基于双基数链的 Tate 对快速算法

陈厚友,马传贵
(郑州信息科技学院,河南郑州 450002)

摘 要: 椭圆曲线上双线性对快速实现的核心是 Miller 算法.本文给出了一种改进的 Miller 算法,其核心思想是将{2,3}-双基数链与 Millier 算法相结合,此算法在计算双线性对时能够有效地减少 Miller 算法中的迭代次数,而更有价值的是,此算法不仅适用于超奇异椭圆曲线同时还适用于一般的椭圆曲线.由本文给出的实验结果可知,新算法与其它现有的算法相比其效率提高约 10.6% ~ 20.3%.

关键词: 双基数链; 除子; Miller 算法; Tate 对
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2011) 02-0408-06

Fast Tate Pairing Algorithm Using Double-Base Chains

CHEN Hou-you, MA Chuan-gui
(*Zhengzhou Information Science and Technology Institute*, *Zhengzhou*, *Henan* 450002, *China*)

Abstract: The fast implementation of bilinear pairing on elliptic curve has heavily depended on the Miller's algorithm. In this paper, an improved Miller's algorithm is presented and the basic idea of this algorithm is that it combines the {2,3}-double-base chains with the Miller's algorithm, thus, it can reduces the iteration times in Miller's algorithm efficiently during the computation of bilinear pairing. What is important, this new algorithm can not only be applied to the case of super-singular elliptic curve, but also can be applied to the case of ordinary elliptic curve. As indicated by the experimental results in this paper, the computational efficiency of our new method has been improved by 10.6% ~ 20.3% on average than other existing methods.

Key words: double-base chains; divisor; Miller's algorithm; Tate pairing

1 引言

自 2000 年 Sakai 等人[1]提出了基于双线性对的身份认证协议后,基于双线性对的密码体系便成为椭圆曲线密码学研究的前沿和热点之一,并且基于双线性对的协议已经被成功地应用于身份加密[2]、短签名[3]以及群签名等多个领域当中.与传统协议相比,采用双线性对来构造协议可有效地减少带宽,但其计算所花费的时间要多于计算模幂或椭圆曲线上的标量乘,因此,构造一个计算双线性对的有效算法对于基于双线性对的密码体系是十分重要的.

计算双线性对的核心是 Miller 算法[4~8].虽然近几年来基于双线性对的密码算法研究得到密码学家们的广泛关注,一系列新的算法不断被提出和改进,但其主要思想都是使用单基数的 Miller 算法.Duursma 等人[9]首先于 2003 年提出了在特征为 p 的 $y^2 = x^p - x \pm 1$, $p \equiv 3 (\mathrm{mod} 4)$ 上的快速 Tate 对算法;Zhao 等人[10]于 2007 年进一步证明了 Miller 算法循环长度最短为 $r^{1/\Phi(k)}$,其中 k 为嵌入度,Φ 为 Euler 函数;文献[11]进一步地给出了适用于超奇异椭圆曲线和一般椭圆曲线的 Tate 对快速算法,并把 Tate 对的计算分为如下三步:(1)计算椭圆曲线上的点加和点倍;(2)计算直线 g, v 的系数;(3)计算 $g(Q), v(Q)$ 的值,迭代 $f_{i,P}(Q)$,最后求幂.此外,Chatterjee 等人[12]在文献[11]的基础上使用了 Jacobian 坐标并采用压缩计算方法进一步提高了 Tate 对的计算效率.Barreto 等人[13]于 2004 年改进了 Duursma[9]所提出的算法,给出了 Tate 对在超奇异椭圆曲线上的一种更快的算法,称为 Eta 对算法,而 Eta 对算法是现有的计算双线性对快速算法之一.Lee 等人[14]于 2008 年又对特征为 p 的 $y^2 = x^p - x \pm 1$ 进行了改进,其工作拓广了 Eta 对的应用领域;Hess 等人[4]于 2006 年提出了 Eta 对的逆,其工作进一步提高了双线性对在特定条件下的运算效率.而另一方面,Granger 等人[5]在 2007 年提出了在椭圆曲线和超椭圆曲线上的 Ate 对算法;同年,Matsuda 等人[6]提出了优化的 Ate 对算法并称其为优化的 Ate 对算法或优化的 twisted Ate 对算法.对于基于 Ate 对的 Miller 算法而言,

收稿日期:2009-06-24;修回日期:2010-09-10
基金项目:国家自然科学基金(No.90704003);国家 863 高技术研究发展计划(No.863-317-01-04-99, No.2007AA012431)

其循环长度由$(t-1) \bmod r$所决定,其中 t 为 q 次 Frobenius 变换的迹,而 r 为椭圆曲线阶的一个大素数因子.

