第 6 卷第 3 期 2008 年 9 月
1672-6553/2008/06(3)/254-6

动力学与控制学报
JOURNAL OF DYNAMICS AND CONTROL

Vol. 6 No. 3
Sep. 2008

基于混沌切换系统的语音加密

林彩霞　郝建红

（华北电力大学电气与电子工程学院，北京　102206）

摘要　鉴于语音信号的“即时性”特点，在分析了混沌掩盖、混沌调制进行加密利弊的基础上，构造了一种混沌切换加密方案，对语音进行了更安全有效地加密. 计算仿真实现了对语音信号的加密，实验表明了此方法的可行性，并对其加密解密效果、抗破译能力、同步时间以及保密强度进行了分析和比较.

关键词　Qi 混沌系统，混沌加性加密，　混沌乘性加密，　混沌切换加密

引 言

混沌理论应用于保密通信已经成为混沌研究的一个重要课题. 混沌是一种特殊的运动形式，它遵循动力学机制，但表现内在的随机性，其应用越来越引起人们的重视[1~3]. 在因特网领域，IP 电话（Internet Phony，因特网电话）技术成为网络的核心技术之一，同时针对 IP 电话等语音通信的攻击越来越严重，如电话窃听、电话跟踪等，这些攻击和干扰对语音通信构成了极大威胁[4]. 本文设计了一种切换加密方案保证语音信息的安全传输.

语音信号的一个特点在于他的“短时性”，也就是我们常说的“即时性”，即：有时在一个短时段呈现随机噪声的特性，而另一段表现周期信号的特性，或二者兼而有之，这一特点是正弦信号和离散信号所不具备的. 语音信号的特征是随时间变化的，只有一段时间内，信号才表现稳定一致的特征，一般来说短时段可取 5 ~ 50 ms，因此对语音信号的加密主要建立在其“短时性”上.

针对图像或语音信号，已经提出很多加密方案，在直接利用混沌进行加密的系统中，主要是把混沌系统作为密钥流发生器，利用它的良好的伪随机性产生看似“一次一密”的密钥流. 文献[5]利用传统的混沌同步方案实现了数字信号的保密通信. 文献[6]提出了两种基于复合离散混沌系统的同步序列密码方法，其加密和解密是一个复合离散混沌系统的相同的迭代过程. 文献[7]提出了两种加密方法，即加性和乘性加密方法，主要是将小能量的信号与混沌信号直接相加或者相乘，文献[8]实现了一类切换混沌系统. 以上加密方案的共同点是采用的都是低维混沌系统，不但容易被破译，而且容易受到攻击，保密性不高，文献[9]也指出，基于低维混沌的通信系统易受自适应同步控制的攻击，不具有很高的保密性. 基于此，本文在改进低维混沌系统简单加性和乘性的基础上，结合语音信号的“短时性”特点，提出了一种多个混沌系统的切换加密方案，其复杂的动力学行为能够用来对语音信号进行安全、准确地加密和解密，保证了语音加密的可靠性和准确性，尤其在大功率语音信号加密上更具优势.

1　语音混沌切换加密方案

目前，将混沌应用于信息加密主要有加性加密和乘性加密[10]，但是这两种方法只适用于小信息信号，对于稍大的信号，在公共信道中，语音将会“浮”出来，所以本文设计了一种混沌切换加密方案来保证较大信号的安全准确传输.

1.1　混沌加密系统

最近，新构造的一个四维自治混沌系统[11~12]，其数学表达式为

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2x_3x_4 \\ \dot{x}_2 = b(x_2 + x_1) - x_1x_3x_4 \\ \dot{x}_3 = -cx_3 + x_1x_2x_4 \\ \dot{x}_4 = -dx_4 + x_1x_2x_3 \end{cases} \tag{1}$$

