第 38 卷 第 2 期 计 算 机 工 程 2012 年 1 月
Vol.38 No.2 Computer Engineering January 2012

• 安全技术 • 文章编号：1000—3428(2012)02—0148—03 文献标识码：A 中图分类号：TP391

# 混沌指数同步在保密通信中的应用

胡成军，李传东

(重庆大学计算机学院，重庆 400044)

**摘 要：**利用 Lyapunov 稳定性理论和线性矩阵不等式技术，给出一类时滞混沌系统指数同步的充分条件，设计指数同步控制器。在此基础上，采用混沌掩盖方法将该控制器应用于保密通信中。基于 Ikeda 混沌系统的仿真结果表明，该方法可准确、快速地恢复出有用信号，并且对噪声具有一定的鲁棒性，能够达到保密通信的目的。

**关键词：**混沌系统；时滞；指数同步；保密通信；谱攻击

# Application of Chaotic Exponential Synchronization in Secret Communication

**HU Cheng-jun, LI Chuan-dong**

(College of Computer Science, Chongqing University, Chongqing 400044, China)

**【Abstract】** Based on Lyapunov stability theory and differential inequality technology, this paper gives a sufficient condition of exponential synchronization by using the linear matrix inequality technique, and designs an exponential synchronization controller. The synchronization controller is applied to secret communications through chaotic masking method. Simulation result based on Ikeda chaotic system shows that this method can accurately and rapidly recover the useful signal, and it is robustness for noise to achieve the purpose of secret communication.

**【Key words】** chaotic system; delayed; exponential synchronization; secret communication; spectrum attack

**DOI:** 10.3969/j.issn.1000-3428.2012.02.048

## 1 概述

自从 Pecora L M 和 Carroll T L[1]于 1990 年提出混沌同步思想以来，混沌的类噪声、对初值的敏感依赖性及其连续宽频谱性质，使它在保密通信中有极好的应用前景[2]。

然而大量的混沌保密通信研究都集中在只有一个正的 Lyapunov 指数的低维混沌系统上，这样的系统由于复杂性不高，在保密通信中很容易被破译。而时滞混沌系统能不受系统维数的限制产生多个正的 Lyapunov 指数，这个特征使其特别适用于保密通信。将时滞混沌系统应用在保密通信中已成为人们研究的热点。

目前，混沌同步的方法有很多，但如果能让响应系统与驱动系统以指数收敛速度达到同步并将这种指数同步方法应用在保密通信中，将更具理论和实际意义。

本文针对一类时滞混沌系统，利用 Lyapunov 稳定性理论和 微分不等式，研究时滞混沌系统的指数同步问题。基于线性矩阵不等式得到指数同步的充分条件，给出指数同步控制器的设计方法。

## 2 问题描述和预备知识

考虑以下时滞混沌系统：

$$\begin{cases}\dot{\boldsymbol{x}}(t)=\boldsymbol{A}\boldsymbol{x}(t)+\boldsymbol{B}f(\boldsymbol{x}(t))+\boldsymbol{C}g(\boldsymbol{x}(t-\tau)) & t>0\\ \boldsymbol{x}(s)=\boldsymbol{\varphi}(s) & -\tau\leqslant s\leqslant 0\end{cases} \tag{1}$$

假设式(1)为驱动系统，而响应系统为：

$$\begin{cases}\dot{\boldsymbol{y}}(t)=\boldsymbol{A}\boldsymbol{y}(t)+\boldsymbol{B}f(\boldsymbol{y}(t))+\boldsymbol{C}g(\boldsymbol{y}(t-\tau))+\boldsymbol{u}(t) & t>0\\ \boldsymbol{y}(s)=\boldsymbol{\psi}(s) & -\tau\leqslant s\leqslant 0\end{cases} \tag{2}$$

其中，$\boldsymbol{x}(t),\boldsymbol{y}(t)\in R^n$ 是式(1)和式(2)的状态向量；$\boldsymbol{A},\boldsymbol{B},\boldsymbol{C}\in R^{n\times n},\tau>0$ 为系统时滞；$f,g:R^n\to R^n$ 是连续向量值函数且满足 $f(0)=g(0)=0$ 和 Lipstchiz 条件，即存在正数 $L_1,L_2$，使对任意的 $\alpha,\beta\in R^m$，有式(3)成立：

$$\|f(\alpha)-f(\beta)\|\leqslant L_1\|\alpha-\beta\|,\|g(\alpha)-g(\beta)\|\leqslant L_2\|\alpha-\beta\| \tag{3}$$

