ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.11, November 2009, pp.3001−3009
doi: 10.3724/SP.J.1001.2009.03651

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

双线性对有效计算研究进展*

赵昌安[1,2], 张方国[1,3+]

[1](中山大学 信息科学与技术学院,广东 广州 510275)

[2](广州大学 计算机科学与教育软件学院,广东 广州 510006)

[3](中山大学 广东省信息安全技术重点实验室,广东 广州 510275)

Research and Development on Efficient Pairing Computations

ZHAO Chang-An[1,2], ZHANG Fang-Guo[1,3+]

[1](School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510275, China)

[2](School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China)

[3](Guangdong Key Laboratory of Information Security Technology, Sun Yat-Sen University, Guangzhou 510275, China)

+ Corresponding author: E-mail: isszhfg@mail.sysu.edu.cn

Zhao CA, Zhang FG. Research and development on efficient pairing computations. *Journal of Software*, 2009, 20(11):3001−3009. http://www.jos.org.cn/1000-9825/3651.htm

Abstract: Pairings have found many cryptographic applications in recent years. The efficiency of implementing these cryptographic applications is determined by the speed of pairing computations. This paper categorizes and reviews the current progress on efficient pairing computations, and suggests the possibility of further research.

Key words: public key cryptography; pairing-based cryptosystem; elliptic curve; pairing computation; efficient algorithm

摘 要: 近年来,双线性对获得了广泛的密码应用.实现这些应用的效率,取决于双线性对的计算速度.分类回顾了双线性对有效计算方面的已有进展,并提出了进一步工作的可能性.

关键词: 公钥密码学;基于双线性对的密码系统;椭圆曲线;双线性对计算;有效算法

中图法分类号: TP309 **文献标识码**: A

双线性对是如下形式的映射:

$$e:G_1\times G_2\to G_T,$$

其中,G_1和G_2是加法群,G_T是乘法群.为了密码协议中的安全需要,一般要求G_1,G_2和G_T中的离散对数问题是难以求解的.双线性对有如下基本特性:

双线性:对任意的$P\in G_1$,$Q\in G_2$和$n\in Z$,有$e(nP,Q)=e(P,nQ)=e(P,Q)^n$.

非退化性:一定存在某个$P\in G_1$和$Q\in G_2$满足$e(P,Q)\neq 1\in G_T$.

* Supported by the National Natural Science Foundation of China under Grant Nos.60773202, 60633030 (国家自然科学基金); the National Basic Research Program of China under Grant No.2006CB303104 (国家重点基础研究发展计划(973)); the Guangdong Provincial Scientific Research Starting Foundation for Doctors of China under Grant No.9451009101003191 (广东省博士科研启动基金)

Received 2007-12-08; Accepted 2009-05-05

可计算性:存在有效的多项式时间算法计算双线性对的值.

双线性对在公钥密码学中早期应用于攻击椭圆曲线上的离散对数问题,即著名的MOV约化(利用双线性Weil对)[1]与FR约化(利用双线性Tate对)[2].其攻击的主要思想是利用双线性对将椭圆曲线群中的离散对数问题归约为相应的有限域乘法子群中的离散对数问题.

双线性对有其独特的性质,即存在两个输入变量,而双线性使得变量前面的系数可以灵活转化.因此,双线性对在密码学中可用来构造很多其他数学工具所不能构造的协议或方案[3].因为诸多密码协议都借助于双线性对这一数学工具,实现这些协议的瓶颈在于能否快速计算双线性对.目前,计算双线性对有两种多项式时间内的算法:一种可有效计算双线性对的算法为Miller算法[4];Stange在 2007 年利用椭圆网(elliptic nets)的性质给出了计算Tate对的另一种多项式时间算法[5].大多数情况下,计算Tate对要比Weil对有效得多,所以大多数改进算法集中于Tate对的计算优化.Tate对的变种,比如Eta对[6]和Ate对[7],因其性能优越已成为IEEE P1363.3 中计算双线性对的候选标准之一.自双线性对得到广泛应用后,如何快速计算双线性对已成为椭圆曲线密码学中的热点基础理论问题.众多学者提出了基于Miller算法的改进技巧,本文对这些有效改进给出简要概括与总结.

本文第 1 节阐述双线性对的相关背景知识.第 2 节简要分析优化 Miller 算法的可能性,并分类讨论目前所提出的各种有效技巧.第 3 节讨论在双线性对计算方面可进一步研究的问题.

1 Tate 对与 Miller 算法

本节首先描述了有限域上椭圆曲线的一些基本知识,包括传统 Tate 对和约化 Tate 对的定义,然后回顾 Miller 算法.

1.1 背景知识

假设F_q为含有q个元素的有限域,其中,q等于素数p的某个幂次.定义E为有限域F_q上的椭圆曲线,O为无穷远点.有理点群$E(F_q)$的阶为$\#E(F_q)$,并有某个大素数r整除$\#E(F_q)$.假设k为满足条件r整除q^k-1 的最小正整数,k称为椭圆曲线$E(F_q)$的嵌入次数.定义$E[r]$为椭圆曲线E的r阶扰子群,即 $E[r]=\{P\in E(\bar{F}_q)\,|\,[r]P=O\}$.嵌入次数的约束使得 $E[r]\subset E(F_{q^k})$.除子[8]D为椭圆曲线E上有理点的有限线性组合.假设 $D=\sum_{P\in E}nP$, 其中,n为整数且$\sum n$ 等于 0.函数f在除子D的赋值定义为$f(D)=\Pi_P f(P)^n$.

