

文章编号:1007-2780(2009)06-0879-03

基于混沌链 C 细胞自动机的加密方法研究

张 玲¹,杨晓利²,梁士利³

(1. 长春理工大学 理学院,吉林 长春 130022,E-mail:lsli@nenu.edu.cn;
2. 长春中医药大学,吉林 长春 130117; 3. 东北师范大学 物理学院,吉林 长春 130024)

摘 要: 提出一种基于混沌细胞自动机的分组密码算法,采用固定边界条件下反向加密正向解密的 Feistel 迭代方式,计算机模拟的实验结果证明:该算法在固定密钥的密文差错扩散率和固定明文的密文差错扩散率接近 50%,可有效对抗差分攻击、穷举明文和穷举密钥攻击。

关 键 词: 混沌;链 C 规则细胞自动机;分组密码
中图分类号: TP309.7 **文献标识码:** A

1 引 言

最近以来,利用细胞自动机(Cellular Automata,CA)进行加密的研究逐步成为热点^[1-5]。CA 所具有的简单、并联、二值特性,被认为是密码技术自主化方面最有希望的核心技术之一。在 CA 的加密应用中,具有混沌特征的规则最具密码学应用价值。wolfram^[6]首先提出 CA 在时空演化四类行为中存在混沌现象;Langton^[7]指出当 $\lambda=0.5$ 时,CA 呈现混沌的动力学行为特征;相比 λ 参数更精确的是 Wuensche^[8]利用回溯 CA 中出现的前驱状态数量而定义的链 C 细胞自动机,这种 CA 有比其他几种行为较低的收敛度,熵值最大,迭代过程具有的混乱与扩散特性适合于密码学应用。本文以一维五邻居链 C 细胞自动机为研究对象,设计了一种分组密码,并对其抵抗攻击能力进行了分析。

2 加密设计机理

在分组密码中明文空间与密文空间是对等的,其加(解)密过程实质上是在密钥的控制下实现同一空间的置换,也就是在相同密钥的作用下明文与密文保持一一对应关系,因此分组密码算法必须保证加密过程与解密过程具有可逆性。

混沌 Chain CA 的状态中具有一个前驱状态概率最大,左右前驱状态概率 Z_{left} 或 Z_{right} 中有一

个为 1,其演化过程具有不可逆性。虽然直接利用混沌 Chain C 规则 CA 实现加(解)密编码无法实现变换的可逆性,但如果在满足一定条件下,其演化过程存在一一对应关系,能够满足系统运转过程的可逆性。

2.1 可逆性证明

在一维五邻居 Chian C 规则的 CA 中,在 t 时刻 5 个邻居细胞的状态可表示为 $a_{i-2}^t, a_{i-1}^t, a_i^t a_{i+1}^t, a_{i+2}^t$,在进行正向迭代时, a_i^t 下一时刻的状态 a_i^{t+1} 可用如下关系式进行描述:

$$a_i^{t+1} = \tau(a_{i-2}^t, a_{i-1}^t, a_i^t, a_{i+1}^t, a_{i+2}^t) \tag{1}$$

对于一个具有左触发行为的 Chian C 规则,改变规则输出表最左边细胞的值,规则输出表的输出将是原来输出值的取反,可表示为如下公式:

$$1 - a_i^{t+1} = \tau(1 - a_{i-2}^t, a_{i-1}^t, a_i^t, a_{i+1}^t, a_{i+2}^t) \tag{2}$$

只有 0 和 1 两种状态的 CA,若同时满足式(1)和式(2),则该 CA 的反向迭代可以表示为:

$$a_{i-2}^t = \tau(a_i^{t+1}, a_{i-1}^t, a_i^t, a_{i+1}^t, a_{i+2}^t) \tag{3}$$

证明:

若 CA 只有 0 和 1 两种状态,则 a_i^{t+1} 与 a_{i-2}^t 之间只有以下两种关系:

(1)当 $a_{i-2}^t = a_i^{t+1}$ 时,由式(1)可以得到式(3);

(2)当 $a_{i-2}^t \neq a_i^{t+1}$ 时, $a_{i-2}^t = 1 - a_i^{t+1}$,且 $a_i^{t+1} = 1 - a_{i-2}^t$,则由式(2)可以得到式(3)。

证明完毕。

由公式(3)可知,如果已知 t 时刻细胞 a_{i-1}^t , $a_i^t, a_{i+1}^t, a_{i+2}^t$ 的状态和 $t+1$ 时刻 a_{i+1}^{t+1} 的状态,便可以惟一地确定 t 时刻细胞 a_{i-2}^t 的状态,由此保证 CA 反向迭代过程的可逆性。

3 效果检验

本算法是一种通过 Feistel 网络迭代分组密码的加密方法,其中分组长度 128 位,采用对称密钥体制,密钥长度为 128 位。

3.1 固定密钥的密文差错扩散率

本方法取输入的 128 bit 都为 0 明文,然后对 128 位中任意的一位进行改变(由 0 变为 1),比较其输出的密文与原明文输出密文对应出错个数。图 1 表示输入明文对应密文出错率。

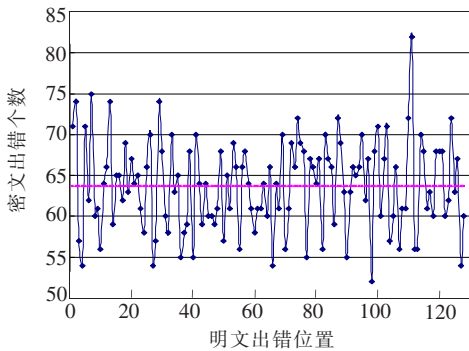


图 1 明文一位出错对应密文出错个数分布图
Fig. 1 Error propagation of ciphertext by the same key, the Plaintext with only one bit difference.

