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

Yun Song , Zhihui Li *

College of Mathematics and Information Science, Shaanxi Normal University, Xi'an, 710062, P. R. China

Abstract

How to construct an ideal multi-secret sharing scheme for general access structures is difficult. In this paper, we solve an open 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 authorized sets than that of the threshold scheme.

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

1. Introduction

Single-secret sharing schemes(SSSS). A secret sharing scheme is a method to distribute a secret among a set P of participants, which includes a pair of efficient algorithms:a distribution algorithm and a reconstruction algorithm, implemented by a dealer and some participants. The distribution algorithm allows a dealer to split a secret s into different pieces, called shares, and distribute them to participants. The reconstruction algorithm is executed by the authorized subsets of parties who are able to reconstruct the secret by using their respective shares. The collection of these authorized sets of participants is called the access structure, $\Gamma \subset 2^P$. A group of participants is called a minimal authorized subsets if they can recover the secret with their shares, and any of its proper subgroups cannot do so. Then, the access structure is determined by the family of minimal authorized subsets, $(\Gamma)_{min}$. The notion of secret sharing was introduced by Shamir [1] and Blakley [2] , who considered the only schemes with a (t, n)-threshold access structure formed by the set of authorized subsets of participants is the set of all subsets of size at least t, for some integer t. In 1987, Ito et al.[3] proved that there

*Corresponding author:Zhihui Li.(snnulzh@25yahoo.com.cn)

exists a secret sharing scheme for any access structure which is more general than the threshold ones. Afterwards, secret sharing schemes have been widely employed in the construction of more elaborate cryptographic primitives and several types of cryptographic protocols(see [4-8]).

A secret sharing scheme is called perfect if any non-authorized subset of participants have no information about the secret, and ideal if the shares are of the same size as that of the secret. An ideal secret sharing scheme is well-known to be the best efficiency that one can achieve with lowest storage complexity and the communication complexity[9].

Multi-secret sharing schemes(MSSS). Multi-secret sharing can be seen as a natural generalization of single secret sharing schemes. In 1994, Blundo et al. [10] studied the more general case in which the set of participants share more than one secret and different secret is related to different access structure. Let $\Gamma = (\Gamma_0, \ldots, \Gamma_{m-1})$ be the m-tuple of access structures on P and let $S_0 \times S_1 \times \cdots \times S_{m-1}$be the set from which the secrets are chosen, where for any $0 \leq j \leq m-1$, each secret s_j to be shared is chosen in S_j. In the definition of a perfect multi-secret sharing scheme, an m-tuple of secrets $(s_0, \ldots, s_{m-1}) \in S_0 \times \cdots \times S_{m-1}$ is shared in an m-tuple $(\Gamma_0, \ldots, \Gamma_{m-1})$ of access structures on P in such a way that, for each $0 \leq j \leq m-1$, the access structure Γ_j is the set of all subsets of P that can recover secret s_j. A perfect multi-secret sharing scheme is defined in [10] such that the following requirements are satisfied.

Definition 1.1. *Let $\Gamma = \{\Gamma_0, \ldots, \Gamma_{m-1}\}$ be an m-tuple of access structures on the set of participants $P = \{P_1, \ldots, P_n\}$. A multi-secret sharing scheme for $\Gamma = \{\Gamma_0, \ldots, \Gamma_{m-1}\}$ is a sharing of the secrets $(s_0, \ldots, s_{m-1}) \in S_0 \times \cdots \times S_{m-1}$ in such a way that, for $0 \leq j \leq m-1$,*

(1) Correctness requirement: Any subset $A \subseteq P$ of participants enabled to recover s_j can compute s_j. Formally, for all $A \in \Gamma_j$, it holds $H(S_j \mid A) = 0$,

(2) Security requirement: Any subset $A \subseteq P$ of participants not enabled to recover s_j, even knowing some of the other secrets, has no more information on s_j than that already conveyed by the known secrets. Formally, for all $A \notin \Gamma_j$ and $T \subseteq \{S_0, \cdots, S_{m-1}\} \backslash \{S_j\}$, it holds $H(S_j \mid AT) = H(S_j \mid T)$.

So far, Multi-secret sharing are widely applied not only in the field of information security but also the theories and models of secret sharing schemes[11-19].

