第 57 卷 第 10 期 2008 年 10 月
1000-3290/2008/57(10)/6188-08

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.10,October,2008

复合元胞自动机系统反向迭代加密技术研究*

平 萍† 赵学龙 张 宏 刘凤玉

(南京理工大学计算机科学与技术学院,南京 210094)

(2008 年 1 月 3 日收到;2008 年 2 月 24 日收到修改稿)

提出了元胞自动机的交叉复合在序列 R 下随机复合的思想,分析了复合元胞自动机系统的密码学特性,利用元胞自动机反向迭代加密技术,构造了两个基于复合元胞自动机的密码系统.新的复合元胞自动机密码系统很好地解决了单一元胞自动机密码系统中存在的误差单向扩散的问题,并且能够以较小的规则半径获得大密钥空间.计算机仿真结果表明,复合元胞自动机密码系统具有良好的扰乱和扩散性能,能够有效地抵抗蛮力攻击和差分分析.

关键词:离散动力系统,复合元胞自动机,反向迭代,分组密码

PACC:0550

1. 引 言

元胞自动机是与连续 Cantor 映射动力系统相对应的离散动力系统,具有时间、空间、状态的离散性[1].最早将元胞自动机引入密码学的是 Wolfram,他首次提出了基于元胞自动机的序列密码算法[2],随后元胞自动机在伪随机数发生器的构造[3],分组密码[4],公钥密码[5]以及 Hash 函数[6]中都取得重要的应用.元胞自动机固有的组成单元的简单性、单元之间作用的局部性、信息处理的高度并行性以及复杂的全局性,使得基于元胞自动机的密码技术已成为国内外研究的热点[7].

Gutowitz 提出了基于触发元胞自动机的分组密码算法(TCA 加密算法)[8],该算法采用了一种特别的触发规则,反向迭代实现加密,正向迭代实现解密,具有简单、方便硬件实现等优点,但也存在如下不足:1)使用单一元胞自动机系统时,只能在左触发规则和右触发规则中选取一种规则作为密钥,导致误差扩散具有单向性,误差传播放大速度较慢,扩散机理不强,攻击者通过寻找密文的相似性就可以获得相关明文信息,从而降低了密码系统的安全性.2)由于使用了一维元胞自动机,要获得较大的密钥空间,必须增大规则的半径,这不仅增加了规则表的存储空间,而且增加了计算的复杂性.3)每一轮需要添加 $2r$ 位随机数,用于构造先导状态,迭代 n 轮需要 $2rn$ 位随机数,因而存在数据膨胀问题,即密文的长度要远大于明文的长度.

针对 Gutowitz 算法中数据膨胀的问题,张传武等人[7]采用循环移位寄存器,提出了基于元胞自动机反向迭代的加密算法,该算法每一轮迭代无需添加随机数,利用数据低位部分的 $2r$ 比特构造先导状态,提高了计算效率和加密速度,解决了数据膨胀的问题,但仍然存在误差单向扩散和需要增大规则半径的问题.

针对上述问题,本文首先给出复合元胞自动机系统模型,分析了复合元胞自动机系统的密码学特性,然后利用元胞自动机的反向迭代加密技术,提出了基于复合元胞自动机系统构造分组密码的新方法.仿真结果表明,复合元胞自动机系统比单一元胞自动机系统具有更好的密码属性,复合元胞自动机系统强化了扩散机理,使构造的密码系统不仅具有双向的误差扩散,而且具有更快速的误差传播速度.另外,复合元胞自动机系统增大了规则的有效半径,以较小的规则半径,就可获得大密钥空间,从而减少了规则表的存储空间和迭代计算中的计算量.

* 国家自然科学基金(批准号:90718021)资助的课题.

† E-mail:pingpingnjust@163.com

2. 复合元胞自动机系统模型

2.1. 元胞自动机相关定义

定义 1　元胞自动机是一个四元组 $CA=(d,S,N,f)$，其中 d 表示空间维数，S 为有限状态集，N 为邻域向量，是由 Z^d 中 m 个不同的位置向量组成，记作 $N=(x_1,x_2,\cdots,x_m)$，f 为局部转换函数，又称为规则，是从 S^m 到 S 的映射.

通常，一维元胞自动机的邻域向量可以表示为 $N=(\langle -r\rangle,\cdots,\langle -1\rangle,\langle 0\rangle,\langle 1\rangle,\cdots,\langle r\rangle)$，其演化过程的一般表达式为

$$s_i^{t+1}=f(s_{i-r}^t,\cdots,s_i^t,\cdots,s_{i+r}^t),i\in Z, \quad (1)$$

其中，s_i^t 为第 i 个元胞在 t 时刻的状态，r 为邻域半径.