通过图 1 可以看出,明文中各个位置的改变对应不一样的出错个数。第 111 位明文由 0 变为 1,对应密文出错位数最大为 82 位;而明文中 98 位由 0 变为 1 时,对应密文出错位数最小为 52 位,改变所有 128 位明文其对应密文的出错均值为 63.72,接近 128 位的 1/2,说明本算法具有良好的扩散性。

3.2 固定明文的密文差错扩散率

固定明文密文差错扩散率是指密钥的 128 位中任意一位改变对于密文的出错的影响情况。这里明文固定为 128 个比特二进制 1,密钥是 128 个比特 0。

通过图 2 可以看出,密钥的一位改变密文出错个数在 48(51 位由 0 变为 1)到 78(32 位由 0 变为 1)之间变化,整个变化范围的均值为 62.99,接

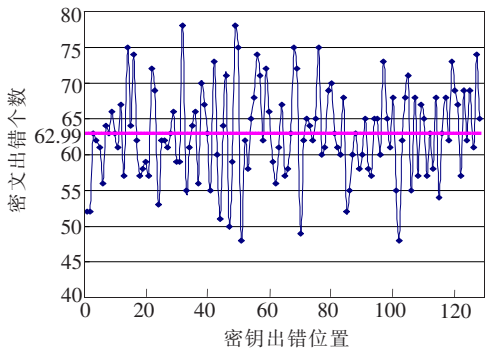


图 2 密钥一位出错对应密文出错个数分布图
Fig. 2 Error propagation of ciphertext based on only 1 bit error of the key

近 128 位的 1/2,说明这种固定明文密文具有良好的差错扩散率。

4 加密效果图

应用本算法进行加密,可加密任意类型计算机处理数据,通过软件仿真实验结果证明加密后的数据可以被全比特恢复。图 3 和图 4 为加密前和加密后的 Lina 图,解密后图像原图像完全相同。



图 3 加密前 Lina 图像
Fig. 3 Original picture of Lina

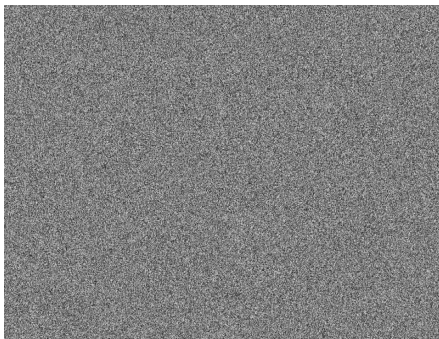


图 4 加密后 Lina 图像
Fig. 4 Encrypted picture of Lina

5 结 论

链 C 规则细胞自动机由于具有最大混沌行

为,其演化过程具有很好的混乱和扩散特性,适合于密码学设计。本文基于一维五邻居的分组密码设计,能有效抵抗已知明文和密文攻击。

参 考 文 献:

[1] Kalso Ali A. An efficient cryptosystem Delta for stream cipher applications [J]. *Computers & Electrical Engineering*, 2009, 35(1):126-140.

[2] Sung Jaechul, Hong Deukjo, Hong Seokhie. Cryptanalysis of an involutinal block cipher using cellular automata [J]. *Information Processing Lett.*, 2007,104(5):183-185.

[3] Fúster-Sabater A, Caballero-Gil P. Linear solutions for cryptographic nonlinear sequence generators [J]. *Phys. Lett. A*, 2007,369(5-6):432-437.

[4] Martín del Rey A, Pereira Mateus J, Rodríguez Sánchez G. A secret sharing scheme based on cellular automata [J]. *Appl. Mathematics and Computation*,2005, 170(2):1356-1364.

[5] Seredynski Franciszek,Bouvry Pascal, Zomaya Albert Y. Cellular automata computations and secret key cryptography [J]. *Parallel Computing*, 2004,30(5-6):753-766.

[6] Wolfram S. Cryptography with cellular automata[C]//*Proceedings of Crypto'85, Lecture Notes in Computer Science*, Berlin, Germany:Springer-Verlag,1985:429-432.

[7] Langton C G. Computation at the edge of chaos:Phase transitions and emergent computation [J]. *Physica*,1990,42: 12-37.

[8] Wuensche A, Lesser M J. *The Global Dynamics of Cellular Automata; An Atlas of Basin of Attraction Fields of One-dimensional Cellular Automata* [M]. California, USA:Addison-Wesley, Publishing Company,1992.

Encryption Based on Chain-Rules Cellular Automata

ZHANG Ling¹, YANG Xiao-li², LIANG Shi-li³

(1. College of Science, Changchun University of Science and Technology, Changchun 130022, China, E-mail: lsl@nenu.edu.cn;
2. Changchun College of Traditional Chinese Medicine, Changchun 130117, China;
3. School of Physics, Northeast Normal University, Changchun 130024, China)

Abstract

This paper presents a block cipher algorithm based on the chain-rules CA, which is by means of iterating cellular automata backward-to-encryption and forward-to-decryption at a fixed boundary. The results show the error propagation of ciphertext with an unchanged key and ciphertext with an unchanged plaintext is close to 50%. This cryptosystem can resist known-plaintext attack and known-ciphertext attack.

Key words: chaos; chain C cellular automata; block cipher

作者简介:张玲(1969—),女,吉林长春人,硕士,讲师,主要从事非线性动力学系统研究。