基于 FPGA 技术的混沌加密系统研究*

刘强[1)] 方锦清[1)†] 赵耿[2)] 李永[1)]

1) (中国原子能科学研究院核技术应用研究所, 北京 102413)

2) (北京电子科技学院计算机系, 北京 100070)

(2011 年 10 月 7 日收到; 2011 年 12 月 7 日收到修改稿)

提出了一种基于混沌加密算法和传统加密算法的混沌加密系统, 并采用 FPGA 技术进行了硬件开发. 根据离散化和数字化技术, 将 Henon 映射和 Logistic 映射作离散化处理, 采用 Verilog HDL 语言和 FPGA 技术产生迭代序列, 结合传统加密算法, 基于 Xilinx 的 FPGA 开发平台进行了硬件实验研究, 并给出了该系统通过互联网上实现了文件加密和解密的通信实验, 结果显示具有网络通信的应用潜力.

关键词: 混沌, 加密, 解密, 现场可编程门阵列

PACS: 05.45.Vx

1 引 言

混沌科学诞生于 20 世纪 60 年代, 90 年代混沌同步与控制取得了突破性进展, 提出了混沌同步与控制的许多方法 [1−6]. 最近 20 多年来, 国内外基于混沌的保密通信应用研究方兴未艾, 发达国家积极推进了一系列混沌保密通信的重大研究计划, 并取得了长足进展. 近年来, 密码学作为信息安全的理论和关键技术与混沌研究密切结合, 美、欧、亚各洲频繁举行密码学和信息安全以及混沌通信学术会议. 令人关注的是, 混沌通信与互联网及军事网络信息安全密切相关, 混沌保密通信技术正在走向实用化 [5−8]. 这方面的专利数量不断增加, 仅我国混沌应用专利总数达到约 200 多项, 其中混沌保密通信相关专利占 1/3 以上.

混沌系统具有对初值的高度敏感性和混沌信号的宽带性等优越性, 因而可以利用混沌系统产生的混沌序列作为密钥序列对数据进行加、解密, 这种算法称之为混沌加密算法. 信息安全是现代社会人们非常关心的问题, 包括信用卡信息、身份证号、私人通信、个人详细资料、公司机密信息、银行帐户信息等等, 混沌加密算法独特的优越性使得相关研究成为了信息安全领域的一个重要课题 [7−15]. 本文将混沌加密算法与传统加密算法相结合, 设计了一种新的、有着应用潜力的混沌加密系统, 该系统可与不同的通信终端通过互联网通信, 保证各种数据传输的安全, 图 1 给出了通过互联网实现混沌保密通信的实验示意图. 本文将 Henon 映射和 Logistic 映射离散化得到混沌序列, 并结合传统加密算法, 采用 FPGA(Field Programmable Gate Array) 平台进行硬件设计和开发, 提出了一种新的混沌加密系统. Henon 映射和 Logistic 映射具有复杂的混沌动力学行为, 数学公式相对简单, 易于在电路上实现. FPGA 作为专用集成电路领域中的一种半定制电路而出现的, 既解决了定制电路的不足, 又克服了原有可编程器件门电路数有限的缺点. 以硬件描述语言 (Verilog 或 VHDL) 所完成的电路设计, 可以经过简单的综合与布局, 快速的烧录至 FPGA 开发板上进行测试, 是现代 IC 设计验证的技术主流. 本文在设计混沌加密和解密算法的基础上, 利用 Xilinx 的 FPGA 开发平台, 进行了文字和文件的加、解密的硬件实验.

2 加密算法

本文提出的混沌加密算法包括 Henon 映射迭代、Feistel 密钥变换、Logistic 映射生成替换表

* 国家自然科学基金 (批准号: 60874087, 61174151, 61170037, 60773120)、北京市自然科学基金 (批准号：4092040) 和中国原子能科学院院长基金 (批准号: YZ2011-20) 资助的课题.

