密码学函数迭代原理信息论分析

吕述望, 范修斌, 张如文
(中国科学技术大学研究生院, 信息安全国家重点实验室, 北京 100039)

摘 要: 在密码编码学中, 经常利用密码学函数迭代技术来实现密码算法, 其所依赖的理论基础包括相关免疫理论, 扩散准则, 雪崩原理等. 本文利用信息论原理以及随机过程理论给出了密码学函数迭代原理分析, 得到了经过密码学函数迭代之后, 输出为均匀分布时, 输入输出互信息极限为零的充分必要条件, 以及在一定条件下输入输出互信息收敛速度的一个上界.

关键词: 密码学函数迭代; 互信息; 马氏链
中图分类号: TN918 文献标识码: A 文章编号: 0372-2112 (2002) 10-1151-03

Information Analysis of Iterative Principle of Cryptographic Function

LV Shu-wang, FAN Xiu-bin, ZHANG Ru-wen
(Graduate School of Academia Sinica, Beijing 100039, China)

Abstract: In cryptographic design, people often use the method of iterative principle of cryptographic function to give the cryptographic algorithm. In this paper, using the information theory and random process method, we get the necessary and sufficient condition of the iterative mutual information becoming to zero and one upper bound of the rate of its convergence under some condition.

Key words: iterative principle of cryptographic function; mutual information; Markov chain

1 引言

在密码编码学中, 人们经常利用密码学函数迭代技术来实现密码算法, 例如 DES、RC4、RC5、AES、序列密码的非线性加工部分等, 其所依赖的理论基础包括相关免疫理论, 扩散准则, 雪崩原理等. 众所周知, 信息论原理是密码编码学以及密码分析学的重要理论组成部分. 本文的出发点是利用信息论原理对密码学函数迭代技术建立信道迭代模型. 在此基础上, 进一步利用随机过程理论, 给出密码学函数迭代原理分析, 得到了经过密码学函数迭代之后输出为均匀分布时, 输入输出互信息极限为零的充分必要条件, 以及在一定条件之下的输入输出互信息收敛速度的一个上界. 显然, 本文结论对于密码学编码有着重要的指导意义. 论文结束部分给出了本文结果的一个应用简介.

2 密码学函数迭代的数学模型以及信道模型

一般密码学函数迭代的数学模型如下:

设 $f(x, y_1)= z_1, f(z_1, z_2)= z_2, \cdots, f(z_{t-1}, y_t)= z_t$, 其中 f 为密码学函数, 即有层密钥输入的密码算法, x 为输入, y_i, i = 1, 2, …, t 为密钥, z_i, i= 1, 2, …, t 为 i 次迭代输出.

我们给出它的信道迭代模型如下:

设 X 为概率空间(8, F, p) 上取值于 Z/ (n) 的随机变量, Y_i, i= 1, 2, …, t 亦为概率空间(8, F, p) 上独立同分布且取值于 Z/ (m) 上的随机变量, X, Y_i, i= 1, 2, …, t, 亦相互独立, 令: $Z_1= f(X, Y_1)$, $Z_2= f(Z_1, Y_2)$, …, $Z_t= f(Z_{t-1}, Y_t)$, 其中 f 为可测变换, Z_i, i= 1, 2, …, t 取值于 Z/ (n), Y_{i+1}, Z_i (1F i< t) 亦相互独立. 我们称 X 为信道输入, Y_i, i= 1, 2, …, t, 为信道噪声, Z_i, i= 1, 2, …, t, 为信道输出.

对于较小的 t, 若输入输出互信息 $I(X, Z_t)$ 较小, 则在密码学编码中, 满足这种性质的密码学函数 f 是较好的. 下面我们主要讨论 $\lim_{t\to\infty} I(X, Z_t)= 0$ 的充要条件, 以及在一定条件之下, 其收敛速度.

3 输出均匀分布时输入输出互信息极限为零的充要条件

我们首先给出上述密码学函数迭代的信道迭代模型基本性质. 为了便于讨论, 令 $X= Z_0$.

定义 1[1] 定义在概率空间(8, F, p) 上的取非负整数值的随机变量列 X_t($X_t= X_t(X)$, XI 8), t= 0, 1, 2, …, 称为马氏链, 如果等式

$$p(X_{q+k}= i_{q+k} \mid X_q= i_q, X_{j_1}= i_{j_1}, \cdots, X_{j_2}= i_{j_2}, X_{j_1}= i_{j_1}) = p(X_{q+k}= i_{q+k} \mid X_q= i_q)$$

对任意正整数 l, q, k, 及任意的非负整数 $j_1> \cdots > j_2> j_1$ (q> j_1), $i_{q+k}, i_q, i_{j_1}, \cdots, i_{j_2}, i_{j_1}$ 成立, 只要式中左方构成的事件的概率大于 0.