Miller 算法效率的提高主要包括两种途径,一种是改进双线性对的构造;而另一种则是在特定条件下寻找 Miller 算法中具体参数的最优化.下面将介绍几种常用的在特定条件下通过取不同参数的优化 Miller 算法[7,8,11,13,15,16].

在计算 Tate 对时,用点代替除子　由于除子和函数除子的支撑一定不相交,因此,$f_{l,P}(D_Q)$可以用 $f_{l,P}(Q+R)/f_{l,P}(R)$代替,其中 $R \in E(F_{q^k})$是椭圆曲线上任意一点.

最终求幂的优化　若 l 能被 N 取代,其中 N 满足 $l \mid N \mid q^k-1$,那么在计算最终求幂时,可用$(q^k-1)/N$取代$(q^k-1)/l$.

可以事先进行预计算　在计算双线性对时,由于通常 P 为一固定的基点,因此,在标量乘和直线的计算过程中可以通过预计算以减少点乘的复杂度.

Miller 算法中参数选择的优化　若选择 $R \in E(F_q)$,则在实现 Miller 算法的过程中 $f_{l,P}(R)$就仅需在有限域 F_q 上进行计算,而不是在扩域 F_{q^k}上进行计算,并且在特定条件下,$f_{l,P}(Q+R)/f_{l,P}(R)$可以用 $f_{l,P}(Q)$替换,这是由于为了使 Tate 对的值唯一,在计算 Tate 对时需要最终$(q^k-1)/l$次幂计算,又因为$(q-1) \mid ((q^k-1)/l)$,于是有 $f_{l,P}(R)^{q-1}=1$,取 $R=\infty$,因此有 $f_{l,P}(Q+R)/f_{l,P}(R)=f_{l,P}(Q)$.

Miller 算法中循环复杂度的优化　l 的重量对降低循环复杂度起到至关重要的作用,因此在满足密码安全性要求的条件下,一般取低重量的 l.

Miller 算法中直线的优化　已有压缩算法和伪乘算法.

更进一步的,由于双基数链自身所具有的一系列优势:极大的稀疏性,也即 K 的 DBNS(double-base number system)表达式中系数的个数非常少;极好的兼容性,即双基数链算法可以和许多标量乘算法结合以提高椭圆曲线标量乘算法的计算效率,这使得近几年采用双基数来实现椭圆曲线标量乘算法的论文不断涌现,并已发展成为目前处理椭圆曲线标量乘算法较流行的一种思路.Zhao 等人[17]于 2008 年首次将双基数链应用于双线性对的计算当中,这一算法不仅能应用在超奇异椭圆曲线上而且还能应用在一般椭圆曲线上,同时与其它现有的算法相比,其效率提高了约 9% ~37.8%.受此思想启发,在 Zhao 等人的基础上,本文进一步对双基数链的生成算法和除子计算进行优化,使得基于双基数链的双线性对计算效率得到进一步的提高,实验数据结果表明,本文所提出的新算法比目前计算双线性对的最快算法其运算效率提高约 10.6% ~20.3%.

2　背景知识

2.1　双线性对的简介

由于 Weil 对的计算最为复杂且一般被认为是两次 Tate 对的运算[18],而对于近几年所提出的新的双线性对,如 Eta 对[7],Ate 对[19]等本质上都是对 Tate 对的改进,其基本思想与 Tate 对都一样,因此,为了节省篇幅,本文在这里仅介绍 Tate 对.

定义 1(Tate 对)　l 是一个正素数,且 $l \mid \#J_E(F_q)$,$(l,q)=1$,E 是域 F_q 上的椭圆曲线,J_E 是 E 上的零除子群,k 是嵌入度,即为使得 $l \mid (q^k-1)$达到最小的 k.设 $J_E[l]=\{P \in J_E \mid lP=\infty\}$,$D_P=\langle P\rangle-\langle\infty\rangle$,$D_Q=\langle Q+R\rangle-\langle R\rangle$,$R \in E(F_{q^k})$,其中$\infty$为 $E(F_q)$的无穷远点.

$$\langle . \rangle_l : J_E[l] \times J_E(F_{q^k})/lJ_E(F_{q^k}) \to F_{q^k}^*/(F_{q^k}^*)^l$$

$$\langle P,Q\rangle_l = f_{l,P}(D_Q)$$

其中 $div(f_{l,P})=lD_P$,且满足 $support(D_Q) \cap support(div(f_{l,P}))=\phi$,$f_{l,P}(D_Q)$为属于$(F_{q^k}^*)^l$的陪集,因此,为了使 Tate 对的值唯一,需要进行$\frac{q^k-1}{l}$次幂计算,即满足 $t(P,Q)=\langle P,Q\rangle_l^{\frac{q^k-1}{l}}=f_{l,P}(D_Q)^{\frac{q^k-1}{l}}$是唯一的.

