现代密码学

——基于安全多方计算协议的研究

孙茂华◎著

Modern Cryptography

Research on Secure Multi-party Computation Protocols

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

现代密码学

——基于安全多方计算协议的研究

孙茂华 著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书以现代密码学中的安全多方计算为主题，以作者近几年的研究成果为主体，结合国内外学者在该领域的研究成果，对安全多方计算的主要研究内容作了系统论述。本书主要分为两部分：第一部分介绍数学、密码学等基础知识(第 1～3 章)，第二部分介绍安全多方计算的基础理论和应用(第 4～10 章)。

本书可作为对安全多方计算感兴趣的读者的入门教材，也可以作为安全多方计算领域科研工作者的参考用书，适合于密码学、信息安全、计算机科学与技术、数学及相关学科的高年级本科生、研究生、教师阅读参考。

图书在版编目 (CIP) 数据

现代密码学：基于安全多方计算协议的研究 / 孙茂华著. — 北京：电子工业出版社，2016.9
ISBN 978-7-121-29995-7

I. ①现… II. ①孙… III. ①密码协议－研究 IV. ①TN918.1

中国版本图书馆 CIP 数据核字(2016)第 233636 号

策划编辑：王志宇
责任编辑：郝黎明
印　　刷：北京中新伟业印刷有限公司
装　　订：北京中新伟业印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×1092　1/16　印张：9.25　字数：236.8 千字
版　　次：2016 年 9 月第 1 版
印　　次：2016 年 9 月第 1 次印刷
定　　价：35.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010)88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：(010)88254523，wangzy@phei.com.cn。

前　言

近几年来，云计算、物联网、移动互联网等新概念、新技术被先后提出，促使信息技术飞速发展。同时，人类生活、沟通方式也随着新技术的普及不断变化。一方面，人类的沟通方式已经由传统的书信、电报、电话形式发展为使用计算机、智能手机、个人数字助理和平板计算机等网络终端设备；另一方面，电子媒体、网络技术不断发展，信息技术不断融入到社会化服务体系中。上述应用的快速进步，又促进了其他信息技术(如数据挖掘、电子商务、云计算技术等)的快速进步。但是，信息技术在给人们带来便捷的同时，信息安全问题也不断凸显。例如，近几年来，信息泄露事件不断发生，国内外多家著名互联网站、银行、公司发生信息泄露事件；网络攻击事件不断发生，且攻击技术不断升级，所造成的影响也越来越恶劣；随着智能终端的不断发展和推广，针对移动智能终端的恶意攻击比率不断提高。信息安全事件频繁发生，在给人们带来经济损失的同时，也给人们敲醒了安全警钟。各国政府和人民开始高度关注信息安全。2014 年 2 月 27 日，我国成立了“中央网络安全和信息化领导小组”。该领导小组着眼于国家安全和长远发展，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强安全保障能力。

安全多方计算融合了密码学和分布式计算技术，是信息安全领域的一个重要研究方向，是现代密码学的重要组成部分，具有重要的研究价值和意义。首先，密码学中已经实现了对称加密算法和公钥加密算法。按照事物从低级往高级发展的必然规律，安全多方计算是密码学发展的必然方向。其次，近几年来分布式计算尤其是云计算技术迅速发展。过去的惨痛教训告诉我们，在一项新技术发展的初期就需要充分考虑安全问题。而伴随着不断发生的云安全事故，云计算安全也逐渐引起了人们的关注。很多安全专家指出，云计算的广泛应用需要向云计算架构中加入更强大的安全措施以保证其安全性，促进云计算应用的重点是解决云计算所面临的各种安全问题。安全多方计算作为一种研究分布式计算环境下多个参与方计算安全性的技术，对保证云计算的安全具有重要意义。再次，安全多方计算具有广泛的应用场景。例如，将安全多方计算应用到拍卖、投票中，实现安全电子拍卖、电子投票；将安全多方计算和数据挖掘技术相结合，实现保护隐私的数据挖掘技术等。可见，对安全多方计算的研究具有重要的理论和应用价值。

