学术论文

生成锁 $\mathscr{P}\langle G, X, X'\rangle$ 和它的中央加密系统

史开泉[1]，陈泽雄[2]
（1. 山东工业大学自动化工程系，济南 250061；
2. 大叶大学资讯工程系，台湾彰化 51505）

[摘要] 利用数据生成技术，提出生成锁 $\mathscr{P}\langle G,X,X'\rangle$ 的概念和由 $\mathscr{P}\langle G,X,X'\rangle$ 构成的中央加密系统。这些系统是：生成锁 $\mathscr{P}\langle G,X,X'\rangle$ 与单齿中央加密系统，生成锁 $\mathscr{P}\langle G,X,X'\rangle$ 与多齿中央加密系统。给出单齿加密—解密算法，多齿加密—解密算法，多齿静态加密—解密算法，多齿动态加密—解密算法，中央加密系统的结构特性。研究指出：任意两个秘密通讯的双方 A 和 B，它们各自选择无规则分布的正整数集合 $X_A=\{x_1, x_2, \cdots, x_n\}$，$X_B=\{x_1, x_2, \cdots, x_m\}$，$m, n\geqslant 4$，$X_A\neq X_B$，利用 $\mathscr{P}\langle G,X,X'\rangle$ 完成双方之间的秘密通讯。研究结果表明，所提出的方法具有良好的应用性，安全性。

[关键词] 生成锁；中央加密系统；多齿加密—解密算法；$\mathscr{P}\langle G,X,X'\rangle$ 存在定理；数位签章唯一性定理

1 引言

1976 年 W. Diffic, M. E. Hellman; 1978 年 R. L. Rivest, A. Shamir, L. Adleman 提出公开钥匙加密系统[1,2]（DH 系统，RSA 系统）并得到了广泛的应用。人们自然想到，是否可以采用“数据生成模型理论”作为工具研究信息系统安全和信息加密？这个构想来自下面的研究：1982 年[3]，1989 年[4]，1994 年[5]给出：给定数据集合 $X=\{x_1, x_2, \cdots, x_n\}$，$\forall x_i\in R^+$，$n\geqslant 4$；$X$ 经过一个简单的算法得到 X 的集合 X^*，由 X^* 得到一个数学模型。通常意义下，这个模型应用于系统状态预测和系统未来行为分析。本文中丢掉这个模型的常规应用，把这个模型加以改造、移植到信息加密系统中，把它公开给所有的合法的通讯者 A_j，$j=1, 2, \cdots, t$；$A_j\in A$，模型成为他们相互之间秘密通讯的枢纽。本文给出的研究结果表明，这个构想和移植是可实现的。

2 预备概念

设 $X=\{x_1, x_2, \cdots, x_n\}$，$n\geqslant 4$ 是一个无规则分布的集合，$X^*=\{x_1^*, x_2^*, \cdots, x_n^*\}$，$\forall x_j^*\in R^+$，是 X 的生成集合，X^* 构成一条折线 $\langle X\rangle$，则存在的指数曲线

$$\hat{X}_{k+1}=\left(x_1-\frac{u}{a}\right)e^{-ak}+\frac{u}{a} \tag{2.1}$$

逼近折线 $\langle X\rangle$。

式 (2.1) 中的参数 u，a 由下式给出[3~5]：

$$\begin{pmatrix} a \\ u \end{pmatrix}=(B^TB)^{-1}B^TY_N \tag{2.2}$$

$$B=\begin{bmatrix} -\frac{1}{2}(x_1^*+x_2^*) & 1 \\ -\frac{1}{2}(x_2^*+x_3^*) & 1 \\ \vdots & \vdots \\ -\frac{1}{2}(x_{n-1}^*+x_n^*) & 1 \end{bmatrix}$$

$$Y_N=(x_2, x_3, \cdots, x_n)^T$$

给定 $k=1, 2, \cdots, p$，由式 (2.1) 得到实数集合 $X'=\{x'_1, x'_2, \cdots, x'_p\}$，$X'$ 称作式 (2.1) 生成的 X 的可拓集合[6]。

