一类不可表示的多部秘密共享拟阵

许静芳[1],崔国华[1],程 琦[2],张 志[1]
(1.华中科技大学计算机学院信息安全实验室,湖北武汉 430074; 2.武汉市数字工程研究所,湖北武汉 430074)

摘 要: 一直以来,理想的存取结构具有的特性是秘密共享领域中主要的开放性问题之一,并且该问题与拟阵论有着密切的联系.多部存取结构是指将参与者集合划分为多个部分,使得同一部分中的参与者在存取结构中扮演等价的角色,由于每个存取结构都可以看作是多部的,于是多部存取结构的特性被广泛地研究.在 EUROCRYPT'07 上,Farras 等人研究了秘密共享方案中理想多部存取结构的特性.他们的工作具有令人振奋的结果:通过研究多部拟阵和离散多拟阵之间的关系,他们得到了多部存取结构为理想存取结构的一个必要条件和一个充分条件,并且证明了一个多部拟阵是可表示的当且仅当其对应的离散多拟阵是可表示的.在文中,他们给出了一个开放性问题:可表示的离散多拟阵具有的特性,即哪些离散多拟阵是可表示的,哪些是不可表示的.本文给出并证明了一类不可表示的离散多拟阵,即给出了一个离散多拟阵为不可表示的离散多拟阵的一个充分条件.我们将这一结论应用于 Vamos 拟阵,于是得到了一族不可表示的多部拟阵,同时我们利用向量的线性相关和线性无关性对 Vamos 拟阵的不可表示性给出了新的证明.

关键词: 理想秘密共享方案; 理想存取结构; 多部存取结构; 多部拟阵; 可表示的多部拟阵; 离散多拟阵
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112 (2010) 01-0117-06

A Family of Non-representable Multipartite Secret Sharing Matroids

XU Jing-Fang[1], CUI Guo-Hua[1], CHENG Qi[2], ZHANG Zhi[1]
(1. *College of Computer Science & Technology, Huazhong University of Science and Technology, Wuhan, Hubei* 430074, *China*;
2. *Wuhan Digital Engineering Institute, Wuhan, Hubei* 430074, *China*)

Abstract: The characterization of the access structures of ideal secret sharing schemes is one of the main open problems in secret sharing and has important connections with matroid theory. Actually, every access structure is multipartite and, hence, in the EUROCRYPT'07, Farras et al dealed with the characterization of ideal multipartite access structures. In their paper, a necessary condition and a sufficient condition for a multipartite access structure to be ideal is obtained. At the same time, they proved that a multipartite matroid is representable if and only if the corresponding discrete polymatroid is representable. In particular, they present an open problem: the characterization of the representable discrete polymatroids, that is, which discrete polymatroids are representable? In this paper, we present a species of non-representable discrete polymatroids, which implies a sufficient condition for a discrete polymatroid to be non-representable. We apply this general result to Vamos matroid and obtain a family of non-representable multipartite matroids. Furthermore, by the linearly dependent and independent vectors, we prove that the Vamos matroid is a non-representable multipartite matroid.

Key words: ideal secret sharing schemes; ideal access structures; multipartite access structures; multipartite matroids; representable multipartite matroids; discrete polymatroids

1 引言

1979 年,Blakley[1] 和 Shamir[2] 分别独立地提出秘密共享的概念.此后,由于秘密共享方案在信息安全领域得到了广泛应用[22~25],秘密共享的理论与模型都得到了迅速发展.简单地说,秘密共享方案就是在多个参与者之间共享一个主秘密,即分发给每个参与者一些相关信息,称为子秘密,使得只有授权集中的参与者才能联合从他们的子秘密中恢复主秘密,同时,非授权集中的参与者联合他们的子秘密不能获得关于主秘密的任何信息.通常称所有授权集的集合为存取结构(设为 Γ),$\min\Gamma=\{A\in\Gamma:\forall\ B\subset A\Rightarrow B\notin\Gamma\}$ 称为最小存取结构,Γ 和 $\min\Gamma$ 是相互唯一确定的.

子秘密的长度是决定秘密共享方案复杂度的主要因素.在所有的秘密共享方案中,子秘密的长度总是大于或等于主秘密的长度.如果每一个子秘密的长度都

收稿日期:2008-10-17;修回日期:2009-03-28
基金项目:国家自然科学基金(No.60403027)

等于主秘密的长度,称该方案为理想的秘密共享方案,理想的秘密共享方案具有的存取结构被称为理想的存取结构.理想的存取结构具有的特性是秘密共享领域中主要的开放性问题之一,并且该问题与拟阵论有着密切的联系.

Brickell[4,18]最先发现了理想秘密共享方案和拟阵之间的联系:每一个理想的存取结构都是与拟阵相关联的,即每一个理想的存取结构都可确定一个拟阵,得到的拟阵称为秘密共享可表示的拟阵.并且每一个可表示的拟阵(即能够被有限域上的一个矩阵所表示)都是秘密共享可表示的拟阵,也就是说,与可表示的拟阵相关联的存取结构均为理想的存取结构.此后,大量的工作用于研究秘密共享可表示的拟阵的特性.其中 Vamos 拟阵是第一个被证明为秘密共享不可表示的拟阵.