$x = [x_1, x_2, x_3, x_4]^T$ 是关于时间 t（单位：s）的状态

2008-04-11 收到第 1 稿，2008-05-15 收到修改稿.
* 华北电力大学博士基金（200708 ）资助项目

变量,a,b,c,c 是正值参数 $a=25,b=2,c=25,d=35$. 取参数时,系统为复杂的混沌系统. 下面我们采用 Qi 混沌系统对语音信号进行加密分析,发射系统采用(1)作为混沌加密的驱动系统,接收端用观测器方法[13]实现与发射系统的同步. 混沌的同步方法有许多,状态观测器同步方法实现简单,而且同步时间较短,所以采用此方法,本文针对 Qi 系统构造的全维状态观测器方程为

$$\begin{cases}\dot{\hat{x}}_1 = -\hat{x}_1 + ax_2 - (a-1)x_1 + x_2x_3x_4\\ \dot{\hat{x}}_2 = -\hat{x}_2 + bx_1 + (b+1)x_2 - x_1x_3x_4\\ \dot{\hat{x}}_3 = -\hat{x}_3 - (c-1)x_3 + x_1x_2x_4\\ \dot{\hat{x}}_4 = -\hat{x}_4 - (d-1)x_4 + x_1x_2x_3\end{cases} \tag{2}$$

用(2)作为加密响应系统,其中 $\dot{x}=[\dot{x}_1,\dot{x}_2,\dot{x}_3,\dot{x}_4]^T$ 是观测器关于时间 t 的状态变量,通过计算可知大概经过 1s 时间,状态观测器和 Qi 混沌系统完全实现同步. 同时,本方案中采用的其他混沌系统也使用状态观测器方法实现同步.

1.2　切换系统方案

对于语音信号的简单加密方式,如加性与乘性加密[10]方式,可以用神经网络、回归映射等方法破译,为了增强抗破译能力,同时结合语音信号的实时性要求,我们把语音信号 s 的幅值作为判据,设计出一种切换加密方式,在发射端一旦检测到符合条件的混沌系统,开关键控操作,利用几个混沌系统的驱动函数对语音信号进行轮换调制,在接收端依照特定的响应系统对接收到的加密语音信号进行解密,具体原理如图 1 所示.

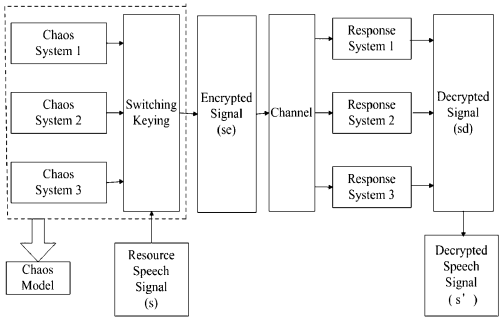

图 1　语音切换加密原理图

Fig. 1　Schematic diagram of chaotic switching encryption for speech

针对语音信号的“短时性”特点,设计信号大于零、等于零和小于零时分别采用三个混沌系统切换加密. 考虑到 *Liu* 系统是一种频谱较宽的混沌系统,而 *Qi* 混沌系统具有较复杂的动力学行为,所以,本文选用 *Liu* 混沌系统、三维 *Qi* 混沌系统、四维 *Qi* 混沌系统作为切换系统. 具体方案如下:

输入端的切换混沌系统为

混沌系统 1 (*liu* 系统)

$$\begin{cases}\dot{x}_1 = a(x_2 - x_1)\\ \dot{x}_2 = bx_1 - kx_1x\\ \dot{x}_3 = hx_1^2 - cx_3\end{cases}$$

接收端对应的解密系统为

解密系统 1

$$\begin{cases}\dot{\hat{x}}_1 = -\hat{x}_1 - (a-1)(x_2 - x_1)\\ \dot{\hat{x}}_2 = -\hat{x}_2 + bx_1 + x_2 - kx_1x_3\\ \dot{\hat{x}}_3 = -\hat{x}_3 + hx_1^2 - (c-1)x_3\end{cases}$$

其中,$a=10,b=40,c=2.5,k=1,h=4$

混沌系统 2(三维 *Qi* 系统)

$$\begin{cases}\dot{y}_1 = a(y_2 - y_1) + y_2y\\ \dot{y}_2 = cy_1 - y_2 - y_1y_3\\ \dot{y}_3 = y_1y_2 - by_3\end{cases}$$

