Secret Sharing Schemes with General Access Structures (Full version)*

Jian Liu[1], Sihem Mesnager[2], and Lusheng Chen[3]

[1] School of Computer Software, Tianjin University, Tianjin 300072, P. R. China and
CNRS, UMR 7539 LAGA, Paris, France
jianliu.nk@gmail.com

[2] Department of Mathematics, University of Paris VIII, University of Paris XIII,
CNRS, UMR 7539 LAGA and Telecom ParisTech, Paris, France
smesnager@univ-paris8.fr

[3] School of Mathematical Sciences, Nankai University, Tianjin 300071, P. R. China
lschen@nankai.edu.cn

Abstract. Secret sharing schemes with general monotone access structures have been widely discussed in the literature. But in some scenarios, non-monotone access structures may have more practical significance. In this paper, we shed a new light on secret sharing schemes realizing general (not necessarily monotone) access structures. Based on an attack model for secret sharing schemes with general access structures, we redefine perfect secret sharing schemes, which is a generalization of the known concept of perfect secret sharing schemes with monotone access structures. Then, we provide for the first time two constructions of perfect secret sharing schemes with general access structures. The first construction can be seen as a democratic scheme in the sense that the shares are generated by the players themselves. Our second construction significantly enhance the efficiency of the system, where the shares are distributed by the trusted center (TC).

Keywords: Secret sharing schemes; general access structures; information rate; orthogonal arrays; resilient functions.

1 Introduction

Secret sharing schemes were first introduced by Blakley [6] and Shamir [32] independently in 1979. Besides secure information storage, secret sharing schemes have numerous other applications in cryptography such as secure multiparty computations [5,15,16], key-distribution problems [27], multi-receiver authentication schemes [36] etc. Note that minimal codes introduced and studied in the literature have applications in secret sharing (see for instance [1],[13],[17],[18],[19],[20],[22]).

* This work is supported by the National Key Basic Research Program of China under Grant 2013CB834204. This paper will appear in the proceedings of the conference "11th International Conference on Information Security and Cryptology" Inscrypt 2015 (IACR) published by Springer.

The secret sharing schemes given in [6] and [32] are for the threshold case, i.e., the qualified groups that can reconstruct the secret key are all the subsets with cardinality no smaller than a threshold. A (t, n) threshold scheme is a method where n pieces of information of the secret key K, called *shares* are distributed to n players so that the secret key can be reconstructed from the knowledge of any t or more shares and the secret key can not be reconstructed from the knowledge of fewer than t shares. But in reality, there are many situations in which it is desirable to have a more flexible arrangement for reconstructing the secret key. Given some n players, one may want to designate certain authorized groups of players who can use their shares to recover the key. This kind of scheme is called secret sharing scheme for general access structure, which generalizes the threshold case. Formally, a secret sharing scheme for general access structure is a method of sharing a secret K among a finite set of players $\mathcal{P} = \{\mathrm{P}_1, \ldots, \mathrm{P}_n\}$ in such a way that

1. if the players in $A \subseteq \mathcal{P}$ are qualified to know the secret, then by pooling together their partial information, they can reconstruct the secret K,
2. any set $B \subset \mathcal{P}$ which is not qualified to know K, cannot reconstruct the secret K.

The threshold secret sharing schemes have received considerably attention, see e.g. [14,21,29,30]. Secret sharing schemes for general monotone access structures were first studied by Ito, Saito, and Nishizeki [25]. The access structure defined in [25] is a set of qualified groups $\mathit{\Gamma}$ which satisfies the monotone property that if $A \in \mathit{\Gamma}$ and $A \subseteq B$, then $B \in \mathit{\Gamma}$. Secret sharing schemes for general monotone access structures have got a lot of attention, and there exist a wide range of general methods of constructing monotone secret sharing schemes [3,4,8,26]. The approaches to the construction of monotone secret sharing schemes based on linear codes can be found in [7,28]. To our best knowledge, all the known secret sharing schemes are designed for realizing monotone access structures. We refer to [16] for a survey on monotone secret sharing schemes.