Tate 对的一个重要性质[15]

若 l 能整除任意的整数 N,且 N 满足 $l \mid N \mid q^k-1$,有 $t(P,Q)=\langle P,Q\rangle_N^{\frac{q^k-1}{N}}$.

2.2　除子的简介

定义 2　$Div(E)=\{D=\sum_{P\in E} m_P[P] : m_P \in \mathbb{Z}\}$,其中,$m_P$ 几乎处处为零,$Div(E)$被称为 E 的除子群,D 为 E 的除子,其次数记作 $\deg(D)=\sum_{P\in E} m_P$,其和记作 $sum(D)=\sum_{P\in E}[m_P]P$,$Div(E)$是 E 所生成的自由 Abel 群.

除子与函数的关系

定义 3　f 是 E 上的有理函数,其生成的除子为$\langle f\rangle=\sum_{P\in E} ord_P(f)\langle P\rangle$,$ord_P(f)$是 f 在点 P 的零点或奇点的阶.若 $supp(\langle f_1\rangle) \cap supp(\langle f_2\rangle)=\varnothing$,有:

$$\langle f_1\rangle+\langle f_2\rangle=\langle f_1 \cdot f_2\rangle$$

$$\langle f_1\rangle-\langle f_2\rangle=\langle \frac{f_1}{f_2}\rangle \text{成立}$$

推论 1　一个除子 D 被称为主除子当且仅当 $\deg(D)=0$,$sum(D)=\infty$.

若一个除子 D 为主除子,那么存在 E 上的有理函数 f 使得 $D=\langle f\rangle$.

引理 1[8]　$P \in E(F_q)$,在 F_{q^k}上的有理函数 $f_{l,P}$,满足:

$$\langle f_{l,P}\rangle = l\langle P\rangle - \langle [l]P\rangle - (l-1)\langle \infty\rangle, l\in \mathbb{Z}$$

那么,对任意的 $i,j\in\mathbb{Z}$,有

$$f_{i+j,P} = f_{i,P}\cdot f_{j,P}\cdot g_{iP,jP}/g_{iP+jP}$$

其中,$g_{iP,jP}$为过点 iP,jP 的直线,当 $i=j$ 时,$g_{iP,jP}$即退化为过点 iP 的切线;v_{iP+jP}为过点 $iP+jP$ 的垂线,当 $i=j$ 时,v_{iP+jP}即退化为过点 $2iP$ 的垂线.

证明 见参考文献[8]

2.3 Miller 算法[20]:

输入 $P\in E(F_q)[n], Q\in E(F_{q^k})/nE(F_{q^k})$

输出 $f\in F_{q^k}$

(1)设 $n=(n_l,n_{l-1},\cdots n_0), n_i\in\{0,1\}$

(2)设 $f\leftarrow 1, T\leftarrow P, i\leftarrow l-1$

(3)$i\leftarrow l-1,\cdots,1,0$ do

{3.1 $f\leftarrow f^2\cdot g_{T,T}(Q)/v_{2T}(Q), T\leftarrow 2T$

如果 $n_i=1$ do

3.2 $f\leftarrow f\cdot g_{T,P}(Q)/v_{T+P}(Q), T\leftarrow T+P$

}

(4)输出 f

其中 $g_{T,P}$为过点 T,P 的直线,当 $T=P$ 时 $g_{T,P}$为过点 T 的切线;v_{T+P}为过点 $T+P$ 的垂线,当 $T=P$ 时 v_{T+P}即为过点 $2T$ 的垂线.

2.4 双基数链

在 2005 年的亚洲密码学会议上,Dimitrov[21]定义了 $\{2,3\}$—双基链为:$\sum_i d_k 2^{a_i}3^{b_i}$,其中 $d_k\in\{-1,1\}$,并同时给出了限制条件 $a_1\geqslant a_2\geqslant a_3\geqslant\cdots$ 和 $b_1\geqslant b_2\geqslant b_3\geqslant\cdots$,也即:设 l 是一个大于零的整数,则 l 的双基数表示为 $l=\sum_{i=1}^{k} d_i 2^{a_i}3^{b_i}$,其中 $d_i\in\{-1,1\}$且 $a_1\geqslant a_2\geqslant\cdots\geqslant a_k\geqslant 0, b_1\geqslant b_2\geqslant\cdots\geqslant b_k\geqslant 0$,其基本思想就是利用贪婪算法把 l 展开成双基数链的形式,相应的具体算法见文献[21].

