·通信保密·

基于神经网络混沌吸引子的混合加密

何 峥[①], 李国刚[①②]

(①国立华侨大学 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】把 Diffe-Hellman 密钥交换协议和流密码算法相结合，设计了一种基于神经网络混沌吸引子的混合加密算法。算法采用基于混沌吸引子的 Diffe-Hellman 公钥体制，保证了密钥分发的安全性，同时拥有流密码速度快的优点，提高了加密速度，因此实用性较好，能够满足下一代通信实时快速的需求。分析了算法的安全性和加解密效率，利用 vc 编程实现算法，并对仿真生成的密钥流和密文进行测试。实验结果表明，算法具有较好的安全性和加解密速度。

【关键词】神经网络混沌吸引子；混合加密算法；密钥流

【中图分类号】TN918.4 【文献标识码】A 【文章编号】1002-0802(2012)05-0050-03

Hybrid Cryptosystem based on Chaotic Attractors of Neural Networks

(①School of Information Science and Engineering, Huaqiao University, Xiamen Fujian 361021, China;
②School of Information Science and Technology, Xiamen University, Xiamen Fujian 361005, China)

【Abstract】By combining key-exchange agreement and stream cipher algorithms, a hybrid encryption algorithm based on chaotic attractors of neural networks is designed. This algorithm, with chaotic attractor-based Diffe-Hellman public-key crypto system, could ensure the security of key distribution while maintaining the high encryption speed of the stream cipher, and thus is of fairly good practicability. The security and the encryption efficiency of the new algorithm are analyzed and discussed. The algorithm is implemented by using VC program, and the simulated key stream and cipher text are tested. The experimental results show that the proposed crypto algorithm is of feasibility and fairly high encryption/decryption speed.

【Key words】chaotic attractors of neural networks; hybrid cryptosystem; public-key cryptosystem

0 引言

传统的公钥算法如 RSA、ECC 等是基于计算的困难性而不是算法的不可逆性[1]。要想保证其安全性，就必须不断增加密钥的长度，这将会增加计算的复杂度、降低加密速度[2]。随着计算技术的进步和密码分析技术的发展，传统的公钥算法正面临着很多威胁。

神经网络由于具有高度的并行性和混沌动力学特性[3]，其并行性使用 FPGA 兑现可以明显缩短加解密的时间以保证实时通信[5]；其混沌动力学特性，是一个非常复杂难解的 NP 问题，既能产生无法预测的序列轨迹，也可以实现不规则的混沌吸引子分类[3]，从而提高算法的安全性。采用混合加密的思路提出一种新的基于神经网络混沌吸引子的混合加密算法，避免了文献[3]中的过度搜索，利用基于混沌吸引子的 Diffe-Hellman 公钥体制保证密钥分发的安全性，同时利用流密码算法提高了加密速度。

收稿日期：2011-12-31。
基金项目：侨办基金（No.10QZR02）；泉州市科技计划（No.2011G6）。
作者简介：何 峥（1986-），女，硕士研究生，主要研究方向为电子通信；李国刚（1973-），男，副教授，主要从事集成电路设计与信息安全方向的研究工作。

1 公钥算法的原理

1.1 神经网络混沌吸引子

假设含有 N 个神经元的离散 Hopfield 神经网络

(HNN，Hopfield Neural Networks)，它的每个神经元状态取值只能为 1 或者 0，设当前神经元的状态为 $S_i(t)$，则它决定了各神经元的下一个状态 $S_i(t+1)$，即：

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

在公式(1) 中，神经元 i 的阈值是 θ_i，神经元 i 和 j 之间的联结权值是 T_{ij}，$\sigma(x)$ 是任意非线性函数，因此设 $\sigma(x)$ 是一个符号函数，则:

$$\sigma(x)=\begin{cases}1, x\geq 0,\\ 0, x<0。\end{cases} \tag{2}$$

Hopfield 已证明系统的能量函数随系统状态的演变而单调下降[5]，它最终将会达到一个稳定的状态，即混沌吸引子[3]。在引入随即变换矩阵 $\boldsymbol{H}$ 以后，原始状态 S 与吸引子 S^u 就会变为新的初始状态 $\hat{S}$ 与吸引子 $\hat{S}^u$ [1]：$\hat{S}=S\boldsymbol{H}$ ；$\hat{S}^u=S^u\boldsymbol{H}$ 。

2 混合加密算法

过饱和贮存的 Hopfield 神经网络(OHNN，Overstoraged Hopfield Neural Networks)模型中混沌吸引子与初始状态间存在一种单向函数关系，如果改变神经网络的联结权值矩阵，混沌吸引子及其相应的吸引域会随之发生改变[4]。设计出一种安全性较高的混合加密算法，如图 1 所示。