A secret sharing scheme can be represented by a set of recovery algorithms which realizes an access structure such that only qualified groups can reconstruct the secret key by pooling their shares. For example, in the bank teller problem described in Chapter 13 of [33], any two out of three tellers are authorized to reconstruct the secret key. It is quite natural to assume that three tellers are permitted to make a requirement on two of them to execute the recovery algorithm and reconstruct the secret key, then any group with two or more tellers is a qualified group. Hence, the access structure considered in this scenario has monotone property. However, for some scenarios, the requirement on fewer players of a group to recover the secret key is not available, and secret sharing schemes with non-monotone access structures may be more preferable. For a secret sharing scheme, it is reasonable to assume that the access structure is public and in the reconstruction phase, the players are anonymous, that is to say, the players will not disclose which group they belong to.

Scenario 1 Suppose that on the network, there are several groups of users who share a large amount of information resources stored by the network center (e.g., a secure cloud storage server) with a secret key. Once the secret key is recovered, only the users who pool their shares will get the access to download the information. For some reasons, the users of the same group are not willing to download their information together with an outsider who does not belong to this group. So, only when all the users of the same group pool their shares, the secret key can be reconstructed, and if an outsider joins, the reconstruction reveals nothing about the secret key.

The access structure in the above scenario is non-monotone, since there exist $A \in \Gamma$ and $B \notin \Gamma$ such that $A \subseteq B$. A secret key can always be recovered by all the users in a qualified group A, but if an outsider, say P, intrudes, the reconstruction by the users in the unqualified (i.e., forbidden) group $B = A \bigcup \mathrm{P}$ reveals nothing about the secret key. Consider that in Scenario 1, different groups of users have independently purchased the access to the database from the network center, and the payment of each group is afforded by every user of this group, thus the costs of the users from different groups may be different. Of course, the users belonging to one group do not hope to download their data together with an outsider. We consider data mining as another example for Scenario 1. Suppose different groups of market investigators are employed by different companies respectively to gather some information from the network center. Because of the market competition, the companies do not hope to disclose what they are gathering to each other, i.e., the market investigators of one company are not willing to reconstruct the secret key and download their information together with an outsider. Thus, the access structures here should be non-monotone.

Secret sharing scheme is also a key tool for secure multiparty computation (MPC) (see [2,15,16]). Secure MPCs solve the problem that n players want to compute some agreed function with their inputs private. For instance, two millionaires want to know who is richer without disclosing their wealths to each other. This millionaire problem, first introduced by Yao [35], is a secure MPC problem which can be solved by monotone secret sharing schemes. A secure MPC protocol can be described as that every player shares his input with all the players by employing some secret sharing scheme, then the players in a qualified group can compute the result of the agreed function, and the players in a forbidden group cannot learn anything about the result and the inputs of the other players, where the qualified and the forbidden groups are determined by the access structure of the employed secret sharing scheme (see [2,15] for more details). In the following scenario, a secure MPC with non-monotone access structure is preferable.

Scenario 2 Suppose that the employees of several different companies are interested in their salary level by comparing their incomes, i.e., they want to know the ranking of the average income of each company by sharing their incomes privately. To avoid the risk of embarrassment, the employees of one company are not willing to compute the ranking result together with an outsider who does not belong to this company. So, only all the employees of the same company can compute the ranking result, and if an outsider joins, the computation reveals nothing about the result.

In the above scenarios, we must guarantee that if B is a qualified group but $A \supseteq B$ is not, then the players in A cannot make a requirement on the players in B to reconstruct the secret key or to compute the result of the agreed function. When all the players in a forbidden group follow the protocol accordingly, they can determine nothing about the secret key or the result of the agreed function.

Perhaps one can find some other means to solve the problems presented in the above scenarios, and Scenario 2 may have less practical significance, but all these are intended primarily as examples to provide us a direction for possible applications of non-monotone secret sharing schemes. Similar practical scenarios could be found.

In this paper, we mainly discuss secret sharing schemes realizing general (not necessarily monotone) access structures. We first describe a general attack model for secret sharing schemes. Afterwards, a formal definition of unconditional security (called perfect) for secret sharing schemes with general access structures is given, which is a generalization of the known perfect monotone secret sharing schemes. Moreover, we propose two constructions for secret sharing schemes realizing general access structures. To the best of our knowledge, this is the first time when constructions of non-monotone secret sharing schemes are proposed. Our first construction is democratic in the sense that the shares are generated by the players themselves instead of distributed by the trusted center (TC). In this construction, TC has to recompute an updated function for every time the secret key changes. The second construction is presented for the sake of efficiency, where the shares are computed and distributed by TC. We also show that the well designed secret sharing schemes presented in this paper are perfect.

