高效的 R-ate 对的参数构造方法

李彬，王新梅
(西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071)

摘　要：为进一步提高 Tate 对的计算效率，在 R-ate 算法的基础上提出了一种新的(A,B)参数选择方法。与 Ate$i$ 方法相比，该方法将(A,B)参数对选择(p^i, r),使得 Ate$i$ 的方程中域的特征 $p\bmod r$ 代替 $p^m\bmod r$，从而大大降低 Miller 循环的次数。但是在 p 取值不当时，有可能造成系统的可实现性降低，因此最后给出一种 p 的取值规则，以确保本方法应用下的系统成功实施。

关键词：双线性配对；Tate 配对；Miller 算法
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1000-436X(2010)01-0118-04

Efficient method of constructing parameters in R-ate paring

LI Bin, WANG Xin-mei
(State Key Lab. of Integrated Service Networks , Xidian Univ. , Xi'an 710071, China)

Abstract: In order to accelerate the computing of Tate paring, a new technique of selection method of parameters (A,B) based on R-ate technique had been proposed. Compared to Ate$i$, this method substitutes $p^m\bmod r$ with $p\bmod r$ in Miller loop, and p was the character of Tate pairing's field. Could bring an advance of a larger reduction of Miller loop comparing with Ate$i$ algorithm by parameters (p^i, r), but it must constraint that field of definitions of p, So at the end, the classical selection rule of p was shown in response for improving the reliability of the method.

Key words: bilinear pairing; Tate pairing; Miller algorithm

1　引言

双线性配对加密体制的研究始于 Boneh 和 Franklin 的 IBE 方案[1]，由于其带宽和效率的优势而备受瞩目[2]。通过有理化的除子运算，双线性配对将椭圆曲线域中的元素映射到有限扩域中，从而避免了复杂的椭圆曲线运算，计算效率和加密带宽等主要指标均有大幅提高。

近年来，双线性配对体制的快速算法研究较为活跃，出现的技术包括：修改基域、降低汉明重量(Hamming weight)、降低 Miller 循环次数、配对压缩等，其核心共同点都是对正则除子有理化算法(Miller 算法)[3]进行优化。Barreto 首先利用某些特殊类型的超奇异椭圆曲线性质，对 Miller 算法中的 $G_{a,b}$ 计算进行了简化，该方法效率虽高但并不具有普遍性[4]。随后 Duursma 和 Lee 在超椭圆曲线域上，通过特殊选择的参数降低 Miller 循环次数 r 的汉明重量，并通过 Frobenius 操作销去除子的幂[5,6]。该算法对 Miller 循环的次数并未减少，但是由于减小 r 的汉明重量，对于 Miller 算法的整体效率还是具有较大的改进。Eta 算法进一步扩展 Duursma-Lee 算法从超椭圆曲线域至超奇异的椭圆曲线域[6,7]。2006 年，Granger 和 Hess 提出的 Ate 算法，是 Eta 对的一般椭圆曲线域扩展[8]，其最优结果是 Miller

收稿日期：2008-12-26；修回日期：2009-09-25
基金项目：博士后基金资助项目(57145)；国家自然科学基金资助项目(90604009,60773002)
Foundation Items: Postdoctoral Foundation (57145); The National Natural Science Foundation of China(90604009, 60773002)

算法循环次数最小可减至 $\Lambda_{r,k}=\lg(r^{1/\phi(k)})$，($\Phi(k)$是欧拉函数)。随后，Zhao 等人在 Ate 算法的基础上提出了 Ate*i*[9]，给出了另一种 Ate 实现方法，虽然最优结果仍为 $\Lambda_{r,k}$，但效率在某些情况下优于 Ate 算法。最近 Lee 提出了 R-ate 算法($R_{A,B}(P,Q)$)[10]，是 Ate*i* 算法的一种扩展。通过参数(A,B)的选择来选择配对的类型，进而可以得到 Miller 循环的配对。在文献[10]中提到的某些情况下，双线性配对的运算效率较 Ate*i* 对效率更高。

本文提出一种新的 R-ate 对(A,B)参数的选择方式，以域的特征 p 作为基数实现有理除子算法中的 Miller 循环次数。与 Ate 和 Ate*i* 算法中 Miller 循环次数以域元素的个数 $q=p^m$ 作为基数相比，以及相比原有的 R-ate 算法的参数选择方法，该方式构建的双线性配对体制，可以有效的降低 Miller 算法的循环次数，提高 Tate 对的计算效率。