空间内所有元胞根据相同的局部转换函数，进行同步更新，从而引起复杂的全局变化是元胞自动机的一个重要特性，因此又可以定义一个全局转换函数

$$F:C^{(t)}\to C^{(t+1)},$$

其中 $C^{(t)}=(\cdots,s_{i-n}^t,\cdots,s_{i-1}^t,s_i^t,s_{i+1}^t,\cdots,s_{i+n}^t,\cdots)$，表示 t 时刻全体元胞的一个状态组合，称作构形，所有可能的构形组成的集合称为构形空间，记作 Γ.

类似于经典力学中的运动都可以用相空间中的轨道来表示，元胞自动机的演化可以用构形空间中构形转移的轨道来描述. 若已知初始构形为 C_0，序列 $\{C_0,F(C_0),F^2(C_0),\cdots,F^n(C_0),\cdots\}$ 称为元胞自动机的前向迭代轨道，其中 $F^n(C_0)$ 表示函数 F 的 n 次复合. 不同的初始构形对应于不同的轨道，但不同初始构形的轨道最后可以趋向少数相同的稳定轨道.

定义 2　如果对某个构形 $C\in\Gamma$，有 $F^n(C)=C$，但对于小于 n 的自然数 k，$F^k(C)\neq C$，则称构形 C 是 F 的一个 n 周期点，$\{C,F(C),\cdots,F^{n-1}(C)\}$ 为 F 的一个 n 周期轨.

当 $n=1$ 时，有 $F(C)=C$，此时称构形 C 是 F 的一个不动点.

假设 1　有限元胞自动机的边界条件为非随机型.

假设 1 保证了性质 1 和性质 2 的正确性.

性质 1　有限元胞自动机的前向迭代轨道最终将进入周期轨.

证明　对于具有 k 个状态，由 L 个元胞组成的有限元胞自动机，共有 k^L 种构形，构形空间的大小是有限的. 从任何一个初始构形开始，元胞自动机的前向迭代轨道是唯一确定的，在迭代 k^L 步以上，必定会遇到一个与先前相同的构形，所以迭代进入了这个稳定的周期轨，当周期等于 1 时，轨道趋于不动点.

图 1 描述了两个有限元胞自动机的前向迭代轨道(采用周期型边界)，图中 t 为离散的时间点，$c(t)$ 为构形 $C^{(t)}$ 的十进制表示. 图 1(a)中的元胞自动机的迭代轨道趋于不动点，(b)中的元胞自动机在迭代 19 次之后进入周期为 15 的周期轨.

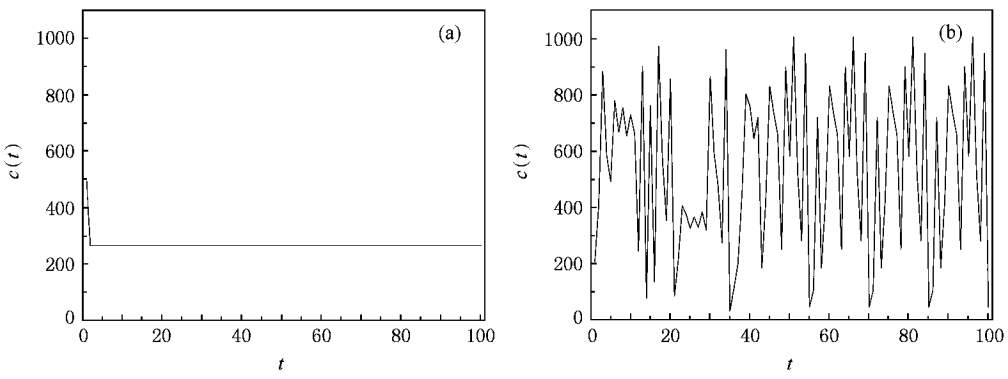


图 1　有限元胞自动机的前向迭代轨道　(a) $L=10,k=2,f=12$；(b) $L=10,k=2,f=30$

性质 1 表明，具有非随机型边界的有限元胞自动机，给定初始条件，其前向迭代轨道最终要进入一个循环，存在动力学特性和密码学特性退化，这些退化对元胞自动机应用系统的安全存在不可忽视的影响，可以利用各种预测技术破译和提取信息. 为了避免迭代轨道的周期性，可以选择随机型边界条件，或者采用本文下面提出的随机复合元胞自动机系统.

2.2. 两个元胞自动机系统的复合

为了研究方便,首先考虑两个元胞自动机系统的复合.

假设 CA_1,CA_2 是两个元胞自动机系统,具有相同的空间维数和有限状态集,它们的全局转换函数分别为 F_1 和 F_2,这样有

定义 3 称

$$C^{(t+1)} = \begin{cases} F_1(C^{(t)}), t = 2k, \\ F_2(C^{(t)}), t = 2k+1, k = 0,1,\cdots, \end{cases} \quad (2)$$

为两个元胞自动机系统 CA_1 和 CA_2 的交叉复合,复合构成的新系统记为(F_1, F_2).

