复合离散混沌动力系统与序列密码体系

李红达, 冯登国
(中国科学院研究生院信息安全国家重点实验室, 北京 100039)

摘 要: 本文构造了复合离散混沌动力系统, 并研究了它不变分布和迭代轨迹的若干性质. 利用两个特殊的离散混沌系统, 提出了基于复合离散混沌动力系统的序列密码体系. 由于复合离散混沌系统对初始条件的敏感性和迭代过程的伪随机性, 本文提出的序列密码算法将明文和密钥序列完全融合在密文序列中, 使它们与密文之间形成了复杂而敏感的非线性关系, 这就防止了密文对有关信息的泄露, 从而使系统具有很高的安全性. 该算法还拥有很大的密钥空间和均匀分布的密文.

关键词: 混沌; 动力系统; 序列密码
中图分类号: TN918 文献标识码: A 文章编号: 0372-2112 (2003) 08-1209-04

Composite Nonlinare Descrete Chaotic Dynamical Systems and Stream Cipher Systems

LI Hong-da, FENG Deng-guo
(State Key Lab of Information Security Graduate School of Chinese Academy of Sciences, Beijing 100039, China)

Abstract: Although discrete chaotic systems is sensitive to initial conditions and its behavior seems to be random, it is not real-ly stochastic process but determinate. It results in that chaos based encryption schemes are not good as we expect. In order to enhance the performance of the encryption algorithms based on discrete chaotic dynamical system, we present composite discrete chaotic dynam-ical systems and gives some results about its invariant distribution density and iteration sequence. We present a new approach to stream cipher utilizing a peculiar composite discrete chaotic dynamical system. Because of its sensitivity to initial conditions and randomness of the iteration sequence, the approach mingles secret keys with plaintext by iterating the chaotic system to produce ciphertext. Therefor they hold very complex and sensitive nonlinear relations. It prevents ciphertext to leak the information of plaintext and secret key and makes the security of the algorithm independent of the complexity of the ciphertext. The algorithm is provided with larger secret space and uniform distributing ciphertext.

Key words: chaos; dynamical system; stream cipher

1 引言

传统的密码体制都基于所谓的困难问题, 随着信息时代的到来和人类计算能力的提高, 人们开始探索不基于某类困难问题的物理编码体制, 混沌加密体制就是其中的一种. 非线性混沌系统由于对初始条件敏感而使其迭代轨迹与初始条件有着复杂的非线性关系, 表现出了很好的伪随机性. 从 Habu-su[4] 于 1991 年最早将离散混沌动力系统用于构造加密算法后, 这方面的研究已经引起了人们的注意, 目前提出的一些基于混沌系统加密算法[3~7, 9~13], 由于加密算法本身的缺陷或离散混沌系统的固有特性安全性一般都不够高[2, 14, 15, 16]. 密码体系实际上是一个由密钥决定的从明文空间到密文空间的可逆变换, 理想的序列密码体系应满足以下几个条件: (1) 有很大的密钥空间; (2) 具有复杂的非线性密码变换, 而且不同密钥对应的完全不同的密码变换; (3) 明文与变换信息很好地融合在一起形成密文, 以减少密文对变换信息的泄露; (4) 密文的分布是均匀的, 以得到大的密文空间. 本文提出的复合离散混沌系统, 其迭代轨迹不仅对初始条件敏感性, 而且还具有更好的伪随机性, 从而为构造具有上述性质的密码体系提供了一个途径. 文中提出的基于复合离散混沌系统的同步序列密码体系, 一方面利用复合离散混沌动力系混沌系统的特性, 建立了一个具有均匀分布的密文的复杂非线性密码变换, 另一方面还通过对复合混沌系统迭代轨迹的选择将变换信息与明文完全融合在一起, 从而减少了密文对信息的泄露, 得到安全的密码系统.