收稿日期: 2001-01-08; 修回日期: 2001-12-31
基金项目: 科技部 973 项目(No. G1999035808); 国家/ 863 项目(No. 2001AA141010)

简记 $_qp_{ij}^{(k)}=p(X_{q+k}=j\mid X_q=i)$, $_qP^{(k)}=(_qp_{ij}^{(k)})(i,j=0,1,2,\cdots)$.

定义 2 称马氏链 $X_t(X_t=X_t(X),X\in\Omega,t=0,1,2,\cdots)$ 为齐次的, 若它的转移概率矩阵 $_qP=P$ 与 q 无关, 即对任意非负整数 q 有: $p(X_{q+1}=j\mid X_q=i)=p_{ij}$, 其中 $p_{ij}^{(1)}=p_{ij}$.

定义 3[2] 一个非负方阵称为随机矩阵, 如果其每行之和为 1.

定义 4[2] 一个非负方阵称为双随机矩阵, 如果其每行每列之和皆为 1.

性质 1 密码学函数迭代输出随机变量列 $\{Z_t\}$ 构成齐次马氏链.

证明 由密码学函数迭代的信道迭代模型可知:

$l,lc\in Z/(m)$, $p(Z_{q+1}=lc\mid Z_q=l)=p(f(l,Y_{q+1})=lc\mid Z_q=l)$, 因为 f 为可测变换, Y_{q+1}, Z_q 相互独立, 故可得:

$$\begin{aligned}&p(Z_{q+1}=lc\mid Z_q=l)\\&=p(f(l,Y_{q+1})=lc)p(Z_q=l)/p(Z_q=l)\\&=p(f(l,Y_{q+1})=lc).\end{aligned}$$

又因为 Y_i, $i=1,2,\cdots$, 为概率空间 (Ω,F,p) 上独立同分布且取值于 $Z/(m)$ 上的随机变量, 故 $p(f(l,Y_{q+1})=lc)$ 与 q 无关, 即 $_qP=P$ 与 q 无关.

对任意正整数 l, q, k, 及任意的非负整数: $j_1>\cdots>j_2>j_1$ $(q>j_1)$ 以及 $i_{q+k},i_q,i_{j_1},\cdots,i_{j_2},i_{j_1}\in Z/(n)$, 由信道迭代模型可知:

$$\begin{aligned}&p(Z_{q+k}=i_{q+k}\mid Z_q=i_q,Z_{j_1}=i_{j_1},\cdots,Z_{j_2}=i_{j_2},Z_{j_1}=i_{j_1})\\&=\sum_{i_{q+k-1},\cdots,i_{q+1}\in Z/(n)}p(Z_{q+k}=i_{q+k},\cdots,Z_{q+1}=i_{q+1}\mid Z_q=i_q,\\&\quad Z_{j_1}=i_{j_1},\cdots,Z_{j_2}=i_{j_2},Z_{j_1}=i_{j_1})\\&=\sum_{i_{q+k-1},\cdots,i_{q+1}\in Z/(n)}p(f(i_{q+k-1},Y_{q+k})=i_{q+k},\cdots,f(i_q,Y_{q+1})=\\&i_{q+1}\mid Z_q=i_q,Z_{j_1}=i_{j_1},\cdots,Z_{j_1}=i_{j_1})\\&=\sum_{i_{q+k-1},\cdots,i_{q+1}\in Z/(n)}p(f(i_{q+k-1},Y_{q+k})=i_{q+k},f(i_{q+k-2},\\&Y_{q+k-1})=i_{q+k-1},\cdots,f(i_q,Y_{q+1})=i_{q+1})\\&=\sum_{i_{q+k-1},\cdots,i_{q+1}\in Z/(n)}p(f(i_{q+k-1},Y_{q+k})=i_{q+k})\,p(f(i_{q+k-2},\\&Y_{q+k-1})=i_{q+k-1})\cdots p(f(i_q,Y_{q+1})=i_{q+1})\\&=\sum_{i_{q+k-1},\cdots,i_{q+1}\in Z/(n)}p_{i_{q+k-1}i_{q+k}}p_{i_{q+k-2}i_{q+k-1}}\cdots p_{i_{q+1}i_{q+2}}=p_{i_qi_{q+k}}^{(k)}=\\&p(Z_{q+k}=i_{q+k}\mid Z_q=i_q).\end{aligned}$$

故由定义 1、定义 2 可知, $\{Z_t\}$ 构成齐次马氏链.

