# 二维可反向迭代细胞自动机在数据加密中的应用

夏学文[1,2] 李元香[3] 曾 辉[2]
(孝感学院计算机与信息科学学院 孝感 432000)[1] (武汉大学计算机学院 武汉 430079)[2]
(武汉大学软件工程国家重点实验室 武汉 430072)[3]

**摘 要** 针对一维触发细胞自动机加、解密速度慢,迭代次数多的问题,提出了一种基于二维触发细胞自动机的数据加密算法。通过邻居细胞间的相互作用与共同演化,反向迭代完成数据加密,正向演化完成数据解密。密钥空间,即反转规则表,随着细胞自动机邻居半径增大呈指数增长,且可以根据不同的安全性要求,通过调整细胞自动机的邻居半径及加密轮次来实现。分析结果表明,该算法可以抵抗蛮力攻击和已知明文、密文以及差分分析攻击,具有较高的安全性。加、解密共享同一硬件结构也使得本算法具有很强的实用性。

**关键词** 触发细胞自动机,数据加密,反转规则
**中图法分类号** TP309 **文献标识码** A

## Data Encryption Algorithm Based on Two Dimension Toggle Cellular Automata

XIA Xue-wen[1,2] LI Yuan-xiang[3] ZENG Hui[2]
(Department of Computer and Information Science, Xiaogan College, Xiaogan 432000, China)[1]
(College of Computer, Wuhan University, Wuhan 430079, China)[2]
(State Key Laboratory of Software Engineering, Wuhan University, Wuhan 430072, China)[3]

**Abstract** A cryptography system based on two dimension toggle cellular automata was proposed to solve the slowness of encryption and decryption based on one dimension toggle cellular automata. The encryption and decryption of data is completed by the co-evolution of the cellular automata. The key space can be adjusted by changing the neighborhood radius and the rounds of encryption. The analysis results show that the cryptosystem can resist brute attack and differential attack, and also has high security. The hardware shared by encryption and decryption made the cryptosystem to have a strong practicability.

**Keywords** Toggle cellular automata, Data encryption, Reversible rule

## 1 引言

近年来,利用细胞自动机(cellular automata,CA)进行密码系统的设计吸引了众多学者,其原因就在于细胞自动机能通过简单的转换规则来实现复杂的行为模式,而且CA中细胞单元并行的简单性及其交互的局部性也使得它易于硬件实现。1985年,Wolfram[1]首次利用细胞自动机来生成密钥流,但该方法有两个弱点:一是生成的密钥流不具有最长周期;二是安全性不够高。此后很多研究表明,可以通过提高细胞自动机结构的复杂性,如提高CA的维数[2,3]或采用动态规则[4]等方法来提高密钥流的周期和安全性(即随机性)。Guan根据复杂系统的多项式方程求逆的困难性,提出了一种基于混合细胞自动机的公钥加密技术[5];S. Nandi提出了利用可编程细胞自动机和群细胞自动机构造序列和分组密码的方法[6],为细胞自动机在密码上的应用开辟了一种新的思想。2002年,Subhayan Sen等人提出了一个新的基于CA的分组密码系统CAC(cellular automata based cryptosystem)[7]。该密码系统是基于两类具有不同周期群的CA。该算法没有像一般分组密码一样采用多轮迭代的方式,而是采用明文在密钥的作用下直接输出密文的方式。2004年,张文涛等人对CAC的一个变形SMCAC进行了分析[8],认为这种SMCA存在明显的缺陷。由此可以看出像CAC这种不采用多次迭代的方式构造的密码算法将使分析变得更简单,攻击起来也相对容易些。2004年,张传武[9]提出了一种基于细胞自动机反向迭代的加密算法,并证明了在明文信息序列中0,1比率为1/2的前提下,该方法具有最大的输出信息熵。而且该算法具有较大的密钥空间和较简单的硬件结构。

本文提出了一种基于二维触发细胞自动机的数据加密算法,该算法较之一维触发细胞自动机加密算法具有更高的并行性,密钥空间及加、解密速度比文献[9]中方法的都有较大的提高。而且分组长度和密钥空间大小可根据用户的不同要求自行设定。

## 2 二维可反向迭代细胞自动机模型

### 2.1 二维反向迭代细胞自动机

到稿日期:2009-04-15 返修日期:2009-06-25 本文受国家自然科学基金(60473014),863计划项目(2007AA01Z290)资助。
夏学文(1974-),男,博士,讲师,主要研究方向为细胞自动机、信息安全、智能计算,E-mail:laughkid@163.com;李元香(1962-),男,博士,教授,博士生导师,主要研究方向为演化算法、并行计算;曾 辉(1980-),男,博士,主要研究方向为智能计算、系统可靠性研究。

