文章编号：1000-5013(2014)05-0519-04 **doi**：10.11830/ISSN.1000-5013.2014.05.0519

采用 OHNN 和 M-LFSR 的字序列密码加密方案

蔺小梅，李国刚，张泽普

（华侨大学 信息科学与工程学院，福建 厦门 361021）

摘要： 结合反馈型离散 Hopfield 神经网络(HNN)和改进型的线性反馈移位寄存器(M-LFSR)的优点，提出基于 OHNN 和 M-LFSR 的字序列密码. 该方案利用离散 Hopfield 神经网络的混沌吸引子对改进型线性反馈移位寄存器的非线性选择输出，实现加密. 安全性分析与仿真验证表明：该算法构造的伪随机序列具有良好的随机性、复杂度等特点，满足密码学的要求.

关键词： 序列密码；线性反馈移位寄存器；离散型 Hopfield 神经网络；混沌吸引子

中图分类号： TN 918.4 **文献标志码**： A

序列密码实质上是一个密钥流发生器，通过将密钥流序列与明文异或完成加密和解密. 传统序列密码软件实现速度慢、效率低[1]，而为了满足高速通信和数据大吞吐量的需求，一类基于字的序列密码被提出[2]. 本文提出由一个改进型的线性反馈移位寄存器(M-LFSR)、一个数据选择器和离散 Hopfield 神经网络(HNN)[3]组成的字序列密码加密方案.

1 理论基础

1.1 改进型线性反馈移位寄存器

传统 LFSR 结构存在合成随机数速度受随机数字长限制的缺陷，即一个时钟通常只能产生 1 bit 的输出，而现代处理器每个时钟可以处理多达 64 bit 的操作，这大大降低了系统的运行效率. 为了弥补这个缺点，需要对传统 LFSR 做出改进.

假设一个 LFSR 的特征多项式为 $f(x)=x^p+x^q+1$，则其所产生的随机序列[4-5]为

$$U_k = a_k + a_{k+1}x + \cdots + a_{k+p-1}x^{p-1}. \tag{1}$$

其中：$\{a_i\}(i=k,k+1,k+2,\cdots)$，$u_k=(k=0,1,2,\cdots)$为多项式，其次数小于 p，系数为 0 或 1，当 $k=0$ 时，$u=0$. 由式(1)可以推出

$$u_{n+p} = xu_{n+p-1}(\mathrm{mod}\ x^p+x^q+1) = u_{n+p}+u_n(\mathrm{mod}\ x^p+x^q+1). \tag{2}$$

式(2)中：$n=0,1,2,\cdots$. 若令 $w_k=(a_k,a_{k+1},\cdots,a_{k+p+1})$，$p>2q$，则可以通过式(2)推导出系数 w_k 之间的递推关系为 $w_{n+p}=w_{n+q}\oplus w_n$. 利用该递推关系式可以得到

$$\begin{cases} a_{n+p} = a_n \oplus a_{n+q}, \\ a_{n+p+(p-q-1)} = a_{n+p-q-1} \oplus a_{n+p-1}, \\ a_{n+p+(p-q)} = a_{n+p-q} \oplus a_{n+p} = a_{n+p-q} \oplus [a_n \oplus a_{n+q}], \\ a_{n+2p-1} = a_{n+p-1} \oplus a_{n+p-q-1} = a_{n+p-1} \oplus [a_{n+q-1} \oplus a_{n+2q-1}]. \end{cases}$$

这表明 w_k 经过模 2 加运算得到 w_{n+p}. 假设 A 和 B 是长度为 L 的寄存器，且满足 $L=p$，$p>2q$.

根据以上算法，改进传统 LFSR，其结构如图 1 所示. 从图 1 可知：对于传统型 LFSR 要输出一个 L 位的随机序列，需要 L 个时钟周期，而 M-LFSR 只需要一个时钟周期就可完成，其吞吐率约为传统型 LFSR 的 L 倍. 它不仅很好地弥补了传统 LFSR 合成随机数速度受随机数字长制约的缺陷，而且提高了系统运行效率. 文献[6]表明：M-LFSR 产生的伪随机性序列功率谱平坦，自相关函数趋于零，能通过均

收稿日期： 2013-07-18

通信作者： 李国刚(1973-)，男，副教授，主要从事集成电路设计与信息安全的研究. E-mail：lgg@hqu.edu.cn.

匀性检验、独立性检验等统计检验,具有良好的统计特性.

