线性秘密共享体制的一般构造

薛 婷,李志慧,宋 云
XUE Ting,LI Zhihui,SONG Yun
陕西师范大学 数学与信息科学学院,西安 710062
College of Mathematics and Information Science,Shaanxi Normal University,Xi'an 710062,China

XUE Ting,LI Zhihui,SONG Yun.General construction of linear secret sharing scheme.Computer Engineering and Applications,2011,47(34):92-94.

Abstract: This paper studies the constructions of linear secret sharing scheme by monotone span program,and gives the corresponding matrixes of monotone span program when the target vector is $\boldsymbol{e}=(1,0,\cdots,0)$.The examples are presented.At last,it gives a sufficient and necessary condition of deciding the multiplication of a linear secret sharing scheme.
Key words: linear secret sharing scheme;monotone span program;multiplicative linear secret sharing scheme

摘 要: 利用单调张成方案讨论了线性秘密共享体制方案的构造,给出了目标向量为 $\boldsymbol{e}=(1,0,\cdots,0)$ 时任意一个接入结构所对应的单调张成方案的矩阵,并给出了相应的例子。最后利用乘性线性秘密共享体制的定义,借助diamond运算给出了判断一个线性秘密共享体制是否为乘性的充要条件。
关键词: 线性秘密共享体制;单调张成方案;乘性线性秘密共享体制
DOI:10.3778/j.issn.1002-8331.2011.34.024 **文章编号:** 1002-8331(2011)34-0092-03 **文献标识码:** A **中图分类号:** TP309

1 引言

秘密共享体制自从Shamir[1]和Blakley[2]在1979年各自独立提出后,作为现代密码学的重要工具之一,在实际中有很多应用。在信息系统中使用的秘密共享,可以防止系统密钥的遗失、损坏和来自敌方的攻击,减小秘密保存者的责任。在 (t,n) 秘密共享体制中,秘密分发者将一个秘密信息分成 n 个秘密份额,分发给 n 个人,当需要恢复秘密信息时,任意少于 t 个的秘密保存者都得不到该秘密的任何信息。

秘密共享体制中秘密的重构大多都是通过求解线性方程组实现的,这就促使了线性秘密共享体制(LSSS)的建立,Brickell[3]在1989年就提出了秘密共享体制线性空间结构,但直到1996年才由A.Beimel[4]给出一般的线性秘密共享体制的数学模型,建立了线性秘密共享体制与可计算单调布尔函数的单调张成方案之间的对应关系。刘木兰[5]利用单调张成方案构造了一批线性秘密共享体制。

但是文献[5]在利用单调张成方案构造线性秘密共享体制时,是在目标向量为 $\boldsymbol{e}=(1,1,\cdots,1)$ 时的情况。本文利用单调张成方案讨论了线性秘密共享方案的构造,给出了目标向量为 $\boldsymbol{e}=(1,0,\cdots,0)$ 时任意一个接入结构所对应的单调张成方案的矩阵,并给出了相应的例子。

2 准备知识

2.1 线性秘密共享体制

设 $P=(p_1,p_2,\cdots,p_n)$ 为 n 个参与者集合,S 为秘密集,K 为有限域,其中 2^P 表示 P 的所有子集构成的集合。$AS\subseteq 2^P$ 为 P 上的接入结构,它是由所有能恢复秘密 s 的参与者子集组成的集合。AS 具有单调递增性,即 $G\in AS$,$G'\supseteq G$,则 $B\in AS$。设 A 为攻击者结构,且具有单调递减性,即 $B\in A$,$B'\subseteq$B,则 $B'\in A$。通常用 (AS,A) 表示由 AS 实现的秘密共享体制,其中 AS 所对应的攻击者结构为 A。

AS 中所有极小元素的集合记作 $AS_{\min}$,A 中所有极大元素的集合记作 $A_{\max}$。则 $(AS_{\min},A_{\max})$ 唯一的确定了 (AS,A)。若 $AS\cup A=2^P$,则称 AS 为完备的。为研究方便,本文只讨论 AS 是完备的情况。