This paper is organized as follows. Formal definitions and necessary preliminaries are introduced in Section 2. In Section 3, we discuss the attack model and the security of secret sharing schemes with general access structures. Perfect democratic secret sharing schemes are constructed in Section 4, and perfect secret sharing schemes with distributed shares are constructed in Section 5. In the last section, we summarize this paper and indicate some future research directions.

2 Preliminaries

For a secret sharing scheme, we denote a *player* by P_i, where $i = 1, 2, \ldots$, the set of all the players by $\mathcal{P}$, the set of all the subsets of $\mathcal{P}$ by $2^{\mathcal{P}}$, and the *trusted center* of the scheme by TC. The groups authorized to reconstruct the secret key are called *qualified*, and the groups unauthorized to reconstruct the secret key are called *forbidden.* The sets of qualified and forbidden groups are denoted by $\varGamma$ and $\varDelta$ respectively, where $\varGamma \subseteq 2^{\mathcal{P}}$ and $\varDelta \subseteq 2^{\mathcal{P}}$. If $\varGamma \bigcap \varDelta = \emptyset$, then the tuple $(\varGamma, \varDelta)$ is called an *access structure.* Moreover, an access structure is called *complete* if $\varGamma \bigcup \varDelta = 2^{\mathcal{P}}$. In this paper, we focus on secret sharing schemes with complete access structures. The set of qualified groups $\varGamma$ is called *monotone increasing* if for each set $A \in \mathit{\Gamma}$, the superset of A is also in $\mathit{\Gamma}$. An access structure $(\mathit{\Gamma}, \mathit{\Delta})$ is called *monotone* if $\mathit{\Gamma}$ is monotone increasing.

Let $\mathscr{S}$ be a secret sharing scheme. We denote the set of all possible secret keys by $\mathbf{K}$, the set of all possible shares of group $A = \{\mathrm{P}_{i_1}, \ldots, \mathrm{P}_{i_m}\} \in 2^{\mathcal{P}}$ by $\mathbf{S}(A)$, i.e., $\mathbf{S}(A) = \mathbf{S}(\mathrm{P}_{i_1}) \times \cdots \times \mathbf{S}(\mathrm{P}_{i_m})$, where $\mathbf{S}(\mathrm{P}_{i_j})$ is the set of all possible shares of P_{i_j} and "×" denotes the Cartesian product. For a qualified group $A \in \mathit{\Gamma}$, there exists a recovery algorithm f_A defined on $\mathbf{S}(A)$ which satisfies $f_A(s(A)) = k$, where $k \in \mathbf{K}$ is the secret key that TC wants to share and $s(A) \in \mathbf{S}(A)$ is the shares of the players in A. Then, a secret sharing scheme $\mathscr{S}$ realizing access structure $(\mathit{\Gamma}, \mathit{\Delta})$ can be viewed as a set of recovery algorithms $\mathcal{F} = \{f_A \mid A \in \mathit{\Gamma}\}$ such that only qualified groups can reconstruct the secret key by pooling their shares.

Definition 1. *[9] Let $\mathscr{S}$ be a secret sharing scheme, $\mathbf{K}$ be the set of all possible secret keys, and for $1 \leqslant i \leqslant n$, $\mathbf{S}(\mathrm{P}_i)$ be the set of all possible shares that P_i might have. Then, the* information rate *of P_i is defined as*

$$\rho_i = \frac{\log_2 |\mathbf{K}|}{\log_2 |\mathbf{S}(\mathrm{P}_i)|},$$

and the information rate *of $\mathscr{S}$ is defined as*

$$\rho = \min\{\rho_i \mid 1 \leqslant i \leqslant n\}. \tag{1}$$

In the following, we introduce some definitions and properties of q-ary functions, which will be useful in constructing secret sharing schemes.

