第 50 卷 第 10 期 2001 年 10 月
1000-3290/2001/50(10)/1856-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.50,No.10,October,2001

利用时空混沌同步进行数字加密通信*

匡锦瑜 邓 昆 黄荣怀

(北京师范大学电子学系,北京 100875)

(2001 年 5 月 31 日收到;2001 年 6 月 14 日收到修改稿)

提出一种利用时空混沌同步的计算机网络数字加密通信方案,并用软件实现了语音双工实时密码通信. 在该方案中,收、发端两个单向耦合映射格点(OCOML)系统被同一混沌信号所驱动而达到同步,其时空混沌输出信号分别用作加密和解密的密钥序列,OCOML 的耦合参数为系统的主密钥. 系统的主要优点是传输效率高,便于用软件实现实时通信,且通信的安全性获得了改善.

关键词:时空混沌同步,密码系统,传输效率

PACC:0545

1 引 言

自从 Pecora[1] 等人提出混沌同步的驱动—响应方案以来,如何将混沌同步理论应用于保密通信就成为非线性动力学和信息科学界关注的一个研究热点.人们相继提出了多种混沌同步通信方案[2—11],这些方案按照混沌信号的用途大致分为两类:一类是将混沌或超混沌信号用作待传消息的载体,把消息掩蔽起来或利用消息对混沌或超混沌信号进行调制,实现扩频通信;另一类是将混沌信号用作密钥或加密函数,对消息进行加密编码,实现密码通信[10,11].

尽管人们提出了很多混沌通信方案,但将这些方案应用于计算机网络通信时,仍有一些问题需要进一步加以研究解决. 例如,在掩蔽通信方案中,驱动信号可以用来重构发送端动力学系统的相空间或估计发送端动力学系统的参数,隐藏在混沌载波中的消息可以被检测出来,即使隐藏在超混沌载波中的消息也不例外[12—16]. 在混沌密码通信方案中,除了传输加密后的消息(即密文)外,还需传输精度足够高的驱动信号,因此传输的数据量增大,传输效率降低,码速率增大,造成低码率信道上实时传输的困难.

为了提高通信的安全性,有些研究者提出利用时空混沌同步系统进行保密通信[6—9],如胡岗等人[7,8]提出了一种利用单向耦合映射格点 OCOML (one-way coupled map Lattice)同步系统的码分多址扩频通信方案,其驱动信号通过另一个秘密信道传送. 本文利用文献[7]中的 OCOML 同步系统设计了一种计算机网络的数据加密通信方案,该方案用同一混沌信号去驱动发送端与接收端的两个 OCOML 系统,使之达到同步.发送端的时空混沌信号不是像文献[7,8]那样用作被消息调制的载波脉冲序列,而是用作对消息进行加密的密钥序列,将消息变换为密文. 接收端的时空混沌信号用作对密文进行解密的密钥序列,将密文还原成消息. 系统的主要优点是传输效率高,便于用软件实现实时通信,且通信的安全性获得了改善. 我们根据这个方案用软件实现了两计算机用户之间的实时语音密码对话.

2 时空混沌同步系统

本文采用的时空混沌系统是一种时间离散、空间离散、状态连续的单向耦合映射格点(OCOML)系统.两个参数完全相同但初始条件不同的 OCOML 系统可由下述方程来描述:

$$x_i(n+1) = (1-\varepsilon_i)f(x_i(n)) + \varepsilon_i f(x_{i-1}(n)), \quad i = 1,2,\cdots,L \tag{1}$$

$$x_0(n) = D(n);$$

$$y_i(n+1) = (1-\varepsilon_i)f(y_i(n)) + \varepsilon_i f(y_{i-1}(n)), \quad i = 1,2,\cdots,L \tag{2}$$

$$y_0(n) = D(n).$$

* 国家自然科学基金(批准号:69773009)资助的课题.

