第35卷 第22期 计 算 机 工 程 2009年11月
Vol.35 No.22 Computer Engineering November 2009
·安全技术· 文章编号：1000—3428(2009)22—0155—04 文献标识码：A 中图分类号：TP309.2

Eisenstein 环上的圆锥曲线公钥密码系统

潘 瑞，王丽君，李端端，李 旭
(辽宁科技大学计算机科学与工程学院，鞍山 114051)

摘 要：为了实现安全有效的曲线密码系统，引入 Eisenstein 环 $Z[\omega]$。论述剩余类环 $Z[\omega]/(r)$ 上圆锥曲线 $C_r(a,b)$ 的基本性质，证明 $C_r(a,b)$ 中分别用映射方式和坐标方式定义的 2 种加法运算的一致性，以 $(C_r(a,b),\oplus)$ 构成一个有限的 Abel 群。验证在 $C_n(a,b)$ 上寻找基点的算法适用于 $C_r(a,b)$，给出 ElGamal 密码系统在 $C_r(a,b)$ 上的数值模拟，结果表明改进后的圆锥曲线密码系统具有明文嵌入方便、运算速度快、易于实现的优点。

关键词：剩余类环；不可分数；圆锥曲线离散对数；公钥密码系统；数值模拟

Public Key Cryptosystem for Conic Curve over Eisenstein Ring

PAN Rui, WANG Li-jun, LI Duan-duan, LI Xu
(College of Computer Science and Engineering, University of Science and Technology Liaoning, Anshan 114051)

【Abstract】 In order to realize secure and effective curves cryptosystem over curves, this paper introduces Eisenstein ring $Z[\omega]$. It discusses some basic properties of conic curve $C_r(a,b)$ over the residue class ring $Z[\omega]/(r)$. It is proved that the two kinds of addition algorithms respectively defined by mapping manner and coordinate manner are consistent with each other. A limited Abel group is composed by $(C_r(a,b),\oplus)$. It validates that the algorihtm which is used for finding a base point over $C_n(a,b)$ is suitable for $C_r(a,b)$. Numerical simulation of ElGamal cryptosystem over $C_r(a,b)$ is given, and the results show that the improved conic curve cryptosystem has several merits such as being easy to embed plaintext, high computing speed and easy to be implemented.

【Key words】 residue class ring; impartibility number; conic curve discrete logarithm; public key cryptosystem; numerical simulation

1 概述

20 世纪 90 年代圆锥曲线的提出及其在公钥密码学中的应用引起了人们的广泛关注，诸多学者对圆锥曲线密码进行了大量研究。

文献[1]首次引入圆锥曲线 $C_p(a,b)$ 上的加法运算“ $\oplus$ ”，并证明 $(C_p(a,b),\oplus)$ 是一个有限加群。文献[2-3]提出基于有限域 F_p 上圆锥曲线的公钥密码系统，并给出 RSA 的圆锥曲线模拟。在此基础上，文献[4]提出有限域上的广义圆锥曲线 $R(a,b)$。文献[5]提出环 Z_n 上圆锥曲线的概念，并讨论了相应的公钥密码协议。本文提出一种基于环 $Z[\omega]/(r)$ 的圆锥曲线加密系统。

2 与 Eisenstein 环 Z[w]相关的预备知识

2.1 相关定义

定义 1[6] 设 $\omega=\left(-1+\sqrt{3}i\right)/2$，$\omega^2+\omega+1=0$，$Z[\omega]=\{a+b\omega \mid a, b\in Z\}$。

由于 Eisenstein.Ferdinard Gotthold Max 最早研究整数 $a+b\omega$ 的性质，因此，此类整数称为 Eisenstein 整数。一般情况下，$Z[\omega]$ 对于复数加法和乘法构成一个环。

定义 2[6] $N(\xi)=\xi\overline{\xi}=|\xi|^2$，其中，$\overline{\xi}$ 表示 ξ 的共轭复数。

对于 $\forall\xi=a+b\omega\in Z[\omega]$，有 $\xi=a+\left(\left(-1+\sqrt{3}i\right)/2\right)b=(a-b/2)+\left(\sqrt{3}b/2\right)i$，$\overline{\xi}=(a-b/2)-\left(\sqrt{3}b/2\right)i=(a-b)-\left(\left(-1+\sqrt{3}i\right)/2\right)b=(a-b)-b\omega$，则有 $N(\xi)=(a-b/2)^2+(3/4)b^2=a^2-ab+b^2$。

定义 3[6] 如果整数 η,ξ 满足 $\eta=\xi\varepsilon$，其中，ε 是单位数，则称 η,ξ 为相伴数或相结合数。

在 $Z[\omega]$ 中共有 6 个单位数，即 $\pm1,\pm\omega,\pm\omega^2$。若 ε 为单位数，则 $N(\varepsilon)=1$。

