JSIAM Letters Vol.8 (2016) pp.9–12 ©2016 Japan Society for Industrial and Applied Mathematics

The optimal ate pairing over the Barreto-Naehrig curve via parallelizing elliptic nets

Hiroshi Onuki[1], Tadanori Teruya[2], Naoki Kanayama[3] and Shigenori Uchiyama[1]

[1] Tokyo Metropolitan University, 1-1 Minami-Osawa, Hachioji, Tokyo 192-0397, Japan
[2] National Institute of Advanced Industrial Science and Technology, 2-4-7 Aomi, Koto-ku, Tokyo 135-0064, Japan
[3] University of Tsukuba, 1-1-1 Tennodai, Tsukuba, Ibaraki 305-8573, Japan

E-mail *onuki-hiroshi@ed.tmu.ac.jp*

Received October 26, 2015, Accepted November 27, 2015

Abstract

In this paper, we discuss the optimal ate pairing over Barreto-Naehrig (BN) curves. First, we give an explicit formula for computing this pairing via elliptic nets associated to the twist curves. Second, we consider parallel algorithms to calculate elliptic nets for computing this pairing. Finally, we evaluate the costs of our parallel algorithms.

Keywords elliptic net, Barreto-Naehrig curve, pairing, parallel computing

Research Activity Group Algorithmic Number Theory and Its Applications

1. Introduction

Background. Recently, Miller's algorithm [1] has been widely used for computing pairings. In 2007, Stange [2] defined elliptic nets and proposed an alternative method for computing pairings based on them. Both methods require $\mathcal{O}(\log(m))$ field operations for computing a pairing over an m-torsion subgroup, but in many cases, the coefficient hiding behind the $\mathcal{O}$ notation of Miller's algorithm is less than that based on elliptic nets. Therefore, Miller's algorithm has been standard for computing pairings.

In the recent years, multi-core processors have become widely available, so parallel algorithms have become important. For Miller's algorithm, Aranha et al. [3] proposed a parallel algorithm. We here focus on parallelizing an elliptic nets algorithm. We deem that elliptic nets algorithm is preferable for parallel computation, based on its computational features.

Contribution. We give an explicit formula for computing the optimal ate pairing over Barreto-Naehrig (BN) curves via the elliptic net associated to the twist curves and construct algorithms to parallelize the computation of this elliptic net. The calculation of an elliptic net is executed through recurrences for the block which consists of some elements in the field. Our algorithms exploit the fact that this calculation can be executed for each element at the same time. Therefore, it is important to reduce the maximal cost in calculations of each element. We construct a new block more suitable for calculating in parallel by adding two elements to the original block. We count the number of multiplications in the field in these algorithms and estimate the efficiencies of our algorithms for some numbers of processors.

Organization. The remainder of this paper is organized as follows. In Section 2, we recall some previous works. In Section 3, we introduce a method to calculate the optimal ate pairing over BN curves via the elliptic net associated to the twist curves. In Section 4, we consider parallelizing the elliptic net associated to the twist curves and estimate the cost of computing the parallelized elliptic nets. Finally, we make some concluding remarks in Section 5.

2. Preliminaries

2.1 Elliptic nets

In 2007, Stange [2] defined elliptic nets associated to elliptic curves and their rational points and introduced an algorithm for computing the Tate pairing via elliptic nets.

In this subsection, we briefly review elliptic nets. See [2] for details.

Elliptic nets are a generalization of elliptic divisibility sequences. We state the definition of an elliptic net as follows:

Definition 1 ([2]) *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 $p, q, r, s \in A$:*

$$\begin{aligned} &W(p+q+s)W(p-q)W(r+s)W(r) \\ &\quad + W(q+r+s)W(q-r)W(p+s)W(p) \\ &\quad + W(r+p+s)W(r-q)W(q+s)W(q) = 0. \end{aligned} \quad (1)$$

Given an elliptic curve E defined over a subfield of $\mathbb{C}$ or a finite field K, and its rational points $P_1, \ldots, P_n \in E$, Stange defined an elliptic net $\mathbb{Z}^n \to \bar{K}$ associated to E and $P_1, \ldots, P_n \in E$. We denote this by $W_{P_1,\ldots,P_n;E}$ or $W_{P_1,\ldots,P_n}$ if it is not confusing.