解密系统 2

$$\begin{cases}\dot{\hat{y}}_1 = -3\hat{y}_1 + ay_2 - (a-3)y_1 - y_1y_3\\ \dot{\hat{y}}_2 = -\dot{y}_2 + cy_1 - y_1y_3\\ \dot{\hat{y}}_3 = -2\dot{y}_3 + y_1y_2 - (c-2)y_3\end{cases}$$

其中,$a=35,b=8/3,c=80$

混沌系统 3(四维 *Qi* 系统)

$$\begin{cases}\dot{z}_1 = a(z_2 - z_1) + z_2z_3z_4\\ \dot{z}_2 = b(z_2 + z_1) - z_1z_3z_4\\ \dot{z}_3 = -cz_3 + z_1z_2z_4\\ \dot{z}_4 = -dz_4 + z_1z_2z_3\end{cases}$$

解密系统 3

$$\begin{cases}\dot{\hat{z}}_1 = -\hat{z}_1 + az_2 - (a-1)z_1 + z_2z_3z_4\\ \dot{\hat{z}}_2 = -\dot{z}_2 + bz_1 + (b+1)z_2 - z_1z_3z_4\\ \dot{\hat{z}}_3 = -\dot{z}_3 - (c-1)z_3 + z_1z_2z_4\\ \dot{\hat{z}}_4 = -\dot{z}_4 - (d-1)z_4 + z_1z_2z_3\end{cases}$$

其中,$a=25,b=2,c=25,d=35$

$x_i,y_i,z_i(i=1,2,3,4)$ 为接收端切换系统的混沌值,$\hat{x}_i,\hat{y}_i,\hat{z}_i(i=1,2,3,4)$ 为解密端状态观测器的值. 采用信源(语音)信号的幅值作为开关键控,当信源(语音)信号的幅值大于 0 的时候,切换到混沌系统 1,当幅值小于 0 的时候,切换到混沌系统 2,当幅值等于 0 的时候,切换到混沌系统 3. 接收

端为各自混沌系统所对应的解密响应系统,即响应系统 1、响应系统 2、响应系统 3. 加/解密数学表达式为

加密信号为

$$se=\begin{cases}x_2+(x_1+s)x_3 & s>\\ y_2+(y_1+s)y_3 & s<0\\ z_2+(z_1+s)z_3 & s=0\end{cases}$$

解密信号为

$$sd=\begin{cases}(se-\hat{x}_2)/x_3-x_1 & s>\\ (se-\hat{y}_2)/y_3-y_1 & s<0\\ (se-\hat{z}_2)/z_3-z_1 & s=0\end{cases}$$

计算中被加密的语音信号是一段鸟鸣声,通过数值计算,加/解密后信号如图 2 所示. 图 2(a)是信源信号,图 2(b)是加密后的信道传输信号,可以看出,加密后的信号完全失去了原始语言信号的特征. 图 2(c)是解密信号,大概经过 2s 同步时间后,其与原始语音信号相同,同步时语音信号会被认为是同步噪声,所以影响了同步时间,使解密同步时间比纯粹混沌系统的同步时间长,图 2(d)是解密信号与原始信号的误差,将两信号每一时刻点的值对应相减,再求其平均值,计算显示两者平均误差小于 2.57×10^{-4},误差很小,能够正确解密信号. 对语音回放,加密信号是非常刺耳的噪声,解密信号在经过一小段类似噪声之后就是很清楚的鸟鸣声信号.

