第33卷 第15期 计 算 机 工 程 2007年8月
Vol.33 No.15 Computer Engineering August 2007
·安全技术· 文章编号：1000—3428(2007)15—0158—02 文献标识码：A 中图分类号：TP309.7

圆锥曲线公钥密码算法的参数选择

徐旭东，靳岩岩，赵 磊
(北京工业大学计算机学院，北京 100022)

摘 要：圆锥曲线密码算法是一种新型的公钥密码算法，其参数选择会直接影响密码算法的安全性。该文分析了由于圆锥曲线的参数选择不当造成圆锥曲线密码算法安全性降低的原因，并给出了有限域 F_p 及环 Z_n 上产生安全圆锥曲线的方法。扩展了张明志提出的圆锥曲线群的定义，从而构造了适用于特征为2的有限域上圆锥曲线的方程。

关键词：圆锥曲线；有限域；环；特征

Parameter Selection of Public-key Cryptosystem Based on Conic Curve

XU Xu-dong, JIN Yan-yan, ZHAO Lei
(College of Computer, Beijing University of Technology, Beijing 100022)

【Abstract】 Conic curve cryptosystem is a new public-key cryptosystem, the parameters selection of conic curve could affect the security of conic curve cryptosystem. The reason that security deterioration in the case of unsuitable parameters are selected over conic curve is analyzed, and the algorithm of generating a secure conic curve equation based on finite field F_p or ring Z_n is given. It expands the definition of conic curve group which is proposed by Zhang Mingzhi, and the new equation could be applied on the finite field whose characteristic is 2.

【Key words】 conic curve; finite field; ring; characteristic

20 世纪 90 年代有学者提出了有限域 F_p 上圆锥曲线 $C_p(a,b)$及其在大整数分解和密码算法中的应用。文献[1]中定义了有限域 F_p 上的圆锥曲线 $C_p(a,b)$和加法运算⊕，并证明了$(C_p(a,b),\oplus)$构成一个有限加群。文献[2, 3]提出了基于有限域 F_p 上圆锥曲线的公钥密码系统，并实现了其在 *RSA* 公钥密码体制中的模拟。文献[4]详细说明了圆锥曲线群在环 Z_n 上的实现。对于上述文献中所提出的圆锥曲线密码算法，圆锥曲线的参数选择会直接影响密码算法的安全性。

1 有限域 F_p 上圆锥曲线的参数选择

1.1 有限域 F_p 上的圆锥曲线

有限域 F_p 上的圆锥曲线 $C_p(a,b)$[1]是指同余方程：

$$C_p(a,b): y^2 \equiv ax^2 - bx \mod p, \quad a,b \in (F_p,*) \tag{1}$$

其中，p 是奇素数。将 $y \equiv xt \pmod p$代入式(1)，则圆锥曲线 $C_p(a，b)$的全部点表示为

$$C_p(a,b): P=\left\{p(t)=(x,y)=\left(b(a-t^2)^{-1},bt(a-t^2)^{-1}\right)\middle| t\in F_p, t^2\neq a\right\}\cup \{p(\infty)=(0,0)\} \tag{2}$$

其中，$(a-t^2)^{-1}$ 为$(a-t^2)$在有限域 F_p 上的乘法逆元。$C_p(a，b)$上，定义如下运算规则：

(1)加法运算⊕：

1)对于 $P=p(t)\in C_p(a，b)$，满足 $p(t)\oplus p(\infty)=p(\infty)\oplus p(t)=p(t)$。

2)设 $P_1=p(t_1), P_2=p(t_2), P_3=p(t_3)$且 $t_1, t_2\neq\infty$，定义 $p(t_1)\oplus p(t_2)=p(t_3)$，其中，

$$t_3=\begin{cases}(t_1+t_2+a)(t_1+t_2)^{-1} \mod p, & (\text{当} t_1+t_2\neq 0 \bmod p)\\ \infty & (\text{当} t_1+t_2\equiv 0 \bmod p)\end{cases} \tag{3}$$