所谓多部存取结构是指,将参与者集合划分为多个部分,使得同一部分中的参与者在存取结构中扮演等价的角色.例如,参与者 p_1 和 p_2 属于同一部分,如果将存取结构中的 p_1 与 p_2 互换,则互换后的存取结构等于互换前的存取结构.实际上,每一个存取结构都是多部的,因为我们可以认为每一个参与者构成一个部分,即部分总数等于参与者总数.研究多部存取结构的特性有着广泛的实际应用前景,尤其是部分总数很小而参与者总数很大的情况.因此研究理想多部存取结构的特性被认为是解决上述开放性问题(即理想存取结构具有的特性)的重要途径之一.

多部存取结构的概念最先由 Shamir 在文献[2]中提到,其中称为加权的门限存取结构.此后,Brickell[4,18]和 Simmons[7]以及众多其他学者[25,26]对理想多部存取结构的特性都进行了研究并且为不同种类的多部存取结构构造了理想的秘密共享方案[3~9,18].文献[10]和[11,12]分别独立地给出了二部存取结构的完全特性.文献[13]和[14]先后给出了理想三部存取结构的部分和完全特性.最近,在 EUROCRYPT'07 上,Farras 等人[14]研究了秘密共享方案中理想多部存取结构的特性.他们的工作具有令人振奋的结果:通过研究多部拟阵和离散多拟阵之间的关系,他们得到了多部存取结构为理想存取结构的一个必要条件和一个充分条件,并且证明了一个多部拟阵是可表示的当且仅当其对应的离散多拟阵是可表示的.在文中,他们给出了一个开放性问题:可表示的离散多拟阵具有的特性,即哪些离散多拟阵是可表示的,哪些是不可表示的.在本文中,由多部拟阵与离散多拟阵之间的对应关系,我们给出并证明了离散多拟阵为不可表示的一个充分条件.具体地,我们将这一结论应用于 Vamos 拟阵,于是得到了一族不可表示的多部拟阵(即 Vamos 家族),同时本文利用向量的线性相关和线性无关性对 Vamos 拟阵的不可表示性给出了新的证明.

2 基本概念

在本节我们将对拟阵以及拟阵与理想秘密共享方案之间的联系,多部存取结构以及多部拟阵与离散多拟阵之间的联系作必要的介绍.

2.1 拟阵和理想秘密共享方案

关于拟阵和理想秘密共享方案的相关知识读者可分别参阅文献[15,17]和[16].

一个拟阵 $\mathcal{M}=(\mathcal{Q},\mathcal{I})$ 由有限集合 $\mathcal{Q}$ 以及集合 $\mathcal{I}\subseteq\mathcal{P}(\mathcal{Q})$($\mathcal{P}(\mathcal{Q})$ 为 $\mathcal{Q}$ 的幂集)构成,使得:

(1)$\varphi\in\mathcal{I}$;

(2)若 $I_1\in\mathcal{I}$ 并且 $I_2\subseteq I_1$,则 $I_2\in\mathcal{I}$;

(3)若 $I_1,I_2\in\mathcal{I}$ 并且 $|I_1|<|I_2|$,则一定存在 $x\in I_2-I_1$ 使得 $I_1\cup\{x\}\in\mathcal{I}$.

其中 $\mathcal{Q}$ 称为拟阵 $\mathcal{M}$ 的基础集(ground set),$\mathcal{I}$ 中的元素称为 $\mathcal{M}$ 的无关集(independent sets).元素个数最大的无关集称为拟阵的基(bases).所有的基组成的集合 $\mathcal{B}$ 唯一确定一个拟阵.由文献有,$\mathcal{B}\subseteq\mathcal{P}(\mathcal{Q})$ 为拟阵在 $\mathcal{Q}$ 上的基所组成的集合,当且仅当:

(1).$\mathcal{B}$ 是非空的;

(2)对于任意 $B_1,B_2\in\mathcal{B}$ 且 $x\in B_1-B_2$,一定存在 $y\in B_2-B_1$ 使得 $(B_1-\{x\})\cup\{y\}$ 是 $\mathcal{B}$ 中的元素.

所有的基拥有相等的元素个数,该元素个数记为拟阵 $\mathcal{M}$ 的秩 $r(\mathcal{M})$(rank).非无关集称为相关集(dependent sets).最小的相关集(即不存在一个相关集为它的子集)称为路(circuit).如果对于每两个点 $x,y\in\mathcal{Q}$,都存在一个路 C 使得 $x,y\in C$,则称该拟阵是连通的(connected).对于任意 $X\subseteq\mathcal{Q}$,X 的所有子集中元素个数最大的无关集所拥有的元素个数等于 X 的秩 $r(X)$.显然,$\mathcal{Q}$ 的秩就是拟阵 $\mathcal{M}$ 的秩.拟阵的秩函数 $r:P(\mathcal{Q})\rightarrow\mathbb{Z}$ 满足:

(1)对于任意 $X\subseteq\mathcal{Q}$,有 $0\leqslant r(X)\leqslant|X|$;

(2)r 是单调递增的,即若 $X\subseteq Y\subseteq\mathcal{Q}$,则 $r(X)\leqslant r(Y)$;

(3)对于任意 $X,Y\subseteq\mathcal{Q}$,有 $r(X\cap Y)+r(X\cup Y)\leqslant r(X)+r(Y)$.

