第 55 卷 第 7 期 2006 年 7 月
1000-3290/2006/55(07)/3283-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.55,No.7,July,2006

驱动函数切换调制实现超混沌数字保密通信

孙 琳[1)] 姜德平[2)]

1)(长沙理工大学物理与电子科学系,长沙 410077)

2)(中南林业科技大学电子与信息工程学院,长沙 410004)

(2005 年 3 月 24 日收到;2005 年 8 月 17 日收到修改稿)

在主动-被动分解同步的基础上,提出了一种利用不同超混沌系统的驱动函数切换调制实现数字保密通信的方案.根据二进制信号‘0’和‘1’的传输情况交替发射两个不同的驱动函数,这就增加了发射信号的复杂度,减少了信号的相关性.且通过进行多次非线性变换加密,进一步设置了新的密钥,使得基于预测法的攻击完全失效.理论分析和模拟结果均表明本方案在实现超混沌数字保密通信时的有效性.

关键词:超混沌,主动-被动分解法,切换调制,保密通信

PACC:0545

1. 引 言

近年来,混沌系统的同步及应用于保密通信已引起国际国内学者的广泛关注[1—8].为了利用混沌信号更好地掩藏信息信号的内容,已经发展了诸多种不同的同步混沌实现保密通信方法.但其中有些方法的保密性能不高,信息信号极易被破译,而且大多数方法中传输信号的幅度不能过大,否则就会使收发端系统失去同步而不能无失真地恢复出信息信号.本文在 Kocarev 和 Parlitz 提出的主动-被动分解同步的基础上[9],提出了一种利用超混沌系统驱动函数调制实现数字保密通信的方案.根据二进制信号‘0’和‘1’的传输情况交替发射两个不同的驱动函数,由于是两个不同超混沌系统的驱动函数对二进制信号进行切换调制,其信号的相关性就大大减小了,这就极大地增加了发射信号的复杂度.同时,为了从根本上克服相空间重构、神经网络、回归映射等预测方法的攻击,设计了一系列非线性变换函数对信息信号进行多次复合变换,使破译更加困难.并且通过采用幅度键控的调制方式和轨道误差积分大小比较判决方式,有效地克服了利用一般混沌同步方法在实现保密通信时要求信息信号幅度很小的缺点,从而使得本方案在工程实际中有一定的实用价值.

2. 主动-被动同步方法

由于 Pecora-Carroll 关于驱动-响应同步方法需要将系统进行特定的分解,使其在实际应用中往往受到很大的限制.1995 年,Kocarev 和 Parlitz 提出了改进方法[9],即主动-被动分解法.

考虑如下的 n 维的动力学系统:

$$\dot{Z} = F(Z), \tag{1}$$

式中 $Z \in R^n$ 为状态向量,F 为光滑的向量场.我们总可以把系统(1)改为如下非自治形式:

$$\dot{X} = f(X, S(t)), \tag{2}$$

其中 $S(t)$ 为所选的驱动变量,它是 X 中变量的函数,即

$$S(t) = h(X) \text{ 或 } \dot{S}(t) = h(X, S). \tag{3}$$

复制一个与(2)式相同的系统作为响应系统

$$\dot{Y} = f(Y, S(t)), \tag{4}$$

显然,响应系统(4)与驱动系统(2)受到相同的信号 $S(t)$ 驱动,由方程(2)及(4)可推导出两系统变量差 $e = X - Y$ 的微分方程为

$$\begin{aligned} \dot{e} &= f(X, S) - f(Y, S) \\ &= f(X, S) - f(X - e, S). \end{aligned} \tag{5}$$

显然(5)式在 $e = 0$ 处有一个稳定的不动点,即响应系统(4)与驱动系统(2)能达到稳定的同步态 $X = Y$.应用 Lyapunov 函数、线性稳定性分析(在 e 为小值情况下)或计算系统(4)的条件 Lyapunov 指数等方法可以证明(2)式和(4)式所示的两个混沌系统能够实现同步.上述分解方法称为主动-被动分解法或有源-无源分解法.响应的同步类型也称为主动-被动(或有源-无源)同步类型.

主动-被动同步方法的最大优点和关键所在就

是可以不受任何限制地选择驱动信号的函数形式，因此，该法具有很大的实用性.在很多情形下，驱动函数可以是一般的函数，它不仅依赖于系统的状态，而且还可以与信息信号有关，通常是信息信号与混沌(超混沌)信号的函数.这个特点使得主动-被动同步方法特别适合于保密通信方面的应用.

