华中师范大学出版基金丛书
学术著作系列

秘密共享方案的构造及其应用研究

许静芳 著

CBJJ

华中师范大学出版社

华中师范大学出版基金丛书
学 术 著 作 系 列

本书由华中师范大学出版社提供的出版基金全额资助

秘密共享方案的构造及其应用研究

许静芳 著

華中師範大學出版社

新出图证(鄂)字 10 号
图书在版编目(CIP)数据

秘密共享方案的构造及其应用研究/许静芳著. —武汉:华中师范大学出版社,2016.8

ISBN 978-7-5622-7427-8

Ⅰ.①秘… Ⅱ.①许… Ⅲ.①信息获取—研究 Ⅳ.①G252.7

中国版本图书馆 CIP 数据核字(2016)第 149940 号

秘密共享方案的构造及其应用研究

责任编辑:罗 挺
责任校对:缪 玲
编 辑 室:学术出版中心
出版发行:华中师范大学出版社有限责任公司
社址:湖北省武汉市珞喻路 152 号
传真:027—67863291
网址:http://press.ccnu.edu.cn
印刷:虎彩印艺股份有限公司
字数:128 千字
开本:787mm×960mm 1/16
版次:2017 年 10 月第 1 版
定价:26.00 元

封面设计:罗明波
封面制作:胡 灿
电 话:027—67863220
电 话:027—67863040(发行部)
027—67861321(邮购)
电子邮箱:press@mail.ccnu.edu.cn
督印:王兴平
印张:9.5
印次:2017 年 10 月第 1 次印刷

欢迎上网查询、购书

目　录

第1章 绪 论

1.1 研究的背景、目的和意义

随着信息技术的快速发展，移动通信技术已从最初的1G(模拟技术，主要业务为语音通信)发展到2G(数字技术，业务包括语音通信与数据业务)，并过渡到3G、4G，移动商务服务得到了快速普及。移动商务相比传统商务和电子商务的最大优势是无处不在，即消费者可借助无线通信网络，通过各种移动终端，包括手机、PDA、笔记本电脑等实现在任何时间、任何地点访问互联网，获取所需的信息和服务。同时，移动服务提供商迫切需要了解影响用户接受和使用移动服务的因素，以便采取有效措施来促进移动服务在消费者中的普及，确保移动商务实施成功。其中，如何保障移动商务环境下的安全性是迫切需要解决的问题。

随着信息安全技术发展和应用的日益推广，秘密共享方案(secret sharing schemes)越来越多地应用于各种安全协议及风险管理中。例如研究在移动商务环境下的安全风险管理，通过分析影响移动商务交易安全的风险因素，建立科学、合理的评价指标体系，选择合适的方法对风险进行评估，综合技术性与管理性措施，构建移动商务交易风险防范体系。采取多学科的理

论和方法，对移动商务交易的风险评估方法和模型进行深入研究，解决不确定性风险知识的表达、推理和管理问题。秘密共享方案属安全领域的前沿内容，特别适合运用于移动商务环境中的风险管理研究。

秘密共享是指多个参与者之间共享一个主秘密，即分发给每个参与者一份子秘密，使得只有授权集中的参与者才能联合从他们的子秘密中恢复主秘密，同时非授权集中的参与者联合他们的子秘密则不能获得关于主秘密的任何信息。所有授权集的集合称为存取结构，它具有单调递增的特性。

秘密共享的概念由 Shamir[101] 和 Blakley[102] 于 1979 年首次提出，他们分别提出了两种不同的方法来构造实现 (t,n) 门限存取结构（threshold access structures）的秘密共享方案，即 n 个成员中至少任意 t 个成员联合他们的子秘密可以恢复主秘密。他们的方案是理想的，即每个子秘密的长度都等于主秘密的长度，此时效率是最优的[130,151]。