定义 4[6] 设 $N(\xi)>1$，若任何分解式 $\xi=\eta\rho$ 都得出 $N(\eta)=1$ 或 $N(\rho)=1$，则称 ξ 为不可分数，常记为 π。

$Z[\omega]$ 中的不可分数包括：(1) $1-\omega$ 和它的相伴数；(2)素数 $p\equiv2(\mathrm{mod}3)$ 和它的相伴数；(3)当素数 $p\equiv1(\mathrm{mod}\ 3)$ 时，满足 $p=x^2-xy+y^2$ 的 12 个不可分数 $x+y\omega$。

定义 5[6] 对于乘法“ $\odot$ ”和加法“ $\oplus$ ”，模 r 的剩余类集 $C_0,C_1,\cdots,C_{l-1}$ 构成一个环，称为模 r 的剩余类环，记为 $D/(r)$。

2.2 Z[w]上的加减乘除运算公式

对于 $\forall a+b\omega,c+d\omega\in Z[\omega]$，加减乘除公式[7]如下：

(1)加法运算公式为

$$(a+b\omega)+(c+d\omega)=(a+c)+(b+d)\omega$$

(2)减法运算公式为

$$(a+b\omega)-(c+d\omega)=(a-c)+(b-d)\omega$$

(3)乘法运算公式为

$$(a+b\omega)\times(c+d\omega)=(ac-bd)+(ad+bc-bd)\omega$$

(4)除法运算公式为

$$(a+b\omega)/(c+d\omega)=(ac-ad+bd)/(c^2-cd+d^2)+((bc-ad)/(c^2-cd+d^2))\omega$$

作者简介：潘 瑞(1982—)，男，硕士研究生，主研方向：网络信息安全；王丽君，教授；李端端、李 旭，硕士研究生

收稿日期：2009-05-25 **E-mail：**panrui4701355@163.com

3 基于环 Z[ω]上圆锥曲线的公钥密码系统

3.1 Z[ω]上的剩余算法

对于 $\forall \beta = a+b\omega \in Z[\omega]$，当给定不可分数 π 时，有 $a+b\omega(\mathrm{mod}\,\pi) \in Z[\omega]$。用 $<\beta>_\pi$ 表示 $a+b\omega\ (\mathrm{mod}\,\pi)$，并要求 $N(<\beta>_\pi) < N(\pi)$。

为了求出上述 $<\beta>_\pi$，设 $\beta = a+b\omega$，$\pi = c+d\omega$，其中，$\beta,\pi \in Z[\omega]$，并做如下处理[7]：

(1)计算 $(a+b\omega)/(c+d\omega)$，设 $(a+b\omega)/(c+d\omega) = A+B\omega$，先求出 $[A]$，$[B]$，$[\bullet]$表示“$\bullet$”的整数部分。

(2)求 $x,y \in Z$，使 $|A-x| \le 1/2$，$|B-y| \le 1/2$，此时可以令 $x=[A]$ 或 $[A]\pm1$，$y=[B]$ 或 $[B]\pm1$ 以进行验证，从而得到 x,y。

(3)计算 $\beta-(x+y\omega)\pi = <\beta>_\pi$。

算法正确性证明如下：由 $<\beta>_\pi = \pi(\beta/\pi-(x+y\omega)) = \pi((A-x)+(B-y)\omega)$ 可知，$|<\beta>_\pi|^2 = |\pi^2((A-x)+(B-y)\omega)^2| = |\pi^2|\left((A-x)^2-(A-x)(B-y)+(B-y)^2\right) \le |\pi|^2\left((A-x)^2+|A-x|\,|B-y|+(B-y)^2\right)$，因此，当 $|A-x| \le 1/2$，$|B-y| \le 1/2$ 时，$|<\beta>_\pi|^2 \le |\pi|^2((1/4)+(1/2)\bullet(1/2)+(1/4)) = (3/4)|\pi^2|$，即 $N(<\beta>_\pi) < N(\pi)$。

3.2 基于剩余类环 Z[w]/(r)上圆锥曲线的公钥密码系统

设 $Z[\omega]/(r)$ 是模 r 的剩余类环，定义 $Z[\omega]/(r)$ 上的圆锥曲线 $C_r(a,b)$ 为同余方程

$$y^2 \equiv ax^2 - bx(\mathrm{mod}\,r) \tag{1}$$

在 $Z[\omega]/(r)$ 上的解 (x,y) 的集合，其中，$r=\pi_1\pi_2$，π_1,π_2 为 2 个不同且满足 $N(\pi_1)\ne N(\pi_2)$ 的不可分数，$(a,r)=(b,r)=1$。

