# 实现分离多级存取结构的黑盒密钥共享体制

陈 祺[1),2)] 裴定一[3)] 赵淦森[2),4)] 纪求华[1),2)]

[1)](广州杰赛科技股份有限公司 广州 510310)

[2)](广州杰赛科技股份有限公司-华南师范大学服务计算联合实验室 广州 510310)

[3)](广州大学数学与信息科学学院 广州 510006)

[4)](华南师范大学计算机学院 广州 510631)

**摘 要** 黑盒密钥共享体制和有限域上的密钥共享体制是不同的.该体制只要求主密钥空间是一个有限交换群,并且可以将群运算和随机挑选群元素等过程作为黑盒调用.尤其是,它与群的结构和除数无关.迄今为止,还没有造出有效的实现非门限存取结构的黑盒密钥共享体制.文中给出了任意交换群上的实现一类非门限存取结构的黑盒密钥共享体制的构造方法.作者使用的工具是环上单调张成方案.首先,作者提出弱单调张成方案的概念,并给出了使用弱单调张成方案构造单调张成方案的方法.然后,利用有理数域上的单调张成方案和有限域上的单调张成方案,构造出了一对互素的弱单调张成方案,最终构造出了实现一类非门限存取结构——分离多级存取结构的有效黑盒密钥共享体制.作者构造的新体制可用于构造新的实现分离多级存取结构的环上安全多方计算协议、线性整密钥共享体制、分布式RSA签名协议和新的零知识证明协议.

**关键词** 黑盒密钥共享体制;单调张成方案;非门限存取结构;安全多方计算;分布式RSA签名

**中图法分类号** TP309 **DOI号**: 10.3724/SP.J.1016.2012.01804

# Black-Box Secret Sharing Scheme for Disjunctive Multi-Level Access Structure

CHEN Qi[1),2)] PEI Ding-Yi[3)] ZHAO Gan-Sen[2),4)] JI Qiu-Hua[1),2)]

[1)](*GCI Science & Technology Co., Ltd., Guangzhou* 510310)

[2)](*GCI Science & Technology Co., Ltd-South China Normal University Services Computing Joint Laboratory, Guangzhou* 510310)

[3)](*School of Mathematics and Information Sciences, Guangzhou University, Guangzhou* 510006)

[4)](*Computer School, South China Normal University, Guangzhou* 510631)

**Abstract** A black-box secret sharing scheme (BBSSS) differs from an ordinary linear secret sharing scheme over finite field. It works in exactly the same way over any finite Abelian group, as it only requires black-box access to group operations and to random group elements. In particular, there is no dependence on e.g. the structure of the group or its order. Until now, the efficient BBSSS for non-threshold access structure has not been constructed. In this paper, we give an approach to construct BBSSS for some non-threshold over arbitrary Abelian group by making use of the technique of monotone span scheme (MSP). First, we introduce the notation of weak MSPs and give the technique to construct the MSP based on weak MSPs. Then, we construct a pair of coprime weak MSPs by using the MSP over rational field and the MSP over finite field. Finally, we construct an efficient non-threshold BBSSS such as BBSSS for disjunctive multi-level access structure. Our new scheme can be applied to construct the new secure multi-party computation protocol over rings, linear integer secret sharing scheme, and distributed RSA signature for disjunctive multi-level access structure, and new zero-knowledge protocol.

**Keywords** black-box secret sharing scheme; monotone span program; non-threshold access structure; secure multi-party computation; distributed RSA signature

---

收稿日期:2012-05-15;最终修改稿收到日期:2012-07-16.本课题得到粤港关键领域重点突破招标项目(20100101-5,TC10BH07-1)和广东省-中国科学院全面战略合作项目基金(2011A090100003)资助.**陈 祺**,男,1978年生,博士,助理研究员,主要研究方向为密码学、信息安全. E-mail: chenqi.math@gmail.com. **裴定一**,男,1941年生,硕士,教授,主要研究领域为数论、密码学. **赵淦森**,男,1977年生,博士,教授,主要研究领域为云计算、信息安全. **纪求华**,男,1976年生,硕士,工程师,主要研究方向为信息安全、云计算.

# 1 引　言

在密钥共享的大多数应用中，都是事先给定了主密钥空间，然后按照访问控制要求（即存取结构）设计相应的密钥共享体制. 但是，在有些应用背景下，关于主密钥空间的信息非常有限，比如只知道它是一个有限群或有限环，它的阶数却是未知的或保密的. 例如，在门限 RSA 密码体制中 $N=pq$ 是 RSA 模数，公钥 $e\in\mathbb{Z}_{\phi(N)}$，私钥 $d\in\mathbb{Z}_{\phi(N)}$，满足 $ed\equiv(\mathrm{mod}(\phi(N))$. 为了将私钥 $d$ 进行 $(t,n)$ 门限化（即使得只有至少 $t$ 个的人联合才能解密，任何少于 $t$ 个的人都无法由密文得到明文），一个自然的想法是把私钥 $d$ 利用密钥共享体制在参与者之间共享. 但是，此时主密钥空间的规模 $\phi(N)$ 必须是保密的. 因此，需要在不知道主密钥空间规模的前提下设计一个 $(t,n)$ 门限密钥共享体制. 更一般地，我们希望设计一个密钥共享体制，它的主密钥空间可以是任意一个有限交换群.

如果一个密钥共享体制的主密钥空间是一个有限交换群（不限定群的阶数），并且可以将群运算和随机挑选群元素等过程作为黑盒调用（即给定输入即得到输出，不需要知道具体的内部处理过程），那么这样的密钥共享体制称为交换群上的黑盒密钥共享体制. 黑盒密钥共享体制与一般的有限域上的密钥共享体制[1-6]是不同的，密钥颁发者构造的 $n$ 个参与者的子密钥为整数环 $\mathbb{Z}$ 上的要分配的主密钥值的线性组合，并且主密钥值是授权集中的参与者所掌握的子密钥的 $\mathbb{Z}$ 上的线性组合. 另外，每一个参与者的子密钥是一个或多个群元素.

## 1.1 研究现状

关于这个问题的参考文献不是很多，Desmedt 和 Frankel[7-8]从门限密码体制出发研究了这个问题. 后来，Cramer 等人[9]进一步研究了这一问题，并提出了黑盒密钥共享体制的概念. Desmedt 和 Frankel[8]以及 Cramer 等人[9-10]构造了黑盒门限密钥共享体制. Cramer 和 Fehr[9]给出了黑盒密钥共享体制与环上单调张成方案（monotone span program）之间的一一对应关系. 周展飞[11]研究了理想黑盒密钥共享体制与普遍理想同态密钥共享体制（universally ideal homomorphic secret sharing schemes）及拟阵之间的关系. King 等人[12-13]也进行了相关研究，特别是估计了这类密钥共享体制随机性（randomness）的复杂度.

黑盒密钥共享体制也有很多重要的应用，可应用于环上黑盒安全多方计算（secure multi-party computation）、零知识证明（zero-knowledge）和线性整密钥共享体制（linear integer secret sharing schemes）的构造等方面. Cramer 等人[14]讨论了该体制在环上安全多方计算中的应用，Cramer 和 Damgård[15]讨论了该体制在零知识证明中的应用，Damgård 和 Thorbek[16]使用构造黑盒密钥共享体制的工具——整数环 $\mathbb{Z}$ 上的单调张成方案——构造了线性整密钥共享体制.

其中，安全多方计算[17-18]和零知识证明[19-20]都是密码学中的重要研究方向，并且都有很多的实际应用. 而线性整密钥共享体制可用于构造任意群中的指数（exponentiation）的安全分布式协议（distributed protocol）[16]. 例如，可以构造适合任意存取结构的具有任意公共指数（public exponents）的分布式 RSA 协议. 这些协议是对门限签名的推广，从而使得签名可应用于更广泛的存取结构中. 但现在也只是有理论上的结果，因为还没有人具体构造出实现非门限存取结构的线性整密钥共享体制. 另外，胡华明和周展飞[21]利用线性整密钥共享体制构造出了好的多方模求逆协议. 因此，考虑到这类体制在环上安全多方计算协议、零知识证明和线性整密钥体制等方面的应用，黑盒密钥共享体制是一个有意义的研究问题.

但迄今为止，在已有文献中只构造出实现门限存取结构的黑盒密钥共享体制，还没有发现有相关文献构造出实现非门限存取结构的黑盒密钥共享体制，尤其是有效的实现非门限存取结构的黑盒密钥共享体制. 虽然 Cramer 和 Fehr[9]将任意交换群上的黑盒密钥共享体制的构造问题转化为环上单调张成方案的构造问题，可以说已经给出了构造黑盒密钥共享体制的充分必要条件，但是他们并没有给出构造实现非门限存取结构的环上单调张成方案的具体方法. 因此，事实上他们并没有构造出实现非门限存取结构的黑盒密钥共享体制.

仅仅研究门限存取结构的黑盒密钥共享体制并不能完全解决实际问题，因为在很多应用中，所遇到的存取结构并不是门限情况的. 例如，银行金库的钥匙共享，核武器发射装置的密钥共享，电子选举中所遇到的存取结构等等. 尤其是在电子选举中（密钥共享在电子选举中有着重要的应用[22]），参与投票的人非常复杂，他们可能来自不同的国家和地区，在投票中的地位也可能互不相同，门限存取结构根本无

法处理这些情况.从而就需要研究非门限存取结构和实现非门限存取结构的密钥共享体制的构造问题.事实上,实现非门限存取结构的密钥共享体制的构造问题一直是密码学中的重要研究问题,有限域上的实现非门限存取结构的密钥共享体制已有大量的研究成果.其中,多重分拆存取结构的性质和实现这一存取结构的密钥共享体制一直是重要的研究对象,对此可参阅文献[3,23-32].该类存取结构主要包括带重量的存取结构[6,23]、多级门限存取结构[25-26,31]、多组织存取结构[3,24,26]、multilevel 存取结构[3,27]、bipartite 存取结构[29]和 tripartite 存取结构[21,24,28]等等.但是在任意交换群上,实现非门限存取结构的黑盒密钥共享体制的研究基本上处于空白阶段.

因此,找到构造实现非门限存取结构的黑盒密钥共享体制的构造方法,尤其是有效黑盒密钥共享体制的构造方法是重要而且值得研究的问题(有效密钥共享体制的概念是由 Beimel[1]提出的,在实际中有很多重要的应用).

### 1.2 主要贡献

本文研究的是任意交换群上的实现非门限存取结构的黑盒密钥共享体制的构造问题.我们构造了实现一类特殊的多重分拆存取结构——分离多极(disjunctive multi-level)存取结构的有效黑盒密钥共享体制.我们的思想是首先构造出 $\mathbb{Z}$ 上实现分离多极存取结构 $\Gamma_0$ 的单调张成方案,然后再基于 Cramer 和 Fehr[9]给出的黑盒密钥共享体制与环上单调张成方案之间的一一对应关系,构造出相应的黑盒密钥共享体制.但是构造 $\mathbb{Z}$ 上实现存取结构 $\Gamma_0$ 的单调张成方案并不是一件容易的事情.

首先我们推广了 Cramer 等人[9]提出的环上单调张成方案的定义,提出弱单调张成方案的概念,并分析了单调张成方案与弱单调张成方案之间的关系,然后通过构造弱单调张成方案来构造单调张成方案.我们证明:如果可以构造出特殊的一类环 $R$ 上的两个互素的 II 类型 $\Gamma$ 弱单调张成方案,则就可以构造出整数环上的 $\Gamma$ 单调张成方案,并给出一种基于含有单位元的交换环 $\Lambda$ 上的 I 类型 $\Gamma$ 弱单调张成方案构造 II 类型 $\Gamma$ 弱单调张成方案的方法.然后,我们构造了整数环上的实现分离多级存取结构的单调张成方案.第一步,我们构造出了一个整数环上的 II 类型弱单调张成方案 $\mathcal{M}_1$.我们先给出整数集上的 I 类型弱单调张成方案和有理数域 $\mathbb{Q}$ 上的单调张成方案之间的关系.这个关系表明:如果存在有理数域 $\mathbb{Q}$ 上的单调张成方案,则可以构造出 $\mathbb{Q}$ 上的 I 类型弱单调张成方案.然后,我们构造了 $\mathbb{Q}$ 上 $\Gamma_0$ 单调张成方案,从而构造出了 $\mathbb{Z}$ 上的 II 类型弱单调张成方案 $\mathcal{M}_1$.第二步,构造出了一个和 $\mathcal{M}_1$ 互素的 II 类型弱单调张成方案.我们先讨论了有限域上实现分离多级存取结构的单调张成方案的构造方法.事实上,Tassa[25]构造了有限域上实现 $\Gamma_0$ 的密钥共享体制.由于有限域上的单调张成方案与线性密钥共享体制是一一对应的关系[1,4-5],所以实际上 Tassa 已经构造出了有限域上的实现 $\Gamma_0$ 的单调张成方案.然后,我们给了一个重要的定理,这个定理证明了 Tassa 的 $\Gamma_0$ 单调张成方案具有一些特殊的性质,这些性质在构造和 $\mathbb{Z}$ 上的 II 类型弱单调张成方案 $\mathcal{M}_1$ 互素的 II 类型 $\Gamma_0$ 弱单调张成方案时有重要的应用.最后,我们构造出了一个和 $\mathcal{M}_1$ 互素的 II 类型弱单调张成方案.从而最终构造出了实现分离多级存取结构的黑盒密钥共享体制.

