GM/Y 5010-2024

秘密分享技术研究

密码行业标准化技术委员会
CRYPTOGRAPHY STANDARDIZATION TECHNICAL COMMITTEE

2024 年 12 月

摘要

随着信息技术的不断发展，数据作为新的生产要素，其流通、共享过程中的隐私保护问题日益凸显。秘密分享（secret sharing）作为一种基础的密码学原语，可有效解决数据存储、流通中的安全隐患问题，是实现数据可用不可见的重要工具。本报告总结归纳了秘密分享的基本模型、安全要求、门限方案、多部结构方案和一般结构方案等典型秘密分享方案；并对同类结构的不同实现方案进行了分析和对比。按照功能特点的不同，我们进一步归纳了可验证、结构动态、前摄安全、鲁棒安全、通信高效以及抗泄漏秘密分享方案，描述了各类方案的特点、实现方法以及研究进展。秘密分享作为一种基础的密码学工具，具有广泛的应用场景，本报告总结了秘密分享在隐私计算、深度学习、区块链以及电子商务等领域的应用情况，简述了相关行业产品，同时梳理了国内外相关的标准化情况。

关键词：秘密分享 门限结构 多部结构 一般结构

目录

前言

秘密分享自提出以来经历了 40 多年的发展，理论成熟度高，应用广泛。国际上，ISO 已发布了两项秘密分享的标准，但国内仍缺乏对秘密分享基本模型、实现方法的规范。本文通过梳理国内外秘密分享的理论进展、产业应用和标准化现状，遴选典型方法，为行业标准制定提供参考。

本研究报告是由密码行业标准化技术委员会根据国家密码管理局批准下达的密码行业标准研究任务。项目名称为《秘密分享技术研究》，项目类型为标准研究类项目，项目所属工作组为基础工作组。

本文件起草单位：中电科网络安全科技股份有限公司、中国科学技术大学、中国电力科学研究院有限公司、格尔软件股份有限公司、北京信安世纪科技股份有限公司、华控清交信息科技（北京）有限公司、山东大学、华东师范大学。

本文件主要起草人：王现方、林璟锵、李智虎、孔凡玉、郑强、张立廷、张宇、李艺、曾鹏。

秘密分享技术研究

1 概述

数据作为新的生产要素，将会是未来社会数字化、数字中国建设的重要基础。中共中央、国务院于 2020 年 4 月发布文件《关于构建更加完善的要素市场化配置体制机制的意见》，提出加快培育数据要素市场，推进政府数据开放共享，提升社会数据资源价值，加强数据资源整合和安全保护。目前，数据的全生命周期保护面临着不同维度、不同层次的安全威胁。国家相继颁发了一系列与数据保护相关的法律法规，例如《网络安全法》、《密码法》、《数据安全法》以及《个人信息保护法》等。学术界与产业界在数据隐私保护方面也进行了研究与探索。当前隐私计算技术被认为是解决数据安全流通问题的行之有效的技术和工具，而秘密分享则是多方安全计算、隐私计算的重要基础密码工具。

在密码学中，一般采取加密的方式保护通信和存储中的数据。现代密码体制设计的思想是密码算法均公开，安全性取决于密钥。由此产生了如何保护密钥安全的问题。若对密钥再进行一次加密，这从根本上并没有解决这个问题。针对密钥保护问题，密码学家 Shamir 和 Blakley 于 1979 年分别提出了秘密分享的概念和相应的设计方案。简而言之，秘密分享就是将想要共享的秘密数据分成许多份额，并将这些份额分发给不同的参与方，使得特定的份额持有者可合作恢复出原始秘密数据。秘密分享这一概念自从被提出以来得到了学者的广泛研究，理论成果丰富。与此同时，秘密分享的应用也得到了迅速的发展，在密码协议层面，当前主要应用于多方安全计算、门限密码学、访问控制、基于属性的加密以及认证方案等等；在业务场景层面，主要应用于隐私计算、电子商务、区块链和深度学习等场景中。目前，秘密分享已经成为密码学的一类重要原语。

秘密分享技术最初用于解决敏感数据的安全存储问题，但随着数据安全保护趋势的变化和发展，在分布式的安全计算中逐渐起到了举足轻重的作用，用于满足数据的安全可控共享以及数据可用不可见的需求。目前，各应用领域中不同的数据保护需求，对秘密分享机制提出了不同层次、类型的应用需求，并且行业内相对缺乏对秘密分享技术的研究。研究梳理目前已有的典型秘密分享方案，分析不同方案的应用特点，能更好地迎合满足不同场景对秘密分享的需求，同时也能更好地促进秘密分享技术在产业界的应用。

本报告旨在研究秘密分享技术的应用现状以及典型的秘密分享技术方案，为制定行业标准提供相关建议。

2 概念与定义

在秘密分享方案中，假定参与者的集合为$P = \{P_1, \cdots, P_n\}$，共n个参与者，记P的幂集为2^P。负责拆分秘密值、分配份额的角色记为 Dealer，一般也称其为可信第三方。Dealer 对秘密进行拆分分享时，通过特定算法将秘密值作为输入，计算输出一些份额，然后将这些份额通过安全信道分给参与方，使得特定参与者的集合可以恢复秘密。在此，能够恢复秘密的参与者集合称为**授权集**，得不到秘密任何信息（在信息论的意义下）或得不到秘密具体值的参与者集合称为**非授权集**。所有授权集的集合记为Γ，称为**访问结构**；所有非授权集的集合记为Δ，称为**敌手结构**。Γ的对偶结构记为Γ^*，$\Gamma^* = \{A: A \subseteq P, A^c \notin \Gamma\}$。若$A \in \Gamma$，并且$A \subseteq B$，则一定有$B \in \Gamma$，这样的$\Gamma$称为**单调递增的**。若$A \in \Delta$，并

且$B \subseteq A$，有$B \in \Delta$，则称Δ为单调递减的。若$A \in \Gamma$，对任意的$x \in P \backslash A$，都有$A \backslash \{x\} \notin \Gamma$，此时称$A$为**极小授权集**。所有极小授权集的集合记为$\Gamma_0$，$\Gamma$可以由$\Gamma_0$唯一确定。若$A \in \Delta$，对任意的$x \in P \backslash A$，都有$A \cup \{x\} \notin \Delta$，则称$A$为**极大非授权集**，$\Delta$也可由所有极大非授权集唯一确定。很显然，$\Gamma \cap \Delta = \emptyset$，如果进一步有$\Gamma \cup \Delta = 2^P$，则称访问结构$\Gamma$为完备的，相应的秘密分享方案也称为完备的。若对任意的$A_1, A_2, A_3 \in \Delta$，均有$A_1 \cup A_2 \cup A_3 \subset P$，则称$\Gamma$满足条件$Q^3$。

秘密分享方案的定义有各种不同的形式，其中以概率分布给出的定义如下。对随机变量X，记其熵为$H(X)$。秘密值的概率分布以随机变量S表示，一个分发方案若满足以下两个条件，则称其为实现访问结构Γ的**完备秘密分享**方案：

a） **正确性** 对任意的授权集$B \in \Gamma$，有$H(S|S_B) = 0$，

b） **隐私性** 对任意的非授权集$T \notin \Gamma$，有$H(S|S_T) = H(S)$。

若上述隐私性要求改为$0 < H(S|S_T) < H(S)$，则方案不是完备的，此时非授权集可获取秘密的部分信息。此外，若方案的安全性依赖于数学困难问题，则方案被称为**计算安全的**。完备安全的秘密分享方案可看作是信息论意义下安全或**无条件安全**。

假定主秘密的取值空间为$\mathbb{S}$， 第i个份额的取值空间为$\mathbb{S}_i$，记$\rho = max_i \frac{log_2 |\mathbb{S}|}{log_2 |\mathbb{S}_i|}$， 称$\rho$为秘密分享方案的**信息率**。信息率刻画了分享一个比特的秘密时相应份额的大小，信息率的大小是对秘密分享方案效率的一个衡量指标。对任意的完美秘密分享方案都有$\rho \leq 1$。若$\rho = 1$，此时对应于最优情况，称这类秘密分享方案为**理想的**，相应的访问结构也称为理想的。若从秘密计算生成份额这一算法过程可以用线性运算得到，则称此类秘密分享方案为**线性的**。线性秘密分享方案由于具有良好的同态性，在密码学中有着重要的应用，而且大多数的秘密分享方案都是线性的。我们在此仅聚焦于线性秘密分享，非线性的秘密分享方案可以参阅文献[1,2,3,4]。

根据敌手的攻击策略和能力，具体可分为**静态敌手**（static）和**适应性敌手**（adaptive），前者在协议运行前已确定好收买攻击的目标参与者；而后者是在协议运行中，根据观测数据动态调整攻击目标。根据敌手的攻击目的，又可分为**半诚实敌手**（semi-honest）和**恶意敌手**（malicious），前者诚实遵守协议仅对其他发送的信息持好奇态度，后者则可任意破坏协议的运行，例如发送协议无关的数据等。在秘密恢复阶段，一般假定各诚实参与者同时公布持有的份额，若被敌手控制的参与者先观测其他诚实参与者公布的份额后再调整公布份额，则称这类敌手为**突发敌手**(rushing)。

秘密分享方案需要各参与者交互通信，根据通信模型不同，可分为**同步通信**、**异步通信**和**混合通信**模型。在同步通信中，每方的发送的信息在约定的时间内总能被接收方收到，并以通信轮数衡量通信复杂度。在异步通信中，传输的消息可被延迟任意长的时间；混合通信则在开始阶段采用同步通信，后期采用异步通信。不同通信模型下，协议的安全性结论截然不同，我们在本报告中仅考虑同步通信模型。

秘密分享方案按照实现的特点，可分为**基础方案**和**功能性方案**，前者满足秘密分享定义的基本要求，具备秘密分发和恢复功能；后者则在基础方案之上具备额外的一些性质，例如可验证性等。在基础方案方面，研究比较多的访问结构是门限结构，以及门限结构的推广形态——多部结构。此外，针对一般性结构的通用设计也有很多成果。在功能性秘密分享方面，可验证秘密分享关注度高，相关成果较为丰富。除此之外，结构动态、前摄安全、鲁棒性等各类功能性方案也备受关注。值得注意的是，功能性方案的描述分类是从方案功能特点出发进行的，不同类型的方案针对的访问结构类型可能一致，例如可验证的门限方案与门限阈值动态方案均属于门限结构的实现方案。

3　典型秘密分享方案

3.1　门限秘密分享

门限访问结构是秘密分享中最早提出的一类结构，也是应用最多、最成熟的结构。这种阈值控制的思想适用于很多分布式场景。门限结构的非正式定义如下：设t,n是正整数,$t \le n$，n为参与者的总个数，t为门限阈值。在(t,n)门限方案里，任意大于等于t个的参与方集合都能计算出秘密值,而任何小于等于$t-1$个参与者的集合都不能计算出秘密的值。其访问结构的形式化描述如下：

$$\Gamma = \{A \subseteq P, |A| \ge t\}.$$

自从 Shamir 提出插值构造方法以来，学术界也尝试着基于不同数学工具构造新型的门限方案，例如基于中国剩余定理（CRT）、线性码的构造等。按照设计方法不同，在此介绍几类典型的门限秘密分享方案，这些方案均是半诚实安全的，即仅考虑半诚实的敌手。

3.1.1　Shamir 方案

假定q为素数次幂，$q > n$，令F_q为有限域，$\alpha_1,\cdots,\alpha_n \in F_q$为所有参与方均掌握的$n$个不同的非零元素。假定$k \in F_q$为准备分享的秘密，Dealer 执行以下操作[5]：

1　份额生成

a）选择F_q中$t-1$个随机的元素$a_1,\cdots,a_{t-1}$，定义多项式$f(x) = k + \sum_{i=1}^{t-1} a_i x^i$；

b）计算$s_j = f(\alpha_j) mod\ q$，将s_j发送给P_j，$1 \le j \le n$。

2　秘密恢复

任意包含t个参与者的集合$B = \{P_{i_1},\cdots,P_{i_t}\}$，计算

$$k = f(0) = \sum_{l=1}^{t} s_{i_l} \prod_{1 \le j \le t, j \ne l} \frac{\alpha_{i_j}}{\alpha_{i_j} - \alpha_{i_l}}$$

Shamir 方案是一种信息论意义下完备安全的理想门限方案。方案的正确性和隐私性由拉格朗日插值定理保证：对任意的域F,任意的t个不同的元素,以及t个取值$y_1,\cdots,y_t$，在域F上存在唯一次数至多是$t-1$的多项式Q，满足$Q(x_j) = y_j$，$1 \le j \le t$。

Shamir 方案的正确性结论如下。对任意包含t个参与者的集合B，该集合持有多项式P的t个不同点，因此可利用拉格朗日插值恢复出原多项式，进而计算$k = f(0)$。假定$B = \{P_{i_1},\cdots,P_{i_t}\}$，可计算

$$Q(x) = \sum_{l=1}^{t} s_{i_l} \prod_{1 \le j \le t, j \ne l} \frac{\alpha_{i_j} - x}{\alpha_{i_j} - \alpha_{i_l}}.$$

可验证$Q(\alpha_{i_l}) = s_{i_l} = P(\alpha_{i_l})$，$1 \le l \le t$。根据插值定理的唯一性，可知$Q(x) = f(x)$，因此$Q(0) = f(0) = k$。参与者集合 B可通过计算以下等式计算出秘密k：

$$Q(0) = \sum_{l=1}^{t} s_{i_l} \prod_{1 \le j \le t, j \ne l} \frac{\alpha_{i_j}}{\alpha_{i_j} - \alpha_{i_l}}.$$

Shamir 方案的隐私性结论如下。对于任意包含$t-1$个参与者的非授权集$T = \{P_{i_1},\cdots,P_{i_{t-1}}\}$，持有多项式的$t-1$个取值。根据插值定理，对任意的$a \in F_q$，存在

唯一的次数至多为$t-1$的多项式f_a，满足$\mathrm{f_a}(0)=\mathrm{a},\mathrm{f_a}(\alpha_{\mathrm{i_l}})=\mathrm{s_{i_l}}$，$1\le l\le t-1$。因此，$T$无法区分随机数$a$和秘密$k$，隐私性得到保证。

3.1.2 McEliece 方案

McEliece 等[6]利用 Reed-Solomon 码构造了一种新型的门限方案，并指出了 Shamir 方案分享份额的过程与 Reed-Solomon 码的编码过程是等价的。Shamir 方案恢复密钥的过程利用拉格朗日插值，而 McEliece 方案则利用 Reed-Solomon 码的译码算来恢复密钥。Reed-Solomon 码的定义如下：

假定q为素数次幂，$q\ge n-1$，令F_q为有限域，$\alpha_1,\cdots,\alpha_n\in F_q\cup\{\infty\}$为$n$个不同的元素。令线性码$C$的长度为$n$：

$$C=\left\{\left(f(\alpha_1),f(\alpha_2),\cdots,f(\alpha_n)\right)\middle|f\in F_q[x],\deg f\le t-1\right\}$$

其中$f(\infty)$定义为x^t 的系数。线性码C即为 Reed-Solomon 码，其参数表示为$[n,t,d]$，t表示线性码的维数，d表示极小距离。每个线性码都具有生成矩阵$\mathrm{G}_{t\times n}$，对信源消息$m\in F_q^t$计算$c=m\cdot G$作为消息的码字。McEliece 方案具体描述如下。

1 份额生成

a) 假定$a_0\in F_q$为秘密，Dealer 生成F_q上的随机向量$a=(a_0,a_1,\cdots,a_{t-1})$；

b) 利用 Reed-Solomon 码的生成矩阵$\mathrm{G}_{t\times n}$，计算$(s_1,s_2,\cdots,s_n)=a\cdot G_{t\times n}$，将份额$s_i$分发给参与者$P_i$。

2 秘密恢复

任意包含t个参与者的集合$B=\{P_{i_1},\cdots,P_{i_t}\}$，调用 Reed-Solomon 码的译码算法恢复出向量a，进而得到秘密a_0。

McEliece 方案是一种信息论意义下完备安全的理想门限方案。该方案的正确性和隐私性由线性码的性质保证。Reed-Solomon 码为极大距离可分码，即 MDS 码，具有很好的纠错能力。假定参与恢复的份额数量为s个，其中有k个是错误份额，只要$s-2k\ge t$，则可利用译码算法恢复原消息a，最终得到秘密a_0，即方案满足正确性。若提供少于t个份额，无法通过译码算法恢复码字，可保证隐私性。

3.1.3 Asmuth-Bloom 方案

Asmuth 等[7]构造了第一个基于中国剩余定理（CRT）的秘密分享方案，即 Asmuth-Bloom 方案。该方案基于互素的整数序列，假定互素序列为$m_0,m_1,\cdots,m_n$，该序列满足以下性质：

- $m_0<m_1<\cdots<m_n$
- $\prod_{i=1}^{t}m_i>m_0\prod_{i=0}^{t-2}m_{n-i}$

满足上述性质的序列为 Asmuth-Bloom (t,n)门限序列。方案具体描述如下。

1 份额生成

a) 令秘密s的取值空间为Z_{m_0}，第i个份额的取值空间为Z_{m_i}，$1\le i\le n$。Dealer 生成随机数r，使得$s'=s+rm_0<\prod_{i=1}^{t}m_i$；

b) 计算$s_i=s'mod\ m_i$，将s_i分发给第i个参与者P_i作为份额，$1\le i\le n$。

2　秘密恢复

任意包含t个参与者的集合$B=\{P_{i_1},\cdots,P_{i_t}\}$，可构造如下方程组

$$\begin{cases} s' = s_{i_1} mod\ m_{i_1} \\ s' = s_{i_2} mod\ m_{i_2} \\ \vdots \\ s' = s_{i_t} mod\ m_{i_t} \end{cases}$$

利用中国剩余定理求解出s'，进而得到秘密$s = s' mod\ m_0$。

Asmuth-Bloom 方案不具备信息论意义下的完备安全性。方案可确保授权集能恢复秘密，非授权集得不到秘密值（但可得到部分信息），这些性质由中国剩余定理提供保障。对任意授权集A，相应参与者的模数乘积总是大于$\prod_{i=1}^{t} m_i$，利用中国剩余定理，该方程组的解模$\prod_{i\in A} m_i$具有唯一的解s'，进而模m_0即得到秘密值s。若A为非授权集，即A至多有$t-1$个份额，则其解方程组得不到唯一的解s'，进而恢复不出秘密s，但可将秘密的取值空间缩小。关于这类方案详细安全性分析可参阅文献[8]。

3.1.4　Mignotte 方案

Mignotte [9]提出了另一种基于中国剩余定理的设计方法，该方法基于 Mignotte (t,n)门限序列。整数序列$m_1,\cdots,m_n$若满足以下性质：

- $m_1 < \cdots < m_n$为互素序列
- $\alpha \le \beta$，$\alpha = 1 + \prod_{i=0}^{t-2} m_{n-i}$，$\beta = \prod_{i=1}^{t} m_i$

则被称为 Mignotte (t,n)门限序列。可发现，在 Asmuth-Bloom (t,n)门限序列中，令$m_0 = 1$，即为 Mignotte (t,n)门限序列。该方案描述如下。

