学 术 论 文

二维可控细胞自动机伪随机序列发生方法研究

朱保平，马　骞，刘凤玉
（南京理工大学计算机科学与技术学院，南京　210094）

［摘要］　提出了一种新的细胞自动机——二维可控细胞自动机。根据二维可控细胞自动机的性质，提出了一种具有梯型结构的二维可控细胞自动机的伪随机序列发生方法。计算机模拟表明，具有梯型结构的二维可控细胞自动机伪随机序列发生器实现简单，产生的序列具有速度高、统计特性好等优点。新的细胞自动机在对称密码学中有广泛地应用。

［关键词］　细胞自动机；伪随机序列发生器；可控；密码学
［中图分类号］ TP309.7　　［文献标识码］ A　　［文章编号］ 1009－1742（2007）06－0043－05

1　引言

伪随机序列发生器广泛应用于序列密码等领域，序列密码的关键问题是产生较长的不可预测的密钥序列。由于真随机序列只能来自于自然现象，在实际应用中生成相当困难，因此采用人工方法生成的伪随机序列被广泛地应用。目前广泛使用的是基于同余和线性反馈移位寄存器的伪随机序列发生器，线性反馈移位寄存器方法适合硬件实现，但是在 VLSI 实现中很难模块化，而线性同余产生方法的主要问题在于不适合硬件实现，获取速度有一定限制，而且同余发生器在密码学中并不适用[1,2]。

1985 年 Wolfram 首次提出了基于一维细胞自动机的伪随机序列[3]，并将它应用于序列密码。文献[3]证明了该随机序列发生器优于其他广泛使用的随机序列发生器如基于同余和线性反馈移位寄存器的伪随机序列发生器。近 10 年来，M. Tomassini 和 Kokolakis 等人对一维细胞自动机伪随机序列发生器进行了广泛地研究[4,5]，目前主要集中于二维细胞自动机伪随机序列发生器的研究。笔者提出了一种新的二维梯形可控细胞自动机伪随机序列发生器，该发生器具有实现简单，统计特性好等优点。

2　二维梯形可控细胞自动机的构造

2.1　二维梯形细胞自动机模型

细胞自动机是一组具有一定状态的细胞单元组成的阵列，细胞的阵列是 n 维的，在实际的应用中 $n=1, 2, 3$。一维细胞自动机是在无限延伸的直线上分布，而二维细胞自动机是在二维欧几里德平面上进行分布，那么由多个一维细胞自动机组合，并且通过一定的关系将它们联系起来构成空间网状结构的细胞自动机就是二维细胞自动机。Von Neumann 型和 Moore 型以及它们的扩展是常见的二维模型，但是这些模型都有较多的邻居细胞而结构复杂。笔者对已有的二维细胞自动机模型分析后，提出一种新的二维梯形细胞自动机模型，在这种邻居模型内中心细胞的邻居成梯状分布，分为左向分布和右向分布 2 种二维梯形细胞自动机模型。图 1 给出了邻居半径 $r=1$ 的 2 种二维梯形细胞自动机模型。如果将模型的细胞空间视为由众多一维细胞自动机的细胞空间组合而成，那么在某个时刻中细胞状态的演化将不仅仅依赖于自身细胞自动机中的细胞，而是更多地被其他的细胞自动机所影响，细胞状态演化的比一维细胞自动机更加具有不可预测

［收稿日期］　2006－09－18；修回日期　2006－11－14
［作者简介］　朱保平（1964－），男，江苏常州市人，南京理工大学副教授，主要研究方向为信息安全与理论

性，同时二维结构也较之一维结构来说具有更好的复杂度。另一方面，模型的细胞邻居选取时滤去某些方向上的细胞，使得邻居细胞的数量适量下降，计算量更接近于一维细胞自动机，同时又便于进一步的扩展。新模型具有二维细胞自动机结构的复杂度，而它的计算复杂度却接近于一维细胞自动机。

