高校应用数学学报
2025, 40(3): 281-293

Markov矩阵的广义可逆性

陆成刚

(浙江工业大学 数学科学学院, 浙江杭州 310023)

摘　要: 对不确定性的输入输出系统, 考虑输入和输出随机变量的概率分布矢量之间的状态转移概率矩阵(即Markov矩阵)的存在性以及唯一性和可逆性, 并且其中的广义可逆性与一次一密理论及公钥密码系统的安全性的一致性关系. 将Markov矩阵视作通信信道, 则当信道容量非零, 则Markov矩阵存在且不唯一且秩不小于2以及不存在广义逆; 当信道容量为零, 则Markov矩阵存在以及唯一且其秩为1, 存在广义逆. 尤其, 当输入输出均为等概率分布时, Markov矩阵存在Moore-Penrose广义逆, 更进一步, 当输入输出的状态数目一致, 则输入或输出的概率分布为该Markov矩阵的平衡态分布. 并且存在广义逆的Markov矩阵恰是公私钥密码体制的非对称加解密的信道, 结合RSA和Elgamal算法给出了正反两方面的示例.

关键词: Markov矩阵; Moore-Penrose广义逆; 一次一密; 公私钥密码体制; RSA算法; Elgamal算法

中图分类号: TN918

文献标识码: A　　**文章编号**: 1000-4424(2025)03-0281-13

§1　引　言

Markov模型的可逆性是一个重要的概念, 在分子热动力学、Monte Carlo模拟、基因工程和网络队列理论中有着广泛的应用[1-2]. Markov模型的可逆性涉及到Markov矩阵的平衡态概率分布的研究, Markov矩阵本身的可逆并没有相关研究工作涉及, 而且即使Markov矩阵存在标准逆, 其逆一般也不是概率矩阵. 然而, 在一类涉及到随机性的输入输出系统中, 对Markov矩阵的可逆性研究有着显著的意义, 并且一定程度上和Markov模型的可逆性相关. 例如, 从由输入到输出的概率矩阵计算出由输出到输入的概率矩阵, 只要满足$p_i\tau_{ji} = q_j s_{ij}$, 这也是Markov模型可逆性的细致平衡方程. 本文所涉的输入输出系统的含义十分广泛, 通信系统、加密系统、存储系统、数据压缩过程、机器学习、甚至基因遗传系统, 等等, 在输入输出框架下, 考虑不确定性因素的影响, 对其中的状态转移概率矩阵的可逆问题的研究, 发现存在广义可逆性和信道容量为零有确定的关系, 本文以公钥密码系统的Elgamal算法和RSA算法[3-5]为应用案例进行了分析, 同时也对传统的一次一密理论作了更进一步的推广[6-7]. §2阐述并列出有关Markov矩阵可逆性的

收稿日期: 2024-08-08　　修回日期: 2025-07-01
基金项目: 浙江重点研发计划: 2022年度“领雁”研发攻关计划(2022C01084)

一些研究结果, 然后在一次一密理论的推广应用(§3)以及公私钥密码系统的案例分析(§4)中进行展开, §5是总结与展望.

§2 Markov矩阵的存在唯一性和可逆性

离散随机变量X和Y分别是输入矢量和输出矢量, 且属于两个不同的概率空间$(\Omega_\chi, F_\chi, P_\chi)$和$(\Omega_Y, F_Y, P_Y)$, 它们的分布分别为$P(X)=\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ p_1 & p_2 & \cdots & p_n \end{pmatrix}$, 且$p_1+p_2+\cdots+p_n=1$, 概率分布矢量为$(p_1 \quad p_2 \quad \cdots \quad p_n)^{\mathrm{T}}$; 以及$P(Y)=\begin{pmatrix} y_1 & y_2 & \cdots & y_m \\ q_1 & q_2 & \cdots & q_m \end{pmatrix}$, 且$q_1+q_2+\cdots+q_m=1$, 概率分布矢量为$(q_1 \quad q_2 \quad \cdots \quad q_m)^{\mathrm{T}}$, 其中$n=|\Omega_\chi|, m=|\Omega_Y|$. 随机变量$X$到$Y$的Markov矩阵或状态转移概率矩阵为

$$P(Y|X)=\begin{pmatrix} \tau_{11} & \tau_{21} & \cdots & \tau_{m1} \\ \tau_{12} & \tau_{22} & \cdots & \tau_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ \tau_{1n} & \tau_{2n} & \cdots & \tau_{mn} \end{pmatrix}. \tag{1}$$

式(1)中$\tau_{ji}=p(Y=y_j|X=x_i)$. 如从X到Y间由确定映射定义, 那么$(\tau_{1i} \quad \tau_{2i} \quad \cdots \quad \tau_{mi})$皆为形如$(\cdots 0 \quad 1 \quad 0 \quad \cdots)$的含一个1其余皆零的向量. 随机变量$X$和$Y$的概率分布满足

$$\begin{pmatrix} q_1 \\ q_2 \\ \vdots \\ q_m \end{pmatrix}=\begin{pmatrix} \tau_{11} & \tau_{21} & \cdots & \tau_{m1} \\ \tau_{12} & \tau_{22} & \cdots & \tau_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ \tau_{1n} & \tau_{2n} & \cdots & \tau_{mn} \end{pmatrix}^{\mathrm{T}}\begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix}. \tag{2}$$

随机变量Y到X的转移概率矩阵为

$$P(X|Y)=\begin{pmatrix} s_{11} & s_{21} & \cdots & s_{n1} \\ s_{12} & s_{22} & \cdots & s_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ s_{1m} & s_{2m} & \cdots & s_{nm} \end{pmatrix}. \tag{3}$$

式(3)中$s_{ji}=p(X=x_j|Y=y_i)$. 随机变量X和Y的概率分布又满足

$$\begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix}=\begin{pmatrix} s_{11} & s_{21} & \cdots & s_{n1} \\ s_{12} & s_{22} & \cdots & s_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ s_{1m} & s_{2m} & \cdots & s_{nm} \end{pmatrix}^{\mathrm{T}}\begin{pmatrix} q_1 \\ q_2 \\ \vdots \\ q_m \end{pmatrix}. \tag{4}$$

由式(2)和(4)得到

$$\begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix}=\begin{pmatrix} s_{11} & s_{21} & \cdots & s_{n1} \\ s_{12} & s_{22} & \cdots & s_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ s_{1m} & s_{2m} & \cdots & s_{nm} \end{pmatrix}^{\mathrm{T}}\begin{pmatrix} \tau_{11} & \tau_{21} & \cdots & \tau_{m1} \\ \tau_{12} & \tau_{22} & \cdots & \tau_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ \tau_{1n} & \tau_{2n} & \cdots & \tau_{mn} \end{pmatrix}^{\mathrm{T}}\begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix} \tag{5}$$

以及

$$\begin{pmatrix} q_1 \\ q_2 \\ \vdots \\ q_m \end{pmatrix} = \begin{pmatrix} \tau_{11} & \tau_{21} & \cdots & \tau_{m1} \\ \tau_{12} & \tau_{22} & \cdots & \tau_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ \tau_{1n} & \tau_{2n} & \cdots & \tau_{mn} \end{pmatrix}^{\mathrm{T}} \begin{pmatrix} s_{11} & s_{21} & \cdots & s_{n1} \\ s_{12} & s_{22} & \cdots & s_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ s_{1m} & s_{2m} & \cdots & s_{nm} \end{pmatrix}^{\mathrm{T}} \begin{pmatrix} q_1 \\ q_2 \\ \vdots \\ q_m \end{pmatrix}. \tag{6}$$

