R-ate 配对的 F_{q^m} 域扩展

李　彬[①]　王新梅[①]　李向军[②]
[①](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　西安　710071)
[②](西安电子科技大学机电工程学院　西安　710071)

摘　要：为解决 R-ate 对实现中的不完全约减问题，提高计算效率，该文提出一种方法 m-R-ate，将 R-ate 对的实现由 F_q 扩展至 F_{q^m} 域中。此外，通过用特征 q 代替 q^m 的方法对 R-ate 的公式进行化简，可大大提高 R-ate 算法效率。实验表明，消除整数不完全约减问题可至少提高 7.8%的效率，粒度更细的(A,B)选择方式可有效的减少 Miller 循环次数，效率高于 Ate_i 算法。

关键词：密码学；双线性配对；Tate 配对；Miller 算法
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2009)11-2713-03

R-ate Extended to F_{q^m}

Li Bin[①]　Wang Xin-mei[①]　Li Xiang-jun[②]
[①](*State Key Lab of Integrated Service Networks*, *Xidian Univ.*, *Xi'an* 710071, *China*)
[②](*College of Electrical-Mechanic Engineering*, *Xidian Univ.*, *Xi'an* 710071, *China*)

Abstract: In order to solve the troubles of incomplete reduction tumbled in the realization of R-ate and efficient compute the R-ate, a new technique named m-R-ate, which extend R-ate from F_q to F_{q^m}, is proposed. Furthermore, in m-R-ate a very efficient algorithm of R-ate is obtained by replacing q^m with the field character q in the formula. That overcoming incomplete reduction will improve the efficiency of R-ate 7.8% at least, and the Miller loop will be reduced by selecting of smaller granularity of (A,B), which is much better than Ate_i.

Key words: Cryptography; Bilinear pairing; Tate pairing; Miller algorithm

1　引言

双线性配对加密算法的研究始于 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，体制上具有天然的优势。近年来，对双线性配对算法效率的改进成为众多学者研究的热点问题。

对于双线性配对计算效率的研究，大部分方法是优化 Miller 提出的正则除子有理化算法[3,4]，即 Miller 算法。Barreto 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普遍性[5]。随后，Hess 提出的 Ate 对算法，是 Eta 对[6]的一般椭圆曲线域扩展[7]，并被 Granger 推广至超椭圆曲线域中[8]，效率具有较大的改进(Miller 算法循环次数最小可减至 $\Lambda_{r,k}=\log_q(r^{1/\phi(k)})$, $\Phi(k)$ 是欧拉函数)。Zhao 等提出了 Ate_i 配对[9]，给出了 Ate 的另一种实现方法，效率在某些情况下优于传统的 Ate。最近，Lee 等提出了 R-ate 对($R_{A,B}(P,Q)$)[10]，可以看作是 Ate_i 的一种扩展形式，当参数 A 和 B 的某些情况下，可以提供更大的灵活性，对 R-ate 对的运算效率有显著提高。

上述算法主要集中在 Tate 对的指数最小化[3]以及 Miller 循环次数的化简问题。我们在研究 R-ate 对的实现时，发现整数约减问题会大大影响 R-ate 对的效率。处理器的字长是以 Word 为单位，通常为 64 bit，当域 F_q 不满足条件($\log_2 q \bmod 64=0$)时，需要在最高位按位-级层次进行运算。解决这一问题有两种途径：一是通过 Yanik 的不完全模等算法[11]进行处理，二是将域 F_q 扩展至 F_{q^m}，使 q^m 接近处理器字长，直接避免此类问题。本文采用第 2 种方法，在 R-ate 对的基础上，提出一种名为 m-R-ate 的扩展配对，通过参数 m 的选择使 q^m 数位尽量接近处理器字长。该方法具有如下优点：

(1)最大程度消除 R-ate 对实现中的整数约减问题带来的影响，提高 R-ate 的效率。

(2)在 R-ate 计算中用域的特征 q 代替 q^m，通过降低(A,B)对的选择和粒度来减小 Miller 循环的次数，提高算法效率。

2008-06-02 收到，2009-06-14 改回
博士后基金(57145)和国家自然科学基金(90604009)资助课题

2 R-ate 对

2.1 R-ate 对的定义

定义 1 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，$G_1=J_C[r]\bigcap\ker(\varphi_q-[1])$，$G_2=J_C[r]\bigcap\ker(\varphi_q-[q])$，$P\in G_1$，$Q\in G_2$。设 $A,B,a,b\in Z$，$A=aB+b$，R-ate 对的定义如下：

$$R_{A,B}(Q,P)=f_{a,BQ}(P)\cdot f_{b,Q}(P)\cdot G_{aBQ,bQ}(P) \tag{1}$$

设 $e(Q,P)^{L_1}=f_{A,Q}(P)^{M_1}$，$e(Q,P)^{L_2}=f_{B,Q}(P)^{M_2}$，$M=lcm(M_1,M_2)$，$L=(M/M_1)L_1-aL_2(M/M_2)$，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。