1　份额生成

a）令秘密s的取值空间为$[\alpha,\beta)$，第i个份额的取值空间为Z_{m_i}，$1 \le i \le n$。

Dealer 执行计算$s_i = s\ mod\ m_i$；

b）将s_i作为份额发送给第i个参与者P_i。

2　秘密恢复

对于任意的授权集B，$|B| \ge$ t，A可构造如下方程组：

$$x = s_i\ mod\ m_i,\ \forall i \in A$$

利用中国剩余定理，该方程组的解模$\prod_{i\in A} m_i$具有唯一的解s，即可恢复出秘密。

Mignotte 体制并不能提供信息论意义下的完备安全性。

该方案的安全性基于极大非授权集可计算的解的个数。令$M = \prod_{i=1}^{t} m_i$，$z_i = \left(\left(\frac{M}{m_i}\right)^{-1} mod\ m_i\right)\cdot(M/m_i)$，根据欧几里得算法，存在$r_i$使得$z_i + r_i m_i = 1$，$1 \le i \le t-1$，当只有$t-1$个份额$s_1,\cdots,s_{t-1}$时，有等式$s = s_1 z_1 + \cdots + s_t z_{t-1}\ mod\ m_1 \cdots m_{t-1}$，即区间$[\alpha,\beta-1]$至少包含$c = [\frac{\beta-1-\alpha}{m_1\cdots m_t}]$个值满足上述等式，并且以相等的概率均可能为秘密$s$。当$c$足够大时，非授权集难以恢复出秘密$s$，但能得到关于秘密的相关信息。关于这类方案详细安全性分析可参阅文献[10]。

3.1.5 GRS 方案

Goldreich 等人[11]提出了另一种门限方案设计方法，与以往基于中国剩余定理的体制不同之处在于，GRS 方案在秘密分发和恢复的过程中均使用中国剩余定理。令$m_0 < m_1 < \cdots < m_n$为互素整数序列，秘密s取值空间为Z_{m_0}，第i个参与者的份额空间为Z_{m_i}。方案描述如下。

1 份额生成

a) Dealer 随机生成$r_i \in Z_{m_i}$，$1 \le i \le t-1$，令$r_0 = s$；利用中国剩余定理计算下述方程组的唯一解s'：

$$x \equiv r_i \bmod m_i,\ 0 \le i \le t-1$$

b) 计算份额$s_i = s' \bmod m_i$，$1 \le i \le n$，将份额s_i分发给第i个参与者P_i。

2 秘密恢复

对于任意的至少包含t个参与者的授权集B，B可构造如下方程组：

$$x = s_i \bmod m_i,\ \forall i \in A$$

利用中国剩余定理，该方程组的解模$\prod_{i\in A} m_i$具有唯一的解s'，进而得到秘密$s = s' \bmod m_0$。

GRS 方案仅能提供信息论意义下近似完备安全性。Quisquater[12]引入了近似完备和近似理想性的概念，并对 GRS 方案进行了详细的分析。方案可保证任意授权集计算得到秘密，因为任意授权集对应的模整数总是大于$\prod_{i=1}^{t} m_i$，可得到唯一的解。对任意的非授权集I，$|I| \le t-1$，秘密所定义的随机变量X关于任意$s, s' \in Z_{m_0}$的统计距离最多为

$$2\frac{\prod_{i\in I} m_i}{\prod_{1\le i\le t-1} m_i}$$

即安全性仅能对$|I| \le t-2$有效。

3.1.6 XOR 方案

为了提高门限方案的运算效率，相关学者研究了如何基于 XOR 运算设计门限体制。例如 Chen 等人[13]提出了基于 XOR 运算的高效门限方案。该方案基于信息分散算法（IDA），一个(t,n)信息分散算法包含两个子算法，即分享算法和恢复算法；分享算法输入源消息m，输出n长的向量S；恢复算法输入S中的任意t个元素，输出源消息m。(t,n)-IDA 的正确性与(t,n)门限方案一致，但 IDA 对隐私性没有要求。即任意的(t,n)门限体制均可看作一个(t,n) – IDA，反之则不成立。

一种典型的系统的(t,n) – IDA 算法构造如下。假定源消息M为有限域F_{2^λ}上的t长向量，令G为公开已知的$n \times t$比特矩阵，G的前t行为单位矩阵，其余行随机填充，使得G的任意t行均是线性无关的。计算$C = GM$，将C中的每个元素分别发给参与者。在消息恢复时，任何t个参与者基于G可重构一个$t \times t$的可逆矩阵G'，进而结合其持有的t个份额，计算出源消息M。分发过程的形式描述如下所示。

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 \\ G[t][0] & G[t][1] & \cdots & G[t][t-1] \\ \vdots & \vdots & \vdots & \vdots \\ G[n-1][0] & G[n-1][1] & \cdots & G[n-1][t-1] \end{pmatrix} \begin{pmatrix} M[0] \\ M[1] \\ \cdots \\ M[t-1] \end{pmatrix} = \begin{pmatrix} M[0] \\ M[1] \\ \cdots \\ M[t-1] \\ C[t] \\ \cdots \\ C[n-1] \end{pmatrix}$$

假定秘密$k \in \{0,1\}^{\lambda}$，将k拆分成t个比特向量，每个比特向量含有k的$\frac{\lambda}{t}$个比特(假定可整除)，将每个比特向量看作$F_{2^{\lambda}}$上的元素，进而$k \in F_{2^{\lambda}}^{t}$。Dealer 执行如下操作。

1　份额生成

a) 生成$F_{2^{\lambda}}$上$t-1$个随机元素$r_1, \cdots, r_{t-1}$，按照对秘密k的处理规则，使得$r_i \in F_{2^{\lambda}}^{t}$；计算$k' = k \oplus r_1 \oplus \cdots \oplus r_{t-1}$；

b) 将$r_1, \cdots, r_{t-1}$，k'作为输入分别调用 IDA，得到长度为n的t个向量$R_1, \cdots, R_{t-1}, K' \in F_{2^{\lambda}}^{n}$，将这些向量组成一个$t \times n$的矩阵$M$，从第二行开始，对$M$的第$i$行循环右移$i-1$位，得到新矩阵$M'$；

c) 将M'的一列分发给相应的参与者。

上述过程中的M和M'的形式矩阵如下。

$$M = \begin{pmatrix} K'[0] & K'[1] & \cdots & K'[n-2] & K'[n-1] \\ R_1[0] & R_1[1] & \cdots & R_1[n-2] & R_1[n-1] \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ R_{t-1}[0] & R_{t-1}[1] & \cdots & R_{t-1}[n-2] & R_{t-1}[n-1] \end{pmatrix}$$

$$M' = \begin{pmatrix} K'[0] & K'[1] & \cdots & K'[n-2] & K'[n-1] \\ R_1[1] & R_1[2] & \cdots & R_1[n-1] & R_1[0] \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ R_{t-1}[t] & R_{t-1}[t+1] & \cdots & R_{t-1}[t-2] & R_{t-1}[t-1] \end{pmatrix}$$

2　秘密恢复

任意的授权集合包含至少t个参与者，进而可调用 IDA 恢复算法得到$R_1, \cdots, R_{t-1}, K'$，即得到$r_1, \cdots, r_{t-1}$，k'。对向量进行异或运算得到秘密$k = k' \oplus r_1 \oplus \cdots \oplus r_{t-1}$。

这类方案可提供信息论意义下完备的安全性。方案依赖于采用 XOR 运算的高效 IDA 算法。当非授权集少于t个参与者时，无法恢复出$r_1, \cdots, r_{t-1}$，k'，由于秘密k是通过异或隐藏的，即攻击者得不到秘密k的任何信息。

3.1.7　CRT 方案

大多数基于中国剩余定理的门限方案依赖于模整数运算，并且不能提供信息论意义下完备的安全性。Ning 等人[14]针对这一问题，基于多项式环上的中国剩余定理设计了一种新型的门限方案。方案描述如下。

Dealer 选择正整数$d_0 \geq 1$，令$m_0 = x^{d_0}$，并选择素数p，方案基于的有限域为F_p。选择两两互素的多项式$m_i(x) \in F_p[x]$，令$d_i = deg(m_i(x))$，$0 \leq i \leq n$。多项式需要满足以下条件：

$$\mathrm{d}_0 \leq d_1 \leq d_2 \leq \cdots \leq d_n$$

$$\mathrm{d}_0 + \sum_{i=n-t+2}^{n} d_i \le \sum_{i=1}^{t} d_i$$

令秘密空间为

$$S = \{g(x) \in F_p[x] | \, deg(g) < d_0\}$$

1 份额生成

a) 假定秘密为$s(x) \in S$，Dealer 随机生成多项式$\alpha(x) \in A$，其中

$$A = \{g(x) \in F_p[x] | \, deg(g) \le \sum_{i=1}^{t} d_i - d_0 - 1\}$$

计算$f(x) = s(x) + \alpha(x)m_0(x)$；

b) 计算份额$s_i(x) = f(x) \, mod \, m_i(x)$，将其发送给第$i$个参与者$P_i$。

2 秘密恢复

对于任意的至少包含t个参与者的授权集$B = \{P_{i_1}, P_{i_2}, \cdots, P_{i_t}\}$，$B$可构造如下方程组

$$\begin{cases} X(x) \equiv s_{i_1}(x) \, mod \, m_{i_1}(x) \\ X(x) \equiv s_{i_2}(x) \, mod \, m_{i_2}(x) \\ \cdots \\ X(x) \equiv s_{i_t}(x) \, mod \, m_{i_t}(x) \end{cases}$$

根据 CRT，授权集可得到次数小于$d = \sum_{j=1}^{t} d_{i_j}$的唯一解$X_0(x) = f(x)$。进而可计算$s(x) = X_0(x) \, mod \, m_0(x)$。

该方案可提供完备安全性，并满足理想性。方案的正确性和隐私性由多项式环上的中国剩余定理保障。当$d_0 = d_1 = \cdots = d_n = d$时，该方案是理想的。该方案可视为 Asmuth-Bloom 方案和 Shamir 方案的抽象与推广。特别地，当$d_0 = 1$，$m_0(x) = x$，$m_i(x) = x - a_i \in F_p[x]$，$s(x) = a_0 \in F_p[x]$，

$$A = \{g(x) \in F_p[x] | \, deg(g) \le t - 2\}$$

此时的方案即为 Shamir 方案。

3.1.8 ramp 方案

在完备的秘密分享方案中，份额的大小至少和秘密的大小一致，即信息率至多为 1。为了新一步降低参与者持有的份额大小提高信息率，相关学者通过降低方案的安全性阈值，设计非完备安全的方案。Blakley 等人[15]提出了第一个非完备安全的门限方案，被称为(r, t, n)-ramp 方案。当参与方的数量小于等于r时，得不到秘密的任何信息（信息论意义下），当参与方的数量大于t时，可恢复出秘密，而当参与方的数量大于等于$r+1$，并且小于等于$t-1$时，可得到消息的部分信息，但不能恢复出消息。方案的具体描述如下。

假定q为素数次幂，$q > n$，令F_q为有限域，$\alpha_1, \cdots, \alpha_n \in F_q$为所有参与方均掌握的$n$个不同的非零元素。

1 份额生成

a) 假定$(k_0, k_1, \cdots, k_{r-1}) \in F_q^r$为准备分享的秘密，Dealer 选择$F_q$中$t-r$个随机的元素$a_r, \cdots, a_{t-1}$，定义多项式$f(x) = \sum_{i=0}^{r-1} k_i x^i + \sum_{i=r}^{t-1} a_i x^i$；

b) 计算$s_j = f(\alpha_j)$，将s_j发送给P_j，$1 \le j \le n$。

2 秘密恢复

对于任意的至少包含t个参与者的授权集$B=\{P_{i_1},P_{i_2},\cdots,P_{i_t}\}$，$B$可利用拉格朗日插值法唯一恢复多项式$f(x)$，进而得到多项式所有系数，恢复秘密$(k_0,k_1,\cdots,k_{r-1})$。

该方案不能提供完备安全性，仅对小于r的参与者集合提供完备安全性。而当非授权集中参与者数量大于等于$r+1$并小于等于$t-1$时，可将密钥的空间限定缩小，进而得到秘密的部分信息。方案的正确性很容易验证，授权集可利用插值法恢复出完整多项式得到秘密。

3.1.9 加性方案

门限方案中要求阈值$t\leq n$，对于$t=n$这一类特殊情形，一般情况下也被归属为门限方案。针对这类特殊情形，研究人员提出了更为高效的设计方法[16]。这类设计方案的思想很简洁，即将秘密值直接在运算域上采用加法拆分。对底层的代数对象不局限于域，对一般的群也适用。方案详细描述如下。

1 份额生成

a) 假定$k\in G$为准备分享的秘密，G为加法群，Dealer 选择G中$n-1$个随机的元素$r_1,r_2,\cdots,r_{n-1}$，并计算$r_n=k-r_1-r_2-\cdots-r_{n-1}$；

b) 将r_i分发给参与者P_i。

2 秘密恢复

所有参与者均需参与秘密恢复，计算$k=r_1+\cdots+r_n$。

这类方案可提供完备安全性，并为理想方案。但方案仅适用于门限阈值为n这一情形。当参与恢复秘密的参与者小于n时，秘密与随机数是不可区分的。

3.1.10 Kikuchi 方案

按照安全假设，秘密分享方案可划分为完备安全和计算安全，前者是信息论意义下的安全，与敌手的计算能力无关，后者则将考虑敌手的计算能力。计算安全的秘密分享方案可降低参与者所持有份额的存储大小，比较适用于大尺寸的秘密数据量。Kikuchi 等人［17］给出了一种计算安全的门限秘密分享方案。该方案用到了 Rabin 的(t,n)-IDA 算法，这种信息分散算法具体描述如下。

令R为环，F为域，$\omega:R\to F^t$为单射，ω和ω^{-1}均可高效计算。(t,n)-IDA 包含两个子算法 IDA.Split 和 IDA.Rec。

1 IDA.Split

a) 假定源信息为$a\in R$，计算$(a_0,\cdots,a_{t-1})=\omega(a)$，令$f(x)=\sum_{i=0}^{t-1}a_ix^i$；

b) 计算$v=(f(1),f(2),\cdots,f(n))$。

2 IDA.Rec

任意t个信息分片数据$f(i)$，可恢复出多项式$f(x)$，进而得到了源信息a。

与门限秘密分享方案相比，(t,n)-IDA 只考虑信息的可恢复性，不关注安全性。令$\phi:F\to R$为伪随机数生成器，假定$a\in R$为计划分享的秘密，文献[17]给出的计算安全(t,n)门限秘密分享方案描述如下：

1 份额生成

a) 生成F中的t个种子$s_0,s_1,\cdots,s_{t-1}$，计算$u_i=\phi(s_i),0\leq i\leq t-1$，$v=a-\sum_{i=0}^{t-1}u_i$；

b) 利用(t,n)门限秘密分享方案，将s_i作为秘密输入，得到输出份额向量$([s_i]_1,[s_i]_2,\cdots,[s_i]_n)$；

c） 将v作为输入，调用(t,n)-IDA 得到输出向量$(v_1,v_2,\cdots,v_n)$;

d） 令$[a]_i=([s_0]_i,[s_1]_i,\cdots,[s_{t-1}]_i,v_i),1\le i\le n$，为参与者$P_i$的份额。

2 秘密恢复

任意t个参与者利用组件门限方案恢复算法可先恢复出$s_i,0\le i\le t-1$，进而计算得到$u_i=\phi(s_i)$，再调用 IDA.Rec 得到v，最终即可得到$a=v+\sum_{i=0}^{t-1}u_i$。

这类方案提供计算安全性，依赖于伪随机数生成器将种子信息在参与者之间共享。参与者持有的份额均属于尺寸较小的域上，而真正的秘密属于大尺寸的环上。方案的安全性和隐私性依赖于信息论安全的门限方案和信息分散组件。

3.1.11 小结

Shamir 方案设计的初衷是为了保护密钥,随后在分布式计算和一般性敏感数据的保护方面得到了广泛的应用。Shamir 方案很适用于运算域为有限域的情形，但在其他运算域的应用场景中，例如整数环，加法群等，就变得不太适用。为此学术界研究提出了各种不同构造方法的门限方案，即 Asmuth-Bloom 方案等。整体来看，这些方案在效率、适用性上各有优缺点，具体对比如下表所示。

表 3.1 门限方案对比

方案类别	完备安全	信息率	依赖组件	运算域	分发效率	恢复效率
Shamir	是	1	无	有限域	$O(nt)$	$O(tlog^2t)$
McEliece	是	1	无	有限域	$O(nt)$	$O(nlog^2n)$
Asmuth-Bloom	否	$\frac{m_0}{m_n}$	无	整数环	$O(n+t)$	$O(t)$
Mignotte	否	$\frac{\beta-\alpha}{m_n}$	无	整数环	$O(n)$	$O(t)$
GRS	近似完备	$\frac{m_0}{m_n}$	无	整数环	$O(n+t)$	$O(t)$
XOR	是	1	IDA	二元扩域	$O(nt)$	$O(t)$
CRT	是	1	无	多项式环	$O(nt)$	$O(tlog^2t)$
Ramp	否	r	无	有限域	$O(nt)$	$O(tlog^2t)$
加性方案	是	1	无	群	$O(n)$	$O(n)$
Kikuchi 方案	否	$\frac{\lvert R\rvert}{(t+1)\lvert F\rvert}$	IDA	有限域和环	$O(nt)$	$O(tlog^2t)$

在上述表格中 Asmuth-Bloom 方案和 GRS 方案的信息率依赖于所选整数序列的规模，假定参与者所用最大整数为m_n，则信息率为即$\frac{m_0}{m_n}$。在渐进意义下，这两类方案的信息率趋近于 1。与之相比，Mignotte 方案的信息率更低。计算安全方案的信息率则依赖于运算域环R和域F。大多数门限方案设计时不采用任何其他独立组件，但 XOR 方案和计算安全方案则都需要信息分散算法（IDA）作为子算法。由此额外带来的优势就是运算域的改变，XOR 方案可在二元扩域上提供比 Shamir 方案更高效的恢复过程；计算安全方案则可将大尺寸环R上的秘密分解为小尺寸域F上的份额，由此降低了存储开销。

3.2 多部结构秘密分享

在门限方案中，每个参与方参与恢复秘密的作用都是等价的，参与方之间可互相替代。但在现实应用中会需要这样的一种情况：不同参与方参与恢复秘密的能力不一致。多部访问结构将参与方划分为不同的部分，相同部分的参与方在恢复秘密时发挥等价的作用。从定义上看，门限方案可看作多部结构的特例。目前多部结构主要可分为分层结构和分块结构。具体而言，在分层结构中，参与方按照恢复秘密的能力被划分为不同的层级，高层次的参与方可替代低层次的参与方；在分块结构中，参与方的集合被划分为不同的小组，每个组内的成员恢复秘密的能力一致，不同组的参与方恢复秘密的能力不一致。目前，这两类访问结构均存在理想的秘密分享方案。

