第 59 卷 第 8 期 2010 年 8 月
1000-3290/2010/59(08)/5281-07

物 理 学 报
ACTA PHYSICA SINICA

Vol. 59, No. 8, August, 2010

基于改进元胞自动机的数字保密通信方案*

张 旭 任 卫 唐冬妮 唐国宁†

(广西师范大学物理科学与技术学院,桂林 541004)

(2009 年 9 月 21 日收到;2009 年 12 月 9 日收到修改稿)

为了提高现有混沌保密通信系统的加解密速度和安全性,提出了一种新的即时同步流密码数字保密通信方案,在该方案中利用改进元胞自动机进行加密,并采用扩展密钥技术和置乱技术. 数值模拟结果表明:该方案能产生随机性很好的流密码,并且具有较高的加解密速度和非常高的抗破译能力.

关键词: 扩展密钥, 保密通信, 元胞自动机

PACC: 0545

1. 引 言

随着近年来世界范围内经济和科学技术的迅猛发展,全世界范围内形成了一个巨大的通信交流网,因此通信安全问题也不可避免的呈现在人们面前,复杂的密码算法会造成通信速度过慢,成本过高,密码算法过于简单往往又会使通信的安全性能大打折扣. 如何研制出高保密性、高加密速度、高抗干扰能力的经济实用型混沌保密通信系统,已成为信息科学界关注的焦点之一[1—15].

由于采用元胞自动机加密通信有利于提高加密速度,人们提出了各种基于元胞自动机加密方案[13—17],但是到目前采用元胞自动机加密仍存在一次性处理信息量过小、误差扩散速度过慢、误差扩散具有单向性、对明文扰乱程度不够、密钥空间较小等问题需要改进.

本文提出一种基于元胞自动机数字保密通信的方案,该方案采用了如下措施:1)用密文直接产生流密码,实现即时同步;2)采用扩展密钥[1]方法,使得流密码的产生与密钥间接有关,这促使流密码对密钥变化的敏感性大大增强;3)采用了置乱[2]措施,提高了抗破译能力;4)采用元胞自动机[13—17]思想进行加密,使得通信过程中实现了并行加解密,这保证了该系统具有高速通信的特点. 下面先介绍使用的改进元胞自动机模型,然后介绍通信方案和数值模拟与分析,最后是应用实例和结论.

2. 改进的一维元胞自动机模型

定义 1 一维元胞自动机 CA 是一个三元组 $CA=(S,R,f)$,其中,S 为有限状态集; R 为邻域半径;f 为映射函数,又简称为规则.

定义 2 设 CA 是由 N 个元胞构成的有限元胞自动机,各元胞排列成一行,按顺序编号为 1,2,…,N,称 $G^{(t)}=(s^t(1),s^t(2),\cdots,s^t(N))$ 为元胞自动机在 t 时刻的一个全局状态配置.

一维元胞自动机的状态集 S 有 2 种状态“0”或“1”;元胞 i 下一时刻的状态由当前时刻元胞 i 以及其最近邻的 $2R$ 元胞的状态共同决定,演化规则为

$$\begin{aligned} s^{t+1}(i) =& f(s^t(i-R),\cdots,s^t(i-1),\\ & s^t(i),s^t(i+1),\cdots,\\ & s^t(i+R)), \end{aligned}$$

其中 $s^t(i)$ 为第 i 个细胞在 t 时刻的状态.

这里提出一种改进的一维元胞自动机模型,在该模型中每一个元胞的状态有多达 2^{24} 个,t 时刻元胞 i 状态用一个串长为 24bit 的整数 $s^t(i)$ 表示,且元胞 i 下一时刻的状态由当前时刻三个元胞 $i-r,i,i+r$ 的状态决定,元胞状态更新规则为

$$\begin{aligned} s^{t+1}(i) =& \mathrm{XOR}((s^t(i-r)\\ & \times s^t(i+r))\bmod 2^{24},s^t(i)),\\ & r\in[1,N/2],1\leqslant i\leqslant N, \end{aligned} \tag{1}$$

* 国家自然科学基金(批准号:10765002)资助的课题.

† 通讯联系人. E-mail:tangguoning@sohu.com

其中 XOR 表示异或,mod 表示求余,×表示相乘,采用周期边界条件.(1)式表示 $s^t(i-r)$ 与 $s^t(i+r)$ 相乘对 2^{24} 求余,将求余结果再与 $s^t(i)$ 异或给出元胞 i 下一时刻的状态 $s^{t+1}(i)$,下面将利用该模型来加密.

