基于神经网络算法的组合序列密码芯片

丁 群[1], 彭喜元[1], 杨自恒[2]
(1. 哈尔滨工业大学自动化测试与控制研究所, 黑龙江哈尔滨 150001; 2. 黑龙江大学电子工程学院, 黑龙江哈尔滨 150080)

摘 要: 序列密码一直是密码学中最重要的加密方式之一. 现提出基于神经网络算法的序列密码加密芯片设计, 在保留原序列良好统计特性基础上, 使输出序列的周期性和线性复杂性均有增加. 利用 FPGA 技术进行序列密码芯片电路设计, 灵活运用现代电子设计方法实现了运算功能和时序分配. 逻辑综合仿真结果验证了芯片电路的正确性. 该研究结果有助于序列密码算法在信息安全及现代保密通信设备中的应用.

关键词: 序列密码; 神经网络; 加密芯片; FPGA
中图分类号: TP309. 7 文献标识码: A 文章编号: 0372-2112 (2006) 03-0409-04

The Cipher Chip of Combining Stream Based on the Neural Network Algorithm

DING Qun[1], PENG Xi-yuan[1], YANG Zi-heng[2]
(1. Department of Automatic Test and Control, Harbin Institute of Technology, Harbin, Heilongjiang 150001, China;
2. Electronic Engineering School, Heilongjiang University, Harbin, Heilongjiang 150080, China)

Abstract Stream cipher has always been one of the most important encryption methods in cryptography. Now we bring in a stream cipher encryption chip design which is based on neural network algorithm and it not only contains the good statistics of m-sequence but also enhances the periodicity and linear complexity of the output sequences. We use FPGA technology to complete the stream cipher circuit design and the modern electronic design method to smoothly realize operation functions and sequential assignment. The result of logical synthesis simulation verifies the correctness of the chip circuit. This research is helpful to the application of stream cipher algorithm in information security and modern secure communication equipment.

Key words stream cipher; neural network; encryption chip; FPGA

1 引言

在密码学领域, 利用密码技术对传输信息进行加密发送、解密接收, 是一种行之有效的方法. 密码学发展至今已有许多优秀的算法发明并得到应用, 例如私钥密码体制中的 DES密码、IDEA 密码、序列密码; 公钥密码体制中的 RSA 密码、椭圆曲线密码等等, 他们各有设计特点和对应的应用领域, 其中序列密码一直是密码学中最重要的加密方式之一[1]. 利用组合 LFSR 序列作为序列密码的前馈电路, 可充分利用 m 序列的良好统计特性和加大输出序列周期和线性复杂度的优势, 但如何在保证前馈电路输出统计特性不被破坏的基础上, 置换与混乱输出关系, 增强密码的保密性仍是从事该领域研究所思考的问题. 传统方法是利用非线性函数对前馈电路输出进行变换, 但在函数设计与生成速度上制约了其发展; 利用某 LFSR 序列产生控制信号去控制并行 LFSR 序列, 这种形式电路如 Geffe发生器、Jenning发生器、交错停走式发生器等等, 易受到相关性攻击[2], 应避免在保密强度要求高的部门应用. 随着现代科学技术的发展, 将神经网络、混沌等算法融入密码学的研究已不断深入[3], 伴随着数字化技术和大规模集成电路的快速发展, 一些算法不仅停止在理论研究与模拟仿真实验上, 利用硬件电路进行设计并实现已逐渐成为事实. 现提出基于神经网络算法的序列密码芯片设计, 并利用 FPGA技术实现该芯片电路, 此电路可为神经网络或混沌等算法的组合序列密码应用奠定基础, 有助于序列密码算法在信息安全及现代保密通信设备中的应用.

收稿日期: 2005-03-01; 修回日期: 2005-09-18
基金项目: 哈尔滨市科学研究基金 (No. 2003AFXXJ022)

2 Hopfield神经网络算法

由离散*Hopfield*神经网络构成迭代系统, 由多个*LFSR*作为神经网络 t时刻输入, 依据网络迭代公式可求得网络在 t+1时刻的输出[4], 其中 T_{ij}表示第 j个神经元到第 i个神经元的权值, f(x)为激活函数.

