一种新颖的混沌分组密码算法

张向华
(重庆教育学院 重庆 400067)

摘 要 在研究已经提出的一些混沌加密算法的基础上,提出了一种新的混沌分组密码算法。算法的密钥包含64位的外部比特流 K 和 Logistic 映射的初值 x_0 两部分,同时也用这个混沌映射定义了一个双射映射。然后通过3种代数运算和由双射映射确定的置换运算还用在64比特的明文上,产生64比特的密文。理论与实验分析表明该算法克服了一些纯混沌密码系统的固有缺陷,同时也具有较高的性能。

关键词 分组密码,混沌映射,代数运算,安全
中图法分类号 TP391 **文献标识码** A

Novel Chaos Block Cipher Algorithm

ZHANG Xiang-hua
(Chongqing Education College, Chongqing 400067, China)

Abstract Based on the study of some existing chaotic encryption algorithms, a new block cipher was proposed. In the proposed cipher, the key is comprised of an external 64-bits K and the initial value x_0 of the logistic map. At the same time, a bijection map was also defined by the logistic map. Then three algebraic operations in the group and permutations were applied on plaintext with block length of multiples of 64 bits to produce ciphertext blocks of the same length. Analysis shows that the proposed block cipher does not suffer from the flaws of pure chaotic cryptosystems.

Keywords Block cipher, Logistic map, Algebraic operation, Security

1 引言

混沌信号既具有类似噪声性能又具有确定的轨道行为。这使得混沌系统在信息隐藏领域和密码系统的密钥流设计中有着广泛的应用。目前,大量的有关混沌加密的算法已经被提出来[1-12]。

实际上,大多数的基于混沌的软件加密技术都是使用混沌映射来产生伪随机序列。然而,Wheeler 等人在文献[9,10]中指出当混沌系统用有限精度的计算机来实现的时候,数字化的混沌系统表现出了许多明显不同的行为。它们的数字动力学行为也远不如连续混沌系统的动力学行为。例如,非常短的周期;依赖于特定的数字精度等。假设采用定点运算,并且有限精度为 L 位(设为二进制),则混沌系统的性能将由于以下两个原因而降低:(1)整个系统中,只有 2^L 有限个离散值来表示混沌轨道。因此,混沌序列的周期将小余等于 2^L。(2)计算机量化误差使得混沌轨道的性能也远不如理论值[11]。

Xun Yi 等人提出了另一种混沌密码系统[3]。在这个密码系统中,由混沌 Tent 映射产生的实值序列通过一个域值函数来确定 $4n$ 比特的噪声向量。同时,也确定了一个4比特位和1~4的排列之间的一个查询表。然后,噪声向量和排列置换操作交替应用到 $4n$ 比特明文上以产生 $4n$ 比特的密文($n\geq 16$)。显然,该密码系统存在如下两个缺陷:(1)查询表太小,只有16项(因为,4比特位至多有16种取值)。(2)v_{ji} 和排列 w_{ji} 之间的关系是固定不变的,与密钥无关。在选择明文攻击下,这两个缺陷有可能成为密码系统的安全漏洞。

在本文中,一种新的基于混沌映射和代数运算的更具安全性的混沌分组密码被提出来了。在这个密码系统中,通过抽取 Logistic 映射拟混沌轨道的相应数字位得到一个伪随机序列。同时,也定义了一个双射函数 $g: r\rightarrow w_{ji}$ 来描述 r 和排列 w_{ji}(1~8)之间的关系。

本文第2节描述了本算法将要用到的一些理论知识;第3节详细描述了本文提出的混沌分组密码算法;第4节是基于该算法的仿真实验;第5节是对该算法的安全性及其性能分析,最后对论文做了总结。

