中国科学(A 辑)
第25卷 第11期 SCIENCE IN CHINA (Series A) 1995年11月

有限自动机公钥密码体制的密码分析*

戴大为 吴 逵 张焕国
(武汉大学计算机科学系,武汉 430072)

摘要 提出一种针对有限自动机公钥密码系统的攻击算法,它可在多项式时间内破译有限自动机公钥密码方案 FAPKC0. 这一算法的基本思想,原则上也可用来攻击其他有限自动机公钥密码方案,因而在设计新的有限自动机公钥密码系统时,必须讨论它是否经得住这种方法的攻击.

关键词 有限自动机 公钥密码 密码分析

由于 Diffie 和 Hellman 的开创性工作[1], 公钥密码系统已受到相当的注意[2]. 文献[3] 指出,有限自动机可用于构造公钥密码系统,基于有限自动机的可逆性理论,提出几种具体实施方案,即文献[3] 中的 FAPKC0 及文献[4] 中的 FAPKC1 和 FAPKC2. 这些方案都具有加、解密速度快,软、硬件实现简单,密钥较短等优点. 这些系统的安全性都建立在求非线性有限自动机的逆的困难性和矩阵多项式因式分解的困难性上. 随后多年,还没有人能成功地破译其中任何一种. 本文的目的是提出一种攻击 FAPKC0 的方法,证明它可以破译 FAPKC0.

为了叙述简洁,我们限于在有限域 GF(2) 上讨论. 令 $x(i), y(i)$ 为 GF(2) 上的m 维向量, A_i, B_i, F_i, F_i' 分别为 GF(2) 上的 $m\times m$ 矩阵. $M1$ 表示下面的延迟 t 步可逆线性自动机:

$$y(i)=\sum_{j=1}^{t} A_j y(i-j)+\sum_{j=0}^{t} B_j x'(i-j),\quad i=0,1,\cdots, \tag{1}$$

Mf是下式表示的延迟0步弱可逆有限自动机:

$$x'(i)=\sum_{j=0}^{r} F_j x(i-j)+\sum_{j=0}^{r-1} F_j' x(i-j)x(i-j-1),\quad i=0,1,2,\cdots, \tag{2}$$

其中 F_0 是满秩阵,且对任何 $x(i)=[a_1,\cdots,a_n]^{\mathrm{T}}$ 和 $x(j)=[b_1,\cdots,b_n]^{\mathrm{T}}$ 有 $x(i)x(j)=[a_1b_1,\cdots,a_nb_n]^{\mathrm{T}}$. 由 Mf 和 $M1$ 串联复合得到有限自动机 M:

$$y(i)=\sum_{j=1}^{t} A_j y(i-j)+\sum_{j=0}^{r+t} C_j x(i-j)+\sum_{j=0}^{r+t-1} C_j' x(i-j)x(i-j-1),$$
$$i=0,1,2,\cdots, \tag{3}$$

其中 $C_j=\sum_i B_i F_{j-i}$, $C_j'=\sum_i B_i F_{j-i}'$.

自动机 M 组成我们的加密算法,即以 M 和一组向量 $\langle x(-1), x(-2),\cdots, x(-r)\rangle$作为

1994-09-22 收稿,1995-08-26 收修改稿
* 国家自然科学基金资助项目

公钥. 当给定明文 $x(0),x(1),\cdots,x(n)$ 时，任取 t 个向量 $x(n+1),\cdots,x(n+t)$ 和 $2t$ 个向量 $y(-1),\cdots,y(-t),x(-r-1),\cdots,x(-r-t)$，然后用(3)式计算密文 $y(0),y(1),\cdots,y(n+t)$. 我们的算法指出，仅用公钥，即 M 和 $x(-1),\cdots,x(-r)$，就可由密文 $y(0),\cdots,y(t)$ 解出 $x(0)$，从而求出明文.