性质 2 由两个有限元胞自动机交叉复合得到的新系统,其前向迭代轨道最终将进入周期轨.

证明 设有两个长度相同的有限元胞自动机 CA_1,CA_2,对应的全局转换函数分别为 F_1,F_2.可构造一个长度相同的新元胞自动机 CA_3,其全局转换函数为 $F_3 = F_2 \circ F_1$,$\circ$表示函数的复合.

从同一个初始构形 C_0 开始,CA_3 的前向迭代轨道为

$$\{C_0, F_2F_1(C_0), F_2F_1F_2F_1(C_0), \cdots\},$$

根据(2)式可得 CA_1,CA_2 交叉复合后新系统的前向迭代轨道为

$$\{C_0, F_1(C_0), F_2F_1(C_0), F_1F_2F_1(C_0), F_2F_1F_2F_1(C_0)\cdots\},$$

可以看出,CA_3 的迭代轨道是由 CA_1,CA_2 交叉复合系统迭代轨道中的偶数步($t = 0,2,4,\cdots$)组成,若能证明 CA_3 的前向迭代轨道最终进入一个周期轨,则交叉复合系统的前向迭代轨道必定也进入一个周期轨,且轨道周期为 CA_3 的两倍.

因为 CA_3 是有限元胞自动机,由性质 1 可知,它的迭代轨道最终将进入周期轨,所以交叉复合系统的前向迭代轨道最终也将进入一个周期轨.

性质 2 表明,交叉复合并没有改变有限元胞自动机系统前向迭代轨道的周期性(如图 2 所示),系统在经历足够的过渡阶段之后,最终进入稳定的周期轨.

定义 4 对任意序列 $R = (r_1, r_2, \cdots) \in \{1,2\}^\infty$,称

$$C^{(t)} = F_{r_t}(C^{(t-1)}), t = 1,2,\cdots \quad (3)$$

为两个元胞自动机系统 CA_1 和 CA_2 在序列 R 下的随机复合,复合构成的新系统记为(F_1, F_2, R).

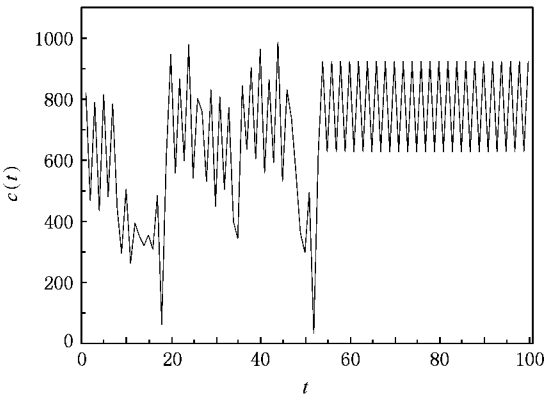


图 2 交叉复合元胞自动机系统的前向迭代轨道($f_1 = 30$, $f_2 = 86$)

随机复合元胞自动机系统是根据随机序列选择迭代函数,因此前向迭代轨道具有不可预测性,即便是对于非随机型边界的有限元胞自动机,也同样可以产生非周期轨道(如图 3 所示),随机复合元胞自动机系统这一特性,适合用于设计序列密码和 Hash 函数.

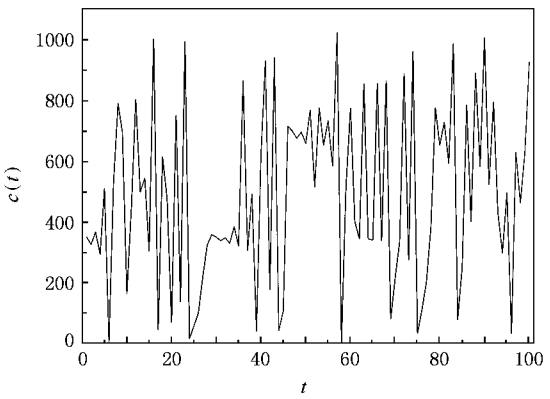


图 3 随机复合元胞自动机系统的前向迭代轨道($f_1 = 30$, $f_2 = 86$)

2.3. 多个元胞自动机系统的复合

定义 5 设 $C^{(t)} = F_q(C^{(t-1)}), q = 0,1,\cdots,k$ 是一组元胞自动机系统,记为$(F_0, \cdots, F_k)$.对任意的序列 $R = (r_1, r_2, \cdots) \in \{0,1,\cdots,k\}^\infty$,称

$$C^{(t)} = F_{r_t}(C^{(t-1)}), t = 1,2,\cdots \quad (4)$$

为元胞自动机系统组在序列 R 下的随机复合,复合构成的新系统记为$(F_0, \cdots, F_k, R)$,其中 R 称为复合序列,$C^{(t)} = F_q(C^{(t-1)}), q \in \{0,1,\cdots,k\}$称为子元

胞自动机系统.