$O_r=(0+0\omega,0+0\omega) \in C_r(a,b)$，$C_r(a,b)$ 是式(1)的解集，即

$$C_r(a,b)=\{(x,y)\in(Z[\omega]/(r))\times(Z[\omega]/(r))\,|\, y^2 \equiv ax^2-bx(\mathrm{mod}\,r)\}$$

因为式(1)的解集等价于同余方程组

$$\begin{cases} y^2 \equiv ax^2-bx(\mathrm{mod}\,\pi_1) \\ y^2 \equiv ax^2-bx(\mathrm{mod}\,\pi_2) \end{cases} \tag{2}$$

的解集，所以利用中国剩余定理并将该定理的适用范围推广到环 $Z[\omega]$ 上(下文简称为推广后的中国剩余定理)后，可得 $C_r(a,b)$ 上的每一点 $P=(x,y)\in C_r(a,b)$ 都能被唯一地表示成一对 $[P_{\pi_1},P_{\pi_2}]=[(x_{\pi_1},y_{\pi_1}),(x_{\pi_2},y_{\pi_2})]$，其中，$P_{\pi_1}\in C_{\pi_1}(a,b)$，$P_{\pi_2}\in C_{\pi_2}(a,b)$。

$$\begin{cases} x \equiv x_{\pi_1}(\mathrm{mod}\,\pi_1) \\ x \equiv x_{\pi_2}(\mathrm{mod}\,\pi_2) \\ y \equiv y_{\pi_1}(\mathrm{mod}\,\pi_1) \\ y \equiv y_{\pi_2}(\mathrm{mod}\,\pi_2) \end{cases} \tag{3}$$

由上述对应关系可知，$C_r(a,b)$ 与 $C_{\pi_1}(a,b)\times C_{\pi_2}(a,b)$ 之间存在一一对应关系。

设 $C_r(a,b)\xrightarrow{\varphi} C_{\pi_1}(a,b)\times C_{\pi_2}(a,b)$，$C_r(a,b)$ 上每一点 $P=(x,y)\in C_r(a,b)$，$P\xrightarrow{\varphi}[P_{\pi_1},P_{\pi_2}]$，$P_{\pi_1}$ 与 P_{π_2} 由式(3)确定，可知 $O\xrightarrow{\varphi}[O_{\pi_1},O_{\pi_2}]$。

相反地，设 P_{π_1} 为 $C_{\pi_1}(a,b)$ 中任意一点，P_{π_2} 为 $C_{\pi_2}(a,b)$ 中任意一点，根据式(3)，由推广后的中国剩余定理可以唯一确定 $C_r(a,b)$ 中的点 P，即 $[P_{\pi_1},P_{\pi_2}]\xrightarrow{\varphi^{-1}}P$，$\varphi^{-1}$ 表示 φ 的逆映射。对于 $C_r(a,b)$ 上任意 2 点 P,Q，其加法运算为

$$P\oplus Q=\varphi^{-1}[P_{\pi_1}\oplus Q_{\pi_1},P_{\pi_2}\oplus Q_{\pi_2}] \tag{4}$$

由此可以得到如下定理：

定理 环 $Z[\omega]/(r)$ 上的圆锥曲线 $(C_r(a,b),\oplus)$ 构成一个有限交换群。

在式(1)的解 (x,y) 中，若 $(x,r)=1$，则令 $y\equiv xt\ (\mathrm{mod}\ r)$ 并代入式(1)，得 $(a-t^2)x\equiv b(\mathrm{mod}\,r)$。对于 $t\in Z[\omega]/(r)$，若 $(a-t^2,r)=1$，则 $x=b(a-t^2)^{-1}\ (\mathrm{mod}\,r)$，$y=bt(a-t^2)^{-1}(\mathrm{mod}\,r)$，可得解集为

$$C_1=\{P_1(t)=(b/(a-t^2),bt/(a-t^2)),(a-t^2,n)=1,\ \forall\ t\in Z[\omega]/r\}$$

若 $x\in Z[\omega]/(r)$，且 $(x,r)=\pi_1$，则令 $x=\pi_1x_1$，此时 $(x,q)=1$，令 $y\equiv xt=\pi_1x_1t(\mathrm{mod}\,r)$ 并代入(1)，得 $\pi_1^2x_1^2t^2\equiv a\pi_1^2x_1^2-bx_1\pi_1(\mathrm{mod}\,r)$，即 $\pi_1(a-t^2)x_1\equiv b(\mathrm{mod}\,\pi_2)$。对于 $t\in Z[\omega]/(\pi_2)$，$(a-t^2,\pi_2)=1$，可得 $x_1\equiv\pi_1^{-1}b(a-t^2)^{-1}\ (\mathrm{mod}\ \pi_2)$，其中，$\pi_1\pi_1^{-1}\equiv1(\mathrm{mod}\,\pi_2)$，$(a-t^2)(a-t^2)^{-1}\equiv1\ (\mathrm{mod}\ \pi_2)$，因此，$x\equiv\pi_1\pi_1^{-1}b(a-t^2)^{-1}(\mathrm{mod}\,r)$，$y\equiv\pi_1\pi_1^{-1}bt(a-t^2)^{-1}\ (\mathrm{mod}\,r)$，由此得到解集为