3. 数字保密通信系统的设计原理

本文在主动-被动同步的基础上，提出了一种分别利用两个超混沌系统的一个驱动函数对二进制信号进行调制实现数字保密通信方法，其系统组成方框图如图1所示.在图1所示的系统中，$m(t)$为随机的二进制比特流数字信号.在设计中，为了减小信号的相关性，增加发射信号的复杂度，驱动函数通过开关键控的作用对 $m(t)$进行调制.当 $m(t)$取“1”时，开关键控控制超混沌系统Ⅰ输出驱动函数为 $h_1(x_1)$；当 $m(t)$取“0”时，开关键控控制超混沌系统Ⅱ输出驱动函数为 $h_2(y_1)$，这样就通过两个互相独立的超混沌系统的驱动函数 $h_1(x_1)$，$h_2(y_1)$随机交替驱动形成了调制信号 $s(t)$，即

$$s(t) = \begin{cases} h_1(x_1), & m(t) = 1, \\ h_2(y_1), & m(t) = 0. \end{cases} \tag{6}$$

由于是不同系统的一个驱动函数对信息信号进行切换调制，这就减小了发射信号所携带信息信号的信息量，降低了发射信号的相关度，且可以通过灵活地选择驱动函数的形式，使得发射信号的无序度增加.因此，即使在传输中发射信号被截获，入侵者也不能通过相空间重构等方法重构出信号.同时，为了彻底抵制预测法的攻击，我们通过对调制信号 $s(t)$ 进行多次非线性变换 $F_n(\cdots(F_2(F_1(\cdot)))\cdots)$加密(其中 $F_i(t)$的选取原则是在 $s(t)$的取值范围内可逆和有界)，从而形成发射信号 $T(t)$，这就进一步增加了新的密匙，使接收者无法破译信号 $m(t)$.

在接收系统中，通过对接收信号 $R(t)$进行与发射端次序相反的逆变换 $F_1^{-1}(\cdots(F_{n-1}^{-1}(F_n^{-1}(\cdot)))\cdots)$解密，得到解密信号 $s'(t)$.将 $s'(t)$同时送入到基于主动-被动同步方法设计的响应系统Ⅰ和响应系统Ⅱ中，显然，对于传输的随机流数字信号而言，根据以上的信号调制方法，在每个时刻 t，只有一个响应系统受到正确的驱动函数作用，因而其轨道误差收敛.而另一个响应系统必然受到非正确的驱动函数的作用，故其轨道误差必然发散，反之亦然.例如当随机数字信号为“1”时，$s(t) = h_1(x_1)$，只有响应系统Ⅰ受到正确的驱动函数作用而实现同步，而响应系统Ⅱ必然受到非正确的驱动函数的作用而不能同步.此时，由于超混沌系统Ⅰ和响应系统Ⅰ之间的轨道误差必然比超混沌系统Ⅱ与响应系统Ⅱ之间的轨道误差的幅度值要小，即可以依此进行积分判决而恢复出原信息信号“1”，反之亦可恢复出信号“0”.

将两响应系统的驱动函数变量分别输入到减法器与 $s'(t)$信号相减，形成误差信号 $|s'(t) - h_1(x_1')|$ 和 $|s'(t) - h_2(y_1')|$，然后分别将此两个误差信号输入到积分器进行积分得

$$d_1(t) = \int_0^T |s'(t) - h_1(x_1')| \,\mathrm{d}t, \tag{7}$$

$$d_2(t) = \int_0^T |s'(t) - h_2(x_1')| \,\mathrm{d}t, \tag{8}$$

式中 T 为一个比特码的宽度，将 $d_1(t)$与 $d_2(t)$输入到比较判决器进行判决即可恢复出原信息信号.当传输的随机数字信号为“1”时，发送端键控输出的驱动函数为 $h_1(x_1)$，响应系统Ⅰ受到同步信号的作用，而响应系统Ⅱ受到非同步信号的作用，因此 $d_1(t)$收敛而 $d_2(t)$发散，此时 $d_1(t) < d_2(t)$，控制判决输出为“1”；反之若传输的随机数字信号为“0”