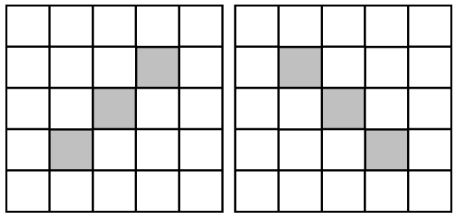

图 **1** 二维梯形细胞自动机模型

Fig.1 Model of two-dimensional trapezoidal CA

2.2 可控细胞自动机

定义 1 如果一个 CA 的一些细胞可被细胞控制信号所控制，该 CA 称为可控细胞自动机（CCA，controllable CA）[6]。

定义 2 如果一个细胞受细胞控制信号控制，该细胞称为可控细胞，否则称为基本细胞。CCA 是可控细胞和基本细胞的组合。针对图 2 显示的二维梯型可控细胞自动机模型，可控细胞受细胞控制信号控制。可控细胞可以在二维细胞空间中随机选取，图 3 中灰色细胞就是随机选择的可控细胞。

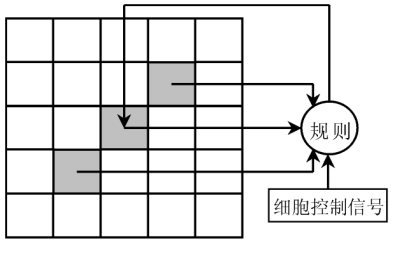

图 **2** 二维梯形可控细胞自动机模型

Fig.2 Model of two-dimensional trapezoidal controllable CA

在细胞自动机中，细胞应该按照相应的状态转移规则进行演化。由于细胞控制信号的存在，不同的规则在不同的时步可以在相同的细胞上实施，这样就增加了细胞自动机开放的、动态的不可预测性。

2.3 状态转移规则的构造

针对细胞空间中的基本细胞和可控细胞分别建立状态转移函数。在梯型邻居模型中细胞自动机中

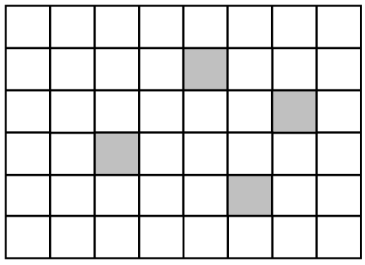

图 **3** 可控细胞的选择

Fig.3 Choice of controllable cell

细胞的状态转移规则的一般表达形式为

$$s_{i,j}^{t+1} = f_{i,j}(s_{i-r,j+r}^{t}, s_{i-r+1,j+r-1}^{t}, \cdots, s_{i,j}^{t}, s_{i+1,j-1}^{t}, \cdots, s_{i+r-1,j-r+1}^{t}, s_{i+r,j-r}^{t}) \quad (1)$$

图 4 和图 5 给出了基本细胞和可控细胞在二维梯形可控细胞自动机模型中的计算框图。

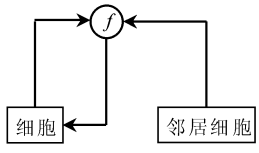

图 **4** 基本细胞的计算框图

Fig.4 Calculation chart of basic cell

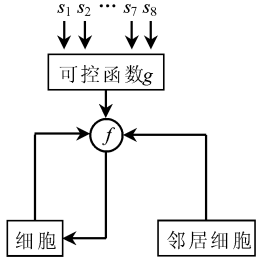

图 **5** 可控细胞的计算框图

Fig.5 Calculation chart of controllable cell

可控函数 g 定义为

$$s = g(s_1, s_2, \cdots, s_8) \bmod 2 \quad (2)$$

其中 $s_i(i = 1, 2, \cdots, 8)$ 是细胞自动机在同一时步从细胞空间中随机选取的 8 个细胞的状态，由它们的状态组合决定可控细胞是否按照规则进行演化。式（2）的作用是将随机选出的 8 个细胞的状态所构成的位串序列对应的二进制数转化为十进制数。当 $s=0$ 时，可控细胞在该时步的演化中保持状态不变；当 $s=1$ 时，可控细胞将按其固有的规则进行状态演化。考虑到计算复杂性会随着细胞自动机的邻居半径的增加而呈指数级增长，取邻居半径 r

