一个用简单物理模型构建的加密系统*

周 庆† 陈 钢 胡 月

(重庆大学计算机学院,重庆 400044)

(2010 年 6 月 20 日收到;2010 年 7 月 12 日收到修改稿)

一些简单的物理模型可产生复杂的行为,并有很强的逻辑表达能力. 基于旋转元器件和格子气两个物理模型设计了一个加密系统,具有可逆、并行、简单、高效的特性. 实验结果证实该系统具有良好的随机性和敏感性. 研究结果表明,采用简单物理模型构建加密系统是一种很有潜力的方法.

关键词: 物理模型, 加密系统, 并行, 效率

PACS: 47.11.Qr, 89.20.Mn, 89.20.Ff

1. 引 言

可逆性,并行性和随机性是自然界中普遍存在的物理性质,这些性质启发人们利用物理模型设计高性能的加密系统. 目前,用于加密的最常见物理模型是混沌系统,如基于混沌系统设计的对称加密系统[1],Hash 函数[2]和随机数产生器[3]. 混沌系统具有很高的初值和系统参数敏感性,这是其用于设计密码系统具有的优势. 然而,基于混沌的加密系统也存在以下不足:

不可逆:混沌系统是不可逆的,因此混沌系统在加密应用中实质仅起流密码的作用,其应用场景受到一定限制;

效率低:基于混沌系统的加密算法通常需要进行多次迭代,每次迭代又涉及较多的乘除法运算,这大大降低了加密效率;

难以并行化:基于混沌的加密系统,为了实现扩散,在加密当前分组时需先加密前一分组,从而使整个加密难以并行运行[4]. 随着分布式技术与多核技术的发展,并行计算已成为趋势,因此现代加密系统应能很好地支持并行化计算.

事实上,一些简单的物理模型被证明具有逻辑普适性(logical universality, LU),如旋转元器件(rotary element, RE)和撞球模型(billiard ball Model, BBM)等. 这说明某些简单物理模型具有强大的计算功能,通过精心构造和测试有可能设计出高性能的加密系统. 本文提出了一个基于简单物理模型的加密系统,其设计目标如下:

1)可逆:系统的所有加密操作均是可逆的;

2)简单:系统加密操作的原理和实现方法简单;

3)高效:系统加密操作在计算机或数字电路上能高速运行;

4)并行:系统加密支持高度并行化运算;

5)安全:系统应具很高的随机性和敏感性.

2. 两个简单物理模型

本文提出的加密系统主要基于 RE 和 HPP 两个简单物理模型,下文首先介绍这两个模型,然后描述它们在计算机或数字电路上的实现方法.

2.1. RE 模型

RE 模型是 Morita 提出的一个简单系统[5],由挡板、球,四个入口和四个出口构成(参见图 1). 挡板有水平和竖直两个状态,入口和出口则有东、南、西、北四个方向. 球进入入口后若与挡板发生碰撞,则挡板和球的方向同时发生改变. 例如,球从北边进入系统,遇到水平的挡板,则球从西边离开系统,同时挡板变为垂直方向. 表 1 列出了各种情况下系统的变化.

* 国家自然科学基金(批准号:61003246,61003256),重庆市自然科学基金(批准号:CSTC2009BB2208)资助的课题.