假设$P\in E[r]$和 $Q\in E(F_{q^k})$, $f_{r,P}$是椭圆曲线E上的有理函数,其对应除子满足$(f_{r,P})=r(P)-r(O)$.除子D_Q等价于$(Q)-(O)$,且除子$(f_{r,P})$和D_Q的支集不相交.比如,可任取一点 $Q_2\in E(F_{q^k})$,令$D_Q=(Q+Q_2)-(Q_2)$即可满足条件.传统的 Tate 对是如下定义的映射:

$$e: E[r]\times E(F_{q^k})/rE(F_{q^k})\to F_{q^k}^*/(F_{q^k}^*)^r,$$

$$e(P,Q)\equiv f_{r,P}(D_Q)=f(Q+Q_2)/f(Q_2).$$

在密码应用中,往往需要得到双线性对映射后唯一确定的值.约化的 Tate 对定义如下:

$$e_r: E[r]\times E(F_{q^k})/rE(F_{q^k})\to \mu_r,$$

$$e_r(P,Q)\equiv f_{r,P}(D_Q)^{(q^k-1)/r},$$

其中,μ_r为 F_{q^k} 中的r次单位根群,即 $\mu_r=\{u\in F_{q^k}\,|\,u^r=1\}$.目前,很多基于双线性对密码协议的安全性依赖于$E[r]$,$E(F_{q^k})/rE(F_{q^k})$ 和μ_r这 3 个群的某些子群中离散对数问题的难解性.对应于AES 80 比特标准的安全性,r要求 160 比特大小,q^k的大小为要求 1 024 比特左右,更详细的安全性参数标准可参见文献[9].

1.2 Miller算法

对任意的点P和点Q,用$l_{P,Q}$表示经过点P和Q的直线.如果P等于Q,则$l_{P,Q}$表示过点P(或Q)与椭圆曲线E相切的直线;当P不是无穷远点时,用v_P表示经过点P的垂线.假设$D_Q=(Q+Q_2)-(Q_2)=(Q_1)-(Q_2)$,其中,$Q_1=Q+Q_2$.假设点$P\in E[r]$,$f_{i,P}$为有理函数,且其除子满足:

$$(f_{j,P}) = j(P) - (jP) - (j-1)(O), j \in Z .$$

对任意的 $i,j \in Z$,有

$$f_{i+j,P}(D_Q) = \frac{f_{i,P}(Q_1) f_{j,P}(Q_1)}{f_{i,P}(Q_2) f_{j,P}(Q_2)} \frac{l_{iP,jP}(Q_1) v_{(i+j)P}(Q_2)}{v_{(i+j)P}(Q_1) l_{iP,jP}(Q_2)}.$$

利用如上公式,约化的双线性对 $f_{r,P}(D_Q)^{(q^k-1)/r}$ 可用 Miller 算法计算.相关算法如下所示:

Miller算法.

输入:素数 $r = \sum_{i=0}^{n} l_i 2^i$,其中,$l_i \in \{0,1\}$,$P \in E[r]$和 $Q, Q_2 \in E(F_{q^k})$ 且$Q_2 \neq O$.并记$Q_1 = Q_2 + Q$.

输出:双线性对$e_r(P,Q)$.

1. $T \leftarrow P$, $f \leftarrow 1$
2. for $i=n-1,n-2,\ldots,1,0$ do
   2.1. $f \leftarrow f^2 \cdot \frac{l_{T,T}(Q_1) v_{2T}(Q_2)}{l_{T,T}(Q_2) v_{2T}(Q_1)}, T \leftarrow 2T$
   2.2. if $l_i=1$ then
   2.3. $f \leftarrow f \cdot \frac{l_{T,P}(Q_1) v_{T+P}(Q_2)}{l_{T,P}(Q_2) v_{T+P}(Q_1)}, T \leftarrow T + P$
3. return $f^{(q^k-1)/r}$

2 双线性对的有效计算

2.1 Miller算法的效率影响因素

一般说来,实现 Miller 算法时,可从以下角度提高计算效率:

(1) 基域F_q和扩域 F_{q^k} 中的基本算术.显然,任何加速底层有限域基本算术的方法都能加快双线性对的计算.在保障安全度的条件下,尽可能选择小的基域,并选择有利于扩域中乘法和求逆运算的不可约多项式来构造扩域.

(2) 素数 r 的进制表示.其表示尽量利于椭圆曲线群中的多倍点运算和 Miller 算法中有理函数赋值的多倍运算.比如,计算在特征为 2 或 3 的有限域上超奇异椭圆曲线中的双线性对时,将 r 用二进制或三进制表示.另外,要使 r 的 Hamming 重量尽量小.显然,数的 NAF 表示可减少点加运算和函数赋值的加法运算.