3. 数字保密通信方案

为了得到高保密性、高加密速度、高抗干扰能力保密通信系统,利用上述元胞自动机进行加密通信,不失一般性,我们取 $N=300$. 利用同步信号作为元胞自动机各元胞的初态,经过 6 轮迭代元胞自动机产生 N 组长度为 24bit 的二进制串流密码,记为 $KS(i)$,它们就是 N 个元胞在第 6 轮迭代后的元胞状态,即 $KS(i)=s^6(i)$. 选择 6 轮迭代是因为当同步信号被改变 1bit 时,这个误差随着迭代轮数 q 增加,将有 3^q 个元胞状态受影响,经过 6 轮迭代误差将扩散到所有元胞上,导致加解密系统的流密码完全不同. 为了满足扩散要求,对于不同轮的迭代,(1)式中的 r 取不同的值,这里第 q 轮迭代取 $r=23q, q=1,2,\cdots,6$. 由于有 N 组流密码,每次加密 N 组长度为 24bit 的二进制串明文,明文记为 $P(i)$,流密码与明文异或 $XOR(KS(i),P(i))$ 得到密文 $C(i)$,该 N 组密文被作为同步信号发射出去,一方面作为接收和发射系统元胞自动机的初态,用于产生下一次加、解密的流密码;另一方面用于本次接收系统的解密,解密方案是 $P(i)=XOR(KS(i),C(i))$.

为了提高元胞自动机保密通信系统的保密性,采取如下措施:1)使用扩展密钥技术. 根据密钥产生 $q=6$ 轮扩展密钥 $Kep(q,i)$,每一轮有 N 个扩展密钥,每一个扩展密钥长度与流密码长度相同;2)使用了置乱技术,即根据一定规律交换两个元胞的状态. 两种技术分别介绍如下.

1)扩展密钥流的生成

设密钥是 240bit 的二进制串,平均分成 10 组,分别记为 $k_0,k_1,\cdots,k_j,\cdots,k_9$,每组都是 24bit 的整数. 通过 $w_{j,0}=\dfrac{k_j}{2^{24}}$ 方式将 10 组密钥转换成(0,1)之间的 10 个小数 $w_{0,0},w_{1,0},\cdots,w_{j,0},\cdots,w_{9,0}$,然后将这 10 个小数分别作为 10 个混沌映射 $w_{j,n+1}=4w_{j,n}(1-w_{j,n})$,$j=0,1,\cdots,9$ 的初值同时开始迭代. 当迭代到 50 步时,将这 10 个映射的值($w_{j,50}, j=0,1,\cdots,9$)乘以 2^{24} 得到的整数作为最初的 10 个扩展密钥,因为混沌映射值域为(0,1),这样得到的扩展密钥是 24bit 的整数. 以后映射每迭代 10 步就按相同方式产生扩展密钥,第 m 次得到的扩展密钥为 $w_{j,50+10m}\times 2^{24}, j=0,1,\cdots,9, m=0,1,2,\cdots$,将在 $m\in[0,29]$ 中产生的 $N=300$ 扩展密钥作为第一轮扩展密钥,记为 $Kep(1,i), i=1,2,\cdots,N$,将在 $m\in[30,59]$ 中产生扩展密钥作为第二轮扩展密钥,记为 $Kep(2,i)$,按此方式产生 6 轮扩展密钥 $Kep(q,i), q=1,2,\cdots,6$.

2)置乱算法

置乱算法一般可以写成

```
j = 1,
do i = 1,300,
  j = (j + s^q(i) + Kep(q + 1,i)) mod 300 + 1,
  Swap(s^q(i),s^q(j)),
end do,
```

其中 q 表示是第 q 轮置乱,其中 $1\leqslant q\leqslant 5$.