### 1.3 论文组织

在第 2 节,我们介绍了密钥共享体制和单调张成方案的一些预备知识和相关概念,然后提出弱单调张成方案的概念,并给出了单调张成方案与弱单调张成方案之间的关系;第 3 节给出了本文的主要结果,构造了整数环上的实现分离多级存取结构的单调张成方案.在第 3.1 节,我们构造出了整数环上的 II 类型弱单调张成方案 $\mathcal{M}_1$.我们先给出整数集上的 I 类型弱单调张成方案和有理数域 $\mathbb{Q}$ 上的单调张成方案之间的关系.然后,我们构造了 $\mathbb{Q}$ 上 $\Gamma_0$ 单调张成方案,从而构造出了 $\mathbb{Z}$ 上的 II 类型弱单调张成方案 $\mathcal{M}_1$.在第 3.2 节,我们讨论了有限域上实现存取结构 $\Gamma_0$ 的单调张成方案的特殊性质.这些性质在构造和 $\mathbb{Z}$ 上的 II 类型弱单调张成方案 $\mathcal{M}_1$ 互素的 II 类型 $\Gamma_0$ 弱单调张成方案时有重要的应用.在 3.3 节,我们构造出了和 $\mathcal{M}_1$ 互素的 II 类型弱单调张成方案.第 3.4 节构造出了 $\Gamma_0$ 有效黑盒密钥共享体制;第 4 节总结了本文的工作并提出了一些需要进一步研究的问题.

## 2 预备知识与相关概念

在这一节,我们首先介绍一些任意交换群上的黑盒密钥共享体制的相关概念,然后提出环上弱单调张成方案的概念,并介绍弱单调张成方案与单调

张成方案之间的关系.

**定义 1**(存取结构). 设$\mathcal{U}=\{u_1,\cdots,u_n\}$是 $n$ 个参与者的集合,$\Gamma\subseteq 2^{\mathcal{U}}$是$2^{\mathcal{U}}$的一个非空子集,其中$2^{\mathcal{U}}$表示$\mathcal{U}$的全部子集所构成的集合,即 $\Gamma$ 是由$\mathcal{U}$的某些子集构成的非空集合. 如果集合 $\Gamma$ 满足单调性,即如果$\mathcal{V}\in\Gamma$,则对任何的$\mathcal{W}\subseteq 2^{\mathcal{U}}$和$\mathcal{V}\subseteq\mathcal{W}$,都有$\mathcal{W}\in\Gamma$,则我们称 $\Gamma$ 是$\mathcal{U}$上的存取结构(access structure).

若 $\Gamma$ 是$\mathcal{U}$上的存取结构,则 $\Gamma$ 中的任何集合都称为授权集,不属于 $\Gamma$ 的$\mathcal{U}$的任何子集都称为非授权集. 设有授权集$\mathcal{V}\in\Gamma$,如果对每一个集合$\mathcal{W}\subset\mathcal{V}$,集合$\mathcal{W}$都是非授权集,那么称$\mathcal{V}\in\Gamma$为极小授权集. 设非授权集$\mathcal{V}\notin\Gamma$,如果对每一个集合$\mathcal{W}\supset\mathcal{V}$,集合$\mathcal{W}$都是授权集,那么称$\mathcal{V}\notin\Gamma$为极大非授权集.

**例 1**(门限存取结构). 设 $t$ 和 $n$ 是满足关系$0<t<n$的整数. 门限存取结构为

$$\Gamma_{t,n}=\{A\subset\mathcal{U}:|A|>t\}.$$

**定义 2.** 设$\mathcal{U}$是 $n$ 个参与者的集合,并假设$\mathcal{U}$由多个级构成,即$\mathcal{U}=\bigcup_{i=0}^{m}\mathcal{U}_i$,其中对所有 $0\le i<j\le m$,$\mathcal{U}_i\cap\mathcal{U}_j=\varnothing$. 设 $\boldsymbol{k}=\{k_i\}_{i=0}^{m}$是一个单调增的整数序列,$0<k_0<\cdots<k_m$,则$(\boldsymbol{k},n)$分离多极(disjunctive multi-level)存取结构 $\Gamma_0$定义为

$$\Gamma_0=\{\mathcal{V}\subseteq\mathcal{U}:\exists\, i\in\{0,\cdots,m\}\text{使得}$$
$$|\mathcal{V}\cap(\bigcup_{j=0}^{i}\mathcal{U}_j)|\ge k_i\}.$$

从现在起,$\Lambda$ 表示含有单位元 1 的交换环(不一定是有限的),$\Gamma$ 是$\mathcal{U}=\{u_1,\cdots,u_n\}$上的存取结构,$\boldsymbol{M}\in\mathbb{Z}^{d,e}$是整数集合上的 $d$ 行 $e$ 列矩阵,并设

$$\psi:\{1,\cdots,d\}\to\{u_1,\cdots,u_n\}$$

是满映射. 我们说 $\boldsymbol{M}$ 的第 $j$ 行($j=\{1,\cdots,d\}$)由$\psi(j)$标号或"$\psi(j)$控制第 $j$ 行". 对于$\mathcal{V}\subset\mathcal{U}$,$\boldsymbol{M}_{\mathcal{V}}$表示 $\boldsymbol{M}$ 限制在标号为$\mathcal{V}$中的成员的行所构成的矩阵.

用 $d_{\mathcal{V}}$ 表示 $\boldsymbol{M}_{\mathcal{V}}$ 的行数. 同样的,对于 $\boldsymbol{x}\in\mathbb{Z}^d$,$\boldsymbol{x}_{\mathcal{V}}\in\mathbb{Z}^{d_{\mathcal{V}}}$表示 $\boldsymbol{x}$ 限制在标号为$\mathcal{V}$中的成员的分量上. 对每个$\mathcal{V}\in\Gamma$,设 $\boldsymbol{\lambda}(\mathcal{V})\in\mathbb{Z}^{d_{\mathcal{V}}}$是一个整数集上的(列)向量. 我们称它为$\mathcal{V}$的恢复向量. 用$\mathcal{R}$表示所有恢复向量组成的集合. 另外,设 $G$ 是一个有限交换群. 我们用加法表示该群的群运算,用 $0_G$表示该群的单位元. 定义映射 $\mathbb{Z}\times G\to G$,$(\mu g)\to\mu\cdot g$,则群 $G$ 可看作是一个 $\mathbb{Z}$-模[33],其中 $0\cdot g=0_G$;当 $\mu>0$ 时,$\mu\cdot g=g+\cdots+g$($\mu$ 个 $g$ 相加);当 $\mu<0$ 时,$\mu\cdot g=-((-\mu)\cdot g)$. 我们有时也用 $\mu g$ 或 $g\mu$ 代替 $\mu\cdot g$.

**定义 3**(黑盒密钥共享体制). 设 $\Gamma$ 是$\mathcal{U}=\{u_1,\cdots,u_n\}$上的存取结构,$\mathcal{B}=(\boldsymbol{M},\psi,R)$定义如上. 则我们称$\mathcal{B}$为整数集上的 $\Gamma$-方案(integer $\Gamma$-scheme).

设 $G$ 是任意一个有限交换群,并设$\mathcal{V}\subset\mathcal{U}$是任意一个非空集合. 对任意一个要分配的主密钥 $\boldsymbol{s}\in G$,设 $\boldsymbol{g}=(g_1,\cdots,g_e)^{\mathrm{T}}\in G^e$,其中 $g_1=\boldsymbol{s}$,$g_2,\cdots,g_e$一致地随机取自群$G$. 定义 $\boldsymbol{s}=\boldsymbol{M}\boldsymbol{g}$. 对于$1\le i\le n$,参与者$u_i$得到的子密钥为 $s_{u_i}=\boldsymbol{M}_{u_i}\boldsymbol{g}$,则称$\mathcal{B}$是可实现存取结构 $\Gamma$ 的黑盒密钥共享体制(以下简称$\mathcal{B}$是 $\Gamma$ 黑盒密钥共享体制),如果下列条件成立:

(1)重构要求. 如果$\mathcal{V}\in\Gamma$,那么 $\boldsymbol{s}_{\mathcal{V}}^{\mathrm{T}}\cdot\boldsymbol{\lambda}(\mathcal{V})=\boldsymbol{s}$ 的概率为 1,其中 $\boldsymbol{\lambda}(\mathcal{V})\in\mathcal{R}$是$\mathcal{V}$的恢复向量;

(2)安全性要求. 如果$\mathcal{V}\notin\Gamma$,那么 $\boldsymbol{s}_{\mathcal{V}}$不能得到关于 $\boldsymbol{s}$ 的任何信息.

下面的定义是由 Beimel[1] 提出的,用来刻画密钥共享体制的数据扩散程度和有效性.

**定义 4**(有效的黑盒密钥共享体制). 设$\mathcal{B}=(\boldsymbol{M},\psi,R)$是 $\Gamma$ 黑盒密钥共享体制. 它的扩张因子定义为 $\eta=t/n$. 如果 $\eta<f(n)$,其中 $f(n)$是关于 $n$ 的一个多项式,则称$\mathcal{B}$是有效的黑盒密钥共享体制.

对于矩阵 $\boldsymbol{N}\in\Lambda^{a,b}$,设 $\mathrm{im}\boldsymbol{N}$ 表示它的列空间,即所有向量 $\boldsymbol{N}\boldsymbol{x}\in\Lambda^a$ 所组成的空间,其中 $\boldsymbol{x}$ 遍历 $\Lambda^b$;设 $\ker\boldsymbol{N}$ 表示满足 $\boldsymbol{N}\boldsymbol{x}=0\in\Lambda^a$ 的所有向量 $\boldsymbol{x}\in\Lambda^b$所组成的空间.

**定义 5**(单调张成方案). 我们称 $\boldsymbol{\varepsilon}=(1,0,\cdots,0)^{\mathrm{T}}\in\Lambda^e$为目标向量. 称$\mathcal{M}=(\Lambda,\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$是 $\Gamma$ 单调张成方案,如果对所有$\mathcal{V}\subset\mathcal{U}$下列条件成立:

(1)如果$\mathcal{V}\in\Gamma$,那么 $\boldsymbol{\varepsilon}\in\mathrm{im}\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}}$;

(2)如果$\mathcal{V}\notin\Gamma$,那么存在 $\boldsymbol{\kappa}=(\kappa_1,\cdots,\kappa_e)^{\mathrm{T}}\in\ker\boldsymbol{M}_{\mathcal{V}}$,其中 $\kappa_1=1$.

我们也称$\mathcal{M}$可计算 $\Gamma$.

另外,定义单调张成方案$\mathcal{M}$的规模为$\mathrm{size}(\mathcal{M})=d$,其中 $d$ 是矩阵 $\boldsymbol{M}$ 的行数.

**命题 1.** 设$\mathcal{B}=(\boldsymbol{M},\psi,R)$是整数集上的 $\Gamma$-方案,则$\mathcal{B}$是 $\Gamma$ 黑盒密钥共享体制当且仅当$\mathcal{M}=(\mathbb{Z},\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$是 $\Gamma$ 单调张成方案,并且对所有的$\mathcal{V}\in\Gamma$,它的恢复向量 $\boldsymbol{\lambda}(\mathcal{V})\in\mathcal{R}$满足 $\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}}\boldsymbol{\lambda}(\mathcal{V})=\boldsymbol{\varepsilon}$.