定义1 文献[6]设 S 为秘密集,R 是随机输入集,S_i 是 p_i 所拥有的份额集。$1\le i\le n$,分配函数

$$\Pi:S\times R\to S_1\times S_2\times\cdots\times S_n$$

称为由 AS 实现的秘密共享体制,若满足以下条件:

$$H(S|\Pi(S,R)|_G)=0,\ \forall G\in AS$$

$$H(S|\Pi(S,R)|_B)=H(S),\ \forall B\notin AS$$

其中 $H(\cdot)$ 是熵函数。

基金项目: 国家自然科学基金(the National Natural Science Foundation of China under Grant No.10571112);中央高校基本科研业务费专项资金资助(No.10871123)。
作者简介: 薛婷(1987—),女,硕士研究生,研究领域为有限域,密码学;李志慧,女,博士,副教授;宋云,女,硕士研究生。E-mail:xwtabc@163.com
收稿日期: 2010-10-13;**修回日期:** 2010-12-27;**CNKI出版:** 2011-05-17;http://www.cnki.net/kcms/detail/11.2127.TP.20110517.1449.011.html

另外,若 $S=K$, $R=K^{l-1}$, $S_i=K^{d_i}$,其中 l、d_i 是正整数, $1\le i\le n$ 。秘密 s 是由接入结构中参与者所持秘密份额的一个线性组合来恢复的,称为由 AS 实现的线性秘密共享体制。

2.2　单调张成方案

Karchmer 和 Wigderson[7]论证了单调张成方案可以作为计算单调布尔函数的模型。为此,先用特征向量表示 $\boldsymbol{P}$ 上的接入结构,设 $G\subseteq AS$,定义 $\boldsymbol{\delta}_G=(\delta_1,\delta_2,\cdots,\delta_n)$, $\delta_i=1$ 当且仅当 $p_i\in G$ 否则 $\delta_i=0$。 $\boldsymbol{\delta}_G$ 称为集合 G 的特征向量。不难看出, n 个参与者集合上的接入结构与二元单调布尔函数有一一对应的关系。换言之,设 $f:\{0,1\}^n\to\{0,1\}$,且满足 $f(\boldsymbol{\delta})=1$ 当且仅当 $G\in AS$,使得 $\boldsymbol{\delta}=\boldsymbol{\delta}_G$ 。

定义 2　文献[8]设 $\boldsymbol{M}$ 是一个四元组 $(K,\boldsymbol{M},\varphi,\boldsymbol{e})$,其中 K 为有限域, $\boldsymbol{M}$ 为 K 上的 $d\times l$ $(l\le d)$ 矩阵, $\boldsymbol{e}$ 为非零的目标向量,不失一般性,常取 $\boldsymbol{e}$ 为 $\{1,0,\cdots,0\}\in K^l$, $\{p_1,p_2,\cdots,p_n\}$ 为标号集。满射 $\varphi:\{1,2,\cdots,d\}\to\{p_1,p_2\cdots,p_n\}$ 给出将矩阵 $\boldsymbol{M}$ 的行用 $p_1,p_2\cdots,p_n$ 进行标记的方式,标记后的矩阵用 $\boldsymbol{M}(\boldsymbol{M},\varphi)=\boldsymbol{M}$ 表示,则四元组 $(K,\boldsymbol{M},\varphi,\boldsymbol{e})$ 称为相对映射 φ 的单调张成方案(MSP)。

$\boldsymbol{M}$ 的行规模指 $\boldsymbol{M}$ 的行数 d ,反映了由 $\boldsymbol{M}$ 所决定的实现接入结构为 AS 的线性秘密共享体制的有效性。 $\boldsymbol{M}$ 的列规模指 $\boldsymbol{M}$ 的列数 l ,反映了秘密重构所需要的计算量。

若 $\boldsymbol{e}\in\mathrm{span}\{\boldsymbol{M}_A\}$ 当且仅当 $f(\boldsymbol{\delta}_A)=1$,称这个 $\boldsymbol{M}(K,\boldsymbol{M},\varphi,\boldsymbol{e})$ 为可计算单调布尔函数的单调张成方案。其中 A 是参与者集合; $\boldsymbol{M}_A$ 表示 $\boldsymbol{M}$ 中被 φ 标记为 p_i 的行组成的矩阵,其中 $p_i\in A$; $\mathrm{span}\{\boldsymbol{M}_A\}$ 表示由 $\boldsymbol{M}_A$ 中的行向量生成的 K 上的线性空间。 $\boldsymbol{\delta}_A$ 是 A 的特征向量。

引理 1　文献[6]设 AS 是 P 上的接入结构, f_{AS} 是 AS 的特征函数,即 $f_{AS}(\boldsymbol{\delta})=1$ 当且仅当 $\boldsymbol{\delta}=\boldsymbol{\delta}_{\mathrm{A}}$, $A\in AS$,则存在一个可计算 f_{AS} 的单调张成方案,当且仅当存在由 AS 实现的线性秘密共享体制。