Let $\mathbb{F}_q$ be a finite field, where q is a power of a prime, then $\mathbb{F}_q^n$ denotes the n-dimensional vector space over the finite field $\mathbb{F}_q$. In this paper, we always assume $q > 2$. Let $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, then $(\mathbb{F}_q^*)^n$ denotes the Cartesian product that $\overbrace{\mathbb{F}_q^* \times \cdots \times \mathbb{F}_q^*}^{n}$. The mappings from the vector space $\mathbb{F}_q^n$ to $\mathbb{F}_q$ are called n-variable *q-ary functions*, which can be uniquely represented in the *algebraic normal form* (ANF), see [31]:

$$F(x) = \sum_{u \in \mathbb{Z}_q^n} a_u x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n},$$

where $\mathbb{Z}_q = \{0, \ldots, q-1\}$, $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, $u = (u_1, \ldots, u_n) \in \mathbb{Z}_q^n$, and $a_u \in \mathbb{F}_q$. In fact, given the values of $F(w)$, $w = (w_1, \ldots, w_n) \in \mathbb{F}_q^n$, the ANF of F can be determined as

$$F(x) = \sum_{w \in \mathbb{F}_q^n} F(w) \prod_{i=1}^{n} \left(1 - (x_i - w_i)^{q-1}\right). \tag{2}$$

For an n-variable q-ary function F, the set $\mathbb{F}_q^n$ is called the *domain set* of F and the vector $(F(v_0), \ldots, F(v_{q^n-1}))$ is called the *value table* of F, where $v_0, \ldots, v_{q^n-1}$ are all the vectors in $\mathbb{F}_q^n$ which have some prescribed order, e.g., the lexicographical order. F is called *balanced* if for any element $a \in \mathbb{F}_q$, the size of the pre-image set satisfies $|F^{-1}(a)| = q^{n-1}$.

More generally, if F is a mapping from $E_1 \subseteq \mathbb{F}_q^n$ to $E_2 \subseteq \mathbb{F}_q$, then E_1 is called the domain set of F, and $(F(v_0), \ldots, F(v_{|E_1|-1}))$ is called the value table of F, where $v_0, \ldots, v_{|E_1|-1}$ are all the vectors in E_1 with some prescribed order. In addition, F is called balanced onto E_2 if for any element $a \in E_2$, the size of the pre-image set satisfies $|F^{-1}(a)| = |E_1|/|E_2|$.

For $i = 1, \ldots, m$, let F_i be a mapping from $E_i \subseteq \mathbb{F}_q^n$ to $\mathbb{F}_q$, where $E_1, \ldots, E_m$ are disjoint sets, then the *concatenation function* F of $F_1, \ldots, F_m$ is the mapping from $\bigcup_{i=1}^m E_i$ to $\mathbb{F}_q$ which satisfies $F(x) = F_i(x)$ for $x \in E_i$, where $i = 1, \ldots, m$.

3 The Security of Secret Sharing Schemes with General Access Structures

For a secret sharing scheme with general access structure (Γ, Δ), we assume that the players in $A \in \Delta$ are passively collaborating to pool their shares and try to reconstruct the secret key. Note that the collaborating players are assumed to execute the protocol correctly and every player will keep his share private, i.e., the attack is *passive*. We also assume that the collaborating players are *static*, which means that the set of collaborating players is fixed during the protocol.

Attack Model The players in $A \in \Delta$ are passively collaborating to find some efficient recovery algorithms to reconstruct the secret key.

For a general access structure, the players in group $A \in \Delta$ will try to guess the secret key by collaborating, and in this case, even if $A \supseteq B \in \Gamma$ (this case only appears in the non-monotone case), the players in B are passively collaborating, and cannot be required to execute their recovery algorithm and reconstruct the secret key independently from A. In Section 1, we present two scenarios to show that this assumption is reasonable for the non-monotone case. Note that a secret sharing scheme can be viewed as a set of recovery algorithms $\mathcal{F} = \{f_A \mid A \in \Gamma\}$. Hence, if the players in $A \in \Delta$ are passively collaborating, they can only try to guess the secret key by employing some known reconstruction algorithms that f_B, $B \in \Gamma$, where $B \nsubseteq A$. Particularly, for monotone access structures, one can just assume that all the players belonging to a forbidden group (which is a proper subset of a qualified group) are passively collaborating to reconstruct the secret key.

