An Improvement of Twisted Ate Pairing Using Integer Variable with Small Hamming Weight

Yumi Sakemi[1], Hidehiro Kato[1], Yasuyuki Nogami[1] and Yoshitaka Morikawa[1]
[1]Graduate School of Natural Science and Technology, Okayama University
3-1-1, Tsushima-naka, Okayama, Okayama 700-8530, Japan
E-mail : [1]{sakemi, kato, nogami, morikawa}@trans.cne.okayama-u.ac.jp

Abstract: Barreto–Naehrig (BN) curve has been introduced as a pairing-friendly elliptic curve over prime field $\mathbb{F}_p$ which has embedding degree 12. Characteristic and Frobenius trace are given as polynomials of integer variable χ. This paper proposes an improvement of Miller's algorithm of twisted Ate pairing with BN curve by χ of small hamming weight. Then, in order to show the efficiency of the proposed method, twisted Ate pairings with BN curve of order $r \approx 2^{158}$ and $r \approx 2^{254}$ are simulated and it is shown that these twisted Ate pairings are carried out with 7.21 milliseconds and 16.5 milliseconds by Pentium4 (3.6GHz), respectively.

1. Introduction

In recent years, cryptographic applications with pairing over elliptic curve such as ID-based cryptography[1] and group signature scheme[2] have been proposed. Unfortunately, pairing is an expensive operation and this is often a bottleneck for the application. In order to make it practical, various pairings such as Ate pairing[3], twisted Ate pairing[4] and *subfield–twisted* Ate pairing [5],[6] have been proposed. In this paper, Barreto–Naehrig (BN) curve[7], that is a typical class of non–supersingular (ordinary) pairing–friendly elliptic curves of embedding degree 12, is dealt with. As a typical feature of BN curve, its characteristic p and Frobenius trace t are given by using *integer variable* χ as

$$p(\chi) = 36\chi^4 - 36\chi^3 + 24\chi^2 - 6\chi + 1, \quad (1a)$$
$$t(\chi) = 6\chi^2 + 1. \quad (1b)$$

Pairing calculation consists of Miller's algorithm calculation $A = f_{s,P}(Q) \in \mathbb{F}^*_{p^k}$ and so-called *final exponentiation* $A^{(p^k-1)/r}$, where s corresponds to the number of iterations in Miller's algorithm, $P \in E(\mathbb{F}_p)$ and $Q \in E(\mathbb{F}_{p^k})$. This paper proposes an improvement of Miller's algorithm of twisted Ate pairing. The calculation cost of Miller's algorithm can be reduced by using s of small hamming weight. In the case of twisted Ate pairing proposed by Matsuda et al.[4], s is given as

$$s = (t-1)^2 - r = -36\chi^3 + 18\chi^2 - 6\chi + 1 \quad (2)$$

Thus, preparing s with small hamming weight is not easy. This paper improves the $f_{s,P}$ calculation by setting χ of small hamming weight to the number of iterations in Miller's algorithm.

In order to show the efficiency of the proposed method, the authors simulated on Pentium4 (3.6GHz) with C language and GMP library [8]. Then, it is shown that, in the cases of $r \approx 2^{158}$ and $r \approx 2^{254}$, the proposed method reduces the calculation times of Miller's algorithm by 7.4% and 14.2%, respectively.

Throughout this paper, p and k denote characteristic and extension degree, respectively. $\mathbb{F}_{p^k}$ denotes k-th extension field over $\mathbb{F}_p$ and $\mathbb{F}^*_{p^k}$ denotes the multiplicative group in $\mathbb{F}_{p^k}$. $X \mid Y$ and $X \nmid Y$ mean that X divides and does not divide Y, respectively.