进一步得到

$$\begin{pmatrix} s_{11} & s_{21} & \cdots & s_{n1} \\ s_{12} & s_{22} & \cdots & s_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ s_{1m} & s_{2m} & \cdots & s_{nm} \end{pmatrix}^{\mathrm{T}} \begin{pmatrix} q_1 \\ q_2 \\ \vdots \\ q_m \end{pmatrix} = \begin{pmatrix} s_{11} & s_{21} & \cdots & s_{n1} \\ s_{12} & s_{22} & \cdots & s_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ s_{1m} & s_{2m} & \cdots & s_{nm} \end{pmatrix}^{\mathrm{T}} \begin{pmatrix} \tau_{11} & \tau_{21} & \cdots & \tau_{m1} \\ \tau_{12} & \tau_{22} & \cdots & \tau_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ \tau_{1n} & \tau_{2n} & \cdots & \tau_{mn} \end{pmatrix}^{\mathrm{T}} \times \begin{pmatrix} s_{11} & s_{21} & \cdots & s_{n1} \\ s_{12} & s_{22} & \cdots & s_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ s_{1m} & s_{2m} & \cdots & s_{nm} \end{pmatrix}^{\mathrm{T}} \begin{pmatrix} q_1 \\ q_2 \\ \vdots \\ q_m \end{pmatrix} \tag{7}$$

和

$$\begin{pmatrix} \tau_{11} & \tau_{21} & \cdots & \tau_{m1} \\ \tau_{12} & \tau_{22} & \cdots & \tau_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ \tau_{1n} & \tau_{2n} & \cdots & \tau_{mn} \end{pmatrix}^{\mathrm{T}} \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix} = \begin{pmatrix} \tau_{11} & \tau_{21} & \cdots & \tau_{m1} \\ \tau_{12} & \tau_{22} & \cdots & \tau_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ \tau_{1n} & \tau_{2n} & \cdots & \tau_{mn} \end{pmatrix}^{\mathrm{T}} \begin{pmatrix} s_{11} & s_{21} & \cdots & s_{n1} \\ s_{12} & s_{22} & \cdots & s_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ s_{1m} & s_{2m} & \cdots & s_{nm} \end{pmatrix}^{\mathrm{T}} \times \begin{pmatrix} \tau_{11} & \tau_{21} & \cdots & \tau_{m1} \\ \tau_{12} & \tau_{22} & \cdots & \tau_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ \tau_{1n} & \tau_{2n} & \cdots & \tau_{mn} \end{pmatrix}^{\mathrm{T}} \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix}, \tag{8}$$

式(7)和(8)是仿Moore-Penrose广义逆的第一和第二条件而列. 转移概率矩阵$P(Y|X)$和$P(X|Y)$须满足如下的联合概率交换法则约束, 即

$$\begin{aligned} \tau_{ji}p_i = p(Y = y_j|X = x_i)p(X = x_i) = p(Y = y_j, X = x_i) = \\ p(X = x_i|Y = y_j)p(Y = y_j) = s_{ij}q_j, \quad \forall i = 1, 2, \cdots, n; j = 1, 2, \cdots, m. \end{aligned} \tag{9}$$

如果随机变量X,Y的概率分布$P(X)$和$P(Y)$, 转移概率矩阵$P(Y|X)$和$P(X|Y)$, 满足式(2), (4)和(9), 则称X和Y间存在一个信道, 记作$\langle X,Y\rangle$.

显然, 对于信道, 可由式(2), (4)和(9)得到它的互信息(或信道容量, 即互信息的最大值)的计算式

$$I(X;Y)=\sum_{j=1}^{m}\sum_{i=1}^{n}p(X=x_i,Y=y_j)\log\frac{p(X=x_i,Y=y_j)}{p(X=x_i)p(Y=y_j)}= \\ H(Y)-H(Y|X)=H(X)-H(X|Y), \tag{10}$$

即互信息可以由两侧分别计算, 并且它们的值相等. 下面证明对于任意的输入输出的离散随机变量一定存在它们之间的转移概率矩阵, 这就是定理1.

定理1 设离散随机变量X服从分布$P(X)=\begin{pmatrix}x_1 & x_2 & \cdots & x_n\\ p_1 & p_2 & \cdots & p_n\end{pmatrix}$且$p_1+p_2+\cdots+p_n=1$; Y服从分布$P(Y)=\begin{pmatrix}y_1 & y_2 & \cdots & y_m\\ q_1 & q_2 & \cdots & q_m\end{pmatrix}$且$q_1+q_2+\cdots+q_m=1$, 则一定存在信道$\langle X,Y\rangle$.

证 首先由

$$\begin{pmatrix}p_1\\ p_2\\ \vdots\\ p_n\end{pmatrix}=\begin{pmatrix}p_1 & p_1 & \cdots & p_1\\ p_2 & p_2 & \cdots & p_2\\ \vdots & \vdots & \ddots & \vdots\\ p_n & p_n & \cdots & p_n\end{pmatrix}_{n\times m}\begin{pmatrix}q_1\\ q_2\\ \vdots\\ q_m\end{pmatrix} \tag{11}$$

以及

$$\begin{pmatrix}q_1\\ q_2\\ \vdots\\ q_m\end{pmatrix}=\begin{pmatrix}q_1 & q_1 & \cdots & q_1\\ q_2 & q_2 & \cdots & q_2\\ \vdots & \vdots & \ddots & \vdots\\ q_m & q_m & \cdots & q_m\end{pmatrix}_{m\times n}\begin{pmatrix}p_1\\ p_2\\ \vdots\\ p_n\end{pmatrix}, \tag{12}$$

可令

$$P(Y|X)=\begin{pmatrix}q_1 & q_1 & \cdots & q_1\\ q_2 & q_2 & \cdots & q_2\\ \vdots & \vdots & \ddots & \vdots\\ q_m & q_m & \cdots & q_m\end{pmatrix}^{\mathrm{T}}_{m\times n} \tag{13}$$

和

$$P(X|Y)=\begin{pmatrix}p_1 & p_1 & \cdots & p_1\\ p_2 & p_2 & \cdots & p_2\\ \vdots & \vdots & \ddots & \vdots\\ p_n & p_n & \cdots & p_n\end{pmatrix}^{\mathrm{T}}_{n\times m}. \tag{14}$$

最后验证满足联合概率交换法则(9),

$$q_jp_i=p(Y=y_j|X=x_i)p(X=x_i)=p(Y=y_j,X=x_i)= \\ p(X=x_i|Y=y_j)p(Y=y_j)=p_iq_j,\quad \forall i=1,2,\cdots,n;j=1,2,\cdots,m. \tag{15}$$

所以信道$\langle X,Y\rangle$存在. 证毕. 后文会讨论定理1构造的信道$\langle X,Y\rangle$的信道容量为零.

很自然地要问任意一对随机变量间是否存在非零容量的信道? 回答是肯定的, 下面从二元

信道角度分析. 即令$m=n=2$, 当X和Y的分布给定时, X和Y之间存在无穷多个的信道, 既有信道容量为零的信道, 也有容量非零的信道.