表 1 文献[21]中双基数链长度

	$a_{\max}$	$b_{\max}$	m	$a_{\max}$	$b_{\max}$	m
文献[21]算法	57	65	45	95	41	37
	76	53	38	103	36	39

其中,表 1 中 $a_{\max}, b_{\max}$为 2,3 最大指数幂,m 表示随机选取的 10000 个 l 在 2,3 最大指数幂相同的情况下,l 展开式中双基数的个数.通过表可以看出双基数链比单基数链更短,这也意味着基于双基数链的 Tate 对计算效率更高.

3 基于双基数链的 Tate 对快速计算

由于双基数链具有极大的稀疏性和极好的兼容性等优点,在 2008 年,Zhao 等人[17]首次把双基数链应用于双线性对计算中,此算法不仅能应用于超奇异椭圆曲线而且还能应用于一般椭圆曲线,并且与其它现有的算法相比,其运算效率提高了约 9% ~37.8%.

由于计算基于{2,3}—双基数链的 Tate 对需要计算三倍点的双线性对,下面将给出基于 Miller 算法的三倍点公式:(符号同第二章)

由引理 1 得:

$$f_{2r,P} = f_r^2 g_{rP,rP}(Q)/v_{2rP}(Q)$$

$$f_{3r,P} = f_{2r,P} f_{r,P} g_{2rP,rP}(Q)/v_{3rP}(Q)$$

因此

$$f_{3r,P}(Q) = f_r^3(Q) g_{rP,rP}(Q) g_{2rP,rP}(Q)/(v_{2rP}(Q)v_{3rP}(Q))$$

算法 1 改进的基于双基数链的 Miller 算法

输入 $P\in E(F_q)[l], Q\in E(F_{q^k})/lE(F_{q^k})$

输出 $f_{l,P}(Q)$

(1)计算 $l=\sum_i d_k 2^{a_i}3^{b_i}$,其中 $a_1\geqslant a_2\geqslant a_3\geqslant\cdots, b_1\geqslant b_2\geqslant b_3\geqslant\cdots$,且 $d_k\in\{-1,1\}$,$Sum\leftarrow\{d_k$ 的个数$\}$

(2)设 $f\leftarrow 1, T\leftarrow P, t\leftarrow 0, a_i\leftarrow a_1, b_i\leftarrow b_1$

(3)$i\leftarrow 1,\cdots, Sum-1$ do

{3.1 $t\leftarrow a_i - a_{i+1}$,如果 $t\geqslant 1$,那么 $f\leftarrow f^2\cdot g_{T,T}(Q)/v_{2T}(Q), T\leftarrow 2T, t\leftarrow t-1$

3.2 $t\leftarrow b_i - b_{i+1}$,如果 $t\geqslant 1$,那么 $f\leftarrow f^3\cdot g_{T,T}(Q)\cdot g_{2T,T}(Q)/v_{2T}(Q)\cdot v_{3T}(Q), T\leftarrow 3T, t\leftarrow t-1$

3.3 如果 $d_{i+1}=1$,那么 $f\leftarrow f\cdot g_{T,P}(Q)/v_{T+P}(Q), T\leftarrow T+P$

3.4 如果 $d_{i+1}=-1$,那么 $f\leftarrow f\cdot g_{T,-P}(Q)/v_{T-P}(Q), T\leftarrow T-P$

3.5 $i\leftarrow i+1$

}

(4)输出 $f^{(q^k-1)/l}$

4 算法 1 的优化及复杂度分析

为了得到算法 1 的复杂度,本文中采用参考文献[17]的符号以及符号之间的转换关系,其中 M,S,I 分别表示有限域 F_q 上的乘法、平方以及求逆;M_k, S_k, I_k 则分别表示有限域 F_{q^k}上的乘法、平方以及求逆;M_b 表示域 F_q 上的元素与域 F_{q^k}上的元素的乘且满足:$M_k = k^{1.6}M, M_b = kM, S=0.8M, I=10M$(其中 k 表示嵌入度).域上的加法和减法忽略不计.

令 TADD,TSUB,TDBL,TTRL 分别表示椭圆曲线上的点加、点减、点倍、三倍点,在计算有理函数 f 时为了有效减少域上的求逆运算,文献[17]证明了结论:$(x_Q - x_1)^{-1} = \bar{x}_Q - x_1, x_1\in F_q^*$.

