论 文

极小特权数组上的理想多秘密共享方案

宋云^①, 李志慧^{①*}, 李永明^②^① 陕西师范大学数学与信息科学学院, 西安 710062^② 陕西师范大学计算机科学学院, 西安 710062

* 通信作者. E-mail: lizhihui@snnu.edu.cn

收稿日期: 2013-11-22; 接受日期: 2014-02-25

国家自然科学基金 (批准号: 61373150) 和陕西省科学技术研究发展计划工业攻关项目 (批准号: 2013k0611) 资助

摘要 如何构造针对一般存取结构的理想的多秘密共享方案是一个比较困难的问题. 本文首先解决了 Spiez 等最近提出的一个公开问题 [*Finite Fields and Their Application*, 2011, 17: 329–342], 即在特权数组存在的前提下, 设计求得任意长度的特权数组的算法. 进一步, 我们利用特权数组理论, 以 Pang 等和 Yang 等的方案为例, 分析了大多现有的基于 Shamir 门限体制的多秘密共享方案均不是完善的. 最后, 基于特权数组的算法, 本文提出了一个多秘密共享方案, 我们证明了该方案是理想的, 并且方案的存取结构中的授权集比门限方案的更加丰富.

关键词 (t, n) 门限 迹 存取结构 极小特权数组 多秘密共享

1 引言

单秘密共享方案 秘密共享是 n 个参与者共享主密钥的方法, 它包含一对有效算法: 一个分配算法和一个重构算法. 其中分配算法是由一个分发者执行, 即分发者确定秘密, 计算其份额并将这些份额分发给参与者; 重构算法是由参与者集合中的授权子集执行, 这些参与者将他们的份额放在一起能够重构出秘密. 参与者中的授权子集所构成的集合叫做存取结构, 其中任意真子集均不能恢复秘密的授权子集称为极小授权子集, 极小授权子集组成的集合称作极小存取结构. Shamir^[1] 及 Blakley^[2] 于 1979 年各自独立提出的秘密共享方案均是针对一种特殊的门限存取结构. 1987 年, Ito 等^[3] 把实现门限存取结构的思想推广, 构造了实现一般存取结构的秘密共享方案. 之后, 秘密共享得到了学者们更加广泛和深入的研究^[4~8]. 一个秘密共享方案称作是完善的, 如果其满足参与者中的任何非授权子集不能得到秘密的任何信息这一条件. 在一个完善的秘密共享体制中, 当密钥空间和份额空间的概率分布一致时, 如果密钥空间所在域的规模和份额空间所在域的规模相同, 则称这个秘密共享方案是理想的, 此时方案的通讯复杂性和存储复杂性都是最低的^[9].

多秘密共享方案 多秘密可看作是单秘密的一个自然扩展. 针对一般存取结构的多秘密共享体制的一般理论是 Blundo 等^[10] 提出的. 令 $\Gamma = \{\Gamma_0, \dots, \Gamma_{m-1}\}$ 是参与者集合 P 上的一个 m 元存取结构组, $S_i (0 \leq i \leq m-1)$ 是密钥空间, 秘密选自 $S_0 \times S_1 \times \dots \times S_{m-1}$, 其中第 j 个秘密 $s_j \in S_j (0 \leq j \leq m-1)$, 且存取结构 Γ_j 是参与者集合的所有子集中唯一能恢复秘密 s_j 的. 以下给出完善的多秘密共享方案的具体定义^[10].

引用格式: 宋云, 李志慧, 李永明. 极小特权数组上的理想多秘密共享方案. 中国科学: 信息科学, 2014, 44: 610–622, doi: 10.1360/N112013-00205

定义 1 设 $\Gamma = \{\Gamma_0, \dots, \Gamma_{m-1}\}$ 是参与者集合 $P = \{P_1, \dots, P_n\}$ 上的一个 m 元存取结构组. 取 $0 \leq j \leq m-1$, 称一个多秘密共享方案对于 Γ 共享 $(s_0, \dots, s_{m-1}) \in S_0 \times \dots \times S_{m-1}$ 是完善的, 如果满足:

- (i) 对所有的 $A \in \Gamma_j, H(S_j|A) = 0$;
- (ii) 对所有的 $A \notin \Gamma_j$ 和 $T \subseteq \{S_0, \dots, S_{m-1}\} \setminus \{S_j\}, H(S_j|AT) = H(S_j|T)$.

直至目前, 多秘密共享方案的相关研究在理论部分和方案的构造上都有了很大的进展^[11~19].

本文结果 虽然多秘密共享方案的研究已取得了很多成果, 但构造一般存取结构上的理想的多秘密共享方案仍然较为困难. 一些学者基于 Shamir 门限方案构造了多秘密共享方案^[13~18], 本文利用文献 [20,21] 中的特权数组理论, 指出了这些方案均不是完善的, 因而也不是理想的. 同时, 文献 [20] 得到了计算具有最大长度的特权数组的算法, 并提出如何在特权数组存在的条件下, 设计求得任意长度的特权数组的算法这一公开问题. 本文解决了这个公开问题, 并基于所得算法, 构造了一个理想的多秘密共享方案. 最后, 将我们所构造的方案与文献 [13,14] 中的 2 个方案在性能上给予了比较.

2 预备知识

2.1 Shamir 秘密共享方案

设 F_q 是一个有限域, 其中 $q = p^s$, p 是一个素数, s 是一个正整数.

在一个 (t, n) 门限秘密共享方案中^[1](方案的参与者人数为 n 且门限 t), 其中 $2 \leq t \leq n$, 秘密分发者将 n 个秘密份额分发给参与者, 并且使得 t 个或 t 个以上的参与者联合能够恢复秘密, 而少于 t 个参与者不能得到秘密的任何信息.

本文中, 我们考虑 Shamir (t, n) 秘密共享方案^[20], 即将秘密作为有限域 F_q 上的多项式 $f(x) = a_0 + a_1x + \dots + a_{t-1}x^{t-1}$ 的一个系数 a_j ($0 \leq j \leq t-1$), 任意选取有限域 F_q 中 n ($n \geq t$) 个两两不同的元素作为参与者的身份, 且将其联合构成一个序列 $(l_1, l_2, \dots, l_n)$, 令 $y_i = f(l_i)$ ($1 \leq i \leq n$), 定义参与者的秘密份额向量 $y = (y_1, \dots, y_n)$.

注 1 由文献 [20] 可知, Shamir (t, n) 门限方案和 Shamir (t, n) 秘密共享方案这 2 个概念是不同的. 前者是将秘密作为多项式 $f(x)$ 的常数项 a_0 , 而后者是将秘密作为多项式 $f(x)$ 的一个系数 a_j ($0 \leq j \leq t-1$), 因此 Shamir (t, n) 门限方案一定是 Shamir (t, n) 秘密共享方案, 反之不一定成立.

定义 2 在 Shamir (t, n) 秘密共享方案中, 有限域 F_q 上的一个序列 $\bar{L} = (l_1, \dots, l_m)$ ($m \leq n$) 称作一个迹, 如果 $\bar{L}$ 中每个分量都是分发给参与者的身份且其中任意 2 个分量均是 F_q 中互不相同的元素.

定义 3 设 $\bar{L} = (l_1, \dots, l_m)$ ($m \leq n$) 是一个迹, 称 $\bar{L}' = (l_{i_1}, \dots, l_{i_s})$ 是迹 $\bar{L}$ 的一个子迹, 其中 $s \leq m$, 且 $l_{i_j} \in \{l_1, \dots, l_m\}$ ($1 \leq j \leq s$).

