基于复合离散混沌动力系统的序列密码算法*

李红达[1+], 冯登国[1,2]

[1](中国科学院 研究生院 信息安全国家重点实验室,北京 100039)

[2](中国科学院 软件研究所 信息安全国家重点实验室,北京 100080)

Stream Cipher Algorithms Based on Composite Nonlinear Discrete Chaotic Dynamical Systems

LI Hong-Da[1+], FENG Deng-Guo[1,2]

[1](State Key Laboratory of Information Security, Graduate School, The Chinese Academy of Sciences, Beijing 100039)

[2](State Key Laboratory of Information Security, Institute of Software, The Chinese Academy of Sciences, Beijing 100080)

+ Corresponding author: Phn: 86-10-88258713, E-mail: lihongda@is.ac.cn

http://www.is.ac.cn

Received 2002-01-30; Accepted 2002-09-17

Li HD, Feng DG. Stream cipher algorithms based on composite nonlinear discrete chaotic dynamical systems. *Journal of Software*, 2003,14(5):991~998.

http://www.jos.org.cn/1000-9825/14/991.htm

Abstract: Two approaches are presented to stream cipher utilizing a peculiar dynamical system called as composite discrete chaotic dynamical system (for short, composite system), which consists of two chaotic dynamical systems. The secret keys are the initial state of the chaotic dynamical systems, and the plaintext is used as its composite sequence that decides the choice of iterating function in the iterating process. Because of sensitivity of the composite system to initial conditions and randomness in the iterating process, the approach mingles secret keys with plaintext when using the composite system to produce ciphertext. Therefore they hold very complex and sensitive nonlinear relations. The algorithm is also provided with uniform distributing ciphertext. These peculiarities prevent ciphertext to leak the information of plaintext and secret key and make the security of the algorithms not depend on the complexity of the ciphertext.

Key words: chaos; composite dynamical system; stream cipher

摘 要: 利用复合离散混沌系统的特性,提出了两个基于复合离散混沌系统的序列密码算法.算法的加密和解密过程都是同一个复合离散混沌系统的迭代过程,取迭代的初始状态作为密钥,以明文序列作为复合系统的复合序列,它决定了迭代过程中迭代函数的选择(或明文与密钥),然后将迭代轨迹粗粒化后作为密文.由于迭代对初始条件的敏感性和迭代函数选择的随机性,密钥、明文与密文之间形成了复杂而敏感的非线性关系,而且密文和明文的相关度也很小,从而可以有效地防止密文对密钥和明文信息的泄露.复合离散混沌系统均匀的不变分

* Supported by the Award Foundation for the K. C. Wong Post-Doctoral of the Chinese Academy of Sciences of China (中国科学院王宽诚博士后工作奖励基金)

第一作者简介: 李红达(1966－),男,陕西延安人,博士,讲师,主要研究领域为分形与混沌理论,密码学.

布还使密文具有很好的随机特性.经分析表明,系统具有很高的安全性.

关键词: 混沌;复合动力系统;序列密码

中图法分类号: TP309 **文献标识码**: A

序列密码是一种重要的私钥密码体制,这方面的研究工作一直是密码学中一个十分活跃的研究课题.目前已提出的序列密码算法[1,2]基本上都是利用密钥流和明文的异或而得到密文,因此,序列密码体系的关键是密钥流的生成,系统的安全性也完全由密钥流的性质所决定.目前提出的攻击方法[3]大都利用了这一特点.

非线性混沌系统具有对初始条件敏感且使其迭代轨迹在一定程度上不可预测的特点,同时与初始条件存在着复杂的非线性关系.由于非线性混沌系统这一良好的密码属性,基于混沌系统的密码体系成为近年来倍受关注的热点之一.自从 Habutsu[4]于 1991 年最早将离散混沌动力系统用于构造加密算法之后,这方面的研究已经引起了人们的注意,提出了一些基于离散混沌系统的加密[5~9]和随机数生成算法[10,11],但安全性一般都不够高[12].本文提出的由两个非线性离散混沌系统构成的复合混沌系统,其迭代过程不仅具有对初始条件的敏感性,而且具有依照复合序列选择迭代函数的灵活性,因此迭代过程还具有一定的随机性,是构造密码体系的理想工具.在分析复合混沌系统迭代性质的基础上,利用复合离散混沌系统的特点,本文提出了两种新的同步序列密码方法,并对安全性进行了分析.该方法的加密和解密是一个复合离散混沌系统相同的迭代过程,而系统的密钥就是迭代初始点.对于给定密钥,迭代过程决定了由明文到密文的密码变换完全由密钥和明文序列共同决定,这使得密钥、明文和密文之间具有复杂而敏感的非线性关系,密钥或明文的微小改变都会使这种非线性关系发生根本的变化.由明文和密钥通过复合混沌迭代系统调制所产生的密文与明文的相关度很小,而且复合混沌系统的特性还保证明文的每个 bit 为等概率地被变为 0 或 1,这一方面减少了密文对明文和密钥信息的泄露,另一方面还使密文序列具有良好的分布特性,有利于抵御统计分析,从而保证密码系统具有很高的安全性.

