基于 OHNN 和驱动表的公钥加密算法*

张泽普[1],李国刚[1,2]
(1.华侨大学 信息科学与工程学院,福建 厦门 361021;
2.厦门大学 信息科学与技术学院,福建 厦门 361005)

摘 要:提出基于过饱和 Hopfield 神经网络(OHNN)和驱动表的公钥加密算法。算法以驱动表作为系统的驱动,经过函数组变换后产生随机数,数据选择器根据 OHNN 生成的混沌吸引子对随机数作非线性选择输出,从而实现加密。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和复杂度,满足密码学的要求。

关键词:过饱和 Hopfield 神经网络;混沌吸引子;驱动表
中图分类号:NP918.4 **文献标识码**:A **文章编号**:1674-7720(2013)12-0048-03

A new public-key cryptography based on overstoraged Hopfield neural network and table-drive

Zhang Zepu[1], Li Guogang[1,2]
(1.School of Information Science and Engineering, Huaqiao University, Xiamen 361021, China;
2.School of Information Science and Technology, Xiamen University, Xiamen 361005, China)

Abstract: This paper proposed a new public-key cryptography based on overstoraged Hopfield neural network and table, In this algorithm, table-drives as a driver pass a group of function and produce random number, data selectors according to chaotic attractor produced by OHNN to choose nonlinear output of random number to achieve encryption. The experiment results show that the sequence correlation properties and randomness of the output sequence produce by the algorithm can meet the requirement for the design of sequence code system.

Key words: overstoraged Hopfield neural network; chaotic attractor; table-drive

序列密码实质上是一个密钥流发生器,它通过将密钥流序列与明文进行异或完成加密和解密。随着密码分析技术的发展和计算机计算能力的增强,传统算法受到了很大的冲击。Hopfield 神经网络具有非常丰富的非线性动力特性和表现在混沌动力学特性方面的复杂性,使其成为现代密码学领域的一个热点。本文结合 OHNN 和驱动表的优点,提出了一种新的序列密码加密算法。该算法不仅避免了同步混沌通信系统中必须要求收发两端严格同步的诸多麻烦和不便,而且消除了密文数据膨胀[1],解决了 LFSRs 时间延迟和特征多项式难选取等问题[2],此外在速度上较二者有很大的提高。

*基金项目:福建省自然科学基金项目(A0640005);侨办基金(10QZR02);泉州市科技计划(2011G6)

1 过饱和 Hopfield 神经网络

在一个 N 阶 Hopfield 神经网络中,如果需要储存的样本总量大于 $0.14N$,则网络中原本存在的稳定的吸引子将发生畸变,且每个状态的收敛域都是混沌的,此时网络拥有过饱和存贮的混沌吸引性质。这样的网络称为过饱和 Hopfield 神经网络,简称 OHNN(Overstoraged Hopfield Neural Network)。在 OHNN 网络中,联结权值矩阵变化时,混沌吸引子和吸引域也随之改变。若 OHNN 的神经元 i 的阈值用 Q_i 表示,神经元 i 和神经元 j 之间的联结权值用 T_{ij} 表示。若神经元的状态取 0 或 1,则网络的传递函数 $\sigma(t)$ 为:

$$\sigma(t)=\begin{cases}1, x\geqslant 0\\ 0, x<0\end{cases} \tag{1}$$

如果当前网络状态为 $S_i(t)$,则其下一状态 $S_i(t+1)$ 为:

$$S_i(t+1)=\sigma\left(\sum_{j=0}^{N-1} T_{ij}S_i(t)+Q_i\right),i=0,1,\cdots,N-1 \quad (2)$$

