一种具有时变密钥的自同步混沌加密方法

鞠 磊[1] 翁贻方[2] 赵 耿[1] 郑德玲[3]
(北京电子科技学院通信工程系 北京 100070)[1] (北京工商大学信息工程学院 北京 100037)[2]
(北京科技大学信息工程学院 北京 100083)[3]

摘 要 混沌系统变量的分离时间能够反映系统参数的近似程度,这为参数探测和同步攻击的实施提供了便利。针对这个混沌系统所共有的安全弱点,通过预处理系统变量并对系统参数扰动,得到了对参数偏差敏感且分离时间与参数差值关系不明显的混沌变量。随后,提出了一种时变密钥自同步混沌加密方法,该方法具有抵御同步攻击的能力,可以实现一次一密的安全思想。安全性分析和仿真实验证明了该方法的可行性和安全性。

关键词 混沌,加密,时变参数,安全性
中图法分类号 TP918.8 **文献标识码** A

Self-synchronization Chaotic Encryption Method with Time-varying Keys

JU Lei[1] WENG Yi-fang[2] ZHAO Geng[1] ZHENG De-ling[3]
(Department of Communication, Beijing Electronic Science and Technology Institute, Beijing 100070, China)[1]
(School of Information Engineering, Beijing Technology and Business University, Beijing 100037, China)[2]
(School of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China)[3]

Abstract The separation-time of system variable can reflect the approximate level of system parameters in the chaotic system, this facilitates parameters detection and synchronizating attack. For soluting this security weaknesses of all the chaos system we got a new chaotic variable by pre-processing the chaotic variable and adding disturbance to the system parameters. The separation-time of new variable can't reflect the approximate level of system parameters almost. Subsequently, a self-synchronization chaotic encryption method with time-varying keys was presented. This method can resist the synchronizating attack and has the capability of one time padding. Security analysis and simulation results show that method is feasibly and safety.

Keywords Chaotic, Encryption, Time-varying keys, Security

混沌系统具有有界性、遍历性、内随机性等独有的特征,近20年来,混沌保密通信的研究一直是个热点。混沌与密码在本质上具有一致性,因此人们利用混沌的某些特性提出了许多不同种类的混沌密码机制。现有的混沌密码已大致涵盖了Hash函数[1]、伪随机数发生器[2]、流密码[3]、分组密码[4,5]、公开钥密码[6,7]等传统密码的主要应用。

密码学中可用密钥长度表示安全程度,并希望每一个可能的密钥应具有相等的抗攻击能力。在混沌安全系统中,混沌系统的参数(或初值)相当于密钥。研究表明,对于系统参数(或初值)存在偏差的耦合同构混沌系统,对应系统变量的分离距离能够反映两系统参数(或初值)的近似程度[8],这种关系可被用来对系统实施同步攻击[9]。因此从密码学角度,动力系统的混沌参数相当于弱密钥。对于非耦合混沌系统,虽然不存在上述问题,但通过观察发现,系统变量的分离速度也能够反映出参数(或初值)的近似度,这给混沌安全系统带来了威胁。

本文首先分析了存在偏差的同构混沌系统变量的分离速度与参数差值的关系,并利用对系统变量预处理和系统参数的扰动,得到了分离速度与参数(或初值)差值关系不明显的混沌变量。在此基础上,设计了一种时变参数自同步混沌加密方法,最后对该方法进行了安全性分析和仿真测试。

1 混沌参数敏感性分析

设n维系统

$$\dot{x}(t)=f(x,t),x\in R^n,x(t_0)=x^0 \tag{1}$$

其中,n维向量函数$f(x)$的各元素$f_i(x),i=1,2,\cdots,n$是x的有界、连续可微单值函数。设参数向量$\alpha\in R^m$使系统(1)处于混沌态,α和初值x^0组成向量$\psi_d=[\alpha \quad x^0]^T,\psi_d\in R^{m+n}$。

系统(1)的同构系统为

$$\dot{y}(t)=f(y,t),y\in R^n,y(t_0)=y^0 \tag{2}$$

同理有参数向量$\beta\in R^m$与初值y^0的组合向量$\psi_r=[\beta \quad y^0]^T$,$\psi_r\in R^{m+n}$。

到稿日期:2008-10-27 返修日期:2009-03-27 本文受国家自然基金"混沌密码的密码分析与设计准则研究(No. 60773120)"资助。
鞠 磊(1971—),男,博士,讲师,主要研究方向为信息安全与可信计算,E-mail:jl@besti.edu.cn;翁贻方(1954—),女,博士,教授,主要研究方向为混沌保密通信;赵 耿(1963—)男,博士,教授,主要研究方向为混沌保密通信与信息安全;郑德玲(1939—),女,教授,博士生导师,主要研究方向为混沌保密通信与人工免疫。