2 预备知识

2.1 混沌伪随机序列的产生

随机数发生器在每一个科学领域都很重要,譬如在密码学领域中密钥流的生成等。文献[7]提出了3种从混沌映射中产生独立同分布的二进制随机序列的方法。根据 Kohda 和 Tsuneda 在文献[7]中所述,Logistic 映射

$$\tau^{n+1}(x)=\mu\tau^n(x)(1-\tau^n(x)),x\in I=[0,1] \quad (1)$$

具有很多与密码学相关的优良特性。这些属性在产生独立同分布的随机数序列方面具有重要意义。本文将采用该文的方法来获得伪随机变量序列。将一个实数 x 表示成如下的二

到稿日期:2008-12-20 本文受重庆市教委资助项目(KJ071504)资助。
张向华(1969-),男,副教授,硕士,主要研究方向为混沌理论及其信息安全。

进制形式：

$$x=0.b_1(x)b_2(x)\cdots b_i(x)\cdots,x\in[0,1],b_i(x)\in\{0,1\} \tag{2}$$

在这个表示形式中，第 i 比特可以表示成：

$$b_i(x)=\sum_{r=1}^{2^i-1}(-1)^{r-1}\Theta_{(r/2^i)}(x) \tag{3}$$

此处，$\Theta_t(x)$ 是一个域值函数，其定义如下：

$$\Theta_t(x)=\begin{cases}0, & x<t\\ 1, & x\geqslant t\end{cases} \tag{4}$$

这样，我们就得到了一个独立同分布的二进制随机序列，$B_i^n=\{b_i(\tau^n(x))\}_{n=0}^{\infty}$。

2.2 双射映射 g 的构造

首先，构造一个如表 1(Table 1)所列的双射映射 $g:r\to w_r$。其中，w_r 是 1,2,3,4,5,6,7,8 的一个排列。

表 1　r 与 1,2,3,4,5,6,7,8 排列的 w_r 之间的关系

r		w_r
Decimal	Binary	
0	00000000	w_0
1	00000001	w_1
…	……	w_i
254	11111110	w_{254}
255	11111111	w_{255}

映射 $g:r\to w_r$ 的映射构造算法[1,2]如下：

Ⅰ. 混沌状态 $\tau^i(x)$。由混沌映射(1)产生一个新的混沌状态 $\tau^{i+1}(x)$。

Ⅱ. 抽取 $\tau^{i+1}(x)$ 的前 8 个不同的数字位，进行模 8 加 1 操作，得到 1～8 的一个排列。如果操做失败(即，状态 $\tau^{i+1}(x)$ 中的数字位通过模 8 加 1 操作不能得到 1～8 的一个排列)或者得到的排列前面已经出现过，则转Ⅰ继续；直到得到 256 个不同的 1～8 的排列为止。

2.3 三种基本的代数运算

2.3.1 群 $Z_{2^{16}+1}^*$ 上的⊙运算

在群 $Z_{2^{16}+1}^*=\{a\mid a\in1,2,\cdots,2^{16}\}$ 中，⊙表示两个元素的模乘操作，即两个元素的乘积再模上 $2^{16}+1$。设 $a,b\in Z_{2^{16}+1}^*$，则 $a\odot b=(a\cdot b)_{2^{16}+1}=c\in Z_{2^{16}+1}^*$。同时，群 $(Z_{2^{16}+1}^*,\odot)$ 是一个可交换群，所以群中的元素的逆元存在且唯一，即 $b=c\odot a^{-1}$。例如，设 $a=457,b=239$，那么 $c=a\odot b=(457\cdot239)_{2^{16}+1}=(109223)_{2^{16}+1}=43686\in Z_{2^{16}+1}^*$，$a^{-1}=53204$，$b=c\odot a^{-1}=(43686\cdot53204)_{2^{16}+1}=239$。

由于 $0\notin Z_{2^{16}+1}^*$ 而 $2^{16}=65536\in Z_{2^{16}+1}^*$，因此用 2^{16} 代替 0。所以，如果一个操作数是 0 时，用 2^{16} 代替，同样，如果结果等于 2^{16}，则用 0 代替。另外，在计算群 $(Z_{2^{16}+1}^*,\odot)$ 的逆元时，采用了扩展的 Euclidean 算法。