Hopfield 神经网络的能量函数在演变过程中单调下降[3]，最终达到稳态，即混沌吸引子。在引入随机变换矩阵 H 后，原始状态 S 和吸引子 S_u 的演变遵循以下规律：

$$\hat{S}=SH \quad (3)$$

$$\hat{S}_u=S_uH \quad (4)$$

式(3)中，$\hat{S}$ 是 S 的更新状态，式(4)中，$\hat{S}_u$ 是 S_u 的更新状态。

2 函数组和数据选择器

2.1 函数组 IF

本文所提出的加密方案中，函数组 IF 由以下函数组成[4]：

$f1(x)=(x>>>7)\hat{}(x>>>18)\hat{}(x>>3)$

$f2(x)=(x>>>17)\hat{}(x>>>19)\hat{}(x>>10)$

$P[x]=g2(Q[x],P[x])$

$g1(x,y)=((x>>>10)\hat{}(y>>>23))+Q[(x\hat{}y) \bmod 1024]$

$Q[i]=g1(P[x],Q[x])$

$g2(x,y)=((x>>>10)\hat{}(y>>>23))+P[(x\hat{}y) \bmod 1024]$

$a(x)=(x) \bmod 1024$

$b(x)=(((x)>>8)+256) \bmod 1024$

$c(x)=(((c)>>16)+512) \bmod 1024$

$d(x)=(((x)>>24)+768) \bmod 1024$

$W(x)=f1(x)\hat{}g2(x,y)+g1(x,y)\hat{}f2(x)$

$m1(x)=h1(P[x])+h2(P[x])$

$h1(x)=Q[a(x)]+Q[b(x)]+Q[c(x)]+Q[d(x)]$

$m2(x)=h1(Q[x])+h2(Q[x])$

$h2(x)=P[a(x)]+P[b(x)]+P[c(x)]+P[d(x)]$

其中定义：$x>>>n=((x>>n)\hat{}(x<<(32-n)))$，$n\in[0,32)$，$x\in(0,2^{32})$。函数 W 产生的随机数用来驱动神经网络；函数 $h1$ 和 $h2$ 产生的随机数用来生成密钥序列；$g1$ 和 $g2$ 用来更新驱动表。

2.2 数据选择器

数据选择器的作用是将二进制随机数位置混叠后输出，具有两个类似于 AES 的 S 盒，一个有 $2N$ 组 L 个表示不同位置的整数(L 为数据流宽度，$L\leqslant 2N$)，另一个有 $2N+1$ 组。在 N 阶 OHNN 网络中，当网络遍历所有的吸引域时，将产生 $2N$ 个混沌吸引子，这些状态是在网络运行过程中，按轨迹遍历的先后顺序与数据选择器 S 盒建立的联系。若当前状态为 $\hat{S}_\mu^3$，该状态是系统轨迹第 6 个遍历的，数据选择器选择 S 盒中的第 6 组变换关系，将随机数位置混叠后输出。当网络联结权值发生变化后，网络遍历的轨迹随之改变，状态与数据选择器的关系也将发生改变。

3 基于 OHNN 和驱动表的公钥加密算法

本文提出的基于 OHNN 和驱动表的加密算法由一个 OHNN、一个函数组、一个数据选择器和两个驱动表组成。每个驱动表中都有 1 024 个不相同的 32 bit 十六进制的随机数。该算法的结构如图 1 所示。

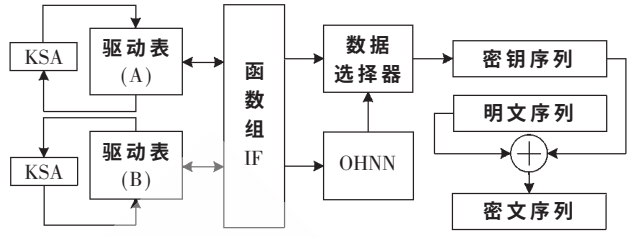

图 1 基于 OHNN 和驱动表的加密算法结构图

其工作原理是：(1)系统得到 OHNN 的权值矩阵后，首先将两个驱动表中的随机数位置混淆；(2)混淆后的驱动表经过函数组 IF 后，由函数 W、$h1$ 和 $h2$ 产生伪随机数，分别记为 $n1$、$n2$ 和 $n3$；另一方面驱动表中随机数由函数 $g1$ 和 $g2$ 更新；(3)$n1$ 经过初始化开关后，初始化数据流流入 OHNN，网络按照式(2)和式(3)演变后生成混沌吸引子；(4)两个数据选择器根据混沌吸引子，选取相应的数据流开关对 $n2$ 和 $n3$ 作非线性选择器，经过编码后转化成密钥序列输出；(5)密钥序列同明文异或后得到密文，完成加密。