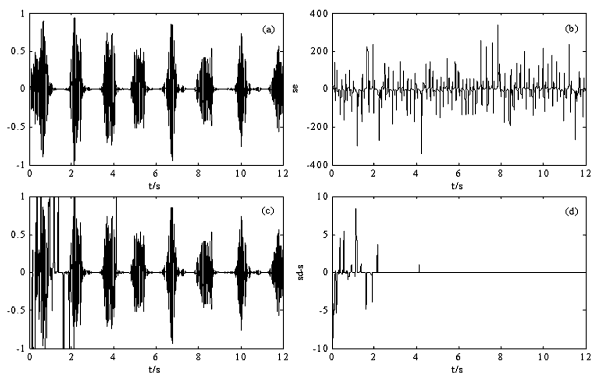

图2 切换加密(a)信源信号,(b)加密语音,(c)解密语音,(d)解密误差

Fig. 2 Chaotic switching encryption (a) source signal (b)encrypted speech (c)decrypted speech (d) decryption error

2 保密性分析

混沌信号是一种随机信号,有丰富的频率分量,只要混沌信号的频带范围足够大,就可以掩盖语音信号. Qi 混沌系统和语音信号的时间域分布如图 3 所示,可见,语音信号与混沌信号相比为弱信号. 两者的频谱分布和如图 4(a)和 4(b)所示,从图中可以看出,混沌信号的功率幅度大于语音信号的功率幅度,所以,当采用加性和乘性加密[10]的时候,混沌信号也会很好的掩盖住语音信号,同时也注意到语音信号频谱集中范围的幅度与此范围的混沌信号幅度很接近,一旦语音信号幅度稍微增加,采用加性和乘性加密时,那么语音信号就会从混沌信号中“浮”出来,而本文设计的切换加密方案,却能很好地解决这一问题.

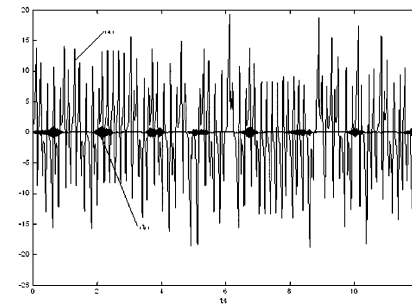

图 3 发射端混沌信号与语音信号:(a)混沌信号,(b)语音信号

Fig. 3 Chaos and speech signal of transmitter: (a)chaos signal, (b)speech signal

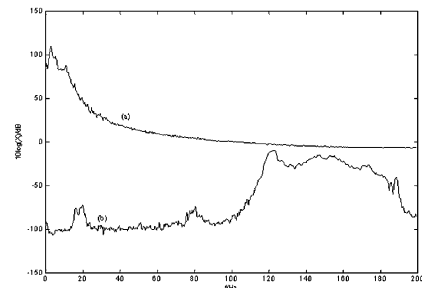

图 4 频谱图:(a)*Qi* 系统频谱,(b)语音信号频谱

Fig. 4 Spectrum: (a)spectrum of Qi system, (b)speech spectrum

上图中,混沌信号与语音信号的功率强度相差比较大,两者的平均功率比为 7.1,对加性、乘性以及本文设计的切换加密都能很好地加密语音信号. 加性加密[7]时发送端信号为 $se=s+x_1$,接收端信号为 $sd=se-\hat{x}_1$,乘性加密[7]时发送端加密信号为 $se=20(s+x_1)/x_2+10x_3$,接收端解密信号 $sd=(s-10\hat{x}_3)\hat{x}_2/20-\hat{x}_1$. 现在增加语音信号的强度,使语音信号与混沌信号的功率比增大,再分别采用加性、乘性和切换加密三种方式对语音信号进行加/解密,图 5、图 6、图 7 分别为语音信号与混沌信号平均功率比为 1、14、56 时的加密结果.

从图 5、6、7 可以看出,在加性方式和乘性方式加密中,随着语音信号功率的增大,语音信号会逐渐“浮”出混沌信号,很容易在传输信道中被破译. 本文设计的切换加密方式对大功率语音信号的加密效果很好,语音信号很难从加密信号中“浮”出来,即使在信道中被截获也很难用传统的解密方式破译,所以此加密方法有很好的加密效果和抗攻击能力.