设 K 为一个有限域,若存在 K 上的一个矩阵 M,其中 M 的每一列与 $\mathcal{Q}$ 中的每一个元素是一一对应的,使得 $I=\{i_1,\cdots,i_k\}\subseteq\mathcal{Q}$ 为无关集当且仅当矩阵 M 中与 I 对应的列是线性无关的,则称拟阵 $\mathcal{M}=(\mathcal{Q},\mathcal{I})$ 为 $\mathbb{K}$ 上可表示的($\mathbb{K}$ - representable).同时,我们称矩阵 M 为拟阵 $\mathcal{M}$ 的一个 $\mathbb{K}$ 上表示法.显然,矩阵 M 的秩等于拟阵 $\mathcal{M}$ 的秩,M 的列数等于 $\mathcal{Q}$ 中的元素个数.

下面我们来介绍拟阵与理想秘密共享方案之间的联系.

在文献[18]中,Brickell 和 Davenport 首次发现了拟

阵与理想秘密共享方案之间的联系.此后大量的学者开始研究秘密共享可表示拟阵的特性.对于一个拟阵 $\mathscr{M}=(\mathscr{Q},\mathscr{I})$和一个点 $p_0\in\mathscr{Q}$(p_0 是一个特殊的参与者称为 dealer),在参与者集合 $P=\mathscr{Q}-\{p_0\}$上,通过确定最小存取结构 $\min\Gamma_{p_0}(\mathscr{M})=\{A\subseteq P: A\cup\{p_0\}$是 $\mathscr{M}$的一个路$\}$(即 $r(A\cup\{p_0\})=r(A)=|A|$),我们可以得到对应的存取结构.以这种形式定义的存取结构称为与拟阵相关联(matroid-related)的存取结构.在文献[18]中给出了存取结构为理想存取结构的一个必要条件,即每一个理想的存取结构都是与拟阵相关联的,具体地说,每一个理想的秘密共享方案(设参与者集合为 P)都可以确定一个拟阵 $\mathscr{M}=(\mathscr{Q},\mathscr{I}$(其中 $\mathscr{Q}=P\cup\{p_0\}$),使得 $\Gamma_{p_0}(\mathscr{M})$为该理想秘密共享方案的存取结构.像这样由理想的秘密共享方案得到的拟阵称为秘密共享可表示(secret sharing representable)的拟阵.

若拟阵 $\mathscr{M}=(\mathscr{Q},\mathscr{I}$可用有限域 $\mathbb{K}$ 上的矩阵 M 来表示,设 M 为一个 $k\times(n+1)$阶矩阵,E 为$\mathbb{K}$ 上一个有限维向量空间,维数 $\dim E=k$.对于任一 $i\in\mathscr{Q}$,定义满射线性映射 $\pi_i: E\to\mathbb{K}$,其中 M 的第 i 列即对应线性形式 π_i.此时,对于任一 $x\in E$,计算 $s_i=\pi_i(x)\in\mathbb{K}$,即为参与者 $i\in P$ 的子秘密,$s=\pi_{p_0}(x)\in\mathbb{K}$ 为主秘密(其中 $\mathscr{Q}=P\cup\{p_0\}$).于是我们利用矩阵 M 的列定义了一个理想秘密共享方案,使得 $\Gamma_{p_0}(\mathscr{M})$为该理想秘密共享方案的存取结构.也就是说,与可表示的拟阵相联的存取结构一定是理想的.文献[4]中给出了这个存取结构为理想存取结构的充分条件,即所有可表示的拟阵都是秘密共享可表示的.

2.2　多部存取结构,多部拟阵和离散多拟阵

(1)设 P 为一个集合,$\mathscr{P}(P)$为 P 的幂集.P 上的一个 m 划分(m-partition)$\Pi=\{P_1,\cdots,P_m\}$是指将 P 划分为 m 个不相交的非空子集,即 $P=P_1\cup\cdots\cup P_m$.

(2)设集合 $\Lambda\subseteq\mathscr{P}(P)$,对于 P 上的一个置换 σ,定义 Λ 的置换为$\sigma(\Lambda)=\{\sigma(A): A\in\Lambda\}$.

(3)若对于每一个满足条件 $\sigma(P_1)=P_1,\cdots,\sigma(P_m)=P_m$(其中 $\Pi=\{P_1,\cdots,P_m\}$为 P 上的一个 m 划分)的 P 上的置换σ,都有 $\sigma(\Lambda)=\Lambda$,则称 $\Lambda\subseteq\mathscr{P}(P)$是 Π 部(Π-partite)的.

(4)若对于一个 m 划分 Π,Λ 是Π 部的,则我们称 $\Lambda\subseteq\mathscr{P}(P)$是 m 部(m-partite)的.

(5)Π 和Π'分别为 P 上的两个划分,若对于每一个 $P_i'\in\Pi'$都一定存在 $P_i\in\Pi$ 使得 $P_i'\subseteq P_i$,则称划分 Π'是划分 Π 的一个细分(refinement).

