

# 混沌同步及其在通信中的应用\*

## Chaotic Synchronization and Applications to Communication

覃团发 唐秋玲 陈光旨\*\*  
Qin Tuanfa Tang Qiuling Chen Guangzhi

(广西大学计算机与信息工程学院 南宁市西乡塘路 10号 530004)  
(College of Computer and Information Engineering,  
Guangxi University, 10 Xixiangtanglu, Nanning, Guangxi, 530004)

**摘要** 基于驱动响应同步和主动被动分拆同步,用洛仑兹电路构造混沌保密通信系统,在不同信噪比下进行汉语语音通信实验,并简要讨论发射电路和接收电路参数有误差对通信质量的影响。

**关键词** 驱动响应同步 主动被动分拆同步 洛仑兹电路 混沌保密通信

中图法分类号 O 414; TN 918

**Abstract** Based on drive-response synchronization and active-passive decomposition synchronization, we construct chaotic secure communication systems with the Lorenz circuit, then experiments of Chinese speech chaotic secure communications are carried out with a few signal noise ratios. That the errors of the parameters of the transmitter and the receiver circuits affect the communication quality is also briefly discussed.

**Key words** drive-response synchronization, active-passive decomposition synchronization, the Lorenz circuit, chaotic secure communication

混沌现象是在非线性动态系统中出现的确定性、类随机的过程。它的特点是对系统初始条件极端敏感,相空间中初始点非常接近的两条轨道随时间的发展会指数地分离,很快变得不相干,系统的长时间行为会显示出某种混乱性。长期以来,人们一直把混沌行为看作是有害的现象,在国际电子工业及其他领域都尽量回避混沌行为。自从 OGY<sup>[1]</sup>在控制混沌方面做了开创性的工作,应用混沌已成为整个非线性科学领域全新和具有挑战性的前沿课题之一<sup>[2]</sup>,尤其混沌在保密通信中的应用最令人瞩目,是当今国际电子学前沿的一个研究热点<sup>[3,4]</sup>。

混沌同步是混沌保密通信的关键技术之一,它的开创性工作由美国海军实验室的 Pecora 和 Carroll (PC)<sup>[5]</sup>完成。他们提出的驱动响应同步技术是在一个混沌信号的驱动下,两个混沌系统之间可以达到自

同步的状态。该技术发展了多种实现混沌保密通信的方法,主要有混沌掩蔽技术<sup>[6-7]</sup>、混沌开关技术<sup>[8-9]</sup>、混沌调制技术<sup>[10]</sup>以及数字混沌通信技术<sup>[11]</sup>,这些研究都取得一些可喜的成果,但 PC同步技术由于受到特定分解的限制,系统最大可能分解方法不超过  $\frac{1}{2}N(N-1)$  ( $N$  为系统的维数),而且要求响应系统的条件李雅普诺夫指数皆为负,这使得构造同步系统受到限制。1995年 L. Kocarev 和 U. Parlitz<sup>[12]</sup>推广了混沌同步的 PC方法,发展为主动被动分拆同步技术,该方法采取十分灵活的普适分解法,更适用于保密通信。本文基于驱动响应同步和主动被动分拆同步,用洛仑兹电路构造混沌通信系统,在不同信噪比下进行汉语语音混沌保密通信实验,并简要讨论发射电路和接收电路参数有误差对通信质量的影响。

### 1 驱动响应同步及其在通信中的应用

假定一个  $n(n = m + k + l)$  维动力系统可分解为真正用于驱动响应系统的  $m$  维变量矢量  $x$  以及不用于驱动的  $k$  维矢量  $y$ ,响应变量用  $l$  维变量矢量  $z$  表示,则驱动响应总体动力学系统表示为:

1998-04-18收稿

\* 国家自然科学基金资助项目(编号: 19562001)

\*\* 广西大学物理系,南宁西乡塘路 10号,530004(Department of Physics, Guangxi University, 10 Xixiangtanglu, Nanning, Guangxi, 530004)

$$\dot{x} = f(x, y), m \text{ 维} \quad \text{驱动} \quad (1)$$

$$\dot{y} = g(x, y), k \text{ 维} \quad (2)$$

$$\dot{z} = h(x, z), l \text{ 维} \quad \text{响应} \quad (3)$$

现复制一个新的响应系统:

$$\dot{z}' = h(x, z') \quad (4)$$

它和子系统  $z$  完全相同, 显然  $z$  和  $z'$  同步的条件是, 当

$$t \rightarrow \infty, |z'(t) - z(t)| \rightarrow 0$$

根据矢量场

$$\Delta \dot{z} = h(x, z) - h(x, z') = D_z h(x, z) \Delta z + o(x, z) \quad (5)$$