由定义 5 可知,要想证明$\mathcal{M}=(\Lambda,\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$是 $\Gamma$ 单调张成方案,只需证明其满足定义 5 中的两个条件. 但一般来说,这是不容易证明的.

下面介绍我们所提出的弱单调张成方案的概念,这些概念是对单调张成方案概念的推广,并且,

我们给出了这些概念和单调张成方案之间的关系.

**定义 6**(I 类型弱单调张成方案). 称$\mathcal{M}=(\Lambda,\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$是 I 类型 $\Gamma$ 弱单调张成方案,如果存在 $\vartheta_1,\vartheta_2\in\Lambda\backslash\{0\}$,使得对所有 $\mathcal{V}\subset\mathcal{U}$,下列条件成立:

(1) 如果$\mathcal{V}\in\Gamma$,则 $\vartheta_1\boldsymbol{\varepsilon}\in\mathrm{im}\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}}$;

(2) 如果$\mathcal{V}\notin\Gamma$,则存在 $\boldsymbol{\kappa}=(\kappa_1,\cdots,\kappa_e)^{\mathrm{T}}\in\ker\boldsymbol{M}_{\mathcal{V}}$,其中 $\kappa_1=\vartheta_2$.

**定义 7**(II 类型弱单调张成方案). 称$\mathcal{M}=(\Lambda,\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$是 II 类型 $\Gamma$ 弱单调张成方案,如果存在 $\vartheta\in\Lambda\backslash\{0\}$,使得对所有 $\mathcal{V}\subset\mathcal{U}$,下列条件成立:

(1) 如果$\mathcal{V}\in\Gamma$,则 $\vartheta\boldsymbol{\varepsilon}\in\mathrm{im}\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}}$;

(2) 如果$\mathcal{V}\notin\Gamma$,则存在 $\boldsymbol{\kappa}=(\kappa_1,\cdots,\kappa_e)^{\mathrm{T}}\in\ker\boldsymbol{M}_{\mathcal{V}}$,其中 $\kappa_1=1$.

**定义 8**(互素的 II 类型弱单调张成方案). 现令 $i=1$ 或 2. 设$\mathcal{M}_i=(\Lambda,\boldsymbol{M}_i,\psi_i,\boldsymbol{\varepsilon}_i)$是 II 类型 $\Gamma$ 弱单调张成方案,其中 $\boldsymbol{M}_i\in\Lambda^{d_i\times e_i}$,并且存在 $\vartheta_i\in\Lambda\backslash\{0\}$,使得对所有 $\mathcal{V}\subset\mathcal{U}$,下列条件成立:

(1) 如果$\mathcal{V}\in\Gamma$,则 $\vartheta_i\boldsymbol{\varepsilon}_i\in\mathrm{im}\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}}$;

(2) 如果$\mathcal{V}\notin\Gamma$,则存在 $\boldsymbol{\kappa}=(\kappa_1^{(i)},\cdots,\kappa_e^{(i)})^{\mathrm{T}}\in\ker\boldsymbol{M}_{\mathcal{V}}$,其中 $\kappa_1^{(i)}=1$.

如果存在 $r_1,r_2\in\Lambda$ 使得 $r_1\vartheta_1+r_2\vartheta_2=1$,则称$\mathcal{M}_1$和$\mathcal{M}_2$是互素的 II 类型弱单调张成方案.

在下一节,我们将通过构造互素的 II 类型 $\Gamma$ 弱单调张成方案来构造 $\Gamma$ 单调张成方案.

**引理 1**[9]. 设 $f(X)\in\mathbb{Z}[X]$是首项系数为 1 的不可约多项式,并记它的次数为 $\deg(f)=\boldsymbol{\lambda}$. 设环 $R=\mathbb{Z}[X]/(f(X))$. 如果$\mathcal{M}=(R,\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$是环 $R$ 上的 $\Gamma$ 单调张成方案,则存在整数集上的 $\Gamma$ 单调张成方案$\hat{\mathcal{M}}=(\mathbb{Z},\hat{\boldsymbol{M}},\hat{\psi},\hat{\boldsymbol{\varepsilon}})$,并且 $\mathrm{size}(\hat{\mathcal{M}})=\boldsymbol{\lambda}\cdot\mathrm{size}(\mathcal{M})$.

下面的两个引理可用于构造实现 $\Gamma_0$ 的单调张成方案. 为了文章的可读性,我们把引理的证明过程放到了附录中.

**引理 2.** 设 $f(X)\in\mathbb{Z}[X]$是首项系数为 1 的不可约多项式,并记它的次数为 $\deg(f)=\boldsymbol{\lambda}$. 设环 $R=\mathbb{Z}[X]/(f(X))$. 如果$\mathcal{M}_1=(R,\boldsymbol{M}_1,\psi_1,\boldsymbol{\varepsilon}_1)$和$\mathcal{M}_2=(R,\boldsymbol{M}_2,\psi_2,\boldsymbol{\varepsilon}_2)$是环 $R$ 上的两个互素的 II 类型 $\Gamma$ 弱单调张成方案,则存在环 $R$ 上的 $\Gamma$ 单调张成方案$\mathcal{M}=(R,\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$. 从而,存在一个整数集上的 $\Gamma$ 单调张成方案$\hat{\mathcal{M}}=(\mathbb{Z},\hat{\boldsymbol{M}},\hat{\psi},\hat{\boldsymbol{\varepsilon}})$并且 $\mathrm{size}(\hat{\mathcal{M}})=\boldsymbol{\lambda}\cdot\mathrm{size}(\mathcal{M})$.

**引理 3.** 设$\mathcal{M}=(\Lambda,\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$是环 $\Lambda$ 上的 I 类型 $\Gamma$ 弱单调张成方案,则可基于$\mathcal{M}$构造出一个 II 类型 $\Gamma$ 弱单调张成方案$\bar{\mathcal{M}}=(\Lambda,\bar{\boldsymbol{M}},\bar{\psi},\bar{\boldsymbol{\varepsilon}})$.

由引理 2 可知,如果可以构造出环 $R$ 上的两个互素的 II 类型 $\Gamma$ 弱单调张成方案,则就可以构造出整数集上的 $\Gamma$ 单调张成方案. 引理 3 给出一种基于环 $\Lambda$ 上的 I 类型 $\Gamma$ 弱单调张成方案构造 II 类型 $\Gamma$ 弱单调张成方案的方法.

## 3 主要结果

这一节将构造出 $\Gamma_0$ 黑盒密钥共享体制. 由于黑盒密钥共享体制的构造问题可转化为整数环上单调张成方案的构造问题,因此,如果能构造出 $\mathbb{Z}$ 上实现 $\Gamma_0$ 的单调张成方案,则就可以构造出相应的黑盒密钥共享体制. 为构造 $\mathbb{Z}$ 上实现 $\Gamma_0$ 的单调张成方案,首先,我们构造出一个 $\mathbb{Z}$ 上的 II 类型弱单调张成方案$\mathcal{M}_1$; 然后,为构造出和$\mathcal{M}_1$互素的 II 类型弱单调张成方案,我们先讨论有限域上满足某些特殊性质的实现 $\Gamma_0$ 的单调张成方案的构造方法; 最后,我们构造出和$\mathcal{M}_1$互素的 II 类型弱单调张成方案,从而构造出 $\Gamma_0$ 黑盒密钥共享体制.

### 3.1 整数环上的 II 类型弱单调张成方案$\mathcal{M}_1$

为构造出整数环 $\mathbb{Z}$ 上的 II 类型弱单调张成方案,首先,我们给出 $\mathbb{Z}$ 上的 I 类型弱单调张成方案有理数域 $\mathbb{Q}$ 上的单调张成方案之间的关系. 这个关系表明:如果存在有理数域 $\mathbb{Q}$ 上的单调张成方案,则就可以构造出 $\mathbb{Z}$ 上的 I 类型弱单调张成方案; 然后,构造了 $\mathbb{Q}$ 上 $\Gamma_0$ 单调张成方案;最终构造出了 $\mathbb{Z}$ 上的 II 类型弱单调张成方案$\mathcal{M}_1$.

**引理 4.** 设 $\boldsymbol{\varepsilon}=(1,0,\cdots,0)^{\mathrm{T}}\in\mathbb{Z}^e$. 存在 I 类型 $\Gamma$ 弱单调张成方案$\bar{\mathcal{M}}=(\mathbb{Z},\bar{\boldsymbol{M}},\psi,\boldsymbol{\varepsilon})$当且仅当存在 $\Gamma$ 单调张成方案$\mathcal{M}=(\mathbb{Q},\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$.

证明. 先证明充分性.

假设$\mathcal{M}=(\mathbb{Q},\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$是 $\Gamma$ 单调张成方案,其中 $\boldsymbol{M}\in\mathbb{Q}^{d\times e}$. 设 $a$ 表示矩阵 $\boldsymbol{M}$ 中所有元素的分母的一个任意公倍数,定义$\bar{\boldsymbol{M}}=a\boldsymbol{M}$,则$\bar{\boldsymbol{M}}\in\mathbb{Z}^{d\times e}$. 下面,将会看到$\bar{\mathcal{M}}=(\mathbb{Z},\bar{\boldsymbol{M}},\psi,\boldsymbol{\varepsilon})$是 I 类型 $\Gamma$ 弱单调张成方案.

对任意$\mathcal{V}\in\Gamma$,方程组$\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}}(X_1,X_2,\cdots,X_{|\mathcal{V}|})^{\mathrm{T}}=\boldsymbol{\varepsilon}$都存在一组非零解

$$(Y_1,Y_2,\cdots,Y_{|\mathcal{V}|})^{\mathrm{T}}\in\mathbb{Q}.$$

因此它也是方程组$\bar{\boldsymbol{M}}_{\mathcal{V}}^{\mathrm{T}}(X_1,X_2,\cdots,X_{|\mathcal{V}|})^{\mathrm{T}}=a\boldsymbol{\varepsilon}$的一组解. 设 $b_{\mathcal{V}}$表示 $Y_1,Y_2,\cdots,Y_{|\mathcal{V}|}$ 的分母的任意一个公倍数,则

$$b_{\mathcal{V}}(Y_1,Y_2,\cdots,Y_{|\mathcal{V}|})^{\mathrm{T}}\in\mathbb{Z}^{|\mathcal{V}|}$$

是方程组$\bar{\boldsymbol{M}}_{\mathcal{V}}^{\mathrm{T}}(X_1,X_2,\cdots,X_{|\mathcal{V}|})^{\mathrm{T}}=ab_{\mathcal{V}}\boldsymbol{\varepsilon}$的一组非零解. 对任意$\mathcal{V}\in\Gamma$,使用这种方法都可以得到一个 $b_{\mathcal{V}}$.

设 $b$ 表示所有 $b_{\mathcal{V}}$ 的一个任意公倍数，其中 $\mathcal{V}\in\Gamma$. 则对任意 $\mathcal{V}\in\Gamma$，有

$$ab\boldsymbol{\varepsilon}\in\mathrm{im}\overline{\boldsymbol{M}}_{\mathcal{V}}^{\mathrm{T}}.$$

如果 $\mathcal{V}\notin\Gamma$，则存在

$$\boldsymbol{\kappa}=(\kappa_1,\cdots,\kappa_e)^{\mathrm{T}}\in\ker\boldsymbol{M}_{\mathcal{V}},$$

其中 $\kappa_1=1$ 且 $(\kappa_1,\cdots,\kappa_e)^{\mathrm{T}}\in\mathbb{Q}^e$. 则有 $(\kappa_1,\cdots,\kappa_e)^{\mathrm{T}}\in\ker\overline{\boldsymbol{M}}_{\mathcal{V}}$. 设 $c_{\mathcal{V}}$ 表示 $\kappa_1,\kappa_2,\cdots,\kappa_e$ 的分母的任意一个公倍数，则

$$c_{\mathcal{V}}(\kappa_1,\cdots,\kappa_e)^{\mathrm{T}}\in\ker\overline{\boldsymbol{M}}_{\mathcal{V}}\text{且 }c_{\mathcal{V}}(\kappa_1,\cdots,\kappa_e)^{\mathrm{T}}\in\mathbb{Z}^e.$$

对任意 $\mathcal{V}\notin\Gamma$，使用这种方法总可以得到 $c_{\mathcal{V}}$. 设 $c$ 表示所有 $c_{\mathcal{V}}$ 的最小公倍数，其中 $\mathcal{V}\notin\Gamma$，则

$$c(\kappa_1,\cdots,\kappa_e)^{\mathrm{T}}\in\ker\overline{\boldsymbol{M}}_{\mathcal{V}}\text{且 }c(\kappa_1,\cdots,\kappa_e)^{\mathrm{T}}\in\mathbb{Z}^e.$$

因此 $\overline{\mathcal{M}}=(\mathbb{Z},\overline{\boldsymbol{M}},\psi,\boldsymbol{\varepsilon})$ 是 I 类型 $\Gamma$ 弱单调张成方案.

