密钥共享体制

刘木兰　周展飞　陈小明

(中国科学院系统科学研究所，北京 100080)

摘要　讲述了密钥共享体制的基本概念和数学模型以及同态密钥共享体制，分析了理想存取结构和拟阵之间的对应关系，研究了完全密钥共享体制的最优信息率，讨论了在实际应用中非常重要的多密钥共享和密钥共享体制中的防欺骗问题.

关键词　密钥共享体制　同态密钥共享体制　多密钥共享　拟阵　最优信息率

现代密码体制的设计思想是使体制的安全性取决于密钥. 密钥的泄漏意味着体制已丧失了安全性，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己方也无法从密文恢复明文，这些都是体制设计者所必须解决的问题. 在密码体制中频繁地更换密钥是保证安全的一个方法，但这种方法在大信息量的今天是不现实的，于是就产生了如何选取、交换、安全地存储和发放密钥的问题（简称为密钥管理或共享控制问题）. 在此背景下，针对上述问题，Blakley[1]和 Shamir[2]分别于 1979 年独立地提出了密钥共享的概念，并分别设计了具体的体制. 由于他们为密钥管理提供了一个崭新的思路，加之计算机网络信息安全的需要，因此许多密码学家致力于密钥共享体制的研究.

近些年在美洲密码会议和欧洲密码会议及有关的杂志上，如 IEEE, J. of Cryptology 等，都出现关于密钥共享体制的文章，但由于没有现成的数学工具，理论上的进展比较艰难，特别是系统的结果还不多见.

密钥共享体制所研究的问题可归结为以下几个方面：

(1) 针对一般存取结构，构造实现该存取结构的具有较高信息率的密钥共享体制.

(2) 运用拟阵等数学工具研究理想存取结构的性质. 目前，由于拟阵的研究尚有许多未解决的问题（如拟阵的可表示性），这方面的研究还处于起步阶段.

(3) 存取结构最优信息率的研究. 这方面的研究对于构造实用的密钥共享体制有着重要意义.

(4) 同态密钥共享体制的研究. 这方面的研究包括同态体制的性质、构造及同态体制在密码学其他领域的应用，如门限数字签名、门限认证体制、电子投票方案等.

(5) 多密钥共享. 考虑同一个受托人集分别以不同的存取结构共享多个主密钥的问题，普通密钥共享理论中的许多结果都可以推广到多密钥共享的情形.

(6) 密钥共享中的防欺骗问题. 密钥共享体制的一个基本假设是在恢复主密钥时，所有受托人都给出自己真实的子密钥. 但是，如果某个或某些受托人出示虚假的子密钥，则在他们自己得到真正的主密钥的同时，可以使其他人得到的都是错误的主密钥. 因此，在密钥共享体制中还必须设计防欺骗的机制.

在本文中，我们将针对上面提出的几个方面的问题，介绍和分析密钥共享体制的概念、模型、方法和重要结果.

1 门限体制

门限体制是最早提出的一种密钥共享体制.

设 t, n 为正整数且 $t \leqslant n$. 简单地说, 一个(t, n)门限体制就是一种 n 个受托人的集合(设为 P)共享一个主密钥 s 的方法. 当密钥管理中心 p_0 $(p_0 \notin P)$允许 P 共享主密钥 s 时, 他根据门限体制中设计的算法产生 n 个子密钥(产生子密钥的方法可以是公开的), 并把这些子密钥分别交给 n 个受托人管理. 子密钥的分发是秘密进行的, 每个受托人只知道他自己保管的子密钥, 别的受托人无法知道他的子密钥. 当受托人子集合 $B \subseteq P$ 想恢复主密钥 s 时, 如果$|B| \geqslant t$, 他们可以用密钥管理中心公开的算法和他们的子密钥计算出主密钥 s; 如果$|B| < t$, 他们就无法确定主密钥 s.

从门限体制的设计思想可以看到, 即使有 $t-1$ 个受托人合谋仍无法恢复主密钥, 同时, 即使 $n-t$ 个受托人遗失了子密钥, 其余的 t 个受托人仍然可以恢复主密钥, 这就妥善地解决了密钥管理中密钥的泄漏和遗失这两个问题.

Blakley 和 Shamir 分别于 1979 年独立地构造了门限体制. Blakley 体制给出的算法是基于有限几何的, 而 Shamir 体制则基于多项式插值. 下面详细地介绍一下 Shamir 体制, 关于 Blakley 体制可参见文献[1, 3].

设 $GF(q)$为有限域, 且 $q \geqslant n+1$. 首先, 密钥管理中心 p_0 选取 $GF(q)$中的 n 个不同的非零元, 记为 x_i, $1 \leqslant i \leqslant n$, 然后 p_0 把 x_i 分配给受托人 p_i, $1 \leqslant i \leqslant n$. x_i 并不是子密钥, 它们可以公开.

当密钥管理中心 p_0 想要 P 共享主密钥 $s \in GF(q)$ 时, 他将按以下步骤进行:

(1) p_0 秘密地随机选取 $GF(q)$中的 $t-1$ 个元素 $a_1, a_2, \cdots, a_{t-1}$, 令 $f(x) = s + \sum_{i=1}^{t-1} a_i x^i$.

(2) 对于 $1 \leqslant i \leqslant n$, 计算 $y_i = f(x_i)$.

(3) 对于 $1 \leqslant i \leqslant n$, p_0 秘密地把子密钥 y_i 给 p_i.