3.2.1 分层方案

分层秘密分享体制最早由 Simmons[18]研究提出，该结构被称为析取分层访问结构。具体定义如下：

令$m, t_1 < t_2 < \cdots < t_m$为正整数，将参与者集合划分为不相交的子集，即$P = \bigcup_{i=1}^{m} U_i$，则析取分层访问结构为：

$$\Gamma = \{V \subseteq P: \exists i \in [1,m]\ s.t. \left| v \cap \left(\bigcup_{j=1}^{i} U_j\right)\right| \geq t_i\}。$$

在析取分层访问结构中，要求授权集包含前i层划分集中的参与者个数至少为t_i个，对某一个 $i \in [1.m]$成立即可。并且可以看出第 i 个划分集 U_i 中的参与者可以代替第 j 个划分集 U_j 中的参与者，$1 \leq i < j \leq m$，这正是分层的体现。

上述分层结构非常适用于参与者恢复能力具有明显层级划分的场景。以银行金库钥匙的保存为例，假定要求至少四人在场才能打开金库，并要求这四人中至少有一个经理。容易看出，在这种要求中有权力的分层，经理可以替代权力比他低的人，要求四人中至少包含一个经理，显然，包含两个、三个经理也都满足要求。参与者按照权力的高低被划分成不同的分组，权力高的分组中的参与者可以替换权力低分组中的参与者。

Tassa[19]利用伯克霍夫插值法设计了一种理想的方案实现上述析取分层访问结构，即析取分层秘密分享体制。伯克霍夫插值问题如下：令

a) $X = \{x_1, \cdots, x_k\}$为实数域$\mathbb{R}$上给定的点集，满足$x_1 < x_2 < \cdots < x_k$；

b) $E = \left(e_{i,j}\right)_{i=1,j=1}^{k,l}$为一个 0,1 二元矩阵，记$I(E) = \{(i,j): e_{i,j} = 1\}, d = |I(E)|$；

c) $C = \{c_{i,j}: (i,j) \in I(E)\}$为$d$个实数的集合；

对应于上述$< X, E, C >$的伯克霍夫插值问题为：求解多项式$f(x) \in \mathbb{R}_{d-1}$，其中

$$f^{(j)}(x_i) = c_{i,j}, (i,j) \in I(E)$$

E被称为插值矩阵。伯克霍夫插值问题可求解的一个必要条件是满足 Polya 条件：

$$|\{(i,j) \in I(E): j \leq t\}| \geq t+1, 0 \leq t \leq l。$$

Tassa 方案的具体描述如下。

假定q为素数，$q > 2^{-t}(t+1)^{(t+1)/2} N^{(t-1)t/2}$，其中$t = t_m, N = max\{|U_i|, i \in [1,m]\}$。参与方$P_{ij} \in U_i$的身份记为$\mathrm{x}_{ij} \in F_q$，并满足$\mathrm{x}_{ik} < x_{jl}, \forall i < j$。

1 份额生成

a) 假设$s \in F_q$为秘密值，Dealer 生成$F_q[x]$上次数为$t-1$的随机多项式$f(x) = \sum_{i=0}^{t-1} a_i x^i$，其中$a_0 = s$；

b） 对于第i层的参与者P_{ij}，其份额为$f^{(t_i-1)}(x_{ij})$，$1 \le i \le m, t_0 = 0$。

2 秘密恢复

对于任意的授权集B，满足 Polya 条件，可利用伯克霍夫插值获取多项式$f(x)$，即得到秘密s。

该方案是理想方案，即可达到信息论意义下安全，并且信息率为 1。上述方案中，不同层级参与者持有的份额中关于密钥信息量的大小不同，具体通过多项式导数来实现。授权参与者恢复秘密时通过伯克霍夫插值法可唯一恢复秘密 s。

Tassa[19]同时研究了析取访问结构的对偶结构，即合取访问结构。该结构具体定义如下：

令$m, t_1 < t_2 < \cdots < t_m$为正整数，将参与方集合划分为不相交的子集，即$P = \bigcup_{i=1}^{m} U_i$，则合取分层访问结构为：

$$\Gamma = \{V \subseteq P: \left|v \cap \left(\bigcup_{j=1}^{i} U_j\right)\right| \ge t_i, \forall i \in [1.m]\}。$$

在上述合取分层访问结构中，要求授权集包含前 i 层划分集中的参与方个数至少为 t_i 个，对任意的$i \in [1,m]$都必须满足，这是与析取结构的根本区别。同样可以看出第 i 个划分集中的参与者可以代替第 j 个划分集中的参与者，$i < j$。

仍以银行金库钥匙的保存为例，此时要求至少 4 人在场才能打开金库，同时要求这四人中至少有一个总监；要求总监和经理中至少 2 个人参与。在这种情形下，最高层要求至少一人，前两层要求至少 2 人，所有参与者要求至少 4 人，这三个条件要同时满足。容易看出，在这种要求中有权力的分层，总监可以替代经历，经理可以替代权力比他低的普通职员；这类应用场景即满足合取分层访问结构。

Tassa 基于同样的原理设计了理想的合取分层秘密分方案，具体描述如下。

假定q为素数，$q > C_n^t(n-t)$，其中$t = t_m$。参与方$P_{ij} \in U_i$的身份记为$x_{ij} \in F_q$，并满足$x_{ik} < x_{jl}, \forall i < j$。

1 份额生成

a） 假设$s \in F_q$为秘密值，Dealer 生成$F_q[x]$上次数为$t-1$的随机多项式$f(x) = \sum_{i=0}^{t-1} a_i x^i$，其中$a_{t-1} = s$；

b） 对于第i层的参与方P_{ij}，其份额为$f^{(t-t_i)}(x_{ij})$，$1 \le i \le m$。

2 秘密恢复

对于任意的授权集B，满足 Polya 条件，可利用伯克霍夫插值获取多项式$f(x)$，即得到秘密s。

该方案可提供信息论意义下的完备安全，并且信息率为 1。与析取方案相似，合取方案仍采用伯克霍夫插值，但不同之处在于，密钥s的位置放到最高项系数位置。

3.2.2 分块方案

与分层结构类似，分块结构将参与者划分为不同的分组，每个组内参与者在恢复秘密时发挥同等作用。每组有着特定的阈值，不同组的参与者恢复秘密时不可相互代替。在分块访问结构中，最为典型的是带有下界的分块访问结构，定义如下：

令$m, t, t_1 < t_2 < \cdots < t_m$均为正整数，并且$t > \sum_{i=1}^{m} t_i$。参与方集合划分为不相交的子集，即$P = \bigcup_{i=1}^{m} U_i$，带有下界的分块访问结构定义为：

$$\Gamma = \{V \subseteq P: |V| \ge t, |V \cap U_i| \ge t_i, \forall\, i \in [1,m]\}。$$

这类结构要求授权集中参与者的大小至少为 t，并且包含每一个分组中的参与者的个数至少为 t_i。直观地理解，每一个划分集 U_i 中至少要参与 t_i 个参与方并且参与方

总数至少为 t 个才能恢复秘密。这是对不同的分组之间公平对待的体现，与分层访问结构不同，在分块访问结构里不同的分组之间参与者不可替换。以银行金库钥匙的保存为例，要求至少 4 人在场才能打开金库，同时要求要求总监和经理中至少 2 个人参与，并且财务职员至少 2 人参与。在这种情形下，总监和经理不能替代财务职员，这三个阈值条件要同时满足才能恢复秘密。

为了设计秘密分享实现这类结构，Tassa[20]等研究了这类结构的对偶，即上述带有下界分块访问结构的对偶结构，具体定义如下：

令$m,t,t_1<t_2<\cdots<t_m$均为正整数，并且$t>\sum_{i=1}^{m}t_i$。参与方集合划分为不相交的子集，即$P=\bigcup_{i=1}^{m}U_i$，带有下界分块访问结构的对偶结构定义为：

$$\Gamma=\{V\subseteq P:|V|\geq t \text{ 或} |V\cap U_i|\geq t_i,\exists\, i\in[1,m]\}。$$

Tassa 等[20]基于二元插值设计了一种概率性的分块秘密分享体制实现上述对偶结构，方案具体描述如下。

1　份额生成

a) 假定$s\in F_q$为秘密值，q为素数，$q>nC_{n+1}^{t}$，Dealer 令$x_i\in F_q$为m个不同的点，$P_i(y)$为F_q上t_i-1次的多项式，满足$P_1(0)=\cdots P_m(0)=s$。定义多项式$p(x,y)=\sum_{i=1}^{m}P_i(y)L_i(x)$，其中$L_i(x)$为集合$\{x_i:1\leq i\leq m\}$上的拉格朗日多项式。参与方$P_{ij}\in U_i$的身份记为$(x_i,y_{ij})\in F_q$；

b) 对于第i层的参与方P_{ij}，其份额为$p(x_i,y_{ij})$，$1\leq i\leq m$；

c) Dealer 取$\sum_{i=1}^{m}t_i-(m-1)-t$个随机的点$(x_i',z)$，要求$x_i'\notin\{x_1,\cdots,x_m\}$，并公布$p(x,y)$在这些随机点的值。

2　秘密恢复

对任意的授权集V，若V包含t个参与者，则V利用公开点的值可得到关于求解秘密s的方程组，求解方程组得到秘密；若$|V\cap U_i|\geq t_i$对某个i成立，则V可直接利用插值法得到s。

该方案可提供信息论意义下的完备安全，但有很小的失败概率无法恢复秘密。方案的正确性由二元插值法保障。当$|V|\geq t$时，V共计可获取$\sum_{i=1}^{m}t_i-(m-1)$个$p(x,y)$的取值，此时多项式$p(x,y)$为关于y的单项式，并且待定系数个数为$\sum_{i=1}^{m}t_i-(m-1)$。建立关于系数的方程组，可以极大的概率求解出所有系数。基于上述方案，利用文献[21]中的对偶方法之间的转换方法，可得到带有下界的分块访问结构的秘密分享方案。

3.2.3　小结

当前，针对多部结构的主要设计方案对比如下表 3.2 所示。

表 3.2　多部秘密分享方案对比

方案类别	结构类型	公共份额	恢复概率	主要工具
[19]	析取/合取结构	否	1	伯克霍夫插值
[20]	带有下界分块结构	是	渐进为 1	二元插值
[28]	广义分层结构	否	渐进为 1	多项式
[29]	细分分块结构	是	渐进为 1	二元插值
[25]	广义分层结构/带有上下界分块结构	否	1	拟阵表示

[26]	带有上下界分块结构	否	1	拟阵表示
[27]	带有上下界分块结构	否	1	线性码

理想多部访问结构的研究和方案实现近年来取得了丰富的成果。2012 年，Farràs 等[22]利用多部拟阵和整多拟阵之间的联系刻画出了所有的理想分层访问结构以及几大类理想多部访问结构。但并未直接给出有效体制的构造方法。2014 年，Farràs 等[23]进一步利用整多拟阵和多部拟阵的联系，给出了几类理想的分块访问结构。随后，Wang 等[24] 于 2015 年提出了几类新的理想分块访问结构。Chen 等[25]于 2019 年研究找出了几类整多拟阵的表示方法，进一步针对理想分层结构给出了具体有效的理想秘密分享方案。采用同样的方法，Chen 等[26] 于 2019 年研究找出了几类整多拟阵的表示方法，进一步针对理想分块结构给出了具体有效的理想秘密分享方案。此外，Chen 等[27]于 2020 年研究了分块存取结构和局部修复线性码的关系，利用几类局部修复线性码构造了新型的理想分块体制。

3.3 一般结构秘密分享

在秘密分享方案研究方面，一个重要的问题是如何针对任意的、一般性单调访问结构，设计完备或者高效的方案。根据现有研究结果，对任意的单调访问结构都存在完备的秘密分享方案，但不一定存在理想方案。这个开创性的工作由 Ito 等人[16] 提出，随后文献 [30] 利用单调公式也构造了一种方法实现任意的单调访问结构。文献[16]主要采用累积数组（Cumulative Arrays，CAS）和多重赋值（Multiple Assignments，MAS）的方法进行构造，并采用门限方案作为基本组件。按照这一构造思想，文献[31，32]分别提出了整数规划的方法构造秘密分享方案，即对一个目标访问结构，在 MAS 中通过整数规划求出最优的门限方案（这里的最优指的是方案的信息率尽可能大），利用这个最优的门限方案生成的份额再进行下一步分发。2015 年，[33]将 MAS 做了进一步的推广，提出了 ramp 指派方案 (RAS)，其思想就是利用 ramp 方案替代 MAS 中的门限方案，并利用线性规划寻找对特定访问结构最优的 ramp 方案。此外，另一类重要的构造方法是将已有方案作为一个子方案，去构造一个更大访问结构的方案。这种方法称为分解构造，例如λ分解构造和(λ,ω)分解构造。整体来看，在一般性秘密分享的构造方面，学术界取得了丰富的研究成果。在此章节介绍几类经典的，针对通用结构的设计方法。

3.3.1 无向完全图方案

Benaloh 等人[4]针对图上的访问结构，设计了一种通用构造方法。假定无向完全图(V,T)具有m个顶点$v_1,\cdots,v_m$，$n=\binom{m}{2}$条边，每条边(v_i,v_j)对应于一个参与者P_{ij}。n个参与者构成了参与者集合P。基于此类图的访问结构定义如下：

$$\Gamma=\{A\subseteq P: A\text{中的边包含一条由}v_1\text{到}v_m\text{的路径}\}$$

针对上述访问结构，具体的秘密分享方案如下。

1 份额生成

a) 假定秘密为$k\in\{0,1\}$，Dealer 随机生成$m-2$个随机比特$r_2,r_3,\cdots r_{m-1}$，令$r_1=k$，$r_m=0$，计算$s_{ij}=r_i\oplus r_j$；

b) 将s_{ij}作为份额分发给参与者P_{ij}。

2 秘密恢复

对任意的授权集，均包含一条v_1到v_m的一条路径$v_1 = v_{i_1} v_{i_2} \cdots v_{i_{l-1}} v_{i_l} = v_m$。这条路径上的参与者将其份额进行异或即可得到密钥$k$，即

$$\left(r_{i_1} \oplus r_{i_2}\right) \oplus \left(r_{i_2} \oplus r_{i_3}\right) \oplus \cdots \oplus \left(r_{i_{l-2}} \oplus r_{i_{l-1}}\right) \oplus \left(r_{i_{l-1}} \oplus r_{i_l}\right) = r_{i_1} \oplus r_{i_l}$$

$$= r_1 \oplus r_m = k$$

该方案是完备安全的，并且信息率为 1。授权集可通过份额异或恢复秘密，非授权集则无法获取秘密的信息。上述方案针对的秘密是比特，也可拓展到更一般的比特串情形。即针对秘密$k \in \{0,1\}^l$，可选取相应长度规模的随机比特串，进行同样的运算操作。这类方法可实现秘密长度为l的分享。

3.3.2 多重赋值方案

任意的单调访问结构，均存在完备的秘密分享方案，Ito 等人[16]给出非常经典的构造方法。令Γ为任意的单调访问结构，k为需要分享的秘密比特，方案具体描述如下。

1 份额生成

a) 对任意的授权集$B = \{P_{i_1}, \cdots, P_{i_l}\} \in \Gamma$，Dealer 选择$l-1$个随机比特$r_1, \cdots, r_{l-1}$，计算$r_l = k \oplus r_1 \oplus \cdots \oplus r_{l-1}$；

b) 将r_j作为份额分发给P_{i_j}。

2 秘密恢复

任意的授权集B，直接将份额进行异或即得到秘密k。

上述方案是完备安全的。在正确性方面，易知任意的授权集合均可通过异或所有的份额恢复密钥。在隐私性方面，对于任意的非授权集T，其至少不包含每个授权集中的一个参与者，即T持有的比特是均匀分布的，与秘密独立。该方案的份额分发过程是按照授权集进行的，从优化的角度考虑，可只对极小授权集进行操作。另一方面，参与者P_j持有的份额数量与其所属于的极小授权集的个数一致，即一个参与者会持有多个秘密份额。

上述方案有另外的一种描述方法。对任意的单调访问结构Γ，假定极大非授权集的个数为m，秘密$k \in F_q$为有限域中的元素，方案描述如下。

1 份额生成

a) Dealer 随机生成有限域中的$m-1$个随机数$r_1, \cdots, r_{m-1}$，计算$r_m = k - r_1 - \cdots - r_{m-1} \bmod q$；将$r_1, \cdots, r_{m-1}, r_m$依次对应于$m$个极大非授权集；

b) 对任意一个参与者P_i，将不包含P_i的那些极大非授权集对应的随机数分给P_i作为份额。

2 秘密恢复

对任意的授权集B，其参与者持有的份额可完全覆盖所有的随机数r_i，进而可恢复出秘密k。

3.3.3 单调电路方案

Benaloh 等[30]基于单调电路对任意的访问结构设计了一种秘密分享方案的构造方法。该方法在一定程度可看作 MSA 方案的推广。这类构造方案通过迭代的思想，从简单访问结构的方案出发，通过访问结构的异或得到复杂访问结构的方案。

假定两个访问结构Γ_1,Γ_2具有相同的参与者集合$\{P_1,\cdots,P_n\}$，可定义两个新的访问结构$\Gamma_{1\vee2}=\Gamma_1\vee\Gamma_2$，$\Gamma_{1\wedge2}=\Gamma_1\wedge\Gamma_2$，其中$\Gamma_{1\vee2}=\{A\subseteq P,A\in\Gamma_1\ or\ A\in\Gamma_2\}$，$\Gamma_{1\wedge2}=\{A\subseteq P,A\in\Gamma_1\ and\ A\in\Gamma_2\}$。假定对$\Gamma_i$存在秘密分享方案$\Sigma_i$，两类方案的秘密值域均是$K=\{0,\cdots,m-1\}$，$m$为正整数。假定参与者$P_i$在方案$\Sigma_i$中的份额空间为$K^{a_{i,j}}$，令$a_j=a_{1,j}+a_{2,j}$。至此，可构造实现$\Gamma_{1\vee2}$和$\Gamma_{1\wedge2}$的秘密分享方案，$P_i$的份额空间为$K^{a_i}$，具体方法如下。

1　份额生成

a）针对访问结构$\Gamma_{1\vee2}$，若分享秘密$k\in K$，只需分别调用Σ_i，将k作为输入，生成份额给参与者即可；

b）针对访问结构$\Gamma_{1\wedge2}$，若分享秘密$k\in K$，选择随机数$k_1\in K$，令$k_2=k-k_1\ mod\ m$，分别调用Σ_i将k_i作为秘密输入，将份额分给参与者。

2　秘密恢复

a）针对访问结构$\Gamma_{1\vee2}$，任意的授权集B可调用方案Σ_i中的恢复算法，进而恢复得到秘密；

b）针对访问结构$\Gamma_{1\wedge2}$，任意的授权集B调用Σ_1和Σ_1中的恢复算法分别得到秘密k_1和k_2，进而恢复秘密k。

若底层方案Σ_i是完备安全的，则上述构造方案也是完备安全的。方案的正确性很容易验证，针对$\Gamma_{1\vee2}$的方案较为简洁易懂，针对$\Gamma_{1\wedge2}$，对任意的非授权集，其至少缺失一个k_i的信息，进而到不到关于秘密k的任何信息。

