第14卷 第3期 电子科学学刊 Vol. 14, No. 3
1992 年 5 月 JOURNAL OF ELECTRONICS May, 1992

$\mathbb{Z}[\omega]$ 环上的两类密码体制*

曹 珍 富
(哈尔滨工业大学数学系,哈尔滨 150006)

摘要 本文在 Eisenstein 环 $\mathbb{Z}[\omega]$ 上得到了两类新的密码体制. 它们分别是推广的 RSA 密码体制和自确认密码体制. 安全性分别基于环 $\mathbb{Z}[\omega]$ 上整数的分解和 $\mathbb{Z}[\omega]$ 环上离散对数的计算.

关键词 计算机密码学; Eisenstein 环;密码体制

一、引 言

随着电子技术的迅速发展,计算机密码学已成为重要的研究课题. 1976 年, Diffie 和 Hellman[1] 提出了公钥密码体制的新概念,使得利用计算机网络进行通信成为现实可行. 1978 年, Rivest, Shamir 和 Adleman[2] 提出了著名的 RSA 公钥密码体制,引起了人们的普遍关注. 后来,许多人又提出了别的一些公钥密码体制,参看文献[3,4]及其所附文献. 孙琦[5]于 1986 年把 RSA 体制推广到一般的代数数域中,他是利用选定主理想为模的方法. 最近,杨义先[6]把公钥交换体制与公钥密码体制相结合,提出了自确认密码体制. 这种体制的特点是假定通信系统内的每一个用户都信得过一个设计中心,该中心的任务就是制造用户从中取出密钥和公钥的"黑盒子".

本文在分析孙琦和杨义先提出的密码体制的基础上,提出了 $\mathbb{Z}[\omega]$ 上的两类新体制. 它们分别是推广的 RSA 体制和自确认密码体制. 论证表明,选择 Eisenstein 环 $\mathbb{Z}[\omega]$, 对实现这两类体制更有利,且更安全可靠.

二、$\mathbb{Z}[\omega]$ 环上的 RSA 体制

我们知道,一个公钥密码体制 G 可表为

$$G=\langle \boldsymbol{s},\boldsymbol{p},\boldsymbol{P},\boldsymbol{C},\boldsymbol{D}\rangle,$$

这里 $\boldsymbol{s},\boldsymbol{p}$ 分别是密钥和公钥, $\boldsymbol{P}$ 和 $\boldsymbol{C}$ 分别是明文和密文, $\boldsymbol{D}$ 是解密算法. RSA 体制的 $\boldsymbol{s},\boldsymbol{p},\boldsymbol{P},\boldsymbol{C}$ 和 $\boldsymbol{D}$ 分别如下:

$\boldsymbol{s}$: $p;q;p,q$ 都是大素数.

$\boldsymbol{p}$: $m(=pq),e$;这里 e 满足 $1<e<\varphi(m)$, 且 $(e,\varphi(m))=1$, $\varphi(m)$ 表 m 的 Euler

1990.08.20 收到,1991.11.04 定稿.
* 国家自然科学基金资助课题.

函数，即当 $m=pq$ 时 $\varphi(m)=(p-1)(q-1)$.

P: n;n 是十进制的正整数，且 $n<m$.

C: $c=\langle n^e\rangle_m$;这里 $\langle\cdot\rangle_m$ 表 · 模 m 的最小非负剩余.

D: 计算 $\langle c^d\rangle_m=n$;这里 d 满足 $0<d<\varphi(m)$，且 $ed\equiv 1(\mathrm{mod}\varphi(m))$.