式中 n 代表离散时间，i 代表空间格点位置，L 代表 OCOML 的长度，ε_i 为耦合参数，且满足 $0 < \varepsilon_i < 1$，$D(n)$为驱动信号时间序列，函数 $f(\cdot)$的形式为

$$f(x) = 4x(1 - x). \tag{3}$$

理论和实验证明[7,8]，若 $\varepsilon_i > 0.75$，$i = 1,2,\cdots,L$，被驱系统(1)和(2)在任何相同驱动信号 $D(n)$的驱动下可以达到同步状态，即两系统各空间单元的均方根误差

$$e(n) = \left\{\frac{1}{L}\sum_{i=1}^{L}[y_i(n) - x_i(n)]^2\right\}^{1/2} \tag{4}$$

随离散时间 n 增大而趋于零. 在本文中，系统的同步精度规定为 $e(n) < 10^{-16}$，$\forall n > T_S$. 这里 T_S 是达到同步所需的时间.

当系统(1)和(2)同步时，OCOML 各空间单元输出信号 $\{x_i(n), i = 1,2,\cdots,L\}$的自相关和互相关特性与驱动信号 $D(n)$的自相关特性有关. 当 $D(n)$取自单向耦合映射格点环(OCRML)[8]时，由于$D(n)$各数据点互不相关，序列 $\{x_i(n), i = 1,2,\cdots,L\}$在时间上互不相关，而且每隔一空间单元(即$|j - i\} \geqslant 2$)，序列 $x_i(n)$与 $x_j(n)$也互不相关. 若 $D(n)$为取自蔡(Chua)系统或 Lorenz 系统的取样时间序列，$D(n)$各数据点具有一定的相关性，本文的数值计算发现，只要 $\varepsilon_i \in [0.85,1)$，$i = 1,2,\cdots,L$，除了最前面的 L_0 个空间单元外，上述结论仍然成立，即序列 $\{x_i(n), i > L_0\}$在时间上互不相关，若$|j - i| \geqslant 2$，i，$j > L_0$，序列 $x_i(n)$与 $x_j(n)$也互不相关.

由于时空序列 $\{x_{L_0+2j}(n), j = 1,2,\cdots,J\}$在计算机的精度范围内是混沌的，而不是周期的，它们又互不相关，故可将它们用作加密密钥序列，应用于密码通信.

3　混沌加密通信方案

3.1　加密方案

现在利用 OCOML 系统构成一个如图 1 所示的数字加密通信系统. 它由一个驱动系统、两个产生密钥的 OCOML 系统和计算机网络组成. 系统的工作过程如下 在驱动序列 $D(n)$的驱动下，发送端和接收端的 OCOML 系统达到同步状态，发送端 OCOML(1)输出的时空混沌信号经某种变换后用作加密密钥序列 $k_1(n), k_2(n),\cdots,k_J(n)$，接收端 OCOML(2)相应的输出信号经相同的变换后用作解密密钥序列 $k_1'(n), k_2'(n),\cdots,k_J'(n)$，待传数据(明文) M 经密钥加密变为密文 C，驱动序列 $D(n)$和密文 C 经混合后送入计算机网络而传到接收端，接收端用解密密钥将密文 C 转换为明文 M'. 当两 OCOML 系统同步时，$k_i(n) = k_i'(n)$，$i = 1,2,\cdots,J$. 因此，$M' = M$，消息被无失真地还原.

图 1 中的驱动系统独立于产生密钥的 OCOML 系统，它可以是时间连续的混沌或超混沌系统，也可以是时空离散的超混沌系统，其功能是产生驱动序列 $D(n)$(当采用连续混沌系统时，其输出混沌信号经适当的取样可形成驱动序列).