定理 1 $R_{A,B}(Q,P)^M=e(Q,P)^L$，$e(Q,P)$ 是 Tate 对。

证明略，详见文献[10]第 3.1 章。

2.2 R-ate 对的规则

文献[10]中给出了(A,B)对的几种典型选择，通过这些选择可形成不同的方案。在介绍这些方案之前，先给出几个常量的定义：

$T_i=q^i \bmod r$，$N_i=\gcd(T_i^{h_i}-1,q^k-1)$，且 $L_i=(T_i^{h_i}-1)/N_i$。

$c_i=\sum_{j=0}^{h_i-1}T_i^{h_i-1-j}(q^i)^j \bmod N_i$，$M_i=(q^k-1)\bmod N_i$。

不同的(A,B)选择，可以产生不同效率的配对，文献[10]中给定 4 种特殊的规择，我们只给出其中有代表性的两个。

定理 2 文献[7]中定义的规则定义如下：

(1) $(A,B)=(q^i,r)$，$R_{A,B}(Q,P)=f_{T_i,Q}(P)$。$L=iq^{i-1}\dfrac{q^k-1}{r}-kq^{k-1}a$，$M=kq^{k-1}\dfrac{q^k-1}{r}$。

(2) $(A,B)=(q^i \bmod r,q^j \bmod r)$，$R_{A,B}(Q,P)=f_{a,Q}(P)^{q^j}\cdot f_{b,Q}(P)\cdot G_{aBQ,bQ}(P)$。$L=d_iL_i-ad_jL_j$，$M=lcm(c_iM_i,c_jM_j)=d_ic_iM_i=d_jc_jM_j$。

可以看出，规则(1)即为 Ate_i 对。

3 *m*-R-ate 的构建

在 R-ate 定义的基础上，本文直接给出 *m*-R-ate 的定义。

定义 2 设 C 为 F_{q^m} 上一非奇异曲线。r 是一个大素数且 $\#J_C(F_q)\,|\,r$。$\varphi_{q^m}:(x,y)\to(x^{q^m},y^{q^m})$ 为 F_{q^m} 域上的 Frobenius 自同态，设 $G_1=J_C[r]\bigcap\ker(\varphi_{q^m}-[1])$，$G_2=J_C[r]\bigcap\ker(\varphi_q-[q])$，$P$ 和 Q 为 C 上的阶为 r 的有理除子，$P\in G_1$，$Q\in G_2$。设 $A,B,a,b\in Z$，$A=aB+b$，R-ate 对的定义如下：

$$R_{m,A,B}(Q,P)=f_{a,BQ}(P)\cdot f_{b,Q}(P)\cdot G_{aBQ,bQ}(P) \tag{2}$$

定理 3 如 F_q 上的 $R_{A,B}(Q,P)$ 为非退化性双线性配对，则 F_{q^m} 中的 $R_{m,A,B}(Q,P)$ 仍为非退化性双线性配对，$R_{A,B}(Q,P)^M=e(Q,P)^L$，L 和 M 的定义同定义 4。

证明 将 q^m 表示为 p，则证明过程同 $R_{A,B}(Q,P)$。

定理 4 已知 $f_{T,\varphi_p(Q)}(P)=(f_{T,Q}(P))^p$，其中 $q^m=p$，则 $f_{T,\varphi_{q^m}(Q)}(P)=(f_{T,Q}(P))^q$。

证明 F_{q^m} 的特征为 q，根据文献[12]的第 1 章系理 4，$x\to x^{q^n}$ 是一个 F_{q^m} 中的自同构($x\in F_{q^m}$，$n>0$)，因此对于 $\varphi_{q^m}:(x,y)\to(x^{q^m},y^{q^m})$ 和 $\varphi_q:(x,y)\to(x^q,y^q)$，可得 $\varphi_{q^m}=\varphi_q^m$。同时 $\varphi_q(Q)=[q]Q,Q\in G_2$。

