第 57 卷 第 3 期 2008 年 3 月
1000-3290/2008/57(03)/1398-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.3,March,2008

一种利用 CPRNG 实现的混沌同步加密通信方案*

李 伟 郝建红 祁 兵

(华北电力大学电气与电子工程学院,北京 102206)

(2007 年 4 月 20 日收到;2007 年 6 月 21 日收到修改稿)

提出了一种利用新型的基于混沌的伪随机数发生器(CPRNG)系统实现的数据加密通信方案. 在该方案中,发、收两端的 CPRNG 系统将驱动系统产生的混沌序列转换为加密密钥序列,利用这些密钥序列对明文数据按字节切换交替加密. 系统的主要优点是在通信的安全性和同步性上有所改善,且便于用软件实现.

关键词:密钥,基于混沌的伪随机数发生器,混沌同步

PACC:0545

1. 引 言

混沌同步理论应用于保密通信是近些年来引起非线性动力学和信息科学界广泛关注的一个研究领域,人们相继提出了多种混沌同步通信方案[1—5],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[4—6].

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,这样隐藏在混沌载波中的消息就可能被检测出来,即使隐藏在超混沌载波中的消息也不例外[6—9]. 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.

由于混沌运动是一类极其特殊的运动形式,它遵循确定性动力机理,但表现内在的随机性,因而非常适合用于产生伪随机数. 为了利用混沌信号更好地掩藏信息数据,增强抗攻击能力,近年来,应用混沌的良好特性已发展和构造诸多伪随机数发生器,即基于混沌的伪随机数发生器(CPRNG)[10—16].

本文引入了新型的 CPRNG 系统代替文献[6]中的时空混沌同步系统,设计了一种新的用于计算机网络的数据加密通信方案,该方案保留了 CPRNG 系统理论上的安全性且不需要驱动信号在网络中传输,从而避免了攻击者利用截获的驱动信号重构发送端动力学系统之后检测出被隐藏在其中的消息的可能性,同时提高了系统的传输效率. 另外,本方案易于用软件实现,且由于使用了 CPRNG 系统,使通信的安全性获得了一定的改善. 我们根据这个方案用软件实现了两计算机用户之间的图文数据密码通信.

2. 新型混沌伪随机数发生器

为了实现混沌同步,本文采用了一种新型的 CPRNG. 下面是 CPRNG 生成的具体算法:

1) 求解混沌动力学系统,产生混沌系统对应的原始密钥,它是 L 组随机序列 $\{x_n(k)\}$($n=1,2,\cdots,L$),其中 L 表示驱动系统的维数,k 表示循环次数,即密钥长度.

2) 为了增强本方案的抗攻击能力,我们对原始密钥进行了复合处理,得到粗粒化输出

$$X_n(k) = C(x_n(k)), \tag{1}$$

其中 C 可以是复合运算或非线性调制运算,$X_n(k)$ 是在区间[0,9]取值的整数. (1)式满足混沌构造随机数发生器的充分条件和附加条件[15,16].

* 华北电力大学博士基金(批准号:200708)资助的课题.

3) 将经过复合处理的原始密钥映射为伪随机序列，即密钥序列 $\{Y_n(k)\}$：

$$Y_n(k) = Y_m, \text{ 当 } X_n(k) = m \text{ 时}, \quad (2)$$

这里 $Y_m(m = 0,1,\cdots,9)$ 是在区间[0,255]取值的整数，Y_m 的具体选取规则见表 1 所列的置换协议. 这种整数化处理一方面满足了图文数据处理的要求，另一方面使得驱动系统和响应系统易于同步，大大改善了加密系统的同步性能.

3. 混沌加密通信方案

3.1. 加密方案

现在利用上述 CPRNG 系统构成一个如图 1 所示的混沌加/解密通信方案. 它由发送端的驱动系统和接收端的响应系统(可据需要灵活选择各种混沌系统)、两个产生密钥的 CPRNG 系统和计算机网络组成.