† E-mail: fjq96@126.com

和 Feistel 加 (解) 密变换四部分, 其中 Henon 映射和 Logistic 映射生成替换表为混沌加密算法, Feistel 密钥变换和 Feistel 加 (解) 密变换是传统加密算法.

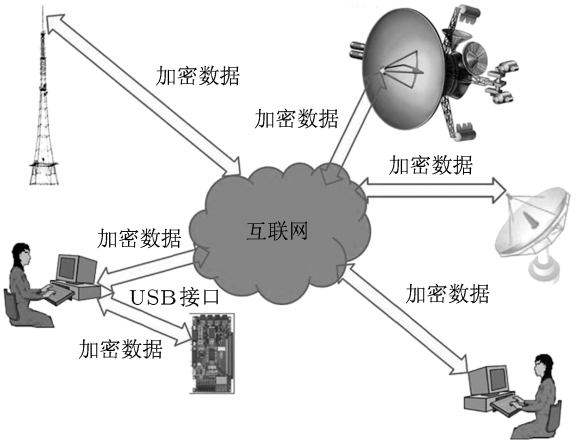

图 1 利用互联网进行混沌加密系统通信的示意图

2.1 Henon 映射

Henon 映射公式如下:

$$\begin{cases} x(n+1) = 1 - ax^2(n) + y(n), \\ y(n+1) = bx(n), \end{cases} \tag{1}$$

其中, $a = 1.4$, $b = 0.3$. 当 $a = 1.4$, $b = 0.3$ 时, lyapunov 指数为正值, 此时 Henon 映射处于混沌态.

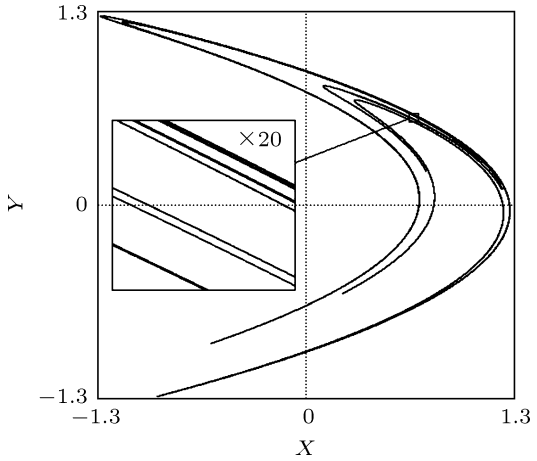

图 2 Henon 映射图

由 Henon 映射图 2 可知, Henon 的 x 变量和 y 变量在迭代过程中, 取值在 $[-2, 2]$ 之间, 而 FPGA 无法直接处理负值和小数, 因此设定参与 Henon 映射迭代的 x 变量和 y 变量位数为 36 位, 其中第 1 到第 32 位为小数位; 第 33 到第 35 位为整数位; 第 36 位为正负标记位, 当第 36 位为 1 时, x 变量和 y 变量为正值, 当第 36 位为 0 时, x 变量和 y 变量为负值.

将用户输入 64 位初始密钥 K 的前 32 位作为 x 变量的初值 $x(0)$, 将后 32 位作为 y 变量的初值 $y(0)$, 进行 100 次的 Henon 映射迭代, 将第 97 次到第 100 次迭代得到的 x 变量的小数位 (前 32 位) 组合作为经过 Henon 映射迭代加密的加密密钥 MK:

$$\mathrm{MK} = [x(100), x(99), x(98), x(97)]. \tag{2}$$

2.2 Feistel 密钥变换

经过 Henon 映射迭代得到的加密密钥 MK 为 16 字节, 将加密密钥 MK 按顺序分为 16 个字段, 每字段一个字节即 $\mathrm{MK} = (K_1, K_2, \cdots K_{16})$. 对加密密钥 $\mathrm{MK} = (K_1, K_2, \cdots K_{16})$ 进行 12 轮 Feistel 密钥变换, 12 轮 Feistel 密钥变换公式如下:

$$\begin{aligned} K_{i,k+1} =& K_{i-1,k} \oplus f_{k-1}[K_{i-1,0}, \cdots, \\ & K_{i-1,k-1}, c_{i,k+1}], \\ & i = 1, \cdots, 12, \quad k = 1, \cdots, 16, \end{aligned} \tag{3}$$

其中, $f_0 = c_0$, $K_{i,16} \equiv K_{i,0}$, $K_{i,17} = K_{i,1}$, $c_{i,0}, \cdots, c_{i,15}$ 是随机选取的 16 字节常数.