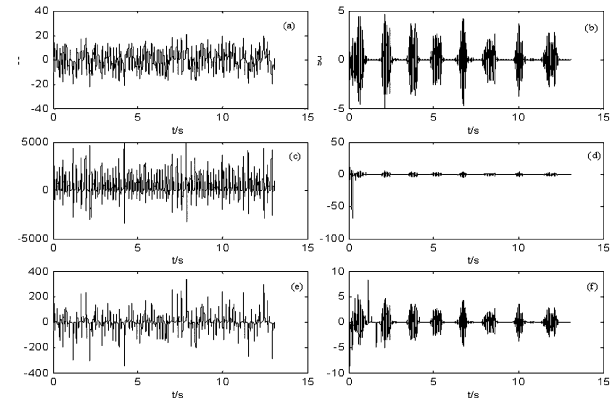

图 5　语音信号与混沌信号平均功率比为 1 时的加/解密信号
(a)加性加密语音,(b)加性解密语音,(c)乘性加密语音,
(d)乘性解密语音,(e)切换加密语音,(f)切换解密语音

Fig. 5　Encryption and decryption signal when the power ratio of speech and chaos signal is 1:(a)chaotic additives encryption; (b)chaotic additives decryption;(c)chaotic multiplicative encryption; (d)chaotic multiplicative decryption; (e)chaotic switching encryption;(f)chaotic switching decryption

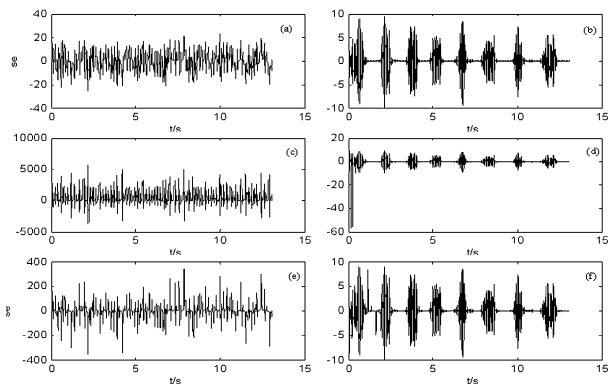

图 6　语音信号与混沌信号平均功率比为 14 时的加/解密信号
(a)加性加密语音,(b)加性解密语音,(c)乘性加密语音,
(d)乘性解密语音,(e)切换加密语音,(f)切换解密语音

Fig. 6　Encryption and decryption signal when the power ratio of speech and chaos signal is 14:(a)chaotic additives encryption; (b)chaotic additives decryption;(c)chaotic multiplicative encryption; (d)chaotic multiplicative decryption; (e)chaotic switching encryption;(f)chaotic switching decryption

从相关函数来看信号的保密性强度[14]. 如图 8 所示. 由图(a)可见,混沌信号的 δ 特性很好,有很强的加密特性. 加密后,语音信号完全淹没在混沌信号中,由图(b)可见,加密信号也有很好的 δ 特性,加密效果比较理想,保密性强度较高.

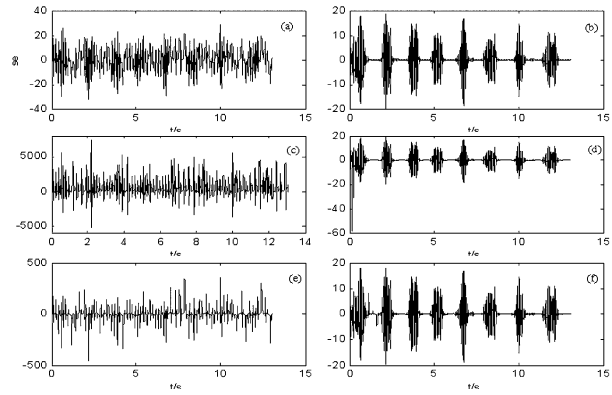

图 7　语音信号与混沌信号平均功率比为 56 时的加/解密信号
(a)加性加密语音,(b)加性解密语音,(c)乘性加密语音,
(d)乘性解密语音,(e)切换加密语音,(f)切换解密语音

Fig. 7　Encryption and decryption signal when the power ratio of speech and chaos signal is 56(a)chaotic additives encryption; (b)chaotic additives decryption;(c)chaotic multiplicative encryption; (d)chaotic multiplicative decryption; (e)chaotic switching encryption;(f)chaotic switching decryption