Let A be any subset of players, $B \in \Gamma$, and $k \in \mathbf{K}$, then given $s(A) \in \mathbf{S}(A)$, the conditional probability determined by algorithm f_B is denoted by $\Pr_B(K = k \mid S(A) = s(A))$, which means that by using algorithm f_B, the players in A can guess the secret key correctly with probability $\Pr_B(K = k \mid S(A) = s(A))$. We use $\Pr(K = k \mid S(A) = s(A))$ for short if there is no risk of confusion, and use $\Pr(K = k)$ to denote the *a prior* probability distribution on the secret key set $\mathbf{K}$. Considering the above attack model, we present a formal definition of unconditional security for secret sharing schemes with general access structures.

Definition 2. *A secret sharing scheme $\mathscr{S}$ with access structure (Γ, Δ) and secret key set $\mathbf{K}$ is* perfect *if $\mathscr{S}$ satisfies the following two properties.*

(i) For any $A \in \Gamma$, the secret key can be reconstructed correctly.

(ii) For any $A \in \mathit{\Delta}$ and any $B \in \mathit{\Gamma}$, where $B \not\subseteq A$, the conditional probability determined by algorithm f_B satisfies

$$\Pr(K = k \mid S(A) = s(A)) = \Pr(K = k)$$

for every $k \in \mathbf{K}$. In other words, by using algorithm f_B, the players in A can learn nothing about the secret key.

Remark 1. For secret sharing schemes with monotone access structures, the concept of perfect system has been introduced in [9] and widely studied (see [2,33] for a survey). If a secret sharing scheme $\mathscr{S}$ with monotone access structure $(\mathit{\Gamma}, \mathit{\Delta})$ satisfies (i) for any $A \in \mathit{\Gamma}$, the secret key can be reconstructed correctly, (ii) for any $A \in \mathit{\Delta}$, the players in A can learn nothing about the secret key, then $\mathscr{S}$ is called perfect. From the above discussion, it is easy to see that the concept of perfect system given in Definition 2 is more general, and for the monotone case, Definition 2 coincides with the standard perfect monotone secret sharing schemes.

For perfect secret sharing schemes with monotone access structures, it is proved that the information rate $\rho \leqslant 1$, see [9,33]. We now show that this result still holds for perfect secret sharing schemes with general access structures.

Theorem 1. *For any perfect secret sharing scheme with general access structure, the information rate satisfies $\rho \leqslant 1$.*

Proof. Suppose that $\mathscr{S}$ is a perfect secret sharing scheme with general access structure $(\mathit{\Gamma}, \mathit{\Delta})$, then there must exist a set $A \in \mathit{\Gamma}$ such that $B = A \setminus \{\mathrm{P}_i\} \in \mathit{\Delta}$ for some $\mathrm{P}_i \in A$. In fact, if for any $A \in \mathit{\Gamma}$ and any $\mathrm{P}_i \in A$, $A' = A \setminus \{\mathrm{P}_i\} \in \mathit{\Gamma}$, then $\emptyset \neq A' \in \mathit{\Gamma}$ and $A' \setminus \{\mathrm{P}_j\} = A \setminus \{\mathrm{P}_i, \mathrm{P}_j\} \in \mathit{\Gamma}$. This process can be continued until we get the contradiction that $\emptyset \in \mathit{\Gamma}$.

Without loss of generality, we assume that $A = \{\mathrm{P}_1, \ldots, \mathrm{P}_m\} \in \mathit{\Gamma}$ and $B = A \setminus \{\mathrm{P}_m\} \in \mathit{\Delta}$. Since $B \in \mathit{\Delta}$ and $\mathscr{S}$ is perfect, when the players in B are collaborating to reconstruct the secret key by using the recovery algorithm f_A, then the conditional probability of the secret key is

$$\Pr(K = k \mid S(B) = s(B)) = \Pr(K = k), \tag{3}$$

where $k \in \mathbf{K}$. Since $A \in \mathit{\Gamma}$, then Eq.(3) implies that for any two distinct secret keys $k_1, k_2 \in \mathbf{K}$, there exist two distinct shares $s_1(\mathrm{P}_m), s_2(\mathrm{P}_m) \in \mathbf{S}(\mathrm{P}_m)$ such that

$$f_A(s(B), s_1(\mathrm{P}_m)) = k_1, \qquad f_A(s(B), s_2(\mathrm{P}_m)) = k_2. \tag{4}$$

Therefore, $|\mathbf{S}(\mathrm{P}_m)| \geqslant |\mathbf{K}|$, and thus $\rho_m \leqslant 1$. Hence, from (1), we have $\rho \leqslant 1$. □

4 Democratic Secret Sharing Schemes

In this section, we present a construction of democratic secret sharing schemes with general access structures, where the shares are generated on the set of all possible shares independently by the players themselves. Moreover, we provide a perfect secret sharing scheme with information rate $\rho = 1$.