† E-mail:tzhou@cqu.edu.cn

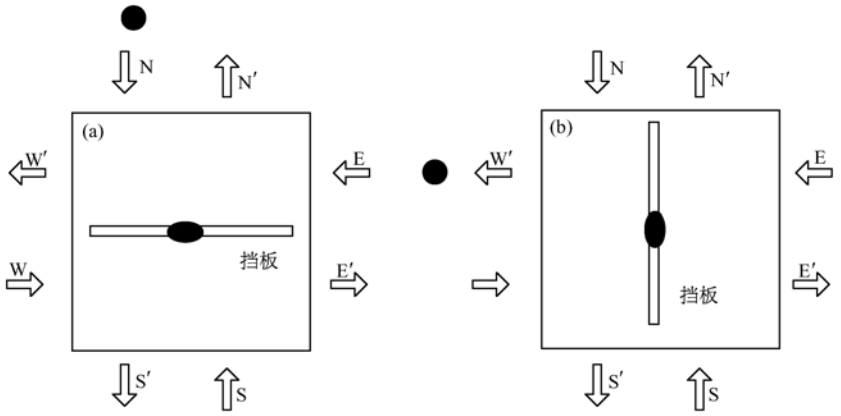

图 1 RE 模型示例 (a)碰撞前系统状态;(b)碰撞后系统状态

尽管系统非常简单,Morita 证明该元器件可组合成任意的逻辑函数,故 RE 模型具有逻辑普适性[5]. RE 模型也是可逆的,即已知球离开系统时各组件的状态,可唯一确定球进入系统前各组件的状态.

表 1 RE 模型中不同情况下挡板和球的变化

挡板方向	球的进入方向			
	n	*e*	*s*	*w*
—	|*w*′	—*w*′	|*e*′	—*e*′
|	|*s*′	—*n*′	|*n*′	—*s*′

2.2. HPP 模型

HPP 模型是 Hardy, Pazzis 和 Pomeau 提出的一个格子气(lattice gas)模型,可以较好地模拟流体运动[6]. HPP 模型由矩形排列的格点构成,每个格点上有 0 至 4 个粒子,其运动方向不同,为东、南、西、北四个方向之一(参见图 2). 每个格点上进行两阶段的变换:碰撞和平移. 在碰撞阶段,若某格点上恰有 2 个粒子,且方向相反,则两个粒子的方向各自右旋 90 度(例如两个南北方向的粒子碰撞后各自变为东西方向);其他情况下各粒子方向保持不变. 在平移阶段,各粒子按各自方向平移到相邻格点.

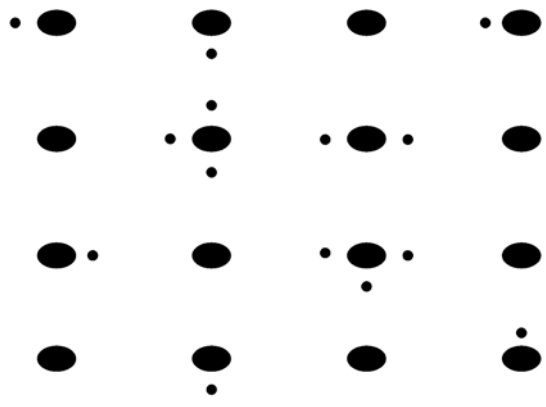

图 2 一个 4×4 格点阵列 HPP 模型示例

HPP 模型具有良好的敏感性,即一个粒子的轻微变化会影响所有其他粒子的状态. 显然,HPP 模型也是可逆的.

2.3. 模型的算法实现

为了在计算机或数字电路上运行,需要将以上物理模型用算法进行描述.

2.3.1. RE 模型的算法实现

可用一个五元组 RE(E,S,W,N,*L*)描述 RE 系统的状态. 其中 E,S,W,N 表示在东、西、南、北方向上是否有球;*L* = 0 表示挡板为水平方向,*L* = 1 为竖直方向. 例如 RE(1,0,0,1,0)表示在东和北两个方向上有球,而挡板是水平的. 在下文中,用$(10010)_2$的十进制数 18 简化表示 RE(1,0,0,1,0).

表 1 定义了仅有一个球时系统的反应,然而在本文提出的加密系统中,RE 模型可能存在 0 至 4 个球. 为此,制定以下规则:

1)系统恰有 1 个球时,按系统状态按表 1 转换;

2)系统恰有 3 个球时,转换后的系统状态与缺少的一个球相反(例如系统在东西南三个方向上有球,其系统状态与仅有北方向的球是相反的);

3)其他情况下,系统状态保持不变.

根据以上规则和表 1,可获得多个球进入 RE 系统的状态转换表(参见表 2).

因此,RE 模型可用查表操作实现.

2.3.2. HPP 模型的算法实现

用四元组 HPP(E,S,W,N)描述一个格点在东、西、南、北方向上是否有粒子存在.(与 RE 模型类似,在下文中用十进制简化表示格点状态.)

碰撞阶段的格点的状态变化由表 3 给出.