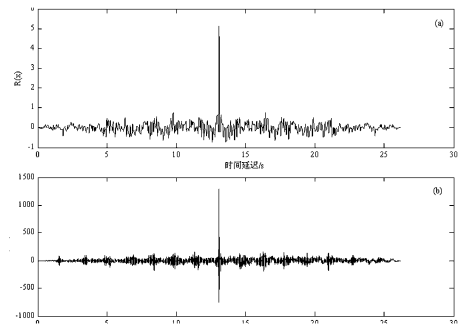

图 8　(a)混沌信号 x_1 的自相关函数,
(b)加密信号与信源信号的互相关函数

Fig. 8　(a)autocorrelation function of chaos signal x_1 (b)coherence function of encryption and source signal

从保密性方面,对于加性加密与乘性加密,很容易利用现有的技术被破译. 切换加密则大大增加了破译和攻击难度:切换加密用三个不同的混沌系统作为驱动函数对语音信号进行轮番加密,传输中加密信号即使被截获,首先,截获者要重构出三个完全不同的混沌系统,其次,还要再分析如何键控混沌系统,最后,要分析用何种解密方法,要全部分析出这三点才能有破译出原始(语音)信号的可能. 另外,密钥空间越大,加密系统的安全性越高,

本文设计的切换系统中,加密端三个混沌系统产生 10 个混沌分量,语音信号有大于 0、小于 0、等于 0 这三种情况,每种情况从这 10 个分量中取 3 个分量中进行加密处理,所以加密端的加密信号有 $3^{C_{10}^3}=3^{120}=1.79\times10^{57}$ 种选择,即加密时的密钥空间很大,由此可见,无论从破译难度上还是从破译工作量上都极大地增强了信号的抗破译能力. 但同时也注意到,上述混沌切换加密方式与简单的加性和乘性加密方式相比,接收端解密系统与发送端混沌系统的同步时间变长,主要是因为同步时语音信号会被认为是同步噪声,所以影响了混沌系统的同步时间,使解密同步时间比纯粹混沌系统的同步时间长,所以,在兼顾了加密解密效果和抗破译能力的同时,却牺牲了混沌系统的同步时间. 在实际传输中可以在语音加密前加一段 2s 的其他语音信号,那么解密 2s 之后的信号就是我们完全所需要的语音信号,既保证了语音信号的正确传输,又保证了语音信号在传输中不被截获者破译.

3 结论

加性、乘性和切换三种加密方式中,加性和乘性加密方式的同步时间很短,但是抗破译能力差,通过键控对三种混沌系统进行切换,轮番对信源信号进行加密,虽然发射端的驱动系统和接收端的响应系统同步时间变长,但其加密效果和抗破译能力却大大优于前两种,尤其在大功率信号的加密方面有着很好的优势. 在进行语音加密的时候,要统筹考虑各方面的性能指标,选择最佳的加密方案和加密方法. 本文设计的切换加密方案对瞬时变化的信号和大能量信号有很好的加密效果,只要混沌系统之间能够很好地进行切换,就可以用切换的思想对语音、视频等信息进行加密处理,具有很好的参考价值.

参 考 文 献

1 S J Li, X Q Mou and Y L Cai. Pseudo-random bit generator based on couple chaotic systems and its application in stream-ciphers cryptography. Progress in cryptology – INDOCRYPT, Lecture Notes in Computer Science, 2001, 2247:316 ~ 329

2 Pecorra L M, Carroll T L. Synchronized chaotic signal and systems. *IEEE ICASSP*, 1992:117 ~ 120

3 I P Smirnov, A L Virovlyansky, G M Zaslavsky. Theory and applications of ray chaos to underwater acoustics. *Phys. Rev. E*, 2001, 64:036221