$D_z h$  是响应系统  $z$  的雅可比行列式对响应变量  $z$  求偏导数, 相应的李雅普诺夫指数, 称为系统  $z$  的条件李雅普诺夫指数。

在  $\Delta z$  很小的极限条件下

$$\Delta \dot{z} = D_z h(x, z) \Delta z \quad (6)$$

若  $z(t)$  是常数或周期态, 则可求出  $D_z h$  的特征值或多重乘子以判断  $z(t)$  的稳定性, 但这里  $z$  受混沌信号  $x$  所驱动, 所以不能作简单的稳定性分析。  $z(t)$  的稳定性分析, 我们用条件李雅普诺夫稳定性判据: 只有当子系统  $z$  的所有条件李雅普诺夫指数均为负数,  $z$  和  $z'$  同步。

下面我们用洛仑兹电路系统构造驱动响应同步的混沌通信系统如图 1 所示。

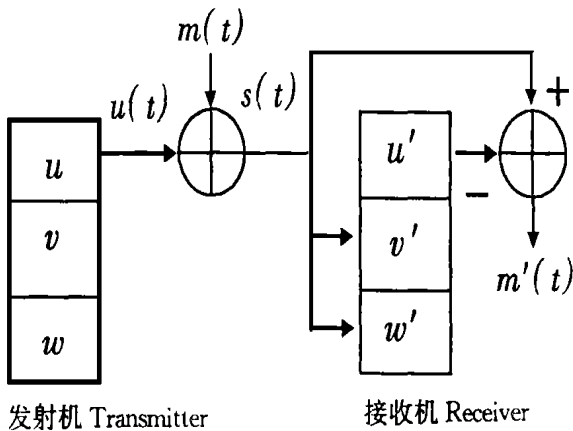


图 1 洛仑兹电路系统构造的混沌通信系统

Fig. 1 Chaotic communication systems with the Lorenz circuits

发射机:

$$\begin{aligned} \dot{u} &= T(v - u) \\ \dot{v} &= V u - v - 20uv \\ \dot{w} &= 5uv - bw \end{aligned} \quad (7)$$

当  $T = 16.0, V = 45.6, b = 4.0$  方程组 (7) 处于混沌状态, 且由  $u$  作驱动信号的  $(v, w)$  组成的子系统的条件李雅普诺夫指数是  $\lambda_1 = -2.42, \lambda_2 = -2.58$ , 且  $u$  的 16 kHz 采样率的频谱图如图 2, 具有类似白噪声的

宽频谱, 可用作掩蔽语音信息信号。因此, 发射机传送信号为

$$s(t) = u(t) + m(t) \quad (8)$$

信息信号  $m(t)$  被直接加到类似随机的混沌信号  $u(t)$  上作为发射信号送出去, 接收机收到发射信号  $s(t)$  后, 再生出混沌信号  $u'(t)$ , 同步后  $u'(t) \approx u(t)$ , 因此可以从发射信号减去  $u'(t)$  而提取信息信号  $m(t)$ , 因此接收机为:

$$\begin{aligned} \dot{u}' &= T(v' - u') \\ \dot{v}' &= V s(t) - v' - 20s(t)w' \\ \dot{w}' &= 5s(t)v' - bw' \end{aligned} \quad (9)$$

恢复出来的信息信号为:  $m'(t) = s(t) - u'(t)$  (10)

