椭圆曲线密码体系研究

· 肖攸安 著 ·

華中科技大學出版社
http://www.hustp.com

椭圆曲线密码体系研究

肖攸安　著

华中科技大学出版社

图书在版编目(CIP)数据

椭圆曲线密码体系研究/肖攸安 著
武汉:华中科技大学出版社,2006年10月
ISBN 7-5609-3858-2

Ⅰ.椭…
Ⅱ.肖…
Ⅲ.因特网-安全技术
Ⅳ.TP393.4

椭圆曲线密码体系研究 肖攸安 著

责任编辑:余 涛 封面设计:潘 群
责任校对:吴 晗 责任监印:张正林

出版发行:华中科技大学出版社
武昌喻家山 邮编:430074 电话:(027)87557437

印 刷:华中科技大学印刷厂

开本:850×1168 1/32 印张:8.125 字数:220 000
版次:2006年10月第1版 印次:2006年10月第1次印刷 定价:15.00元
ISBN 7-5609-3858-2/TP·621

内 容 提 要

椭圆曲线密码体系是当前信息安全领域的研究热点之一，本书在分析和研究椭圆曲线密码学的最新研究成果的基础上，分7章总结了作者在该领域所完成的一系列的研究工作。其中，第1章从网络信息安全现状出发，分析了所面临的安全威胁，归纳了人们所提出的安全需求，给出了相应的解决方案，引出了椭圆曲线公钥密码体系。第2章主要介绍和讨论了在本书中所要用到的椭圆曲线密码体系的基本数学理论基础和相关的背景知识。第3章在介绍有限域上的离散椭圆曲线的基础上，深入讨论了椭圆曲线有限群上的椭圆曲线离散对数问题，归纳了安全椭圆曲线选取准则。第4章研究了椭圆曲线有限群阶的计算问题，深入研究了SEA数点算法。第5章根据安全通信的需要，在讨论通信协议安全性问题的基础上，研究和分析了作者所设计的可用于椭圆曲线密码体系的密钥生成、密钥协商、密钥分配、信息加密、数字签名等多种安全高效的密码方案。第6章和第7章深入研究了椭圆曲线密码体系实现中的若干关键技术，给出了典型方案的具体实现算法和实验结果。

本书适用于信息、计算机及相关专业的博士、硕士研究生和高年级本科生，也可作为信息安全领域的研究人员和专业技术人员的参考书。

前　言

随着信息技术和网络技术的飞速发展，信息安全问题成为人们日益关注的焦点。作为信息安全技术重要基础的密码学，其主要目的是防止信息系统内的机密信息被非法访问者破译，使机密信息和重要数据得以不必通过专用的特别设施进行传输和储存，大大降低信息传输的成本和信息存储的费用。

公钥密码学是密码学的重要分支，它基于某一类公认的、在计算上不可行的数学难题，使用一对不同的密钥完成信息保密任务。由于公钥密码体系所用到的一对密钥中的一个密钥是可以公开的，因此它可以被广泛应用于诸如数字签名、身份认证、数据加密和密钥管理等众多领域，对信息安全技术具有非常重要的意义。

椭圆曲线离散对数问题是目前公认的可用于公钥密码体系的三大数学难题之一。基于椭圆曲线离散对数问题而构筑的公钥密码体系就是椭圆曲线公钥密码体系。与其他公钥密码体系相比，椭圆曲线公钥密码体系具有密钥短、强度高、参数少等特殊的优势，特别适用于空间受限、带宽受限等场合，因此得到了人们的广泛关注。经过10余年的研究，椭圆曲线公钥密码体系开始从学术理论研究阶段逐步走向实际应用阶段，成为目前最有前途的一种公钥密码体系，极有可能成为现存公钥密码体系的替代者。因此，加速对作为信息安全技术的核心基础之一的椭圆曲线密码学的研究，对于促进我国信息化工程建设的高速发展，增强我国的经济竞争实力，维护我国的主权独立和战略安全，具有十分重要的意义。

目前，椭圆曲线公钥密码体系开始从学术理论研究阶段走向

应用实现阶段，受到学术界、开发商、政府部门、密码标准研制组织等有关各界的重视，成为当前密码学界的研究热点，是现今最有前途的公钥密码体系。

虽然目前国际上已对椭圆曲线公钥密码体系进行了较为广泛的研究，但在国内，尚处于起步阶段，与国际先进水平相差较远。本书针对实际应用的需要，对椭圆曲线公钥密码体系及其相关的理论及应用技术展开了深入的研究。

具体而言，本书对椭圆曲线公钥密码体系研究的贡献主要体现在以下几个方面。

（1）*在密钥生成方面*

提出和实现了三种高效快捷的、适用于不同场合的真随机密钥生成方法XRNGS，并设计了相关装置；设计和实现了新型基本密钥对生成算法；研究了公钥可信度问题，并申请了国家发明专利（03128073.0，200510018917.5，200510018918.X，200510018920.7）。