系统的工作过程如下 在发送端，利用混沌系统产生出多组混沌序列，这些混沌序列经过本方案设计的 CPRNG 系统的处理后对应产生多组伪随机序列作为密钥序列，用这些密钥序列对明文数据按字节交替加密. 密文数据通过计算机网络传输到接收端. 在接收端，利用对应的同步混沌系统和对应的 CPRNG 系统准确地重构密钥，对密文数据解密，从而明文数据被无失真地还原.

图 1 中的驱动系统可以选取多种混沌系统或超混沌系统，其功能是产生对应于不同系统的取样时间序列作为驱动 CPRNG 系统的驱动序列.

发送端与接收端的 CPRNG 系统的功能相同，将驱动序列通过处理转换为加密密钥序列，表 1 是实现 CPRNG 系统功能的置换协议表.

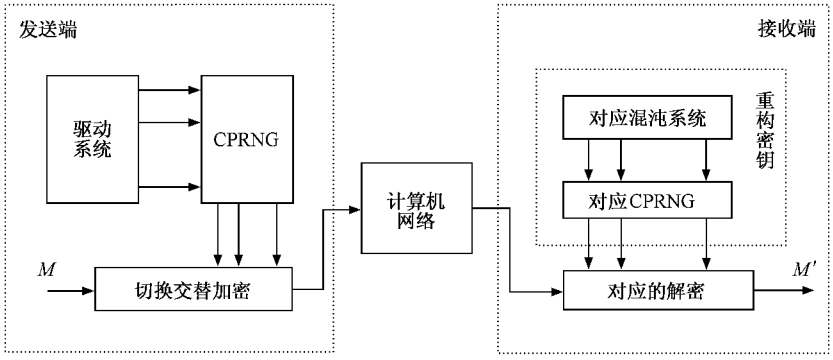

图 1　混沌加/解密通信方案

表 1　置换协议表(Lorenz 系统驱动)

变量		对应取值									
$x_n(n=1,2,3)$		0	1	2	3	4	5	6	7	8	9
x_1	$x_1\geqslant 0$	120	168	72	216	24	144	96	192	48	240
	$x_1<0$	219	27	171	75	123	3	195	51	147	99
x_2	$x_2\geqslant 0$	119	172	68	224	16	146	94	198	42	250
	$x_2<0$	232	32	182	82	132	7	207	56	157	107
x_3	$x_3\geqslant 0$	112	162	62	212	12	137	87	187	37	237
	$x_3<0$	239	31	186	83	135	5	213	57	161	109

表 1 中 $x_n(n = 1,2,3)$ 表示驱动系统在某一离散时间点上的取值，当 $x_n \geqslant 0$ 或 $x_n < 0$ 时，分别对应着两组不同的整数，每组有 10 个整数，取值在[0,255]之间，6 组中的 60 个数没有重复，且要尽量保证每一组中任意相邻两整数之间的码距最大，这样做的目的是为了使生成的密钥序列具有良好的随机性. 为了保证解密密钥与加密密钥具有更好地一致性，我们对 $x_n(n = 1,2,\cdots,L)$ 进行如下的变换：

$$X_n = \text{int}[(\text{abs}(x_n) - \text{int}(\text{abs}(x_n))) \times 10], \quad n = 1,2,\cdots,L, \quad (3)$$

式中 int(·)表示取整，abs(·)表示取绝对值，在我们的方案中，选取 Lorenz 系统作为驱动系统，$L = 3$，变量 X_n 是在区间[0,9]取值的整数. 因为每次变换得到的变量 $X_n(n = 1,2,\cdots,L)$ 的值都是唯一确定的，

那么由表 1 中行与列的交叉位置上的三个数可以确定密钥序列 $Y_n(n=1,2,\cdots,L)$.

例如,假设根据 $x_n(n=1,2,3)$的正负选定的三组整数在表 1 中用深灰色标识,再假设对应 $x_n(n=1,2,3)$的变量 $X_n(n=1,2,3)$的取值分别为 2,5,7,其所在的列元素在表 1 中也用深灰色标识,则行与列的交叉位置上的三个数就构成了密钥 $Y_n(n=1,2,3)$,在图中用浅灰色标识,接下来就可以对明文数据进行加密了.