这些概念[14]可直接应用于存取结构,因为存取结构 $\Gamma\subseteq\mathscr{P}(P)$,其中 P 为参与者集合.同样,它们也可直接应用于拟阵,因为拟阵 $\mathscr{M}=(\mathscr{Q},\mathscr{I}$中 $\mathscr{I}\subseteq\mathscr{P}(\mathscr{Q})$.对于 $\mathscr{Q}$上的一个 m 划分Π,若 $\mathscr{I}\subseteq\mathscr{P}(\mathscr{Q})$或者 $\mathscr{B}\subseteq\mathscr{P}(\mathscr{Q})$是 Π 部的,则称拟阵 $\mathscr{M}=(\mathscr{Q},\mathscr{I}$是 Π 部的.

设 $\mathscr{M}=(\mathscr{Q},\mathscr{I}$是一个连通拟阵,点 $p_0\in\mathscr{Q}$,$\Pi=\{P_1,\cdots,P_m\}$和 $\Pi_0=\{\{p_0\},P_1,\cdots,P_m\}$分别为集合 $P=\mathscr{Q}-\{p_0\}$和集合 $\mathscr{Q}$上的划分,则存取结构 $\Gamma=\Gamma_{p_0}(\mathscr{M})$是 Π 部的当且仅当拟阵 $\mathscr{M}$是 Π_0 部的.

对于每一个整数 $m\geqslant 1$,考虑集合 $J_m=\{1,\cdots,m\}$.用$\mathbb{Z}_+^m$表示向量 $\boldsymbol{u}=(u_1,\cdots,u_m)\in\mathbb{Z}^m$ 组成的集合,其中 $u_i\geqslant 0(i\in J_m)$.设 $\Pi=\{P_1,\cdots,P_m\}$是集合 P 上的一个划分,对于每一个 $A\subseteq P$ 和 $i\in J_m$,定义 $\Pi_i(A)=|A\cap P_i|$,则通过考察 $\Pi(A)=(\Pi_1(A),\cdots,\Pi_m(A))$,我们得到划分 Π 定义了一个映射$\Pi:\mathscr{P}(P)\to\mathbb{Z}_+^m$.若 $\Lambda\subseteq P(P)$是 Π 部的,则 $A\in\Lambda$ 当且仅当$\Pi(A)\in\Pi(\Lambda)$,也就是说,划分 Π 和向量集合$\Pi(\Lambda)\subset\mathbb{Z}_+^m$完全确定 Λ.

离散多拟阵由 Herzog 在文献[21]中首次引入,它是与多部拟阵密切相关的一个概念.因此,在研究理想多部存取结构的特性时它扮演着十分重要的角色.在介绍离散多拟阵的概念之前先引入一些符号.设 $u,v\in\mathbb{Z}_+^m$,对于每一个 $i\in J_m$,若 $u_i\leqslant v_i$,则称 $u\leqslant v$.若 $u\leqslant v$且$u\neq v$,则称 $u<v$.我们定义 $w=u\vee v$,其中 $w_i=\max(u_i,v_i)$.向量 $\boldsymbol{u}\in\mathbb{Z}_+^m$ 的模记为$|u|=u_1+\cdots+u_m$.对于每一个子集 $X\subseteq J_m$,$u(X)=(u_i)_{i\in X}\in\mathbb{Z}_+^{|X|}$及$|u(X)|=\sum_{i\in X}u_i$.

在基础集 J_m 上的一个离散多拟阵是指一个非空有限的向量集合 $D\subset\mathbb{Z}_+^m$,它同时满足:

(1)若向量 $\boldsymbol{u}\in D$,且向量 $\boldsymbol{v}\in\mathbb{Z}_+^m$ 使得 $\boldsymbol{v}\leqslant\boldsymbol{u}$,则必有 $\boldsymbol{v}\in D$;

(2)对于每一对向量 $\boldsymbol{u},\boldsymbol{v}\in D$,若$|u|<|v|$,则必存在向量 $\boldsymbol{w}\in D$ 使得$\boldsymbol{u}<\boldsymbol{w}\leqslant\boldsymbol{u}\vee\boldsymbol{v}$.

由拟阵的无关集的相关公理容易得到下面的命题,它反映了多部拟阵与离散多拟阵之间的关系.

命题 1　设 Π 为集合 $\mathscr{Q}$上的一个划分,$\mathscr{I}\subseteq\mathscr{P}(\mathscr{Q})$为一个 Π 部的 $\mathscr{Q}$上子集的集合,则 I 为一个Π 部拟阵 $\mathscr{M}=(\mathscr{Q},\mathscr{I}$的所有无关集的集合当且仅当 $\Pi(I)\subset\mathbb{Z}_+^m$为一个离散多拟阵.

离散多拟阵 D 中所有最大的元素都称为 D 的基,即若对于向量 $\boldsymbol{u}\in D$,不存在任意向量 $\boldsymbol{v}\in D$ 使得$\boldsymbol{u}<\boldsymbol{v}$,则向量 $\boldsymbol{u}$ 是 D 的一个基.同拟阵一样,所有的基组成的集合唯一确定一个离散多拟阵.文献[21]中证明了以下的结论.

