frac{W_{P,Q}(1,1)^{q-1}}{W_{P,Q}(2,1)^q} \right\}^{C_S \frac{q^k-1}{N}};$$

that is, $\mathrm{Ate}_S^{\mathrm{twist}}(\cdot,\cdot)$ is a bilinear pairing. When $r \nmid L$, by [19], $\mathrm{Ate}_S(\cdot,\cdot)$ and $\mathrm{Ate}_S^{\mathrm{twist}}(\cdot,\cdot)$ are nondegenerate.

Theorem 12. Consider Barreto-Naehrig curves with embedding degree 12, which are the pairing friendly elliptic curves. Then we have a bilinear pairing:

$$\begin{aligned} S(\cdot,\cdot) : G_2 \times G_1 &\longrightarrow \mathbb{F}_{p^{12}}^\times \\ (Q,P) &\longmapsto \Bigg\{ \left(\frac{W_{Q,P}(1+x,1)}{W_{Q,P}(1+x,0)} \frac{W_{Q,P}(1,0)^{1+x-x^2} W_{Q,P}(2,0)^x}{W_{Q,P}(1,1)^{1-x} W_{Q,P}(2,1)^x} \right) \\ &\qquad g_{xQ,pxQ}(P) g_{p^3xQ,p^{10}xQ}(P) g_{xQ+pxQ,p^3xQ+p^{10}xQ}(P) \Bigg\}^{\frac{p^{12}-1}{r}}. \end{aligned}$$

Proof. With [24] and Theorem 9, we can prove this theorem.

4 Conclusion

In this paper, we express Miller function in terms of elliptic nets and use elliptic nets to compute some optimized pairings, which is a new approach to computing pairings. This method has a comparable loop length with Miller's algorithm. Since there is a Miller function corresponding to a pairing, elliptic nets can be used to compute all the pairings. In the elliptic net algorithm, the cost of Double is the same as that of DoubleAdd while the cost of DoubleAdd is almost twice that of Double in Miller's algorithm. Then elliptic nets can be against side channel attacks. Further, this method with elliptic nets can be further improved and it can serve as an alternative for Miller's algorithm. The elliptic net is a new tool for elliptic curves, and we hope it can be applied into some areas of cryptography.

Acknowledgements

This work was supported by National Natural Science Foundation of China (Grant Nos. 61272499, 10990011), and Science and Technology on Information Assurance Laboratory (Grant No. KJ-11-02). Yanfeng Qi acknowledges support from Aisino Corporation Inc. The authors would like to thank anonymous reviewers for their helpful advice and comments.

References

1 Boneh D, Franklin M. Identity-based encryption from the Weil pairing. In: Kilian J, ed. Proceedings of CRYPTO2001, Vol. 2139 of Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2001. 213–229

2 Joux A. A one round protocol for tripartite Diffie-Hellman. In: Proceedings of Algorithmic Number Theory Symposium on Algorithmic Number Theory. London: Springer-Verlag, 2000. 385–394

3 Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing. In: Boyd C, ed. Proceedings of ASIACRYPT 2001, Vol. 2248 of Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2001. 514–532

4 Boneh D, Crescenzo G D, Ostrovsky R, et al. Public-key encryption with keyword search. In: Proceedings of Eurocrypt 2004. Berlin: Springer-Verlag, 2004. 506–522

5 Yao A C, Zhao Y. Computationally-Fair Group and Identity-Based Key-Exchange. In: Agrawal M, Cooper S B, Li A, eds. Vol. 7287 of Lecture Notes in Computer Science. Berlin/Heidelberg: Springer-Verlag, 2012. 237–247

6 Eissa T, Razak S A, Ngadi M D A. Towards providing a new lightweight authentication and encryption scheme for MANET. Wirel Netw, 2011, 17: 833–842

7 Cheng P Q, Gu Y, Lv Z H, et al. A performance analysis of identity-based encryption schemes. In: Chen L, Yung M, Zhu L, eds. INTRUST 2011, LNCS 7222. Berlin/Heidelberg: Springer-Verlag, 2012. 289–303

8 Fujioka A, Suzuki K. Sufficient condition for identity-based authenticated key exchange resilient to leakage of secret keys. In: Kim H, ed. ICISC 2011, LNCS 7259. Berlin/Heidelberg: Springer-Verlag, 2012. 490–509

9 Barreto P S L M, Kim H Y, Lynn B, et al. Efficient algorithms for pairing-based cryptosystems. In: Proceedings of Advances in Cryptology—CRYPTO 2002, LNCS 2442. Berlin/Heidelberg: Springer-Verlag, 2002. 354–369

10 Aranha D F, Karabina K, Longa P, et al. Faster explicit formulas for computing pairings over ordinary curves. In: Advances in Cryptology—EUROCRYPT 2011, LNCS 6632. Berlin/Heidelberg: Springer-Verlag, 2011. 48–68

11 Cheung R C C, Duquesne S, Fan J F, et al. FPGA implementation of pairings using residue number system and lazy reduction. In: Cryptographic Hardware and Embedded Systems—CHES 2011, LNCS 6917. Berlin/Heidelberg: Springer-Verlag, 2011. 421–441

12 Stange K E. The Tate pairing via elliptic nets. In: Pairing-Based Cryptography—PAIRING 2007, LNCS 4575. Berlin: Springer, 2007. 329–348

13 Everest G, van der Poorten A, Shparlinski I, et al. Recurrence Sequences. Vol. 104 of Mathematical Surveys and Monographs. American Mathematical Society, 2003. 163–175

14 Shipsey R. Elliptic divibility sequences. Dissertation for the Doctoral Degree. University of London, 2001

15 Ward M. Memoir on elliptic divisibility sequences. Amer J Math, 1948, 70: 31–74

16 Stange K E. Elliptic nets and elliptic curves. Dissertation for the Doctoral Degree. Brown University, 2008

17 Hess F. Pairing lattices. In: Galbraith S D, Paterson K G, eds. Pairing 2008, LNCS 5209. Berlin: Springer-Verlag, 2008. 211–224

18 Hess F, Smart N, Vercauteren F. The Eta-pairing revisited. IEEE Trans Inform Theory, 2006, 52: 4595–4602

19 Matsuda S, Kanayama N, Hess F, et al. Optimised versions of the Ate and twisted Ate pairings. In: the 11th IMA International Conference on Cryptography and Coding, LNCS 4887. Berlin: Springer-Verlag, 2007. 302–312

20 Hong H, Lee E, Lee H S, et al. Simple and exact formula for minimum loop length in Ate_i pairing based on Brezing-Weng curves. Designs Codes Cryptogr, 2013, 67: 271–292

21 Barreto P S L M, Naehrig M. Pairing-friendly elliptic curves of prime order. In: Selected Areas in Cryptography—SAC 2005, LNCS 3897. Berlin: Springer, 2006. 319–331

22 Freeman D, Scott M, Teske E. A taxonomy of pairing-friendly elliptic curves. J Cryptol, 2010, 23: 224–280

23 Duquesne S, Frey G. Background on pairings. In: Handbook of Elliptic and Hyperelliptic Curve Cryptography. Boca Raton: Chapman & Hall/CRC, 2006. 115–124

24 Nogami Y, Akane M, Sakemi Y, et al. Integer variable χ-based Ate pairing. In: Galbraith S D, Paterson K G, eds. Pairing 2008, LNCS 5209. Heidelberg: Springer, 2008. 178–191