作者在过去的学习过程中发现，市面上的现代密码学书籍中往往将安全多方计算作为其中一个章节进行介绍。事实上，安全多方计算发展至今，已经积累了丰富的基础理论和研究成果。本书以现代密码学中的安全多方计算为研究重点，带领读者学习密码学中安全多方计算的基础知识和近期研究成果，希望帮助读者尽快进入这一领域。本书的内容以作者攻读博士学位期间的研究成果为基础，结合国内外学者在安全多方计算领域的最新研究进展和作者对该领域的认识，经过仔细归纳整理而成。

本书共10章，第1～3章介绍基础知识，第4～10章介绍安全多方计算及其应用。其中，第6～10章分别介绍了安全多方计算在数据比较、科学计算、电子投票、计算几何及集合运算5个领域中的应用。

本书得以顺利完成，首先要感谢我的博士生导师——北京邮电大学罗守山教授。罗老师学识渊博、治学严谨、淡泊名利。罗老师带我走上了安全多方计算的研究之路。短短的博士三年，我不仅跟罗老师学到了如何做研究，更主要的是学习到了他严谨的治学态度和“仁远乎哉，我欲仁斯仁至矣”的精神品质。在此，再次感谢罗老师对我的悉心指导和辛勤培养。2010—2013年我参加了由罗守山老师创办的安全多方计算讨论组，由衷感谢庞雷博士、贾哲博士、耿涛博士、许芬博士，感谢他们将自己掌握的知识、学习方法和经验进行了无私的分享。还要感谢武汉理工大学的于晓敏为本书所做的不厌其烦的工作及电子工业出版社的王志宇编辑对本书出版所付出的辛苦劳动。

本书的出版还得到了首都经济贸易大学青年科学基金(2014XJQ016)、首都经济贸易大学青年科研启动基金(恶意模型下的安全多方计算技术)、国家社科基金项目(15AGL001)、北京市教委科技面上项目(KM201410038001)的支持，在此一并表示感谢。

由于水平有限，书中难免有谬误之处，恳请读者批评和指正。近些年来，安全多方计算乃至密码学的理论和技术都在飞速发展，由于篇幅有限，很多新理论和新成果未能在本书中体现，敬请读者谅解。

孙茂华

目　录

第1章
绪　论

1.1　密码学的发展历史

密码学是一门发展中的交叉学科，由于其古老而深奥，对一般人来说既神秘又陌生。过去，密码学仅用于军事领域。随着计算机的发展和普及，基于数学和计算机的密码学得到了迅猛发展。纵观密码学的发展历史，可以将密码学划分为经典密码学和现代密码学两个阶段。

20 世纪 80 年代以前的密码学是一种艺术，被称为经典密码学。经典密码学阶段又被划分为两个时期。1949 年之前是经典密码学发展的第一个时期，被称为古典密码学阶段。密码学的历史十分悠久。早在 4000 年前，埃及人就开始使用密码实现传递消息的保密性。这个阶段的典型密码技术有凯撒密码和维吉尼亚密码等。在这长达几千年的时间里，人们使用了纸、笔或者简单器械实现的代换或置换来满足消息加密的需求。1883 年，Kerchoffs 第一次明确提出了“加密算法应建立在算法的公开且不影响明文和密钥安全的基础上”的编码原则，这个原则得到了广泛的认可，是古典密码学阶段的重要成果。从 1949 年到 1975 年，密码学成为一门独立的学科，是经典密码学发展的第二个时期。1949 年，美国数学家 Shannon 发表了论文《保密系统的通信理论》，论文在信息论的基础上阐述了关于密码系统分析、评价和设计的科学思想。文中所提出的破译密码的计算理论已和计算机理论中的计算复杂性理论结合起来，成为评价密码安全性的一个重要准则。Shannon 的这篇论文也成为近代密码学开始的标志。在经典密码学发展的第二个时期中，密码机的出现使信息保密由手工方式转换为机器自动计算，大大提高了信息安全保护水平；同时，数据的安全性不再基于算法的保密性，而是基于密钥的保密性。从使用者的身份来看，经典密码学阶段的成果主要被军事和智囊机构使用。例如，明朝著名抗倭将领、军事家戚继光发明并使用了“反切密码”用于传递军事机密，他还专门编写了一本《八音字义便览》用于培训情报人员和通信兵。第二次世界大战中，各个国家都致力于密码的截获和破译，密码技术成为直接影响二战胜败的重要因素。例如，1941 年我国著名密码破译专家池步洲截获并破译了日本的一份密电，提前获知了日本准备偷袭珍珠港的情报。可惜，蒋介石将情报通报给美军之后并没有得到美军的重视，铸成了后来著名的珍珠港偷袭事件。在第二次世界大战中，英国成功破译了德军的“恩尼格码”密码(图 1-1)，帮助盟军掌握了第二次世界大战欧洲战场的主导权。