1　预备知识

根据有限自动机可逆性理论[5]，存在唯一的 t 阶输入存贮线性有限自动机 $M2$ 为 $M1$ 的延迟 t 步逆. 令 $M2$ 为

$$x'(i)=\sum_{j=0}^{t} D_j y(i-j),\quad i=0,1,2,\cdots,$$

那么 $M1$ 可由 $M2$ 经过下面的步骤得到. 令

$$G_1=[0\ 0\ \cdots\ 0\ 0\ E\ D_0\ 0\ D_1\ \cdots\ 0\ D_t]$$

为 $1\times 2(2t+1)$ 分块矩阵，其中每一块都是 GF(2) 上的 $m\times m$ 矩阵，0 是零矩阵，E 是单位阵.

一般，对 $i=1,2,\cdots,t+1$，令

$$G_i=[B_0^i\ 0\ B_1^i\ 0\ \cdots\ B_t^i\ D_0^i\ 0\ D_1^i\ \cdots\ 0\ D_t^i]$$

为 $1\times 2(2t+1)$ 分块矩阵，每一子块都是 GF(2) 上的 $m\times m$ 矩阵. 那么存在变换序列 $R_a(P_1)$，R_{b1}，$R_a(P_2)$，$R_{b2},\cdots,R_a(P_t),R_{bt}$，使得

$$G_1\xrightarrow{R_a(P_1)}G_1'\xrightarrow{R_{b1}}G_2\rightarrow\cdots\xrightarrow{R_a(P_t)}G_t'\xrightarrow{R_{bt}}G_t,$$

其中变换 $R_a(P_i)$ 映射 G_i 为 $G_i'=P_iG_i$，P_i 为满秩阵，P_i 的选择是使 $P_iD_0^i$ 的下面 k_i 行全为 0，而上面 $m-k_i$ 行线性无关. R_{bi} 则将 $G_i'=(g_{rs})$ 映射为 $G_{i+1}=(h_{rs})$ 使得

$$h_{rs}=\begin{cases} g_{rs}, & \text{当 } r=1,\cdots,m-k_i,\ s=1,\cdots,2m(2t+1)\text{ 时},\\ g_{r,s+2m}, & \text{当 } r=m-k_i+1,\cdots,m,\ s=1,\cdots,2m2t\text{ 时},\\ 0, & \text{当 } r=m-k_i+1,\cdots,m,\ s=2m2t+1,\cdots,2m(2t+1)\text{ 时}.\end{cases}$$

最后，$M1$ 根据下式由 G_{t+1} 得到

$$A_j=(D_0^{t+1})^{-1}\ D_j^{t+1},\quad j=1,2,\cdots,t,$$
$$B_j=(D_0^{t+1})^{-1}\ B_j^{t+1},\quad j=0,1,\cdots,t.$$

矩阵 D_0^{t+1} 和 B_j^{t+1} 在下面的讨论中至关重要，为了简化，以 D 记 D_0^{t+1}，以 B_j' 记 B_j^{t+1}. 补充令 $k_0=m,k_{t+1}=0,m_i=k_i-k_{i+1}$，则 $m=m_0+\cdots+m_t$. 把 B_j' 写成分块矩阵：

$$B_j'=\begin{bmatrix} B_{jt}'\\ \vdots\\ B_{j0}'\end{bmatrix},\quad j=0,1,\cdots,t,$$

其中 B_{js}' 是 $m_s\times m$ 矩阵，$s=0,1,\cdots,t$. 那么 B_{js}' 有如下性质：

(1) 对 $s>j$，$B_{js}'=0$；

(2) 对 $j=0,1,\cdots,t$，B_{jj}' 的行向量线性无关；

(3) 对 $s>j$，B_{js}' 的每一行都是 $B_{jj}',B_{j+1,j+1}',\cdots,B_{tt}'$ 的行的线性组合；

(4) $\begin{bmatrix} B_{tt}'\\ \vdots\\ B_{00}'\end{bmatrix}$ 是满秩矩阵.