上述构造方法可看作 MSA 构造的推广，例如，给定一个访问结构$\Gamma=\{B_1,\cdots,B_l\}$，定义$\Gamma_i=\{B_1,\cdots,B_i\}$，显然$\Gamma_i=\Gamma_{i-1}\vee\{B_i\}$，$1\le i\le l$。对任意的$\{B_i\}$，均存在完备的秘密分享方案，即只需要把秘密均匀拆分给$\{B_i\}$中的参与者即可。利用上述单调电路构造即实现了访问结构Γ的秘密分享方案，这种构造与 MSA 构造是等价的。

3.3.4　单调张成方案

目前，大多数设计的秘密分享方案均是线性的，即份额的分发过程可看作线性映射。具体而言，有限域F上的一个线性秘密分享方案，其秘密的值域为F，参与运算的随机向量为F上的向量，每个份额也可看作F上的向量，并且份额向量的每个分量均是由秘密和随机向量的固定线性组合得到。

线性秘密分享方案的刻画可以用单调张成方案 MSP（monotone span programs）描述，利用矩阵描述线性方案的线性映射。另一方面，一个 MSP 也同时蕴含了其实现的秘密分享方案的访问结构。根据已有研究成果，线性秘密分享方案和单调张成方案是等价的。MSP 的具体定义如下[34]。

单调张成方案可描述为一个三元组$\mathcal{M}=(F,M,\rho)$，其中F为域，M为F上大小为$a\times b$的矩阵，$\rho:\{1,\cdots,a\}\to\{P_1,\cdots,P_n\}$为标签映射，将$M$的每行映射给某个参与者。$a$表示$\mathcal{M}$的大小。对任意的$A\subseteq\{P_1,\cdots,P_n\}$，令$M_A$表示$M$的子矩阵：由参与者$A$拥有的行组成。如果$M_B$的行可张成向量$e_1=(1,0,\cdots,0)$，则称$\mathcal{M}$对$B$是可容的。如果对任意的$B\in\Gamma$，　M_B的行可张成向量$e_1=(1,0,\cdots,0)$，则称$\mathcal{M}$对访问结构Γ可容。

一个单调张成方案包含了一个实现其可容访问结构的秘密分享方案。具体描述如下。

令$\mathcal{M}=(F,M,\rho)$为单调张成方案，可容的访问结构为Γ，假定参与方P_j标定M的行数为a_j，则存在实现Γ的秘密分享方案，并且P_j的份额为F^{a_j}的一个向量。这种方案的信息率为$\max_{1\le j\le n}a_j$。具体方法如下。

1　份额生成

a）假定秘密$k\in F$，Dealer 选择F上$b-1$个随机数$r_2,\cdots,r_b$，令$r=(k,r_2,\cdots,r_b)$；

b） 计算$(s_1,\cdots,s_a)=Mr$，将对应参与者P_j的a_j个元素分发作为其份额。

2 秘密恢复

对每个授权子集$B\in\Gamma$,令$N=M_B$，N的所有行可张成向量e_1，即存在向量v，使得$e_1=vN$。授权集B中参与者的份额为Nr。B可恢复出秘密：

$$v(Nr)=(vN)r=e_1\cdot r=k。$$

上述方案是完备安全的。对任意非授权集$T\notin\Gamma$，M_T的行不能张成向量e_1，即$rank(M_T)<rank\begin{pmatrix}M_T\\e_1\end{pmatrix}$，由线性代数的性质可知$|kernel(M_T)|>|kernel\begin{pmatrix}M_T\\e_1\end{pmatrix}|$，即存在向量$w\in F^b$使得$(M_T)w=0,e_1\cdot w=1$。对任意的非授权集$T$的份额$(s_1,\cdots,s_{|T|})$，令$r=(0,r_2,\cdots,r_b)$，满足$(M_T)r=(s_1,\cdots,s_{|T|})$，即$r$是秘密$k=0$的份额生成向量。对任意的$k\in F$，令$r'=r+kw$，则$r'_1=k$，向量$r'$关于秘密$k$生成相同的份额：

$$(M_T)r'=(M_T)(r+kw)=(M_T)r+k(M_T)w=(M_T)r=(s_1,\cdots,s_{|T|}).$$

即任意可能的秘密k均能产生该份额向量。隐私性由此得到保障。

3.3.5 线性码方案

McEliece 于 1981 年指出了 Shamir 体制和 Reed-Solomon 码之间的关系，开创了利用线性码研究秘密分享方案的先河。这种构造针对的是门限结构，对一般的访问结构，也可利用线性码进行方案设计。Massey[35]给出了利用一般线性码设计秘密分享的方法。

令C为有限域F_q上码长为$n+1$，维数为k的线性码，简记为$[n+1,k]$线性码。令$\mathrm{C}^{\perp}$为C的对偶码，设$C^{\perp}$的生成矩阵为$H=(h_0,h_1,\cdots,h_n)$。假定秘密为$s\in F_q$,方案具体描述如下。

1 份额生成

a） Dealer 随机选择向量$u\in F_q^{n-k}$，满足$u\cdot h_0=s$；

b） 计算$u\cdot H=(s,c_1,\cdots,c_n)$，将$c_i$发送给$P_i$作为其份额，$1\le i\le n-1$。

2 秘密恢复

对任意的授权集B，可利用相应份额与C中的码字运算恢复秘密。

该方案为完备安全方案，并且为理想方案。上述方案中，假定参与者的个数为n，这种构造确定的授权集如下。令G为一个$[n+1,k]$线性码C的生成矩阵，在利用G构造的秘密分享方案中，一个参与者的集合$\{P_{i_1},P_{i_2},\cdots,P_{i_m}\}$，$1\le i_1\le\cdots\le i_m\le n$，$1\le m\le n$，为授权集当且仅当在对偶码$C^{\perp}$中存在如下的码字：

$$(1,0,\cdots,0,c_{i_1},0,\cdots,0,c_{i_m},0,\cdots,0),$$

其中至少存在一个j，$1\le j\le m$，使得$c_{ij}\neq 0$。

对一个向量$c=(c_0,c_1,\cdots,c_n)$，其支撑集定义为这样的集合：$\{0\le i\le n,c_i\neq 0\}$。向量的汉明重量定义为向量支撑集的大小。如果向量$c_2$的支撑集包含向量$c_1$的支撑集，则称$c_1$被$c_2$所覆盖。如果一个线性码的非零码字$c$只能覆盖它的倍数而不能覆盖其他任何非零码字，则称该码字c为极小码字。线性码的覆盖问题就是确定出该码的所有极小码字，这个问题一般是一个很困难的问题。由上述分析可知，利用C构造的秘密分享方案中其极小授权集和$\mathrm{C}^{\perp}$中第一个分量为 1 的极小码字有着一一对应关系。但对一个一般性的线性码解决其覆盖问题是很困难的，即确定其对应的访问结构是很困难的。但是某些特殊情况下，这个结构是清楚的。Ding 等人在文献[36]给出了如下的结论。

令C为F_q上一个参数为$[n+1,k]$的线性码，其生成矩阵为$G=[g_0,g_1,\cdots,g_n]$。如果C中的每一个码字均为极小码字，则在其基于$C^{\perp}$的秘密分享方案中，共计有q^{k-1}个极小授权集，并且有下面两个结论：

a） 若g_i是g_0的倍数，则参与者P_i一定出现在每一个极小授权集中；

b） 若g_i不是g_0的倍数，则参与者P_i一定出现在$(q-1)q^{k-2}$个极小授权集中。

对于任意一般性的线性码难以确定出其实现的访问结构，但对于所有码字都是极小码字的线性码，可由上述条件确定出。

3.3.6 多线性方案

在基于单调张成方案的构造中，秘密为有限域的一个元素。基于此类技术思想，可进一步推广设计，将秘密取自有限域中的向量。文献[37,38]提出了此类推广方案，称之为多线性秘密分享。这类方案的主要构造工具是下述单调张成方案的推广形态，即多目标单调张成方案。

一个多目标单调张成方案是一个四元组$\mathcal{M}=(F,M,\rho,V)$，其中F为有限域，M为F上大小为$a\times b$的矩阵，$\rho:\{1,\cdots,a\}\to\{P_1,\cdots,P_n\}$为标签映射，将$M$的每行映射为某个参与者，$V=\{e_1,\cdots,e_c\}\in F^b$为向量集，其中$1\le c<b$，对任意的$A\subseteq\{P_1,\cdots,P_n\}$有以下两种情况之一：

a） M_A的行张成向量集$\{e_1,\cdots,e_c\}$中的每个向量，此时称M可容A;

b） 或M_A的行不张成向量集$\{e_1,\cdots,e_c\}$张成空间中的任何向量。

如果对任意的授权集$B\in\Gamma$，有M可容B，则称M可容Γ。

令$\mathcal{M}=(F,M,\rho,V)$为可容Γ的多目标单调张成方案，$|V|=c$，每个参与者P_j拥有M的a_j行，则存在实现Γ的多线性秘密分享方案。此时，秘密为F^c中的向量，参与者P_j的份额为F^{a_j}中的向量，这种方案的信息率为$\max_{1\le j\le n}a_j/c$。在具体机制构造上，假定秘密为$k_1,\cdots,k_c$，方案描述如下。

1 份额生成

a） Dealer 选择F上$b-c$个随机数$r_{c+1},\cdots,r_b$，令$r=(k_1,\cdots,k_c,r_{c+1},\cdots,r_b)$；

b） 计算份额向量Mr，将标记为P_j的行对应的份额分发给P_j。

2 秘密恢复

对每个授权子集$B\in\Gamma$,令$N=M_B$，N的所有行可张成向量$e_1,\cdots,e_c$，即存在向量$v_1,\cdots,v_c$，使得$e_i=v_iN,1\le i\le c$。授权集B中参与者的份额为 Nr。B可恢复出秘密：

$$v_i(Nr)=(v_iN)r=e_i\cdot r=k_i,1\le i\le c。$$

3.3.7 小结

通用构造方法更多考虑的是秘密分享方案的存在性，针对特定访问结构进行专有设计，可提供更高效的方案。上述几类通用构造方案在结构适用性、信息率等方面各有优劣，具体对比如下表 3.3 所示。

在表3.3中，无向图构造所实现的访问结构有限，仅针对无向图中特定路径的集合。多重赋值方法则可实现任意单调访问结构，但通常情况下方案的信息率很低，即参与方需持有很多份额。单调电路构造则是一种迭代构造思想，需将目标访问结构拆分为一些基础访问结构的异或，具体构造方法也依赖于底层结构的实现方案。单调张成构造方案所实现的结构依赖于方案的矩阵，对任意访问结构构造单调张成方案是一个困难问题，可以说这类构造并不能实现任意访问结构。与之类似，线性码构造需要确定其对偶码中所有极小码字的分布，这个问题只针对特定线性码易于求解，因此并不能实现任意的访问结构。多线性的构造是单调张成构造的直接推广，可分享多个秘密，在其他方面具备与单调张成相同的优缺点。此外，从各个方案的信息率特点可看到，一般性的方案很难

给出信息率较优的实现方案。根据现有研究结果，任意单调访问结构均存在完备安全的秘密分享方案，但一般性的构造实现方法中信息率很低，即每个参与方需持有很多份额，这些份额大约是关于参与者个数n的一个指数级。

表 3.3　一般结构实现方案对比

方案类别	访问结构	依赖组件	信息率	主要工具	秘密类型
无向图	图中两个特定点的路径集合	无	1	比特异或	任意长度的比特串
多重赋值	任意单调访问结构	加性方案	依赖于极小授权集	累积数组	群中元素
单调电路	任意单调访问结构	底层结构实现方案	依赖于访问结构的表示形式	访问结构的异或运算	群中元素
单调张成	矩阵的可容结构	无	依赖于标签映射	有限域上矩阵运算	有限域中元素
线性码	难以明确	无	1	代数编码	有限域中元素
多线性	矩阵的可容结构	无	依赖于标签映射	有限域上矩阵运算	有限域中多个元素

在一般性结构的方案设计方面，一个重要的问题是分析其最优信息率。即需要确定对于任意一个访问结构，其最优信息率是多少。特别地，由于理想访问结构是最优的，还需要刻画什么样的访问结构是理想的。关于最优信息率的求解，在特殊访问结构有了一些研究结果，例如，文献[39,40]给出了仅有 5 个参与者访问结构的最优信息率；文献[41,42]则研究了仅有 6 个参与者图访问结构的最优信息率问题。目前，秘密分享研究中，最优信息率的求解和理想结构的刻画是通用方案设计中两个重要的基本研究问题。虽然当前有关这两个问题取得了很多研究结果，但并没有完全被解决。

4　功能性秘密分享

4.1　可验证方案

秘密分享在应用时需要考虑的一类重要的情形是如何抵抗内部欺骗者。具体而言，在秘密分发阶段，Dealer 有可能针对特定的参与者有偏见（或其他原因），以至于分发给该参与者错误的份额，进而导致该参与者在以后恢复秘密时不能正确恢复；另一种情形是存在被敌手控制的恶意参与者，即当一个授权集合尝试恢复秘密时，某些恶意参与者提供伪造、错误的份额，导致正常的秘密无法恢复。同时恶意参与方可能又得到了其他参与方的正确份额，进而恶意参与者自己可以恢复秘密。针对这种应用场景，需要设

计一种可以对份额的正确性进行验证的秘密分享方案，即可验证的秘密分享体制（Verifiable Secret Sharing，简记为VSS）。这类体制需满足以下两个功能：

a) 参与者收到份额后可利用Dealer公开的相关值验证自己份额的正确性；

b) 当参与者集合尝试恢复秘密时，参与者之间可以相互验证份额的正确性，并可验证最终恢复秘密的正确性。

Chor 等人[43]于 1985 年提出了可验证秘密分享的概念，用以解决分发者欺骗问题。可验证秘密分享是在基础秘密分享方案之上增加验证算法而形成的。随着研究的进展，目前已提出的诸多VSS 方案也提供了防止分享者欺骗的功能。

从安全模型划分，VSS也可分为计算安全和无条件安全两种，前者一般依赖于困难问题安全假设。目前大多数VSS聚焦于门限结构情形，一般结构的相关研究可参阅文献[44]。

在计算安全VSS方案方面，Feldman 于 1987 年首先提出了不需可信机构的非交互式(t,n)门限VSS 协议[45]，该协议基于Shamir 门限体制和计算离散对数的困难性假设。该方案在半诚实安全模型下，可确保各参与方判断最终的秘密是否正确，但不能抵抗rushing敌手，具体描述如下。

1 份额生成

a) 设p，q为两个大素数，满足$q|(p-1)$，令G_q为 $\mathbb{F}_p^*$的唯一q阶子群，g为G_q的生成元。G_q上的离散对数问题是困难的。设 Dealer 分享的秘密为$s \in \mathbb{F}_q$，Dealer 随机选择多项式 $f(x)=\sum_{k=0}^{t-1} a_k x^k$，这里 $a_0=s$。公开承诺 $C_k = g^{a_k} \bmod p$，$0 \le k \le t-1$；

b) 秘密发送份额 $s_i = f(x_i)$ 给参与者 P_i。

2 份额验证

参与者 P_i 根据收到的份额利用之前的承诺值进行验证：

$$g^{s_i} \bmod p \stackrel{?}{=} \prod_{k=0}^{t-1} C_k^{x_i{}^k}$$

若等式成立，则接受份额 s_i，否则拒绝。

3 秘密恢复

任意包含t个参与者的集合$B=\{P_{i_1},\cdots,P_{i_t}\}$，利用插值法可恢复秘密$s$，并进行验证 $g^s \stackrel{?}{=} C_0$。

在上述方案中，公开承诺值$c_0 = g^{a_0}$中泄露了秘密s的相关信息。为了保证公开信息中不会泄露秘密的任意信息，Pedersen给出了可完美隐藏消息的方案，方案为半诚实安全模型，不可抵抗rushing敌手。该方案可完美隐藏秘密的信息，但每个参与者需要持有两个份额。

具体描述如下[46]：

1 份额生成

a) 设p，q为两个大素数，满足$q|(p-1)$，令G_q为 $\mathbb{F}_p^*$的唯一q阶子群，G_q上的离散对数问题是困难的。g,h为G_q的两个生成元，$log_g h$ 的值是未知的。设秘密为$s \in \mathbb{F}_q$，Dealer 随机选取一个 $k \in_R \mathbb{F}_q$，构造两个随机多项式

$f(x)=\sum_{i=0}^{t-1}a_i x^i$，$g(x)=\sum_{i=0}^{t-1}b_i x^i$，其中$a_0=s$，$b_0=k$，公开承诺值$C_i=g^{a_i}h^{b_i} \bmod p$，$0\le i\le t-1$；

b) 参与者的份额为(s_i,k_i)，$s_i=f(x_i)$，$k_i=g(x_i)$。

2 份额验证

参与者收到份额后可验证：

$$g^{s_i}h^{k_i} \stackrel{?}{=} \prod_{l=0}^{t-1} C_l^{x_i{}^l}$$

若等式成立则接受份额。

3 秘密恢复

任意包含t个参与者的集合$B=\{P_{i_1},\cdots,P_{i_t}\}$，利用插值法可恢复秘密$s$和$k$。并验证等式$C_0=g^s h^k$是否成立。

上述两类秘密分享方案的可验证性均依赖于离散对数的困难性，可基于椭圆曲线群上的离散对数困难问题给出不同的描述方式。

令$\mathcal{Z}$为有限域$\mathbb{F}_p$上的椭圆曲线群，阶数为素数q,G为$\mathcal{Z}$的生成元。Feldman 可验证秘密分享描述如下。

1 份额生成

a) 设 Dealer 分享的秘密为$s\in\mathbb{F}_q$,Dealer 随机选择多项式 $f(x)=\sum_{k=0}^{t-1}a_k x^k$，这里 $a_0=s$。公开承诺$C_k=[a_k]G$，$0\le k\le t-1$；

b) 秘密发送份额 $s_i=f(x_i)$ 给参与者 P_i。

2 份额验证

参与者 P_i 根据收到的份额利用之前的承诺值进行验证：

$$[s_i]G \stackrel{?}{=} \sum_{k=0}^{t-1}[x_i^k]\,C_k$$

若等式成立，则接受份额 s_i，否则拒绝。

3 秘密恢复

任意包含t个参与者的集合$B=\{P_{i_1},\cdots,P_{i_t}\}$，利用插值法可恢复秘密 s，并进行验证 $[s]G \stackrel{?}{=} C_0$。

表 4.1 展示了现有无条件安全门限 VSS 在分享阶段的轮数对比。

表 4.1 无条件安全门限 VSS 方案对比

方案	n	总轮数	广播轮数	底层方案	运算域	复杂度
[49]	$n>3t$	7	5	Shamir	有限域	poly(n,t)
[48]	$n>3t$	5	3	Shamir	有限域	poly(n,t)
[48]	$n>3t$	4	3	Shamir	有限域	poly(n,t)
[48]	$n>3t$	3	2	Replicate	群	exp(n,t)
[50]	$n>3t$	3	2	Shamir	有限域	poly(n,t)
[51]	$n>3t$	3	1	Shamir	有限域	poly(n,t)