Our results. Although fruitful results for the multi-secret sharing have been obtained, it is still difficult to devise ideal multi-secret sharing schemes for general access structures. In this paper, by using the theory of privileged coalitions[20,21], we point out that several multi-secret sharing schemes (see[13-18])based on Shamir's threshold scheme are not perfect, and thus are not ideal. In[20] Spiez et al. obtained an algorithm to construct the privileged coalitions of maximal length and put forward how to design an algorithm of privileged coalitions of any length if such coalitions exist. Motivated by these concers, we solve this open problem and devise an ideal multi-secret sharing scheme(IMSSS) for families of access structures based on the algorithm mentioned above. Finally, we compare our scheme with two additional schemes[13,14] according to their performance analysis.

The rest of the paper is organized as follows: In Section 2, the basic definitions of secret Shamir's secret sharing scheme and privileged coalitions are reviewed, an algorithm of privileged coalitions of any length is designed as well. In Section 3 and 4, based on theories of privileged coalitions and corresponding algorithm, we shall present our ideal multi-secret sharing scheme and make some discussions. Finally, some remarks are given in the conclusion Section.

2. Preliminaries

2.1. Shamir's secret sharing scheme

In a (t, n) **threshold secret sharing scheme**(a scheme with n participants and threshold t), where $2 \leq t \leq n$, a dealer does not disclose a secret data to the participants but only distributes n shares amongest them in such a way that at least t or more participants can collectively efficiently reconstruct the secret but no coalition of less than t participants can obtain noting about the secret.

In the paper, we consider **Shamir's secret sharing schemes**[20] with the secret placed as a coefficient a_i of the scheme polynomial $f(x) = a_0 + a_1x + \cdots + a_{t-1}x^{t-1}$, where $\mathbf{a} = (a_0, \ldots, a_{t-1}) \in F_q^t$ (q is a prime power). For a fix $f(x)$ and an j, such scheme is uniquely defined by a sequence $\mathbf{L} = (l_1, l_2 \ldots, l_n) \in F_{q^*}^n$ of pairwise different public identities, allocated to participants, called in [20] a track. The shares $y_i = f(l_i)$ $(1 \leq i \leq n)$ assigned to participants are secret.

Remark 1. Shamir's (t, n) threshold secret sharing and Shamir's secret sharing are different. A Shamir's (t, n) threshold secret sharing must be a Shamir's secret sharing, but a Shamir's secret sharing may not be a Shamir's (t, n) threshold secret sharing.

In fact, the public identities $\mathbf{L}$ define the $n \times t$ matrix $\mathbf{A(L)} = (l_\mu^\nu)_{\substack{1 \leq \mu \leq n \\ 0 \leq \nu \leq t-1}}$ over F_q which gives the shares by $\mathbf{A(L)a}^T = \mathbf{y}^T$. Since $\mathbf{L}$ is a track any coalition of t participants determines a $t \times t$ non-singular Vandermonde submatrix of the matrix $\mathbf{A(L)}$ consisting of the corresponding rows of the matrix $\mathbf{A(L)}$, i.e.,

(i) all $t \times t$ submatrices of $\mathbf{A(L)}$ are non-singular.

A Shamir's secret sharing is a Shamir's (t, n) threshold secret sharing if and only if

(ii) all $(t-1) \times (t-1)$ submatrices of the matrix obtained from the matrix $\mathbf{A(L)}$ by removing its j-th column are non-singular.

The track $\mathbf{L}$ corresponding to such matrix $\mathbf{A(L)}$ satisfying two above conditions is called $(t, j)-$admissible[21].

Definition 2.1. *Let $0 \leq j \leq t-1$. If the track $\boldsymbol{L} \in F_q^n$, where $n \geq k$, defines a Shamir's (t, n) threshold secret sharing with the secret placed as a coefficient a_j of the scheme polynomial $f(x) = a_0 + a_1x + \cdots + a_{t-1}x^{t-1}$, then $\boldsymbol{L}$ is called a $(t, j)-$admissible track.*

Note that if the track $\mathbf{L} \in F_q^n$ is not $(t, j)-$admissible, then it contains a subtrack consisting of less than t participants which can reconstruct the secret by themselves, forming a privileged coalition[20].