命题 2.1 集合 X^* 构成的折线 $\langle X\rangle$ 具有近

[收稿日期] 1999－10－18；修回日期 1999－12－24

[作者简介] 史开泉（1945－），男，山东莱州市人，山东工业大学教授，博士生导师

似的指数规律，反之亦真。

命题2.2 给定模型（2.1），则存在一个集合X'。X'是式（2.1）生成的。

定理2.1（非可逆性定理）模型（2.1）记作$\mathscr{P}\langle G,X,X'\rangle$；$\mathscr{P}\langle G,X,X'\rangle(X)$和$\mathscr{P}\langle G,X,X'\rangle(X')$分别是$\mathscr{P}\langle G,X,X'\rangle$关于集合$X$的变换和$\mathscr{P}\langle G,X,X'\rangle$关于集合$X'$的变换，则

$$\mathscr{P}\langle G,X,X'\rangle(X)\neq \mathscr{P}\langle G,X,X'\rangle(X')。 \tag{2.3}$$

定理的意义：如果把X'定义成为被A加密的密文，若X'被盗，利用X'通过$\mathscr{P}\langle G,X,X'\rangle$得不到$A$的明文$X$。

定理2.2（可拓推非等值定理）给定模型（2.1），x'_i，x'_j是模型（2.1）在点i，j的可拓值[6]，若$i\neq j$，则

$$x'_i\neq x'_j \tag{2.4}$$
$$x'_i,x'_j\in R^+,i,j\in(1,2,\cdots,r)$$

（命题2.1，2.2，定理2.1，2.2证明略）。

3 生成锁$\mathscr{P}\langle G,X,X'\rangle$与单齿中央加密系统

定义3.1 给定$X=\{x_1,x_2,\cdots,x_n\}$，$\forall x_i\in N^+$，$n\geqslant 4$；由式（2.1）和式（2.2）构成一个锁称作数据生成锁，简称生成锁，记作$\mathscr{P}\langle G,X,X'\rangle$。

定义3.2 具有$\mathscr{P}\langle G,X,X'\rangle$的加密系统称一个中央加密系统，如果：

1）$\mathscr{P}\langle G,X,X'\rangle$是$A_i$，$A_j\in A$，$i\neq j$关于密文$C_j$的公共通道；

2）$\forall i$，j，$(A_i,A_j)\subset A\times A$通过$\mathscr{P}\langle G,X,X'\rangle$完成双方秘密通讯，$i\neq j$。

其中：$A=\{A_1,A_2,\cdots,A_r\}$，A_1，A_2，$\cdots$，A_r是系统的合法通讯者。

定义3.3 称$\varphi\langle X,X'\rangle$是打开$\mathscr{P}\langle G,X,X'\rangle$的钥匙，$X$称作$\varphi\langle X,X'\rangle$的毛坯，$X'$称作$\varphi\langle X,X'\rangle$上的牙齿集，$\forall x'_i\in X'$称作$\varphi\langle X,X'\rangle$第$i$个牙齿。

显然对于同一个毛坯X，可以赋予它不同数目的牙齿。例如，同一个X可以分别赋予牙齿数$|X'_1|=1$，$|X'_2|=6$，$|X'_3|=8$。因此X与X'_1，X'_2，X'_3构成三只不相同的钥匙：$\varphi\langle X,X'_1\rangle$，$\varphi\langle X,X'_2\rangle$和$\varphi\langle X,X'_3\rangle$。

定义3.4 集合X'的基数$\eta=|X'|$，称$\varphi\langle X,X'\rangle$的牙齿数。

定义3.5 称$\varphi\langle X,X'\rangle$中的$X$是中央加密系统的公开钥匙，称$\varphi\langle X,X'\rangle$中的$X'$是中央加密系统的秘密钥匙。

定理3.1（$\mathscr{P}\langle G,X,X'\rangle$中央共享特性定理）设$A=\{A_1,A_2,\cdots,A_m\}$是秘密通讯者的集合，$\mathscr{P}\langle G,X,X'\rangle$是生成锁，则$(A_i,A_j)\subset A\times A$，$A_i\neq A_j$通过$\mathscr{P}\langle G,X,X'\rangle$完成秘密通讯，$i,j\in(1,2,\cdots,m)$。