(2)点 P 的逆元：记作$-P$，当 $P=p(t)$时，则

$$-P=p(-t), -p(\infty)=p(\infty) \tag{4}$$

(3)标量乘运算*：k 为整数且 $P=p(t)\in C_p(a，b)$，记

$$k*P=k*p(t)=\begin{cases}\underbrace{p(t)\oplus p(t)\oplus\cdots\cdots\oplus p(t)}_{k\uparrow} & (\text{当}k>0)\\ p(\infty) & (\text{当}k=0)\\ (-k)*p(-t) & (\text{当}k<0)\end{cases} \tag{5}$$

文献[1]中证明了圆锥曲线$(C_p(a,b), \oplus)$的点和运算构成群，利用圆锥曲线群$(C_p(a,b), \oplus)$可构造基于离散对数的密钥交换协议和公钥密码系统的方法，如 Diffie-Hellman 密钥交换协议、ElGamal 加密方案、Massey-Omura 加密方案等。在加密操作过程中，需要将明文 m 表示为圆锥曲线 $C_p(a,b)$上点(即明文嵌入)，编码算法为 $x_m=b(m^2+m+a)^{-1}, y_m=bm(m^2+m+a)^{-1}$；在解密操作过程中，译码算法为 $m=y_m x_m^{-1}$。

1.2 参数选择与安全性

在式(1)所定义的圆锥曲线方程 $C_p(a,b)$中包含两个参数，它们的选择范围和圆锥曲线密码算法安全性的关系为

(1)参数 b：由于该参数仅在明文嵌入与译码中起作用，因此其取值对于圆锥曲线的安全性不会产生任何影响。

(2)参数 a：由于该参数涉及到圆锥曲线群上的计算，其取值直接影响到圆锥曲线密码体制的安全性，因此需要进行讨论。

1)当 a 为有限域 F_p 上的二次剩余，即当 Legendre 符号 $(\frac{a}{p})=1$ 时，通过构造映射：设 θ_1 和 θ_2 为模 p 的二次剩余 a

基金项目：北京市教委科技发展计划基金资助面上项目(05007012200501)

作者简介：徐旭东(1961－)，男，副教授，主研方向：计算机安全，编译原理，算法分析；靳岩岩、赵 磊，硕士研究生

收稿日期：2006-08-15 **E-mail：**xuxudong@bjut.edu.cn

的两个根(其中 $\theta_1 \neq \theta_2$),在已知 θ 的情况下可以构造从有限域 F_p 上的圆锥曲线群($C_p(a, b),\oplus$)到有限域 F_p 上的普通乘法群($Z_p^*,*$)的映射[5]：

$$\phi_a(t)=\frac{t+\theta_1}{t-\theta_2} \tag{6}$$

其中，$\theta_1^2=\theta_2^2=a$。

经过式(6)映射后,有限域 F_p 上的圆锥曲线群的离散对数的安全性被降低到有限域 F_p 上的乘法群上的离散对数问题的安全性。特别地，当 a 为有限域 F_p 上的二次剩余且 θ 为 a 的二重根时，不仅可按照式(6)构造从圆锥曲线群($C_p(a,b),\oplus$)到有限域 F_p 上的乘法群($Z_p^*,*$)的映射，还可以按照式(7)构造从有限域 F_p 上的圆锥曲线加群($C_p(a,b),\oplus$)到有限域 F_p 上的普通加法群($Z_p,+$)的映射：

$$\phi_a(t)=\frac{1}{t-\theta} \tag{7}$$

其中，$\theta^2=a$。

经过式(7)映射后,有限域 F_p 上的圆锥曲线群的离散对数的安全性被降低到有限域 F_p 上的普通加法群上的离散对数问题的安全性。此时圆锥曲线上的标量乘运算可以通过域上的乘法运算求解，因而可通过域上的除法计算求解任意点的逆元。从而使得定义在该圆锥曲线上的加群($C_p(a,\ b),\oplus$)变得毫无安全性可言。

2)当 a 不是有限域 F_p 上的二次剩余,即在 F_p 域上不存在 a 的平方根 θ 使 $\theta^2=a$ 时，此时需通过扩域才有可能在规模至少是有限域 F_{p^2} 的域上构造与圆锥曲线群($C_p(a,\ b),\oplus$)同构的普通乘法群。由于有限域 F_{p^2} 上操作数的长度比有限域 F_p 上操作数的长度多了一倍，因此，此时构成的映射并未降低原有限域 F_p 上的圆锥曲线离散对数的安全性。