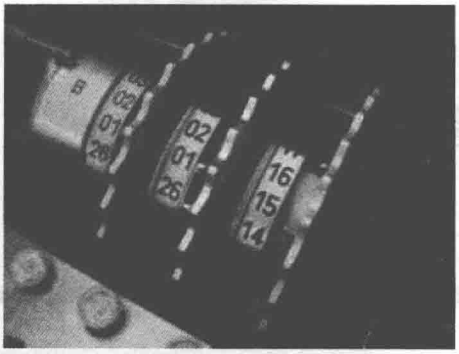

图 1-1　恩尼格码密码机

1976 年，Diffie 和 Hellman 发表了《密码学新方向》，提出了一种新的密码设计思想，证明了通信双方在不传输密钥的情况下实现保密通信的可能性。这篇文章开创了公钥密码学的新纪元。从此，密码学进入了现代密码学阶段。20 世纪 80 年代以后，计算机的性能得到了飞速提高，同时计算机网络逐步建立并发展起来。计算机网络将原来孤立的单机系统连接在一起，实现了信息和资源的共享。然而，随之而来的信息安全问题也不断凸显。由于信息在处理、存储、传输和使用上有严重的脆弱性，很容易被泄露、窃取、篡改、伪造和破坏。人们开始使用防火墙、入侵检测设备和安全路由器等方式来抵御安全威胁。防火墙、入侵检测设备和安全路由器等安全网关设备中使用了大量的密码学算法。近几年来，随着云计算、物联网、移动互联网等技术的进步和普及，新的安全威胁不断出现。这也促进密码学算法的不断发展。不同于经典密码学的军事化用途，现代密码学技术已经被广泛应用在日常生活中的各个方面。例如，银行使用密码学协议来保障网上银行的安全性；计算机基于密码学方法实现访问权限控制等。可以看出，现代密码学已经不再单纯为军方或智囊机构使用，而是成为国家机构、公司、组织和网民共同使用的技术。

1.2　现代密码学体制

现代密码学发展至今，主要分为密码编码学和密码分析学两个分支。

密码编码学致力于建立难以被敌手攻破的安全密码体制。一个密码系统通常由明文空间、密文空间、密钥空间、加密算法和解密算法五部分组成。被加密的原始信息称为明文，加密后的信息称为密文。加密过程就是根据一系列的规则(称为加密算法)将明文转换为密文的过程。解密过程是加密过程的逆过程，是指根据另外一系列规则(称为解密算法)，将密文转换为明文的过程。加密过程和解密过程往往需要使用一对密钥进行控制，分别称为加密密钥和解密密钥。在密码编码学中，根据整个协议中的加密密钥和解密密钥是否相同可以将密码编码学算法划分为对称密码学算法和公钥密码学算法。

对称密码学算法的出现早于公钥密码学算法。在对称密码体制中，通信双方使用同一个密钥实现加密和解密。因此，对称密码体制也被称为是单钥密码体制。对称密码体制的安全性依赖于密钥的保密性，而不是算法的保密性。也就是说，即使加密算法是公开的，只要密钥没有公开，信息的保密性依然可以保证。流密码和分组密码是对称密码算法中最常见的两类算法。流密码采用逐字加密方式完成加密。分组密码首先将信息分组，每个分组中包含多个字符，然后逐组进行加密。对称加密体制中最大的问题是密钥的分发和管理非常复杂且实施代价很高。尤其是大型网络中，当用户较为分散且数量较多时，对称加密体制的开销极高。但是，对称加密算法由于加密速度快，适用于高速保密通信。在公钥密码学算法中，通信双方使用不同的密钥分别实现加密和解密。因此，公钥密码体制也被称

为是双钥密码体制或非对称密码体制。用于加密的密钥被称为公钥，是公开的。用于解密的密钥被称为私钥，是需要保密的。公钥密码学算法的安全性要求之一是通过公钥计算出私钥在计算上是困难的。相对于对称加密体制，公钥加密体制在密钥的分配和管理上容易得多。但是，由于公钥加密体制多数使用复杂的数学计算，多数公钥密码学算法的运算效率远远低于对称密码学算法的运算效率。