接下来证明必要性.

假设 $\overline{\mathcal{M}}=(\mathbb{Z},\overline{\boldsymbol{M}},\psi,\boldsymbol{\varepsilon})$ 是 I 类型 $\Gamma$ 弱单调张成方案，其中 $\overline{\boldsymbol{M}}\in\mathbb{Z}^{d,e}$，则当 $\mathcal{V}\in\Gamma$ 时，存在 $\vartheta_1,\vartheta_2\in\mathbb{Z}\backslash\{0\}$，使得对所有 $\mathcal{V}\subset\mathcal{U}$，有

$$\vartheta_1\boldsymbol{\varepsilon}\in\mathrm{im}\overline{\boldsymbol{M}}_{\mathcal{V}}^{\mathrm{T}};$$

当 $\mathcal{V}\notin\Gamma$ 时，存在 $\boldsymbol{\kappa}=(\kappa_1,\cdots,\kappa_e)^{\mathrm{T}}\in\ker\overline{\boldsymbol{M}}_{\mathcal{V}}$，其中 $\kappa_1=\vartheta_2$. 现设 $\overline{\boldsymbol{M}}\in\mathbb{Q}^{d,e}$，则可知：当 $\mathcal{V}\in\Gamma$ 时，

$$\boldsymbol{\varepsilon}\in\mathrm{im}\overline{\boldsymbol{M}}_{\mathcal{V}}^{\mathrm{T}};$$

当 $\mathcal{V}\notin\Gamma$ 时，

$$(\kappa_1/\vartheta_2,\cdots,\kappa_e/\vartheta_2)^{\mathrm{T}}\in\ker\overline{\boldsymbol{M}}_{\mathcal{V}}.$$

因此 $\overline{\mathcal{M}}=(\mathbb{Q},\overline{\boldsymbol{M}},\psi,\boldsymbol{\varepsilon})$ 是 $\Gamma$ 单调张成方案. 证毕.

由这一引理可知：为构造 $\mathbb{Z}$ 上 I 类型 $\Gamma$ 弱单调张成方案，只需构造 $\mathbb{Q}$ 上 $\Gamma$ 单调张成方案. 下面，我们介绍 $\mathbb{Q}$ 上 $\Gamma_0$ 单调张成方案的构造方法. 首先，我们介绍 Birkhoff 插值理论[34]，这是构造 $\mathbb{Q}$ 上 $\Gamma_0$ 单调张成方案时要用到的工具.

**Birkhoff 插值问题**：设 $X=\{x_1,\cdots,x_k\}$ 是 $\mathbb{Q}$ 上给定的点集，其中 $x_1<x_2<\cdots<x_k$；$\boldsymbol{E}=(e_{i,j})_{i=1\,j=0}^{k\quad l}$ 是一个矩阵，$I(\boldsymbol{E})=\{(i,j):e_{i,j}=1\}$，$d=|I(\boldsymbol{E})|$（从现在起假设矩阵 $\boldsymbol{E}$ 的最右列是非零的）；$C=\{c_{i,j}:(i,j)\in I(\boldsymbol{E})\}$，是一个有 $d$ 个有理数的集合，则对应于三元组 $\langle X,\boldsymbol{E},C\rangle$ 的 Birkhoff 插值问题指的是找到一个满足下面 $d$ 个等式的多项式 $P(x)\in\mathbb{R}_{d-1}[x]$ 的问题

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

其中的矩阵 $\boldsymbol{E}$ 称为插值矩阵.

**定义 9.** 插值矩阵 $\boldsymbol{E}$ 中的 $l$-序列是矩阵 $\boldsymbol{E}$ 的某一行中最长的连续 $l$ 序列；即它是一个形式三元组 $(i,j_0,j_1)$，其中，$1\leq i\leq k$，$0\leq j_0\leq j_1\leq l$，使得对所有 $j_0\leq j\leq j_1$，$e_{i,j}=1$，同时 $e_{i,j_0-1}=e_{i,j_1+1}=0$（假设 $e_{i,-1}=e_{i,l+1}=0$. 称一个 $l$-序列 $(i,j_0,j_1)$ 为支撑的（supported），如果 $\boldsymbol{E}$ 在序列的首项元素（leading entry）中的西北和西南处都有 1；即存在 $i_{nw}<i$，$i_{sw}>i$ 和 $j_{nw},j_{sw}<j_0$ 使得 $e_{i_{nw},j_{nw}}=e_{i_{sw},j_{sw}}=1$.

**引理 5**[1]. 假设 $x_1<x_2<\cdots<x_k$. 如果插值矩阵 $\boldsymbol{E}$ 满足下列条件，则 Birkhoff 插值问题有唯一解：

(1)（Pólya 条件）对每个 $0\leq t\leq l$，$l$ 是最高阶导数，$|\{(i,j)\in I(\boldsymbol{E}):j\leq t\}|\geq t+1$；

(2) $\boldsymbol{E}$ 不包含奇数长度的支撑的 $l$-序列.

下面，我们介绍 $\mathbb{Q}$ 上 $\Gamma_0$ 单调张成方案的构造方法. 首先我们构造出了有理数域 $\mathbb{Q}$ 上的实现存取结构 $\Gamma_0$ 的密钥共享体制，其构造如下：

(1) 主密钥颁发者选择一个随机多项式 $P(x)\in\mathbb{R}[x]$，其中

$$P(x)\sum_{i=0}^{k-1}a_ix^i\text{且 }a_{k-1}=S.$$

(2) 主密钥颁发者使用 $\mathbb{Q}$ 中的元素 $u$ 标识参与者 $u\in\mathcal{U}$.

(3) 主密钥颁发者用下面的方式分配子密钥给所有参与者：第 $i$ 级的每个参与者 $u\in\mathcal{U}_i$，$0\leq i\leq m$，收到子密钥 $P^{(k-k_i)}(u)$.

由这个密钥共享体制，可得到下面的方案 $\mathcal{M}=(\mathbb{Q},\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$：

设 $\boldsymbol{r}:\mathbb{Q}\to\mathbb{Q}^k$ 定义为

$$\boldsymbol{r}(x)=(x^{k-1},x^{k-2},\cdots,x,1),$$

并且对所有 $i\geq0$，设 $\boldsymbol{r}^{(i)}(x)$ 表示该向量的 $i$ 阶导数. 设

$$\mathcal{U}_0=\{u_1,\cdots,u_{t_0}\},$$
$$\mathcal{U}_1=\{u_{t_0+1},\cdots,u_{t_1}\},$$
$$\vdots$$
$$\mathcal{U}_m=\{u_{t_{m-1}+1},\cdots,u_{t_m}\},$$

$t_m=n$ 且 $u_i\in\mathbb{Q}$，$u_1<u_2<\cdots<u_n$. 定义

$$M=(\boldsymbol{r}^{(k-k_0)}(u_1),\cdots,\boldsymbol{r}^{(k-k_0)}(u_{t_0});\boldsymbol{r}^{(k-k_1)}(u_{t_0+1}),\cdots,\boldsymbol{r}^{(k-k_1)}(u_{t_1});\cdots;\boldsymbol{r}(u_{t_{m-1}+1}),\cdots,\boldsymbol{r}(u_{t_m})).$$

假设 $t_{-1}=1$，定义满函数 $\psi:\{1,\cdots,d\}\to\mathcal{U}$：$\psi(j)=u_{t_{i-1}+j}\in\mathcal{U}_i$，对 $t_{i-1}\leq j\leq t_i$ 和 $0\leq i\leq m$，并定义目标向量为 $\boldsymbol{\varepsilon}=(1,0,\cdots,0)^{\mathrm{T}}\in\mathbb{Q}^k$.

**定理 1.** $\mathcal{M}=(\mathbb{Q},\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$ 是 $\Gamma_0$ 单调张成方案.

证明. 设 $\mathcal{V}=\{v_1,\cdots,v_{|\mathcal{V}|}\}\subset\mathcal{U}$ 并假设

$$\begin{cases}v_1,\cdots,v_{l_0}\in\mathcal{U}_0\\ v_{l_0+1},\cdots,v_{l_1}\in\mathcal{U}_1\\ \vdots\\ v_{l_{m-1}+1},\cdots,v_{l_m}\in\mathcal{U}_m\end{cases}\tag{1}$$

其中 $0\leq l_0\leq\cdots\leq l_m=|\mathcal{V}|$，则$\mathcal{V}$是授权集当且仅当存在 $0\leq i\leq m$ 使得 $l_i\geq k_i$.

只需证明如果$\mathcal{V}\in\Gamma_0$是极小授权子集，则 $\boldsymbol{\varepsilon}\in\mathrm{im}\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}}$. 因为由线性代数知识可知，如果 $R$ 是域，则 $\boldsymbol{\varepsilon}\notin\mathrm{im}\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}}$表明存在 $\boldsymbol{\kappa}=(\kappa_1,\cdots,\kappa_e)^{\mathrm{T}}\in\ker\boldsymbol{M}_{\mathcal{V}}$，其中 $\kappa_1=1$. 一般地，可假设$\mathcal{V}$中的参与者由式(1)表示(其中 $l_m=k$)，并且这些标识在 $\mathbb{Q}$ 中以通常的情况排序，即 $v_1<v_2<\cdots<v_k$. 现证明在 $\mathbb{Q}$ 中 $\boldsymbol{\varepsilon}\in\mathrm{im}\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}}$.

只需考虑满足下列条件的极小授权子集$\mathcal{V}\in\Gamma_0$：

(1) $\left|\mathcal{V}\cap\left(\bigcup_{j=0}^{i}\mathcal{U}_j\right)\right|=k_i$；

(2) 对所有 $l<i$，$\left|\mathcal{V}\cap\left(\bigcup_{j=0}^{l}\mathcal{U}_j\right)\right|<k_l$.

设$\tilde{\boldsymbol{M}}_{\mathcal{V}}$表示去掉矩阵 $\boldsymbol{M}_{\mathcal{V}}$的后 $k-|\mathcal{V}|$列所得到的 $\boldsymbol{M}_{\mathcal{V}}$的$|\mathcal{V}|\times|\mathcal{V}|$子式. 因为矩阵 $\boldsymbol{M}_{\mathcal{V}}$的后 $k-|\mathcal{V}|$列都是全零向量，所以如果$\tilde{\boldsymbol{M}}_{\mathcal{V}}$是正则的，即在 $\mathbb{Q}$ 上 $\det(\tilde{\boldsymbol{M}}_{\mathcal{V}})\neq0$，则 $\boldsymbol{\varepsilon}\in\mathrm{im}\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}}$.

为了证明 $\tilde{\boldsymbol{M}}_{\mathcal{V}}$是正则的这个事实，我们注意到$\tilde{\boldsymbol{M}}_{\mathcal{V}}$所要处理的 Birkhoff 插值问题所对应的插值矩阵 $\boldsymbol{E}$ 具有梯队形式(echelon form). 确实，$\boldsymbol{E}$ 的每一行都只有一个元素为 1，并且从 $\boldsymbol{E}$ 的第 1 行到最后一行，1 的位置是单调非下降的：在前 $l_0$ 行，1 出现在第 $j=0$ 列；在接下来的 $l_1-l_0$ 行，1 出现在第 $j=l_0$ 列，依此类推. 因此矩阵 $\boldsymbol{E}$ 并没有定义 9 意义下的支撑的 1-序列. 从而，由引理 5 可知：在 $\mathbb{Q}$ 上 $\det(\tilde{\boldsymbol{M}}_{\mathcal{V}})\neq0$. 证毕.