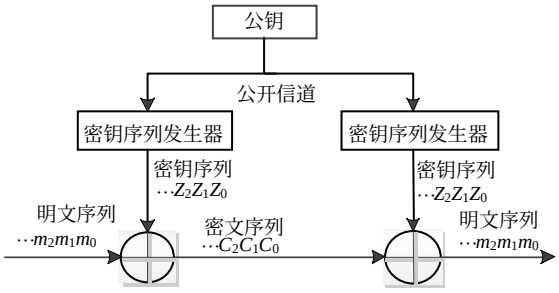

图1 基于神经网络混沌吸引子的混合加密算法

发送方和接收方利用自己的私钥和对方的公钥计算出公共密钥 $\hat{T}$，作为新的联结权值矩阵，并为图2中的神经网络使用，用以产生密钥序列，对明文进行加密。为进一步增强信息传输安全，防止中间欺骗者攻击，可采用带认证的Diffie-Hellman密钥交换协议，保密通信的双方采用数字签名和公钥证书来相互确认对方的身份是否合法[7]。

图2中，密钥序列发生器把若干m序列作为序列密码的驱动源，把离散Hopfield神经网络作为非线性函数的控制部分，进行选择输出。m序列的良好统计性被保留了的同时，复杂度和周期性也得到了提高。各线性反馈移位寄存器(LFSR，Liner Feedback Shift Register)的初始值从公共密钥T矩阵中随机选取适当个元素处理后确定（比如，大于等于0的设为1，小于0的设为0），且通信双方必须一致。

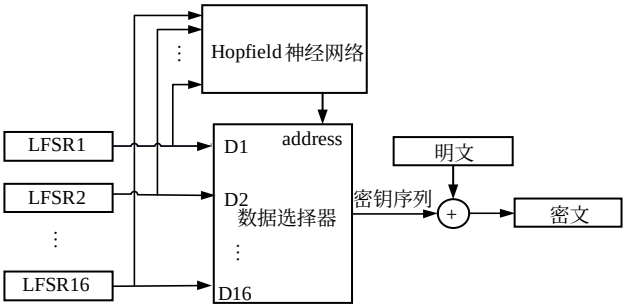

图 2 密钥序列发生器

混合加密方法如下：

1）密钥的生成：同一组内的用户选取同一个 n 阶奇异方阵 T_0，作为联结权值矩阵。用户 A 和 B 任意选择 2 个可交换矩阵族的同阶方阵 H_a 和 H_b。H_a 为用户 A 的私钥将其保密，$T_a=H_aT_0H_a'$ 为用户 A 的公钥将其公开。同理，用户 B 将私钥 H_b 保密，把公钥 T_b 公开。同一组内的两个用户 A 与 B，可以把 $\hat{T}=H_aT_bH_a'=H_bT_aH_b'$ 来作为他们之间通信时的公共密钥。

2）明文的处理：由于文件在存储器里或在网络中传输时的形式都是以字节为基本单元的二进制形式，所以在设计时将明文转换成串行的比特流。

3）密文的生成: 把 2^n 个 LFSR 的输出值当作神经网络的输入值，在加密器中根据新的公共密钥 $\hat{T}$ 计算出新的吸引子，再依照产生的新的吸引子，对 2^n 个 LFSR 的输出值进行 N 选一操作(N 位神经元的联结权值矩阵共有 $2N$ 个混沌吸引子, 在本设计中分成 2 组, 每组 N 个混沌吸引子), 由此产生密钥序列, 和明文 M 进行异或，生成密文 C 输出。

3 安全性分析

3.1 算法安全性分析

设计采用的联结突触矩阵 T_0 是奇异方阵，可得 T_a、T_b 和 $\hat{T}$ 也是奇异方阵。虽然从 T_0、H_a 和 H_b 能很容易计算出 T_a、T_b 和 $\hat{T}$，但要从 T_a、T_b 和 $\hat{T}$ 计算出 H_a 和 H_b 却非常困难，尤其当 n 较大时[6]。

方案中假设 OHNN 是由 N 个神经元所组成的，其混沌吸引子数目为 $2N$。可得每个随机变换矩阵 $\boldsymbol{H}$ 都存在 $N!$种可能情况，即它的密钥空间为 $N!$。如果攻击采用穷举法，则搜寻某一随机变换矩阵 $\boldsymbol{H}$，就可能需要运行 $N!$次。如果采用的是每秒钟能计算 10^6 个变换矩阵的专业计算机，那么神经元的个数 N 就决定了遍历变换矩阵 $\boldsymbol{H}$ 的空间所需要的时间 t。当 N=32 时, 成功搜索一次变换矩阵就需要 10^{20}MIPS Years, 远远超过现在所能接受的安全水平 10^{12}MIPS

Years[3]。对于其他算法, 如 RSA 算法最少需要 1 024 位密钥才能确保安全性[8]。

因此可以得出，基于奇异矩阵分解的困难性和 OHNN 的非线性特性设计的混合加密算法具有较高的安全性。

3.2 相关性测试

选取内容重复的明文 3K，如“神经网络混沌吸引子加密”。密钥流的自相关函数如图 3 所示，图中选取的相关间隔为 $-6\times10^4-6\times10^4$。自相关函数变化越小，说明对应的序列随机性越好[9]。