命题 2　一个非空子集 $\mathscr{B}\subset\mathbb{Z}_+^m$为一个离散多拟阵的所有基组成的集合当且仅当它同时满足:

(1)B 中所有的元素拥有相等的模;

(2)对于每一对向量 $\boldsymbol{u},\boldsymbol{v}\in B$,若 $u_i>v_i$,则必存在

$j\in J_m$ 使得 $u_j < v_j$ 且 $u - e_i + e_j \in \mathscr{B}$,其中 e_i 表示 $\mathbb{Z}^m$ 的规范基中的第 i 个向量.

由 $h(X) = \max\{|u(X)|: u\in D\}$ 定义的函数 $h: P(J_m)\to\mathbb{Z}$ 称为基础集 J_m 上的一个离散多拟阵 D 的秩函数.下面的命题是文献[21]的结论.

命题 3 一个函数 $h: P(J_m)\to\mathbb{Z}$ 为基础集 J_m 上的一个离散多拟阵的秩函数当且仅当它同时满足:

(1) $h(\varphi) = 0$;

(2) h 是单调递增的:若 $X\subseteq Y\subseteq J_m$,则 $h(X)\leqslant h(Y)$;

(3)若 $X, Y\subseteq J_m$,则 $h(X\cup Y) + h(X\cap Y)\leqslant h(X) + h(Y)$.

此外,一个离散多拟阵 D 的秩函数完全确定 D,即 $D = \{u\in\mathbb{Z}_+^m: |u(X)|\leqslant h(X)$ for all $X\subseteq J_m\}$.

对于基础集 J_m 上的一个离散多拟阵 D 以及每一个 $X\subseteq J_m$,定义基础集 X 上的离散多拟阵 $D(X)$ 为 $D(X) = \{u(X): u\in D\}\subset Z_+^{|X|}$(这一概念在本文中将多次用到).

设 $\mathbb{K}$ 为一个有限域,E 为 $\mathbb{K}$ 上的一个向量空间,$V_1, \cdots, V_m$ 为 E 上的 m 个子空间.不难验证,由 $h(X) = \dim(\sum_{i\in X} V_i)$ 定义的映射 $h: \mathscr{P}(J_m)\to\mathbb{Z}$ 正好是离散多拟阵 $D\subset\mathbb{Z}_+^m$ 的秩函数.此时,我们说 D 是 $\mathbb{K}$ 上可表示的,子空间 $V_1, \cdots, V_m$ 为 D 的一个 $\mathbb{K}$ 上表示法.下面的命题是文献[14]中证明的结论,它反映了可表示的多部拟阵与可表示的离散多拟阵之间的关系.

命题 4 设 $\mathscr{M} = (\mathscr{Q}, \mathscr{I})$ 为一个 Π 部的拟阵,$D = \Pi(\mathscr{I})$ 为其对应的离散多拟阵.若 $\mathscr{M}$ 是 $\mathbb{K}$ 上可表示的,则 D 也是;反之,若 D 是 $\mathbb{K}$ 上可表示的,则在 $\mathbb{K}$ 的某个有限延展域上,$\mathscr{M}$ 是可表示的.

3 一类不可表示的多部拟阵

本节我们将给出并证明一类不可表示的多部拟阵,即给出了一个离散多拟阵为不可表示的离散多拟阵的一个充分条件,这对于文献[14]中给出的开放性问题,即可表示的离散多拟阵的特性,将是一个新的贡献.

定理 1 设 $D\subset\mathbb{Z}_+^m$ 为基础集 J_m 上的一个离散多拟阵,若存在一个真子集 $X\subset J_m$ 使得基础集 X 上的离散多拟阵 $D(X)$ 是一个不可表示的离散多拟阵,其中 $D(X) = \{u(X): u\in D\}\subset\mathbb{Z}_+^{|X|}$,则必有 D 是一个不可表示的离散多拟阵,与 D 对应的多部拟阵是一个不可表示的多部拟阵.

证明 设 $D\subset\mathbb{Z}_+^m$ 为基础集 J_m 上的一个离散多拟阵,存在一个真子集 $X\subset J_m$ 使得基础集 X 上的离散多拟阵 $D(X)$ 是一个不可表示的离散多拟阵,其中 $D(X) = \{u(X): u\in D\}\subset\mathbb{Z}_+^{|X|}$,假设 D 在某个有限域 $\mathbb{K}$ 上是可表示的,即存在 $\mathbb{K}$ 上的一个向量空间 $E = \mathbb{K}^s$,其中 $s = h(J_m)$,使得 E 的 m 个子空间 $V_1, \cdots, V_m$ 为 D 的一个 $\mathbb{K}$ 上表示法.设 $X = \{x_1, \cdots, x_r\}$,于是与 $X\subset J_m$ 中的元素对应的子空间分别为 $V_{x_1}, \cdots, V_{x_r}$.由于 $D(X) = \{u(X): u\in D\}\subset\mathbb{Z}_+^{|X|}$,于是得到 $E = \mathbb{K}^s$ 的 r 个子空间 $V_{x_1}, \cdots, V_{x_r}$ 为 $D(X)$ 的一个 $\mathbb{K}$ 上表示法,即 $D(X)$ 是一个 $\mathbb{K}$ 上可表示的离散多拟阵,这与 $D(X)$ 是一个不可表示的离散多拟阵相矛盾,假设错误.因此,D 是一个不可表示的离散多拟阵,根据命题 4,容易得到与 D 对应的多部拟阵是一个不可表示的多部拟阵,得证.