1.2 离散神经网络模型

文中采用工作中过饱和状态下的离散型 Hopfield 神经网络.假设每个神经元状态只为 0 或 1,那么它的下一个状态 $S_i(t+1)$ 取决于当前各神经元的状态 $S_i(t)$,即

$$S_i(t+1)=\sigma\Big(\sum_{j=0}^{N-1}T_{i,j}(t)S_i(t)+\vartheta_j\Big),\qquad i=0,1,\cdots,N-1.$$

上式中:神经元 i 的阈值为 ϑ_j,与神经元 j 之间的联接权值为 $T_{i,j}$;$\sigma(x)$为任一非线性函数,设为单位阶跃函数.则系统在 t 时刻的能量函数为

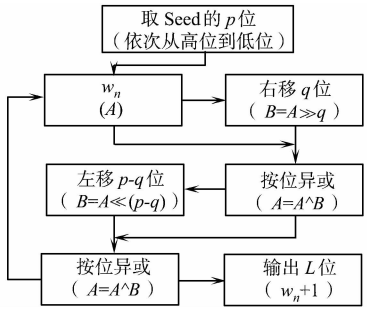


图 1 改进型 LFSR 结构图

Fig. 1 Structure of M-LFSR

$$E(t)=\frac{1}{2}\sum_{i,j}T_{i,j}(t)S_i(t)S_j(t). \tag{3}$$

在文献[7]中,Hopfield 已证明式(3)是随系统状态的演进而单调下降,最终会达到一种稳定状态,即混沌吸引子,且其吸引域所包含的状态消息间存在不可预测的关系.如果改变联结权值矩阵 $\boldsymbol{T}$,则吸引子及其相应的吸引域都会发生改变.在引入随机变换矩阵 $\boldsymbol{H}$ 后,原初始状态 S 和吸引子 S_μ,可由 $\hat{S}=S\boldsymbol{H}$ 和 $\hat{S}_\mu=S_\mu\boldsymbol{H}$ 更新,得到新的初始状态 S 和吸引子 $\hat{S}_\mu$,而且这个过程是单向、不可逆的[8].

2 系统结构及原理

所提出的新的字序列密码加密方案,其结构由 M-LFSR,N 阶离散 Hopfield 神经网络和数据选择器组成,如图 2 所示.系统的工作原理:M-LFSR 作为系统驱动部分,产生随机数,OHNN 作为系统的控制单元,是一个单向陷门函数,控制数据选择器对伪随机数的非线性选择,得到的初始矩阵,网络演变后生成混沌吸引子.数据选择器根据混沌吸引子对随机数进行非线性选择,输出伪随机数,经过编码后,得到密钥序列.密钥序列一方面经过扰动函数,反馈到 M-LFSR 扰动更新 M-LFSR;另一方面,同明文序列异或产生密文序列,实现加密.

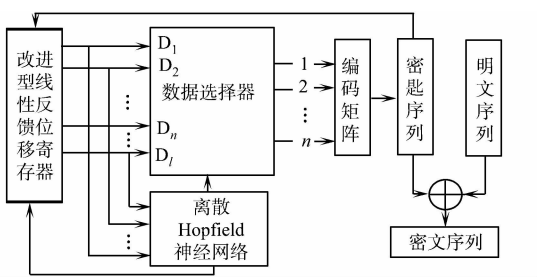


图 2 系统结构图

Fig. 2 System structure

神经网络采用 N 阶的,吸引子总数为 $2N$,均分为个数相等的 α 和 β 两类[9].文中将混沌吸引子分类,选择 N 路数据开关,故混沌吸引子和数据是 2 对 1 的映射关系,吸引子和数据选择器里面的 S 盒的映射关系是在系统运行过程中建立的.另外,还有一路初始化开关.数据选择器将系统产生的随机数转化为二进制(L 位),然后随机选择 $A(L,M)$中的 $N+1$ 种($M\leqslant L$),M 为密钥序列宽度.在这些排列组合中,一种作为初始化开关,其他 N 种作为数据开关.S 盒的数据由 $A(L,M)$随机产生的.文中拟采用的阶数 N 为 16.

3 系统安全性能分析及测试

3.1 抗暴力攻击

若文中采用对称加密,由于离散神经网络由 N 个神经元所组成的,则每个随机变换矩阵 H 都存在 $N!$ 种可能,即它的密钥空间为 $N!$.若采用穷举法攻击,要得到目标随机变换矩阵,需要运行 $N!$ 次.假设采用每秒钟能计算 10^5 个变换矩阵的专业计算机,当 $N=32$ 时,遍历一次就需要 10^{20} MPIS Years,远远超出现在所能接受的安全水平,即 10^{12} MPIS Years[3].