孙琦[5]把上述体制推广到一般的代数数域 $Q(\theta)$ 上，这里 θ 是一个 n 次代数整数. 设 $\mathbb{Z}[\theta]$ 是 $Q(\theta)$ 的代数整环，$\omega_1,\cdots,\omega_n$ 是 $\mathbb{Z}[\theta]$ 的一组整底，Δ 为 $Q(\theta)$ 的基数，$m=p_1\cdots p_k;p_1,\cdots,p_k$ 为不同的素数，且 $p_i\nmid\Delta(i=1,\cdots,k)$. 则 RSA 体制在 $\mathbb{Z}[\theta]$ 上的推广如下:

s: $P_1,\cdots,P_l$;这里 $P_1\cdots P_l=[m]$.

p: $[m],e$; 这里 e 满足 $1<e<\varphi([m])$，且 $(e,\varphi([m]))=1$，$\varphi([m])=m^n\cdot\prod_{i=1}^{l}\left(1-\frac{1}{N(P_i)}\right)$.

P: $a_1\omega_1+\cdots+a_n\omega_n$; 这里 $a_1,\cdots,a_n$ 的联结即得十进制数 $a_1*\cdots*a_n$ (*表联结)，且 $0\leqslant a_i<m(i=1,\cdots,n)$.

C: $b_1\omega_1+\cdots+b_n\omega_n=\langle(a_1\omega_1+\cdots+a_n\omega_n)^e\rangle_{[m]}$;这里 $\langle\cdot\rangle_{[m]}$ 也称为模[m]的最小非负剩余，是指 b_i 满足 $0\leqslant b_i<m(i=1,\cdots,n)$.

D: 计算 $\langle(b_1\omega_1+\cdots+b_n\omega_n)^d\rangle_{[m]}=a_1\omega_1+\cdots+a_n\omega_n$; 这里 d 满足 $0<d<\varphi([m])$，且 $ed\equiv 1\ (\mathrm{mod}\ \varphi([m]))$.

显然，代数整环 $\mathbb{Z}[\theta]$ 上的 RSA 体制是以理想数 [m] 作为模的. 这种体制实现的最大的困难是参数的选择. 作为 RSA 体制的一个十分自然的推广，我们在 Eisenstein 环 $\mathbb{Z}[\omega](\omega=(-1+\sqrt{-3})/2)$ 上，构造 RSA 体制. 这种体制与 RSA一样，易于实现，且安全性更好，它与文献[5]的方法不同.

在 $\mathbb{Z}[\omega]$ 中，素数是: (1)1—ω 和它的相伴数; (2)有理素数 $p\equiv 2(\mathrm{mod}3)$ 及其相伴数; (3) $x+\omega y,x+\bar{\omega}y$ 及其相伴数，这里 x,y 满足 $x^2-xy+y^2=p\equiv 1\ (\mathrm{mod}3)$ 是有理素数. 而且熟知[7]，设 $\alpha\in\mathbb{Z}[\omega]$，$\pi$ 是 $\mathbb{Z}[\omega]$ 中的素数，如果 $\pi\nmid\alpha$，则 $\alpha^{N(\pi)-1}\equiv 1\ (\mathrm{mod}\pi)$.

记 $\phi(\alpha)=(N(\pi_1)-1)(N(\pi_2)-1)$，这里 $\alpha=\pi_1\pi_2,\pi_i(i=1,2)$ 都是 $\mathbb{Z}[\omega]$ 上的素数，且 $N(\pi_i)(i=1,2)$ 很大[1]，则显然有: 对与 α 互素的 β (记为$(\alpha,\beta)=1$[7])，成立 $\beta^{\phi(\alpha)}\equiv 1\ (\mathrm{mod}\alpha)$. 下面简述新体制的构成.

s: π_1,π_2;

p: α,s;这里 s 满足 $1<s<\phi(\alpha)$，且 $(s,\phi(\alpha))=1$.

P: $m_1+m_2\omega$;这里 m_1,m_2 满足 $N(m_1+m_2\omega)<N(\alpha),m=m_1*m_2$(即 m_1,m_2 是 m 分成两段的结果).