[52]	$n>3t$	3	2	Shamir	有限域	poly(n,t)
[48]	$n>4t$	2	1	Shamir	有限域	poly(n,t)

无条件安全 VSS 方案不依赖于任何计算安全假设，但对敌手结构有着严格的要求。现有研究成果表明，信息论安全的门限 VSS 方案要求$n \geq 3t+1$[47]。在同步通信模型中，方案的效率一般通过轮数衡量，Gennaro[48]给出了无条件安全 VSS 通信复杂度的下界结论：

a) 不存在轮数为 1 的无条件安全 VSS；

b) 若轮数为 2，则存在无条件安全 VSS 当且仅当$n>4t$；

c) 若轮数大于等于 3，则存在无条件安全 VSS 当且仅当$n>3t$。

因此，无条件安全门限 VSS 的最优通信轮数为 3 轮。目前无条件安全门限 VSS 现有设计方法中，秘密的恢复均需要一轮，主要差别在于分享阶段。方案复杂度大多数是关于n和t的多项式时间。

对于$n>3t$，最优的通信轮数为 3，在实用中可选择 AKP 方案[52]，该方案在同步通信模型下，可抵抗恶意敌手、静态敌手，方案描述如下。

基础协议 wcom：

1 Dealer 和每个参与方并行执行以下过程：

a) Dealer 计划共享秘密$g(x)$，选择随机的对称二变量多项式$G(x,y)$，该多项式关于每个变量的次数至多为t，并满足$G(x,0)=g(x)$。Dealer 将$g_i(x)=G(x,i)$发送给参与者P_i；

b) 每个参与者P_i选择一个次数至多为t的随机多项式$r_i(x)$，将$r_{ij}=r_i(j)$发送给P_j；

2 每个参与者P_i令其份额为$s_i=g_i(0)$。对每一对(i,j)，参与者P_i和P_j分别广播$m_i(x)=g_i(x)+r_i(x)$和$m_{ij}=r_{ij}+g_j(i)$；

3 对每一对(i,j)，若$m_i(j)\neq m_{ij}$，则P_i、P_j和 Dealer 分别广播

$$\left(g_i(j),r_i(j)\right),\left(g_j(i),r_{ij}\right),G(i,j);$$

4 局部计算：如果$r_i(j)=r_{ij}$并且$g_i(j)\neq g_j(i)$则称(P_i,P_j)为冲突对。在冲突对中，若Dealer广播的$G(i,j)$不等于$g_i(j)$则将P_i标记为unhappy，同样的情形也标记P_j。令W为所有happy参与者的集合，如果$|W|<n-t$，则标记Dealer为discarded，并将 W 置为空集，将 unhappy 参与者的份额置为⊥。

假定秘密为s，Dealer 选择一个随机的对称二变量多项式$F(x,y)$，该多项式关于每个变量的次数至多为t，并满足$F(0,0)=s$。

1 dealer 和每个参与方并行执行以下过程：

a) Dealer 将$f_i(x)=F(x,i)$发送给参与者P_i；

b) 每个参与者P_i选择一个次数至多为t的随机多项式$h_i(x)$，充当临时 Dealer 角色将该多项式作为秘密调用基础协议 wcom，将该过程记为 wcomi；

2 对每一对(i,j)，参与者P_i和P_j分别广播$p_i(x)=f_i(x)+h_i(x)$和$p_{ij}=h_{ij}+f_j(i)$，其中h_{ij}为 wcomi 中P_j的份额；同时并行执行 wcomi 中的步骤 2；

3 对每一对(i,j)，若$p_i(j)\neq p_{ij}$，则P_i、P_j和 Dealer 分别广播

$\left(f_i(j),h_i(j)\right),\left(f_j(i),h_{ij}\right),F(i,j)$。同时并行执行 wcomi 中的步骤 3；

4 局部计算：如果$h_i(j) = h_{ij}$并且$f_i(\mathrm{j}) \neq f_j(\mathrm{i})$则称$(P_i, P_j)$为冲突对。在冲突对中，若 Dealer 广播的$F(i,j)$不等于$f_i(j)$则将$P_i$标记为 unhappy，同样的情形也标记$P_j$。令$V$表示 happy 集合。参与者执行 wcomi 中的局部计算步骤，$1 \leq i \leq n$。令W_i表示 wcomi 中的 happy 参与者。如果$p_i(j) \neq p_{ij}$并且$h_i(j) \neq h_{ij}$，则将P_j从W_i中移除。如果$|V \cap W_i| < n - t$或者 b)中的$p_i(j)$不等于 c)中的$f_i(j) + h_i(j)$，对某个j成立，则将P_i从V中移除。如果$|V| < n - t$，遗弃 Dealer，并令$V = P$。否则，对于$P_i \notin V$，基于$\{p_j(i) - h_{ji}\}_{P_j \in V; P_i \in W_j}$恢复出次数为$t$的多项式$f_i(x)$，并重置替换。

最终每个参与者输出$f_i(0)$和$f_i(x)$，并基于插值法或 Berlekamp-Welch 算法[53]恢复出秘密。

4.2 结构动态方案

秘密分享所提供的秘密保护能力依赖于安全环境条件，当敌手策略、能力或安全环境条件发生改变时，方案所提供的保护能力也会改变。例如，敌手的能力变强，可增加收买、腐蚀参与者的个数，此时敌手结构发生了变化，相应的方案也应做调整。一个通常的做法是，将原先所有份额作废，由 Dealer 根据新的访问结构重新下发。但这强烈依赖于 Dealer 在线，对应用不友好。相关学者提出了结构动态可变的方案以解决此类问题。

目前，结构动态方案的研究主要聚焦于门限结构，即在秘密恢复之前，参与者的安全环境以及敌手的安全策略会发生变化。敌手腐蚀能力越来越强，需要动态提高门限阈值。Blundo 等人[54]于 1993 年最早提出了动态变化的这种思想。文献[55]针对基于中国剩余定理的门限秘密分享，利用格密码设计了门限阈值变化方案，并且参与者之间无需安全信道。并进一步在文献[56]利用格基约化算法给出了标准 Shamir 方案的阈值变化设计方法。Martin 等[57]给出了门限可变方案的份额尺寸下界，达到下界的方案被称为最优的门限结构可变方案。文献[58]利用 packed Shamir 方案给出了最优的门限可变的方案，Zhang 等人[59]基于此做了进一步的优化，降低了份额尺寸。Jia 等[60]基于中国剩余定理设计了一种门限可变的方案，密钥恢复阶段的计算效率较高。除了标准的门限结构可变方案之外，相关学者也研究了 ramp 方案的动态化设计，最新的研究成果可参考[61，62]。在门限可变方案中，假设门限由t变为$t' > t$，则小于t'的参与者可获得秘密的部分信息。当前所有提出的无条件安全门限可变方案均具有这个缺点，为了解决该问题，Zhang 等[59]进一步设计了一种计算安全的门限可变方案，文件[60]同样给出了一种基于中国剩余定理的计算安全门限可变方案。

下面描述[59]中给出的最优门限结构可变方案。该方案可抵抗半诚实敌手，更新阶段不需要 Dealer 参与，并且不要求参与者之间相互通信。假设方案的阈值由t变化增加到t'，秘密的值域为$S = F_q^{t'-t+1}$，$x_i \in F_q$为n个不同的非零随机元。

1 份额生成

a) Dealer 随机生成多项式$f_1, \cdots, f_{t'-t+1} \in F_q[x]$：

$$f_1(x) = a_{1,0} + a_{1,1}x + \cdots + a_{1,t-1}x^{t-1},$$

$$f_2(x) = a_{2,0} + a_{2,1}x + \cdots + a_{2,t-1}x^{t-1} + a_{2,t}x^t,$$

$$\cdots$$

$f_{t'-t+1}(x) = a_{t'-t+1,0} + a_{t'-t+1,1}x + \cdots + a_{t'-t+1,t'-1}x^{t'-1}$，并满足：对$i \in [1, t'-t+1]$，$a_{i,i-1} = a_{i+1,i-1} = \cdots = a_{t'-t=1}$，即$f_i(x) = f_{i-1}(x) + x^{i-1}g_{i-1}(x)$，其中$g_{i-1}(x) \in F_q[x]$，次数小于$t$；秘密$s = (a_{t'-t+1,0}, a_{t'-t+1,1}, \cdots, a_{t'-t+1,t'-t})$.

b) 参与者P_i的份额为$s_i = \left(f_1(x_i), f_2(x_i), \cdots, f_{t'-t+1}(x_i)\right) \in F_q^{t'-t+1}$；

2 阈值变化

当门限阈值由t变为t′时，份额更新函数定义为：

$$h_i: (s_{i,1}, s_{i,2}, \cdots, s_{i,t'-t+1}) \to s_{i,t'-t+1};$$

3 秘密恢复

在阈值变化前，对于任意大于等于t的参与者可直接利用插值法恢复出多项式$f_1(x), \cdots, f_{t'-t+1}(x)$,进而确定秘密；当阈值改变到t′时，任意大于等于t′的参与者集合可利用插值法恢复多项式$f_{t'-t+1}(x)$，即可得到秘密值。

4.3 前摄安全方案

在传统(t, n)门限方案中，参与者收到份额后留存直至秘密恢复。如果秘密为长期保存的，则参与者的份额也需要长期保存，这其实增加了敌手攻击的风险。例如，敌手在固定时间段内可攻击获得一个参与者的份额，如果份额长期不变，敌手在一定时间后有可能可获得t个份额，进而恢复秘密。因此传统的门限方案并不适用于长期保存秘密。为此,学者们提出了秘密分享的前摄安全性(proactive security)。在前摄安全方案中，秘密的生命周期被划分成不同的时间段（period），在初始时仍由 Dealer 生成分发份额。而在每个时间段开始时，参与者之间共同更新各自的份额，并擦除旧份额，同时保持原秘密不变。在此条件下，敌手在前一个时间段内获取的份额对下一个时间段是无效的。在传统门限方案中，敌手只需在秘密生命周期内获取足够份额即可，而在前摄安全方案中，敌手必须在固定时间段内获取足够的份额，这就增加了敌手攻击的难度。

Ostrovsky 等[63]最先提出了前摄安全的思想。Herzberg 等[64]提出了第一个前摄安全方案。文献[66,67]则设计多秘密的前摄安全方案。Schultz 等[65]设计了参与者可动态变化的前摄安全门限方案，Baron 等[68]则进一步兼顾考虑方案通信效率问题，设计了新的方法。Maram 等[69]结合区块链提出了一种新的设计方法，该方案允许参与者和阈值均发生变化。Karim[70]设计了不诚实大多数模型下，允许参与者变化的前摄方案。对于一般结构的前摄安全研究可参阅文献[71,72，73]。

Meng[74]等设计了第一个基于中国剩余定理的完备安全前摄门限方案，可抵抗半诚实敌手，方案描述如下。

1 份额生成

Dealer 选择正数$d_0 > 1$，并令$m_0(x) = x^{d_0}$，选择素数p以及两两互素的多项式$m_i(x) \in F_p[x]$，$i = 0,1,\cdots,n$，使得$m_0(x)$与这些多项式均互素，并且所有多项式的次数均等于d_0；dealer 从$S = \{g(x) \in F_p[x] | \deg(g) < d_0\}$中选择秘密$s(x)$，并生成随机多项式$\alpha(x) \in A = \{g(x) \in F_p[x] | \deg(g) < (t-1)d_0\}$，计算

$$f(x) = s(x) + \alpha(x)m_0(x) = s(x) + \alpha(x)x^{d_0}$$

参与者P_i的份额为$s_i(x) = f(x) \bmod m_i(x)$。

2 份额更新

假定秘密保存的时间T可划分为时间段$T_0, T_1, \cdots, T_l$。在每个时间段的开始，参与者运行以下步骤：

a) 每个参与者P_i拥有时间段T_{c-1}的旧份额$s_{i,c-1}$，准备计算时间段T_c的新份额$s_{i,c}(x)$；

b) P_i选择一个随机多项式$\beta_{i,c}(x) \in A$，计算

$$\Delta s_{i,c}^{j}(x) = \beta_{i,c}(x) m_0(x) mod\ m_j(x)$$

并将$\Delta s_{i,c}^{j}(x)$发送给参与者P_j，$1 \le j \le n, j \ne i$，自己留存$\Delta s_{i,c}^{i}(x)$。

c) 参与者P_j收到$n-1$个更新份额后，计算$s_{j,c}(x)$如下：

$$s_{j,c}(x) = \left(s_{j,c-1}(x) + \sum_{i=1}^{n} \Delta s_{i,c}^{j}(x) \right) mod\ m_j(x)$$

d) 每个参与者留存新份额$s_{j,c}(x)$，并擦除旧份额$s_{j,c-1}(x)$和中间值$\Delta s_{i,c}^{j}(x)$

3 秘密恢复

假定t个参与者在时间段T_l计算恢复秘密s(x)，则可利用份额构造如下方程组：

$$\begin{cases} f(x) + \sum_{c=1}^{l} \sum_{i=1}^{n} \beta_{i,c}(x) m_0(x) \equiv s_{1,l}(x) mod m_1(x) \\ f(x) + \sum_{c=1}^{l} \sum_{i=1}^{n} \beta_{i,c}(x) m_0(x) \equiv s_{2,l}(x) mod m_1(x) \\ \cdots \\ f(x) + \sum_{c=1}^{l} \sum_{i=1}^{n} \beta_{i,c}(x) m_0(x) \equiv s_{t,l}(x) mod m_1(x) \end{cases}$$

令$f_l(x) = f(x) + \sum_{c=1}^{l} \sum_{i=1}^{n} \beta_{i,c}(x) m_0(x)$，则$deg\left(f_l(x)\right) < td_0$，并且$deg\left(m_1(x)\right) = \cdots = deg\left(m_t(x)\right) = d_0$，$t$个参与者可利用中国剩余定理恢复求解出$f_l(x)$，进而得到$s(x) = f_l(x) mod\ m_0(x)$。

4.4 鲁棒安全方案

鲁棒性秘密分享方案(robust secret sharing)是指，当所有参与者参与恢复秘密时，即使某些参与者提交错误份额，秘密仍可以极大概率恢复。恢复失败的概率记为δ，并将此类方案记为δ-鲁棒方案。这类方案主要用于抵抗恶意敌手破坏秘密的正常恢复。在应用方面，鲁棒安全方案可用于增强基本秘密分享方案所提供的安全存储能力，即可容忍损坏、篡改份额；另一方面，鲁棒安全方案可用于无条件安全消息传输，可保障窃听信道模型中消息的安全传输。

Shamir 门限方案与 MS 方案是等价的，Shamir 方案具备天然的鲁棒性，并提供了最优的鲁棒性[75]，可抵抗小于$n/3$个错误份额。相关研究成果表明，当不诚实方的比例大于总参与者数量 1/2 时，鲁棒方案是不可能构造的。当不诚实方的比例为 1/3 或更大时，也不可能总是正确地重构秘密（即概率为 1），在这种情况下，小的错误概率是不可避免的。因此当前鲁棒门限方案大多聚焦于$n = 2t + 1$的情形。例如，Rabin 等人[76]于 1989 年利用消息鉴别码(MAC)提出了第一个鲁棒方案,每个参与者分别持有$n-1$个密钥和标签，密钥用于认证其他参与者份额的正确性，标签被其他参与者用于验证该份额的正确性。该方案随后被 Cramer 等人[77]进行了优化，减低份额的尺寸，但重构协议效率较低。Cevallos 等[78]进一步完善了设计，提出了 rushing 敌手模型下的多项

式时间恢复算法。Manurangsi 等[79]则利用无向图顶点确定算法设计了较优的方案，同样可抵抗 rushing 敌手。

Cevallos 等人利用 MAC 算法针对$n = 2t + 1$情形设计了δ-鲁棒方案，$\delta = 2^{-\kappa}$，消息空间为$\{0,1\}^m$时，每个参与者持有的份额大小为$m + O(\kappa + n(logn + logm))$。方案可抵抗 rushing 敌手和半诚实敌手，具体描述如下。

1 份额生成

a) 对秘密$s \in F_{2^m}$，Dealer 利用 Shamir 方案计算$s_1, \cdots, s_n$；对每一对$i, j \in [n]$，选择随机$key_{ij} \in K$，计算$\tau_{ij} = MAC(key_{ji}, s_i)$；

b) Dealer 分发给P_i的份额为$\sigma_i = (s_i, \tau_{i1}, \cdots, \tau_{in}, key_{i1}, \cdots, key_{in})$

2 秘密恢复

a) P_i将$s_i, \tau_{i1}, \cdots, \tau_{in}$发送给重构器$R$；

b) P_i将$key_{i1}, \cdots, key_{in}$发送给重构器$R$；

c) 对每一对$i, j \in [n]$，若$\tau_{ij} = MAC(key_{ji}, s_i)$则$R$令$v_{ij} = 1$，否则为 0；

d) R计算最大的子集$I \subseteq [n]$:

$$\forall i \in I: \left|\left\{j \in I \middle| v_{ij} = 1\right\}\right| = \sum_{j \in I} v_{ij} \geq t + 1$$

e) 令$c = |I| - (t + 1)$为腐蚀参与方的最大值，R利用译码相关算法可计算次数为t的多项式$f(x)$，使得$f(x_i) = s_i$对I中至少$t + 1 + \frac{c}{2}$个参与方成立；如果不存在此类多项式，则输出失败，否则输出$s = f(0)$。

文献[80] 针对$n = 2t + 1$情形则构造了另一种高效的δ-鲁棒秘密分享方案，$\delta = e\left(\frac{t+1}{2^q}\right)^{\frac{t+1}{2}}$，消息空间为$\{0,1\}^m$时，每个参与者持有的份额大小为$m + (2n + t - 2)q$。方案的份额相对更小一些，可抵抗 rushing 敌手，具体描述如下。

令m, q为两个正整数，满足$2^m, 2^q > n$，令$\alpha_i \in F_{2^m} \backslash \{0\}$为$n$个不同的元素，并保证这些元素在$F_{2^q}$中也不相同。

1 份额生成

a) Dealer 选择次数至多为t的随机多项式$f(x) \in F_{2^m}[X]$，满足$f(0) = s$，计算$s_i = f(\alpha_i)$；

b) 如果$q < m$，令$l = m/q$，$s_j = s_{j,1} || \cdots || s_{j,l}$；Dealer 选择随机元素$d_{i,1}, \cdots, d_{i,t}, g_{i,j} \in F_{2^q}$，计算

$$b_{i,j} = \begin{cases} g_{i,j} s_j + \sum_{k=1}^{t} \alpha_i^k d_{j,k}, q \geq m \\ \sum_{k=1}^{l} g_{i,j}^k s_{j,k} + \sum_{k=1}^{t} \alpha_i^k d_{j,k}, q < m \end{cases}$$

$j = 1, \cdots, i-1, i+1, \cdots, n$，$i = 1,2 \cdots, n$。

c) 参与者P_i的份额为$S_i = (s_i, d_{i,1}, \cdots, d_{i,t}, g_{i,1}, \cdots, g_{i,i-1}, g_{i,i+1}, \cdots, g_{i,n}, b_{i,1}, \cdots, b_{i,i-1}, b_{i,i+1}, \cdots, b_{i,n})$