由定理 1 和引理 4 可知，可构造出 $\mathbb{Z}$ 上的 I 类型 $\Gamma_0$ 弱单调张成方案$\mathcal{M}$. 然后，由引理 3 就可以构造 $\mathbb{Z}$ 上的 II 类型 $\Gamma_0$ 弱单调张成方案$\mathcal{M}_1$. 从而可以容易地得到下面的结果.

**推论 1.** 可构造出 $\mathbb{Z}$ 上的 II 类型 $\Gamma_0$ 弱单调张成方案$\mathcal{M}_1$.

### 3.2 有限域上具有特殊性质的 $\Gamma_0$ 单调张成方案

在这一节，我们首先介绍有限域 $\mathbb{F}_q$ 上的 $\Gamma_0$ 单调张成方案的构造方法. 事实上，Tassa[25] 构造了有限域上实现 $\Gamma_0$ 的密钥共享体制. 由于有限域上的单调张成方案与与线性密钥共享体制是一一对应的关系[1,4-5]，所以实际上 Tassa 已经构造出了有限域上的实现 $\Gamma_0$ 的单调张成方案. 然后，我们给出一个重要的定理，这个定理证明了 Tassa 的 $\Gamma_0$ 单调张成方案具有一些特殊的性质，这些性质在构造和 $\mathbb{Z}$ 上的 II 类型弱单调张成方案$\mathcal{M}_1$互素的 II 类型 $\Gamma_0$ 弱单调张成方案时有重要的应用.

首先，介绍 Tassa[25] 构造的有限域上的实现 $\Gamma_0$ 的密钥共享体制如下：

(1) 主密钥颁发者选择一个随机多项式 $P(x)\in\mathbb{F}_q[x]$，其中

$$P(x)\sum_{i=0}^{k-1}a_ix^i\text{ 且 }a_{k-1}=S.$$

(2) 主密钥颁发者使用 $\mathbb{F}_q$ 中的元素 $u$ 标识参与者 $u\in\mathcal{U}$.

(3) 主密钥颁发者用下面的方式分配子密钥给所有参与者：第 $i$ 级的每个参与者 $u\in\mathcal{U}_i$，$0\leq i\leq m$，收到子密钥 $P^{(k-k_i)}(u)$.

从而可以构造出下面的单调张成方案 $\mathcal{M}=(\mathbb{F}_q,\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$：

定义 $\boldsymbol{r}:\mathbb{F}_q\to\mathbb{F}_q^k$为

$$\boldsymbol{r}(x)=(x^{k-1},x^{k-2},\cdots,x,1),$$

并对所有 $i\geq0$，设 $\boldsymbol{r}^{(i)}(x)$表示该向量的 $i$ 阶导数. 设

$$\mathcal{U}_0=\{u_1,\cdots,u_{t_0}\},$$
$$\mathcal{U}_1=\{u_{t_0+1},\cdots,u_{t_1}\},$$
$$\vdots$$
$$\mathcal{U}_m=\{u_{t_{m-1}+1},\cdots,u_{t_m}\},$$

$t_m=n$ 且 $u_i\in\mathbb{F}_q$，$u_1<u_2<\cdots<u_n$. 定义

$$\begin{aligned}\boldsymbol{M}=(&\boldsymbol{r}^{(k-k_0)}(u_1),\cdots,\boldsymbol{r}^{(k-k_0)}(u_{t_0});\\&\boldsymbol{r}^{(k-k_1)}(u_{t_0+1}),\cdots,\boldsymbol{r}^{(k-k_1)}(u_{t_1});\cdots;\\&\boldsymbol{r}(u_{t_{m-1}+1}),\cdots,\boldsymbol{r}(u_{t_m})).\end{aligned}$$

假设 $t_{-1}=1$，定义满函数 $\psi:\{1,\cdots,d\}\to\mathcal{U}$：$\psi(j)=u_{t_{i-1}+j}\in\mathcal{U}_i$，对 $t_{i-1}\leq j\leq t_i$ 和 $0\leq i\leq m$，并定义目标向量为 $\boldsymbol{\varepsilon}=(1,0,\cdots,0)^{\mathrm{T}}\in\mathbb{F}_q^k$.

下面我们将给出一个重要的定理. 设

$$\min\Gamma_0=\{\mathcal{V}\text{是 }\Gamma_0\text{的极小授权子集：}\left|\mathcal{V}\cap\left(\bigcup_{j=0}^{i}\mathcal{U}_j\right)\right|=k_i$$
且 $\left|\mathcal{V}\cap\left(\bigcup_{j=0}^{l}\mathcal{U}_j\right)\right|<k_l$对所有 $l<i\in\{0,1,\cdots,m\}\}$，

$\Gamma_0^-=\{\mathcal{V}\notin\Gamma_0:\mathcal{V}$只差一个参与者就成为 $\min\Gamma_0$ 中的一个授权子集$\}$，

对任意$\mathcal{V}\in\min\Gamma_0$，设$\tilde{\boldsymbol{M}}_{\mathcal{V}}$表示矩阵 $\boldsymbol{M}_{\mathcal{V}}$的$|\mathcal{V}|\times|\mathcal{V}|$子式，它是通过去掉 $\boldsymbol{M}_{\mathcal{V}}$的后 $k-|\mathcal{V}|$列而得到的；对任意$\mathcal{V}\in\Gamma_0^-$，设$\hat{\boldsymbol{M}}_{\mathcal{V}}$表示矩阵 $\boldsymbol{M}_{\mathcal{V}}$的$|\mathcal{V}|\times|\mathcal{V}|$子式，它是通过去掉 $\boldsymbol{M}_{\mathcal{V}}$的第 1 列和后 $k-|\mathcal{V}|-1$ 列所得到的.

**定理 2.** 在阶数

$$q>k(k-1)(m+1)\binom{n}{\lfloor n/2\rfloor}+k-1$$

的有限域 $\mathbb{F}_q$上可以构造出满足下列条件的 $\Gamma_0$ 单调张成方案$\mathcal{M}=(\mathbb{F}_q,\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$：

(1) 对任意$\mathcal{V}\in\min\Gamma_0$，矩阵$\tilde{\boldsymbol{M}}_{\mathcal{V}}$是正则的；

(2) 对任意$\mathcal{V}\in\Gamma_0^-$，矩阵$\hat{\boldsymbol{M}}_{\mathcal{V}}$是正则的.

证明.　对任意$\mathcal{V}\in\min\Gamma_0$，假设标识$\mathcal{V}$中参与者的元素由式(1)给出，且这些标识在$\mathbb{F}_q$中以通常的情况$v_1<v_2<\cdots<v_k$排序. 设

$$\rho=\frac{k(k-1)}{2(q-k+1)}.$$

首先证明：对任意$\mathcal{V}\in\min\Gamma_0$，$\tilde{\boldsymbol{M}}_{\mathcal{V}}$的行列式不为零的概率至少为$1-\rho$，即

$$Prob(\det(\tilde{\boldsymbol{M}}_{\mathcal{V}})=0)\leq\rho.$$

我们将使用数学归纳法证明这一结论. 注意到当$k_i=0,1$时，这是显然成立的. 接下来证明当$k_i>1$时，结论也成立. 设

$$\boldsymbol{v}=(v_{i+2},\cdots,v_{i+|\mathcal{V}|}),$$
$$(v_{i+1},\boldsymbol{v})=(v_{i+1},v_{i+2},\cdots,v_{i+|\mathcal{V}|}),$$

并设$\mu_{|\mathcal{V}|-1}(\boldsymbol{v})$表示矩阵$\tilde{\boldsymbol{M}}_{\mathcal{V}}$的一个$(|\mathcal{V}|-1)\times(|\mathcal{V}|-1)$子式的行列式(该子式是通过去掉$\tilde{\boldsymbol{M}}_{\mathcal{V}}$的第1行和第1列而得到的)，则按$\tilde{\boldsymbol{M}}_{\mathcal{V}}$的第1行展开行列式，可得到一个关于$v_i$的多项式

$$\det(\tilde{\boldsymbol{M}}_{\mathcal{V}})=\sum_{j=0}^{k_i-2}c_i v_{i+1}^j+\mu_{|\mathcal{V}|-1}v_{i+1}^{k_i-1},$$

其中常量$c_i$是依赖于$\boldsymbol{v}$的. 设$\Omega$表示所有使得$\mu_{|\mathcal{V}|-1}=0$的$\boldsymbol{v}\in\mathbb{F}_q^{|\mathcal{V}|}$所构成的集合，则

$$\begin{aligned}Prob(\det(\tilde{\boldsymbol{M}}_{\mathcal{V}})=0)=&\sum_{\boldsymbol{v}\in\mathbb{F}_q^{k-1}\setminus\Omega}Prob(\det(\tilde{\boldsymbol{M}}_{\mathcal{V}})=0\,|\,\boldsymbol{v})Prob(\boldsymbol{v})+\\&\sum_{\boldsymbol{v}\in\Omega}Prob(\det(\tilde{\boldsymbol{M}}_{\mathcal{V}})=0\,|\,\boldsymbol{v})Prob(\boldsymbol{v}).\end{aligned}$$

如果$\boldsymbol{v}\in\mathbb{F}_q^{k-1}\setminus\Omega$，则$\det(\tilde{\boldsymbol{M}}_{\mathcal{V}})$是一个关于$v_{i+1}$的次数为$k_i-1$的多项式. 因此，$v_k$存在至多$k_i-1$个值使$\det(\tilde{\boldsymbol{M}}_{\mathcal{V}})=0$. 这表明

$$Prob(\det(\tilde{\boldsymbol{M}}_{\mathcal{V}})=0\,|\,\boldsymbol{v})\leq\frac{k_i-1}{q-(|\mathcal{V}|-1)}\leq\frac{k-1}{q-k+1}.$$

如果$\boldsymbol{v}\in\Omega$，则$\det(\tilde{\boldsymbol{M}}_{\mathcal{V}})$是一个关于$v_{i+1}$的次数小于$k_i-2$的多项式. 由于$\boldsymbol{v}$是$|\mathcal{V}|-1$维向量，所以由诱导假设可知

$$Prob(\det(\tilde{\boldsymbol{M}}_{\mathcal{V}})=0\,|\,\boldsymbol{v})\leq\frac{(k-1)(k-2)}{2(q-k+2)}.$$

因此可以证明

$$Prob(\det(\tilde{\boldsymbol{M}}_{\mathcal{V}})=0)\leq\frac{k-1}{q-k+1}+\frac{(k-1)(k-2)}{2(q-k+2)}\leq\rho.$$

接下来证明对任意$\mathcal{V}\in\Gamma_0^-$，$Prob(\det(\tilde{\boldsymbol{M}}_{\mathcal{V}})=0)\leq\rho$. 和上面的证明思路一样，可以证明

$$Prob(\det(\tilde{\boldsymbol{M}}_{\mathcal{V}})=0)\leq\frac{(k-1)(k-2)}{2(q-k+2)}<\rho.$$

因为$\min\Gamma_0$中极小授权子集的数量至多为

$$\sum_{i=1}^{m}\binom{n}{k_i}\leq(m+1)\binom{n}{\lfloor n/2\rfloor},$$

$\Gamma_0^-$中非授权子集的数量至多为

$$\sum_{i=1}^{m}\binom{n}{k_i-1}\leq(m+1)\binom{n}{\lfloor n/2\rfloor},$$

所以矩阵$\boldsymbol{M}$满足条件(1)和(2)的概率为

$$1-2(m+1)\binom{n}{\lfloor n/2\rfloor}\rho.$$

因此，如果

$$q>k(k-1)(m+1)\binom{n}{\lfloor n/2\rfloor}+k-1,$$

则存在一个矩阵$\boldsymbol{M}$满足题设中的两个条件. 证毕.

### 3.3　$\boldsymbol{R}$上和$\mathcal{M}_1$互素的弱$\boldsymbol{\Gamma_0}$单调张成方案

由推论1可知，可构造出$\mathbb{Z}$上的II类型$\Gamma_0$弱单调张成方案$\mathcal{M}_1$. 设$R=\mathbb{Z}[X]/(f(X))$. 自然地，也可以把$\mathcal{M}_1$作为$R$上的II类型$\Gamma_0$弱单调张成方案. 这一节将构造出和$\mathcal{M}_1$互素的$R$上II类型弱单调张成方案.

