用简单物理模型构建通用对称加密系统*

周 庆† 何校栋 胡 月

(重庆大学计算机学院, 重庆 400044)

(2010 年 11 月 28 日收到;2010 年 12 月 17 日收到修改稿)

提出了扩展 HPP 模型,并与 RE 阵列结合,构建了一个对称加密系统. 该系统适用于任意维度和精度的数字对象,并具有空间性、并行性和高效性的特点. 实验结果表明,加密系统具有良好的随机性和敏感性.

关键词: 物理模型, 对称加密, 通用性, 并行计算

PACS: 47. 11. Qr, 89. 20. Mn, 89. 20. Ff

1. 引 言

互联网及移动通信使信息的产生、传播和存储更加方便快捷. 今天,通过手机或计算机,人们能以极低的成本分享文本、音频、图像、视频及其他类型的数字对象. 与此同时,如何保护这些对象的安全也成为用户们极为关心的问题,而密码学是保护这些数据的最有效的手段之一.

随机性和敏感性是对称加密系统基本的安全要求,也是自然界中普通存在的现象,因此研究者尝试将物理模型用于对称加密系统的设计. 基于混沌的加密算法一直是新型对称加密系统的研究热点[1]. 然而,混沌加密算法实用化的主要障碍在于效率问题:混沌系统需要进行多次迭代,每次迭代又涉及较多的乘除法运算;此外混沌加密算法难以兼顾并行加密和安全性两个要求[2].

为了解决以上问题,我们提出基于两个简单物理模型 RE(Rotary Element)和 HPP 模型的加密系统,具有简洁、高效,支持并行加密等优点[3]. 然而,该系统仅能支持分组长度为 5 比特(bit)的明文,这大大限制了系统的实用性.

与自然界类似,数字对象也具有多样化,其空间维度从一维到高维不等,每个元素可用一到几十比特的精度表示. 表 1 列出了一些常见的数字对象的维度和精度. 传统对称加密算法在处理这些对象时,均转换成一维数据再进行加密. 这种方式一方面需要消耗额外的转换时间,另一方面也不能利用对象的空间特性提高加密效率.

表 1 常见数字对象的维度和精度

数字对象	文本	音频	黑白图像	灰度图像	真彩色图	彩色视频	虚拟现实	数据仓库
维度	1	1	2	2	2	3	4	≥ 3
精度	8 或 16	≥ 8	1	8	24	24	≥ 8	≥ 1

鉴于某些物理模型对空间维度和精度有很好的适应性,我们希望借用其空间特性,设计一种可适用于任何空间维度和表示精度的对称加密系统,并保留其并行性、高效性、随机性和敏感性的优点. 本文通过提出扩展 HPP 模型、与 RE 阵列相结合,并给出模型的数字化实现和具体算法,实现了以上目标.

2. RE 阵列与扩展 HPP 模型

2.1. RE 阵列

RE 模型是 Morita 提出的一个简单系统[4],由挡板、球,四个入口和四个出口构成(参见图 1(a)). 小球从 e, s, w, n 四个入口之一进入系统,与挡板发生碰撞后,从 e', s', w', n' 四个出口之一退出系统. 表 2 给出球与挡板的相互作用,这说明一个 RE 模型处理的数据精度为 3 比特.

* 国家自然科学基金(批准号:61003246 和 61070246)和重庆市自然科学基金(批准号:2009BB2208)资助的课题.

† E-mail: tzhou@cqu.edu.cn

表 2 RE 模型中球出入系统前后球与挡板的状态

挡板方向	球的进入方向			
	n	e	s	w
—	$\mid w'$	$— w'$	$\mid e'$	$— e'$
$\mid$	$\mid s'$	$— n'$	$\mid n'$	$— s'$

将多个 RE 模型排列成 m 行 n 列可组成 RE 阵列. Morita 设计了一种特殊的 RE 阵列[5],要求除最后一行某个 RE 的挡板为水平状态外,其余所有 RE 的挡板均为竖直状态;并要求每个 RE 的 w' 出口必须与某个 RE 的 e 入口连成一个通道. 图 1(b)显示了一个满足此要求的 3 行 2 列的 RE 阵列.

