文章编号:1000 - 582X(2005)01 - 0082 - 04

一种混沌加密算法及其 CPLD 实现*

李 强,杨 欣,黄席樾
(重庆大学 自动化学院,重庆 400030)

摘 要:混沌序列以其容易生成性、初值敏感性、复杂的伪随机性等,已成为一种经常用到的序列加密方法。讨论了一种混沌加密算法,此算法需生成 2 个混沌序列,并用 *M* 序列对明文置乱,以增强保密性。据此算法设计出一块实用的加密解密专用芯片,内部所有模块均用 AHDL(Altera Hardware Description Language)语言编制完成,并下载到 CPLD(Complex Programmable Logical Device)芯片中。最后设计出实验板,在 2 台 PC 机间完成了实验。

关键词:混沌序列;M 序列;Logistic 映射;加密
中图分类号:TP309.7 **文献标识码**:A

随着通信技术的不断发展,信息安全已成为一个非常重要的研究领域。不管是政府、企业还是个人在传递机密信息时,都希望信息在传输过程中不被非法截取、篡改、伪造等。因此,人们在发送机密信息时都采用加密的方法,只有拥有正确密钥的人才能解密出正确的信息。

自从英国数学家 Matthews[1]正式提出一类混沌加密方法以来,各种各样的混沌加密算法层出不穷。由于混沌序列对初值的变化非常敏感,因此,初值的微小变化都能使生成的混沌序列大相径庭。混沌序列以其复杂的伪随机性,已成为序列密码加密方法中经常选用的方法。

1 混沌系统基础

混沌是服从决定性方程的非线性动力学系统的一种复杂的运动状态[2]。在混沌系统中有两类非常重要的非线性动力学系统。一类是 Logistic 映射,一类是 Chebyshev 映射。

Logistic 映射定义如下:

$$X_{n+1}=\mu X_n(1-X_n)$$

其中 $0<X_n<1$, $1<\mu<4$。Schuster 导出,当 $3.569\,945\,6\cdots<\mu<4$ 时 Logistic 映射处于混沌状态。

K 阶 Chebyshev 映射定义如下:

$$\tau(X_{n+1})=\cos(\mu(\cos^{-1}X_n))$$

其中 $-1<X_n<1$。

通过简单的变量代换,Logistic 映射同样可以在区间(-1,1)上定义,其形式如下:

$$X_{n+1}=1-\lambda X_n^2$$

其中 $0\leqslant\lambda\leqslant2$。在 $\lambda=2$ 的满射条件下,Logistic 映射 Chebyshev 映射是拓扑共形的,其所生成的概率分布函数也是相同的[3]。

2 混沌加密算法

2.1 混沌加密序列生成

本算法选用经过变量代换的 Logistic 映射:

$$X_{n+1}=1-\lambda X_n^2,$$

其中 $\lambda=2$,进行迭代生成混沌序列 $\{X_n, n=0,1,\cdots\}$。所生成的混沌序列 X_n 值是在(-1,1)之间的小数,将 X_n 中的每一个值都用二进制补码表示出来。如:$X_k=0.4$ 是混沌序列 X_n 中的一个值,将其转换为二进制补码的过程如下:

0.4 * 2 = 0.8 0
0.8 * 2 = 1.6 1
0.6 * 2 = 1.2 1
0.2 * 2 = 0.4 0
0.4 * 2 = 0.8 0

* 收稿日期:2004 - 09 - 12
基金项目:重庆市科委攻关项目(2003035 - 02)
作者简介:李强(1979 -),男,重庆人,硕士,研究方向:混沌加密,图像处理。

$$0.8 * 2 = 1.6 \quad 1$$
$$0.6 * 2 = 1.2 \quad 1$$
$$0.2 * 2 = 0.4 \quad 0$$
$$\vdots$$

因此，0.4 的二进制补码为 01100110…，长度可按要求取任意长度。若 X_n 序列中某一值为负数，可先将其绝对值化为二进制数，再按位取反加 1，可得到其二进制补码。

