系 统 科 学 与 数 学
J. Sys. Sci. & Math. Scis.
11 (1) (1991), 91—96

破译一个新的背包公钥密码系统[1)]

章 照 止
(中国科学院系统科学研究所,北京 100080)

1. 引 言

1978 年 Merkle 和 Hellman[1] 提出了第一个基于背包问题的公钥密码系统. 其后又提出了许多更复杂的基于背包问题的公钥系统(见[2]及其后所引文献). 1982 年以来提出了许多破译背包公钥系统的方法[3-11]. 这些方法虽然是针对两类系统即含超递增序列的背包系统和低密度背包系统而设计的. 但由 Adlemorn[3] 首先建议的用 Lenstra 等[13]发明的格基约化算法来攻击迭代背包系统是有一定普遍意义的. 事实上应用这一算法,使至今已发表的背包系统, 除文献[12]提出的以外,都已被破译[2]. 最近何敬民和卢开澄[14]又提出了一个新的背包公钥系统(以下简称何-卢系统). 由于何-卢系统不含超递增序列,且系统密度可达很高,因此他们认为这一系统是基于一般背包问题, 现有方法都不能破译它,故它是安全的. 本文的目的是指出, 由于何-卢系统包含了一个两两互素的数列, 使它不难破译,故它也是不安全的. 从目前的研究看来,任何由迭代伪装的易解背包系统,其安全性是难以保证的.

2. 何-卢背包公钥系统简述

何-卢系统的加密和解密步骤如下:

1) 随机选取 k 个正整数 $m_1, m_2, \cdots, m_k$ 满足 $(m_i, m_j) = 1$, $1 \leqslant i < j \leqslant k$.

2) 计算

$$m = m_1 \cdot m_2 \cdots m_k; M_i = m/m_i, \quad 1 \leqslant i \leqslant k;$$

M_i' 满足 $1 \leqslant M_i' < m_i$, $M_i M_i' = 1 \pmod{m_i}$.

3) 计算

$$a_i = M_i M_i' \pmod{m}, \quad 1 \leqslant i \leqslant k. \tag{1}$$

4) 随机选取正整数 w, 满足 $(w, m) = 1$; 计算

$$a_i' = w a_i \pmod{m}, \quad 1 \leqslant i \leqslant k. \tag{2}$$

5) 随机选取两个正整数 w', m' 满足

$$w' < m'; \ (w', m') = 1;$$

$$m' > \max\ (a_1' x_1 + a_2' x_2 + \cdots + a_k' x_k), \tag{3}$$

1) 本工作得到国家自然科学基金及中国科学院数学研究所(开放)的部分资助.
1990 年 3 月 19 日收到.

其中 $x=(x_1,x_2,\cdots,x_k),0\leqslant x_i<10^l$ 表示明文.

6) 计算

$$a_i''=w'a_i'(\mathrm{mod}\ m'),\quad 1\leqslant i\leqslant k. \tag{4}$$

7) 公钥为 $a_1'',a_2'',\cdots,a_k''$ 和 m', 应用它将明文 x 变换为密文

$$c=a_1''x_1+a_2''x_2+\cdots+a_k''x_k(\mathrm{mod}\ m'). \tag{5}$$

8) 密钥为 $m_1,m_2,\cdots,m_k,m,w,w'$; 应用它容易从密文 c 译出明文 x. 首先计算

$$c'=w'^{-1}c=a_1'x_1+a_2'x_2+\cdots+a_k'x_k,$$

其中 w'^{-1} 为 w' 模 m' 的逆. 然后计算

$$c''=w^{-1}c'(\mathrm{mod}\ m)=a_1x_1+\cdots+a_kx_k(\mathrm{mod}\ m).$$

于是若 $x_i<m_i$, 则 $x_i=c''(\mathrm{mod}\ m_i),1\leqslant i\leqslant k$.