令 $\boldsymbol{e}(t)=\boldsymbol{y}(t)-\boldsymbol{x}(t)$ 为同步误差，则误差系统为：

$$\dot{\boldsymbol{e}}(t)=\boldsymbol{A}\boldsymbol{e}(t)+\boldsymbol{B}f(\boldsymbol{y}(t)-\boldsymbol{x}(t))+\boldsymbol{C}(g(\boldsymbol{y}(t-\tau))-g(\boldsymbol{x}(t-\tau)))+\boldsymbol{u}(t) \tag{4}$$

其中，控制器 $\boldsymbol{u}(t)=-k\boldsymbol{e}(t)$，$k$ 为控制强度。

**定义** 如果存在 $\theta>0$ 和 $\rho>0$，对于系统的每个解 $\boldsymbol{e}(t)$，有式(5)成立：

$$\|\boldsymbol{e}(t)\|\leqslant\rho\boldsymbol{e}^{-\theta t}\sup_{-\tau\leqslant\lambda\leqslant 0}\{\|\boldsymbol{e}(\lambda)\|\},\forall t>0 \tag{5}$$

则该系统是指数稳定的，其中，$\theta$ 为指数收敛率；$\|.\|$ 为欧几里德范数。

**引理 1** 假设函数 $\boldsymbol{x}(t)$ 在区间 $t\in(-\tau,0)$ 非负，且满足[3]：

$$\dot{\boldsymbol{x}}(t)\leqslant-k_1\boldsymbol{x}(t)+k_2\boldsymbol{x}(t-\tau),\ t\geqslant 0 \tag{6}$$

其中，$k_1,k_2$ 为正常数，且 $k_1>k_2$，则有：

$$\boldsymbol{x}(t)\leqslant\|\boldsymbol{x}(0)\|_\tau\boldsymbol{e}^{-rt},\ t\geqslant 0 \tag{7}$$

其中，$\|\boldsymbol{x}(0)\|_\tau=\max_{-\tau\leqslant t\leqslant 0}|\boldsymbol{x}(t)|$；$r$ 是方程 $-r=-k_1+k_2\boldsymbol{e}^{-r\tau}$ 的唯一正根。

**引理 2** 给定实矩阵 $\boldsymbol{x}\in R^m,\boldsymbol{y}\in R^m$ 和参数 $\varepsilon>0$，使以下

**基金项目：**国家自然科学基金资助项目(60974020)

**作者简介：**胡成军(1983－)，男，硕士，主研方向：混沌控制，保密通信；李传东，教授、博士后

**收稿日期：**2011-04-06 **E-mail：**258480435@qq.com

不等式成立[4]：

$$2\boldsymbol{x}^{\mathrm{T}}\boldsymbol{y}\leqslant\varepsilon\boldsymbol{x}^{\mathrm{T}}\boldsymbol{x}+\varepsilon^{-1}\boldsymbol{y}^{\mathrm{T}}\boldsymbol{y} \tag{8}$$

其中，$\varepsilon$ 是任意正实数。

## 3　指数同步控制器的设计

**定理** 如果存在正常数 $\alpha,\beta,k,\mu_1,\mu_2$，使以下条件成立：

(1) $\boldsymbol{A}+\boldsymbol{A}^{\mathrm{T}}+\alpha\boldsymbol{B}\boldsymbol{B}^{\mathrm{T}}+\alpha^{-1}L_1^{\,2}\boldsymbol{I}+\beta\boldsymbol{C}\boldsymbol{C}^{\mathrm{T}}-2k\boldsymbol{I}\leqslant 0$；