2　R-ate 定义

IBE 方案[11]采用的双线性配对技术是 Weil 对，然而 Koblitz 和 Menezes 证明了绝大多数情况下，Tate 对的效率都优于 Weil 对[12]，因此目前大多数双线性配对的快速算法都是基于 Tate 技术进行优化。下面首先给出 Tate 对和 R-ate 的定义。

定义 1　Tate pairing

F_q 为一个有限域，设 $q=p^m$，p 为大素数。E 为 F_q 上一非奇异椭圆或超椭圆曲线，O 为其无穷远点，整数 r 满足 $r\,|\,\#E(F_q)$ 且 r 是一个大素数。k 为满足 $r\,|\,q^k-1$ 的最小正整数，称为嵌入因子。设 $P\in E[r]$，$Q\in E(F_{q^k})$。对于点 P 和任意正整数 i，Tate 对定义为 $e:E[r]E(F_{q^k})/rE(F_{q^k})\to F_{q^k}^*/(F_{q^k}^*)^r$。

定义 2　Ate*i* pairing

设 C 为 F_q 上一非奇异曲线，$q=p^m$。r 是一个大素数且 $\#J_C(F_q)\,|\,r$。t 为 C 的 Frobenius 迹，根据 Hess 定理有 $\#C(F_q)=q-1+t$。$T=t-1$，设 $\varphi_q:(x,y)\to(x^q,y^q)$ 为 F_q 域上的 Frobenius 自同态，$G_1=J_C[r]\cap ker(\varphi_q-[1])$，$G_2=J_C[r]\cap ker(\varphi_q-[q])$，$P\in G_1$，$Q\in G_2$。则

1) $f_{T^i,r}(Q,P)$ 是一个非退化双线性配对；

2) 设 a 是满足 $T_a^i\equiv 1 \bmod r$ 的最小正整数，$N=\gcd(T_a^i-1,q^k-1)$，$T_a^i-1=LN$，则 $e(Q,P)^L=f_{T^i,Q}(P)^{c(q^k-1)/N}$，其中 $c=\sum_{j=0}^{a-1}T_i^{a-1-j}(q^i)^j$。

定义 3　R-ate pairing

设 C 为 F_q 上一非奇异曲线。r 是一个大素数且 $\#J_C(F_q)\,|\,r$。设 $\varphi_q:(x,y)\to(x^q,y^q)$ 为 F_q 域上的 Frobenius 自同态，$G_1=J_C[r]\cap ker(\varphi_q-[1])$，$G_2=J_C[r]\cap ker(\varphi_q-[q])$，$P\in G_1$，$Q\in G_2$。设 $A,B,a,b\in Z$，$A=aB+b$，R-ate 对的定义为

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

设 $e(Q,P)^{L_1}=f_{A,Q}(P)^{M_1}$，$e(Q,P)^{L_2}=f_{B,Q}(P)^{M_2}$，$M=\mathrm{lcm}(M_1,M_2)$，$L=\dfrac{M}{M_1}L_1-aL_2\dfrac{M}{M_2}$，如果 L 不是 r 的一个因子，则 $R_{A,B}(Q,P)$ 是一个非退化性的双线性配对，$R_{A,B}(Q,P)^M=e(Q,P)^L$。其中 $(A,B)=(q^i,r)$ 时，R-ate 对即为 Ate*i* 对，即 $R_{A,B}(Q,P)=f_{T_i,Q}(P)$。

$$L=iq^{i-1}\frac{q^k-1}{r}-kq^{k-1}a，\quad M=kq^{k-1}\frac{q^k-1}{r}。$$

R-ate 对即为 Ate*i* 对的证明如下:

因为 $a=\dfrac{q^i-b}{r}r$，所以 $G_{aBQ,bQ}(P)=\dfrac{h_{aBQ,bQ}(P)}{h_{aBQ+bQ}(P)}=\dfrac{h_{q^i}(P)}{h_{q^i}(P)}=1$。

所以 $f_{q^i,r}(Q,P)=f_{q^i,Q}(P)f_{b,Q}(P)G_{aBQ,bQ}(P)$ => $R_{A,B}(Q,P)=f_{b,Q}(P)$。

3　(*A, B*)选择的另一种方法

首先修改 G_1 和 G_2 的定义域，$q=p^m$，p 为大素数，设 $T_1=G_1=J_C[r]\cap ker(\varphi_q-[1])$，$T_2=J_C[r]\cap ker(\varphi_p-[p])$。在 Ate 对中，通过修改 Q 的定义域，将取值限定为 $J_C[r]$ 中一个子集，从而可通过特殊技术减小 Miller 循环的次数。与 $G_2=J_C[r]\cap ker(\varphi_q-[q])$ 相比，T_2 是 $J_C[r]$ 中一个更小的子集。虽然在特征数 p 较小的情况下，T_2 的取值不是很理想，但是在 p 较大的域中，T_2 的取值具有较大的灵活性，因此这样的定义域仍然可以提供较高的可实现性。下面给出(A,B)的选择方法。