随机改变转置矩阵 $\boldsymbol{H}$ 其中的一位，得到的两密文的互相关函数如图 4 所示。互相关函数取值越接近 0，说明两个序列越互不相关[9]。图 4 表明密钥微小改变可引起密文完全改变，雪崩效应明显。

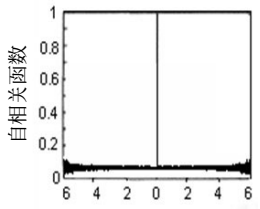

图 3 密钥流的自相关图

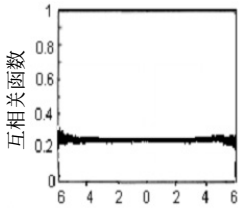

图 4 密文的互相关图

3.3 随机性测试

使用美国国家标准与技术与技术委员会(NIST, National Institute of Standards and Technonlgy)制定的考评随机和伪随机序列的测试标准 SP800-22[10]对本算法的产生的密钥序列进行随机性测试。测试样本为 100 组，每组 10^6 个数据。若 P-Value 的值小于 0.01，则认为测试的序列为非随机序列，反之则认为序列是随机序列[11]。通过表 1 的测试结果，可以看出算法产生的随机序列具有较好的随机性。

表 1 密钥流的 SP800-22 测试结果

测试项目（Test）	P-Value
单频率测试（Frequency）	1.000 000
块频率测试（Block Frequency）	0.950 485
累积和测试（Cumulative Sums）	0.911 413
行程测试（Runs）	0.097 364
块的最长行程测试（Longest Run）	0.739 918
非重叠模板匹配测试（Non-overlapping Template）	0.991 468
重叠模板匹配测试（Overlapping Template）	0.350 485
通用统计测试（Universal）	0.350 458
近似熵测试（Approximate Entropy）	0.017 912
随机偏离测试（Random Excursions）	0.901 933
随机偏离变量测试（Random Excursions Variant）	0.901 933
线性复杂度测试（Linear Complexity）	0.213 309

3.4 加解密速度和信息率分析

实际编程中为提高流密钥序列随机性，采用16个LFSR输入，级数分别选为：11、13、17、19、21、25、29、31、37、39、41、43、47、53、59、61，其反馈本原多项式分别为(11,2,0), (13, 4, 3, 1, 0), (17, 6, 0), (19, 5, 2, 1, 0), (21,2,0), (25, 3, 0), (29, 2,0), (31,13,0), (37,6,4,1,0), (39,4,0), (41,3,0), (47,5,0), (43,6,4,3,0), (53,6,2,1,0), (59,7,4,2,0), (61,5,2,1,0) [12]。混合加密算法避免了过度搜索，同时消除了密文膨胀，加密过程中计算1次混沌吸引子就可以加密1bit明文信息，实际测量的加密速度比文献[3]平均快7倍。测试环境：计算机采用联想开天M5250，CPU为Intel(R) Pentium(R) 3.40GHz 3.39GHz，0.99GB内存，编译器采用VC++6.0。

4 结语

把神经元触突矩阵作为陷门函数，以 Diffie-Hellman 公钥密码体制为依据, 提出了一种新的基于神经网络混沌吸引子的混合加密算法。算法具有可靠的安全性和较好的加密速度。可以用 FPGA 硬件实现神经网络，克服了用软件实现并行性差、速度慢的弱点，以实现实时高速加密通信[13]。因此，该加密算法满足信息传输的安全、高效的需求，为信息安全提供了一种新思路。

参考文献

[1] 蔡家楣,刘多,陈铁明. 神经网络密码学研究综述[J]. 计算机应用, 2007,27(06):219-222.

[2] 朱香卫,肖亮,吴慧中.密码技术与数字水印技术比较[J].信息安全与通信保密,2008,41(07)：208-210.

[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:自然科学版, 2007,46(2):187-192.

[4] 刘年生,郭东辉.一种新的基于神经网络混沌吸引子的公钥密码算法[J].集美大学学报:自然科学版,2005, 10(02):125-133.

[5] HOPFIELD,JOHN J.Neurons, Dynamics and Computation [J]. Physics Today, 1994,47(02):40-46.

[6] GUO D, CHENG L M, CHENG L L. A New Symmetric Probabilistic Encryption Scheme Based on Chaotic Attractors of Neural Networks[J]. Applied Intelligence,1999, 10(01): 71-84.

[7] 刘传领,范建华.RSA非对称加密算法在数字签名中的应用[J].通信技术,2009,42(03)：192-196.

[8] 葛峰,金伟信,段本钦. 1024位RSA算法的FPGA设计研究[J].军事通信技术, 2009,30(1):81-85.

[9] 张雪锋,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(04): 2289-2297.

[10] 董斌辉,周健勇,黄金辉. 混沌伪随机序列生成算法研究[J].信息安全与通信保密,2009(11)：327-330.

[11] 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,2009:35-37,248-249,92-105.

[12] SCHNEIER B. 应用密码学[M].北京:机械工业出版社, 2000:265-276.

[13] 黄泽锷,禹思敏,周武杰.基于FPGA技术的混沌数字加密与硬件实现[J].通信技术,2008,12(41):343-346.