由迹与子迹的定义可知, 在 Shamir (t, n) 秘密共享方案中, 序列 $\bar{L} = (l_1, \dots, l_n)$ 就是一个迹. 这时, 迹 $\bar{L}$ 中的元素恰为分发给所有参与者的身份, 其子迹 $\bar{L}'$ 为部分参与者的身份所构成的序列. 若子迹 $\bar{L}'$ 能确定出秘密, 则持有子迹 $\bar{L}'$ 中分量的参与者集合即为 Shamir (t, n) 秘密共享方案的一个授权子集.

事实上, 迹 $\bar{L} = (l_1, \dots, l_n)$ 可以确定有限域 F_q 上的 $n \times t$ 矩阵 $A(\bar{L}) = (l_{\mu}^{\nu})_{\substack{1 \leq \mu \leq n \\ 0 \leq \nu \leq t-1}}$, 并且可通过 $A(\bar{L})a^T = y^T$ 得到参与者的秘密份额. 因为 t 个份额持有者的身份所构成的迹可以确定矩阵 $A(\bar{L})$ 中的一个 t 阶非奇异的范德蒙德 Vandermonde 子式, 即,

(i) 矩阵 $A(\bar{L})$ 中的所有 t 阶子式均是非奇异的.

Shamir (t, n) 秘密共享方案是一个 (t, n) 门限方案当且仅当

(ii) 所有通过移去矩阵 $A(\bar{L})$ 的第 j 列后得到的 $t-1$ 阶子式均是非奇异的.

我们将满足上述 2 个条件的矩阵 $A(\bar{L})$ 所对应的迹 $\bar{L}$ 称作一个 (t, j) - 可允许迹^[15].

定义 4^[21] 设 $0 \leq j \leq t-1$. 如果迹 $\bar{L} \in F_q^n$ 能定义一个将秘密作为多项式 $f(x) = a_0 + a_1x + \dots + a_{t-1}x^{t-1}$ 的一个系数 $a_j (0 \leq j \leq t-1)$ 的 Shamir (t, n) 门限方案, 则称迹 $\bar{L}$ 是一个 (t, j) - 可允许迹.

同时, 如果迹 $\bar{L} = (l_1, \dots, l_n) \in F_q^n$ 不是 (t, j) - 可允许的, 则迹 $\bar{L}$ 中必包含一个少于 t 个就能恢复秘密的参与者身份所构成的子迹 L .

2.2 极小特权数组

定义 5^[20] 设 $r < t, j$ 为一定值, 其中 $0 < j < t-1$. 在一个 Shamir (t, n) 秘密共享方案中, 迹 $\bar{L}$ 的子迹 $L = (l_{i_1}, l_{i_2}, \dots, l_{i_r}) \in F_q^r$ 是一个 (t, j) - 特权数组, 如果迹 L 所对应的秘密份额能重构出秘密 a_j , 其中 a_j 为多项式 $f(x)$ 的系数.

定义 6 设 $r < t, j$ 为一定值, 其中 $0 < j < t-1$. 如果迹 $L = (l_{i_1}, l_{i_2}, \dots, l_{i_r}) \in F_q^r$ 为一个 (t, j) - 特权数组, 且迹 L 不存在子迹能恢复秘密, 则称迹 L 为一个 (t, j) - 极小特权数组.

由定义 6 可知, 持有 (t, j) - 极小特权数组中分量的参与者一定是能恢复秘密 a_j 的某个 Shamir (t, n) 秘密共享方案中的一个极小授权子集.

我们很容易得出, 长度为 t 的迹所对应的秘密份额一定可以重构出秘密, 其中秘密是多项式 $f(x)$ 的系数, 又长度为 r 的 (t, j) - 特权数组可以扩充为长度为 t 的迹, 所以有下面定义:

定义 7 设 $r < t, j$ 为一定值, 其中 $0 < j < t-1$. 长度为 t 的迹 L 是一个 (t, j) - 非扩展迹, 如果 L 不能由一个 (t, j) - 极小特权数组扩充而得到.

由定义 7 可知, 持有 (t, j) - 非扩展迹中分量的参与者一定是能恢复秘密 a_j 的某个 Shamir (t, n) 秘密共享方案中的一个极小授权子集.

因此, Shamir (t, n) 秘密共享方案中的极小授权子集是由极小特权数组和非扩展迹决定的, 所以研究极小特权数组的相关性质对于确定方案中的存取结构起着关键的作用.

定理 1^[20] 对 $0 < j < t-1, j < r \leq t-1$. 设 $L = (l_{i_1}, l_{i_2}, \dots, l_{i_r}) \in F_q^r$ 是一个迹, 且 $t \leq q$. 则迹 L 是一个 (t, j) - 特权数组当且仅当 $\tau_\omega(L) = 0$, 其中 $\tau_\omega(L)$ 表示由 $l_{i_1}, l_{i_2}, \dots, l_{i_r}$ 组成的次数为 ω 的初等对称多项式, $\omega \in \{r-j, \dots, t-1-j\}$.

2.3 求任意长度的 (t, j) - 特权数组的算法

本小节研究了文献 [20] 提出的一个公开问题, 即在特权数组存在的前提下, 我们给出求得任意长度的 (t, j) - 特权数组的一个算法, 见算法 1. 为了方便举例说明, 将重点研究那些分量的取值限制在迹 $(1, 2, \dots, N)$ 中的迹 L , 取有限域 F_p (p 是素数), 其中 $N \leq p$, 此时称 L 为关于 N 的迹. 通过算法 1 能够得到长度为 r , 关于 N 的 (t, j) - 特权数组. 由于 $\frac{t+1}{2} \leq r \leq t-1$, 最短的特权数组的长度为 $r_{\min}$, 个数为 $N_{\min}$, 则根据 (t, j) - 极小特权数组的定义, 如果从长度为 r 的 (t, j) - 特权数组剔除其中 $\binom{r-r_{\min}}{p-r_{\min}} N_{\min}$ 个非极小特权数组, 即可求得所有的有限域 F_p 上长度为 r , 关于 N 的 (t, j) - 极小特权数组.

作为具体实例, 本文在附录部分以图表的形式给出了有限域 F_p 上关于 $N = 13$ 的 $(7, j)$ -极小特权数组 ($j = 1, 2, 3, 4, 5$) 的数目以及长度最短的 $(7, 3)$ -极小特权数组, 见附录表 A1 和表 A2. 易看出, 当素数 p 超过某一数值后, 分量取值限制在迹 $(1, 2, \dots, N)$ 中的特权数组是不存在的, 故有以下定理.

算法 1

输入 正整数 t, r, j , 其中 $t \geq 3, \frac{t+1}{2} \leq r \leq t-1, t-r \leq j \leq r-1$.

输出 所有的有限域 F_p 上长度为 r , 关于 N 的 (t, j) -特权数组.

1. 计算 j 的取值集合, 并设 $a \leftarrow r-j, b \leftarrow t-1-j$, 取 J 为从 a 到 b 所有整数的集合.

2. 得到所有的有限域 F_p 上长度为 r , 关于 N 的迹.

2.1. $B = (1, 2, \dots, n)$, for $i = 1$ to N .

2.1.1 for $j = i+1$ to N .

if $B(j) > B(i)$, ($B(j)$ 表示数组 B 的第 j 个位置上的元素).

2.1.1.1 for $k = j+1$ to N .

if $B(k) > B(j)$,

$\vdots$

依次进行 $r-1$ 次循环嵌套, 则 $(\dots, \underbrace{B(k), B(j), B(i)}_r)$ 即为迹.

3. 利用一元高次方程的韦达定理的原理, 在第 2 步所得的迹中找出所有的 (t, j) -特权数组.

3.1. for $i = 1$ to $b-a+1$,

3.1.1. $p \leftarrow J(i)$, 遍历第 2 步所得的每个迹 L , 令 $C = 1$,

for $j = 1$ to r ,

$C \leftarrow C \times (x + L(j))$,

3.1.2. $f \leftarrow C$, m 为多项式 f 升幂展开式的系数所在向量,

$s \leftarrow m(r-p+1)$, 则 $v_p \leftarrow \text{mod}(s, p)$.