收稿日期: 2001-12-05; 修回日期: 2002-07-01
基金项目: 中科院王宽诚博士后工作奖励基金; 信息安全国家重点实验室开放课题

2 离散混沌系统

2.1 两个特殊的离散混沌系统

我们首先在[0,1]上构造两个特殊的非线性离散混沌动力系统,并对其性质进行分析. 在[0,1]定义函数

$$f_0(x)=\sqrt{|2x-1|} \tag{1}$$

$$f_1(x)=1-\sqrt{|2x-1|} \tag{2}$$

由此可以得到两个非线性迭代系统 $x_{n+1}=f_r(x_n)$, $r=0,1$, 它们具有如下性质:

引理 1 (1) $x_{n+1}=f_r(x_n)$, $r=0,1$ 是混沌迭代系统.

(2) 对应的不变分布密度函数(invariant distribution density,简称不变分布)分别是 $Q_0(x)=2x$ 和 $Q_1(x)=2-2x$.

证明 (1) 由于在(0,1)上, $f_q'(x)>1$, 则由动力系统的 Lyapunov 指数的定义[19]可知 $x_{n+1}=f_r(x_n)$, $r=0,1$ 都是离散混沌动力系统.

(2) 同样,由于在(0,1)上, $f_q'(x)>1$, 存在唯一的分布密度函数 $Q(x)$ 满足[8]

Ó $Q(x)\geq 0$.

Ó $\int_{[0,1]}Q(x)\,dx=1$.

Ó $Q(x)=PQ(x)$. 其中 P 是著名 Perron-Frobenius 算子.

由 $Q(x)=PQ(x)=\frac{d}{dx}\int_{f_r^{-1}([0,x])}Q(t)\,dt$ 可得,

$$Q_0(x)=\frac{d}{dx}\left(-\int_{\frac{1}{2}(1-x^2)}^{\frac{1}{2}}Q_0(t)\,dt+\int_{\frac{1}{2}}^{\frac{1}{2}(1+x^2)}Q_0(t)\,dt\right)$$

$$=Q_0\left(\frac{1-x^2}{2}\right)x+Q_0\left(\frac{1+x^2}{2}\right)x$$

不难验证 $Q_0(x)=2x$ 正是满足条件的唯一解. 同理可得 $Q_1(x)=2-2x$.

为进一步研究系统的属性,我们考察迭代序列的相关性. 依文献[8],迭代序列 $\{x_n=f(x_{n-1})\}$ 的自相关函数定义为:

$$C_f(n)=\frac{1}{R^2}\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}(x_i-\bar{x})(x_{i+n}-\bar{x}) \tag{3}$$

其中 $\bar{x}$ 与 R^2 分别是它的均值和方差. 由 Birkhoff 遍历定理,式(3)又可以写为:

$$C_f(n)=\frac{1}{R^2}\left(\int_{[0,1]}(x-\bar{x})(f^{(n)}(x)-\bar{x})\,dx\right) \tag{4}$$

它反映所有迭代轨迹的自相关函数的一种平均. 一般希望得到具有 $C_f(n)=D(n)$ 性质的迭代系统或序列,但对式(1)、(2), $x=2/3$, 利用 $f_r^{(n)}(1-x)=f_r^{(n)}(x)$, 经适当的变换得:

$$C_{fr}(n)=\frac{1}{R^2}\left(\int_0^{\frac{1}{2}}\left(x-\frac{2}{3}\right)\left(f_r^{(n)}(x)-\frac{2}{3}\right)dx+\int_{\frac{1}{2}}^{1}\left(x-\frac{2}{3}\right)\left(f_r^{(n)}(x)-\frac{2}{3}\right)dx\right)$$

$$=\frac{2}{3}C_{fr}(n-1)=\left(\frac{2}{3}\right)^n C_{fr}(0)$$

尽管它们的相关函数不满足 $C_f(n)=D(n)$,但衰减很快.