由定义 5 可知，当元胞自动机系统组中只有一个元胞自动机时，复合序列为一固定常数序列，该复合系统就退化为单一的元胞自动机系统；当元胞自动机系统组中只有两个元胞自动机时，该复合系统就是前面提到的两个元胞自动机系统在序列 R 下的随机复合.显然，多个元胞自动机系统的随机复合同样具有良好的密码学性质，并且具有更灵活的参数选择性，可根据需要选择子元胞自动机系统的个数和复合序列的长度.

3. 元胞自动机反向迭代加密技术

3.1. 元胞自动机反向迭代加密原理

元胞自动机的前向迭代是指给定一个 t 时刻的构形 $C^{(t)}$，根据规则计算 $(t+1)$ 时刻的构形 $C^{(t+1)}$，反向迭代是指根据一个 t 时刻的构形 $C^{(t)}$，确定一个可能的 $(t-1)$ 时刻的构形 $C^{(t-1)}$，一般称构形 $C^{(t+1)}$ 为构形 $C^{(t)}$ 的后继，构形 $C^{(t-1)}$ 为构形 $C^{(t)}$ 的前驱.通常，元胞自动机的前向迭代具有确定性，即给定一个初始构形，其前向迭代轨道是唯一的，而元胞自动机的反向迭代轨道并不唯一，因为任何一个构形可以有一个或多个前驱，甚至没有前驱.图 4 描述了元胞自动机的前向迭代和反向迭代过程，从图中可以看出任何一个构形有且只有一个后继，但可能有多个前驱，根据这个特点，若将明文信息编码为系统反向迭代的初始构形，在反向迭代过程中，每次迭代随机选择多个前驱中的一个，那么迭代最终得到的构形就是密文，又因为元胞自动机前向迭代轨道具有唯一性，解密过程中只需将密文编码为系统前向迭代的初始构形，前向迭代与反向迭代相同次数，便能恢复出明文.

利用元胞自动机的反向迭代实现加密，前向迭代实现解密需要保证元胞自动机的任何一个构形至少有一个前驱，但是并非所有元胞自动机都具有此性质.

在文献[7,8]中，均采用了一种特殊的触发元胞自动机(TCA)，取具有触发特性的规则为密钥，实现反向迭代加密技术.下面给出触发元胞自动机的定义：

定义 6　对于系统状态空间 $S=\{0,1\}$ 的二值元胞自动机，如果局部转换函数满足

1) 改变邻域内一个元胞在某个时刻的状态值，保持其他元胞不变；

2) 局部转换函数的输出值反转.

则称之为触发元胞自动机，称该局部转换函数为触发规则.

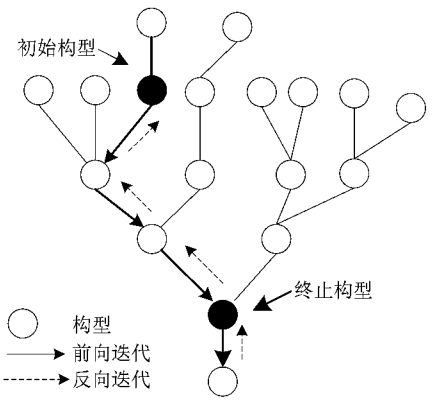


图 4　元胞自动机的前向迭代和反向迭代

具有左触发特性或者右触发的元胞自动机能够快速构造某个构形的前驱，实现元胞自动机的反向迭代，如图 5 所示，规则 30 具有左触发的特性(改变邻域内最左边元胞的状态值，保持其他元胞状态不变，规则输出值反转)，给出 $t-1$ 时刻构形中最右边两个元胞的状态就可以根据规则表以及 t 时刻的构形从右往左计算出 $t-1$ 时刻所有元胞的状态，这个过程称为构造先导状态.