采用上述技术后加解密过程如下:1)先将同步信号与扩展密钥异或作为元胞自动机的初态 $s^0(i)=XOR(Kep(1,i),C(i))$;2)按规则(1)式演化得到 $s^1(i)$,然后按置乱算法交换两个元胞 i 和 j 的状态;3)过程 2)接着演化 4 次;4)按规则(1)式再演化一次得到 $s^6(i)$,给出流密码 $KS(i)=s^6(i)$;5)加密系统作加密 $C(i)=XOR(KS(i),P(i))$,传输 $C(i)$,并返回 $C(i)$ 作为元胞自动机初值产生下一次流密码,解密系统进行解密 $P(i)=XOR(KS(i),C(i))$. 加密流程如图 1 所示. 只要密钥和同步信号相同,加解密系统的流密码 $KS(i)$ 就相同,从而保证正确解密. 这样一次同步完成保密通信 $300\times 24=7200$ bit. 除加密端第一次的 7200 bit 的流密码为随机产生外,其余流密码均为以上方法产生.

4. 保密通信系统的性能分析

由于这里生成的流密码为即时同步流密码,它的产生与加密的明文有关,下面取三种明文:1)二进制码全为“0”;2)二进制码全为“1”;3)二进制码为“0”与“1”相间,分析在这三种特殊的明文下分别得到的流密码的随机性和密钥敏感性.

4.1. 流密码的随机性分析

这里引进文献[9]中的频数检验、序列检验、游程检验和自相关检验来检测流密码的随机性. 每回

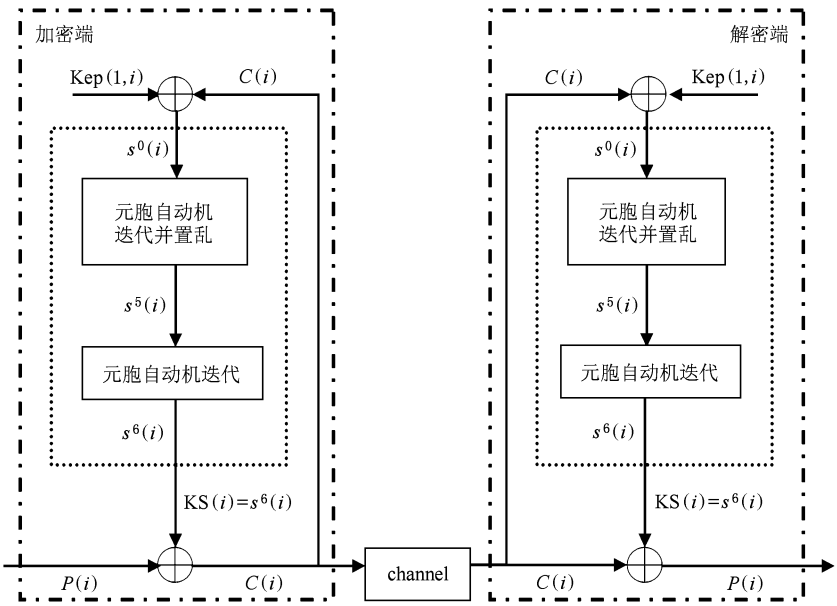

图 1　加解密流程图

检测取连续生成 500 次的流密码(每次 7200 bit),得到长度为 $L=500\times7200=3.6\times10^6$ 二进制序列,对于每一种明文,取不同的初始流密码,进行 1000 回检测,将检测结果取平均.

4.1.1. 频数检验

频数检验是用来测试流密码序列中 0 和 1 的个数是否大致相同,这也是序列具有随机性的最基本保证. 设所测试的二值序列含有 n_0 个“0”,n_1 个“1”,计算检验统计量

$$\chi^2=\frac{(n_0-n_1)^2}{L},$$

对应显著性水平为 5% 的 χ^2 值查表得 $\chi_5^2=3.841$,所以只要 $\chi^2\leqslant3.841$,则说明序列通过检验.

4.1.2. 序列检验

对随机序列来说,如果由 0 和 1 所组成的各种子块是等分布的,就意味序列出现相同和不同相邻元素的概率大致相等,保证了序列的每个 bit 不依赖于它前面的 *bit*. 设 $n_{00},n_{10},n_{01},n_{11}$ 分别表示“00”,“10”,“01”,“11”这四种模式出现的个数. 计算检验统计量

$$\chi^2=\frac{4}{L-1}\sum_{i=0}^{1}\sum_{j=0}^{1}(n_{ij})^2-\frac{2}{L}\sum_{i=0}^{1}(n_i)^2+1,$$

对应显著性水平为 5% 的 χ^2 值 $\chi_5^2=5.991$,所以只要 $\chi^2\leqslant5.991$,则说明序列通过检验.