4.1 TADD 的计算

输入:$P=(x_P,y_P), T=(x_1,y_1)\in E(F_q), Q=(x_Q, y_Q)\in E(F_{q^k}), f\in F_{q^k}^*$

输出:f

(1) $T_3=(x_3,y_3)\leftarrow ECADD(T,P)$

(2) $g\leftarrow(y_Q+y_3)-\lambda(x_Q-x_3)$

(3) $v\leftarrow x_Q-x_3$

(4) $f\leftarrow f\cdot(g\bar{v})$

(5)输出 f

根据多项式扩展算法[11,16],有:

$$g\bar{v}=\frac{(y_Q+y_3)-\lambda(x_Q-x_3)}{x_Q-x_3}=\frac{y_Q+y_3}{x_Q-x_3}-\lambda$$
$$=(y_Q+y_3)(\bar{x}_Q-x_3)-\lambda$$
$$=y_Q\bar{x}_Q+y_3\bar{x}_Q-(y_Q+y_3)x_3-\lambda$$

其中 g 过点 P, T 以及 $-T_3$,因此有: $g=(y_Q-y_P)-\lambda(x_Q-x_P)=(y_Q+y_3)-\lambda(x_Q-x_3)$. 为了优化 TADD,选择 $g=(y_Q+y_3)-\lambda(x_Q-x_3)$,由于 $y_Q\bar{x}_Q$ 可以预计算,于是计算 $y_3\bar{x}_Q$ 和 $(y_Q+y_3)x_3$ 需要 $2M_b$,因此,计算 TADD 总共需要 $M_k+2M_b+ECADD$. 若采用文献[16]给出的伪乘算法,当 $k\geqslant 3$ 时可以优化为 $M_k+1.5M_b+ECADD$,而预计算则需要 $M_k+7M_{k/2}+I_{k/2}$.

4.2 TSUB 的计算

在计算有理函数 $f_{r,P}$时,由文献[4]可知,当 $r<0$ 时,有: $\langle f_{r,P}\rangle=-\langle f_{-r,P}\rangle-\langle v_{rP}\rangle$. 因此,可设 $P=(x_P,y_P)$,其中 $P\in E(F_q)$, $Q=(x_Q,y_Q)$, $Q\in E(F_{q^k})$,有:

$$f_{-1}g(Q)=\frac{(y_Q+y_P)-\lambda(x_Q-x_P)}{x_Q-x_P}=\frac{y_Q+y_P}{x_Q-x_P}-\lambda$$

其中$\frac{y_Q+y_P}{x_Q-x_P}$可以预计算.

TSUB 算法

输入: $T=(x_1,y_1)$, $P=(x_P,y_P)$, $T,P\in E(F_q)$, $Q=(x_Q,y_Q)\in E(F_{q^k})$, $f\in F_{q^k}^*$

输出: f

(1) $T_4=(x_4,y_4)\leftarrow ECADD(T,-P)$

(2) $f_{-1}g(Q)\leftarrow\frac{y_Q+y_P}{x_Q-x_P}-\lambda$

(3) $v\leftarrow x_Q-x_4$

(4) $f\leftarrow f\cdot(f_{-1}g\bar{v})$

(5)输出 f

利用多项式扩展算法[11,16],令 $T_{sub}=\frac{y_Q+y_P}{x_Q-x_P}$,则:

$$f_{-1}g\bar{v}=\left(\frac{y_Q+y_P}{x_Q-x_P}-\lambda\right)(\bar{x}_Q-x_4)=(T_{sub}-\lambda)(\bar{x}_Q-x_4)$$
$$=T_{sub}\bar{x}_Q-\lambda\bar{x}_Q-(T_{sub}-\lambda)x_4$$

其中 $T_{sub}\bar{x}_Q$ 可以预计算,而计算 $\lambda\bar{x}_Q$, $(T_{sub}-\lambda)x_4$ 花费 $2M_b$,因此,TSUB 的计算总共需要 $M_k+2M_b+ECADD$,预计算需要 I_k+M_k.

4.3 TDBL 的计算

输入: $T=(x_1,y_1)\in E(F_q)$, $Q=(x_Q,y_Q)\in E(F_{q^k})$, $f\in F_{q^k}^*$

输出: f

(1) $T_2=(x_2,y_2)\leftarrow ECDBL(T)$

(2) $g\leftarrow(y_Q+y_2)-\lambda(x_Q-x_2)$

(3) $v\leftarrow x_Q-x_2$

(4) $f\leftarrow f^2\cdot(g\bar{v})$

(5)输出 f

利用多项式扩展算法[11,16],有:

$$g\bar{v}=\frac{(y_Q+y_2)-\lambda(x_Q-x_2)}{x_Q-x_2}=\frac{y_Q+y_2}{x_Q-x_2}-\lambda$$
$$=(y_Q+y_2)(\bar{x}_Q-x_2)-\lambda$$
$$=y_Q\bar{x}_Q+y_2\bar{x}_Q-(y_Q+y_2)x_2-\lambda$$

其中 g 过点 T 和点 $-T_2$,因此, $g=(y_Q-y_1)-\lambda(x_Q-x_1)=(y_Q+y_2)-\lambda(x_Q-x_2)$. 为了优化 TDBL,选择 $g=(y_Q+y_2)-\lambda(x_Q-x_2)$,而 $y_Q\bar{x}_Q$ 已预计算,于是计算 $y_2\bar{x}_Q$, $(y_Q+y_2)x_2$ 花费 $2M_b$,因此,TDBL 计算总共需要 $M_k+S_k+2M_b+ECDBL$. 若采用文献[16]给出的伪乘算法,则可以优化到 $M_k+S_k+1.5M_b+ECDBL$.