Table 1. Secret Sharing Scheme I

Initialization Phase:

1. For a player $\mathrm{P}_i \in \mathcal{P}$, where $1 \leqslant i \leqslant n$, P_i randomly chooses $\alpha_i \in \mathbb{F}_q^*$ as his share, and then transmits α_i secretly to the trusted center TC.
2. The access structure $(\mathit{\Gamma}, \mathit{\Delta})$ is public.

Sharing Phase:

1. Suppose TC wants to share a secret key $k \in \mathbb{F}_q^*$, then TC chooses a q-ary function $F : \mathbb{F}_q^n \to \mathbb{F}_q$ which satisfies
$$F(x) = k, \quad \text{if } x = \sum_{i \in A} \alpha_i e_i \text{ for some } A \in \mathit{\Gamma}, \tag{5}$$
where $e_1, \ldots, e_n$ are the identity vectors in $\mathbb{F}_q^n$, and for other $x \in \mathbb{F}_q^n$, $F(x)$ are carefully chosen.
2. TC computes the algebraic normal form of F by using Eq.(2),
$$F(x) = \sum_{u=(u_1,\ldots,u_n) \in \mathbb{Z}_q^n} a_u x_1^{u_1} \cdots x_n^{u_n}.$$
3. TC publishes the algebraic normal form of F.

Reconstruction Phase:

For any $A = \{\mathrm{P}_{i_1}, \ldots, \mathrm{P}_{i_m}\} \in 2^{\mathcal{P}}$, the players in A do as follows.

1. **Determine the recovery algorithm.**
The players in A get
$$f_A(x_{i_1}, \ldots, x_{i_m}) = F(0, \ldots, 0, x_{i_1}, 0, \ldots, 0, x_{i_m}, 0, \ldots, 0)$$
as their recovery algorithm.
2. **Compute the secret key.**
The players in A pool their shares and compute $f_A(\alpha_{i_1}, \ldots, \alpha_{i_m})$.

4.1 A General Description

Let e_i be the *identity vector* in $\mathbb{F}_q^n$ with 1 in the i-th position and zeros elsewhere, where q is a power of a prime. By abuse of notation, we write a set $A = \{i_1, \ldots, i_m\}$ for $A = \{\mathrm{P}_{i_1}, \ldots, \mathrm{P}_{i_m}\} \subseteq \mathcal{P}$.

In Table 1, we present a construction of democratic secret sharing schemes realizing general access structures.

4.2 Perfect Democratic Secret Sharing Schemes Realizing General Access Structures

As shown in Table 1, given a set of n players $\mathcal{P} = \{\mathrm{P}_1, \ldots, \mathrm{P}_n\}$ with general access structures $(\mathit{\Gamma}, \mathit{\Delta})$ and secret key set $\mathbf{K} = \mathbb{F}_q^*$, one can always construct a democratic secret sharing scheme. Clearly, the security of Secret Sharing

Scheme I depends heavily on the choice of the q-ary function F. In Table 2, an explicit construction of q-ary functions is presented. Employing such functions in Secret Sharing Scheme I, one can get perfect democratic secret sharing schemes. We first introduce some useful notations below.