3.2. if $v_p = 0$, then return (L) .

定理 2 若 $p \geq \tau_{t-1-j}(Z)$, 则有限域 F_p 上分量取值限制在迹 $(1, 2, \dots, N)$ 上的 (t, j) -特权数组不存在, 其中 $Z = (N-t+2, \dots, N-1, N)$.

证明 对于 F_p 上分量取值限制在迹 $(1, 2, \dots, N)$ 的 (t, j) -特权数组, 若最大长度, 即 $t-1$ 长的特权数组不存在, 则 F_p 上的任意长度的 (t, j) -特权数组均不存在.

假设存在分量取值限制在迹 $(1, 2, \dots, N)$ 且长度为 $t-1$ 的特权数组 L . 根据定理 2.7, $\tau_\omega(L) = 0 \pmod p$, $\omega \in \{r-j, \dots, t-1-j\}$. 由于 $p \geq \tau_{t-1-j}(Z)$, 其中 $Z = (N-t+2, \dots, N-1, N)$, 又 $\tau_{t-1-j}(Z) \geq \tau_\omega(L)$ 对于所有 $\omega \in \{r-j, \dots, t-1-j\}$. 故可得 $p \geq \tau_\omega(L)$, 与 $\tau_\omega(L) = 0 \pmod p$ 矛盾. 即不存在长度为 $t-1$ 的特权数组.

注 2 定理 2 给出了分量取值受限时特权数组不存在时的素数的下界, 但由文献 [21] 的推论 2 可知, 在不对分量取值进行特别限制的情况下, 对于一个参与者人数为 n 的 Shamir (t, n) 秘密共享方案, 若 $t-1 \leq n \leq q$ 且 $1 \leq j \leq t-2$, 则 (t, j) -特权数组总是存在的, 故对特权数组的研究是很有意义的.

3 一个理想的多秘密共享方案

本文考虑的多秘密共享方案在密钥空间和份额空间的取值均是等概率的. 如果方案重构出的所有秘密的域的规模与参与者各自所持有份额所在域的规模相同时, 这个多秘密共享方案被称作是理想的^[19]. 下面我们针对参与者集合 P 上的一个存取结构组设计一个理想的多秘密共享方案.

3.1 存取结构的确定

令 $P = \{P_1, \dots, P_n\}$ 是参与者的集合, 首先我们定义方案的 $t-1$ 元存取结构组 $\Gamma = \{\Gamma_0, \dots, \Gamma_{t-2}\}$.

(1) $(\Gamma_0)_{\min} = \{A \subseteq P \mid |A| = t\}$.

(2) $(\Gamma_j)_{\min} = \{A \subseteq P \mid L_A \text{ 是 } (t, j)\text{- 极小特权数组或 } (t, j)\text{- 非扩展迹}\} \quad (1 \leq j \leq t-2)$.

其中, L_A 是极小授权子集 A 所对应的迹.

作为多项式 $f(x) = a_0 + a_1x + \dots + a_{t-1}x^{t-1}$ 的系数的秘密 a_j , 可先利用算法 1 得出 $(t, j)\text{- 非扩展迹}$ 和 $(t, j)\text{- 特权数组}$, 由于迹的分量是参与者的身份, 由此可确定出 $(\Gamma_j)_{\min}$.

显然, $A \subseteq P$ 可能恢复出多于一个秘密. 比如, 如果 $A \in \Gamma_i$ 且 $A \in \Gamma_j$, 则集合 A 中的参与者联合既能恢复 s_i 又能恢复 s_j , 其中 $0 \leq i, j \leq t-2$ 且 $i \neq j$.

例 1 令 $P = \{P_1, P_2, P_3, P_4, P_5, P_6\}$, $t = 5, q = 7$, 则由算法 1 可得有限域 F_7 上的 $(5, 1)\text{- 极小特权数组}$ 是 $(1, 2, 5, 6)$, $(1, 3, 4, 6)$ 及 $(2, 3, 4, 5)$; $(5, 2)\text{- 极小特权数组}$ 是 $(1, 2, 4)$, $(3, 5, 6)$; $(5, 3)\text{- 极小特权数组}$ 是 $(1, 2, 5, 6)$, $(1, 3, 4, 6)$ 及 $(2, 3, 4, 5)$. 不失一般性, 将特权数组中的数 i 分发给参与者 P_i , 其中 $1 \leq i \leq 6$. 方案的 4 元存取结构组 $\Gamma = \{\Gamma_0, \Gamma_1, \Gamma_2, \Gamma_3\}$ 定义如下:

$$\begin{aligned} (\Gamma_0)_{\min} &= \{\{P_1, P_2, P_3, P_4, P_5\}, \{P_1, P_2, P_3, P_4, P_6\}, \{P_1, P_2, P_4, P_5, P_6\}, \{P_1, P_2, P_3, P_5, P_6\}, \{P_1, P_3, \\ &\quad P_4, P_5, P_6\}, \{P_2, P_3, P_4, P_5, P_6\}\}, \\ (\Gamma_1)_{\min} &= (\Gamma_3)_{\min} = \{\{P_1, P_3, P_4, P_6\}, \{P_1, P_2, P_5, P_6\}, \{P_2, P_3, P_4, P_5\}\}, (\Gamma_2)_{\min} = \{\{P_1, P_2, P_4\}, \\ &\quad \{P_3, P_5, P_6\}\}. \end{aligned}$$

3.2 多秘密共享方案的构造

3.2.1 初始化阶段

设 $s_0, \dots, s_{t-2}$ 是在参与者中要共享的秘密, 其中 $(s_0, \dots, s_{t-2}) \in S_0 \times \dots \times S_{t-2}$. 分发者 D 随机在有限域 F_q 中选择 n 个两两互不相同的元素 l_i 作为参与者 P_i 的身份, 且 l_i 的值公开, $1 \leq i \leq n$. 同时, 利用算法 1, D 可得到 $(t, j)\text{- 非扩展迹}$ 和 $(t, j)\text{- 极小特权数组}$, 而后根据 3.1 小节确定出存取结构 $(\Gamma_j)_{\min}$, 其中 $0 \leq j \leq t-2$.

3.2.2 共享分配阶段

由分发者 D 执行以下步骤:

(1) 在 F_q 中随机选择一个元素, 记为 a_{t-1} . 由于 $s_0, \dots, s_{t-2}$ 为在参与者中共享的秘密, 故构造 $t-1$ 次多项式:

$$f(x) = s_0 + \dots + s_{t-2}x^{t-2} + a_{t-1}x^{t-1} \pmod{q}.$$

(2) 对于 $1 \leq i \leq n$, 计算 $y_i = f(l_i)$.

(3) 对于 $1 \leq i \leq n$, 将 y_i 通过秘密信道发送给参与者 P_i 作为他的秘密份额.