密码分析学主要是研究如何根据已经收集到的信息获得明文。对密码进行分析的尝试称为攻击。当前，攻击的方法主要有穷举攻击、统计分析攻击和数学分析攻击三类。根据密码分析时所利用的数据来源不同，也可以将攻击分为唯密文攻击、已知明文攻击、选择明文攻击和选择密文攻击四类。

如今，现代密码学作为一门重要的交叉学科，在促进信息化的健康发展中起了十分重要的作用。同时，现代密码学已经同生物学、量子学等学科有效结合，形成了生物特征密码学、视觉密码学、量子密码学等多个子学科。

1.3 现代密码学与安全多方计算

安全多方计算是现代密码学的一个研究分支，是现代密码学的重要组成部分。不同的密码学分支研究的目的不同。例如，公钥密码学算法最早是为了解决密钥分配问题而诞生的。当然，公钥密码学算法发展至今已经不再仅仅应用于密钥分配。安全多方计算主要解决分布式环境下多个参与者之间的计算安全性问题。可以先通俗地这样理解安全多方计算所解决的问题：分布式环境下，通信双方或多方如何在保护自己输入信息的前提下，完成某个功能函数计算。

安全多方计算协议的构造需要使用密码学中的很多工具。例如，秘密共享、茫然传输、同态加密算法、零知识证明等。本书第 3 章将对这些密码学工具进行介绍。

安全多方计算作为密码学的一部分，也经常被作为底层模块去构造更加复杂的密码学协议。例如，本书第 7.4 节中使用安全多方计算协议构造多秘密共享协议。

安全多方计算可以看成是密码学和不同应用场景下的计算问题相结合的产物。例如，安全多方集合运算是使用密码学技术解决分布式环境下多个参与者之间安全地计算集合的交、并或其他运算问题。按照应用场景的不同，可以将安全多方计算进行分类，如图 1-2 所示。

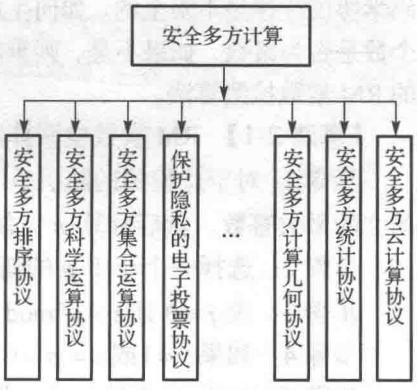

图 1-2 安全多方计算的分类

国际著名密码学家 Goldwasser 曾经说过：“安全多方计算今天所处的地位正是公钥密码学算法 10 多年前所处的地位。它是密码学研究中一个极其重要的工具，它在计算科学中的应用才刚刚开始，丰富的理论将使它成为计算科学中一个必不可少的组成部分。”

第2章
数学基础

现代密码学是建立在数学、计算机科学等基础学科之上的。《老子·德经》有云：合抱之木，生于毫末；九层之台，起于累土；千里之行，始于足下。本章介绍现代密码学中的一些常用数学基础知识。

2.1 预备知识

2.1.1 素数

整数集合用 $\mathbb{Z}$ 表示，对于整数集合中的元素 $a,b\in\mathbb{Z}$，如果存在一个整数 c，使得 $a*c=b$ 成立，则称 a 整除 b，记作 $a|b$。如果 $a|b$ 并且 a 是正整数，则称 a 是 b 的一个除数。如果加上条件 $a\notin\{1,b\}$，则称 a 是 b 的一个非平凡除数或称为因子。正整数 $p>1$ 如果没有因子，则为素数；也就是说，素数只有 1 和自身两个除数。一个大于 1 的正整数如果不是素数则为合数。我们约定 1 既不是素数也不是合数。

很多密码学协议中都需要生成素数。生成一个小的素数比较容易，然而基于小素数的密码学协议往往是不安全的。如何生成一个大素数？我们可以选择一个较大的数，然后检查这个数是否为素数，如果不是，则重新选择并检查，直到产生一个大素数为止。下面介绍著名的 RM 素数检测算法。