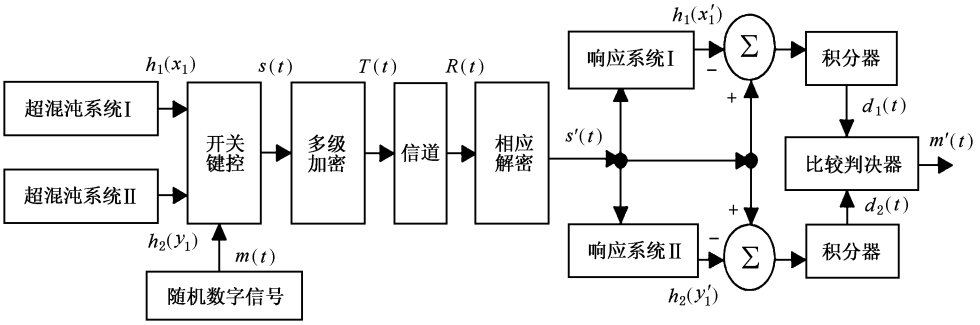

图1 数字保密通信系统设计方框图

时,发射端键控输出的驱动函数是 $h_2(y_1)$,则有 $d_2(t) < d_1(t)$,控制判决输出为"0",判决控制具体如下:

$$m'(t) = \begin{cases} 1, d_1(t) < d_2(t), \\ 0, d_1(t) > d_2(t). \end{cases} \tag{9}$$

4. 数值研究

选取两个超混沌系统为例进行数值模拟研究,一个超混沌系统是 Tamasevicius 等人[10]提出的超混沌 *LC* 振荡电路模型,它由运算放大器构成负阻元件,其无量纲方程为

超混沌系统Ⅰ

$$\begin{cases} \dot{x}_1 = a \cdot x_1 - x_2 - x_3, \\ \dot{x}_2 = x_1, \\ \dot{x}_3 = c \cdot (x_1 - x_4), \\ \dot{x}_4 = e \cdot [x_3 - b \cdot (x_4 - 1) H(x_4 - 1)], \end{cases} \tag{10}$$

其中 $H(\cdot)$为单位阶跃函数,当 $x \geqslant 0$ 时,$H(x) = 1$;当 $x < 0$ 时,$H(x) = 0$. 当系统(10)的参数取为 $a = 0.7, b = 10, c = e = 3$ 时,其 Lyapunov 指数谱为 $(0.123, 0.067, 0.000, -9.750)$[10],此时系统处于超混沌振荡状态.

另一个超混沌系统是由文献[11]提出的,其无量纲形式如下:

超混沌系统Ⅱ

$$\begin{cases} \dot{y}_1 = \alpha \cdot y_1 - y_2, \\ \dot{y}_2 = y_1 - y_3 - \beta \cdot y_2, \\ \dot{y}_3 = y_2 - y_4, \\ \dot{y}_4 = y_3 - y_5 - \beta \cdot y_4, \\ \dot{y}_5 = 8 \cdot (y_4 - d) H(y_4 - d) - \varepsilon \cdot y_5, \end{cases} \tag{11}$$

其中 $\alpha = 0.3, \beta = 0.05, \varepsilon = 1, d = 3$,$H(\cdot)$为同上的单位阶跃函数.根据文献[11]的分析结果,系统(11)在上述取值条件下有三个正性 Lyapunov 指数,系统具有超混沌行为.

按照前述主动-被动同步方法的原理,可以灵活选择驱动函数的形式,其函数形式亦可以作为密钥使用.本文在系统(10)中选择驱动函数形式 $h_1(x_1) = x_1$,在系统(11)中选择驱动函数形式为 $h_2(y_1) = y_1$. 系统(10)和系统(11)对应的响应系统Ⅰ和响应系统Ⅱ分别如(12),(13)式所示.

响应系统Ⅰ

$$\begin{cases} \dot{x}'_1 = x_1 + (a - 1) \cdot x'_1 - x'_2 - x'_3, \\ \dot{x}'_2 = x'_1, \\ \dot{x}'_3 = c \cdot (x'_1 - x'_4), \\ \dot{x}'_4 = e \cdot [x'_3 - b \cdot (x'_4 - 1) H(x'_4 - 1)]. \end{cases} \tag{12}$$

响应系统Ⅱ

$$\begin{cases} \dot{y}'_1 = y_1 + (\alpha - 1) \cdot y'_1 - y'_2, \\ \dot{y}'_2 = y'_1 - y'_3 - \beta \cdot y'_2, \\ \dot{y}'_3 = y'_1 - y'_4, \\ \dot{y}'_4 = y'_3 - y'_5 - \beta \cdot y'_4, \\ \dot{y}'_5 = 8 \cdot (y'_4 - d) H(y'_4 - d) - \varepsilon \cdot y'_5. \end{cases} \tag{13}$$