定义 1 设系统(1)和(2)在初始状态 x^0, y^0 下的解 $x(t)=\varphi(t;t_0,x^0), y(t)=\varphi(t;t_0,y^0)$，满足 Lipschitz 条件。若系统(1)与(2)的同步误差

$$e=(x-y), e\in R^n \tag{3}$$

满足

$$\lim_{t\to\infty}\| e(t)\| = \| x(t)-y(t)\| \equiv 0, t>t_0 \tag{4}$$

其中，$\| x(t)-y(t)\| = [\sum_{i=1}^{n}(x_i-y_i)^2]^{\frac{1}{2}}$ 是欧几里德范数，称系统(1)与(2)同步。当初值满足 $x^0, y^0 \subset D(t_0)$，称 $D(t_0)$ 为同步区域。

定义 2 令系统(1)和(2)的 ψ_d, ψ_r 存在微小偏差

$$\delta=\sum_{i=1}^{m}|\alpha_i-\beta_i|+\sum_{j=1}^{n}|x_j^0-y_j^0|=10^{-l} \tag{5}$$

其中，l 为大于零的整数。若同步误差 e 在经过时间 $\tau(\tau>t_0)$，达到稳态后的范数满足

$$\| e\| = \| x-y\| > L \tag{6}$$

其中，$L(L>0)$是预先设定的轨道分离的下确界，则称混沌系统(1)与(2)的轨道完成分离，并称 τ 为系统(1)和(2)的参数或初值偏差为 l 级时的分离时间。

分离时间 τ 描述了参数(或初值)存在偏差的同构混沌系统变量的分离速度，τ 越小分离速度越快，系统变量对参数(或初值)的敏感度也越高，越能够提供高的安全特性。

考虑处于混沌态的 Lorenz 系统

$$\begin{cases}\dot{x}_1=-\alpha_1 x_1+\alpha_1 x_2\\ \dot{x}_2=-x_1 x_3+\alpha_2 x_1-x_2\\ \dot{x}_3=x_1 x_2-\alpha_3 x_3\\ \psi_d=[10\quad 28\quad 8/3\quad 10\quad 1\quad 10]^T\end{cases} \tag{7}$$

构造非耦合同构系统，令初值相同而参数存在偏差，即 $\delta=\sum_{i=1}^{m}|\alpha_i-\beta_i|=10^{-l}$，取 $L=10^{-4}$，则 l 与 τ 的关系如图 1 所示。

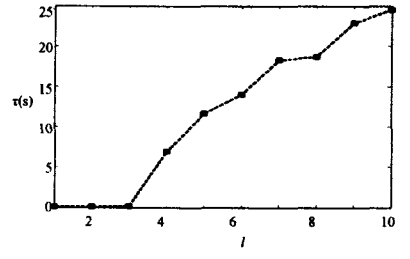

图 1 Lorenz 系统参数偏差与分离时间的关系

图 1 曲线说明了 Lorenz 系统变量的分离时间与参数的偏差量级数存在明显对应关系，特别在参数偏差较小时分离时间较长，这都为参数探测和同步攻击的实施提供了条件。实验表明 Rösslor 系统、细胞神经网络(CNN)系统以及 Logistic 等混沌系统都存在此类问题，是混沌系统存在的一个共同安全弱点。

2 参数敏感性改善方法

定义 3 对于 n 维系统(1)，当参数向量 α 取值 α_{ch} 时系统为混沌状态。如果对于任意给定的实数 $\varepsilon>0$，使得参数向量满足 $|\alpha-\alpha_{ch}|\leqslant\varepsilon$ 时，系统(1)仍为混沌的，则称 ε 为系统(1)的混沌参数范围。

设混沌系统参数向量 $\alpha_s(t), \alpha_s\in R^m$ 为

$$\alpha_s(t)=\alpha_{ch}+\mu(x), \mu\in R^m \tag{8}$$

当满足 $\| \mu(x)\| <\varepsilon$ 时，ε 是系统的混沌参数范围，称 $\alpha_s(t)$为混沌时变参数向量，$\mu(x)$为变量预处理函数。

取 x 为 lorenz 系统变量的函数，令 $\mu(x)$为：

$$\mu(x)=\nu x_s \tag{9}$$

其中，$x_s=\omega x-fix(\omega x)$，$\nu,\omega\in R$，$fix(\cdot)$为取整运算。

构造两 Lorenz 同构系统，令初值相同而参数存在偏差 $\delta=\sum_{i=1}^{m}|\alpha_i-\beta_i|=10^{-l}$，改变定值参数 α_2 为时变参数：

$$\alpha_{s2}(t)=\alpha_{ch2}+\mu(x_1), \mu\in R^m \tag{10}$$

其中，$\omega_2=10^2$。在 $\nu=0$(无时变)时依据式(9)得到变量 x_{s1}，$\nu=0.1$时得到变量 x_{s2}，取 $L=10^{-4}$，则变量 x_1, x_{s1}, x_{s2}相对应的 l 与 τ 关系曲线如图 2 所示。