然而在现实应用中很多情况下需要实现非门限存取结构（即通用的存取结构）的秘密共享方案[146,157,158]。例如，参与者集合中某些成员比其他成员具有更高的等级。在这种情况下，为了克服门限存取结构的局限性，Shamir 在门限秘密共享方案的基础上做了简单的改进[1]，即根据其等级，为每个成员分配一定数目的子秘密（而不是一个子秘密），使得只有子秘密数目之和达到某一数值时，持有这些子秘密的成员联合方可恢复主秘密。显然，该方案是非理想的，因为为每个成员分配的子秘密的总长度大于等于主秘密的长度。关于秘密共享方案的相关综述可参照 Stison 和 Simmons 的研究文献[141,169]。

对于任意一个存取结构来说，都存在一个实现该结构的秘密共享方案[7,8]，但是子秘密的长度总是大于等于主秘密的长度[10,11]。子秘密的长度是决定秘密共享方案效率的主要因素，当子秘密的长度等于主秘密的长度时方案的效率是最优的，称为理想的秘密共享方案（ideal secret sharing schemes），对应的存取结构称为理想的存取结构（ideal access structures）。并不是所有的存取结构都存在实现该结构的理想的秘密共享方案，即为非理

想的存取结构，因此理想的存取结构的特征描述成为秘密共享领域中一个急待解决的困难问题，拟阵论与这一问题有着非常密切的联系，大量的研究工作围绕着这一主题而展开，即运用拟阵论的知识寻找理想的存取结构的特征进而为其构造理想的秘密共享方案。

如何描述理想的存取结构具有的特性，这是一个秘密共享领域中极其重要且长期存在的问题。拟阵论(matroid theory)与这一问题有着非常密切的联系[12,13]，即每一个理想的存取结构都可确定一个拟阵，同时与可表示的拟阵相关联的所有存取结构均为理想的。由此可见，拟阵的可表示性对于解决这一问题是尤其有价值的。本书通过证明可表示的和不可表示的多部拟阵(multipartite matroids)所满足的充分或者必要条件进而得到多部存取结构为理想的充分或者必要条件，为解决理想的存取结构具有的特性这一悬而未决的问题做出了新的贡献。

根据得到的理想的存取结构的特性，将其应用于具体的存取结构，从而为其构造理想的秘密共享方案。针对不同的应用环境，秘密共享方案实现的存取结构一般都有一定的实际背景，例如门限存取结构[14,15,16,17]、多部存取结构[18,19,20,21]、基于图的存取结构[22,23,24,25]等。为这些特殊类别的存取结构构造理想的秘密共享方案是非常有实际应用价值的。因此，本书的另一个研究重点是通过运用得到的理想的存取结构的特性，针对门限存取结构和基于图的连通性(connectivity of graphs)的存取结构，分别构造了一个理想的秘密共享新个体加入(new member joining)协议和一个理想的基于图的连通性的多密钥共享体制。

除了利用 Shamir 的插值多项式来构造秘密共享方案外，利用其他的数学工具同样可以实现秘密共享。例如，基于中国剩余定理的秘密共享方案[3]以及基于图的秘密共享方案。对于基于中国剩余定理的秘密共享方案而言，已有的方案大多是针对门限存取结构来构造的。同样地，基于图的秘密共享方案仅仅局限于实现秩为 2 的存取结构。因此，如何将基于中国剩余定理的秘密共享方案以及基于图的秘密共享方案所实现的存取结构推广到一般的

情况是非常有价值的。本书的一个重点就是基于中国剩余定理构造实现通用存取结构的秘密共享方案，以及构造基于图的实现通用存取结构的秘密共享方案。

在实际应用过程中，针对不同的应用环境，秘密共享方案所实现的存取结构一般都有一定的实际背景，例如，多秘密共享中每一个参与者集合的子集需要恢复与之相对应的主秘密，基于秘密共享来实现群组密钥高效且安全的传送等。为这些特殊类别的存取结构构造理想的秘密共享方案是非常有实际应用价值的。因此，本书的另一个研究重点是通过运用线性秘密共享方案的效率优势，针对多秘密共享以及群组密钥传送需实现的具体的存取结构，分别构造了一个理想的多秘密共享方案和一个基于线性秘密共享的高效的群组密钥传送协议。