4 Sol M, Savelsbergh M. The generation pickup and delivery problem. *Transportation Science*, 1995, 29(1):17 ~ 29

5 Murali K. Heterogeneous chaotic systems based cryptography. *Physics Letters A*, 2000, 272(3):184 ~ 192

6 李红达,冯登国. 基于复合离散混沌动力系统的序列密码算法. 软件学报,2003,14(5):991 ~ 998(Li Hongda, Feng Dengguo. Stream cipher algorithms based on composite nonlinear discrete chaotic dynamical systems. *Journal of Software*, 2003, 14(5):991 ~ 998(in Chinese))

7 孙志华,郝建红. 两种混沌加密方式的计算分析. 动力学与控制学报,2007,5(1):39 ~ 43(Sun Zhihua, Hao Jianhong. Analysis on two kinds of chaotic encrypting modes. *Journal of Dynamics and Control*, 2007, 5(1):39 ~ 43(in Chinese))

8 刘扬正,姜长生,林长圣,熊星,石磊. 一类切换混沌系统的实现. 物理学报,2007,56(6):3107 ~ 3112(Liu Yangzheng, Jiang Changsheng, Lin Changsheng, Xiong Xing, Shi Lei. A Class of switchable 3D chaotic systems. *Acta Phys. Sin*, 2007, 56(6):3107 ~ 3112 (in Chinese))

9 易开样,孙鑫,石教英. 一种基于混沌序列的图像加密算法. 计算机辅助设计与图形学学报,2000,12(9):672 ~ 676(Yi Kaiyang, Sun Xin, Shi Jiaoying. A King of Image Encrypting algorithm Based on Chaos Array. *Computer Asis Design and Image Journal*, 2000, 12(9):672 ~ 676(in Chinese))

10 胡岗等. 混沌控制. 上海:科技教育出版社,2000(Hu Gang. Chaos control. ShangHai: science and technology &education publishing company, 2000(in Chinese))

11 Qi Guoyuan, Du Shengzhi, Chen Guanrong, Chen Zengqiang, Yuan Zhuzhi. On a four-dimensional chaotic system. *Chaos, Soliton &Fractals*, 2005, 23:1671 ~ 1682

12 张宇辉,齐国元,刘文良,阎彦. 一个新的四维混沌系统理论分析与电路实现,物理学报,2006,55:3307 ~ 3341(Zhang Yuhui, Qi Guoyuan, Liu Wenliang, Yan Yan. Theoretical analysis and circuit implementation of a new four dimensional chaotic system. *Acta Phys. Sin*, 2006, 55:3307 ~ 3341 (in Chinese))

13 高铁杠,陈增强,袁著祉,顾巧论. 基于观测器的混沌系统的同步研究. 物理学报,2004,53:1305 ~ 1308(Gao Tiegang, Chen Zengqiang, Yuan Zhuzhi, Gu Qiaolun. Study on synchronization of chaotic systems based on observer. *Ac-*

ta Phys. Sin,2004,53:1305 ~ 1308(in Chinese))

14　谢鲲,雷敏,冯正进. 一种超混沌系统的加密特性分析. 物理学报,2005,54:1267 ~ 1272(Xie Kun, Lei Min, Feng Zhengjie. A Study of a kind hyper chaotic cryptosystem security. *Acta Phys. Sin*,2005,54:1267 ~ 1272(in Chinese))

SPEECH ENCRYPTION BASED ON CHAOTIC SWITCHING SCHEME*

Lin Caixia　Hao Jianhong

(*School of Electric and Electronic Engineering*, *North China Electric Power University*, *Beijing*　102206, *China*)

Abstract　In view of the real-time property of speech, and based on the advantages and disadvantages of chaos masking, chaos modulation in speech encryption, a new kind of scheme for chaos switching encryption was constructed to encrypt speech effectively. The computational approaches realized the encryption of speech, and the results verified the feasibility of the scheme. Meanwhile, the encryption and decryption affections, anti-attacking, synchronization time and cryptosystem security were analyzed and compared.

Key words　Qi chaos system, chaotic additives encryption, chaotic multiplicative encryption, chaotic switching encryption

Received 11 April 2008, revised 15 May 2008.

* The project supported by the Specialized Research Fund for the Doctoral Program of North China Electric Power University (200708)