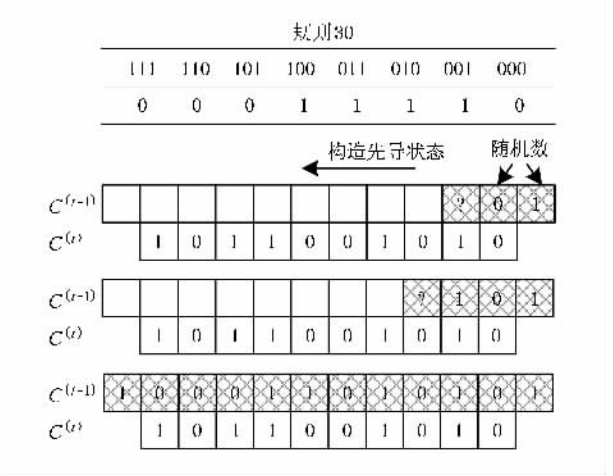


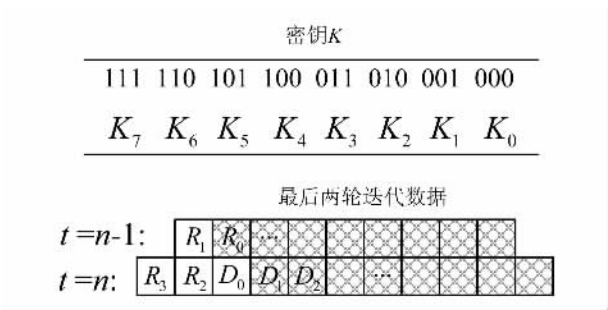
图 5　构造构形 $C^{(t)}$ 的前驱 $C^{(t-1)}$

3.2. 引入随机数对密码系统安全性影响分析

利用动力系统反向迭代加密通常需要引入随机数序列以确定反向路径，由于每次引入的随机数序列不同，使得系统的反向迭代轨道具有不可预测性，攻击者很难得到唯一的明文密文对.但是，引入的随

机数序列对系统的安全性存在隐患,一个典型的例子是文献[9]采用选择明文攻击方法,对一个基于反向迭代混沌映射的密码系统[10]进行了分析.而在基于元胞自动机的反向迭代加密过程中,取触发规则为密钥,每一轮迭代也需要引入 $2r$ 位随机数确定先导状态,因此迭代 n 次共引入 $2rn$ 位随机数,事实上,通过下面的分析可以发现这些随机数应当具有比密钥更高的安全性,必须由系统中专门的随机数发生器产生,即便是系统合法的用户也无法获知每次加密使用的随机数序列.

现在考虑,若随机数序列由每个加密者产生,并作为明文的一部分,则攻击者可进行如下的选择明文攻击,从而恢复密钥($r=1$).



观察最后两轮迭代引入的随机数和最终密文,其中 $D_0=f(R_3,R_2,R_1)$,若令随机数 $R_3=0$,$R_2=0$,$R_1=0$,则由 $D_0=f(0,0,0)=K_0$ 可恢复密钥中的 1 bit,从而攻击者可以通过对(R_3,R_2,R_1)取不同的值恢复整个密钥.

如果随机数序列由系统产生,并对所有使用者保密,则攻击者只能获取密文中的随机数(R_3,R_2),在未知 R_1 的情况下,无法恢复密钥的任何信息.可见,令加密方、解密方以及攻击方都没有权限访问随机数序列,在一定程度上提高了系统的安全性,但系统仍然可能产生某些弱随机数,如全 0 或者全 1 的情况,从而形成安全漏洞,因此有必要采用良好的伪随机数发生器和判断机理,例如文献[11]中提出的一种新型的混沌伪随机数发生器,可作为本文密码系统中的随机数发生器,其优点在于伪随机数发生器的周期长度可准确预测,采用简单算法可有效排除产生短周期的弱密钥,因此能够避免产生某些弱随机数,保证加密系统具有较高的安全性.

4. 复合 TCA 密码系统设计

复合 TCA 密码系统的设计是基于元胞自动机反向迭代加密技术,其安全性能比单一元胞自动机系统更好,下面给出两个复合 TCA 密码系统设计方案.

方案 1 交叉复合 TCA 密码系统

随机选取一个左触发规则 f_L 和一个右触发规则 f_R 构造一个交叉复合元胞自动机系统(F_L,F_R),将明文编码为复合系统的初始状态,取 f_L 和 f_R 共同作为密钥,加密过程为该复合元胞自动机系统的反向迭代过程,奇数轮迭代使用左触发规则 f_L,在数据的最左端添加 $2r$ bit 随机数构造先导状态,偶数轮迭代使用右触发规则 f_R,在数据最右端添加 $2r$ bit 随机数构造先导状态,迭代最终获得的状态即为密文.解密过程是复合元胞自动机系统的正向迭代过程,以相反的次序使用规则,这就是说在解密第一轮迭代使用加密过程中最后一轮的规则,在解密第二轮迭代使用加密过程中最后第二轮的规则,如此等等.

方案 2 随机复合 TCA 密码系统

假设加密共有 n 轮反向迭代,则随机选取一个左触发规则 f_L 和一个右触发规则 f_R,以及长度为 n 的复合二进制序列 $R=(r_1,r_2,\cdots,r_n)\in\{0,1\}^n$,构造一个随机复合元胞自动机系统($F_L$,$F_R$,$R$),将明文编码为复合系统的初始状态,取 f_L,f_R 和 R 共同作为密钥.新的复合系统在每一轮加密过程中,按照复合序列选择不同的规则,规定若 $r_i=0$,则使用左触发规则,在数据的最左端添加 $2r$ bit 随机数构造先导状态 若 $r_i=1$,则使用右触发规则,在数据最右端添加 $2r$ bit 随机数构造先导状态.解密过程,根据复合序列 R 构造一个新的复合序列 $\tilde{R}=(r_n,r_{n-1},\cdots,r_1)$,也就是说以相反的次序使用规则.对于随机复合元胞自动机系统来说,由于复合序列的随机性,使得规则选择具有一定的随机性,迭代轨道当然也不可预测,破译者即便获得了密钥中 f_L 和 f_R,但因为不知道复合序列,也就无法恢复明文.与交叉复合 TCA 密码系统相比,随机复合 TCA 密码系统具有更高的安全性.