综上所述，为了保证圆锥曲线公钥密码体制的安全性，需要取适当的 a 值，从而使 $(\frac{a}{p})=-1$，即在有限域 F_p 上 a 不是模 p 的二次剩余，二次剩余的判定可通过 *Euler* 判别法计算。参数 a 的取值算法具体描述如下：

算法 有限域 F_p 上产生圆锥曲线参数 a 的算法

输入 模 p 的取值。

输出 适当的 a 值。

步骤 1 随机取适当的 a 值；

步骤 2 计算 $a^{\frac{p-1}{2}}$；

步骤 3 若 $a^{\frac{p-1}{2}}=1 \bmod p$ 返回步骤 1；

步骤 4 得到适当的 a 值，算法结束。

2 环 Z_n 上圆锥曲线的参数选择

环 Z_n 上的圆锥曲线 $C_n(a,b)$[4]是指同余方程：

$$C_n(a,b): y^2 \equiv ax^2-bx \mod n,\quad (a,n)=(b,n)=1 \tag{8}$$

其中，p,q 为两个不等的奇素数；$n=pq$。模 n 下的加、减、乘法运算构成了环 Z_n 上的运算，根据式(3)可得到 $C_n(a,\ b)$上的点，并通过在 $C_n(a,\ b)$的点上定义加法运算⊕，从而得到环 Z_n 上的圆锥曲线群($C_n(a,\ b),\oplus$)。其中，环 Z_n 中加法运算⊕的定义类似于式(2)~式(5)。

对于环 Z_n 上的圆锥曲线($C_n(a,\ b),\oplus$)的应用[3, 4]，如利用环 Z_n 上的圆锥曲线对 *RSA* 公钥密码体制进行模拟。若按照式(6)构造从环 Z_n 上的圆锥曲线群到环 Z_n 上的乘法子群的映射，则必须要在环 Z_n 上计算参数 a 的二次剩余。当合数 n 为两相异素数 $p,\ q$ 的乘积时，对于模 n 的二次剩余问题有[6]：

(1)在未知 n 的分解的情况下，模 n 的二次剩余判定问题(*QRP*)是一个数学难题；

(2)分解 n 的计算等价于求模 n 的平方根。

由此可见，当合数 n 的分解未知时，在环 Z_n 中无论是二次剩余的判断问题还是平方根的求解问题都是困难的。因此，构造从环 Z_n 上的圆锥曲线群到环 Z_n 上的乘法子群的映射是困难的。

综上所述，当圆锥曲线建立在环 Z_n 上时，为了避免安全上的漏洞，提高运算的安全性，对于参数 a 的取值可选择如下两种情况，其中的 $(\frac{a}{p})$ 或 $(\frac{a}{q})$ 可通过 *Euler* 判别法计算：

(1) $(\frac{a}{p})=-1,(\frac{a}{q})=1$ 或 $(\frac{a}{p})=1,(\frac{a}{q})=-1$：此时，*Jaccobi* 符号 $(\frac{a}{n})=(\frac{a}{p})(\frac{a}{q})=-1$。根据*Jaccobi*符号的概念可知,当*Jaccobi*符号结果为–1 时，在环 Z_n 中不存在 a 的二次剩余。

(2) $(\frac{a}{p})=-1,(\frac{a}{q})=-1$：尽管此时 *Jaccobi* 符号 $(\frac{a}{n})=(\frac{a}{p})(\frac{a}{q})=1$，但在环 Z_n 中并不存在 a 的二次剩余。

3 扩展的圆锥曲线及其参数选择

在特征 $char(F)=2$ 的有限域上,任何元素 t 与 2 的标量乘 $2*t=t+t=0$，其中，0 指 $char(F)=2$ 的有限域域中的零元。由式(5)可知：当 $t_1=t_2=t\neq\infty$且 $t_1+t_2\neq 0$ 时，$p(t_3)=2*p(t)=p((t^2+a)(2t)^{-1})$。特别地，在特征 $char(F)=2$ 的有限域上 $p(t_3)=2*p(t)=p(\infty)$，即在特征 $char(F)=2$ 的有限域上圆锥曲线群仅存在阶为 2 的子群。显然，该运算使得圆锥曲线上的离散对数运算不能够加密任何数据。

