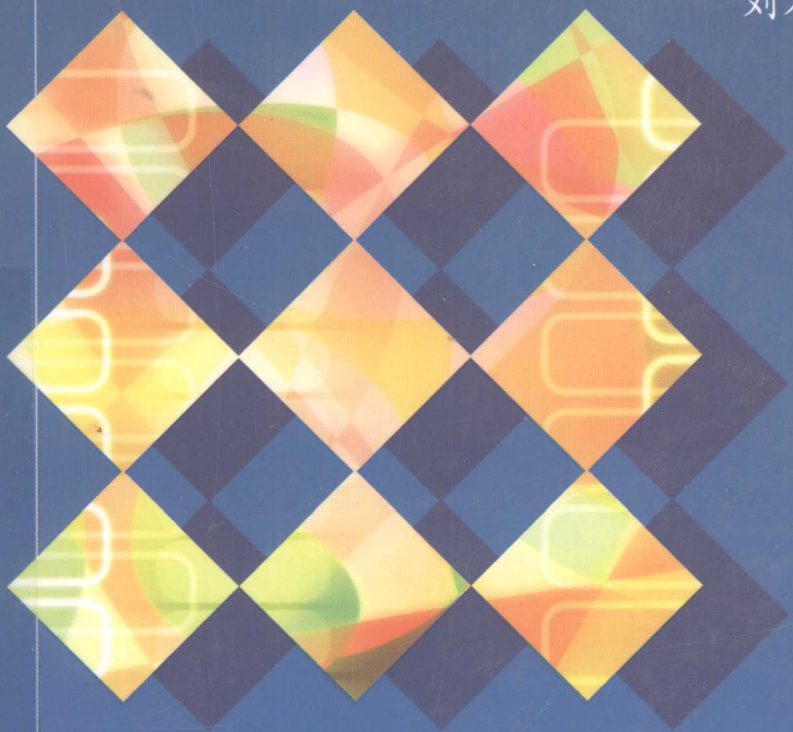
国家科学技术学术著作出版基金
国家重点基础研究发展计划(973)项目

“十一五”国家重点图书出版规划项目
国家自然科学基金项目

# 密钥共享体制和安全多方计算

## Secret Sharing Schemes and Secure Multiparty Computation

刘木兰　张志芳　著



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

国家科学技术学术著作出版基金　十一五国家重点图书出版规划项目
国家重点基础研究发展计划（973）项目　国家自然科学基金项目

# 密钥共享体制和安全多方计算

## Secret Sharing Schemes and Secure Multiparty Computation

刘木兰　张志芳　著

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

## 内 容 简 介

本书共分 5 章. 第 1 章讲述密钥共享体制的基本概念和数学模型. 第 2 章系统讲述线性密钥共享体制和线性多密钥共享体制. 第 3 章讲述密钥共享体制的几个应用. 第 4 章讲述密钥共享体制的信息率. 第 5 章从密钥共享体制应用的角度讲述安全多方计算理论，特别给出了几个典型的安全多方计算协议安全性的详细证明.

本书可作为密码学和信息安全、网络安全、电子商务、计算机科学和信息科学等专业研究生和大学本科高年级学生的教学参考书，也可作为有关科研人员、工程技术人员的参考书.



**图书在版编目（CIP）数据**

密钥共享体制和安全多方计算/刘木兰，张志芳著. —北京：电子工业出版社，2008.2
ISBN 978-7-121-05792-2

Ⅰ. 密… Ⅱ. ①刘…②张… Ⅲ. 密码—安全技术—计算 Ⅳ. TN918.2

中国版本图书馆 CIP 数据核字（2008）第 005012 号

策划编辑：秦 梅
责任编辑：周宏敏
印 刷：北京市铁成印刷厂
装 订：三河市金马印装有限公司
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：787×980 1/16 印张：16 字数：358 千字
印 次：2008 年 2 月第 1 次印刷
印 数：3 000 册 定价：45.00 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。