【算法 2-1】 RM 素数检测算法

步骤 1：对于待检测的随机数 p，计算 b。b 是 2 整除 $p-1$ 的次数，即 2^b 是能整除 $p-1$ 的 2 的最大幂数。然后计算 m，使得 $n=1+2^b m$。

步骤 2：选择一个小于 p 的随机数 a。

步骤 3：设 $j=0$ 且 $z=a^m \bmod p$。

步骤 4：如果 $z=1$ 或 $z=p-1$，那么 p 通过测试，p 可能是素数。

步骤 5：如果 $j>0$ 且 $z=1$，那么 p 不是素数。

步骤 6：设 $j=j+1$。如果 $j<6$ 且 $z\neq p-1$，则计算 $z=z^2 \bmod p$，然后回到步骤 5。如果 $z=p-1$，那么 p 通过测试，p 可能是素数。

步骤 7：如果 $j=b$ 且 $z\neq p-1$，那么 p 不是素数。

2.1.2 模运算

【定义 2-1】（同余的模）

设 a,b 是整数，如果 $a=b+kn$ 对某些 k 成立，那么就说 a,b 模 n 同余，记作 $a\equiv b(\mathrm{mod}\,n)$，$n$ 称为同余的模。

模 n 运算的结果一定是 0 到 $n-1$ 之间的一个数，从 0 到 $n-1$ 的整数组成的集合包括了模 n 的所有结果，或者说模 n 运算的结果一定落在这个集合中，称这个集合为模 n 运算的最小剩余集，记作 $Z_n=\{0,1,2,\cdots,n-1\}$。

2.1.3 群

【定义 2-2】（群的定义）

一个非空集合 G 对于一个二元运算“*”来说作为一个群，假如

Ⅰ. G 对于“*”来说是闭的；

Ⅱ. 结合律成立，即对于 G 的任意三个元 a、b、c 满足

$$a*(b*c)=(a*b)*c$$

Ⅲ. G 中至少存在一个左单位元 e，使得

$$e*a=a$$

Ⅳ. 对于 G 的每一个元 a，在 G 中至少存在一个左逆元 a^{-1}，使得

$$a^{-1}*a=e$$

例如，假设 G 是全体整数的集合，G 对于普通加法来说作成一个群。假设 G 是所有不等于零的整数的集合，G 对于普通乘法来说不作成一个群。

一个群 G 中元素的个数可以是有限的，也可以是无限的。如果一个群中元素的个数是一个有限整数，则称这个群为有限群。否则的话，这个群称为无限群。一个有限群的元的个数称为这个群的阶。

由于在一个群里结合律是成立的，因此 $a_1*a_2*\cdots*a_n$ 有意义。又由于群对于“*”来说是闭的，因此 $a_1*a_2*\cdots*a_n$ 是 G 的某一个元。这样，可以把 n 个相同的元 a 来相乘。因为用普通乘法的符号来表示群的运算，所以可以使用符号 a^n 来表示 n 个相同的元 a 的乘法，即