下面以驱动系统(10)和响应系统(12)为例,验证其同步的可行性.令两系统的轨道误差为

$$e_i = x'_i - x_i, i = 1, 2, \cdots, 4. \tag{14}$$

由(12)式减去(10)式可得误差系统为

$$\begin{cases} \dot{e}_1 = (a - 1) \cdot e_1 - e_2 - e_3, \\ \dot{e}_2 = e_1, \\ \dot{e}_3 = c \cdot (e_1 - e_4), \\ \dot{e}_4 = e \cdot (e_3 - b e_4). \end{cases} \tag{15}$$

若要实现驱动系统(10)与响应系统(12)的同步,则误差系统(15)必须满足零解渐近稳定.根据李雅普诺夫稳定性理论[12],取李雅普诺夫函数 $V = (e_1^2 + e_2^2 + e_3^2/c + e_4^2/e)/2 \geqslant 0$,则

$$\begin{aligned} \dot{V} &= e_1 \dot{e}_1 + e_2 \dot{e}_2 + e_3 \dot{e}_3 / c + e_4 \dot{e}_4 / e \\ &= e_1 [(a - 1) \cdot e_1 - e_2 - e_3] + e_2 e_1 \\ &\quad + e_3 (e_1 - e_4) + e_4 (e_3 - b e_4) \\ &= (a - 1) \cdot e_1^2 - b \cdot e_4^2. \end{aligned} \tag{16}$$

因为 $a = 0.7, b = 10$,所以 $\dot{V} \leqslant 0$. 根据 Lyapunov 稳定性定理[12]可知误差系统(15)零解渐近稳定,即当 $t \to \infty$ 时,$X' \to X$,构造的响应系统Ⅰ与超混沌系统Ⅰ可实现主动-被动同步.同理可得 构造的响应系统Ⅱ也可以同步超混沌系统Ⅱ.因此,只要两个驱动函数的选择可以实现对应系统间的同步,就可以保证相应的误差系统的轨道是收敛的,调制信号就可以得到完全恢复.

用于加密的非线性变换函数取

$$F_1(x) = \begin{cases} \dfrac{1}{\sqrt{x}}, & x > 1 \\ e^x + 1, & -1 \leqslant x \leqslant 1, \\ \dfrac{1}{\sqrt{-x}}, & x < -1, \end{cases}$$

$$F_2(x) = \begin{cases} 0.4(x-10)^2, & x \geqslant 0, \\ -(x+5)^2, & x > 0. \end{cases}$$

首先考虑理想信道的情况,我们用四阶龙格-库塔法进行数值模拟,积分步长取为 0.008,(10)式所示系统和其同步响应系统 Ⅰ 的初始状态分别为 $x(0) = (0.05, 0.02, 0.01, 0.03)$, $x'(0) = (0.03, 0.01, 0.03, 0.04)$;(11)式所示系统和其同步响应系统 Ⅱ 的初始状态分别为 $y(0) = (5.56, 3.7, -3.0, -3.56, 0.3)$, $y'(0) = (-3.8, -3.0, 4.0, 3.5, 5.5)$,得到模拟结果分别如图 2—6 所示.

图 2 为信息信号,图 3 所示为发射信号 $T(t)$,图 4,5 为接收端检测到的轨道误差,图 6 为恢复的解调信号.由图 3 可知,发射信号具有明显的无序性和随机特征,驱动函数切换调制的加密效果显著;图 6 所示的解调信号与图 2 所示的发送信号相比除了微弱延迟外完全一致(误码率极小),信息信号得到无失真恢复.在实际数值模拟中,考虑到误差信号的幅度差别和记忆效应,积分器的积分时间下限不是取 0,而是取 $0.75T$.因为在某一时刻驱动函数由 $h_1(x_1)$ 驱动转为 $h_2(y_1)$ 作用时,有一个很短的暂态过程,若积分器的积分时间下限取为 0,比较判别时则容易产生误判.信息传输速率的上限取决于所采用的超混沌系统的同步化速度,同步建立速度越快,信息信号恢复时产生误码的机会越小.