1 复合离散混沌系统

定义 1. 设 $x_i=f_q(x_{i-1}),q=0,1$,是两个离散混沌动力系统,对任意序列 $R=(r_1,r_2,\ldots)\in\{0,1\}^\infty$,称

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

为这两个迭代系统在序列 R 下的复合离散混沌动力系统(简称为复合代系统),记为(f_0,f_1,R),其中 R 称为复合序列.对 $q=0$ 或 $q=1$,$x_i=f_q(x_{i-1}),i=1,2,\ldots$,称为它的子系统.

复合迭代系统(1)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,则复合迭代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,比单个的其子系统的行为要复杂得多.

定理 1. 设 $N(q)$表示复合序列 $R=\{r_i\}$前 N 个元素中 q 的个数,若 $\lim\limits_{N\to\infty}\dfrac{N(q)}{N}=\alpha(q)$,则复合迭代系统(1)的不变分布密度函数(invariant distribution density,简称不变分布)为

$$\rho(x)=\alpha(0)\rho_0(x)+\alpha(1)\rho_1(x), \tag{2}$$

其中 $\rho_0(x),\rho_1(x)$ 分别是子系统的不变分布密度函数.

证明:设复合迭代系统的不变分布为 $\rho(x)$.将迭代过程统一表示为 $x_i=F(x_{i-1})$,用 $P(\cdot)$ 表示概率,那么对[0,1]上任意的 x_0,

$$P(F(t)\in[0,1])=\sum_{r=0}^{1}P(f_q(t)\in[0,x],q=r)\alpha(r)=\sum_{r=0}^{1}\alpha(r)\int_{f_r^{-1}(t)\in[0,x]}\rho_r(t)\mathrm{d}t,$$

于是得到

$$\rho(x)=\frac{\mathrm{d}}{\mathrm{d}x}P(F(t)\in[0,1])=\sum_{r=0}^{1}\alpha(r)\frac{\mathrm{d}}{\mathrm{d}x}\int_{f_r^{-1}(t)\in[0,x]}\rho_r(t)\mathrm{d}t,$$

由此便知结论正确. □

定义 2. 设 $x_i=f_q(x_{i-1})$, $\rho=\rho_q(x)$ $(q=0,1)$是两个离散混沌动力系统和对应的不变分布,若存在正实数 $0<\alpha<1$,使 $\alpha\rho_0(x)+(1-\alpha)\rho_1(x)\equiv1$,则称它们分布互补;若还有 $f_0(x)+f_1(x)=1$,则称它们严格互补.

由定义及复合迭代系统的不变分布公式(2)可以看出,分布互补的离散混沌动力系统组一定存在复合序列

R,使得在R下的复合迭代系统具有均匀分布.若构成它的子系统都具有均匀的不变分布,则在任意的复合序列R下,复合系统具有均匀不变分布.

现在,我们在[0,1]上构造一对严格互补的非线性复合离散混沌动力系统.在[0,1]定义函数

$$f_0(x)=\begin{cases}1-\sqrt{1-2x}, & 0\le x<\dfrac{1}{2},\\ \sqrt{2x-1}, & \dfrac{1}{2}\le x\le 1\end{cases}\qquad f_1(x)=\begin{cases}\sqrt{1-2x}, & 0\le x<\dfrac{1}{2}\\ 1-\sqrt{2x-1}, & \dfrac{1}{2}\le x\le 1\end{cases}. \tag{3}$$

下面的定理说明了它们及相应的两个非线性迭代系统的性质.

定理 2. (1) $f_q^{-1}(E)=\{x: f_q(x)\in E\}$ 是 Lebesgue 意义下的保测变换.

(2) $x_i=f_q(x_{i-1})$是混沌迭代系统,且不变分布函数均为 $\rho(x)=1$,从而对任意的复合序列 R,(f_0,f_1,R) 具有均匀的不变分布.

(3) 它们严格互补.

证明:(1) 设 $I=(x_0,x_0+\Delta x)\subset[0,1]$, $\Delta x>0$,由 $f(x)$ 的性质易验证 $\mu\{f_0^{-1}(I)\}=\Delta x$,即 f_0^{-1} 对任意的开区间是保测的,从而可知 f_0^{-1} 对任意的可测集在 Lebesgue 测度意义下保测.同理可证 f_1^{-1} 也是保测的.