当 t 个受托人 $p_{i_1}, p_{i_2}, \cdots, p_{i_t}$ 要恢复主密钥 s, 他们已知 $y_{i_j} = f(x_{i_j})$ $(1 \leqslant j \leqslant t)$, 且 x_{i_j} $(1 \leqslant j \leqslant t)$ 两两不同. 由于 $f(x)$的次数至多为 $t-1$, $y_{i_j} = f(x_{i_j})$ $(1 \leqslant j \leqslant t)$. 利用 Vandermonde 行列式性质, 方程组 $\sum_{k=0}^{t-1} a_k x_{i_j}^k = y_{i_j}$ $(1 \leqslant j \leqslant t)$有唯一解$(a_0 = s, a_1, \cdots, a_{t-1})$, 于是得到主密钥 s.

当 $t-1$ 个受托人想要恢复主密钥 s 时, 首先, 他们可以得到 $t-1$ 个有 t 个未定元的线性方程. 如果假定 $y_0 \in GF(q)$为主密钥, 由于 $y_0 = f(0)$, 他们共可以得到 t 个线性方程, 此时线性方程组的系数矩阵为 Vandermonde 矩阵, 方程组有唯一解. 这说明 $GF(q)$中的任何一个元都可能是主密钥, 因而他们没有得到关于主密钥 s 的任何信息.

2 存取结构和一般密钥共享体制

在 Shamir 的门限体制中, 每个受托人的权限是一样的. 但实际上, 由于受托人的地位和职能的不同, 其权限通常是不相同的. 因此, 我们必须考虑一般的密钥共享体制.

设 P 为受托人集合, A 为 P 的子集族, 如果受托人子集 A 有性质: $A \in \mathsf{A}$ 当且仅当 A 可以恢复主密钥, 则称 A 为 P 上的存取结构, 子集合 $A \in \mathsf{A}$ 为授权集. 同时, 称 $\mathsf{B} = 2^P \setminus \mathsf{A}$ 为 P 上的非存取结构, 子集合 $B \in \mathsf{B}$ 为非授权集. 作为存取结构的特例, $\mathsf{A} = \{A \subseteq P: |A| \geqslant t\}$称为门限

存取结构，其中$|A|$表示集合 A 中元素的个数.

设 $A\in \mathsf{A}$ 且 $A\subseteq B\subseteq P$，由于 B 的一部分受托人集合 A 就可以恢复主密钥，显然 B 也可以恢复主密钥. 即存取结构满足单调性：如果 $A\in \mathsf{A}$ 且 $A\subseteq B\subseteq P$，则 $B\in A$.

设 $\mathsf{A}\subseteq 2^P$ 为 P 上的存取结构，$\mathsf{B}\subseteq 2^P$ 为非存取结构，令

$$\mathsf{A}_{\mathrm{m}}=\{A\in \mathsf{A}:\forall\, B\subset A\Rightarrow B\notin A\},$$

$$\mathsf{B}_{\mathrm{M}}=\{A\in \mathsf{B}:\forall\, B\supset A\Rightarrow B\notin B\}.$$

称 A_{m} 为 P 上的极小存取结构，子集合 $A\in \mathsf{A}_{\mathrm{m}}$ 为极小授权集，B_{M} 为 P 上的极大非存取结构，子集合 $B\in \mathsf{B}$ 为极大非授权集. 对于子集族 $C\subseteq 2^P$，令 $\mathrm{cl}(\mathsf{C})=\{B\subseteq P:\exists A\in \mathsf{C}\ \ \text{st.}\ B\supseteq A\}$，通常称 $\mathrm{cl}(\mathsf{C})$ 是 C 的闭包. 如果 A 是单调的，则 $\mathrm{cl}(\mathsf{A}_{\mathrm{m}})=\mathsf{A}$. 从上面的讨论可以看出存取结构 A 和极小存取结构 A_{m} 相互确定. 因此，在描述存取结构 A 时，通常只需给出 A_{m} 就行了. 另一方面，我们总假设 $\bigcup_{A\in \mathsf{A}_{\mathrm{m}}}A=P$，否则存在 $p\in P\setminus\bigcup_{A\in \mathsf{A}_{\mathrm{m}}}A$，说明 p 的子密钥的信息对恢复主密钥不起作用，这时称存取结构 A 为退化的，反之称为非退化的.

实际上，存取结构是根据需要预先给定的. Ito 等人[4]证明了对于 $A\subseteq 2^P$，存在实现存取结构 A 的密钥共享体制当且仅当 A 满足单调性. 因此，称单调的子集族为存取结构.

陈小明[5]在受托人集上定义了一种关于存取结构的等价关系，以此给出了存取结构化简的方法，简化后的存取结构保持了简化前的存取结构的基本特性，尤其是保持信息率不变.

Ito 等人把实现门限体制的思想推广到一般的存取结构情况，并在 Shamir 体制的基础上构造了实现一般存取结构的密钥共享体制，或者说给出了一个实现一般存取结构的算法. 利用他们的算法，对于任何事先给定的存取结构，都可给出一个实现该存取结构的密钥共享体制，因而一般存取结构的概念是有实际意义的. 1990 年，Benaloh 和 Leichter[6]给出通过设计一种单调逻辑线路(等价于单调逻辑公式)来实现一个存取结构(一个存取结构可能有多个单调逻辑线路来实现)，而后根据逻辑线路图采用一种反向回追的方法，就可以构造出一个实现该存取结构的完全密钥共享体制，这是一个形象直观的方法.

3　密钥共享体制的数学模型

本节给出由 Brickell 和 Davenport[7]提出的密钥共享体制的数学模型.

通常，在密钥共享体制中，主密钥取值的集合称为主密钥空间；同样对于一个受托人 $p\in P$，称他的子密钥取值的集合为 p 的子密钥空间.