二维细胞自动机(2-Dimension Cellular Automata, 2-D CA)是一种时间、空间和状态都离散的动力系统,根据细胞在二维平面上的分布结构,2-D CA 通常可分为三角、四方或六边形三种网格划分,但四方这种网格划分方式更易于用软件模拟和硬件实现,因此应用较为广泛。加之其具有规整、模块化以及内在并行性等特点,使得 2-D CA 尤其适用于密码学。

在 CA 中,有一类具有特性性质的 CA,其细胞单元的转换状态与其领域状态配置中的某个单元的状态值之间存在线性关系,即改变领域状态配置中这一单元的状态值将直接导致转移状态的改变,称该单元为触发细胞,该 CA 采用的规则称为反转规则,这类 CA 称为触发细胞自动机(Toggle CA, TCA)[10]。对于规模为 $M\times N$(即 $M$ 行 $N$ 列)的细胞构成的某二维触发细胞自动机(2-D TCA),若选择单元 $S^t_{i,j+r}$ 为触发单元,则该 CA 的迭代过程可简单描述为:

$$1+S^{t+1}_{i,j}=f(S^t_{i-r,j-r},\cdots,S^t_{i,j},\cdots,1+S^t_{i,j+r},\cdots,S^t_{i+r,j+r})$$
$$0\leqslant i\leqslant M,0\leqslant j\leqslant N \qquad (1)$$

其中,$S^t_{i,j}\in\{0,1\}$ 表示第 $i$ 行 $j$ 列的细胞在 $t$ 时刻的状态,$r$ 为细胞自动机的规则半径,+为异或运算。若 2-D CA 采用 Von-Neumann 邻居方式,即细胞迭代过程中只与其上、左、下、右邻居进行信息传递,则 1-D TCA 的迭代模式可直接扩展到 2-D TCA,因此本文将选用循环边界的 Von-Neumann 邻居方式。根据触发细胞所在位置可分别定义相应的 TCA。表 1 为邻居半径 $r=1$ 时的二维右触发细胞自动机的反转规则表。

表 1 二维右触发细胞自动机

| $S^t_{i,j},S^t_{i-1,j},S^t_{i,j-1},S^t_{i+1,j},S^t_{i,j+1}$ | $S^{t+1}_{i,j}$ | $S^t_{i,j},S^t_{i-1,j},S^t_{i,j-1},S^t_{i+1,j},S^t_{i,j+1}$ | $S^{t+1}_{i,j}$ |
|---|---|---|---|
| 0 0 0 0 0 | 0 | 0 0 0 0 1 | 1 |
| 0 0 0 1 0 | 1 | 0 0 0 1 1 | 0 |
| 0 0 1 0 0 | 1 | 0 0 1 0 1 | 0 |
| 0 0 1 1 0 | 1 | 0 0 1 1 1 | 0 |
| 0 1 0 0 0 | 1 | 0 1 0 0 1 | 0 |
| 0 1 0 1 0 | 1 | 0 1 0 1 1 | 0 |
| 0 1 1 0 0 | 0 | 0 1 1 0 1 | 1 |
| 0 1 1 1 0 | 1 | 0 1 1 1 1 | 0 |
| 1 0 0 0 0 | 1 | 1 0 0 0 1 | 0 |
| 1 0 0 1 0 | 1 | 1 0 0 1 1 | 0 |
| 1 0 1 0 0 | 0 | 1 0 1 0 1 | 1 |
| 1 0 1 1 0 | 1 | 1 0 1 1 1 | 0 |
| 1 1 0 0 0 | 1 | 1 1 0 0 1 | 0 |
| 1 1 0 1 0 | 1 | 1 1 0 1 1 | 0 |
| 1 1 1 0 0 | 0 | 1 1 1 0 1 | 1 |
| 1 1 1 1 0 | 1 | 1 1 1 1 1 | 0 |

### 2.2 反转规则表

利用触发细胞自动机的特性,可以构造任意规则半径的细胞自动机的反转规则表。对于规则半径为 $r$,$S\in\{0,1\}$ 的 2-D CA,其规则表的大小为 $2^{4r+1}$。以二维右触发细胞自动机为例,构造半径为 $r$ 的反转规则表的算法如下。