于是,定理 1 给出了一个离散多拟阵 $D\subset\mathbb{Z}_+^m$ 为不可表示的离散多拟阵的充分条件.需要指出的是该充分条件并不是必要的.例如,对于 Vamos 拟阵来说,设与 Vamos 拟阵对应的离散多拟阵为 D_V,其基础集为 $J_4 = \{1,2,3,4\}$,由文献[14]可知,基础集 $J_m(m\leqslant 3)$ 上所有的离散多拟阵都是可表示的,因此以每一个子集 $X\subset J_4$ 为基础集的离散多拟阵 $D_V(X)$ 都是可表示的,而 D_V 却是一个不可表示的离散多拟阵.

4 由 Vamos 拟阵导出的一族不可表示的多部拟阵

本节我们利用向量的线性相关和线性无关性对 Vamos 拟阵的不可表示性给出了新的证明,然后将定理 3.1 应用于 Vamos 拟阵得到了一族不可表示的多部拟阵.

Vamos 拟阵是第一个被证明为秘密共享不可表示的拟阵.在文献[19]中,Seymour 利用图论的知识给出并证明了 Vamos 拟阵是一个秘密共享不可表示的拟阵.此后,文献[20]利用几何学的知识也给出了一个 Vamos 拟阵秘密共享不可表示的简短证明.下面我们将利用向量的线性相关和线性无关性对 Vamos 拟阵的不可表示性进行证明.首先给出 Vamos 拟阵的定义.

所谓 Vamos 拟阵 $\mathscr{M} = (\mathscr{Q}, \mathscr{I})$ 是指:$\mathscr{Q} = \{1,2,3,4,5,6,7,8\}$,所有的四点集合均为拟阵的基除了下列 5 个四点集合:$\{1,2,3,4\}$,$\{1,2,5,6\}$,$\{1,2,7,8\}$,$\{3,4,5,6\}$,$\{3,4,7,8\}$.所有的基组成的集合 $\mathscr{B}$ 唯一确定该拟阵.

命题 5 Vamos 拟阵是一个不可表示的拟阵.

证明 对于 Vamos 拟阵 $\mathscr{M} = (\mathscr{Q}, \mathscr{I})$,考虑基础集 $\mathscr{Q} = \{1,2,3,4,5,6,7,8\}$ 上的一个划分 $\Pi_0 = \{P_1, P_2, P_3, P_4\}$,其中 $P_1 = \{1,2\}$,$P_2 = \{3,4\}$,$P_3 = \{5,6\}$,$P_4 = \{7,8\}$.容易验证,$\mathscr{I}\subseteq\mathscr{P}(\mathscr{Q})$ 是 Π_0 部的,即 Vamos 拟阵 $\mathscr{M} = (\mathscr{Q}, \mathscr{I})$ 是一个四部拟阵.考虑划分 Π_0 定义的映射 $\Pi_0: \mathscr{P}(\mathscr{Q})\to\mathbb{Z}_+^4$,我们得到与 Vamos 拟阵 $\mathscr{M} = (\mathscr{Q}, \mathscr{I})$ 对应的离散多拟阵为 $D_V = \Pi_0(\mathscr{I})$.对于每一个非基的四点集合 A,计算 $\Pi_0(A)$,于是得到 $(2,2,0,0)$,$(2,0,2,0)$,$(2,$

0,0,2),(0,2,2,0),(0,2,0,2).同样地,对于每一个基 B,计算 $\Pi_0(B)$,于是得到(1,1,1,1),(1,1,2,0),(1,1,0,2),(1,2,1,0),(1,2,0,1),(1,0,1,2),(1,0,2,1),(0,1,1,2),(0,1,2,1),(0,2,1,1),(2,1,0,1),(2,1,1,0),(2,0,1,1),(0,0,2,2).容易验证,对于每一个三点集合 C,必存在一个基 B 使得 $\Pi_0(C) < \Pi_0(B)$.因为 $\Pi_0(B) \in D_V$,于是有 $\Pi_0(C) \in D_V$.因此,Vamos 拟阵中所有的三点集都是无关集.

假设在有限域 $\mathbb{K}$ 上存在一个矩阵 M 能够表示 Vamos 拟阵,设每一个点 $i \in \mathcal{Q}$ 对应矩阵 M 的列向量 v_i.显然,M 的所有列向量都是非零向量,因为 M 的任意三个列向量都是线性无关的.同时,M 的任意四个列向量都是线性无关的除了 (v_1, v_2, v_3, v_4),(v_1, v_2, v_5, v_6),(v_1, v_2, v_7, v_8),(v_3, v_4, v_5, v_6),(v_3, v_4, v_7, v_8).考虑这五个线性相关的向量组,对于其中任意一个向量组来说,其中任意三个列向量都是线性无关的,因此在有限域 $\mathbb{K}$ 上,每一个向量都可由其他三个向量唯一的线性表示.以下的运算都是在有限域 $\mathbb{K}$ 上进行的:

对于向量组 (v_1, v_2, v_7, v_8),设

$$v_8 = a_1 v_1 + a_2 v_2 + a_7 v_7 \tag{1}$$

对于向量组 (v_3, v_4, v_7, v_8),设

$$v_8 = a_3 v_3 + a_4 v_4 + a_7' v_7 \tag{2}$$

其中 $a_1, a_2, a_7, a_3, a_4, a_7' \in \mathbb{K}$,

并且 $a_1, a_2, a_7, a_3, a_4, a_7' \neq 0$.