定义 3.1　设 $P=\{p_1, p_2, \cdots, p_n\}$ 为受托人集合，$\mathsf{A}\subseteq 2^P$ 为 P 上的存取结构，$S, S_1, S_2,\cdots, S_n$ 为 $n+1$ 个有限集. 对于 $i=1, 2, \cdots, n$，p_i 对应的子密钥随机变量仍用 p_i 表示. 特别地，p_0 表示主密钥对应的随机变量，集合 $\pi\subseteq S\times S_1\times\cdots\times S_n$ 为随机向量$(p_0, p_1,\cdots, p_n)$的概率空间. $\forall\, a\in p$，a 的概率 $P(a)>0$. 实际上，$a=(s_0, s_1, \cdots, s_n)\in p$ 表示对主密钥 $s_0\in S$ 的一种可能的子密钥分配方法，称为密钥分配规则（注意对固定的 s_0 可存在不同的分配规则）. 若 p 满足下列条件，则称 p 为实现存取结构 A 的密钥共享体制：

(1) $\forall\, A\in \mathsf{A}$, $H(S\mid A)=0$;

(2) $\forall\, A\notin \mathsf{A}$, $0<H(S\mid A)\leqslant H(S)$,

其中 $H(\cdot)$ 是熵函数.

设 $A=\{p_{i_1}, p_{i_2}, \cdots, p_{i_k}\} \subseteq P \cup \{p_0\}, k \leqslant n+1$ 且 $i_1 < i_2 < \cdots < i_k$, $\alpha = (a_0, a_1, \cdots, a_n) \in p$, 称 $a(A)=(a_{i_1}, a_{i_2}, \cdots, a_{i_k})$ 为 a 在 A 上的限制. 设 $S'_i = \{a(p_i): a \in p\}\ (1 \leqslant i \leqslant n), S' = \{a(p_0): a \in p\}$, 分别称 S'_i 和 S' 为密钥共享体制的子密钥空间和主密钥空间, 为方便起见, 仍用 S 和 S' 表示主密钥空间和子密钥空间.

定义 3.2 如果密钥共享体制 p 满足

$$H(S \mid A) = H(S), \quad \forall A \notin \mathrm{A},$$

则称 p 为完全的(perfect), 否则称为不完全的.

由信息论的知识可知, 在完全的密钥共享体制中, 非授权集得不到有关主密钥的任何信息, 显然这是我们所希望的. 然而在实际上, 不完全的密钥共享体制是存在的, 但是, 对于任何存取结构 A 都存在实现存取结构 A 的完全密钥共享体制, 只要假设 Ito 体制中的分配规则等概分布, 其给出的体制就是完全的.

在研究密钥共享体制时, 用下面的定义方式[7]说明问题将比较方便.

定义 3.3 设 $P=\{p_1, p_2, \cdots, p_n\}$ 为受托人集合, $\mathrm{A} \subseteq 2^P$ 为 P 上的存取结构, $S, S_1, S_2, \cdots, S_n$ 为 $n+1$ 个有限集. 集合 $p \subseteq S \times S_1 \times \cdots \times S_n$ 满足 $S = \{\alpha(p_0): \alpha \in p\}$, $S_i = \{a(p_i): a \in p\}$, $1 \leqslant i \leqslant n$. 如果 p 满足下列条件, 则称 p 为实现存取结构 A 的弱完全密钥共享体制:

(1) $\forall A \in \mathrm{A}, \forall a, b \in p, a(A) = b(A) \Rightarrow a(p_0) = b(p_0)$;

(2) $\forall A \notin \mathrm{A}, \forall a \in p, s \in S, \exists b \in p$ st. $a(A)=b(A), b(p_0)=s$.

实际上, 定义 3.1 的条件(1)与定义 3.3 的条件(1)是等价的.

Brickell[7]证明了在没有数据扩展的条件下, 弱完全与完全是等价的. 实际上, 由于弱完全体制较完全体制易于处理, 且所得结果对于完全体制同样成立, 因而目前许多研究工作都是针对弱完全体制的. 另一方面, 由于弱完全体制在防止受托人合谋攻击方面性质与完全体制非常接近, 因此在实际应用中同样有着重要意义.

在所有密钥共享体制中, 完全(弱完全)的密钥共享体制把非授权集摆到了与非受托人同等的地位, 从而防止了非授权集对体制的合谋攻击, 加强了体制的安全性. 近些年来, 对密钥共享体制的研究都是围绕完全体制而展开的.

完全性对密钥共享体制是非常关键的要求. 例如, 对由 20 个字符组成的系统最高权限口令, 如果使用由两个人分别掌管前 10 个和后 10 个的共享控制, 则在安全性上是有严重问题的. 因为, 系统的最高权限口令为 20 个字符, 说明 10 个字符不能保证安全, 而分段后, 两个受托人各拥有口令的一半的信息, 因而对他们来说, 还是有背叛的条件. 用密钥共享的理论来解释, 这是一种不完全的密钥共享体制, 有非存取结构 A(两个人中的任何一个所成的集)使得 $H(S \mid A) < H(S)$, 因而非授权集(单个的受托人)掌握了主密钥的大量信息, 很可能成功地攻击主密钥.

我们可以用阵列的形式来表示密钥共享体制, 阵列的每一行就是一个分配规则, 阵列的第 i 列表示 p_i 的子密钥的所有可能的取值. 阵列是可以公开的, 当受托人集合要恢复主密钥时, 他们根据子密钥寻找一个符合条件的分配规则. 如果是授权集, 他们就可以确定主密钥, 反之则不行. 当然, 为了体制的安全性, 密钥空间一般取得很大, 上述阵列也相当大, 这样给搜索分配规则带来很大的困难, 因而在实际使用密钥共享体制时, 通常使用算法来确定主密

钥，如 Shamir 体制.