由于人的语音频率范围在 300 Hz 至 3 400 Hz 之间, 中文语音“r”“z”的 1 秒钟波形及 8k Hz 采样率的频谱如图 3

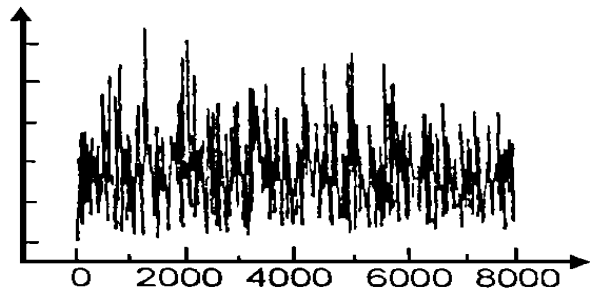
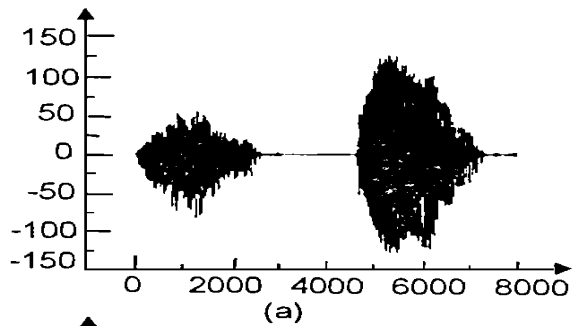


图 2 Fig. 2



(a)

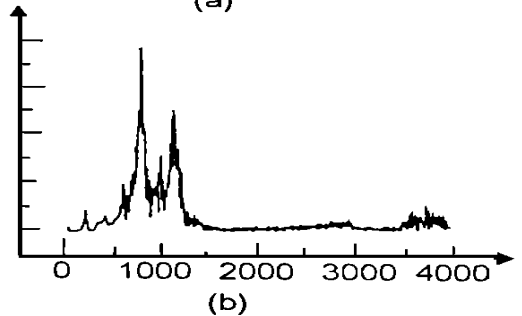


图 3 Fig. 3

1) 当接收系统参数为  $T = 16.0, V = 45.6, b = 4.0$

i) 不同的混沌噪声强度和语音信号强度信噪比 (SNR) 对语音信号掩蔽的听感比较以及恢复出来的语音信号信噪比的测试结果是:

传输信号                      恢复出的信号

SN R	听 感	SN R	听 感
0dB	清 晰	21dB	很 清晰
- 6dB	模 糊	16dB	很 清晰
- 12dB	非 常 模 糊	11dB	清 晰
- 18dB	听 不 见	6dB	清 晰

ii) 信噪比为 - 18dB 时 传 送 信 号 的 波 形 及 频 谱 如

图 4, 恢复出来的语音信号的波形和频谱如图 5

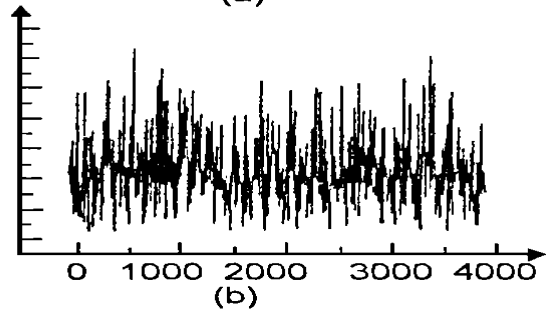
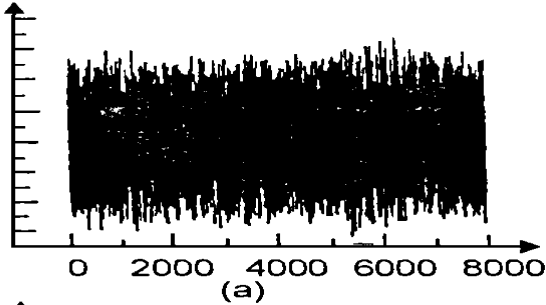


图 4 Fig. 4

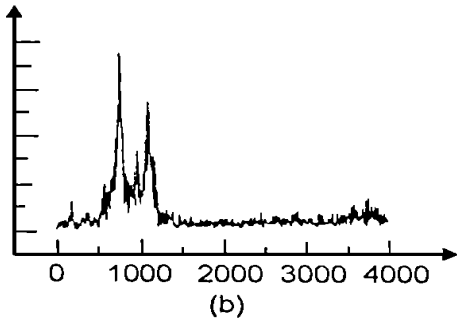
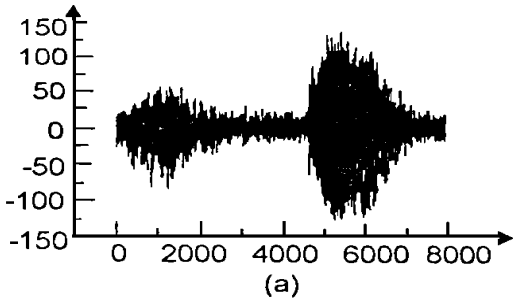