$$O_i(t+1)=f\left(\sum_{\substack{j=1\\ i\neq j}}^{n}T_{ij}O_j(t)\right),\quad i=1,2,\cdots,n \tag{1}$$

$$f(x)=\begin{cases}1, & x\geqslant 0\\ 0, & x<0\end{cases} \tag{2}$$

设网络在 t时刻, 输入 n维向量为 $X(t)=\{x_1,x_2,\cdots\cdots,x_n\mid x_1x_2\cdots\cdots x_n\in\{0,1\}\}$, 神经网络中 p个 n维记忆模式为 $\xi=\{\xi_\mu\mid\mu=1,2,\cdots\cdots,p;\ \xi\in\{-1,1\}\}$, P=2n+1, 采用*Hebb*规则的外积和法进行权值设计[5,6], 为了方便硬件制作再将联接权值离散化.

$$T_{ij}=\sigma\left(\frac{1}{n}\sum_{\mu=1}^{P}\xi_{\mu i}\xi_{\mu j}^{T}\right)=\sigma\left(\frac{1}{n}\sum_{\mu=1}^{P}(2\zeta_{\mu i}-1)(2\zeta_{\mu j}-1),\ \zeta\in\{0,1\}\right) \tag{3}$$

$$\sigma(x)=\begin{cases}+1, & x>0\\ 0, & x=0\\ -1, & x<0\end{cases} \tag{4}$$

根据证明将 $\zeta=\{A,B,C\}$, 即 P=2n+1向量代入公式(3)可求得联结权值 T_{ij}或权值矩阵 T[5,6], 其中

$A=\{a_i\mid i=1,2,\cdots,n,\ a_i\in\{0,1\}\}$,

$a_1=(\underbrace{1,1,\cdots\cdots,1}_{n/2\text{个}},\underbrace{0,0,\cdots\cdots,0}_{n/2\text{个}})$, $a_i=\Delta(a_1,i-1)$

$B=\{b_i\mid i=1,2,\cdots,n,\ b_i\in\{0,1\}\}$,

$b_1=(\underbrace{1,1,\cdots\cdots,1}_{(n/2)+1\text{个}},\underbrace{1,0,0,\cdots\cdots,0}_{(n/2)-1\text{个}})$, $b_i=\Delta(b_1,i-1)$

$C=[\underbrace{1111\cdots\cdots1}_{n\text{个}}]^T$, $\Delta(\alpha,i)$为 α向量左移 i次.

设输入 n=8, $a_1=[11110000]$, $b_1=[11111000]$

$$A=\begin{bmatrix}1&1&1&1&0&0&0&0\\1&1&1&0&0&0&0&1\\1&1&0&0&0&0&1&1\\1&0&0&0&0&1&1&1\\0&0&0&0&1&1&1&1\\0&0&0&1&1&1&1&0\\0&0&1&1&1&1&0&0\\0&1&1&1&1&0&0&0\end{bmatrix}$$

$$B=\begin{bmatrix}1&1&1&1&1&0&0&0\\1&1&1&1&0&0&0&1\\1&1&1&0&0&0&1&1\\1&1&0&0&0&1&1&1\\1&0&0&0&1&1&1&1\\0&0&0&1&1&1&1&1\\0&0&1&1&1&1&1&0\\0&1&1&1&1&1&0&0\end{bmatrix},\quad C=\begin{bmatrix}1\\1\\1\\1\\1\\1\\1\\1\end{bmatrix}$$

由式(3)、(4)得

$$T=\begin{bmatrix}1&1&0&-1&-1&-1&0&1\\1&1&1&0&-1&-1&-1&0\\0&1&1&1&0&-1&-1&-1\\-1&0&1&1&1&0&-1&-1\\-1&-1&0&1&1&1&0&-1\\-1&-1&-1&0&1&1&1&0\\0&-1&-1&-1&0&1&1&1\\1&0&-1&-1&-1&0&1&1\end{bmatrix}$$

利用联结权阵 T, 由 n个*LFSR*输出代入公式(1)(2), 迭代后可稳定到 P个 n维记忆模式, 通过此记忆模式可对应转换产生神经网络输出. 为了隐藏权值矩阵 T或联结权值 T_{ij}, 引入可置换非齐异性矩阵 H, 置换后新的联结权阵为

$$T'=HTH^T \tag{5}$$

通过改变可置换非齐异性矩阵 H, 根据公式(5)产生新的隐藏权值矩阵 T', 将 T'作为变化后的 T代入公式计算, 可得到不同的记忆模式和转换不同的输出. 此非齐异性矩阵 H在密码算法中可相当于又一级密钥, 当密钥不同时, 进入不同的记忆模式中, 输出序列由此改变, 当密钥相同时, 进入相同的记忆模式, 输出序列相同, 能使解密能正确进行. 通过矩阵 H的选取, 可以模拟不同的非线性函数, 避免了在传统电路设计中, 模拟不同的非线性函数需要变换不同电路的缺陷. 而且如果将此 H矩阵保密, 确定网络中存储信息是很困难的, 随着 H矩阵空间向量增多, 搜索加密信息将更加困难.