例 3.1　设 $P=\{p_1, p_2, p_3, p_4\}$为受托人集合，$\mathsf{A}_m = \{\{p_1, p_2\}, \{p_2, p_3\}, \{p_3, p_4\}\}$. 主密钥空间 $S=\{0, 1\}$,子密钥空间 $S' =\{0, 1, 2\}$. 表 1 给出实现极小存取结构 A_m 的密钥共享体制.

首先注意到对于任意一个主密钥存在不同的分配规则，同时尽管极小授权集 A(即 $A \in \mathsf{A}_m$)无法确定分配规则，但它们仍然可以恢复主密钥. 如当 p_1, p_2 的子密钥分别为 1, 1 时，在这个密钥共享体制中尽管有两个不同的分配规则满足条件，但这两个分配规则对应的子密钥相同.

表 1

p_0	p_1	p_2	p_3	p_4
0	0	0	1	1
0	0	0	2	2
0	1	1	2	2
0	1	1	0	0
0	2	2	0	0
0	2	2	1	1
1	0	1	1	2
1	0	2	2	1
1	1	2	2	0
1	1	0	0	2
1	2	0	0	1
1	2	1	1	0

4　理想的存取结构和拟阵

在完全密钥共享体制的研究中，Karnin 等人[8]证明了以下定理：

定理 4.1　设 $P=\{p_1, p_2,\cdots, p_n\}$为受托人集合，A 为非退化存取结构，$p$ 为实现存取结构 A 的完全密钥共享体制，S 为主密钥空间，S_i $(1\leqslant i\leqslant n)$为子密钥空间，则 $H(S_i)\geqslant H(S)$, $1\leqslant i\leqslant n$.

从信息论的角度来看，$H(S)$表示对主密钥空间进行编码后主密钥的最小平均长度($H(S_i)$也如此). 定理 4.1 表明了在完全密钥共享体制中子密钥码字的最小平均长度比主密钥码字的大，即在完全密钥共享体制中存在数据扩散. 出于安全性的考虑，主密钥空间通常取得较大，以防止攻击者的穷尽搜索，因而数据扩散进一步增加了子密钥码字的长度，显然给子密钥的保管带来了困难. 因此，我们希望寻找没有数据扩散的完全体制.

Brickell[9]引进了理想密钥共享体制的概念.

定义 4.1　设 $P=\{p_1, p_2,\cdots, p_n\}$为受托人集合，A 为非退化存取结构，$p$ 为实现存取结构 A 的完全密钥共享体制，S 为主密钥空间且$|S| = m$, S_i $(1\leqslant i\leqslant n)$为子密钥空间. 如果对于 $1\leqslant i\leqslant n$, $|S_i|=|S|$, 则p 称为理想密钥共享体制，A 为 m-理想的. 如果存在正整数 $m\geqslant 2$，使得 A 为 m-理想的，则称 A 为理想的. 如果对于任意正整数 $m\geqslant 2$，A 都是 m-理想的，则称 A 为一致理想的.

如果主密钥空间等概分布，则对于 $1\leqslant i\leqslant n$, $\log_2|S_i|\geqslant H(S_i)\geqslant H(S) = \log_2|S|$, 即$|S_i|\geqslant|S|$, 因此定义 4.1 是自然合理的.

Shamir 体制给出的(t, n)门限存取结构是 q-理想的，其中 q 为素数幂且 $q\geqslant n+1$.

设 A_1, A_2 分别为集合 P_1, P_2 上的存取结构. 如果存在 1-1 映射f: $P_1 \to P_2$，使得 $A\in \mathsf{A}_1$ 当且仅当$f(A)\in \mathsf{A}_2$，则称 A_1 和 A_2 同构，记为 $\mathsf{A}_1 \cong \mathsf{A}_2$. 显然，$\mathsf{A}_1$ 为 m-理想的充要条件是 A_2 为 m-理想的.

如果 p 是理想的密钥共享体制，则 S_i $(1\leqslant i\leqslant n)$与 S 无本质差别，可以用 S 表示主密钥空间和子密钥空间，称为密钥空间.

理想存取结构的研究始于 Brickell 和 Davenport[7]，他们的工作指出了理想存取结构与拟阵之间的内在联系. 关于拟阵可参阅文献[10]. 在叙述重要结果之前，还需要两个定义.

定义 4.2　设 P 为受托人集合，$P' = P\cup\{p_0\}$, p 为 P 上的密钥共享体制. 对于 $A\subseteq P'$ 和 p

$\in P'$，如果 $H(p \mid A) = H(p)$，则称 p 与 A 关于 p 无关；如果 $H(p \mid A) = 0$，则称 p 关于 p 依赖于 A. 进而，对于 $A \subseteq P'$，如果存在 $p \in A$，使得 p 关于 p 依赖于 $A \setminus \{p\}$，则称 A 为关于 p 的相关集. 如果对于任意的 $p \in A$，p 与 $A \setminus \{p\}$ 关于 p 无关，则称 A 为关于 p 的无关集.

定义 4.3 设 P 为受托人集合，A 为 P 上的存取结构，$P' = P \cup \{p_0\}$，设 M = (P', C) 为 P' 上的拟阵，C 为 M 的圈集. 如果

$$\mathsf{A}_{\mathrm{m}} = \{C - \{p_0\} \mid p_0 \in C \in \mathsf{C}\},$$

则称拟阵 M 适合存取结构 A.