（2）*在密钥管理领域*

设计和实现了新型高效的XKAS密钥协商方案和XKDS密钥分配方案，针对不同条件下的应用问题，研究了相应的改进和扩展方法技术。以此为基础，设计并实现了XKAS密钥协商方案，并申请了两项国家发明专利（03128072.2.公开号：CN1455543A；申请号：03128074.9.）。

（3）*在数据加密方面*

对原有的EC-ElGamal加密算法进行了改进，提出了XEC-ElGamal数据加密算法，设计和实现了基于密钥共享思想的混合数据加密方案XHES，该方案结合了两种密码体系的优点，具有很好的性能和实用价值，并申请了国家发明专利（03128222.9）。

目　录

第1章 绪 论

随着计算机网络特别是因特网的迅猛发展，数字化社会基本成型。网络的开放性使得运行在网上的各种商务活动、政务活动等网络通信活动的安全问题显得更为突出。可以说，安全问题是一切基于网络的通信活动得以正常运行的前提和基础。为了更好地研究网络信息安全问题，本书在介绍网络经济和电子商务发展以及网络信息安全现状之后，通过分析网络通信活动所面临的各种安全威胁、总结人们所提出的各种安全需求、研究相应的安全策略和相关的安全技术，引出了本书的研究主题——椭圆曲线公钥密码体系。

1.1 网络信息安全

Internet 和计算机网络的飞速发展，社会信息化步伐的加快以及网络通信的国际化、信息化、无纸化、低成本、高效率等，使得基于网络的电子商务、电子政务等各种网络社会活动受到了全世界的广泛关注，得到了极其迅猛的发展。

据统计，由于网络技术的导入，美国从1995年到1999年的秘书数量减少了17%，批发和零售业的采购人员减少了16%，节约了大量人力成本。2000年全球网上交易总额达1970亿美元，2001年则达到了3810亿美元，而2002年突破8000亿美元大关，2004年整

体营业额更是达到了创纪录的27748亿美元，几乎成几何级数地增加。通过电子商务实现的交易已经占全球贸易总交易额的20%以上，拥有相当的分量。

在我国，基于网络的各种商务和政务活动也获得了长足的发展。2005年版的《中国电子商务盈利模式研究报告》等资料的数据显示：2004年，我国已建成各类配送中心1000多家，网上银行50余家，企业与个人客户超过1000万户。2004年，我国电子商务的增长率为73.7%，营业额达到4800亿元人民币，网上购物在线支付交易总金额达到6.8亿元，2005年达到15.7亿元。截止到2005年4月，国内互联网用户人数已经超过1亿，其中参与网上购物的比例为37.9%。这说明网络经济、电子商务等基于网络的社会经济活动正在得到飞速发展，它们将成为未来信息社会经济发展的主要推动力。

虽然网络经济中孕育着巨大的商机和财富，吸引了大量投资，但也吸引了罪犯的注意力，网络犯罪的比例日益增加。

在过去的几年中，出现了一连串针对网络，特别是针对因特网的攻击。这些攻击影响巨大，不仅造成了巨大的损失，而且还严重打击了人们对电子商务的信心，使得人们几乎“谈网色变”。

在1999年3月爆发的Melissa病毒和2000年5月爆发的LoveLetter病毒都是利用Outlook电子邮件附件进行传播的，另外恶意代码也都是利用Microsoft公司开发的Script语言缺陷进行攻击的，所不同的是Melissa是Microsoft Word宏病毒，而LoveLetter则是VBScript病毒。Outlook的用户数量众多，使得这两种病毒能够迅速蔓延并造成了极大的危害。它们引起了当时人们对信息安全现状的深思，无形中对信息安全的设施和人才队伍的发展起了很大的促进作用，刺激了企业和公司对网络安全的投资，使得专业的网络安全紧急响应小组得以出现和壮大。

2000年2月，人们刚刚为基本解决“千年虫问题”而松了一口气时，又迎来了分布式拒绝服务攻击DDoS的闪电般突然袭击：全球知名网站雅虎第一个宣告因为遭受分布式拒绝服务攻击而彻底崩溃后，紧接着Amazon.com、CNN、E*Trade、ZDNet、Buy.com、Excite和eBay等其他7大知名网站也几乎在同一时间彻底崩溃。虽然，这场危机仅持续了10个多小时，但其影响却十分深远。因特网上大量的机器进行分布式计算，如DDoS、分布式扫描和分布式口令破解等，使得一个攻击者能够达到许多意想不到的强大效果，并直接导致了2002年的针对因特网寻址系统DNS的主要根服务器的DDoS攻击，几乎导致整个Internet崩溃。