$$C_2=\{P_2(t)=(\pi_1\pi_1^{-1}b(a-t^2)^{-1},\pi_1\pi_1^{-1}bt(a-t^2)^{-1}),(a-t^2,\pi_2)=1,\forall t\in Z[\omega]/(\pi_2),\pi_1\pi_1^{-1}\equiv1(\mathrm{mod}\,\pi_2),(a-t^2)(a-t^2)^{-1}\equiv1\ (\mathrm{mod}\ \pi_2)\}$$

若 $x\in Z[\omega]/(r)$，且 $(x,r)=\pi_2$，则同理可得解集为

$$C_3=\{P_3(t)=(\pi_2\pi_2^{-1}b(a-t^2)^{-1},\pi_2\pi_2^{-1}bt(a-t^2)^{-1}),(a-t^2,\pi_1)=1,\forall t\in Z[\omega]/(\pi_1),\pi_2\pi_2^{-1}\equiv1(\mathrm{mod}\,\pi_1),(a-t^2)(a-t^2)^{-1}\equiv1(\mathrm{mod}\ \pi_1)\}$$

综上所述，可得 $C_r(a,b)=C_1\cup C_2\cup C_3\cup O_r$，由此可知 $\#C_r(a,b)=|C_1|+|C_2|+|C_3|+1$。

以坐标方式定义环 $Z[\omega]/(r)$ 上圆锥曲线 $C_r(a,b)$ 的加法运算“$\oplus$”，即对任意的 $P=(x_1,y_1)\in C_r(a\ b)$，$Q=(x_2,y_2)\in C_r(a,b)$，定义 $P\oplus Q$ 如下：

(1)当 $P\ne Q$ 时，$P\oplus Q$ 的定义分为如下 4 种情况：

1) 若 $(x_2-x_1,r)=1$，则 $P\oplus Q=P_1(t)\in C_1$，其中，$t=(y_2-y_1)(x_2-x_1)^{-1}(\mathrm{mod}\,r)$；

2) 若 $(x_2-x_1,r)=\pi_1$，则 $P\oplus Q=P_2(t)\in C_2$，其中，$t=(y_2-y_1)(x_2-x_1)^{-1}(\mathrm{mod}\,\pi_2)$；

3) 若 $(x_2-x_1r)=\pi_2$，则 $P\oplus Q=P_3(t)\in C_3$，其中，$t=(y_2-y_1)(x_2-x_1)^{-1}(\mathrm{mod}\,\pi_1)$；

4)若 $(x_2-x_1,r)=r$，则 $P\oplus Q=O_r$。

(2)当 $P=Q$ 时，$P\oplus Q=2P=2(x_1,y_1)$ 的定义分为如下

4 种情况：

1)若 $(y_1,r)=1$，则 $2P=P_1(t)\in C_1$，其中，$t=(2ax_1-b)(2y_1)^{-1}(\mathrm{mod}\,r)$；

2)若 $(y_1,r)=\pi_1$，则 $2P=P_2(t)\in C_2$，其中，$t=(2ax_1-b)(2y_1)^{-1}(\mathrm{mod}\,\pi_2)$；

3)若 $(y_1,r)=\pi_2$，则 $2P=P_3(t)\in C_3$，其中，$t=(2ax_1-b)(2y_1)^{-1}(\mathrm{mod}\,\pi_1)$；

4)若 $(y_1,r)=r$，则 $2P=O_r$。

命题 1 $C_r(a,b)$ 上通过映射和坐标定义的 2 种加法是一致的。

下文针对 $P\neq Q$ 时的情况 1)进行证明，其他情况下的证明方法类似。

设 $P=(x_1,y_1)\in C_r(a,b)$，$Q=(x_2,y_2)\in C_r(a,b)$，则可以 $P\xrightarrow{\varphi}\left[P_{\pi_1},P_{\pi_2}\right]$，$P_{\pi_1}=\left(x_{1_{\pi_1}},y_{1_{\pi_1}}\right)$，$P_{\pi_2}=\left(x_{1_{\pi_2}},y_{1_{\pi_2}}\right)$ 和 $Q\xrightarrow{\varphi}\left[Q_{\pi_1},Q_{\pi_2}\right]$，$Q_{\pi_1}=\left(x_{2_{\pi_1}},y_{2_{\pi_1}}\right)$，$Q_{\pi_2}=\left(x_{2_{\pi_2}},y_{2_{\pi_2}}\right)$ 由式 (3) 确定。