假设已经构造出一个$\mathbb{Z}$上的II类型$\Gamma_0$弱单调张成方案$\mathcal{M}_1=(\mathbb{Z},\boldsymbol{M}_1,\psi_1,\boldsymbol{\varepsilon}_1)$. 设$\vartheta\in\mathbb{Z}$使得对任意$\mathcal{V}\in\Gamma_0$，$\vartheta\boldsymbol{\varepsilon}_1\in\mathrm{im}\boldsymbol{M}_{1\mathcal{V}}^{\mathrm{T}}$. $\Phi_\vartheta$表示所有大于等于2且小于等于$\vartheta$的整素数所构成的集合. 令

$$\lambda>\left\lfloor\log\left(k(k-1)(m+1)\binom{n}{\lfloor n/2\rfloor}+k-1\right)\right\rfloor.$$

设$f(X)\in\mathbb{Z}[X]$是一个任意的首项系数为1的$\lambda$次不可约多项式，使得对所有$p\in\Phi_\vartheta$，$f_p(X)$($f(X)$的系数模$p$同余后所得到的多项式)在$\mathbb{F}_p[X]$上都是不可约的. 现将$\mathcal{M}_1$作为$R$上的II类型弱$\Gamma_0$单调张成方案.

由$f(X)$的定义可知，对所有$p\in\Phi_\vartheta$，$R/(p)$都是有限域. 确实，对所有$p\in\Phi_\vartheta$，有$R/(p)\simeq\mathbb{Z}[X]/(p,f(X))\simeq\mathbb{F}_p[X]/(f_p(X))\simeq\mathbb{F}_{p^\lambda}$. 注意：对所有$p\in\Phi_\vartheta$，环$R$中的所有理想$(p)$都是不同的极大理想. 从而由中国剩余定理可知，

$$R/(Q_\vartheta)\simeq\prod_{p\in\Phi_\vartheta}\mathbb{F}_{p^\lambda},\ \text{其中}\ Q_\vartheta=\prod_{p\in\Phi_\vartheta}p\in\mathbb{Z}.$$

假设对任意$p\in\Phi_\vartheta$，单调张成方案$\mathcal{M}^{(p)}=(\mathbb{F}_{p^\lambda},\boldsymbol{M}^{(p)},\psi,\boldsymbol{\varepsilon}^{(p)})$满足定理2，其中

$$\begin{aligned}\boldsymbol{M}^{(p)}&=(\alpha_{i,j}^{(p)})_{n\times k}\\&=(\boldsymbol{r}^{(k-k_0)}(u_1^{(p)}),\cdots,\boldsymbol{r}^{(k-k_0)}(u_{t_0}^{(p)});\\&\quad\boldsymbol{r}^{(k-k_1)}(u_{t_0+1}^{(p)}),\cdots,\boldsymbol{r}^{(k-k_1)}(u_{t_1}^{(p)});\cdots;\\&\quad\boldsymbol{r}(u_{t_{m-1}+1}^{(p)}),\cdots,\boldsymbol{r}(u_{t_m}^{(p)}))\in\mathbb{F}_{p^\lambda}^{n,k}\end{aligned}$$

并且$\boldsymbol{\varepsilon}^{(p)}=(1,0,\cdots,0)^{\mathrm{T}}\in\mathbb{F}_{p^\lambda}^k$. 选择任意的

$$\begin{aligned}\boldsymbol{M}&=(\alpha_{i,j})_{n\times k}\\&=(\boldsymbol{r}^{(k-k_0)}(u_1),\cdots,\boldsymbol{r}^{(k-k_0)}(u_{t_0});\\&\quad\boldsymbol{r}^{(k-k_1)}(u_{t_0+1}),\cdots,\boldsymbol{r}^{(k-k_1)}(u_{t_1});\cdots;\\&\quad\boldsymbol{r}(u_{t_{m-1}+1}),\cdots,\boldsymbol{r}(u_{t_m}))\in R^{n,k},\end{aligned}$$

使得

$$u_i\in R\xrightarrow{\varphi}R/(Q_\vartheta)\ni\bar{u}_i\xrightarrow{\hat{f}}(u_i^{(p)})_{p\in\Phi_\vartheta}\in\prod_{p\in\Phi_\vartheta}\mathbb{F}_{p^\lambda},$$

其中 $\varphi$ 是自然满同态，$\hat{f}$ 是隐式(implicit)同构，且 $1\leqslant i\leqslant n$.

下面将看到可以使用 $\boldsymbol{M}$ 构造出 I 类型弱单调张成方案 $\mathcal{M}=(R,\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$，然后可以基于 $\mathcal{M}$ 构造出 II 类型弱单调张成方案 $\mathcal{M}_2$.

**引理 6.** 对任意 $\mathcal{V}\in\Gamma_0$，都存在 $\vartheta_1\in R\backslash\{0\}$ 使得 $\vartheta_1\boldsymbol{\varepsilon}\in\mathrm{im}\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}}$.

证明. 由定理 2 已知对于任意 $p\in\Phi_\vartheta$，对任意 $\mathcal{V}\in\min\Gamma_0$，都有 $\widetilde{\boldsymbol{M}}_{\mathcal{V}}^{(p)}$ 是正则的，即 $\det(\widetilde{\boldsymbol{M}}_{\mathcal{V}}^{(p)})\neq0$. 现假设 $\bar{\boldsymbol{M}}=(\bar{\alpha}_{i,j})_{n\times k}$. 由于 $\hat{f}$ 是隐式同构，所以

$$\det(\bar{\widetilde{\boldsymbol{M}}}_{\mathcal{V}}^{(p)})=\hat{f}^{-1}((\det(\widetilde{\boldsymbol{M}}_{\mathcal{V}}^{(p)}))_{p\in\Phi_\vartheta})\in(R/(Q_\vartheta))^*,$$

其中 $(R/(Q_\vartheta))^*$ 表示 $R/(Q_\vartheta)$ 中的所有可逆元所构成的集合. 因此 $\det(\bar{\widetilde{\boldsymbol{M}}}_{\mathcal{V}})\neq0$. 设

$$\bar{\boldsymbol{\varepsilon}}=(1,0,\cdots,0)^{\mathrm{T}}\in R^{|\mathcal{V}|},$$

则在 $R$ 的分式域 $K$ 中(注意 $R$ 中没有零因子)方程组 $\widetilde{\boldsymbol{M}}_{\mathcal{V}}^{\mathrm{T}}(X_1,X_2,\cdots,X_{|\mathcal{V}|})^{\mathrm{T}}=\boldsymbol{\varepsilon}$ 有唯一解. 因此，由 Cramér 法则，可得到解

$$X_i=B_i/\det(\widetilde{\boldsymbol{M}}_{\mathcal{V}}^{\mathrm{T}}),\ i=1,\cdots,|\mathcal{V}|,$$

其中 $B_i\in R,i=1,\cdots,|\mathcal{V}|$. 这表明在 $R$ 中方程组 $\widetilde{\boldsymbol{M}}_{\mathcal{V}}^{\mathrm{T}}(X_1,X_2,\cdots,X_{|\mathcal{V}|})^{\mathrm{T}}=\det(\widetilde{\boldsymbol{M}}_{\mathcal{V}}^{\mathrm{T}})\boldsymbol{\varepsilon}$ 有唯一解. 因此在环 $R$ 中，$\det(\widetilde{\boldsymbol{M}}_{\mathcal{V}}^{\mathrm{T}})\bar{\boldsymbol{\varepsilon}}\in\mathrm{im}\bar{\widetilde{\boldsymbol{M}}}_{\mathcal{V}}^{\mathrm{T}}$. 设 $\boldsymbol{\varepsilon}=(1,0,\cdots,0)^{\mathrm{T}}\in R^k$. 由于 $\boldsymbol{M}_{\mathcal{V}}$ 的后 $k-|\mathcal{V}|$ 列都是零向量，所有在环 $R$ 上 $\det(\widetilde{\boldsymbol{M}}_{\mathcal{V}}^{\mathrm{T}})\boldsymbol{\varepsilon}\in\mathrm{im}\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}}$. 设

$$\vartheta_1=\prod_{\mathcal{V}\in\min\Gamma_0}\det(\widetilde{\boldsymbol{M}}_{\mathcal{V}}^{\mathrm{T}}),$$

则可得出结论：对任意 $\mathcal{V}\in\Gamma_0$，$\vartheta_1\boldsymbol{\varepsilon}\in\mathrm{im}\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}}$. 证毕.

**引理 7.** 对任意 $\mathcal{V}\notin\Gamma_0$，存在 $\vartheta_2\in R\backslash\{0\}$ 使得存在 $\boldsymbol{\kappa}=(\kappa_1,\cdots,\kappa_e)^{\mathrm{T}}\in\ker\boldsymbol{M}_{\mathcal{V}}$，其中 $\kappa_1=\vartheta_2$.

证明. 对任意 $\mathcal{V}\in\Gamma_0^-$，假设 $\boldsymbol{s}_{\mathcal{V}}$ 表示 $\boldsymbol{M}_{\mathcal{V}}$ 的第 1 列，$\hat{\boldsymbol{M}}_{\mathcal{V}}$ 表示 $\boldsymbol{M}_{\mathcal{V}}$ 的 $|\mathcal{V}|\times|\mathcal{V}|$ 子式，该子式是通过去掉 $\boldsymbol{M}_{\mathcal{V}}$ 的第 1 列和最后 $k-|\mathcal{V}|-1$ 列而得到的.

假设 $\bar{\boldsymbol{M}}=(\bar{\alpha}_{i,j})_{n\times k}$，$\hat{\bar{\boldsymbol{M}}}_{\mathcal{V}}$ 表示 $\bar{\boldsymbol{M}}$ 的 $|\mathcal{V}|\times|\mathcal{V}|$ 子式，该子式是通过去掉 $\bar{\boldsymbol{M}}$ 的最后 $k-|\mathcal{V}|-1$ 列而得到的.

由于对任意 $p\in\Phi_\vartheta$，$\hat{\boldsymbol{M}}_{\mathcal{V}}^{(p)}$ 都是正则的，所以

$$\det(\hat{\bar{\boldsymbol{M}}}_{\mathcal{V}})=\hat{f}^{-1}((\det(\hat{\bar{\boldsymbol{M}}}_{\mathcal{V}}^{(p)}))_{p\in\Phi_\vartheta})\in(R/(Q_\vartheta))^*.$$

从而 $\det(\hat{\bar{\boldsymbol{M}}}_{\mathcal{V}})\neq0$. 因此在 $R$ 的分式域 $K$ 中，方程组

$$\hat{\bar{\boldsymbol{M}}}_{\mathcal{V}}(\kappa_2,\cdots,\kappa_{|\mathcal{V}|+1})^{\mathrm{T}}=-\boldsymbol{s}_{\mathcal{V}}$$

有唯一解. 由 Cramér 法则，可得到解

$$\kappa_i=C_i/\det(\hat{\bar{\boldsymbol{M}}}_{\mathcal{V}}),\ i=2,\cdots,|\mathcal{V}|+1,$$

其中 $C_i\in R$. 这表明

$$(\det(\hat{\bar{\boldsymbol{M}}}_{\mathcal{V}})\kappa_2,\cdots,\det(\hat{\bar{\boldsymbol{M}}}_{\mathcal{V}})\kappa_{|\mathcal{V}|+1})^{\mathrm{T}}$$

是方程组 $\hat{\bar{\boldsymbol{M}}}_{\mathcal{V}}(X_2,\cdots,X_{|\mathcal{V}|+1})^{\mathrm{T}}=-\det(\hat{\bar{\boldsymbol{M}}}_{\mathcal{V}})\boldsymbol{s}_{\mathcal{V}}$ 在环 $R$ 中的一组解. 因此

$$(\det(\hat{\bar{\boldsymbol{M}}}_{\mathcal{V}}),\det(\hat{\bar{\boldsymbol{M}}}_{\mathcal{V}})\kappa_2,\cdots,\det(\hat{\bar{\boldsymbol{M}}}_{\mathcal{V}})\kappa_{|\mathcal{V}|+1})^{\mathrm{T}}\in\ker\boldsymbol{M}_{\mathcal{V}}^{\dagger}.$$

其中 $\boldsymbol{M}_{\mathcal{V}}^{\dagger}$ 表示 $\boldsymbol{M}_{\mathcal{V}}$ 的 $|\mathcal{V}|\times(|\mathcal{V}|+1)$ 子式，该子式是通过去掉 $\boldsymbol{M}_{\mathcal{V}}$ 的最后 $k-|\mathcal{V}|-1$ 而得到的.