2.2 复合离散混沌动力系统

定义 1 设 $x_i=f_q(x_{i-1})$, $q=0,1,\cdots,k$ 是定义在[0,1]上的一组离散混沌动力系统,对任意序列为 $R=(r_1,r_2,\cdots)\in I\{0,1,\cdots,k\}^{]}$,称

$$x_i=f_{r_i}(x_{i-1}),\ i=1,2,\cdots \tag{5}$$

为迭代系统组在序列 R 下的复合系统, R 为复合序列. $x_i=f_q(x_{i-1})$, $q=0,1,\cdots,k$ 称为子系统.

复合迭代系统的动力行为与复合序列 R 有关,若当 i 充分大时, r_i 为常数,则复合系统退化为单一混沌系统. 一般地,复合迭代系统保持了所有子迭系统的混沌特性,比其单个子系统的行为要复杂得多.

定理 1 若 $|f_q'(x)|>1$, $q=0,\cdots,k$, 那么对任意的复合序列 R,复合系统式(5)是离散混沌系统.

证明 设 $R=\{r_i\}$ 是任意复合序列, $\{x_i\}$ 是由初始点 x_0 得到的迭代序列,由 Lyapunov 指数的定义[19]易知式(5)的 Lyapunov 指数 $K>0$, 所以是离散混沌系统.

定理 2 设 $N(q)$ 表示复合序列 $R=\{r_i\}$ 前 N 个元素中 q 的个数,若 $\lim_{n\to\infty}[N(q)/N]=A(q)$, 则式(5)不变分布密度函数是

$$Q(x)=A(0)Q_0(x)+\cdots+A(k)Q_k(x) \tag{6}$$

其中 $Q_0(x),\cdots,Q_k(x)$ 分别是子系统的不变分布密度函数.

证明 设复合混沌系统的不变分布密度函数为 $Q(x)$. 根据假设,我们可以认为 $P(r_i=q)=A(q)$. 为方便,迭代过程统一表示为 $x_i=F(x_{i-1})$,那么对任意的 $x\in[0,1]$, $P(F(t)\in[0,x])=\sum_{r=0}^{k}P(f_q(t)\in[0,x],\ q=r)$. 而 $P(f_r(t)\in[0,x])=\int_{f_r(t)\in[0,x]}Q(t)\,dt$, 于是 $Q(x)=\frac{d}{dx}P(F(t)\in[0,x])=\sum_{r=0}^{k}A(r)\frac{d}{dx}\int_{f_r(t)\in[0,x]}Q(t)\,dt$. 由此便知结论正确.

3 基于复合离散混沌动力系统的序列密码

本节采用由混沌动力系统(1)与(2)在任意二进制序列 $R=\{r_i\}$ 下的复合离散混沌动力系统,有如下的结论.

定理 3 设 $f_0(x)$, $f_1(x)$ 分别由式(1)与(2)所定义,那么由式(5)所定义的复合离散混沌动力系统具有如下性质:

Ó 若 $\lim_{N\to\infty}[N(0)/N]=1/2$, 则复合混沌系统具有均匀不变分布.

Ó 对任意给定序列 $\{r_i\}$, 迭代序列 $\{x_i\}$ 的自相关函数满足 $C(n)=D(n)$.

证明 第一个性质由定理 1 及引理 3 可得. 对第二个性质,记 $f_{D(m,n)}(x)=f_{D(m+1)}\circ\cdots\circ f_{D(m+n)}(x)$, 则由式(4)得

$$C(n)=\frac{1}{R^2}\int_{[0,1]}\left(x-\frac{1}{2}\right)\left(f_{D(m,n)}(x)-\frac{1}{2}\right)dx$$

若 $n>0$, 令 $y=1-x$, 代入上式,利用 $f_i(1-x)=f_i(x)$, $i=0,1$, 得

$$C(n)=-\frac{1}{R^2}\int_{[0,1]}\left(y-\frac{1}{2}\right)\left(f_{D(m,m)}(y)-\frac{1}{2}\right)dy$$

由此可得结论.