设 $R=P+Q$，$R\xrightarrow{\varphi}\left[R_{\pi_1},R_{\pi_2}\right]$，$R_{\pi_1}=P_{\pi_1}+Q_{\pi_1}=\pi_1(t_{\pi_1})$，$R_{\pi_2}=P_{\pi_2}+Q_{\pi_2}=\pi_2(t_{\pi_2})$。

证明：设 $P\neq Q$，$(x_2-x_1,r)=1$。因为 $(x_2-x_1,r)=1\Rightarrow(x_2-x_1,\pi_1)=1\Rightarrow\left(x_{2_{\pi_1}}-x_{1_{\pi_1}},\pi_1\right)=1\Rightarrow t_{\pi_1}\equiv\left(y_{2_{\pi_1}}-y_{1_{\pi_1}}\right)\left(x_{2_{\pi_1}}-x_{1_{\pi_1}}\right)^{-1}(\mathrm{mod}\,\pi_1)$，同理推得 $t_{\pi_2}\equiv\left(y_{2_{\pi_2}}-y_{1_{\pi_2}}\right)\left(x_{2_{\pi_2}}-x_{1_{\pi_2}}\right)^{-1}(\mathrm{mod}\,\pi_2)$，所以 $t=(y_2-y_1)(x_2-x_1)^{-1}(\mathrm{mod}r)$。又因为 $\left[R_{\pi_1},R_{\pi_2}\right]\xrightarrow{\varphi^{-1}}R=P_1(t)$，$t=(y_2-y_1)(x_2-x_1)^{-1}(\mathrm{mod}\,r),(x_2-x_1,r)=1$，所以情况 1)成立。

3.3 关于环 Z[w]/(r)上某些圆锥曲线基点的算法

设 $r=\pi_1\pi_2$，π_1,π_2 为 2 个不同且满足 $N(\pi_1)\neq N(\pi_2)$ 的不可分数，且不存在 $t_1\in Z[\omega]/(\pi_1)$，使 $t_1^2\equiv a(\mathrm{mod}\,\pi_1)$，不存在 $t_2\in Z[\omega]/(\pi_2)$，使 $t_2^2\equiv a(\mathrm{mod}\,\pi_2)$。其中，$N(\pi_1)+1=2p$，$N(\pi_2)+1=2q$，$p,q$ 为素数，则曲线 $C_r(a,b)$ 中存在点 G，其阶 $N_r=2pq$。称 G 为 $C_\pi(a,b)$ 的一个基点。

此时，集合 $S=\{O,G,2G,\cdots,(N_r-1)G\}$ 构成 $C_r(a,b)$ 的一个子群，成为由基点 G 生成的群。在群 S 中相应的离散对数问题如下：给定 2 点 $M,N\in S$，求出 $e\in Z$，$e>0$，使 $M=eN$ 是非常困难的。该问题称为 $C_r(a,b)$ 上的离散对数问题。

命题 2 给出了环 $Z[\omega]/(r)$ 上某些圆锥曲线基点的算法。

命题 2 设 $r=\pi_1\pi_2$，π_1,π_2 为 2 个不同且满足 $N(\pi_1)\neq N(\pi_2)$ 的不可分数，且不存在 $t_1\in Z[\omega]/(\pi_1)$，使 $t_1^2\equiv a(\mathrm{mod}\,\pi_1)$，不存在 $t_2\in Z[\omega]/(\pi_2)$，使 $t_2^2\equiv a(\mathrm{mod}\,\pi_2)$，其中，$N(\pi_1)+1=2p$，$N(\pi_2)+1=2q$，$p,q$ 为素数，则有 2 种情形：

(1)当 $a-b=(1+0\omega)(\mathrm{mod}\,r)$ 时，有

$$G=\begin{cases}P_1(1+0\omega) & \text{若条件1成立}\\ P_1(a) & \text{若条件2成立}\end{cases}$$

条件 1 $(1+0\omega,1+0\omega)$ 是 $C_{\pi_1}(a,b)$ 的生成元或 $(1+0\omega,1+0\omega)$ 是 $C_{\pi_2}(a,b)$ 的生成元。

条件 2 $(1+0\omega,1+0\omega)$ 是 $C_{\pi_1}(a,b)$ 的 P 阶元或 $(1+0\omega,1+0\omega)$ 是 $C_{\pi_2}(a,b)$ 的 Q 阶元。