2. Fundamentals

2.1 Elliptic Curve and Barreto–Naehrig curve

Let $\mathbb{F}_p$ be prime field and E be an elliptic curve over $\mathbb{F}_p$. $E(\mathbb{F}_p)$ that is the set of rational points on the curve, including the *infinity point* $\mathcal{O}$, forms an additive Abelian group. Let $\#E(\mathbb{F}_p)$ be its order, consider a large prime number r that divides $\#E(\mathbb{F}_p)$. The smallest positive integer k such that r divides $p^k - 1$ is especially called *embedding degree*. One can consider a pairing such as Tate and Ate pairings on $E(\mathbb{F}_{p^k})$. Usually, $\#E(\mathbb{F}_p)$ is written as

$$\#E(\mathbb{F}_p) = p + 1 - t \quad (3)$$

where t is the Frobenius trace of $E(\mathbb{F}_p)$. Characteristic p and Frobenius trace t of Barreto–Naehrig (BN) curve [7] are given by using an integer variable χ as Eqs.(1). In addition, BN curve E can be written as

$$E : y^2 = x^3 + b,\ b \in \mathbb{F}_p \quad (4)$$

whose embedding degree is 12. In this paper, let $\#E(\mathbb{F}_p)$ be a prime number r for instance.

2.2 Twisted Ate Pairing

Let ϕ be Frobenius endomorphism, i.e.,

$$\phi : E(\mathbb{F}_{p^{12}}) \to \mathbb{E}(\mathbb{F}_{p^{12}}) : (x, y) \mapsto (x^p, y^p), \quad (5)$$

Then, let $\mathbb{G}_1$ and $\mathbb{G}_2$ be

$$\mathbb{G}_1 = E[r] \cap \mathrm{Ker}(\phi - [1]), \quad (6a)$$
$$\mathbb{G}_2 = E[r] \cap \mathrm{Ker}([\zeta_6]\phi^2 - [1]), \quad (6b)$$

where ζ_6 is a primitive 6-th root of unity and let $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$, twisted Ate pairing $\alpha(\cdot, \cdot)$ is defined as

$$\alpha(\cdot,\cdot) : \begin{cases} \mathbb{G}_1 \times \mathbb{G}_2 & \to \mathbb{F}^*_{p^{12}}/(\mathbb{F}^*_{p^{12}})^r \\ (P, Q) & \mapsto f_{s,P}(Q)^{(p^{12}-1)/r}. \end{cases} \quad (7)$$

In general, $A = f_{s,P}(Q)$ is calculated by Miller's algorithm[5], then so–called *final exponentiation* $A^{(p^{12}-1)/r}$ follows. The number of calculation loops of Miller's algorithm of twisted Ate pairing with BN curve is determined by $\lfloor \log_2 s \rfloor$, where s is given by

$$\begin{aligned} s &= (t-1)^2 \bmod r \\ &= 36\chi^3 + 18\chi^2 + 6\chi + 1. \end{aligned} \quad (8)$$

It is said that calculation cost of Miller's Algorithm is about twice of that of final exponentiation.

2.3 Divisor

Let D be the principal divisor of $Q \in E$ given as

$$D = (Q) - (\mathcal{O}) = (\mathcal{Q}) - (\mathcal{O}) + div\,(1). \quad (9)$$

For scalars $a, b \in Z$, let aD and bD be written as

$$\begin{aligned} aD &= (aQ) - (\mathcal{O}) + div\,(f_{a,Q}), & (10a) \\ bD &= (bQ) - (\mathcal{O}) + div\,(f_{b,Q}), & (10b) \end{aligned}$$

where $f_{a,Q}$ and $f_{b,Q}$ are the rational functions for aD and bD, respectively. Then, addition for divisors is given as

$$aD + bD = (aQ) + (bQ) - (\mathcal{O}) + div\,(f_{a,Q} \cdot f_{b,Q} \cdot g_{aQ,bQ}), \quad (11a)$$

where $g_{aQ,bQ} = l_{aQ,bQ}/v_{aQ+bQ}$, $l_{aQ,bQ}$ denotes the line passing through two points aQ, bQ, and v_{aQ+bQ} denotes the vertical line passing through $aQ + bQ$. Moreover, the following relation holds.

$$a(bD) = \sum_{i=0}^{a-1}(bQ) - a(\mathcal{O}) + div\left(f_{b,Q}^{a} \cdot f_{a,bQ}\right). \quad (11b)$$

Thus, let $(a+b)D$ and $(ab)D$ be written as

$$\begin{aligned} (a+b)D &= ((a+b)Q) - (\mathcal{O}) + div\,(f_{a+b,Q}), & (12a) \\ (ab)D &= (abQ) - (\mathcal{O}) + div\,(f_{ab,Q}), & (12b) \end{aligned}$$

we have the following relation.

$$\begin{aligned} f_{a+b,Q} &= f_{a,Q} \cdot f_{b,Q} \cdot g_{aQ,bQ}, & (13a) \\ f_{ab,Q} &= f_{b,Q}^{a} \cdot f_{a,bQ} = f_{a,Q}^{b} \cdot f_{b,aQ}. & (13b) \end{aligned}$$

Miller's algorithm calculates $f_{s,Q}$ efficiently.