输入:长度为 $2^{4r}$ 的任意二进制串$(b_{2^{4r}-1},b_{2^{4r}-2},\cdots,b_0)$;

输出:长度为 $2^{4r+1}$ 的反转规则表 $T$:$(t_{2^{4r+1}-1},t_{2^{4r+1}-2},\cdots,t_0)$;

算法:

1. $i=2^{4r}-1$;
2. 若 $b_i=0$,则 $t_{2i}=0,t_{2i+1}=1$;若 $b_i=1$,则 $t_{2i}=1,t_{2i+1}=0$;
3. $i=i-1$;若 $i\geqslant 0$,转 2;
4. 结束。

由反转规则表的构造算法可以知道,对于任意二维触发细胞自动机,可以构造出 $2^{2^{4r}}$ 种不同的反转规则表。

### 2.3 算法描述

2-D TCA 中细胞迭代加、解密过程是 1-D TCA 的加、解密过程在二维上的扩展,现以规模为 $M\times N$ 的二维右触发细胞自动机为例,采用右触发规则进行加、解密,具体算法如下。

加密算法:

1. $i=0$;
2. for ($n=0;n<N;n++$)
   {
   for ($m=0;m<M;m++$)
   $\{S^{t+1}_{m,0}=f_i(S^t_{m,N-1},S^t_{m-1,N-1},S^t_{m,N-2},S^t_{m+1,N-1},S^t_{m,0})$;
   }
   将整个 2-D CA 进行一次整体循环左移;
   };
3. $i=i+1$,若 $i<$Max *Iteration times*, goto 2;
4. 结束。

解密算法:

1. $i=$Max *Iteration times* $-1$;
2. for ($n=0;n<N;n++$)
   {
   将整个 CA 进行一次整体循环右移;
   for ($m=0;m<M;m++$)
   $\{S^{t+1}_{m,0}=f_i(S^t_{m,N-1},S^t_{m-1,N-1},S^t_{m,N-2},S^t_{m+1,N-1},S^t_{m,0})$;
   }
   };
3. $i=i-1$,若 $i\geqslant 0$,goto 2;
4. 结束。

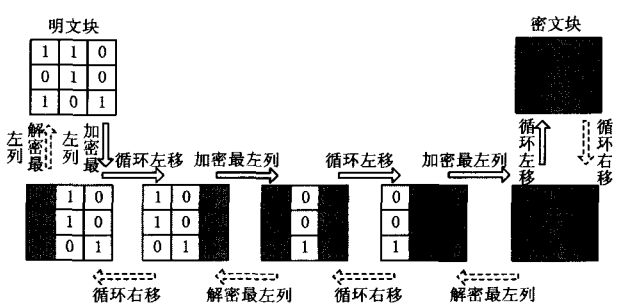
通过对加密、解密过程的比较可以看出,加解密方案只有两点不同:循环移位的方向相反;移位与异或运算的次序不同,加密时是先运算后移位,而解密时是先移位后运算。因此可以将加、解密系统共享一个功能模块,该结构由一个规模为 $M\times N$ 的移位寄存器、$i$ 个反转规则表和 $M$ 个异或运算单元组成。

由于在加密过程中,数据块加密的方向总是和触发细胞的位置保持一致(例如,若触发细胞为右触发细胞 $S^t_{i,j+r}$,则加密是从左至右对明文块进行加密),即密文中信息位总是只与其加密方向上的其它信息位相关。因此为了提高密文中信息位之间的相关性,增强加密系统的安全性,实际应用中每一轮加密应在上、下、左、右 4 个不同方向上选用相应的触发细胞$(S^t_{i-r,j},S^t_{i+r,j},S^t_{i,j-r},S^t_{i,j+r})$和反转规则各进行一次迭代加密。

## 3 仿真实验与安全性分析

### 3.1 仿真实验

为简便起见,下面利用 2-D TCA 对 3×3 规模的明文在一个方向上进行一次迭代加密,迭代所用的右触发规则如表 1 所列。加、解密过程及结果如图 1 所示。




(实线箭头方向为加密,虚线箭头方向为解密)