2.2. Minimal privileged coalition

Definition 2.2. *[20] Let $r < t$ and fix j, $0 < j < t-1$. A coalition of r participants $\boldsymbol{L} = (l_1, l_2, \cdots, l_r) \in F_q^r$ is said to be a $(t, j)-$privileged coalition, if they can reconstruct the secret, placed as the coefficient a_j of the scheme polynomial $f(x) = a_0 + a_1 x + \cdots + a_{t-1}x^{t-1}$.*

Definition 2.3. *Let $r < t$ and fix j, $0 < j < t-1$. A coalition of r participants $\boldsymbol{L} = (l_1, l_2, \cdots, l_r) \in F_q^r$ is said to be a $(t, j)-$minimal privileged coalition, if $\boldsymbol{L}$ is a privileged coalition without any subtracks that can reconstruct the secret.*

Note that the tracks of length t, which can be extended by privileged coalitions of length r, can reconstruct the secrets placed as any coefficients of the scheme polynomial. Then we would have

Definition 2.4. *Fix j, $0 < j < t-1$. A coalition of t participants $\boldsymbol{L} = (l_1, l_2, \cdots, l_t) \in F_q^t$ is said to be a $(t, j)-$unextended track, if $\boldsymbol{L}$ can not be extended by a $(t, j)-$privileged coalition.*

By Definition 2.3, the minimal authorized subsets of Shamir's secret sharing schemes are determined by minimal privileged coalitions and unextended tracks. Therefore, constructing minimal privileged coalitions become the key to the determination of the access structures. In order to devise an algorithm to obtain privileged coalitions, we will need the following theorem about the characterization of $(t, j)-$privileged coalitions whose proof can be found in[20].

Theorem 2.5. *Assume that $0 < j < t-1$, $j < r \leq t-1$. Let $\boldsymbol{L} = (l_1, l_2, \cdots, l_r) \in F_q^r$ be a track, and let $t \leq q$. Then $\boldsymbol{L}$ is a $(t, j)-$privileged coalition if and only if*

$$\tau_\omega(\boldsymbol{L}) = 0, \quad for\ all\ \omega \in \{r-j, \cdots, t-1-j\},$$

where $\tau_\omega(\boldsymbol{L})$ denotes the elementary symmetric polynomial of total degree ω.

2.3. Privileged coalitions of any length

In this section, we solve an open problem proposed in[20] recently, namely to design an algorithm of privileged coalitions of any length if such coalitions exist. For simplicity, we will focus on the tracks whose value of each component is clamped to the range of $\{1, 2, \cdots, N\}$, and we call these coalitions $(t, j)-$privileged coalitions with respect to N. Using Algorithm 1 we can obtain $(t, j)-$privileged coalitions with respect to N of length r over F_p (p is a odd prime). By Definition 2.3, for the given t, r with $\frac{t+1}{2} \leq r \leq t-1$, we can obtain $(t, j)-$minimal privileged coalitions with respect to N of length r by detaching $\binom{r-r_{min}}{p-r_{min}} N_{min}$ non-minimal privileged coalitions from $(t, j)-$privileged coalitions of length r, where N_{min} denotes the number of privileged coalitions of the shortest length r_{min}.

As an illustration, we investigate the Shamir's secret scheme with the number of participants $n = 13$ and threshold $t = 7$. In the appendix, we then present two

tables of $(7, j)-$minimal privileged coalitions with respect to $N = 13$ of any length if such coalitions exist.

Algorithm 1

Input positive integers t, r, j with $t \geq 3$, $\frac{t+1}{2} \leq r \leq t-1$, $t - r \leq j \leq r - 1$.

Output all of the $(t, j)-$privileged coalitions of length r with respect to N over F_p.

1. Compute the range of values for j, and set $a \leftarrow r - j$, $b \leftarrow t - 1 - j$. Take J is a set of all integers from a to b.
2. Obtain all of the tracks of length r with respect to N over F_p.
   2.1. $B = (1, 2, \cdots, n)$, for $i = 1$ to N
      2.1.1 For $j = i + 1$ to N
         If $B(j) > B(i)$ ($B(j)$ denotes the elements of the $j-$th position of the array B),
         2.1.1.1 For $k = j + 1$ to N
         If $B(k) > B(j)$
         $\vdots$
         $r-1$ Nested loops are carried out in turn, then $\underbrace{(\cdots, B(k), B(j), B(i))}_{r}$ is a track.
3. Find $(t, j)-$privileged coalitions from the tracks obtained in Step 2 by means of the principle about Vieta theorem of high power equation.
   3.1. For $i = 1$ to $b - a + 1$
      3.1.1. Set $p \leftarrow J(i)$, and go through tracks that obtained in Step 2. Let $C = 1$. For $j = 1$ to r
         Set $C \leftarrow C \times (x + \mathbf{L}(j))$
      3.1.2. Set$f \leftarrow C$, and select $\mathbf{m}$ as a vector whose components are coefficients of the expansion of $f(x)$ in ascending power of x. Set $s \leftarrow \mathbf{m}(r - p + 1)$, then set $v_p \leftarrow mod(s, p)$.
   3.2. If $v_p = 0$, then return $(\mathbf{L})$.