(2)当 $a-b=(4+0\omega)(\mathrm{mod}\,r)$ 时，有

$$G=\begin{cases}P_1(2+0\omega) & \text{若条件3成立}\\ P_1(a/(2+0\omega)) & \text{若条件4成立}\end{cases}$$

条件 3 $(1+0\omega,2+0\omega)$ 是 $C_{\pi_1}(a,b)$ 的生成元或 $(1+0\omega,2+0\omega)$ 是 $C_{\pi_2}(a,b)$ 的生成元。

条件 4 $(1+0\omega,2+0\omega)$ 是 $C_{\pi_1}(a,b)$ 的 P 阶元或 $(1+0\omega,2+0\omega)$ 是 $C_{\pi_2}(a,b)$ 的 Q 阶元。

下文针对情形(1)进行证明，按相同方法可以证明情形(2)。

证明：由于 $a-b=(1+0\omega)(\mathrm{mod}\,r)$，可知 $x=y=1+0\omega$ 是式 (1) 的解，即 $(1+0\omega,1+0\omega)\in C_r(a,b)$，同理可知 $(1+0\omega,1+0\omega)\in C_{\pi_1}(a,b)$，$(1+0\omega,1+0\omega)\in C_{\pi_2}(a,b)$，由于 $C_{\pi_1}(a,b)$ 和 $C_{\pi_2}(a,b)$ 均为循环群，因此 $\#C_{\pi_1}(a,b)=N(\pi_1)+1=2p$，$\#C_{\pi_2}(a,b)=N(\pi_2)+1=2q$。若 $(1+0\omega,1+0\omega)$ 是 $C_{\pi_1}(a,b)$ 的生成元或 $(1+0\omega,1+0\omega)$ 是 $C_{\pi_2}(a,b)$ 的生成元，则 $(1+0\omega,1+0\omega)$ 在 $C_{\pi_1}(a,b)$ 中的阶为 $2p$ 或 $(1+0\omega,1+0\omega)$ 在 $C_{\pi_2}(a,b)$ 中的阶为 $2q$，此时，可以容易地推得 $(1+0\omega,1+0\omega)$ 在 $C_r(a,b)$ 中的阶为 $2rs$，即 $G=P_1(1+0\omega)$。

由于 $\left(ba^{-1},0+0\omega\right)\in C_r(a,b)$，因此可知 $\left(ba^{-1},0+0\omega\right)$ 是 $C_{\pi_1}(a,b)$ 和 $C_{\pi_2}(a,b)$ 的 2 阶点。如果 $(1+0\omega,1+0\omega)$ 是 $C_{\pi_1}(a,b)$ 的 p 阶元或 $(1+0\omega,1+0\omega)$ 是 $C_{\pi_2}(a,b)$ 的 q 阶元，那么在 $C_{\pi_1}(a,b)$ 中，$(1+0\omega,1+0\omega)\oplus\left(ba^{-1},0+0\omega\right)=\pi_1(1+0\omega)\oplus\pi_1(0+0\omega)=\pi_1(a)=A_{\pi_1}$ 的阶为 $2p$ 或在 $C_{\pi_2}(a,b)$ 中，$(1+0\omega,1+0\omega)\oplus\left(ba^{-1},0+0\omega\right)=\pi_2(1+0\omega)\oplus\pi_2(0+0\omega)=\pi_2(a)=A_{\pi_2}$ 的阶为 $2q$。设 $\left[A_{\pi_1},A_{\pi_2}\right]\xrightarrow{\varphi^{-1}}A$，则 $A=P_1(a)$，因此，可以容易地推断出 $P_1(a)$ 的阶为 $2pq$，即 $P_1(a)=G$。证毕。

4 基于环 Z[w]/(r)上圆锥曲线的 ElGamal 密码系统

4.1 系统描述

选定 $Z[\omega]/(r)$ 上的圆锥曲线：$y^2\equiv ax^2-bx\,(\mathrm{mod}\,r)$，其中，$a,b\in Z[\omega]/(r)$，$(a,r)=(b,r)=1$。$r=\pi_1\pi_2$，$\pi_1,\pi_2$ 为 2 个不同且满足 $N(\pi_1)\neq N(\pi_2)$ 的不可分数，满足如下条件：不存在 $t_1\in Z[\omega]/(\pi_1)$，使 $t_1^2\equiv a(\mathrm{mod}\,\pi_1)$ 以及不存在 $t_2\in Z[\omega]/(\pi_2)$，使 $t_2^2\equiv a(\mathrm{mod}\,\pi_2)$，且 $N(\pi_1)+1=2p$，$N(\pi_2)+1=2q$，p,q 为素数。(若存在 $t_1\in Z[\omega]/(\pi_1)$，使 $t_1^2\equiv a(\mathrm{mod}\,\pi_1)$，$N(\pi_1)-1$ 含有大素因子，且存在 $t_2\in Z[\omega]/(\pi_2)$，使 $t_2^2\equiv a\,(\mathrm{mod}\,\pi_2)$，$N(\pi_2)-1$ 含有大素因子，则仍然可以应用到密码算法)。将此圆锥曲线记为 $C_r(a,b)$，则 $\#C_r(a,b)=(N(\pi_1)+1)(N(\pi_2)+1)$。选取 $G\in Z[\omega]/(r)$，其阶 $N_r=lcm\{\#C_{\pi_1}(a,b),\#C_{\pi_2}(a,b)\}=lcm\{N(\pi_1)+1,N(\pi_2)+1\}=2pq$，即 G 为基点。