定理2 离散随机变量X服从分布$P(X)=\begin{pmatrix}X=0 & X=1\\ p_0 & p_1\end{pmatrix}$且$p_0+p_1=1$; Y服从分布$P(Y)=\begin{pmatrix}Y=0 & Y=1\\ q_0 & q_1\end{pmatrix}$且$q_0+q_1=1$, 则存在如式(16)和(17)转移概率矩阵的信道$\langle X,Y\rangle$.

$$P(Y|X)=\begin{pmatrix}1-k & \frac{q_0-(1-k)p_0}{p_1}\\ k & \frac{q_1-kp_0}{p_1}\end{pmatrix}^{\mathrm{T}}, \tag{16}$$

$$P(X|Y)=\begin{pmatrix}(1-k)\frac{p_0}{q_0} & \frac{kp_0}{q_1}\\ 1-(1-k)\frac{p_0}{q_0} & 1-\frac{kp_0}{q_1}\end{pmatrix}^{\mathrm{T}}, \tag{17}$$

其中$0<k\le\min\{1,\frac{q_1}{p_0}\}$且$0<1-k\le\frac{q_0}{p_0}$.

证 根据$0<k\le\min\{1,\frac{q_1}{p_0}\}$及$0<1-k\le\frac{q_0}{p_0}$知道转移概率矩阵$P(Y|X)$和$P(X|Y)$的每个元素均是介于0到1的概率值, 且每一行均为一固定条件的概率分布, 只要验证它们满足式(2), (4)和(9). 首先

$$\begin{pmatrix}q_0\\ q_1\end{pmatrix}=\begin{pmatrix}1-k & \frac{q_0-(1-k)p_0}{p_1}\\ k & \frac{q_1-kp_0}{p_1}\end{pmatrix}\begin{pmatrix}p_0\\ p_1\end{pmatrix};\begin{pmatrix}p_0\\ p_1\end{pmatrix}=\begin{pmatrix}(1-k)\frac{p_0}{q_0} & \frac{kp_0}{q_1}\\ 1-(1-k)\frac{p_0}{q_0} & 1-\frac{kp_0}{q_1}\end{pmatrix}\begin{pmatrix}q_0\\ q_1\end{pmatrix}. \tag{18}$$

其次验证得$P(X=0,Y=0)=P(Y=0|X=0)P(X=0)=(1-k)p_0=(1-k)\frac{p_0}{q_0}q_0=P(X=0|Y=0)P(Y=0)$. 同理可以验证$P(X=0,Y=1)$, $P(x=1,Y=0)$和$P(x=1,Y=1)$的类似上述的式子, 所以满足条件式(9).

定理2中构造的信道的互信息为

$$\begin{aligned}I(X;Y)=H(X)-H(X|Y)=-p_0\log p_0-p_1\log p_1+\\ \{q_0[\frac{1-kp_0}{q_0}]\log\frac{1-kp_0}{q_0}+(1-\frac{1-kp_0}{q_0})\log(1-\frac{1-kp_0}{q_0})]+\\ q_1[\frac{kp_0}{q_1}\log\frac{kp_0}{q_1}+(1-\frac{kp_0}{q_1})\log(1-\frac{kp_0}{q_1})]\},\end{aligned} \tag{19}$$

它一般不为零, 所以信道容量也不为零.

定理3 离散随机变量X服从分布$P(X)=\begin{pmatrix}x_1 & x_2 & \cdots & x_n\\ p_1 & p_2 & \cdots & p_n\end{pmatrix}$且$p_1+p_2+\cdots+p_n=1$; 且由$X$到$Y$的转移概率矩阵

$$P(Y|X)=\begin{pmatrix}\tau_{11} & \tau_{21} & \cdots & \tau_{m1}\\ \tau_{12} & \tau_{22} & \cdots & \tau_{m2}\\ \vdots & \vdots & \ddots & \vdots\\ \tau_{1n} & \tau_{2n} & \cdots & \tau_{mn}\end{pmatrix}, \tag{20}$$

则$P(X)$及$P(Y|X)$确定了唯一的信道, 其中Y服从分布$P(Y)=\begin{pmatrix}q_1\\ q_2\\ \vdots\\ q_m\end{pmatrix}=\begin{pmatrix}\sum_{j=1}^{n}\tau_{1j}p_j\\ \sum_{j=1}^{n}\tau_{2j}p_j\\ \vdots\\ \sum_{j=1}^{n}\tau_{mj}p_j\end{pmatrix}$, 而从$Y$到$X$的转移概率矩阵为

$$P(X|Y)=\begin{pmatrix}s_{11} & s_{21} & \cdots & s_{n1}\\ s_{12} & s_{22} & \cdots & s_{n2}\\ \vdots & \vdots & \ddots & \vdots\\ s_{1m} & s_{2m} & \cdots & s_{nm}\end{pmatrix}, \tag{21}$$

其中$s_{ij}=\dfrac{\tau_{ji}p_i}{q_j}=\dfrac{\tau_{ji}p_i}{\sum_{t=1}^{n}\tau_{jt}p_t}$. 即当$X$分布及$X$到$Y$的转移条件概率分布已知时, X和Y间存在着唯一确定的信道.

证 首先

$$P(Y)=\begin{pmatrix}q_1\\q_2\\\vdots\\q_m\end{pmatrix}=\begin{pmatrix}\tau_{11}&\tau_{21}&\cdots&\tau_{m1}\\\tau_{12}&\tau_{22}&\cdots&\tau_{m2}\\\vdots&\vdots&\ddots&\vdots\\\tau_{1n}&\tau_{2n}&\cdots&\tau_{mn}\end{pmatrix}^{\mathrm{T}}\begin{pmatrix}p_1\\p_2\\\vdots\\p_n\end{pmatrix}=\begin{pmatrix}\sum_{j=1}^{n}\tau_{1j}p_j\\\sum_{j=1}^{n}\tau_{2j}p_j\\\vdots\\\sum_{j=1}^{n}\tau_{mj}p_j\end{pmatrix},\tag{22}$$

其次

$$\begin{pmatrix}p_1\\p_2\\\vdots\\p_n\end{pmatrix}=\begin{pmatrix}s_{11}&s_{21}&\cdots&s_{n1}\\s_{12}&s_{22}&\cdots&s_{n2}\\\vdots&\vdots&\ddots&\vdots\\s_{1m}&s_{2m}&\cdots&s_{nm}\end{pmatrix}^{\mathrm{T}}\begin{pmatrix}q_1\\q_2\\\vdots\\q_m\end{pmatrix}=\begin{pmatrix}\sum_{j=1}^{m}s_{1j}q_j\\\sum_{j=1}^{m}s_{2j}q_j\\\vdots\\\sum_{j=1}^{m}s_{nj}q_j\end{pmatrix}.\tag{23}$$