(2) $\beta^{-1}L_2^{\,2}\boldsymbol{I}-\mu_2\boldsymbol{I}\leqslant 0$；

(3) $\mu_1-\mu_2>0$。

则驱动混沌系统(1)和响应混沌系统(2)指数同步。

证明：选择 Lyapunov 函数为：

$$V(t)=\boldsymbol{e}(t)^{\mathrm{T}}\boldsymbol{e}(t) \tag{9}$$

$V$ 沿误差系统(4)的求导为：

$$\dot{\boldsymbol{V}}(t)=2\boldsymbol{e}(t)^{\mathrm{T}}\dot{\boldsymbol{e}}(t)=2\boldsymbol{e}(t)^{\mathrm{T}}\left[\boldsymbol{A}\boldsymbol{e}(t)+\boldsymbol{B}\left(f\left(\boldsymbol{y}(t)\right)-f\left(\boldsymbol{x}(t)\right)\right)+\boldsymbol{C}\left(g\left(\boldsymbol{y}(t-\tau)\right)-g\left(x(t-\tau)\right)\right)+\boldsymbol{u}(t)\right]$$

根据引理 2，则有：

$$\dot{\boldsymbol{V}}(t)=2\boldsymbol{e}(t)^{\mathrm{T}}\left[\boldsymbol{A}\boldsymbol{e}(t)+\boldsymbol{B}\left(f\left(\boldsymbol{y}(t)\right)-f\left(\boldsymbol{x}(t)\right)\right)+\boldsymbol{C}\left(g\left(\boldsymbol{y}(t-\tau)\right)-g\left(\boldsymbol{x}(t-\tau)\right)\right)-k\left(\boldsymbol{y}(t)-\boldsymbol{x}(t)\right)\right]=\boldsymbol{e}(t)^{\mathrm{T}}\left(\boldsymbol{A}+\boldsymbol{A}^{\mathrm{T}}-2k\boldsymbol{I}\right)\boldsymbol{e}(t)+$$
$$2\boldsymbol{e}(t)^{\mathrm{T}}\times\left[\boldsymbol{B}\left(f\left(\boldsymbol{y}(t)\right)-f\left(\boldsymbol{x}(t)\right)\right)+C\left(g\left(\boldsymbol{y}(t-\tau)\right)-g\left(\boldsymbol{x}(t-\tau)\right)\right)\right]\leqslant\boldsymbol{e}(t)^{\mathrm{T}}\left(\boldsymbol{A}+\boldsymbol{A}^{\mathrm{T}}-2k\boldsymbol{I}\right)\boldsymbol{e}(t)+\alpha\boldsymbol{e}(t)^{\mathrm{T}}\boldsymbol{B}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{e}(t)+$$
$$\alpha^{-1}\left\|f\left(\boldsymbol{y}(t-\tau)\right)-f\left(x(t-\tau)\right)\right\|^2+\beta\boldsymbol{e}(t)^{\mathrm{T}}\boldsymbol{C}\boldsymbol{C}^{\mathrm{T}}\boldsymbol{e}(t)+\beta^{-1}\left\|g\left(\boldsymbol{y}(t-\tau)\right)-g\left(\boldsymbol{x}(t-\tau)\right)\right\|^2\leqslant$$
$$\boldsymbol{e}(t)^{\mathrm{T}}\left(\boldsymbol{A}+\boldsymbol{A}^{\mathrm{T}}+\alpha\boldsymbol{B}\boldsymbol{B}^{\mathrm{T}}+\alpha^{-1}L_1^{\,2}I+\beta\boldsymbol{C}\boldsymbol{C}^{\mathrm{T}}-2k\boldsymbol{I}\right)\boldsymbol{e}(t)+\boldsymbol{e}(t-\tau)^{\mathrm{T}}\left(\beta^{-1}L_2^{\,2}\boldsymbol{I}\right)\boldsymbol{e}(t-\tau)^{\mathrm{T}}=$$
$$\boldsymbol{e}(t)^{\mathrm{T}}\ \left(\boldsymbol{A}+A^{\mathrm{T}}+\alpha\boldsymbol{B}\boldsymbol{B}^{\mathrm{T}}+\alpha^{-1}L_1^{\,2}I+\beta\boldsymbol{C}\boldsymbol{C}^{\mathrm{T}}+\left(\mu_1-2k\right)\boldsymbol{I}\right)\times\ \boldsymbol{e}(t)-\mu_1\boldsymbol{e}(t)^{\mathrm{T}}\boldsymbol{e}(t)+$$
$$\boldsymbol{e}(t-\tau)^{\mathrm{T}}\left(\beta^{-1}L_2^{\,2}\boldsymbol{I}-\mu_2\boldsymbol{I}\right)\boldsymbol{e}(t-\tau)+\mu_2\boldsymbol{e}(t-\tau)^{\mathrm{T}}\boldsymbol{e}(t-\tau)$$