3. Main Proposal

3.1 Introduction of Miller's Algorithm

Several improvements for Miller's algorithm have been given. Barreto et al. proposed *reduced* Miller's algorithm. **Fig**.1 shows the calculation flow of *reduced* Miller's algorithm for $f_{s,P}(Q)$. It consists of functions shown in **Algorithm 1** and **Algorithm 2**, *see* **Table** 1.

In the case of twisted Ate pairing, let $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$ and s be given by Eq.(8), $f_{s,P}(Q)$ becomes an element in $\mathbb{F}^*_{p^{12}}$. In **Fig**.1, s_i is i-th bit of the binary representation of s from the lower, FMUL and FSQR denote multiplication and squaring over $\mathbb{F}_{p^{12}}$, EADD and EDBL denote elliptic curve addition and doubling over $\mathbb{G}_1$. As shown in the algorithm, *main operation* is repeated $\lfloor \log_2 s \rfloor$ times but *additional operation* is only carried out when s_i is 1. Thus, the calculation cost of Miller's Algorithm can be reduced by reducing the number of *additional operations*. Preparing s of small hamming weight is not easy; however, preparing BN curve with χ of small Hamming weight is quite easy. **Table** 2 shows all $\chi's$ of Hamming weight 3 that gives 158–bit and 254–bit prime order BN curve. Note that s is given with χ as Eq.(8). Using such χ of small Hamming weight, first calculate $f_{\chi,P}(Q)$, $f_{\chi^2,P}(Q)$, $f_{\chi^3,P}(Q)$ by Miller's algorithm. Then, combining them we can obtain $f_{s,P}(Q)$. Thus, the number of *additional operations* is substantially reduced.

Algorithm 1 : FSQR and EDBL of Fig.1

Input :	$T \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$
Output :	f, T
	FSQR
1.	$\lambda_{T,T} \leftarrow (3x_T^2)/(2y_T)$
2.	$l_{T,T}(Q) \leftarrow (x_Q - x_T)\lambda_{T,T} - (y_Q - y_T)$
3.	$f \leftarrow f^2 \cdot l_{T,T}(Q)/v_{T+T}(Q)$
4.	return f
	EDBL
5.	$x_{2T} \leftarrow \lambda_{T,T}^2 - 2x_T$
6.	$y_{2T} \leftarrow (x_T - x_{2T})\lambda_{T,T} - y_T$
7.	return $T \leftarrow 2T$

Algorithm 2 : FMUL and EADD of Fig.1

Input :	$P, T \in \mathbb{G}_1, \mathbb{Q} \in \mathbb{G}_2$
Output :	f, T
	FMUL
1.	$\lambda_{T,P} \leftarrow (y_P - y_T)/(x_P - x_T)$
2.	$l_{T,P}(Q) \leftarrow (x_Q - x_P)\lambda_{T,P} - (y_Q - y_P)$
3.	$f \leftarrow f \cdot l_{T,P}(Q)/v_{T+P}(Q)$
4.	return f
	EADD
5.	$x_{T+P} \leftarrow \lambda_{T,P}^2 - x_T - x_P$
6.	$y_{T+P} \leftarrow (x_P - x_{T+P})\lambda_{T,P} - y_P$
7.	return $T \leftarrow T + P$

3.2 Proposed Method

Proposed method calculates $f_{s,P}$ using $f_{\chi,P}$, $f_{\chi^2,P}$ and $f_{\chi^3,P}$, where $f_{\chi,P}$, $f_{\chi^2,P}$ and $f_{\chi^3,P}$ are the rational functions for χD, $\chi^2 D$ and $\chi^3 D$, respectively and are given as follows.