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。

服务热线：（010）88258888。

# 作 者 序

本书从 2004 年立项到 2007 年完成，历时 3 年多，最后的版本与开始的想法已有相当大的改变. 最初，主要打算讲述线性密钥共享体制和密钥共享体制的信息率. 因为前者的内容比较完整，包括了我和我的学生在该领域取得的比较系统的成果；后者是密钥共享理论的一个重要内容，虽然近些年，这方面的研究工作已不太活跃，但仍不失为理论研究的一个重要方面，而且其中有些算法的原始想法至今可能仍有其可借鉴之处. 关于安全多方计算，开始只是把它作为密钥共享体制的一个应用来看，但是随着我们研究工作的不断进展，使得我们体会到有必要将它独立出来. 除了讲述安全多方计算的一些重要结果，包括我们自己的一些成果之外，特别是要讲清楚安全多方计算的安全性含义和关于安全性的严格证明，这点也正是初学者难以掌握的地方. 这种想法的结果使得安全多方计算的内容占了本书约三分之一的篇幅，故而本书的书名由“密钥共享理论、模型及其应用”改为“密钥共享体制和安全多方计算”.

本书没有追求讲述密钥共享体制的方方面面，而是着重于讲述线性密钥共享体制. 当然，这从技术与应用角度来看，它也是密钥共享体制最重要的内容. 至于安全多方计算，除基本概念和思想之外，重点着眼于应用线性密钥共享体制解决安全多方计算的安全性问题. 因此，在本书中，关于可验证密钥共享体制、计算密钥共享体制及针对主动攻击的安全多方计算等都讨论得很少. 我们希望将来能有机会对此进行弥补.

刘木兰

2007 年 11 月于北京

# Introduction

The present monograph consists of five chapters. Chapter 1 introduces some basic concepts and general models of secret sharing schemes, including access structures, secret sharing schemes, information rate, homomorphic secret sharing schemes, dynamic secret sharing schemes and verifiable secret sharing schemes. In particular, based on distributions of random variables it describes the definitions of perfect secret sharing schemes, statistical secret sharing schemes and computational secret sharing scheme in a uniform way. It also introduces the relationship between ideal secret sharing schemes and matroids.

Chapter 2 makes a systematic study of the theory of linear secret sharing schemes and linear multi-secret sharing schemes by using monotone span programs. It displays quite a few examples of linear secret sharing schemes along with the corresponding monotone span programs. It also studies the dual access structure and the rearrangement of access structures. Moreover, it points out the security problem in the reconstruction phase of multi-secret sharing schemes and fixes up the problem by a simple secure multiparty computation protocol.

Chapter 3 contains the applications of secret sharing schemes in threshold signature schemes, electronic auction, electronic voting, commitment schemes and linear codes. Besides, it introduces the recent work about black-box secret sharing schemes.

Chapter 4 mainly studies the information rate of secret sharing schemes. It introduces how to compute the information rate by graph decomposition, and lists the information rate for all the access structures with five players.

Chapter 5 is about secure multiparty computation, especially the multiparty computation protocols based on linear secret sharing schemes. First, it introduces some concepts and known results of secure multiparty computation. Then it explains the security for multiparty computation and displays the proofs of the security for three multiparty computation protocols in detail. After that, four sections focus on the multiplicative linear secret sharing scheme which is an important tool for securely computing multiplications. In particular, it presents a specific construction for the multiplicative linear secret sharing scheme based on connectivity of graphs. Chapter 5 also provides a specific multiparty computation protocol with statistical security based on random walks on graphs. Moreover, it introduces parallel multi-party computation

and builds a general protocol for parallel multiparty computation by using linear multi-secret sharing schemes. At the end, it presents a solution for the classical problem in secure two-party computation, that is, Yao's Millionaires' problem.

M. Liu, Z. Zhang

# 前　言

随着因特网、计算机和通信技术的飞速发展，全球正步入信息化时代. 每天都有海量信息在因特网上传输，其中不乏大量涉及政治、经济、金融及人们生活中的敏感信息. 因此，如何在开放互联网的环境下保护信息的安全存储、传输等便成为非常紧迫和严峻的问题. 实际上，信息系统的整体安全强度主要取决于加密机制的加密强度（当然人员管理问题也非常重要，但这不属于技术讨论的范围），而加密机制的核心是密码算法. 密码算法（包括对称算法和非对称算法）是指用于加密和解密的两个函数或变换，它们分别被加密密钥和解密密钥控制. 密码体制，也称为密码系统，是由算法和所有可能的明文、密文、密钥等组成的. 如果一个密码体制的安全性基于算法的保密，则它的安全性就很成问题. 因为大量的、经常变换的用户群是无法使用它的. 例如，一个用户离去，其他用户就得改变算法. 实现一个算法的成本是很高的. 现代密码学采用密钥解决这个问题. 实际上，密钥就是算法的参数，因而密钥改变的成本相对算法改变的成本是很小的. 由此导致现代密码体制的设计思想是算法公开，使体制的安全性取决于密钥，即在算法公开后，在很大的密钥空间中随机选取一个密钥来控制算法. 密钥的泄露意味着体制丧失安全性，而由于意外事故（人为的或非人为的）导致的密钥遗失还可能致使合法者也无法从密文恢复明文. 进而，在密码体制中频繁地更换密钥是保证安全的一种方法，但这种方法在大信息量的今天是不现实的，于是产生了如何选取、交换、安全地存储和发放密钥等问题，即密钥管理问题.