为了使圆锥曲线公钥密码体制在特征为 2 的有限域上实现，将原圆锥曲线的定义方程扩展为式(9)的形式：

$$y^2+cxy=ax^2-bx \tag{9}$$

根据文献[1]中圆锥曲线的相关性质，由式(9)推导出特征 $char(F)=2$ 有限域上的圆锥曲线方程上群的运算：

(1)对于加法运算⊕，有 $p(t_1)\oplus p(t_2)=p(t_3)$，其中：

$$t_3=\begin{cases}\begin{cases}(t_1t_2+a)(t_1+t_2+c)^{-1} & t_1+t_2\neq 0\\ \infty & t_1+t_2=0\end{cases} & t_1\neq\infty,t_2\neq\infty\\ t_1 & t_2=\infty\\ t_2 & t_1=\infty\end{cases} \tag{10}$$

(2)当 $t\neq 0$ 且 $t\neq\infty$时，倍乘运算*为

$$2*p(t)=p(t)\oplus p(t)=p(\frac{t^2+a}{2t+c})$$

综上所述，改进后的圆锥曲线中增加了参数 c，通过改变参数 c 的取值可以使圆锥曲线公钥密码体制建立在任意特征的有限域上。设 $t\neq 0$ 且 $t\neq\infty$，参数 c 的取值按如下方式进行产生：

(1)当 $char(F)\neq 2$ 时，此时令参数 $c=0$，从而倍乘 $2*p(t)=p(t)\oplus p(t)=p(\frac{t^2+a}{2t+c})=p(\frac{t^2+a}{2t})\neq 0$；

(2)当 $char(F)=2$ 时，此时令参数 $c\neq 0$，从而倍乘 $2*p(t)=p(t)\oplus p(t)=p(\frac{t^2+a}{2t+c})=p(\frac{t^2+a}{c})\neq 0$。

4 结束语

通过上述分析可知，有限域 F_p 和环 Z_n 上圆锥曲线密码算法安全性主要取决于参数 a 的选择。本文给出了有限域 F_p

（下转第 180 页）

每个类别中提取 300 左右的词作为该类的特征词，训练结束。

测试时，将测试网页进行分词后，再与训练词库中的词进行匹配，把匹配成功的词语抽取出来作为该网页的特征词，然后运用前面介绍的模糊综合评判算法进行计算。

2.2 测试结果及评价方法

本实验的归类处理采用最大隶属度原则和阈值法相结合的方法，首先保证测试网页对各个类别的隶属度有超过最低阈值的，否则视为不属于任何类别的另类网页。满足最低阈值后，把测试网页归入隶属度最大的类别中。对可分别归属于两类以上的兼类网页，测试方法是在上述处理方法的基础上，进一步判断最大的隶属度和其他隶属度之间的差值，如果差值小于设定常数，则说明该网页隶属于某几个类别的程度相差不大，把该网页归入相应的多个类中。准确率和召回率是传统的信息检索领域中常用的评价指标，准确率表征的是分类的正确性，召回率表征的是分类的完整性。笔者主要采用这两项指标对分类器性能进行评价。单类网页测试结果及评价指标值如表 1 所示。对于分类错误的网页分析见表 2。10 个兼类网页的测试结果见表 3。

表 1　单类网页测试结果及评价指标值

	财经	科技	体育	教育	军事	娱乐	总计
应有网页数	20	20	20	20	20	20	120
实际网页数	23	22	17	19	19	20	120
正确网页数	17	16	16	18	18	17	102
召回率(%)	85	80	80	95	95	85	85
准确率(%)	73.9	72.7	94.1	94.7	94.7	85	85

表 2　分类错误的网页分析

	财经	科技	体育	教育	军事	娱乐	总计
应有网页	20	20	20	20	20	20	120
错误网页	3	4	4	2	2	3	18
应归于第 2 隶属度的网页数	2	4	3	2	2	2	15

表 3　兼类网页的测试结果

网页数	财经	科技	体育	教育	军事	娱乐	总计
应有	7	5	2	4	0	2	20
实际	5	6	0	4	0	2	17
正确	3	5	0	3	0	2	13

结果表明，有 6 个网页成功地归入了所属的 2 个类别中，有 3 个网页只归入 1 个类别，1 个网页归入了错误的类别。

2.3 结果分析

(1)在隶属于单个类别的网页分类结果中，总体召回率和准确率均达到了 85.0%，分类效率是比较高的。对分类错误的网页进行分析可以得知，83.3%的分类错误网页应归于其计算得出的第二大隶属度的类别中，因此，可以在今后的研究中关注网页的第 2 隶属类别，以期进一步提高分类正确率。