3. An ideal multi-secret sharing scheme

When the probability distributions over the secrets and shares are uniform, a secret sharing scheme is said to be ideal if all secrets and shares are the same size[19]. In this section we firstly define a (t-1)-tuple $\Gamma = (\Gamma_0, \ldots, \Gamma_{t-2})$ of access structures and then we devise an IMSSS which realizes such a (t-1)-tuple $\Gamma = (\Gamma_0, \ldots, \Gamma_{t-2})$ of access structures.

3.1. Definition of the access structures

Let $P = \{P_1, \ldots, P_n\}$ be the set of participants, we firstly define such an (t-1)-tuple $\Gamma = (\Gamma_0, \ldots, \Gamma_{t-2})$ as follows:

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

(2) $(\Gamma_j)_{min} = \{A \subseteq P \mid \mathbf{L}_A$ *is either a* $(t,j)-$ *unextended track or a* $(t,j)-$ *privileged coalition*, $(1 \leq j \leq t-2)\}$.

As each component of a track can be used as the identity of the participants, we can determine the minimal authorized subsets of $(\Gamma_j)_{min}$ for the secret placed as a coefficient a_j of the scheme polynomial $f(x) = a_0 + a_1 x + \cdots + a_{t-1}x^{t-1}$ by getting both (t,j)-unextended track and (t,j)-privileged coalition using the Algorithm 1.

Obviously, a subset $A \subseteq P$ is likely to reconstruct more than one secret. For example, if $A \in \Gamma_i$ and $A \in \Gamma_j$, then A can reconstruct not only s_i but also s_j, where $0 \leq i, j \leq t-2$ and $i \neq j$.

Example 3.1 Let $P = \{P_1, P_2, P_3, P_4, P_5, P_6\}, t = 5, q = 7$. Without loss of generality, D distributes i to participant P_i for $1 \leq i \leq 6$. It follows from algorithm 1 that (5,1)-privileged coalition over F_7 is $(1,2,5,6)$, $(1,3,4,6)$ and $(2,3,4,5)$; (5,2)-privileged coalition is $(1,2,4),(3,5,6)$; (5,3)-privileged coalition is $(1,2,5,6)$, $(1,3,4,6)$ and $(2,3,4,5)$, but without (t,j)-unextended track. Hence $(t-1)$-tuple $\Gamma = (\Gamma_0, \ldots, \Gamma_{m-2})$ can be defined as follows:

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

3.2. Construction of the IMSSS

3.2.1. Initialization phase

Note that $s_0, \ldots, s_{t-2}$ denote t-1 secrets to be shared, where $(s_0, \ldots, s_{t-2}) \in S_0 \times \cdots \times S_{t-2}$. The dealer D randomly chooses n pairwise different l_i and assigns them to every participant P_i as their public identity, where $l_i \in F_q^*$ for $1 \leq i \leq n$. Then D computes the (t,j)-unextended track and (t,j)-privileged coalition by means of algorithm 1 for $0 \leq j \leq t-2$.

3.2.2. Distribute phase

The dealer D performs the following steps:

(1) Choose an integer a_{t-1} from F_q^* and construct $(t-1)$th degree polynomial $f(x) \bmod q$, where $0 < s_0, \ldots, s_{t-2}, a_{t-1} < q$ as follows:$f(x) = s_0 + \cdots + s_{t-2}x^{t-2} + a_{t-1}x^{t-1} \mod q$.

(2) Compute $y_i = f(l_i) \mod q$ for $i = 1, 2 \ldots, n$ and distribute them to every participant P_i as secret shares by a secret channel.

3.2.3. Recovery phase

Assume that $(0 \leq j \leq t-2)$. for any $A \in (\Gamma_j)_{min}$, if $|A| = t$, then any subset $A \in (\Gamma_j)_{min}$ can reconstruct the secret s_j by solving equation system $\mathbf{A}(\mathbf{L}_A)\ \mathbf{a}^T = \mathbf{y}^T$, where $\mathbf{L}_A$ is corresponding track of A; if $|A| < t$ and $\mathbf{L} = (l_{i_1}, l_{i_2}, \ldots, l_{i_r}) \in F_q^r$ is a (t,j)-privileged coalition of A, let $\mathbf{L}_A^{'} = (l_{i_1}, l_{i_2}, \ldots, l_{i_r}, l_{i_{r+1}}, \ldots, l_{i_t}) \in F_q^t$, then the participants in A can reconstruct the secret s_j by solving equation system $\mathbf{A}(\mathbf{L}_A^{'})\ \mathbf{a}^T = \mathbf{y}^T$, where $\mathbf{a} = (s_0, \ldots, s_{t-2}, a_{t-1}) \in F_q^t$, $\mathbf{y} = (y_{i_1}, \ldots, y_{i_t})$, and $\mathbf{A}(\mathbf{L}_A)$, $\mathbf{A}(\mathbf{L}_A^{'})$ are all $t \times t$ matrix which can be specifically written as $(l_\mu^\nu)_{\substack{1 \leq \mu \leq n \\ 0 \leq \nu \leq t-1}}$.