在混沌序列生成过程中，选用 $\lambda = 2$，以及将 X_n 序列中的每一个值都用二进制补码表示出来，都是为了在 CPLD 中实现起来较为方便。

2.2 *M* 序列扰动

加入 *M* 序列进行扰动是为了增强密文的保密性。为配合对明文置乱的 3 种方法，即对明文左移、右移、逆序，需让 *M* 序列产生 3 种状态。以 4 阶的 *M* 序列…1 1 1 1 0 0 0 1 0 0 1 1 0 1 0 …为例，按如下方法可获得第 3 种状态：任取 *M* 序列中相邻的 2 位 M_k 和 M_{k+1} 进行异或，若 M_k xor $M_{k+1} = 0$，说明 M_k 与 M_{k+1} 同为 0 或同为 1，那么就让 M_k 变为第 3 种状态，即让明文完全逆序，反之，M_k xor $M_{k+1} = 1$，说明 M_k 与 M_{k+1} 必 1 个为 0、1 个为 1，当 $M_k = 0$ 时，明文左移；当 $M_k = 1$ 时，明文右移。

2.3 算法原理及步骤

本混沌加密系统为三密钥系统。加密时需给定 2 个混沌序列的初值 X_0 和 Y_0，以及 *M* 序列的阶数 N_0。由于混沌序列的初值敏感性，初值的微小变化都会使产生的混沌序列完全不同，所以，解密时必须给定相同的初值 X_0，Y_0 和 N_0，才能解密得到正确的明文。加密步骤如下：

Step 1　给定初值 X_0，产生混沌序列 X_n（X_n 序列中的每个值 X_k 用二进制补码表示）；给定初值 Y_0，产生混沌序列 Y_n（Y_n 序列中的每个值 Y_k 用 2 进制补码表示）；给定初值 N_0，产生 *M* 序列。

Step 2　取 *M* 序列中相邻的 2 位 M_k 和 M_{k+1}；取混沌序列 Y_n 中的一个值 Y_k；如果 M_k xor $M_{k+1} = 1$ and $M = 0$，那么明文循环左移，左移的位数由 Y_k 的前 3 位决定；如果 M_k xor $M_{k+1} = 1$ and $M = 0$，那么明文循环右移，右移的位数由 Y_k 的前 3 位决定；如果 M_k xor $M_{k+1} = 0$，那么明文完全逆序，即明文的最高位 *d*7 与最低位 *d*0 交换，*d*6 与 *d*2 交换，其他位以此类推。

Step 3　取混沌序列 X_n 中的 1 个值 X_k 与置乱后的明文按位异或，输出即为密文。

3　解密算法

解密时必须输入正确的密钥（混沌序列的初值 X_0 和 Y_0，以及 *M* 序列的阶数 N_0），再将加密算法逆向运算可解密出正确的明文。解密的关键是 Step 2，加密时对明文左移的条件，在解密时应变为对明文右移。同样，加密时对明文右移的条件，在解密时应变为对明文左移，移位的次数仍由混沌序列 Y_n 中的 1 个值 Y_k 的前 3 位决定。解密步骤如下：

Step 1　给定初值 X_0、产生混沌序列 X_n（X_n 序列中的每个值 X_k 用 2 进制补码表示）；给定初值 Y_0，产生混沌序列 Y_n（Y_n 序列中的每个值 Y_k 用 2 进制补码表示）；给定初值 N_0，产生 *M* 序列。

Step 2　取 *M* 序列中相邻的 2 位 M_k 和 M_{k+1}；取混沌序列 Y_n 中的 1 个值 Y_k，如果 M_k xor $M_{k+1} = 1$ and $M = 0$，那么明文循环右移，右移的位数由 Y_k 的前 3 位决定；如果 M_k xor $M_{k+1} = 1$ and $M = 0$，那么明文循环左移，左移的位数由 Y_k 的前 3 位决定；如果 M_k xor $M_{k+1} = 0$，那么明文完全逆序，即明文的最高位 *d*7 与最低位 *d*0 交换，*d*6 与 *d*2 交换，其他位以此类推。

Step 3　取混沌序列 X_n 中的 1 个值 X_k 与置乱后的明文按位异或，输出即为密文。

4　CPLD 实现

本算法选用 ALTERA 的 MAX7000S 系列的 CPLD 实现。所有模块均用 AHDL（Altera Hardware Description Language）语言在其开发工具 MAX + PLUS II 10.1 中编制完成。