(2) 在区间(0,1)上 $f_q'(x)>1$,故对应的动力系统的 Lyapunov 指数 $\lambda_q>0$,正的 Lyapunov 指数意味着混沌[13]. 对任意的 $q=0,1$,存在惟一的分布密度函数 $\rho(x)$ 满足[14]: $\rho(x)\ge 0$, $\int_{[0,1]}\rho(x)\mathrm{d}x=1$,并且 $\rho(x)=\dfrac{\mathrm{d}}{\mathrm{d}x}\int_{f_r^{-1}([0,1])}\rho(t)\mathrm{d}t$, 而 $\rho(x)=1$ 正是满足条件的惟一解.

(3) 由(2)与定义易得. □

2 基于复合离散混沌动力系统的序列密码

本节基于由式(3)构成的复合离散混沌动力系统,建立两个新的序列密码体系.首先定义算子 $T_j:[0,1]\to\{0,1\}$ 为 $T_j(x)=\lceil 2^j x\rceil \bmod 2$,用于将由离散混沌动力系统得到的迭代序列 $\{x_i\}$ 转化为二进制序列 $\{s_i^j\}$.设复合系统的不变分布为 $\rho(x)$,我们定义[0,1]的子集E的概率测度 $\mu(E)=\int_E\rho(x)\mathrm{d}x$,其中积分为Lebesgue积分.当 $\rho(x)=1$,集 E 的概率测度就是 Lebesgue 测度.由于由式(3)得到的两个混沌系统严格互补,而且当 $x\ne\dfrac{3}{5},\dfrac{5}{8}$ 时, $T_j(f_0(x))+T_j(f_1(x))=1$ 成立,从而使得由复合系统的迭代轨迹在用算子 T_j 生成的二进制序列有良好的属性.

定理 3. 设 $R=\{r_i\}$ 是任意二进制序列, $\{x_i\}$ 是复合系统 (f_0,f_1,R) 的迭代轨迹,则对任意的 $j>0$, $s_i^j=T_j(x_i)$ 的各 bit 位独立同分布,即 $\forall(a_1,a_2,...,a_n)\in\{0,1\}^n$,有 $P(s_i^j=a_i,i=1,2,...,n)=2^{-n}$.

证明:只对 $j=1$ 给出证明,一般情况类似.记 s_i^1 为 s_i,由于 $\mu\{x:T_j(f_0(x))=0\}=\mu\{x:T_j(f_1(x))=0\}=\dfrac{1}{2}$,故对任意的 i,有 $P(s_i=1)=P(s_i=0)=\dfrac{1}{2}$,其中 $P(r_i=q)$ 表示 q 在 R 中出现的概率,则若 n=1,有

$$P(s_1=a_1)=P(r_1=0)P(s_1=a_1,r_1=0)+P(r_1=1)P(s_1=a_1,r_1=1)=\frac{1}{2}.$$

现假设 $n=k$ 时成立,当 $n=k+1$ 时,

$$P(s_i=a_i,i=1,2,...,k+1)=P(r_{k+1}=0)P(s_i=a_i,i=1,2,...,k+1;r_{k+1}=0)+P(r_{k+1}=1)P(s_i=a_i,i=1,2,...,k+1;r_{k+1}=1),$$

记

$$E(n,R_k)=\{x_0:s_i=a_i,i=1,2,...,k\},$$

其中 $R_k=(r_1,r_2,...,r_k)$, $E(0)=\{x_0:T_j(f_0(x))=a_{k+1}\}$,则

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

由此得到结论. □

下面给出基于非线性复合混沌系统的序列密码体系,不失一般性,我们假设明文是一个二进制的序列,即 $M=m_1m_2...m_L$.

算法 1.

(1) 算法描述

该算法以迭代的初始点 x_0 为密钥,其加密和解密是复合系统相同的迭代过程.我们假定 x_0 满足 $\forall n>0, f_0^{(n)}(x\_0)\neq\frac{1}{2}$.加密时,对明文的每一个 bit 位 m_i,选择密文 c_i,使得 $T_j(f_{c_i}(x_{i-1}))=m_i$,并令 $x_i=f_{m_i}(x_{i-1})$,而解密算法与加密算法相同.序列密码体系的加密算法可以描述如下:

① 选定一个迭代初值 x_0.

② i 从 1 到 L,完成下列步骤:$x_i=f_0(x_{i-1})$;$c_i=T_j(x_i)\oplus m_i$;若 $m_i=1$,则 $x_i:=1-x_i$.

③ 获得密文 $C=c_1c_2...c_L$.

加密过程是复合混沌系统的迭代过程,以明文的一个bit位 m_i 作为迭代所选取的函数的下标,而使迭代轨迹点满足 $T_j(x_i)=m_i$,经过混沌迭代的这种调制之后,明文和密钥序列已完全被融合在合密文(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 开始的所有 bit 位.

