文章编号: 1006-5431(2003) 05-0336-02

密码学函数输入输出互信息收敛速度分析*

刘维奇, 刘　博
(山西大学 数学系, 山西 太原 030006)

摘　要: 针对密码学函数迭代模型, 给出其输入输出互信息收敛速度在一定条件下的一个上界.

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

Analysis of Mutual Information Rapidity of Convergence of Cryptographic Function

LIU Wei-qi, LIU Bo
(Dept. of Mathematics, Shanxi University, Taiyuan 030006, China)

Abstract: Using the information theory of cryptographic function and random process method, one upper bound of the rate of its convergence is acquired.

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

密码学是信息技术研究的重要课题之一, 它的基本问题是信息在传输过程中的安全保密问题. 作者通过建立信息传输过程中密码学函数的迭代模型, 给出其输入输出互信息收敛速度在一定条件下的一个上界, 改进了文献[1]中的结果.

1　密码学函数迭代的数学模型以及信道模型

密码学函数迭代的数学模型如下: 设 $f(x, y_1) = z_1$, $f(z_1, y_2) = z_2$, …, $f(z_{t-1}, y_t) = z_t$, 式中 f 为密码学函数, 即有层密钥的密码算法; x 为输入; y_i, $i = 1, 2, \cdots, t$ 为密钥; z_i, $i = 1, 2, \cdots, t$ 为 i 次迭代输出.

给出它的信道模型: 设 X 为概率空间 (Ω, F, p) 上取值于 $Z/(n)$ 的随机变量, Y_i, $i = 1, 2, \cdots, t$ 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, X, Y_i, $i = 1, 2, \cdots, t$ 相互独立. 令 $Z_1 = f(X, Y_1)$, $Z_2 = f(Z_1, Y_2)$, …, $Z_t = f(Z_{t-1}, Y_t)$, 式中 f 为可测变换, Z_i, $i = 1, 2, \cdots, t$ 取值于 $Z/(n)$, Y_{i+1}, $Z_i (1 \leq i \leq t)$ 亦相互独立. 称 X 为信道输入; Y_i, $i = 1, 2, \cdots, t$ 为信道噪声; Z_i, $i = 1, 2, \cdots, t$, 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, 下面主要讨论 $I(X, Z_t)$ 的收敛速度.

2　密码学函数迭代过程中输入输出互信息收敛速度分析

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　定义在概率空间 (Ω, F, p) 上的取非负整数值的随机变量列 $X_t (X_t = X_t(\omega), \omega \in \Omega)$, $t = 0, 1, 2, \cdots$, 成为马氏链, 如果等式 $p(X_{q+k} = i_{q+k} \mid X_q = i_q, X_{j_l} = i_{j_l}, \cdots, X_{j_2} = i_{j_2}, X_{j_1} = i_{j_1}) = p(X_{q+k} = i_{q+k} \mid X_q = i_q)$, 对任意正整数 l, q, k 及任意的非负整数 $j_l > \cdots > j_2 > j_1 (q > j_l)$, $i_{q+k}, i_q, i_{j_l}, \cdots i_{j_2}, i_{j_1}$ 成立, 只要式中左方构成的事件概率大于 0. 简记 ${}_qp_{ij}^{(k)} = p(X_{q+k} = j \mid X_q = i)$.

定义 2　称马氏链 $X_t (X_t = X_t(\omega), \omega \in \Omega)$, $t = 0, 1, 2, \cdots$, 为齐次的, 若它的转移概率矩阵 ${}_qP = P$ 与 q

* 收稿日期: 2003-06-18
基金项目: 山西省回国留学人员科研基金资助项目
作者简介: 刘维奇(1963-), 男, 硕士, 副教授. 主要从事概率论与数理统计方面的研究.

© 基金项目 (c) 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

无关, 即对任意非负整数 q 有: $p(X_{q+1}=j \mid X_q=i)=p_{ij}$, 式中 $p_{ij}^{(1)}=p_{ij}$.