在实际中，人们特别关心的往往是对一类极为关键的密钥如何存储才能保证安全. 密码学家常常会举下面的例子：如何保存和控制导弹发射程序的密钥？我们称这个密钥为主密钥. 为安全起见，当然不能将此主密钥交给多人保管，但直接由一个人掌握也是不安全的，因为可能存在密钥的遗失乃至个人的不忠诚行为. 针对这类问题，著名密码学家 A. Shamir [120] 和 G. Blakley [18] 于 1979 年分别独立地提出了密钥共享（share a secret 或 secret sharing，也称为秘密共享或秘密分享）的概念. （根据 Shamir 和 Blakley 最初建立共享概念的背景，我们将 secret sharing 译为“密钥共享”并一直沿用至今. 有的人使用 secret sharing 的直译“秘密分享”，也有人使用“秘密共享”. 本书采用的是“密钥共享”这种译法.）Shamir 和 Blakley 分别设计了实现的算法. Shamir 的算法是基于有限域上的多项式插值，也可以说是基于求解有限域上的线性方程组. Blakley 的算法是基于有限几何. 他们的想法和工作为密钥管理提供了一个崭新的思路. 由于在信息安全中的广泛应用，密钥共享体制一经提出便得到了快速的发展.

Shamir 等提出的密钥共享体制是针对一种特殊的、称为门限结构的密钥共享. 实际上，一组人如何共享一个主密钥，或者说如何控制一个主密钥，需要根据实际情况决定，即根据具体情况的要求，某些人的信息放在一起就可恢复主密钥，这些人构成授权集；同时某些人的信息即使放在一起也不能恢复出主密钥，这些人构成非授权集. 于是就产生了存取结构（access structure）的概念. M. Ito 等人[77] 在 1987 年给出了一个实现一般存取结构的密钥共享算法. 这个算法在本质上是 Shamir 的子密钥分配想法的推广，但每人掌握的子密钥信息量很大，致使数据扩散很大，因而该方法并不实用. 当然，讨论的问题越一般，算法就越复杂，应用起来就越不方便. 至于使用 Blakley 几何方法构建共享体制方面，在 G. J. Simmons 的《当代密码学》一书 [123] 中给出了多个例子. 这种方法比较直观，但不易用于处理复杂的情形. 通过对 Shamir 和 Blakley 体制及其变形的研究可以发现，它们有一个共同的特点，就是它们的算法基本上是通过对子密钥信息的线性计算来恢复主密钥信息的. 1989 年 E. F. Brickell [30] 提出了密钥共享体制的线性空间结构. 1992 年，D. R. Stinson [127] 推广了 Brickell 的方法. 直到 1996 年 A. Beimel [8] 在他的博士论文中明确地提出线性密钥共享体制的一般模型，同时他建立了线性密钥共享体制与用于计算布尔函数的单调张成方案之间的对应关系. 2004年，肖亮亮与刘木兰 [138] 给出了利用单调张成方案构造实现几类存取结构的模型和算法. Shamir 和 Blakely 的算法及其已知的多数推广算法都可看做线性模型的特例. Ito 等人的算法从利用单调张成方案构造的线性模型来看一目了然. 事实上，线性密钥共享体制的一般模型可帮助我们设计许多具体应用需要的密钥共享模型，因此它具有广泛的应用. 但是，线性实现不等于最优实现，这就要求研究线性最优实现及有效实现的问题.