4.4 TTRL 计算

输入: $T=(x_1,y_1)\in E(F_q)$, $Q=(x_Q,y_Q)\in E(F_{q^k})$, $f\in F_{q^k}^*$

输出: f

(1) $T_5=(x_5,y_5)\leftarrow ECTRL(T)$

(2) $g\leftarrow\frac{g_{T,T}(Q)g_{T,2T}(Q)}{v_{2T}(Q)}$

(3) $v\leftarrow x_Q-x_5$

(4) $f\leftarrow f^2\cdot f\cdot(g\bar{v})$

(5)输出 f

为了优化计算 TTRL 需要如下引理:

引理 2[22]　若直线 g 过点 P, Q 且 $P\in E$, $Q\in E$, $P+Q=(x_3,y_3)$,令 $\tilde{g}(R)=g(-R)$,于是有:

$$N_{K(x,y)/K(x)}(g)=-(x-x_P)(x-x_Q)(x-x_3)=\tilde{g}g$$

其中 N 表示范数. 相关证明请参见文献[22].

根据上述引理,有:

$$\frac{g_{T,T}(Q)g_{2T,T}(Q)}{v_{2T}(Q)v_{3T}(Q)}=\frac{g_{T,T}(Q)g_{2T,T}(Q)g_{2T,T}(-Q)}{v_{2T}(Q)v_{3T}(Q)g_{2T,T}(-Q)}$$
$$=\frac{g_{T,T}(Q)N_{K(x,y)/K(x)}(g_{2T,T})(Q)}{v_{2T}(Q)v_{3T}(Q)g_{2T,T}(-Q)}$$
$$=-\frac{g_{T,T}(Q)(x_Q-x_T)}{g_{2T,T}(-Q)}=-\frac{g_{T,T}(Q)v_T(Q)}{g_{2T,T}(-Q)}$$

利用多项式扩展算法[11,16],有:

$$g\bar{v}=\frac{g_{T,T}(Q)g_{T,2T}(Q)}{v_{2T}(Q)v_{3T}(Q)}=-\frac{g_{T,T}(Q)v_{2T}(Q)}{g_{T,2T}(-Q)}$$
$$=-\frac{g_{T,T}(Q)(x_Q-x_2)}{(-y_Q-y_2)-\lambda_2(x_Q-x_2)}$$
$$=\frac{g_{T,T}(Q)}{(y_Q+y_2)(\bar{x}_Q-x_2)+\lambda_2}$$

$$= \frac{g_{T,T}(Q)}{(y_Q\bar{x}_Q + y_2\bar{x}_Q) - x_2(y_Q + y_2) + \lambda_2}$$

因此,$g\bar{v}$ 的计算需要 $M_k + 2M_b$,由于 $y_Q\bar{x}_Q$ 已预计算,因此,TTRL 的计算总共需要 $3M_k + S_k + 2M_b + ECTRL$.

限于篇幅的考虑,2-迭代以及 3-迭代可类似由文献[17]得到.

表 2 新算法中 Tate 对计算时每一步的复杂度

	运算	复杂度	预计算
参考文献[17]	TADD	$M_k + 2.5M_b + I + 3M + S$	$2M_k + I_{k/2} + 7M_{k/2}$
	TSUB	$M_k + 2M_b + I + 3M + S$	$2M_k + I_k$
	TDBL	$M_k + S_k + 3.5M_b + I + 4M + 2S$	$2M_k$
	TTRL	$3M_k + S_k + 2M_b + I + 9M + 4S$	$2M_k$
优化后算法 1	TADD	$M_k + 2M_b + I + 2M + S$	$M_k + 7M_{k/2} + I_{k/2}$
	TSUB	$M_k + 1.5M_b + I + 2M + S$	$M_k + I_k$
	TDBL	$M_k + S_k + 1.5M_b + I + 2M + 2S$	0
	TTRL	$3M_k + S_k + 2M_b + I + 7M + 4S$	0

5 实验数据分析

5.1 实验数据

根据目前椭圆曲线公钥密码安全性要求,椭圆曲线子群的阶至少为 160 比特,q^k 至少为 1024 比特.为了与现有算法相比较,不妨取 $\log_2^l = 160$, $M_k = k^{1.6}M$, $S_k = k^{1.6}S$, $M_b = kM$, $S = 0.8M$, $I = 10M$, $I_k = I + k^2M$.