若攻击者绕过 HNN 复杂的 NP 问题,转而针对 M-LFSR 分析.在此种情况下,系统开关选择每个时钟都在变化,约有 1.26×10^{22}($A(32,16)$)种选择.攻击者要尝试 1.26×10^{22} 次,才能得到一个时钟的密钥序列.假设采用我国的"天河一号"超级计算机,运算速度是 2.570×10^{17} 次·s^{-1},每年也只能解密出约 1 KB 的信息.在现有计算机计算水平下,这种攻击方式是徒劳的.

3.2　抗矩阵分析和差分分析

若采用公钥加密体制，文献[3]从正交分解、奇异值分解和三角分解出发，逐一论证了 HNN 网络的安全性是可靠的. 由于整个密码系统是不规则的，在加密过程中，即使同一明文序列加密后，得到的密文序列也不可能是相同的 . 而且，在解密过程采用自吸引的方法，故差分密码分析对该算法是无效的.

3.3　随机性测试

采用为 RedHat 9.0 测试平台，依据美国国家标准与技术委员会(NIST)制定的考评随机和伪随机序列的测试标准 SP800-22. 首先在 VC 上得到的密钥序列样本，然后将测试样本为 100 组，每组 10^5 个数据，最后在测试平台上逐一得到测试指标，结果如表 1 所示 . 表 1 中：P_H 为最高值；P_L 为最低值 . 设 $\alpha=0.01$，若计算出的 P 值小于 α，则测试序列不为随机序列；反之，则不是随机序列[10]. 从表 2 可知：算法产生的密钥序列具有较好的随机性.

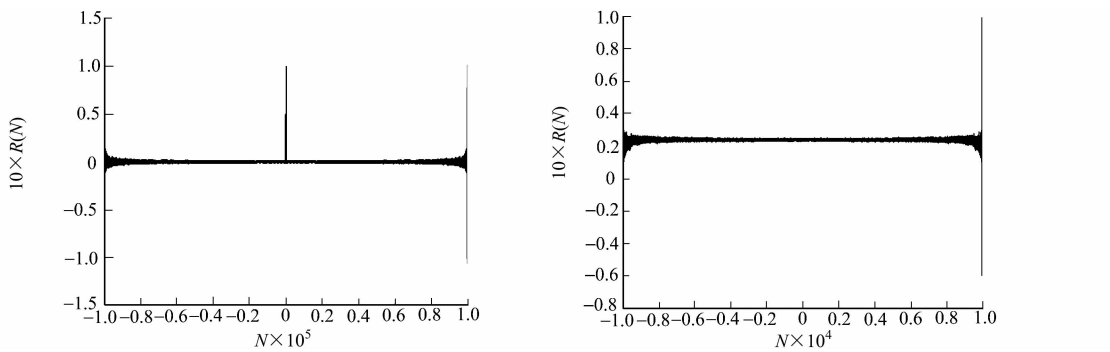
表 1　随机序列的随机性测试

Tab. 1　Random test of random sequence

测试样本	P_H	P_L	测试样本	P_H	P_L
Frequency	0.984 043	0.595 549	Block Frequency	0.971 897	0.679 024
Cumulative Sums	0.984 242	0.410 556	Runs	0.999 078	0.333 213
Longest Run of Ones	0.989 068	0.496 386	Rank	0.949 536	0.159 044
Discrete Fourier Transform	0.926 884	0.118 754	Non-Overlapping Template	0.978 072	0.173 082
Overlapping Template	0.965 781	0.286 319	Linear Complexity Test	0.933 851	0.178 718
Universal	0.966 669	0.144 169	Approximate Entropy	0.950 958	0.115 881
Random Excursions	0.981 982	0.200 173	Random Excursions Variant	0.981 792	0.165 642
Serial	0.770 014	0.102 229			

3.4　相关性测试

1) 自相关测试 . 选取内容重复的明文，如“钓鱼岛自古以来就是中国的领土!”，经加密后，得到一份密钥序列. 若自相关函数变化越小，表明序列随机性越好[10]. 测试结果如图 3(a)所示 . 图 3(a)表明：自相关函数变化很小，序列随机性好. 2) 互相关测试 . 随机改变矩阵 $\boldsymbol{H}$ 其中的一位，得到另一份密钥序列样本. 若互相关函数越接近零，说明两个序列越互不相关[11]. 测试结果如图 3(b)所示 . 图 3(b)表明：两份密钥序列的互相关系数很小，相关度很低，一个微小改变可以引起雪崩效应.