2001年7月出现的基于微软IIS缓冲溢出漏洞进行感染的红色代码变种蠕虫病毒，在首次爆发的短短9个小时内，以迅雷不及掩耳之势感染了250 000台服务器，其速度和深入范围之广引起了全球媒体的注意。红色代码蠕虫不仅篡改英文站点、发动DoS拒绝服务攻击、格式化目标系统硬盘，还在每月20日～28日对白宫的WWW站点的IP地址发动DoS攻击，迫使白宫的所有WWW主机都不得不全部更改自己的IP地址。之后，红色代码不断出现变种，其破坏力也更强。在红色代码II肆虐时，有近2万台服务器和500万个网站被感染，造成了更加惊人的损失。

2001年，“9·11”恐怖袭击事件发生一个星期后出现的尼姆达Nidma蠕虫病毒，利用了IIS缺陷、IE浏览器和Outlook的JavaScript脚本执行的缺陷、硬盘共享的缺陷等至少4种微软产品的漏洞，通过多种不同的途径来进行传播，能感染多种Windows操作系统，仅用了不到半小时就传遍了整个世界，在全球各地攻击了830万台计算机，占用了大部分的网络带宽。Nidma先后出现了9代变种，累计造成将近10亿美元的经济损失。

2003年出现的SQL Slammer蠕虫王和最近出现的Blaster冲

击波病毒，都是利用系统漏洞感染了近70%的Windows网络，从而导致因特网大面积堵塞，使整个网络面临全面瘫痪，造成了巨大的经济损失。特别是冲击波病毒及其变种，不仅感染了近百万台计算机，而且还被认为是"8·14"北美大规模长时间停电事件的罪魁祸首，造成了不下500亿美元的直接经济损失。

除了病毒攻击和恶意攻击以外，直接针对网络社会的政治经济活动的攻击也在不断增加。除了因特网网站以外，卫星通信、ATM和无线网络通信也成为新的攻击目标。

2002年，"资料隐码"自动攻击程序利用大型主机Unix系统的溢出漏洞以及SQL Injection方法，通过网站查询参数，将攻击代码植入网站的数据库，穿透防火墙，直接盗取电子商务和网络银行数据库中的个人资料和密码，骗过交易安全审核机制，展开非法网络交易。据报道，近80%的网络银行、70%的电子商务网站都沦为该程序的攻击目标。欧、美、韩、日等连续发生大规模的身份盗用和冒领欺诈事件，黑客轻易地接管账户，进行虚假交易，让不知情的合法使用者买单付费。一时间人心惶惶，网络电子交易活动陷入低谷。仅仅在2003年2月，就有多达220万个维萨(VISA)和万事达(Master)卡账户、3500万个AOL账号的关键信息被盗，迫使多家银行不得不暂时关闭相关业务。

RSA公司在2003年6月发布的统计数据称：仅2002年，就出现了62 000起黑客攻击事件，因数据被盗窃、身份证被盗窃等事件引发的损失就高达590亿美元。

Card Systems公司主要为万事达、维萨等公司提供信用卡服务，每年能处理高达150亿美元的信用卡客户和商户的结账。2005年6月，恶意黑客闯入了Card Systems公司的客户资料库，窃取了多达4 000万个信用卡账户的资料，导致数十万名用户的账户被盗用，成为有史以来最严重的信息安全事件之一。

美国联邦调查局和美国互联网欺诈投诉中心在2005年8月发布的统计数据显示:2005年上半年,共发生2.37亿次安全攻击活动,同比增长50%,针对政府、金融服务、制造厂商和医疗部门的事件日益增加。我国国家计算机网络应急技术处理协调中心的统计数据表明:2004年针对金融网站和电子商务网站的网络仿冒诈骗攻击比2003年增长了220多倍,中国银行网站、中国工商银行网站等多家金融网站均遭到这类攻击,造成了巨大的经济损失。

所有这些都大大减弱了人们对网络经济的热情,减慢了电子商务的发展速度。因此,如何保障维护网络信息社会的正常秩序、保障网络信息的安全,成为当前急需解决的首要问题。

全球领先的网络安全技术公司赛门铁克公司在2005年9月发布的2005年度上半年互联网安全威胁研究报告中指出,中国受到的网络攻击数量占全球检测到的攻击总数的6%,仅次于美国,位列第二;此外,有18%的攻击事件和攻击跳板来自中国。而另一方面,我国的信息安全技术水平目前还处在低水平状态,在世界范围内,被排在等级最低的"第四类"。因此,我们必须努力促进信息安全技术领域的自主开发,涌现一批具有自主知识产权的信息安全产品。对网络信息安全的研究不仅是必要的,而且是急需的。它不仅关系到我国网络经济和信息化建设的成败,更关系到国家利益和国家安全。