3.2.3 秘密重构阶段

设 $a = (s_0, \dots, s_{t-2}, a_{t-1}) \in F_q^t$. 对于任何 $A \in (\Gamma_j)_{\min}$ ($0 \leq j \leq t-2$), 若 $|A| = t$, 记极小授权子集 A 所对应的迹为 L_A , 不妨设 $L_A = (l_{j_1}, l_{j_2}, \dots, l_{j_t}) \in F_q^t$ 且 $1 \leq j_1 < \dots < j_t \leq n$, 则可以通过求解方程组 $A(L_A) a^T = y^T$ 恢复秘密 s_j , 其中 $A(L_A)$ 是 t 阶矩阵且可表示为 $(l_\mu^\nu)_{\substack{j_1 \leq \mu \leq j_t \\ 0 \leq \nu \leq t-1}}$, $y = (y_{j_1}, \dots, y_{j_t})$; 若 $|A| < t$, 即极小授权子集 A 所对应的是长度为 r 的 (t, j) - 极小特权数组 $L = (l_{i_1}, l_{i_2}, \dots, l_{i_r}) \in F_q^r$. 记 $L'_A = (l_{i_1}, l_{i_2}, \dots, l_{i_r}, l_{v_1}, l_{v_2}, \dots, l_{v_{t-r}}) \in F_q^t$, 可以通过求解方程组 $A(L'_A) a^T = y^T$ 恢复秘密 s_j , 其中 $A(L'_A)$ 是 t 阶矩阵且可表示为 $(l_\mu^\nu)_{\substack{\mu \in \{i_1, \dots, i_r, v_1, \dots, v_{t-r}\} \\ 0 \leq \nu \leq t-1}}$, $y = (y_{i_1}, \dots, y_{i_r}, y_{v_1}, \dots, y_{v_{t-r}})$. 由于 L_A 是特权数组, 则极小授权子集 A 中的参与者只需利用 $y_{i_1}, \dots, y_{i_r}$ 就可通过求解方程组重构出秘密 s_j .

为了证明方案的完善性, 我们首先引入广义 Vandermonde 行列式的一些结果. 一般地, 对于一个具有 k 个未定元的向量 $x = (x_1, \dots, x_k)$ 和一个 k 个递增的非负整数所构成的向量 $c = (c_1, \dots, c_k)$, 称 $V_c(x) = \det((x_\mu^{c_\nu})_{1 \leq \nu, \mu \leq k})$ 为广义 Vandermonde 行列式. 令 $e_k = (0, \dots, k-1)$, 如果 $c = e_k$, 则 $V_c(x)$ 就是经典的 Vandermonde 行列式 $V(x) = \prod_{1 \leq i < j \leq k} (x_j - x_i)$.

定理 3 上述多秘密共享方案是完善的.

证明 当 $j = 0$ 时, 根据 (t, n) 门限秘密共享方案的完善性可得该方案满足定义 1 的 2 个条件. 下面证明 $1 \leq j \leq t-2$ 时的情况.

(i) 当 $A \in \Gamma_j$ 时. 若 $|A| = t$, 通过求解方程组 $A(L_A) a^T = y^T$, 根据克拉默法则, 其唯一解就是秘密 s_j . 若授权子集 A 所对应的迹是长度为 r 的 (t, j) - 特权数组, 不妨设 $L = (l_1, l_2, \dots, l_r)$. 由定理 1 知, $\tau_\omega(L) = 0$, 其中 $\omega \in \{r-j, \dots, t-1-j\}$. 又由文献 [20] 的引理 2 知, $\tau_\omega(L) = 0$ ($\omega \in \{r-j, \dots, t-1-j\}$) 成立的充要条件是

$$\tau_{t-1-j}(L \parallel \hat{u}_m) = 0, \quad (1)$$

其中 $1 \leq m \leq t-r$, $u = (u_1, \dots, u_{t-r}) \in F_q^{t-r}$ 是一个与 $L = (l_1, \dots, l_r)$ 不相交的迹, $\hat{u}_m$ 表示将 u 的第 m 个分量移去所得的向量. 令

$$y_k = \begin{cases} f(l_k), & \text{当 } k \in \{1, \dots, r\}, \\ f(u_{k-r}), & \text{当 } k \in \{r+1, \dots, t\}, \end{cases}$$

及 $L'_A = (l_1, l_2, \dots, l_r, u_1, \dots, u_{t-r}) \in F_q^t$, 则重构阶段解方程组 $A(L'_A) a^T = y^T$ 的过程中所得秘密 s_j 为

$$\begin{aligned} s_j = & \frac{1}{V(L \parallel u)} \left(\sum_{k=1}^r (-1)^{k+j+1} V(\hat{L}_k \parallel u) \tau_{t-1-j}(\hat{L}_k \parallel u) y_k \right. \\ & \left. + \sum_{k=r+1}^t (-1)^{k+j+1} V(L \parallel \hat{u}_{k-r}) \tau_{t-1-j}(L \parallel \hat{u}_{k-r}) y_k \right), \end{aligned} \quad (2)$$

由 (1) 和 (2) 式知, $y_{r+1}, \dots, y_t$ 的系数均为 0, 故 (t, j) - 极小特权数组能恢复秘密 s_j . 即 $\forall A \in \Gamma_j, H(S_j | A) = 0$.

(ii) 当 $A \notin \Gamma_j$ 时. 由 (i) 的证明过程可知, 对于 $1 \leq j \leq t-2$, 若 $|A| < t$ 且集合 A 所对应的迹 L 不是 (t, j) - 特权数组, 则 (1) 式不成立, 那么 (2) 式中的 $y_{r+1}, \dots, y_t$ 的系数不为 0. 所以即使集合 A 中的参与者知道除 s_j 以外的其余的秘密, 也无法获得有关秘密 s_j 的任何信息. 这表明对所有的 $A \notin \Gamma_j$ 和 $T \subseteq \{S_1, \dots, S_{t-2}\} \setminus \{S_j\}$, $H(S_j | AT) = H(S_j | T)$.

表 1 方案的特性比较

Table 1 The comparison of performance among three schemes

The comparison of performance	Our scheme	Yang's scheme	Pang's scheme
Recover multi-secrets	Yes	Yes	Yes
Each participant holds only one share	Yes	Yes	Yes
Recover secrets by Lagrange interpolating polynomials	No	Yes	Yes
Different secrets are associated with different access structures	Yes	No	No
Access structures possess more vivid authorized sets	Yes	No	No
The scheme is perfect	Yes	No	No
The scheme is ideal	Yes	No	No

3.3 方案分析

由文献 [21] 可知, 对于建立在有限域 F_q 上的 Shamir (t, n) 秘密共享方案, 若参数 t, n, q 满足 $t-1 \leq n \leq q$ 且 $1 \leq j \leq t-2$, 则 (t, j) -特权数组一定存在, 即对满足上述条件的 q , 特权数组总是存在的. 在实际应用中, 可使有限域 F_q 的 q 的取值较大, 以防止穷搜索攻击. 因此, 该方案可广泛应用于电子投票, 电子拍卖以及无线传感器网络等场景中.

容易看出, 上述方案也是一个理想的多秘密共享方案. 在 2004 年和 2005 年, Yang 等 [13] 和 Pang 等 [14] 分别基于 Shamir (t, n) 门限构造了多秘密共享方案, 由于这 2 个方案均是采用 Lagrange 插值操作, 使得秘密重构时的计算量较小. 但上述 2 个方案在秘密重构阶段都需利用 Lagrange 插值公式来构造以秘密作为系数的多项式, 而由于特权数组的存在 [20], 就使得少于 t 个参与者的联合便能得到多项式的某些系数从而进一步获得秘密的有关信息, 造成信息泄露, 因此这 2 个方案都不是完善的. 下面的表 1 将 Yang 等的方案 [13], Pang 等的方案 [14] 与我们的方案在一些性能方面给予比较.

由特权数组的理论也易知, 文献 [15~18] 中构造的多秘密共享方案也均不是完善的, 因而也不是理想的.

4 结论

本文在 Shamir 秘密共享方案的基础上, 基于极小特权数组的有关概念, 构造了一个多秘密共享方案, 并证明了该方案是理想的. 同时, 为了获得方案的存取结构, 在特权数组存在的前提下, 设计出了求得任意长度的特权数组的算法. 在实际生活中, 我们可以根据需要, 对 t 取不同的值分别做实验, 将最后的数据集合成一个数据库, 每次只要调入结果即可作为参与者的身份用于方案的构造中.