根据定理的条件(1)和条件(2)，可得：

$$\dot{\boldsymbol{V}}(t)\leqslant-\mu_1\boldsymbol{e}(t)^{\mathrm{T}}\boldsymbol{e}(t)+\mu_2\boldsymbol{e}(t-\tau)^{\mathrm{T}}\boldsymbol{e}(t-\tau)=$$
$$-\mu_1\boldsymbol{V}\left(\boldsymbol{e}(t)\right)+\mu_2\boldsymbol{V}\left(\boldsymbol{e}(t-\tau)\right)$$

又由定理的条件(3)和引理 1，有：

$$\dot{\boldsymbol{V}}(t)\leqslant\left\|\boldsymbol{V}(0)\right\|_{\tau}\boldsymbol{e}^{-rt}$$

其中，$\left\|\boldsymbol{V}(0)\right\|_{\tau}=\max\limits_{-\tau\leqslant S\leqslant 0}\left|\left(\boldsymbol{\psi}(s)-\boldsymbol{\varphi}(s)\right)^{\mathrm{T}}\left(\boldsymbol{\psi}(s)-\boldsymbol{\varphi}(s)\right)\right|$；$r$ 是方程 $r=\mu_1-\mu_2\boldsymbol{e}^{-rt}$ 的唯一正根。从而得到：

$$\left\|\boldsymbol{e}(t)\right\|\leqslant\sqrt{\left\|\boldsymbol{V}(0)\right\|_{\tau}\boldsymbol{e}^{-rt}}=\sqrt{\left\|\boldsymbol{V}(0)\right\|_{\tau}}\,\boldsymbol{e}^{-\frac{r}{2}t}$$

根据定义，误差系统(4)是指数稳定的，即驱动时滞混沌系统(1)和响应混沌时滞系统(2)指数同步。

## 4　数值仿真

以典型的 Ikeda-type 方程为例验证理论的正确性：

$$\dot{\boldsymbol{x}}(t)=-a\boldsymbol{x}(t)+b\sin\left(\boldsymbol{x}(t-\tau)\right) \tag{10}$$

当参数取值为 $a=1.0,b=5.0,\tau=2$ 时，系统将产生混沌吸引子，其误差系统为：

$$\dot{\boldsymbol{e}}(t)=-\boldsymbol{e}(t)+5\left(\sin\left(y(t-2)\right)-\sin\left(\boldsymbol{x}(t-2)\right)\right)-k\boldsymbol{e}(t) \tag{11}$$

利用 Matlab 进行仿真，分别选取驱动系统和响应系统的初值为 $x_0=-1$、$y_0=4$，同时易知 $L=5$，根据定理，可令 $k=15$，仿真结果如图 1 所示。

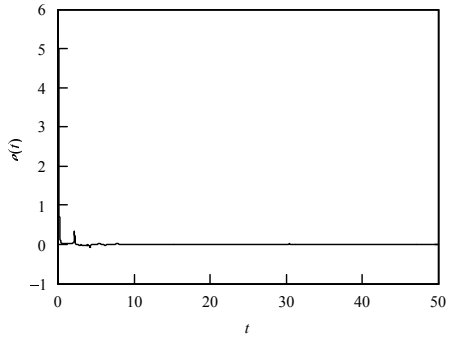


**图 1　Ikeda 系统同步误差变化**

由此可知：在控制器(5)的控制下，同步误差较快地趋于零值，即驱动时滞系统(1)和反馈时滞系统(2)达到了很好的指数同步。

## 5　指数同步在保密通信中的应用

以 Ikeda 时滞混沌系统为例，将前面提到的指数同步方法应用到混沌保密通信中。设需要传输的有用信号是 $\boldsymbol{m}(t)$，发射端输出的混合类噪声信号是 $\boldsymbol{s}(t)=\boldsymbol{x}(t)+c\boldsymbol{m}(t)$，接收端恢复出的信号为 $\boldsymbol{r}(t)$，则有：

$$\lim_{t\to\infty}\boldsymbol{r}(t)=\lim_{t\to\infty}c^{-1}\left(\boldsymbol{s}(t)-\boldsymbol{y}(t)\right)=$$
$$\lim_{t\to\infty}c^{-1}\left(\boldsymbol{x}(t)+c\boldsymbol{m}(t)-\boldsymbol{y}(t)\right)=$$
$$\lim_{t\to\infty}\left(c^{-1}\boldsymbol{e}(t)+\boldsymbol{m}(t)\right)=\boldsymbol{m}(t) \tag{12}$$