=1，状态空间 $s=\{0,1\}$。这样可对式（1）进行简化，得转换规则为

$$s_{i,j}^{t+1}=f_{i,j}(s_{i-1,j+1}^{t},s_{i,j}^{t},s_{i+1,j-1}^{t}) \tag{3}$$

为便于说明，根据二维梯形邻居模型的特点，采用与基本细胞自动机相似的编号方法对普通细胞的转态转移规则进行编号，细胞状态取 0 或 1，$l_7=f(111)$，…，$l_1=f(001)$，$l_0=f(000)$，邻域状态映射的组合 $\sum_{i=0}^{7} l_i 2^i$ 计算出十进制数就是自动机规则的编号。

3　二维梯形可控细胞自动机伪随机序列发生器

二维梯形可控细胞自动机伪随机序列发生方法是基于图 6 所示的二维网格，由 n 行和 m 列组成，采用循环边界条件，初始时在细胞空间中任意选取若干细胞作为可控细胞（图 6 中灰色细胞）。可控的二维细胞自动机模型在有 N 个细胞的细胞空间中进行迭代演化，将细胞空间中的细胞按矩阵方式编号并进行分组，每组 3 行，同行的细胞使用相同的转移规则，不同行的选择不同的规则。每个时步迭代结束后从 N 个细胞中选取 M 个细胞作为一组 0，1 位串序列输出，构成期望长度的伪随机数。所用转换规则 f，g，h 分别取规则 105，150，165，基本细胞的演化函数为

$$\begin{aligned} C_2^{t+1}&=f(C_1^t,C_2^t,C_3^t),\\ C_3^{t+1}&=g(C_2^t,C_3^t,C_4^t),\\ C_4^{t+1}&=h(C_3^t,C_4^t,C_5^t) \end{aligned} \tag{4}$$

可控细胞的转换函数为

$$C_3^{t+1}=\begin{cases} f(C_2^t,C_3^t,C_4^t) & \text{当 } s=1\\ C_3^t & \text{当 } s=0 \end{cases} \tag{5}$$

其中 s 由式（2）计算得到。

4　实验数据分析

伪随机序列发生器在使用前应经过统计测试。采用两种测试方法：**a**. 利用 George Marsaglia 开发的伪随机数测试软件包 Diehard 进行测试；**b**. 采用美国联邦信息处理标准[7]公布的加密模块指定的伪随机数统计测试方法。

4.1　Diehard 测试

用 George Marsaglia 开发的伪随机数测试软件包 Diehard 对二维梯形可控细胞自动伪随机序列发生器（2DTCCA）进行一系列的测试，并与移位寄存器随机序列发生器（shift register generator）、同余发生器（congruence generator）进行对比分析。从表 1 的测试结果可见，2DTCCA 随机序列发生器要优于常用的移位寄存器发生器和同余发生器。

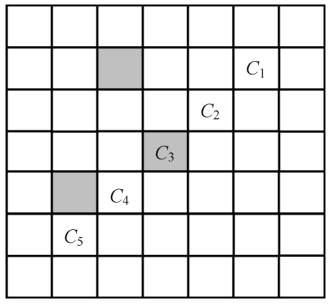

图 **6**　二维梯形可控细胞自动机阵列图

Fig.6　Display chart of two-dimensional trapezoidal controllable CA

表 **1**　**2DTCCA** 与其他发生器的测试结果

Table 1　Test results of 2DTCCA and other generator

Test mane	2DTCCA	Shiftregister	Congruence
Birthday spacings	√	√	√
Overlapping perm	√	×	×
Ranks of 31×31	√	×	√
Ranks of 32×32	√	×	√
Ranks of 6×8 matrices	√	×	×
The bit stream test	√	×	×
Monkey tests	√	×	×
Count the 1s in a stream of	√	×	×
Count the 0s in a stream of	√	×	×
Parking lot test	√	√	×
Minimum distance	√	√	×
Random spheres test	√	√	√
The squeeze test	√	√	×
Overlapping sums test	√	√	√
Run test	√	√	×
The craps test	√	√	×