在公钥密码系统中，本加密方案使用到了基于混沌吸引子的 Diffe-Hellman 密码交换协议[1]。假设用户 A 和 B 需要通信，双方任意选取非奇异变换方阵 H_a 和 H_b 作为私钥，计算得到公钥 T_a 和 T_b，然后交换公钥。若 A 向 B 发送信息，A 利用 H_a 和 T_b 计算得到 $\hat{T}$；密钥发生器得到 $\hat{T}$ 后开始运行，输出密钥序列，同明文序列异或后生成密文序列，直到明文加密结束。解密时，用户 B 利用 H_b 和 T_a 计算出 $\hat{T}$，用于解密。

4 仿真测试及安全性分析

4.1 随机性测试

本文采用 VC++6.0 编程，在 RedHat9.0 测试平台上依据美国国家标准与技术委员会(NIST)制定的 SP800-22[5] 对样本进行测试，测试样本为 100 组，每组 10^5 个数据。显著水平 $\alpha=0.01$，若计算出的 P-Value 值小于 α，则认为测试序列不为随机序列；反之，则认为序列是随机序列[6]。测试结果如表 1 所示，可以看出，算法产生的密钥序列具有较好的随机性。

4.2 相关性测试

选取内容重复大小合适的明文，加密后得到一份密钥序列。随机改变矩阵 H 其中的一位，加密后得到另一份密钥序列。相关函数越小，序列的随机性越好或越不相干[7]。测试结果如图 2 和图 3 所示。图 2 说明序列随机性好，图 3 说明算法对初值参数敏感，一个微小的改变都可以引起雪崩效应。

4.3 加解密测试

本文对《静夜思》进行加解密，如图 4 和图 5 所示。

表 1 随机序列随机性测试

测试类别	P-Value High	P-Value Low
Frequency	0.991 537	0.100 904
Block Frequency	0.971 897	0.679 024
Cumulative Sums	0.984 242	0.198 909
Runs	0.851 383	0.080 519
Longest Run of Ones	0.995 756	0.129 998
Rank	0.917 032	0.122 795
Discrete Fourier Transform	0.926 884	0.168 669
Non-overlapping Template	0.995 073	0.150 435
Overlapping Template	0.976 338	0.253 738
Linear complexity test	0.933 851	0.178 718
Universal	0.930 228	0.049 859
Approximate Entropy	0.976 366	0.105 581
Random Excursions	0.800 232	0.046 316
Random Excursions Variant	0.975 221	0.153 461
Serial	0.934 635	0.100 990