Brickell 等人给出了下面的结果：

定理 4.2[7,11] 设 P 为受托人集合，A $\subseteq 2^P$ 为 P 上的非退化存取结构，且 $P' = P \cup \{p_0\}$. 如果 p 为实现 A 的理想密钥共享体制，S 为密钥空间且 $|S| = q \geqslant 2$，$B \subseteq P'$ 是任意给定的子集合，则

(1) 存在连通拟阵 M = (P', C) 适合 A，其中 C 为 M 的圈集；

(2) A 为关于 p 的无关集当且仅当 A 为适合 A 的拟阵 M 的无关集；

(3) $r(A) = \log_m |p(A)|$，其中 $p(A) = \{a(A) \mid a \in p\}$，$r(A)$ 为 A 在拟阵 M 中的秩.

定理 4.3 在定理 4.2 的假设下，如果适合存取结构 A 的连通拟阵 M = (P', C) 在 $GF(q)$ 上可表，$p \in P'$，则极小存取结构 $\mathsf{A}_{\mathrm{m}} = \{C \setminus \{p\} \mid p \in C \in \mathsf{C}\}$ 为理想的.

对于任一实现存取结构 A 的理想密钥共享体制，可以得到相应的适合 A 的拟阵. Martin 给出了由理想存取结构求对应拟阵的算法和如何利用拟阵性质判断 A 是理想的.

(1) 计算 $\mathsf{C}_0 = \{A \cup \{p_0\} : A \in \mathsf{A}_{\mathrm{m}}\}$；

(2) 对于任意 $C_1, C_2 \in \mathsf{C}_0$，计算

$$E(C_1, C_2) = C_1 \cup C_2 \setminus \bigcap_{\{C_3 \in \mathsf{C}_0 \mid C_3 \in C_1 \cap C_2\}} C_3;$$

(3) 令 E 为所有极小的 $E(C_1, C_2)$ 的集合；

(4) 令 C = $\mathsf{C}_0 \cup \mathsf{E}$.

由定理 4.2 和 Martin 的算法可知，对于每个理想的（非退化）存取结构，存在唯一的连通拟阵与之对应. 反之对于每个拟阵 M，是否存在实现非退化存取结构 A 的理想密钥共享体制且 M 为适合 A 的拟阵，Seymour[12] 给出了反例.

Stinson[13] 研究了密钥共享体制的分解结构，刘木兰和周展飞[14, 15] 给出了通过对已有体制进行替换和收缩的方法构造新体制.

5 同态密钥共享体制

在研究密钥共享体制的过程中，Benaloh[16] 发现在 Shamir 体制中，分配规则具有可加性，即任意两个分配规则对应位相加得到的仍然是分配规则. 他们把具有这种性质的体制称为同态体制，并首次运用同态体制构造秘密投票选举体制. 此后，同态体制被广泛地应用于面向群体的密码系统，如非交互式面向数字签名体制、门限认证体制等[17].

下面是同态密钥共享体制的确切定义.

定义 5.1 设 P 为受托人集合，$A \subseteq 2^P$ 为 P 上的（非退化）存取结构. p 为实现存取结构 A 的完全密钥共享体制. 有限乘法封闭集 S，S_i $(1 \leqslant i \leqslant n)$ 分别为主密钥空间和子密钥空间. 对分配规则 $a = (a_0, a_1, \cdots, a_n)$，$b = (b_0, b_1, \cdots, b_n) \in p$ 定义 $a * b = (a_0 b_0, a_1 b_1, \cdots, a_n b_n)$. 如果对于任意

$a, b \in p$, 有 $a*b \in p$, 则称 p 为同态的.

设 P 为受托人集合, $\mathsf{A} \subseteq 2^P$ 为 P 上的存取结构. 如果存在 $A \in \mathsf{A}_m$, 使得 $|A| \neq 1$, 则称 A 为非平凡存取结构[18].

Frankel 等人[18, 19]研究了同态体制, 得到了如下结果:

定理 5.1 设 P 为受托人集合, $\mathsf{A} \subseteq 2^P$ 为非平凡存取结构, p 为实现 A 的完全同态密钥共享体制, 主密钥空间为有限群 S, 则 S 为 Abel 群.

定理 5.2 设 p 为理想同态密钥共享体制, 主密钥空间 S 为有限群, 子密钥空间 S_i $(1 \leqslant i \leqslant n)$ 为有限乘法封闭集, 则对于 $1 \leqslant i \leqslant n$, $S_i \cong S$.

定理 5.3 设 P 为受托人集合, $\mathsf{A} \subseteq 2^P$ 为存取结构. 设 G 为有限 Abel 群, 存在实现 A 以 G 为密钥空间的理想同态密钥共享体制当且仅当对于 G 的任意 Sylow 子群 G', 存在实现 A 以 G' 为密钥空间的理想同态密钥共享体制, 而且存在无限个有限 Abel 群, 对于其中任何一个群 G, 不存在以 G 为密钥空间的理想同态 (t, n) 门限体制, 其中 $n > 2$, $t \geqslant 2$.

刘木兰和周展飞[20]研究了循环群上理想同态密钥共享体制, 他们引进了良好集和环上模拟阵的表示的概念, 完成了循环群上理想同态密钥共享体制的分类. 在此基础上, 给出了图存取结构在循环群上理想同态的充要条件, 并找到了一类存取结构, 它们对有限循环群 G 是 G-理想同态的. 从理论上, 文献[20]对循环群理想同态密钥共享体制的解决是完整的, 但由于环上拟阵表示很难描述, 因此距实际应用有较大距离. 陈小明[21]给出了 Galois 环上模拟阵的一个判别算法.

对于密钥空间为一般的群, 还没有完全解决.