2 秘密恢复

a) 每个参与者P_i向重构器R发送$(s_i', d_{i,1}', \cdots, d_{i,t}')$；

b) 每个参与者P_i向重构器R发送$(g_{i,1}', \cdots, g_{i,i-1}', g_{i,i+1}', \cdots, g_{i,n}', b_{i,1}', \cdots, b_{i,i-1}', b_{i,i+1}', \cdots, b_{i,n}')$；

c） 如果P_i的认证标签可以被P_j接受通过，则R令$v_{ij} = 1, i, j \in \{1,2,\cdots,n\}$，否则设为 0，具体验证等式如下：

$$b'_{i,j} = \begin{cases} g'_{i,j}s'_j + \sum_{k=1}^{t} \alpha_i^k d'_{j,k}, q \geq m \\ \sum_{k=1}^{l} g_{i,j}^{\prime k} s'_{j,k} + \sum_{k=1}^{t} \alpha_i^k d'_{j,k}, q < m \end{cases}$$

d） 令I满足如下条件：

$$\forall i \in I: \left|\{j \in I | v_{ij} = 1\}\right| = \sum_{j \in I} v_{ij} \geq t + 1$$

则I包含了所有的诚实参与者。I中被腐蚀的参与者最多为

$$e = |I| - (t + 1)$$

e） 使用I中的至少$t + 1 + e/2$个参与者的份额，调用 Reed-Solomon 码的纠错算法，恢复出一个次数至多为t的多项式，并满足$f(\alpha_i) = s_i'$；如果不存在这样的多项式，则输出$\perp$，否则输出$s = f(0)$。

针对一般性的访问结构，Kurosawa[81]给出了方案鲁棒性的条件，即访问结构若为Q^3，则该访问结构存在鲁棒性方案。关于通用结构鲁棒方案设计更详细的内容可参阅文献[82]。

4.5 通信高效方案

通信高效（communication efficient）秘密分享方案关注的是这样一类应用场景：需要恢复秘密的用户从参与者中获取份额恢复秘密，但用户比较关注数据传输的通信量，期望在能恢复秘密的前提下，通信传输量最小。在一般的理想秘密分享方案中，恢复秘密时需要从极小授权集中获取每个参与者的份额，利用恢复算法恢复秘密；此时的通信量即为极小授权集的大小（每个参与者持有一份）。现在相关成果表明，可通过增加参与恢复的参与者数量，用于降低实际的通信量，即要求尽可能多的参与者参与恢复，从每个参与者仅获取部分信息。

文献[83]最早提出了通信高效秘密分享的思想，针对固定的门限阈值给出了通信量的下界值，并设计了完备安全的方案达到通信量的下界，即最优通信高效门限方案。文献[84]则进一步丰富了相关成果，针对任意的可变阈值设计了最优通信高效门限方案，并进一步推广到 ramp 方案。该文献给出了额外通信量（CO）的下界：对于(r, t, n)ramp 方案，秘密的长度为k（取秘密的值域空间中k个值），对任意的参与者集合$|I| \geq t$，CO 的下界为

$$CO(I) \geq \frac{kr}{|I| - r}.$$

达到下界的方案具备最小通信量，被称为最优通信方案。当前通信高效方案大多都聚焦于门限结构。

文献[84]针对 ramp 方案给出的最优构造方法适用于静态和半诚实敌手，方案具体描述如下。

1 份额生成

假设秘密为m，m为有限域F_q上长度为$|m| = kb$的向量，要求$|m|$为集合

$\{d - r: t \le d \le n\}$中元素的最小公倍数；其中$k = t - r, b = \frac{|m|}{k}$。令

$D = \{d_1, d_2, \cdots, d_{|D|}\}$,满足$n \ge d_1 \ge d_2 \ge \cdots \ge d_{|D|} = t$，对于$i \in [n - t + 1]$，令

$$p_i = \begin{cases} \frac{kb}{d_1 - r} & i = 1 \\ \frac{kb}{d_i - r} - \frac{kb}{d_{i-1} - r} & i > 1 \end{cases}$$

Dealer 构造b个多项式，其中构造p_i个次数为$d_i - 1$的多项式。对于所有的多项式，低次的r个系数均为随机数。对于$i = 1$，这p_1个多项式的其余系数为秘密信息，秘密信息共有mb个符号，每个多项式携带$d_1 - r$个符号，正好分配完。对于$i > 1$，多项式未确定的$d_i - r$个系数为更高次数多项式（次数大于$d_i - 1$）中d_i到$d_{i-1} - 1$的系数。次数大于$d_i - 1$的多项式共有$\sum_j^{i-1} p_j = \frac{kb}{d_{i-1} - r}$个，需要分享的系数共有

$(d_{i-1} - d_i)\frac{kb}{d_{i-1} - r}$；另一方面，次数为$d_i - 1$的多项式共有$p_i$个，每个待定的系数为

$d_i - r$个，总共待定系数为$(d_i - r)(\frac{kb}{d_i - r} - \frac{kb}{d_{i-1} - r})$，可验证这两个数目相等，即分配合理。最终计算这$b$个多项式在$n$个不同点的值，每个参与者持有$b$个多项式的赋值。

2　秘密恢复

当可获取d_i个参与者的信息时，首先利用插值法可恢复次数为$d_i - 1$的所有多项式，进而利用多项式系数间的关系，可确定出次数为$d_{i-1} - 1$的多项式中大于$d_i - 1$的系数。再利用次数为$d_{i-1} - 1$的多项式的赋值，可恢复出所有次数为$d_{i-1} - 1$的多项式。继续迭代最终可恢复所有次数为$d_1 - 1$的多项式，即获得了秘密m。整个过程的通信量为$d_i \sum_{j=1}^{i} p_j$，达到了下界最优值。

Bitar[85]等进一步利用 Staircase 线性码设计了最优的通信高效门限方案，但要求将秘密和份额都拆分成小域上的元素。Yan[86]等完善了[83]中的构造方法，利用多项式给出了另一种最优门限构造，方案描述如下。

1　份额生成

令$S = F_q^v$为秘密的集合，v为整数，$q > n + v$为素数次幂。令$x_1, \cdots, x_n \in F_q \backslash \{1, 2, \cdots, v\}$为公开的$n$个不同元素，$s = (r_1, r_2, \cdots, r_v) \in F_q^v$为秘密，$t$为门限阈值。

Dealer 选择v个多项式$f_i(x)$,，次数为$t + i - 2, 1 \le i \le v$，多项式满足：

$f_1(1) = r_1;$

$f_2(1) = r_1, f_2(2) = r_2;$

$f_3(1) = r_1, f_3(2) = r_2, f_3(3) = r_3;$

$\vdots$

$f_v(1) = r_1, f_v(2) = r_2, f_v(3) = r_3, \cdots, f_v(v) = r_v;$

Dealer 将$s_j = (f_1(x_j), f_2(x_j), \cdots, f_v(x_j))$分发给$P_j$作为份额。

2 秘密恢复

假设参与恢复秘密的集合为A，$|A| = l > v, t \le l \le t + v - 1$，假设$A = \{P_1, \cdots, P_l\}$，计算$k = v \bmod l - t + 1$。若$k = 0$，则$P_j$贡献份额

$(f_{l-t+1}(x_j), f_{2(l-t+1)}(x_j), f_{3(l-t+1)}(x_j), \cdots, f_v(x_j))$，参与者可依次恢复多项式

$f_{l-t+1}(x), f_{2(l-t+1)}(x)$直至$f_v(x)$，进而可计算出秘密。若$k \neq 0$，则$P_1, P_2, \cdots, P_{t+k-1}$贡献$(f_{l-t+1}(x_j), f_{2(l-t+1)}(x_j), f_{3(l-t+1)}(x_j), \cdots, f_{v-k}(x_j), f_v(x_j))$，对于$1 \le j \le t + k - 1$；

其余参与者贡献$(f_{l-t+1}(x_j), f_{2(l-t+1)}(x_j), f_{3(l-t+1)}(x_j), \cdots, f_{v-k}(x_j))$，对于$t + k \le j \le l$。

类似地可依次恢复多项式$f_{l-t+1}(x), f_{2(l-t+1)}(x)$直至$f_{v-k}(x)$和$f_v(x)$，最终恢复得到秘密。

4.6 抗泄漏方案

抗泄漏（leakage resilient）秘密分享可容忍非授权集合敌手获取其他参与者份额的部分信息，并保证秘密的安全。目前大多数抗泄漏方案聚焦于局部场景（local）：敌手指定一个非授权集，并对于其余的参与者指定一个泄露函数；函数的输入为这些参与者的份额，输出为固定小数目的比特；敌手可在分发协议完成后获得非授权集的份额以及泄露函数的输出比特。

抗泄漏秘密分享这一思想最早是由 Goyal[87]和 Benhamouda[88]分别提出的，并给出了特定门限阈值的抗泄漏设计方法。而在这之前，抗泄漏的思想在秘密分享领域已经开始了探索，Davi 等[89]构造第一个$(2,2)$秘密分享方案，在抵抗适应性敌手获取份额有界信息条件下，可提供统计意义上安全。Liu 等[90]则设计了抗泄漏的非延展码，该方案可看作具备抗泄漏和非延展性的$(2,2)$秘密分享。Goyal[91]等则针对一般性访问结构，针对非适应性敌手，提出了抗泄漏的秘密分享方案。Kumar[92]等则聚焦于多个参与者的份额联合泄露问题，提出了新的模型的解决方法。Srinivasan 等[93]聚焦于通用门限方案的抗泄漏设计，并针对信息率和抗泄漏信息率提出了几乎最优的方法；他们给出了一种转变方法，可以将任意访问结构的秘密分享方案转变为局部抗泄漏方案，仅损失很小的信息率。

我们在此描述 Srinivasan 的通用转换编译器方法，该方法依赖于强种子提取器（strong seeded extractor），给定种子的情况下，强种子提取器的输出接近均匀分布，提取器的具体示例化可参阅文献[94]。

令消息空间为M，消息比特长度为ρ。访问结构Γ的秘密分享过程为 Share，重构过程为 Rec。$Ext: \{0,1\}^{\eta} \times \{0,1\}^{d} \to \{0,1\}^{\rho}$为强种子提取器。

1 份额分发

a) 假定需要分享的秘密为$m \in M$，利用 Share 算法得到了份额$(Sh_1, \cdots, Sh_n)$；

b) 选择均匀随机的种子$s \in \{0,1\}^{d}$，以及混淆比特串$r \in \{0,1\}^{\rho}$；

c) 对每个$i \in [n]$：选择随机$\omega_i \in \{0,1\}^{\eta}$，计算$Sh_i' = Sh_i \oplus Ext(\omega_i, s)$；

d) 调用$(2, n)$的 Shamir 门限秘密分享，将(s, r)作为秘密生成份额$S_1, \cdots, S_n$；

e） 每个参与者的份额为$(\omega_i, Sh_i' \oplus r, S_i)$。

2 秘密恢复

a） 给定授权集的份额，首先利用$(2，n)$的 Shamir 门限秘密分享恢复算法，得到$(s，r)$；

b） 对每个参与者，计算$Sh_i' = S_i' \oplus r$；并计算$Sh_i = Sh_i' \oplus Ext(\omega_i, s)$；

c） 利用恢复算法 Rec 得到原始消息m。

4.7 小结

基本的秘密分享体制可提供消息的机密性保护这一功能，即针对特定的访问结构，限制可恢复秘密的参与者集合。随着技术的应用，不同场景、不同安全需求对基本的秘密分享提出了更多的功能性要求。可验证性秘密分享方案可视为最早的功能性秘密分享，相关的研究成果和设计方法较为丰富也较为成熟。可验证方案的发展一方面受到多方安全计算协议的设计与应用促进，令一方面也受到了电子投票等行业专用领域安全协议设计的需求。与之相比，结构动态方案和前摄安全方案则更多的聚焦于敌手收买参与者能力的变化，方案设计的初衷更多考虑的是安全模型的多样性。鲁棒性安全方案侧重于份额的存储安全或恶意伪造，可视为增强基本秘密分享方案能力的一种措施。通信高效方案和抗泄漏方案的研究起步相对较晚，但针对典型结构也有一些成熟的设计方法。

值得一提的是，上述功能性秘密分享方案的划分仅仅是按照功能特点进行分类，不同方案之间是可兼容的，即单个方案可同时具备多个功能。例如，可验证方案也可同时具备结构动态、前摄安全等性质，鲁棒安全方案也能可具备通信高效等性质。这些方案的特点和适应性对比如下表所示。

表 4.2 功能性秘密分享方案对比

方案类别	问题聚焦	较为适用场景	参考方法	依赖组件
可验证	腐蚀参与者进行恶意欺骗	需要检验份额有效性和正确性的场景	[46，52]	计算安全下依赖承诺方案
结构动态	敌手腐蚀能力逐渐变强	访问结构动态变化的场景	[59]	计算安全下依赖公钥加密
前摄安全	敌手仅在固定周期内攻击有效	秘密需长期保存的场景	[74]	无
鲁棒安全	抵抗错误份额干扰恢复过程	秘密恢复需具备抗干扰能力的场景	[78]	计算安全下依赖 MAC
通信高效	降低恢复过程通信量	秘密恢复需降低通信量的场景	[84,86]	无
抗泄漏	份额可泄露部分部分信息	秘密份额易泄露部分信息的	[94]	计算安全下依赖种子提取器

		场景		

5　方案对比分析

秘密分享方案种类繁多，第三、四章节针对主流的典型方案和功能性方案进行了梳理。为了更好地理解、使用这些方案，表 5.1 围绕秘密分享的一般性质做了对比分析。值得注意的是，不同类别方案的侧重点不一样，表 5.1 在此仅将一些共性、可对比的性质列出进行分析。其中，“访问结构”是指方案所实现的结构，即能恢复秘密的参与者集合类型；“信息率”是指方案中秘密空间与最大份额空间的比值，可用于衡量方案的存储效率；“安全类别”是指方案是否依赖于数学困难问题，即是计算安全或信息论安全；“完备安全”是指信息论安全的方案能否保证非授权集获取不到关于秘密的任何信息；“同态性”是指在访问结构不变的情况下，方案生成的份额是否具备特定的同态运算功能；“敌手模型”是指方案可抵抗的敌手类型，即静态/适应性敌手、半诚实/恶意敌手等；“依赖组件”是指方案的实现是否依赖于其他密码原语或密码组件（随机数是每个方案必须的，在此不考虑随机数生成组件）；“公开数据”是指方案在分发份额后，是否会公开一些公共信息用于辅助秘密的恢复（参与方身份信息的公开是每个方案必须的，在此不考虑身份信息公开的问题）；“功能特点”是指方案所具备的功能，包括秘密分享的基本功能以及基本功能之外的公开验证等特定功能等。

表 5.1　主流秘密分享方案对比

方案类别	访问结构	信息率	安全类别	完备安全	同态性	敌手模型	依赖组件	公开数据	功能特点
Shamir 方案[5]	(t,n)门限结构	1	信息论安全	是	份额加法同态	静态、半诚实	无	无	基本功能
McEliece 方案[6]	(t,n)门限结构	1	信息论安全	是	份额加法同态	静态、半诚实	无	无	份额纠错
Asmuth-Bloom 方案[7]	(t,n)门限结构	渐进于 1	信息论安全	否	否	静态、半诚实	无	无	基本功能
Mignotte 方案[9]	(t,n)门限结构	渐进于 1	信息论安全	否	否	静态、半诚实	无	无	基本功能
GRS 方案[11]	(t,n)门限结构	渐进于 1	信息论安全	否	否	静态、半诚实	无	无	基本功能
XOR 方案[13]	(t,n)门限结构	1	信息论安全	是	否	静态、半诚实	信息分散算法（IDA）	无	基本功能

CRT 方案[14]	(t,n)门限结构	1	信息论安全	是	否	静态、半诚实	无	无	基本功能
ramp 方案[15]	(r,t,n)门限结构	大于1	信息论安全	否	份额加法同态	静态、半诚实	无	无	基本功能

表 5.1　主流秘密分享方案对比（续）

方案类别	访问结构	信息率	安全类别	完备安全	同态性	敌手模型	依赖组件	公开数据	功能特点
加性方案[16]	(n,n)门限结构	1	信息论安全	是	份额加法同态	静态、半诚实	无	无	基本功能
Kikuchi 方案[17]	(t,n)门限结构	大于1	计算安全	否	份额加法同态	静态、半诚实	信息分散算法IDA	无	基本功能
Tassa 方案[19]	析取/合取分层结构	1	信息论安全	是	份额加法同态	静态、半诚实	无	无	基本功能
Tassa 方案[20]	分块结构	1	信息论安全	是	份额加法同态	静态、半诚实	无	公开部分多项式值	基本功能
Benaloh 方案[4]	无向完全图结构	1	信息论安全	是	份额加法同态	静态、半诚实	无	无	基本功能
多重赋值方案[16]	一般结构	小于1	信息论安全	是	份额加法同态	静态、半诚实	无	无	基本功能
单调电路方案[30]	一般结构	小于1	信息论安全	是	份额加法同态	静态、半诚实	底层结构方案	无	基本功能
单调张成方案[34]	一般结构	小于1	信息论安全	是	份额加法同态	静态、半诚实	无	无	基本功能

线性码方案[35]	一般结构	1	信息论安全	是	份额加法同态	静态、半诚实	无	无	基本功能

表 5.1　主流秘密分享方案对比（续）

方案类别	访问结构	信息率	安全类别	完备安全	同态性	敌手模型	依赖组件	公开数据	功能特点
Feldman 方案[45]	(t,n)门限结构	1	计算安全	否	份额加法同态	静态、半诚实	离散对数求解困难的群	多项式的承诺值	秘密、份额的可验证性
AKP 方案[52]	(t,n)门限结构	1	信息论安全	是	份额加法同态	静态、恶意	无	无	秘密、份额的可验证性
TCSS 方案[59]	(t,n)门限结构	小于1	信息论安全	是	份额加法同态	静态、半诚实	无	无	阈值变化
Cevallos 方案[78]	(t,n)门限结构	小于1	信息论安全	是	否	Rushing、半诚实敌手	消息鉴别码	无	份额容错
CESS 方案[84]	(r,t,n)门限结构	1	信息论安全	是	份额加法同态	静态、半诚实	无	无	通信量最优
Srinivasan 方案[93]	一般结构	小于1	计算安全	否	否	静态、半诚实	种子提取器	无	抗信息泄露

6　应用与标准化现状

6.1　应用场景

秘密分享作为一项数据拆分的密码技术，可为数据存储和流通提供有效的防护方法。作为密码原语，秘密分享可用于设计更高层次的密码协议，例如门限密码和多方安全计

算等。作为单独的数据保护方法，秘密分享可与其他技术融合使用，提供更好的数据隐私保护解决方法，例如与深度学习和区块链等技术的融合。另外，秘密分享也可与具体场景结合，用于设计专用场景协议，例如电子拍卖协议和电子投票协议等。