图 5 Fig. 5

2) 当接收系统的参数与发射机的参数有大约 3% 的误差时, 恢复出来的信号误差小于 1dB, 这样表明发射系统和接收系统仍然能近似同步; 当接收系统的参数与发射系统的参数的误差达到 10%, 则不能

从接受系统提取语音信号。

## 2 主动被动分拆同步及其在通信系统中的应用

考虑一个非线性的自治系统

$$\dot{z} = F(z) \quad (11)$$

我们总可以把 (11) 改写成非自治形式

$$\dot{x} = f(x, s(t)) \quad (12)$$

其中  $s(t)$  为所选的某种驱动变量

$$s(t) = h(x) \text{ 或 } s(t) = h(x, s)$$

接收系统是被  $s(t)$  驱动的复制品

$$\dot{y} = f(y, s(t)) \quad (13)$$

由式 (12)、(13) 可导出系统的变量差  $e = x - y$  满足:

$$\dot{e} = f(x, s) - f(y, s) = f(x, s) - f(x - e, s) \quad (14)$$

在  $e = 0$  处有一个稳定的不动点, 式 (12)、(13) 存在一个稳定的同步态。

我们可以在  $e$  为小值的情况下, 应用线性化的稳定性分析方法或李雅普诺夫函数的方法证明  $x$  和  $y$  达到稳定同步。一般情况, 我们倾向于用条件李雅普诺夫指数来判断是否达到同步。当式 (12) 的所有条件李雅普诺夫指数皆为负数, 它是一个没有驱动的且趋向于一个不动点的被动系统, 因此称这里给出的分拆  $h$  和  $f$  为主动被动分拆技术, 相应的同步为主动被动同步。用洛仑兹电路来构造的混沌保密通信系统如图 6

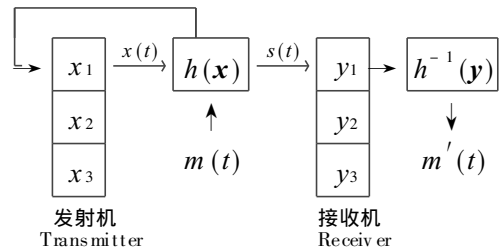


图 6 Fig. 6

发射系统:

$$\begin{aligned} \dot{x}_1 &= -16x_1 + s(t) \\ \dot{x}_2 &= 45.6x_1 - x_2 - 20.0x_1x_3 \\ \dot{x}_3 &= 5.0x_1x_2 - 4.0x_3 \end{aligned} \quad (15)$$

方程 (15) 的条件李雅普诺夫指数是  $\lambda_1 = -2.42$ ,

$\lambda_2 = -2.58, \lambda_3 = -16.0$

$$\text{传送信号: } s(t) = 16x_2 + m(t) \quad (16)$$

$m(t)$  是加入的信息信号。

接收系统:

$$\begin{aligned} \dot{y}_1 &= -17y_1 + s(t) \\ \dot{y}_2 &= 45.6y_1 - y_2 - 20.0y_1y_3 \\ \dot{y}_3 &= 5.0y_1y_2 - by_3 \end{aligned} \quad (17)$$

恢复的信息信号:  $m'(t) = s(t) - 16y_2$

下面的实验仍然是传送信息信号为图 3 的中文语音信号“1”“2”。

1) 接收系统和发射系统参数相同, 即式 (17) 中  $T=16.0, V=45.6, b=4.0$  又因式 (15) 的全部条件李雅普诺夫指数全为负, 因此接收系统和发射系统能准确同步。传送信号的中文语音“1”“2”和混沌噪声信噪比为  $-18\text{dB}$  时的波形和频谱如图 7, 恢复出来的语音信号及其波形如图 8 实验结果表明信息信号能准确地被恢复。