6 最优信息率

完全密钥共享体制信息率的研究最早始于 Benaloh 和 Leichter[6], 他们发现对于某些存取结构, 所有实现这些存取结构的完全密钥共享体制都不是理想的. 例如:

定理 6.1[6] 设 $P = \{p_1, p_2, p_3, p_4\}$ 为受托人集合, $\mathsf{A}_m = \{\{p_1, p_2\}, \{p_2, p_3\}, \{p_3, p_4\}\}$ 为极小存取结构, p 为实现 A_m 的完全密钥共享体制, 则 p 不是理想的.

为了研究完全密钥共享体制的数据扩展程度, Brickell 等人[22]引入了信息率的概念.

定义 6.1 设 P 为受托人集合, $\mathsf{A} \subseteq 2^P$ 为 P 上的 (非退化) 存取结构, S 为主密钥空间, 且 $|S| = m$, S_i $(1 \leqslant i \leqslant n)$ 为子密钥空间. $PS(\mathsf{A}, m)$ 为实现存取结构 A 的完全密钥共享体制, $PS(\mathsf{A}, m)$ 的信息率定义为

$$r(PS(\mathsf{A}, m)) = \min_{p_i \in P} \frac{\log m}{\log |S_i|}.$$

为了刻画存取结构的特点, Blundo 等人[23]引入了最优信息率的概念:

$$r(\mathsf{A}) = \sup \{r(PS(\mathsf{A}, m)): m \geqslant 2 \text{ 为整数}\},$$

$r(\mathsf{A})$ 称为存取结构 A 的最优信息率, 简称存取结构 A 的信息率.

Capocelli 等人[24]首次把信息论的方法引入完全密钥共享体制信息率的研究, 给出了一些存取结构信息率的上界.

在研究存取结构信息率的过程中, Brickell 等人[22]引入了图分解的方法, 在此基础上 Blundo 等人发展了这种方法, 计算了一批图存取结构的信息率.

设 P 为受托人集合, $\mathsf{A}\subseteq 2^P$ 为 P 上的存取结构且对于任意 $A\in \mathsf{A}_m$, $|A|=2$. 以 P 为顶点集作图 T, 使得 p_i, $p_j\in P$ $(i\neq j)$有一条边相连当且仅当$\{p_i, p_j\}\in \mathsf{A}_m$. 这样, 就得到了存取结构与图之间的对应关系, 它们是相互确定的. 我们把与图 T 对应的存取结构 A 称做基于图 T 的存取结构, 或称为图存取结构 T. 此时, $\mathsf{A}_m=E(T)$, 其中 $E(T)$为对应图 T 的边集.

Blundo 等人得到如下结果并构造了信息率不大于 2/3 的图存取结构:

定理 6.2 设 T 为连通图且 T 不是完全多部图, 则$r(T)\leqslant 2/3$.

同时, Blundo 等人[23, 13]讨论了诸如路、圈等图存取结构的信息率. Blundo 等人[25]还改进了一类存取结构的信息率的估计的上界. 特别是他们提出了下面的定义和定理, 由此得到了一种直接从存取结构的组合性质来估计信息率上界的方法, 省略了许多重复的计算过程.

定义 6.2 给定 P 上存取结构 A, 称受托人序列 $B=\{b_1,\cdots, b_m\}$是 A-独立的, 如果 B (看成集合)$\notin$ A 而且存在 P 的子集 A 的非空子集族 X_i, $i=1,\cdots,m$, 使得: 对 $i=1,\cdots,m$, $\{b_1,\cdots,b_i\}\cup X_i\in$ A 且$\{b_1,\cdots,b_{i-1}\}\cup X_i\notin$ A.

定理 6.3 给定 P 的存取结构 A, 如果存在 A-独立的受托人序列 B, 则 A 是授权集时$r(\mathsf{A})\leqslant |A|/(|B|+1)$, A 是非授权集时 $r(\mathsf{A})\leqslant |A|/|B|$.

周展飞在其博士论文[1)]中计算了受托人数为 5 的 156 个存取结构的信息率, 得到其中 136 个存取结构最优信息率的精确值. 同时, 文献[26]也得到了相同的结果(在个别地方的分类方法稍有不同).

7 多密钥共享

在很多情形下, 同一受托人集要共享多个主密钥, 而且不同的主密钥对应不同的存取结构. 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, 但有多种导弹, 因而有多个发射指令, 每个发射指令对应的共享控制的方式是不一样的, 这就是多密钥共享的一个典型环境. Franklin 等人[27]在研究无条件安全的多部计算的通信复杂性时, 也用到了多密钥共享的概念.

当然, 我们可以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, 这种方法的明显缺陷是受托人所需要管理的子密钥太多, 数据量太大.

除文献[28]以外, 多密钥共享体制方面的研究工作多数考虑的是门限存取结构, 多密钥共享体制的一般理论(针对一般存取结构)是 Blundo 等人[29]总结提出的. 他们提出了两种多密钥共享体制的一般模型, 并证明了两者是等价的.

设 P 是受托人集, $S_1,\cdots, S_m$ 是 m 个主密钥空间, 记 $SC=S_1\times\cdots\times S_m$, $P_{SC}(s_1, \cdots, s_m)$ 是 SC 上的概率分布. 对任意的 $p\in P$, 以 $S(p)$表示 p 的所有可能的子密钥的集合(即子密钥空间). 对任意的受托人集 $A=\{p_{i_1},\cdots, p_{i_r}\}$ (此处 $i_1\leqslant i_2\leqslant\cdots\leqslant i_r$), 记 $S(A)=S(p_{i_1})\times\cdots\times S(p_{i_r})$.