针对同一组人（或共享控制集合）要共同控制或共享多个密钥或秘密，而且不同的主密钥对应不同的密钥控制要求的问题，产生了多密钥共享控制的概念. 例如，在一个导弹发射的指挥机构里，发射指令需要进行共享控制，但由于有多种型号的导弹，故有多个不同的发射指令. 由于导弹型号或功能不同，每个发射指令需要进行的共享控制方式也不同，不同权限的人在共享控制中起的作用也不同. 这就需要研究和设计多密钥共享体制. W. Jackson 等人 [79] 于 1994 年研究了多密钥门限体制结构以及用拟阵讨论了理想多密钥共享体制 [78]. C. Blundo 等人 [23] 于 1998 年讨论了多密钥共享体制的随机性，肖亮亮和刘木兰 [139] 于2005年利用单调张成方案研究了线性多密钥共享体制的性质和模型. 至今，多密钥共享体制的已有结果不多. 因此，多密钥共享体制的结构和构造，特别是安全且高效的模型的建立，还需要进一步的研究.

从密钥共享体制效率的角度来看，希望数据扩散越小越好. 最理想的情况是子密钥信息没有数据扩散，即理想密钥共享体制. 但对某些存取结构，不存在理想密钥共享体制 [13]，于是迫使人们研究完美密钥共享体制. 所谓完美密钥共享，就是使非授权集将其掌握的子密钥信息放在一起，不只要求不能恢复主密钥，而且要求无法得到关于主密钥的任何信息. 显然，这是构造共享体制的合理要求. 由于不是理想的，因此需要研究完美密钥共享体制的数据扩

散情况. 为此，Brickell 和 Stinson [33] 引入了信息率的概念，用于度量数据扩散的程度. 进而，Blundo 等人 [25] 引入了最优信息率的概念. 具有最优信息率的体制是我们想要的. 但在实际上，最优信息率的计算非常困难，因为要在所有可能的实现方法中挑出最好的. 实际上，人们往往给出存取结构信息率的界，这方面可参见 R. M. Capocelli 等人 [35]、E. F. Brickell 等人 [33] 和 周展飞 [153] 的工作. Beimel 在 1996 年提出了有效密钥共享体制的概念 [8]，它刻画了怎样的数据扩散程度可以被接受. 例如，Shamir 的门限密钥共享体制就是线性有效的. 与信息率相比，有效密钥共享体制从应用的角度看更为实际. 因此，在 20 世纪 90 年代后半期之后，就很少见到讨论存取结构信息率的文章了. 关于有效密钥共享体制的一个公开问题是：对于任何一个存取结构，是否存在有效密钥共享体制来实现它? 事实上，确实有存取结构不存在线性有效密钥共享体制实现它 [11]. 这使人们必须研究非线性密钥共享体制. 目前，关于非线性密钥共享体制的结果很少. 对于根据具体需要给出的存取结构，我们猜想，大部分存在线性有效的密钥共享体制实现它们. 因此针对一些存取结构构造出实现它们的线性有效密钥共享体制是很有意义的工作.

Shamir 和 Blakley 提出密钥共享后不久，R. J. McEliece 和 D. Sarwate [102] 于 1981 年就提出了密钥共享的防欺骗问题. 因为在共享控制中，有一些成员可能出示虚假的密钥以欺骗其他成员. 针对防欺骗问题，B. Chor 等人 [40] 于 1985 年提出了可验证密钥共享（verifiable secret sharing）的概念. 可验证密钥共享通过验证解决防欺骗问题，具有良好的安全性质，它在安全多方计算中具有重要应用.

在 Beimel 2001 年的文章 [10] 中提到统计密钥共享体制. 计算密钥共享体制是 1994 年 H. Krawczyk 在其文章 [89] 中提出的. 这两类体制至今研究成果还不是很多. 由于信息安全发展的需要，它们将越来越受到人们的重视.

密钥共享的应用十分丰富，数字签名 [92]、电子拍卖 [66]、电子选举 [12] 等是它的几个典型的应用领域.