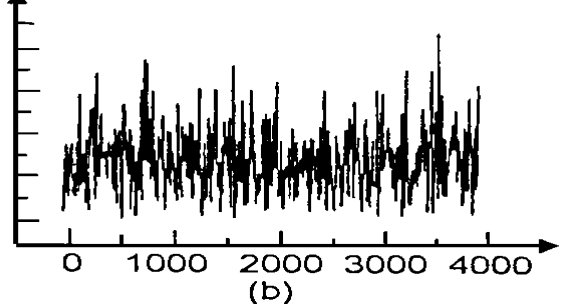
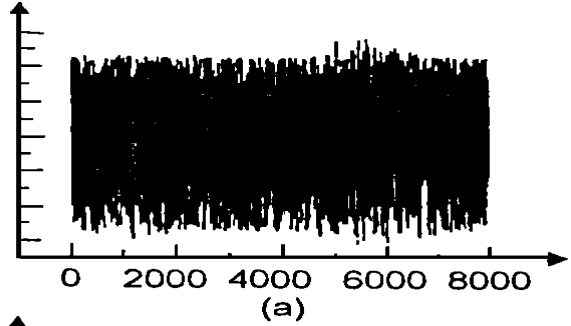


图 7 Fig. 7

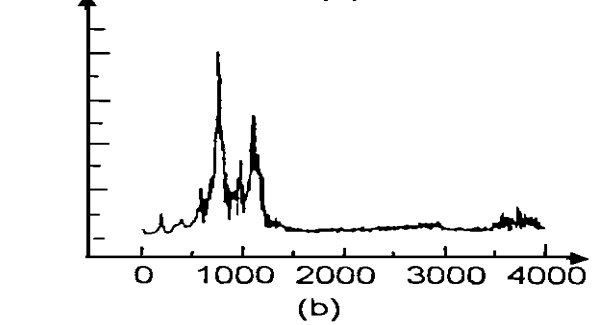
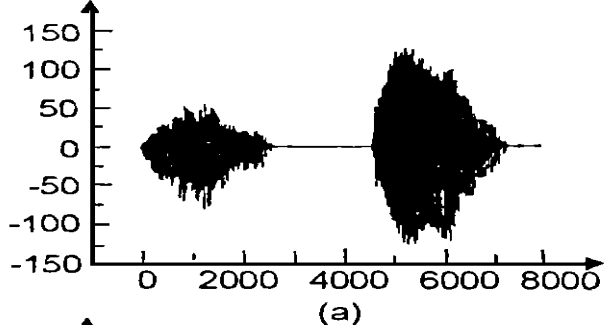


图 8 Fig. 8

2) 接收系统参数与发射系统不同, 如方程 (17)

中  $T=15.6, V=45.0, b=4.2$ , 两系统参数最大误差可达  $5\%$ 。实验结果: 传送信号的信噪比为  $-18\text{dB}$  时的波形和频谱如图 9, 恢复出来的信号波形和频谱如图 10 仅能近似恢复信号, 听感比较模糊。

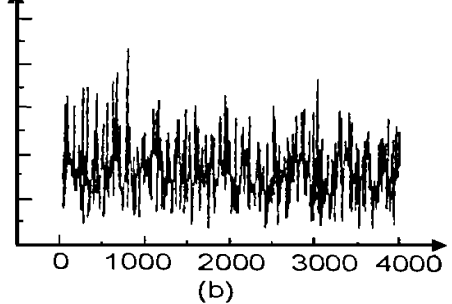
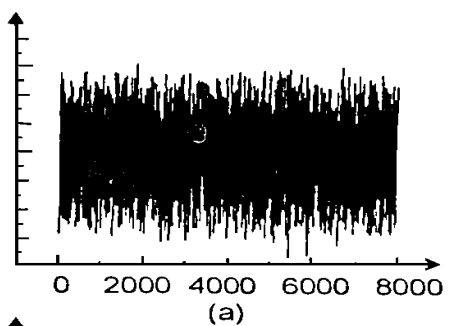


图 9 Fig. 9

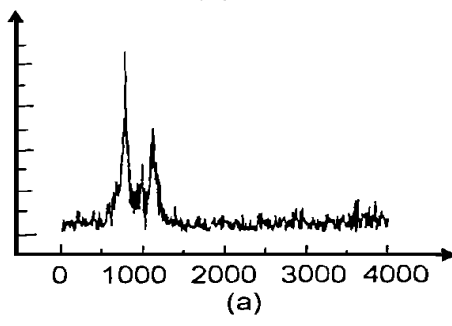
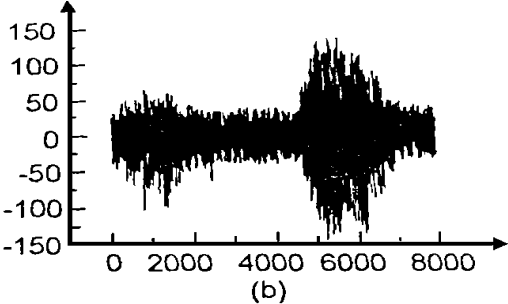