$(A,B)=(p^i,r)$，则根据定义，有 $p^i=ar+b$。

$f_{p^i,r}(Q,P)=f_{p^i,Q}(P)f_{b,Q}(P)G_{arQ,bQ}(P)$ => $R_{A,B}(Q,P)=f_{b,Q}(P)$。

因为 $b = p^i \bmod r$，所以 $R_{A,B}(Q,P) = f_{p^i \bmod r, Q}(P)$。

$L = ip^i \dfrac{p^i - 1}{r} - kp^{i-1}a$，$M = kp^{i-1}\dfrac{p^i - 1}{r}$，$e(Q,P)^L = R(Q,P)^M$。

证明 F_q 的特征为 p，根据文献[13]的第一章系理 4，$x \to x^q$ 是一个 F_q 中的自同构（$x \in F_q, n > 0$），因此定义 2 个域上的自同态：

$\varphi_q : (x,y) \to (x^q, y^q)$，$x \in T_1$。

$\varphi_p : (x,y) \to (x^p, y^p)$，$x \in T_2$。

因为 T_2 是 T_1 的子集，可得 $\varphi_{p^m} = \varphi_p^m$。同时 $\varphi_p(Q) = [p]Q, Q \in T_2$。

同时，已知 φ_{p^m} 在 F_{p^m} 上为纯不可分，对于 $x \in Ker(\varphi_{p^m})$，总存在 $x^{p \wedge m^e} \in Ker(\varphi_{p^m})$，$e$ 为任意整数。则总存在 m^e，使得 $x^{p \wedge m^e} \in Ker(\varphi_p)$，推论得出 φ_p 在 F_{p^m} 上也为纯不可分。

因此：

$$f_{T,\varphi_p(Q)}(Q) = T(\varphi_p(Q)) - (T\varphi_p(Q)) - (T-1)(O).$$

$$(\varphi_p) * (f_{T,\varphi_p(Q)}(Q)) = p^i(\varphi_p(Q)) - (p^i \varphi_p(Q))$$

$$-(p^i - 1)(O) = (f_{T,Q}^{p^i}).$$

$$(\varphi_p) * (f_{T,\varphi_p(Q)}(Q)) = (f_{T,\varphi_p(Q)}(Q) \circ \varphi_p^i).$$

$f_{T,\varphi_p(Q)}(Q) \circ \varphi_p^i = (f_{T,Q}(Q))^{p^i} \circ \varphi_p^i$，故 $f_{T,\varphi_p(Q)}(P) = (f_{T,Q}(P))^p$ 得证。

在此基础上，应用文献[10]的定理 2 和定理 3 即可得出

$$e(Q,P)^{ip^{i-1}} = f_{p^i \bmod r, Q}(P)^{kp^{k-1}}$$

可以看出，$(A,B) = (p^i, r)$ 的选择，将 Miller 算法的循环次数改为 p^i。与定义 2 相比，这种 R-ate 对形式上与 Ate*i* 算法一致，因此该选择参数之后的 R-ate 对是对 Ate*i* 算法的一种改进。

4 性能分析

本方法的(A,B)选择粒度更细，对于 R-ate 算法的求幂和 Miller 算法的循环次数都不同程度的改进。设 $(A,B) = (p^i \bmod r, p^j \bmod r)$ $(0<i<k)$。则 $p^i \bmod r$ $(0<i<mk)$ 比 $q^j \bmod r$ 的粒度更细，显然 $p^i \bmod r \leqslant q^j \bmod r$。因此 a,b 值均小于原有的规则。同时，根据此定义，R-ate 对实际上被修改为 $e(Q,P)^{ip^{i-1}} = f_{p^i,Q}(P)^{kp^{k-1}}$，与 Ate*i* 算法相比，修改后的 R-ate 对循环次数最小可降至 $\varLambda'_{r,k} = \dfrac{1}{m}\lg(r^{1/\phi(k)})$，其中 $q = p^m$。

然而，在特征为 2、3 之类较小的基域中，$T_2 = J_C[r] \cap ker(\varphi_p - [p])$ 被限定在 F_2、F_3 中。例如 F_3 中，通过构造映射 $\varPhi$：$F_{3^n} \to F_3$，可将 Q 点映射到 F_3 中。$\varPhi$ 的构造相对容易，然而在挠群 $J_C[r]$ 与 $ker(\varphi_3 - [3])$ 的交集可能为空，也就是说未必能找到满足 T_2 的规则的点 Q。因此特征 p 过小的基域上应用此规则，可能会降低系统的可实现性。