C: $n_1+n_2\omega=\langle(m_1+m_2\omega)^s\rangle_\alpha$;这里 $N(n_1+n_2\omega)<N(\alpha)$，符号 $\langle\cdot\rangle_\alpha$ 与文献[7]的定义相同(以下不加解释的符号均同于文献[7]).

D: 计算 $\langle(n_1+n_2\omega)^t\rangle_\alpha=m_1+m_2\omega$;这里 t 满足 $0<t<\phi(\alpha)$，且 $st\equiv 1\ (\mathrm{mod}\ \phi(\alpha))$.

1) 这里 π_i 的选取是非常容易的，例如见文献[8].

下面介绍新体制 $\langle \boldsymbol{s},\boldsymbol{p},\boldsymbol{P},\boldsymbol{C},\boldsymbol{D}\rangle$ 的安全性分析. 从公开的 α,s 和传送途中截获的 $n_1+n_2\omega$,破译者欲破译密码有两个可能的方法: 一是直接分解 α,因为如能分解 α,就可求出 $\phi(\alpha)$, 从而求出 t, 因而可破译密码; 二是已知 α, s 和截获的密码 $n_1+n_2\omega=\langle(m_1+m_2\omega)^t\rangle_\alpha$,直接求 $\mathbf{Z}[\omega]$ 上模 α 的离散对数. 但这比求整环 $\mathbb{Z}$ 上的离散对数还难. 而分解 α,必须先分解 $N(\alpha)$ 或令 $\alpha=(a_1+b_1\omega)(a_2+b_2\omega)$, 求解 $a_i,b_i(i=1,2)$, 但这两点都是十分困难的. 在 $N(\pi_1),N(\pi_2)$ 都很大时, $N(\alpha)=N(\pi_1)N(\pi_2)$ 是两个很大素数的乘积. 要分解 $N(\alpha)$ 已经等于说要攻破所有的大整数分解的体制 (包括原始的 RSA 体制). 一般说来,这是很难做到的. 更何况对新体制而言,分解完 $N(\alpha)$ 后, 还要通过分别解不定方程 $N(\pi_i)=x_i^2-x_iy_i+y_i^2(i=1,2)$,求 $x_i+y_i\omega,x_i+y_i\bar{\omega}(i=1,2)$ 和它们的相结合数,这在 $N(\pi_i)(i=1,2)$ 很大时,也是十分困难的.

如果令 $\alpha=(a_1+b_1\omega)(a_2+b_2\omega)$,来求解 $a_i,b_i(i=1,2)$,则令 $\alpha=a+b\omega$,有

$$a=a_1a_2-b_1b_2,\quad b=a_1b_2+a_2b_1-b_1b_2$$

解这个不定方程也是十分困难的. 因为 a^2-ab+b^2 很大 (是两个大素数的乘积) a_i, $b_i(i=1,2)$都是任意整数,故用试凑法是得不到解答的. 因此, Eisenstein 环 $\mathbf{Z}[\omega]$ 上的这类公钥密码体制比原始的 RSA 体制安全性更好,而实现的方法则与 RSA 一样,密文没有数据扩张. 文献[7]给出了求 $\langle\cdot\rangle_\alpha$ 的算法,使用该文中的算法,新体制极易用计算机实现.

三、新型的自确认密码体制

新的自确认密码体制也可以叫做新的密钥分配密码体制. 为了方便, 下面我们直接以 $\mathbf{Z}[\omega]$ 中的某些概念来实现的体制为例. 设 π 是 $\mathbf{Z}[\omega]$ 中的素数, $N(\pi)$ 很大. 选 $\alpha\in\mathbb{Z}_{>0}$(正整数集),$(\alpha,N(\pi)-1)=1$. 于是 π,α 公开. 两个用户 i,j 想通话,可用明文的形式接通,然后用户 i,j 分别任选 $x_i,x_j\in\mathbb{Z}_{>0}$,计算 $\langle\alpha^{x_i}\rangle_{N(\pi)-1}\triangleq y_i,\langle\alpha^{x_j}\rangle_{N(\pi)-1}\triangleq y_j$, 这里为了保密系统的安全性计, 可选 $N(\pi)-1=6q$, q 是大素数. i 和 j 互送 y_i 和 y_j. 于是知

$$\langle y_i^{x_j}\rangle_{N(\pi)-1}=\langle\alpha^{x_ix_j}\rangle_{N(\pi)-1}=\langle y_j^{x_i}\rangle_{N(\pi)-1}\triangleq k$$