综上所述，本书的研究目的是针对每个拟阵和存取结构都是多部的这一特点以及多部拟阵与离散多拟阵(discrete polymatroids)之间的密切联系，从离散多拟阵的基集合以及秩函数等多个角度出发，分别研究和证明了可表示的以及不可表示的多部拟阵所满足的多个充分或者必要条件，进而得到多部存取结构为理想的多个充分或者必要条件[26,27,28,29,30,31]。随后，通过将这些结论应用于两类具体的存取结构，针对门限存取结构和基于图的连通性的存取结构，分别构造了一个理想的秘密共享新个体加入协议[32]和一个理想的基于图的连通性的多密钥共享体制[33]，并且证明了方案的安全性和正确性。同时，本书针对已有的秘密共享方案使用的数学工具以及所实现的存取结构的局限性，从已有的基于中国剩余定理以及基于图的秘密共享方案出发，分别构造了实现通用存取结构的基于中国剩余定理以及基于标记图的秘密共享方案。随后，通过运用线性秘密共享方案的效率优势，针对实际应用中两类具体的存取结构，即多秘密共享以及群组密钥传送中实现的存取结构，分别构造了一个理想的线性多秘密共享方案和一个基于线性秘密共享的高效的群组密钥传送协议，同时证明了方案的安全性和正确性。

1.2 国内外研究概况

秘密共享概念的产生源于实际应用需求，即需要在多个参与者之间安全高效地共享一个主秘密。在秘密共享方案中，只有授权集中的参与者才能联合从他们的子秘密中恢复主秘密，所有这些授权集的集合称为存取结构。如何为各种类别的存取结构构造高效的秘密共享方案成为秘密共享领域的核心研究问题。自 Shamir 和 Blakley 于 1979 年分别在他们的经典论文[101,102]中首次提出秘密共享的概念及(t,n)门限秘密共享方案开始，秘密共享方案受到了大量学者的关注，一直成为密码学领域研究的热点。

1.2.1 理想的存取结构的特征描述

在秘密共享方案中，只有授权集中的参与者才能联合从他们的子秘密中恢复主秘密，所有这些授权集的集合称为存取结构。子秘密的长度是决定秘密共享方案效率的主要因素，当子秘密的长度等于主秘密的长度时方案的效率是最优的，称为理想的秘密共享方案，对应的存取结构称为理想的存取结构。

显然，(t,n)门限存取结构只是通用存取结构中的一种特殊情况，大多数存取结构都是非门限的。Shamir 和 Blakley 利用拉格朗日插值多项式构造了一个经典的秘密共享方案，即理想的门限秘密共享方案。由此可见，门限存取结构属于理想的存取结构。然而，并不是对于所有的存取结构来说都存在实现该结构的理想的秘密共享方案，即存在非理想的存取结构，例如，与 Vamos 拟阵相关联的所有的存取结构都是非理想的[38]。于是，哪些存取结构为理想的，哪些为非理想的，如何完全描述理想的存取结构具有的特性这一问题成为秘密共享领域中极其重要且一直未能解决的问题。

在此问题上，Brickell 和 Davenport 做出了非常有价值的工作，他们于 1991 年首次发现了理想的秘密共享与拟阵论之间的密切关系，证明了每个理想的存取结构都是与一个拟阵相关联的，即每个理想的存取结构可明确确

定一个拟阵，这是一个存取结构为理想的必要条件[12]。此后，大量的学者开始关注由拟阵所导出的存取结构的特性以及拟阵的相关特性。沿着这一研究方向，Brickell 又得到了一个构造理想的秘密共享方案的有效方法：存取结构为理想的一个充分条件[13]，即与可表示的拟阵相关联的所有存取结构均为理想的。由此可见，研究拟阵的可表示性问题对于理想的存取结构的特征描述无疑是非常有价值的。