下面来说明利用单调张成方案如何来构造线性秘密共享体制。

已知 $\boldsymbol{M}(K,\boldsymbol{M},\varphi,\boldsymbol{e})$,公开 $\boldsymbol{M}$,随机选取 $s\in K$, $r_i(1\le i\le l-1)\in K$ 为随机数, $\boldsymbol{e}=(1,0,\cdots,0)$ 。分发者计算 $\boldsymbol{M}_i\boldsymbol{y}^{\mathrm{T}}$, $\boldsymbol{y}=(s,r_1,\cdots,r_{l-1})$,并发送给每个参与者。若 $A\in AS$,则 $\boldsymbol{e}\in\mathrm{span}\{\boldsymbol{M}_A\}$,所以存在 $b_1,b_2,\cdots,b_t$,使得 $\boldsymbol{e}=(b_1,b_2,\cdots,b_t)\,\boldsymbol{M}_A$, t 为 A 的参与者个数。所以 $\boldsymbol{s}=\boldsymbol{s}\boldsymbol{y}^{\mathrm{T}}=((b_1,b_2,\cdots,b_t)\boldsymbol{M}_A)\,\boldsymbol{y}^{\mathrm{T}}=(b_1,b_2,\cdots,b_t)(\boldsymbol{M}_A\boldsymbol{y}^{\mathrm{T}})$ 。

3　一般线性秘密共享体制的构造

3.1　实现一般存取结构的线性秘密共享体制 1

设 $P=\{p_1,p_2,\cdots,p_n\}$ 是参与者集合,令

$$AS_{\min}=\left\{\{p_{i_1},p_{i_2},\cdots,p_{i_{n_1}}\},\{p_{i_{1+n_1}},p_{i_{2+n_1}},\cdots,p_{i_{n_1+n_2}}\},\cdots,\{p_{i_{1+\sum_{j=1}^{k-1}n_j}},\cdots,p_{i_{\sum_{j=1}^{k}n_j}}\}\right\}$$

其中 $1\le i_s\le n$, $1\le s\le\sum_{j=1}^{k}n_j$ 。下面构造实现 $AS_{\min}$ 的单调张成方案。

K 是有限域, $d=\sum_{i=1}^{k}n_i$ 。取 d 维非零向量 $\boldsymbol{v}=\boldsymbol{e}_1=(1,0,\cdots,0)$,令 $d\times d$ 阶

$$\boldsymbol{M}=\begin{pmatrix}
1&1&0&\cdots&0&-1&0&0&0&\cdots&0&0&\cdots&0&0&0&0&\cdots&0\\
0&-1&1&\cdots&0&0&0&0&0&\cdots&0&0&\cdots&0&0&0&0&\cdots&0\\
\vdots&\vdots&\vdots&&\vdots&\vdots&\vdots&\vdots&\vdots&&\vdots&\vdots&&\vdots&\vdots&\vdots&\vdots&&\vdots\\
0&0&0&\cdots&-1&1&0&0&0&\cdots&0&0&\cdots&0&0&0&0&\cdots&0\\
1&0&0&\cdots&0&0&1&0&-1&\cdots&0&0&\cdots&0&0&0&0&\cdots&0\\
0&0&0&\cdots&0&0&-1&1&0&\cdots&0&0&\cdots&0&0&0&0&\cdots&0\\
\vdots&\vdots&\vdots&&\vdots&\vdots&\vdots&\vdots&\vdots&&\vdots&\vdots&&\vdots&\vdots&\vdots&\vdots&&\vdots\\
0&0&0&\cdots&0&0&0&0&0&\cdots&-1&1&\cdots&0&0&0&0&\cdots&0\\
\vdots&\vdots&\vdots&&\vdots&\vdots&\vdots&\vdots&\vdots&&\vdots&\vdots&&\vdots&\vdots&\vdots&\vdots&&\vdots\\
1&0&0&\cdots&0&0&0&0&0&\cdots&0&0&\cdots&0&1&0&-1&\cdots&0\\
0&0&0&\cdots&0&0&0&0&0&\cdots&0&0&\cdots&0&-1&1&0&\cdots&0\\
\vdots&\vdots&\vdots&&\vdots&\vdots&\vdots&\vdots&\vdots&&\vdots&\vdots&&\vdots&\vdots&\vdots&\vdots&&\vdots\\
0&0&0&\cdots&0&0&0&0&0&0&0&0&\cdots&0&0&0&0&\cdots&-1
\end{pmatrix}$$