We now state how to compute the elements of the elliptic net $W_{P,Q}(m,1), W_{P,Q}(m,0)$ $(m \in \mathbb{N})$. Stange defined a block centered on k (shown in Fig. 1) to consist of a first vector of eight consecutive terms of the sequence $W(i,0)$ centered on terms $W(k,0)$ and $W(k+1,0)$, and

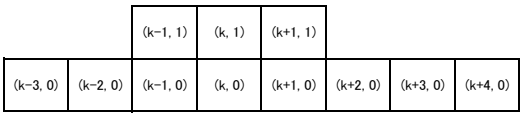

Fig. 1. A block centered on k.

a second vector of three consecutive terms $W(i,1)$ centered on the term $W(k,1)$.

Stange defined two functions:

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

From equation (1), Stange showed the following recurrences, which can be used for calculating the functions above:

Proposition 2 ([2]) *Let W be an elliptic net associated to an elliptic curve and two rational points. Then*

$$W(2k-1,0) = W(k+1,0)W(k-1,0)^3 - W(k-2,0)W(k,0)^3, \tag{2}$$

$$W(2k,0) = \frac{1}{W(2,0)}\big(W(k,0)W(k+2,0)W(k-1,0)^2 - W(k,0)W(k-2,0)W(k+1,0)^2\big), \tag{3}$$

$$W(2k-1,1) = \frac{1}{W(1,1)}\big(W(k+1,1)W(k-1,1)W(k-1,0)^2 - W(k,0)W(k-2,0)W(k,1)^2\big), \tag{4}$$

$$W(2k,1) = W(k-1,1)W(k+1,1)W(k,0)^2 - W(k-1,0)W(k+1,0)W(k,1)^2, \tag{5}$$

$$W(2k+1,1) = \frac{1}{W(-1,1)}\big(W(k-1,1)W(k+1,1)W(k+1,0)^2 - W(k,0)W(k+2,0)W(k,1)^2\big), \tag{6}$$

$$W(2k+2,1) = \frac{1}{W(2,-1)}\big(W(k+1,0)W(k+3,0)W(k,1)^2 - W(k-1,1)W(k+1,1)W(k+2,0)^2\big). \tag{7}$$

Given an elliptic curve E with Weierstrass form $y^2 = x^3+Ax+B$ and its rational points $P=(x_1,y_1)$ and $Q=(x_2,y_2)$ with $Q \neq \pm P$, the initial values of the elliptic net W associated to E and P,Q and the constants in recurrences in proposition 2 are given as follows:

$$W(1,0) = 1, \tag{8}$$

$$W(2,0) = 2y_1, \tag{9}$$

$$W(3,0) = 3x_1^4 + 6Ax_1^2 + 12Bx_1 - A^2, \tag{10}$$

$$W(4,0) = 4y_1(x_1^6 + 5Ax_1^4 + 20Bx_1^3 - 5A^2x_1^2 - 4ABx_1 - 8B^2 - A^3), \tag{11}$$

$$W(0,1) = W(1,1) = 1, \tag{12}$$

$$W(2,1) = 2x_1 + x_2 - \left(\frac{y_2-y_1}{x_2-x_1}\right)^2, \tag{13}$$

$$W(-1,1) = x_1 - x_2, \tag{14}$$

$$W(2,-1) = (y_2+y_1)^2 - (2x_1+x_2)(x_1-x_2)^2. \tag{15}$$

Stange introduced a formula for computing the Tate pairing based on elliptic nets:

Theorem 3 ([2]) *Let E be an elliptic curve defined over a finite field K, m be a positive integer, $P \in E(K)[m]$ and $Q \in E(K)$. Then the Tate pairing $\tau_m : E(K)[m] \times E(K)/mE(K) \to K^*/(K^*)^m$ satisfies the following equation:*

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

2.2 BN curves and the pairing

In this subsection, we recall the definitions of BN curves [4] and the optimal ate pairing [5].