为建立基于它的序列密码体系,定义算子组 $T_j:[0,1]\to\{0,1\}$ 为 $T_j(x)=\lfloor 2^j x\rfloor \bmod 2$, 于是可以将由复合离散混沌动力系统式(5)得到的混沌序列 $\{x_i\}$ 转化为二进制数字序列组 $\{s_i^j\}$. 对具有不变分布 $Q(x)$, 我们定义[0,1]上的子集 E 的概率测度 $L(E)=\int_E Q(x)\,dx$, 其中的积分为 Lebesgue 积分. 于是有如下的定理:

定理 4　对任意的 $j>0$, 有

(1) 若二进制复合序列$\{r_i\}$满足 $P(r_i=1)=1/2$, 则$\{s_i^j\}$各 bit 位独立同分布, 即 $P(a_1,\cdots,a_n)\in F_2^n$, 有

$$p(s_i=a_i,\ i=1,2,\cdots,n)=2^{-n}$$

(2) 序列$\{s_i^j\}$的自相关函数满足 $C_s(n)=D(n)$.

证明　我们只对 $j=1$ 给出证明, j 等于其它值类似. 为叙述方便, n 次复合迭代简记为 $x_n=F^{(n)}(x_0)$.

(1) 由于 $P(r_i=1)=1/2$, 故复合混沌系统既有均匀的不变分布 $Q(x)=1$. 若 $n=1$, $P(s_1^j=a_1)=P(s_1^j=a_1, r_1=0)+P(s_1^j=a_1, r_1=1)=1/2$. 现假设 $n=k$ 时成立, 当 $n=k+1$ 时,

$$P(s_i=a_i, 1\leqslant i\leqslant k+1)=P(s_i=a_i, 1\leqslant i\leqslant k, r_{i+1}=0)+P(s_i=a_i, 1\leqslant i\leqslant k, r_{i+1}=1)$$

记 $E(n,R_k)=\{x: s_i=a_i,\ i=1,2,\cdots,k\}$, 其中 $R_k=(r_1,\cdots,r_k)$, $E(0)=\{x: T_j(F^{(k+1)}(x))=0\}$, 则

$$\begin{aligned}P(s_i=a_i, 1\leqslant i\leqslant k+1)&=\frac{1}{2}L(E(n,R_k)\cap E(0))\\&\quad+\frac{1}{2}L(E(n,R_k)\cap([0,1]-E(0)))\\&=\frac{1}{2}L(E(n,R_k))\\&=\frac{1}{2}P(s_i=a_i,\ i=1,2,\cdots,k)\end{aligned}$$

由此得结论.

(2) 对任意的 R_k 及正整数 n, 由式(4)得

$$\begin{aligned}C_s(n)&=\frac{1}{R^2}\left(Q_{[0,1]}\left(T_jx-\frac{1}{2}\right)\left(T_jF^{(n)}(x)-\frac{1}{2}\right)dx\right)\\&=\frac{1}{R^2}\left(Q_{\frac{1}{2}}\left(T_jx-\frac{1}{2}\right)\left(T_jF^{(n)}(x)-\frac{1}{2}\right)dx\right)\\&\quad+\frac{1}{R^2}\left(Q_{\frac{1}{2}}\left(T_j(1-x)-\frac{1}{2}\right)\left(T_jF^{(n)}(x)-\frac{1}{2}\right)dx\right)\end{aligned}$$

由于 $T_j(1-x)+T_j(x)=1$ 除有限个点外成立, 从而可得 $C_s(n)=D(n)$.

假设明文是一个二进制的序列, 即 $M=m_1m_2,\cdots,m_L$. 首先确定一个移位寄存器 G, 其输出序列为 $R=\{r_i\}$, 要求输出序列的 0 与 1 大体均衡. 以$\{U(r_i, m_i)\}$作为系统的复合序列, 其中 U为布尔函数. 为简单取 $U(r_i, m_i)=r_i\oplus m_i$. 下面为了叙述方便, 称 G 为复合序列生成器, R 为复合序列. 序列密码体系的加密过程为图 1. 具体算法描述如下:

(1) 选定一个迭代初值 x_0, 生成器 G 的初值 g_0 及变换 T_j 的参数 j.