1.2 安全威胁和安全需求

对网络信息安全研究而言,首先需要明确网络社会所受到的各种安全威胁,归纳出人们对网络安全性的一系列需求,为寻求进一步的解决策略做准备。本节将针对网络信息安全的研究需要,首

先分析网络信息社会所受到的安全威胁以及人们提出的安全需求。

在本书的讨论中，始终假定通信各方是通过一条不安全的、开放的公开信道（如 Internet）相互连接的，并认为恶意的第三方（以下统称攻击者）拥有强大的计算能力，有能力控制网络上的信息流的传输。这样，在通信各方之间传输的信息就有可能被攻击者非法阅读和篡改。这里需要注意的是，攻击者并不一定都是局外人，有可能就是系统的一个或多个合法用户。在某些情况下，甚至可能就是通信的一方（如电子交易中的欺诈者）。

对于一个网络通信系统，可以根据信息流的流动状况来分析其工作是否正常、是否受到攻击。

在正常情况下，信息流是从数据发送方的数据源流到数据接收方的目的地，这种正常情况下的信息流动可以用图 1-1 来表示。

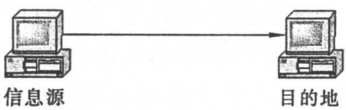

图 1-1　正常的信息流动

当信息流动与图 1-1 所描述的不同时，说明通信过程受到了攻击。这些攻击可以按不同的规则和标准进行分类。在本书中，作者参考了 Steve Kent 提出的攻击分类法，结合目前的网络信息安全的发展情况，根据攻击过程中攻击者的介入程度将这些攻击分成被动攻击和主动攻击两大类。

1.2.1　被动攻击

被动攻击（Passive Attack）是指攻击者在不干扰信息流动的情况下，从网络通信双方所交换的信息数据流中获取所需要的信

息。被动攻击在实践中表现为窃听和监视。由于它并不干扰消息的传输，所以非常难以检测，但可以防止攻击者从所得到的信息流中获得有效的信息。

一般地，被动攻击下的信息流动可以用图1-2来表示。

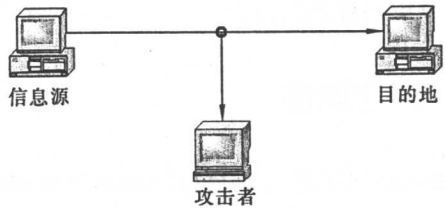

图1-2 被动攻击

根据对所截获的信息的处理方式不同，被动攻击又可以细分为两种类型：析出消息型和通信量分析型。

1. 析出消息

析出消息是指直接从信息数据流中获取所需要的消息，例如，攻击者截获了正在传输的电子邮件并获知其中的具体内容。

2. 通信量分析

当通信的双方使用加密等技术对所传输的消息进行了屏蔽和变换，使得攻击者无法直接从所截获的信息中析出消息时，攻击者可以通过观察所交换的信息的频率、长度等通信量，应用统计学方法分析消息的性质，猜测消息中所包含的可能的内容，这就是通信量分析。

由于被动攻击难以被检测，所以，对付被动攻击的重点在于防范，即防范攻击者从所截获的信息流中获得有效的信息。

对于析出消息型被动攻击，可以用加密技术来预防；而对于通信量分析型被动攻击，则要求经过加密等处理后的信息在统计学上无规律，即该加密算法具有雪崩效应，且每次传输过程中，相同的消息经过加密处理后所得到的信息不同——通过一次一密来预防这种通信量分析型被动攻击。

1.2.2　主动攻击

对于网络通信活动而言，主动攻击(Active Attack)的危害更大，特别是通信各方彼此互不信赖时，这种攻击对通信活动的威胁就显得更为严重。与被动攻击相反，主动攻击者直接参与网络通信，干扰信息的流动，篡改信息的内容，甚至产生虚假的信息流。具体地说，主动攻击有四种类型：伪装攻击、重放攻击、篡改消息和拒绝服务。

1. 伪装攻击

伪装攻击是指攻击者通过产生一个虚假的信息流，伪装成另一个合法的通信实体，参与通信过程。伪装攻击一般与其他类型的攻击联合使用。例如，攻击者可以截获过去的某一合法的鉴别信息，通过对该信息的重放，伪装成某一合法的通信实体参与通信。

伪装攻击下的信息流动如图 1-3 所示。

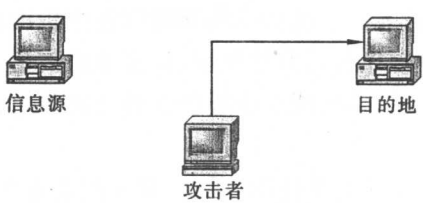

图 1-3　伪装攻击