图 10 Fig. 10

### 3 结语

混沌信号具有类似白噪声的宽频谱且由确定系统产生, 很适合于用来掩蔽信息信号。在本文中我们选定的电路系统的参数产生的频谱较宽, 完全能覆盖一般人的语音频谱, 基于驱动响应同步和主动被动分拆同步及其在保密通信中的应用可得出如下结论: 第

一,在发射系统和接受系统参数无误差下,两种同步方式在相同的信噪比下对信息信号的掩蔽能力相同。但在驱动响应同步方法中,信息信号是直接加在混沌载体上,这时,由混沌信号和信息信号之和共同强迫接收机,发射机仅由混沌信号驱动,发射系统和接收系统近似同步,恢复出来的信号有一定误差。而主动被动分拆同步,信息信号是注入到作为发射机的动力学系统中,因此,发射系统和接收系统能准确同步,信息信号被准确恢复。第二,在满足同步条件的情况下,主动被动分拆同步方法采用灵活多变形式,且该同步方式对系统参数比驱动响应同步敏感,有更好的保密性和更高的抗破译能力。但驱动响应同步由于其结构简单,且易于实现亦有其实用的价值。

### 参考文献

- 1 Ott E, Grebogi C, Yorke J A. Controlling chaos. *Physical Review Letters*, 1990, 64 (11): 1196~ 1199.
- 2 方锦清. 非线性系统中混沌控制与同步及其应用前景. *物理学进展*, 1996, 16 (1): 1~ 74.
- 3 Chua L O, Hasler. Special issue on chaos in nonlinear electronic circuits. *IEEE Transactions on CAS*, 1993, 40 (10, 11): 637~ 884.
- 4 Kennedy M P, Ogorzalek. Special issue on chaos synchronization and control: theory and application. *IEEE Transactions on Circuits and Systems*, 1997, 44( 10): 853 ~ 1039.

- 5 Pecora L M , Carroll T L. Synchronization in chaotic systems. *Physical Review Letters*, 1990, 64 ( 8): 821~ 824.
- 6 Cuomo K M, Oppenheim A V, Strogatz S H, Synchronization of lorenz-based chaotic circuits with applications to communications. *IEEE Trans. On CAS*, 1993, CAS-40 (10), 626~ 633
- 7 Kocarev L, Halle K S, Eckert R et al. . Experimental demonstration of secure communications via chaotic synchronization. *Int J Bifurcation and Chaos* , 1992, 2 (3): 709~ 713.
- 8 Ponnitz U, Chua L O, Kocarev L et al. . Transmission of digital by chaotic synchronization. *Int J Bifurcation and Chaos* 1992, 2 973~ 977.
- 9 Dedien H, Kennedy M P, Hasler M. Chaos shift keying, M: modulation and demodulation of a chaotic carrier using self-synchronizing chua's circuits. *IEEE Trans, on CAS*, 1993, CAS-40 (11): 634~ 643.
- 10 Halle K S, Wa C W, Itoh M et al. Spread spectrum communication through modulation of chaos. *Int J Bifurcation and Chaos*, 1993, 3 (2): 469~ 477.
- 11 Frey D R. Chaotic digital encoding an approach to secure communication. *IEEE Trans, on CAS*, 1993, CAS 40 ( 10): 660~ 666.
- 12 Kocorev L. Parlitz V. General approach for chaotic synchronization with applications to communication. *Physical Review Letters*, 1995, 74 (25): 5028~ 5031.

(责任编辑: 邓大玉)

(上接第 258页 Continue from page 258)

- 18 张尚通,许崇任.转基因微生物生态学及大田释放风险评估研究. *应用生态学报*, 1994, 5 (3): 325~ 330.
- 19 Nordlee J et al. . Identification of a Brazil-nut allergen in transgenic soybeans. *The New England J Medicine*, 1996, 334: 688~ 692.

- 20 Burkhardt P K. Genetic engineering of provitamin A biosynthesis in rice endosperm. In: *International Rice Research Institute. Proceeding of the III International Rice Genetic Symposium*, Abstract. 1995. 178.
- 21 Meek S D. Letter to the editor. *Aust J Biotechnology*, 1991, 5 (1): 25~ 29, 47.

(责任编辑: 蒋汉明)