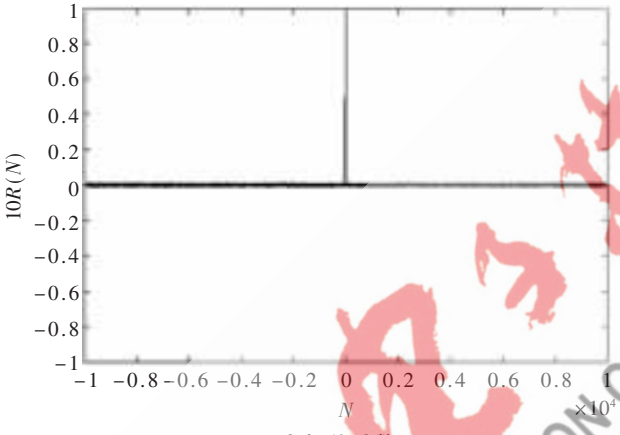

图 2 自相关系数

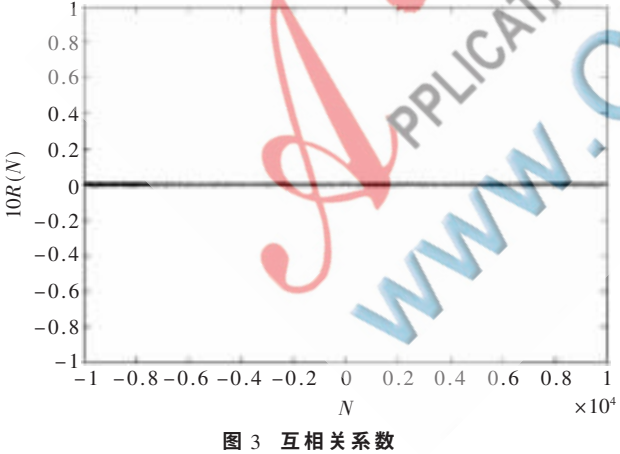

图 3 互相关系数

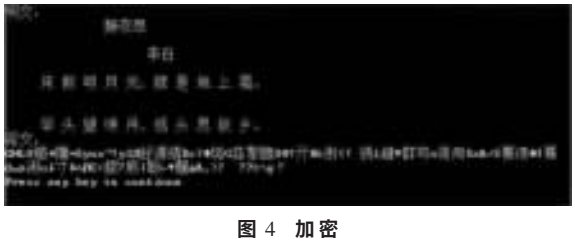

图 4 加密

测试平台：联想开天 M5250，CPU Intel® Pentium® 3.40 GHz 3.39 GHz，内存 0.99 GB，此时系统运行速度是参考文献[2]的 17 倍多。

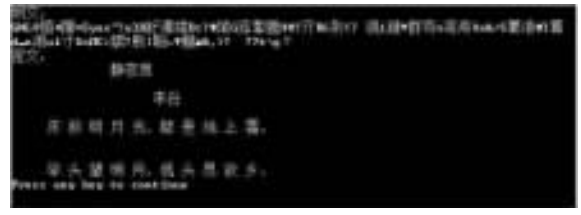

图 5 解密

4.4 安全性分析

本文所提出的算法在公钥体制中的安全性基于 OHNN 的混沌特性和奇异矩阵的难分解性。对于 LU 分解，它所分解出的矩阵乘积形式与 T 产生所使用的矩阵乘积形式不同，而且大多数情况下，LU 分解不是唯一的。对于 QR 分解，T_a、T_b 和 $\hat{T}$ 都是奇异方阵，它们是不能通过该方法来分解的。对于奇异值分解，虽然它是最可靠的分解法，但是它所花时间是 QR 分解法所花时间的近 10 倍多，本文中这种方式的分析不具有时效性。

由于公钥在公共信道中传递，容易遭到窃取。假设分析者得到了 T_a 和 T_b，有两种方法可以尝试推导出 $\hat{T}$。其一，虚构一个 N 阶非奇异矩阵 H_i，测试 $H_iT_0H_i^T$ 是否等于 $\hat{T}_i$，该方法的计算时间复杂性为 $O(2^{n^2})$，当 n 较大时，计算量太大，实际上是不可能计算的。其二，求解矩阵 X，使其满足：$\hat{T}=T_aXT_b=H_aT_0H_a^TXH_bT_0H_b^T=H_aH_bT_0H_b^TH_a^T=H_bH_aT_0H_a^TH_b^T$，然而此方程无解。

假如分析者采用穷举法，暴力攻击系统。由于 OHNN 由 N 个神经元所组成，每个随机变换矩阵 H 都存在 $N!$ 种可能，即系统的密钥空间为 $N!$。要得到目标随机变换矩阵，分析者需要进行 $N!$ 次运算。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，尝试一次就需要 10^{20} MIPS Years，远远超出了现在所能接受的安全水平 10^{12} MIPS Years[1]。

参考文献

[1] 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.

[2] 何峥，李国刚.基于神经网络混沌吸引子的混合加密算法[J].通信技术，2012，45(5)：49-52.

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

[4] Wu Hongjun.A new stream cipher HC-256[EB/OL].[2004].http://eprint.iacr.org/2004/092.pdf.

[5] NIST.A statistical test suit for random and pseudo-random number generators for cryptographic applications[OL].[2010].http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf.

[6] 廖晓峰,肖迪,陈勇,等.混沌密码学原理及其应用[M].北京:北京科学出版社,2009.
[7] 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.

(收稿日期:2013-02-20)

作者简介:

张泽普,男,1986年生,硕士研究生,主要研究方向:通信加密。

李国刚,男,1973年生,副教授,主要研究方向:集成电路设计与信息安全。