$\boldsymbol{M}$ 为 $(n_1+n_2+\cdots+n_k)\times(n_1+n_2+\cdots+n_k)$ 矩阵,标号函数 φ 定义为 $\varphi(j)=p_{i_j}$, $1\le j\le\sum_{l=1}^{k}n_l$,得到单调张成方案 $\boldsymbol{M}(\boldsymbol{M},\varphi)$ 。容易验证: $\boldsymbol{M}(\boldsymbol{M},\varphi)$ 相对 $\boldsymbol{e}$ 可计算单调特征函数 f_{AS} ,进而利用引理中的方法可以得到实现 AS 的线性秘密共享体制。

一般来说,这里的 $\boldsymbol{M}$ 不一定是理想的。可能 $\boldsymbol{M}$ 的行数 d 很大,即 $\boldsymbol{M}$ 决定的子秘密信息量可能很大。但是 $\boldsymbol{M}$ 确实可以给出实现 $AS_{\min}$ 的线性秘密共享体制。

例 1　假定 $P=\{p_1,p_2,p_3,p_4\}$ 是所有参与者组成的集合,极小接入结构为:

$$AS_{\min}=\{\{p_1,p_2,p_4\},\{p_1,p_3,p_4\},\{p_2,p_3\}\}$$

利用本文 3.1 节的方法,构造相应的单调张成方案如下:

K 为有限域,8 维非零向量 $\boldsymbol{e}=\{1,0,0,0,0,0,0,0\}$,令

$$\boldsymbol{M}=\begin{pmatrix}
1&1&0&-1&0&0&0&0\\
0&-1&1&0&0&0&0&0\\
0&0&-1&1&0&0&0&0\\
1&0&0&0&1&0&-1&0\\
0&0&0&0&-1&1&0&0\\
0&0&0&0&0&-1&1&0\\
1&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&-1
\end{pmatrix}$$

标号映射 φ 定义为

$$\varphi=\begin{pmatrix}1&2&3&4&5&6&7&8\\p_1&p_2&p_4&p_1&p_3&p_4&p_2&p_3\end{pmatrix}$$

于是,得到了可以计算 f_{AS} 的单调张成方案 $\boldsymbol{M}(\boldsymbol{M},\varphi)$,进一步可以得到实现 AS 的线性秘密共享体制。

3.2　实现一般存取结构的线性秘密共享体制 2

设 $P=\{p_1,p_2,\cdots,p_n\}$ 是参与者集合, $A_{\max}$ 是 P 上的极大攻击者结构,设 $A_{\max}=\{B_1,B_2,\cdots,B_K\}$,且 $P\backslash B_1=\{p_{i_1},p_{i_2},\cdots,p_{i_{n_1}}\},\cdots,P\backslash B_K=\{p_{i_{1+\sum_{j=1}^{k-1}n_j}},\cdots,p_{i_{\sum_{j=1}^{k}n_j}}\}$,构造相应的单调张成方案如下所示。

设 K 是有限域和 $|K|>k$, k 维非零向量 $\boldsymbol{v}=\boldsymbol{e}_1=(1,0,\cdots,0)$,令矩阵为:

$$\boldsymbol{M}=\begin{pmatrix}
1&1&0&0&\cdots&0\\
\vdots&\vdots&\vdots&\vdots&&\vdots\\
1&1&0&0&\cdots&0\\
0&-1&1&0&0&0\\
\vdots&\vdots&\vdots&\vdots&&\vdots\\
0&-1&1&0&\cdots&0\\
0&0&-1&1&\cdots&0\\
\vdots&\vdots&\vdots&\vdots&&\vdots\\
0&0&-1&1&\cdots&0\\
\vdots&\vdots&\vdots&\vdots&&\vdots\\
0&0&0&0&\cdots&-1\\
\vdots&\vdots&\vdots&\vdots&&\vdots\\
0&0&0&0&\cdots&-1
\end{pmatrix}$$

$\boldsymbol{M}$ 为 $(n_1+n_2+\cdots+n_k)\times l$ 矩阵,标号函数 φ 定义为 $\varphi(j)=$

p_{i_j}，$1\le j\le\sum_{l=1}^{k}n_l$，得到单调张成方案 $\boldsymbol{M}(\boldsymbol{M},\varphi)$。