待传输的消息可以是语音、文字和图像,其中语音信号要先进行抽样和量化,使其转化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. 可采用的加/解密算法很多,我们采用对称加密方法:

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 均按字节选取. 由于异或运算具有如下规律:

$$m \text{ Xor } y \text{ Xor } y = m \tag{4}$$

即如果 m 是明文,y 是密钥,则 m Xor y 是密文. 上式表明,将密文再与加密时所用的密钥异或又可得到原明文. 因此,我们可以用同一密钥实现对加密文件的解密. 于是,可以进行如下的切换交替加/解密变换:

$$c = m \text{ Xor } Y_j, \text{ 当} \left(\sum_{n=1}^{s} X_n\right) \bmod s = j-1 \text{ 时,} \tag{5}$$

式中 $Y_j(j=1,2,\cdots,s)$取自密钥集 $Y_n(n=1,2,\cdots,L)$,$s\leqslant L$.

本方案的主密钥是驱动系统的系统参数和初始参数,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.

3.2. 安全性

上述密码模式在密码学中是一种按字节进行加密的序列密码[17]. 下面我们来讨论系统的安全性.

根据文献[18]的定理 11.3.3 和 11.3.4 可知,安全的密码系统必须满足以下要求:1)由密钥序列组成的密钥集应该足够大,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,密钥序列是由混沌动力学系统产生的,其长度可以通过选取不同的初始参数来控制,从而可以根据需要产生不同长度的密钥序列,即密钥集足够大能够满足对不同长度的明文数据加密的要求,而且该方案采用上述 CPRNG 系统来保证解密密钥与加密密钥相一致,避免了大量密钥的传输或存储.

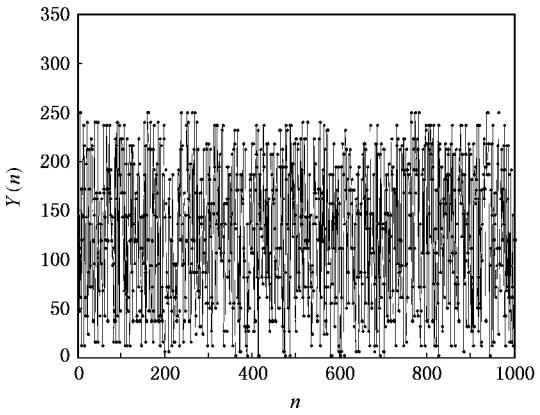

图 2 伪随机序列取值分布(Lorenz 系统驱动)

利用上述方案,我们选取 Lorenz 系统作为驱动系统,对密钥中某连续的 1000 个字节所对应的取值分布进行了分析,如图 2 所示. 图中横坐标表示的是连续字节,纵坐标表示的是密钥在对应字节中的取值,取值的范围是 0—255 之间的整数. 从图中可以明显看出,任意两个相邻的密钥取值的跳跃间隔疏密不同,在整个坐标轴上密钥的取值没有周期,具有很强的随机性.

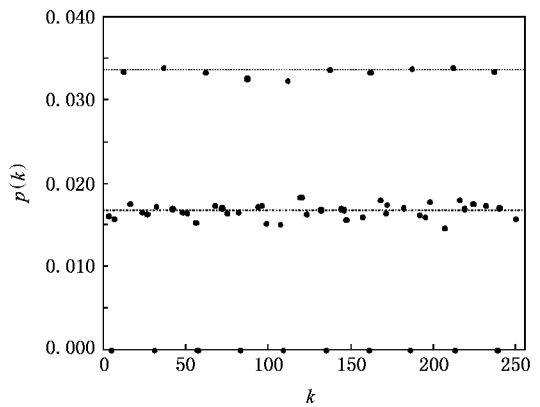

图 3 密钥序列的概率密度函数(Lorenz 系统驱动)

为了检查密钥的概率分布,我们对系统运行时的所有密钥进行统计,获得如图 3 所示的密钥概率密度函数. 该图是对密钥序列按字节连续抽样 60000 次得到的,其横坐标表示密钥中所有可能的取值,纵坐标表示每种取值出现的概率. 设每种可能的取值在 60000 次连续抽样过程中出现的概率为