表 2 多球情况下的 RE 模型的状态转换表(状态用十进制数表示)

原状态	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
新状态	0	1	5	9	16	8	6	7	17	3	10	11	12	13	27	29
原状态	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
新状态	4	2	18	19	20	21	14	28	24	25	15	23	26	22	30	31

表 3 HPP 模型碰撞阶段的状态变化表(状态用十进制表示)

原状态	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
新状态	0	1	2	3	4	10	6	7	8	9	5	11	12	13	14	15

在平移阶段,将整个 HPP 系统用四个矩阵表示,分别对应四个方向. 矩阵的每个元素等于 0 或者 1,表示该格点在该方向上是否有粒子存在. 平移意味着对四个矩阵的元素进行移位(在本文中,规定矩阵的最后一行(列)与第一行(列)相邻). 例如,对应东方向的矩阵元素应全体向右移动 1 列(最后一列移动到第一列). 对应西、南和北方向的矩阵则全体向下、向左和向上移动一行或一列.

综上所述,HPP 模型可通过查表操作和移位操作实现. 此外,在碰撞和平移阶段,各元素的操作均可并行实现.

3. 加密算法设计

本节基于前面两个模型提出一个加密算法,明文排列成 m 行 n 列的矩阵,每个元素(分组)的长度为 5 bit.

3.1. 加密流程

加密流程如下:

1)每个元素看作一个 RE 系统(各元素的 5 bit 分别对应 RE 系统的 E,S,W,N,L 分量),各 RE 系统并行工作.

2)用轮密钥 K 改变各元素的 L 分量. 若元素对应的轮密钥位为 0,L 不变;否则对 L 求反(等价于将挡板旋转 90°).

3)将整个矩阵看作一个 HPP 系统进行变换(各元素前 4bit 分别对应 HPP 格点的 E,S,W,N 分量).

4)返回第 1 步继续下一轮加密,或者结束加密.

3.2. 轮密钥产生算法

在加密流程的第 2 步使用了轮密钥来改变各元素的 L 分量,因此每轮需产生 $m \times n$bit 的轮密钥. 这里我们使用二维混沌耦合映象格子模型来生成轮密钥. 在该模型中,每个格点并行作混沌迭代,再与相邻格点进行耦合(耦合系数为 μ)(参见图 3). (1)式给出了第 i 行第 j 列格子值 $x_{i,j}$的变化公式

$$F(x_{i,j}) = (1 - M\mu)f(x_{i,j}) + \sum_{x \in N(x_{i,j})} \mu f(x), \quad (1)$$

其中 $N(x_{i,j})$ 表示 $x_{i,j}$的全体相邻格点,M 表示相邻格点的个数,根据格点位置的不同,其值可能等于 2,3 或 4. f 为 logistic 函数,由(2)式定义.

$$f(x) = 4x(1 - x). \quad (2)$$

每轮迭代后 $x_{i,j}$的值介于 0 到 1 之间,若 $x_{i,j} > 0.5$,则对应格点的轮密钥等于 1,否则等于 0,由此每轮可产生 $m \times n$bit 的密钥.

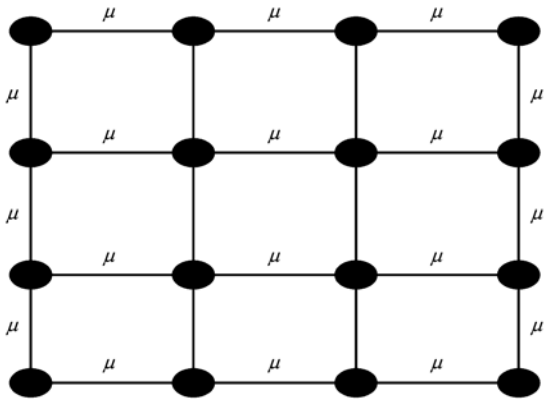

图 3 一个 4×4 的混沌耦合映象格子示例

系统各格点的初值由 128 bit 的外部密钥确定. 首先将 128 bit 分成 4 组,每组 32 bit. 然后按(3)式将每组转换为一个介于 0 和 1 之间的数.

$$h(k) = \sum_{i=1}^{32} 2^{-i} k_i, \quad (3)$$

其中 k_i 表示 k 的第 $i$bit. 由(3)式将 4 组 32 bit 转换成 4 个数 A, B, C, D,再由(4)式确定全体格点的初值.

$$x_{i,j} = \frac{Ai + B(n - i) + Cj + D(m - j)}{m + n}. \quad (4)$$

轮密钥各比特的产生可并行进行,但轮密钥产生过程不是可逆的.