参考文献

- 1 Shamir A. How to share a secret. Commun ACM, 1979, 22: 612-613
- 2 Blakley G R. Safeguarding cryptographic keys. Proc Afips Ncc, 1979, 48: 313-317
- 3 Ito M, Saito A, Nishizeki T. Secret sharing schemes realizing general access structures. In: Proceedings of the IEEE Global Telecommunications Conference, Japan, 1987. 99-102
- 4 Li Z H, Xue T, Lai H. Secret sharing scheme from binary linear codes. Inform Sci, 2010, 180: 4412-4419

- 5 Yuan J, Ding C S. Secret sharing schemes from three classes of linear codes. *IEEE Trans Inform Theory*, 2006, 52: 206–212
- 6 Parakh A, Kak S. Space efficient secret sharing for implicit data security. *Inform Sci*, 2011, 181: 335–341
- 7 Tang C M, Gao S H. Leakproof secret sharing protocols with applications to group identification scheme. *Sci China Inf Sci*, 2012, 55: 1172–1185 [唐春明, Gao S H. 防泄露的秘密共享方案及其在群身份认证协议中的应用. *中国科学: 信息科学*, 2012, 42: 634–647]
- 8 Yuan H, Zhang F T, Huang X, et al. Certificateless threshold signature scheme from bilinear maps. *Inform Sci*, 2010, 180: 4714–4728
- 9 Hsu C F, Tang X M, Cheng Q, et al. Multipartite matroids and secret sharing. *Chinese Sci Bull*, 2010, 55: 2438–2444
- 10 Blundo C, Santis A De, Crescenzo G Di, et al. Multi-secret sharing schemes. In: *Advances in Cryptology-CRYPTO'94*. Berlin: Springer, 1994. 150–163
- 11 Liu M L, Xiao L L, Zhang Z F. Linear multi-secret sharing schemes based on multi-party computation. *Finite Fields Th App*, 2006, 12: 704–713
- 12 Das A, Adhikari A. An efficient multi-use multi-secret sharing scheme based on hash function. *Appl Math Lett*, 2010, 23: 993–996
- 13 Yang C C, Chang T Y, Hwang M S. A (t, n) multi-secret sharing scheme. *Appl Math Comput*, 2004, 151: 483–490
- 14 Pang L J, Wang Y M. A new (t, n) multi-secret sharing scheme based on Shamir's secret sharing. *Appl Math Comput*, 2005, 167: 840–848
- 15 Dehkordi M H, Mashhadi S. An efficient threshold verifiable multi-secret sharing. *Comput Stand Inter*, 2008, 30: 187–190
- 16 Shao J, Cao Z F. A new efficient (t, n) verifiable multi-secret sharing (VMSS) based on YCH scheme. *Appl Math Comput*, 2005, 168: 135–140
- 17 Dehkordi M H, Mashhadi S. New efficient and practical verifiable multi-secret sharing schemes. *Inform Sci*, 2008, 178: 2262–2274
- 18 Zhao J J, Zhang J J, Zhao R. A practical verifiable multi-secret sharing scheme. *Comput Stand Inter*, 2007, 29: 138–141
- 19 Jackson W A, Martin K M, Okeefe C M. Ideal secret sharing schemes with multiple secrets. *J Crypt*, 1996, 9: 233–250
- 20 Spiez S, Timofeev A, Urbanowicz J. Non-admissible tracks in Shamir's scheme. *Finite Fields Th App*, 2011, 17: 329–342
- 21 Schinzel A, Spiez S, Urbanowicz J. Admissible tracks in Shamir's scheme. *Finite Fields Th App*, 2010, 16: 449–462

附录 A

表 A1 有限域 F_p 上关于 $N = 13$ 的 $(7, j)$ -极小特权数组的个数

Table A1 The number of $(7, j)$ -minimal privileged coalitions in the track $(1, \dots, 13)$ over F_p for $1 \leq j \leq 5$

p	$j=1$	$j=2$	$j=3$	$j=4$	$j=5$	p	$j=1$	$j=2$	$j=3$	$j=4$	$j=5$
13	72	114	71	93	132	137	15	10	11	18	0
17	101	69	76	72	98	139	18	12	10	13	0
19	90	53	72	57	92	149	13	13	8	8	0
23	72	61	58	63	83	151	12	9	13	13	0
29	60	43	51	46	26	157	14	10	13	10	0
31	58	51	40	39	32	163	13	16	9	7	0
37	51	49	38	27	76	167	13	12	9	11	0
41	44	36	38	27	94	173	8	13	11	10	0
43	41	40	35	34	94	179	7	11	9	10	0
47	41	32	36	39	76	181	7	8	12	9	0
53	26	35	35	27	31	191	5	4	11	10	0
59	32	25	28	24	5	193	12	8	7	8	0
61	27	32	31	28	2	197	10	10	11	9	0
67	21	32	25	22	0	199	7	13	9	8	0
71	26	22	22	23	0	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
73	23	24	21	31	0	809	1	2	3	0	0
79	24	20	22	15	0	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
83	23	21	24	25	0	5231	0	0	1	0	0
89	18	12	15	18	0	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
97	18	24	15	17	0	31601	0	1	0	0	0
101	19	10	21	17	0	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
103	18	20	14	20	0	199999	0	0	0	0	0
107	21	14	12	18	0	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
109	18	18	9	16	0	499253	0	0	0	0	0
113	12	14	16	16	0	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
127	12	12	16	19	0	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
131	13	7	11	12	0	≥ 725597	0	0	0	0	0

表 A2 有限域 F_p 上关于 $N = 13$ 的长度最短的 $(7, 3)$ -特权数组
Table A2 $(7, 3)$ -privileged coalitions with the shortest length in the track $(1, \dots, 13)$ over F_p