4.1.3. 游程检验

游程是序列中由连续相同的 0 或 1 组成的一个子串,其前导和后继元素都与该元素不同. 游程检验主要是检验待测序列中游程总数是否符合随机性要求. 记长度为 S 的游程出现的次数为 C_s,则游程总数 $C=\sum C_s$,用下式计算:

$$C=1+\sum_{i=0}^{L-2}r(i),$$

其中

$$r(i)=\begin{cases}1, b_i\neq b_{i+1},\\ 0, b_i=b_{i+1}.\end{cases}$$

对于长度为 L 的二元随机序列,游程总数的数学期望为 $E(C)=L/2$. 若 C 越接近 $E(c)$,则该序列的随机性越好. 采用 $D=\left|\frac{C-E(C)}{E(C)}\right|$ 衡量,则 D 的值越小序列的随机性越好.

4.1.4. 自相关检验

自相关检验用来检验待测序列和将其逻辑左移 d 位后的序列之间的关联程度. 一个随机的序列应该与其逻辑左移任意位的序列是独立的,其关联程度应该很低. 对二进制序列 $b_1,b_2,\cdots,b_L$,有 $A(d)=\sum_{i=1}^{L-d}(b_ib_{i+d}),0\leqslant d\leqslant L$. $A(d)$ 表示待测序列和将其逻辑左移 d 位的序列之间相同且为 1 的元素的个数. 若该序列是随机的,则 $A(d)$ 的数学期望为 $E(d)=\frac{n_1^2(L-d)}{L^2}$,若 $A(d)$ 越接近 $E(d)$,就说明序列的

随机性越好. 采用 $D(d) = \left|\frac{A(d) - E(d)}{E(d)}\right|$ 衡量,则 $D(d)$ 值越小序列的随机性越好.

表 1 随机性分析

	频数检验(平均值)	序列检验(平均值)	频数检验(通过率)/%	序列检验(通过率)/%	游程检验(平均值)
明文为全 0	1.2323	4.2896	92.1	82.4	0.0004350
明文为全 1	1.1718	4.1023	93.4	85.1	0.0004084
明文为 0,1 相间	1.2114	4.2100	92.5	83.1	0.0004224

表 2 自相关性分析

d	明文为全 0	明文为全 1	明文为 0,1 相间
0	1.00	1.00	1.00
1	0.0004189	0.0004190	0.0004298
10^1	0.0004293	0.0004080	0.0004208
10^2	0.0004307	0.0004364	0.0004276
10^3	0.0004251	0.0004260	0.0004066
10^4	0.0004106	0.0004265	0.0004294
10^5	0.0004526	0.0004392	0.0004477

表 1 给出了随机性分析结果,表 2 给出了自相关性分析结果,可以看出,这种通信方案生成的流密码的随机性非常理想,并且针对不同种类的明文,由该方案生成的自同步流密码随机性基本一致,与具体的明文无关.

4.2. 密钥敏感性分析

密码系统理想的"雪崩效应"应当是密钥每 1 bit变化都将引起相应的密文的 bit 数以 $\rho = 50\%$ 的概率发生改变. 假设密钥在其任意位置改变 1 bit 时某次输出的 7200 bit 流密码中总共有 N_0bit 发生改变,定义总改变概率为 $\rho_{tot} = \frac{N_0}{7200}$. 假设第 M 次输出的流密码其总改变概率为 $\rho_{tot}(M)$,图 2 给出了改变概率 $\rho_{tot}(M)$ 随 M 的变化,可见密钥在其任意位置改变 1 bit 都导致各流密码中有约 50% bit 发生改变.

为看出密钥改变 1 bit 时对单个流密码 KS(i)的影响,假设在第 M 次第 i 个元胞产生流密码 KS(i)中有 $N_0^M(i)$个 bit 发生改变,则改变概率定义为