3 密码芯片电路设计

由8个*LFSR*序列作为驱动源的组合序列密码电路结构如图1所示. 将神经网络模块、数据选择器模块等视为*Rueppel*序列发生器的非线性函数部分, 这样根据多个*LFSR*序列作为驱动源的特性得知, 当 $LFSR_i$(i=1,2,…,n)的级数 $N_1,N_2,\cdots\cdots,N_n$两两互素且满足一定条件时, 该组合序列输出周期为 $\prod_{i=1}^{n}(2^{N_i}-1)$, 线性复杂度同时接近于 $\prod_{i=1}^{n}(2^{N_i}-1)$[7,8]. 为了使输出序列有尽可能大的线性复杂度, 各 N_i应尽可能接近 N/n, 其中 $N=N_1+N_2+\cdots+N_n$. 当 N_i确定以后, 为使每个 $LFSR_i$(i=1,2,……,n)生成周期为 $2^{N_i}-1$的 m序列, 其充要条件是使其特征多项式为本原多项式.

为验证电路逻辑功能, 在实验中设 8个*LFSR*的级数分别选为: 3,4,5,7,11,13,17,19, 根据实现函数所需硬件最少的原则, 选定 $LFSR_i$(i=1,2,……,8)本原多项式如下:

$f_1(x)=x^3\oplus x\oplus 1$, $f_2(x)=x^4\oplus x\oplus 1$, $f_3(x)=x^5\oplus x^2\oplus 1$,

$f_4(x)=x^7\oplus x\oplus 1$, $f_5(x)=x^{11}\oplus x^2\oplus 1$, $f_6(x)=x^{13}+x^4\oplus x^3\oplus x\oplus 1$, $f_7(x)=x^{17}\oplus x^3\oplus 1$, $f_8(x)=x^{19}\oplus x^5\oplus x^2\oplus x+1$

该组合序列输出周期为 $\prod_{i=1}^{n}(2^{N_i}-1)=4.7631\times10^{23}$, 线性复杂度接近于此周期. 较单个 *LFSR* 输出序列相比, 输出序列周期、密钥选择空间和线性复杂度均大幅度增加.

利用硬件描述语言 *VHDL* 进行编程, 分别从系统级、模块级、寄存器传输级实现自顶向下进行设计, 在程序设计中依次对 *LFSR* 模块、神经网络模块、状态控制模块、寄存器传输级电路模块的输入输出关系、内部工作过程、算法、寄存器传输数据与控制流等功能等进行描述. *LFSR* 模块中 8个移位寄存器的输出作为提供神经网络模块运算的初始数据, 同时送往数据锁存器, 在时序控制电路 (状态机)的控制下变换数据形成序列输出. 神经网络模块对来自组合 *LFSR* 序列的并行输入信号进行迭代, 从而产生数据选择器控制信号, 控制组合 *LFSR* 序列任意输出. 这样既能保持原 m序列良好统计特性, 又能使 *LFSR* 组合序列输出呈现非线性输出特性.