所以，传送的有用信号在接收端能够被准确恢复出来，从而达到保密通信的目的。在仿真时，选取正弦信号 $\boldsymbol{m}(t)=sin(2t)$作为待加密信号，当 $c=0.5$ 时，基于指数同步方法实现保密通信的仿真结果，如图 2~图 4 所示。

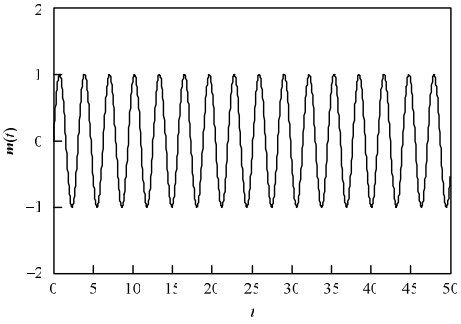


**图 2　有用信号 $m(t)$的仿真结果**

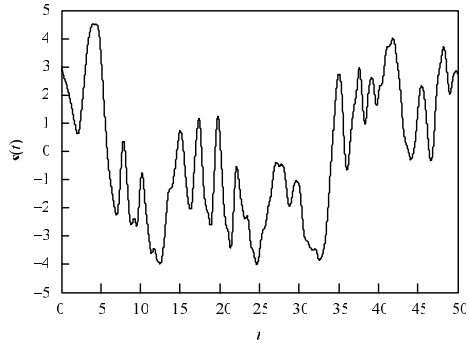


**图 3　混合类噪声信号 $s(t)$的仿真结果**

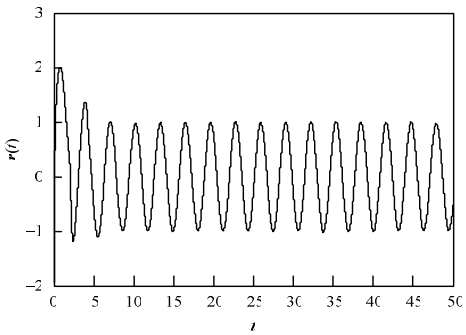


**图 4 接收器恢复的有用信号 $r(t)$仿真结果**

可以看出，在控制器 $\boldsymbol{u}(t)$的作用下，接收系统可以快速恢复出有用信号，达到保密通信的目的。

在理论上，对于有用信号 $\boldsymbol{m}(t)$ 的具体形式没有限制。当系统是 $n$ 维时，可采用文献[5]提出的发送单路组合信号以实现系统的同步控制。即先找到与系统(1)能完全同步的响应系统，再由该系统解出与系统(1)同步的系统。

利用此方案，目前已知的混沌系统大部分都可通过传递单路信号实现同步。

为了验证此方案的抗噪性能。假设系统存在内部噪声 $n_1=\sin(0.01t)$，则响应系统变为：

$$\dot{\boldsymbol{y}}(t)=-\left(\boldsymbol{y}(t)+n_1\right)+5\sin\left(\boldsymbol{y}(t-\tau)\right) \tag{13}$$