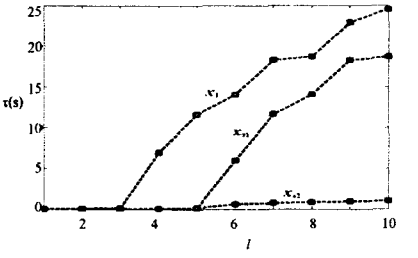

图 2 x_1, x_{s1}, x_{s2}相对应的 l 与 τ 的关系

由图 2 可知，当系统参数取固定值时($\nu=0$)，x_{s1}对参数变化的敏感性要好于 x_1，而当参数为时变时($\nu=0.1$)，得到的混沌变量 x_{s2}对参数变化敏感性较好，对应变量分离时间与参数差值的关系不明显，且具有近似均匀性，因此 x_{s2}更适合作为明文信息的调制变量。

3 时变密钥混沌加密系统

3.1 系统设计

密码学中用密钥长度表示安全程度，在混沌同步保密通信中，混沌系统的参数和初值相当于密钥。根据 Shannon 的信息理论，“一次一密”是最安全的，如果混沌系统的参数或初值是某种程度上的随机变量，将可能取得近似“一次一密”的效果。利用式(8)得到时变参数时，是充分利用了混沌系统自身的内随机特性，通过函数 $\mu(\cdot)$产生伪随机变量叠加到混沌系统参数上，形成了一种具有伪随机特性的动态密钥。据此，可设计一种时变密钥混沌加密系统，其结构如图 3 所示。

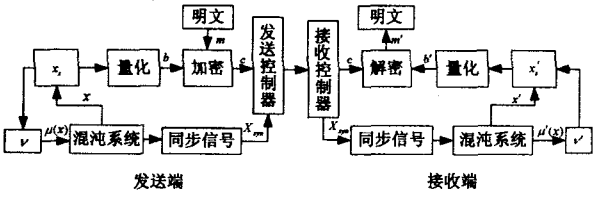

图 3 时变密钥混沌加密系统

图 3 中 x 为 Lorenz 变量，b 为对 x_s 量化生成二值伪随机序列，m 为明文，c 为密文，加解密采用二值异或方式；x'为接收端为 Lorenz 变量，b'为接收端量化二值伪随机序列，m'为解密明文。X_{syn}为同步信号，X_{syn}为定时采集的 Lorenz 系统变量值。发送控制器则负责将定时采集的同步信息 X_{syn}按一定字长对其编码与密文 c 按照一定格式连接发送给接收端。接收控制器负责将同步信号 X_{syn}和密文 c 分离，利用 X_{syn}定时驱动接收端系统，迫使其与发送端同构混沌同步，使得 $b'=b$(参数相同时)以实现对密文的解密。

3.2 可行性与安全性分析

当接收端的参数设置与发送端一致时，由于同步信息 X_{sym} 直接将接收端当前系统状态值替换，接收端在下一步迭代时会产生与发送端相同的状态变量，即 $x'=x$，从而得到 $x'_s=x_s$。在相同 x_s 作用下，接收端系统参数也跟随发送端变化，生成 $b'=b$，可得到 $m'=m$。同步信息 X_{sym} 是定时发送的，即使在异步接收情况下也能正确解密。

为增加实用性，同步信息 X_{sym} 大都以明文传递，攻击者可利用 X_{sym} 驱动本地系统实现同步攻击。而在本系统中，用于加密的二值序列来源于对参数变化敏感的变量 x_s，攻击者可利用实施同步攻击的时间很短。同时由于 $\mu(x)$ 作为随机扰动加入到收发双方混沌系统中，参数是时变的，攻击者即使得到某时刻精确参数值，仍然无法对随后的密文解密。

4 仿真分析

采用 Lorenz 系统变量 x_1 作为被处理变量，取 $\omega=100$，按照式(9)得到 x_s。x_1，x_s 波形如图 4 所示，相关特性如图 5 和图 6 所示，可见 x_s 特性明显优于 x_1，更适合生成用于加密的二值伪随机序列。