4. 性能分析

本节对第 3 节提出的算法的性能进行分析,检查其是否满足我们在第 1 节中设定的目标.

1)可逆

加密包括三个过程,其中 RE 模型和 HPP 模型都是可逆的,根据轮密钥旋转挡板也是一个可逆过程. 因此整个加密过程是可逆的,从而使解密方可正确解密. (注意,尽管轮密钥的产生过程是不可逆的,但在加密方和解密方共享 128 bit 的外部密钥,因此加密和解密方可产生相同的轮密钥.)

2)简单

RE 模型和 HPP 模型的原理和实现都非常简单,根据轮密钥旋转挡板也是简单操作.

3)高效

整个加密算法在实现时仅包含查表、移位和异或运算,均可用软件或数字电路快速实现. 仅轮密钥的产生涉及乘法运算,但每轮每个元素只需 1 次乘法. 总体而言,加密系统的运算效率较高.

4)并行

矩阵的各个元素在系统的 4 个过程(即 RE 模型、挡板旋转、HPP 模型以及轮密钥产生)均可并行运算,对于一个含 $m \times n$ 个元素的系统而言,加密时间可减少 mn 倍,可见系统的并行性很高.

5)安全

HPP 模型具有很高的敏感性,而 RE 模型和轮密钥的生成提高了系统的随机性. 实验结果证实了系统的随机性和敏感性.

综上所述,该系统实现了第 1 节中提出的 5 个目标.

5. 实验结果

实验主要检测加密系统的随机性和敏感性. 明文选用 128×128 的 Lena 图像,仅加密每个像素的前 5 个 bit. 密钥随机选择为 0xccbe6e9fa78da7f4bca76da24595350f,耦合参数 μ 设为 0.00001,加密轮数设为图像边长的 2 倍,即 256 轮.

5.1. 随机性检测结果

5.1.1. 直方图

直方图表示图像像素值的分布. 随机性好的密文其直方图应是均匀的. 图 4 说明加密后密文的分布是均匀的.

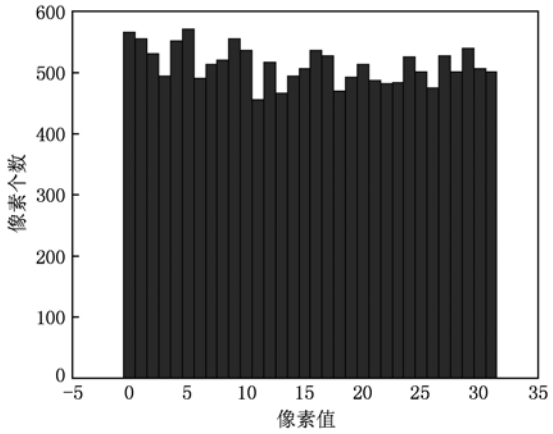

图 4 密文直方图

5.1.2. 相关性检测

图像相邻像素间有很强的相关性,好的加密算法应去除这种相关性. 表 4 列出了加密前后随机选择的不同方向上 1000 对相邻像素的相关系数. 由表 4 可以看出相邻密文像素的相关性很低.