随后，Seymour[38]证明得出 Brickell 和 Davenport 的研究[12]中存取结构为理想的必要条件是非充分的，他给出了第一个反例，即由 Vamos 拟阵所导出的一个存取结构是非理想的存取结构，Matus[39]给出了其他的一些反例。接着，Simonis 和 Ashikhmin[40]指出 Brickell 的研究文献[13]中存取结构为理想的充分条件是非必要的，他给出了一个反例：non-Pappus 拟阵是不可表示的，而由它所导出的一个存取结构是理想的存取结构。Marti-Farre 和 Padro[41]将 Brickell 和 Davenport[12]的结论一般化为：如果一个秘密共享方案中所有子秘密的长度均小于 3/2 倍的主秘密的长度，则该方案所实现的存取结构必与一个拟阵相关联。

基于寻找一般性结论的困难性，许多学者通过研究特殊类别的存取结构的特性来获得理想的存取结构的特征描述的部分结论。Stinson[42]和 Jackson 等[43]分别研究了参与者集合中包含四个以及五个成员的存取结构，Brickell 等[12,22,34,44,45]研究了用图来定义的存取结构，Padro 和 Saez 研究了二部的存取结构[18]，研究了包含三个或四个最小授权集的存取结构[46]，研究了任意两个最小授权集的交集至多为 1 的存取结构[47]，Marti-Farre 和 Padro 详细讨论了秩为 3 的存取结构[48,49]，并专门研究了权重的门限存取结构[50]。以上这些被具体论述过的特殊类别的存取结构，与之相关联的拟阵均为可表示的拟阵，于是可得到，这些存取结构均为理想的存取结构。由此可见，拟阵的可表示性问题的探究对于获取理想的存取结构的特征描述的确是十分有意义的。

在特殊类别的存取结构中，基于多部存取结构的实际应用价值以及每个

存取结构都可以看作多部的这一优良特性，大量学者通过研究多部的存取结构来获取理想的存取结构的一般特性。多部的存取结构，简单地说，是指将参与者集合划分为多个部分，使得同一部分中的参与者在存取结构中扮演等价的角色，即在存取结构中互换同一部分中的两个参与者，其结果是互换前后存取结构保持不变。实际上，每个存取结构都是多部的，因为可以认为每个参与者构成一个部分，即部分总数等于参与者总数。研究多部存取结构的特性有着广泛的实际应用前景，尤其是部分总数很小而参与者总数很大的情况。因此研究理想的多部存取结构的特性被认为是获取理想的存取结构具有的一般特性的重要途径之一。

多部存取结构的概念最先由 Shamir[4] 提到，其中称为权重的门限存取结构，在文中被首次考虑到。Beimel、Tassa 和 Weinreb[50] 给出了理想的权重门限存取结构的完全描述，这一完全描述将 Padro 和 Saez 等[18,51] 得出的部分结果推广到一般情况。最近，Beimel 和 Weinreb[52] 证明得到了关于实现权重门限存取结构的秘密共享方案中子秘密长度的一个新的重要结论，即为准多项式的。Brickell[13] 为不同种类的多部存取结构构造了理想的秘密共享方案，文中被称为多级的以及被间隔的存取结构，之前 Simmons[53] 同样讨论过此类的存取结构。Tassa 等[19,54,55] 为各种各样的多部存取结构构造理想的秘密共享方案提出了其他的一些构造方法，其中关于构造这些理想方案的复杂性问题同时被考虑到。理想的二部存取结构特性的完全描述分别由 Saez 等[18,56,57] 给出，即所有的二部存取结构均为理想的。Herraz 和 Collins[20,58] 给出了关于理想的三部存取结构特性的部分结论，这一问题在 *Ideal Multipartite Secret Sharing Schemes*[21] 中得到最终解决，文中给出了理想的三部存取结构特性的完全描述，即所有的三部存取结构均为理想的。*Ideal Multipartite Secret Sharing Schemes*[21] 的主要贡献在于，将多部拟阵与离散多拟阵之间的密切联系[59] 及相关概念[60,61] 应用于秘密共享领域，从而得到了一般性的结论。最近，沿用 *Ideal Multipartite Secret Sharing Schemes*[21] 的研究方法，由于多部存取结构包含层次存取结构，*Threshold multi-secret*

sharing scheme for cheat-proof among weighted participants[62]得到了理想的层次存取结构的完全描述，即每个层次存取结构都是理想的。