密钥变换的结果为 16 字节 $(K_{12,1}, K_{12,2}, \cdots, K_{12,16})$, 根据公式 (4) 对 $(K_{12,1}, K_{12,2}, \cdots, K_{12,16})$ 计算得到 $(y_0, y_1, y_2, \cdots, y_7)$, 将 $(y_0, y_1, y_2, \cdots, y_7)$, 作为 Logisitc 混沌映射的初始条件.

$$\begin{aligned} & (y_0, y_1, y_2, \cdots, y_7) \\ =& \mathrm{RH}(K_{12,1}, K_{12,2}, \cdots, K_{12,16}) \\ & \oplus \mathrm{LH}(K_{12,1}, K_{12,2}, \cdots, K_{12,16}). \end{aligned} \tag{4}$$

加密变换子密钥为:

$$\begin{aligned} z_i =& \mathrm{LH}(K_i) \oplus \mathrm{RH}(K_i) = (z_{i,0}, z_{i,1}, \cdots z_{i,7}), \\ & i = 1, \cdots, 12, \end{aligned} \tag{5}$$

其中, $\mathrm{LH}(K_i)$ 为取左 8 字节函数, $\mathrm{RH}(K_i)$ 为取右 8 字节函数.

2.3 Logistic 映射

Logistic 映射是一维映射, 从数学形式上来看是一个非常简单的混沌映射, 但 Logistic 映射具有极其复杂的动力学行为, 因此在保密通信领域的应用十分广泛, 其数学表达公式如下:

$$X_{n+1} = \mu X_n (1 - X_n), \tag{6}$$

其中 $\mu \in [0,4]$, $X \in [0,1]$. 研究表明当 $X \in [0,1]$ 时, Logistic 映射处于混沌状态, 也就是说, 初始条件 X_0 在 Logistic 映射作用下产生的序列是非周期的、不收敛的.

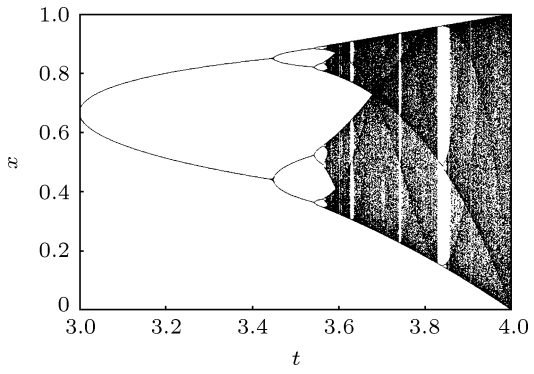

图 3 Logistic 映射的序列分叉 - 混沌图

本文利用 Logistic 混沌映射算法产生混沌映射替换表 g, 混沌映射替换表 g 用 16 进制数值表示, 混沌映射初始条件为 $(y_0, y_1, \cdots, y_7)$, 由上一步的密钥变换得到.