解密算法与加密算法相同,由密钥 x_0 及得到的密文序列 c_i,利用关系 $m_i=T_j(f_0(x_{i-1}))\oplus c_i$ 及 $x_i=f_{m_i}(x_{i-1})$,我们可以递推得到明文 M 和轨迹序列 $\{x_i\}$,具体算法描述如下:

① 选定一个迭代初值 x_0.

② i 从 1 到 L,完成下列步骤: $x_i=f_0(x_{i-1})$; $m_i=T_j(x_i)\oplus c_i$;若 $m_i=1$,则 $x_i:=1-x_i$.

③ 获得密文 $M=m_1m_2...m_L$.

(2) 算法分析

离散混沌系统由于其迭代轨迹对初始条件敏感而使其行为很复杂,在一定程度上不可预测.对于复合离散混沌动力系统来说,迭代过程中不断地变换所使用的迭代函数,使迭代过程不仅具有对初始条件的敏感性,而且还具有一定的随机性,迭代轨迹当然也不可预测.与传统的序列密码体系不同,复合混沌系统迭代过程使明文很自然地嵌入到了密文(迭代序列)当中,一方面使得密文不再具有明文的统计特性,防止了密文对明文及密钥信息的泄露,另一方面也使它们之间具有敏感而复杂的关系.这种由明文和密钥通过复合混沌系统的调制产生密文的方法,使得系统的安全性不再完全依赖于密文的外在复杂性.在以后的叙述中,记明文 M 用密钥 x_0 加密后的密文为 $C=E(x_0,M)$.

定理 4. 设明文序列为 $M=m_1m_2...m_L$, $C=E(x_0,M)=c_1...c_L$,记 $\alpha(M,x_0,n)=\frac{1}{n}\#\{i:c_i=m_i,i\le n\}$,则有 $\lim_{n\to\infty}\alpha(M,x_0,n)=\frac{1}{2}$.进一步地,在概率测度意义下,对任意的 i 有 $P(m_i=c_i)=(m_i\neq c_i)=\frac{1}{2}$.

证明:设 j=1,对给定的 M 与 x_0,由于 $\#\{i:c_i=m_i\}=\#\left\{i:x_{i-1}\in\left[0,\frac{3}{8}\right)\cup\left[\frac{1}{2},\frac{5}{8}\right)\right\}$,而对任意的复合序列 R, (f_0,f_1,R) 具有均匀的不变分布,因此其迭代轨迹 $\{x_i\}$ 在[0,1]上的分布也是均匀的,故

$$\lim_{n\to\infty}\frac{1}{n}\#\{i:c_i=m_i\}=\mu\left(\left[0,\frac{3}{8}\right)\cup\left[\frac{1}{2},\frac{5}{8}\right)\right)=\frac{1}{2},$$

由此可得结论成立.对于一般情况,由于 $\#\{i:c_i=m_i\}=\#\{i:T_j(f(x_{i-1}))=0\}$,而 f_0^{-1} 是保测的,从而不难证明结论成立. □

定理说明,加密时明文 M 大约有一半的 bit 位将发生改变,从而明文和密文之间的相关度[3]很小,而且随着 n 的增大,相关度趋于 0.明文经过复合混沌系统的调制,在定义的概率测度意义下,它的每一 bit 都以 0.5 的概率改变或保持不变,由此可知密文对明文信息的泄露较少.我们用对长为 10 000 的 0 序列和 1 序列进行加密实验,得到的密文序列中 1 的个数与长度之比 $\alpha(M,x_0,n)$ 都在 0.5 附近,而对一般的随机明文序列,结果更接近 0.5,实验结果与定理结论一致.图 1 是明文长为 10 000 的 0 序列时,将 $\alpha(M,x_0,n)$ 看成密钥 x_0 的函数所得结果.明文与密文之间的相关度定义为

$$R(x_0,n)=\frac{1}{n}(\#\{c_i|c_i=m_i,1\le i\le n\}-\#\{c_i|c_i\ne\ m\_i,1\le i\le n\}).$$

图 2 是对一个取定的明文,在随机选取的 4 个密钥下,明文与对应的密文的相关度关于长度 n 的图像,由此可以看出定理的结论.

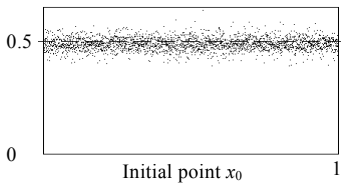

Fig.1 The distribution of $\alpha(M,x_0,n)$, where n=10000,M=0^n

图 1 $\alpha(M,x_0,n)$的分布, n=10000, M=0^n

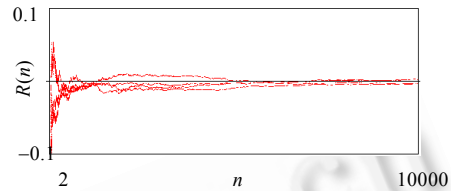

Fig.2 Correlation degree function $R(x_0,n)$ of different key x_0

图 2 不同密钥的相关度函数 $R(x_0,n)$

定理 5. 记 $T=T_1$,对任意的两个二进制序列 M,C,若 $|M|=|C|$,必存在 $x_0\in[0,1]$,使 $E(x_0,M)=C$.