任取 $1<e<N_r$，计算 $Y=eG$，具体如下：

公钥为 r,a,b,G,Y，私钥为 e，明文 m 按上述算法嵌入到圆锥曲线上的一点 $P_1(m)=(x_m,y_m)$ 中，此时的算法描述如下：

(1)加密算法：任取 s，计算 $C_1=sG$，$C_2=P_1(m)\oplus sY$，得到密文 $C=(C_1,C_2)$。

(2)解密算法：1)计算 $eC_1=s(eG)=sY$；2)计算 $C_2\oplus(-eC_1)=P_1(m)$，对 $P_1(m)$ 使用译码算法就能得到明文 m。

该系统的安全性基于 $C_r(a,b)$ 上计算离散对数的困难性。

4.2 系统的数值模拟

A 方选取圆锥曲线 C：$y^2 \equiv (3+5\omega)x^2-(2+5\omega)x \pmod{(-88-45\omega)}$，即 $a=3+5\omega$，$b=2+5\omega$，$r=-88-45\omega$，$a-b=(1+0\omega)\pmod r$ 满足命题 2。此时，$\pi_1=3+7\omega$，$\pi_2=1+13\omega$，$p=(N(\pi_1)+1)/2=(37+1)/2=19$，$q=(N(\pi_2)+1)/2=(157+1)/2=79$，$N_r=2pq=3\,002$，任取 $e=21$。

由于 $(1+0\omega,1+0\omega)$ 在 $C_{\pi_1}(3+5\omega,2+5\omega)$ 中的阶为 19，因此根据命题 2，可以取基点 $G=P_1(3+5\omega)=(56+8\omega,-1+0\omega)$。

任取 $e=21$(保密)并计算得其二进制表示为 $(1,0,1,0,1)$，通过计算可得 $Y=21G=2^2(2^2P_1(3+5\omega)+P_1(3+5\omega))+P_1(3+5\omega)=P_1(-6-19\omega)$。

此时，公开基点 $G=P_1(3+5\omega)$ 和 $Y=P_1(-6-19\omega)$，对明文 $m=80+43\omega$ 进行加密，其过程如下：

(1)将明文 m 按 $Z[\omega]$ 上的剩余算法对 r 取余得到 m'，其中，$m'=m+kr$，$k\in Z[\omega]$，$m'=(80+43\omega)+1\times(-88-45\omega)=-8-2\omega$，$k=1+0\omega$。

(2)任取 s=10，计算 $C_1=10G=10P_1(3+5\omega)=P_1(-41-21\omega)$。

(3)计算 $C_2=P_1(m')\oplus sY=P_1(-8-2\omega)\oplus 10P_1(-6-19\omega)=P_1(-8-2\omega)\oplus P_1(34+3\omega)=P_1(58-\omega)$。

经上述处理后，传送 (C_1,C_2)。

该密码体制的解密过程描述如下：

(1)计算 $21C_1=21P_1(-41-21\omega)=P_1(34+3\omega)$。

(2)计算 $C_2\oplus(-eC_1)=P_1(58-\omega)\oplus P_1(-34-3\omega)=P_1(-8-2\omega)$，得 $m'=-8-2\omega$。

(3)计算 $m=m'-kr=(-8-2\omega)-(1+0\omega)(-88-45\omega)=80+43\omega$，得到明文 $80+43\omega$，结束。

5 结束语

本文阐述基于环 $Z[\omega]/(r)$ 上的圆锥曲线密码系统，它是基于环 Z_n 上圆锥曲线密码系统在表数范围上的进一步扩充。给出 ElGamal 密码系统在 $Z[\omega]/(r)$ 上的圆锥曲线的实现过程。本文工作有利于 $Z[\omega]/(r)$ 上的圆锥曲线密码系统在信息安全密码系统中的快速实现。

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]//密码学进展会议论文集. 北京: 科学出版社, 1998: 45-49.