定理3.2（$\mathscr{P}\langle G,X,X'\rangle$存在定理）给定集合$X=\{x_1,x_2,\cdots,x_n\}$，$n\geqslant 4$，$\forall x_i\in R^+$，$i\in(1,2,\cdots,n)$，则$\mathscr{P}\langle G,X,X'\rangle$存在。

定理3.3（$\varphi\langle X,X'\rangle$存在定理）由$\mathscr{P}\langle G,X,X'\rangle$构成的中央加密系统中，存在非空集合；$X$与$X'$构成$\varphi\langle X,X'\rangle$。

定理3.4（$\varphi\langle X,X'\rangle$最小牙齿数定理）设$\mathscr{P}\langle G,X,X'\rangle$是生成锁，$\varphi\langle X,X'\rangle$是打开$\mathscr{P}\langle G,X,X'\rangle$的钥匙，则$\varphi\langle X,X'\rangle$具有最小牙齿数$\eta_{\min}$，而且

$$\eta_{\min}=1 \tag{3.1}$$

定理3.5（$\varphi\langle X,X'\rangle$最大牙齿数定理）设$\mathscr{P}\langle G,X,X'\rangle$是生成锁，$\varphi\langle X,X'\rangle$是打开$\mathscr{P}\langle G,X,X'\rangle$的钥匙，则$\varphi\langle X,X'\rangle$具有最大牙齿数$\eta_{\max}$，而且

$$\eta_{\max}=\zeta \tag{3.2}$$

其中$\zeta\in N^+$。

定理3.1～3.5是直接的事实。

3.1 中央加密系统的牙齿非零准则

在中央加密系统中，通讯的双方A_i，$A_j\in A$实现秘密通讯的充分必要条件是$\varphi\langle X,X'\rangle$中的集合$X$，$X'$，他们的基数$|X|$，$|X'|$满足$|X|\geqslant 4$，$|X'|\geqslant 1$；$i$，$j\in(1,2,\cdots,t)$，$i\neq j$。

3.2 中央加密系统的加密—解密算法

约定：A是密文C的发送者，B是密文C的接受者，X_A是A的加密的公开钥匙，X'_A是A的加密的秘密钥匙；X_B是B的加密的公开钥匙，X'_B是B的加密的秘密钥匙；$|X_A|$，$|X_B|\geqslant 4$，$X_A\neq X_B$，$|X'_A|$，$|X'_B|\geqslant 1$；M是明文m_j的集合，$M=\{m_1,m_2,\cdots,m_p\}$，C是密文c_j的集合，$C=\{c_1,c_2,\cdots,c_p\}$。设A，B各自选取$\varphi\langle X,X'\rangle$的毛坯$X_A$，$X_B$；$X_A=\{x_1,x_2,\cdots,x_n\}$，$X_B=\{x_1,x_2,\cdots,x_m\}$，$m\geqslant 4$，$n\geqslant 4$，

$\forall x_i \in X_A$，$\forall x_j \in X_B$，x_i，$x_j \in N^+$；X_A，X_B，公开于 A，B 的双方，A，B 各自选取 $\varphi\langle X,X'\rangle$ 的齿数 $|X'_A|$，$|X'_B|$，而且 $X'_A=\{x'_i\}$，$X'_B=\{x'_j\}$，A 对 X'_A，B 对 X'_B 各自严格保密。