证明:设 $M=m_1m_2...m_n$, $C=c_1c_2...c_n$,记 (f_0,f_1,M) 以 x_0 为初始点的迭代序列为 $(x_0,x_1,...,x_n)$.任取 x_n,使满足 $T(x_n)=c_n,x_n\ne 0,\frac{1}{2},1$.记 x',x'' 分别是 x_n 在 $f_{c_n}(x)$ 下的两个原象,则必有 $x'<\frac{1}{2}<x''$ (或 $x''<\frac{1}{2}<x'$),选择 $x_{n-1}=x'$ 或 $x_{n-1}=x''$,使其满足 $T(x_{n-1})=m_{n-1}$.对 x_{n-1} 进行同样的过程,可以得到 x_{n-2}.如此一直重复上面的步骤,便可得到 x_0. □

定理 5 说明,在一次一密意义下,该算法在理论上是安全的,但由于受到实际计算精度的限制,这一理想的序列密码算法实际上无法实现.在有限精度下,当 j=1 时,若密码分析者得到了部分密文和对应的明文序列,利用定理 5 中的反向迭代方法,可以得到迭代序列$\{x_i\}$某项的近似值,它与实际值仅在有效精度的最后一位不同,因此也就很容易得到精确值,这等同于获得了密钥.为了提高其安全性,可以取离散化算子 T_j 中的 $j\ge 2$,这样一方面提高了迭代过程对密钥和明文的敏感性,另一方面还增加了分析者利用已知的部分明、密文序列,采用反向迭代获得密钥或某次的迭代轨迹的难度.

例如,当 j=2 时,对任意的 x_n 在 $f_{c_n}(x)$ 的两个原象 x',x'' 不再一定满足 $T_j(x')\oplus T_j(x'')=1$,反向迭代能否完成与选择的迭代初值有关,所以用定理 5 的方法无法获得密钥或迭代序列$\{x_i\}$某项的近似值.

算法 2.

(1) 算法描述

算法 2 的密钥由迭代的初始点 x_0 和 q_0 组成,其中 q_0=0,1.迭代过程就是获得序列$\{x_i\}$和$\{q_i\}$的过程:对明文的每一个 bit 位 m_i,计算 $q_i=T_1(f_0(x_{i-1}))\oplus q_{i-1}$,然后选择密文 c_i,使得 $T_1(f_{c_i}(f_{q_i}(x_{i-1})))=m_i$,并令 $x_i=f_{m_i}(f_r(x_{i-1}))$,其中 $r=q_i\oplus q_{i-1}$.具体的加密算法如下:

① 选定迭代初值 x_0 及 q_0.

② i 从 1 到 L,完成下列计算:

$$y_{i-1}=f_0(x_{i-1}),q_i=T_1(y_{i-1})\oplus q_{i-1};x_i=f_0(y_{i-1}),c_i=T_1(x_i)\oplus m_i\oplus q_i;$$

若 $c_i\ne q_i\oplus q_{i-1}$,则 $x_i=1-x_i$.

③ 获得密文 $C=c_1c_2...c_L$.

与前面的加密算法相比,这里增加了一次迭代,使得明文与密文的关系变得更复杂,可有效地抵御前面提出的反向迭代分析法,从而提高了安全性.相应的解密过程如下:

① 获得迭代初值 x_0 及 q_0.

② i 从 1 到 L,完成下列计算:

$$y_{i-1}=f_0(x_{i-1}),q_i=T_1(y_{i-1})\oplus q_{i-1};x_i=f_0(y_{i-1}),m_i=T_1(x_i)\oplus c_i\oplus q_i;$$

若 $c_i\ne q_i\oplus q_{i-1}$,则 $x_i=1-x_i$.

③ 获得密文 $M=m_1m_2...m_L$.