5. 仿真结果与分析

5.1. 加密解密结果

对方案 1 和方案 2 进行仿真实验,取迭代次数 $n=10$,密钥 $f_L=30$,$f_R=90$ 以及方案 2 中的随机复合序列 $R=(1,1,1,0,0,1,0,1,0,1)$.表 1 和表 2 为

交叉复合 TCA 密码系统的加密和解密过程，表 3 和表 4 为随机复合 TCA 密码系统的加密和解密过程.

表 1　交叉复合 TCA 密码系统的加密过程

t	Rule	交叉复合TCA密码系统加密过程
0		1010100100111111001010000100000
1	30	0101011100001001101011111000000
2	90	1110111001010111100010011000000000
3	30	1001100110101010011110000111111111110
4	90	0111100001110111010011010100110010
5	30	1010011111001100110000101011010000110110
6	90	0010000110010110100101011101101111000110
7	30	1110000001110001011010110010100010010000001
8	90	1100101010110000001001000111101111010000000110
9	30	0011010110001111101101111001000100110000000001
10	90	1010010001111110011011011001011111010010101010010

表 2　交叉复合 TCA 密码系统的解密过程

t	Rule	交叉复合TCA密码系统解密过程
0		1010010001111110011011011001011111010010101010010
1	90	0011010110001111101101111001000100110000000110
2	30	1100101010110000001001000111101111010000000110
3	90	1110000001110001011010110010100010010000110
4	30	0010000110010110100101011101101111000110
5	90	1010011111001100110000101011010000110110
6	30	0111100001110111010011010100110010
7	90	1001100110101010011110000111111110
8	30	1110111000101011110001001100000000
9	90	0101011100001001101011110000000
10	30	1010100100111110010100001000

表 3　随机复合 TCA 密码系统的加密过程

t	Rule	随机复合TCA密码系统加密过程
0		1010100100111110010100001000000
1	90	0010001011100110100010101111100
2	90	0000101000110000111010111011001100
3	90	0000010000011111100100011011010010
4	30	1111110111111100100110111010000101101101
5	30	1001001100100111000011001011101010001010
6	90	1000101101010000110101001011100100010100010
7	30	0111110001100000010101101101100111010111000
8	90	0100111000001111111101110001111000110111001111100
9	30	1011010000000100100110011101001110100010000100000
10	90	1101101111111111010000111100100001101111101010000000

表 4　随机复合 TCA 密码系统的解密过程

t	Rule	交叉复合TCA密码系统解密过程
0		1010010001111110011011011001011111010010101010010
1	90	0011010110001111101101111001000100110000000110
2	30	1100101010110000001001000111101111010000000110
3	90	1110000001110001011010110010100010010000110
4	30	0010000110010110100101011101101111000110
5	90	1010011111001100110000101011010000110110
6	30	0111100001110111010011010100110010
7	90	1001100110101010011110000111111110
8	30	1110111000101011110001001100000000
9	90	0101011100001001101011110000000
10	30	1010100100111110010100001000

5.2. 密钥空间分析

单一 TCA 密码系统以触发规则为密钥，邻域半径为 r 的元胞自动机共有 $2^{2^{2r}}$ 个左触发规则和 $2^{2^{2r}}$ 个右触发规则，因此密钥空间为 $2\times 2^{2^{2r}}$；交叉复合 TCA 密码系统中由于交叉使用一个左触发规则和一个右触发规则，它的密钥空间为 $2^{2^{2r}}\times 2^{2^{2r}}$；对于随机复合 TCA 密码系统，密钥空间不仅与触发规则数量有关，还与复合序列 R 有关，若复合序列长度为 n，那么它的密钥空间为 $2^n\times 2^{2^{2r}}\times 2^{2^{2r}}$. 在相同半径情况下，比较上述三个密码系统的密钥空间，结果如表 5 所示.

可以看出在相同半径情况下，复合 TCA 密码系统的密钥空间要远大于单一 TCA 密码系统，因此可以使用较小的规则半径，获得大密钥空间，这样不仅缩小了规则表的存储空间而且减少了元胞更新时的计算量.