3.2.1　A 关于 B 的单齿加密算法

step 1. A 向中央加密系统提出 A 与 B 通讯的申请，中央系统接受申请。

step 2. A 选取 $X_A=\{x_1, x_2, \cdots, x_n\}$，$\forall x_i \in N^+$，通过式 (2.1) 和式 (2.2) 构成的 $\mathscr{P}\langle G,X,X'\rangle$，$A$ 秘密选取 $1\leqslant|X'_A|\leqslant p$ 和 $X'_A=\{x'_i\}$，完成 $\{x'_i\}=int\{x'_i\}$。

step 3. 对于给定的明文 $m_k \in M$，A 利用 X'_A 将 m_k 半加密成密文 c'_k（A 对 m_k 数位签章）。

$$c'_k=\{\underset{x'_i\in X'_A}{x'_i}\}\oplus m_k。\tag{3.3}$$

step 4. A 利用 X_B 将 c'_k 全加密成密文 C_k

$$c_k=\{\underset{\substack{j=1,2,\cdots,m\\ x_j\in X_B}}{x_j}\}\oplus(\{\underset{x'_j\in X'_A}{x'_i}\}\oplus m_k)。\tag{3.4}$$

step 5. 中央系统把 c_k 送给 B。

step 6. END

B 关于 A 的单齿加密算法与上面类似，略。

3.2.2　B 关于 A 的单齿解密算法

step 1. B 利用 X_B 对密文 c_k 还原解密，得到半密文 c'_k

$$c'_k=\bigoplus_{j=1,x_j\in X_B}^{m}(C_k)。\tag{3.5}$$

step 2. 请求 A 回答 $|X'_A|$，A 将 $|X'_A|=t\in N^+$ 装入信封内，将信封密封后寄给 B，并回答 B 的询问。

step 3. B 利用 X_A，通过 $\mathscr{P}\langle G,X,X'\rangle$ 求得到 $X'_A=\{x'_i\}$，利用 $\{x'_i\}$ 将半密文 c'_k 还原解密成明文 $m_k\in M$：

$$m_k=\bigoplus_{x'_i\in X'_A}(\bigoplus_{j=1,x_j\in X_B}^{m}(c_k))。\tag{3.6}$$

step 4. A 向 B 声明，$X'_A=\{x'_i\}$ 作废，A 丢弃 $\{x'_i\}$。

step 5. END

4　生成锁 $\mathscr{P}\langle G,X,X'\rangle$ 与多齿中央加密系统

考虑到信息的安全，防止对密文 C_i 的破解与攻击，本节对上一节的讨论加以推广；在本节中，X'_A 是一个单元素集合 $\{x'_i\}$，在下面的讨论中，$X'_A=\{x'_1, x'_2, \cdots, x'_\alpha\}$。

定理 4.1　（数位签章唯一性第 1 定理）设 $\varphi\langle X,X'\rangle$ 是打开 $\mathscr{P}\langle G,X,X'\rangle$ 的钥匙，X 和 X' 分别是 $\varphi\langle X,X'\rangle$ 的毛坯和牙齿集，$|X'|$ 和 $|X''|$ 是毛坯 X 的两个牙齿数，若 $|X'|\neq|X''|$，$\forall m_j\in M$ 满足

$$c_j\neq c'_k,\tag{4.1}$$

其中：$c_j=X'\oplus m_j$，$c'_k=X''\oplus m_j$，c_j，c'_j 分别是明文 m_j 的两个数位签章。

证明：给定 $X=\{x_1, x_2, \cdots, x_n\}$，$\forall x_j\in N^+$；由 2 中的 (2.1) - (2.2) 可以得到 X'，X''；$X'=\text{int}\{x'_1,x'_2, \cdots, x'_p\}$，$X''=\text{int}\{x''_1, x''_2, \cdots, x''_q\}$，令 $p<q$，p，$q\in N^+$，则有 $|X'|\neq|X''|$，对同一个 $m_j\in M$，则有

$$c_j=X'\oplus m_j\neq X''\oplus m_j=c'_j\tag{4.2}$$

例如：$|X'|=4$，$|X''|=7$，$|X|=\text{int}\{x'_1,x'_2,x'_3,x'_4\}=\{2,3,7,9\}$，$X''=\text{int}\{x''_1,x''_2,x''_3,x''_4,x''_5,x''_6,x''_7\}=\{2,3,7,9,10,12,14\}$，$m_j=108$，则有 $X'\oplus m_j\neq X''\oplus m_j$，$c_j=\{2,3,7,9\}\oplus\{108\}\neq\{2,3,7,9,10,12,14\}\oplus\{108\}=c''_j$。对于给定的 $|X'|$，则明文 m_j 的数位签章 c'_j 是唯一的。数位签章的唯一性在生成锁 $\mathscr{P}\langle G,X,X'\rangle$ 和它的中央加密系统中具有重要意义。