(2) i 从 1 到 L, 完成下列步骤:

Ó 由 G 得到 r_i, 确定迭代所采用的函数的下标: $q(i)=r_i\oplus m_i$

Ó 迭代计算: $x_i=f_{q(i)}(x_{i-1})$, 若 $T_j(x_i)=T_j(1-x_i)$, 则令 $x_i=f_{q(i)}(\sqrt{0.99}x_{i-1})$

Ó 离散化混沌轨迹, 得到密文 bit 位: $c_i=T_j(x_i)$

(3) 获得密文 $C=c_1,\cdots,c_L$

以迭代的初值 x_0 和序列生成器 G 的初始向量 g_0 作为密钥, 密文是 $C=c_1,\cdots,c_L$. 加密算法中当 $T_j(x_i)=T_j(1-x_i)$ 时, 令 $x_i=f_{q(i)}(\sqrt{0.99}x_{i-1})$ 是为了用简单的方法使 $T_j(x_i)\neq T_j(1-x_i)$, 从而保证在解密时能获得加密过程中所选取的迭代函数的下标. 加密过程是复合混沌系统的迭代过程, 以 $m_i\oplus r_i$ 作为迭代是所选取的函数的下标, 而迭代轨迹点位置作为密文 c_i, 经过混沌迭代的这种调制后, 明文和密钥序列已完全被融合在复合密文(混沌系统的轨迹)中, 明文的任一位 m_i 将影响密文的从 c_i 到 c_L 的所有 Bit 位.

解密算法也简单. 由密钥 x_0 和 g_0, 可以得到加密时所得到的轨迹序列$\{x_i\}$和复合序列$\{r_i\}$, 并利用 $f_1(x)=1-f_0(x)$ 和 $T_j(x_i)\neq T_j(1-x_i)$, 就可以得到加密迭代过程中所采用的函数下标序列 $q(i)$, 再由 $q(i)=m_i\oplus r_i$ 便可恢复明文. 解密过程如图 2, 具体的算法可详细描述如下:

(1) 获得密钥 x_0 及 g_0

(2) i 从 1 到 L, 完成下列步骤:

Ó 迭代计算并离散化混沌轨迹: $xc_i=f_1(xc_{i-1})$, 若 $T_j(xc_i)=T_j(1-xc_i)$, 则令 $xc_i=f_1(\sqrt{0.99}x_{i-1})$, $s_i=T_j(xc_i)$

Ó 确定迭代采用函数下标: $q(i)=1-s_i\oplus c_i$

Ó 由 G 得到 r_i, 获得到明文 bit 位: $m_i=r_i\oplus q(i)$

(3) 获得明文 $M=m_1,\cdots,m_L$

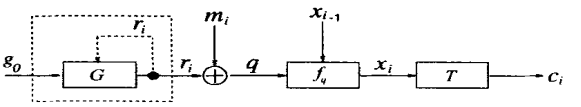

图 1　加密算法

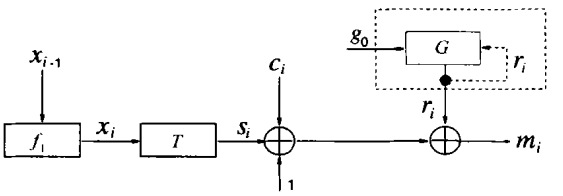

图 2　解密算法

与传统的序列密码体系不同, 加密过程通过复合混沌系统的调制使明文很自然地嵌入到了密文(迭代序列)中, 这一方面使得密文不再具有明文的统计特性, 另一方面使他们之间具有敏感而复杂的关系, 防止了密文对明文及密钥信息的泄露. 因此, 密码体系的安全性不依赖于复合序列生成器 G 的特性, 从而可以不要或放宽对密钥序列 r_i 的周期性和复杂性等方面要求. 为了得到均匀分布的密文序列, 只要由 G 生成的密钥序列的具有均匀分布的 0 和 1 即可, 因此可以很方便地构造简单快速的序列生成器 G, 比如简单的移位寄存器. 复合混沌系统的特性完全可以保证算法的密码强度, 可以使用简单的生成器 G, 甚至使用固定的 r_i, 而只以 x_0 为密钥.