Definition 4 *An elliptic curve $E : y^2 = x^3 + b$ over a finite prime field $\mathbb{F}_p$ is called a BN curve when $m = \#E(\mathbb{F}_p)$ is prime and there exists an integer z such that $p = 36z^4+36z^3+24z^2+6z+1$ and $m = 36z^4+36z^3+18z^2+6z+1$. The integer z is called the BN parameter.*

The BN curve has the embedding degree $k = 12$. Let $\pi : (x,y) \mapsto (x^p, y^p)$ be the Frobenius endomorphism, and G_1 and G_2 be the 1-eigenspace and the p-eigenspace of π acting on $E[r]$, respectively. The optimal ate pairing [5] $\alpha_{opt} : G_1 \times G_2 \to \mathbb{F}_{p^{12}}$ is defined by

$$(P,Q) \mapsto (f_{6z+2,Q}(P) \cdot l_1(P) \cdot l_2(P))^{\frac{p^{12}-1}{m}}, \tag{16}$$

where $f_{n,R}$ denotes the Miller function [1], and where l_1 and l_2 are the lines through $(6z+2)Q$ and $\pi(Q)$, and $(6z+2)Q + \pi(Q)$ and $-\pi^2(Q)$, respectively. The Miller function and the line functions are normalized.

A BN curve E has a unique sextic twist [6] $\tilde{E}$ defined over $\mathbb{F}_{p^2}$ with $m | \#\tilde{E}(\mathbb{F}_{p^2})$; let $\Psi : \tilde{E} \to E$ be the associated twisting isomorphism. There exists non-square and non-cube $\xi \in \mathbb{F}_{p^2}$ such that $\tilde{E}$ is given by $y^2 = x^3 + B/\xi$, and Ψ is given by $(x,y) \mapsto (\omega^2 x, \omega^3 y)$ where $\omega \in \mathbb{F}_{p^{12}}$ is a sixth root of ξ. The preimage $\tilde{G_2} = \Psi^{-1}(G_2)$ is contained in $\tilde{E}(\mathbb{F}_{p^2})$; this property is exploited in calculating the pairing.

2.3 The optimal ate pairing via elliptic nets

Ogura et al. [7] gave explicit formulae based on elliptic nets for computing some variants of the Tate pairing, which contained the optimal ate pairing. We use the following:

Theorem 5 ([7]) *Let E be a BN curve defined over $\mathbb{F}_p$ with the BN parameter z and $m = \#E(\mathbb{F}_p)$, and G_1, G_2 be the subgroups of $E[m]$ stated in Section 2.2. Then for*

$P \in G_1$ *and* $Q \in G_2$,

$$f_{6z+2,Q}(P)^{\frac{p^{12}-1}{m}} = \left(\frac{W_{Q,P}(6z+2,1)}{W_{Q,P}(6z+2,0)}\right)^{\frac{p^{12}-1}{m}}. \quad (17)$$

3. Twisted elliptic nets

In an elliptic net associated to an elliptic curve and its rational points P, Q, a first vector in its block $W(i,0)$ depends only on P and a second vector $W(i,1)$ depends on P and Q. Therefore, in BN curves, all elements in the elliptic net block are in $\mathbb{F}_{p^{12}}$, whereas in the twist curves, the elements in the first vector are in $\mathbb{F}_{p^2}$. Therefore, we may compute the elliptic net associated to the twist curves more efficiently than that associated to BN curves. For computing the optimal ate pairing over BN curves via the elliptic net associated to the twist curves, we give the relation between the elliptic net associated to BN curves and that associated to the twist curves:

Theorem 6 *Let E be a BN curve and $G_1, G_2, \tilde{E}, \omega, \Psi$ be as stated in Section 2.2. Let $P \in G_1, Q \in G_2$ and $\tilde{P}, \tilde{Q} \in \tilde{E}$ such that $\Psi(\tilde{P}) = P, \Psi(\tilde{Q}) = Q$. Then*

$$W_{Q,P;E}(n,0) = \omega^{1-n^2} W_{\tilde{Q},\tilde{P};\tilde{E}}(n,0), \quad (18)$$

$$W_{Q,P;E}(n,1) = \omega^{n-n^2} W_{\tilde{Q},\tilde{P};\tilde{E}}(n,1). \quad (19)$$