说明 由于接入结构中的元素 $G\in AS$，对每个 i，$1\le i\le k$，$G\cap(P\backslash B_i)\neq\Phi$，因此 $\boldsymbol{M}_G$ 必定有行向量 $(1,1,0,\cdots,0),(0,-1,1,\cdots,0),\cdots,(0,0\cdots,-1)$，于是 $\boldsymbol{e}\in\text{span}(\boldsymbol{M}_G)$。对于任一攻击者结构中的元素 $B\notin AS$，必有某个 i，$1\le i\le k$，使得 $B\subseteq B_i$，从而 $\boldsymbol{M}_B$ 的第 i 列全为0，所以 $\boldsymbol{e}\notin\text{span}(\boldsymbol{M}_B)$。显然，单调张成方案 $\boldsymbol{M}(\boldsymbol{M},\varphi)$ 可计算 f_{AS}，进而由引理可以得到 $AS_{\min}$ 的线性秘密共享体制。

例2 由例1 知 $AS_{\min}$ 相应的极大攻击结构为：

$A_{\max}=\{\{p_1,p_2\},\{p_1,p_3\},\{p_2,p_4\},\{p_3,p_4\}\}$

利用3.2的方法，构造相应的单调张成方案如下：

K 为有限域，4维非零向量 $\boldsymbol{e}=\{1,0,0,0\}$，令

$$\boldsymbol{M}=\begin{pmatrix}1&1&0&0\\1&1&0&0\\0&-1&1&0\\0&-1&1&0\\0&0&-1&1\\0&0&-1&1\\0&0&0&-1\\0&0&0&-1\end{pmatrix}$$

标号映射 φ 定义为

$$\varphi=\begin{pmatrix}1&2&3&4&5&6&7&8\\p_3&p_4&p_2&p_4&p_1&p_3&p_1&p_2\end{pmatrix}$$

于是，得到了可以计算 f_{AS} 的单调张成方案 $\boldsymbol{M}(\boldsymbol{M},\varphi)$，进一步可以得到实现 AS 的线性秘密共享体制。

4 乘性的线性秘密共享体制

线性秘密共享体制是信息论意义下的安全多方计算协议的重要工具，安全多方计算的任务是保密函数赋值问题，因此计算的本质是加法和乘法。由于线性秘密共享体制是线性的，故对加法的安全多方计算的安全性是由线性秘密共享体制保证的。但是对于乘法则需要构造乘性的线性秘密共享体制加以保证。

接下来利用乘性线性秘密共享体制的定义，借助diamond运算给出了判断一个线性秘密共享体制是否为乘性的充要条件。

定义3 文献[8]设 $\boldsymbol{M}(K,\boldsymbol{M},\varphi,\boldsymbol{e})$ 是由接入结构 AS 实现的线性秘密共享体制，对于 K 上的任意 d 维向量 $\boldsymbol{x}=(x_1,x_2,\cdots,x_d)$，$\boldsymbol{y}=(y_1,y_2,\cdots,y_d)$，定义 K^d 上的二元运算“$\diamond$”为：

$$\boldsymbol{x}\diamond\boldsymbol{y}=(x_iy_j|1\le i\le d,\phi(i)=\phi(j))$$

设 $\boldsymbol{x}=(x_{11},\cdots,x_{1d_1},\cdots,x_{n1},\cdots,x_{nd_n})$，$\boldsymbol{y}=(y_{11},\cdots,y_{1d_1},\cdots,y_{n1},\cdots,y_{nd_n})$，其中 $\sum_{i=1}^{n}d_i=d$，$(x_{i1},\cdots,x_{id_i}),(y_{i1},\cdots,y_{i_{d_i}})$ 是根据 φ 分发给的 p_i 的份额的分量，则

$$\boldsymbol{x}\diamond\boldsymbol{y}=(x_{11}y_{11},\cdots,x_{11}y_{1d_1},\cdots,x_{1d_1}y_{11},\cdots,x_{1d_1}y_{1d_1},\cdots,x_{n1}y_{n1},\cdots,x_{n1}y_{nd_n},\cdots,x_{nd_n}y_{n1},\cdots,x_{nd_n}y_{nd_n})$$

记 $\boldsymbol{M}=(M_1,M_2,\cdots,M_l)$，则

$$\boldsymbol{M}_\diamond=(M_1\diamond M_1,\cdots,M_1\diamond M_l,M_2\diamond M_1,\cdots,M_2\diamond M_l,\cdots,M_l\diamond\mathrm{M}_l,\cdots,M_l\diamond M_l)$$