在结束这一节时，我们不证明而列出下列定理.

定理 1 如果(1)式表示的线性有限自动机是延迟t步可逆的，则$\begin{bmatrix} 0 & \cdots & 0 \\ A_t & \ddots & \vdots \\ \vdots & \ddots & 0 \\ A_1 & \cdots & A_t \end{bmatrix}$的每一列都是$\begin{bmatrix} B_0 & \cdots & B_{t-1} & 0 & \cdots & 0 \\ 0 & \ddots & \vdots & B_t & \ddots & \vdots \\ \vdots & \ddots & B_0 & \vdots & \ddots & 0 \\ 0 & \cdots & 0 & B_1 & \cdots & B_t \end{bmatrix}$的列的线性组合.

2 对有限自动机 M 的分析

我们先从B_j'的性质出发，分析(3)式中C_j和(1)式中的B_j的性质.令

$$L_j=B_j'F_0+B_{j-1}'F_1+\cdots+B_0'F_j,\ j=0,1,\cdots,t.$$

由于$B_j=D^{-1}B_j'$，$C_j=\sum B_iF_{j-i}$，所以$C_j=D^{-1}L_j$. 关于L_j,C_j,B_j有以下引理.

引理 1 把L_j写成分块矩阵:

$$L_j=\begin{bmatrix} L_{jt} \\ \vdots \\ L_{j0} \end{bmatrix},\ j=0,1,\cdots,t,$$

其中对$s=0,1,\cdots,t$，L_{js}是$m_s\times m$矩阵. 则(1)$s>j$时，$L_{js}=0$; (2)对$j=0,1,\cdots,t$，L_{jj}的行向量线性无关.

引理 2 存在一个求满秩阵Q的算法SQ，使得$QC_j(j=0,1,\cdots,t)$具有与L_j同样的性质，即若将QC_j写成分块矩阵:

$$QC_j=\begin{bmatrix} C_{jt} \\ \vdots \\ C_{j0} \end{bmatrix},\quad j=0,1,\cdots,t,$$

其中对$s=0,1,\cdots,t$，C_{js}是$m_s\times m$矩阵，则(1)$s>j$时，$C_{js}=0$; (2)对$j=0,1,\cdots,t$，C_{jj}的行向量线性无关.

证 算法SQ

step 1. 求满秩阵P_0，使P_0C_0的上面$m-m_0$行全为0，下面m_0行线性无关.

step 2. $Q\leftarrow P_0$，$i\leftarrow 1$.

step 3. while $i\leqslant t$ do

求一满秩阵P_1，使得若$P_1QC_i=(p_{rs})$，$QC_i=(q_{rs})$，则当$r=1,2,\cdots,(m-(m_0+\cdots+m_i))$，$s=1,2,\cdots,m$时，$p_{rs}=0$; 当$r=(m-(m_0+\cdots+m_{i-1})+1),\cdots,m$，$s=1,2,\cdots,m$时，$p_{rs}=q_{rs}$. 而当$r=(m-(m_0+\cdots+m_i)+1,\cdots,(m-(m_0+\cdots+m_{i-1}))$时，行向量$[p_{r1},\ldots,p_{rm}]$线性无关.

$$Q\leftarrow P_1Q,$$
$$i\leftarrow i+1.$$

step 4. 输出Q

令$0P_i$表示以下操作：求一满秩阵Q，使得对$j=0,1,\cdots,i$，QC_j具有性质(I)：若$QC_j=$

$\begin{bmatrix} C_{jt} \\ \vdots \\ C_{j0} \end{bmatrix}$，其中对 $s=0,1,\cdots,t$，C_{js} 是 $m_s\times m$ 矩阵，则 (1) 对 $s>j$，$C_{js}=0$. (2)C_{jj} 的行线性无关.