$$\begin{aligned} \chi D &= (\chi P) - (\mathcal{O}) + div(f_{\chi,P}) & (14) \\ \chi^2 D &= (\chi^2 P) - (\mathcal{O}) + div(f_{\chi^2,P}) & (15) \\ \chi^3 D &= (\chi^3 P) - (\mathcal{O}) + div(f_{\chi^3,P}) & (16) \end{aligned}$$

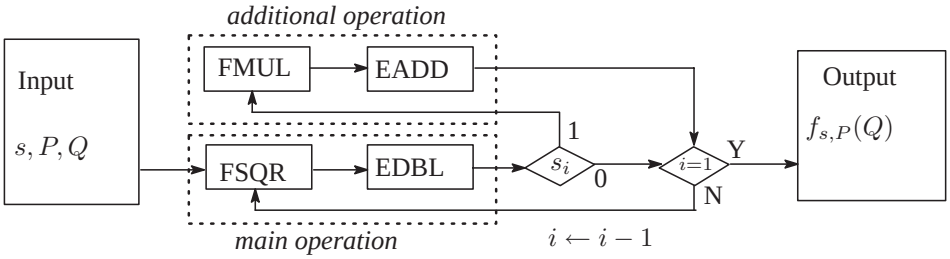

Figure 1. Calculation flow of Miller's algorithm

Table 1. Notations used in **Algorithm 1** and **Algorithm 2**

s_i :	i–th bit of the binary representation of s from the lower.
$l_{T,T}$:	the tangent line at T.
$l_{T,P}$:	the line passing through T and P.
v_{T+T} :	the vertical line passing through $2T$.
v_{T+P} :	the vertical line passing through $T+P$.
$\lambda_{T,T}$:	the slope of the tangent line $l_{T,T}$.
$\lambda_{T,P}$:	the slope of the line $l_{T,P}$.

Table 2. χ of small Hamming weight that gives 158–bit and 254–bit prime order BN curve

$p(\chi)$	χ	Hw(s)
158 bit	$2^{38}+2^{15}+2^{14}$	65
	$2^{38}+2^{27}+2^{16}$	62
	$2^{38}+2^{28}+1$	36
	$-2^{38}-2^{32}-2^{5}$	47
254 bit	$2^{62}+2^{46}+2^{29}$	83
	$2^{62}+2^{35}+2^{24}$	82
	$2^{62}+2^{55}+1$	36
	$-2^{62}-2^{41}-2^{23}$	43

Algorithm 3 shows Miller's algorithm whose initial value of f is f'. According to Eq.(11b), $f_{\chi^2,P}$ is calculated using $f_{\chi,P}$ by **Algorithm 3**. In this calculation, we need χP; however, we can obtain χP in $f_{\chi,P}$ calculation.

Similarly, $f_{\chi^3,P}$ can be calculated by **Algorithm 3**.

Then $f_{s,P}$ is calculated by combining $f_{\chi,P}$, $f_{\chi^2,P}$ and $f_{\chi^3,P}$ where s deformated as

$$\begin{aligned} s &= 3(\,12\chi^3+6\chi^2+2\chi\,)+1 \\ &= 6(\,3(\,2\chi^3+\chi^2\,)+\chi\,)+1. \end{aligned} \tag{17}$$

Let $s_1 = 2\chi^3+\chi^2$, according to Eq.(13a), we have $f_{s_1,P}$ as

$$f_{s_1,P} = f^2_{\chi^3,P}\cdot g_{\chi^3 P,\chi^3 P}\cdot f_{\chi^2,P}\cdot g_{2\chi^3 P,\chi^2 P}. \tag{18}$$

Then, let $s_2 = 3s_1+\chi$, we have $f_{s_2,P}$ as

$$f_{s_2,P} = f^3_{s_1,P}\cdot g_{s_1 P,s_1 P}\cdot g_{2s_1 P,s_1 P}\cdot f_{\chi,P}\cdot g_{3s_1 P,\chi P}. \tag{19}$$

Let $s_3 = 3s_2$, we have $f_{s_3,P}$ as

$$f_{s_3,P} = f^3_{s_2,p}\cdot g_{s_2 P,s_2 P}\cdot g_{2s_2 P,s_2 P}. \tag{20}$$

Algorithm 3 :Miller's Algorithm whose initial value of f is f'.