4.1 系统基本构成

系统主要由 2 个混沌序列发生器，1 个 *M* 序列发生器，加密运算模块，控制模块等组成。如图 1 所示。

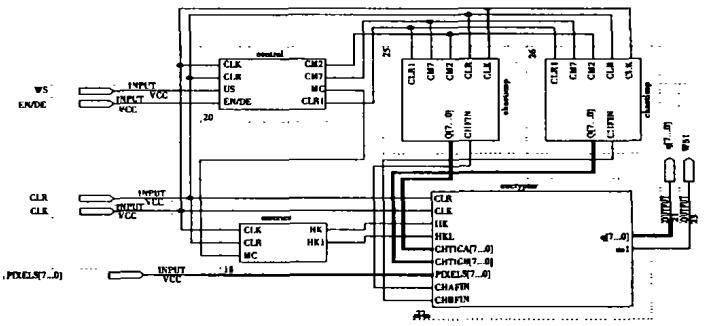


图 1　系统基本构成

4.1.1　混沌序列发生器

混沌序列发生器中包含循环移位寄存器（16 位左移，16 位右移），16 位全加器，及一些必要的控制信号。如图 2 所示。

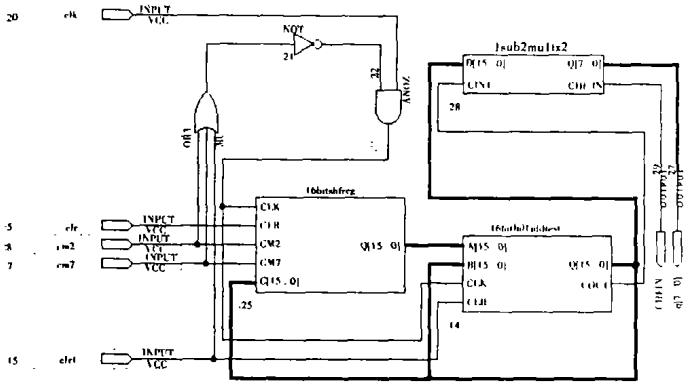


图 2 混沌序列发生器

所用 Logistic 映射的迭代公式为:

$$X_{n+1} = 1 - 2X_n^2$$

其中的乘方运算,减法运算,均转换为补码的加法运算实现。

将混沌序列 X_n 中 1 个值 X_k 存入 16 位循环左移寄存器和 16 位循环右移寄存器中,在 CLK 时钟脉冲的控制下进行移位,每移 1 次,将 16 位循环右移寄存器的最低位与 16 位循环左移寄存器的每一位相与,得到的结果送 16 位全加器作累加,经过 7 个 CLK 脉冲后可得到一个 X_k 的值。

将得到的 X_k 值左移 1 位,即可得 $2X_k$ 的值。如果 16 位全加器有进位,或 X_k 的首位为 1,说明 $2X_k$ 大于 1,那么就对其按位取反加 1,即得到 $1-2X_k$ 的值,反之,说明 $2X_k$ 小于 1,那么直接就可得到 $1-2X_k$ 的值。图 3 是 MAX + PLUS II 对混沌序列发生器仿真的结果。

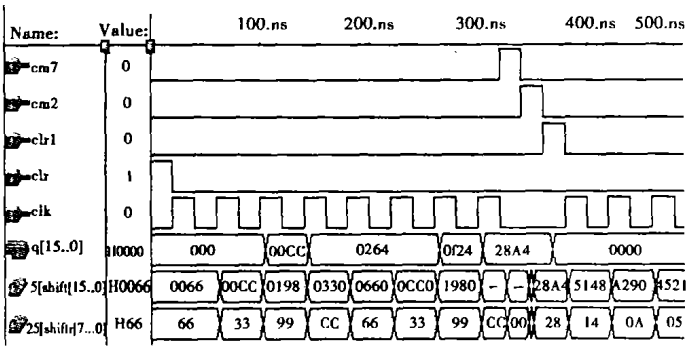


图 3 混沌序列发生器仿真结果

4.1.2 加密运算模块

加密运算模块包含 1 个 16 位循环移位寄存器,通过循环移位寄存器上的 R/L 信号可控制其进行左移或右移。R/L 信号的值由 M_k 与 M_k 异或,并判断 M_k 的状态后决定。