由于 $\boldsymbol{M}_{\mathcal{V}}$ 的最后 $k-|\mathcal{V}|-1$ 列都是零向量，所以存在

$$(\det(\hat{\bar{\boldsymbol{M}}}_{\mathcal{V}}),\det(\hat{\bar{\boldsymbol{M}}}_{\mathcal{V}})\kappa_2,\cdots,\det(\hat{\bar{\boldsymbol{M}}}_{\mathcal{V}})\kappa_k)^{\mathrm{T}}\in\ker\boldsymbol{M}_{\mathcal{V}}.$$

令 $\vartheta_2=\prod_{\mathcal{V}\in\Gamma_0^-}\det(\hat{\bar{\boldsymbol{M}}}_{\mathcal{V}}^{\mathrm{T}})$，则对任意 $\mathcal{V}\in\Gamma_0^-$，都有

$$(\vartheta_2,\vartheta_2\kappa_2,\cdots,\vartheta_2\kappa_k)^{\mathrm{T}}\in\ker\boldsymbol{M}_{\mathcal{V}}.$$

另外，每一个非授权子集添加至多 $k$ 个参与者后都可成为一个授权子集(当然这个授权子集不一定是极小的). 一般地，可假设 $\mathcal{V}$ 只差一个参与者就成为授权子集. 现假设

$$t=\min\{i\in\{0,\cdots,m\}:|\mathcal{V}|<k_i\},$$

则要考虑下列两种情况：

(1) $\mathcal{V}$ 添加 $\mathcal{U}_t$ 中的一个参与者可成为一个授权子集；

(2) $\mathcal{V}$ 添加 $\mathcal{U}_i$ 中的一个参与者可成为一个授权子集，其中 $i<t$.

在第 1 种情况，$|\mathcal{V}|=k_t-1$ 且 $\mathcal{V}\in\Gamma_0^-$，因此

$$(\vartheta_2,\vartheta_2\kappa_2,\cdots,\vartheta_2\kappa_k)^{\mathrm{T}}\in\ker\boldsymbol{M}_{\mathcal{V}}.$$

接下来处理第 2 种情况. 通过对 $\mathcal{V}$ 添加 $k_t-|\mathcal{V}|-1$ 个 $\bigcup_{j=0}^{t}\mathcal{U}_j$ 中的参与者，我们构造一个非认证子集 $\mathcal{V}_0$，使得对所有 $l<t$，都有 $|\mathcal{V}_0\cap(\bigcup_{j=0}^{l}\mathcal{U}_j)|<k_l$ 成立. 由于 $|\mathcal{V}|\geqslant k_i$，所以 $k_t-k_i>k_t-|\mathcal{V}|-1$. 所以可以构造出这样的集合 $\mathcal{V}_0$. 在这种情况，$|\mathcal{V}_0|=k_t-1$ 且 $\mathcal{V}\in\Gamma_0^-$，所以

$$(\vartheta_2,\vartheta_2\kappa_2,\cdots,\vartheta_2\kappa_k)^{\mathrm{T}}\in\ker\boldsymbol{M}_{\mathcal{V}_0}.$$

从而由于 $\mathcal{V}\subset\mathcal{V}_1$，所以

$$(\vartheta_2,\vartheta_2\kappa_2,\cdots,\vartheta_2\kappa_k)^{\mathrm{T}}\in\ker\boldsymbol{M}_{\mathcal{V}}.$$

因此对任意 $\mathcal{V}\notin\Gamma_0$，都有

$$(\vartheta_2,\vartheta_2\kappa_2,\cdots,\vartheta_2\kappa_k)^{\mathrm{T}}\in\ker\boldsymbol{M}_{\mathcal{V}}.$$

证毕.

**定理 3.** 可构造出和 II 类型弱单调张成方案 $\mathcal{M}_1$ 互素的 $R$ 上 II 类型 $\Gamma_0$ 弱单调张成方案.

证明.　由引理 6 和引理 7 可知，可以使用矩阵 $\boldsymbol{M}$ 构造出 I 类型弱单调张成方案 $\mathcal{M}=(R,\boldsymbol{M},\psi,\boldsymbol{\varepsilon})$；然后根据引理 3，可基于 $\mathcal{M}$ 构造出 II 类型弱单调张成方案 $\mathcal{M}_2=(R,\boldsymbol{M}_2,\psi_2,\boldsymbol{\varepsilon}_2)$，其中对任意 $\mathcal{V}\in\Gamma_0$，$\vartheta_1\vartheta_2\boldsymbol{\varepsilon}_2\in\mathrm{im}\boldsymbol{M}_{2\mathcal{V}}^{\mathrm{T}}$.

由于 $\varphi(\vartheta_1),\varphi(\vartheta_2)\in(R/(Q_\vartheta))^*$，所以 $\varphi(\vartheta_1\vartheta_2)\in(R/(Q_\vartheta))^*$. 则存在 $a,b\in R$ 使得 $a\vartheta_1\vartheta_2=1+bQ_\vartheta$. 另外，$\vartheta$ 是 $Q_\vartheta$ 的因子，所以 $\vartheta_1\vartheta_2$ 和 $\vartheta$ 是互素的. 因此，$\mathcal{M}_2$ 和 $\mathcal{M}_1$ 是互素的 II 类型弱单调张成方案. 证毕.

### 3.4　实现分离多级存取结构的有效黑盒密钥共享体制

本节将给出实现分离多级存取结构 $\Gamma_0$ 的有效黑盒密钥共享体制，这类体制在实际中有很多的应用.

**推论 2.**　可构造出有效 $\Gamma_0$ 黑盒密钥共享体制.

证明.　因为 $\mathcal{M}_1=(\mathbb{Z},\boldsymbol{M}_1,\psi_1,\boldsymbol{\varepsilon}_1)$ 是 II 类型 $\Gamma_0$ 弱单调张成方案，且 $\mathrm{size}(\mathcal{M}_1)=n$. 另外由引理 1 可知

$$\mathrm{size}(\mathcal{M}_2)=n\left(\left\lfloor\log\left(k(k-1)(m+1)\binom{n}{\lceil n/2\rceil}+k-1\right)\right\rfloor+1\right).$$

因此根据引理 1，可构造出 $\mathbb{Z}$ 上的 $\Gamma_0$ 单调张成方案 $\mathcal{M}$，其规模为

$$n\left(\left\lfloor\log\left(k(k-1)(m+1)\binom{n}{\lceil n/2\rceil}+k-1\right)\right\rfloor+2\right).$$

基于这个 $\Gamma_0$ 单调张成方案 $\mathcal{M}$，可构造出实现 $\Gamma_0$ 的黑盒密钥共享体制. 由于这个体制的扩张因子

$$\begin{aligned}\eta&=\mathrm{size}(\mathcal{M})/n\\&=\left\lfloor\log\left(k(k-1)(m+1)\binom{n}{\lceil n/2\rceil}+k-1\right)\right\rfloor+2\\&<f(n),\end{aligned}$$

其中 $f(n)$ 是一个关于 $n$ 的多项式，所以该体制是有效的.　证毕.

## 4　结　论

本文给出了实现分离多级门限存取结构的有效黑盒密钥共享体制的构造方法，首先，推广了环上单调张成方案的定义，提出了弱单调张成方案的概念，并讨论了弱单调张成方案与单调张成方案之间的关系. 然后，利用有理数域 $\mathbb{Q}$ 上的单调张成方案和有限域上的单调张成方案，构造出了实现分离多级存取结构的黑盒密钥共享体制. 具体地，我们推广了 Cramer 等人[9]构造门限黑盒密钥共享体制的方法，结合 Tassa[25]构造的有限域上的实现分离多级存取结构的密钥共享体制(注意：Tassa 并没有构造出实现级门限存取结构的黑盒密钥共享体制)，构造出了实现分离多极存取结构的有效黑盒密钥共享体制. 是否可以使用我们的方法构造出实现其它非门限存取结构的黑盒密钥共享体制是一个值得进一步研究的问题. 另外，我们所构造的整数环上的实现分离多级门限存取结构的单调张成方案的规模并不是最小的，即所构造的相应的黑盒密钥共享体制的扩张因子并不是最优的. 因此，如何构造出扩张因为最优的实现分离多级存取结构的黑盒密钥共享体制也是一个值得进一步研究的问题.

## 参　考　文　献


[1] Beimel A. Secure schemes for secret sharing and key distribution[Ph. D. dissertation]. Technion, Haifa, 1996

[2] Blakley G R. Safeguarding cryptographic keys//Proceedings of the National Computer Conference 1979. New York, USA, 1979, 48: 313-317

[3] Brickell E F. Some ideal secret sharing schemes. Journal of Combinatorial Mathematics and Combinatorial Computing, 1989, 9(2): 105-113

[4] Gál A. Combinatorial methods in Boolean function complexity[Ph. D. dissertation]. University of Chicago, Chicago, USA, 1995

[5] Karchmer M, Wigderson A. On span programs//Proceedings of the Structures in Complexity Theory'93. San Diego, California, USA, 1993: 102-111

[6] Shamir A. How to share a secret. Communications of the ACM, 1979, 22(11): 612-613

[7] Desmedt Y, Frankel Y. Homomorphic zero-knowledge threshold schemes over any finite abelian Group. SIAM Journal on Discrete Mathematics, 1994, 7(4): 667-679

[8] Desmedt Y, Frankel Y. Threshold cryptosystems//Proceedings of the CRYPTO 1989. Santa Barbara, California, USA, 1990: 307-315

[9] Cramer R, Fehr S. Optimal black-box secret sharing over arbitrary abelian groups//Proceedings of the CRYPTO 2002. Santa Barbara, California, USA, 2002: 272-287

[10] Cramer R, Fehr S, Stam M. Primitive sets over number fields and black-box secret sharing//Proceedings of the CRYPTO 2005. Santa Barbara, California, USA, 2005: 344-360

[11] Zou Zhanfei. Classification of universally ideal homomorphic secret sharing schemes and ideal black-box secret sharing schemes//Proceedings of the CISC 2005. Beijing, China, 2005: 370-383

[12] King B. Some results in linear secret sharing[Ph. D. dissertation]. University of Wisconsin-Milwaukee, Milwaukee, USA, 2001

[13] King, B. Randomness required for linear threshold sharing schemes defined over any finite abelian group//Proceedings of the ACISP 2001. Syndey, Australia, 2001: 376-391

[14] Cramer R, Fehr S, Ishai Y, Kushilevitz E. Efficient multi-party computation over rings//Proceedings of the EUROCRYPT 2003. Warsaw, Poland, 2003: 596-613

[15] Cramer R, Damgård I. On the amortized complexity of zero-knowledge protocols//Proceedings of the CRYPTO 2009. Santa Barbara, California, USA, 2009: 177-191

[16] Damgård I, Thorbek R. Linear integer secret sharing and distributed exponentiation//Proceedings of the PKC 2006. New York, USA, 2006: 75-90

[17] Yao A. Protocols for secure computation//Proceedings of the FOGS 1982. Chicago, 1982: 160-164

[18] Goldreich O, Micali S, Wigderson A. How to play ANY mental game//Proceedings of the 19th Annual ACM Conference on Theory of Computing. New York, 1987: 218-229

[19] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof systems. SIAM Journal on Computing, 1989, 18(1): 186-208

[20] Blum M, Feldman P, Micali S. A non-interactive zero-knowledge proof systems. SIAM Journal on Computing, 1991, 20(6): 1084-1118

[21] Hu Hua-Ming, Zhou Zhan-Fei. General multi-party protocol for computing inverses over a shared secret modulus. Chinese Journal of Computers, 2010, 33(6): 1040-1049(in Chinese) (胡华明, 周展飞. 基于秘密共享模数的一般性多方求逆协议. 计算机学报, 2010, 33(6): 1040-1049

[22] Benaloh J. Secret sharing homomorphisms: Keeping shares of a secret//Proceedings of the CRYPTO 1986. Santa Barbara, California, USA, 1987: 251-260