式(23)中$s_{ij}=\dfrac{\tau_{ji}p_i}{\sum_{t=1}^{n}\tau_{jt}p_t}$, 从而$\sum\limits_{j=1}^{m}s_{ij}q_j=\sum\limits_{j=1}^{m}\dfrac{\tau_{ji}p_i}{\sum_{t=1}^{n}\tau_{jt}p_t}q_j=\sum\limits_{j=1}^{m}\dfrac{\tau_{ji}p_i}{\sum_{t=1}^{n}\tau_{jt}p_t}\sum\limits_{t=1}^{n}\tau_{jt}p_t=\sum\limits_{j=1}^{m}\tau_{ji}p_i=p_i$. 最后验证满足联合概率交换法则

$$\begin{aligned}\tau_{ji}pi=p(Y=y_j|X=x_i)p(X=x_i)=p(X=x_i,Y=y_j)=\\p(X=x_i|Y=y_j)p(Y=y_j)=s_{ij}q_j.\end{aligned}\tag{24}$$

另外在此信道的互信息为

$$H(Y)-H(Y|X)=\sum_{i=1}^{m}\sum_{j=1}^{n}\tau_{ij}p_j\log\frac{\tau_{ij}}{\sum_{t=1}^{n}\tau_{it}p_t}.\tag{25}$$

又

$$\begin{aligned}H(X)-H(X|Y)=-\sum_{i=1}^{n}p_i\log p_i+\sum_{j=1}^{m}q_j(\sum_{i=1}^{n}s_{ij}\log s_{ij})=\\-\sum_{i=1}^{n}p_i\log p_i+\sum_{j=1}^{m}\sum_{i=1}^{n}q_js_{ij}\log\frac{\tau_{ji}p_i}{\sum_{t=1}^{n}\tau_{jt}p_t}=\\-\sum_{i=1}^{n}p_i\log p_i+\sum_{j=1}^{m}\sum_{i=1}^{n}q_js_{ij}\log p_i+\sum_{j=1}^{m}\sum_{i=1}^{n}q_js_{ij}\log\frac{\tau_{ji}}{\sum_{t=1}^{n}\tau_{jt}p_t}=\\-\sum_{i=1}^{n}p_i\log p_i+\sum_{j=1}^{m}\sum_{i=1}^{n}\tau_{ji}p_i\log p_i+\sum_{j=1}^{m}\sum_{i=1}^{n}\tau_{ji}p_i\log\frac{\tau_{ji}}{\sum_{t=1}^{n}\tau_{jt}p_t}=\\-\sum_{i=1}^{n}p_i\log p_i+\sum_{i=1}^{n}p_i\log p_i+\sum_{j=1}^{m}\sum_{i=1}^{n}\tau_{ji}p_i\log\frac{\tau_{ji}}{\sum_{t=1}^{n}\tau_{jt}p_t}=\sum_{j=1}^{m}\sum_{i=1}^{n}\tau_{ji}p_i\log\frac{\tau_{ji}}{\sum_{t=1}^{n}\tau_{jt}p_t}.\end{aligned}\tag{26}$$

由式(25)和(26)可见$H(Y)-H(Y|X)=H(X)-H(X|Y)$. 该确定的信道符合两侧计算出的容量等值平衡. 唯一性是显然的.

考虑X到Y的一个确定映射, 假设$m\geq n$, 即$P(Y|X)$的每行$(\tau_{1j}\quad\tau_{2j}\quad\cdots\quad\tau_{mj}),\forall j=1,2,\cdots,n$. 形如$(\cdots\quad 0\quad 1\quad 0\quad\cdots)$含一个1, 其余皆零的单位向量. 此时$H(Y|X)=0$但$H(X|Y)\geq 0$, 自然仍有$H(Y)-H(Y|X)=H(X)-H(X|Y)$. 式(9)保证了信道从两侧计算的容

量等值. 下面给出一个例子因为违背式(9), 导致不满足两侧信道容量等值特性.

例1 X服从分布$P(X)=\begin{pmatrix}X=0 & X=1\\ \frac{1}{3} & \frac{2}{3}\end{pmatrix}$, Y服从分布$P(Y)=\begin{pmatrix}Y=0 & Y=1\\ \frac{7}{12} & \frac{5}{12}\end{pmatrix}$, 而$P(X|Y)$和$P(Y|X)$各自满足, $\begin{pmatrix}7/12\\5/12\end{pmatrix}=\begin{pmatrix}3/4 & 1/2\\1/4 & 1/2\end{pmatrix}\begin{pmatrix}1/3\\2/3\end{pmatrix}$, 又$\begin{pmatrix}1/3\\2/3\end{pmatrix}=\begin{pmatrix}1/6 & 17/30\\5/6 & 13/30\end{pmatrix}\begin{pmatrix}7/12\\5/12\end{pmatrix}$. 但$1/4=(3/4)(1/3)=p(Y=0|X=0)p(X=0)=p(X=0,Y=0)\neq p(X=0|Y=0)p(Y=0)=(1/6)(7/12)=7/72$. 不满足式(9). 此时$H(Y)-H(Y|X)=0.043\neq 0.031=H(X)-H(X|Y)$.

定理1和定理2说明在普遍情况下一般任意一对随机变量之间一定存在一个或多个Markov矩阵, 下面的定理阐述出现唯一性或可逆性的情况.

定理4 设离散随机变量X服从分布$P(X)=\begin{pmatrix}x_1 & x_2 & \cdots & x_n\\ p_1 & p_2 & \cdots & p_n\end{pmatrix}$且$p_1+p_2+\cdots+p_n=1$; Y服从分布$p(Y)=\begin{pmatrix}y_1 & y_2 & \cdots & y_m\\ q_1 & q_2 & \cdots & q_m\end{pmatrix}$ 且$q_1+q_2+\cdots+q_m=1$, 当

$$H\begin{bmatrix}q_1 & q_2 & \cdots & q_m\end{bmatrix}-\sum_{k=1}^{n}p_kH\begin{bmatrix}\tau_{1k} & \tau_{2k} & \cdots & \tau_{mk}\end{bmatrix}>0,$$

从X到Y的Markov矩阵$\begin{pmatrix}\tau_{11} & \tau_{12} & \cdots & \tau_{1n}\\ \tau_{21} & \tau_{22} & \cdots & \tau_{2n}\\ \vdots & \vdots & \ddots & \vdots\\ \tau_{m1} & \tau_{m2} & \cdots & \tau_{mn}\end{pmatrix}$存在, 不唯一, 且秩大于等于2, 不存在广义逆.

当$H\begin{bmatrix}q_1 & q_2 & \cdots & q_m\end{bmatrix}-\sum_{k=1}^{n}p_kH\begin{bmatrix}\tau_{1k} & \tau_{2k} & \cdots & \tau_{mk}\end{bmatrix}=0$, 则$\begin{pmatrix}\tau_{11} & \tau_{12} & \cdots & \tau_{1n}\\ \tau_{21} & \tau_{22} & \cdots & \tau_{2n}\\ \vdots & \vdots & \ddots & \vdots\\ \tau_{m1} & \tau_{m2} & \cdots & \tau_{mn}\end{pmatrix}$存在唯一, 秩为1 且存在广义自反逆(当输入输出为等概率分布时, 存在满足全部条件的Moore-Penrose广义逆); 进一步, 当输入输出的状态数目一致, 而且输入输出为等概率分布时, 输入输出的状态概率分布为该矩阵的稳定态分布.