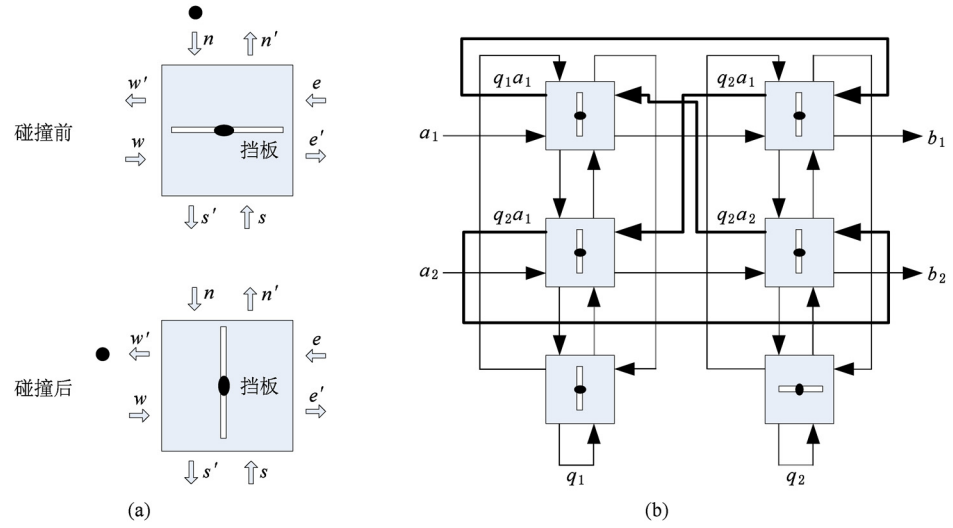

图 1 RE 模型与 RE 阵列 (a) RE 模型; (b) 一个 3 行 2 列的 RE 阵列

Morita 证明这类阵列可等价于一个状态机[5]. 假设仅最后一行第 j 列 RE 的挡板为水平状态,且第 i 行第 j 列 RE 的 w' 出口与第 m 行第 n 列 RE 的 e 入口相连,则球从左边第 i 行进入系统后的过程如下:

1) 保持所有挡板状态不变,球从第 1 列一直前进到第 j 列;

2) 将第 i 行第 j 列挡板改为水平;

3) 将最后一行第 j 列挡板改变为竖直;

4) 将第 i 行第 j 列挡板改为竖直;

5) 从第 i 行第 j 列 w 出口转到第 m 行第 n 列 e 入口;

6) 将最后一行第 n 列挡板改为水平;

7) 从第 m 行最后一列退出.

因此,球从第 i 行进入系统前,仅最后一行第 j 列的挡板为水平方向;球从第 m 行退出后,仅最后一行第 n 列的挡板为水平方向,系统的状态变化可表示为 $(q_i, a_j)\rightarrow(q_m, b_n)$.

注意,该状态变化规则正是由 w' 出口与 e 入口的连线决定的. 表 3 给出了图 1(b)中 RE 阵列的状态变化表. 通过改变阵列的行数和列数,RE 阵列可处理任意精度的数据. 设表示精度为 m,则 RE 阵列的行数 M 和列数 N 由下式确定:

$$\begin{cases} M = 2^{[\frac{m}{2}]} + 1, \\ N = 2^{[\frac{m}{2}]}, \end{cases} \quad \begin{cases} M = 2^{[\frac{m}{2}]} + 1, \\ N = 2^{[\frac{m}{2}]}. \end{cases} \tag{1}$$

此时,RE 阵列可对 $\left[\frac{m}{2}\right] + \left[\frac{m}{2}\right] = m$ 比特的数据进行处理.

表 3 RE 阵列的状态变化关系

原状态	(q_1, a_1)	(q_1, a_2)	(q_2, a_1)	(q_2, a_2)
新状态	(q_1, b_2)	(q_1, b_2)	(q_1, b_2)	(q_1, b_1)

2.2. 扩展 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,每个格点的精度为 4 比特. 这里我们提出一种扩展 HPP 模型,可处理任意维度和任意精度的数据.

扩展 HPP 模型同样由格点构成,每个格点的坐标一个 d 维向量,每个格点的精度为 m(即包含 m 比特数据). 与 HPP 模型相同,扩展 HPP 模型每轮变换包含两个阶段,即平移和碰撞. 其中碰撞采用 RE 阵列模型,平移阶段可由下式表示:

$$\alpha_1^{(n)}(x) = p_1(\alpha^{(n-1)}(x + s_i)), \tag{2}$$

其中 $\alpha^{(n)}(x)$ 表示模型经 n 轮迭代后,位于坐标 x 上值,$\alpha_i^{(n)}(x)$ 表示 $\alpha^{(n)}(x)$ 的第 i 比特,s_i 表示扩展 HPP 模型的第 i 个领域. p_i 表示投影函数:

$$p_i(x) = x \cdot e_i p_i(x) = x \cdot e_i, \quad (3)$$

其中·表示内积运算,$e_i = [\alpha_1, \cdots, \alpha_d]$,$a_i = 1$,$a_i = 0$,$i \neq j$.