采用 Logistic 混沌映射将 8 字节实数转换为 1 字节整数, 公式如下所示:

$$g(y_n) = y_{n+1} = \frac{y_n(2^{128} - y_n)}{2^{126}}, \tag{7a}$$

$$g'(y_n) = g(y_n) \oplus 00000000000000FF, \tag{7b}$$

$$g(i) = g'(y_n), \quad i = 0, 1, 2, \cdots, 255, \tag{7c}$$

混沌映射替换表 g 为:

$$\begin{aligned} f_j =& \{F(x_1 \oplus x_2 \oplus \cdots \oplus x_j \oplus z_j) \to g(i)\}, \\ & i = 0, \cdots, 255, \quad j = 0, \cdots, F. \end{aligned} \tag{8}$$

2.4 Feistel 加、解密算法

明文加密算法使用了 12 轮的 Festiel 算法进行加密, Festiel 算法在明文加密部分的具体算法如下: i 为加密轮, $i = 1, \cdots, 12$; k 为分组字节长, $k = 1, \cdots, 8$. 每次加密和解密 64 位明文, 将 64 位明文分组, 每组 8 字节, 明文为 $B_i = x_{i,0}, x_{i,1}, \cdots, x_{i,7}$, 加密算法采用 12 轮 Feistiel 加密变换, 具体算法如下:

第一轮:

$$\begin{aligned} x_{1,2} =& x_{0,1} \oplus f_0[z_{0,0}], \quad f_0[z_{0,0}] = z_{0,0}, \\ x_{1,3} =& x_{0,2} \oplus f_1[x_{0,1}, z_{0,1}] \\ & \vdots \\ x_{1,9} =& x_{0,8} \oplus f_7[x_{0,1}, x_{0,2}, x_{0,3}, x_{0,4}, x_{0,5}, x_{0,6}, \\ & x_{0,7}, z_{0,7}], \\ x_{0,8} =& x_{0,0}, \\ x_{1,1} =& x_{1,9}, \end{aligned}$$

第二轮:

$$\begin{aligned} x_{2,2} =& x_{1,1} \oplus f_0[z_{1,0}], \quad f_0[z_{1,0}] = z_{1,0}, \\ x_{2,3} =& x_{1,2} \oplus f_1[x_{1,1}, z_{1,1}], \\ & \vdots \\ x_{2,9} =& x_{1,8} \oplus f_7[x_{1,1}, x_{1,2}, x_{1,3}, x_{1,4}, x_{1,5}, x_{1,6}, \\ & x_{1,7}, z_{1,7}], \\ x_{1,8} =& x_{1,0}, \\ x_{2,1} =& x_{2,9}, \\ & \vdots \end{aligned}$$

第十二轮:

$$\begin{aligned} x_{12,2} =& x_{11,1} \oplus f_0[z_{11,0}], \\ f_0[z_{1,0}] =& z_{1,0}, \\ x_{12,3} =& x_{11,2} \oplus f_1[x_{11,1}, z_{11,1}], \\ x_{12,4} =& x_{11,3} \oplus f_2[x_{11,1}, x_{11,2}, z_{11,2}], \\ & \vdots \\ x_{12,9} =& x_{11,8} \oplus f_7[x_{11,1}, x_{11,2}, x_{11,3}, x_{11,4}, \\ & x_{11,5}, x_{11,6}, x_{11,7}, z_{11,7}] \\ x_{11,8} =& x_{11,0}, \\ x_{12,1} =& x_{12,9}, \end{aligned}$$

$f_1, \cdots, f_7$ 函数形式为:

$$\begin{aligned} f_j =& f(x_1, \cdots x_j, z_j) \\ =& \{F(x_1 \oplus x_2 \oplus \cdots \oplus x_j \oplus z_j) \to g(i)\}, \\ & j = 1, \cdots, 7 \end{aligned}$$

其中, $\to$ $g(i)$ 表示用混沌映射替换表 g 中的值进行替换, 经过 12 轮 Festiel 变换得到的密文为: $x_{12,2}, x_{12,3}, x_{12,4}, x_{12,5}, x_{12,6}, x_{12,7}, x_{12,8}, x_{12,9}$.