(3) 椭圆曲线群中的点加和多倍点运算.在整个双线性对的计算过程中,都需要多倍点运算.因此,有效的多倍点公式可加速双线性对计算.

(4) 尽量减少扩域中的运算.从Miller算法中可以看到,每一次循环都需要计算分母并求逆.如果分母的值在扩域中且其求逆相当复杂,则可以考虑用两个中间变量f_1和f_2来替代一个中间变量f,到最后求逆一次即可.

(5) Miller 算法中的循环次数.显然,循环次数越少,计算速度越快.

(6) 最后的幂运算.最直接的一个加速思想就是利用有限域中 Frobenius 映射加快最后的幂运算.

(7) 椭圆曲线的坐标系统选取.一般来说,当基域中的求逆与乘法运算耗时比例大于 16 时,射影坐标系统优于仿射坐标系统.对特殊的椭圆曲线,可构造特殊的射影坐标来加速双线性对计算.

现有的改进算法大多从以上一个或者多个角度对 Miller 算法进行优化,下面这一节将简要分析目前已有算法的改进思想.

2.2 Miller算法的改进概述

双线性对可用椭圆曲线群或者超椭圆曲线上的除子类群来构造,而且其具体计算都已经被有效实现,可参见Scott等人开发的Miracl软件包的IBE部分[10],或者Ben Lynn开发的PBC软件包[11].下面将从不同理论角度来综

述目前已发现的Miller算法改进技巧.

2.2.1 加快有限域中的基本运算

胡磊等人研究了一类超奇异椭圆曲线(曲线的嵌入次数为 3)中的双线性对计算[12],给出了明晰的扩域构造并提出了快速计算扩域乘法和求逆的公式,且大大优化了Tate对的最后幂运算.文献[13]将直线赋值方程展开,这样,更新中间变量f时,分子分母中直线系数相同的部分可重用,因而节省了计算开销.Kobayashi等人利用有限域中共轭元技巧将直线赋值时所需要的求逆转化为扩域中的乘法运算[14].

有的密码协议可能需要计算多个双线性对相乘的值.Granger等人[15]和Scott[16]分别独立讨论了双线性对乘积的计算.其优化思想为:计算过程中可以共用中间变量f和最后的幂运算;在仿射坐标系统下,计算点加或倍点时的多个求逆可用Montgomery技巧减少为 1 个.

Koblitz和Menezes提出了适于双线性对计算的扩域(pairing-friendly fields)的概念[9].由于计算Tate对涉及到最后幂运算,因此有限域中的幂运算技巧也可提高Tate对的计算效率.Koblitz等人在文献[9]中认为,在高安全度(即安全度至少大于AES 128 比特)时,计算Weil对将比计算Tate对有效.这是根据Weil对的定义,计算Weil对无需最后的幂运算,但需要计算两次不同的Miller链循环所得出的结论.可是,他们高估了Tate对的最后幂运算开销.Granger等人优化了Tate对中的最后幂运算[17],并论证了在任何安全度下计算Tate对都将比Weil对有效.利用双线性对的赋值都为代数环面中的元素这一事实,Granger等人进一步给出了加速最后幂运算的新方 法[18].值得一提的是,胡磊同样利用代数环面这一工具对一类超奇异曲线上的双线性对给出了有效的压缩 方法[19].

在一些特殊的曲线上计算双线性对时,可以完全不需要最后的幂运算.Galbraith等人论述了在特征 2 和特征 3 的超奇异曲线上的Eta对不需要最后幂运算的情形[20],而超椭圆曲线上的Ate对[21]在计算时也不需要最后的幂运算.

2.2.2 利用椭圆曲线群中点的标量乘快速运算技巧

任何关于椭圆曲线群中点的标量乘快速运算的方法都有可能诱导一个双线性对快速运算的方法.Galbraith等人利用了无须求逆的 3 倍点公式加速了特征为 3 的有限域上超奇异椭圆曲线中的双线性对计算[22].Montgomery等人提出了直接计算[2]$P+Q$的技巧[23],并将其推广到Miller算法中有理函数赋值的 2 倍与加法的情形,此技巧在椭圆曲线子群的阶r不是低Hamming重量时较为有效.椭圆曲线子群的阶r如果用双重基链表示则可加速椭圆曲线群中点的标量乘运算[24],文献[25]也是正利用双重基链的表示加速了Tate对的计算.Scott受椭圆曲线的自同态可加速标量乘的启发[26],改进了两类非超奇异椭圆曲线双线性对的计算[27].

Duursma等人研究了有限域 F_{p^m} 上的一类超椭圆曲线$y^2=x^p-x+d$(其中,$d=\pm 1$)的Tate对计算[28],将此曲线上除子类群的阶r用其倍数$p^{mp}+1$ 来代替,并在Miller链中按p进制展开,因而p倍除子公式在此可得到充分利用,且整个计算过程不再需要Miller算法中除子的加法运算和有理函数赋值的加法运算.将r用其他值代替仍有可能构成双线性对这一思想,正激发了后来Eta对和Ate对的出现.