Proof It follows immediately by induction. **(QED)**

We express the Miller function by the elliptic net associated to the twist curves:

Theorem 7 *We use the same notation as in Theorem 6. Then*

$$f_{6z+2,Q}(P)^{\frac{p^{12}-1}{m}} = W_{\tilde{Q},\tilde{P};\tilde{E}}(6z+2,1)^{\frac{p^{12}-1}{m}}. \quad (20)$$

Proof It follows from Theorems 5 and 6 and the fact that the final exponentiation eliminates ω and the elements in $\mathbb{F}_{p^2}$ i.e., $\omega^{(p^{12}-1)/m} = 1$ and $x^{(p^{12}-1)/m} = 1$ for all $x \in \mathbb{F}_{p^2}$. **(QED)**

We now state the main theorem of this section, which shows how to compute the optimal ate pairing over BN curves via the elliptic net associated to the twist curves.

Theorem 8 *Let W be an elliptic curve associated to the sextic twist $\tilde{E}$ of a BN curve E defined over $\mathbb{F}_p$ with the BN parameter z and $m = \#E(\mathbb{F}_p)$. Given the block centered on $6z+2$ of W, the optimal ate pairing $\alpha_{opt}(P,Q)$ over E can be obtained by calculating the following values, where $\tilde{P}, \tilde{Q}$ denote the points in $\tilde{E}$ correspond to P, Q respectively, and $W(i)$ denotes $W(6z+2+i,0)$ for brevity:*

$$X = x_{\tilde{Q}} W(0)^2 - W(1)W(-1),$$

$$Y = \frac{W(2)W(-1)^2 - W(-2)W(1)^2}{4y_{\tilde{Q}}},$$

$$\tilde{X} = \omega^{2(p-1)} x_{\tilde{Q}}^p W(0)^2,$$

$$\tilde{Y} = \omega^{3(p-1)} y_{\tilde{Q}}^p W(0)^3,$$

$$X_d = X - \tilde{X}, \quad Y_d = Y - \tilde{Y},$$

$$X_R = \left(\frac{2b}{\xi}\right) W(0)^6 + X\tilde{X}(X+\tilde{X}) - 2Y\tilde{Y},$$

$$Y_R = \left[Y\tilde{Y} - \left(\frac{3b}{\xi}\right) W'(0)^6\right] Y_d + 3X\tilde{X}(X\tilde{Y} - \tilde{X}Y),$$

$$Z_R = X_d W(0),$$

$$l_1 = X_d(y_{\tilde{P}} W(0)^3 - Y) - Y_d(x_{\tilde{P}} W(0)^2 - X),$$

$$l_2 = [X_R - \omega^{2(p^2-1)} x_{\tilde{Q}} Z_R^2](y_{\tilde{P}} Z_R^3 - Y_R) - [Y_R + \omega^{3(p^2-1)} y_{\tilde{Q}} Z_R^3](x_{\tilde{P}} Z_R^2 - X_R).$$

Then we have

$$\alpha_{opt}(P,Q) = (W(6z+2,1) l_1 l_2)^{\frac{p^{12}-1}{m}}. \quad (21)$$

Proof From the fact that the final exponentiation eliminates ω and the elements in proper subfields of $\mathbb{F}_{p^{12}}$ and that the x-coordinate of Q is in $\mathbb{F}_{p^6}$, after a lengthy calculation, it follows that $l_i^{(p^{12}-1)/m} = l_i(P)^{(p^{12}-1)/m}$ for $i = 1, 2$, where $l_i(P)$ are the line functions described in Section 2.2. Eq. (21) immediately follows from this and Theorem 7. **(QED)**

4. Parallelization

4.1 Outline of our parallelization

In this section, we consider parallelizing the calculation of the elliptic net associated to the twist curves of BN curves. Our strategy for the parallelization is to distribute the elements of the elliptic net block to each processor. We introduce two techniques for computing the elliptic net, eliminating the multiplication by the inverse of $W(-1,1)$, and extending the block. The former is for 4 or fewer processors, the latter is for 6 or more processors.