解密过程是加密过程的逆变换:

$$\begin{aligned} x_{i-1,k} =& x_{i,k+1} \oplus f_{k-1}[x_{i-1,1}, \cdots, \\ & x_{i-1,k-1}, z_{i-1,k-1}], \\ f_0 =& z_{i,0}, \\ x_8 =& x_0, \\ x_1 =& x_9, \end{aligned} \tag{9}$$

3 混沌加密系统实验

混沌加密系统的硬件开发平台采用 Xilinx 公司的 ISE 软件进行开发, ISE 软件是使用 Xilinx 的 FPGA 平台的必备的设计工具, 它可以完成 FPGA 开发的全部流程, 包括设计输入、仿真、综合、布局布线、生成 BIT 文件、配置以及在线调试等, 功能非常强大. ISE 软件的功能完整, 使用方便, 能够提供最佳的时钟布局、更好的封装和时序收敛映射, 从而获得更高的设计性能. 使用 ISE 开发软件将上述的加密算法利用 Verilog HDL 语言进行编写、仿真和封装, 这样计算机可通过 USB 接口与 FPGA 开发板的 USB 接口通信, 能够将需要加、解密的明文数据通过 FPGA 开发板的 USB 接口传输到加密芯片, 实现对明文数据的加、解密. 我们对混沌加密系统进行了两种实验:

1) 对需要加密的文字, 包括字母、数字、汉字等进行加密, 原文是 “中华人民共和国 abcd1234”, 加密之后的密文变为: “抗颐、獯雄婴袚 □“X[Z]”.

2) 直接对需要加、解密的文件进行加、解密, 原文件、加密文件和解密文件如图 4—6 所示, 从图可见: 文件的加、解密的效果很好, 这说明本文提出的算法对密钥变化具有高度敏感性, 该算法达到了扩散、置乱和混淆的保密效果, 从而证明基于混沌和传统加密相结合的保密方法有效性, 并且其实验装置已经通过互联网络的保密试验取得了成功.

4 总 结

本文提出的混沌加密系统在加密算法方面将混沌加密算法和传统加密算法相结合, 混沌加密算法中使用了两种混沌映射进行迭代, 分别是 Henon 映射和 Logistic 映射, Henon 映射用于产生初始密钥的迭代, 而 Logistic 映射则是用于产生置换表, 传统加密算法方面采用了 Feistel 加、解密变换. 混沌

图 4 原文件图

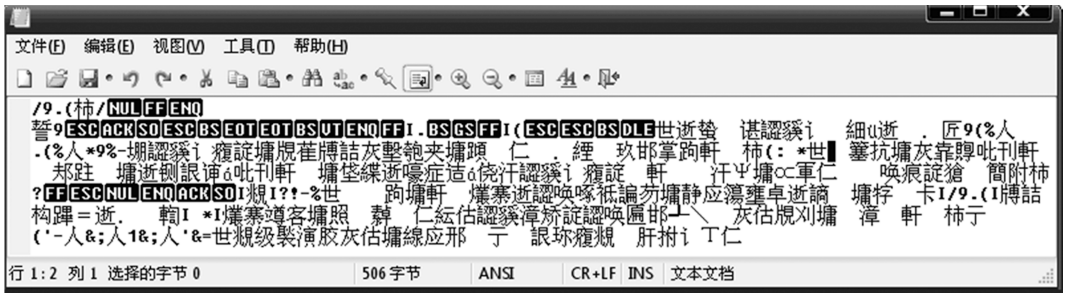

图 5 加密文件图

图 6 解密文件图

加密系统的加密算法复杂度、抗穷举破译性能更高, 并且算法采用 Verilog HDL 语言进行编写, 可移植到其他 FPGA 开发板上. 混沌加密系统的硬件采用的是 Xilinx 公司的 FPGA 开发板, 混沌加密系统通过访问 FPGA 开发板的 USB 接口, 将需要加、解密的数据通过 USB 接口发往加密芯片, 并且能将加、解密结果实时保存在计算机上. 经过多项数据加、解密测试证明, 我们提出的混沌加密系统具有算法抗破译性强、精度高、处理速度快、操作简单、用途广泛的优点, 还能够根据用户的需要对混沌加密系统的算法进一步进行优化, 满足用户不同的需要, 对于通过互联网络进行混沌保密通信, 有一定的应用潜力.