定理 7.1 设$(\mathsf{A}_1,\cdots, \mathsf{A}_m)$是 P 上 m 个存取结构的有序组, 一个实现$(\mathsf{A}_1,\cdots, \mathsf{A}_m)$的Ⅰ型完全多密钥共享体制是分配规则集$p\subset S(P)\times SC$ 上的随机向量(要求此随机向量满足 $\forall a\in p$, $p(a)>0$, 为方便起见 p_i 对应的边际随机变量仍然用 p_i 表示), 满足

(1) $\forall A\in \mathsf{A}_i$, $H(S_i|A)=0$;

1) 周展飞. 密钥共享体制——性质结构和构造. 中国科学院系统科学研究所博士论文, 1997

(2) $\forall A \notin \mathsf{A}_i$ 及 $T \subset \{S_1, \cdots, S_m\} - \{S_i\}$, $H(S_i \mid AT) = H(S_i \mid T)$.

注意，以上的条件(1)说明当 A 对存取结构 A_i 是授权集时，A 中的受托人的子密钥的取值可以决定主密钥 s_i 的取值，条件(2)说明 A 对存取结构 A_i 是非授权集时，不含主密钥 s_i 以外的其他任何一组主密钥 T 加上 A 中的受托人的子密钥所含有的主密钥 s_i 的信息量，等于主密钥组 T 所含的主密钥 s_i 的信息量，即原来的主密钥组 T 含有 s_i 的信息量不随 A 中的子密钥的加入而增加.

文献[29]还给出了一种在形式上与单密钥共享体制更为接近的多密钥共享体制的定义. 对于任意的 $A \subset P$，定义 $S_A = \{S_i \mid A \in \mathsf{A}_i\}$，称之为 A-主密钥集. 在定义 7.1 中，将条件(1)和(2)分别改为

(1′) $\forall A \in P$, $H(S_A \mid A) = 0$;

(2′) $\forall A \in P$ 及 $T \subset \{S_1, \cdots, S_m\} - S_A$, $H(T \mid A) = H(T)$, 则称 p 为实现 $\{\mathsf{A}_1, \cdots, \mathsf{A}_m\}$ 的Ⅱ型完全多密钥共享体制.

文献[29]证明，Ⅰ型和Ⅱ型完全多密钥共享体制是等价的，它们都可以作为一般的多密钥共享体制的定义. 单密钥共享体制理论的许多结果在多密钥共享体制上都有相应的推广，例如文献[28]讨论了理想多密钥共享体制及其与拟阵的关系.

8 密钥共享体制中的防欺骗问题

近些年来，许多学者开始考虑密钥共享体制的防欺骗问题，显然在共享控制中，有一些受托人集或单个的受托人可能出示虚假的密钥，欺骗别的受托人，因此密钥共享体制中必须设置防欺骗的机制.

多数的防欺骗的研究工作是针对门限体制的. 在假定欺骗者具有无限的计算能力的条件下，如果一个密钥共享体制能使得欺骗成功的概率不超过某个固定的 e (<1)，则称该体制是无条件安全的. 最早研究门限体制的防欺骗问题的是 McEliece 和 Sarwate[30]，他们利用纠错码理论构造了一种门限密钥共享体制，使得最多含 e 个欺骗者的 $k+2e$ 个受托人能够正确地恢复主密钥.

Tompa 和 Woll[31]考虑的情形是 $k-1$ 个受托人想合谋欺骗一个诚实的受托人，他们证明 Shamir[2]的 (n, k) 门限体制在防欺骗方面很脆弱，因为一个欺骗者(受托人)可以以相当高的概率成功地欺骗 $k-1$ 个诚实的受托人，即他出示一个设计好的虚假的子密钥，如果其他 $k-1$ 个受托人出示真正的子密钥，则他得到真正的主密钥而其他人得到错误的主密钥的概率相当大. 他们还提出了一种在门限体制中防欺骗的算法，即将真正的主密钥空间 S_{legal} 限制为可能的主密钥空间 S 的一个真子集，这时 $k-1$ 个受托人合谋想欺骗一个诚实的受托人成功的概率小于 $1 - k \mid S_{\text{legal}} \mid / \mid S \mid$. 这种方案虽然能够探测到出现了欺骗行为，但不能识别出欺骗者.

Brickell 和 Stinson[32]改进了 Blakley[1]的 (n, k) 门限体制，使得诚实的受托人可以识别出欺骗者，即使只有一个诚实的受托人，其余的 $n-1$ 个受托人想合谋使他得到错误的主密钥，欺骗成功的概率也只是 $\dfrac{n-k+1}{\mid S \mid -1}$. 同时，Rabin 和 Ben-Or[33]也设计了一种基于文献[2]的 (n, k) 门限密钥共享体制，这种体制与 Brickell 和 Stinson[32]的体制有相似的性质，但欺骗成功的概率更

小, $n-1$ 个受托人欺骗一个诚实的受托人成功的概率为 $1-\left(1-\frac{1}{|s|-1}\right)^{n-k+1}$. Carpentieri[34]也设计了一种可以识别欺骗者的门限体制, 其主要特点是体制的信息率比以上两种的要高, 因此更为实用.

最近 Padro 等[35]提出了两种能探测欺骗行为的密钥共享体制, 第 1 种除了能实现门限存取结构外还能实现其他一些存取结构, 它的信息率是 $\frac{1}{2}$, 该文证明在同样的安全性要求下, 这几乎达到了最优信息率. 第 2 种只能实现门限存取结构, 其信息率是 $\frac{1}{3}$, 它能以相当高的概率探测到欺骗行为. 这两种体制中欺骗成功的概率是由主密钥空间的熵决定的一个固定的值.