因此，算法 SQ 不过是执行操作序列 $0P_0,0P_1,\cdots,0P_t$. 因 $C_0=D^{-1}L_0$，L_0 的秩为 $m_0\neq 0$，故 $0P_0$ 是可执行的. 当已执行了操作 $0P_{i-1}$ 时，就得到了一个满秩阵 Q，使得对 $j=0,1,\cdots,i-1$，QC_j 具有性质 (I). 因为 $QC_j=QD^{-1}L_j$ 根据引理 1 中 L_j 所具有的性质，显然，QD^{-1} 具有下面的形状：

$$QD^{-1}=\begin{bmatrix} Q_i & & & 0 \\ * & Q_{i-1} & & \\ \vdots & \ddots & Q_1 & \\ * & \cdots & * & Q_0 \end{bmatrix},$$

其中 Q_j 是 $m_j\times m_j$ 非异方阵对 $j=0,1,\cdots,i-1$，对角线以上的元素全为 0，而 Q_i 为 $m'\times m'$ 非异方阵，其中 $m'=m_i+\cdots+m_t$. 考虑矩阵 $QC_i=QD^{-1}L_i$，它最上面的 $m_i+\cdots+m_t$ 个行是

$$[Q_i \quad 0\ \cdots\ 0]\ L_i=Q_i\begin{bmatrix} L_{it} \\ \vdots \\ L_{ii} \end{bmatrix},$$

故其秩为 m_i. 从而可求得 $(m_i+\cdots+m_t)\times(m_i+\cdots+m_t)$ 非异方阵 P，使 $P[Q_i\ 0\ \cdots\ 0]L_i$ 最下面的 m_i 行线性无关而其他行全为 0. 令 $P_1=\begin{bmatrix} P & 0 \\ 0 & E \end{bmatrix}$，其中 E 是 $(m_1+\cdots+m_{i-1})\times(m_1+\cdots+m_{i-1})$ 阶单位阵，那么 P_1 就是 $0P_i$ 要求的那个非异方阵 Q. 这就证明了，如果 $0P_{i-1}$ 是可执行的，$0P_i$ 也是可执行的. 因此，算法 SQ 出口处的 Q 就满足引理的条件. 这就完成了引理的证明.

根据上面的证明，令算法 SQ 求得的矩阵为 Q，则 QD^{-1} 是下面的下三角分块阵：

$$QD^{-1}=\begin{bmatrix} Q_t & & & 0 \\ * & Q_{t-1} & & \\ \vdots & \ddots & Q_1 & \\ * & \cdots & * & Q_0 \end{bmatrix}.$$

由于

$$QB_j=QD^{-1}B_j'=QD^{-1}\begin{bmatrix} B_{jt}' \\ \vdots \\ B_{j0}' \end{bmatrix},$$

根据第 2 节所述 B_j' 的性质，容易推得

引理 3　设对 $j=0,1,\cdots,t$

$$QB_j=\begin{bmatrix} B_{jt} \\ \vdots \\ B_{j0} \end{bmatrix},$$

其中对 $s=0,1,\cdots,t$，B_{js} 是 $m_s\times m$ 矩阵，则 (1) 对 $s>j$，$B_{js}=0$；(2) 对 $j=0,1,\cdots,t$，B_{jj} 的行线性无关；(3) 对 $s<j$，B_{js} 的每一行都是 $B_{jj},B_{j+1,j+1},\cdots,B_{tt}$ 的行的线性组合.

现在我们说明怎样由 (3) 式解出 $x(0)$.