2.2.3 减少 Miller 链中的无关运算

在众多Miller算法的改进中,Barreto等人给出了一个非常优美的改进[29],证明了在最后幂运算下,函数f在除子D_Q(其中,Q不是无穷远点)的赋值等于f在有理点Q的赋值,即

$$e_r(P,Q)=f_{r,P}(D_Q)^{(q^k-1)/r}=f_{r,P}(Q)^{(q^k-1)/r}.$$

这使得计算$e_r(P,Q)$时,赋值f的迭代更新公式可替换为

$$f_{(i+j),P}(Q)=f_{i,P}(Q)f_{j,P}(Q)l_{iP,jP}(Q)/v_{(i+j)P}(Q).$$

这一替换显著提高了计算速度.另外,为了避免计算$v_{(i+j)P}(Q)=x_Q-x_{(i+j)P}$的逆(其中,$x_{(i+j)P}$和$x_Q$分别为点$(i+j)P$和$Q$的$x$坐标),根据 F_{q^k} 的任意真子域中的非零元素在最后幂运算下都等于 1,可构造$x_{(i+j)P}$和x_Q都在真子域中,则可以舍去 $1/v_{(i+j)P}(Q)$这一部分的运算.在$E(F_q)[r]$中取P和Q,并通过变形映射ϕ [30]使得$\phi(Q)$的x坐标在 F_{q^k} 的真子域中,而y坐标在扩域 F_{q^k} 中.定义新的双线性对$e_d(P,Q)=e_r(P,\phi(Q))$.于是,计算新定义双线性对$e_d(P,Q)$的迭代公式就变为

$$f_{(i+j),P}(Q)=f_{i,P}(Q)f_{j,P}(Q)l_{iP,jP}(Q).$$

此时,计算新定义的双线性对已不涉及扩域中的求逆运算.

由于变形映射仅存在于超奇异椭圆曲线和嵌入次数为 1 的非超奇异曲线中,因此,上面的消除分母技巧不适用于嵌入次数大于 1 的非超奇异椭圆曲线情形.Barreto等人研究了嵌入次数k为偶数的非超奇异椭圆曲线情形,发现可利用曲线上的同构映射ψ使得$\psi(Q)$的x坐标在子域中,而y坐标在扩域中,其中,Q为E的扭曲线E'上的点.这使得在非超奇异曲线上同样可用分母消除技巧[31].

2.2.4 减少 Miller 算法中的循环次数

用Miller算法计算$f_{r,P}(Q)$的循环次数与r的比特长度有关.如果将r用较小的整数T代替并仍保持有理函数的双线性,就可以用$f_{T,P}(Q)$定义新的双线性对.Eta对和Ate对正是基于这一思想而产生的.因为Eta对可看作Ate对在超奇异曲线上的对应情形,所以在此仅讨论Ate对以及Ate对的一些改进.

在密码应用中,椭圆曲线子群的阶r一般为某个大素数,假设P和Q属于$E[r]$.令T为小于r的非零正整数,显然,T和r互素,即$(T,r)=1$,则存在某个最小的正整数a使得T^a模r等于 1.那么有整数L使得$T^a-1=Lr$.因为双线性对$e_r(P,Q)$的某个固定幂次仍然保持双线性,故可定义新的双线性对:

$$e_r(P,Q)^L=(f_{r,P}(Q)^{(q^k-1)/r})^L=f_{Lr,P}(Q)^{(q^k-1)/r}.$$

利用除子的性质和 $P\in E[r]$这一事实,可导出

$$f_{Lr,P}=f_{T^a-1,P}=f_{T^a,P}f_{-1,P}l_{P,-P}=f_{T^a,P}.$$

而又由文献[6]的引理 2,可得:

$$f_{T^a,P}=f_{T,P}^{T^{a-1}}f_{T,TP}^{T^{a-2}}\cdots f_{T,T^{a-1}P}.$$

至此,如果能够得到 $f_{T,T^iP}(Q)$ (其中,$1\le i\le a-1$)和$f_{T,P}(Q)$的某些转化关系,就有可能构造新的双线性对.

一种乐观的思路是选择合适的T和P,使得 f_{T,T^iP} 恰好是$f_{T,P}$的某个固定幂次.假设曲线$E(F_q)$的Frobenius迹为t.Hess等人正是选择 $T=t-1,P\in E[r]\cap Ker(\pi_q-[q])$ 和$Q\in E(F_q)[r]$(其中,π_q为曲线E的Frobenius映射),利用π_q为纯不可分映射这一事实证明了 $f_{T,T^iP}(Q)=(f_{T,P}(Q))^{q^i}$. 可定义约化的Ate对为

$$\tilde{e}(P,Q)=f_{T,P}(Q)^{(q^k-1)/r}.$$

由上定义可知,计算 Ate 对的循环次数由 $T=t-1$ 的比特长度所决定.由 Hasse 定理,t 的大小为 $\sqrt{q}$.当满足条件 $T=t-1<r$ 时,计算 Ate 对总是比计算 Tate 对有效.