$P_i(i=1,2,\cdots,60)$，则 $\sum_{i=1}^{60} P_i = 1$. 从图中可以看出，大部分取值(40 个)在 60000 次连续抽样过程中出现的次数在 1000 次左右，概率约等于 1/60，只有 20 个点游离在外，分别对应两组(每组对应 10 个点)可能的取值，其中一组出现的概率约为 1/30，而另一组出现的概率为 0. 一组取值出现的概率为零说明该组值在密钥序列中没有出现，即原始的混沌序列中的某一组值恒为正值($x_n \geqslant 0, n=1,2,3$)或者恒为负值($x_n < 0, n=1,2,3$)，当出现这种情况时，出现的取值的概率就自然会增加两倍，约等于 1/30，而没有出现的取值的概率就是 0，这就解释了图中出现游离点的原因. 照此推之，若上述情况不出现的话，所有可能取值的出现次数都应分布在 1000 次左右，即概率都约等于 1/60，从而证明了密钥的所有可能取值是近似等概率随机出现的，也就是说产生密钥的 CPRNG 系统可以近似认为是一个理想信息源.

另外，在众多的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，可以检测出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 CPRNG 系统是完全不同的系统，驱动序列与 CPRNG 系统只有间接的映射关系，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 CPRNG 系统的参数. 因此，与掩蔽法相比，本方案有利于安全性的改善.

3.3. 同步性

在本系统中，系统的同步特性对驱动系统(Lorenz 系统)的系统参数(本方案中取 $a=10$，$b=8/3$，$c=30$) 很敏感，为了说明这个问题，我们使收发两端的驱动系统的参数 c 相差 Δc，考察系统的同步性能.

在收发两端驱动系统达到同步状态时，系统的均方根误差

$$e(n) = \left\{ \frac{1}{L} \sum_{i=1}^{L} [x_i'(n) - x_i(n)]^2 \right\}^{1/2} \qquad (6)$$

随离散时间 n 增大而趋于零. 式中 n 表示离散时间，L 表示驱动系统的维数，$x_i(n)$ 和 $x_i'(n)$ 表示发收两端在某一离散时间上对应的原始密钥值. 在本方案中，系统的同步精度规定为 $e(n) < 10^{-16}$，$\forall n > T_S$，其中，T_S 是收发两端达到同步所需的时间.

图 4 给出了 $\Delta c = 10^{-13}$ 时的系统均方根误差 $e(n)$ 随 n 而上升的曲线. 由图可知，系统参数的微小差别将迅速破坏收发两端的同步状态，同时这种系统同步性对初始参数的敏感依赖性也大大增强了加密系统的安全性.

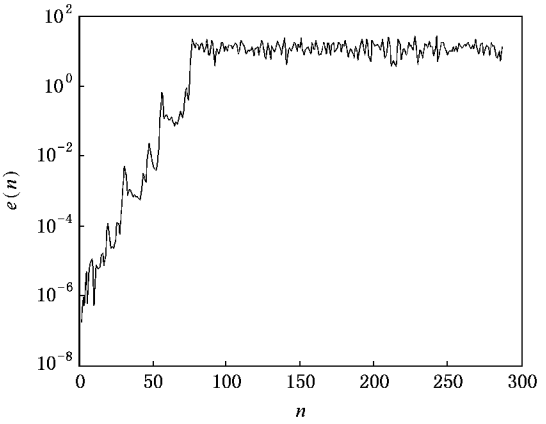

图 4　系统参数 c 的微小差别造成 $e(n)$ 随 n 增大的特性(Lorenz 系统驱动)

实际上，全部参数值的各种可能组合(主密钥)的数目很多，即主密钥空间很大，攻击者几乎无法准确猜测主密钥，因为枚举这些参数的各种可能组合所花的计算时间太长，即使耗费了巨大的人力、物力近似地猜测出了主密钥，攻击者仍需要估计 CPRNG 系统的参数，这样在很大程度上增强了数据的保密性能.