p	Nr.	The $(7, 3)$ -privileged coalitions with the shortest length in the track $(1, \dots, 13)$ over F_p
13	3	$\{12, 8, 5, 1\} \{11, 10, 3, 2\} \{9, 7, 6, 4\}$
17	1	$\{11, 10, 7, 6\}$
19	3	$\{13, 5, 4, 3, 1\} \{13, 9, 8, 5, 2\} \{10, 8, 7, 6, 2\}$
23	2	$\{10, 9, 8, 6, 1\} \{13, 11, 8, 7, 1\}$
29	3	$\{11, 4, 3, 2, 1\} \{11, 9, 7, 5, 1\} \{12, 9, 6, 4, 3\}$
31	1	$\{9, 8, 5, 3, 1\}$
37	2	$\{12, 10, 8, 5, 1\} \{7, 6, 4, 3, 2\}$
41	1	$\{11, 9, 7, 6, 4\}$
43	35	$\{10, 5, 4, 3, 2, 1\} \{12, 6, 5, 3, 2, 1\} \{11, 10, 9, 5, 3, 1\} \{13, 7, 5, 4, 2, 1\} \{12, 11, 6, 4, 2, 1\}$ $\{11, 9, 7, 4, 2, 1\} \{13, 11, 9, 5, 2, 1\} \{11, 10, 7, 6, 2, 1\} \{11, 8, 6, 3, 2, 1\} \{12, 10, 8, 6, 5, 4\}$ $\{13, 12, 11, 6, 5, 4\} \{13, 10, 8, 7, 6, 4\} \{11, 9, 8, 5, 4, 1\} \{13, 9, 8, 6, 4, 1\} \{11, 10, 8, 7, 4, 1\}$ $\{12, 11, 10, 9, 4, 1\} \{12, 11, 8, 6, 5, 1\} \{13, 11, 9, 7, 6, 1\} \{13, 11, 10, 8, 6, 1\} \{13, 9, 5, 4, 3, 2\}$ $\{12, 10, 8, 6, 3, 2\} \{10, 9, 8, 7, 3, 2\} \{13, 12, 10, 5, 4, 2\} \{13, 11, 9, 6, 4, 2\} \{12, 10, 8, 7, 4, 2\}$ $\{12, 9, 8, 6, 5, 2\} \{13, 10, 8, 6, 5, 2\} \{11, 9, 8, 7, 6, 2\} \{8, 7, 5, 4, 3, 1\} \{11, 10, 9, 8, 4, 3\}$ $\{12, 11, 10, 6, 5, 3\} \{13, 12, 11, 8, 6, 3\} \{11, 10, 9, 8, 7, 5\} \{11, 7, 6, 5, 4, 3\} \{12, 11, 8, 4, 3, 2\}$
47	1	$\{13, 11, 9, 8, 2\}$
53	35	$\{11, 6, 5, 3, 2, 1\} \{12, 10, 7, 3, 2, 1\} \{7, 6, 5, 4, 2, 1\} \{12, 11, 8, 4, 2, 1\} \{12, 8, 6, 5, 2, 1\}$ $\{3, 9, 6, 5, 2, 1\} \{11, 9, 7, 5, 2, 1\} \{11, 10, 9, 6, 2, 1\} \{12, 11, 5, 4, 3, 1\} \{12, 9, 7, 5, 3, 1\}$ $\{13, 10, 8, 6, 3, 1\} \{10, 9, 8, 7, 3, 1\} \{13, 12, 11, 10, 3, 1\} \{9, 8, 7, 6, 4, 1\} \{13, 10, 9, 6, 4, 1\}$ $\{13, 12, 10, 6, 5, 1\} \{13, 12, 9, 8, 6, 1\} \{13, 12, 10, 4, 3, 2\} \{9, 8, 6, 5, 3, 2\} \{13, 9, 8, 7, 3, 2\}$ $\{13, 11, 8, 7, 4, 2\} \{13, 10, 8, 7, 5, 3\} \{13, 11, 8, 7, 6, 3\} \{12, 11, 10, 7, 6, 3\} \{10, 8, 7, 5, 4, 2\}$ $\{13, 12, 7, 5, 4, 2\} \{11, 10, 9, 5, 4, 2\} \{13, 11, 10, 9, 8, 2\} \{12, 11, 9, 7, 6, 2\} \{13, 12, 10, 8, 6, 2\}$ $\{11, 8, 6, 5, 4, 3\} \{12, 10, 9, 5, 4, 3\} \{11, 10, 8, 7, 4, 3\} \{11, 9, 7, 6, 5, 3\} \{13, 12, 11, 9, 2, 1\}$
59	28	$\{10, 7, 6, 3, 2, 1\} \{11, 8, 5, 4, 2, 1\} \{12, 10, 5, 4, 2, 1\} \{10, 8, 7, 4, 2, 1\} \{11, 7, 6, 5, 2, 1\}$ $\{13, 6, 5, 4, 3, 1\} \{13, 8, 7, 6, 3, 1\} \{12, 9, 8, 7, 6, 5\} \{12, 9, 8, 6, 3, 1\} \{12, 8, 7, 5, 4, 1\}$ $\{13, 10, 9, 7, 4, 1\} \{13, 12, 8, 6, 5, 1\} \{12, 11, 9, 8, 5, 1\} \{10, 9, 8, 7, 5, 3\} \{11, 10, 7, 4, 3, 2\}$ $\{13, 12, 11, 10, 6, 5\} \{13, 11, 8, 4, 3, 2\} \{13, 11, 10, 6, 3, 2\} \{13, 12, 10, 8, 3, 2\} \{13, 10, 7, 6, 5, 2\}$ $\{13, 11, 10, 8, 5, 2\} \{13, 12, 11, 9, 8, 2\} \{12, 9, 7, 5, 4, 3\} \{13, 12, 11, 7, 4, 3\} \{11, 10, 9, 8, 4, 3\}$ $\{12, 10, 9, 5, 3, 2\} \{12, 11, 10, 9, 8, 7\} \{11, 10, 8, 6, 5, 4\}$
61	31	$\{10, 9, 5, 3, 2, 1\} \{11, 10, 6, 3, 2, 1\} \{12, 10, 7, 4, 2, 1\} \{12, 9, 6, 5, 2, 1\} \{13, 11, 7, 5, 2, 1\}$ $\{13, 12, 8, 6, 2, 1\} \{13, 11, 9, 4, 2, 1\} \{13, 8, 6, 4, 3, 1\} \{12, 11, 6, 5, 3, 1\} \{11, 9, 8, 5, 3, 1\}$ $\{12, 11, 10, 5, 4, 1\} \{10, 8, 7, 6, 5, 1\} \{13, 12, 11, 9, 6, 5\} \{13, 12, 10, 9, 5, 1\} \{13, 12, 11, 8, 7, 1\}$ $\{12, 6, 5, 4, 3, 2\} \{10, 9, 6, 4, 3, 2\} \{12, 10, 8, 5, 3, 2\} \{13, 12, 10, 7, 6, 1\} \{13, 12, 8, 6, 5, 4\}$ $\{13, 12, 9, 7, 5, 3\} \{13, 11, 10, 5, 3, 2\} \{13, 9, 7, 6, 3, 2\} \{12, 11, 8, 7, 3, 2\} \{13, 12, 9, 7, 4, 2\}$ $\{10, 9, 7, 6, 5, 2\} \{13, 12, 11, 10, 9, 2\} \{11, 10, 7, 6, 5, 3\} \{12, 10, 7, 5, 4, 3\} \{13, 11, 9, 6, 4, 3\}$ $\{13, 12, 10, 8, 4, 3\}$