(2)从兼类网页的分类结果看，10 篇兼类网页其中有 6 篇成功地归入到所属的 2 个类别中，由于兼类问题处理复杂，能取得这样的效率，因此模糊综合评判算法能比较好地处理网页兼类的问题，该技术可以根据用户需要进行灵活处理。

(3)从各个类别来看，无论从单类测试还是在兼类测试，训练词库比较大的类别准确率相对较低。主要是由于大类训练文本篇幅较长，训练后的词库容量较大，使得待分类网页在大类中的隶属程度要普遍大于在小类中的隶属程度，而使一些原属于小类的网页误归入大类中，造成大类中含有较多的“噪声”文本而降低了准确率，这可以通过增大训练样本数量对各个类别的词库容量进行平衡来解决。

3　结论

网页信息的自动分类是互联网信息处理领域中的一项重要研究课题。传统的基于统计的分类方法只能机械地把网页分入确定的某一类别中，不利于用户对网页所要表达的信息进行充分完整的了解，尤其是当网页含有多个主题时，确定的单一分类方式更凸显其劣势。本文为了更完整地反映网页信息，引入了模糊数学的相关理论对网页分类进行研究，通过模糊结果使用户对网页信息有更完整的了解。此外，还对网页分类结果进行灵活的处理，通过最大隶属度原则和设定阈值方式，可以有效地过滤出异类网页和解决兼类网页的合理归类问题，使归类结果科学合理。在实际运用中，网页的类型和主题通常复杂多样，可以针对实际情况和用户目的，进行灵活的处理，这也正体现了本文的研究意义，但还存在一些不足，主要表现在对各因素权重的确定和特征词隶属函数的确定方面，这也是影响分类性能的关键，而这方面目前却没有比较权威的理论支持，只能在反复的试验中总结规律，这也是今后要进一步研究的地方。

参考文献

1 Yang Yiming, Liu Xin. A Reexamination of Text Categorization Methods[C]//Proceedings of ACM SIGIR Conference on Research and Development in Information Retrieval. 1999: 42-49.

2 李雪蕾, 张冬荣. 一种基于向量空间模型的文本分类方法[J]. 计算机工程[J], 2003, 29(10): 90-92.

3 Yang Y, Pederen J P. A Comparative Study on Feature Selection in Text Categorization[C]//Proceedings of the 14th International Conference on Machine Learning, Nashville Tennessee, USA. 1997: 412-420.

4 单松巍, 冯是聪, 李晓明. 几种典型特征选取方法在中文网页分类上的效果比较[J]. 计算机工程与应用, 2003, 39(22): 146-148.

（上接第 159 页）

及环 Z_n 上产生安全圆锥曲线的方法，并通过扩展文献[1]中定义的圆锥曲线和加法运算，提出了适用于特征为 2 的有限域上安全圆锥曲线的方程。

参考文献

1 张明志. 用圆锥曲线分解整数[J]. 四川大学学报(自然科学版), 1996, 33(4): 356-359.

2 曹珍富. 基于有限域 F_p 上圆锥曲线的公钥密码系统[C]//第五届中国密码学学术会议. 北京: 科学出版社, 1998: 45-49.

3 曹珍富. RSA 与改进的 RSA 的圆锥曲线模拟[J]. 黑龙江大学自然科学学报, 1999, 16(4): 15-18.

4 孙　琦, 朱文余, 王　标. 环 Z_n 上圆锥曲线和公钥密码协议[J]. 四川大学学报(自然科学版), 2005, 42(3): 471-478.

5 DAI Zongduo, YE Dingfeng, PEI Dingyi, et al. Cryptanalysis of ElGamal Type Encryption Schemes Based on Conic Curves[J]. Electronics Letters, 2001, 37(7).

6 Schneier B. Applied Cryptography: Protocals, Algorithms, and Sourcecode in C[M]. 2nd ed. John Wiley & Sons Inc, 1996.