定理 4.2（数位签章唯一性第 2 定理）设 $\varphi\langle X,X'\rangle$ 是打开 $\mathscr{P}\langle G,X,X'\rangle$ 的钥匙，X 是 $\varphi\langle X,X'\rangle$ 的毛坯，X'，X''是两个牙齿集，$|X'|$，$|X''|$是毛坯 X 的两个牙齿数，若 $|X'|=|X''|$，$X'\neq X''$，则 $\forall m_j\in M$ 满足

$$c_j\neq c'_j\tag{4.3}$$

定理 4.2 由定理 4.1 得到。

A，B 各自选取 $\varphi\langle X, X'\rangle$ 的毛坯 $X_A=\{x_1,x_2,\cdots,x_n\}$ 和 $X_B=\{x_1,x_2,\cdots,x_m\}$，$m\geqslant4$，$n\geqslant4$；$\forall x_i\in X_A$，$\forall x_j\in X_B$，$x_i$，$x_j\in N^+$；$X_A$，$X_B$ 公开于 A，B 的双方。A 和 B 各自选取 $\varphi\langle X, X'\rangle$ 的齿数 $|X'_A|$ 和 $|X'_B|$，$X'_A=\{x'_1,x'_2,\cdots,x'_\alpha\}$，$X'_B=\{x'_1,x'_2,\cdots,x'_\beta\}$，$M$ 是明文 m_j 的集合，$M=\{m_1,m_2,\cdots,m_t\}$。A 对 X'_A，B 对 X'_B 各自严格保密。

4.1　多齿中央静态加密系统与加密—解密算法

4.1.1　A 关于 B 的多齿中央静态加密系统的加密算法

step 1. A 向中央加密系统提出与 B 通讯的申请，并得到确认。

step 2. A 利用 $X_A=\{x_1, x_2, \cdots, x_n\}$ 和 $\mathcal{P}\langle G, X, X'\rangle$，$A$ 秘密选取 $X'_A=\text{int}\{x'_1, x'_2, \cdots, x'_\alpha\}=\{x'_1, x'_2, \cdots, x'_\alpha\}$。

step 3. 对于给定的明文 $m_k\in M$，A 利用 X'_A 将 m_k 半加密成密文 c'_k（A 对 m_k 数位签章）。

$$c'_k=\bigoplus_{x'_i\in X'_A, i=1,2,\cdots,\alpha}\{x'_i\}m_k \tag{4.4}$$

step 4. A 利用 X_B 将 c'_k 加密成全密文 c_k

$$c_k=\bigoplus_{x_j\in X_B, j=1,2,\cdots,m}\{x_j\}c'_k=\bigoplus_{j=1, x_j\in X_B}^{m}\left(\bigoplus_{i=1, x'_i\in X'_A}^{\alpha}(m_k)\right)。 \tag{4.5}$$

step 5. 中央系统把密文 c_k 送给 B。

step 6. END

4.1.2 B 关于 A 的多齿中央静态加密系统的解密算法

step 1. B 利用 X_B 对密文 c_k 还原解密得到 c'_k

$$c'_k=\bigoplus_{j=1, x_j\in X_B}^{m}(c_k)。 \tag{4.6}$$

step 2. B 询问 A，$|X'_A|=?$，A 回答并给出一个集合 $\bar{X}=\{1, 2, \cdots, \alpha\}$，用信封把 $\bar{X}$ 装入并封口，将信送于 B。

step 3. B 利用 $\bar{X}$ 和 X_A 通过 $\mathcal{P}\langle G, X, X'\rangle$ 得到 $X'_A=\text{int}\{x'_1, x'_2, \cdots, x'_\alpha\}$，$B$ 对 c'_k 还原解密，得到明文 m_k。

$$m_k=\bigoplus_{i=1, x'_i\in X'_A}^{\alpha}\left(\bigoplus_{j=1, x_j\in X_B}^{m}(C_k)\right)。 \tag{4.7}$$