优化后算法 1 需要预计算的复杂度为: $T_{pre} = 2M_k + I_k + 7M_{k/2} + I_{k/2}$.

优化后算法 1 的复杂度为算法 1 的 3.3 步取期望值(即点加和点减的个数相等时的复杂度).

$$\begin{aligned} & a_{\max}TDBL + b_{\max}TTRL + \frac{m}{2}(TADD + TSUB) + T_{pre} \\ &= (a_{\max} + 3b_{\max} + m + 2)M_k + (a_{\max} + b_{\max})S_k \\ &\quad + (1.5a_{\max} + 2b_{\max} + 1.75m)M_b \\ &\quad + (a_{\max} + b_{\max} + m)I + (2a_{\max} + 7b_{\max} + 2m)M \\ &\quad + (2a_{\max} + 4b_{\max} + m)S + I_k + 7M_{k/2} + I_{k/2} \end{aligned}$$

本实验的实施平台:Pentium(R)4CPU 2.0GHz,256MB,程序调用 MIRACL 函数库.

表 3 在不同条件下新算法 1 的复杂度(数据来源于表 1)

$a_{\max}$	$b_{\max}$	m	复杂度		
			$k=4$	$k=6$	$k=8$
57	65	45	7386M	11506M	15606M
76	53	38	7321M	11151M	15269M
95	41	37	7180M	10859M	14921M
103	36	39	7307M	10902M	14917M

5.2 算法间的比较

在这里仅将新算法与目前最快的两种算法文献[16,17]相比较.为了在相同条件下进行比较,本文随机选取文献[16,17]中的标量 l 为一长为 160 比特的大数,并取算法中点加和点减运算次数相等.

表 4 各种算法间复杂度比较

算法	复杂度		
	$k=4$	$k=6$	$k=8$
新算法 2	7321M	11151M	15269M
{2,3} – Miller 算法[17](2008)	8350M	12554M	17085M
有符号的 Miller 算法[16](2006)	9196M	13685M	18121M

通过表 4 容易发现新算法 2 比目前现有的最快两种算法其运算效率提高了约 10.6% ~ 20.3%,并且新算法同样适应于 $k = 2$ 的情况.

6 结论

目前基于双线性对的协议已经被成功地应用于身份加密、短签名、群签名等多个领域当中,因此,基于双线性对的密码体系便成为椭圆曲线密码学研究的前沿和热点之一.但其计算所花费的时间要多于计算模幂或椭圆曲线上的标量乘,因此,构造一个计算双线性对的有效算法对于基于双线性对的密码体系是十分重要的.

本文在 Miller 算法的基础上,将双基数链与 Miller 算法相结合,建立起了基于双基数链的 Tate 对快速计算的优化算法.本文中所提出的新算法在计算双线性对时不仅能够有效减少 Miller 算法的迭代次数,并且能够同时应用于超奇异椭圆曲线以及一般的椭圆曲线,且使得 Tate 对的计算更高效.由于 Weil 对的计算最为复杂且一般被认为是两次 Tate 对计算,而近几年来所提出的新双线性对如 Eta 对、Twisted Eta 对、Ate 对、Twisted Ate 对等都是对 Tate 对的改进,其主要思想都一样,因此,本文所给出的新算法同样适用于其它双线性对的运算.试验数据表明,新算法不仅继承了双基数链标量乘算法的优点,优化了传统的 Miller 算法在双线性对中的计算,值得注意的是,本文给出的优化算法比目前现有的最快算法其运算效率提高了约 10.6% ~ 20.3%并且新算法同样适应于基于{2,3,5} – 多基数的 Tate 对快速算法.

参考文献:

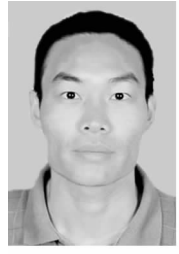
[1] R Sakai, K Ohgishi, M Kasahara. Cryptosystems based on pairing [A]. SCIS2000[C]. Japan, Okinawa, 2000. 26 – 28.

[2] B FU, J P LI. Efficient fuzzy vault based on pairing and its application to fingerprint encryption[J]. Chinese Journal of Electronics, 2010, 19 (2E): 249 – 255.