性质 2 密码学函数迭代过程中, 转移概率矩阵 P 为随机矩阵.

证明 由密码学函数迭代的信道模型可知:

$$i\in Z/(n),\ \sum_{j\in Z/(n)}p_{ij}=\sum_{j\in Z/(n)}p(Z_{q+1}=j\mid Z_q=i)=1.$$

故由定义 3 可知, 转移概率矩阵 P 为随机矩阵.

性质 3 密码学函数迭代过程中, 转移概率矩阵 P^t 亦为随机矩阵.

证明 显然当 t=1 时, 命题成立. 假设 t=k 时命题成立, t=k+1 时, $i\in Z/(n)$, $\sum_{j\in Z/(n)}p_{ij}^{(k+1)}=\sum_{l\in Z/(n)}p_{il}^{(k)}\sum_{j\in Z/(n)}p_{lj}=\sum_{j\in Z/(n)}p_{lj}\sum_{l\in Z/(n)}p_{il}^{(k)}=\sum_{j\in Z/(n)}p_{lj}=1$.

引理 1[3] 设 X 为密码学函数的输入, Y 为密码学函数的输出, 其信道模型中转移概率矩阵为 P, 则: $I(X,Y)=0\Leftrightarrow$ X, Y 相互独立.

在密码学编码时, 重要的编码准则之一为最终的密码学函数的输出应为均匀分布. 下面我们讨论在输出为均匀分布, 输入输出互信息为零时, 转移概率矩阵的性质.

推论 1 设为密码学函数的输入, Y 为密码学函数的输出, 其信道模型中转移概率矩阵为 P, 若 $i\in Z/(n)$, $p(X=i)>0$, $j\in Z/(n)$, $p(Y=j)=\frac{1}{n}$, 则: $I(X,Y)=0\Leftrightarrow\forall i,j$, $p_{ij}=\frac{1}{n}$.

证明 若 X, Y 相互独立, 则:

$$\begin{aligned}&j\in Z/(n),p_{ij}=p(Y=j\mid X=i)\\&=\frac{p(X=i,Y=j)}{p(X=i)}=\frac{p(X=i)p(Y=j)}{p(X=i)}=p(Y=j)=\frac{1}{n}.\end{aligned}$$

若 $\forall i,j,p_{ij}=\frac{1}{n}$, $p(X=i,Y=j)=p_{ij}p(X=i)=\frac{1}{n}p(X=i)=p(X=i)p(Y=j)$.

故由引理 1 可知命题成立.

引理 2 设 X 为密码学函数的输入, Y 为密码学函数的输出, 其信道模型中转移概率矩阵为 P, 若 $i,j\in Z/(n)$, $p_{ij}=\frac{1}{n}$, 则: $I(X,Y)=0$, Y 为均匀分布.

证明 Y 为均匀分布显然.

$$\begin{aligned}I(X,Y)&=E\log\frac{p(X,Y)}{p(X)p(Y)}\\&=\sum_{i,j\in Z/(n)}p(X=i,Y=j)\log\frac{p(X=i,Y=j)}{p(X=i)p(Y=j)}\\&=\sum_{i,j\in Z/(n)}p(X=i,Y=j)\log\frac{p(Y=j\mid X=i)p(X=i)}{p(X=i)p(Y=j)}\\&=\sum_{i,j\in Z/(n)}p(X=i,Y=j)\log\frac{p(X=i)}{p(X=i)}=0.\end{aligned}$$

由上述分析可知, 密码学函数迭代过程中, 若当转移概率矩阵 P 的幂 P^t 的极限存在且 $\lim_{t\to\infty}P^t=\frac{1}{n}J$, 其中 J 为元素全 1 矩阵, 则这样的密码学函数迭代具有较好的密码学意义. 若 P^t 的极限存在且记为 V, 则易得:

引理 3 $V=PV=VP$.

证明 $V=\lim_{t\to\infty}P^t=P\lim_{t\to\infty}P^{t-1}=PV$, $V=(\lim_{t\to\infty}P^{t-1})P=VP$.