67	25	{12, 10, 6, 3, 2, 1} {10, 8, 7, 3, 2, 1} {8, 6, 5, 4, 2, 1} {11, 9, 8, 5, 2, 1} {12, 11, 9, 6, 2, 1}
		{13, 12, 8, 5, 3, 1} {11, 9, 7, 5, 4, 1} {13, 12, 11, 6, 4, 1} {10, 8, 7, 6, 5, 1} {12, 9, 8, 7, 6, 1}
		{12, 11, 10, 8, 6, 1} {9, 7, 6, 5, 3, 2} {13, 12, 9, 5, 3, 2} {12, 11, 9, 8, 4, 1} {12, 9, 6, 5, 4, 2}
		{13, 9, 8, 6, 5, 2} {13, 9, 7, 5, 4, 3} {12, 11, 8, 5, 4, 3} {9, 8, 7, 6, 4, 3} {11, 10, 7, 6, 4, 3}
		{13, 12, 10, 9, 8, 6} {12, 11, 9, 6, 5, 3} {13, 11, 10, 8, 7, 3} {13, 10, 8, 7, 5, 4} {13, 11, 9, 8, 5, 4}
71	22	{13, 12, 4, 3, 2, 1} {13, 10, 9, 3, 2, 1} {11, 10, 6, 4, 2, 1} {7, 6, 5, 4, 3, 1} {13, 8, 5, 4, 3, 1}
		{13, 9, 7, 4, 3, 1} {9, 8, 5, 4, 2, 1} {11, 9, 8, 4, 3, 1} {12, 11, 9, 7, 4, 1} {10, 9, 7, 6, 5, 1}
		{12, 11, 10, 9, 6, 1} {10, 6, 5, 4, 3, 2} {10, 9, 7, 4, 3, 2} {12, 10, 8, 5, 4, 2} {13, 12, 11, 6, 4, 2}
		{13, 11, 10, 7, 4, 2} {13, 12, 9, 8, 5, 2} {13, 9, 8, 7, 6, 2} {10, 9, 8, 6, 4, 3} {12, 11, 8, 7, 4, 3}
		{13, 12, 10, 9, 7, 3} {13, 12, 11, 10, 9, 5}
73	21	{13, 8, 4, 3, 2, 1} {10, 8, 5, 3, 2, 1} {12, 10, 9, 5, 2, 1} {12, 11, 9, 6, 2, 1} {10, 9, 7, 4, 3, 1}
		{13, 12, 9, 4, 3, 1} {13, 10, 7, 5, 3, 1} {13, 9, 8, 7, 3, 1} {12, 11, 8, 7, 6, 1} {12, 11, 10, 8, 3, 2}
		{11, 9, 8, 5, 4, 2} {13, 11, 10, 8, 4, 2} {13, 11, 7, 6, 5, 2} {11, 10, 9, 6, 5, 2} {13, 12, 8, 7, 5, 2}
		{13, 11, 10, 9, 7, 2} {11, 10, 8, 6, 4, 3} {12, 8, 7, 6, 5, 3} {12, 10, 9, 8, 6, 4} {13, 12, 9, 8, 5, 4}
		{12, 11, 10, 7, 5, 3}
79	22	{9, 7, 6, 3, 2, 1} {13, 11, 10, 3, 2, 1} {13, 10, 5, 4, 2, 1} {13, 7, 6, 5, 2, 1} {10, 9, 6, 5, 2, 1}
		{13, 12, 10, 8, 2, 1} {12, 11, 7, 5, 3, 1} {10, 9, 7, 5, 4, 1} {12, 11, 8, 5, 4, 1} {9, 6, 5, 4, 3, 2}
		{11, 9, 7, 5, 3, 2} {12, 8, 7, 6, 4, 2} {13, 10, 8, 6, 5, 2} {11, 8, 6, 5, 4, 3} {13, 12, 10, 5, 4, 3}
		{13, 9, 8, 7, 4, 3} {12, 8, 7, 6, 5, 3} {13, 12, 9, 7, 5, 3} {13, 11, 9, 8, 5, 4} {12, 11, 10, 7, 6, 4}
		{13, 11, 10, 9, 6, 5} {13, 11, 10, 8, 7, 6}
83	24	{12, 5, 4, 3, 2, 1} {13, 7, 4, 3, 2, 1} {8, 7, 6, 4, 2, 1} {12, 11, 7, 4, 2, 1} {13, 10, 5, 4, 3, 1}
		{10, 8, 6, 5, 3, 1} {13, 10, 7, 6, 3, 1} {13, 12, 9, 8, 4, 1} {12, 9, 8, 6, 5, 1} {11, 10, 9, 8, 5, 1}
		{13, 11, 8, 7, 6, 1} {12, 11, 7, 5, 3, 2} {12, 9, 8, 6, 3, 2} {11, 10, 9, 6, 3, 2} {13, 9, 7, 6, 4, 2}
		{12, 10, 9, 6, 4, 2} {12, 11, 10, 8, 4, 2} {12, 11, 10, 6, 5, 2} {13, 12, 10, 7, 5, 2} {9, 8, 7, 5, 4, 3}
		{13, 12, 10, 8, 4, 3} {12, 10, 9, 7, 5, 4} {11, 10, 9, 8, 7, 4} {13, 12, 11, 10, 9, 7}
89	15	{12, 9, 5, 4, 2, 1} {9, 8, 6, 5, 2, 1} {13, 11, 5, 4, 3, 1} {12, 11, 8, 5, 3, 1} {11, 8, 6, 5, 4, 1}
		{13, 12, 8, 5, 4, 1} {13, 7, 5, 4, 3, 2} {13, 11, 10, 8, 7, 3} {13, 11, 10, 4, 3, 2} {12, 10, 9, 5, 3, 2}
		{11, 10, 9, 6, 5, 2} {12, 11, 10, 7, 6, 2} {12, 8, 6, 5, 4, 3} {13, 12, 7, 6, 5, 3} {13, 12, 11, 10, 6, 3}
97	1	{12, 11, 10, 5, 4}
101	21	{12, 10, 4, 3, 2, 1} {11, 10, 7, 3, 2, 1} {13, 9, 8, 3, 2, 1} {12, 10, 7, 5, 2, 1} {13, 10, 7, 6, 2, 1}
		{11, 9, 8, 7, 2, 1} {13, 11, 9, 8, 6, 3} {13, 12, 11, 7, 2, 1} {10, 7, 5, 4, 3, 1} {13, 11, 8, 4, 3, 1}
		{9, 7, 6, 5, 4, 1} {12, 10, 9, 6, 4, 1} {11, 10, 9, 7, 6, 1} {13, 11, 7, 6, 5, 4} {12, 11, 8, 7, 3, 2}
		{13, 9, 6, 5, 4, 2} {13, 10, 9, 8, 6, 2} {13, 10, 8, 6, 4, 3} {12, 11, 10, 8, 4, 3} {12, 10, 9, 6, 5, 3}
		{13, 11, 10, 9, 8, 5}
103	14	{10, 7, 5, 4, 2, 1} {12, 10, 6, 4, 2, 1} {12, 11, 9, 4, 2, 1} {12, 11, 8, 6, 2, 1} {12, 7, 6, 4, 3, 1}
		{9, 8, 5, 4, 3, 2} {12, 11, 10, 7, 5, 4} {13, 10, 9, 5, 3, 2} {11, 10, 9, 5, 4, 2} {13, 12, 11, 9, 5, 2}
		{10, 9, 6, 5, 4, 3} {13, 12, 10, 5, 4, 3} {12, 9, 7, 6, 5, 3} {13, 11, 10, 8, 7, 4}
107	12	{13, 12, 10, 3, 2, 1} {10, 8, 6, 4, 2, 1} {12, 9, 8, 4, 2, 1} {12, 11, 7, 6, 2, 1} {13, 12, 7, 5, 4, 1}
		{13, 12, 11, 10, 4, 1} {11, 10, 9, 8, 6, 1} {11, 9, 8, 5, 3, 2} {13, 10, 7, 6, 5, 2} {13, 12, 11, 9, 8, 3}
		{12, 10, 9, 7, 5, 4} {13, 9, 8, 7, 6, 5}