将(3)中的方程

$$y(i)=\sum A_j y(i-j)+\sum C_j x(i-j)+\sum C_j' x(i-j)x(i-j-1),\quad 0\leqslant i\leqslant t-1$$

组合成一个大矩阵方程:

$$A'\begin{bmatrix} y(t)\\ \cdot\\ \cdot\\ \cdot\\ y(1)\\ y(0)\end{bmatrix}=A\begin{bmatrix} y(-1)\\ y(-2)\\ \cdot\\ \cdot\\ y(-t+1)\\ y(-t)\end{bmatrix}+C\begin{bmatrix} x(t)\\ x(t-1)\\ \cdot\\ x(0)\\ \cdot\\ x(-r-t)\end{bmatrix}+C'\begin{bmatrix} x(t)x(t-1)\\ \cdot\\ x(1)x(0)\\ x(0)x(-1)\\ \cdot\\ x(-r-t+1)x(-r-t)\end{bmatrix},\qquad (4)$$

其中

$$A'=\begin{bmatrix} E & A_1 & \cdots & A_t\\ \cdot & \cdot & \cdot & \cdot\\ \cdot & & \cdot\ \cdot & \cdot\\ \cdot & & & A_1\\ 0 & \cdots & & E\end{bmatrix},\quad A=\begin{bmatrix} 0 & \cdots & & 0\\ A_t & \cdot & & \cdot\\ \cdot & & \cdot\ \cdot & \cdot\\ \cdot & & \cdot & 0\\ A_1 & \cdots & & A_t\end{bmatrix},$$

$$C=\begin{bmatrix} C_0 & \cdots & C_{r+t} & 0\\ \cdot & & \cdot & \\ & \cdot & & \cdot\\ & & \cdot & \\ 0 & C_0 & \cdots & C_{r+t}\end{bmatrix},\quad C'=\begin{bmatrix} C_0' & \cdots & C_{r+t-1}' & 0\\ \cdot & & \cdot & \\ & \cdot & & \cdot\\ & & \cdot & \\ 0 & C_0' & \cdots & C_{r+t-1}'\end{bmatrix}.$$

以

$$[Q]=\begin{bmatrix} Q & & 0\\ & \cdot & \\ & & \cdot\\ 0 & & Q\end{bmatrix}$$

记对角线元素为 Q, 其他元素全为 0 的分块对角方阵. 以$[Q]$乘(4)式得

$$[Q]A'\begin{bmatrix} y(t)\\ \vdots\\ y(0)\end{bmatrix}=[Q]A\begin{bmatrix} y(-1)\\ \vdots\\ y(-t)\end{bmatrix}+[Q]C\begin{bmatrix} x(t)\\ \vdots\\ x(-r-t)\end{bmatrix}+[Q]C'\begin{bmatrix} x(t)x(t-1)\\ \vdots\\ x(-r-t+1)x(-r-t)\end{bmatrix}.\qquad (5)$$

令

$$B'=\begin{bmatrix} B_0 & \cdots & B_{t-1} & 0 & \cdots & 0\\ 0 & \ddots & \vdots & B_t & \ddots & \vdots\\ \vdots & \ddots & B_0 & \vdots & \ddots & 0\\ 0 & \cdots & 0 & B_1 & \cdots & B_t\end{bmatrix},\ B=\begin{bmatrix} B_0 & \cdots & B_t & 0\\ & \ddots & & \ddots\\ 0 & & B_0 & \cdots\ B_t\end{bmatrix},$$

即 B' 是从 B 去掉第$(t+1)$列子块得到的分块矩阵. 由定理 1, 存在矩阵 H, 使 $A=B'H$, 故 $[Q]A=[Q]B'H$. 令

$$I=\begin{bmatrix} 0 & \cdots & 0 \\ C_{r+t} & \cdots & \vdots \\ \vdots & \ddots & 0 \\ C_{r+1} & \cdots & C_{r+t} \end{bmatrix},\quad I'=\begin{bmatrix} 0 & \cdots & 0 \\ C_{r+t-1} & \cdots & \vdots \\ \vdots & \ddots & 0 \\ C'_{r} & \cdots & C'_{r+t-1} \end{bmatrix}$$

是分别由 C 和 C' 的最右 t 个子块列组成的矩阵,有 $[Q]I=[Q]B'J$ 和 $[Q]I'=[Q]B'J'$,其中

$$J=\begin{bmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \\ F_r & & \vdots \\ \vdots & \ddots & 0 \\ F_{r-t+1} & \cdots & F_r \end{bmatrix},\quad J'=\begin{bmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \\ F'_{r-1} & & \vdots \\ \vdots & \ddots & 0 \\ F'_{r-t} & \cdots & F'_{r-1} \end{bmatrix},$$