Input: $P\in\mathbb{G}_1$, $Q\in\mathbb{G}_2$, $f'\in\mathbb{F}_{p^{12}}$
Output: $f_{\chi,P'}(Q)$

1. $f \leftarrow f'$, $T \leftarrow P$.
2. For $i = \lfloor \log_2(s) \rfloor$ downto 1:
3. $\quad f \leftarrow f^2\cdot l_{T,T}(Q)/v_{T+T}(Q)$.
4. $\quad T \leftarrow 2T$.
5. $\quad$ If $s[i]=1$,then:
6. $\quad\quad f \leftarrow f\cdot f'\cdot l_{T,P}(Q)/v_{T+P}(Q)$.
7. $\quad\quad T \leftarrow T+P$.
8. Return f

Since $s = 2s_3+1$, $f_{s,P}$ can be obtained as

$$f_{s,P} = f^2_{s_3,P}\cdot g_{s_3 P,s_3 P}\cdot g_{2s_3 P,P}. \tag{21}$$

As mentioned above, the proposed method calculates $f_{s,P}$ by using $f_{\chi,P}$, $f_{\chi^2,P}$ and $f_{\chi^3,P}$. Thus, the proposed method can reduce the number of *additional operations* when χ has a small hamming weight. Inversely, since the proposed method needs combining $f_{\chi,P}$, $f_{\chi^2,P}$ and $f_{\chi^3,P}$, its calculation cost is not less than the calculation cost of the conventional method.

4. Cost Evaluation and Simulation

4.1 Cost Evaluation

This section compares the calculation costs of the proposed and conventional methods. In order to make the cost evaluation simple, we only take the calculation costs for multiplication and inversion in finite field into acount. In what follows, M_1 and I_1 denotes the calculation costs for multiplication and inversion in $\mathbb{F}_p$, respectively. Following the cost evaluation manner of [4][9], let $M_{12} = 45M_1$, where M_{12} denotes the calculation cost of a multiplication in $\mathbb{F}_{p^{12}}$. Then, calculating $l_{T,T}(Q)$ and $l_{T,P}(Q)$ need ($7M_1$+I_1) and ($8M_1$+I_1), respectively. Let C_{pro} and C_{con} be the calculation costs of the proposed and conventional methods, respectively they are become

$$\begin{aligned} C_{con} &= (99M_1+I_1)\cdot\lfloor\log_2(s)\rfloor+(55M_1+I_1)\cdot \mathrm{Hw(s)} \\ &\quad +(246M_1+2I_1) \end{aligned} \tag{22}$$

$$\begin{aligned} C_{pro} &= (297M_1+3I_1)\cdot\lfloor\log_2(\chi)\rfloor+(255M_1+3I_1)\cdot \mathrm{Hw}(\chi) \\ &\quad +(669M_1+9I_1) \end{aligned} \tag{23}$$

Then, supposing that Hw(χ)=3, $\lfloor\log_2(\chi)\rfloor = \frac{1}{3}\lfloor\log_2(s)\rfloor$ and roughly $I_1 = 10M_1$, we obtain the condition that Hw(s)

Table 3. parameters of twisted Ate pairing

size of p, r	158 bit	254 bit
BN curve	$y^2 = x^3+10$	$y^2 = x^3+10$
χ	$-2^{38}-2^{32}-2^5$	$2^{62}+2^{35}+2^{24}$
Hw(s)	47	82
Hw(χ)	3	3

Table 4. comparison of timings[ms]

p, r		158bit	254bit
Miller part	conventional	6.05	14.5
	proposed	5.19	12.0
final exponentiation		2.02	4.45
total	conventional	8.07	19.0
	proposed	7.21	16.5
elliptic curve scalar multiplication*	$\mathbb{G}_1 \in \mathbb{E}(\mathbb{F}_p)$**	0.92	2.31
	$\mathbb{G}'_2 \in \mathbb{E}'(\mathbb{F}_{p^2})$	2.72	7.01

*Average timings with random scalars and exponents of $\lfloor \log_2(r) \rfloor$ bit.