发送端 OCOML(1)的输出信号 $x_{L_0+2}(n)$，$x_{L_0+4}(n),\cdots,X_{L_0+2J}(n)$是在区间(0,1)取值的实数序列，通过下述变换可将它们转换为加密密钥序列，即

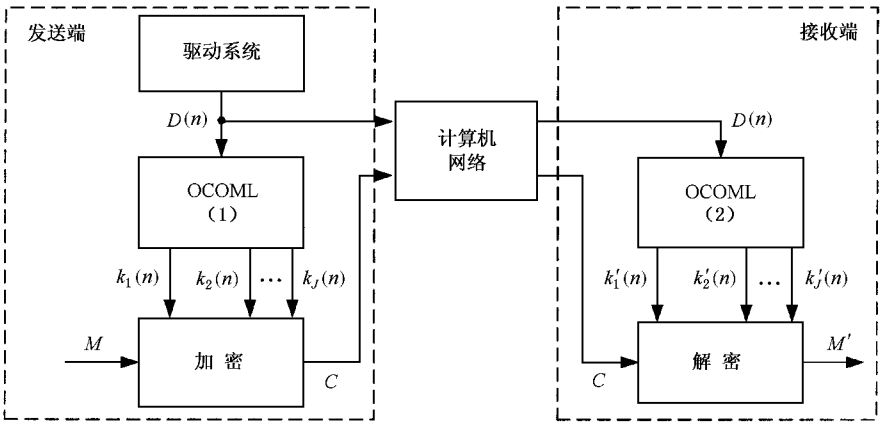

图 1　加密通信方案

$$k_j(n) = \mathrm{INT}[x_{L_0+2j}(n) \times 10^{15}] \bmod 2^b,$$
$$j = 1,2,\cdots,J, \tag{5}$$

式中 INT[·]表示取整，b 是每个密钥的长度，在我们的实验中，$b = 32$，$k_j(n)$是在区间$[0,2^{32}-1]$取值的整数.

同样，接收端 OCOML(2)相应的输出信号 $y_{L_0+2j}(n)$通过相同的变换被转换为解密密钥序列，即

$$k_j'(n) = \mathrm{INT}[y_{L_0+2j}(n) \times 10^{15}] \bmod 2^b,$$
$$j = 1,2,\cdots,J, \tag{6}$$

待传输的消息可以是语音、文字和图像. 先对这类信号进行取样和量化，使消息(明文)变为以字节为单位的数据序列，然后选取一种加密算法，将其变换为密文.

加密和解密算法可采用多种算法，作为一个例子，我们采用如下简单算法.

设明文 $M = \{m_1 m_2 \cdots\}$的每个数据 m 和密文 $C = \{c_1 c_2 \cdots\}$对应的数据 c 均为 q 位($q = 8,16,32$)，加密变换为

$$c = (m + k) \bmod 2^q, \tag{7}$$

解密变换为

$$m' = (c - k') \bmod 2^q, \tag{8}$$

式中 k、k'分别取自密钥集 $\{k_j(n), j = 1,2,\cdots,J\}$和 $\{k_j'(n), j = 1,2,\cdots,J\}$.

本方案的主密钥是 OCOML 的一组耦合参数 $\{\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_L\}$，发送端与接收端事先约定一组参数，通信结束时，该组参数被舍弃.

上述密码模式在密码学中是一种按字节或 q 位的字进行加密的序列密码[17]. 下面我们来讨论系统的安全性和传输效率.

3.2 安全性

在上述序列密码算法中，若密钥的数目不少于明文样本的数目，每个明文样本数据恰有一个不同的密钥将其加密成密文数据，且所有密钥的选取是等概率的，根据文献[18]的定理 11.3.3 和 11.3.4，这种加密算法是安全的. 因此，对密码系统的要求是：1)由密钥序列组成的密钥集应足够大，以满足大量明文数据加密的要求，且保证解密密钥与加密密钥相一致；2)密钥应等概率地随机产生. 在上述方案中，密钥是由时空混沌系统产生的，两 OCOML 系统的同步精度很高(同步误差小于 10^{-16})，可以提供一个大的密钥集，而且该方案依靠同步来保证解密密钥与加密密钥相一致，可以避免大量密钥的传输或存储. 为了检查密钥的概率分布，我们将系统运行时的所有密钥进行统计，获得如图 2 所示的密钥概率密度函数. 由图可知，无论驱动信号取自 Chua 系统还是 OCRML 系统，密钥都等概率地分布在一个大的密钥集上. 只要明文样本数小于密钥集的密钥数，密钥序列不重复使用，这种加密方法是相当安全的.