安全多方计算最早由 A. Yao [142] 在 1982 年提出. 当时，他通过“姚氏百万富翁问题”提出安全两方计算问题. 在 1987 年，O. Goldreich 等人 [70] 考虑了安全多方计算问题. 至今，安全多方计算的研究已取得了丰硕的成果，可参见参考文献 [6, 39, 113, 112, 46]. 事实上，安全多方计算问题是从众多具体的密码学问题中抽象出来的，对它的研究以及由此得到的一些结论对于具体的密码学问题都有着指导意义，它能在原则上告诉我们哪些问题是可以解决的，哪些问题是不可能解决的. 可以说，安全多方计算蕴涵了对任何密码协议问题在原则上的实现方案，它是分布式密码学和分布式计算研究的一个基本问题. 在本书中，除介绍安全多方计算的基本概念和已有的主要结果外，特别给出了几个具体的安全多方计算协议安全性的严格而详细的证明，以使读者理解安全多方计算中安全性的确切含义. 由于乘性单调张成方案是实现安全多方计算协议的重要工具，因此在本书中对乘性单调张成方案给出了比较全面的讲述. 考虑到密钥共享、随机算法和安全多方计算这3个领域的内在联系，刘木兰等人 [148] 从

密钥共享体制出发，采用随机算法恢复主密钥，进而将其用于安全多方计算，得到一个具有统计安全性的安全多方计算协议的例子. 该例子有助于人们对统计安全多方计算理论的研究. 此外，安全多方计算理论的研究刺激了乘性密钥共享体制的研究 [106, 96].

密钥共享和安全多方计算在信息安全理论与应用中占有越来越重要的地位. 本书的写作目的，是使读者学习密钥共享和安全多方计算的基本知识以及近期新的理论及技术，希望有助于读者尽快地进入这一领域的前沿，同时有助于信息安全领域的工程技术人员开发新的应用领域和促进技术创新.

本书的内容是这样安排的：第 1 章介绍密钥共享的基本概念和模型，给出了完美密钥共享体制、统计密钥共享体制和计算密钥共享体制的统一形式的定义. 特别是讲述了图存取结构，介绍了动态密钥共享体制和可验证密钥共享体制. 第 2 章讲线性密钥共享体制，系统地讲述了线性密钥共享体制和线性多密钥共享体制，并指出线性多密钥共享体制特有的在重构阶段的信息泄露问题及解决方案. 这章最后一节（即2.9节）指出了研究非线性密钥共享体制的原因并给出了非线性密钥共享体制的例子. 第 2 章是本书的重点. 第 3 章介绍密钥共享的应用. 我们希望通过几种典型的应用理解前面讲的概念和使读者学会使用这些模型. 当然这些应用本身也是很有意义的. 第 4 章讲密钥共享体制的信息率. 主要讲述秩为 2 的存取结构的信息率及 $\lambda$-分解方法，列出了 5 个参与者的所有可能的存取结构的信息率，同时介绍了有效密钥共享体制和计算有效密钥共享体制. 第 5 章讲安全多方计算. 在介绍了安全多方计算的基本概念和已有结果的基础上，花了较大篇幅讲安全多方计算的一般实现办法，包括基于不经意传输协议的安全多方计算、基于同态密码算法的安全多方计算和基于线性密钥共享体制的安全多方计算，同时给出每个协议的安全性证明. 由于乘性单调张成方案是安全地计算乘法的重要工具，我们用了4节的篇幅讲述有关内容. 此外，我们详细地讲述了并行安全多方计算协议. 最后一节，针对安全多方计算的经典问题“姚氏百万富翁问题”介绍了一个解决方案. 我们建议，只对密钥共享体制感兴趣的读者可只阅读前 4 章；对密钥共享理论感兴趣的读者可只阅读前 3 章；对安全多方计算感兴趣的读者，可阅读第 1、2 和 5 章. 当然，读者可以根据自己的需要做出各种选择.

本书第 1 章 1.1 节至 1.7 节，第 2 章 2.1 节至 2.4 节，2.6 节至 2.8 节，第 4 章，第 5 章 5.1 节至 5.3 节，5.5 节至 5.9 节主要由第一作者执笔；第 1 章的 1.8 节和 1.9 节，第 2 章的 2.5 节和 2.9 节，第 3 章，第 5 章的 5.4 节、5.10 节和 5.11 节主要由第二作者执笔. 由于作者水平有限，文中定有谬误之处，敬请读者批评和指正. 进而，由于信息安全理论与技术发展速度极快，文献海量，因此有关的新理论与成果可能在本书中没能及时反映，敬请读者原谅.