(2) 算法分析

为方便起见,记 $I_1=\left[0,\frac{39}{128}\right)$, $I_2=\left[\frac{39}{128},\frac{3}{8}\right)$, $I_3=\left[\frac{3}{8},\frac{55}{128}\right)$, $I_4=\left[\frac{55}{128},\frac{1}{2}\right)$, $J_1=\left[\frac{1}{2},\frac{73}{128}\right)$, $J_2=\left[\frac{73}{128},\frac{5}{8}\right)$, $J_3=\left[\frac{5}{8},\frac{89}{128}\right)$, $J_4=\left[\frac{89}{128},1\right)$; $I_{uv}=I_u\cup I_v, I_{uv}=I_u\cup I_v$.由 $f_0(x),f_1(x)$ 的定义可以看出,$f_0(f_0(x))=f_1(f_1(x))\equiv F_0(x)$, $f_0(f_1(x))=f_1(f_0(x))\equiv F_1(x)$.而且 F_0,F_1 与 f_0,f_1 具有相同的性质.因此算法 2 实际上是由 F_0,F_1 构成的复合系统的迭代过程,而 F_0,F_1 也是严格互补的,故迭代轨迹具有均匀的不变分布,因此不难证明定理 4 仍然成立.

定理 6. 设明文序列为 $M=m_1m_2...m_L$, $E(x_0,M)=c_1c_2...c_L$, 记 $\alpha(M,x_0,n)=\frac{1}{n}\#\{i:c_i=m_i,i\le n\}$, 则有 $\lim_{n\to\infty}\alpha(M,x_0,n)=\frac{1}{2}$,而且在概率测度意义下, $P(m_i=c_i)=P(m_i\ne c_i)=\frac{1}{2}$.

证明:设 $N=\#\{i:c_i=m_i,i\le n\}$.由于 $m_i=c_i\Leftrightarrow T_1(f_{m_i}(f_{q_i}(x_{i-1})))=m_i\Leftrightarrow T_1(f_0(f_{q_i}(x_{i-1})))=0$,从而有

$$N=\#\left\{i:f_0(f_{q_i}(x_{i-1}))\in\left[0,\frac{1}{2}\right)\right\}.$$

由算法可以看出,当 $q_{i-1}=0$ 时, $q_i\oplus q_{i-1}=T_1(f_0(x_{i-1}))$;当 $q_{i-1}=1$ 时, $q_i\oplus q_{i-1}=T_1(f_1(x_{i-1}))$.记 $r_i=T_1(f_0(x_{i-1}))$,令

$$N_1=\#\{i:q_{i-1}=0,T_1(f_0(f_{r_i}(x_{i-1})))=0\}=\#\{i:q_{i-1}=0,x_{i-1}\in I_{14}\cup J_{14}\},$$

$$N_2=\#\{i:q_{i-1}=1,T_1(f_0(f_{\bar{r}_i}(x_{i-1})))=0\}=\#\{i:q_{i-1}=1,x_{i-1}\in I_{23}\cup J_{23}\},$$

$$N_3=\#\{i:q_{i-1}=0,T_1(f_0(f_{r_i}(x_{i-1})))=1\}=\#\{i:q_{i-1}=0,x_{i-1}\in I_{23}\cup J_{23}\},$$

$$N_4=\#\{i:q_{i-1}=1,T_1(f_0(f_{\bar{r}_i}(x_{i-1})))=1\}=\#\{i:q_{i-1}=1,x_{i-1}\in I_{14}\cup J_{14}\}.$$

由于序列 $\{q_i\}$ 具有均匀分布的 0 和 1,从而得到

$$\lim_{n\leftarrow\infty}\frac{N_1}{n}=\lim_{n\leftarrow\infty}\frac{N_4}{n}=\frac{1}{2}\mu(I_{14}\cup J_{14}),\ \lim_{n\leftarrow\infty}\frac{N_2}{n}=\lim_{n\leftarrow\infty}\frac{N_3}{n}=\frac{1}{2}\mu(I_{23}\cup J_{23}).$$

由 $N=N_1+N_2$ 可得

$$\lim_{n\leftarrow\infty}\alpha(n)=\lim_{n\leftarrow\infty}\frac{1}{n}(N_1+N_2)=\frac{1}{2}\lim_{n\leftarrow\infty}\frac{1}{n}(N_1+N_2+N_3+N_4)=\frac{1}{2}.$$

进一步地,利用迭代轨迹 $\{x_i\}$ 在 [0,1] 上的均匀分布性,我们可以得到

$$P(m_i=c_i)=P(x_{i-2}\in I_{12}\cup J_{12})P\left(f_0(f_{q_i}(x_{i-1}))\in\left[0,\frac{1}{2}\right)\middle|x_{i-2}\in I_{12}\cup J_{12}\right)+$$

$$P(x_{i-2}\in I_{34}\cup J_{34})P\left(f_0(f_{\bar{q}_i}(x_{i-1}))\in\left[0,\frac{1}{2}\right)\middle|x_{i-2}\in I_{34}\cup J_{34}\right)$$

$$=\mu(I_{12}\cup J_{12})\mu(I_{14}\cup J_{14})+\mu(I_{34}\cup J_{34})\mu(I_{23}\cup J_{23})=\frac{1}{2}.$$