2.3.2 群 $Z_{2^{64}}$ 上的⊞运算和 F_2^{64} 上的⊕运算

另外的两种代数运算是在群 $F_2^{64}=\{a\mid a\in0,1,2,\cdots,2^{64}\}$ 中，⊕表示两个元素的按位异或操作。在群 $Z_{2^{64}}=\{a\mid a\in0,1,2,\cdots,2^{64}\}$ 中，⊞表示两个元素的模加操作。即两个元素相加再模上 2^{64}。设 $a,b\in Z_{2^{64}}$，则 $a\boxplus b=(a+b)\bmod 2^{64}=c\in Z_{2^{64}}$。

3 新的分组密码系统

3.1 混淆与扩散过程

首先，用第 2.1 节描述的方法得到一个具有独立同分布性质的伪随机序列 B，并将其分为 64 比特一组，得到 $B_j(j=0,1,2,\cdots)$。对于 $j=0,1,\cdots$，设 $V_j=(v_{j0},v_{j1},\cdots,v_{j7})=(B_{j+2}\oplus K)$，这里，⊕表示按位异或；$v_{ji}(i=0,1,\cdots,7)$ 是一个 8 位的二进制位串，则 v_{ji} 的十进制值位于 0 到 255 之间；K 是一个外部密钥。

然后，构造一个置换/代换映射 $f_{ji}(\cdot)$：

设有一个 64 位的二进制位串 $M=(M_1,M_2,M_3,M_4,M_5,M_6,M_7,M_8)$，$f_{ji}(\cdot)$ 的定义如下：

$$f_{ji}(M_1,M_2,\cdots,M_k,\cdots,M_8)=[w_{ji}(r_{ji}(M_1),r_{ji}(M_2),\cdots,r_{ji}(M_k),\cdots,r_{ji}(M_8))] \tag{5}$$

其中 $M_k(k=1,2,\cdots,8)$ 是一个 8 位的二进制位串。$r_{ji}(\cdot)$ 表示 M_k 与 v_{ji} 在代数群 $(Z_{2^8+1}^*,\odot)$ 中的模 2^8+1 乘运算，即

$$r_{ji}(M_k)=M_k\odot v_{ji}=M_k\cdot v_{ji}\bmod(2^8+1) \tag{6}$$

$w_{ji}(\cdot)$ 表示把 $(r_{ji}(M_1),r_{ji}(M_2),\cdots,r_{ji}(M_k),\cdots,r_{ji}(M_8))$ 按照第 2.2 节的映射 g 中 w_{ji} 所对应的排列进行重新排序。例如：$v_{ji}=(01100001)_2$，$w_{ji}=(4,6,1,3,5,8,7,2)$，$M_3=(01100010)_2$，由于 $v_{ji}\odot M_3=(11111110)_2=254$，则

$$\begin{aligned}&f_{ji}(M_1,M_2,M_3,M_4,M_5,M_6,M_7,M_8)\\&=[w_{ji}(r_{ji}(M_1),r_{ji}(M_2),r_{ji}(M_3),r_{ji}(M_4),r_{ji}(M_5),r_{ji}(M_6),r_{ji}(M_7),r_{ji}(M_8))]\\&=w_{ji}[M_1',M_2',(11111110),M_4',M_5',M_6',M_7',M_8']\\&=(M_4',M_6',M_1',(11111110),M_5',M_8',M_7',M_2')\\&=(M_4',M_6',M_1',M_3',M_5',M_8',M_7',M_2')\end{aligned}$$

此处，$M_k'=r_{ji}(M_k)=M_k\odot v_{ji}=M_k\cdot v_{ji}\bmod(2^8+1)$。当 i 从 0 到 7 时，记

$$f_j=f_{j7}\circ\cdots\circ f_{ji}\circ\cdots f_{j0} \tag{7}$$

$$f_j^{-1}=f_{j0}^{-1}\circ\cdots\circ f_{ji}^{-1}\circ\cdots f_{j7}^{-1} \tag{8}$$

此处，f_j 与 f_j^{-1} 分别是 f_{ji}(i 从 0 到 7)和 f_{ji}^{-1}(i 从 7 到 0)的复合运算。

$$f_{ji}^{-1}(M_1,M_2,\cdots,M_k,\cdots,M_8)=[w_{ji}^{-1}(r_{ji}^{-1}(M_1),r_{ji}^{-1}(M_2),\cdots,r_{ji}^{-1}(M_k),\cdots,r_{ji}^{-1}(M_8))] \tag{9}$$