引理 4 若 $\lim_{t\to\infty}P^t=\frac{1}{n}J$, 则 P 为双随机矩阵.

证明 由性质 1, 引理 3 可知: $PJ=JP$, 故 $j\in Z/(n)$, $\sum_{k\in Z/(n)}p_{kj}=\sum_{k\in Z/(n)}p_{jk}=1$.

引理 5[4] $\lim_{t\to\infty}P^t=\frac{1}{n}J\Leftrightarrow P$ 为双随机矩阵且存在 $t>0$, $\forall i,j\in Z/(n)$, $p_{ij}^{(t)}>0$.

由引理 5 以及推论 1 可得:

定理 1　密码学函数的迭代过程中, 若 $P\in Z/(n)$, $p(X=i)>0$ 且其极限输出为均匀分布时, 则: $\lim_{t\to\infty} I(Z_0, Z_t)=0$

P 为双随机矩阵且存在 $t>0$, $P_{ij}\in Z/(n)$, $p_{ij}^{(t)}>0$.

推论 2　设 X 为密码学函数的输入, P 为双随机矩阵且存在 $t>0$, $P_{ij}\in Z/(n)$, $p_{ij}^{(t)}>0$, 则密码学函数迭代极限输出为均匀分布.

证明　由引理 2, 引理 5 易得.

由上述分析可知, 满足定理 1 条件的双随机矩阵具有较好的密码编码学性质, 特别是在密码学函数迭代过程设计之中, 可以对此加以充分利用.

4　密码学函数迭代过程中输入输出互信息收敛速度分析

引理 6[5]　当 $x>0$, $\ln x\le x-1$.

令 $p(X=i)=r_i$, $P\in Z/(n)$.

引理 7　$p(Z_t=j, X=i)=r_i p_{ij}^{(t)}$.

证明　$p(Z_t=j, X=i)=p(Z_t=j\mid X=i)r_i=r_i p_{ij}^{(t)}$.

引理 8[2]　双随机矩阵的积仍为双随机矩阵.

定理 2　若 P 为双随机矩阵且满足:

$$P\in Z^+, P_{ij}\in Z/(n), p_{ij}^{(t)}\ge\frac{1}{n}\left(1-\frac{1}{t^k}\right), k\in R^+,$$ 则:

$$I(X, Z_t)\le\frac{1}{\ln 2}\left(\frac{n^2}{t^k-1}\right).$$

证明

$$I(X, Z_t)=E\log\frac{p(X, Z_t)}{p(X)p(Z_t)}$$

$$=\sum_{i,j\in Z/(n)}p(X=i, Z_t=j)\log\frac{p(X=i, Z_t=j)}{p(X=i)p(Z_t=j)}$$

$$\overset{\text{引理7}}{=}\sum_{i,j\in Z/(n)}r_i p_{ij}^{(t)}\log\frac{r_i p_{ij}^{(t)}}{r_i p(Z_t=j)}=\sum_{i,j\in Z/(n)}r_i p_{ij}^{(t)}\log\frac{p_{ij}^{(t)}}{\sum_{k\in Z/(n)}r_k p_{kj}^{(t)}}$$

$$\overset{\text{引理6}}{\le}\frac{1}{\ln 2}\sum_{i,j\in Z/(n)}r_i p_{ij}^{(t)}\left(\frac{p_{ij}^{(t)}}{\sum_{k\in Z/(n)}r_k p_{kj}^{(t)}}-1\right)$$

$$\le\frac{1}{\ln 2}\sum_{i,j\in Z/(n)}\left(\frac{p_{ij}^{(t)}}{\sum_{k\in Z/(n)}r_k p_{kj}^{(t)}}-1\right)=\frac{1}{\ln 2}\sum_{i,j\in Z/(n)}\frac{p_{ij}^{(t)}}{\sum_{k\in Z/(n)}r_k p_{kj}^{(t)}}-n^2\right)$$

$$=\frac{1}{\ln 2}\left(\sum_{j\in Z/(n)}\sum_{i\in Z/(n)}\left(\frac{p_{ij}^{(t)}}{\sum_{k\in Z/(n)}r_k p_{kj}^{(t)}}\right)-n^2\right)$$

$$=\frac{1}{\ln 2}\left(\sum_{j\in Z/(n)}\frac{1}{\sum_{k\in Z/(n)}r_k p_{kj}^{(t)}}\sum_{i\in Z/(n)}p_{ij}^{(t)}-n^2\right)$$