Matsuda等人令$T=(t-1) \bmod r$,提出了优化的Ate对[32].此时,T显然总小于r,这说明了计算优化的Ate对总是比计算Tate对效率要高.Zhao等人[33]选取 $T_i\equiv(t-1)^i \bmod r$, 其中,$1\le i\le k-1$.利用 π_q^i 都是纯不可分映射证明 $f_{T_i,P}(Q)^{(q^k-1)/r}$ 都是双线性对,这种双线性对称为广义的双线性Ate对或Ate$_i$对[33].随着i的变化,T_i的取值有可能比$T=(t-1) \bmod r$的值要小.Lee等人利用双线性Tate对和某一Ate$_i$对的比值组合构造了R-ate对[34],这种双线性对的迭代循环次数可达到界$\log r^{1/\varphi(k)}$.文献[35]从抽象角度论述了所有双线性对的集合可构成一个群[35],这一事实不仅简单地重新解释了R-ate对,而且还可说明多个不同Ate$_i$对的组合仍然为双线性对,并且这些双线性对的迭代循环次数也可能达到界$\log r^{1/\varphi(k)}$.Vercauteren利用格归约算法构造了最优Ate对[36],并猜想双线性对的迭代循环次数最低下界为$\log r/\#\varepsilon$,其中,ε表示线性独立且可计算的自同态最大集合.Hess利用格论对目前所有已发现的双线性对函数给出了框架性结构[37],并证明Vercauteren的猜想是成立的.

另一种想法是利用椭圆曲线自同态环中的某些特殊元素来构建$f_{T,TP}$和$f_{T,P}$的关系.在椭圆曲线的自同态环中,除了Frobenius映射以外,另一个可以利用的元素为非平凡自同构.我们利用某些特殊曲线上的非平凡自同构ϕ,对满足特定条件的正整数T和点P,得到了等式$f_{T,TP}=f_{T,P}\cdot\phi$.利用这一观察,可得到与文献[27]一样的双线性对.因为Ate对及其变种在嵌入次数较小时并不奏效,比如当嵌入次数$k=2$ 时,界$\log r^{1/\varphi(k)}$等于$\log r$,所以利用非平凡自同构构造的双线性对在嵌入次数较小的条件下($k=2$)效率优于Ate对.

Galbraith等人综述了超椭圆曲线上的双线性对计算,并将椭圆曲线上的双线性对与超椭圆曲线上的双线

性对进行效率比较,认为超椭圆曲线在双线性对应用中不会有太大的优势[38].也有不少研究者改进了超椭圆曲线上阿贝尔簇的双线性对计算效率,文献[21]将Ate对推广到超椭圆曲线阿贝尔簇上,Fan等人在一类特殊超椭圆曲线上利用自同构将Miller链缩为原来的 1/4.利用某些超椭圆曲线具有两个无穷远点的特性,文献[39]提出了实模型下超椭圆曲线的双线性对计算技巧.

为了节省带宽,点压缩技术已成为椭圆曲线密码系统中的经典方法.而不少基于双线性对的密码协议也需要点压缩技术,比如BLS短签名[40].Scott和Barreto首先提出了压缩双线性对的概念[41],并压缩了特征为 3 有限域上超奇异椭圆曲线的双线性对.胡磊利用双线性对的值属于代数环面的事实,给出了一种有效的双线性对压缩技巧[19].Galbraith和Lin给出了基于x坐标计算双线性对的算法,在嵌入次数为 2 时特别有效[42].

3 总结和展望

自从双线性对在公钥密码学中得到广泛应用以来,双线性对的有效计算也引起了学者们的足够重视,正如上一节所分析的,取得了很多突破性的进展.但是,这一领域仍有许多问题亟待解决.

从双线性对的快速计算角度来看,有如下问题值得关注:

- 椭圆曲线或超椭圆曲线上的双线性对计算的本质在于已知有理函数的除子等价形式,如何计算该有理函数在相关点的赋值.Miller 算法成功地运用倍点-加和切-割线组合来完成这一计算过程.是否可以构造其他方法,从已知的除子等价形式导出对应的有理函数,进而求出有理函数在相关点的赋值?
- 虽然当下双线性对的计算效率已满足目前安全度(AES 80 比特)的需要,但是当安全度提高时,双线性对的计算速度与其他公钥密码体制中的基本运算,比如RSA中的模乘运算和有限域中的幂运算相比,在效率上仍然有差距.Koblitz等人详细讨论了在高安全度时双线性对计算所引发的一些问题[19].因此,如何提高高安全度下的双线性对计算效率仍需要进一步研究.
- 由于双线性 Tate 对的计算效率优于双线性 Weil 对,所以目前诸多改进结果都基于双线性 Tate 对,而双线性 Weil 对的有效优化较少.与双线性 Tate 对相比,Weil 对无需最后幂运算.我们猜测,在某些特殊曲线上可构造 Weil 对的变种,在效率上优于 Tate 对的变种.比如嵌入次数为 2 时,最后幂运算在整个 Tate 对计算过程中占较大比重,而且计算 Weil 对的变种时标量乘运算都在基域中完成,如果循环次数可以缩短,就有可能构造效率更优的 Weil 对变种.
- Stange 于 2007 年利用椭圆网(椭圆除序列)的性质给出了一种计算双线性 Tate 对的多项式时间算法,该算法也适用于双线性 Weil 对的计算.但与 Miller 算法相比,该算法的效率仍然较低.而且 Miller 算法的适用范围要比 Stange 算法广泛,这是因为 Miller 算法的本质是解决了一类已知除子等价形式的有理函数计算相关点赋值的问题.但是Stange算法的优势在于计算过程中无须任何求逆,因此该算法值得进一步优化.
- 特征为 2 或 3 的有限域在硬件实现上有特别优势,目前仅有嵌入次数分别为 4 或 6 的超奇异椭圆曲线可用于双线性对计算,具有一定的曲线选择局限性.可寻找在这些小特征有限域上适于双线性对计算的非超奇异椭圆曲线或者超椭圆曲线.
- 考虑某些与应用密切相关的双线性对计算,比如在ZSS短签名[43]中需要计算反身双线性对$e(P,P)$,是否可充分利用P和Q相同的优势来加快双线性对的计算?另外,一些密码应用中要求r为合数,那么合数阶的双线性对是否存在特别的加速方法?
- 与椭圆曲线相比,超椭圆曲线具有更丰富的自同态环结构,能否利用其自同态环中的某些特别元素加快超椭圆曲线上的双线性对有效计算或构造具有更短 Miller 链的双线性对?
- 近年来,不少研究者在非 Weierstrass 形式的椭圆曲线上提出了有效安全的标量乘运算.能否寻找类似的技巧设计双线性对计算,以抵抗侧信道攻击或者时间攻击?
- 双线性对的计算效率与相关曲线参数紧密相关.目前,适于双线性对的超椭圆曲线并不多,如何构造更多这类曲线值得深入研究.