然而在实际的通信系统中,信道中的噪声总是不可避免的.因此有必要研究发射信号 $T(t)$ 叠加噪声时解调信号 $m'(t)$ 的恢复情况.当在 $T(t)$ 中加入强度为 G 的高斯白噪声时,解调恢复信号 $m'(t)$ 的误码率(ECR)随噪声强度变化的曲线如图 7 所示.由图可见,当噪声强度 G 小于 1.9 时,误码率 ECR 趋近于零,信息信号可以得到无失真恢复,从而说明本通信设计方案具有良好的抗噪声性能.

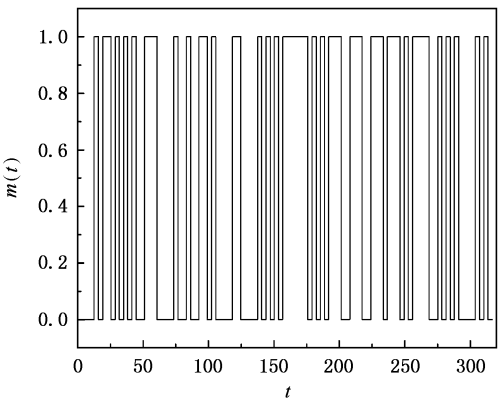

图 2 发射端信息信号 $m(t)$ 的波形图

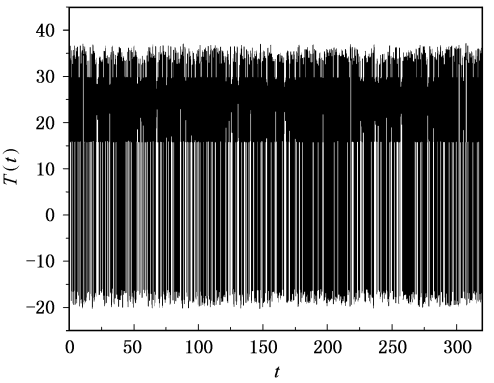

图 3 发射信号 $T(t)$ 的波形图

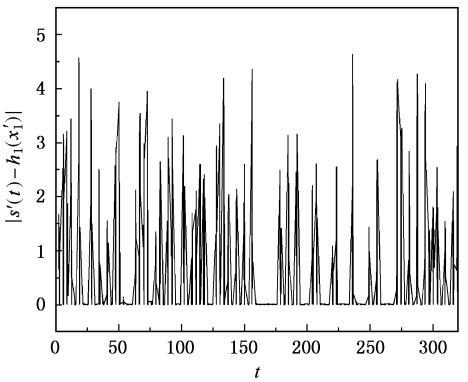

图 4 误差信号 $|s'(t) - h_1(x'_1)|$ 的波形图

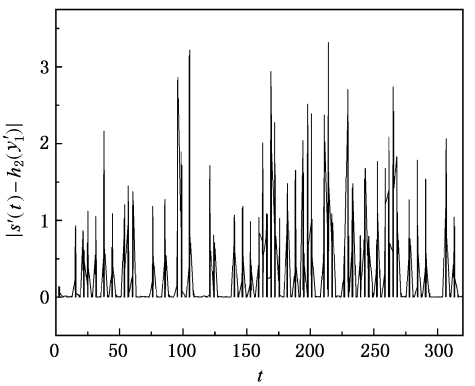

图 5 误差信号 $|s'(t) - h_2(y'_1)|$ 的波形图

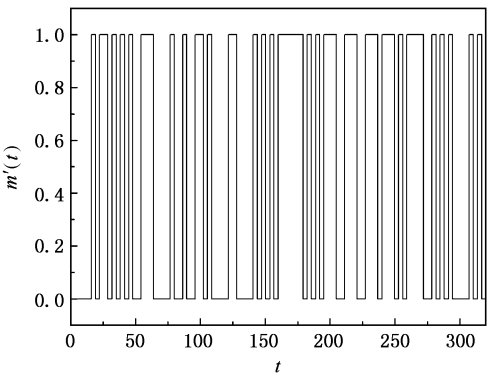

图 6 接收端解调信号 $m'(t)$ 的波形图

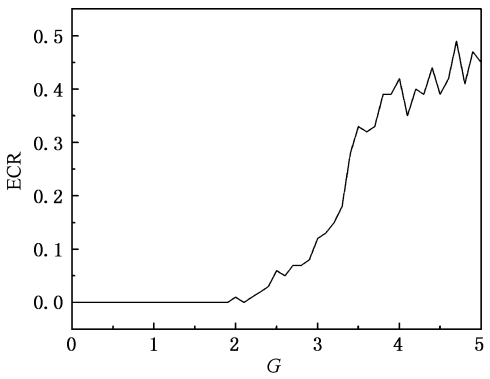

图 7　误码率与噪声强度的关系曲线

5. 结　　语

众所周知，数字通信系统以其抗干扰能力强，易于加密，易于大规模集成等特点，在通信行业将取代模拟通信而占主导地位.因此，混沌理论在数字保密通信中的应用研究也就更具现实意义.事实上，主动-被动同步方法包含了驱动-响应同步的情形，是一种更一般的方法，因此我们设计的方案具有更好的普适性.此外，由于是不同超混沌系统的一个驱动函数的交替发射，这就减小了信号的相关性，且通过对发射信号进行一系列的非线性变换，极大地增强了通信系统的保密性能.同时可以灵活地选择驱动函数的形式作为密钥，如果破译者不知道其函数形式，也就不可能对信号进行破译.研究表明，由于采用两个超混沌同步模型中不同驱动函数切换调制，使得我们提出的方案可以有效地抵制幅度为 1.9 的噪声污染，这比文献[4]中当 $G < 0.13$ 时误码率 ECR 才趋向零的效果要好，说明本通信系统对噪声具有良好的鲁棒性.

感谢罗晓曙教授对本工作的悉心指导.

[1] Boccaletti S, Farini A, Arecchi F T 1997 *Phys. Rev.* E **55** 4979

[2] Boutayeb M, Darouach M, Rafaralahy H 2002 *IEEE Trans. Circuits Syst.* I **49** 345

[3] Luo X S, Fang J Q, Wang L F 1999 *Acta Phys. Sin.* **48** 2022 (in Chinese) [罗晓曙、方锦清、王力虎 1999 物理学报 **48** 2022]

[4] Luo X S, Wang B H, Jiang P Q 2003 *J. China Institute of Commun.* **24** 60 (in Chinese) [罗晓曙、汪秉宏、蒋品群 2003 通信学报 **24** 60]

[5] Zhang J S, Xiao X C 2001 *Acta Phys. Sin.* **50** 2121 (in Chinese) [张家树、肖先赐 2001 物理学报 **50** 2121]

[6] Li G H, Xu D M, Zhou S P 2004 *Acta Phys. Sin.* **53** 706 (in Chinese) [李国辉、徐得名、周世平 2004 物理学报 **53** 706]

[7] Li J F, Li N, Lin H 2004 *Acta Phys. Sin.* **53** 1694 (in Chinese) [李建芬、李　农、林　辉 2004 物理学报 **53** 1694]