First, we describe the elimination of the multiplication by the inverse of $W(-1,1)$. As we stated in section 2.1, $W(1,1) = 1$ in the elliptic net associated to an elliptic curve. Therefore, in the recurrences (4) – (7), the calculation cost of (4) is equal to that of (5), the calculation cost of (6) is equal to that of (7), and the calculation cost of (4) is a cost of one multiplication less than that of (6). Defining the modified elliptic net, we may exchange the calculation cost of (4) for that of (6). Let $\tilde{W}$ be an elliptic net associated to the twist of a BN curve and its two rational points; then we define the modified elliptic net $\tilde{W}'$ of $\tilde{W}$ as follows:

$$\tilde{W}'(s,t) := \tilde{W}(-1,1)^{st} \tilde{W}(s,t), \quad \forall s, \forall t \in \mathbb{Z}. \quad (22)$$

A modified elliptic net is also an elliptic net, so we may compute it by proposition 2. The constants in the recurrence (4) – (7) of $\tilde{W}$ and $\tilde{W}'$ are in the following fields:

$$\tilde{W}(1,1) = 1, \quad \tilde{W}(-1,1) \in \mathbb{F}_{p^6}, \quad \tilde{W}(1,1) \in \mathbb{F}_{p^{12}},$$

$$\tilde{W}'(1,1) \in \mathbb{F}_{p^6}, \quad \tilde{W}'(-1,1) = 1, \quad \tilde{W}'(1,1) \in \mathbb{F}_{p^{12}}.$$

Since $\tilde{W}'(n,0) = \tilde{W}(n,0)$ for all $n \in \mathbb{N}$ and since the final exponentiation eliminates $\tilde{W}(-1,1)$, we can replace $\tilde{W}$ by $\tilde{W}'$ in Theorem 8. The calculation of **Double** is based on the recurrences (4) and (6), whereas the calculation of **DoubleAdd** is not based on the recurrence (4). Therefore this modification reduces the calculation cost of **DoubleAdd** without changing that of **Double**.

In the rest of this subsection, we state a technique

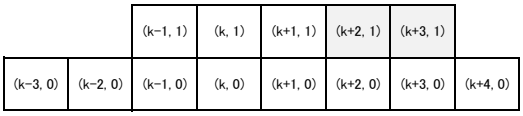

Fig. 2. An extended block centered on k.

Table 1. Costs of the longest path.

number of processors	Double	DoubleAdd
1	$108m_2$	$114m_2$
4	$36m_2$	$42m_2$
6	$32m_2$	$32m_2$
8	$30m_2$	$30m_2$
10	$24m_2$	$24m_2$

which reduces the cost of calculating an elliptic net, given sufficiently many processors. If we have, for example, 22 processors, we can compute **Double** or **DoubleAdd** as follows:

Step 1. Each processor calculates one term in the recurrences of Proposition 2.

Step 2. Half of the processors add two terms.

Step 3. Some processors multiply the sum above by the inverse of constants. (where these inverses are precomputed.)

In this procedure, the calculation which has the largest cost in Step 1 is a cost of calculating $W(k-1,1)W(k+1,1)W(k+2,0)^2$ (for example) and that in Step 3 is a cost of multiplying by the inverse of $W(2,-1)$. Therefore for computing **Double** or **DoubleAdd** with 22 processors, we need the time to calculate the above operations and that for Step 2. Because we cannot reduce this time even if we increase the number of processors used, this is the critical path in this algorithm.

As we stated in the above, the recurrences (4) and (5) have no multiplications by inverses. Therefore, if we use only the recurrences (4) and (5) for calculating the second vector of the elliptic net block, then we can reduce the critical path. (The cost for calculating the first vector does not affect the critical path because the elements in the first vector are in $\mathbb{F}_{p^2}$, in which the operation costs are relatively low.) To do so, we extend the elliptic net block. We add the two additional elements $W(k+2,1)$ and $W(k+3,1)$ to the second vector. (See Fig. 2.)