5 *p* 值的选取

为保证 $T_2 = J_C[r] \cap ker(\varphi_p - [p])$ 中存在尽可能多的元素，p 应该选取尽可能大的素数。但 p 过大则会导致 Tate 对计算效率的下降。如何平衡系统的可实现性和效率，是一个关键问题。本文给出规则：在保证 F_q 的长度为 160bit 的情况下，k 值选取 5~30，能保证 T_2 集合中存在元素，且系统具备相当的安全性[14]。

例：p=4294903007; q= p^5; E 为 Fq 上 k=6 的椭圆曲线[13]。

q= 1461392258539978793039251637338741330163180531807(160bit)；

r= 13063255688422174813106568961(96bit);

对于 $q^i \bmod r$，Miller 循环的最小次数为 i=5，Ate*i* 算法的 Miller 循环次数为 lb(96A360909C5414AFA768C3B)=94，而应用本规则，$p^j \bmod r$，Miller 循环的最小次数为当 j=12 时，lb(583192B596648424622C37F)=91。

6 结束语

本文在 R-ate 对的基础上提出了一种参数(A,B)的选择方法，与 Ate 和 Ate*i* 算法相比，该方法在特征值 p 较大的基域中能够显著的减小 Miller 算法循环的次数，提高 Tate 对计算的效率。然而在特征值 p 过小的基域中，由于 Q 点的选取存在困难，系统的可实现性有所下降。因此本文最后对 p 值的选取制定提供了一种规则，以避免 p 过小的情况。该方法效率较 Ate*i* 对更高，实际是一种通过定义域的替换以及运算规则的改变形成的新型 R-ate 双线性配对算法。

参考文献：

[1] BONEH D, FRANKLIN M. Identity-based encryption from weil pairing[EB/OL]. http://eprint.iacr.org/, 2008.

[2] ZHOU FC, XU J, XU H F. Research of STR multicast key management protocol based on bilinear pairing in ad hoc network[J]. Journal on Communications ,2008,10: 123-131.

[3] MILLER V. Short Programs for Functions on Curves[C]. Unpublished Manuscript ,1986.

[4] BARRETO P S L M, KIM H Y, LYNN B, *et al*. Effcient algorithms for pairing-based cryptosystems[A]. Advances in Cryptology - CRYPTO 2002[C]. LNCS Springer-Verlag, 2002.354-368.

[5] DUURSMA I, LEE H. Tate pairing implementation for hyperelliptic curves $y2 = xp\ i\ x + d$[A]. Advances in Cryptography - AsiaCrypt 2003[C]. LNCS, pringer-Verlag, 2003. 111-123.

[6] BARRETO P S L M, GALBRAITH S, SCOTT M. Effcient pairing computation on supersingular abelian varieties[J]. Design, Codes and Cryptography, 2007, 42(3): 239-271.

[7] HESS F, SMART N P, VERCAUTEREN F. The Ate pairing revisited[J]. IEEE Trans Information Theory, 2006, 52: 4595-4602.

[8] GRANGER R, HESS F, OYONO R, et al. Ate pairing on hyperelliptic curves[A]. Advances in Cryptology - EuroCrypt 2007[C]. Springer-Verlag LNCS4515, 2007. 430-447.

[9] ZHAO C, ZHANG F, HUANG J. A note on the Ate pairing[EB/OL]. http://eprint.iacr.org/2007/247, 2007.

[10] LEE E, LEE H S, PARK C M. Efficient and generalized paring computation on abelian varieties[EB/OL]. http://eprint.iacr.org/2008/040, 2008.

[11] BARRETO P S L M, GALBRAITH S, SCOTT M. Effcient pairing computation on supersingular abelian varieties[C]. Design, Codes and Cryptography, 2007, 42(3): 239-271.

[12] KOBLITZ N, MENEZES A. Pairing-based cryptography at high security level. [EB/OL]. http://eprint.iacr.org/, 2008.

[13] WAN Z.X. Algebra and Coding[M]. Higher Education Press.1982.

[14] GALBRAITH S D, HARRISON K, SOLDERA D. Implementing the Tate pairing[A]. Algorithmic Number Theory Symposium - ANTS-V[C]. LNCS Springer-Verlag, 2002. 324-337.

作者简介：

李彬（1976-），男，山东诸城人，西安电子科技大学通信工程学院博士后，主要研究方向为编码理论与技术、无线通信等。

王新梅（1937-），男，浙江浦江人，西安电子科技大学通信工程学院教授、博士生导师，主要研究方向为编码理论与技术、通信网中的安全理论与技术。