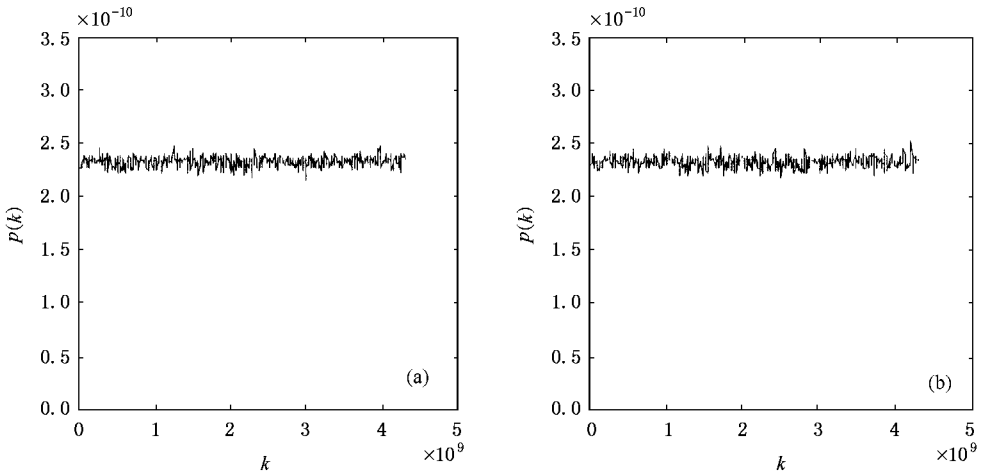

图 2 密钥序列的概率密度函数 (a) Chua 系统驱动，(b) OCRML 系统驱动

在本系统中，系统的同步特性对 OCOML 的耦合参数 $\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_L$ 很敏感，为了说明这个问题，我们在两 OCOML 系统同步时，使两系统的 ε_1 相差 $\Delta\varepsilon_1$，考察系统的同步性能. 图 3 给出了 $\Delta\varepsilon_1 = 2^{-32}$ 时，系统均方根误差 $e(n)$随 n 而上升的曲线. 由图可知，耦合参数的微小差别将迅速破坏两系统的同

步状态. 因此,全部参数值的各种可能组合(主密钥)的数目很大,即主密钥空间很大,攻击者实际上无法准确猜测主密钥,因为检验这些参数的各种可能组合所花的计算时间太长.

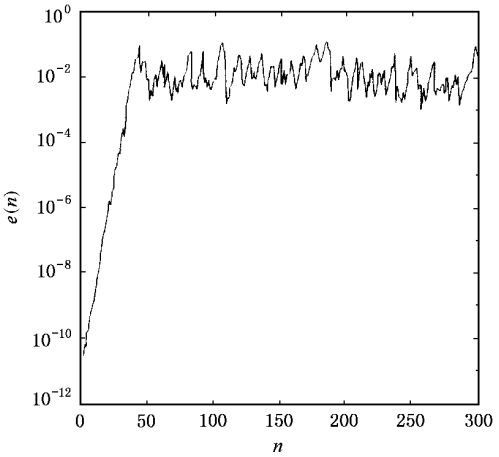

图 3　耦合参数 ε_1 的差别造成 $e(n)$ 随 n 而增大的特性($\varepsilon_i \in [0.85,1)$, $\Delta\varepsilon_1 = 2^{-32}$, $L = 40$,驱动系统为 OCRML)

在掩蔽法混沌同步通信方案中,驱动信号是发送端动力学系统某一变量的时间序列,它携带着该动力学系统的信息,利用非线性预测、参数估计或其他技术[12—16],可以检测隐藏在驱动信号中的消息,消息传输的安全度不高. 在本方案中,驱动系统与 OCOML 系统是完全不同的动力学系统,驱动序列与 OCOML 系统无关,攻击者只能从驱动信号获取驱动系统的动力学性质,估计驱动系统的参数,而无法估计 OCOML 系统的参数. 和掩蔽法相比,本方案有利于安全性的改善.