step 4. A 向 B 声明，A 的秘密钥匙 $X'_A=\{x'_1, x'_2, \cdots, x'_\alpha\}$ 作废，A 丢弃 X'_A

step 5. END

4.2 多齿中央动态加密系统与加密—解算算法

4.2.1 A 关于 B 的多齿中央动态加密系统的加密算法

step 1. A 向中央加密系统提出与 B 通讯的申请，并得到确认。

step 2. A 利用 $X_A=\{x_1, x_2, \cdots, x_n\}$ 和 $\mathcal{P}\langle G, X, X'\rangle$，$A$ 秘密选取 $X'_A=\text{int}\{x'_1, x'_2, \cdots, x'_\alpha\}=\{x'_1, x'_2, \cdots, x'_\alpha\}$。

step 3. A 选取一个规则 f，将 X'_A 变换成一个新的 $X'_{f(A)}=\{f_1, f_2, \cdots, f_\alpha\}$，$f$ 是秘密的。

step 4. 对于给定的明文 $m_k\in M$，A 利用 $X'_{f(A)}$ 将 m_k 半加密成密文 c'_k（A 对 m_k 数位签章）

$$c'_k=\bigoplus_{f_i\in X'_{f(A)}, i=1,2,\cdots,\alpha}\{f_i\}m_k。 \tag{4.8}$$

step 5. A 利用 f 将 X_B 变换成新的 $X_{f(B)}=\{f'_1, f'_2, \cdots, f'_m\}$，利用 $X_{f(B)}$ 将 c'_k 加密成全密文 c_k。

$$c_k=\bigoplus_{f'_j\in X_{f(B)}, j=1,2,\cdots,m}\{f'_j\}c'_k=\bigoplus_{j=1, f'_j\in X_{f(B)}}^{m}\left(\bigoplus_{i=1, f_i\in X'_{f(A)}}^{\alpha}(m_k)\right)。 \tag{4.9}$$

step 6. 中央系统把密文 c_k 送给 B。

step 7. END。

4.2.2 B 关于 A 的多齿中央动态加密系统的解密算法

step 1. B 向 A 询问规则 f，$|X'_A|=?$ A 给出回答；将 f，$|X'_A|$ 装入信封，对信封封口并送于 B。

step 2. 利用 f，B 将 X_B 变换成新的 $X_{f(B)}=\{f'_1, f'_2, \cdots, f'_m\}$，对密文 c_k 还原解密得到 c'_k。

$$c'_k=\bigoplus_{j=1, f'_j\in X_{f(B)}}^{m}(c_k)。 \tag{4.10}$$

step 3. B 利用 $|X_A|$ 和 X_A，通过 $\mathcal{P}\langle G, X, X'\rangle$ 得到 $X'_A=\{x'_1, x'_2, \cdots, x'_\alpha\}$；$B$ 利用 f 对 X'_A 变换成 $X'_{f(A)}$。

step 4. B 利用 $X'_{f(A)}$ 将密文 c'_k 还原解密，得到明文 m_k。

$$m_k=\bigoplus_{i=1, f_i\in X'_{f(A)}}^{\alpha}\left(\bigoplus_{j=1, f'_j\in X_{f(B)}}^{m}(c_k)\right)。 \tag{4.11}$$

step 5. A 向 B 声明，X'_A 和规则 f 作废，A 丢弃 X'_A 和规则 f。

step 6. END。

在本节中，我们给出一个规则 f，利用 f 将 X'_A 变换成 $X'_{f(A)}$，目的是保证 X'_A 的安全。假若 X'_A 被盗取，X'_A 对盗取者是无意义的。反之，利用 f 将 X'_B 进行变换也是保证 X'_B 的安全。显然，规则 f 可以很容易找到。

4.3 多齿中央静态加密与多齿中央动态加密的意义和区别

1）在静态加密系统中，$X'_A=\{x'_1, x'_2, \cdots, x'_\alpha\}$ 是 A 的秘密钥匙，在对明文的 $m_j\in M$ 进行半加密（A 对 m_j 数位签章）中，X'_A 的形式没有发生变化，或者说 A 的秘密钥匙 X'_A 和在加密中的 X'_A 是一样的，它们之间保持相对静止状态。