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模型可知

$\forall l, l \in Z/(m)$, $p(Z_{q+1}=l \mid Z_q=l)=p(f(l,Y_{q+1})=l \mid Z_q=l)$, 因为 f 为可测变换, Y_{q+1}, Z_q 相互独立, 故可得 $p(Z_{q+1}=l \mid Z_q=l)=p(f(l,Y_{q+1})=l)$; 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 $p(f(l,Y_{q+1})=l)$ 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 $j_l>\cdots>j_2>j_1(q>j_l)$, $i_{q+k}, i_q, i_{j_l}, \cdots i_{j_2}, i_{j_1} \in Z/(n)$, 由信道迭代模型可知

$$p(Z_{q+k}=i_{q+k} \mid Z_q=i_q, Z_{j_l}=i_{j_l}, \cdots, Z_{j_1}=i_{j_1}) = \sum_{i_{q+k-1},\cdots,i_{q+1}\in Z/(n)} p(f(i_{q+k-1},Y_{q+k})=i_{q+k}, \cdots, f(i_q,Y_{q+1})=i_{q+1} \mid Z_q=i_q, Z_{j_l}=i_{j_l}, \cdots, Z_{j_1}=i_{j_1}) = \sum_{i_{q+k-1},\cdots,i_{q+1}\in Z/(n)} p(f(i_{q+k-1},Y_{q+k})=i_{q+k}, f(i_{q+k-2},Y_{q+k-1})=i_{q+k-1}, \cdots, f(i_q,Y_{q+1})=i_{q+1}) = \sum_{i_{q+k-1},\cdots,i_{q+1}\in Z/(n)} p_{i_{q+k-1}i_{q+k}}, p_{i_{q+k-2}i_{q+k-1}} \cdots p_{i_q i_{q+1}} = p_{i_q i_{q+k}}^{(k)} = p(Z_{q+k}=i_{q+k} \mid Z_q=i_q),$$

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.

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.

引理 1　当 $x>0$, $\ln x \le x-1$ 时, 令 $p(X=i)=r_i$, $\forall i \in Z/(n)$.

引理 2　$p(Z_t=j, X=i)=r_i p_{ij}^{(t)}$.

定理　若 P 为随机矩阵且满足 $\forall t \in Z^+$, $\forall i,j \in Z/(n)$, $p_{ij}^{(t)} \ge (1/n)Q(t)$, $Q(t)$ 为 t 的函数, $0<Q(t)<1$, 则 $I(X,Z_t) \le n^2(1/Q(t)-1)$; 若 $\lim\limits_{t\to\infty} Q(t)=1$, 则 $\lim\limits_{t\to\infty} I(X,Z_t)=0$.

证明

$$I(X,Z_t)=\sum_{i,j\in Z/(n)} p(X=i,Z_t=j)\log\frac{P(X=i,Z_t=j)}{P(X=i)P(Z_t=j)}=\sum_{i,j\in Z/(n)} r_i p_{ij}^{(t)}\log\frac{r_i p_{ij}^{(t)}}{r_i P(Z_t=j)} \le$$

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

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

$$(n/Q(t))\sum_{j\in Z/(n)}\sum_{i\in Z/(n)} p_{ij}^{(t)}-n^2 \le (n/Q(t))\sum_{i\in Z/(n)} 1-n^2 = n^2(1/Q(t)-1).$$

当 $\lim\limits_{t\to\infty} Q(t)=1$ 时, $\lim\limits_{t\to\infty} I(X,Z_t)=\lim\limits_{t\to\infty} n^2\left(\frac{1}{Q(t)}-1\right)=0$. 证毕.

推论　若 P 为双随机矩阵且满足 $\forall t \in Z^+$, $\forall i,j \in Z/(n)$, $p_{ij}^{(t)} \ge (1/n)(1-(1/t^k))$, $k \in R^+$, 则

$$I(X,Z_t) \le (1/\ln 2)(n^2/(t^k-1)).$$

推论就是文献[1]的主要结果, 定理相对于推论有了很大的改进, 对于随机矩阵的要求由双随机矩阵变为随机矩阵, 而且对于 p_{ij} 的要求也由 $p_{ij}^{(t)} \ge (1/n)(1-(1/t^k))$ 变为 $p_{ij}^{(t)} \ge (1/n)Q(t)$, $Q(t)$ 为大于 0 小于 1 的函数, 从而放宽了初始条件的要求. 推论只是定理的特殊情形, 定理中当矩阵为双随机矩阵且 $Q(t)$ 为 $(1/n)(1-(1/t^k))$ 时, 由定理易得推论.

3　应用简介

对于给定的序列密码设计中的转移概率矩阵, 可以计算出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, 以及序列密码设计中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着重要的指导意义.

参考文献:

[1]　吕述望. 密码学函数迭代原理信息论分析[J]. 电子学报, 2002, 30(10): 1511-1513.

[2]　张鸣瑞, 邹世开. 编码理论[M]. 北京: 北京航空航天大学出版社, 1990. 2-10

[3]　王梓坤. 随机过程通论[M]. 北京: 北京师范大学出版社, 1996. 50-57, 126-151.

[4]　沈永欢, 梁在中等. 实用数学手册[M]. 北京: 科学出版社, 1979. 818-836.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net