6.1.1 隐私计算

隐私计算为数据的安全流通提供了新的解决思路，可有效挖掘出数据的价值并使数据不出域，满足数据可用不可见的价值流通需求。隐私计算的技术路线主要包括可信计算、联邦学习和多方安全计算。其中，秘密分享可用于设计通用和专用的多方安全计算协议，例如 BGW 协议、门限密码协议等；也可用于设计具体的安全函数计算协议，例如文献[115]针对非线性函数时计算精度有损失、通信轮数过高等问题，提出了一种基于秘密分享的隐私保护计算方法，包括安全比较协议、安全对数协议、安全指数协议等。本小节主要从门限密码和多方安全计算这两个方面简述秘密分享在隐私计算领域的应用。

门限密码学主要聚焦于n个参与方之间共享私钥的场景，使得其中一定阈值数目（例如，大于等于t个）的参与方都可以执行与密钥相关的操作（例如，解密或签名），但少于特定阈值的任何参与方集合都不能执行操作。门限密码是多方安全计算在特定领域的应用，主要实现的功能是分布式的解密或签名，以保护密钥的安全。值得注意的是，采用秘密分享方案共享私钥，然后再重构私钥进行解密或签名的这类解决方案并不适用，因为在第一次操作之后，密钥被重构出，自此以后任何一方都可以自行解密或签名。相比而言，门限密码所需的是t个参与方参与到密钥的每一个操作运算中，不会泄露部分私钥和完整私钥。

门限密码学可用于需要多个签名者来生成签名的应用场景，并且同样适用于高度机密文档仅应由法定人数解密和查看的应用场景中。此外，门限密码可用于提供高级别的密钥保护，即将密钥在多个设备或参与者中共享，通过一种安全协议来实现密钥的运算，在协议的运行过程中不会泄露私钥的任何信息。这在一定程度上增强了密钥保护，使得攻击者必须攻破多个设备才能恢复密钥。门限密码学在 2000 年初期引起了研究者的兴趣，但在随后的十几年里，相关研究成果很少，并没有吸引学者的注意力。但是，最近几年门限密码学的热度在上升。例如，许多区块链创业公司都在部署门限密码以进行密钥保护。例如，ECDSA 的门限签名设计与应用研究备受关注。秘密分享在门限密码学中的应用按照密码机制的不同，可分为分布式密钥生成应用以及门限签名/解密应用。文献[95]采用秘密分享技术设计了分布式$(t，n)$门限 KGC 生成机制，不增加额外的困难问题安全假设。$(t，n)$门限方案使得$t-1$个 KGC 不能共谋恢复用户的私钥。方案计算过程仅需要有限域上加减乘除、椭圆曲线倍点等基本运算。通过交互通信，多方 KGC 分别给用户下发部分私钥，使得用户私钥由用户自己运算得到，并满足 SM9 私钥的标准格式。在门限签名/解密方面，文献[96]设计了商用密码 SM2 的门限签名、解密机制，文献[97]采用秘密分享设计了 ECDSA 的门限签名机制。

多方安全计算的通用计算方法有很多技术路线，其中基于秘密分享的协议可实现算术电路的计算。在此以半诚实模型为例，即参与方均遵守协议的执行，但会尝试通过获得的数据推导更多的信息。半诚实模型下的多方安全计算概念描述如下。令F为一个有限域，假定n个参与方为$P_1,\cdots,P_n$，并且至多t个$(t<n)$参与方为腐蚀参与者。每个参与方P_i持有秘密输入$x_i \in F$，参与方按照协议计算函数$f(x_1,\cdots,x_n)$，要求满足正确性：协议结束后，每个参与者均得到函数输出值$f(x_1,\cdots,x_n)$；以及隐私性：包含$t-1$个参与方的集合T仅能得到输入值$\{x_j\}_{p_j\in T}$和函数输出值推导出的信息，得不到其他任何信息。

下面以 Shamir 方案为例，介绍基于秘密分享的安全加法和乘法运算。令$k_1, k_2 \in F$为两个秘密，分别利用 Shamir (t,n)门限方案生成份额$\{s_{i,1},\cdots,s_{i,n}\}$，$i \in \{1,2\}$，则$s_{1,1}+s_{2,1},\cdots,s_{1,n}+s_{2,n}$为秘密$k_1+k_2$利用 Shamir (t,n)门限方案生成的份额；$s_{1,1}\cdot s_{2,1},\cdots,s_{1,n}\cdot s_{2,n}$为秘密$k_1\cdot k_2$利用 Shamir $(2t+1,n)$门限方案生成的份额。在上述乘法计算时，门限阈值由t扩张到$2t+1$，为了使得乘法份额仍保持阈值t，可通过下述方式计算，此时假定$n=2t+1$。秘密x_1和x_2利用 Shamir (t,n)门限方案生成份额$s_{1,j}, s_{2,j}, 1 \le j \le n$：

a) 每个参与方$\mathrm{P_j}$计算$\mathrm{s_j}=s_{1,j}\cdot s_{2,j}$，利用 Shamir (t,n)门限方案分享s_j，得到的份额记为$q_{j,1},\cdots,q_{j,n}$，并将$q_{j,l}$发送给参与方p_l；

b) 令$\beta_l=\prod_{1\le j\le l, j\ne l}\frac{\alpha_{ij}}{\alpha_{ij}-\alpha_{il}}$，则每个参与方$p_l$计算$u_l=\sum_{j=1}^{n}\beta_j q_{j,l}$，则$u_1,\cdots,u_n$即为$x_1\cdot x_2$的 Shamir (t,n)门限份额。

利用上述协议，可安全计算任意可表示为算术电路的函数，F上具有n个输入的算法电路是一个非循环图，具体以下性质：a)具有唯一出度为 0 的节点，记为输出点；b)具有n个入度为 0 的节点，称为输入门，每个门对应一个变量x_i；c)每个中间节点为乘法门×，或加法门+，每个中间节点的入度为 2。

假定每个参与方P_j持有x_j，令$G_1, G_2, \cdots, G_l$为电路按照一定拓扑顺序排列的所有门，并假设前n个门为输入门，即G_i对应于$x_i, 1 \le \mathrm{i} \le \mathrm{n}$。算术电路的安全计算是确保每个中间值均是$(t,n)$门限方案的份额，在协议的开始阶段，每个参与方将其输入值利用(t,n)门限方案进行分享。按照处理顺序，在第i个门的开始阶段，参与方持有门G_i的两个输入的(t,n)门限份额，在第i个门的结束阶段，参与方持有门G_i的输出值的(t,n)门限份额，在协议结束时，最终结果由所有份额恢复得到。形式化的描述如下：

a) 参与方P_j的输入：$x_j \in F$

b) 初始化：每个参与方P_j利用 Shamir (t,n)门限方案分享秘密x_i，生成的份额记为$q_{i,1}, q_{i,2}, \cdots, q_{i,n}$，并将$q_{i,j}$发送给$p_j$；

c) 计算过程：对于$i=n+1$到l，计算门G_i的输出值份额，假设门G_i的输入边来自于门G_j和G_k，$j,k<i$，并且参与者持有这两个门的输出值份额$q_{j,1},\cdots,q_{j,n}$和$q_{k,1},\cdots,q_{k,n}$；如果G_i为加法门，则每个参与方P_m局部计算$q_{i,m}=q_{j,m}+q_{k,m}$，并将其作为G_i输出值的份额；如果果G_i为乘法门，则利用上述乘法计算协议，得到门G_j和G_k输出值乘积的份额。

d) 计算结果恢复：每个参与方P_m将份额$q_{l,m}$发送给P_1，P_1利用份额$q_{l,1},\cdots,q_{l,t}$调用门限秘密恢复算法，得到计算值，并将计算值发送给所有参与方。

6.1.2 深度学习

深度学习（Deep Learning）是近几年人工智能领域的主要研究方向。深度学习的主要任务是通过构建深度卷积神经网络（Deep Neural Network，DNN）和采用大量样本数据作为输入，最终会得到一个具有强大分析能力和识别能力的模型，该模型包含了 DNN 的构成参数以应用于实际工作。目前深度学习在在图像识别、语音识别已经取得了非凡的突破。分布式深度学习（DDL）提供了一种深度学习的隐私保护解决方案，可实现多方共同学习深度模型，而无需明确共享本地数据集。秘密分享在分布式的深度学习领域发挥了一定的价值，为分布式的深度学习提供了技术基础。

文献[98]采用秘密分享技术设计了一个隐私保护 DDL 框架，使得所有参与者都可以以低通信和低计算成本保持各自本地数据集的私密性，同时能保证学习模型的准确性和高效性。这种方法允许每个参与者将训练过程中的干预参数拆分为份额，并将聚合结

果上传到云服务器。在理论上可证明即使云服务器与某些参与者串通，特定参与者的本地数据集也可以很好地免受半诚实模型下的云服务器以及其他参与者的攻击。协同深度学习是一种用于处理构建更好的深度学习模型所需的训练数据量的方法。在协同深度学习中，中央服务器收集用户数据并运行深度学习算法以获得更准确的模型。然而，集中的训练数据收集会导致严重的隐私泄露问题和训练数据完整性受损。文献[99]采用多秘密分享技术提出了一种保护隐私的协同深度学习模型，将所有训练数据通过会话密钥生成多个份额，并在训练数据发送之前通过哈希算法保证完整性。通过实验验证，这种新模型可以保护训练数据的隐私和完整性，并保持深度学习模型的准确性。

6.1.3 区块链

区块链属于算法高度密集的工程，应用了大量的密码算法。区块链达成的共识本质上是对密码算法所基于的数学难题的共识，所以密码技术可以看作是区块链技术的核心。Shamir 的门限体制已广泛用于各种区块链中用于提供数据的健壮性保护。此外，秘密分享体制也在区块链链上和链下的私钥保护中发挥着举足轻重的作用，例如基于秘密分享的比特币门限签名机制，存储的部分私钥份额丢失或被盗也不会造成任何损失。秘密分享也用于设计区块链上的安全投票协议[100]。文献[101]采用秘密分享技术设计了一种动态更新的区块链节点数据共享机制，使得区块链中的委员会节点可长期持有特定秘密值，并具备份额动态更新的功能。文献[102]探索了如何利用区块链存储秘密，将区块链看作一个长期可信的秘密存储工具，设计了如何将秘密信息存储在区块链中的方法，并设定秘密可恢复的条件。在具体技术上，采用了新型的前摄秘密分享体制作为核心工具，在 POS 公链上给出了可扩展性的构造方法。这种机制可以抵抗动态变化的小规模敌手集合。这种解决方法可以在小规模区块链节点中存储和恢复秘密，并且节点在恢复秘密之前都是彼此不可识别的，具备匿名的特点。这种方案可容忍动态敌手控制 POS 区块链网络中 1/4 的算力，并在参与者规模上具备一定的扩展性。

6.1.4 电子商务

电子商务通常会采用数字签名、身份认证等密码技术保护通信信息的安全。而较为复杂的协议系统也会采用秘密分享作为基本组件，例如电子商务中的电子现金、电子拍卖、公平交换以及电子投票等均使用到了秘密分享[103]。

Stadler[104]指出可公开验证秘密分享技术能够应用于可撤消匿名性的电子现金系统的设计中，可用来以可信机构的公钥可验证地加密用户跟踪信息。在这样的电子支付系统中，通常情况下，用户是不可跟踪的，但如果用户利用系统的匿名性进行非法交易或犯罪活动，那么系统借助于可信机构的帮助，就可找到用户的真实身份。

电子拍卖是电子商务中极为活跃的一个方面，现有相关方案中有很多采用了秘密分享技术。文献[105] 给出了一组密封式拍卖协议，在这些协议中假定了分布式的拍卖代理，投标及确定中标价的过程中利用了基于秘密分享的方法。这些拍卖协议具有几个方面的优点：投标人的标书即使在拍卖结束后仍然是保密的；既适用于第一价位拍卖又适用于第二价位拍卖；效率较高，具有实用价值。文献[106]也是利用基于秘密分享的安全计算提出了适用于第二价位拍卖的网上电子拍卖方案。这一方案能够对除了中标人之外的所有投标人的标书保密，并具有较高的效率。

公平交换协议能够保证在电子交易的过程该中，交易双方能够获得对方要交易的电子商品，保证交易公平进行。即如果交易双方都是诚实的，那么协议运行结束时，各自交换得到对方的东西。文献[107]提出了一种基于公开可验证秘密分享的公平交易协议，

通信双方将自己的秘密份额公开可验证地分享对对方，每次验证通过后执行下一次分享。文献[108]则利用可验证秘密分享设计了一种基于半可信第三方的公平交互协议。文献[109]利用 Pederson 方案设计出一种半可信离线的两方公平交换协议，半可信的第三方只需离线就能完成工作。协议的执行不需要半可信第三方的直接参与，只有当某一方需要帮助时，或协议执行发送错误时才需要第三方的介入。

电子投票使得选举更加经济便捷，应用也越来越普及，例如俄罗斯的大选也采用了电子投票作为选举方式。基于秘密分享的电子投票协议，是电子投票协议设计的典型方法之一[110]。主要思想是将选票份额分给其他参与者，再利用安全求和计算出最终的结果。Schoenmakes[111]率先提出了基于公开可验证秘密分享的电子投票方案；Iftene[112]提出了一种基于中国剩余定理秘密分享的电子投票方法，但仅限于 Yes/no 这一简单情形；Nair 等[113]提出了基于秘密分享的电子投票方案，用位表示选票，使用秘密份额传输和计算，用 Shamir 方案对秘密份额进行求和。Zhao 等[114]提出了基于 Shamir 秘密分享和 K-匿名的电子投票方案，利用秘密分享的同态性，可满足投票的正确、匿名、一致和抗欺骗性。

6.2 相关产品

秘密分享作为一项基础的密码原语，相关产品中很少仅以该技术作为核心研发产品。秘密分享相关产品主要有采用秘密分享技术的隐私计算产品和密钥管理产品。前者以隐私计算平台和系统为主要表现形式，例如，

a) **PrivPy 高效可扩展的通用多方计算平台** 该平台支持基于秘密分享的高效通用计算，安全性上计算引擎使用的是$(2,4)$秘密分享与(n,n)秘密分享引擎；
b) **蚂蚁摩斯隐私计算平台** 该平台的底层协议之一是$(2,3)$秘密分享；
c) **矩阵元 Resetta** 该框架的开源版本主要基于 SecureNN 三方秘密分享协议实现；
d) **富数 FMPC 安全计算产品** 该产品融合了包括秘密分享在内的多方计算、隐匿查询、联邦学习等技术。
e) **Sharemind 多方安全计算平台** 该平台底层协议采用了$(3,3)$加性秘密分享方案用于拆分数据。
f) **Sepior 密钥管理产品** 该产品采用了(t,n)秘密分享方案提供了门限签名、门限密钥生成等密钥管理功能。

采用秘密分享技术的相关密钥管理产品主要有二级密码软模块、移动安全认证系统、门限数字钱包以及门限密钥管理系统等。安全二级密码软模块采用秘密分享对敏感数据参数进行拆分，部分份额分别存储于本地和后台；单侧数据份额泄露不会引发敏感数据的泄露。移动安全认证系统则采用秘密分享技术分散用户私钥，提供了更安全的私钥保护方法。门限数字钱包采用秘密分享将签名资产私钥分散存储，并以门限签名机制控制钱包转账操作。门限密钥管理系统采用秘密分享将密钥分散存储在不同服务器中，提供更健壮的保护机制。例如，GM/T 0034-2014 中明确了 CA 和 KMC 的根密钥需采用密钥分割或秘密分享的方式备份，并采用了$(3,5)$秘密分享机制对 CA 私钥进行拆分保存。GM/T 0028-2014 中明确了安全三级的明文关键安全参数可采用知识拆分方式进行输入或输出。

6.3 标准化现状

在国内标准化方面，目前无秘密分享相关标准。在国际标准化方面，ISO 发布了两项有关秘密分享技术的标准：《ISO/IEC 19592-1:2016 Information technology —

Security techniques — Secret sharing — Part 1: General》和《ISO/IEC 19592-2:2017 Information technology — Security techniques — Secret sharing — Part 2: Fundamental mechanisms》。ISO/IEC 19592-1 规范了秘密分享技术的一般模型和性质要求，在模型方面规范了参与角色，以及秘密分享方案涉及的消息空间、份额数量、访问结构等模型参数；在性质要求方面，提出了消息机密性和可恢复性这两项基本性质要求，并规范了复杂度、信息率等可选性质要求。ISO/IEC 19592-2 规范了秘密分享基本实现机制，包含 Shamir 方案、ramp Shamir 方案、加法方案、一般敌手结构的加法秘密分享方案以及计算安全秘密分享方案等。针对每个方案提出了通用要求和性质要求，规范了消息分享算法以及消息恢复算法。

此外，美国国家标准与技术研究院（NIST）在 2019 年发布了文件 NISTIR 8214《密码原语的门限方案—门限密码学标准化与验证的挑战和机遇》，旨在探索门限方案实现密码原语门限化的可行性，分析了与密码原语门限方案标准化相关的挑战和机遇，并将秘密分享作为门限密码的一项基本技术进行了概述。NIST 进一步在 2020 年发布了文件 NISTIR 8214A《NIST 关于密码原语门限方案规范的路线图》，该文档为 NIST 制定密码原语门限方案标准化的准备工作，同时也分析了秘密分享技术在门限密码方案中的作用。

参考文献

[1] Renvall A., Ding C. A nonlinear secret sharing scheme. ACISP, 56-66, 1996.

[2] Beimel A., Ishai Y. On the Power of Nonlinear Secret-Sharing, IEEE Conference on Computational Complexity, 188-202, 2001.

[3] Beimel A., Weinreb E. Separating the Power of Monotone Span Programs over Different Fields. FOCS, 428-437, 2003.

[4] Beimel A. Secret-sharing schemes: a survey[C]//International conference on coding and cryptology. Springer, Berlin, Heidelberg, 2011: 11-46.

[5] Shamir, A. How to share a secret, Commun. ACM, 22(11), 612-613, 1979.

[6] McEliece, R.J. Sarwate, D. V. On sharing secrets and Reed-Solomon codes, Communications of the ACM, 24(9), 583-584, 1981.

[7] C. A. Asmuth and J. Bloom. A Modular Approach to Key Safeguarding. IEEE Transactions on Information Theory, 29(2):208－210, Mar. 1983. (also in the National Telecommunications Conference, Houstan, Dec. 1980).

[8] Dragan, C.C., T, iplea, F.L.: On the Asymptotic Idealness of the Asmuth-Bloom Threshold Secret Sharing Scheme. Inf.Sci. 463-464, 75-85 (2018).

[9] M. Mignotte. How to Share a Secret? In T. Beth, editor, Workshop on Cryptography, volume 149 of Lecture Notes in Computer Science, pages 371－375, Burg Feuerstein, 1982.

[10] Dragan, C.C.: Security of CRT-based Secret Sharing Schemes. PhD thesis, Alexandru Ioan Cuza University of Iasi, Romania Faculty of Computer Science, (2013).

[11] O. Goldreich, D. Ron, and M. Sudan. Chinese Remaindering with Errors. IEEE Transactions on Information Theory, 46(4):1330－1338, Mar. 2000.