致谢 本工作为国家自然科学基金资助项目(批准号: 19831070).

参 考 文 献

1 Blakley G R. Safeguarding cryptographic keys. In: Proc AFIPS 1979 Nat Computer Conf, Vol 48. 1979. 313~317

2 Shamir A. How to share a secret. Commun ACM, 1979, 22(11): 612~613

3 万哲先, 刘木兰. 密钥共享体制的几何. 中国计算机学会信息保密专业委员会论文集. 1992. 1~6

4 Ito M, Saito A, Nishizeki T. Secret sharing scheme realizing general access structure. In: Proc IEEE Global Telecommunications Conf, Globecom 87. 1987. 99~102

5 陈小明. 密钥共享体制的存取结构的化简. 科学通报, 1999, 44(15): 1599~1603

6 Benaloh J, Leichter J. Generalized secret sharing and monotone functions. Lecture Notes in Computer Science, 403. Berlin, New York: Springer-Verlag, 1990. 27~35

7 Brickell E F, Davenport D M. On the classification of ideal secret sharing schemes. J Cryptology, 1991, 4(2): 123~134

8 Karnin E D, Greene J W, Hellman M E. On secret sharing systems. IEEE Trans on Inform Theory, 1983, IT-29(1): 35~41

9 Brickell E F. Some ideal secret sharing schemes. J Comb Math Comb Comput, 1989, 6: 105~113

10 Welsh D J A. Matroid Theory. London: Academic, 1976

11 Beimel A, Chor B. Universally ideal secret sharing schemes. IEEE Trans on IT, 1994, IT-40(3): 786~794

12 Seymour P D. On secret sharing matroids. J Comb Theory, Ser B, 1992, 56: 69~73

13 Stinson D R. Decomposition construction for secret sharing schemes. IEEE Trans on IT, 1994, 40: 118~125

14 刘木兰, 周展飞. 理想存取结构的替换. 中国计算机学会信息保密专业委员会论文集, 1998. 174~180

15 刘木兰, 周展飞. 理想存取结构的收缩. 密码与信息, 1998, 3: 1~8

16 Benaloh J C. Secret sharing homomorphisms: keeping shares of a secret secret. Advances in Cryptology-CRYPTO'86. LNCS, Vol 263. New York: Springer-Verlag, 1987. 251~260

17 Desmedt Y, Frankel Y. Shared generation of authenticators and signatures. Advances in Cryptology-CRYPTO'91. LNCS, Vol 576. New York: Springer-Verlag, 1992. 457~469

18 Frankel Y, Desmedt Y, Burmester, M. Non-existence of homomorphic general sharing schemes for some key spaces. Advances in Cryptology-CRYPTO'92. LNCS, Vol 740. New York: Springer-Verlag, 1993. 549~556

19 Frankel Y, Desmedt Y. Classification of ideal homomorphic threshold schemes over finite abelian groups. Advances in Cryptology-EUROCRYPT'92. LNCS, Vol 658. New York: Springer-Verlag, 1993. 25~34

20 刘木兰, 周展飞. 循环群上理想同态密钥共享体制. 中国科学, E 辑, 1998, 28(6): 524~533

21 陈小明. Galois 环上模拟阵的判别算法. 应用数学学报(待发表)

22 Brickell E F, Stinson D R. Some improved bounds on the information rate of perfect secret sharing schemes. J Cryptology, 1992, 5(3): 153~166

23 Blundo C, de Santis A, Stinson D R, et al. Graph decomposition and secret sharing schemes. Advances in Cryptology-CRYPTO' 92. LNCS, Vol 740. New York: Springer-Verlag, 1993. 1~24
24 Capocelli R M, de Santis A, Gargano L, et al. On the size of shares of secret sharing schemes. J Cryptology, 1993, 6(3): 157~169
25 Blundo C, de Santis A, de Simone R, et al. Tight bounds on the information rate of secret sharing schemes. Design Codes and Cryptography, 1997, 11: 107~122
26 Jackson W A, Martin K M. Perfect secret sharing schemes on five participants. Design Codes and Cryptography, 1996, 9: 267~286
27 Franklin M, Yung M. Communication complexity of secure computation. In: Proceedings of 24th Annual ACM Symposium on Theory of Computation. 1992. 699~710
28 Jackson W A, Martin K M, O' Keefe C M. Ideal secret sharing schemes with mutiple secrets. J Cryptology, 1996, 9: 233~250
29 Blundo C, de Santis A, Di Crescenzo G. Multi-secret sharing schemes. In: Advances in Cryptology-CRYPTO' 94. LNCS, Vol 839. New York: Springer-Verlag, 1995. 150~163
30 McEliece R J, Sarwate D V. On sharing secrets and Reed-Solomon codes. Communications of the ACM, 1981, 24: 583~584
31 Tompa M, Woll H. How to share a secret with cheater. J Cryptology, 1988. 1: 133~139
32 Brickell E F, Stinson D R. The detection of cheaters in threshold schemes. SIAM J Disc Math, 1991, 4: 502~510
33 Ben-Or M, Rabin T. Verifiable secret sharing and multipart rotocols with honest majority. In: Proceedings of 21st ACM Symposium on Theory of Computing. 1989. 73~85
34 Carpentieri M. A perfect threshold secret sharing scheme to identify cheaters. Designs, Codes and Cryptography, 1995, 5: 183~187
35 Padro C, Saez G, Villar, J L. Detection of cheater in vector space secret sharing schemes. Designs, Codes and Cryptography, 1999, 16: 57~85

(2000-01-19 **收稿**)