与双线性对计算紧密相关的问题是双线性对的安全使用问题,最能影响基于双线性对的密码协议安全的是双线性对逆问题.Galbraith等人给出了框架性的论述[44],认为利用现有的工具很难解决双线性对逆问题.我们建议能否寻找一些特殊的双线性对,求解这些双线性对的逆的复杂度低于直接求解离散对数问题,这也将对某些应用的安全性产生影响.

基于双线性对的密码体制以其特有的优点引起研究者的广泛关注,在最近的几年中得到快速发展.这一体制不仅在理论研究上有了大量的研究成果和突破,而且在工业界也已经有了许多应用实例.随着应用的逐渐广泛,国际上许多标准组织也在积极地进行这一密码体制的标准化工作.2006 年,国际标准化组织(ISO)在ISO/IEC 14888-3 中给出了两个利用双线性对设计的基于身份的签名体制的标准;IEEE也组织了专门的基于双线性对的密码体制的工作组(IEEE P1363.3)[45],并从 2006 年 2 月开始一直到现在,还在征集基于双线性对的密码体制的标准草案,从基于双线性对的加密,到签名,再到密钥协商,到签密等,以及包括实现这些体制的双线性对的安全参数选取、实现算法等标准的草案.不少新提出的双线性对都已成为标准之一.2007 年 8 月,NIST也在着手制定基于身份的密码体制和基于双线性对的密码体制的标准.我国也已经启动了基于身份的密码体制的标准化工作,并已经取得了一些进展.双线性对的计算效率对实现基于双线性对的密码协议具有非常重要的影响.构造安全并可高效计算的双线性对是椭圆曲线密码学领域中的基础理论研究重点.

References:

[1] Menezes A, Okamoto T, Vanstone S. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. on Information Theory, 1993,39(5):1639−1646.

[2] Frey G, Rück H. A remark concerning *m*-divisibility and the discrete logarithm in the divisor class group of curves. Mathematics Computation, 1994,62(206):865−874.

[3] Paterson KG. Cryptography from Pairing-Advances in Elliptic Curve Cryptography. Cambridge: Cambridge University Press, 2005. 215−252.

[4] Miller VS. The Weil pairing and its efficient calculation. Journal of Cryptology, 2004,17(4):235−261.

[5] Stange KE. The Tate pairing via elliptic nets. In: Takagi T, ed. Proc. of the Pairing 2007. LNCS 4575, Berlin, Heidelberg: Springer-Verlag, 2007. 329−348.

[6] Barreto PSLM, Galbraith S, Ó'hÉigeartaigh C, Scott M. Efficient pairing computation on supersingular Abelian varieties. Designs, Codes and Cryptography, 2007,42(3):239−271.

[7] Hess F, Smart P, Vercauteren F. The Eta pairing revisited. IEEE Trans. on Information Theory, 2006,52(10):4595−4602.

[8] Silverman JH. The Arithmetic of Elliptic Curves. New York: Springer-Verlag, 1986.

[9] Koblitz N, Menezes A. Pairing-Based cryptography at high security levels. In: Smart NP, ed. Proc. of the Cryptography and Coding. LNCS 3796, Berlin, Heidelberg: Springer-Verlag, 2005. 13−36.

[10] Scott M. Multiprecision integer and rational arithmetic C/C++ library. 2005. http://www.shamus.ie/

[11] Ben L. The pairing-based cryptography library. 2006. http://crypto.stanford.edu/pbc/

[12] Hu L, Dong J, Pei D. An implementation of cryptosystems based on Tate pairing. Journal of Computer Science and Technology, 2005,20(2):264−269.