指数同步抗噪分析如图 5 所示，由此可知，本文方案对内部噪声干扰具有较强的鲁棒性。

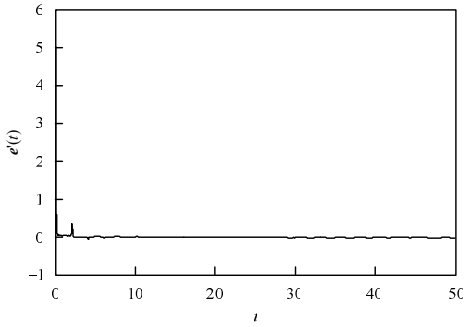


**图 5 指数同步抗噪分析**

另外，对 $\boldsymbol{x}(t)$作功率谱分析，所得结果如图 6 所示，可见该方案也能有效抵御谱攻击[6]。

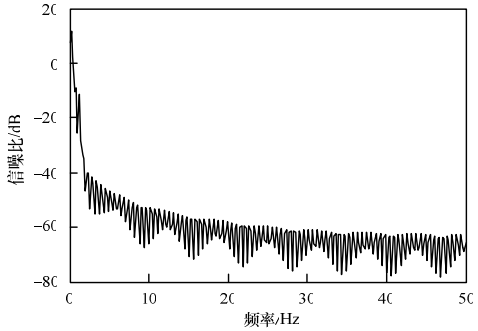


**图 6 $x(t)$的功率谱仿真结果**

## 6 结束语

本文讨论了一类时滞混沌系统的指数同步和保密通信问题，采用驱动-响应同步方法，基于 Lyapunov 稳定性理论和线性矩阵不等式技术，给出一类时滞混沌系统的指数同步的充分条件和指数同步控制器的设计方法，实现了性能良好的混沌指数同步，将其应用于保密通信中。最后基于 Ikeda 混沌系统的仿真验证了该理论的有效性，由此可见，本文方法具有良好的实用价值。

## 参考文献

[1] Pecoral L M, Carroll T L. Synchronization in Chaotic Systems[J]. Physical Review Letters, 1990, 64(8): 821-824.

[2] 渠慎明，郑文奎. 基于状态观测器的混沌同步保密通信[J]. 计算机工程, 2010, 36(12): 182-183, 186.

[3] Halanay A. Differential Equations: Stability, Oscillations, Time Lags[M]. New York, USA: Academic Press, 1965: 377-383.

[4] Chen Maoying, Zhou Donghua, Shang Yun. Integrity Control of Chaotic Systems[J]. Physics Letters A, 2006, 350(3/4): 214-220.

[5] Peng J H, Ding E J, Ding M, et al. Synchronization Hyperchaos with a Scalar Transmitted Signal[J]. Physical Review Letters, 1996, 76(6): 904-907.

[6] 王明军，王兴元. 基于一阶时滞混沌系统参数辨识的保密通信方案[J]. 物理学报, 2009, 58(3): 1467-1472.

编辑 陆燕菲

(上接第 147 页)

和 $pw_B$。目前设计的协商协议多存在漏洞，启发式设计方法容易出错，有必要采用形式化证明方法分析密钥协商协议，这也是笔者下一步的研究方向。

## 参考文献

[1] Abdalla M, Fouque P A, Pointcheval D. Password-based Authenticated Key Exchange in the Three-party Setting[C]//Proceedings of the 8th International Workshop on Theory and Practice in Public Key Cryptography. Berlin, Germany: [s. n.], 2005.

[2] Abdalla M, Pointcheval D. Simple Password-based Encrypted Key Exchange Protocols[C]//Proceedings of Cryptology-CT-RSA'05. San Francisco, California, USA: Springer-Verlag, 2005.

[3] 胡红宇，李军义. 改进的基于口令的群密钥协商协议[J]. 计算机工程, 2011, 37(3): 132-133, 136.

[4] Lu Rongxing, Cao Zhenfu. Simple Three-party Key Exchange Protocol[J]. Computers & Security, 2006, 26(1): 94-97.

[5] Guo Hua, Li Zhoujun, Mu Yi, et al. Cryptanalysis of Simple Three-party Key Exchange Protocol[J]. Computers & Security, 2008, 27(1/2): 16-21.

[6] Kin Hyun-Seok, Choi Jin-Young. Enhanced Password-based Simple Three-party Key Exchange Protocol[J]. Computers and Electrical Engineering, 2009, 35(1): 107-114.

[7] 胡学先，刘文芬. 对两个三方口令认证密钥交换协议的分析[J]. 信息工程大学学报, 2010, 11(1): 104-107.

[8] Lee Tian-Fu, Hwang Tzonelih, Lin Chun-Li. Enhanced Three-party Encrypted Key Exchange Without Server Public Keys[J]. Computers and Security 2004, 23(7): 571-577.

编辑 金胡考