4　实验与分析

由于密文 C 的每一 bit 位 c_i 与密钥及明文的若干 bit 位 $m_1,\cdots,m_i$ 有关, 复合离散混沌动力系统的迭代过程使它们已成一个整体, 相互之间具有复杂的非线性关系. 由于对任意的 $c=0$ 或 $c=1$, $L\{x: T_j(f_0(x))=c\}+L\{x: T_j(f_1(x))=c\}=1$, 密码分析者在获得密文的情况下, 试图进行反向的迭代以得

到密钥或明文的信息是完全不可能的. 由算法可以看出: 在无限精度意义下, 对确定的复合序列生成器 G 和两个任意等长的二进制序列 M, C 及 g_0, 可以找到初始点(密钥) x_0, 使 M, C 是其对应的明文和密文. 当运算为有限精度时, 在一定尺度上保持了这个性质, 在很广泛的条件下, 我们可以得到均匀分布的密文, 因此可以有效地抵抗统计分析. 以迭代的初始点 x_0 作为密钥, 算法也拥有很大的密钥空间, 足以抵御强力攻击.

基于复合混沌系统的序列密码算法, 使明文、密钥与密文之间的关系敏感而复杂. 同一明文, 不同的密钥所产生的密文是完全不同的; 而同样的密钥, 对相似明文可以得到差别很大的密文. 若取二进制序列生成器 G 为 $r_i = 1 \oplus r_{i-1}$, $r_0 = 1$, 离散化算子 T_j 的参数分别取为 j = 1, 4, 6, 用两个不同的密钥 $x_0 = 0.3164857$ 与 $x_1 = 0.3164858$ 对大量随机序列进行了加密和解密测试, 结果表明: (1) 当 j = 1 时, 它们对同一明文加密后的密文(或同一密文解密后的明文) 分别大约有 30.5%) 42.7% 的 bit 位不同; 当 j = 4, 6 时, 大约有 45.8%) 50.7% 的 bit 位为不同. 这说明 j 的值影响系统对密钥的依赖程度, j 的增大提高密文对密钥的敏感性; (2) 由于 $L\{x: T_j(f_r(x)) = r\} = E\{x: T_j(f_r(x)) = 1 - r\} = 1/2 (r = 0, 1)$, 而迭代轨迹均匀分布, 所以密文 C 序列与 $\{r_i \oplus m_i\}$ 的相关度[18] A(n) 也很小, 这说明密文对明文的泄露很少. 图 3 为随机选取的三个不同的密钥 x_0 对一个随机的明文序列的相关度 A(n) 与长度 n 的关系(j = 4).

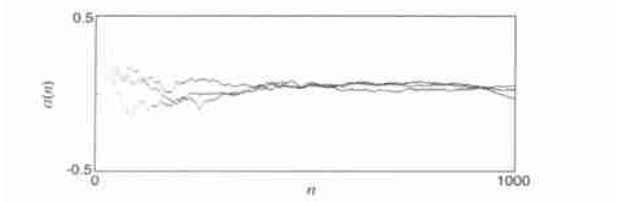

图 3 相关度 A(n)

5 结论

基于复合混沌系统的序列密码系统, 利用了复合混沌系统对初始条件的敏感性和迭代过程的伪随机性, 使明文和密钥与密文间的关系敏感而复杂, 明文和密钥完全融合在密文中, 这有利于减少了密文对明文和密钥信息的泄露, 因此具有很高的安全性. 文中提出的序列密码算法有如下特点: (1) 有较大的密钥空间; (2) 系统有良好的安全性; (3) 具有均匀分布的密文且对密钥很敏感; (4) 明文每一 bit 与密文的若干 bit 有关, 反之亦然.

参考文献:

[1] Bruce Schneier. Applied Cryptgraphy: Protocols, Algorithms, and Source Code in C [M]. John Wiley & Sons Inc, New York, 1993, 191- 216.