4. 图像密码通信

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 操作系统下的编程工具实现了两计算机用户之间的静态图像密码通信. 为了增强人机交互性，软件的界面采用了面向对象的编程语言 VB6.0 来设计，整个程序是在 Windows 平台下完成的，可以运行在 WinNT/2000/XP 等操作系统上.

通信双方各自持有加/解密软件，互相协商好主密钥后，可以进行图文密码通信. 本例中通信双方传输的数据信息是一幅 lenna 图像(256 像素 × 256 像素 × 8 位深度)，其加/解密通信前后的效果如图 5 所示. 其中，图 5(a)是原始图像，图 5(b)是发送端用户采用上述方案加密后的图像，图 5(c)是接收端用户利用本软件解密后的图像.

另外，图 5(d)是当接收端参数 c 取 $c' = c + 10^{-13}$ 时所得到的解密图像. 由此可见，上述方案对参数是非常敏感的，参数略有差异，密文不能解密；

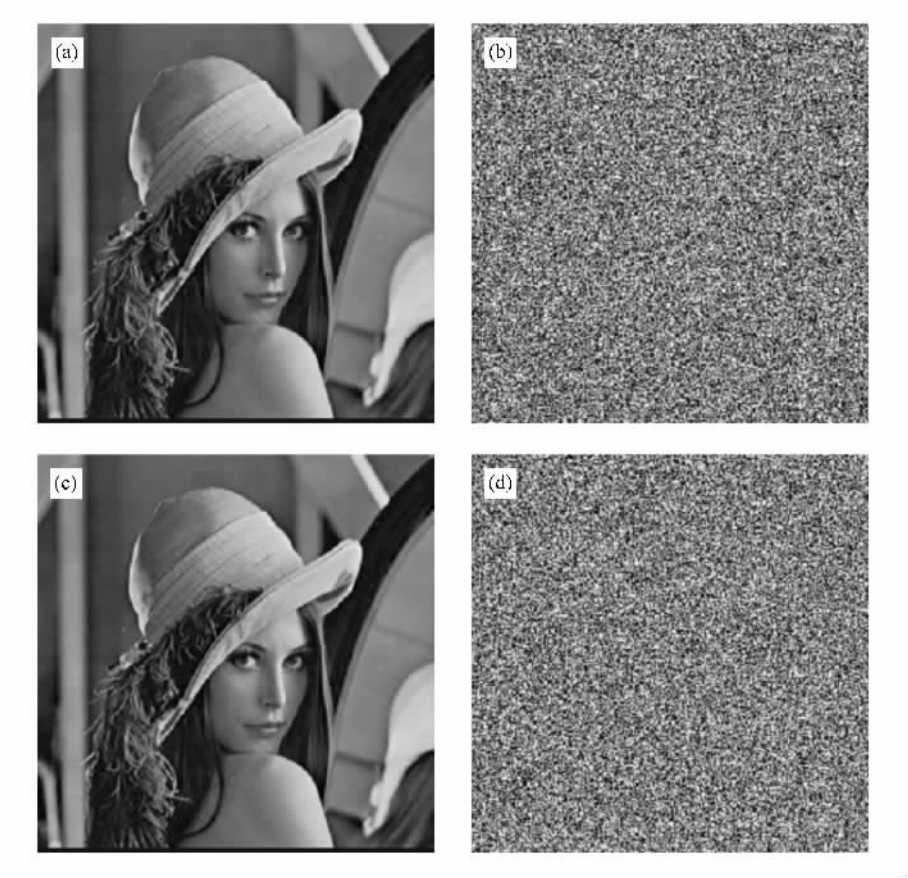

图 5 静态图像密码通信效果(Lorenz 系统驱动) (a)原始图像;(b)加密后的图像;(c)参数相同时的解密图像;(d)参数 c 相差 10^{-13} 时的解密图像

只有参数完全相同时,才能精确解密. 这进一步验证了本方案具有良好的抗破译性,同时它也是本方案安全性高的一个重要原因.