证 由式(2)可知$(\tau_{1k}\quad \tau_{2k}\quad \cdots\quad \tau_{mk})^{\mathrm{T}}$是固定条件的条件概率分布矢量, $\sum_{j=1}^{m}\tau_{jk}=1$, 因此信息熵为$H\begin{bmatrix}\tau_{1k} & \tau_{2k} & \cdots & \tau_{mk}\end{bmatrix}$. 由式(2)知

$$\begin{pmatrix}q_1\\q_2\\\vdots\\q_m\end{pmatrix}=\sum_{k=1}^{n}p_k\begin{pmatrix}\tau_{1k}\\\tau_{2k}\\\vdots\\\tau_{mk}\end{pmatrix},$$

且熵函数$H\begin{bmatrix}.&.&\cdots&.\end{bmatrix}$为上凸(参见[8]), 利用Jensen不等式得到

$$H\begin{bmatrix}q_1 & q_2 & \cdots & q_m\end{bmatrix}-\sum_{k=1}^{n}p_kH\begin{bmatrix}\tau_{1k} & \tau_{2k} & \cdots & \tau_{mk}\end{bmatrix}\geq 0,$$

当且仅当各$\begin{pmatrix}\tau_{1k}\\\tau_{2k}\\\vdots\\\tau_{mk}\end{pmatrix}$, $k=1,2,\cdots,n$不全相同时有

$$H\begin{bmatrix}q_1 & q_2 & \cdots & q_m\end{bmatrix}-\sum_{k=1}^{n}p_kH\begin{bmatrix}\tau_{1k} & \tau_{2k} & \cdots & \tau_{mk}\end{bmatrix}>0,$$

故至少存在$\begin{pmatrix}\tau_{1k_1}\\ \tau_{2k_1}\\ \vdots\\ \tau_{mk_1}\end{pmatrix}\neq\begin{pmatrix}\tau_{1k_2}\\ \tau_{2k_2}\\ \vdots\\ \tau_{mk_2}\end{pmatrix}$, $k_1\neq k_2$, 又各$\begin{pmatrix}\tau_{1k}\\ \tau_{2k}\\ \vdots\\ \tau_{mk}\end{pmatrix}$都为概率分布矢量, 故$\begin{pmatrix}\tau_{1k_1}\\ \tau_{2k_1}\\ \vdots\\ \tau_{mk_1}\end{pmatrix}$和$\begin{pmatrix}\tau_{1k_2}\\ \tau_{2k_2}\\ \vdots\\ \tau_{mk_2}\end{pmatrix}$线性无关, 所以$R\begin{pmatrix}\tau_{11}&\tau_{12}&\cdots&\tau_{1n}\\ \tau_{21}&\tau_{22}&\cdots&\tau_{2n}\\ \vdots&\vdots&\ddots&\vdots\\ \tau_{m1}&\tau_{m2}&\cdots&\tau_{mn}\end{pmatrix}\geq 2$, 且从式(7)和式(8)看到不满足Moore-Penrose的广义逆条件. 当$H\begin{bmatrix}q_1&q_2&\cdots&q_m\end{bmatrix}-\sum_{k=1}^n p_kH\begin{bmatrix}\tau_{1k}&\tau_{2k}&\cdots&\tau_{mk}\end{bmatrix}=0$时, 各$\begin{pmatrix}\tau_{1k}\\ \tau_{2k}\\ \vdots\\ \tau_{mk}\end{pmatrix}, k=1,2,\cdots,n$完全相同, 所以$\begin{pmatrix}\tau_{1k}\\ \tau_{2k}\\ \vdots\\ \tau_{mk}\end{pmatrix}=\begin{pmatrix}q_1\\ q_2\\ \vdots\\ q_m\end{pmatrix}, k=1,2,\cdots,n$. 则式(2)变成式(12), 且

$$R\begin{pmatrix}\tau_{11}&\tau_{12}&\cdots&\tau_{1n}\\ \tau_{21}&\tau_{22}&\cdots&\tau_{2n}\\ \vdots&\vdots&\ddots&\cdots\\ \tau_{m1}&\tau_{m2}&\cdots&\tau_{mn}\end{pmatrix}=1.$$

又由式(12)和(11)知

$$\begin{pmatrix}p_1&p_1&\cdots&p_1\\ p_2&p_2&\cdots&p_2\\ \vdots&\vdots&\ddots&\vdots\\ p_n&p_n&\cdots&p_n\end{pmatrix}_{n\times n}=\begin{pmatrix}p_1&p_1&\cdots&p_1\\ p_2&p_2&\cdots&p_2\\ \vdots&\vdots&\ddots&\cdots\\ p_n&p_n&\cdots&p_n\end{pmatrix}_{n\times m}\begin{pmatrix}q_1&q_1&\cdots&q_1\\ q_2&q_2&\cdots&q_2\\ \vdots&\vdots&\ddots&\vdots\\ q_m&q_m&\cdots&q_m\end{pmatrix}_{m\times n}\tag{27}$$

以及

$$\begin{pmatrix}q_1&q_1&\cdots&q_1\\ q_2&q_2&\cdots&q_2\\ \vdots&\vdots&\ddots&\vdots\\ q_m&q_m&\cdots&q_m\end{pmatrix}_{m\times m}=\begin{pmatrix}q_1&q_1&\cdots&q_1\\ q_2&q_2&\cdots&q_2\\ \vdots&\vdots&\ddots&\vdots\\ q_m&q_m&\cdots&q_m\end{pmatrix}_{m\times n}\begin{pmatrix}p_1&p_1&\cdots&p_1\\ p_2&p_2&\cdots&p_2\\ \vdots&\vdots&\ddots&\vdots\\ p_n&p_n&\cdots&p_n\end{pmatrix}_{n\times m}.\tag{28}$$

进一步有

$$\begin{pmatrix}p_1&p_1&\cdots&p_1\\ p_2&p_2&\cdots&p_2\\ \vdots&\vdots&\ddots&\vdots\\ p_n&p_n&\cdots&p_n\end{pmatrix}_{n\times m}=$$

$$\begin{pmatrix}p_1&p_1&\cdots&p_1\\ p_2&p_2&\cdots&p_2\\ \vdots&\vdots&\ddots&\vdots\\ p_n&p_n&\cdots&p_n\end{pmatrix}_{n\times m}\begin{pmatrix}q_1&q_1&\cdots&q_1\\ q_2&q_2&\cdots&q_2\\ \vdots&\vdots&\ddots&\vdots\\ q_m&q_m&\cdots&q_m\end{pmatrix}_{m\times n}\begin{pmatrix}p_1&p_1&\cdots&p_1\\ p_2&p_2&\cdots&p_2\\ \vdots&\vdots&\ddots&\vdots\\ p_n&p_n&\cdots&p_n\end{pmatrix}_{n\times m}\tag{29}$$

以及

$$\begin{pmatrix}q_1&q_1&\cdots&q_1\\ q_2&q_2&\cdots&q_2\\ \vdots&\vdots&\ddots&\vdots\\ q_m&q_m&\cdots&q_m\end{pmatrix}_{m\times n}=$$

$$\begin{pmatrix} q_1 & q_1 & \cdots & q_1 \\ q_2 & q_2 & \cdots & q_2 \\ \vdots & \vdots & \ddots & \vdots \\ q_m & q_m & \cdots & q_m \end{pmatrix}_{m\times n} \begin{pmatrix} p_1 & p_1 & \cdots & p_1 \\ p_2 & p_2 & \cdots & p_2 \\ \vdots & \vdots & \ddots & \vdots \\ p_n & p_n & \cdots & p_n \end{pmatrix}_{n\times m} \begin{pmatrix} q_1 & q_1 & \cdots & q_1 \\ q_2 & q_2 & \cdots & q_2 \\ \vdots & \vdots & \ddots & \vdots \\ q_m & q_m & \cdots & q_m \end{pmatrix}_{m\times n} . \tag{30}$$