√ means pass，× — means fail

4.2　随机统计测试

采用美国联邦信息处理标准公布的加密模块指定的伪随机数统计测试方法：任何伪随机数发生器产生的 20 kb 伪随机序列经单比特、扑克、游程和自相关的 4 项基本测试，若有一个测试没有通过，则没有通过 FIPS 的随机性测试。采用 105，150，

165 规则的组合，在可控细胞数量为 3 的条件下产生测试序列。测试所需的 20 kb 使用如下方法产生：二维梯形可控维细胞自动机模型在 300 个细胞组成的细胞空间中进行迭代演化，从每次迭代后的 300 个细胞中抽取 50 个细胞作为输出，进行 400 时步的连续迭代，产生 20 kb 伪随机序列构成测试所需要的样本，实验 80 次。图 7 至图 12 为输出序列的伪随机统计特性对比。

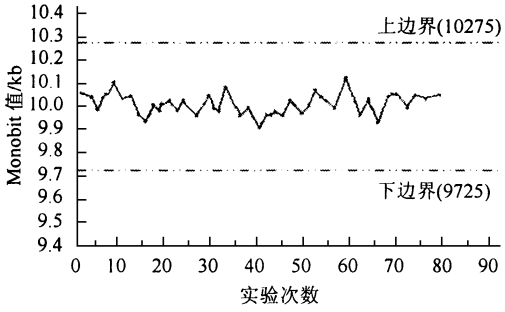

图 **7** **1** 的单比特测试结果

Fig.7 Result of 1's monobit test

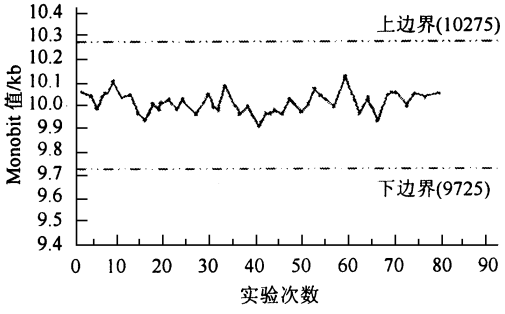

图 **8** **0** 的单比特测试结果

Fig.8 Result of 0's monobit test

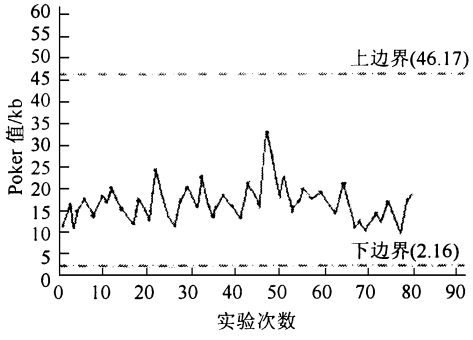

图 **9** 扑克测试结果

Fig.9 Result of poker test

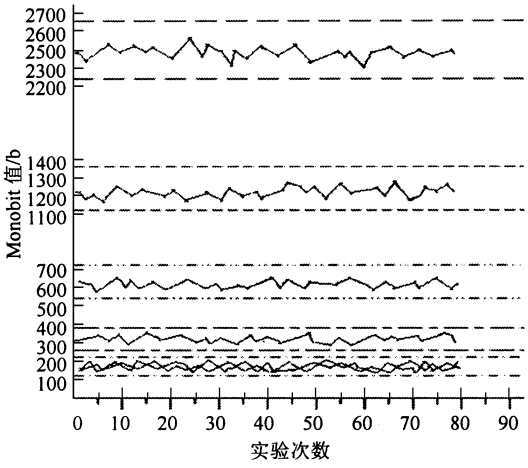

图 **10** **1** 的游程测试结果

Fig.10 Result of 1's runs test

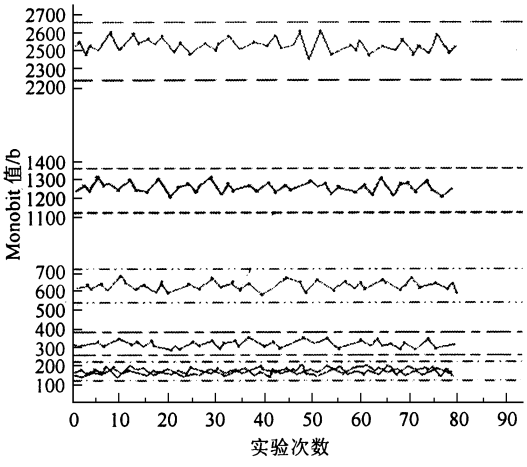

图 **11** **0** 的游程测试结果

Fig.11 Result of 0's runs test

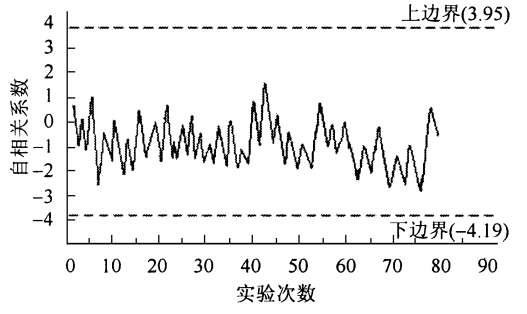

图 **12** 自相关测试结果

Fig.12 Result of Self-relevance test

5 结语

构造的基于二维梯形可控细胞自动机的伪随机

序列发生器，结构规则简单，易于 VLSI 实现。计算机模拟表明该随机序列发生器能产生通过所有测试的高质量伪随机数，该发生器优于其他相关的伪随机序列发生器，能快速地产生伪随机序列，便于计算机硬件实现，这种新的细胞自动机在对称密码学中有广泛应用。

参考文献

[1] Schneier B. 应用密码学 [M]. 吴世忠，祝世雄，张文政译. 北京：机械工业出版社，2000. 293～297

[2] 赵学龙，王庆梅，许满武，等. 基于一维扩展元胞自动机的伪随机数发生器研究 [J]. 计算机科学，2005，32(4)：137～139

[3] Wolfram S. Cryptography with cellular automata [A]. Advances in Cryptology'85，Proceedings LNCS 218，Springer 1986. 429～432