以上所有被研究过的多部存取结构，同样地，与之相关联的拟阵均为可表示的拟阵，于是这些存取结构均为理想的存取结构，即可按照 Brickell[13]的方法为这些存取结构构造理想的线性秘密共享方案。于是再一次说明，本书研究的拟阵的可表示性问题对于解决理想的存取结构的特征描述这一悬而未决的问题来说是极其有价值的。

1.2.2 理想的秘密共享方案的构造

通过运用得到的理想的存取结构的特征，针对不同的实际应用环境，为某一类别的存取结构构造出理想的秘密共享方案显然是非常有实际应用价值的，例如门限存取结构、多部存取结构、基于图的存取结构等。一直以来，这方面的研究工作成为众多学者关注的热点。

(1)门限秘密共享新个体加入协议。

门限秘密共享方案实现的存取结构实质上是最简单的多部存取结构，即一部的存取结构，根据得到的理想的存取结构的特性可知所有一部的存取结构均为理想的。自从 Shamir 和 Blakley 利用拉格朗日插值多项式构造了一个经典的秘密共享方案，即理想的门限秘密共享方案，门限存取结构成为大家所熟知且应用最广泛的一类存取结构[63,64,65]。在现实应用中，n 个秘密份额持有者所组成的集合往往会频繁更新。因此，从现实应用的角度来讲，需要有一种高效且安全的为新个体产生并分配秘密份额的方法，即理想的门限秘密共享新个体加入协议。

一直以来，门限秘密共享新个体加入协议的研究主要集中在怎样尽可能地减少协议的计算量和通信次数，以便于密钥管理和增加无线网络环境中通信的可靠性，并且不需要可信中心的协议更具吸引力，同时协议的运行能够满足以下安全性要求：①秘密 S 的任何信息不会被泄漏；②新个体的秘密份额 s_{n+1} 只有他本人知道；③所有旧成员的秘密份额 s_i 是安全的。

已有方案中，*Ubiquitous and robust authentication services for Ad Hoc*

wireless networks[66]提出的 shuffling 方案无需可信中心，仅需要 t 个旧成员的合作就能为任意的新个体安全地产生秘密份额。然而，shuffling 方案共需要 t^2-1 次秘密通信。Wong 等学者[67]提出了一个无需可信中心的非交互式的秘密共享新个体加入协议，该协议共需要 t^2 次秘密通信。最近又有许多学者提出了新的秘密共享新个体加入协议[68,69,70,71]。董攀等学者[68]基于 ElGamal 密码体制[72]针对 (t,n) 门限方案提出了一个秘密共享新个体加入协议(为方便起见，我们将他们的协议称为 Dong 协议)，他们的工作具有令人振奋的结果：无需可信中心，无需改动原有秘密份额，仅需任意 t 个旧成员合作产生新个体的秘密份额，通信次数由已有的 t^2 次秘密通信减少到 $6t$ 次广播通信。在他们的文章中给出了安全性分析，得出该协议满足前文所述的安全性。接着李慧贤等[69,70,71]先后构造了多个秘密共享新个体加入协议，这些协议中均无需可信中心，无需改动原有秘密份额，仅需任意 t 个旧成员合作产生新个体的秘密份额，不同的是协议所需的通信量，其中李慧贤等[69]提出的协议所需的通信次数最少，仅需 $(3t+2)$ 次广播。