$$a^n=a*a*\cdots*a\quad（n\text{是正整数}）$$

并且也把 a 称为 a 的 n 次乘方（简称 n 次方）。

【定义 2-3】（交换群）

一个群 G 称为交换群，假如

$$a*b=b*a$$

对于 G 的任何两个元 a、b 都成立。

【定义 2-4】（单位元）

一个群 G 中唯一能使

$$e*a=a*e=a\qquad（a\text{是}G\text{的任意元}）$$

的元 e 称为群 G 的单位元。

【定义 2-5】（逆元）

唯一能使

$$a^{-1} * a = a * a^{-1} = e$$

的元 a^{-1} 称为元 a 的逆元，有时也简称逆。

【定义 2-6】（阶）

对于群 G 的一个元 a，能够使得

$$a^m = e$$

的最小的正整数 m 称为 a 的阶。

【定义 2-7】（循环群）

如果一个群 G 的每一个元都是 G 的某一个固定元 a 的乘方，就把 G 称为循环群；也就是说，G 是由元 a 所生成的，并且用下面符号来表示

$$G = (a)$$

其中，a 称为 G 的一个生成元。

2.2 密码学困难性假设

现代密码学方案尤其是公钥密码学方案的安全性是建立在解决某些问题的困难性假设基础上的。例如，RSA 公开密钥算法是基于大数分解困难性假设设计的，ElGamal 加密算法是基于离散对数困难性假设设计的，Paillier 加密算法的安全性依赖于合数剩余判定困难性假设。那么，在密码学中什么样的问题是困难的呢？困难并不是无法计算或无法攻破，很多学者致力于研究当前密码学中常用困难性假设问题的解决算法并已经取得了一系列进展。例如，对于满足如下假设的大数分解困难性问题，已经陆续有更短运行时间的算法被提出。假设 $N = pq$，p 和 q 是两个长度相等但大小不同的素数，大数分解问题要求对 N 进行分解，即求出 N 的素因子。Pollard 提出的 RHO 方法是一种通用因子分解方法，针对上述大数分解问题，该算法的时间复杂度是 n 的指数函数，其中 n 是大数 N 的长度。Pomerance 提出的二次筛算法也是一种通用因子分解方法，该算法的时间复杂度是 n 的亚指数函数。尽管解决这些困难性假设问题已经取得了一些成果，但是当前没有找到多项式时间算法或概率多项式时间算法来解决这些问题。因此，当合理选择参数时，人们认为攻破基于这些困难性问题的密码学方案在时间上是不可接受的，从而保证了这些密码学方案在一段时间之内的安全性。当然，随着信息技术的不断进步，如果有一天这些困难性假设不再成立，那么这些假设所对应的密码学方案的安全性也将荡然无存。

本节介绍现代密码学方案中常用的困难性假设问题，深入理解这些问题可以帮助人们更好地设计密码学方案。

2.2.1 大数分解困难性假设

在数论中，对一个数进行因子分解是一个古老的问题。分解一个小的数相对比较容易，例如下面使用试除法得到一个数的因子分解，其中 p_i 是互不相等的素数并且 $x_i \geq 1$。

$$12 = 2^2 \times 3$$

$$88 = 2^3 \times 11$$

$$\vdots$$

$$N = p_1^{x_1} p_2^{x_2} \cdots p_k^{x_k}$$

然而，分解一个较大的数就不是这么容易了。尽管当前已经有二次筛算法、连分式算法、普通数域筛选法等一系列研究成果，但是正如上文中提到的，这些算法无法在多项式时间或概率多项式时间内解决问题。因此，在当前的计算能力下，解决大数分解问题是困难的。这就是大数分解困难性假设，其形式化定义如下。

给定一个大数 N，N 满足 $N = pq$，其中 p 和 q 是两个长度相等但大小不等的素数，即 $|p| = |q| = l$。对于任意的多项式时间算法 $A(N) = (p', q')$，存在一个可忽略的函数 $\mathrm{neg}(n)$ 满足

$$P_r\left[(A(N) = (p', q')) \wedge ((p', q') = (p, q))\right] \leqslant \mathrm{neg}(n)$$

2.2.2 离散对数困难性假设

首先解释什么是离散对数。给定素数 p，假设 α 是 Z_p^* 上的生成元，β 是 Z_p^* 上的元素，如果整数 x 满足 $\alpha^x \bmod p = \beta$，则称 x 是关于 α 底 β 的对数，记作 $x = \log_\alpha \beta$。下面讨论定义在任意循环群上的离散对数。假设 $\mathbb{G}$ 是 n 阶循环群，g 是 $\mathbb{G}$ 上的生成元，则对于任意的 $h \in \mathbb{G}$，存在唯一 $x \in Z_n$ 使得 $g^x = h$。当循环群 $\mathbb{G}$ 已时，称 x 是关于 g 底 h 的对数，记作 $x = \log_g h$。可以看出，对于任意整数 x'，如果 $g^{x'} = h$，则 $x = x' \bmod n$。从这个角度来讲，离散对数的值在“有限”范围内，而传统对数值的范围是无穷集合。尽管存在这种差别，但是传统对数的很多规则仍然适用于离散对数。例如，假设 e 是循环群 $\mathbb{G}$ 的单位元，则 $\log_g e = 0$。

严格的离散对数困难性假设如下：假设 p 是一个大素数且 $|p| = l$，$\alpha \in Z_p^*$ 是一个生成元，$\beta \in Z_p^*$ 且满足 $\alpha^x \bmod p = \beta$。对于任意的多项式时间算法 $A(\alpha, \beta, p)$，存在一个可忽略的函数 $\mathrm{neg}(n)$ 满足

$$P_r\left[(A(\alpha, \beta, p) = x) \wedge (\alpha^x \bmod p = \beta)\right] \leqslant \mathrm{neg}(n)$$