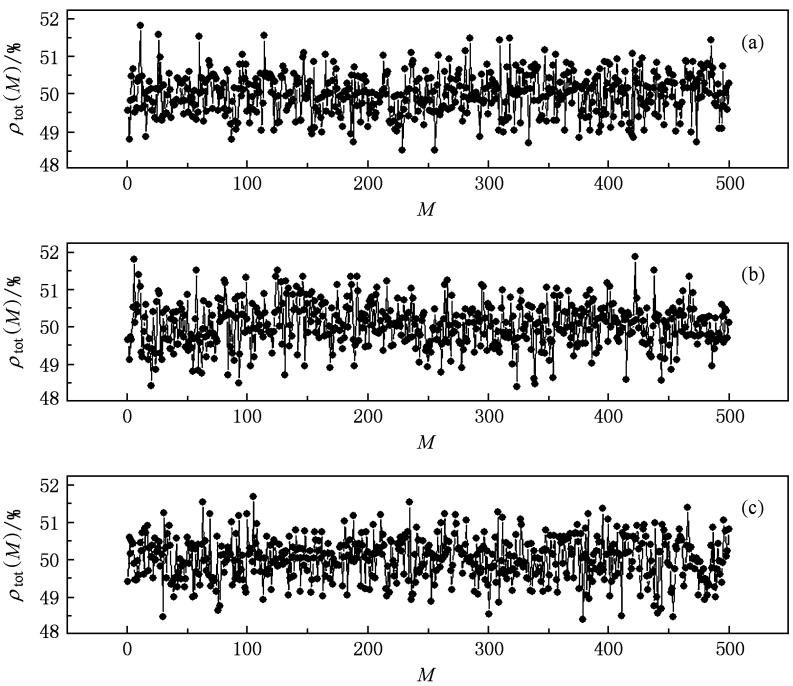

图 2 密钥改变 1 bit 时各次输出流密码的总改变概率 (a)明文为全 0;(b)明文为全 1;(c)明文为 0 与 1 相间

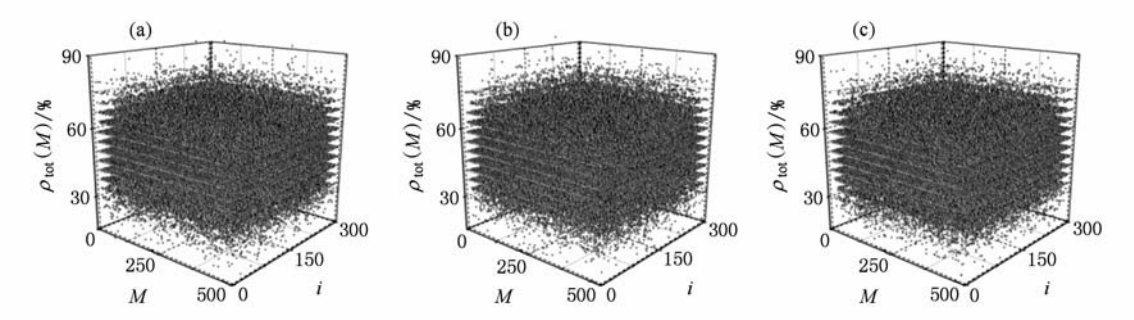

图 3　密钥改变 1 bit 时各元胞在各次输出流密码中的改变概率　(a)明文为全 0;(b)明文为全 1;(c)明文为 0 与 1 相间

$\rho_{tot}(M,i)=\frac{N_0^M(i)}{24}$,图 3 给出了 $\rho_{tot}(M,i)$ 随 M 和 i 变化的三维图,该图显示,当密钥任意位置改变 1 bit 时,各流密码 KS(i)都发生改变,改变概率从 20% 到 80% 不等.

5. 应 用 实 例

下面以著名的 lenna 图为实例进行通信实验,假设通信双方通信前已经事先约定好密钥. lenna 图是一幅 256 像素 ×256 像素 ×8 位色度的图像,对其加密需要 524288 bit 的流密码,因此至少需要传递 73 次才能将画从发射系统传到接收系统. 其加/解密图像如图 4 所示,其中 4(a)为原始图像,4(b)为正确的密钥解密下的解密图像,4(c)为解密端密钥在任意位误差 1 bit 时的解密图像,4(d)为同步信号传输过程中第 45 次同步信号受到 1 bit 扰动时的解密图像. 结果表明该保密通信系统具有极好的保密

图 4　lenna 图为实验的通信效果图　(a)原始图像;(b)为正确的密钥解密下的解密图像;(c)为解密端密钥任意误差 1 bit 时的解密图像;(d)为同步信号传输过程中第 45 次同步信号受到 1 bit 扰动时的解密图像

性,只要密钥有一点不同,就不能正确解密,当一次同步信号受到干扰,就会使下一次的解密完全失败,但不会影响以后的解密.