[4] Tomassini M，Sipper M，Zolla M，et al. Generating high-quality random numbers in parallel by cellular automata [J]. Future Gener Comput Syst 1999，16：291～305

[5] Kokolakis I，Andreadis I，Tsalids Ph. Comparison between cellular automata and linear feedback shift registers based pseudo-random number generators [J]. Microprocess Microsyst，1997，20：643～658

[6] Guan Shenguei，Zhang Shu. Pseudorandom number generation based on controllable cellular automata [J]. Future Generation Computer Systems，2004，20：627～641

[7] FIPS. FIPS140-2：Security Requirements for ryptographic Modules [S]. http://csrc. nist. gov/publications/fips/fips140－2/fips1402.pdf，2001

Two-dimensional Controllable Cellular Automata Based Pseudo Random Bit Sequence Generator

Zhu Baoping，Ma Qian，Liu Fengyu

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

[**Abstract**] A novel cellular automata (CA)—two-dimensional controllable CA—is proposed in this paper. According to characteristics of two-dimensional controllable CA，a pseudo random generating method based on two-dimensional controllable CA with a trapezoidal structure is presented. Simulation demonstrates that pseudo random bit sequence generator based on the two-dimensional controllable CA with a trapezoidal structure is easily implemented，and can generate high speed bit sequence and excellent statistical properties. This novel CA is widely used in symmetrical cryptography.

[**Key words**] cellular automata；pseudorandom number generators；controllable；cryptography