[13] Izu T, Takagi T. Efficient computations of the Tate pairing for the large MOV degrees. In: Lee PJ, ed. Proc. of the ICISC 2002. LNCS 2587, Berlin, Heidelberg: Springer-Verlag, 2003. 283−297.

[14] Kobayashi T, Aoki K, Imai H. Efficient algorithms for Tate pairing. IEICE Trans. on Fundamentals, 2006,E89-A(1):134−143.

[15] Granger R, Smart NP. On computing products of pairings. Technical Report, CSTR-06-013, Bristol: University of Bristol, 2006. 1−11.

[16] Scott M. Computing the Tate pairing. In: Menezes AJ, ed. Proc. of the CT-RSA 2005. LNCS 3376, Berlin, Heidelberg: Springer-Verlag, 2005. 293−304.

[17] Granger R, Page D, Smart NP. High security pairing-based cryptography revisited. In: Hess F, ed. Proc. of the Algorithmic Number Theory Symp.-VII. LNCS 4076, Berlin, Heidelberg: Springer-Verlag, 2006. 480−494.

[18] Granger R, Page D, Stam M. On small characteristic algebraic Tori in pairing based cryptography. LMS Journal of Computation and Mathematics, 2006,9(3):64−85.

[19] Hu L. Compression of Tate pairings on elliptic curves. Journal of Software, 2007,18(7):1799−1805 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/1799.htm

[20] Galbraith S, Ó'hÉigeartaigh C, Sheedy C. Simplified pairing computation and security implications. Journal of Mathematical Cryptology, 2007,1(3):267−281.

[21] Granger R, Hess F, Oyono R, Theriault N, Vercauteren F. Ate pairing on hyperelliptic curves. In: Naor M, ed. Proc. of the Advances in Cryptology—EuroCrypt 2007. LNCS 4515, Berlin, Heidelberg: Springer-Verlag, 2007. 430−447.

[22] Galbraith SD, Harrison K, Soldera D. Implementing the Tate pairing. In: Fieker C, ed. Proc. of the Algorithm Number Theory Symp.-V. LNCS 2369, Berlin, Heidelberg: Springer-Verlag, 2002. 324−337.

[23] Eisentraer K, Lauter K, Montgomery PL. Fast elliptic curve arithmetic and improved Weil pairing evaluation. In: Joye M, ed. Proc. of the CT-RSA 2003. LNCS 2612, Berlin, Heidelberg: Springer-Verlag, 2003. 343−354.

[24] Dimitrov VS, Imbert L, Mishra PK. Efficient and secure elliptic curve point multiplication using double-base chains. In: Roy B, ed. Proc. of the Advances in Cryptology—Asiacrypt 2005. LNCS 3788, Berlin, Heidelberg: Springer-Verlag, 2005. 59−78.

[25] Zhao, CA, Zhang F, Huang J. Efficient Tate pairing computation using double-base chains. Science China Series F—Information Science, 2008,51(8):1096−1105.

[26] Gallant RP, Lambert RJ, Vanstone SA. Faster point multiplication on elliptic curves with efficient endomorphisms. In: Kilian J, ed. Proc. of the Advances in Cryptology-Crypto 2001. LNCS 2139, Berlin, Heidelberg: Springer-Verlag, 2001. 190−200.

[27] Scott M. Faster pairings using an elliptic curve with an efficient endomorphism. In: Maitra S, ed. Proc. of the Progress in Cryptology—INDOCRYPT 2005. LNCS 3797, Berlin, Heidelberg: Springer-Verlag, 2005. 258−269.

[28] Duursma I, Lee HS. Tate pairing implementation for hyperelliptic curves $y^2=x^p-x+d$. In: Laih CS, ed. Proc. of the Advances in Cryptology—Asiacrypt 2003. LNCS 2894, Berlin, Heidelberg: Springer-Verlag, 2003. 111−123.

[29] Barreto PSLM, Kim HY, Lynn B, Scott M. Efficient algorithms for pairing-based cryptosystems. In: Yung M, ed. Proc. of the Advances in Cryptology—Crypto 2002. LNCS 2442, Berlin, Heidelberg: Springer-Verlag, 2002. 354−368.

[30] Verheul E. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. In: Pfitzmann B, ed. Proc. of the Advances in Cryptology—Eurocrypt 2001. LNCS 2045, Berlin, Heidelberg: Springer-Verlag, 2001. 195−210.

[31] Barreto PSLM, Lynn B, Scott M. On the selection of pairing-friendly groups. In: Matsui M, ed. Proc. of the Selection Area in Cryptology—SAC 2003. LNCS 3006, Berlin, Heidelberg: Springer-Verlag, 2004. 17−25.

[32] Matsuda S, Kanayama N, Hess F, Okamoto E. Optimised versions of the Ate and twisted Ate pairings. In: Galbraith SD, ed. Proc. of the Cryptography and Coding 2007. LNCS 4887, Berlin, Heidelberg: Springer-Verlag, 2007. 302−312.

[33] Zhao CA, Zhang F, Huang J. A note on the Ate pairing. Int'l Journal Information Security, 2008,7(6):379−382.

[34] Lee E, Lee HS, Park CM. Efficient and generalized pairing computation on Abelian varieties. IEEE Trans. on Information Theory, 2009,55(4):1793−1803.