4. Correctness and security proof

In order to prove that our scheme is perfect, we need to introduce some results on the generalized the Vandermonde determinants. As usual, for a $k-$tuple of indeterminates $\mathbf{x} = (x_1, \ldots, x_k)$ and a $k-$tuple of increasing non-negative integers $\mathbf{c} = (c_1, \ldots, c_k)$ we call $V_{\mathbf{c}}(\mathbf{x}) = \det((x_\mu^{c_\nu})_{1\leq\nu,\mu\leq k})$ generalized Vandermonde determinant. Write $\mathbf{e}_k = (0, \ldots, k-1)$. If $\mathbf{c} = \mathbf{e}_k$ then $V_{\mathbf{c}}(\mathbf{x})$ equals the classical Vandermonde determinant $V(\mathbf{x}) = \prod_{1\leq i<j\leq k}(x_j - x_i)$.

Theorem 4.1. *The scheme presented in Section 3 is a perfect multi-secret sharing scheme.*

Proof. When $j = 0$ due to the perfect property of the (t, n) secret sharing schemes, our scheme satisfies the two conditions of Definition 1.1. Now we consider that $1 \leq j \leq t-2$.

(1) If $|A| = t$, then by solving equation system $\mathbf{A}(\mathbf{L}_A)\ \mathbf{a}^T = \mathbf{y}^T$, the participants in A can obtain the unique solution s_j in terms of Cramer rule. If $|A| < t$ and $\mathbf{L} = (l_{i_1}, l_{i_2}, \ldots, l_{i_r}) \in F_q^r$ is a (t, j)-privileged coalition of A, by Theorem 2.5, $\tau_\omega(\mathbf{L}) = 0$, for all $\omega \in \{r-j, \cdots, t-1-j\}$. By Lemma 2[20], $\tau_\omega(\mathbf{L}) = 0$ for all $\omega \in \{r-j, \cdots, t-1-j\}$ if and only if

$$\tau_{t-1-j}(\mathbf{L} \mid\mid \hat{\mathbf{u}}_m) = 0 \quad for\ all\ m,\ 1 \leq m \leq t-r, \qquad (1^{'})$$

let $\mathbf{u} = (u_1, \ldots, u_{t-r}) \in F_q^{t-r}$ be a track disjoint with $\mathbf{L}$, and $\hat{\mathbf{u}}_m$ denotes the sequence obtained from $\mathbf{u}$ by removing the term u_m. Let

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

and let $\mathbf{L}_A^{'} = (l_{i_1}, l_{i_2}, \ldots, l_{i_r}, u_1, \ldots, u_{t-r}) \in F_q^t$, then s_j can be obtained by solving equation system $\mathbf{A}(\mathbf{L}_A^{'})\ \mathbf{a}^T = \mathbf{y}^T$

$$\begin{aligned} s_j \ = \ & \frac{1}{V(\mathbf{L} \mid\mid \mathbf{u})}\Big(\sum_{k=1}^{r}(-1)^{k+j+1}V(\hat{\mathbf{L}}_k \mid\mid \mathbf{u})\tau_{t-1-j}(\hat{L}_k \mid\mid \mathbf{u})y_k + \\ & \sum_{k=r+1}^{t}(-1)^{k+j+1}V(\mathbf{L} \mid\mid \hat{\mathbf{u}}_{k-r})\tau_{t-1-j}(\mathbf{L} \mid\mid \hat{\mathbf{u}}_{k-r})y_k. \quad (2^{'}) \end{aligned}$$

By $(1^{'})$ and $(2^{'})$, (t, j)-privileged coalition of A can compute the secret s_j. Hence, it holds that for all $A \in \Gamma_j, H(S_j \mid A) = 0$.