6. 结 论

本文提出一种基于元胞自动机思想的数字保密通信的方案,该方案采用混沌映射来获得的扩展密钥,使得产生的流密码对密钥的变化具有极高的敏感性,加上采用置乱技术,极大地提高了抗破译能力;采用改进元胞自动机模型加密,保证了该系统产生的流密码有较好的随机性,同时具有高加密速度的特点,采用 C 语言程序在 PC 联想双核计算机(2.66 GHz)上模拟加解密,得到加解密速度约为 50.8834 Mbit/s. 虽然该加解密速度比以往的元胞自动机加密速度有很大提高,但依旧慢于 AES 的加密速度,因此我们希望以后的元胞自动机加密方案中能提出更快的加密速度方案,同时也期望文中这种加密方案在实际中能得到应用.

[1] Dai R 2007 *MS Thesis* (Guilin: Guangxi Normal University) (in Chinese) [代 榕 2007 硕士学位论文(桂林:广西师范大学)]

[2] Mantin I, Shamir A 2002 *Lecture Notes in Computer Science: Fast Software Encryption* **2355** 152

[3] Li w, Hao J H, Qi B 2008 *Acta Phys. Sin.* **57** 1398 (in Chinese) [李 伟、郝建红、祁 兵 2008 物理学报 **57** 1398]

[4] Xiang F, Qiu S S 2008 *Acta Phys. Sin.* **57** 6132 (in Chinese) [向 菲、丘水生 2008 物理学报 **57** 6132]

[5] Zhang J Z, Wang A B, Wang Y C 2009 *Acta Phys. Sin.* **58** 3793 (in Chinese) [张建忠、王安帮、王云才 2009 物理学报 **58** 3793]

[6] Sun Y H, Cao J D, Feng G 2008 *Phys. Lett.* A **372** 5442

[7] Su Z K, Wang F Q, Lu Y Q, Jin R B, Liang R S, Liu S H 2008 *Acta Phys. Sin.* **57** 3016 (in Chinese) [苏志锟、王发强、路轶群、金锐博、梁瑞生、刘颂豪 2008 物理学报 **57** 3016]

[8] Ye W P, Dai Q L, Wang S H, Lu H P, Kuang J Y, Zhao Z F, Zhu X Q, Tang G N, Huang R H, Hu G 2004 *Phys. Lett.* A **330** 75

[9] Wang Y W 2007 *Ph. D. Dissertation* (Jilin: Jilin University) (in Chinese) [王有维 2007 博士学位论文(吉林:吉林大学)]

[10] Sun F Y, Liu S T, Lü Z W 2007 *Chin. Phys.* **16** 3616

[11] Xu S J, Wang J Z, Yang S X 2008 *Chin. Phys.* B **17** 4027

[12] Li J F, Li N 2002 *Chin. Phys.* **11** 1124

[13] Zhang C W, Lin L B 2005 *IEEE international Symposium on Communications and information Technology* **1** 031

[14] Zhang C W, Shen Y Q, Pen Q C 2004 *Chinese Journal of Computers* **27** 125 (in Chinese) [张传武、沈野樵、彭启琮 2004 计算机学报 **27** 125]

[15] Ping P, Zhao X L, Zhang H, Liu F Y 2008 *Acta Phys. Sin.* **57** 6188 (in Chinese) [平 萍、赵学龙、张 宏、刘凤玉 2008 物理学报 **57** 6188]

[16] Wolfram S 1984 *Physica* D **10** 1

[17] Wolfram S 1986 *Adv. Appl. Math.* **7** 123

Digital secure communication scheme based on improved cellular automata*

Zhang Xu　Ren Wei　Tang Dong-Ni　Tang Guo-Ning†

(*College of Physics and Technology, Guangxi Normal University, Guilin* 541004, *China*)

(Received 21 September 2009; revised manuscript received 9 December 2009)

Abstract

In order to enhance the encryption speed and secrecy of the current chaotic secure communication system, a scheme of digital secure communication based on the stream cipher produced by real-time synchronization is presented. A improved cellular automata is used for encryption in the secure communication scheme while the expanded key technology and confusion technology are adopted. Numerical results show that the secure communication scheme can produce good pseudo-randomness stream ciphers while it has very fast speeds of encryption and decryption and high anti-attack ability.

Keywords: the expanded key, secure communication, cellular automata

PACC: 0545

* Project supported by the National Natural Science Foundation of China (Grant No. 10765002).

† Corresponding author. E-mail: tangguoning@sohu.com