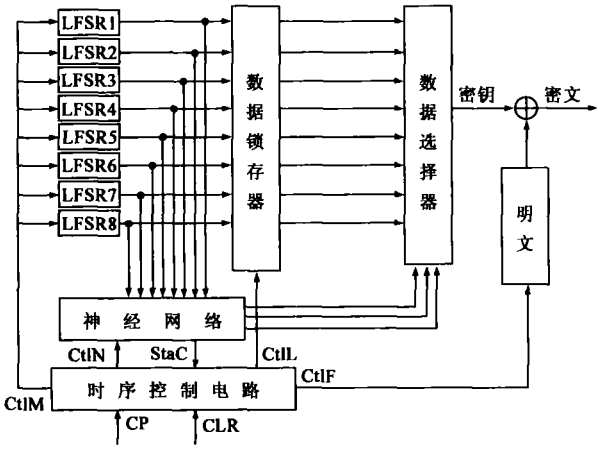

图 1 组合序列密码芯片电路结构图

状态机是控制整个电路时序的模块, 初始化后首先发出 **CtlM** 信号启动 **LFSR** 序列模块工作, 使组合 **LFSR** 序列在时钟的作用下产生一组移位输出信号; 状态机产生 **CtlN** 信号启动神经网络模块进行运算, 当神经网络运算完毕后发出 **StaN** 信号送往状态机模块, 状态机得知该信号后, 确认已运算完毕, 发出信号 **CtlL** 将数据锁存器的内容送往数据选择器模块; 数据选择器模块根据控制端产生信号控制 **LFSR** 序列输出, 该输出序列与明文相异或后产生密文进行发送, **CtlF** 是控制与明文保持同步的信号. 在时序图中 **DOUT1** 至 **DOUT8** 为 8个 **LFSR** 移位寄存器信号, **FIFOUT** 为输出码流速度控制信号, **QData** 为数据选择器输入信号, 其中前 3位为神经网络转换输出的控制信号, 后 8位为 8个 **LFSR** 移位寄存器输出信号.

逻辑综合仿真结果验证其电路的正确性, 组合序列密码芯片时序电路图如图 2所示.

该电路的特点为: (1)利用神经网络的非线性构成数据选择器控制信号, 在保留了原 m 序列良好统计特性基础上, 输出周期和线性复杂度大幅度增加, 达到了非线性变换的目的. (2)神经网络算法非同于以往的加密算法, 同混沌密码算法都是近年来融入密码系统中新的研究分支, 使研究密码方法的范围扩大, 为密码破译者增加了难度. (3)该电路用 **FPGA** 技术进行设计, 灵活的运用状态机概念实现电路的时序分配, 使硬件电路与数学算法有机结合一起, 另外由于 **FPGA** 技术的特点使所设计电路易移植和更改, 这对密码的设计十分有利. (4)在原有密钥的基础上, 神经网络非齐异性矩阵 **H** 可作为二级密钥, 这使密钥总数大有提高, 增强了密码的安全性.

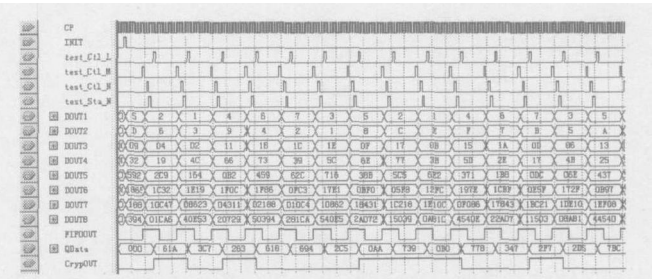

图 2 组合序列密码芯片时序电路图

4　加密芯片电路输出测试

利用 **ALTERA** 公司的 **QuartusII** 工具和目标芯片 **EP20K300EQC240** 设计[9], 对逻辑综合结果进行仿真后完成硬件下载功能, 共占用逻辑单元 **524** 个, 存储位 **128** 个. 为验证其输出序列的平衡性、相关性及游程等特性, 对下载后输出序列利用 **Agilent1693A** 逻辑分析仪进行数据测试、存储并利用 **MATLAB** 进行统计分析.

在实际应用中, 如果平稳随机序列满足各态历经性, 统计均值可用时间均值代替. 取一个有限的计算系统能够承受的时间均值和时间自相关序列, 并用它们作为统计均值和统计自相关序列的估值[10]. 根据此理论设定一初始数据, 在一段时间内观测其输出序列的平衡性、游程性、自相关性及互相关性, 基本满足密码序列输出要求, 现以自相关特性测试为例进行说明.

将神经网络序列转化成 $X=\{x(n)\mid n=0,1,2,\cdots\cdots,x(n)\in\{-1,1\}\}$, 使序列输出概率密度关于 0对称. 取测试序列 $N=12\times10^4$, 并利用自相关函数的估值公式 (6)进行仿真, 得到该神经网络序列的自相关特性如图 3所示. 可看出该密码序列输出具有较好的自相关特性, 在 0值处

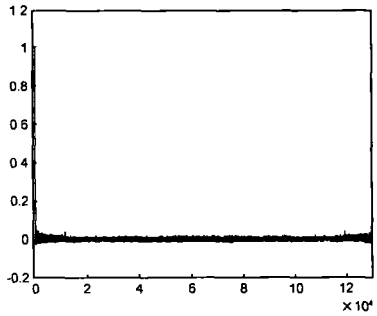

图3　输出序列自相关特性

峰值尖锐,其他值近似为 0,类似于 δ函数.