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

因此，$f_{T,\varphi_q(Q)}(Q)=T(\varphi_q(Q))-(T\cdot\varphi_q(Q))-(T-1)(O)$。$(\varphi_q)*(f_{T,\varphi_q(Q)}(Q))=q^i(\varphi_q(Q))-(q^i\cdot\varphi_q(Q))-(q^i-1)(O)=(f_{T,Q}^{q^i})$。$(\varphi_q)*(f_{T,\varphi_q(Q)}(Q))=(f_{T,\varphi_q(Q)}(Q)\circ\varphi_q^i)$。$f_{T,\varphi_q(Q)}(Q)\circ\varphi_q^i=(f_{T,Q}(Q))^{q^i}\circ\varphi_q^i$，故 $f_{T,\varphi_q(Q)}(P)=(f_{T,Q}(P))^q$。 证毕

对于 R-ate 提供的 2 种规则，在 F_{q^m} 上转化为如下形式(T_i，N_i，c_i，M_i 也分别改为 F_{q^m} 之上的定义)：

(1) $(A,B)=(p^i,r)$，$R_{m,A,B}(Q,P)=f_{T_i,Q}(P)$。这里 $T_i=p^i \bmod r$，$0<i<k$，k 是 F_{q^m} 的嵌入因子。$L=ip^i\dfrac{p^i-1}{r}-kp^{i-1}a$，$M=kp^{i-1}\dfrac{p^i-1}{r}$。这也就是在 F_{q^m} 中的 Ate_i 对。

(2) $(A,B)=(p^i \bmod r,p^j \bmod r)$，$R_{m,A,B}(Q,P)=f_{a,Q}(P)^{p^j}\cdot f_{b,Q}(P)\cdot G_{aBQ,bQ}(P)$。$L=d_iL_i-ad_jL_j$，$M=lcm(c_iM_i,c_jM_j)=d_ic_iM_i=d_jc_jM_j$。

应用定理 3,可对第(2)种规则进行改进，我们将其定为规则(3)。

(3) $(A,B)=(q^i \bmod r,q^j \bmod r)$，$R_{m,A,B}(Q,P)=f_{a,Q}(P)^{q^j}\cdot f_{b,Q}(P)\cdot G_{aBQ,bQ}(P)$。$L=d_iL_i-ad_jL_j$，$M=lcm(c_iM_i,c_jM_j)=d_ic_iM_i=d_jc_jM_j$。

证明 $T_i=q^i \bmod r$，$T_j=q^j \bmod r$，则根据定义，有 $T_i=aT_j+b$。$f_{T_i,Q}(P)=f_{T_j,Q}^a(P)\cdot f_{a,T_jQ}(P)\cdot f_{b,Q}(P)\cdot G_{aT_jQ,bQ}(P)$。

根据定理 4，有 $f_{a,T_jQ}(P)=f_{a,Q}(P)^{q^j}$，故 $R_{m,A,B}(Q,P)=f_{a,Q}(P)^{q^j}\cdot f_{b,Q}(P)\cdot G_{aBQ,bQ}(P)$，即规则(3)成立。 证毕

4 性能分析

据统计，在 $F_{2^{160}}$ 域中，处理器字长为 16 的运算

平台上，相比常规二进制方法，不完全约减算法能够提高 7.8%的运算效率[11]，m-R-ate 方法从根本上避免整数约减问题，显然对 R-ate 算法的效率提升应大于 7.8%。

同时，m-R-ate 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。下面详细分析此改进的效果。式(1)的 R-ate 的算法如下：

Input : $P,Q\in C,a,b,j\in Z,m_1=\max\{a,b\},\quad m_2=\min\{a,b\}$

Output : $R(Q,P)=R_{m,A,B}(Q,P)=f_{a,Q}(P)^{p^j}\cdot f_{b,Q}(P)\cdot G_{aBQ,bQ}(P)$

(1) compute $f_a,\ f_b,aQ,$ where $\{a,b\}=\{m_1,m_2\}$;

(2) $c\leftarrow[m_1/m_2],d\leftarrow m_1-c\cdot m_2$;

(3) $f_{m_w,m_2Q}\leftarrow M(Q,P,m_2)$; $f_{c,m_2,c\cdot m_2Q}\leftarrow M(m_2Q,P,c)$; $f_{d,dQ}\leftarrow M(Q,P,d)$;

(4) $f_1\leftarrow f_{m_2}^c\cdot f_{c,m_2}\cdot f_d$; $f_{m_1}\leftarrow f_1\cdot G_{cm_2Q,dQ}(P)$;