2）在动态加密系统中，$X'_A=\{x'_1, x'_2, \cdots, x'_\alpha\}$ 是 A 的秘密钥匙。为了防止 X'_A 盗取或复制，X'_A 并不直接应用于明文 $m_j\in M$ 的加密，只

是一个虚设。A 利用规则 f，将 X'_A 变换成一个新的 $X'_{f(A)}$ 应用于明文 $m_j \in M$ 的加密。显然，$X'_{f(A)}$ 的形式相对 X'_A 是变化的，他们之间保持动态关系 f，f 的选择具有一个很大的自由空间，在应用中对于同一个明文文件，可以选择一个或多个 f。

5 $\mathscr{P}\langle G, X, X'\rangle$ 和它的中央加密系统的结构与特性

5.1 P〈G, X, X′〉构成的中央加密系统的结构关系

1）公开/秘密钥匙配制：$X_A = \{x_1, x_2, \cdots, x_n\}$，$X_B = \{x_1, x_2, \cdots, x_m\}$，$X'_A = \{x'_1, x'_2, \cdots, x'_\alpha\}$，$X'_B = \{x'_1, x'_2, \cdots, x'_\beta\}$，$\varphi\langle X_A, X'_A\rangle$，$\varphi\langle X_B, X'_B\rangle$。

2）构造 $X_A \times X_A$ 上的关系 f。

3）$\mathscr{P}\langle G, X, X'\rangle$ 生成中央系统。

4）加密输出 $C_k = \mathscr{P}\langle G, X, X'\rangle(m_k) = X_{f(B)} \oplus (X'_{f(A)} \oplus m_k)$

其中：$X_{f(B)} = f(X_B)$，$X'_{f(A)} = f(X'_A)$。

5.2 P〈G, X, X′〉构成的中央加密系统特性

1）秘密钥匙的一次有效特性

无论 A 将明文 m_j 加密成密文 c_j 将 c_j 送于 B，或者 B 将明文 m_i 加密成密文 c_i 将 c_i 送于 A；A，B 的各自秘密钥匙 X'_A, X'_B（或者 $X'_{f(A)}, X'_{f(B)}$）只使用一次，在密文 c_j 送给对方之后，X'_A, X'_B（或者 $X'_{f(A)}, X'_{f(B)}$）被废除，新的 X'_A, X'_B（或者 $X'_{f(A)}, X'_{f(B)}$）被 A，B 各自秘密选用。

2）秘密钥匙选择的非唯一性

无论 A 或者 B，只要选择公开钥匙 X_A 或者 X_B，通过中央系统各自得到 $X'_A = \{x'_1, x'_2, \cdots, x'_\alpha\}$ 和 $X'_B = \{x'_1, x'_2, \cdots, x'_\beta\}$ 若干个秘密钥匙。

3)公开-秘密钥匙的非静态特性

A 和 B 的公开钥匙 X_A, X_B，秘密钥匙 X'_A, X'_B 都是以集合为定义的。根据一般的数学理论，在集合 X_A（或者 X_B）上定义一个变换或规则 f 使 X_A（X_B）变成新的 $X_{f(A)}$（$X_{f(B)}$）。同理，X'_A, X'_B 变成新的 $X'_{f(A)}$，$X'_{f(B)}$。即 $X_A \xrightarrow{f} X_{f(A)}$，$X_B \xrightarrow{f} X_{f(B)}$，$X'_A \xrightarrow{f} X'_{f(A)}$，$X'_B \xrightarrow{f} X'_{f(B)}$。由于 f 的选取是非唯一的，上述过程是一个动态过程。公开钥匙、秘密钥匙的非静态特性应用于中央加密系统，给密文的攻击者制造了障碍。