3.3　传输效率

前面已经提到,在已有的混沌同步通信方案中,传输密文的同时需要传输驱动信号,造成传输效率低下,或传输码率过高. 在我们的加密方案中,每个驱动信号样本可以驱动 OCOML 系统同时产生 J 个密钥,对 J 个明文数据进行加密编码,因此,每传输一个驱动信号样本数据可同时传输 J 个密文数据,和已有的混沌同步通信方案相比,消息样本数和驱动信号样本数之比由 1∶1 提高到 J∶1,对于相同长度的消息来说,驱动信号样本数将减少至原来的$\frac{1}{J}$. 当 J 足够大时,由于传输驱动信号而造成的数据增量变得很小. 传输效率获得极大的提高. 这种高效率的传输方案为语音信号的计算机网络实时密码通信提供了一种新的方法.

4　双工实时语音密码通信

上述方案的优点之一是容易用软件来实现,为此我们利用 Windows 下的编程工具实现了两计算机用户之间的双工实时语音密码通信. 界面采用了面向对象的编程语言 Delphi4 来设计,主界面如图 4 所示. 整个程序是在 Windows 平台下完成的,可以运行在 Win98,WinNT/2000 等操作系统上.

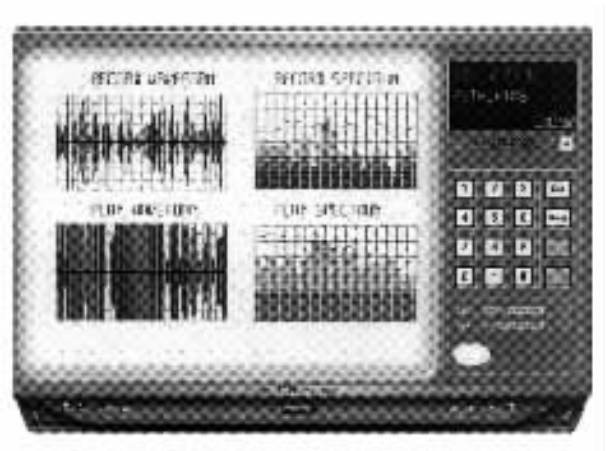

图 4　程序的主界面

通信双方传输的信息包括控制信令和传输数据两部分. 控制信令包括连接建立、连接拆除、通信速率协商等,传输数据包括驱动信号和语音数据. 语音信号以 8 kHz 的取样率进行取样,每个样本量化为 8 bit. 利用 Windows 自带的声解码器(Codec) GSM6.10 将每秒 64 kbit 的语音数据压缩到每秒 16 kbit. 驱动系统是 OCRML,被驱 OCOML 系统的长度为 40. 每个驱动样本量化为 32bit,它可以驱动 OCOML 同时产生 20 个密钥,密钥的长度为 32bit,每个密钥可加密 8—32bit 的语音数据. 驱动数据的长度是密文长度的$\frac{1}{5}$—$\frac{1}{20}$. 数据传输的码速率为 19.2—16.8 kbit/s.

为了实现双工通信,程序中使用了两个主密钥,一个用于用户甲的加密系统和用户乙的解密系统,另一个用于用户乙的加密系统和用户甲的解密系统,两用户协商主密钥后,可进行流畅的语音密码对话.