即用户 i 和 j 得到了一个公共的数据 k,这就可以当作两个用户 i,j 进行秘密通信的共同密钥. 以上构成了公钥分配密码体制. 事实上,这种公钥分配密码体制再加上如下步骤, 就成为自确认密码体制:

用户 i 计算

$$\langle(m_1+m_2\omega)^k\rangle_\pi\triangleq\beta$$

这里 $N(m_1+m_2\omega)<N(\pi)$. 将 β 发送给用户 j. 用户 j 收到 β 后, 由于用户 j 也已知 k, 且由 $(\alpha,N(\pi)-1)=1$ 知 $(k,N(\pi)-1)=1$, 故可求出 h 使得 $hk\equiv1\pmod{N(\pi)-1}$. 因此计算

$$\langle\beta^h\rangle_\pi=\langle(m_1+m_2\omega)^{hk}\rangle_\pi=m_1+m_2\omega$$

即恢复了 $m_1+m_2\omega$. 用户 j 的解密中使用了 $(m_1+m_2\omega)^{N(\pi)}\equiv m_1+m_2\omega\pmod{\pi}$.

这是一个不同于文献[6]的自确认密码体制. 它由下述几个部分构成:

$$\langle \pi, \alpha, k_{ij} = \langle \alpha^{x_i x_j} \rangle_{f(\pi)}, \mathscr{D} \rangle \triangleq \boldsymbol{H}$$

这里 π, α 是满足一定条件的任选的两个公开参数；$f(\pi)$是 π 的一个函数，它的形式由公开 π, α 时的条件来决定(可有多种形式)；x_i, x_j 分别是用户 i, j 任选的两个正整数；$\mathscr{D}$ 是用户 i, j 获得共同密钥 k_{ij} 后对明文的加、解密算法. 我们前面在 Eisenstein 环 Z[ω] 上的自确认密码体制，其参数分别为：π 为 Z[ω] 中的素数；$\alpha \in Z_{>0}$；π 和 α 满足条件：$N(\pi)$ 很大，$(\alpha, N(\pi) - 1) = 1$，且 $N(\pi) - 1 = 6q$，q 是大素数；$f(\pi) = N(\pi) - 1$；$\mathscr{D}$ 采用 Z[ω] 中幂剩余互逆变换. 显然，$\boldsymbol{H}$ 体制的自确认性主要在 $k_{ij} = \langle \alpha^{x_i x_j} \rangle_{f(\pi)}$ 上，因为任一个另外的用户 r，假冒用户 i 与 j 对话，则用户 r 只能得到 $k_{rj} = \langle \alpha^{x_r x_j} \rangle_{f(\pi)}$. 如果用户 r 用 k_{rj} 进行加密并冒充 i 发送给 j，则 j 将用 k_{ij} 来解密，因而得出一串毫无意义的符号串.

在 $\boldsymbol{H}$ 体制中，去掉 $\mathscr{D}$ 部分，就是密钥分配密码体制. 关于这种体制，除了前述 $f(\pi) = N(\pi) - 1$ 的体制外，还可有：π 是 Z[ω] 中的素数；$N(\pi)$很大，且 $N(\pi) - 1$ 含有大素数因子；再选 $\alpha \in Z[\omega], (\alpha, \pi) = 1$，则