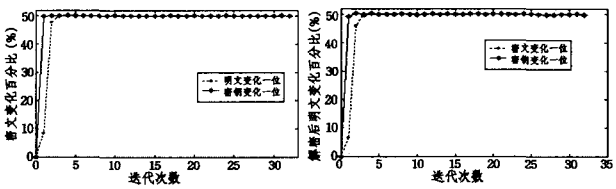
图 1 利用表 1 规则对 3×3 规模的数据进行加、解密的过程

通过图中所示的加、解密过程可以知道,对规模为 $N\times N$

的数据块进行一次迭代加(解)密,需要进行 $N$ 次运算(每次运算包括一次细胞状态的转换和一次移位操作),而利用 1-D TCA 对于同样规模的数据块进行一次迭代加(解)密则需要 $N^2$ 次运算。因此,2-D TCA 大大提高了加(解)密的速度。

### 3.2 安全性分析

分组密码分析中很重要的一项就是研究明文、密文或密钥改变一位后密文的变化情况。一个好的加密系统必须满足"雪崩"效应,即任意改变明文、密文或密钥的一位后,其误差传播应该使得相应的密(明)文变化 50%左右。这样就能有效抵抗差分分析方法的攻击。通过加密算法可以知道,如果改变 $M\times N$ 规模的明文块中第一个待加密列(或行)中的某信息位,则将直接影响本次迭代加密中后续列(或行)的加密效果,因此改变该列(或行)的信息位将具有最好的"雪崩"效应;同理,如果改变离待加密列(或行)最远的列(或行)中的某信息位(不包括参与查表运算的细胞),则在本次迭代加密中只会影响该细胞的加密结果,因而具有最差的"雪崩"效应。为了不失一般性,本文将改变 2-D CA 的中心细胞来对本加密算法进行测试。图 2 给出了不同迭代次数下规模为 320×320 的分组数据在出现单个明文误差、密文误差和密钥误差时的传播情况。




(a)单个明文误差和密钥误差在加、解密时所引起的误差传播　　(b)单个密文误差和密钥误差在加、解密时所引起的误差传播

图 2

反转规则,即密钥是由利用规则生成算法对伪随机数发生器产生的序列得到的。由于反转规则的变化将会影响 2-D TCA 中的所有细胞,即其影响具有全局性,因此密钥的微小变化在 1～2 次迭代后就可以满足"雪崩"效应。而明(密)文,即 TCA 的细胞状态的变化在迭代过程中所产生的影响是局部性的,只有通过多次的迭代,这种影响才能扩散到整个 TCA 中。从图中也可以看出,若要满足"雪崩"效应,明(密)文的改变比密钥的改变需要更多的迭代次数。事实上,由于细胞邻居半径 $r$ 的不同,会使得 CA 的规则表(即密钥)长度也不同。因而随着 $r$ 的不同,单个密钥的不同所产生的误差传播速度也有所不同,即 $r$ 越大,密钥误差传播速度越慢。仿真实验结果表明,对规模为 $N\times N$ 的数据块进行加密时,单个密钥误差约在 $2/r$ 次迭代后传播到整个 TCA,而单个明(密)文误差则需要 $3/r\sim 4/r$ 次迭代后才能传播到整个 TCA。

由于在加密过程中,数据块加密的方向总是和触发细胞的位置保持一致(例如,若触发细胞为右触发细胞 $c^t_{i,j+r}$,则加密是从左至右对明文块进行加密),即密文中信息位总是只与其加密方向上的其它信息位相关。而且为了降低加密系统硬件实现的复杂度,细胞自动机的邻居半径不能选得过大,但较小的邻居半径又达不到安全性的要求。因此为了强化加密时明文信息位之间依赖关系的复杂性,降低硬件成本,增强加密系统的安全性,实际应用中每一轮加密应在上、下、左、右 4 个不同方向上选用相应的触发细胞($c^t_{i-r,j}$,$c^t_{i+r,j}$,$c^t_{i,j-r}$,$c^t_{i,j+r}$)和反转规则($f_1$,$f_2$,$f_3$,$f_4$)各进行一次(或多次)迭代加密。这样,在不增加硬件复杂性的前提下,密钥空间就扩展了 4 倍。而解密时的顺序则完全相反,即从右、左、下、上 4 个方向依次选用相应的触发细胞和反转规则进行解密,这样加密系统的密钥就由这多个规则表共同构成,增加了密钥空间,且细胞自动机的硬件实现也更简单。