5. 结 论

本文提出了一种利用新型混沌伪随机数发生器(CPRNG)实现的数据加/解密通信方案,并用软件实现了计算机之间的密码通信. 由本方案设计的 CPRNG 系统可以使解密密钥准确地与加密密钥相一致,其产生的密钥序列具有良好的随机性,并且在整个密钥集中等概率分布,从而有效地改善了传统数据加密方法中存在的同步性差且无法简单解决的缺陷. 另外,本方案中的驱动系统独立于 CPRNG 系统,攻击者无法估计出 CPRNG 系统的参数,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. 这种改进的加密通信方案在安全性能要求比较高的数据加密领域具有潜在的应用前景.

[1] Kocarev L, Parlitz U 1995 *Phys. Rev. Lett.* **74** 5028
[2] Zhang Y, Dai M, Hua Y, Ni W, Du G 1998 *Phys. Rev.* E **58** 3022
[3] White J K, Muloney J V 1999 *Phys. Rev.* A **59** 2422
[4] He R, Vaidya P G 1998 *Phys. Rev.* E **57** 1532
[5] Götz M, Kelber K, Schwarz W 1997 *IEEE Trans. CAS-*Ⅰ **44** 963
[6] Kuang J Y, Deng K, Huang R H 2001 *Acta Phys. Sin.* **50** 1856 (in Chinese) [匡锦瑜、邓 [illegible] 黄荣怀 2001 物理学报 **50** 1856]
[7] Sharma N, Poonacha P G 1997 *Phys. Rev.* E **56** 1242
[8] Zhou C, Lai C H 1999 *Phys. Rev.* E **60** 320
[9] Short K M, Parker A T 1998 *Phys. Rev.* E **58** 1159
[10] Sang T, Wang R, Yan Y 2001 *IEEE Trans. Commun.* **49** 620
[11] Stojanovski T, Kocarev L 2001 *IEEE Trans. Circ. Syst.* Ⅰ **48** 281
[12] Xiao F H, Yan G R, Han Y H 2004 *Acta Phys. Sin.* **53** 2877 (in Chinese) [肖方红、阎桂荣、韩宇航 2004 物理学报 **53** 2877]
[13] Sheng L Y, Cao L L, Sun K H *et al* 2005 *Acta Phys. Sin.* **54** 4031 (in Chinese) [盛利元、曹莉凌、孙克辉等 2005 物理学报 **54**

4031]

[14] Zhang H, Wang X F, Li C H *et al* 2005 *Acta Phys. Sin.* **54** 4006 (in Chinese) [张　翰、王秀峰、李朝晖等 2005 物理学报 **54** 4006]

[15] Wang L, Wang F P, Wang Z J 2006 *Acta Phys. Sin.* **55** 3964 (in Chinese) [王　蕾、汪芙平、王赞基 2006 物理学报 **55** 3964]

[16] Kohda T 2002 *Proc. IEEE* **90** 641

[17] Schneie B 1996 *Applied Cryptography Second Edition* (John Wiley & Sons, Inc.) § 9.4

[18] Yang Y X, Lin X D 1992 *Cryptography* (Beijing: People 's Posts and Telecommunications Publishing House) § 11.3 (in Chinese) [杨义先、林须端 1992 编码密码学(北京:人民邮电出版社) § 11.3]

An encryption approach to chaos synchronization communications by using CPRNG *

Li Wei　Hao Jian-Hong　Qi Bing

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

(Received 20 April 2007; revised manuscript received 21 June 2007)

Abstract

A data encryption approach to chaos synchronization communications by using a novel chaos-based pseudo-random number generator (CPRNG) is proposed. Chaotic sequence generated by the drive system is turned into encryption keys in CPRNG and the data can be alternately encrypted according to byte by using the keys. The advantages of the cryptosystem are its higher level of security and synchronization, and it is easily implemented by software.

Keywords: encryption keys, chaos-based pseudo-random number generator, chaos synchronization

PACC: 0545

* Project supported by the Foundation for Doctor of North China Electric Power University (Grant No. 200708).