由此可得结论成立. □

定理说明,在加密时明文序列的每个 bit 位都以 0.5 的概率发生改变或保持不变,也就是说,与明文相比,密文序列中大约有一半的 bit 位发生改变,这使密文 C 与明文 M 的相关度很小,而且随着长度的增加还趋于 0,同时还可以保证密文序列中 0 和 1 的分布大体均匀,这使得算法可以有效地抵御统计分析.定理中的 $\alpha(M,x_0,n)$ (我们称为分布函数)很好地刻画,密文中 1 的分布情况,说明了密钥与密文 0,1 分布特性之间的关系.我们取定 $q_0=1$,对固定长度的 0 序列和 1 序列进行加密实验,除一些特殊的密钥之外,加密得到的密文序列中 1 的个数和长度之比大都在 0.5 附近.对一般随机的明文序列,结果更理想.图 3 是明文为 0 序列,n=10 000 时,将 $\alpha(M,x_0,n)$ 看作密钥 x_0 的函数时的图像.图 4 是明文为 0 序列,10 个不同的密钥分别为 $0.4145862374623450+10^{-16}i$,($i$=1,…,9),将 $Rl(M,x_0,n)$ 看作 n 的函数时的绘制图像.由此可以看出,密钥微小的变动不仅会导致密文有很大的改变,而且它们对于 0 与 1 的分别也有很大的差异.

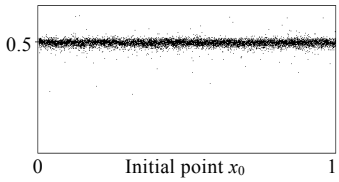

Fig.3 $\alpha(M,x_0,n)$, when n=10000 and M=0^n

图 3 分布函数 $\alpha(M,x_0,n)$, n=10000, M=0^n

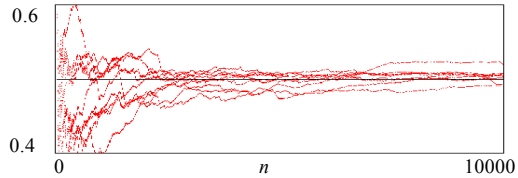

Fig.4 $\alpha(M,x_0,n)$ of different key x_0, when M=0^n

图 4 不同密钥 x_0 的分布函数 $\alpha(M,x_0,n)$, M=0^n

由加密算法可以看出,c_i,m_i,x_{i-1} 三者之间有着密切的关系,若仅知道其中的一个,另外两个仍然无法确定,因此密码分析者仅由得到的密文序列 C 无法获得明文和密钥的信息.由于迭代过程不仅与密钥有关,而且还与被加密的明文有关,因此分析者要对获得的密文序列解密,必须知道迭代的初始状态,在分析者仅有密文序列的情况下无法解密获得的密文.即使密码分析者已经得到了密文序列和相应的明文序列,要确定以后迭代的起始点或初始密钥仍然是不可能的,从而对密文的后续序列也无法解密.

假设密码分析者已经得到密文序列 $C=c_1c_2...c_n$ 和对应的明文序列 $M=m_1m_2...m_n$,欲确定下次迭代的起始点 x_n.若 $c_n=m_n$,则

$$f_{q_n}(x_{n-1})\in\left[0,\frac{3}{8}\right)\cup\left[\frac{1}{2},\frac{5}{8}\right),$$

从而得到 $x_{n-1}\in I_{14}\cup J_{14}$,当 $q_{n-1}=0$ 时;$x_{n-1}\in I_{23}\cup J_{23}$,当 $q_{n-1}=1$ 时.同理,若 $c_n\neq m_n$,则有 $x_{n-1}\in I_{23}\cup J_{23}$,当 $q_{n-1}=0$ 时;$x_{n-1}\in I_{14}\cup J_{14}$,当 $q_{n-1}=1$ 时.这说明在任何情况下,x_{n-1} 都可能是 [0,1] 上的任意一点.

由关系 $x_{n-1}=f_{c_{n-1}}(f_{q_n\oplus q_{n-1}}(x_{n-2}))$ 可知,当 $q_{n-2}=0$ 时,x_{n-2} 应满足下列关系之一:

$$x_{n-2}\in f_{c_{n-1}}^{-1}(f_{q_{n-1}}^{-1}([0,1]))\cap(I_{12}\cup J_{12}),$$

或

$$x_{n-2}\in f_{c_{n-1}}^{-1}(f_{q_{n-1}}^{-1}([0,1]))\cap(I_{34}\cup J_{34}).$$

当 $q_{n-2}=1$ 时,x_{n-2} 应满足下列关系之一:

$$x_{n-2}\in f_{c_{n-1}}^{-1}(f_{1\oplus q_{n-1}}^{-1}([0,1]))\cap(I_{12}\cup J_{12}),$$