3. 破译方法

由(4)可得方程

$$w'^{-1}a_i''-t_im'=a_i',\quad 1\leqslant i\leqslant k, \tag{6}$$

其中 t_i 为非负整数. 由(3)知存在 $d>0$, 使

$$a_i'<m'/d,\quad 1\leqslant i\leqslant k. \tag{7}$$

因 $a_i'<m\approx 10^{kl}$, $m'\approx k10^{kl+l}$, 故 $d\approx k10^l$, 取适当大的 $n\leqslant k$, 令

$$\begin{aligned}\boldsymbol{b}_1&=(a_2'',a_3'',\cdots,a_n'',k^{-1}),\\ \boldsymbol{b}_2&=(a_1'',0,\cdots,0,0),\\ &\cdots\ \cdots\ \cdots\ \cdots\\ \boldsymbol{b}_n&=(0,0,\cdots,a_1'',0)\end{aligned} \tag{8}$$

为 n 个 n 维线性独立向量. 其中的 $a_1'',a_2'',\cdots,a_n''$ 也可用任意的 $a_{i_1}'',a_{i_2}'',\cdots,a_{i_n}''$, $1\leqslant i_1<i_2<\cdots<i_n\leqslant k$ 代替. 设 L 为由 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$ 张成的 n 维欧氏空间 R^n 中的格,即

$$L=\left\{\boldsymbol{v};\ \boldsymbol{v}=\sum_{i=1}^{n}z_i\boldsymbol{b}_i,z_i\in Z\right\}; \tag{9}$$

其中 Z 为整数环. 考虑(6)中与 $\boldsymbol{b}_1,\cdots,\boldsymbol{b}_n$ 中所取 a_i'' 对应的 n 个方程

$$w'^{-1}a_i''-t_im'=a_i',\quad 1\leqslant i\leqslant n. \tag{6}'$$

将(6)'两边除以 $m'a_i''$ 得

$$\frac{w'^{-1}}{m'}-\frac{t_i}{a_i''}=\frac{1}{m'}\left(\frac{a_i'}{a_i''}\right),\quad 1\leqslant i\leqslant n. \tag{10}$$

(10)中第 1 个方程减第 i 个方程,得

$$\frac{t_i}{a_i''}-\frac{t_1}{a_1''}=\frac{1}{m'}\left(\frac{a_1'}{a_1''}-\frac{a_i'}{a_i''}\right),\quad 2\leqslant i\leqslant n. \tag{11}$$

将(11)两边乘以 $a_1''a_i''$, 得

$$t_ia_1'-t_1a_i''=\frac{1}{m'}(a_1'a_i''-a_i'a_1''),\quad 2\leqslant i\leqslant n. \tag{12}$$

由(8)可见

$$\boldsymbol{v} = -t_1\boldsymbol{b}_1 + \sum_{i=2}^{n} t_i\boldsymbol{b}_i$$

$$= (t_2a_1'' - t_1a_2'', t_3a_1'' - t_1a_3'', \cdots, t_na_1'' - t_1a_n'', -t_1k^{-1}) \in L.$$

由(7)和(12)，Adleman 发现 $\boldsymbol{v}$ 是格 L 中的一个短向量. 因此在大多数情况下可用 Lenstra 等的格基约化算法求出 $\boldsymbol{v}$，从而求得 $t_1, t_2, \cdots, t_n$ (参看文献[3,7,13,16]).

其次由(6)'及 $0 < a_i' < m'/d$ 得

$$\frac{t_im'}{a_i''} \leqslant w'^{-1} \leqslant \frac{t_im'}{a_i''} + \frac{m'}{da_i''}, \quad 1 \leqslant i \leqslant n. \tag{13}$$

对较大的 a_i''，m'/da_i'' 很小甚至小于 1，故由(13)可求得 w'^{-1}.

下一步由(6)及 $0 < a_i' < m'/d$，得

$$\frac{w'^{-1}a_i''}{m'} - \frac{1}{d} \leqslant t_i \leqslant \frac{w'^{-1}a_i''}{m'}, \quad n < i \leqslant k. \tag{14}$$

因此由(14)可求得 $t_{n+1}, \cdots, t_k$.

现在将 t_i, w'^{-1} 代入(6)，即可求得 $a_1', a_2', \cdots, a_k'$.

再下一步，由(1)，(2)易见 $M_i | a_i'$，$1 \leqslant i \leqslant k$. 因此有 $m_i | a_i'$，对一切 $j \neq i$ 成立. 应用欧几里得算法计算

$$\gcd(a_1', \cdots, a_{i-1}', a_{i+1}', \cdots, a_k') = r_i', \quad 1 \leqslant i \leqslant k.$$

则 $m_i | r_i'$，$1 \leqslant i \leqslant k$. 因 $(m_i, a_i') = 1$，故得

$$(m_i, r_j') = 1, \quad j \neq i. \tag{15}$$

计算 $r' = r_1'r_2'\cdots r_k'$，$R_i'' = r'/r_i'$，$r_i = r_i'/(r_i', R_i'')$，由 $m_i | r_i'$，(15) 及 r_i 的计算过程易见

$$m_i | r_i, (r_i, a_i') = 1, \ 1 \leqslant i \leqslant k; (r_i, r_j) = 1, \ i \neq j. \tag{16}$$

计算 s_i 满足 $0 \leqslant s_i < r_i$，$a_i' = s_i \pmod{r_i}$. 解同余方程组

$$y = s_i \pmod{r_i}, \ 1 \leqslant i \leqslant k. \tag{17}$$

根据中国剩余定理，在 $0 \leqslant y < r = r_1r_2\cdots r_k$ 范围内解是唯一的.