将明文置入循环移位寄存器中,取 Y_n 序列中的一个值 Y_k 的前 3 位得到移位的次数,通过控制循环移位寄存器的 CLK 脉冲就可控制其移位的位数。在程序中,把 Y_k 的前 3 位作为 CASE 语句的转移条件,进入对应的 CASE 语句后,启用相应的计数器,并使闸门信号有效,让 CLK 脉冲能进入循环移位寄存器。

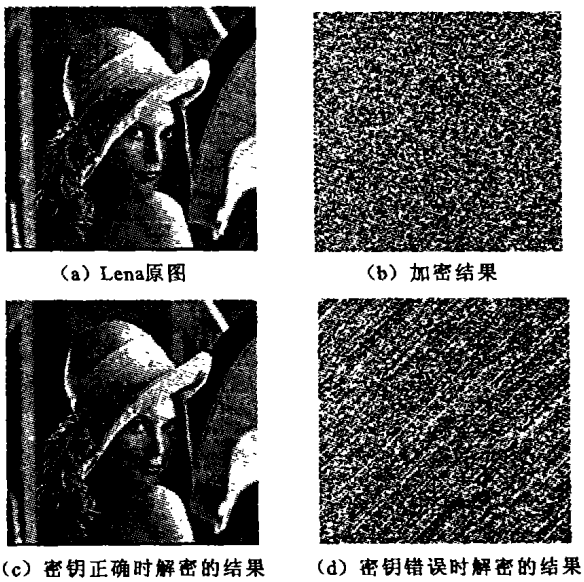
移位或完全逆序后的明文与 X_n 序列中的值 X_k 异或后输出,此输出即为密文。

5 实验结果

为实际验证加密效果,设计了专用的实验板,以下载了程序的 CPLD 为中心、辅以单片机,串行收发器等构成。利用串口通信,在 2 台 PC 机间完成了实验。

系统上电后,实验板初始化、置加密/解密位 EN/DE 为 1(EN/DE = 1 为加密、EN/DE = 0 为解密)。1 台计算机(PC1)通过串口送 1 个字节明文到串行收发器 U1(MAX232),由其转换后送到单片机 U2(AT89C52)的串口,单片机将此字节明文读出,送到 CPLD 的 Pixels[7 ·· 0]引脚,并向 CPLD 的 WS 引脚发一个脉冲,CPLD 收到此脉冲后,将字节明文信号读入。经 CPLD 内部加密后的密文,从 CPLD 的 Q[7 ·· 0]引脚输出到单片机 U3 的 P1 口,并置 WS1 信号为低,引发单片机中断,将此密文读入,再通过它的串口发送到串行收发器,经转换后送另一台计算机(PC2)的串口,完成 1 个字节明文的加密通信。以此类推,可完成任意字节长度的明文的加密解密。

采用本算法对图像、文本进行了加密解密实验。图 4 为对图像加密解密的结果,图 4(b)是对 Lena 原图加密后的结果,密钥为 $X_0 = 0.4, Y_0 = 0.6, N_0 = 4$。图 4(d)是密钥错误时解密的结果,密钥为 $X_0 = 0.400\,01, Y_0 = 0.600\,01, N_0 = 4$。



(a) Lena原图 (b) 加密结果

(c) 密钥正确时解密的结果 (d) 密钥错误时解密的结果

图 4 图像加密解密结果

图 5 为对文本加密解密的结果。图 5(b)是对文本加密后的结果,密钥为 $X_0 = 0.4, Y_0 = 0.6, N_0 = 4$。

图 5(d)是密钥错误时解密的结果，密钥为 X_0 = 0.400 01，Y_0 = 0.600 01，N_0 = 4。

Chaotic systems are sensitive to initial conditions and chaotic parameters.