此处，$r_{ji}^{-1}(M_k)=M_k\odot v_{ji}^{-1}=M_k\cdot v_{ji}^{-1}\bmod(2^8+1)$，$v_{ji}^{-1}$ 是 v_{ji} 在群 $(Z_{2^8+1}^*,\odot)$ 中的逆元。

3.2 加密与解密过程

加密过程：

1) 将原始的明文 P(二进制位流)按顺序分成 $(P_1,P_2,\cdots,P_n)$ 块。每块长为 64 比特。如果最后一块 P_n 不足 64 比特，则在后面补上 0，并设 $C_0=B_0$，$P_0=B_1$。

2) 每一块 64 比特的明文 P_{j+1}，$(j=0,1,2,\cdots,n-1)$，执行以下几步操作，得到输出 64 比特的密文 C_{j+1}，$(j=0,1,2,\cdots,n-1)$：

① $T_{j+1}\leftarrow C_j\boxplus B_{j+2}$

② $S_{j+1}\leftarrow P_{j+1}\oplus T_{j+1}$

③ $R_{j+1}\leftarrow f_j(S_{j+1})$

④ $X_{j+1}\leftarrow P_j\boxplus B_{j+2}$

⑤ $C_{j+1}\leftarrow R_{j+1}\oplus X_{j+1}$

解密过程实际上是上述加密过程的逆过程，如下：

① $X_{j+1}\leftarrow P_j\boxplus B_{j+2}$

② $S_{j+1}\leftarrow C_{j+1}\oplus X_{j+1}$

③ $R_{j+1}\leftarrow f_j^{-1}(S_{j+1})$

④ $T_{j+1}\leftarrow C_j\boxplus B_{j+2}$

⑤ $P_{j+1} \leftarrow R_{j+1} \oplus T_{j+1}$

4 仿真实验

在一个密码系统中，安全性是首要的问题。下面我们将从理论和仿真实验方面来阐述本文提出的加密算法的安全性。在下面的分析与实验过程中，由于 $0 \notin Z_{2^8+1}^*$ 而 $2^8 = 256 \in Z_{2^8+1}^*$，因此用 2^8 代替 0。另外，在计算群 $(Z_{2^8+1}^*, \odot)$ 的逆元时，我们采用了扩展的 Euclidean 算法。

设 $x_0 = 0.476567340535646$，$\mu = 3.99999996$，$K =$ "*Cryption*"。为了避免瞬态效应，忽略 Logistic 映射开始迭代的 250 次，首先按照第 2.2 节的方法构造 $g: r \to w_{ji}$ 的映射，接着按照第 3 节的方法来加密一个 3200 字节的文本文件和一个 256×256 像素的灰度图像文件，实验结果如图 1 所示。

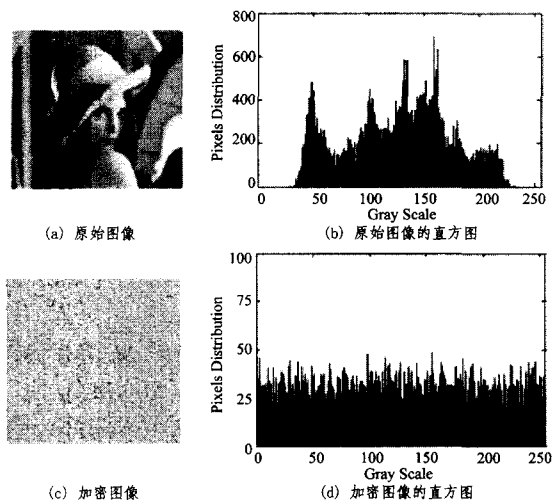

图 1 原始图像和加密图像的像素分布

实验结果表明，该算法能够正确地加/解密文件。注意，当用本文的算法来加密文本文件时，在密文中可能存在一些不可打印的字符。

5 安全性与性能分析

5.1 密钥空间

在下面的分析中，我们采用了 IEEE 754 [14] 浮点数标准。设 $x_0 = 0.x_1x_2\cdots x_{15}$，又因为任意的 64 比特都可以作为密钥 K，所以算法的密钥空间约为 $(10^{15}) \times 2^{64} \approx 2^{113.83}$（注，由于 Logistic 映射的控制参数 μ 的取值范围比较窄，因此没有把它考虑为密钥）。