定义4 文献[6]设 $\boldsymbol{M}(K,\boldsymbol{M},\varphi,\boldsymbol{e})$ 是由接入结构 AS 实现的线性秘密共享体制，若存在 $\sum_{i=1}^{n}d_i^2$ 维重组向量 $\boldsymbol{z}$ 使得对任意的 $s,s'\in K,\rho,\rho'\in K^{l-1}$ 有

$$ss'=\boldsymbol{z}(\boldsymbol{M}(s,\rho)^{\mathrm{T}}\diamond\boldsymbol{M}(s',\rho')^{\mathrm{T}})$$

成立，则称 $\boldsymbol{M}$ 是乘性的。

引理2 文献[6]设 $\boldsymbol{M}(K,\boldsymbol{M},\varphi,\boldsymbol{e})$ 是由接入结构 AS 实现的线性秘密共享体制，若 $\boldsymbol{e}\in\text{span}(\boldsymbol{M}_\diamond)$，其中 $\boldsymbol{e}=(1,0,\cdots,0)$，则称 $\boldsymbol{M}$ 是乘性的。

定理1 设 $\boldsymbol{M}(K,\boldsymbol{M},\varphi,\boldsymbol{e})$ 是由接入结构 AS 实现的线性秘密共享体制，$\boldsymbol{M}_\diamond$ 是矩阵 $\boldsymbol{M}$ 的菱形积，则线性秘密共享体制是乘性的等价于 $\boldsymbol{M}_\diamond$ 生成的不是整个线性空间。

一般而言，刻画一个秘密共享体制是否是乘性的较难，刻画一个线性秘密共享体制是乘性的也不容易。由引理可知 $\boldsymbol{e}\in\text{span}(\boldsymbol{M}_\diamond)$ 时，$\boldsymbol{M}$ 是乘性的；此时若存在 $\boldsymbol{x}=(x_1,x_2,\cdots x_l)$ 使得 $\boldsymbol{M}_\diamond\boldsymbol{x}^{\mathrm{T}}=\boldsymbol{e}$ 成立即可。从而只需 $rank(\boldsymbol{M}_\diamond)<l+1$，$\boldsymbol{M}_\diamond$ 生成的不是整个空间。

推论 Shamir的门限秘密共享体制 (t,n) 在 $2t<n$ 之下是乘性的。

证明 若设 $a_1,a_2,\cdots,a_n$ 为 K 中互不相同的 $n(n<|K|)$ 个数，由文献[5]知，(t,n) 门限秘密共享体制所对应的单调张成方案的矩阵为：

$$\boldsymbol{G}=\begin{pmatrix}1&a_1&a_2&\cdots&a_n\\1&a_1^2&a_2^2&\cdots&a_n^2\\\vdots&\vdots&\vdots&&\vdots\\1&a_1^t&a_2^t&\cdots&a_n^t\end{pmatrix}$$

则

$$\boldsymbol{G}_\diamond=\begin{pmatrix}1&a_1&a_2&\cdots&a_n\\1&a_1^2&a_2^2&\cdots&a_n^2\\\vdots&\vdots&\vdots&&\vdots\\1&a_1^t&a_2^t&\cdots&a_n^t\\\vdots&\vdots&\vdots&&\vdots\\1&a_1^{2t}&a_2^{2t}&\cdots&a_n^{2t}\end{pmatrix}$$

当 $2t<n$ 时，显然 $rank(\boldsymbol{G}_\diamond)=2t<n+1$，故此时的线性秘密共享体制是乘性的。

参考文献：

[1] Shamir A.How to share a secret[J].ACM Commum,1979,22:612-613.

[2] Blakley G R.Safeguarding cryptographic keys[C]//Proceedings of AFIPS 1979,1979:313-317.

[3] Brickell E F.Some ideal secret sharing schemes[C]//Proceedings of the Conference on EUROCRYPT 1989,1989:468-475.

[4] Beimel A,Chor B.Communication in key distribution schemes[J].IEEE Trans on Info Theory,1996,42(1):19-28.

[5] Liu Mulan.Secret sharing scheme and the secure multiparty computation[M].[S.l.]:Electronic Industry Press,2008.

[6] Zhang Zhifang,Liu Mulan.Strongly multiplicative and 3-multiplicative linear secret sharing schemes[C]//Proceedings of the Conference on ASIACRYPT 2008,2008,5350:16-36.

[7] Karchmer M,Wigdersom A.On span programs[C]//Proc of the 8th Annual Structure in Complexity Theory Conference,San Diego,California,18-21 May 1993.[S.l.]:IEEE Computer Society Press,1993:102-111.

（下转160页）