为了实现模型的通用性,必须确定 s_i 的计算方法. 下式给出了一种快速算法:

$$s_i = \begin{cases} n_i + R, & n_i + R \neq 0, \\ R, & n_i + R = 0, \end{cases} \quad (4)$$

其中 $n_i = (\alpha_{d-1}, \alpha_{d-1}, \cdots, \alpha_0)$,$\alpha_{d-1}\alpha_{d-2}\cdots\alpha_1\alpha_0$ 为 i ($i = 1, 2, \cdots, m$)的 r 进制表示,即

$$i = \alpha_{d-1}r^{d-1} + \alpha_{d-2}r^{d-2} + \cdots + \alpha_1 r + \alpha_0, \quad (5)$$

$$r = \lfloor \sqrt[d]{m+1} \rfloor, r = \lfloor \sqrt[d]{m+1} \rfloor, \quad (6)$$

R 表示平移向量,定义为

$$R = \left(-\left[\frac{r}{2}\right], -\left[\frac{r}{2}\right], \cdots, -\left[\frac{r}{2}\right] \right). \quad (7)$$

表 4 列出根据(4)式计算的,在某些维度和精度下的领域集合.

表 4 不同维度和精度下的领域集合举例

维度 d	精度 m	s_1—s_m
1	6	−2, −1, −3, 1, 2, 3
2	6	(−1,0), (−1,1), (0, −1), (−1, −1), (0,1), (1, −1)
3	7	(−1, −1,0), (−1,0, −1), (−1,0,0), (0, −1, −1), (0, −1,0), (0,0, −1), (−1, −1, −1)
4	4	(−1, −1, −1,0), (−1, −1,0, −1), (−1, −1,0,0), (−1,0, −1, −1)

(2)式的实质是将第 i 个相邻格点的第 i 个比特移动到本格点到第 i 个比特位置上. 图 2 显示了一个精度为 6 比特的二维扩展 HPP 模型在平移阶段移动比特的过程.

2.3. 模型的数字化实现

RE 阵列和扩展 HPP 模型原为物理模型,而加密通常以软件或数字电路的方式实现. 下面给出模型的数字化实现方法.

Morita 提出的 RE 阵列等价于一个确定状态机,可由状态图表示. 特别地,我们要求该状态图只包含一个环,此时 RE 阵列等价于一个排列. 因此我们可用替换表来实现排列,从而实现 RE 阵列的功能. 我们提出的排列产生算法如下:

步骤 1 给定一个初值,产生一个含 2^m 个状态的混沌序列;

步骤 2 对混沌序列进行排序;

步骤 3 将 2^m 个排序序号作为产生的排列.

这里我们选用的混沌映射为 logistic 映射,

$$x_{n+1} = 4x_n(1 - x_n), \quad (8)$$

其初值 $x_0 = 0.12345678$. 表 5 给出 $m = 3$ 时,产生的一个替换表.

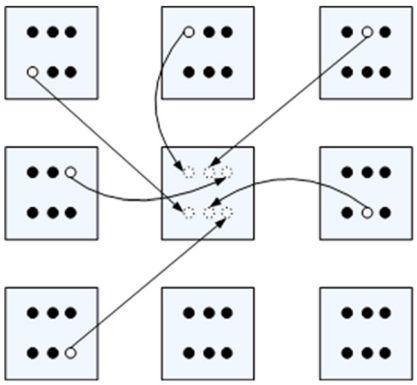

图 2 扩展 HPP 模型平移阶段举例

表 5 RE 陈列对应的替换表 ($m = 3$)

原状态	0	1	2	3	4	5	6	7
新状态	3	0	4	1	6	5	7	2

扩展 HPP 模型平移阶段则可通过内存读写操作实现,即从内存中读取数据再写入到新的存贮地址. 这说明 RE 阵列和扩展 HPP 模型均可由简单的数字运算实现.