循环群上的离散对数困难性假设如下：给定 n 阶循环群 $\mathbb{G}$，g 是 $\mathbb{G}$ 上的生成元，h 是 $\mathbb{G}$ 上的元素。对于任意的多项式时间算法 $A(\mathbb{G}, g, h)$，存在一个可忽略的函数 $\mathrm{neg}(n)$ 满足

$$P_r\left[(A(\mathbb{G}, g, h) = x) \wedge (x \in Z_n) \wedge (g^x = h)\right] \leqslant \mathrm{neg}(n)$$

2.2.3 Diffie-Hellman 问题

Diffie-Hellman 问题与上节介绍的离散对数困难性假设具有一定的相关性。常用的 Diffie-Hellman 问题分为两类，一类是计算 Diffie-Hellman 问题，简称 CDH；另一类是判定 Diffie-Hellman 问题，简称 DDH。

给定 n 阶循环群 $\mathbb{G}$，g 是 $\mathbb{G}$ 上的生成元，h_1 和 h_2 都是 $\mathbb{G}$ 上的元素。计算 Diffie-Hellman 问题是指计算 $g^{\log_g h_1 \cdot \log_g h_2}$。判定 Diffie-Hellman 问题是指判定 $\mathbb{G}$ 上的元素 h' 是否满足 $h' = g^{\log_g h_1 \cdot \log_g h_2}$。

第3章
密码学基础

某公司打算将一个包含重要商业机密的秘密信息告诉 n 个员工。但是，公司不希望任何一个员工单独获得秘密信息，它希望至少 t 个员工同时在场时才能获知秘密信息。那么，这个公司该如何实现秘密的分发呢?

这是秘密共享的典型应用场景，秘密共享是安全多方计算常用的密码学原语之一。如果把安全多方计算看作高楼，那么秘密共享、茫然传输、同态加密技术、零知识证明技术、比特承诺等密码学原语就是这座高楼的地基。和很多其他领域相同，安全多方计算的地基一直在不断地发展和完善。本章将为读者展示设计安全多方计算协议时常用的密码学原语。

3.1 秘密共享

现代密码学体制基于 Kerchhoff 假设，即一个秘密系统的安全性与它所使用的密钥的安全性相关，与它所采用的加解密算法无关。对称加密系统的安全性取决于其所使用密钥的安全性；公钥加密系统的安全性取决于其所使用私钥的安全性。因此，为了保证秘密系统的安全性，密钥的管理极为重要。在传统的密钥管理方案中，为了防止密钥丢失，往往将密钥在多处进行备份。但是，随着密钥备份数量的增加，密钥被泄露的概率也不断增加。为了解决上面的问题，1979 年 Shamir 和 Blakley 分别提出了秘密共享的概念和解决方案。一个完整的秘密共享算法由子秘密生成算法、秘密分发算法和秘密恢复算法三部分组成。

【定义 3-1】（秘密共享）

秘密发布者 D 根据访问结构 Γ 将秘密在参与者 P 中分享，每个参与者得到的秘密份额被称为子秘密。访问结构 Γ 定义了参与者的授权子集，由任意授权子集中的参与者贡献出他们持有的子秘密可以恢复被共享的秘密，但是非授权子集中的参与者不能获得关于秘密的任何有用信息。

【定义 3-2】（(t-n)门限秘密共享）

一个秘密共享算法被称为是 $(t-n)$ 门限秘密共享算法，如果它满足：秘密分发阶段秘密发布者 D 将秘密 $s \in GF(q)$ 在 n 个参与者 $\{p_1, p_2, \cdots, p_n\}$ 之间共享；秘密恢复阶段，至少需要 t 个参与者贡献出他们的子秘密才能恢复出秘密。

3.1.1 研究进展

秘密共享不论在理论研究还是在实际应用方面，都具有非常重要的价值。因此，秘密共享的概念被提出后，国内外众多学者纷纷加入到秘密共享的研究行列中。图 3-1 显示了秘密共享算法的最新研究方向和理论基础。