$$R_{XX}(m)=\frac{1}{N}\sum_{n=0}^{N-|m|-1}x(n)x(n+|m|) \qquad (6)$$

5 结论

利用离散 *Hopfield* 神经网络算法作为 *LFSR* 组合序列密码控制电路,在保持原 m序列良好的统计特性基础上达到非线性变换的目的,同时由于神经网络运算矩阵 H 的改变产生不同的输出,扩大密钥空间,增加了算法的复杂性.所增加的密钥空间只能限制在非齐异性矩阵 H范围内,如何进一步扩大密钥空间需要研究;另外当神经网络输入 $n>8$时,迭代次数增多,运算速度明显变慢,在实时加密时需要考虑与选择.此加密芯片经 *VHDL* 设计并生成,整个时序由状态机控制,逻辑关系符合电路设计要求.此研究结果有助于加快神经网络加密芯片的应用,也有助于其他算法的序列密码加密芯片设计,例如混沌序列密码芯片等,使加密算法更灵活有效地应用到信息安全和现代保密通信设备中.

参考文献:

[1] 卢开澄. 计算机密码学-计算机网络中的数据保密与安全[M]. 北京:清华大学出版社, 1998. 185-195.
Lu Kaicheng. Computer Cryptography-The Data Encryption and Security in Computer Network[M]. Beijing: Tsinghua University Press, 1998. 185-195. (in Chinese)

[2] Bruce Schneier. 应用密码学[M]. 吴世忠, 等译. 北京:机械工业出版社, 2000. 264-269.
Bruce Schneier. Application Cryptography[M]. Translated by Wu Shizhong et al. Beijing: Mechanical Technology Press, 2000. 264-269. (in Chinese)

[3] 李红达,冯登国. 复合离散混沌动力系统与序列密码体系[J]. 电子学报, 2003, 31(8): 1209-1212.
Li Hongda, Feng Dengguo. Complex discrete chaotic dynamic system and stream cipher System[J]. Dianzi Xuebao, 2003, 31(8): 1209-1212. (in Chinese)

[4] 韩力群. 人工神经网络理论、设计及应用[M]. 北京:化学工业出版社, 2002. 98-103.
Han Liqun. Artificial Neural Network Theory, Design and Application[M]. Beijing: Chemistry Technology Press, 2002. 98-103. (in Chinese)

[5] Chi-kwong Chan, L M. Cheng. The Convergence Properties of a Clipped Hopfield Network and its Application in the Design of Keystrem Generator[J]. IEEE Transactions on Neural Networks, 2001, 12(2): 340-348.

[6] Chi-kwong Chan, L M. Cheng. The CHNN nonlinear combination generator[A]. The 5th IEEE International Conference on Electronics, Circuits and Systems. Lisbon, Portugal, 1998, 2: 257-260.

[7] M. Tatebayashi, N. Matsuzaki, D B. Newman. A cryptosystem using digital signal processors for mobile communication[A]. IEEE International Conference on World Prosperity Through Communications. Boston, 1989, 3: 1145-1148.

[8] Emil Simion, N. Constantinescu. Complexity computations in code cracking problems[A]. The 24th International Spring Seminar on Electronics Technology. Romania, 2001. 225-232.

[9] 潘松, 黄继业, 王国栋. 现代 DSP技术[M]. 西安: 西安电子科技大学出版社, 2003. 57-91.
Pan Song, Huang Jiye, Wang Guodong. Modern DSP Technology[M]. Xi'an: XIDIAN University Press, 2003. 57-91. (in Chinese)

[10] 赵淑清, 郑薇. 随机信号分析[M]. 哈尔滨: 哈尔滨工业大学出版社, 1999. 80-86.
Zhao Shuqing, Zheng Wei. Pseudorandom Signals Synthesis[M]. Harbin: Harbin Institute of Technology Press, 1999. 80-86. (in Chinese)

作者简介:

丁 群 女, 1957年出生于黑龙江省哈尔滨市,黑龙江大学电子工程学院教授,目前在哈尔滨工业大学自动化测试与控制系攻读博士学位.主要从事电路与系统、硬件加密技术等方面的研究工作. **E-mail: ding-qun@263.net**

彭喜元 男, 1961年出生于内蒙古四子王旗,哈尔滨工业大学自动化测试与控制系教授,博士生导师,主要从事自动测试技术、智能故障诊断及信息安全等方面的研究工作.
E-mail: pxy@hit.edu.cn