联立等式(1)、(2),有

$$(a_7' - a_7) v_7 = a_1 v_1 + a_2 v_2 - a_3 v_3 - a_4 v_4 \tag{3}$$

对于向量组 (v_1, v_2, v_3, v_4),设

$$v_4 = b_1 v_1 + b_2 v_2 + b_3 v_3 \tag{4}$$

其中 $b_1, b_2, b_3 \in \mathbb{K}$,并且 $b_1, b_2, b_3 \in \mathbb{K}$.

如果在等式(3)中 $(a_7' - a_7) \neq 0$,联立等式(3)、(4),我们得到 (v_1, v_2, v_3, v_7) 是线性相关的,这与 $\{1,2,3,7\}$ 为 Vamos 拟阵的一个基相矛盾,因此,在等式(3)中必有 $(a_7' - a_7) = 0$,即 $a_7' = a_7$.于是我们得到:

$$a_1 v_1 + a_2 v_2 = a_3 v_3 + a_4 v_4 \tag{5}$$

对于向量组 (v_1, v_2, v_5, v_6),设

$$v_6 = c_1 v_1 + c_2 v_2 + c_5 v_5 \tag{6}$$

对于向量组 (v_3, v_4, v_5, v_6),设

$$v_6 = c_3 v_3 + c_4 v_4 + c_5' v_5 \tag{7}$$

同理,我们能够得到 $c_5 = c_5'$ 以及

$$c_1 v_1 + c_2 v_2 = c_3 v_3 + c_4 v_4 \tag{8}$$

计算等式 $c_1(5) - a_1(8)$,有:

$$(a_2 c_1 - a_1 c_2) v_2 = (a_3 c_1 - a_1 c_3) v_3 + (a_4 c_1 - a_1 c_4) v_4 \tag{9}$$

因为 (v_2, v_3, v_4) 是线性无关的,于是有:

$$a_2 c_1 - a_1 c_2 = 0 \tag{10}$$

计算等式 $c_1(1) - a_1(6)$,有:

$$c_1 v_8 - a_1 v_6 = (a_2 c_1 - a_1 c_2) v_2 + a_7 c_1 v_7 - a_1 c_5 v_5 \tag{11}$$

联立等式(10)、(11),有:

$$c_1 v_8 - a_1 v_6 = a_7 c_1 v_7 - a_1 c_5 v_5 \tag{12}$$

因为 $a_1, c_1, a_7, c_5 \neq 0$,由等式(12)我们得到 (v_5, v_6, v_7, v_8) 是线性相关的,这与 $\{5,6,7,8\}$ 为 Vamos 拟阵的一个基相矛盾.因此,假设错误,在有限域上不可能存在一个矩阵能够表示 Vamos 拟阵,即 Vamos 拟阵是一个不可表示的拟阵,得证.

根据多部拟阵与离散多拟阵之间的关系,对于 Vamos 拟阵 $\mathcal{M} = (\mathcal{Q}, \mathcal{D})$ 来说,通过基础集 $\mathcal{Q} = \{1,2,3,4,5,6,7,8\}$ 上的一个划分 $\Pi_0 = \{P_1, P_2, P_3, P_4\}$,其中 $P_1 = \{1,2\}$,$P_2 = \{3,4\}$,$P_3 = \{5,6\}$,$P_4 = \{7,8\}$,以及该划分 Π_0 定义的映射,我们可以得到与 Vamos 拟阵 $\mathcal{M} = (\mathcal{Q}, \mathcal{D})$ 对应的离散多拟阵 $D_V = \Pi_0(I)$.由定理 1 可知,对于任意一个基础集 J_m 上的离散多拟阵 D 来说,如果存在一个真子集 $X \subset J_m$,其中 $|X| = 4$,使得 $D(X) = D_V$,则 D 必是一个不可表示的离散多拟阵,于是与 D 对应的多部拟阵是一个不可表示的多部拟阵.由此可见,由 Vamos 拟阵可以导出一族不可表示的多部拟阵,我们称之为 Vamos 家族 $F_{D_V} = \{D \subset \mathbb{Z}_+^m : D(X) = D_V, X \subset J_m$ 且 $|X| = 4\}$,其中的每一个离散多拟阵都是不可表示的.

5　结论

根据多部拟阵与离散多拟阵之间的对应关系,本文给出并证明了离散多拟阵为不可表示的一个充分条件.当我们把这一结论应用于 Vamos 拟阵时,于是得到了一族不可表示的多部拟阵(即 Vamos 家族),同时文中利用向量的线性相关和线性无关性给出了 Vamos 拟阵为不可表示的新的证明.这些结论对于 EUROCRYPT'07 上给出的开放性问题,即可表示的离散多拟阵具有的特性,将是一个新的贡献.

参考文献:

[1] G R Blakley. Safeguarding cryptographic keys[A]. In Proc AFIPs I979 National Computer Conference, Vol. 48[C]. New York, 1979. 313 – 317.

[2] A Shamir. How to share a secret[J]. Communication of the ACM, 1979, 22(11): 612 – 613.