(a) 自相关系数　　(b) 互相关系数

图 3　相关性测试

Fig. 3　Self-correlation test

3.5　加解密测试

测试平台为 Lenovo Z460，CPU 为 Intel(R) Core(TM)i5，内存 2.00 GB. 系统中，M-LFSR 的特征函数为：$f(x)=x^{33}+x^{13}+1$，$p=33$，$q=13$，$L=32$，密钥序列宽度 $M=16$. 在此成功完成对内容为古诗《静夜思》txt 文档的加解密测试. 加密过程中计算 1 次混沌吸引子就可以加密 1 bit 明文信息，对 txt 文档实际测量的加解密速度为 423,412 $b \cdot s^{-1}$，是文献[12]的 17 倍，是文献[3]的 7 倍.

4　结论

提出的基于 OHNN 和 M-FSR 的字序列密码加密算法不仅可以在不同的密码体制中实现，而且密

钥序列的宽度可以调整,最高可达到 p,并由特征多项式决定.所涉及的该方案不仅需要具有良好密码学特性,较高软件实现效率,而且由于每次输出的是一个字而非一个比特,其吞吐量大幅度提升[12],还解决了 LFSRs 之间的延迟和本原多项式难选取的问题[13],保证了其安全.

新方案经理论分析和软件测试,具有可靠的安全性和较高的效率,在不影响系统的速度的前提下,可以增加神经网络阶数,提高系统复杂度,使系统更加安全,为通信加密提供了一种新的选择.

参考文献:

[1] FENG Deng-guo,FENG Xiu-tao,ZHANG Wen-tao,et al. Loiss: A byte-oriented stream cipher[J]. Lecture Notes in Computer Science,2011,6639,109-125.

[2] EKDAHL P,JOHANSSON T. A new version of the stream cipher SNOW[J]. Lecture Notes in Computer Science,2002,2595,47-61.

[3] 刘年生,郭东辉.基于神经网络混沌吸引子的公钥密码算法安全性分析及其实现[J].厦门大学学报:自然科学版,2007,46(2):187-193.

[4] GAO Hui-xuan. Statistical computing[M]. Beijing:Peking University Press,1996:80-120.

[5] MATTEIS A D,PAGNUTTI S. Long rang correlation in linear and nonlinear random number generation[J]. Parallel Computing,1990,14(1):207-210.

[6] 崔嵬,李承恕.线性反馈移位寄存器的改进算法及其电路实现[J].北京交通大学学报,2004,28(5):69-72.

[7] HOPFIELD J J. Neurons, dynamics and computation[J]. Physics Today,1994,47(2):40-46.

[8] LI Guo-gang,GUO Dong-hui. One-way property proof in public key cryptography based on OHNN[J]. Procedia Engineering,2011,15(1/2):1812-1816.

[9] CHAN C K,CHENG L M. The convergence properties of a clipped Hopfield network and its application in the design of key stream generator[J]. IEEE Trans Neural Networks,2001,12(2):340-348.

[10] 廖晓峰,肖迪,陈勇,等.混沌密码学原理及其应用[M].北京:科学出版社,2009:35-37,92-105,248-249.

[11] 张雪峰,范九伦.基于线性反馈移位寄存器和混沌系统的伪随机序列生成方法[J].物理学报,2010,59(4):2289-2297.

[12] 曾光,韩文报,斯雪明.字序列密码驱动部分设计分析[J].电子科技大学学报,2007,36(6):1485-1488.

[13] 何峥,李国刚.基于神经网口护盾吸引子的混合加密算法[J].通信技术,2012,45(5):49-52.

An Word Oriented Encryption Scheme Based on OHNN and M-LFSR

LIN Xiao-mei, LI Guo-gang, ZHANG Ze-pu

(College of Information Science and Engineering, Huaqiao University, Xiamen 361021, China)

Abstract: A new encryption technique in word-oriented stream cipher has been proposed. It consists modified linear feedback shift register simu-lated (M-LFSR), and a feedback discrete-time Hopfield neural networks (HNN). Nonlinearity of the M-LFSR has been chosen by the chaotic attractors of discrete-time HNN as the output to achieve encryption. Safety analysis and simulation have shown that the pseudo-random sequence constructed by the proposed algorithm has been characterized by good randomness and complexity, which meets the requirements of cryptography.

Keywords: stream cipher; linear feedback shift register simu-lated; Hopfield neural networks; chaotic attractors

(**责任编辑**:黄仲一 **英文审校**:吴逢铁)