下面分两种情况进行讨论:

(1) $r_i = m_i$，$1 \leqslant i \leqslant k$. 这时有

定理 1. 若 $r_i = m_i$，$1 \leqslant i \leqslant k$，则 $y = w$.

证. 由(2)知

$$a_i' = wa_i - l_im, \quad 1 \leqslant i \leqslant k, \tag{18}$$

其中 l_i 为非负整数. 又由 $a_i' = M_iM_i' = 1 \pmod{m_i}$，得 $a_i' = w \pmod{m_i}$，故 w 也满足同余方程组(17). 由 $w < m$ 及解的唯一性证得 $y = w$.

在此情况下，我们已求得了全部密钥. 因此可应用它们从密文 c 译出明文 x.

定理 2. 记 $d_i = \gcd(a_1'/m_i, \cdots, a_{i-1}'/m_i, a_{i+1}'/m_i, \cdots, a_k'/m_i)$，则下列条件等价:

1) $\gcd(a_1', \cdots a_{i-1}', a_{i+1}', \cdots, a_k') = m_i$;

2) $d_i = 1$;

3) $\gcd(w(a_1+c_1m)/m_i,(l_1+c_1w)m/m_i,\cdots,w(a_{i-1}+c_{i-1}m)/m_i,(l_{i-1}+c_{i-1}w)m/m_i,w(a_{i+1}+c_{i+1}m)/m_i,(l_{i+1}+c_{i+1}w)m/m_i,\cdots,w(a_k+c_km)/m_i,(l_k+c_kw)m/m_i)=1.$ (19)

其中 $c_1,\cdots,c_{i-1},c_{i+1},\cdots,c_k$ 为任意非负整数，$l_1,\cdots,l_{i-1},l_{i+1},\cdots,l_k$ 由(18)给出.

证. 1)和2)等价是显然的. 现证2)和3)等价. 记(19)中等号左边的 $\gcd(\cdots)=e_i$，若 $e_i>1$，则由

$$w(a_i+c_im)-(l_i+c_iw)m=a_i' \tag{20}$$

得 $d_i>1$. 反之若 $d_i>1$，不妨设 d_i 为素数，否则可用 d_i 的素数因子代替. 对任一 $j\neq i$，因 $d_i|(a_i'/m_i)$，故由(18)知，$d_i|(wa_j/m_i)$ 当且仅当 $d_i|(l_jm/m_i)$. 因此只可能有两种情况:

1) $d_i|(wa_j/m_i)$ 和 $d_i|(l_jm/m_i)$ 同时成立;

2) $(d_i,wa_j/m_i)=(d_i,l_jm/m_i)=1$. 在情况1)，取 $c_j=0$，则有 $d_i|(w(a_i+c_jm)/m_i,(l_i+c_iw)m/m_i)$. 在情况2)，设 $wa_j/m_i=h_j(\mathrm{mod}\ d_i)$，$1\leqslant h_j<d_i$. 由于 $(d_i,wm/m_i)=1$，故存在 c_j 满足 $1\leqslant c_j<d_i$ 和 $c_jwm/m_i=d_i-h_j(\mathrm{mod}\ d_i)$，取这一 c_j，我们有 $d_i|(w(a_i+c_jm)/m_i,(l_j+c_jw)m/m_i)$. 这就证明了存在一组非负整数 $c_1,\cdots,c_{i-1},c_{i+1},\cdots,c_k$，使 $d_i|e_i$，故 $e_i>1$. 定理证毕.