(2) If $A \notin \Gamma_j$, then $|A| < t$ and $\mathbf{L}_A$ is not a $(t, j)-$ privileged coalition. In view of $(1^{'})$, there exists a $m^{'}$, where $1 \leq m^{'} \leq t-r$ such that $\tau_{t-1-j}(\mathbf{L} \mid\mid \hat{\mathbf{u}}_{m^{'}}) \neq 0$. Thus, the share $y_{m^{'}+r}$ of $u_{m^{'}}$ is needed. By $(2^{'})$ we can obtain that the participants in A have no information on s_j, even knowing some of the other secrets. Hence, it holds that $H(S_j \mid AT) = H(S_j \mid T)$, where T denotes the secrets that A can compute.

Therefore, according to Definition 1.1, the scheme is a perfect multi-secret sharing scheme.

As a consequence, our scheme is an ideal and perfect linear multi-secret sharing scheme. In 2004 and 2005, Yang et al.[13] and Pang et al.[14] proposed multi-secret sharing schemes based on Shamir's threshold secret sharing, respectively, which are relatively efficient with lower cost of computing due to the Lagrange interpolation operation that is employed in the process of schemes construction. However, The existence of the privileged coalitions and the Lagrange interpolation polynomial participants use will result in a fact that the union of less than t participants may compute the coefficients of the polynomial corresponding to secrets by solving equation system, thereby obtaining further information about the secret. Consequently, both of the two schemes are not perfect, i.e., there is information leakages. Table 1 is for the comparison among three schemes.

Likewise, the multi-secret sharing schemes[15-18] are not perfect, and thus are not ideal.

Remark 2. The validity of the shares can be verified in a verifiable secret sharing scheme, thus participants are not able to cheat. Based on our scheme, we can further construct an ideal verifiable multi-secret sharing scheme by adding the existing verifiability methods where the intractability of discrete logarithm problem is frequently employed (see[15-18]).

Table 1 The comparison of performance among three schemes

Capability	Our scheme	Yang's scheme.	Pang's scheme
Multi-secret	Yes	Yes	Yes
Each participant holds only one share	Yes	Yes	Yes
Recover multi-secrets by Lagrange interpolating polynomials	No	Yes	Yes
Access structures corresponding to each secret is the same	No	Yes	Yes
Access structures possess more vivid authorized sets	Yes	No	No
The scheme is perfect	Yes	No	No
The scheme is ideal	Yes	No	No

5. Conclusions

In this paper, we consider an ideal multi-secret sharing scheme based on the theories of minimal privileged coalitions and Shamir's secret sharing, where for a set of participants $P = \{P_1, \ldots, P_n\}$, each subset of Γ_j carries different target secret s_j for $0 \leq j \leq t-2$. In particular, in order to obtain privileged coalitions, we devise an algorithm of privileged coalitions of any length if such coalitions exist. In real terms, we can integrate data into a database which obtained from the experiment for different value t in accordance with our needs, and then we can extract the results as identities of participants applied to the construction of the scheme for practical applications.

6. Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant No. 60873119).

7. References

[1] A. Shamir, How to share a secret, Commun ACM, 1979(22) 612C613.

[2] G.R. Blakley, Safeguarding cryptographic keys, Proc Afips Ncc, 48(1979) 313-317.

[3] M.Ito, A.Saito, T.Nishizeki, Secret sharing schemes realizing general access structures, In: Proceedings of the IEEE Global Telecommunications Conference. Japan, 1987, 99-102.

[4] Z.H.Li, T.Xue, H.Lai. Secret sharing scheme from binary linear codes, Information Sciences, 180(2010) 4412-4419.

[5] Y.Jin, C.S.Ding, Secret sharing schemes from three classes of linear codes, IEEE Trans Inform Theory, 52(2006) 206-212.

[6] A.Parakh , S.Kak, Space efficient secret sharing for implicit data security. Information Sciences, 181(2011) 335-341.

[7] C.Tang, S.GAO, Leakproof secret sharing protocols with applications to group identification scheme, Sci Sin Math, 42(2012) 634-647.

[8] H.Yuan, F.T.Zhang, X.Huang, et al. Certificateless threshold signature scheme from bilinear maps, Information Sciences, 180(2010)4714-4728.

[9] G.D. Crescenzo, C. Galdi, Hypergraph decomposition and secret sharing, Discrete Applied Mathematics, 157(2009) 928C946.

[10] C.Blundo, A.De Santis, G.Di Crescenzo, A.Giorgio Gaggia, U.Vaccaro, Multi-secret sharing schemes.In: Advances in Cryptology-CRYPTO'94, Lecture Notes in Computer Science, 839(1994) 150-163.

[11] M.L. Liu, L.L.Xiao, Z.F. Zhang, Linear multi-secret sharing schemes based on multi-party computation, Finite Fields and Their Applications, 12(2006) 704-713.