表 5　相同半径下的密钥空间比较

密码系统	$r=1$	$r=2$	$r=3$
单一 TCA 的密钥空间	32	1.31×10^5	3.69×10^{19}
交叉复合 TCA 的密钥空间	256	4.29×10^9	3.4×10^{38}
随机复合 TCA 的密钥空间	2.6×10^5	4.4×10^{12}	3.48×10^{41}

5.3. 误差扩散方向比较

在文献[8]中采用了一种实验方法测试明文误差传播过程：随机选取一明文序列，改变明文中的一位，保持密钥不变，得到的密文序列与原明文的加密结果进行逐位比较，相同用‘－’表示，不同则用‘＊’表示. 表 6—8 给出了对三个密码系统的测试结果.

表 6　单一 TCA 密码系统的误差扩散过程

t	Rule	单一TCA密码系统的误差扩散
0		----------*----------
1	30	---------**---------
2	30	---*****-**------------
3	30	***-**-*-*--------------------
4	30	-**-*--*-*----------------------
5	30	--***----*----------------------
6	30	*--*--****----------------------
7	30	-*****-*-**----------------------
8	30	***--*-*-*----------------------
9	30	*-****-*-**----------------------
10	30	*****--***----------------------

表 7　交叉复合 TCA 密码系统的误差扩散过程

t	Rule	交叉复合TCA密码系统的误差扩散
0		----------*----------
1	30	---------**---------
2	90	----------**********--
3	30	---*******-*****-****-*----
4	30	-----**--***--**--**------
5	30	-*****-*---**-***-*-*-*---------
6	90	---**---*-*---*--***-***-*-*---
7	30	--****-----*-----****--***-*-*-*------
8	90	----**-*-*-*******-*****-----*----*---
9	30	***-*-*-*---*******-***-**-*----**-----
10	90	--**-**-****-*-**--**-**-**-******--------

表 8　随机复合 TCA 密码系统的误差扩散过程

t	Rule	随机复合TCA密码系统的误差扩散
0		----------*----------
1	90	----------*-*-*-*-*-*--
2	90	----------*---*---*---
3	90	----------*-*-------*--
4	30	----------**-****-*******----
5	30	------**-*-*-***-*--**-**------
6	90	---------***-***----*-**-**-*---
7	90	----------**-**-----*--*----*----
8	30	----------***--*--------**--*--**------
9	90	----------**-*----------****-*--*-*---
10	30	---***-***-*-**----------***--**--*-*------

从结果可以看出，单一 TCA 密码系统的明文误

差扩散存在单向性,使用左触发规则,误差只向左传播,使用右触发规则,误差只向右传播,导致密文中有很多比特不受明文改变的影响.而复合 TCA 密码系统,是两类不同的触发元胞自动机(左触发和右触发)的复合,因此误差扩散是双向的,密文对初值更加敏感.

5.4. 数据敏感性统计分析

密码系统理想的'雪崩效应'应当是密钥或明文的每一 bit 变化都将引起密文每 bit 以 50% 的概率发生变化.但有时不仅要关注明文变化对密文的影响,而且要关注对中间数据的影响,即研究误差传播的过程,因为元胞自动机系统是一个迭代系统,研究误差传播过程有利于选择密码系统合适的迭代次数.

在初值敏感性实验中,保持密钥不变,对 100 bit 的明文分组,每次改变其一位上的值,计算这两段仅相差 1 bit 的明文在 n 步迭代后差别的比特数,然后对各个明文比特改变情况下的 N 次计算结果求平均值,并最终得到第 n 步迭代后的平均数据位变化率

$$P_n = \frac{1}{L_n N}\sum_{i=1}^{N} B_{n,i} \times 100\%, n \in \{0,1,2,\cdots\}, \quad (5)$$

其中,N 为统计次数,$B_{n,i}$ 为第 n 步迭代,第 i 次测试结果变化的比特数,L_n 为第 n 步迭代总的比特数,在这里 $L_n = L_M + 2rn$,其中 L_M 为明文长度.

图 6 给出了不同迭代步数情况下,平均数据位变化率的分布情况.

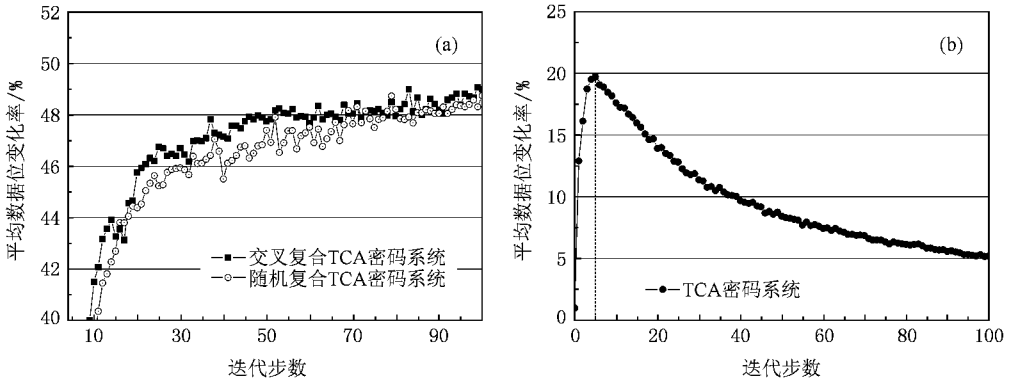


图 6 明文敏感性统计分析 (a) 复合 TCA 密码系统($r = 2$);(b) 单一 TCA 密码系统($r = 2$)