(2)多部的秘密共享方案。

将理想的多部存取结构的特征运用于构造理想的多部秘密共享方案，这个方向的工作最初由 Simmons[53]提出了两类存取结构，即多级的和被间隔的存取结构，并猜想存在实现该存取结构的理想的秘密共享方案。基于线性代数的理论，Brickell[13]提出了一种通用的方法，为不仅仅是门限存取结构构造理想的秘密共享方案，同时将这一方法用于构造特定的理想的秘密共享方案，从而证明了 Simmons 的猜想。多级的和被间隔的存取结构实际上就是多部的存取结构，即将参与者集合划分为多个部分，使得同一部分中的参与者在存取结构中扮演等价的角色。利用不同种类的插值多项式，Tassa 等[54,55]为许多类别的多部存取结构构造了理想的秘密共享方案，其中有些存取结构具有分级的特性。虽然 Tassa 等[54,55]构造的方法都是基于 Brickell 提出的通用的线性代数方法，但是他们为多级的以及被间隔的存取结构提出的构造方案比 Brickell 提出的方案更加简单，效率更高。Xlg[19]为理想的多

部秘密共享方案提出了一些其他构造方法。需要指出的是，所有这些构造方案中主秘密的可能值组成的集合都必须满足集合大小为某一特定值。

(3) 基于图的秘密共享方案。

由于现实生活中的许多问题都可以用图来做模型，实现与图有关的存取结构的秘密共享方案也被广泛地研究。在秘密共享领域，用图表示的存取结构被 Brickell[12,37]、Blundo[22,44,45] 和 Stinson[42,73,74] 以及最近许多其他学者[75,23,24]所研究，图中每个顶点表示一个参与者，每条边表示一个授权集。利用 Shamir 的门限方案，Sun 和 Shieh[25,76,77]提出了一系列基于图的结构的秘密共享方案。最近 Guo[78]给出了一个基于图的攻击结构(即所有非授权集的集合)的秘密共享方案。在上述这些方案中，由于一条边只能连接 2 个顶点，图只能用来表示授权集(或非授权集)中参与者个数最多为 2 的结构。基于这一事实，Weng 等[79,80]研究了如何用超图(即一条边可以连接多个顶点)来克服这一瓶颈。虽然 Weng 方案[79]将 Sun 方案进行了推广，但超图的引入仍不能满足实现基于图的通用存取结构的要求。

另外一类基于图的秘密共享方案，即实现基于图的连通性的存取结构的秘密共享方案，它由于具有重要的实际应用价值而同样被许多学者研究。考虑如下情形：一个大公司有 m 个子公司，任意两个子公司之间有一个管理员负责这两个子公司之间的通信信道，当两个子公司 i 和 j 通信时需要使用对应的一个主密钥，希望设计一个密钥共享体制，使得某个管理员集合能够恢复该主密钥当且仅当他们负责的信道可以组成一条从子公司 i 到 j 的路，即可以实现 i 和 j 之间的通信。Beimel 等[36,81,82]都考虑过这样的存取结构并设计了相关的密钥共享体制，但他们的方案仅限于共享一个主密钥。实际上，m 个子公司需要共享总共 $m(m-1)/2$ 个主密钥。

1993 年，Blundo[83,84]等人针对同一参与者集合共享多个主密钥，而且不同的主密钥对应不同的存取结构，提出多密钥共享的概念。当然，如果简单地对每个主密钥都构造一个密钥共享体制来实现多密钥共享也未尝不可(我们称这种方法为直和)，但这种方法的明显缺点是参与者所需管理的子密钥

太多、数据量太大，效率会非常低下，显然不是理想的秘密共享方案[85,86,87,88]。在信息安全领域提出的任何一个模型与算法必须同时考虑到安全性与效率，因此，多密钥共享是一个新课题，是许多学者研究的热点[89,90,91,92,93]。因为没有适当的数学工具，构造理想的多密钥共享体制是很困难的，怎样运用已有的理想的存取结构的特征来构造理想的多秘密共享方案将是非常具有挑战性的课题。