[3] 祁明, L Harn. 基于离散对数的若干新型代理签名方案[J]. 电子学报, 2000, 28(11): 114 – 118.
Qi Ming, L Harn. Some new proxy signature schemes based on

discrete logarithms[J]. Acta Electronica Sinica, 2000, 28(11): 114 – 118. (in Chinese)
[4] F Hess, N P Smart, F Vercauteren. The eta pairing revisited [J]. IEEE Trans, Information Theory, 2006, 52(02): 4595 – 4602.
[5] Granger, F Hess, R Oyono, N Theriault, F Vercauteren. Ate pairing on hyperelliptic curves [A]. Proc EuroCrypt 2007[C]. Berlin Heidelberg: Springer-Verlag, 2007. 430 – 447.
[6] S Matsuda, N Kanayama, F Hess, E Okamoto. Optimised versions of the Ate and twisted Ate pairings [OL]. To appear at Eleventh IMA International Conference on Cryptography and Coding, Cirencester, http://eprint. iacr. org/2007/013. pdf. 2007.
[7] S Galbraith, K Harrison, D Soldera. Implementing the Tate pairing [A]. Algorithm Number Theory Symposium ANTS [C]. Berlin Heidelberg: Springer-Verlag, 2002. 324 – 337.
[8] P S L M Barreto, H Y Kim, B Lynn, M Scott. Efficient algorithms for pairing-based cryptosystems [A]. Cryptology Crypto'2002[C]. Berlin Heidelberg: Springer-Verlag, 2002. 354 – 368.
[9] I M Duursma, H S Lee. Tate pairing implementation for hyperelliptic curves y2 = xp – x + d [A]. Advances in Cryptology-ASIACRYPT 2003[C]. Berlin Heidelberg: Springer-Verlag , 2003. 111 – 123.
[10] C A Zhao, F Zhang, J Huang. A Note on the Ate Pairing [OL]. P reprint, 2007. http://eprint. iacr. org/2007/247. pdf.
[11] T Izu, T Takagi. Efficient computation of the Tate pairing for the Large MOV degree[A]. ICISC2002[C]. Berlin Heidelberg: Springer-Verlag, 2003. 283 – 297.
[12] S Chatterjee, P Sarkar, R Barua. Efficient computation of tate pairing in projective coordinate over ceneral characteristic fields [A]. Information Security and Cryptolgy [C]. ICISC2004, Berlin Heidelberg: Springer-Verlag, 2005, 168 – 181.
[13] P S L M Barreto, S Galbraith, C Eigeartaigh, M Scott. Efficient pairing computation on supersingular abelian varieties [OL]. Codes and Cryptography, Cryptology eprint Atchives, http://eprint. iacr. org, 2004/375. pdf
[14] E Lee, H S Lee, Y Lee. Eta pairing computation on general divisor over hyperelliptic curves [J]. Journal of Symbolic Computation , 2008, 43(6): 452 – 474.
[15] S Galbraith, K Harrison, D Soldera. Implementing the Tatepairing [A]. Algorithmic Number Theory Symposium-ANTS[C]. Berlin Heidelberg: Springer-Verlag, 2002. 324 – 337.
[16] T Kobayashi, K Aoki, H Imai. Efficient algorithms for Tate pairing [J]. IEICE Trans Fundam, 2006, 89(01): 134 – 143.
[17] C A Zhao, F G Zhang, J W Huang. Efficient tate pairing computation using double-base chains [J]. Science in China Series F-Information Science, 2008, 51(08): 1096 – 1105.
[18] A J Menezes, N Koblitz. Pairing-based cryptography at high security levels [A]. Cryptography and Coding [C]. Berlin Heidelberg: Springer-Verlag, 2005. 13 – 36.
[19] R Granger, F Hess, R Oyono, N Theriault, F Vercauteren. Ate Pairing onHyperelliptic Curves [A]. EUROCRYPT 2007[C]. Berlin Heidelberg: Springer-Verlag, 2007. 430 – 447.
[20] S Victor. The Weil pairing and its efficient calculation [J]. Journal of Cryptology, 2004, 17(04): 235 – 261.
[21] V S Dimitrov, L Imbert, P K Mishra. Efficient and secure elliptic curve point multiplication using double-base chains [A]. ASIACRYPT 2005 [C]. Berlin Heidelberg: Springer-Heidelberg, 2005. 59 – 78.
[22] I Blake, K Murty, G Xu. Refinements of Miller's algorithm for computing weil/TaTepairing [J]. Journal of Algorithms, 2006, 58(2): 134 – 149.

作者简介:



陈厚友　男,1979 年生于山东省微山县.硕士研究生,研究方向椭圆曲线密码学.
E-mail: chenhouyou1979@gmail.com

马传贵　男,1962 年生于山东菏泽.教授、博士生导师.研究方向密码学和无线网络安全.
E-mail: chuanguima@sina.com