如果密码分析人员采用蛮力攻击，他们不需要知道 Logistic 映射的细节，譬如初始值 x_0 和控制参数 μ。但他们必须知道密钥 K 和双射映射 $g: r \to w_r$。根据前面第二节双射映射的构造知道，此时的密钥空间大约是 $8! \cdot (8!-1)\cdots(8!-255) \cdot 2^{64}$，这对于当今的计算能力来说，是一个非常大的数了。

5.2 扩散与混淆分析

在本文提出的加密算法中，混和使用了 3 种不同代数群中的运算：群 $(F_2^{64}, \oplus)$ 中的按位异或运算，群 $(Z_{2^8+1}^*, \odot)$ 中的模 2^8+1 乘运算，群 $(Z_{2^{64}}, \boxplus)$ 中的模 2^{64} 加运算。由于 3 种运算的任何两种都不满足分配律和结合律（即，3 种运算互不相容），再加上 $w_{ji}(\cdot)$ 的重排，因此算法获得了很好的扩散与混淆作用。下面来证明 $(Z_{2^8+1}^*, \odot)$ 是可交换群。

由于 2^8+1 是一个素数，所以 $Z_{2^8+1}^* = \{a \mid a \in 1, 2, \cdots, 256\}$ 对模 2^8+1 乘法运算 $\odot$（$\odot, a \odot b = (a \cdot b)_{2^8+1}$）构成交换群。其证明过程如下：

设 $m = 2^8+1 = 257$，则 m 是一个素数。

① $\odot$ 运算是自封的

假设 $a, b \in Z_m^*$，即 $0 < a, b < m$。因为 m 是素数，所以 $(a, m) = (b, m) = 1$ 且 $(ab, m) = 1$。设 m 去除 ab 所得的商是 q，余数是 $(ab)_m$，即：

$ab = qm + (ab)_m$，$0 \leqslant (ab)_m < m$。

所以 $(ab, m) = ((ab)_m, m)$，所以 $((ab)_m, m) = 1$，所以 $a \odot b = (ab)_m \in Z_m^*$。

② $\odot$ 运算是可交换的

设 $a, b \in Z_m^*$，则 $a \odot b = (ab)_m = (ba)_m = b \odot a$。所以，$\odot$ 运算是可交换的。

③ $\odot$ 运算是可结合的

设 $a, b, c \in Z_m^*$。如果 $m \mid a-b$，则 $(a)_m = (b)_m$。由于 $ab - (a)_m(b)_m = a(b-(b)_m) + (a-(a)_m)(b)_m$ 是 m 的倍数，所以，$m \mid ab - (a)_m(b)_m$。因此，$(ab)_m = ((a)_m(b)_m)_m$。另一方面，$c \in Z_m^*$，则 $c = (c)_m$。所以

$$\begin{aligned}(a \odot b) \odot c &= ((ab)_m \cdot c)_m = ((ab)_m \cdot (c)_m)_m \\ &= ((ab)c)_m = (a(bc))_m = (a(bc)_m)_m \\ &= a \odot (b \odot c)\end{aligned}$$

④ 单位元 e 的属性

对所有的 $g \in Z_m^*$，由于 $1 \odot g = (1 \times g)_m = g = (g \times 1)_m = g \odot 1$，因此 1 是群 $(Z_m^*, \odot)$ 中的单位元。

⑤ 逆元的唯一存在性

设 $a \in Z_m^*$，则 $(a, m) = 1$，所以存在整数 c, d 使得 $1 = ca + dm$，所以 $(c, m) = 1$，$((c)_m, m) = 1$，$(c)_m \in Z_m^*$，$1 = ca + dm = (ca + dm)_m = (ca)_m = ((c)_m \cdot a)_m = (c)_m \odot a$。因此 $(c)_m = a^{-1}$，逆元的唯一存在性得证。