[12] M. Quisquater, B. Preneel, and J. Vandewalle. On the Security of the Threshold Scheme Based on the Chinese Remainder Theorem. In D. Naccache and P. Paillier, editors, Public Key Cryptography, volume 2274 of Lecture Notes in Computer Science, pages 199－210. Springer, 2002.

[13] Chen L, Laing T M, Martin K M. Efficient, XOR-Based, Ideal (t, n)- threshold Schemes. International Conference on Cryptology and Network Security. Springer, Cham, 2016: 467-483.

[14] Ning Y., Miao F., Huang W., Meng K., Xiong Y., Wang X.: Constructing Ideal Secret Sharing Schemes Based on Chinese Remainder Theorem. ASIACRYPT 2018. LNCS 11274, 310-331, 2018.

[15] G. R. Blakley, C. Meadows. Security of Ramp Schemes. Advances in Cryptology, Crypto'84. LNCS 196, 242-268, 1985.

[16] M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structure. In Proc. of the IEEE Global Telecommunication Conf., Globecom 87, pages 99－102, 1987. Journal version: Multiple assignment scheme for sharing secret. J. of Cryptology, 6(1):15-20, 1993.

[17] Kikuchi, R., Chida, K., Ikarashi, D., et al.: ‘Secret sharing with shareconversion: achieving small share-size and extendibility to multiparty computation’, IEICE Trans.., 2015, 98, A(1), pp. 213 - 222

[18] G.J. Simmons, How to (really) share a secret, Springer Lect. Not. Comp. Sc.,1990, 403: 390-448.

[19] T. Tassa, Hierarchical threshold secret sharing, J. of Cryptology, 2007, 20(2): 237-264.

[20] T. Tassa and N. Dyn, Multipartite secret sharing by bivariate interpolation, J. of Cryptology, 2009, 22(2): 227-258

[21] S. Fehr, Efficient construction of the dual span program. Manuscript, May 1999

[22] O. Farràs, J. Martí-Farré, C. Padró.: Ideal multipartite secret sharing schemes, J. Cryptol., 25(3), 434-463, 2012.

[23] O. Farràs, C. Padró, C. Xing, A. Yang.: Natural generalizations of threshold secret sharing, IEEE Trans. Inf. Theory, 60(3), 1652-1664, 2014

[24] Y. Wang, Q. Wu, D. W, et al.: Further ideal multipartite access structures from integer polymatroids, Sci. China Inf. Sci. , 58(7): 1 - 13, 2015

[25] Q. Chen, C. Tang, Z. Lin: Efficient Explicit Constructions of Multipartite Secret Sharing Schemes. ASIACRYPT 2019. LNCS, 11922,505-536, 2019

[26] Q. Chen, C. Tang, Z. Lin: Efficient explicit constructions of compartmented secret sharing schemes, Des. Codes Cryptogr., 87(12): 2913-2940, 2019.

[27] Q. Chen, C. Tang, Z. Lin: Compartmented Secret Sharing Schemes and Locally Repairable Codes, IEEE Trans. Commun., 68(10): 5976-5987, 2020

[28] X. Wang, F-W. Fu and X. Guang: Probabilistic Secret Sharing Schemes for Multipartite Access Structures, IEICE Trans. Fundamentals.,, E99-A(4): 856-862, 2016.

[29] X. Wang, C. Xiang and F-W. Fu: Secret Sharing Schemes for Compartmented Access Structures, Cryptogr. Commun., 9(5): 625-635, 2017.

[30] J. Benaloh, J. Leichter. Generalized secret sharing and monotone functions. Advances in Cryptology, CRYPTO’88, LNCS 403, 27-35, 1990.

[31] M.Iwamoto, H. Yamamoto, H. Ogawa. Optimal multiple assignments based on integer programming in secret sharing schemes. In: ISIT 2004, Chicago, 16 - 16, 2004.

[32] 李 强, 颜 浩, 陈克非. 利用-门限方案实现任意访问结构的新方法. 上海交通大学学报. 38(1), 103-106, 2004.

[33] Q. Li, X. Li, X. Lai, K. Chen. Optimal assignment schemes for general access structures based on linear programming. Des. Codes Cryptogr. 74, 623 - 644, 2015.

[34] M. Karchmer and A. Wigderson. On span programs. In Proc. of the 8th IEEE Structure in Complexity Theory, pages 102 - 111, 1993.

[35] J.L. Massey, “Minimal codewords and secret sharing”, Proceedings of the 6th Joint Swedish-Russian Workshop on Information Theory, 1993: 276-279.

[36] C. Ding and J. Yuan, “Covering and secret sharing with linear codes”, Springer Lect. Not. Comp. Sc., 2003, 2731: 11-25.

[37] M. Bertilsson and I. Ingemarsson. A construction of practical secret sharing schemes using linear block codes. In J. Seberry and Y. Zheng, editors, Advances in Cryptology

- AUSCRYPT ’92, volume 718 of Lecture Notes in Computer Science, pages 67–79. Springer-Verlag, 1993.

[38] M. van Dijk. A linear construction of perfect secret sharing schemes. In A. De Santis, editor, Advances in Cryptology - EUROCRYPT ’94, volume 950 of Lecture Notes in Computer Science, pages 23–34. Springer-Verlag, 1995.

[39] W. Jackson, K. M. Martin. Perfect Secret Sharing Schemes on Five Participants. Des. Codes Cryptogr. 9, 267–286, 1996.

[40] C. Padró, L. Vázquezb, A. Yang. Finding lower bounds on the complexity of secret sharing schemes by linear programming. Discrete Appl. Math. 161, 1072–1084, 2013.

[41] M. V. Dijk, On the information rate of perfect secret sharing schemes, Des. Codes Cryptogr. 6, 143–169, 1995.

[42] M. Gharahi, M. H. Dehkordi. The complexity of the graph access structures on six participants. Des. Codes Cryptogr. 67 (2), 169-173, 2013.

[43] Chor B, Goldwasser S. Verifiable secret sharing and achieving si multaneity in the presence of faults. Proceedings of 26 th IEEE symposium on Foundations of computer science. Portland: IEEE, 1985

[44] A. Choudhury, K. Kurosawa, and A. Patra. The Round Complexity of Perfectly Secure General VSS. In ICITS, volume 6673 of Lecture Notes in Computer Science, pages 143–162. Springer, 2011.

[45] Feldman P,A practical scheme for noninteractive verifiable secret shar ing [A] .Proceedings of 28 th IEEE symposium on Foundations of Com puter Science [C] . Canada:IEEE, 1987.

[46] Pedersen T P. Noninteractive and information theoretic secure verifiable secret sharing. CRYPTO, 1991

[47] Anirudh, C., Ashish Choudhury, and Arpita Patra. "A Survey on Perfectly-Secure Verifiable Secret-Sharing." IACR Cryptol. ePrint Arch. 2021 (2021): 445.

[48] R. Gennaro, Y. Ishai, E. Kushilevitz, and T. Rabin. The Round Complexity of Verifiable Secret Sharing and Secure Multicast. In STOC, pages 580–589. ACM, 2001.

[49] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation (Extended Abstract). In STOC, pages 1–10. ACM, 1988.

[50] M. Fitzi, J. A. Garay, S. Gollakota, C. Pandu Rangan, and K. Srinathan. Round-Optimal and Efficient Verifiable Secret Sharing. In TCC, volume 3876 of Lecture Notes in Computer Science, pages 329–342. Springer, 2006.

[51] J. Katz, C. Y. Koo, and R. Kumaresan. Improving the Round Complexity of VSS in Point-topoint Networks. Inf. Comput., 207(8):889–899, 2009.

[52] B. Applebaum, E. Kachlon, and A. Patra. The Round Complexity of Perfect MPC with Active Security and Optimal Resiliency. In FOCS, pages 1277–1284. IEEE, 2020.

[53] F. J. MacWilliams and N. J. A. Sloane. The Theory of Error Correcting Codes. North-Holland Publishing Company, 1978

[54] Blundo, C., Cresti, A., De Santis, A., Vaccaro, U.: Fully dynamic secret sharing schemes. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 110–125. Springer, Heidelberg (1994).

[55] Steinfeld, R., Pieprzyk, J., Wang, H.: Lattice-based threshold-changeability for standard CRT secret-sharing schemes. Finite Fields Appl. 12(4), 653–680 (2006)

[56] Steinfeld2, R., Pieprzyk, J., Wang, H.: Lattice-based threshold changeability for standard shamir secret-sharing schemes. IEEE Trans. Inf. Theory 53(7), 2542– 2559 (2007)

[57] K.M. Martin, J. Pieprzyk, R. Safavi-Naini, H. Wang, Changing thresholds in the absence of secure channels, in: ACISP' 99: Proceedings of the 4th Australasian Conference on Information Security and Privacy, in: Lecture Notes in Computer Science, vol. 1587, Springer, 1999, pp. 177–191

[58] Wang, H., Wong, D.S.: On secret reconstruction in secret sharing schemes. IEEE Trans. Inf. Theory 54(1), 473–480 (2008)

[59] Zhang, Z., Chee, Y.M., Ling, S., Liu, M., Wang, H.: Threshold changeable secret sharing schemes revisited. Theory Comput. Sci. 418, 106–115 (2012)

[60] Xingxing Jia, Daoshun Wang, Daxin Nie, Xiangyang Luo, Jonathan Zheng Sun, A New Threshold Changeable Secret Sharing Scheme Based on the Chinese Remainder Theorem, Information Sciences (2018)

[61] Jian Ding, Changlu Lin, Fuchun Lin:Optimal Threshold Changeable Secret Sharing with New Threshold Change Range. ProvSec 2020: 361-378

[62] Lin F., Ling S., Wang H., Zeng N. (2019) Threshold Changeable Ramp Secret Sharing. In: Mu Y., Deng R., Huang X. (eds) Cryptology and Network Security. CANS 2019. Lecture Notes in Computer Science, vol 11829. Springer, Cham. https://doi.org/10.1007/978-3-030-31578-8_17

[63] Ostrovsky R, Yung M. How to withstand mobile virus attacks. In: Proceedings of the 10th ACM Conference on Principles of Distributed Systems. 1991, 51–59

[64] Herzberg A, Jarecki S, Krawczyk H, Yung M. Proactive secret sharing or: how to cope with perpetual leakage. In: Proceedings of Annual International Cryptology Conference. 1995, 339–352

[65] Schultz D A, Liskov B, Liskov M. MPSS: mobile proactive secret sharing. In: Proceedings of the 27th ACM Symposium on Principles of Distributed Computing. 2008, 458

[66] Zou H, Wang J. Multi-level threshold multi-secret sharing scheme with proactive security. Journal of Computer Applications, 2009

[67] Feng B, Guo C, Li M, Wang Z. A novel proactive multi-secret sharing scheme. International Journal of Network Security, 2015, 17(2): 123–128

[68] Baron J, El Defrawy K, Lampkins J, Ostrovsky R. Communication optimal proactive secret sharing for dynamic groups. In: Proceedings of International Conference on Applied Cryptography and Network Security. 2015, 23–41

[69] S. K. D. Maram, F. Zhang, L. Wang, et al.: Churp: Dynamic-committee proactive secret sharing. Proceedings of the 2019 ACM SIGSA, 2019

[70] Karim Eldefrawy, Tancr`ede Lepoint, and Antonin Leroux. Communicationefficient proactive secret sharing for dynamic groups with dishonest majorities. In ACNS (1), volume 12146 of Lecture Notes in Computer Science, pages 3–23. Springer, 2020.

[71] Dehkordi M H, Mashhadi S, Oraei H. A proactive multi stage secret sharing scheme for any given access structure. Wireless Personal Communications, 2019, 104(1): 491–503

[72] Mashhadi S. Secure publicly verifiable and proactive secret sharing schemes with general access structure. Information Sciences, 2017, 378: 99－108

[73] Nikov V, Nikova S, Preneel B, Vandewalle, J. Applying general access structure to proactive secret sharing schemes. IACR Cryptology ePrint Archive, 2002, 2002: 141

[74] Keju Meng, Fuyou Miao, Yu Ning, et.al., A proactive secret sharing scheme based on Chinese remainder theorem. Frontiers Comput. Sci. 15(2): 152801 (2021).

[75] Mahdi Cheraghchi, Nearly optimal robust secret sharing. Des. Codes Cryptogr. 87(8): 1777-1796 (2019).

[76] Rabin:Tal Rabin and Michael Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority (extended abstract). In 21st Annual ACM Symposium on Theory of Computing, pages 73－85. ACM Press, May 1989.

[77] Cramer :Ronald Cramer, Ivan Damgard, and Serge Fehr. On the cost of reconstructing a secret, or VSS with optimal reconstruction phase. CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science, pages 503－523.

[78] Cevallos :Alfonso Cevallos, Serge Fehr, Rafail Ostrovsky, and Yuval Rabani. Unconditionallysecure robust secret sharing with compact shares. In David Pointcheval and Thomas Johansson, editors, Advances in Cryptology – EUROCRYPT 2012.

[79] Manurangsi P, Srinivasan A, Vasudevan P N. Nearly optimal robust secret sharing against rushing adversaries.Annual International Cryptology Conference. Springer, Cham, 2020: 156-185.

[80] Partha Sarathi Roy, Avishek Adhikari, Rui Xu,et.al., An Efficient Robust Secret Sharing Scheme with Optimal Cheater Resiliency. SPACE 2014: 47-58.

[81] K. Kurosawa. General error decodable secret sharing scheme and its application. Cryptology ePrint Archive, Report 2009/263, 2009. http://eprint.iacr.org/

[82] Martin, Keith M., Maura B. Paterson, and Douglas R. Stinson. Error decodable secret sharing and one-round perfectly secure message transmission for general adversary structures. Cryptography and Communications 3.2 (2011): 65-86.

[83] H. Wang and D. S. Wong, “On secret reconstruction in secret sharing schemes,” IEEE Trans. Inf. Theory, vol. 54, no. 1, pp. 473－480, Jan. 2008.

[84] W. T. Huang et al., “Communication efficient secret sharing,” IEEE Trans. Inf. Theory, vol. 62, no. 12, pp. 7195－7206, Dec. 2016.

[85] R. Bitar and S. E. Rouayheb, “Staircase codes for secret sharing with optimal communication and read overheads,” IEEE Trans. Inf. Theory, vol. 64, no. 2, pp. 933－934, Feb. 2018.

[86] Xingfu Yan, Changlu Lin, Rongxing Lu, Chunming Tang:Design of Secret Reconstruction With Optimal Communication Efficiency. IEEE Commun. Lett. 22(8): 1556-1559 (2018)

[87] Goyal : Goyal, V., Kumar, A.: Non-malleable secret sharing. In: Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, 25－29 June 2018, pp. 685－698 (2018)

[88] BD:Benhamouda, F., Degwekar, A., Ishai, Y., Rabin, T.: On the local leakage resilience of linear secret sharing schemes. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018, Part I. LNCS, vol. 10991, pp. 531－561.

[89] Francesco Davi, Stefan Dziembowski, and Daniele Venturi. Leakage-resilient storage. In International Conference on Security and Cryptography for Networks, pages 121–137. Springer, 2010

[90] Feng-Hao Liu and Anna Lysyanskaya. Tamper and leakage resilience in the split-state model. In CRYPTO, pages 517–532, 2012.

[91] Vipul Goyal and Ashutosh Kumar. Non-malleable secret sharing for general access structures. In CRYPTO, pages 501–530. Springer, 2018.

[92] Ashutosh Kumar, Raghu Meka, Amit Sahai:Leakage-Resilient Secret Sharing Against Colluding Parties. FOCS 2019: 636-660

[93] Akshayaram Srinivasan, Prashant Nalini Vasudevan:Leakage Resilient Secret Sharing and Applications. CRYPTO (2) 2019: 480-509

[94] Guruswami, V., Umans, C., Vadhan, S.P.: Unbalanced expanders and randomness extractors from Parvaresh-Vardy codes. J. ACM 56(4), 20 (2009)

[95] 王现方，涂彬彬.基于 SM9 密钥的门限化处理方法、装置、设备及存储介质.CN 202110327728.5

[96] 尚铭，马原，林璟锵,等. SM2 椭圆曲线门限密码算法. 密码学报，2014, 1(002):155-166.

[97] Ran C , Gennaro R , Goldfeder S , et al. UC Non-Interactive, Proactive, Threshold ECDSA with Identifiable Aborts. ACM CCS '20.

[98] Duan J, Zhou J, Li Y. Privacy-Preserving distributed deep learning based on secret sharing. Information Sciences, 2020, 527: 108-127.

[99] W. S. Lestari, R. Purba, A. Halim and A. Halim,Privacy-Preserving Collaborative Deep Learning Using Verifiable Multi-Secret Sharing Scheme, 2020 3rd International Conference on Mechanical, Electronics, Computer, and Industrial Technology (MECnIT), 2020, pp. 296-301

[100] S. Bartolucci, P. Bernat, and D. Joseph, \SHARVOT: secret share-based voting on the blockchain," Available: http://arxiv.org/abs/1803.04861

[101] S. K. D. Maram, F. Zhang, L. Wang, et al.: Churp: Dynamic-committee proactive secret sharing. Proceedings of the 2019 ACM SIGSA, 2019.

[102] Benhamouda F, Gentry C, Gorbunov S, et al. Can a Blockchain Keep a Secret?, TPMPC, 2020.

[103] 张福泰，赵福祥，王育民. 可验证秘密分享及其应用. 电子学报，2002, 30(10):1519-1525.

[104] Stadler M, Publicly verifiable secret sharing, In Advances in cryptology. EUROCRYPT'96

[105] Harkavy M,Kikuch H,Tygar J D. Electronic auctions with private bids . Proc of the 3 rd USENIX Workshop on ElectronicCommerce . Massachusetts,USA: USENIX, 1998.

[106] Kikuchi H,Harkavy M,Tygar J D.Multiround anonymous auction protocols . Proc. Of the first IEEE workshop on dependable and real time E- Commerce Systems.New York: IEEE, 1998.

[107] 金新娟.基于公开可验证秘密分享的公平交易协议研究.武汉理工大学学报：信息与管理工程版，2005,27(5)，171-173.

[108] Asokan N, Shoup V, Waider M. Optimistic fair exchange of digital signatures. Eurocrypt 98, LNCS 1403:591-606.

[109] 李江华，可验证秘密分享及在电子商务中的应用. 安徽大学，硕士学位论文，2009.

[110] 蒲泓全, 崔喆, 刘霆,等. 安全性电子投票方案研究综述[J]. 计算机科学, 2020, 47(9):8.

[111] Schoenmakes B, A simple publicly verifiable secret sharing scheme and its application to electronic voting. Crypto 99,148-164.

[112] Iftene S, General secret sharing based on the Chinese Remainder Theorem with applications in e-voting. Electronic Notes in Theoretical Computer Science,2007,186(1):67-84.

[113] Nair D G,Binuv P,Kumar G S, An improved e-voting scheme using secret sharing based secure multi-party computation. ICCN-2014:130-137.

[114] Zhao Q Y,Liu Y N. E-voting scheme using secret sharing and K-anonymity ICBWC2017:893-900.

[115] 熊礼治, 周文浩, 夏志华. 一种基于秘密分享的隐私保护计算方法, CN 202011291344.4