在加密和解密过程中,密钥由 CA 系统本身决定。半径为 $r$ 的 2-D TCA 系统有 $2^{4r+1}$ 种状态,同时有 $2^{2^{4r+1}}$ 种规则,由于采用的是两个状态一组的反转规则,因此每个细胞自动机实际的密钥空间有 $2^{2^{4r}}$,表现出指数形式的增长。如果取 $r=2$,则密钥空间可达到 $2^{2^{4r}}=2^{256}\approx 1.158\times 10^{77}$,且当 $r$ 每增加 1 时,密钥空间增加为自身的 16 次方,即 $K_{r+1}=K_r^{16}$。在实际应用中,为了降低硬件复杂度,$r$ 可取较小值,而通过多次迭代后,采用不同的反转规则来加强系统的安全性。对于采用穷举法攻击,如果系统的复杂度按指数形式增长,那么系统实际为有效安全的。由于本加密系统的密钥复杂度呈指数增长,因此采用穷举搜索密钥是不可能的,即系统在计算上是安全的。

**结束语**　本文给出了一种基于 2-D TCA 的数据加密算法,该算法将 Gutowitz 关于触发规则和反向迭代的思想扩展到 2-D CA。由于求解 2-D CA 的逆规则是一个 NP 问题[11,12],因此本算法具有更高的安全性。其加、解密的速度也比文献[9]中的有较大的提升。实验分析结果表明:(1)密钥空间随规则半径 $r$ 的增长呈指数增长,密钥空间大,要求存储量低;(2)具有抵抗穷举法的蛮力攻击和已知明文、已知密文攻击的能力,同时具有抗差分分析的能力;(3)加、解密使用相同的功能模块,从而降低了成本,提高了性能;(4)数据块的大小及迭代时密钥的大小可根据需要动态改变。

## 参 考 文 献


[1] Wolfram S. Cryptography with cellular automata[J]. Advances in Cryptology,1985:429-432

[2] Tomassini M, Sipper M, Perrenoud M. On the Generation of High-Quality Random Numbers by Two-Dimensional Cellular Autoamta[J]. IEEE Trans. on Computer,2000,49(10):1146-1151

[3] Guan Sheng-uei, Zhang Shu, Quieta M T. 2-D CA Variation With Asymmetric Neighborship for Pseudorandom Number Generation[J]. IEEE Trans. on computer-aided design of integrated circuits and systems,2004,23(3):378-388

[4] Guan Sheng-uei, Zhang Shu. An Evolutionary Approach to the Design of Controllable Cellular Automata Structure for Random Number Generation[J]. IEEE Trans. on Evolutionary Computation,2003,7(1):23-36

[5] Guan P. Cellular automata public-key cryptosystem[J]. Complex Systems,1987,1:51-57

[6] Nandi S, Kar B K, Pal P. Chaudhuri, Theory and application of cellular automata in cryptography[J]. IEEE Trans. on Computer,1994,43(12):1346-1356

[7] Sen S, Shaw C, Ray D, et al. Cellular Automata Based Cryptosystem (CAC)[C]//Proceedings of the 4th International Conference on Information and Communications Security. Singapore,2002:303-314


(下转第 60 页)

时，随着负载的增大，端到端时延近似线性增大。由此图可知，在拥塞控制算法的设计中，当根据 $P(A)$ 和 $W_S$ 迭代的 $p$ 结果达到稳定时，可以依据端到端时延 $W_S$ 的增加来探测负载的大小，从而决定是否启动拥塞避免过程。

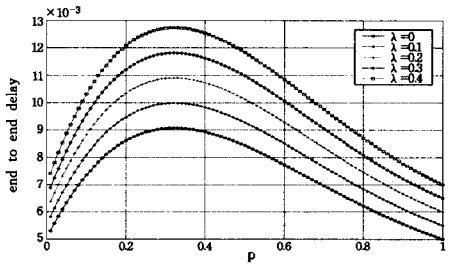



图 3　端到端时延 vs 传输成功概率

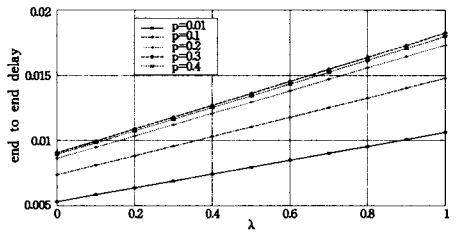



图 4　端到端时延 vs 到达速率

**结束语**　本文从对无线网络拥塞的原理分析出发，针对无线网络信道接入控制特点对网络拥塞与端到端时延、分组交付率以及最大重传次数的关系等方面进行了量化分析，并提出依据这些量化关系进行拥塞控制算法设计的途径、方法和原则。本文所采用的排队模型是理想的无队长限制的 M/G/1 模型，这种模型在节点缓存较大的情况下可适用，但在缓存数量有限的情况下则与实际有较大出入。鉴于此，本文下一步的工作重点将对排队模型作进一步的优化，以构建一种更符合节点实际的数学模型。另外，本文中将 $p$ 和 $\lambda$ 作为独立变量处理，下一步将讨论 $p$ 与 $\lambda$ 的内在联系和量化关系。