[3] 王 标, 朱文余, 孙 琦. 基于剩余类环 Z_n 上圆锥曲线的公钥密码体制[J]. 四川大学学报: 工程科学版, 2005, 37(5): 112-117.

[4] Dai Zongduo, Pei Dingyi, Yang Junhui, et al. Cryptanalysis of a Public Key Cryptosystem Based on Conic Curves[C]//Proc. of International Workshop on Cryptographic Techniques & E-commerce. Hong Kong, China: [s. n.], 2000.

[5] 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.

[6] 柯 召, 孙 琦. 数论讲义下册[M]. 2 版. 北京: 高等教育出版社, 2001.

[7] 陈天华. Eisenstein 环上的一类公钥密码体制极其实现[D]. 哈尔滨: 哈尔滨工业大学, 2003.

编辑 陈 晖

(上接第 154 页)

(2)根据 ρ 并通过哈希函数生成一个只有用户知道的关键 α。通过 α 用户可以对所有关键词加密。在本文中，假设 $\alpha=g_1^{\alpha}$，则 $h_{Alice,From}=g_1^a$，$h_{Bob,To}=g_1^b$。

(3)输入 ρ,α 和一个文件(如表 1 所示)后，用户对文件进行加密，加密后得到的加密文件表示为

$$\begin{aligned}C_i=\{&C_1=(e(\alpha,g_2^{r1}),g_2^{r1},(h_{Alice,From})^{r1},(h_{Bob,To})^{r1}),\cdots),\\&C_2=(e(\alpha,g_2^{r2}),g_2^{r2},(h_{Alice,From})^{r2},(h_{Charlie,To})^{r2}),\cdots),\\&\cdots\\&C_n=(e(\alpha,g_2^{rn}),g_2^{rn},(h_{Dave,From})^{rn},(h_{Alice,To})^{rn}),\cdots)\}\end{aligned}$$

(4)根据关键生成算法定义可知 $V_1=e(\alpha,g_2^{r1})=e(g_1^{\alpha},g_2^{r1})=g_T^{\alpha r1}$，因此，“能力”的计算公式为

$$T=(\alpha\prod_{t=1}^{2}H(W_{jt}))^s,g_2^s)=(\alpha(H(Alice_{From})H(Bob_{To}))^s,g_2^s)=(\alpha((h_{Alice,From})(h_{Bob,To}))^s,g_2^s)$$

由于该过程采用本文提出的算法，因此只须执行 3 步，若采用常用的“能力”生成办法[5]，则至少需要 12 步[4-5]。可见，本文设计的“能力”生成算法是有效的。

(5)服务器继续验证测试，以确定用户需要哪个事件，即

$$Test(T,C_1)=\frac{e(\alpha((h_{Alice,From})(h_{Bob,To}))^s,g_2^{r1})}{e((h_{Alice,From})^{r1}(h_{Bob,To})^{r1},g_2^s)}=\frac{e(g_1^{\alpha}((g_1^a)(g_1^b))^s,g_2^{r1})}{e((g_1^a)^{r1}(g_1^b)^{r1},g_2^s)}=\frac{e(g_1^{\alpha}((g_1^{a+b}))^s,g_2^{r1})}{e((g_1^{a+b})^{r1},g_2^s)}=\frac{e(g_1^{\alpha+c})^s,g_2^{r1})}{e((g_1^c)^{r1},g_2^s)}=\frac{g_T^{(\alpha+cs)r1}}{g_T^{cr1s}}=g_T^{\alpha r1}$$

因为 $V_1=e(\alpha,g_2^{r1})=e(g_1^{\alpha},g_2^{r1})=g_T^{\alpha r1}$，所以服务器输出表 1 中的第 1 个事件给用户，查询过程结束。

3 结束语

本文在现有搜索算法的基础上，实现一种有效、安全的新算法，较好地解决了如何在加密数据中搜索多个连接关键词的问题。

参考文献

[1] 徐 军, 卢建朱. 数据库字段安全分级的加密方案[J]. 计算机工程, 2008, 34(4): 179-180.

[2] 汤光明, 王亚弟. 信息隐藏安全性研究[J]. 计算机工程, 2008, 34(16): 183-185.

[3] 杨 燕, 谭成翔. 安全短消息系统的研究与实现[J]. 计算机工程, 2008, 34(6): 124-126.

[4] Ryu Eun-Kyung, Tsuyoshi T. Efficient Conjunctive Keyword-searchable Encryption[C]//Proc. of AINAW'07. Niagara Falls, Canada: IEEE Press, 2007: 409-414.

[5] Golle P, Staddon J. Secure Conjunctive Keyword Search over Encrypted Data[C]//Proceedings of Applied Cryptography and Network Security Conference. Berlin, Germany: Springer, 2004: 31-45.

编辑 陈 晖