第一图书网, tushu007.com

<<格理论与密码学>>

图书基本信息

书名：<<格理论与密码学>>

13位ISBN编号：9787030363848

10位ISBN编号：7030363841

出版时间：2013-1

出版时间：周福才、 徐剑 科学出版社 (2013-01出版)

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

内容概要

《格理论与密码学》主要介绍格理论中的基础理论、关键技术及其在密码学中的典型应用。
主要包括三方面内容：格理论与密码学的基础知识，包括数论基础、抽象代数基础、向量空间、对称密码体制、公钥密码体制、哈希函数等；格理论的基础理论和关键技术，包括格的基本定义、格中的计算性难题、最短向量问题、最近向量问题、二维格中的高斯格基约减算法、LLL格基约减算法及其衍生和变形、LLL与apprCVP问题以及格基约减算法的MATLAB实现；格理论在密码学中的典型应用，包括基于格的密码系统分析方法以及基于格理论的哈希函数。

《格理论与密码学》可供从事信息安全、密码学、数学、计算机、通信等专业的科技人员参考，也可供高等院校相关专业的师生参考。

<<格理论与密码学>>

书籍目录

前言 第1章数学基础 1.1数论基础 1.1.1整除性和最大公因子 1.1.2模运算 1.1.3中国剩余定理 1.1.4利用中国剩余定理求解二次同余式 1.1.5唯一分解性和有限域 1.1.6有限域中的乘方和原根 1.2抽象代数基础 1.2.1群 1.2.2环 1.2.3可约性和商环 1.2.4多项式环与欧几里得算法 1.2.5多项式环的商和素数阶有限域 1.2.6卷积多项式环 1.3向量空间 1.3.1基本概念 1.3.2范数与正交基 习题 第2章密码学 2.1对称密码体制 2.1.1对称密码体制原理 2.1.2DES算法 2.1.3AES算法 2.2公钥密码体制 2.2.1公钥密码体制的产生 2.2.2公钥密码体制原理 2.2.3Diffie—Hellman密钥交换协议 2.2.4RSA密码系统 2.2.5ElGamal密码系统 2.2.6椭圆曲线密码系统 2.3哈希函数 习题 第3章格的定义与相关性质 3.1格的基本定义 3.2格中的计算性难题 3.3最短向量问题 3.3.1Hermite定理和Minkowski定理 3.3.2高斯启发式 3.4最近向量问题 习题 第4章格基约减算法与实现 4.1二维格中的高斯格基约减算法 4.2LLL格基约减算法及其衍生和变形 4.2.1LLL格基约减算法 4.2.2LLL算法的衍生和变形 4.3LLL与apprCVP问题 4.4格基约减算法的MATLAB实现 4.4.1基本函数 4.4.2计算Hadamard比率函数 4.4.3生成优质基函数 4.4.4计算矩阵的行范数函数 4.4.5向量正交化函数 4.4.6LLL算法的实现 习题 第5章格理论在密码学中的应用 5.1基于格难题的密码系统 5.1.1概述 5.1.2GGH公钥密码系统 5.1.3基于格的GGH密码学分析 5.2同余密码系统及分析 5.2.1同余密码系统 5.2.2基于格的同余密码学分析 5.3背包密码系统及分析 5.3.1背包问题 5.3.2超递增序列背包 5.3.3MH背包公钥密码系统 5.3.4基于格的背包密码学分析 5.4NTRU密码系统及分析 5.4.1NTRU密码系统 5.4.2NTRU的安全性 5.4.3基于格的NTRU密码学分析 习题 第6章基于格理论的哈希函数及应用 6.1预备知识 6.1.1抗碰撞哈希函数 6.1.2Merkle树 6.1.3认证数据结构概述 6.2基于格理论的哈希函数 6.2.1LBH的数学基础 6.2.2LBH的基本结构 6.2.3LBH的安全性 6.2.4LBH的代价分析 6.3基于LBH的更新优化认证数据结构 6.3.1LBH—UOADS基本思想 6.3.2LBH—UOADS构建方案 6.3.3LBH—UOADS的关键算法 6.3.4LBH—UOADS的正确性和安全性证明 6.3.5LBH—UOADS的代价分析 6.4基于LBH—UOADS的数据查询认证方案 6.4.1数据查询认证框架 6.4.2查询认证过程 6.4.3安全性分析 6.4.4代价分析和比较 习题 参考文献

章节摘录

版权页： 插图： 第1章数学基础 本章将介绍本书用到的一些基本的数学概念和符号。
1.1节和1.2节分别简要介绍数论和抽象代数的基础知识，对这些内容不熟悉的读者可以参考更详细的参考书籍；1.3节主要介绍定义在m上的向量空间的概念和性质。
充分理解本章内容对于其余各章的学习是非常必要的。
1.1数论基础 数论和代数学是现代密码学的基础。
本节将介绍数论中的一些重要定理和结论。
数论是研究整数性质的一个数学分支，其研究对象是整数（自然数）。
整数在计算机科学、密码学与信息安全、数字信号处理等领域起到了重要的作用。
本节将介绍整除性和整数的分解，带余除法以及求解最大公因子的相关算法；并介绍模运算的运算法则与性质，以及求解线性同余方程组的方法；此外还介绍了素数、有限域、模除法运算的概念；最后介绍了有限域中的乘方和原根的性质。
1.1.1整除性和最大公因子 若a，b是整数，则可以分别计算a+b，a—b，ab，且所得结果均是整数。
这种性质称为对元素运算的封闭性。
但是对除法运算并不能总是满足这种运算封闭性。
例如，不能用2去除3，因为3/2并不是整数，由此引出了整除性的基本概念。
定义1.1设a，b是整数，b≠0。
若存在整数c，满足a＝bc，则称b整除a或a被b整除，记为b｜a。
命题1.1设a，b，c∈¢，则有 （1）若a｜b，b｜c，则a｜c； （2）若a｜b，b｜a，则a＝±b； （3）若a｜b，a｜c，则a｜（b+c）且a｜（b—c）。
定义1.2a和b的公因子是能够同时整除二者的正整数。
顾名思义，最大公因子就是满足d｜a，d｜b的最大的正整数d，用gcd（a，b）来表示。
在不存在歧义的情况下也可以表示成（a，b）。
最大公因子的概念虽然简单，但有很多应用。
下面介绍几种计算最大公因子的方法。
定义1.3（带余除法）设a，b是正整数，则存在唯一的q和r满足a＝bq+r，0≤r＜b若求a和b的最大公因子，首先对a作带余除法，即a＝bq+r，0≤r＜b若d是a和b的公因子，则d也能够整除r；若e是b和r的公因子，e也能够整除a。
换言之，有gcd（a，b）＝gcd（b，r） 重复此过程，对b作带余除法，即b＝rq′+r′，0≤r′＜r则有gcd（b，r）＝gcd（r，r′） 此过程将使余数越来越小，最终为0，此时有gcd（s，0）＝s＝gcd（a，b）。

编辑推荐

《格理论与密码学》可供从事信息安全、密码学、数学、计算机、通信等专业的科技人员参考，也可供高等院校相关专业的师生参考。

第一图书网, tushu007.com

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com