[23] Beimel A, Tassa T, Weinreb E. Characterizing ideal weighted threshold secret sharing. SIAM Journal on Discrete Mathematics, 2008, 22(1): 360-397

[24] Herranz J, Sáez G. New results on multipartite access structures. IEEE Proceedings on Information Security, 2006, 153(4): 153-162

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

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

[27] Simmons G J. How to (really) share a secret//Proceedings of the CRYPTO 1988. Santa Barbara, California, USA, 1990: 390-448

[28] Collins M J. A note on ideal tripartite access structures. Available at http://eprint.iacr.org/2002/193/

[29] Padró C, Sáez G. Secret sharing schemes with bipartite access structure. IEEE Transactions on Information Theory, 2000, 46(4): 2596-2604

[30] Ghodosi H, Pieprzyk J, Safavi-Naini R. Secret sharing in multilevel and compartmented groups//Proceedings of the ACISP 1998. Brisbane, Queensland, Australia, 1998: 367-378

[31] Farràs O, Padró C. Ideal hierarchical secret sharing schemes//Proceedings of the TCC 2010. ETH Zurich, Switzerland, 2010: 219-236

[32] Farràs O, Martí-Farré J, Padró C. Ideal multipartite secret sharing schemes//Proceedings of the EUROCRYPT 2007. Boston, Massachusetts, 2007: 448-465

[33] Lang, S. Algebra. 2nd Edition. Boston: Addison-Wesley Publishing Co., 1984

[34] Lorentz G G, Jetter K, Riemenschneider S D. Birkhoff interpolation (Encyclopedia of Mathematics and its Applications, Vol. 19). Boston, Massachusetts: Addison-Wesley, 1983

[35] Atkinson K, Sharma A. A partial characterization of poised Hermite-Birkhoff interpolation problems. SIAM Journal on Numerical Analysis, 1969, 6(2): 230-235

## 附 录.

1. 引理 2 的证明

证明. 设 $\boldsymbol{M}_1 \in R^{d_1, e_1}$ 是一个矩阵,并且它的 $d_1$ 行由满映射

$$\psi_1 : \{1, \cdots, d_1\} \to \{u_1, \cdots, u_n\}$$

标号;$\boldsymbol{M}_2 \in R^{d_2, e_2}$ 是一个矩阵,并且它的 $d_2$ 行由满映射

$$\psi_1 : \{1, \cdots, d_1\} \to \{u_1, \cdots, u_n\}$$

标号. 根据定义 7, 我们知道当 $\mathcal{V} \in \Gamma$ 时, 存在 $\vartheta_1, \vartheta_2 \in R \backslash \{0\}$,使得

$$\vartheta_1 \boldsymbol{\varepsilon}_1 \in \mathrm{im}\boldsymbol{M}_{1\mathcal{V}}^{\mathrm{T}} \text{且 } \vartheta_2 \boldsymbol{\varepsilon}_2 \in \mathrm{im}\boldsymbol{M}_{2\mathcal{V}}^{\mathrm{T}};$$

当 $\mathcal{V} \notin \Gamma$ 时, 存在

$$\boldsymbol{\kappa} = (\kappa_1, \cdots, \kappa_{e_1})^{\mathrm{T}} \in \ker \boldsymbol{M}_{1\mathcal{V}},$$

$$\boldsymbol{\iota} = (\iota_1, \cdots, \iota_{e_2})^{\mathrm{T}} \in \ker \boldsymbol{M}_{2\mathcal{V}},$$

且 $\kappa_1 = 1$, $\iota_1 = 1$. 由于 $\mathcal{M}_1$ 和 $\mathcal{M}_2$ 是互素的 II 类型弱单调张成方案, 因此存在 $r_1, r_2 \in R$, 使得 $r_1\vartheta_1 + r_2\vartheta_2 = 1$.

现定义一个新的单调张成方案矩阵 $\boldsymbol{M} \in R^{d_1+d_2, e_1+e_2-1}$ 如下

$$\begin{pmatrix} \boldsymbol{M}_{11} & \boldsymbol{M}_{12} & \boldsymbol{0} \\ \boldsymbol{M}_{21} & \boldsymbol{0} & \boldsymbol{M}_{22} \end{pmatrix},$$

其中 $\boldsymbol{M}_{i1}$ 表示矩阵 $\boldsymbol{M}_i (i=1,2)$ 的第 1 列, $\boldsymbol{M}_{i2}$ 表示矩阵 $\boldsymbol{M}_i (i=1,2)$ 的后 $e_i - 1$ 列构成的矩阵, $\boldsymbol{0}$ 表示全零矩阵. 定义满映射 $\psi : \{1, \cdots, d_1 + d_2\} \to \{u_1, \cdots, u_n\}$ 如下:

$$\psi(i) = \begin{cases} \psi_1(i), & i = 1, \cdots, d_1 \\ \psi_2(i - d_1), & i = d_1 + 1, \cdots, d_1 + d_2 \end{cases}.$$

设矩阵 $\boldsymbol{M}$ 的 $d_1 + d_2$ 行由满映射 $\psi$ 标号. 定义目标向量

$$\boldsymbol{\varepsilon} = (1, 0, \cdots, 0)^{\mathrm{T}} \in R^{e_1+e_2-1}.$$

当 $\mathcal{V} \in \Gamma$ 时, 因为对任意 $r, s \in R$,

$$(r\vartheta_1 + s\vartheta_2, 0, \cdots, 0) \in \mathrm{im}\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}},$$

所以 $(r_1\vartheta_1 + r_2\vartheta_2, 0, \cdots, 0) \in \mathrm{im}\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}}$, 即 $\boldsymbol{\varepsilon} \in \mathrm{im}\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}}$. 当 $\mathcal{V} \notin \Gamma$ 时,可知存在 $\boldsymbol{\kappa} = (\kappa_1, \cdots, \kappa_{e_1})^{\mathrm{T}} \in \ker \boldsymbol{M}_{1\mathcal{V}}$,其中 $\kappa_1 = 1$,且存在 $\boldsymbol{\iota} = (\iota_1, \cdots, \iota_{e_2})^{\mathrm{T}} \in \ker \boldsymbol{M}_{2\mathcal{V}}$,其中 $\boldsymbol{\iota}_1 = 1$. 设

$$\boldsymbol{\gamma} = (\kappa_1, \cdots, \kappa_{e_1}, \iota_2, \cdots, \iota_{e_2})^{\mathrm{T}} \in R^{e_1+e_2-1},$$

则可推出 $\boldsymbol{\gamma} \in \ker \boldsymbol{M}_{\mathcal{V}}$.

因此 $\mathcal{M} = (R, \boldsymbol{M}, \psi, \boldsymbol{\varepsilon})$ 是 $\Gamma$ 单调张成方案. 从而,由引理

1 可知，存在整数集上的 $\Gamma$ 单调张成方案 $\hat{\mathcal{M}}=(\mathbb{Z},\hat{M},\hat{\psi},\hat{\boldsymbol{\varepsilon}})$ 且它的规模 $\mathrm{size}(\hat{\mathcal{M}})=\lambda\cdot\mathrm{size}(\mathcal{M})$. 证毕.

2. 引理 3 的证明.

证明. 由定义 6 可知，存在 $\vartheta_1,\vartheta_2\in\Lambda\backslash\{0\}$，使得：当 $\mathcal{V}\in\Gamma$ 时，$\vartheta_1\boldsymbol{\varepsilon}\in\mathrm{im}\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}}$；当 $\mathcal{V}\notin\Gamma$ 时，存在 $\boldsymbol{\kappa}=(\kappa_1,\cdots,\kappa_e)^{\mathrm{T}}\in\ker\boldsymbol{M}_{\mathcal{V}}$，其中 $\kappa_1=\vartheta_2$.

设矩阵 $\overline{\boldsymbol{M}}$ 是将矩阵 $\boldsymbol{M}$ 的第 1 列中的元素都乘以 $\vartheta_2$，而其它位置的元素保持不变所得到的新矩阵. 则当 $\mathcal{V}\notin\Gamma$ 时，存在 $\bar{\boldsymbol{\kappa}}=(1,\bar{\kappa}_2,\cdots,\bar{\kappa}_e)^{\mathrm{T}}\in\ker\overline{\boldsymbol{M}}_{\mathcal{V}}$；当 $\mathcal{V}\in\Gamma$ 时，方程组 $\boldsymbol{M}_{\mathcal{V}}^{\mathrm{T}}(X_1,X_2,\cdots,X_{|\mathcal{V}|})^{\mathrm{T}}=\vartheta_1\boldsymbol{\varepsilon}$ 存在一个非零解

$$(Y_1,Y_2,\cdots,Y_{|\mathcal{V}|})^{\mathrm{T}}\in R^{|\mathcal{V}|}.$$

因此 $(Y_1,Y_2,\cdots,Y_{|\mathcal{V}|})^{\mathrm{T}}\in R^{|\mathcal{V}|}$ 也是方程组

$$\overline{\boldsymbol{M}}_{\mathcal{V}}^{\mathrm{T}}(X_1,X_2,\cdots,X_{|\mathcal{V}|})^{\mathrm{T}}=\vartheta_1\vartheta_2\boldsymbol{\varepsilon}$$

的一个解，故 $\vartheta_1\vartheta_2\boldsymbol{\varepsilon}\in\mathrm{im}\,\overline{\boldsymbol{M}}_{\mathcal{V}}^{\mathrm{T}}$. 从而，可知 $\overline{\mathcal{M}}=(\Lambda,\overline{\boldsymbol{M}},\bar{\psi},\boldsymbol{\varepsilon})$ 是实现存取结构 $\Gamma$ 的 II 类型弱单调张成方案. 证毕.

**CHEN Qi**, born in 1978, Ph. D., assistant researcher. His research interests include cryptography and information security.

**PEI Ding-Yi**, born in 1941, M. S., professor. His research area covers number theory and cryptography.

**ZHAO Gan-Sen**, born in 1977, Ph. D., professor. His research interests include cloud computation and information security.

**JI Qiu-Hua**, born in 1976, M. S., engineer. His research interests include information security and cloud computation.

**Background**

The idea of black-box secret sharing was first considered by Desmedt and Frankel. The original motivation for looking at black-box secret sharing was their application to threshold RSA. Later, Cramer et al. further studied this problem and proposed the notation of black-box secret sharing scheme (BBSSS). Desmedt and Frankel and Cramer et al. constructed BBSSS for threshold access structure. Cramer and Fehr gave the relations between BBSSS and monotone span programs (MSP) over rings. Zhou researches the relations between ideal BBSSSs and Universally ideal homomorphic secret sharing schemes and matroids. King studied the randomness complexity of BBSSS.

There are many important applications of BBSSS in the constructions of cryptography protocols. Cramer et al. constructed a black-box ring multi-party computation protocol based on BBSSS. Cramer and Damgård discussed its application in zero-knowledge. Damgård and Thorbek constructed linear integer secret sharing scheme (LISSS) based on it, and constructed distributed RSA protocol based on the resulting LISSS. Additional, Hu and Zhou constructed better multi-party protocol for computing inverses over modulus by using LISSS. Therefore, BBSSS is very worthy of study, taking into account the value of its application.

However, only the efficient threshold BBSSS was constructed by Cramer et al. and the efficient BBSSSs for non-threshold access structure have not been constructed until now. Although Cramer and Fehr translated the construction of BBSSS into the construction of MSP over rings, and it can be said that they already gave the necessary and sufficient conditions to construct BBSSS, but they didn't gave the technique to construct the MSP over rings.

Hence how to construct efficient BBSSSs realizing non-threshold access structures is still an unresolved problem.

In this paper, we give an approach to construct BBSSS for some non-threshold access structure over arbitrary Abelian group by making use of the technique of MSP, and construct an efficient non-threshold BBSSS for disjunctive multi-level access structure. Our new scheme can be applied to construct the new secure multi-party computation protocol over rings, linear integer secret sharing scheme, and distributed RSA signature for disjunctive multi-level access structure, and new zero-knowledge protocol.

This research work was supported by the Vital and Breakthrough Tender Program of Key Area in Guangdong Province and Hong Kong (Grant No. 20100101-5, TC10BH07-1), and Strategic Co-operation Program of Guangdong Province and Chinese Academy of Sciences (Grant No. 2011A090100003).