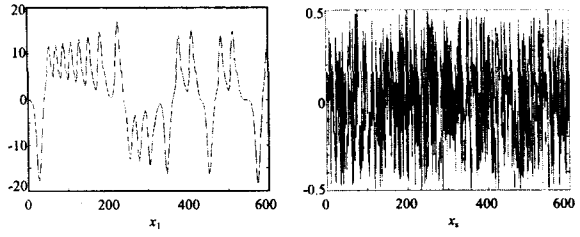

图 4 x_1，x_s 波形

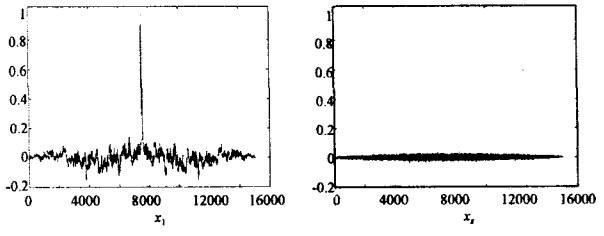

图 5 自相关特性

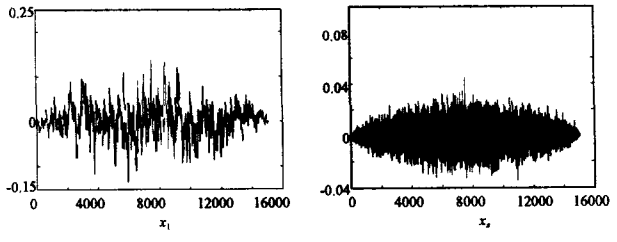

图 6 互相关特性

设明文信息为正弦信号的二值编码，同步信息为 $X_{sym}=[x_{1sym}\ x_{2sym}\ x_{3sym}]$，即同步信息为定时提取的 3 个变量的数值，则不同情况下的加解密测试如图 7 所示，正确解密时接收端晚于发送端 200 步，错误解密时参数差为 $\delta=\sum_{i=1}^{m}|\alpha_i-\beta_i|=10^{-6}$。

结束语 本文分析了混沌系统变量发散速度与参数差值的关系，通过对系统变量预处理和增加系统参数扰动，得到了具有较好的随机特性且分离时间与参数差值关系不明显的混沌变量。在前期分析基础之上，本文设计了一种时变参数自同步混沌加密方法。该方法采用参数差值关系不明显混沌变量生成序列密码，因此可以抵御同步攻击。同时，作为加密系统密钥的混沌系统参数是时变的，体现了一次一密的安全思想，因此具有高的安全性。安全性与可行性分析以及加解密测试表明，本文所设计的时变参数自同步混沌序列密码是安全可行的。

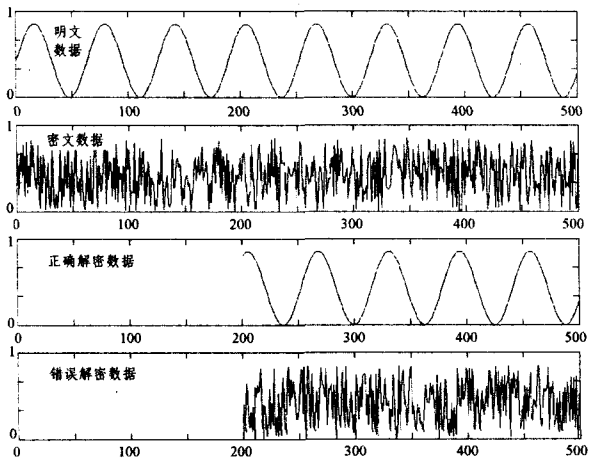

图 7 加解密测试

参 考 文 献

[1] Kwok H S, Tang W K S. A Chaos - based Cryptographic Hash Function for Message Authentication[J]. International Journal of Bifurcation and Chaos, 2005, 15(12): 4043

[2] Li P, et al. Analysis of A Multiple - Output Pseudo - random - bit Generator Based on a Spatiotemporal Chaotic System[J]. International Journal of Bifurcation and Chaos, 2006, 16(10): 2949

[3] Boesgaard M, et al. Rabbit: A New High-Performance Stream Cipher[C] // T. Johansson, ed. International Association for Cryptologic Research 2003, FSE 2003, LNCS 2887. 2003: 307

[4] Tang Gu-oping, Liao Xiao-feng, Chen Yong. A novel method for designing S-boxes based on chaotic maps[J]. Chaos, Solitons & Fractals, 2005, 23: 413

[5] Chen G, et al. An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps[J]. Chaos, Solitons and Fractals, 2007, 31: 571

[6] Tenny R, Tsimring L S. Additive Mixing Modulation for Public Key Encryption Based on Distributed Dynamics [J]. IEEE Transactions on Circuits and Systems—I: Regular Papers, 2005, 52(3): 672

[7] Kocarev L, Makraduli J, Amato P. Public-Key Encryption Based on Chebyshev Polynomials[J]. draft, 2005: 1

[8] 翁贻方，郑德玲，鞠磊. 一类具有时变参数的混沌同步保密通信方法[J]. 北京科技大学学报，2008，30(8)：952

[9] Parlitz U, Junce L, Kocarev L. Synchronization-based parameter estimation from time series[J]. Phys Rev E, 1996, 54(6): 6253