或

$$x_{n-2}\in f_{c_{n-1}}^{-1}(f_{1\oplus q_{n-1}}^{-1}([0,1]))\cap(I_{34}\cup J_{34}).$$

从而 x_{n-2} 也可以是 [0,1] 上的任意一点.若想用定理 5 中的反向迭代方法,利用 $C=c_1c_2...c_n$ 和 $M=m_1m_2...m_n$ 估计序列 $\{x_i\}$ 中的某个点,那么对 x_{i-1} 的任意一个估计值 x'_{i-1},反向迭代一次得到 4 个满足条件的 x_{i-2} 的估计值 x'_{i-2},迭代 N 次可得到 4^N 个满足条件的 x_{n-N-1} 的估计值 x'_{n-N-1}.若计算采用双精度,那么迭代平均收敛速度大约也要 28 次,即反向迭代至收敛需迭代 28 次.这样取 x_{n-1} 在 8 个小区间上的任意 8 个估计值,反向迭代得到了 2^{59} 个 x_{n-N-1} 的估计值 x'_{n-N-1}.为得到 x_n 的准确值,我们需要对这 2^{59} 个近似值以及在双精度下的临近值进行正向迭代比较,以确定 x_n,从而可知获得 x_n 的复杂度不低于 2^{60} 的穷尽搜索.

3 结 论

基于复合混沌系统的序列密码算法,利用了复合混沌系统对初始条件的敏感性和迭代过程的随机性,使得明文和密钥与密文的非线性关系很复杂,明文每一 bit 与密文的若干 bit 有关,反之亦然.它们之间的关系还很敏感,明文和密钥任何微小的改变必然导致密文发生很大的变化.复合混沌系统均匀的不变分布还使得密文也具有均匀分布性,减少了密文对明文和密钥信息的泄露.基于复合混沌系统的序列密码算法的另一个特点是,明文序列经过一个复合混沌系统的调制,很好地融于复合混沌系统的迭代轨迹的信息之中,可以有效地抵御统计分析等一些已有的分析方法.这些特点使得算法具有很高的安全性.

References:

[1] Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code. New York: John Wiley & Sons Inc., 1994. 347~375.

[2] Feng DG, Pei DY. Introduction to Cryptography. Beijing: Science Press, 1999. 54~100 (in Chinese).

[3] Feng DG. Cryptanalysis. Beijing: Tsinghua University Press, 2000. 55~92 (in Chinese).

[4] Habutsu T, Nishio Y, Sasase I, Mori S. A Secret Key Cryptsystem by Iterating a Chaotic Map. LNCS 547, Berlin: Springer-Verlag, 1991. 127~136.

[5] Götz M, Kelber K, Schwarz W. Discrete-Time chaotic encryption systems-part I: Statistical design approach. IEEE Transactions on Circuits System-1: Fundamental Theory and Applications, 1997,44(10):963~970.

[6] Alvarez E, Fernández A, García P, Jiménez J, Marcano A. New approach to chaotic encryption. Physics Letters A, 1999,263: 373~375.

[7] Biham E. Cryptanalysis of the chaotic-map cryptosystem suggested. In: Davies DW, ed. Proceedings of the EUROCRYPT'91. LNCS 547, Berlin: Springer-Verlag, 1991. 532~534.

[8] Baptista MS. Cryptography with chaos. Physics Letters A, 1998,240(12):50~54.

[9] Kotulski Z, Szczepański J. Application of discrete chaotic dynamical systems in cryptography——DCC method. International Journal of Bifurcation and Chaos, 1999,9(6):1121~1135.

[10] Stojanovski T, Kocarev L. Chaos-Based random number generators——Part I: Analysis. IEEE Transactions on Circuits System-1: Fundamental Theory and Applications, 2001,48(3):281~288.

[11] Stojanovski T, Pihl J, Kocarev L. Chaos-Based random number generators——Part II: Practical realization. IEEE Transactions on Circuits System-1: Fundamental Theory and Applications, 2001,48(3):382~385.

[12] Jakimoski G, Kocarev L. Chaos and cryptography: block encryption ciphers based on chaotic maps. IEEE Transactions on Circuits System-1: Fundamental Theory and Applications, 2001,48(2):163~169.

[13] Wu XX, Chen Z. An Introduction to Chaos. Shanghai: Shanghai Sciences and Technology Press, 2001. 57~83 (in Chinese).

[14] Baranovsky A, Daems D. Design of one-dimensional chaotic maps with prescribed statistical properties. International Journal of Bifurcation and Chaos, 1995,5(6):1585~1598.

附中文参考文献:

[2] 冯登国,裴定一.密码学导引.北京:科学出版社,1999.54~100.

[3] 冯登国.密码分析学.北京:清华大学出版社,2000.55~92.

[13] 吴祥兴,陈忠.混沌学导论.上海:上海科学技术文献出版社,2001.57~83.