由式(29)和(30)知$\begin{pmatrix} p_1 & p_1 & \cdots & p_1 \\ p_2 & p_2 & \cdots & p_2 \\ \vdots & \vdots & \ddots & \vdots \\ p_n & p_n & \cdots & p_n \end{pmatrix}_{n\times m}$与$\begin{pmatrix} q_1 & q_1 & \cdots & q_1 \\ q_2 & q_2 & \cdots & q_2 \\ \vdots & \vdots & \ddots & \vdots \\ q_m & q_m & \cdots & q_m \end{pmatrix}_{m\times n}$互成自反广义逆, 但由式(27)和(28)知$\begin{pmatrix} p_1 & p_1 & \cdots & p_1 \\ p_2 & p_2 & \cdots & p_2 \\ \vdots & \vdots & \ddots & \vdots \\ p_n & p_n & \cdots & p_n \end{pmatrix}_{n\times n}$和$\begin{pmatrix} q_1 & q_1 & \cdots & q_1 \\ q_2 & q_2 & \cdots & q_2 \\ \vdots & \vdots & \ddots & \vdots \\ q_m & q_m & \cdots & q_m \end{pmatrix}_{m\times m}$均非对称矩阵, 所以$\begin{pmatrix} p_1 & p_1 & \cdots & p_1 \\ p_2 & p_2 & \cdots & p_2 \\ \vdots & \vdots & \ddots & \vdots \\ p_n & p_n & \cdots & p_n \end{pmatrix}_{n\times m}$与$\begin{pmatrix} q_1 & q_1 & \cdots & q_1 \\ q_2 & q_2 & \cdots & q_2 \\ \vdots & \vdots & \ddots & \vdots \\ q_m & q_m & \cdots & q_m \end{pmatrix}_{m\times n}$不是Moore-Penrose广义逆, 但当输入和输出为等概率分布$\begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix} = \begin{pmatrix} 1/n \\ 1/n \\ \vdots \\ 1/n \end{pmatrix}$和$\begin{pmatrix} q_1 \\ q_2 \\ \vdots \\ q_m \end{pmatrix} = \begin{pmatrix} 1/m \\ 1/m \\ \vdots \\ 1/m \end{pmatrix}$时, 则

$$\begin{pmatrix} p_1 & p_1 & \cdots & p_1 \\ p_2 & p_2 & \cdots & p_2 \\ \vdots & \vdots & \ddots & \vdots \\ p_n & p_n & \cdots & p_n \end{pmatrix}_{n\times n} = \begin{pmatrix} 1/n & 1/n & \cdots & 1/n \\ 1/n & 1/n & \cdots & 1/n \\ \vdots & \vdots & \ddots & \vdots \\ 1/n & 1/n & \cdots & 1/n \end{pmatrix}_{n\times n}$$

和

$$\begin{pmatrix} q_1 & q_1 & \cdots & q_1 \\ q_2 & q_2 & \cdots & q_2 \\ \vdots & \vdots & \ddots & \vdots \\ q_m & q_m & \cdots & q_m \end{pmatrix}_{m\times m} = \begin{pmatrix} 1/m & 1/m & \cdots & 1/m \\ 1/m & 1/m & \cdots & 1/m \\ \vdots & \vdots & \ddots & \vdots \\ 1/m & 1/m & \cdots & 1/m \end{pmatrix}_{m\times m}$$

均为对称矩阵, 此时$\begin{pmatrix} p_1 & p_1 & \cdots & p_1 \\ p_2 & p_2 & \cdots & p_2 \\ \vdots & \vdots & \ddots & \vdots \\ p_n & p_n & \cdots & p_n \end{pmatrix}_{n\times m}$与$\begin{pmatrix} q_1 & q_1 & \cdots & q_1 \\ q_2 & q_2 & \cdots & q_2 \\ \vdots & \vdots & \ddots & \vdots \\ q_m & q_m & \cdots & q_m \end{pmatrix}_{m\times n}$互成Moore-Penrose广义逆. 最后令$m = n$并$\begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix} = \begin{pmatrix} 1/n \\ 1/n \\ \vdots \\ 1/n \end{pmatrix}$和$\begin{pmatrix} q_1 \\ q_2 \\ \vdots \\ q_n \end{pmatrix} = \begin{pmatrix} 1/n \\ 1/n \\ \vdots \\ 1/n \end{pmatrix}$, 则

$$\begin{pmatrix} 1/n \\ 1/n \\ \vdots \\ 1/n \end{pmatrix} = \lim_{N\to+\infty} \begin{pmatrix} 1/n & 1/n & \cdots & 1/n \\ 1/n & 1/n & \cdots & 1/n \\ \vdots & \vdots & \ddots & \vdots \\ 1/n & 1/n & \cdots & 1/n \end{pmatrix}_{n\times n}^{N} \times \begin{pmatrix} 1/n \\ 1/n \\ \vdots \\ 1/n \end{pmatrix}, \tag{31}$$

即输入输出分布$\begin{pmatrix} 1/n \\ 1/n \\ \vdots \\ 1/n \end{pmatrix}$为该状态转移概率矩阵$\begin{pmatrix} 1/n & 1/n & \cdots & 1/n \\ 1/n & 1/n & \cdots & 1/n \\ \vdots & \vdots & \ddots & \vdots \\ 1/n & 1/n & \cdots & 1/n \end{pmatrix}_{n\times n}$的平衡态分布.

§3 一次一密理论相关的应用

香农的一次一密和完善保密性理论认为只要使用一次性密码本, 并且密钥和明文等长就能保证完善保密性. 本节先论证一次一密的完善保密性并不需要密钥等概率分布, 也不需要密钥与明文互相独立的前提条件. 所谓完善保密性即$P(X)=P(X|Y)$, 意思是通过密文无法提供知道明文的任何信息. 而该定义$P(X)=P(X|Y)$等价于输入输出的互信息为零(即信道容量为零), 即$P(X)=P(X|Y)\Leftrightarrow H(X)=H(X|Y)\Leftrightarrow I(X;Y)=H(X)-H(X|Y)=0$.

设明文, 密文和密钥均为0及1二进制序列, 一次一密即为密钥序列和明文等长, 位与位之间一一对齐采用二元有限域的加法, 所以明文序列、密钥序列和密文序列中知道任意两个序列就可以基于有限域加法能计算出其余的一个序列. 基于信道容量为零的角度证明一次一密的完善保密性, 这个证明既不需要以密钥等概率作为前提条件, 也不需要密钥K与明文X互相独立, 这就是定理5.

定理5 设一次一密的过程以确定的加密和解密运算而关联的随机变量为明文X, 密钥K和密文Y, 则明文X和密文Y间的互信息为零.