定理2有两点启示. 一是由于 $m_1,m_2,\cdots,m_k,w$ 是独立随机选取的. 因此 $a_1'/m_i,\cdots,a_{i-1}'/m_i,a_{i+1}'/m_i,\cdots,a_k'/m_i$ 也可近似地看作是独立随机的. 对于 $k-1$ 个独立随机选取的正整数 $n_1,n_2,\cdots,n_{k-1}$，$\gcd(n_1,n_2,\cdots,n_{k-1})=1$ 的概率近似等于 $\zeta(k-1)^{-1}$，其中 $\zeta(k)$ 是 Riemann 的 Zeta 函数(见[15] p.50. 这一概率当 k 增大时很快趋于1. 例如当 $k-1=3$ 时为0.832；当 $k-1=4$ 时为0.9239. 对于何-卢系统，为了保证系统的密度高而信息膨胀又较小，需要取 k 尽可能大[14]. 因此可以认为 $r_i=m_i$，$1\leqslant i\leqslant k$ 出现的可能性很大，是基本情况. 另一启示是 $r_i>m_i$ 是小概率事件，但也是可能出现的.

(II) 至少存在一个 i 使 $r_i>m_i$. 记 $r=r_1r_2\cdots r_k,R_i=r/r_i,1\leqslant i\leqslant k$. 令 R_i' 为满足 $1\leqslant R_i'<r_i,R_iR_i'=1(\mathrm{mod}\ r_i)$ 的正整数. 再令 $b_i=R_iR_i'(\mathrm{mod}\ r)$，$b_i'=yb_i(\mathrm{mod}\ r)$，$1\leqslant i\leqslant k$. 这时我们有

定理3. 若至少存在一个 i 使 $r_i>m_i$，则 $(y,r)=1$，且 $y=w+tm$，其中 t 为非负整数. $y=w$ 的充要条件是 $y<m$.

证. 由(16)中 $(r_i,a_i')=1$ 及 $a_i'=s_i(\mathrm{mod}\ r_i)$，得 $(s_i,r_i)=1$，$1\leqslant i\leqslant k$. 于是由(17)得 $(y,r_i)=1$，$1\leqslant i\leqslant k$. 证得 $(y,r)=1$.

令 s_i' 满足 $0\leqslant s_i'<m_i$，$s_i=s_i'(\mathrm{mod}\ m_i)$. 由 $m_i|r_i$ 得 $a_i'=s_i'(\mathrm{mod}\ m_i)$，$y=s_i'(\mathrm{mod}\ m_i)$，$1\leqslant i\leqslant k$，定理1中已证 $a_i'=w(\mathrm{mod}\ m_i)$，从而有 $w=s_i'(\mathrm{mod}\ m_i)$，$1\leqslant i\leqslant k$. 故 w 和 y 满足同样的同余方程组. 于是由 $0\leqslant w<m$，$0\leqslant y<r$ 及 $m|r$ 得 $y=w+tm$，且 $y=w$ 的充要条件是 $t=0$，即 $y<m$.

定理4. 若至少存在一个 i 使 $r_i>m_i$，则 $a_i'=b_i'$，$1\leqslant i\leqslant k$，且应用求得的 $r_1,r_2,\cdots,r_k,r,y$ 作密钥仍可从密文 c' 译出明文 x.

证. 因 s_i 满足 $a_i'=s_i(\mathrm{mod}\ r_i)$，又由 $b_i=1(\mathrm{mod}\ r_i)$，$b_i'=yb_i(\mathrm{mod}\ r)$ 及 $(y,r)=$

1，得 $b'_i \equiv y(\bmod r_i)$. 故由(17)得 $b'_i \equiv s_i(\bmod r_i)$. 从而有 $r_i|(b'_i - a'_i)$. 另一方面，由 $r_i|a'_i$, $r_i|b'_i$ 得 $r_i|(b'_i - a'_i)$, $j \neq i$. 因此得 $r|(b'_i - a'_i)$. 但由 $0 \leqslant a'_i < m < r$ 及 $0 \leqslant b'_i < r$ 得 $|b'_i - a'_i| < r$. 故必有 $b'_i - a'_i = 0$, 即 $b'_i = a'_i$.

由定理 3 知 $(y,r) = 1$, 故存在 y^{-1} 满足 $0 \leqslant y^{-1} < r$, $yy^{-1} \equiv 1(\bmod r)$. 故有

$$y^{-1}a'_i \equiv y^{-1}b'_i \equiv yy^{-1}b_i \equiv b_i(\bmod r). \tag{21}$$

因此得

$$\begin{aligned} y^{-1}c' &\equiv y^{-1}(a'_1x_1 + a'_2x_2 + \cdots + a'_kx_k) \pmod r \\ &\equiv b_1x_1 + b_2x_2 + \cdots + b_kx_k(\bmod r). \end{aligned} \tag{22}$$

因 $x_i < m_i \leqslant r_i, 1 \leqslant i \leqslant k$, 故由 (22), $r_i|b_i$, $j \neq i$ 及 $b_i \equiv 1(\bmod r_i)$ 得 $y^{-1}c' \equiv x_i(\bmod r_i)$, $1 \leqslant i \leqslant k$. 因此，可用 $r_1, r_2, \cdots, r_k, r, y$ 及 c' 求出 $x_1, x_2, \cdots, x_k$. 定理证毕.