## 参 考 文 献


[1] Department of Defense. MIL-STD-2045-47001C[S]. 2002

[2] Das S, Lin Chuang, Ren Fengyuan. Alleviating Congestion Using Traffic-Aware Dynamic Routing in Wireless Sensor Networks [C]// IEEE Communication Society. Sensor, Mesh and Ad Hoc Communications and Networks2008. San Francisco: IEEE Communication Society, June 2008: 233-241

[3] Kang J, Zhang Y, Nath B. Tara: Topology-aware resource adaptation to alleviate congestion in sensor networks [J]. IEEE Trans. on Parallel and Distributed Systems, 2007, 18(7): 919-931

[4] Feng K-T, Hsu Y-P. Cross-layer routing for congestion control in wireless sensor networks[C]// IEEE Communication Society. Radio and Wireless Symposium2008. Orlando, FL: Jan: IEEE Communication Society, 2008: 783-786

[5] Sundaresan K, Anantharaman V, Hsieh Hung-yun, et al. ATP: A Reliable Transport Protocol for Ad Hoc Networks[J]. IEEE Transactions on Mobile Computing, 2005, 4(6): 588-603

[6] Wang Neng-chung, Huang Yung-fa, Liu Wei-lun. A Fuzzy-Based Transport Protocol for Mobile Ad Hoc Networks[C]// IEEE Computer Society. Sensor Networks, Ubiquitous and Trustworthy Computing2008. Taiwan: IEEE Computer Society, 2008: 320-325

[7] Biaz S, Vaidya N. Discriminating congestion losses from wireless losses using interarrival times at the receiver[C]// IEEE Computer Society. Application-Specific Systems and Software Engineering and Technology. Texas: IEEE Computer Society, Mar. 1999: 10-17

[8] Cen S, Cosman P C, Voelker G M. End-to-end Differentiation of Congestion and Wireless Losses[J]. IEEE Trans. on Networking, 2003(10): 703-717

[9] Tobe Y, Tamura Y, Molano A, et al. Achieving moderate fairness for UDP flows by path-status classification[C]// IEEE Communication Society. Proc. 25th Annu. IEEE Conf. Local Computer Networks (LCN 2000). Tampa, FL: IEEE Communication Society, Nov. 2000: 252-261

[10] Gerla M, Sanadidi M Y, Wang R, et al. TCP Westwood: Congestion Window Control using Bandwidth Estimation[C]// IEEE Communication Society. GLOBECOM 2001. San Antonio Texas: IEEE Communication Society, 2001: 1698-1702

[11] Medidi M, Wang Jiong, Garudapuram G, et al. An Analytical Model and Performance Evaluation of Transport Protocols for Wireless Ad Hoc Networks[C]// IEEE. ANSS 2008. Ottava Canada: IEEE, April 2008: 131-138

[12] Hu Wenbin, Zhang Deingyi, Lin Fu. An improved TCP congestion control mechanism based on double-windows for wireless network[C]// IEEE. ISWPC 2008. Santorini Greece: IEEE, 2008: 504-507

[13] Dai J-W, Chiang L-F. Hierarchical wireless mobile MPLS mechanism using foreign tracking agent based on M/G/1 with capacity c queueing model[J]. Communications, IET, 2007, 1(5): 903-908


(上接第 48 页)


[8] 张文涛，卿斯汉，吴文玲. 对一个基于细胞自动机的分组密码分析的分析[J]. 软件学报，2004，15(5)：767-771

[9] 张传武，沈野樵，彭启宗. 细胞自动机反向迭代加密技术研究[J]. 计算机学报，2004，27(1)：125-129

[10] Gutowitz H, Victor J D, Knight B W. Local structure for cellular automata[J]. Physica D, 1987, 28: 18-48

[11] Kari J. Reversiblity of 2 D cellular automata is undecidable [J]. Physica D, 1990, 45(1-3): 379-385

[12] Kari J. Reversibility and surjectivity problems of cellular automata[J]. Journal of Computer Systems Sciences, 1994, 48(1): 149-182