所以得到

$$[Q][A\ I\ I']=[Q]B'[H\ J\ J'].$$

根据这个等式得到

引理 4　若 $[Q]B'$ 的第 j 个行向量是它的另外几个行向量的线性组合,那么 $[Q][A\ I\ I']$ 的第 j 个行向量也是它的对应的另外几个行向量的线性组合.

(5)式中,$y(-1),\cdots,y(-t),x(-r-1),\cdots,x(-r-t)$ 是未知的参数,但它们前面的系数是矩阵 $[Q][A\ I\ I']$ 的元素. 由引理 4,可以通过使系数为零来消去这些未知参数.

因为对每个 $i=1,2,\cdots,t$,当 $(i*m+m_t+\cdots+m_{t+i-1}+1)\leqslant k\leqslant(i*m+m_t+\cdots+m_{t-i})$ 时,$[Q]B'$ 的第 k 行是集合 $\{v|v$ 是 $[Q]B'$ 的第 $(j*m+k)$ 行对 $j=1,\cdots,i,k=1,2,\cdots,(m_t+\cdots+m_{t-i+1})\}$ 中一些行的线性组合. 由引理 4 知道,存在一满秩阵 P,使得对 $i=1,2,\cdots,t$ 和 $(i*m+m_t+\cdots+m_{t-i+1}+1)\leqslant k\leqslant(i*m+m_t+\cdots+m_{t-i})$,$P[Q][A\ I\ I']$ 的第 k 行为零,而其他行都与 $[Q][A\ I\ I']$ 的对应行相同. 以 P 乘(5)式,得到

$$P[Q]A'\begin{bmatrix} y(t) \\ \vdots \\ y(0) \end{bmatrix}=P[Q]A\begin{bmatrix} y(-1) \\ \vdots \\ y(-t) \end{bmatrix}+P[Q]C\begin{bmatrix} x(t) \\ \vdots \\ x(-r-t) \end{bmatrix}+P[Q]C'\begin{bmatrix} x(t)x(t-1) \\ \vdots \\ x(-r-t+1)x(-r-t) \end{bmatrix}. \tag{6}$$

把(6)式中的系数矩阵都写成分块矩阵的形状,使每个矩阵都有 $(t+1)^2$ 个子块行,其第 i 个子块行由 m_j 个 GF(2) 上的行向量组成,这里 $j=(t-i)\bmod(t+1)$,$i=0,1,\cdots,(t+1)^2-1$,而这些系数矩阵的每个子块列都由 GF(2) 上的 m 个列向量组成. 注意可以选择 P 使得 $P[Q]C$ 和 $P[Q]C'$ 最左 $(t+1)$ 个子块列分别与 $[Q]C$ 和 $[Q]C'$ 的最左 $(t+1)$ 个子块列相同. 对 $i=0,1,\cdots,t$,$P[Q]A$ 的第 $(i*(t+1)+i+1)$ 个子块行全为 0,而 $P[Q]C$ 和 $P[Q]C'$ 的第 $(i*(t+1)+i+1)$ 个子块列分别具有下面的形状:

$$[0\ \cdots\ 0\ D_{i0}\ \ D_{i1}\ \cdots\ D_{ir}\ \ 0\ \cdots\ 0]$$

和

$$[0\ \cdots\ 0\ D'_{i0}\ \ D'_{i1}\ \cdots\ D'_{i,r-1}\ 0\ \cdots\ 0],$$

即它们的最左和最右的 t 个子块全为 0. 把 $P[Q]A'$ 的第 $(i*(t+1)+i+1)$ 个子块行记为 $[A'_{i0}\cdots A'_{it}]$,由(6)式得到

$$A'_{i0}y(t)+\cdots+A'_{it}y(0)=D_{i0}x(0)+\cdots+D_{ir}x(-r)+D'_{i0}x(0)x(-1)+\cdots+$$
$$D'_{i,r-1}x(-r+1)x(-r),\ i=0,1,\cdots,t. \tag{7}$$