$$\overset{\text{引理8}}{=}\frac{1}{\ln 2}\left(\sum_{j\in Z/(n)}\frac{1}{\sum_{k\in Z/(n)}r_k p_{kj}^{(t)}}-n^2\right)$$

$$\le\frac{1}{\ln 2}\left(\sum_{j\in Z/(n)}\frac{1}{\frac{1}{n}\left(1-\frac{1}{t^k}\right)\sum_{k\in Z/(n)}r_k}-n^2\right)=\frac{1}{\ln 2}\left(\sum_{j\in Z/(n)}\frac{\sum_{l=0}^{\rfloor}\frac{1}{t^{lk}}}{\frac{1}{n}}-n^2\right)$$

$$=\frac{1}{\ln 2}\left(n\sum_{j\in Z/(n)}\sum_{l=0}^{\rfloor}\frac{1}{t^{lk}}-n^2\right)=\frac{1}{\ln 2}\left(n^2\sum_{l=0}^{\rfloor}\frac{1}{t^{lk}}-n^2\right)$$

$$=\frac{1}{\ln 2}n^2\sum_{l=0}^{\rfloor}\frac{1}{t^{lk}}=\frac{1}{\ln 2}\frac{1}{t^k}n^2\sum_{l=0}^{\rfloor}\frac{1}{t^{lk}}=\frac{1}{\ln 2}\frac{1}{t^k}n^2\frac{1}{1-\frac{1}{t^k}}=\frac{1}{\ln 2}\left(\frac{n^2}{t^k-1}\right).$$

5　应用简介

众所周知, 对于一般的分组密码, 输入输出状态集合都比较大, 当层密钥相互独立时, 转移概率矩阵的方幂计算所需要的时间与空间对于目前的计算能力来说是困难的. 但对序列密码的设计, 本文结果有着重要的指导意义. 一般意义上, 序列密码的设计可分为如下四部分: (1)源序列发生器; (2)非线性加工; (3)输出合成; (4)结合函数.

由于以域上或环上的本原多项式为源序列发生器的输出序列带有线性痕迹, 所以我们要对其进行非线性加工, 其中密码学函数迭代技术是实现非线性加工的主要技术之一, 这时密码学函数迭代的输入输出状态集一般较小, 故转移概率矩阵的方幂计算所需要的时间与空间对于目前的计算能力来说是容易做到的. 对于给定的序列密码设计中非线性加工部分的转移概率矩阵, 我们可以计算出定理 2 中的参数 k, 从而可以求得密码学函数迭代过程中, 输入输出互信息的收敛速度的上界 $\frac{1}{\ln 2}\left(\frac{n^2}{t^k-1}\right)$, 以及序列密码设计中非线性加工部分所需要的密码学函数迭代次数. 故本文结果对密码学编码, 特别是序列密码的编码有重要的指导意义. 显然满足定理 2 条件的 P 是存在的, 例如 $P=\frac{1}{n}J$. 我们将在以后的工作中, 对满足定理 2 条件的条件从理论上进一步加以分析与研究.

参考文献:

[1]　王梓坤. 随机过程通论 [M]. 北京: 北京师范大学出版社, 1996.

[2]　柳柏濂. 组合矩阵论 [M]. 北京: 科学出版社, 1996.

[3]　Thomas M Cover, Joy A Thomas. Elements of information theory [M]. NewYork: Y & Sons, Inc., 1991.

[4]　H Minc. Nonnegative matrices [M]. New York: John Wiley & Sons, 1988.

[5]　数学手册 [Z]. 北京: 人民教育出版社, 1979.

作者简介:

吕述望　男, 1941 年 3 月生于江苏沭阳, 中国科技大学研究生院(北京)信息安全国家重点实验室教授, 博士研究生导师, 1965 年毕业于中国科学技术大学无线电电子学系, 国家 973 计划课题组负责人, 长期从事密码学的研究、设计和分析工作, 曾获国家科技进步一等奖一项, 二等奖两项; 中国科学院科技进步一等奖一项; 省部级科技进步一等奖一项, 二等奖一项.

范修斌　男, 1966 年 11 月出生于山东新泰, 中国科技大学研究生院(北京)信息安全国家重点实验室在站博士后, 1989 年毕业于山东大学数学系, 2000 年获郑州信息工程大学博士学位, 主要研究方向为概率论在信息安全中的应用, 已发表学术论文二十余篇.