** *Projective cordinate* is used.

satisfies $C_{pro} > C_{con}$ as

$$\begin{aligned} &\mathrm{Hw(s)} < 4.38\mathrm{Hw}(\chi) + 7.58, \\ &4.38\mathrm{Hw}(\chi) + 7.58 \leftrightharpoons 20.7, \\ &\mathrm{Hw(s)} < 20. \end{aligned} \tag{24}$$

According to **Table** 2, Hw(s) that satisfies Eq.(24) does not exist. Thus, in the case of using χ with small hamming weight that gives 158–bit and 254–bit prime order BN curves, the calculation cost of the proposed method is less than that of the conventional method.

4.2 Simulation result

In order to show the efficiency of the proposed method, the authors simulated twisted Ate pairing with BN curve of order $r \approx 2^{158}, 2^{254}$. In this simulation, the authors used χ and BN curve shown in **Table** 3. **Table** 4 shows the simulation result. As a reference, **Table** 5 shows timings of multiplication(mul), inversion(inv) in some subfield of $\mathbb{F}_{p^{12}}$ and squaring in $\mathbb{F}_{p^{12}}$. According to **Table** 4, in the cases of $r \approx 2^{158}$ and $r \approx 2^{254}$, the proposed method reduced the calculation times of Miller's algorithm by 7.4% and 14.2%, respectively.

5. Conclusion

Using BN curve whose embedding degree is 12, this paper proposed an improvement of Miller's algorithm of twisted Ate pairing by using χ of small hamming weight. The proposed method improved $f_{s,P}$ calculation by setting χ of small hamming weight. In order to show the efficiency of the proposed method, the authors simulated on Pentium4 (3.6GHz) with C language and GMP library [8]. Then, it was shown that, in the cases of $r \approx 2^{158}$ and $r \approx 2^{254}$, the proposed method reduced the calculation times of Miller's algorithm by 7.4% and 14.2%, respectively.

Table 5. Timing each operation in extension field[μs]

p, r		158 bit	254 bit
$\mathbb{F}_p$	mul	0.41	0.65
	inv	4.93	8.43
$\mathbb{F}_{p^2}$	mul	1.08	1.65
	inv	6.82	11.4
$\mathbb{F}_{p^4}$	mul	2.92	4.39
	inv	12.4	19.6
$\mathbb{F}_{p^6}$	mul	5.98	7.78
	inv	22.8	32.4
$\mathbb{F}_{p^{12}}$	mul	14.7	21.6
	inv	54.2	80.3
	sqr	13.2	19.7

6. Acknowledgement

This work is supported by "Strategic Information and Communications R&D Promotion Programme" from the Ministry of Internal Affairs and Communications, Japan.

References

[1] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing", SCIS2000, Jan. 2000.

[2] T. Nakanishi, and N. Funabiki, "Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps", ASIACRYPT 2005, LNCS, Vol. 3788, pp. 533-548, Dec. 2005.

[3] H. Cohen and G. Frey, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, *Discrete Mathematics and Its Applications*, Chapman & Hall CRC, 2005.

[4] S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto, "Optimised versions of the Ate and Twisted Ate Pairings," IACR, ePrint, Available at http://eprint.iacr.org/2007/013.pdf

[5] A. J. Devegili, M. Scott, and R. Dahab, "Implementing Cryptographic Pairings over Barreto-Naehrig Curves," LNCS, Vol.4575, pp. 197-207, 2007.

[6] M. Akane, H. Kato, T. Okimoto, Y. Nogami, and Y. Morikawa, "An Improvement of Miller's Algorithm in Ate Pairing with Barreto–Naehrig Curve," Proc. of Computer Security Symposium 2007 (CSS2007), pp. 489–494, 2007.

[7] P. S. L. M. Barreto, and M. Naehrig. "Pairing-Friendly Elliptic Curves of Prime Order", SAC 2005, LNCS, Vol. 3897, pp. 319-331, 2006.

[8] GNU MP, http://gmplib.org/

[9] F. Hess, N. Smart, and F. Vercauteren, "The Eta Pairing Revisited", IEEE Trans. Information Theory, pp. 4595-4602, 2006.

[10] A. J. Devegili, M. Scott, and R. Dahab, "Implementing Cryptographic Pairings over Barreto-Naehrig Curves", LNCS, Vol. 4575, pp. 197-207, 2007.