从图 6 可以看到,交叉复合 TCA 在迭代约 50 次之后平均数据位变化率就能达到 48% 以上,非常接近理想的 50%,随机复合 TCA 在迭代约 70 次以后也能达到 48% 以上,两者均具有良好的明文敏感性.而单一 TCA 加密系统最大平均数据变化率只有 20%,并且在迭代 5 步达到峰值之后,呈现递减的趋势,这是因为明文的任何微小改变都不会影响到每一步迭代引入的随机数.

下面对密钥敏感性进行实验,随机选取明文和密钥,然后保持明文不变,每次对密钥进行微小扰动,计算平均数据位变化率,结果如图 7 所示.

实验结果表明,随着迭代步数的增加,复合 TCA 密码系统的平均数据位变化率接近理想的 50%,因此具有良好的抵抗差分分析能力.

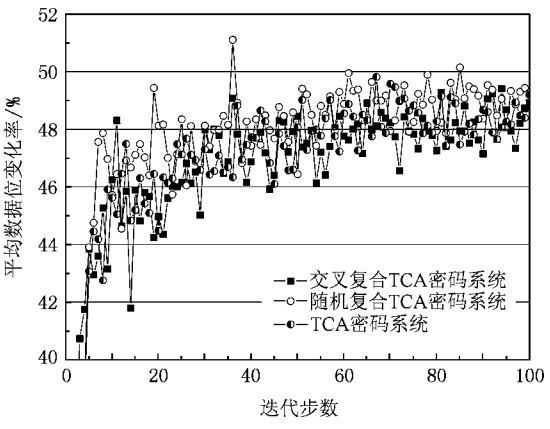


图 7 密钥敏感性统计分析

6. 结　论

本文构建了多种形式的复合元胞自动机模型，利用元胞自动机的反向迭代加密技术，给出了两种基于复合元胞自动机系统的密码构造方案.这两种方案解决了单一元胞自动机加密系统中的误差单向扩散问题，并且可以取较小的规则半径，获得大密钥空间.结果表明，复合元胞自动机系统比单一元胞自动机系统具有更好的密码属性，元胞自动机的复合形式具有十分重要的密码学应用价值，可应用于需要长周期的序列密码和需要良好扩散和扰乱性能的分组密码.

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

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

[3] Zhang C W, Lin L B 2005 *IEEE International Symposium on Communications and Information Technology* 1031

[4] Zhao X L, Li Q M, Xu M W, Liu F Y 2005 *IEEE International Conference on Systems, Man and Cybernetics* 499

[5] Guan P 1987 *Complex System* **1** 51

[6] Mihaljevic M, Zheng Y, Imai H 1999 *IEICE Trans. Fund. Electr.* E82-A 40

[7] 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]

[8] Gutowitz H 1994 Method and Apparantus for Encryption, Decryption and Authentication Using Dynamical Systems USA: 5,365,589

[9] Biham E 1991 *Advances in Cryptology Proceedings of EUROCRYPT '91* 532

[10] Habutsu T, Nishio Y, Sasase I, Mori S 1991 *Lecture Notes in Computer Science, Advances in Cryptology, Proceedings of EUROCRYPT '91* 127

[11] 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]

Encryption based on inverse iterating composition cellular automata system*

Ping Ping†　Zhao Xue-Long　Zhang Hong　Liu Feng-Yu

(*Department of Computer Science and Technology, Nanjing University of Science & Technology, Nanjing* 210094, *China*)

(Received 3 January 2008; revised manuscript received 24 February 2008)

Abstract

The concepts of cross composition cellular automata and random composition cellular automata are introduced, and their feasibility in application to cryptosystem is analyzed. We use the inverse iteration of cellular automata to encrypt, and construct two encryption systems based on composition cellular automata. The new encryption systems effectively solve the problem of one way error diffusion in a single cellular automata system and acquire large key space with small rule radius. Simulation experiment shows that the diffusion and confusion properties of the new composition system are ideal, it resists brute attack and differential cryptanalysis.

Keywords: discrete dynamical system, composition cellular automata, inverse iteration, block ciphers

PACC: 0550

* Project supported by the National Natural Science Foundation of China (Grant No. 90718021).

† E-mail: pingpingnjust@163.com