证 由加密, 解密运算的确定性易知此三个条件熵为零, 即$H(X|(Y,K))=H(Y|(X,K))=H(K|(X,Y))=0$. 又$H(Y,(X|K))=H(Y)+H(X|(K,Y))=H(X|K)+H(Y|(X,K))$, 及$H(Y,(K|X))=H(Y)+H(K|(X,Y))=H(K|X)+H(Y|(K,X))$, 得到$H(Y)=H(K|X)=H(X|K)$. 同理$H(X)=H(Y|K)=H(K|Y)$和$H(K)=H(X|Y)=H(Y|X)$. 所以$H(Y)-H(Y|X)=H(K|X)-H(K)$, 该式左边$H(Y)-H(Y|X)\geq 0$, 而右边$H(K|X)-H(K)\leq 0$, 得到$H(Y)-H(Y|X)=0=H(K|X)-H(K)$. 同理得到$H(X)-H(X|Y)=0=H(K|Y)-H(K)$. 所以$I(X;Y)=H(X)-H(X|Y)=H(Y)-H(Y|X)=0$. 即明文和密文之间的互信息为零, 而这说明明文和密文之间的信道容量为零.

从上述推导过程可以看出, 虽然没有使用明文X与密钥K互相独立作为条件, 但最终也可得出明文X和密文Y及密钥K间两两独立, 也意味着密钥等概率分布是非必要的, 而密钥和明文、密文的等熵是必要的.

这里密钥K不是直接和明文X作运算产生密文, 而是由X依照条件概率随机生成K, 再由K生成Y. 因此把前后的转移概率矩阵相乘可以得到由X直接生成Y的转移概率矩阵. 这个生成算法可以采用Monte Carlo机制来模拟概率, 然后控制输出的比特值. 可见由密钥参与计算的加密过程实质上和含噪声通信信道输出是等效的.

定理1构造的信道$\langle X,Y\rangle$的信道容量为零. 事实上, 由§2的式(11)和(12), $H(X)-H(X|Y)=-\sum_{i=1}^{n}p_i\log p_i-\sum_{j=1}^{m}q_j[-\sum_{i=1}^{n}p_i\log p_i]=0=-\sum_{j=1}^{m}q_j\log q_j-\sum_{i=1}^{n}p_i[-\sum_{j=1}^{m}q_j\log q_j]=H(Y)-H(Y|X)$. 又由定理4, 对通信信道容量为零的信道而言, 其转移概率矩阵必形如§2的式(11)和(12), 理由是信道容量为零等价于完善保密性, 完善保密性即为满足$P(X|Y=y_i)=P(X)=P(X|Y=y_j)$或$P(Y|X=x_i)=P(Y)=P(Y|X=x_j)$的相同概率分布的要求.

在§2的式(19)中令$k=q_1$时$H(X)-H(X|Y)=-p_0\log p_0-p_1\log p_1+\{q_0[p_0\log p_0+p_1\log p_1]+q_1[p_0\log p_0+p_1\log p_1]\}=0$, 此时§2的式(18)退化为

$$\begin{pmatrix}q_0\\q_1\end{pmatrix}=\begin{pmatrix}q_0&q_0\\q_1&q_1\end{pmatrix}\begin{pmatrix}p_0\\p_1\end{pmatrix};\quad \begin{pmatrix}p_0\\p_1\end{pmatrix}=\begin{pmatrix}p_0&p_0\\p_1&p_1\end{pmatrix}\begin{pmatrix}q_0\\q_1\end{pmatrix}. \tag{32}$$

特别地, 当$p_0 = q_0$ (同时又$p_1 = q_1$)时, 式(32)又变为

$$\begin{pmatrix} p_0 \\ p_1 \end{pmatrix} = \begin{pmatrix} p_0 & p_0 \\ p_1 & p_1 \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}; \quad \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} = \begin{pmatrix} p_0 & p_0 \\ p_1 & p_1 \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}. \tag{33}$$

式(33)表示的信道即为香农一次一密机制, 且明文、密文和密钥等熵[6-7]. 而式(32)表示的是一种推广的香农一次一密机制, 明文和密文的熵可以不相等, 从而有利于掩盖明文的熵, 同时还能保持完善保密性(即信道容量为零).

§4 公钥密码系统相关的应用

教科书式RSA的加解密是确定算法, 它的安全性是基于计算复杂性, 正因为是确定算法, 所以攻击者可以选择一段密文, 利用公开的密钥, 计算与此段密文的未知明文成倍数的明文的密文, 这是潜在的安全风险. 引入随机密钥的完善保密性则是体现密码系统抵抗各种攻击的能力的属性. 下面首先证明Elgamal算法的加密和签名机制满足随机密钥下的完善保密性, 然后再证明使用随机填充处理的RSA仍不满足随机填充加密下的完善保密性.

为讨论Elgamal算法的输入输出的转移概率矩阵, 首先简要描述Elgamal执行加密和签名的实现方式：Elgamal加密, 考虑大素数阶有限循环群(G, p), 其中G是p的本原根, 即$G^{p-1} = 1(\mathrm{mod}\, p)$, 接收方随机选取一个$x \in \{1, 2, \cdots, p-1\}$作为私钥, 并把$(G^x, G, p)$作为公钥发布, 这里由于离散对数计算的困难性(为单向函数)知道G^x计算x并不易. 发送方随机选取$y \in \{1, 2, \cdots, p-1\}$作为临时密钥, 则任意明文$m \cdot = G^m \in \{G, G^2, \cdots, G^{p-1}\}$的加密密文为$(C_1, C_2)$, 其中$C_1 = G^y$而$C_2 = (G^x)^y G^m$. 接收方解密方式为$\frac{C_2}{C_1^x} = \frac{G^{xy} G^m}{G^{xy}} = G^m$. Elgamal签名, 发送方取$x \in \{1, 2, \cdots, p-1\}$作为私钥, 并发布公钥$(G^x, G, p)$, 然后随机选取$y \in \{1, 2, \cdots, p-1\}$作为临时密钥、且$\gcd(y, p-1) = 1$, 对明文$m \in \{0, 1, 2, \cdots, p-1\}$作签名$(C_1, C_2)$, 其中$C_1 = G^y$而$C_2 = (m - C_1 x) y^{-1}$. 验证签名, 先计算$G^m$, 看是否满足$(G^x)^{C_1} C_1^{C_2} = G^{xG^y + y(m - C_1 x) y^{-1}} = G^m$.

根据Elgamal加密或签名中C_2的表达式, 由于涉及运算都是确定性运算, 只是随机选取密钥, 因此可以得到执行的算法的输入明文和输出密文的转移概率矩阵, 加密时的信道表示为输入概率乘以转移矩阵, 得到输出概率分布的形式为

$$\begin{pmatrix} \frac{1}{p-1} \\ \frac{1}{p-1} \\ \vdots \\ \frac{1}{p-1} \end{pmatrix} = \begin{pmatrix} \frac{1}{p-1} & \frac{1}{p-1} & \cdots & \frac{1}{p-1} \\ \frac{1}{p-1} & \frac{1}{p-1} & \cdots & \frac{1}{p-1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{p-1} & \frac{1}{p-1} & \cdots & \frac{1}{p-1} \end{pmatrix} \begin{pmatrix} \frac{1}{p-1} \\ \frac{1}{p-1} \\ \vdots \\ \frac{1}{p-1} \end{pmatrix}. \tag{34}$$

