《密码学讲义》

图书基本信息

书名：《密码学讲义》

13位ISBN编号：9787030263858

10位ISBN编号：7030263855

出版时间：2010-2

出版社：科学

作者：李超//屈龙江

页数：196

《密码学讲义》

前言

随着美国AES计划、欧洲NESSIE计划和esTREAM计划的实施，密码学的理论与方法研究遇到了前所未有的发展机遇和挑战。如何设计安全、高效的对称密码体制和非对称密码体制，已经成为信息安全领域中的重要问题。　　序列密码是一类重要的对称密码体制，它在加解密速度和硬件实现规模两方面具有明显优势，非常适合在大量数据传输和资源受限的场合使用。早期的序列密码研究主要围绕线性反馈移位寄存器序列及其扩展序列展开，这些扩展序列包括前馈序列、非线性组合序列和钟控序列等。由于线性问题具备一些良好的数学理论和方法作为支撑，线性反馈移位寄存器序列及其扩展序列的密码学性质的研究取得了非常丰富的成果。相比之下，非线性反馈移位寄存器序列的密码学性质的研究所取得的成果就很少。特别是2004年欧洲esTREAM计划推出的序列密码算法，大都采用非线性驱动和非线性迭代，使得对这些序列密码算法的理论研究遇到了重大的挑战。如何从理论上刻画eSTREAM计划获胜算法的安全性，是国际密码学者需要解决的重要问题。本书第一部分内容就是利用Galois域的基本理论与方法，较为系统地研究Galois域上线性反馈移位寄存器序列及其扩展序列的密码学性质，即本书的第2章和第3章。然后利用图论和组合数学等数学工具研究Galois域上非线性反馈移位寄存器序列的一些密码学性质，即第4章。系统地掌握这些经典的序列密码设计与分析理论和方法，对于进一步研究eSTREAM计划中的现代序列密码具有重要的意义。　　分组密码是另一类重要的对称密码体制，是保障信息机密性和完整性的重要技术。由于与序列密码的实现机理不同，分组密码的研究主要围绕分组密码的设计、分析、工作模式、快速实现和检测等方面展开。分组密码的设计与分析是一对既相互对立又相互统一的矛盾体，二者的互动决定了分组密码的发展。分组密码的安全性分析为分组密码的设计提供了源源不断的新鲜思想，而各种深思熟虑的设计又给分组密码的分析提出了严峻的挑战。只有对分组密码分析具有深刻的理解和敏锐的感觉，才有可能设计出安全有效的分组密码。分组密码的工作模式是利用分组密码解决实际问题的密码方案，直接影响分组密码在实际应用中的安全性和有效性。分组密码的快速实现和检测是评估分组密码的重要组成部分，为分组密码的设计、分析和应用提供重要的量化指标和技术参数。美国AES计划和欧洲NESSIE计划的实施极大地推动了分组密码理论与方法的发展，使得分组密码的研究从经验设计走向了理论设计的道路。

《密码学讲义》

内容概要

《密码学讲义》从数学的角度较为系统地介绍了序列密码、分组密码和公钥密码的基本理论与方法，利用周期序列的幂级数表示、根表示和迹表示研究了线性反馈移位寄存器序列及其变种的密码学性质；利用图论和组合数学等工具研究了非线性反馈移位寄存器序列的状态图性质，重点介绍M序列的存在性、构造与计数；介绍了五类典型分组密码算法的加解密流程、分组密码的设计原理以及一些常见的分析方法；讨论了RSA体制和椭圆曲线密码体制的基本原理及其相关的数学问题。
《密码学讲义》可以作为密码学与信息安全专业的本科生和研究生的教学用书，也可以作为从事密码学和信息安全研究的科技人员的参考书。

《密码学讲义》

书籍目录

《密码学讲义》

章节摘录

分组密码是对称密码学中一个重要分支，分组密码的研究始于20世纪70年代，研究的主要内容包括两个方面：分组密码的设计和分组密码的分析.分组密码的设计与分析是既相互对立又相互依存的两个方面.从分组密码的发展来看，正是由于这种相互对立，才促进了分组密码的飞速发展.分组密码早期研究主要围绕美国数据加密标准DES进行，推出了许多类似于I）ES的分组密码，比如，I，OKI密码、FEAL密码和GOST密码等。1977-1990年间，由于对DES密码的攻击没有取得突破性进展，分组密码的设计与分析发展较为缓慢.20世纪90年代以后，由于针对DES算法的差分密码攻击和线性密码攻击的提出，人们不得不研究新的密码结构.由xue jia Lai和Masseyr设计的国际数据加密算法I：DEA[10]fInternational Date Encryption Aigorithm）打破了DES类密码的垄断局面，其设计思想主要是混合使用来自不同群中运算.随后出现的Square密码、Shar · k密码和Safer-64密码都采用了结构非常清晰的代替一置换网络，这类密码的特点是算法每一轮由较为明确的混淆层（S盒）和扩散层（P置换）组成，SPN结构的最大优点是能够从理论上证明一个密码算法能否抵抗差分密码攻击和线性密码攻击.1997年，NIST为了履行其法定职责，发起了一场推选用于保护敏感的联邦信息的对称密码算法的活动，在世界范围内征集美国的高级加密标准AES，以取代DES算法.1998年，NIST宣布接收15个候选分组密码算法并提请全世界密码学者协助分析这些候选算法，包括对每个算法的安全性和效率特性进行初步检验.NIsT考察了这些初步的研究结果，选定MARS，RC6，Rijndael，Seipent和Twofish等五个分组密码算法作为参加决赛的算法，经公众对决赛算法进行进一步的分析和评论，2000年，NIS7、决定推荐比利时人Daemen和Rijmen设计的Rijndael密码作为AES算法.继美国推出AES计划以后，欧洲于2000年启动了新欧洲签名、完整性和加密计划fNew European Schemes for Signatui.es，Integrityand Encryption，NESSIE），以适应21世纪信息安全发展的全面需求.该计划为期三年，主要目的就是通过公开征集和进行公开透明的测试、评估，提出一套高效的密码标准，以保持欧洲工业界在密码学研究领域的领先地位2003年，NESSIE工作组公布了包括分组密码、公钥密码、认证码、杂凑函数和数字签名等在内的17个标准算法，其中MISTYl，Camellia，SHACAL三个分组密码算法连同AES算法一起作为欧洲新世纪的分组密码标准算法.这些计划的兴起，使得分组密码研究从经验设计走向理论设计的道路，分组密码理论得到飞速发展，同时，分组密码理论的发展也带动了密码学其他分支的发展.2004年，在欧洲ESTREAM计划的序列密码标准算法的征集活动中，涌现了一大批基于分组密码的工作模式构造的新的序列密码算法，如Salsa 20，LEX等都是基于这种模式设计的随着MD系列Hash函数碰撞攻击的成功。

《密码学讲义》

版权说明