[1] Ott E, Grebogi C, York J A 1990 *Phys. Rev. Lett.* **64** 1196

[2] Pecora L M, Carroll T L 1990 *Phys. Rev. Lett.* **64** 821

[3] Ditto W L, Rauseo S N, Spano M L 1990 *Phys. Rev. Lett.* **65** 3211

[4] Lau F C M, Tse C K 2003 *Chaos-Based Digital Commmunication System* (New York: Springer-Verlag) p1

[5] Fang J Q 2002 *Mastering Chaos and Developing High-New Technology* (Beijing: Atomic Energy Press) p1 (in Chinese) [方锦清 2002 驾驭混沌与发展高新技术 (北京: 原子能出版社) 第 1 页]

[6] Zhao G, Fang J Q 2003 *Prog. Phys.* **23** 212 (in Chinese) [赵耿, 方锦清 2003 物理学进展 **23** 212]

[7] Fang J Q 2010 *J. Syst. Eng.* **25** 725 (in Chinese) [方锦清 2010 系统工程学报 **25** 725]

[8] Fang J Q, Zhao G 2009 *Chin. New Tech. Prod.* **154** 18 (in Chinese) [方锦清, 赵耿 2009 中国新技术新产品 **154** 18]

[9] Huang E Z, Yu S M, Zhou W J 2008 *Commun. Tech.* **12** 343 (in Chinese) [黄泽锷, 禹思敏, 周武杰 2008 通信技术 **12** 343]

[10] Wang M, Qiu H B, Zheng J Y 1997 *Inf. Sec. Commun.* **1** 8 (in Chinese) [王玫, 仇洪冰, 郑继禹 1997 信息安全与通信保密 **1** 8]

[11] Zhao G, Fang J Q 2003 *Nat. Mag.* **25** 21 (in Chinese) [赵耿, 方锦清 2003 自然杂志 **25** 21]

[12] Zhang Z X, Yu S M 2010 *Acta. Phys. Sin.* **59** 3017 (in Chinese) [张朝霞, 禹思敏 2010 物理学报 **59** 3017]

[13] Zhao G, Fang J Q 2003 *Prog. Phys.* **23** 212 (in Chinese) [赵耿, 方锦清 2003 物理学进展 **23** 212]

[14] Ming F H, Wang E R 2010 *Acta. Phys. Sin.* **59** 7657 (in Chinese) [闵富红, 王恩荣 2010 物理学报 **59** 7657]

[15] Zhou W J, Yu S M 2010 *Acta. Phys. Sin.* **58** 113 (in Chinese) [周武杰, 禹思敏 2010 物理学报 **58** 113]

Research of Chaotic encryption system based on FPGA technology*

Liu Qiang[1)] Fang Jin-Qing[1)†] Zhao Geng[2)] Li Yong[1)]

1) (*Department of Nuclear Technology Application, China Institute of Atomic Energy, Beijing* 102413*, China*)

2) (*Department of Computer Science and Technology, Beijing Electronic Science and Technology Institute, Beijing* 100070*, China*)

(Received 7 October 2011; revised manuscript received 7 December 2011)

Abstract

In this paper, a kind of chaos encryption system is presented based on chaotic encryption algorithm and traditional encryption algorithm, and hardware is implemented by using the FPGA technology. According to discrete and digital technologies, Henon Map and Logistic Map are applied, and chaotic iteration sequence is generated by using Verilog HDL language and FPGA technology. By combining the traditional iteration algorithm, the files are encrypted and decrypted. Based on Xilinx FPGA exploitation platform, secret communication experiments on Internet are successefully. The devise has potential prospective applications in internet secrecy communication.

Keywords: chaos, encrypt, decrypt, FPGA

PACS: 05.45.Vx

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60874087, 61174151, 61170037, 60773120), the Beijing Natural Science Foundation (Grant No.4092040) and the China Institute of Atomic Energy Dean Foundation (Grant No. YZ2011-20).

† E-mail: fjq96@126.com