[3] A Beimel, T Tassa, E Weinreb. Characterizing ideal weighted threshold secret sharing[A]. Second Theory of Cryptography Conference, TCC 2005, Lecture Notes in Comput. Sci. 3378[C]. 2005. 600 – 619.

[4] E F Brickell. Some ideal secret sharing schemes[J]. J. Combin. Math. and Combin. Comput. 1989, 9: 105 – 113.

[5] J Herranz, G Saez. New Results on Multipartite Access Struc-

tures[OL]. Cryptology ePrint Archive, Report 2006/048, http://eprint.iacr.org/2006/048.
[6] S-L Ng. Ideal secret sharing schemes with multipartite access structures[J]. IEE Proc.-Commun. 2006, 153: 165 – 168.
[7] G J Simmons. How to (Really) Share a Secret[A]. Advances in Cryptology CRYPTO '88, Lecture Notes in Comput. Sci. 403 [C]. 1990. 390 – 448.
[8] T Tassa. Hierarchical threshold secret sharing[A]. First Theory of Cryptography Conference, TCC 2004, Lecture Notes in Comput. Sci. 2951[C]. 2004. 473 – 490.
[9] T Tassa, N Dyn. Multipartite secret sharing by bivariate interpolation[A]. Proceedings of 33rd International Colloquium on Automata, Languages and Programming, ICALP 2006, Lecture Notes in Comput. Sci. 4052[C]. 2006. 288 – 299.
[10] C Padr_o, G S_aez. Secret sharing schemes with bipartite access structure[J]. IEEE Trans. Inform. Theory, 2000, 46: 2596 – 2604.
[11] S-L Ng, M Walker. On the composition of matroids and ideal secret sharing schemes[J]. Des. Codes Cryptogr. 2001, 24: 49 – 67.
[12] S-L Ng. A representation of a family of secret sharing matroids[J]. Des. Codes Cryptogr. 2003, 30: 5 – 19.
[13] M J Collins. A Note on Ideal Tripartite Access Structures [OL]. Cryptology ePrint Archive, Report 2002/193, http://eprint.iacr.org/2002/193.
[14] Oriol Farras, Jaume Martí Farré, Carles Padró. Ideal multipartite secret sharing schemes[A]. Advances in Cryptology-EUROCRYPT 2007[C]. Springer, 2007. 448 – 465.
[15] D J A Welsh. Matroid Theory[M]. Academic Press, London, 1976.
[16] D R Stinson. An explication of secret sharing schemes[J]. Des. Codes Cryptogr. 1992, 2: 357 – 390.
[17] J G Oxley. Matroid theory[M]. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1992.
[18] E F Brickell, D M Davenport. On the classification of ideal secret sharing schemes[J]. J. Cryptology, 1991, 4: 123 – 134.
[19] P D Seymour. On secret-sharing matroids[J]. J. Combin. Theory Ser. B, 1992, 56: 69 – 73.
[20] J Simonis, A Ashikhmin. Almost affine codes[J]. Des. Codes Cryptogr. 1998, 14: 179 – 197. 1
[21] J Herzog, T Hibi. Discrete polymatroids[J]. J. Algebraic Combin. 2002, 16: 239 – 268.
[22] J Xu, Z Zhang, D Feng. Identity Based Threshold Proxy Signature[J]. Chinese Journal of Electronics, 2006, 15(1): 183 – 189.
[23] 鲁荣波,何大可,王常吉.一种门限代理签名方案的分析和改进[J].电子学报,2007,35(1):145 – 149.
Lu Rongbo, He Dake, Wang Changji. Cryptanalysis and Improvement of a Threshold Proxy Signature Scheme from Bilinear Pairings[J]. Acta Electronica Sinica., 2007, 35(1): 145 – 149. (in Chinese)
[24] 桑永宣,曾吉文.两种无证书的分布环签名方案[J].电子学报,2008,36(7):1468 – 1473.
Sang Yongxuan, Zeng Jiwen. Two Certificateless Distributed Ring Signature Scheme[J]. Acta Electronica Sinica, 2008, 36 (7): 1468 – 1473. (in Chinese)
[25] R Cramer, V Daza, et al. On codes, matroids and secure multiparty computation from linear secret sharing schemes[J]. IEEE Trans on Information Theory, 2008, 54(6): 2644 – 2657.
[26] A Beimel, N Livne. On Mtroids and Nonideal Secet Sharing [J]. IEEE Trans on Information Theory, 2008, 54(6): 2626 – 2643.

作者简介:

许静芳 女,1978 年生于湖北襄樊,华中科技大学计算机科学与技术学院博士生,主要研究领域为秘密共享,容忍入侵,多方安全计算.
E-mail: cherryjingfang@gmail.com

崔国华(通信作者) 男,1947 年生于湖北武汉,博士,华中科技大学计算机科学与技术学院教授,博士生导师,主要研究领域为信息安全,算法分析,数值分析.
E-mail: cgh3986@163.com

程 琦 男,1977 年生于湖北应城,华中科技大学计算机科学与技术学院硕士,工程师,主要研究领域为秘密共享、网络安全.

张 志 女,1977 年生于湖北武汉,副教授,华中科技大学计算机科学与技术学院博士生,主要研究领域为网络安全、数字签名.