4）秘密钥匙曝光滞后特性

在 3，4 的算法中，B 接到密文后都要毫无例外要求 A 给出回答 $|X'_A|$，然后 B 利用 A 的公开钥匙算出 A 的秘密钥匙 X'_A，使密文解密成明文，显然，A 的秘密钥匙 X'_A 已经曝光于 B。事实上，这种曝光对于 X'_A 的存在已失去意义。在这之前，A 已利用 X'_A 完成对明文的半加密（数位签章），由于秘密钥匙的一次有效特性，在 A 的秘密钥匙库中，X'_A 被废除，永远不会再被采用。

参考文献

[1] Diffie W, Hellman M E. New directions in cryptography, IEEE transactions on information theory, 1976, 1T-22 (6): 644～654

[2] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key CryptoSystem, communication of the associaation for computing machinery, 1978, 21 (2): 120～126

[3] Deng J L. Control problems of gray system, systems and control letters, 1982, 1 (5): 285～294

[4] Deng J L. Introduction to gray system theory, the journal of gray system, 1989, 1 (1): 1～19

[5] 史开泉. 灰色信息关系理论 [M]. 中国台北：全华科技图书出版公司，1994.12～54

[6] Cai W. Introduction of extension sets, BUSEFAL, 1984, (19): 49～57

The Generating Lock $\mathscr{P}\langle G, X, X'\rangle$ and Its Central Encrypting System

Shi Kaiquan[1], Chen Zexiong[2]

(1. *Department of Automation Engineering, Shandong University of Technology, Shandong Jinan* 250061, *China*; 2. *Department of Computer Science and Information Engineering, Dayeh University, Chang hua Taiwan* 51505, *China*)

[**Abstract**] The conception of the generating lock $\mathscr{P}\langle G,X,X'\rangle$ and the central encrypting system composed of $\mathscr{P}\langle G,X,X'\rangle$ with data generating technology are proposed in this paper[3~6]. These systems include the generating lock $\mathscr{P}\langle G,X,X'\rangle$ and single-tooth central encrypting system, and the generating lock $\mathscr{P}\langle G,X,X'\rangle$ and multi-tooth central encrypting system. The single-tooth encrypting-decrypting algorithm multi-tooth encrypting-decrypting algorithm, multi-tooth static encrypting-decrypting algorithm, multi-tooth dynamic encrypting-decrypting algorithm as well as the structure character of central encrypting system are provided. The paper points out that arbitrary two persons A and B can choose irregular distributed positive integer sets, $X_A=\{x_1,x_2,\cdots,x_n\}$, $X_B=\{x_1,x_2,\cdots,x_m\}$, $m\geqslant 4$, $n\geqslant 4$, $X_A\neq X_B$, respectively and complete their secret communication with $\mathscr{P}\langle G,X,X'\rangle$. The experiment result shows that the method proposed has good application character and security character.

[**Key words**] the generating lock; the central encrypting system; multi-tooth encrypting-decrypting algorithm; $\mathscr{P}\langle G,X,X'\rangle$ existence theorem; digital signature uniqueness theorem

我国低温超导 NbTi 合金材料制备工艺独持

[**本刊讯**] 铌钛超导合金广泛应用于高能物理加速器、磁悬浮列车、核磁共振成像仪等高科技产品领域。NbTi 超导合金锭、棒更是一种技术含量高的产品，其国际市场一直为美国华昌公司所垄断。

目前，我国西北有色金属研究院已研制成功能制备高质量 NbTi 合金锭、棒的新工艺。该工艺不同于美国华昌公司，具有独自的创新工艺特色，在提高 NbTi 合金锭、棒质量方面处于国际先进水平。西北有色金属研究院研制成功高质量、低成本的 NbTi 超导合金锭、棒，对 NbTi 超导体的应用及相关领域的发展，尤其对高新技术产业化具有非常重要的意义。

美国华昌公司采用粉末冶金和电弧熔的方法制备 NbTi 锭、棒，其成分均匀性高并可大批量生产；西北有色金属研究的方法同样也可以小批量生产与华昌公司同一标准的高质量 NbTi 锭、棒，尤其是杂质氧含量非常低，其 NbTi 超导线的 Jc 曾创国际最高水平。

* * *