本书的写作得到蔡吉人、沈昌祥和周仲义3位院士和吕述望研究员的支持和帮助，作者在此表示衷心感谢. 作者感谢周展飞博士和肖亮亮博士为本书的写作提供的他们的相关研究结果以及给予的帮助. 作者受益于由刘木兰研究员主持的、在中国科学院数学与系统科学研究院信息安全中心自 2000 年到 2006 年举办的系列讨论班，包括应用密码学基础讨论班、椭圆

曲线与超椭圆曲线密码体制讨论班、随机算法讨论班、密钥共享体制讨论班、安全多方计算讨论班、可证安全性讨论班、零知识讨论班等. 在此，作者感谢积极参加讨论班的章照止研究员、冯荣权教授、李俊全博士、邓映蒲博士、高莹博士、肖亮亮博士、唐春明博士、曹正军博士、郭丽峰博士和邓燚、涂自然、潘彦斌、张艳娟、张艳硕等各位同学. 作者还要感谢邵祖英同志和电子工业出版社的秦梅同志对本书的出版付出的辛勤劳动. 本书的完成得到了国家科学技术学术著作出版基金、国家重点基础研究发展计划（973）项目（项目编号 2004CB318004），国家自然科学基金项目（项目编号90304012）和中国科学院数学机械化重点实验室的资助，在此一并表示感谢.

# 目　录

# 第 1 章　密钥共享体制的基本概念和模型

密钥共享的概念和密钥共享体制是针对密钥管理中密钥的泄露问题和遗失问题提出的. 自从 Blakley[18] 和 Shamir[120] 于 1979 年分别独立地提出了密钥共享的概念以来，人们在密钥共享理论和密钥共享技术与应用方面取得了丰硕的成果. 而且，密钥共享理论与技术在密码学和信息安全理论与技术中已占有重要的地位. 本章从最简单的门限密钥共享体制入手，介绍密钥共享的基本概念和模型，并且对完美、统计和计算密钥共享体制用随机变量的分布和可忽略函数给出统一形式的定义，进而对理想存取结构及其相关的拟阵、信息率和图存取结构给出较为详细的介绍. 在后面几节，将介绍同态密钥共享体制、动态密钥共享体制和可验证密钥共享体制.

## 1.1　门限密钥共享体制

1979年，Blakley 用有限几何方法设计了门限密钥共享体制，Shamir 用多项式插值的算法设计了门限密钥共享体制. 由于门限密钥共享体制简单、有效和易于实现，因此得到了广泛的应用. 要学习和研究一般密钥共享体制，最好的方法是从了解门限密钥共享体制开始. 因此，本节将详细地讲述门限密钥共享体制，并给出用线性代数方法和几何方法构造密钥共享体制的例子.

设 $t,n$ 为两个正整数，且 $t \leqslant n$. $P=\{P_1,\cdots,P_n\}$ 是 $n$ 个共享密钥的参与者的集合，也称为受托人集合. 一个 $(t,n)$ 门限密钥共享体制是指：如果 $n$ 个参与者要共享密钥 $s$，通常称 $s$ 为主密钥，则需要有一个密钥管理中心，用 $P_0$ 表示，以及满足重构要求和安全性要求的两个算法，通常称为分配算法和重构算法（或恢复算法）. 密钥管理中心 $P_0$ 利用分配算法和主密钥 $s$ 生成 $n$ 个值 $s_1,\cdots,s_n$，称为子密钥. 然后，$P_0$ 将子密钥 $s_i$ $(1 \leqslant i \leqslant n)$ 秘密地发送给参与者 $P_i$，$P_i$ 不得向外泄露 $s_i$. 这里，重构要求是指：集合 $P$ 中的任何 $t$ 个或多于 $t$ 个的参与者的子密钥放在一起，通过重构算法可以恢复出主密钥 $s$. 由此推出，即使 $n-t$ 个参与者遗失了子密钥，剩下的 $t$ 个参与者仍然可以恢复出主密钥. 安全性要求是指在已知少于 $t$ 个子密钥的信息时，不能恢复出主密钥 $s$，即少于 $t$ 个参与者即使合谋也得不到主密钥. 需要指出，上面提到的子密钥分配算法和主密钥重构算法都是公开的，而且主密钥重构算法是由分配算法所决定的，或者说，当设计分配算法时，就蕴含着同时给出相应的重构算法. 密钥管理中心是可信的第三方，它不会泄露主密钥信息和欺骗参与者.