在此情况下，我们求得的密钥虽与原密钥不完全相同，但应用它们仍可从密文 c 解出明文 x.

4. 例

例 1[14]. 设 $k = 4, (m_1, m_2, m_3, m_4) = (11, 13, 17, 19)$, 算得 $m = 46189$ 及

$$a = (a_1, a_2, a_3, a_4) = (29393, 35530, 29887, 43758).$$

取 $w = 10$, 算得

$$a' = (a'_1, a'_2, a'_3, a'_4) = (16796, 31977, 21736, 21879).$$

再取 $m' = 1979170$, $w' = 411$, 算得

$$a'' = (a''_1, a''_2, a''_3, a''_4) = (965646, 1267527, 1016816, 1075589).$$

若明文 $x = (x_1, x_2, x_3, x_4) = (7, 5, 2, 14)$, 则密文

$$c \equiv 501485 \pmod{1979170}.$$

破译过程：用格基约化算法计算

$$\begin{aligned} \boldsymbol{b}_1 &= (1267527,\ 1016816,\ 1075589,\ 0.25), \\ \boldsymbol{b}_2 &= (965646,\ 0,\ 0,\ 0), \\ \boldsymbol{b}_3 &= (0,\ 965646,\ 0,\ 0), \\ \boldsymbol{b}_4 &= (0,\ 0,\ 965646,\ 0) \end{aligned}$$

的约化基. 求出约化基中最短的向量为

$$\boldsymbol{v} = (-4845, -1976, -1547, -1174.75).$$

解联立方程组

$$\begin{cases} -0.25t_1 = -1174.75, \\ 965646t_2 - 1267527t_1 = -4845, \\ 965646t_3 - 1016816t_1 = -1976, \\ 965646t_4 - 1075589t_1 = -1547. \end{cases}$$

求得

$$(t_1, t_2, t_3, t_4) = (4699, 6168, 4948, 5234).$$

利用(13)求得

$$w'^{-1}=\left\lceil\frac{t_1m'}{a_1''}\right\rceil=\left\lceil\frac{4699\times 1979170}{965646}\right\rceil=9631,$$

其中 $\lceil x\rceil$ 表示不小于 x 的最小整数. 然后利用(6)求出 (a_1',a_2',a_3',a_4') 与前面算出的相同. 再用欧几里得算法,求出

$$(r_1,r_2,r_3,r_4)=(11,13,17,19).$$

因 r_i 都是素数,故必有 $r_i=m_i,i=1,2,3,4$. 因此为情况(I). 计算 $r=m=46189$ 及

$$(s_1,s_2,s_3,s_4)=(10,10,10,10).$$

由定理 1 知,解同余方程组(17)即得 $w=10$, 由此可求得 $w^{-1}=4619$. 我们已求得全部正确的密钥. 因此可按第 2 节的解密步骤由 c 解出 x:

$$\begin{aligned}c'&=w'^{-1}c=9631\times 501485\\&=4829802035=627235(\mathrm{mod}\ 1979170),\\c''&=w^{-1}c'=4619\times 627235\\&=2897198465=39629\ (\mathrm{mod}\ 46189),\\x&=(x_1,x_2,x_3,x_4)=(39629(\mathrm{mod}\ 11),39629(\mathrm{mod}\ 13),\\&39629(\mathrm{mod}\ 17),39629(\mathrm{mod}\ 19))=(7,5,2,14).\end{aligned}$$