$$k_{ij} = \langle \alpha^{x_i x_j} \rangle_{\pi}$$

由 $\langle y_i^{x_j} \rangle_{\pi} = \langle y_j^{x_i} \rangle_{\pi}, y_i = \langle \alpha^{x_i} \rangle_{\pi}$ 和 $y_j = \langle \alpha^{x_j} \rangle_{\pi}$ 求 k_{ij} 等价于求 Z[ω] 中模 π 的对数，但 $N(\pi)$很大，且 $N(\pi) - 1$ 含有大素数因子，例如 $N(\pi) - 1 = 6q$，q 为大素数，故已知 y_i, α, π 求 x_i 满足 $y_i = \langle \alpha^{x_i} \rangle_{\pi}$ 是十分困难的[1].

用户 i 和 j 得到共同的密钥 $k_{ij} = k_{ji}$ 后，用什么方法进行加密、解密已不成问题了. 这里不再讨论.

四、结　论

本文提出了 Z[ω] 环上的两类密码体制，即

(1) 把 RSA 体制推广到 Eisenstein 环上；

(2) 提出了新的自确认密码体制模式，并在 Z[ω] 环中提出了具体的构造方法.

这两种体制的实现，都仅仅与 Z[ω] 环中求最小非负剩余有关. 设 $\beta = a + b\omega$，$\sigma = c + d\omega$，这里 $\beta, \sigma \in Z[\omega]$，则求 $\langle \beta \rangle_{\sigma}$ 可按如下方法进行：

第一步：计算 $(a + b\omega)/(c + d\omega) \triangleq A + B\omega$，此处

$$A = \frac{ac - ad + bd}{c^2 - cd + d^2}, \quad B = \frac{bc - ad}{c^2 - cd + d^2}$$

第二步：求 $x, y \in Z$ 使得 $|A - x| \leqslant 1/2, |B - y| \leqslant 1/2$；

第三步：计算 $\beta - (x + y\omega)\sigma = \langle \beta \rangle_{\sigma}$ 即为所求.

这个算法的正确性证明和 x, y 的求法参见文献[7].

由于 Z[ω] 环中的整数分解和离散对数的计算都较通常整环 Z 中的困难，所以本文提出的两种体制的安全性更好些.

综上所述，本文在 Eisenstein 环 Z[ω] 上提出的两类密码体制，具有容易实现、安全

1) 我们注意到 Z[θ] 中求离散对数也是十分困难的，因此根据文献[5]可以给出 Z[θ] 中的密钥分配密码体制.

性好等特点. 因此是值得注意的密码体制.

参 考 文 献

[1] W. Diffie, M. Hellman, *IEEE Trans. on IT*, **IT-22** (1976)6,644—654.
[2] R. L. Rivest, A. Shamir, L. A. Adleman, *Comms. of ACM*, **21** (1978) 2,120—126.
[3] 曹珍富,电子学报,**16**(1988)4,120—121.
[4] 曹珍富,刘锐,高校应用数学学报,**4**(1989)1,1—5.
[5] 孙琦,四川大学学报(自然科学版),**23**(1986)2,22—27.
[6] 杨义先,通信学报,**9**(1988)3,50—53.
[7] 曹珍富, Eisenstein 环 $Z[\omega]$ 上的一类公钥密码体制,全国第三届密码学会会议录,西安, 1988 年 12 月,第 178—186 页.
[8] R. K. Guy, Unsolved Problems in Number Theory, Springer, New York, (1981), A16.

TWO NEW TYPES OF CRYPTOSYSTEMS OVER EISENSTEIN'S RING $Z[\omega]$

Cao Zhenfu

(Department of Mathematics, Harbin Institute of Technology, Harbin 150006)

Abstract A new type of public key cryptosystem and a new type of auto-authentication cryptosystem over Eisenstein's ring $Z[\omega]$ are presented. The security of these two types of cryptosystems depends on the difficulty of integer factoring and logarithmic computation in $Z[\omega]$.

Key words Computer cryptology; Eisenstein's ring; Cryptosystem