3. 加密算法的设计与分析

3.1. 加密流程

加密由多轮构成,每轮加密包括三个过程,即扩展 HPP 模型平移阶段,RE 阵列替换以及轮密钥异或. 其中轮密钥异或指将生成的轮密钥与明文进行异或运算. 图 3 的左部分显示了加密流程.

3.2. 轮密钥产生算法

我们规定外部密钥的长度为 128 比特,通过将密钥进行重复铺叠可产生与数字对象相同大小的初始轮密钥. 由于每轮所需轮密钥不同,还需设计轮密钥产生算法. 这里给出的轮密钥产生算法与加密流程类似,包含扩展 HPP 模型平移阶段和 RE 阵

列替换两个过程(参见图 3 右部分).

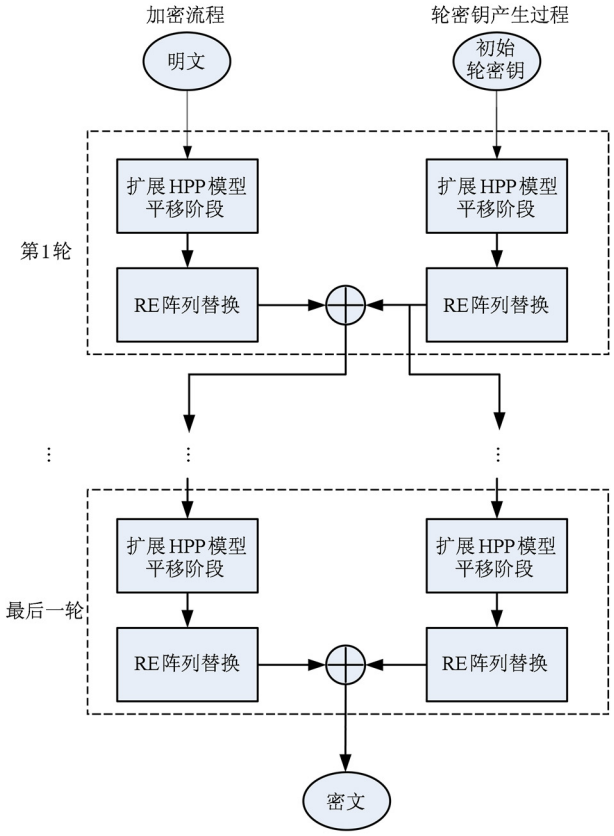

图 3 加密流程与轮密钥产生过程

3.3. 算法性能分析

基于 RE 阵列和扩展 HPP 模型的加密算法具有以下优点:

通用性 模型可适用于任意维度和精度的数字对象. 扩展 HPP 模型对整个数字对象进行操作,可支持任意维度和精度的对象;RE 阵列对每个格点进行操作,可支持任意精度的格点.

空间性 模型直接在 d 维空间上对数据进行操作,在扩展 HPP 模型的平移阶段利用对象的空间性进行加密,与传统加密算法相比,提高了加密效率.

并行性 加密算法对所有格点的操作可同时进行,因此所有格点的加密是并行的.

高效性 对每个格点的操作只包含替换、内存读写及异或三种最快速的操作,因此加密效率很高(表面上看,(4)式和(8)式使用了乘法计算,但其计算结果均为常数,故可在加密之前存贮,在加密时仅涉及内存读取操作).

安全性 通过引入混沌映射,提高了 RE 阵列替换的随机性和敏感性(但是加密中并未直接进行混沌映射计算,而是采用混沌映射的结果,从而保证了加密效率);扩展 HPP 模型则将局部敏感性扩展到整个图像. 实验结果证实了算法良好的随机性与敏感性.

需注意的是,当数字对象的精度较高时,实现 RE 阵列所需的存储空间较大.

4. 实验结果

实验测试加密算法的通用性和安全特性. 密钥为 128 比特的 **0** 向量,测试对象包括文本、音频、图像和视频. 其中图像为灰度和彩色 Lena 图像,音频为一段手机铃声,视频由 6 帧经处理后的 Lena 图像构成(参见图 4). 实验表明本文算法适用于以上所有对象.