例 2. 在例 1 中取 $w=35$, 其它不变. 即 $(m_1,m_2,m_3,m_4),m,m',w',x=(x_1,x_2,x_3,x_4)$ 都同例 1. 这时算得的 $a=(a_1,a_2,a_3,a_4)$ 也同例 1. 算得

$$a'=(a_1',a_2',a_3',a_4')=(12597,42636,29887,7293).$$

省略计算 $a''=(a_1'',a_2'',a_3'',a_4'')$ 及由 a'' 和 m' 计算 w'^{-1} 和 $a'=(a_1',a_2',a_3',a_4')$ 的过程. 设已算出的 a' 与前面算出的相同,且已算出

$$c'=\sum_{i=1}^{4}a_i'x_i=463235\ (\mathrm{mod}\ 1979170).$$

破译过程:用欧几里得算法,算出

$$(r_1,r_2,r_3,r_4)=(11,13,51,19),$$

因 $r_3>m_3$, 故为情况 (II). 算出 $r=138567$ 及

$$(s_1,s_2,s_3,s_4)=(2,9,1,16),$$

解同余方程组(17),得 $y=92413$. 由定理 4 知,虽然求得的密钥 $(r_1,r_2,r_3,r_4),r,y$ 与原密钥 $(m_1,m_2,m_3,m_4),m,w$ 不完全相同,但应用它们仍可按第 2 节的解密步骤由 c' 解出 x. 先由 y 和 r 算出 $y^{-1}=21115$, 然后计算

$$\begin{aligned}c''&=y^{-1}c'=9781207025=39629(\mathrm{mod}\ 138567),\\x&=(x_1,x_2,x_3,x_4)=(39629(\mathrm{mod}\ 11),39629(\mathrm{mod}\ 13),39629(\mathrm{mod}\ 51,\\&39629(\mathrm{mod}\ 19))=(7,5,2,14).\end{aligned}$$

叶柏青同志编了格基约化算法的程序并计算了例. 李大兴同志建议作者注意文献[16],作者谨表示衷心感谢.

参 考 文 献

[1] Merkle, R. C. and Hellman, M. E., *IEEE Trans. Information Theory*, IT-24 (1978), 525—530.
[2] Brickell, E. F. and Odlyzko, A. M., Cryptanalysis: A survey of recent results, *Proc. IEEE*, 76 (1988), 578—593.
[3] Adleman, L. M., Advances in Cryptography-Proc. Crypto 82, Plenum Press, 1983, 303—308.
[4] Adleman, L. M., Proc. 15th Annual ACM Symp. on Theory of Computing, 1983, 402—412.
[5] Brickell, E. F., Advances in Cryptology-Proc. Crypto 83, Plenum Press, 1984, 25—37.
[6] Lagarias, J. C., Advances in Cryptology-Proc. Crypto 83, Plenum Press, 1984, 3—23.
[7] Brickell, E. F., Lagarias, J. C. and Odlyzko, A. M., Advances in Cryptology-Proc. Crypto 83, Plenum Press, 1984, 39—42.
[8] Brickell, E. F., Advances in Cryptology-Proc. Crypto 84, Springer-Verlag, 1985, 342—358.
[9] Lagarias, J. C. and Odlyzko, A. M., *J. Assoc. Comp. Math.*, 32(1985), 229—246.
[10] Shamir, A., Proc. 23rd IEEE Symp. on Foundations of Computer Science, 1982, 145—152.
[11] Ingemarsson, I., Cryptography-Proc. Burg Feuerstein 1982, Springer, 1983, 309—315.
[12] Chor, B. and Rivest, R. L., Advances in Cryptology-Proc. Crypto 84, Springer-Verlag, 1985, 54—65.
[13] Lenstra, A. K., Lenstra, H. W. and Lovász, L., *Mathematische Annalen*, 261 (1982), 515—534.
[14] 何敬民、卢开澄，背包公钥密码系统的安全性与设计，清华大学学报(自然科学版)，28: 1(1988)，89—97。
[15] Schroeder, M. R., Number Theory in Science and Communication, Springer-Verlag, 1984.
[16] Frieze, A. M., *SIAM J. Comp.*, 15: 2 (1986), 536—539.

BREAKING A NEW KNAPSACK PUBLIC KEY CRYPTOSYSTEM

ZHANG ZHAO-ZHI

(*Institute of Systems Science, Academia Sinica, Beijing*, 100080)

ABSTRACT

Recently, He Jingmin and Lu Kaicheng[14] devised a new knapsack public key cryptosystem. The system does not involve any superincreasing sequence of knapsack components. In addition, it has a high density when the system parameters are properly chosen, and so is thought to be unbreakable by any existing methods. In this paper, a method for breaking the system of He and Lu is given. By using this method, a solution of the private key can be found from the public key, with high probability, the calculated private key is exactly the private key of the system. In case they are not the same, the calculated private key can still be used for correct decryption.