109	9	{10, 9, 5, 4, 3, 1} {13, 12, 7, 4, 3, 1} {11, 10, 9, 7, 5, 1} {13, 11, 10, 8, 7, 1} {13, 12, 9, 7, 3, 2} {13, 7, 6, 5, 4, 3} {10, 8, 6, 5, 4, 3} {13, 12, 9, 8, 6, 4} {10, 9, 8, 7, 6, 5}
113	1	{13, 12, 7, 5, 2}
127	16	{9, 6, 5, 3, 2, 1} {13, 11, 9, 3, 2, 1} {13, 12, 5, 4, 2, 1} {11, 10, 8, 5, 3, 1} {13, 11, 8, 7, 3, 1} {9, 8, 7, 6, 5, 1} {13, 10, 9, 8, 7, 1} {13, 12, 8, 4, 3, 2} {13, 9, 8, 5, 3, 2} {12, 11, 8, 5, 3, 2} {11, 10, 8, 5, 4, 2} {13, 12, 10, 9, 7, 2} {10, 9, 8, 5, 4, 3} {13, 8, 7, 6, 5, 3} {13, 11, 10, 9, 5, 4} {13, 12, 10, 8, 6, 4}
131	11	{11, 6, 5, 4, 2, 1} {13, 8, 6, 4, 2, 1} {12, 11, 9, 5, 2, 1} {9, 8, 6, 4, 3, 2} {13, 12, 11, 10, 8, 2} {13, 12, 8, 7, 6, 5} {10, 8, 7, 6, 5, 3} {13, 11, 10, 7, 5, 3} {12, 11, 10, 9, 5, 3} {13, 10, 8, 7, 5, 4} {13, 11, 10, 8, 6, 4}
137	11	{13, 12, 10, 7, 2, 1} {13, 7, 6, 4, 3, 1} {11, 10, 8, 5, 4, 1} {13, 11, 10, 9, 4, 1} {10, 8, 7, 5, 3, 2} {11, 10, 9, 8, 5, 2} {12, 11, 10, 9, 7, 2} {10, 9, 7, 6, 5, 3} {13, 11, 7, 6, 5, 3} {13, 9, 8, 7, 6, 4} {12, 11, 9, 8, 6, 5}
139	10	{13, 12, 8, 3, 2, 1} {9, 7, 6, 4, 2, 1} {13, 7, 6, 5, 3, 1} {12, 10, 9, 7, 3, 1} {11, 10, 9, 6, 5, 1} {8, 7, 6, 5, 4, 2} {11, 6, 5, 4, 2} {10, 9, 8, 5, 4, 2} {13, 12, 9, 7, 4, 3} {13, 12, 11, 7, 5, 3}
149	1	{13, 10, 6, 5, 1}
151	13	{10, 9, 8, 7, 2, 1} {11, 9, 8, 7, 3, 1} {13, 12, 10, 7, 6, 1} {12, 11, 9, 8, 6, 1} {11, 8, 6, 4, 3, 2} {10, 9, 8, 4, 3, 2} {11, 10, 7, 6, 4, 2} {12, 9, 7, 6, 5, 2} {12, 11, 9, 8, 7, 2} {12, 10, 7, 6, 4, 3} {12, 11, 10, 9, 8, 3} {13, 12, 8, 7, 6, 4} {13, 10, 9, 8, 7, 5}
157	13	{12, 9, 6, 3, 2, 1} {11, 7, 5, 4, 2, 1} {13, 8, 5, 4, 2, 1} {10, 7, 6, 5, 3, 1} {13, 11, 9, 7, 3, 1} {11, 10, 9, 8, 3, 1} {13, 10, 7, 5, 4, 1} {12, 9, 8, 5, 3, 2} {12, 11, 8, 7, 5, 2} {13, 9, 8, 6, 4, 3} {12, 10, 9, 8, 6, 3} {13, 10, 8, 6, 5, 4} {13, 12, 11, 10, 6, 3}
163	9	{11, 10, 7, 5, 3, 2} {13, 12, 11, 5, 3, 2} {9, 8, 6, 5, 4, 2} {11, 8, 7, 5, 4, 2} {13, 12, 7, 6, 4, 2} {13, 10, 8, 7, 5, 2} {11, 10, 9, 8, 6, 2} {11, 9, 7, 5, 4, 3} {13, 12, 11, 10, 9, 6}
167	9	{12, 9, 6, 4, 2, 1} {13, 11, 6, 5, 2, 1} {12, 9, 7, 4, 3, 1} {12, 11, 10, 7, 3, 1} {13, 12, 7, 6, 4, 1} {12, 10, 7, 5, 3, 2} {12, 11, 10, 9, 6, 2} {11, 9, 7, 5, 4, 3} {13, 12, 11, 10, 9, 6}
173	1	{13, 12, 9, 7, 6}
179	9	{12, 11, 9, 3, 2, 1} {12, 10, 6, 5, 2, 1} {13, 8, 7, 5, 2, 1} {8, 7, 6, 5, 3, 1} {10, 9, 7, 6, 3, 1} {12, 11, 7, 6, 4, 1} {12, 8, 7, 5, 4, 3} {13, 11, 10, 7, 4, 3} {13, 11, 10, 7, 6, 5}
181	12	{8, 5, 4, 3, 2, 1} {13, 11, 7, 4, 2, 1} {9, 8, 7, 6, 2, 1} {13, 11, 10, 8, 3, 1} {13, 12, 10, 6, 4, 1} {12, 10, 8, 7, 5, 4} {11, 9, 6, 5, 3, 2} {12, 11, 10, 7, 3, 2} {13, 9, 8, 7, 5, 2} {13, 12, 10, 8, 7, 2} {13, 11, 10, 9, 7, 3} {9, 7, 5, 4, 3, 2}
191	11	{10, 7, 5, 3, 2, 1} {11, 7, 6, 4, 2, 1} {13, 10, 7, 4, 3, 1} {13, 11, 7, 6, 3, 1} {13, 12, 11, 9, 4, 1} {13, 12, 7, 6, 3, 2} {12, 10, 9, 6, 3, 2} {13, 8, 7, 6, 5, 4} {11, 10, 9, 7, 5, 4} {13, 12, 10, 8, 5, 4} {12, 11, 10, 8, 6, 4}
193	7	{12, 11, 10, 8, 2, 1} {11, 10, 8, 4, 3, 1} {13, 11, 5, 4, 3, 2} {10, 8, 7, 4, 3, 2} {11, 10, 8, 6, 3, 2} {13, 11, 8, 7, 6, 5} {12, 10, 9, 8, 7, 2}
197	11	{11, 9, 5, 3, 2, 1} {12, 9, 8, 6, 2, 1} {12, 11, 10, 7, 2, 1} {13, 9, 7, 5, 3, 1} {11, 8, 7, 6, 3, 1} {13, 11, 8, 5, 3, 2} {12, 8, 7, 5, 4, 2} {13, 9, 7, 6, 5, 2} {12, 11, 7, 5, 4, 3} {12, 11, 10, 6, 4, 3} {13, 11, 10, 8, 5, 4}

		{13, 9, 4, 3, 2, 1}	{13, 11, 8, 5, 2, 1}	{13, 10, 8, 6, 4, 1}	{11, 10, 9, 8, 7, 1}	{12, 8, 6, 5, 4, 2}
199	9	{12, 11, 10, 6, 4, 2}	{12, 10, 7, 6, 5, 2}	{10, 9, 8, 7, 5, 2}	{12, 11, 10, 6, 5, 3}	
$\vdots$		$\vdots$				
≥ 22787		no privileged coalitions		(proven)		

An ideal multi-secret sharing scheme based on minimal privileged coalitions

SONG Yun¹, LI ZhiHui^{1*} & LI YongMing²

¹ School of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062, China;

² School of Computer Science, Shaanxi Normal University, Xi'an 710062, China

*E-mail: lizhihui@snnu.edu.cn

Abstract How to construct an ideal multi-secret sharing scheme for general access structures is difficult. In this paper, we solve a public problem proposed by Spiez et al. recently [Finite fields and their application, 2011, 17: 329–342], namely to design an algorithm of privileged coalitions of any length if such coalitions exist. Furthermore, in terms of privileged coalitions, we show that most of the existing multi-secret sharing schemes based on Shamir threshold secret sharing are not perfect by analyzing Yang et al.'s scheme and Pang et al.'s scheme. Finally, based on the algorithm mentioned above, we devise an ideal multi-secret sharing scheme for families of access structures, which possesses more vivid qualified sets than that of the threshold scheme.

Keywords (t, n) threshold, track, access structure, minimal privileged coalitions, multi-secret sharing

SONG Yun was born in 1987. She received the M.S. degree in cryptography from Shaanxi Normal University in 2012. She is currently a Ph.D. candidate in cryptography at Shaanxi Normal University. Her research interests lie in information security and quantum secret sharing.

LI ZhiHui was born in 1966. She received the Ph.D. degree in computer software and theory from the Northwestern Polytechnical University, Xi'an, China. She is currently a Professor in the College of Mathematics and Information Science at Shaanxi Normal University in China. She has published more than 60 academic papers in international conferences and journals in the areas of information security and coding theory. Her research interests are in the areas of information security, coding theory and quantum information.

LI YongMing was born in 1966. He received the Ph.D. degree from the Sichuan University. He is currently a Professor in the College of Computer Science at Shaanxi Normal University in China. His research interests are in the areas of computational intelligence, quantum logic, quantum computation and quantum information. Dr. Li has published over 200 technical papers in international journals and conferences.