[12] A.Das, A.Adhikari, An efficient multi-use multi-secret sharing scheme based on hash function, Applied Mathematics Letters, 23(2010)993-996.

[13] C.C. Yang, T.Y. Chang, M.S.Hwang, A (t, n) multi-secret sharing scheme, Applied Mathematics and Computation, 151(2004) 483-490.

[14] L.J Pang, Y.M Wang, A new (t, n) multi-secret sharing scheme based on Shamir's secret sharing, Applied Mathematics and Computation, 167(2005)840-848.

[15] M.H.Dehkordi, S.Mashhadi. An efficient threshold verifiable multi-secret sharing. Computer Standards and Interfaces, 30(2008) 187-190.

[16] J.Shao, Z.F. Cao, A new efficient (t, n) verifiable multi-secret sharing (VMSS) based on YCH scheme. Applied Mathematics and Computation, 168(2005) 135-140.

[17] M.H.Dehkordi, S.Mashhadi. New efficient and practical verifiable multi-secret sharing schemes.Information Sciences, 178(2008) 2262-2274.

[18] J.J.Zhao, J.J. Zhang, R.Zhao, A practical verifiable multi-secret sharing scheme, Computer Standards and Interfaces,29(2007) 138-141.

[19] W.A. Jackson, K.M.Martin, C,M. Okeefe, Ideal Secret Sharing Schemes with Multiple Secrets, J Crypt, 9(1996) 233-250.

[20] S.Spiez, A.Timofeev , J.Urbanowicz, Non-admissible tracks in Shamir's scheme, Finite Fields and Their Application, 17(2011) 329-342.

[21] A.Schinzel, S.Spiez, J.Urbanowicz, Admissible tracks in Shamir's scheme, Finite Fields and Their Application, 16(2010) 449-462.

Table 2 The number of $(7, j)$-minimal privileged coalitions in the track $(1, \ldots, 13)$ 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	⋮	⋮	⋮	⋮	⋮	⋮
73	23	24	21	31	0	809	1	2	3	0	0
79	24	20	22	15	0	⋮	⋮	⋮	⋮	⋮	⋮
83	23	21	24	25	0	5231	0	0	1	0	0
89	18	12	15	18	0	⋮	⋮	⋮	⋮	⋮	⋮
97	18	24	15	17	0	31601	0	1	0	0	0
101	19	10	21	17	0	⋮	⋮	⋮	⋮	⋮	⋮
103	18	20	14	20	0	199999	0	0	0	0	0
107	21	14	12	18	0	⋮	⋮	⋮	⋮	⋮	⋮
109	18	18	9	16	0	499253	0	0	0	0	0
113	12	14	16	16	0	⋮	⋮	⋮	⋮	⋮	⋮
127	12	12	16	19	0	⋮	⋮	⋮	⋮	⋮	⋮
131	13	7	11	12	0	≥ 725597	0	0	0	0	0

Table 3 The $(7,3)$-privileged coalitions with the shortest length in the track $(1,\ldots,13)$ over F_p