表 4 明文和密文图像中相邻像素的相关系数

	明文	密文
水平	0.9578	0.0228
竖直	0.9164	−0.0083
对角	0.8850	0.0301

5.2. 敏感性检测结果

5.2.1. 明文和密钥的敏感性

好的加密系统应具有敏感性,以提高系统抵抗穷举攻击的能力. 在最理想情况下,当明文或密钥改变 1 bit,应有 50% 的密文位改变. 图 5 列出了当

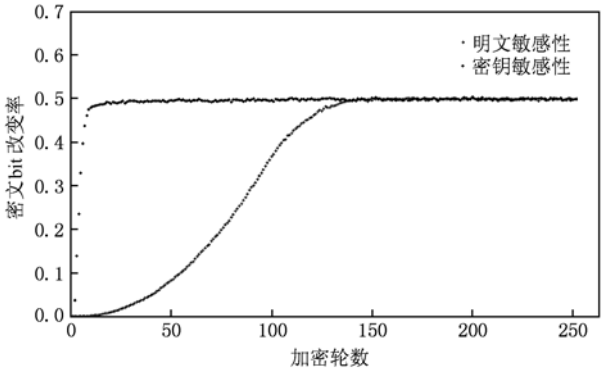

图 5 明文和密文的敏感性

明文或密钥改变 1 bit 时,密文位的改变率. 由图 5 可知,密钥改变 1 bit,经 25 轮加密后密文位的改变率稳定在 50% 左右;明文改变 1 bit,经 150 轮加密后密文位改变率也稳定在 50% 左右.

5. 2. 2. UACI 值

UACI 值指两个密文像素的平均距离与最大可能距离的比值,在理想情况下,两个随机密文的 UACI 值应接近 1/3. 表 5 列出了明文或密钥改变 1 bit 后,经 150—157 轮加密后 UACI 值. 表 5 说明,经 150 轮加密后,UACI 值稳定到 1/3 左右.

表 5 明文或密钥改变 1 bit,密文的 UACI 值

轮数	150	151	152	153	154	155	156	157
明文改变 1bit	0. 3299	0. 3311	0. 3329	0. 3327	0. 3294	0. 3281	0. 3309	0. 3282
密钥改变 1bit	0. 3326	0. 3329	0. 3330	0. 3316	0. 3342	0. 3285	0. 3335	0. 3322

6. 结 论

本文基于两个简单的物理模型设计了一个加密系统,分析和实验结果表明该系统具有可逆、并行、简单、高效和安全的特性. 本文的研究表明,基于某些基本物理原理和模型设计加密系统是很有潜力的.

本文提出的加密系统仍有两个缺点,一是要求明文每个分组的长度为 5 bit,限制了加密系统的实用范围;二是轮密钥的产生使用了混沌系统,降低了加密效率. 此外,该系统的安全性仍待密码学专家的广泛分析. 这三者将是下一步的研究内容.

[1] Sahar M, Amir M E 2009 *Chaos*, *Solitons & Fractals* **42** 1745

[2] Sheng L Y, Cao L L, Sun K H, Wen J 2005 *Acta Phys. Sin.* **54** 4031 (in Chinese) [盛利元、曹莉凌、孙克辉、闻 姜 2005 物理学报 **54** 4031]

[3] Zhou Q, Hu Y, Liao X F, 2008 *Acta Phys. Sin.* **57** 5413 (in Chinese) [周 庆、胡 月、廖晓峰 2008 物理学报 **57** 4031]

[4] Zhou Q, Wong K W, Liao X, Xiang T, Hu Y 2008 *Chaos*, *Solitons & Fractals* **38** 1081

[5] Morita K 2001 *Proceedings of* 3*rd Int. Conf. on Machines*, *Computations*, *and Universality* Chisinau, Moldova, 2001 p102

[6] Hardy J, Pazzis O, Pomeau Y 1976 *Physical Rreview* A **13** 1949

A cryptosystem based on simple physical models*

Zhou Qing† Chen Gang Hu Yue

(*College of Computer Science, Chongqing University, Chongqing* 400044, *China*)

(Received 20 June 2010; revised manuscript received 12 July 2010)

Abstract

It is well known that some simple physical models can lead to complex behaviors. Moreover, some simple models possess a strongly logical expression ability. A cryptosystem is proposed based on two simple physical modes, which has the performances of its reversibility, parallelism, simplicity and efficiency. The simulation results show that the system presents satisfactory randomness and sensitivity. It is a promising method to use simple physical models for constructing a good cryptosystem.

Keywords: physical model, cryptosystem, parallel, efficiency

PACS: 47.11.Qr, 89.20.Mn, 89.20.Ff

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61003246, 61003256), the Natural Science Foundation of Chongqing, China (Grant No. CSTC2009BB2208).

† E-mail: tzhou@cqu.edu.cn