[35] Zhao CA, Zhang F, Huang J. All pairings are in a group. IEICE Trans. on Fundamentals, 2008,E91-A(10):3084−3087.

[36] Hess F. Pairing lattices. In: Galbraith SD, ed. Proc. of the Pairing 2008. LNCS 5209, Berlin, Heidelberg: Springer-Verlag, 2008. 18−38.

[37] Vercauteren F. Optimal pairings. Technical Report, 2008/096, Cryptology ePrint Archive, 2008. http://eprint.iacr.org/2008/096

[38] Galbraith SD, Hess F, Vercauteren F. Hyperelliptic pairing. In: Takagi T, ed. Proc. of the Pairing 2007. LNCS 4575, Berlin, Heidelberg: Springer-Verlag, 2007. 108−131.

[39] Galbraith SD, Lin X, Morales DJM. Pairings on hyperelliptic curves with a real model. In: Galbraith SD, ed. Proc. of the Pairing 2008. LNCS 5209, Berlin, Heidelberg: Springer-Verlag, 2008. 265−281.

[40] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing. In: Boyd C, ed. Proc. of the ASIACRYPT 2001. LNCS 2248, Berlin, Heidelberg: Springer-Verlag, 2001. 514−532.

[41] Scott M, Barreto PSLM. Compressed pairings. In: Franklin M, ed. Proc. of the CRYPTO 2004. LNCS 3152, Berlin, Heidelberg: Springer-Verlag, 2004. 140−156.

[42] Galbraith SD, Lin X. Computing pairings using x-coordinates only. Designs, Codes and Cryptography, 2009,50(3):305−324.

[43] Zhang F, Safavi-Naini R, Susili W. An efficient signature scheme from bilinear pairings and its applications. In: Bao F, ed. Proc. of the PKC 2004. LNCS 2947, 2004. 277–290.
[44] Galbraith SD, Hess F, Vercauteren F. Aspects of pairing inversion. IEEE Trans. on Information Theory, 2008,54(12):5719–5728.
[45] IEEE P1363.3 Working Group. Identity-Based public key cryptography. 2006. http://grouper.ieee.org/groups/1363/IBC/index.html

附中文参考文献:

[19] Hu L. Compression of Tate pairings on elliptic curves. Journal of Software, 2007,18(7):1799–1805. http://www.jos.org.cn/1000-9825/18/1799.htm

赵昌安(1980－),男,湖南慈利人,博士,讲师,CCF 学生会员,主要研究领域为密码与编码中的算法理论.

张方国(1972－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为密码学理论与应用.

****

第 4 届中国可信计算与信息安全学术会议(CTCIS 2010)

征 文 通 知

为了加强我国可信计算和信息安全领域学术研究和技术交流，促进我国可信计算和信息安全领域的学术繁荣、技术进步和产业发展，由中国计算机学会容错专业委员会主办，教育部高等学校信息安全类专业教学指导委员会指导，北京工业大学和国家信息中心承办的第 4 届中国可信计算与信息安全学术会议将于 2010 年 5 月 21 日－23 日在北京工业大学举行。会议将邀请本领域的专家学者，针对可信计算与信息安全领域的关键技术深入研讨，邀请军队、政府、企业代表对可信应用和信息安全产业等热点问题广泛交流。会议重点征集可信计算与信息安全理论和技术方面的研究论文。

会议录用的英文稿件将在《武汉大学学报自然科学版》(英文版）上发表，录用的中文稿件在《武汉大学学报（信息科学版)》（EI 源刊全文检索)、《北京工业大学学报》(EI 源刊全文检索)、《武汉大学学报（理学版)》(核心期刊）上发表，优秀稿件推荐到《通信学报》(EI 源刊全文检索）发表。欢迎各位专家学者、研究开发者、工程技术人员及该领域的企事业人士踊跃投稿参加。

一、征文范围（包括但不限于）

1．可信计算理论：可信计算模型，信任根与信任链传递理论，可信度量理论，信任管理
2．可信软件：安全代码设计，操作系统安全，数据库安全，恶意软件防护，嵌入式软件安全，软件容错
3．可信计算体系结构：可信计算平台，可信平台模块，可信存储，虚拟机，安全芯片，嵌入式安全，硬件容错
4．安全测试：可信计算系统与部件测试，安全测试理论与模型，安全测试技术
5．网络与通信安全：网络安全，可信网络连接，可信网格，通信网络安全
6．密码学：密码学理论，密码技术，密码应用
7．信息隐藏：信息隐藏，数字水印，数字版权管理
8．可信计算与信息安全应用：电子政务安全，电子商务安全

三、重要日期

征文截止日期：2009 年 12 月 10 日　　录用通知日期：2010 年 1 月 20 日
修改稿返回日期：2010 年 2 月 25 日　　会议日期：2010 年 5 月 21 日－5 月 23 日

四、联系方式

地址：北京市朝阳区平乐园 100 号 北京工业大学计算机学院 100124
联系人：公备，施光源
电话：86010-67396818
E-mail：tcs@bjut.edu.cn

五、会议网站：http://www.tc2010.org/