(5) $m_1Q\leftarrow c\cdot m_2Q+dQ$;

(6) $f_2\leftarrow f_a^{p^j}\cdot f_b$;

(7) $Q_1\leftarrow\phi^j(aQ)$;

(8) $f_3\leftarrow f_2\cdot G_{Q_1,bQ}(P)$;

(9) return f_3。

设 $(A,B)=(q^i \bmod r,q^j \bmod r)$，$0<i<m^i$。则 $q^i \bmod r$ $(0<i<mk)$比 $p^j \bmod r$ 的粒度更细，显然 $q^i \bmod r\leqslant p^j \bmod r$。因此规则(3)中的 a,b 值均小于规则(2)，对于算法 4-1 的第 3 步中，m_2，c，d 的值都有所减小。算法 1 中的第(6)步。$f_2\leftarrow f_a^{p^j}\cdot f_b$ 优化为 $f_2\leftarrow f_a^{q^j}\cdot f_b$，计算量最少可减至原有的 $1/m$ 次幂。

例　在计算平台处理字长为16的情况下：

p=4294903007；$q=p^5$；E为 F_q 上k=6的椭圆曲线。

q=146139225853997879303925163733874133016318053180 7(160 bit)；

r=13063255688422174813106568961(96 bit)。

对于 $q^i \bmod r$，Miller 循环的最小次数为 i=5，$\log_2(96A360909C5414AFA768C3B)=92$，而 $p^i \bmod r$，Miller 循环的最小次数为 i=12，$\log_2(583192B596648424622C37F)=91$，次数有所减少。在某些例子中，Miller 循环次数减少更为显著，由于篇幅原因，本文不再赘述，详情请参见文献[9]附录。

5　结束语

m-R-ate 方法将 F_q 上 R-ate 对扩展到 F_{q^m} 域中，可以有效减少进位运算带来的不必要运算量损耗，增加算法的效率。同时证明了对于 R-ate 的规则(3)，采用 F_{q^m} 的特征 q 替换 q^m 进行 R-ate 的运算的可行性，替换能大大增加 R-ate 的效率，具有很强的实用性。定理 3 中对于 Ate_i 等体制的改进效果较为明显，笔者将在今后的工作中进一步研究。

参 考 文 献

[1] Boneh D and Franklin M. Identity-based encryption from Weil pairing[C]. Advances in Cryptology-CRYPTO 1998, http://eprint.iacr.org/.

[2] Brezing F and Weng A. Elliptic curves suitable for pairing based cryptography[J]. Designs, Codes and Cryptography, http://eprint.iacr.org/2003/143/.

[3] Galbraith S D, Harrison K, and Soldera D. Implementing the Tate pairing[C]. Algorithmic Number Theory Symposium - ANTS-V, 2002, LNCS, Vol. 2369: 324–337.

[4] Miller V. Short programs for functions on curves, Unpublished Manuscript, 1986. http://crypto.stanford.edu /miller/miller.pdf.

[5] Barreto P S L M, Kim H Y, Lynn B, and Scott M. Effcient algorithms for pairing-based cryptosystems[C]. Advances in Cryptology-CRYPTO 2002, 2002, LNCS, Vol 2442: 354–368.

[6] Barreto P S L M, Galbraith S, and 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, and Vercauteren F. The Eta pairing revisited[J]. *IEEE Transactions on Information Theory*, 2006, 52(2): 4595–4602.

[8] Granger R, Hess F, Oyono R, Theriault N, and Vercauteren F. Ate pairing on hyperelliptic curves[C]. Advances in Cryptology-EuroCrypt 2007, 2007, LNCS4515: 430–447.

[9] Zhao C, Zhang F, and Huang J. A note on the ate pairing[C]. Preprint.2007. Available at http://eprint.iacr.org/2007/247.

[10] Lee E, Lee H-S, and Park C M. Efficient and generalized paring computation on abelian varieties[C]. Preprint, 2008. Available at http://eprint.iacr.org/2008/040.

[11] Yanik T, Savas E, and Koc C K. Incomplete reduction in modular arithmetic[J]. *IEEE Proc Comput. Digit. Tech*, 2002, 149(2): 46–52.

[12] 万哲先.《代数与编码. 高等教育出版社, 1982: 46–71.

李　彬：　男，1976 年生，博士后，研究方向为网络安全、电子交易研究.

王新梅：　男，1937 年生，教授，博士生导师，主要研究领域为通信、纠错码、密码等.

李向军：　女，1967 年生，副教授，博士生，研究方向为信息系统安全、软件理论等.