Shamir 的 $(t,n)$ 门限密钥共享体制[120] 是最简单、最有效、也是最实用的一类密钥共享

体制. 它的分配算法和重构算法如下：

*分配算法*：设 $\mathbb{F}_q$ 为 $q$ 元有限域，$q$ 是素数并且 $q>n$. 为了使集合 $P=\{P_1,\cdots,P_n\}$ 中的 $n$ 个参与者共享主密钥 $s$，$s\in\mathbb{F}_q$，密钥管理中心 $P_0$ 按下面的步骤进行工作：

**步骤1** $P_0$ 秘密地在 $\mathbb{F}_q$ 中一致地随机选取 $t-1$ 个元素，记为 $a_1,\cdots,a_{t-1}$；并取以 $x$ 为变元的多项式 $f(x)=s+\sum\limits_{i=1}^{t-1}a_ix^i$.

**步骤2** 对于 $1\leqslant i\leqslant n$，$P_0$ 计算 $f(i)$，记为 $y_i=f(i)$.

**步骤3** 对于 $1\leqslant i\leqslant n$，$P_0$ 秘密地将 $(i,y_i)$ 分配给 $P_i$，这可通过一个秘密安全信道传输完成，$P_i$ 不得向任何人泄露 $y_i$. 至此，$P_0$ 的任务即告完成.

*重构算法*：不失一般性，设 $P_1,\cdots,P_l$ 是 $P$ 中任意选定的 $l$ $(l\geqslant t)$ 个参与者，这 $l$ 个参与者掌握的全部子密钥集合为 $\{(1,y_1),\cdots,(l,y_l)\}$. 考虑下面的方程组：

$$\begin{pmatrix}1&1&\cdots&1\\1&2&\cdots&2^{t-1}\\\vdots&\vdots&\vdots&\vdots\\1&l&\cdots&l^{t-1}\end{pmatrix}\begin{pmatrix}s\\a_1\\\vdots\\a_{t-1}\end{pmatrix}=\begin{pmatrix}y_1\\y_2\\\vdots\\y_l\end{pmatrix}. \tag{1.1.1}$$

式 (1.1.1) 可以看做 $t$ 个变元的线性方程组，系数矩阵的秩是 $t$，这由 $1,2,\cdots,n$ 在 $\mathbb{F}_q$ 中两两不同和范德蒙矩阵的性质保证. 事实上，它的任何不同的 $t$ 行构成 $t\times t$ 的范德蒙矩阵，所以是秩为 $t$ 的可逆阵. 因此当 $l\geqslant t$ 时，$s,a_1,\cdots,a_{t-1}$是它的唯一解，于是得到主密钥 $s$.

对于 $l<t$，$l$ 个参与者要恢复主密钥 $s$ 时，情况又如何呢? 首先，他们可得到含有 $t$ 个变元的 $l$ $(l<t)$ 个方程的线性方程组. 若 $l=t-1$，则我们得到含有 $t$ 个变元的 $t-1$ 个方程. 假设这 $t-1$ 个参与者用他们掌握的 $t-1$ 个子密钥猜得主密钥为 $s_0$（不管用什么方法猜）. 由于将 $s_0=f(0)$ 和关于子密钥的 $t-1$ 个方程放在一起可得到唯一解，因此对主密钥的任何假设值 $s_0$ 都存在唯一的多项式 $f_{s_0}(x)$，使得 $y_j=f_{s_0}(j)$，$1\leqslant j\leqslant l$，和 $s_0=f_{s_0}(0)$. 于是，没有一个主密钥的可能值被排除，换句话说，$t-1$ 个参与者合谋得不到主密钥的任何信息. 一般来说，对于 $l<t$，对任意给定的 $s$，关于 $(a_1,\cdots,a_{t-1})$ 的方程组 [即式(1.1.1)] 都有相同个数的解，由此推出：从 $\{((1,y_1),\cdots,(l,y_l))\}$ 得不到主密钥 $s$ 的任何信息，或者说，要得到 $s$，其工作量与穷搜索相同.

因此，分配算法和重构算法满足了重构及安全性要求，即任何 $t$ 个或多于 $t$ 个的参与者联合起来可以恢复出主密钥，而任何少于 $t$ 个的参与者即使合谋也不能恢复出主密钥，进而得不到主密钥的任何信息.