5 结 论

本文提出了一种利用时空混沌同步的数据加密通信方案,并用软件实现了计算机之间的双工实时密码通信. 由同步的 OCOML 系统产生的密钥互不相关,并且在一个大的密钥集中均匀分布. 驱动信号独立于 OCOML,不能被用来估计 OCOML 的参数,用计算机猜测这些参数的处理复杂度高,通信的安全性获得了改善. 系统每传输一个驱动信号样本,可同时传输多个消息密文,传输效率获得极大的提高. 这种高效率的加密通信方案为实现消息的计算机网络实时密码传输提供了一种新的方法.

感谢胡岗教授对本文提出了宝贵的建议.

[1] L. M. Pecora, T. L. Carroll, *Phys. Rev. Lett.*, **64**(1990), 821.
[2] K. M. Cuomo, A. V. Oppenheim, *Phys. Rev. Lett.*, **71**(1993), 65.
[3] H. Dedicu, M. P. Kennedy, Hasler, *IEEE Trans. CAS-*Ⅱ, **40**(1993), 634.
[4] L. Kocarev, U. Parlity, *Phys. Rev. Lett.*, **74**(1995), 5028.
[5] X. Luo *et al.*, *Acta Physica Sinica*, **48**(1999), 2022(in Chinese) [罗晓曙等, 物理学报, **48**(1999), 2022].
[6] Y. Zhang, M. Dai, Y. Hua, W. Ni, G. Du, *Phys. Rev.*, **E58**(1998), 3022.
[7] G. Hu, J. Xiao, J. Yang, F. Xie, Z. Qu, *Phys. Rev.*, **E56**(1997), 2738.
[8] J. H. Xiao, G. Hu, Z. Qu, *Phys. Rev. Lett.*, **77**(1996), 4162.
[9] J. K. White, J. V. Muloney, *Phys. Rev.*, **A59**(1999), 2422.
[10] R. He, P. G. Vaidya, *Phys. Rev.*, **E57**(1998), 1532.
[11] M. Götz, K. Kelber, W. Schwarz, *IEEE Trans. CAS-I*, **44**(1997), 963.
[12] K. M. Short, *Int. J. Bifurcation Chaos Appl. Sci. Eng.*, **4**(1994), 959.
[13] K. M. Short, A. T. Parker, *Phys. Rev.*, **E58**(1998), 1159.
[14] U. Parlity, *Phys. Rev. Lett.*, **76**(1996), 1232.
[15] N. Sharma, P. G. Poonacha, *Phys. Rev.*, **E56**(1997), 1242.
[16] C. Zhou, C. H. Lai, *Phys. Rev.*, **E60**(1999), 320.
[17] Bruce Schneie, Applied Cryptography, Second Edition (John Wiley & Sons, Inc., 1996), § 9.4.
[18] Y. Yang, X. Lin, Crptography (People 's Posts and Telecommunications Publishing House, Beijing, 1992), § 11.3. [杨义先、林须端,编码密码学 (人民邮电出版社,北京,1992), § 11.3].

AN ENCRYPTION APPROACH TO DIGITAL COMMUNICATION BY USING SPATIOTEMPORAL CHAOS SYNCHRONIZATION*

KUANG JING-YU DENG KUN HUANG RONG-HAI
(*Department of Electronics, Beijing Normal University, Beijing* 100875, *China*)
(Received 31 May 2001; revised manuscript received 14 June 2001)

ABSTRACT

An encryption approach to digital communication by using spatiotemporal chaos synchronization is proposed. Two one-way coupled map lattice (OCOML) systems driven by a chaotic signal are synchronized. The chaotic outputs of the OCOML systems serve as the encryption and decryption keys and the main secret key is a set of coupling parameters of the OCOML. The advantages of the cryptosystem are its high communication efficiency, higher level of security and easy implementation by software. An example of duplex real-time voice communication between two computer users is described.

Keywords: spatiotemporal chaos synchronization, cryptosystem, communication efficiency.
PACC: 0545

* Project supported by the National Natural Science Foundation of China (Grant No. 69773009).