This extension of the block allows us to compute **Double** or **DoubleAdd** without the recurrences (6) and (7). Although this technique increases the total cost, the cost of the critical path is reduced to the following three operations; one multiplication in $\mathbb{F}_{p^{12}}$, one multiplication of the elements in $\mathbb{F}_{p^{12}}$ and $\mathbb{F}_{p^2}$, and one addition in $\mathbb{F}_{p^{12}}$.

Based on the above, we construct algorithms for computing the elliptic net with 1, 4, 6, 8 and 10 processors. In the 4-processor algorithm, an extended block is not used because 4 processors is too few to overcome the increase in the total cost.

4.2 Estimating the cost

In this subsection, we estimate the costs of our parallel algorithms by which we compute the elliptic net associated to the twist curves of BN curves. We assume the finite fields implemented by the tower extension $\mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^6} \subseteq \mathbb{F}_{p^{12}}$ stated in [8]. In this paper, the cost means the number of multiplications in the finite fields, namely, we ignore the number of additions. m_i denotes the cost of multiplication in $\mathbb{F}_{p^i}$ and s_i denotes the cost of squaring in $\mathbb{F}_{p^i}$. Based on the method stated in [8], we estimate the cost in terms of m_2 as follows:

$$m_{12} = 18m_2, \quad s_{12} = 12m_2, \quad m_6 = 6m_2, \quad s_2 = \frac{2}{3}m_2.$$

The cost of multiplying an element of $\mathbb{F}_{p^i}$ by one of $\mathbb{F}_{p^j}$ with $i|j$ is $(j/i)m_i$.

For the above setting, the costs of the longest path in the algorithms are listed in Table 1.

For 10-processor algorithm, we achieve a cost that is equal to that of the critical path.

5. Conclusion

In this work, we constructed a method for computing the optimal ate pairing over BN curves via the elliptic net associated to the twist curves, and algorithms to parallelize the computation of this elliptic net. Our algorithm for 10 processors has the lowest cost for computing our extended block (without parallelizing the field operations), and its cost of the field multiplication is about 22% that of a single processor.

The implementation of our algorithms in a computer is a future work.

Acknowledgments

This work was supported by a research grant from the KDDI Foundation "A study on improvement of pairing-based cryptography" and a Grant-in-Aid for Scientific Research (C) (24540135).

References

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

[2] K.E. Stange, The Tate pairing via elliptic nets, in: Proc. of Pairing Conference 2007, T. Takagi et al. eds., LNCS, Vol. 4575, pp. 329–348, Springer-Verlag, Berlin, 2007.

[3] D. F. Aranha, E. Knapp, A. Menezes and F, Rodriquez-Heníquez, Parallelizing the Weil and Tate Pairings, in: Proc. of Cryptography and Coding 2011, L. Chen ed., LNCS, Vol. 7089, pp. 275–295, Springer-Verlag, Berlin, 2011.

[4] P. S. L. M. Barreto and M. Naehrig, Pairing-Friendly Elliptic Curves of Prime Order, in: Proc. of SAC 2005, B. Preneel and S. Tavares eds., LNCS, Vol. 3897, pp. 319–331, Springer-Verlag, Berlin, 2006.

[5] F. Vercauteren, Optimal pairings, IEEE Trans. Inf. Theory, **56** (2010), 455–461.

[6] F. Hess, N. Smart and F. Vercauteren, The eta pairing revisited, IEEE Trans. Inf. Theory, **52** (2006), 4595–4602.

[7] N. Ogura, N. Kanayama, S. Uchiyama and E. Okamoto, Cryptographic Pairings Based on Elliptic Nets, in: Proc. of IWSEC 2011, T. Iwata and M. Nishigaki eds., LNCS, Vol. 7038, pp. 65–78, Springer-Verlag, Berlin, 2011.

[8] D. F. Aranha, K. Karabina and P. Longa, C. H. Gebotys, J. López., Faster Explicit Formulas for Computing Pairings over Ordinary Curves, in: Proc. of EUROCRYPT 2011, K. G. Paterson ed., LNCS, Vol. 6632, pp. 48–68, Springer-Verlag, Dordrecht, 2011.