若在上面的算法中，选取 $\mathbb{F}_q$ 中 $n$ 个互不相同的非零值 $x_1,\cdots,x_n$，$P_0$ 秘密地将 $(x_i,y_i=f(x_i))$ 分配给 $P_i$，$1\leqslant i\leqslant n$. 对于任意 $l$ 个参与者 $P_{i_1},\cdots,P_{i_l}$，与式 (1.1.1) 对应的方程组为

$$\begin{pmatrix} 1 & x_{i_1} & x_{i_1}^2 & \cdots & x_{i_1}^{t-1} \\ 1 & x_{i_2} & x_{i_2}^2 & \cdots & x_{i_2}^{t-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{i_l} & x_{i_l}^2 & \cdots & x_{i_l}^{t-1} \end{pmatrix} \begin{pmatrix} s \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} y_{i_1} \\ y_{i_2} \\ \vdots \\ y_{i_l} \end{pmatrix}, \tag{1.1.2}$$

其中，$y_{i_j} = f(x_{i_j}), 1 \leqslant j \leqslant l$. 整个讨论与刚才所述完全相同.

我们也可以不用解线性方程组的方法，而直接用多项式插值的方法来重构主密钥. 对于任意 $t$ 个子密钥，不失一般性，记为 $(x_i, y_i)$，其中 $y_i = f(x_i)$, $i = 1, 2, \cdots, t$. 参与者 $P_1, \cdots, P_t$ 共同计算

$$\begin{aligned} h(x) = {} & y_1 \frac{(x-x_2)(x-x_3)\cdots(x-x_t)}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_t)} + y_2 \frac{(x-x_1)(x-x_3)\cdots(x-x_t)}{(x_2-x_1)(x_2-x_3)\cdots(x_2-x_t)} + \cdots \\ & + y_t \frac{(x-x_1)(x-x_2)\cdots(x-x_{t-1})}{(x_t-x_1)(x_t-x_2)\cdots(x_t-x_{t-1})}. \end{aligned} \tag{1.1.3}$$

显然，$h(x)$ 是一个 $t-1$ 次多项式. 注意，每个加项的分母均不为 0，这也是我们要求 $x_1, \cdots, x_n$ 互不相同的原因. 容易验证，对于 $i = 1, \cdots, t$, $y_i = h(x_i)$. 根据域上多项式的性质：两个 $t-1$ 次多项式，如果在 $t$ 个不同点的取值都相同，那么这两个多项式恒等，推出 $h(x) = f(x)$，进而有$h(0) = f(0) = s$，于是得到主密钥 $s$. 如果 $t$ 个以上的参与者共同重构主密钥，则只需要其中任意 $t$ 个参与者的子密钥就够了.

**例1.1.1** 考虑 (3,5) 门限密钥共享体制，即 $n = 5, t = 3$. 设参与者集合为 $P = \{P_1, P_2, P_3, P_4, P_5\}$，令主密钥在有限域 $\mathbb{F}_7$ 中取值，参与者希望共享的主密钥为 $s = 1$. 按照 Shamir 的方案，因为门限为 3，故密钥管理中心 $P_0$ 在 $\mathbb{F}_7$ 中随机取两个数，设 $a_2 = 1, a_1 = 2$，将其分别作为二次多项式 $f(x)$ 的二次项系数 $a_2$ 和一次项系数 $a_1$，并令常数项 $a_0 = s = 1$，于是得到二次多项式 $f(x) = x^2 + 2x + 1$. 对于 $x_1 = 1, x_2 = 2, x_3 = 3, x_4 = 4, x_5 = 5$，计算：

$$\begin{aligned} y_1 &= f(x_1) = f(1) \equiv 4 \pmod 7, \\ y_2 &= f(x_2) = f(2) = 9 \equiv 2 \pmod 7, \\ y_3 &= f(x_3) = f(3) = 16 \equiv 2 \pmod 7, \\ y_4 &= f(x_4) = f(4) = 25 \equiv 4 \pmod 7, \\ y_5 &= f(x_5) = f(5) = 36 \equiv 1 \pmod 7. \end{aligned}$$

上面的运算是在 $\mathbb{F}_7$ 中进行的，即用模 7 运算实现 $\mathbb{F}_7$ 中的计算. 然后 $P_0$ 将 $(x_i, y_i)$ 秘密发送给 $P_i$, $1 \leqslant i \leqslant 5$.

我们说 $P$ 中的任意 3 人联合可恢复出主密钥. 不妨设 $A = \{P_1, P_2, P_3\}$，于是 $A$ 中参与