图 4 视频包含的 6 帧 Lena 图像

表 6 显示了各数字对象的实验结果. 其中 "1 的比例"指密文中比特 1 所占比例,实验结果均接近 0.5;"比特改变率"真指明文改变 1 比特后,发生改变的密文比特所占比例,同样接近理论值 0.5;这两个指标分别说明加密算法具有良好的随机性和敏感性. 收敛轮数指比特改变率首次接近 0.5 的加密轮数,它决定了加密所需的最少轮数,因而将影响加密所需时间. 实验表明,除音频加密外,其他数字对象的收敛轮数均远小于对象大小. 这是因为选用的音频长度较大而精度较小,在实际应用中,加密的并行化可很好地弥补这一缺陷.

表 6 各种数字对象的实验结果

类型	名称	维数	精度	大小	1 的比例	比特改变率	收敛轮数
文本	《蜀道难》	1	16	340	0.5173	0.5029	25
音频	手机铃声	1	8	5, 000	0.4959	0.4954	747
图像	Lena	2	8	128 × 128	0.5023	0.4992	79
彩图	Lena	2	24	128 × 128	0.5008	0.5005	36
视频	Lena	3	24	128 × 128 × 6	0.5003	0.4999	69

表 7 视频加密的 UACI 值

轮数	69	70	71	72	73	74	75	76
UACI	85.30	85.33	85.30	85.40	85.20	85.43	85.32	85.33

实验同时计算了其他安全指标,如 UACI 和相关系数. 由于篇幅限制,这里列出视频加密的结果作为代表,其他对象的实验结果是类似的.

UACI 指明文改变 1 比特后,密文对应字节间的平均距离,表 7 列出视频加密在 69 至 76 轮之间密文的 UACI 值,均接近理论值 85.33.

相关系数指相邻格点间的相关系数,对于图像、视频等数字对象,其值接近于 1;加密后该指数应接近于 0. 表 8 列出了 3 种有相邻关系的像素间的相关系数. 在每种相邻关系下,随机选择 1000 对像素进行测试. 表 8 说明,相邻密文像素间不存在明显的相关性.

表 8 明文和密文图像中 $x(i, j, k)$ 与相邻象素的相关系数

相邻像素	明文相关系数	密文相关系数
$x(i+1, j, k)$	0.9406	0.0181
$x(i+1, j+1, k)$	0.8744	−0.0282
$x(i+1, j+1, k+1)$	0.7791	−0.0196

5. 结 论

数字对象,如文本、图像、视频等,在维度和精度上具有多样性. 本文分析了 RE 阵列的特性,在 HPP 模型的基础上提出扩展 HPP 模型,并将之用于数字对象的对称加密. 研究结果表明,本文提出的算法可用于任意维度和精度的数字对象,且具有并行性、空间性和高效性,在安全方面满足随机和敏感的要求.

在两种特殊情况下,本文算法仍有不足. 一是加密一维数字对象(如音频)时收敛轮数较高,而传统加密算法可直接处理一维数据,此时用传统加密算法更佳;二是当精度过高($m > 26$)时,所需的存储空间较多,故当 m 较大时,最好采用空间复杂度较小的算法来实现 RE 阵列,这是我们下一步的研究内容.

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

[2] Zhou Q, Wong K W, Liao X 2008 *Chaos, Solitons & Fractals* **38** 1081

[3] Zhou Q, Chen G, Hu Y, 2011 *Acta Phys. Sin.* **60** 044701 (in Chinese) [周 庆、陈 钢、胡 月 2011 物理学报 **60** 044701]

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

[5] Morita K 2003 *Grammars and Automata for String Processing* (Boca Raton: CRC) p 285

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

A universal cryptosystem based on two simple physical models*

Zhou Qing† He Xiao-Dong Hu Yue

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

(Received 28 November 2010; revised manuscript received 17 December 2010)

Abstract

Digital objects, such as images, videos, digital warehouse are diverse in the sense of dimension and representation-precision. Conventional encryption algorithms treat all digital objects as one-dimensional data, thus they cannot make it effective to take advantage of their spatial characteristics. A cryptosystem is constructed by combining RE arrays with extended HPP model we proposed. The cryptosystem is applicable to digital object of arbitrary dimension and representation-precision. Moreover, it has the merits of spatiality, parallelism, and high efficiency. Experimental results demonstrate that the cryptosystem has satisfactory randomness and sensitivity.

Keywords: physical model, symmetric cryptography, universality, parallel computing

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

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61003246, 61070246) and the Natural Science Foundation of Chongqing (Grant No. CSTC2009BB2208).

† E-mail: tzhou@cqu.edu.cn