5.3 统计测试

根据 Shannon 理论，一个好的加密算法应该具有良好的抗统计攻击能力。文本文件中的字符都是一些可见字符，其 ASCII 码值位于 033～126 之间，用本文中的算法加密之后，其 ASCII 码分布于 0～255 之间且更加均匀，因而具有更好的抗统计攻击能力。

实验统计结果如图 2 所示，表明密文的分布完全不同于明文，其在整个 ASCII 码表上的分布更加均匀。

当然，由式(1)产生的伪随机序列也具有很好的伪随机特性。这些良好的统计特性表明明文和密文之间有相对较好的独立性。

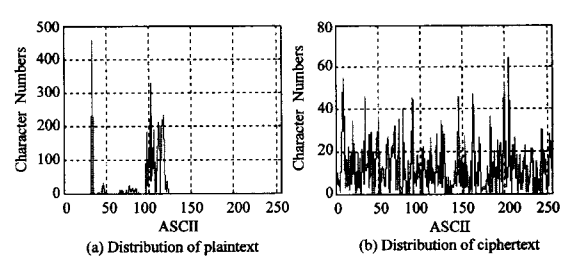

图 2 明文与密文的分布

5.4 密钥敏感性测试

任何一种密码系统，都需提供 3 种重要特性来防止密码分析 [23]，即：

1)对密钥敏感：对同一明文，密钥的微小变化将产生完全不同的密文。

2)对明文敏感:对同一密钥,明文的微小变化将产生完全不同的密文。

3)明文到密文的映射是随机的:一个好的密码系统,密文中不应该存在任何固定模式。

由于本节的加密算法的密钥是由 x_0,K 两部分组成的,因此我们将从两个方面来进行密钥敏感性测试。

1)保持 x_0 不变,改变密钥 K 的最后一位。修改后的密钥 K'="*Cryptiom*"。然后用密钥 K'和 x_0 解密图 1 (c),实验结果如图 3(c)所示。

2)保持 K 不变,改变 x_0 的最后一位。修改后的密钥 x_0'=0.476567340535645。然后用密钥 K 和 x_0'解密图 1(c),实验结果如图 3(d)所示。

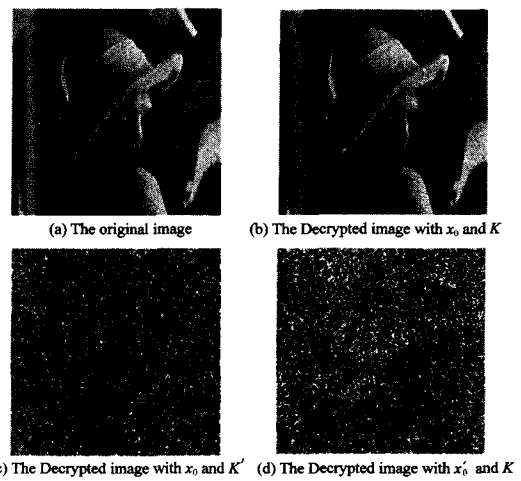

图 3 密钥敏感性测试

实验结果表明,尽管密钥只有微小的差异,但也导致了解密的失败。因此,这个新的加密算法保持了密钥敏感性。同时,我们在实验中也发现,两个只有 2^{-15} 微小差异的初值 x_0 和 x_0',按照第 2.2 节算法构造的双射映射也几乎完全不同。

5.5 排列分析

正如在文献[14]中所述,PRN 是独立同分布的。除非知道混沌系统的初始值 x_0 和控制参数 μ,否则很难从 PRN 序列的前面位来预测下一位。同时,只有混沌实值轨道 $\tau^n(x)$ 的部分位参与了构造 PRN 序列。因此,在进行密码分析时,对 x_0 的猜测和加密系统的重构变成了不可能。