p	Nr.	$(7,3)$-privileged coalitions with the shortest length
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} {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} {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, 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} {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} {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} {11, 9, 7, 4, 2, 1}{13, 10, 8, 7, 6, 4}{13, 11, 9, 7, 6, 1}{11, 10, 9, 8, 4, 3}{13, 11, 9, 6, 4, 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} {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} {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} {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} {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} {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} {3, 9, 6, 5, 2, 1} {10, 9, 8, 7, 3, 1}{13, 12, 10, 4, 3, 2}{12, 11, 10, 7, 6, 3}{13, 12, 10, 8, 6, 2}
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} {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} {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, 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, 11, 10, 9, 8, 7}{11, 10, 8, 6, 5, 4}{13, 8, 7, 6, 3, 1}{10, 9, 8, 7, 5, 3}{13, 6, 5, 4, 3, 1} {12, 10, 9, 5, 3, 2}{13, 10, 7, 6, 5, 2}{12, 11, 9, 8, 5, 1}
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, 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, 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, 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} {12, 10, 7, 5, 4, 3}{13, 11, 9, 6, 4, 3}{13, 12, 10, 8, 4, 3}{13, 11, 9, 4, 2, 1}{13, 12, 10, 9, 5, 1} {11, 10, 7, 6, 5, 3} {13, 12, 8, 6, 2, 1}{13, 12, 11, 9, 6, 5} {13, 12, 8, 6, 5, 4}{13, 12, 11, 10, 9, 2} {13, 12, 9, 7, 5, 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, 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} {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} {12, 11, 9, 6, 5, 3}{13, 11, 10, 8, 7, 3}{13, 10, 8, 7, 5, 4}{13, 11, 9, 8, 5, 4}{11, 9, 7, 5, 4, 1} {13, 12, 10, 9, 8, 6}{13, 12, 8, 5, 3, 1}{13, 12, 9, 5, 3, 2}{11, 10, 7, 6, 4, 3}{12, 11, 9, 8, 4, 1}
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} {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, 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} {10, 9, 8, 6, 4, 3}{12, 11, 8, 7, 4, 3}{13, 12, 10, 9, 7, 3}{13, 12, 11, 10, 9, 5}{13, 9, 7, 4, 3, 1} {10, 6, 5, 4, 3, 2}{13, 9, 8, 7, 6, 2}
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, 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, 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, 10, 9, 8, 6, 4}{13, 12, 9, 8, 5, 4}{12, 11, 10, 7, 5, 3}{13, 11, 10, 8, 4, 2}{13, 12, 9, 4, 3, 1} {12, 8, 7, 6, 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} {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} {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, 11, 9, 8, 5, 4}{12, 11, 10, 7, 6, 4}{13, 11, 10, 9, 6, 5}{13, 11, 10, 8, 7, 6}{13, 12, 10, 8, 2, 1} {12, 8, 7, 6, 4, 2}{13, 12, 9, 7, 5, 3}
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} {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, 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} {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} {10, 8, 6, 5, 3, 1}{12, 11, 7, 5, 3, 2}{12, 11, 10, 6, 5, 2} {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, 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, 8, 6, 5, 4, 3}{13, 12, 7, 6, 5, 3}{13, 12, 11, 10, 6, 3}{13, 12, 8, 5, 4, 1}{12, 11, 10, 7, 6, 2}
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} {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} {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} {12, 11, 10, 8, 4, 3}{12, 10, 9, 6, 5, 3}{13, 11, 10, 9, 8, 5}{11, 9, 8, 7, 2, 1}{12, 10, 9, 6, 4, 1} {13, 10, 8, 6, 4, 3}
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} {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} {12, 9, 7, 6, 5, 3}{13, 11, 10, 8, 7, 4}{9, 8, 5, 4, 3, 2}{13, 12, 10, 5, 4, 3}
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} {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, 12, 11, 10, 4, 1}{13, 9, 8, 7, 6, 5}
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} {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, 12, 11, 10, 4, 1}{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} {10, 8, 6, 5, 4, 3}{13, 12, 9, 8, 6, 4}{10, 9, 8, 7, 6, 5}{13, 7, 6, 5, 4, 3}
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} {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} {10, 9, 8, 5, 4, 3}{13, 8, 7, 6, 5, 3}{13, 11, 10, 9, 5, 4}{13, 12, 10, 8, 6, 4}{9, 8, 7, 6, 5, 1} {13, 12, 10, 9, 7, 2}
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} {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} {13, 12, 8, 7, 6, 5}
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} {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} {11, 10, 9, 8, 5, 2}
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} {11, 6, 5, 4, 2}{10, 9, 8, 5, 4, 2}{13, 12, 9, 7, 4, 3}{13, 12, 11, 7, 5, 3}{8, 7, 6, 5, 4, 2}
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} {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}{10, 9, 8, 4, 3, 2}
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} {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}{11, 10, 9, 8, 3, 1}
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} {11, 10, 9, 8, 6, 2}{11, 9, 7, 5, 4, 3}{13, 12, 11, 10, 9, 6}{13, 10, 8, 7, 5, 2}
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, 11, 10, 9, 6, 2}{11, 9, 7, 5, 4, 3}{13, 12, 11, 10, 9, 6} {12, 10, 7, 5, 3, 2}
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, 8, 7, 5, 4, 3}{13, 11, 10, 7, 4, 3}{13, 11, 10, 7, 6, 5}{12, 11, 7, 6, 4, 1}
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} {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} {12, 10, 8, 7, 5, 4}{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} {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} {13, 12, 7, 6, 3, 2}
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} {12, 10, 9, 8, 7, 2}{13, 11, 8, 7, 6, 5}
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} {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, 11, 8, 5, 3, 2}
199	9	{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} {12, 10, 7, 6, 5, 2} {10, 9, 8, 7, 5, 2}{12, 11, 10, 6, 5, 3} {12, 11, 10, 6, 4, 2}
⋮		⋮
≥ 22787		no privileged coalitions (proven)