[8] Yang S P, Niu H Y, Tian G 2001 *Acta Phys. Sin.* **50** 619 (in Chinese) [杨世平、牛海艳、田　钢 2001 物理学报 **50** 619]

[9] Kolcarev L, Parlitz U 1995 *Phys. Rev. Lett.* **74** 5028

[10] Tamasevicius A, Namajunas, Cenys A 1996 *Electron Lett.* **32** 957

[11] Chen J F, Yue L J, Peng J H 2000 *J. Northeast Normal Univer.* **32** 26 (in Chinese) [陈菊芳、岳丽娟、彭建华 2000 东北师范大学学报 **32** 26]

[12] Xu S Q 1980 *Stable Theory for Ordinary Differential Equations* (Shanghai: Shanghai Scientific and Technological Publishing House) (in Chinese) [许淞庆 1980 常微分方程稳定性理论 (上海：上海科学技术出版社) 87]

A switch-modulated method for hyperchaotic digital secure communications based on drive functions

Sun Lin[1)] Jiang De-Ping[2)]

1) (*Department of Physics and Electronic Science, Changsha University of Science and Technology, Changsha* 410077, *China*)

2) (*College of Electronics and Information Engineering, Central South Forestry University, Changsha* 410004, *China*)

(Received 24 March 2005; revised manuscript received 17 August 2005)

Abstract

In this paper, a scheme for digital secure communications is proposed by using different drive functions of hyperchaotic systems based on APD approach. Two different drive functions can be alternately sent according to the transmission of binary signal "0" and "1", which will enhance the complexity and decrease the correlation of transmitted signals. Meanwhile, by designing compound nonlinear function transformation for transmitted signals to further intercalate the secret key, a determined intruder is very difficult to retrieve the contents of message signal using forecasting method. Theoretical analysis and numerical simulation results show that this method is effective.

Keywords: hyperchaos, APD, switch modulation, secure communication

PACC: 0545