上式输入输出皆为$p-1$长度的等概率分布. 式(34)从加解密过程使用素数生成的乘法群元素, 不含0, 故得. 签名时的信道表示为

$$\begin{pmatrix} \frac{1}{p} \\ \frac{1}{p} \\ \vdots \\ \frac{1}{p} \end{pmatrix} = \begin{pmatrix} \frac{1}{p} & \frac{1}{p} & \cdots & \frac{1}{p} \\ \frac{1}{p} & \frac{1}{p} & \cdots & \frac{1}{p} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{p} & \frac{1}{p} & \cdots & \frac{1}{p} \end{pmatrix} \begin{pmatrix} \frac{1}{p} \\ \frac{1}{p} \\ \vdots \\ \frac{1}{p} \end{pmatrix}. \tag{35}$$

此式输入输出皆为p长度的等概率分布. 式(35)由于签名的明文可以取0, 故得. 显然, 这两种情形计算得到的信道容量皆为零. 且符合定理4的广义可逆性, 以及输入输出的概率分布均为平衡态分布. 这表明公钥密码系统的“不可逆”(“不可破解”)与Markov矩阵的广义可逆性之间的一致性. 关于随机填充RSA格式, 考虑原始数据长度为n比特, 附加填充的随机数据的长度

为m比特, 于是输入明文的变量X可以看作为$(\frac{1}{2^n}\quad\frac{1}{2^n}\quad\cdots\quad\frac{1}{2^n})$的概率分布, 输出的密文的变量$Y$为$(\frac{1}{2^{n+m}}\quad\frac{1}{2^{n+m}}\quad\cdots\quad\frac{1}{2^{n+m}})$的概率分布, 并且易知如下的条件概率

$$p(Y=y|X=x)=\begin{cases}\dfrac{1}{2^m}; & x\quad as\quad part\quad of\quad y\\ 0; & x\quad not\quad part\quad of\quad y\end{cases}. \tag{36}$$

反之

$$p(X=x|Y=y)=\begin{cases}1; & x\quad \text{as}\quad \text{part}\quad \text{of}\quad y\\ 0; & x\quad \text{not}\quad \text{part}\quad \text{of}\quad y\end{cases}. \tag{37}$$

此处"x as part of y"("x作为y的部分")的涵义是指y作为密文到它对应的明文x都有确定的概率1决定(尽管作为单向函数的求逆并不易, 但因RSA是确定运算, 所以存在确定的逆, 概率为1), 而"x not part of y"("x不为y的部分")指x并非密文y对应的明文. 此时可以透过加解密操作, 直接在添加随机填充的角度下, 看x是否是y的一部分而决定式(36)和(37)的条件概率. 于是填充式RSA的加密信道为

$$\begin{pmatrix}\frac{1}{2^{m+n}}\\ \frac{1}{2^{m+n}}\\ \vdots\\ \frac{1}{2^{m+n}}\end{pmatrix}=\begin{pmatrix}0 & \cdots & \frac{1}{2^m} & \cdots\\ \frac{1}{2^m} & \cdots & \cdots & 0\\ \vdots & \vdots & \ddots & \frac{1}{2^m}\\ 0 & \cdots & \cdots & \cdots\end{pmatrix}_{2^{m+n}\times 2^n}\begin{pmatrix}\frac{1}{2^n}\\ \frac{1}{2^n}\\ \vdots\\ \frac{1}{2^n}\end{pmatrix}. \tag{38}$$

解密信道为

$$\begin{pmatrix}\frac{1}{2^n}\\ \frac{1}{2^n}\\ \vdots\\ \frac{1}{2^n}\end{pmatrix}=\begin{pmatrix}0 & \cdots & 1 & \cdots\\ 1 & \cdots & \cdots & 0\\ \vdots & \vdots & \ddots & 1\\ 0 & \cdots & \cdots & \cdots\end{pmatrix}_{2^n\times 2^{n+m}}\begin{pmatrix}\frac{1}{2^{n+m}}\\ \frac{1}{2^{n+m}}\\ \vdots\\ \frac{1}{2^{n+m}}\end{pmatrix}. \tag{39}$$

式(38)的概率转移矩阵中每一列有2^m个$\frac{1}{2^m}$, 其余都是零; 每一行只有1个$\frac{1}{2^m}$, 其余都是零. 式(39)的概率转移矩阵中每一列有1个1, 其余都为零; 每一行有2^m个1, 其余都为零. 从式(38)和(39)计算得到$H(Y)-H(Y|X)=n=H(X)-H(X|Y)$, 填充式RSA不满足随机加密下的完善保密性, 即随机填充并不等效于随机密钥.

§5 总结与展望

本文研究了Markov过程的概率转移矩阵的可逆性, 对公钥密码系统在随机计算里获得的"抗攻击"能力使用信道容量为零的机制进行了解释, 并且发现完善保密性和Markov矩阵的广义可逆性有关联, 以及随机填充RSA算法并不符合信道容量为零的原则. 将来拟进一步研究可获得信道容量为零的RSA随机化算法.

参考文献:

[1] Trendelkamp-Schroer Benjamin, Wu Hao, Fabian Paul, et al. Estimation and uncertainty of reversible Markov models[J]. The Journal of Chemical Physics, 2015, 143: 174101.

[2] Brill P H, Cheung Chi ho, Hlynka Myron, et al. Reversibility checking for Markov chains[J]. Communications on Stochastic Analysis, 2018, 12(2): Article 2.

[3] Taher ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472.

[4] Rivest R, Shamir A, Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 1978, 21(2): 120-126.

[5] Coron J S, Joye M, Naccache D, et al. Universal Padding Schemes for RSA[C]. In: Yung M, eds, Advances in Cryptology-CRYPTO 2002. Lecture Notes in Computer Science, vol 2442. Berlin: Springer.

[6] Shannon Claude. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[7] 陆成刚, 王庆月. 一次一密理论的再认识[J]. 高校应用数学学报, 2022, 37(4): 426-430.

[8] Thomas M Cover, Joy A Thomas. Elements of Information Theory[M]. John Wiley and Sons, 2005.

Generalized invertibility of Markov matrices

LU Cheng-gang

(School of Mathematical Sciences, Zhejiang University of Technology, Hangzhou 310013, China)

Abstract: For uncertain input-output systems, the existence, uniqueness and reversibility of the state transition probability matrix (i.e., Markov matrix) between the probability distribution vectors of input and output random variables are considered, as well as the consistency relationship between the generalized reversibility and the one-time pad theory and the security of the public key cryptosystem. Considering the Markov matrix as a communication channel, when the channel capacity is non-zero, the Markov matrix exists, is not unique, has a rank not less than 2, and does not have a generalized inverse; when the channel capacity is zero, the Markov matrix exists, is unique, has a rank of 1, and has a generalized inverse. In particular, when the input and output are both equally probable distributions, the Markov matrix has a Moore-Penrose generalized inverse. Furthermore, when the number of states of the input and output is the same, the probability distribution of the input or output is the equilibrium state distribution of the Markov matrix. And the Markov matrix with a generalized inverse is exactly the channel for asymmetric encryption and decryption of the public-private key cryptosystem. Combining RSA and Elgamal algorithms, positive and negative examples are given.

Keywords: Markov matrix; Moore-Penrose generalized inverse; one-time pad; public-private key cryptography; RSA algorithm; Elgamal algorithm

MR Subject Classification: 15A09 ; 15B51; 60J10