[2] E Biham. Cryptanalysis of the chaotic2map cryptosystem suggested at EUROCRYPT. 91 [A]. ed. D. W. Davies, Advance in cryptology2EU2ROCRYPT91 [C]. LNCS 547, Springer2Verlag, Berlin: 532- 534.

[3] Marco G tz, Kristina Kelber, Wolfgang Schwarz. Discrete2time chaotic encryption systems2part 1: statistical design applied [J]. IEEE Trans. circuits syst. 1997, 44(10): 963- 970.

[4] T Habutsu, Y Nishio, I Sasase, S mori. A secret key cryptsystem by it2erating a chaotic map [A]. Advance in cryptology2EOROCRYPTc 91 [C]. Springer2verlag, Berlin, 127- 136.

[5] E Alvarez, A FernÅndez, P Garcia, J Jim nez, A Marcano. New ap2proach to chaotic encryption [J]. Physics letters A, 1999, 263: 373- 375.

[6] M S Baptista. Cryptography with chaos [J]. Physics Letters A, 1998, 240(12): 50- 54.

[7] Zbigniew Kotulski, Janusz Szczepaô ski. Application of discrete chaotic dynamical systems in cryptography2DCC method [J]. Internatiobal J. Bifurcation and Chaos, 1999, 9(6): 1121- 1135.

[8] A Baranovsky, D Daems. Design of one2dimensional chaotic maps with prescribed statistical properties [J]. Int. J. Bifurcation and Chaos, 1995, 5(6): 1585- 1598.

[9] J Fridrich. Symmetric ciphers based on two2dimensional chaotic maps [J]. Int J Bifurcation and Chaos, 1998, 8(6): 1259- 1284.

[10] Toni Stojanovski, Ljupc ¡o Kocarev. Chaos2based random number gen2erators- - part I: analysis [J]. IEEE Trans Circuits Syst. I. 2001, 48(3): 281- 288.

[11] Toni Stojanovski, Johnny Pihl, Ljupc ¡o Kocarev. Chaos2based random number generators- - part II: practical realization [J]. IEEE Trans Circuits Syst. I, 2001, 48(3): 382- 385.

[12] Janusz Szczepaacuteô ski, Zbigniew Kotulski. On some models of pseu2dorandom number generators based on chaotic dynamical system. http: / / www. counterpane. com/ biblio.

[13] Naoki Masuda, Kazuyuki Aihara. Cryptosystems with discretized chaotic maps [J]. IEEE Trans. Circuits Syst. I, 2002, 49(1): 28- 40.

[14] Ljupc ¡o Kocarev. Cgaos2based cryptography: A brief overview [J]. IEEE Trans. Circuits Syst. magazina, 2001, 1(3): 6- 21.

[15] Goce Jakimoski, Ljupc ¡o Kocarev. Chaos and cryptography: block en2cryption ciphers based on chaotic maps [J]. IEEE Trans Circuits Syst. I, 2001, 48(2): 163- 169.

[16] G Alvarez, F Montoya, M Romera, G. Pastor. Cryptanalysis of a chaotic encryption system [J]. Physics Letters A, 2000, 276: 191- 196.

[17] 冯登国, 裴定一. 密码学导引 [M]. 北京: 科学出版社, 1999: 56- 106.

[18] 冯登国. 密码分析学 [M]. 北京: 清华大学出版社, 2000: 55- 92.

[19] 吴祥兴, 陈忠, 等. 混沌学导论 [M]. 上海: 上海科学技术文献出版社, 2001: 57- 83.

作者简介:

李红达 男, 1960 年 7 月生于陕西省延安市, 现在中科院研究生院信息安全国家重点实验室的博士后流动站, 主要从事分形与混沌理论与应用、理论密码学等领域的研究. Email: lihongda@is. ac. cn.

冯登国 男, 1965 年 5 月生于陕西省, 博士, 研究员, 博士导师. 研究方向: 信息安全.