67	104	97	111	116	105	99	32	115	121	115
116	101	109	115	32	97	114	101	32	115	101
110	115	105	116	105	118	101	32	116	111	32
105	110	105	116	105	97	108	32	99	111	110
100	105	116	105	111	110	115	32	97	110	100
32	99	104	97	111	116	105	99	32	112	97
114	97	109	101	116	101	114	115	46	*	*

(a)明文及其数字信息

228	155	66	211	82	13	208	102	95	4	181
218	21	2	255	75	82	46	75	84	167	129
50	169	132	24	245	144	172	209	185	114	143
148	223	193	1	214	206	221	53	54	40	44
106	134	248	76	26	113	48	23	166	120	102
185	63	75	206	252	48	202	134	99	8	156
10	51	150	251	157	168	2	27	218	*	*

(b)密文数字信息

Chaotic systems are sensitive to initial conditions and chaotic parameters.

67	104	97	111	116	105	99	32	115	121	115
116	101	109	115	32	97	114	101	32	115	101
110	115	105	116	105	118	101	32	116	111	32
105	110	105	116	105	97	108	32	99	111	110
100	105	116	105	111	110	115	32	97	110	100
32	99	104	97	111	116	105	99	32	112	97
114	97	109	101	116	101	114	115	46	*	*

(c)密钥正确时解密的明文及其数字信息

248	49	8	113	30	173	159	61	90	206	208
159	166	174	162	176	33	65	70	243	128	132
181	29	26	42	148	143	85	113	125	82	123
160	45	61	98	128	164	9	245	108	148	21
155	160	169	19	52	142	225	79	22	116	236
115	233	56	140	70	106	255	175	186	229	121
79	252	120	129	235	207	68	198	214	*	*

(d)密钥错误时解密的明文及其数字信息

图 5　文本加密解密结果

6　结束语

由 2 台 PC 机间进行的加解密实验可以看出，此算法是一种保密性较好、实现较为方便的算法。其硬件可实现性，说明这种芯片设计方案是可行的，为其实际应用于各种需要加密的场合，提供了有力的保证。需要提醒一点的是，混沌序列都有其过渡过程，不同的初值，其过渡过程的长度是不相同的，因此，在实际操作时，跳过了混沌序列前面的 1 000 个字节。另外，M 序列的阶数选择较高阶为宜，以增强算法保密性。

参考文献：

[1] MATTHEWS. On the Derivation of a Chaotic Encryption Algorithm [J]. Cryptologia, 1989, (4): 29 - 42.

[2] 刘秉正. 非线性动力学与混沌基础[M]. 长春：东北师范大学出版社，1995.

[3] 易开祥，孙鑫，石教英. 一种基于混沌序列的图像加密算法[J]. 计算机辅助设计与图形学学报，2000，12(9)：672 - 676.

[4] YEN JUI - CHENG, GUO JIUN - IN. A New Chaotic Key - based Design For Image Encryption and Decryption [J]. Circuits and Systems, 2000, (4): 49-52.

[5] YEN JUI-CHENG, GUO JIUN-IN. A New Image Encryption Algorithm and Its VLSI Architecture [J]. Signal Processing Systems, 1999, 99: 430 - 437.

[6] 赵嘉莉，罗四维，温津伟. 基于神经网络的混沌加密算法[J]. 计算机研究与发展，1998，38(12)：1 475 - 1 479.

[7] 王相生，甘骏人. 一种基于混沌的序列密码生成方法[J]. 计算机学报，2002，25(4)：351 - 356.

[8] 唐秋玲，覃团发，陈光旨. 混沌图像加密[J]. 广西大学学报(自然科学版)，1999，24(1)：61 - 64.

Encryption Algorithm Based on Chaotic Sequences and Its CPLD Implementation

LI Qiang, YANG Xin, HUANG Xi-yue

(College of Automation, Chongqing University, Chongqing 400030, China)

Abstract: Encryption algorithm based on chaotic sequences have become an often-used encryption method, owing to its ease of generation, sensitive to its initial condition, complex pseudo-random. The authors discuss an encryption algorithm based on chaotic sequences. The algorithm needs to generate two chaotic sequences and uses m-sequences as the perturbation sequence in order to enhance security. According to the algorithm mentioned above, they design the encryption and decryption chip using AHDL(Altera Hardware Description Language) and implement it with CPLD.

Key words: chaotic sequences; m-sequences; logistic map; encryption

(编辑　张　苹)