排列几乎是所有的传统密码系统的基本操作。在许多的密码系统中,排列只是根据设计者预先定义的方式重新排列输入元素,是与密钥无关的。在实际的密码分析过程中,由于这种排列很容易被差分分析攻破,因此它对算法安全性几乎没有什么意义。然而,在本文提出的加密算法中,排列是与密钥相关的,不同的消息块有不同的排列方式,从而增加了密码分析的难度。

结束语 本文提出了一种基于混沌映射和群上代数运算的分组密码算法。该算法中的密文依赖于明文、由 Logistic 映射产生的伪随机序列、置换运算和代数群上的运算。它弥补了一些纯混沌密码算法的缺陷。大的密钥空间、三种群运算的扩散与混淆和排列置换运算保证了新的密码系统对统计攻击及其选择明文攻击等常用密码分析方法都有很好的抗攻击能力。

参 考 文 献

[1] Yang Huaqian, Liao Xiaofeng, Wong Kwok-wo, et al. A new block cipher based on chaotic map and group theory. Chaos, Solitons and Fractals, Impress (doi:10.1016/j.chaos.2007.07.056)

[2] Tang G, Liao XF. A method for designing dynamical S-boxes based on discretized chaotic map[J]. Chaos, Solitons & Fractals 276, 2005, 23:1901-1909

[3] Xun Y, How T C, Kheong S C. A new block cipher based on chaotic tent maps[J]. IEEE Trans Circuits Syst I 278, 2002, 49(12):1826-1829

[4] Jakimoski G, Kocarev L. Chaos and cryptography: block encryption ciphers based on chaotic maps[J]. IEEE Trans Circuits Syst I 280, 2001, 48(2):163-288

[5] Stojanovski T, Kocarev L. Chaos-based random number generators—Part I: Analysis[J]. IEEE Trans Circuits Syst I 282, 2001, 48(3):281-288

[6] Stojanovski T, Kocarev L. Chaos-based random number generators—Part II: Practical realization[J]. IEEE Trans Circuits Syst I 284, 2001, 48(3):382-385

[7] Kohda T, Tsuneda A. Statistics of Chaotic Binary Sequences[J]. IEEE Transactions on Information Theory, 1997, 43(1):104-112

[8] Li Shujun, Mou Xuanqin, Cai Yuanlong. Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography[C]// Progress in cryptology-Indo-Crypt 2001, Lecture notes in computer science. vol. 290 2247, December 2001:316-329

[9] Wheeler D D. Problems with chaotic cryptosystems[J]. Cryptologia, 1989, XIII(3):243-250

[10] Wheeler D D, Mathews R A J. Supercomputer investigations of a chaotic encryption algorithm[J]. Cryptologia, 1991, XV(2):140-152

[11] Wei Jun, Liao Xiaofeng, Wong Kwok-wo, et al. A new chaotic cryptosystem[J]. Chaos, Solitons & Fractals, 2006, 30:1143-1252

[12] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps[J]. Int J Bifurcat Chaos, 1998, 8(6):1259-1284

[13] Goldberg D, Priest D. What every computer scientist should know about floating-point arithmetic[J]. ACM Comp Surv295, 1991, 23(1):5-48

[14] Knuth D E. Seminumerical algorithms. The art of computer programming, 3rd ed. vol. 2, Reading, (MA): Addison Wesley, 1998

(上接第 87 页)

参 考 文 献

[1] Viswanath P, Tse D N C, Laroia R. Opportunistic beamforming using dump antennas[J]. IEEE Trans. Information Theory, 2002, 48(6):1277-1294

[2] Knopp R, Humblet P A. Information capacity and power control in single-cell multiuser communications[C]// IEEE Internet Communicaiton Conference. 1995:331-335

[3] Sharif M, Hassibi B. On the capacity of MIMO broadcast channel with partial side information[J]. IEEE Trans. Information Theory, 2005, 51(2):506-522

[4] Hassibi B, Marzetta T L. Multiple-antennas and isotropically random unitary inputs: The received signal density in closed form[J]. IEEE Trans. Information Theory, 2002, 48(6):1473-1484

[5] Vicario J L, Bosisio R, Haro C A. A throughput analysis for opportunistic beamforming with quantized feedback. Personal, Indoor and Mobile Radio Communications, 2006: