学校编号：10384　　分类号_____密级_____
学　　号：B9924005　　UDC_____

厦门大学博士学位论文

神经网络混沌加密算法及其在下一代互联网安全通信中的应用研究

Chaotic Encryption Scheme Based on Neural Networks and its Application in Secure Communications of IPng

刘　年　生

指 导　教 师：　吴伯僖 教授
　　郭东辉 教授

申请学位级别：　博　　士
专 业 名　称：凝 聚 态 物　理
论文提交日期：2003 年 10 月　日
论文答辩日期：2003 年　　月　日
学位授予单位：厦　门　大　学
学位授予日期：2003 年　　月　日

答辩委员会主席：_____
评　　阅　　人：_____

二〇〇三 年 十 月

博士学位论文

神经网络混沌加密算法及其在下一代互联网安全通信中的应用研究

Chaotic Encryption Scheme Based on Neural Networks and its Application in Secure Communications of IPng

刘年生

厦门大学学位论文原创性声明

兹呈交的学位论文，是本人在导师指导下独立完成的研究成果。本人在论文写作中参考的其他个人或集体的研究成果，均在文中以明确方式标明。本人依法享有和承担由此论文而产生的权利和责任。

厦门大学
二00三年十月

神经网络混沌加密算法及其在下一代互联网安全通信中的应用研究

摘 要

网络安全问题是下一代互联网研究的关键问题之一，而加密算法又是网络安全问题的核心。为了满足下一代互联网多媒体实时性安全通信的要求，既需要选用复杂性高的加密算法，以增强信息的安全性，又希望所选用的加密算法能以并行方式实现快速运算，以缩短加密和解密的时间来保证实时通信。其中，既能实现快速并行运算又有混沌动力学复杂行为的人工神经网络一直被认为是用来设计下一代互联网通信所需的加密算法的最佳选择之一。因此，本博士论文工作的主要内容是:

先综合分析下一代互联网的主要特点，说明下一代互联网的安全问题关键在于加密算法；并通过介绍现有几种加密算法，指出加密算法的安全性取决于加密算法的复杂性。然后，通过分析混沌神经网络的复杂动力学行为和并行处理特点，说明混沌神经网络在下一代互联网安全通信中应用的可行性。

在这基础上，我们提出了四种新的基于混沌特性安全算法，它们分别为:（1）基于神经网络的混沌序列分组对称加密算法；主要利用神经网络的混沌特性，将其所产生混沌二进制序列进行群加密。（2）基于神经网络混沌同步的加密算法；采用遮盖的方法进行混沌同步调制来实现信息的保密。（3）基于神经网络混沌吸引子的公钥加密算法；根据原神经网络混沌吸引子的对称几率加密算法和 Diffie-Hellman 公钥体制原理，给出一种数学上证明是安全的公钥加密算法。（4）基于混沌序列的图像信息隐藏技术；将需要隐藏传送的图像以混沌噪声的形式加入到载体图像的时空变换谱中，接收者根据混沌序列的相关特性利用相应的混沌噪声来提取所隐藏的图像，该技术具有良好的信息安全性、不可觉察性和较高的隐藏容量。

最后，根据所提出的加密算法来设计 IPSec 协议的实现方案，并在 Linux 操作系统的平台下具体实现下一代互联网 IPv6 的 IPSec 协议及其加密方案。

关键词：神经网络；混沌系统；加密算法；信息隐藏；IPv6；IPSec

Chaotic Encryption Scheme Based on Neural Networks and its Application in Secure Communications of IPng

Abstract

Networking security is one of key problems in the study of IPng, and the encryption algorithm selected for IPSec is the core of this key problem. In order to meet the requirements of multimedia real time communications via the IPng, the encryption algorithm should have higher complexity for the security of information system, and higher processing speed for the efficiency of information encryption and decryption. So, neural networks, with the properties of nonlinear dynamics such as chaotic behavior and parallel processing, are regarded as one of good design options for encryption algorithm applied in the communications of IPng. For this, my PhD project is arranged to focused on the application of neural network in the security of IPng, and summarized as follows:

In order to show that the networking security mainly depends on encryption algorithms in the IPng, we detailed on the IPng protocol (i.e IPv6) and analyzed its security scheme (i.e. IPSec). Meanwhile, after summarizing the principles of conventional standard encryption algorithms and their performance, we pointed out that the computational complexity and parallel-computing ability are the key factors of encryption algorithms for applications in the real-time secure communication of IPng. And then, we analyzed the chaotic behaviors of neural networks and their parallel computing abilities, and presented the advantages of chaotic encryption scheme based neural networks for applications in IPng.

As the results of my PhD research project, 4 kinds of new chaotic encryption schemes based on neural networks are proposed: (1) the symmetric block encryption scheme based on chaotic series. Using the chaotic binary series generated by neural networks, the sensitive information is encrypted in the form of group encryption; (2) the symmetric encryption scheme based on chaotic synchronization. The principle of data encryption in the scheme is implementing chaotic synchronization modulation by chaos masking; (3) the public key encryption scheme based on chaotic attractor. This scheme is derived from the previous symmetric probabilistic encryption scheme based on chaotic attractor of neural networks and Diffie-Hellman key agreement protocol. We prove that this scheme is secure and reliable from the standpoint of mathematics; (4) the images hiding scheme based on chaotic sequence. The information of hidden image is added to the transformation spectrum of cover image as a kind of noise. A legal information receiver can be extracted the hidden image using the chaotic series which he knows himself. This technique has good properties with security, imperceptibility and high hiding capacity of the hidden information.

The implementation scheme of IPSec is designed according to encryption algorithms proposed in the end, and we introduce how to add encryption schemes proposed to IPSec, and how to implement IPSec in the Linux operation system.

Key words: Neural Networks; Chaotic System; Encryption Scheme; IPv6; IPSec

目录

CONTENTS

第一章 绪论

本博士论文工作目的是希望通过对神经网络混沌动力学系统的复杂性研究，提出具有复杂性意义的安全加密算法，并实际应用到下一代互联网通信中去。为了强调本论文工作的必要性和可行性，本章首先通过介绍 Internet 互联网发展的现状，说明网络安全问题是下一代互联网研究的关键问题之一；并通过回顾人类通信加密算法研究的发展历程，说明复杂性和并行性是今后加密算法实现网络实时安全通信的必然要求；然后，通过简述神经网络的强大信息并行能力及其混沌特性在加密算法中应用研究的成果，说明混沌神经网络在下一代互联网安全通信中应用的可行性，并指出该应用研究课题中需要解决的一些重点问题；最后，简要概括本论文其他各章节的内容和成果。

§1.1 Internet 互联网发展的现状

随着 Internet 技术的发展，网络空间已成为现代社会人们赖以生存和发展的基础[1，2]；**Internet** 已成为全球性的多媒体通信网络，用户持续增多，如：美国 **United Yellow Pages，Inc** 对美国互联网用户统计与预测，如图 1.1 所示。

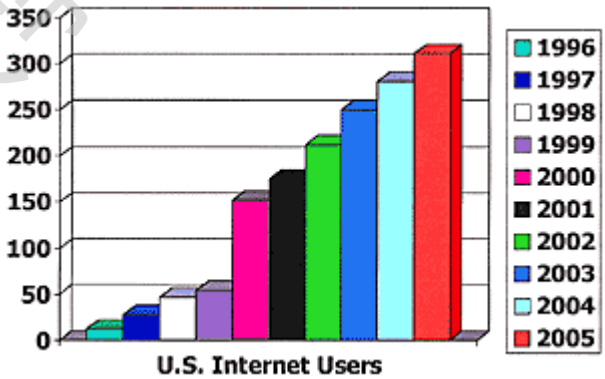

图 1.1 美国互联网用户数的统计与预测（单位：million）

Internet 规模的不断扩大，使得现行 IPv4 互联网所面临的一些问题日益突出[3]，主要表现在：（1）IP 地址耗尽；（2）通信链接没有带宽和流量控制功能，服务质量(Quality of Service)没有保证；（3）IPv4 的 **Internet** 安全性相当脆弱；**Internet** 在最初设计时主要解决异质性问题，没有考虑解决包括信息的保密安全在内的其它问题。尽管后来采取了各种不同的补救措施来解决这些问题，但是并不能彻底解决 IPv4 本身固有的缺陷[4]。因此，人们希望通过制订新的互联网协议来实现能够满足各种通信业务要求的高质量下一代互联网。

为此， IETF (The Internet Engineering Task Force)组织于 1994 年 11 月将在 IPv4 基础上改进的 IPv6 (Internet Protocol Version 6)认定为“the Next Generation Internet Protocol”，即下一代 **Internet** 互联网的协议标准[5]，并在全世界范围内建立起 IPv6 的实验平台——“6bone” 实验网[6]。目前世界上至少有 40 多个国家接入了“6bone” 实验网，许多生产厂家包括 IBM、 HP、 Sun、 Cisco 等公司也已开始生产适应于 IPv6 的路由器、网卡等产品，并开发适于 IPv6 的操作系统，如 Linux、Windows NT 等，可见 IPv6 的实用日期就要到来了。

§1.2 下一代互联网的安全问题

目前我们使用的以 IPv4 为基础的互联网络存在各种各样的信息安全问题，如伪装（欺骗）、窃听、非法接入、篡改、抵赖、伪造、拒绝服务、设置后门和传播病毒等等网络攻击现象。近年来，网络攻击次数应该是逐年增加，愈来愈频繁，如图 1.2 所示[7]。攻击事件的频繁发生表明现行的 IPv4 在协议设计上的安全脆弱性。为了弥补这一不足，IETF 在设计 IPv6 协议时就成立了十多个与安全方面有关的工作组，从网络层安全体系结构、协议、策略、加密算法和密钥管理等多方面进行深入的讨论、改进与标准化，相继推出了近百个 Internet 安全标准草案与推荐标准，如 RFC2401、RFC2402 等等[8，9]，从而构筑出下一代互联网的信息安全基本体系。在这种安全体系结构中，除了保留原应用程

序本身所提供的安全性功能外，开始强化网络层安全作用，把加密算法与安全机制相互隔离，这样对于安全机制公开的公共通信网络，其信息安全就取决于加密算法的安全性。 因此，加密算法的研究可以说是解决下一代互联网信息安全问题的核心[10，11]。

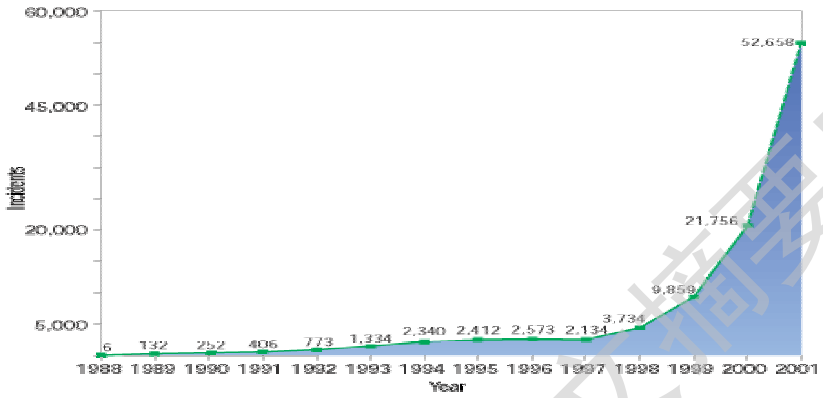

图 1.2　1988 年至 2001 年网络攻击事件统计

其实，加密算法自古就有，早在公元前两世纪一位希腊人就提出了一种棋盘密码算法，但这种加密方式根本经不起已知明文法攻击。在此基础上进行多种改进，如采用移位置换方法的 Caesar 密码、多表置换的 Vigenere 密码、线性变换的 Hill 密码等等，它们构成了传统密码算法[12]，这些密码算法只是作为一种变换的技巧，缺乏信息安全性的理论证明，很容易被破译。直到 20 世纪四十年代末，才由 C. E. Shannon 从信息论的角度提出了“一次一密”完全保密的加密通信理论[13]，使得密码学从一种技巧变为一门学科。到了 1976 年在 W. Diffie 等人提出了非对称密码系统的概念[14]，即公钥加密，才算是开创了现代通信密码学的研究，它从根本上解决了对称密码系统中所存在的密钥分配和消息认证等问题，随后产生了许多基于这一思想的现代加密算法，如 RSA(Rivest-Shamir-Adleman) [15]、ECC(Elliptic Curve Cryptography) [16]等等。1977 年美国正式公布实施数据加密标准 DES（Data Encryption Standard）[17]，

后来该标准又被 ISO（International Standardization Organization，国际标准化组织）所采纳，成为国际上第一个公开的数据加密标准。

另一方面， 在加密技术不断发展的同时， 密码分析技术也得到了较快的发展，从传统的穷举攻击法发展到差分密码分析法、线性密码分析法和非线性密码分析法[18-22]，使得目前公布的各种加密算法如 DES、RSA 和 ECC 等等均不能保证其理论安全性[23]。特别是， 随着计算机性能的不断提高和网络计算的不断发展，原来认为是安全的加密算法从其计算安全性来看日益降低，例如：1998 年 5 月美国 Electronic Frontier Foundation 宣布，以一台价值 20 万美元的计算机改装成的专用解密机，只用 56 小时破译了采用 56 bits 密钥的 DES[23]。因此，为了保证通讯中信息的安全性，需要研究和提出计算复杂性更高的加密算法或新的密码系统。 鉴于加密算法的复杂性要求，如神经网络密码[24]、混沌密码[25]、量子密码[26]以及 DNA 密码[27]等基于复杂性的密码系统近年来得到了普遍的重视。但是，复杂性高的加密算法必定会影响其在互联网安全通信的实时性应用，只有那些既具有高度计算复杂性又具有实时并行处理功能的系统才有可能兑现成为比较理想的加密算法，以满足下一代互联网实时安全通信的要求。

此外，互联网的加密通信还要考虑到加密隐藏问题，即加密通信既要保证加密的信息不被非法接收者解密，最好又能做到实时通信不被干扰或破坏。一般来说，加密传输的密文对非法接收者来说是表现为一些乱码，很容易引起攻击者的注意，从而受其恶意的破坏或干扰，为此可以采用信息隐藏技术[28，29]来弥补。信息隐藏技术可以说是从另外一个角度来实现网络信息安全通信，它将敏感信息隐藏在某种载体（包括文字、图片和声音等）中，让攻击者从网络传输的大量媒体中无法辨认哪一个或哪些是隐藏有敏感信息的载体。因此，近年来信息隐藏技术也倍受关注，并已有许多研究成果，特别在数字水印技术方面，已经实际运用到数字音像产品的产权保护上。 不过，适用于网络实时安全通信的信息隐藏技术还需要进一步的研究，由于它对算法的安全性、载体的不

可觉察性和隐藏容量等提出了更高的要求，需要提出新的技术方案来满足这些要求。

§1.3 神经网络及其在混沌加密算法

人类的思维活动自古以来一直是人们最感兴趣的课题之一。在古代，人们总是认为人类的思维活动是在心脏部位完成的，后来人们才逐渐意识到人类思维活动应该是由大脑来完成的。因此，人们希望通过研究动物大脑的细胞结构和活动机理来详细了解人类各种智能活动行为如学习、联想、识别及睡眠等等，从而去模拟创造具有人工智能的机器或生物。

但是，由于实验条件的限制，直到上个世纪 40 年代即 1943 年才由美国神经生理学家 W. S. McCulloch 和数学家 W. H. Pitts 根据解剖学和生理学方面的成果提出了“以逻辑符号来描述神经元及由其组成的神经网络，以通过对神经元间联结强度和神经元阈值的适当选择来表征大脑内神经元对外部世界的感官活动”这一基本思想的人类思维活动 M-P 神经元模型[30]；而后于 1949 年美国心理学者 D. O. Hebb 根据心理学中条件反射机理[31]，指出人类的学习行为是通过大脑中生物神经元间连接强度变化(即 Hebb 学习规则)完成的。此后，在 M-P 神经元模型和 Hebb 学习规则基础上，有关“能够模拟大脑的神经元网络结构和思维行为”的神经网络成为人们致力于研究和创造人工智能的重要方向之一，至今也取得了一系列重要研究成果[32-48]。

如今，人们对大脑的结构已有清楚的认识[49]，人类大脑大约是由 10^{12} 个比较简单类似的生物神经元组成的，且每个神经元要与其它 10^{3} 个神经元相互联结，形成了具有 10^{14}-10^{15} 个突触联结的神经网络系统。所以，有关神经网络的理论研究实际上就是研究分析这种由大量非线性单元组成并行复杂系统的信息处理能力。正是由于神经网络所具有强大的信息处理能力，它已经在互联网通信领域得到了一些应用如信号识别、预测、均衡和编码、信元调度优化、路由选择等等[50-55]。特别在 1990 年 K. Aihara 等人[56]根据生物神经元的

混沌特性提出了混沌神经网络概念之后，人们开始意识到神经网络的混沌复杂性有望在加密通信中得到应用。经过科学家们十多年来的努力，有关神经网络混沌加密算法的研究也取得了一些成果， 如 V. Milanovic 等人[57]基于神经网络混沌同步特性提出了一种同步加密的保密通信方案; K. R. Crounse 等人[58]基于细胞神经网络混沌序列不可预测性提出了序列分组对称加密方案; 以及 D. Guo 等人[59]基于神经网络混沌分类吸引子的随机分组对称加密方案等等。

但是,这些神经网络混沌加密方案大多数未就加密算法的安全性进行深入的分析[60]，且有些神经网络混沌加密方案从实用性上看似乎是不科学的。 因此，有关神经网络混沌加密算法的研究不仅要提出具有创新性的加密方案， 而且要从数学意义上证明加密算法的安全性和实用性。

§1.4 本论文研究工作的重点

在互联网通信安全问题日益突出的今天，其核心问题即加密算法的研究可以说倍受人们关注。形形色色的加密算法不断被陆续提出，但这些加密算法的安全性普遍经不起密码专家的复杂性攻击[61]。即使是目前普遍使用标准加密算法如 RSA、ECC 等，由于其加解密速度问题，也不适用于实现下一代互联网多媒体实时安全通信。因此，本博士论文工作的研究目的就是希望将既具有混沌动力学复杂行为又有快速并行信息处理能力的神经网络引入到密码学中，提出具有复杂性意义的神经网络混沌加密算法，并在下一代互联网实时安全通信中得到实际的应用。

为了具体地介绍本博士论文的工作内容和重点，我们按以下章节来安排本论文的撰写，即：在第二章中我们介绍 IPv6 协议结构，说明下一代互联网的主要特点和安全协议 IPSec 的兑现原理。第三章则是简要介绍现行几种标准加密算法的兑现原理，并分析其安全性和实用性，以说明加密算法的安全性和实用性在于算法的复杂性和并行性。第四章先是通过介绍了混沌动力学系统的特性

和复杂度分析方法，说明神经网络混沌加密算法在复杂度和并行处理速度方面能够满足下一代互联网实时安全通信的要求，然后综述了现有的几种神经网络混沌加密算法的兑现原理及其通信应用情况，指出这些加密算法需要进一步改进的地方。第五章是本论文的重点，我们根据前面几章的分析结果，从神经网络的混沌复杂性和信息处理并行性出发，在这一章里提出了三种新的神经网络混沌加密算法，并分别分析它们的安全性和实用性。第六章则是提出了一种基于神经网络混沌序列相关性原理的图像传输信息隐藏加密方案，并具体分析该加密方案的安全性及其通信性能指标。为了兑现我们所提出加密算法和方案在下一代互联网中的实际应用，第七章将具体介绍 IPSec 如何嵌入新的加密算法并在以 Linux 为操作系统的 IPv6 互联网环境中的实现。最后一章，我们对所做的博士论文工作进行总结，并说明今后进一步研究的方向。

第二章 下一代互联网协议的特点与安全机制

为了解决现行 Internet 互联网所存在的 IP 地址耗尽、服务质量控制、网络安全等问题[4，5]，国际互联网组织 IETF 于 1990 年就开始着手下一代互联网协议 IPng (Internet Protocol Next Generation)的研究。 经过对各种设计方案评估和筛选，于 1994 年 7 月就确定采用 SIPP (Simple IP Plus)设计方案[62]为下一代互联网的基础协议，并于同年 9 月发布了协议草案“The Recommendation for the IP Next Generation Protocol”[63]，1995 年底正式确定了 IPng 的协议规范，称为“IP version 6”即 IPv6，以区别于目前普遍使用 IPv4 版本。

本章将通过介绍 IPv6 的地址结构和类型，来具体说明 IPv6 在地址管理机制与服务质量控制方面的特点，以及其安全机制的兑现原理。

§2.1 IPv6 的地址结构

为了保证互联网 Internet 使用的延续性和更新的兼容性，下一代互联网协议 IPv6 保留了 IPv4 的大部分设计想法，但在地址结构和管理机制、服务质量控制和网络安全性等方面进行了较大的改进。与 IPv4 的地址结构及其管理机制相比，IPv6 是通过增加地址长度来扩大地址空间，并通过改变地址的表示方法以增加新的地址类型，从而建立起新的管理机制。 如采用层次性结构化地址表示法， 便于路由地址的层次性管理，以减轻骨干路由器的负载，防止路由瓶颈；该表示法也便于自动寻址和自动配置功能的实现，简化了网络节点的管理与维护；也支持移动计算，使得网络地址管理更加简单。因此， IPv6 的地址结构与类型是 IPv6 协议最主要的内容之一，也是 IPv6 网络的基础与关键问题。