1.2.3 基于中国剩余定理的秘密共享方案的研究现状

已有的著名的秘密共享方案包括基于插值多项式的 Shamir 方案[101]，基于平面几何的 Blakley 方案[102]，基于中国剩余定理的 Asmuth-Bloom 方案[3]。这些秘密共享方案都是实现门限存取结构的，称为门限秘密共享方案，即任意 t 个或者更多个子秘密联合能够恢复主秘密，同时任意$(t-1)$个或者更少个子秘密联合不能获得关于主秘密的任何信息。门限秘密共享方案已被广泛应用于各种安全协议中[118,119,120,121,122]。

显然，(t,n)门限存取结构只是通用存取结构中的一种特殊情况，大多数种类的存取结构都是非门限的。在各种类别的存取结构中，基于多部存取结构的实际应用价值以及每个存取结构都可以看作多部的这一优良特性，大量学者通过研究多部的存取结构来获取理想的存取结构的一般特性。多部的存取结构，简单地说，是指将参与者集合划分为多个部分，使得同一部分中的参与者在存取结构中扮演等价的角色，即在存取结构中互换同一部分中的两个参与者，其结果是互换前后存取结构保持不变。实际上，每一个存取结构都是多部的，因为可以认为每一个参与者构成一个部分，即部分总数等于参与者总数。研究多部存取结构的特性有着广泛的实际应用前景，尤其是部分总数很小而参与者总数很大的情况。因此研究理想的多部存取结构的特性被认为是获取理想的存取结构具有的一般特性的重要途径之一。

多部存取结构的概念最先由 Shamir[101]提到，其中称为权重的门限存取结构，这些存取结构也被 Padro 等[104,105]研究过。Beimel、Tassa 和 Weinreb[106]给出了理想的权重门限存取结构的完全描述。Brickell[107]为不

同种类的多部存取结构构造了理想的秘密共享方案，文中被称为多级的以及被间隔的存取结构，之前 Simmons[108] 同样讨论过此类的存取结构。Herranz 等的研究[109,110,111,112] 为各种各样的多部存取结构构造理想的秘密共享方案提出了其他的一些构造方法，其中关于构造这些理想方案的复杂性问题同时被考虑到。理想的二部存取结构特性的完全描述分别由 Padro 和 Saez 等[105,113,114] 给出，即所有的二部存取结构均为理想的。Beimel 等[106,115,119] 给出了关于理想的三部存取结构特性的部分结论，这一问题在 *Ideal Multipartite Secret Sharing Schemes*[116] 中得到最终解决，文中给出了理想的三部存取结构特性的完全描述，即所有的三部存取结构均为理想的。*Ideal Multipartite Secret Sharing Schemes*[116] 的主要贡献在于，将多部拟阵与离散多拟阵之间的密切联系及相关概念应用于秘密共享领域，从而得到了一般性的结论。

门限秘密共享实现的存取结构实际上是最简单的多部存取结构，即一部的存取结构。大多数基于中国剩余定理构造的秘密共享方案都是实现门限存取结构的，例如 Asmuth-Bloom 方案[103]、Mignotte 方案[125] 以及 Kaya 方案[117,123] 等。Iftene[124] 讨论了如何基于中国剩余定理为其他一些非门限的存取结构构造秘密共享方案，即分隔式的存取结构以及权重的门限存取结构。实际上，这两种存取结构都属于多部存取结构的两种特殊形式。基于多部存取结构的实际应用价值以及每个存取结构都可以看作多部的这一优良特性，如何利用中国剩余定理构造实现多部存取结构的秘密共享方案是非常有价值的。

1.2.4 基于图的秘密共享方案的研究现状

根据前文介绍的基于图的秘密共享方案的基本内容可知，如何将任意一个存取结构与一个图相关联，即如何实现基于图的通用存取结构秘密共享方案是一个有待解决的问题。

同时，由于一个恶意的参与者有可能提供一份虚假的子秘密给其他的参与者，通过引入子秘密的可验证性这一问题得到了解决。在一个可验证的秘