把(7)式的 $t+1$ 个等式写成一个矩阵方程(8):

$$\begin{bmatrix} A'_{00}\cdots A'_{0t} \\ \vdots \\ A'_{t0}\cdots A'_{tt} \end{bmatrix}\begin{bmatrix} y(t) \\ \vdots \\ y(0) \end{bmatrix}=\begin{bmatrix} D_{00} \\ \vdots \\ D_{t0} \end{bmatrix}x(0)+\begin{bmatrix} D_{01}\cdots D_{0r} \\ \vdots \\ D_{t1}\cdots D_{tr} \end{bmatrix}\begin{bmatrix} x(-1) \\ \vdots \\ x(-r) \end{bmatrix}+$$
$$\begin{bmatrix} D'_{00} \\ \vdots \\ D'_{t0} \end{bmatrix}x(0)x(-1)+\begin{bmatrix} D'_{01}\cdots D'_{0,r-1} \\ \vdots \\ D_{t1}\cdots D_{t,r-1} \end{bmatrix}\begin{bmatrix} x(-1)x(-2) \\ \vdots \\ x(-r+1)x(-r) \end{bmatrix}. \tag{8}$$

由于 $D_{j0}=C_{jj}=Q_jB'_{jj}F_0$, $D'_{j0}=Q_jB'_{jj}F'_0$, 且 Mf 是0步弱可逆的, 故(8)式对 $x(0)$ 可解.

3 攻击算法及其复杂性

综合第2节的分析, 概述攻击算法如下.

算法 A

输入: (3)式的系数矩阵 A_j, C_j, C'_j, 一组向量 $x(-1),\cdots,x(-r)$, 密文 $y(0),\cdots,y(n+t)$,

输出: (8)式的系数矩阵, 明文 $x(0),\cdots,x(n)$.

step 1. 调用算法 SQ 求矩阵 Q.

step 2. 计算$[Q]A'$, $[Q]A$, $[Q]C$, $[Q]C'$.

step 3. 构造引理4中所述矩阵$[Q][A\ I\ I']$.

step 4. 计算(6)式中的 P.

step 5. 计算 $P[Q]A'$, $P[Q]C$, $P[Q]C'$, 并用它们构造(7)式中的 A'_{ij}, D_{ij}, D'_{ij} 和(8)式中的系数矩阵.

step 6. 由(8)式中计算 $x(0),\cdots,x(n)$.

我们知道下面的定理是正确的.

定理2 算法 A 在关于 r,t,m,n 的多项式时间内, 可以破译由(3)式所定义的有限自动机密码.

我们用C语言将算法A编程, 对 $r=t=20, m=8$, 在 COMPAQ 386/33M 机器上, 构造(8)式仅花1～2s. 恢复明文的速度达到5 000 bytes/s.

致谢 陶仁骥、陈世华先生仔细阅读了本文初稿, 并提出了宝贵意见, 特致谢意.

参 考 文 献

1 Diffie W, Hellman M. New directions in cryptography. IEEE Trans on Information Theory, 1976, 22(6):644 ～ 654
2 Diffie W. The first ten years of public key cryptography. Proceeding of the IEEE, 1986, 76(5):560 ～ 577
3 陶仁骥, 陈世华. 一种有限自动机公开钥密码体制和数字签名. 计算机学报, 1985,8(6):401 ～ 409
4 Tao Renji, Chen Shihua. Two varieties of finite automaton public key cryptosystem and digital signature. J of Computer Science and Technology, 1986, 1(1):9 ～ 18
5 陶仁骥.有限自动机的可逆性. 北京: 科学出版社, 1979

中国科学A辑(中)95.11