For $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, let $\mathrm{supp}(x) = \{i \mid x_i \neq 0\}$ denote the support set of x. Then, for an n-variable q-ary function F and a set $A \subseteq \mathcal{P}$, $F|_A$ denotes the restriction of F to the set

$$E_A = \{x \in \mathbb{F}_q^n \mid \mathrm{supp}(x) = A\}, \tag{6}$$

i.e., $F|_A : E_A \to \mathbb{F}_q$ satisfies $F|_A(x) = F(x)$ for $x \in E_A$. For a set $E \subseteq \mathbb{F}_q^n$ and an element $a \in \mathbb{F}_q^n$, $a + E = \{a + e \mid e \in E\}$. For $s(\mathrm{P}_i) \in \mathbf{S}(\mathrm{P}_i)$, $i \in A$, which are the shares of players in A, define $\boldsymbol{s}(A) = \sum_{i \in A} s(\mathrm{P}_i) e_i \in \mathbb{F}_q^n$, then for $B \subseteq A$, we denote by $F|_{s(A \setminus B) \times B}$ the restriction of F to the set

$$E_{s(A \setminus B) \times B} = \boldsymbol{s}(A \setminus B) + E_B. \tag{7}$$

Moreover, for $B \subseteq A$, we denote by $F|_{s(A \setminus B) \times \overline{B}}$ the restriction of F to the set

$$E_{s(A \setminus B) \times \overline{B}} = \{(x_1, \ldots, x_n) \in E_{s(A \setminus B) \times B} \mid x_i \neq s(\mathrm{P}_i), i \in B\}. \tag{8}$$

Clearly, if $B = \emptyset$, then $F|_{s(A \setminus B) \times B} = F|_{s(A \setminus B) \times \overline{B}} = F(\boldsymbol{s}(A))$.

Proposition 1. *For $A \subseteq \mathcal{P}$, the set E_A can be partitioned into disjoint subsets $E_{s(A \setminus B) \times \overline{B}}$, where $B \subseteq A$, i.e.,*

$$E_A = \bigcup_{B \subseteq A} E_{s(A \setminus B) \times \overline{B}}, \tag{9}$$

where for two distinct subsets $B_1, B_2 \subseteq A$,

$$E_{s(A \setminus B_1) \times \overline{B_1}} \bigcap E_{s(A \setminus B_2) \times \overline{B_2}} = \emptyset. \tag{10}$$

Proof. We first prove (10). Since $B_1 \neq B_2$, then without loss of generality, we assume that $i \in B_1$ but $i \notin B_2$. Suppose that there exists $x = (x_1, \ldots, x_n) \in E_{s(A \setminus B_1) \times \overline{B_1}} \bigcap E_{s(A \setminus B_2) \times \overline{B_2}}$, then we have $x_i \neq s(\mathrm{P}_i)$ since $i \in B_1$. However, $i \notin B_2$ implies that $x_i = s(\mathrm{P}_i)$, a contradiction. Hence, (10) holds.

It is obvious that $\bigcup_{B \subseteq A} E_{s(A \setminus B) \times \overline{B}} \subseteq E_A$. Suppose that $|A| = m$, then since the sets $E_{s(A \setminus B) \times \overline{B}}$, where $B \subseteq A$, are disjoint, we have that

$$\left| \bigcup_{B \subseteq A} E_{s(A \setminus B) \times \overline{B}} \right| = \sum_{B \subseteq A} |E_{s(A \setminus B) \times \overline{B}}| = \sum_{i=0}^{m} \binom{m}{i} (q-2)^i = (q-1)^m = |E_A|. \tag{11}$$

Therefore, (9) holds, and we get the desired result. □

By using Proposition 1, we can prove that Construction I in Table 2 outputs a q-ary function. A full proof of the following lemma is provided in Appendix A.

Table 2. Construction I

```
Input:   Secret shares $s(\mathrm{P_i}) \in \mathbb{F}_q^*$, $i = 1, \ldots, n$;
         Secret key $k \in \mathbb{F}_q^*$;
         Access structure $(\mathit{\Gamma}, \mathit{\Delta})$.
Output:  A function $F : \mathbb{F}_q^n \to \mathbb{F}_q$.

Step 1:  For every subset of players $A \in \mathit{\Delta}$, set $F|_A = 0$, i.e., $F|_A$ is a zero function.
Step 2:  For every subset of players $A = \{\mathrm{P}_{i_1}, \ldots, \mathrm{P}_{i_m}\} \in \mathit{\Gamma}$, execute the following two steps.
         1. Set $F(\boldsymbol{s}(A)) = k$.
         2. Define $n_0 = 1$ and $N_0 = 0$. From $l = 1$ to $l = m$, do as follows.
            For every $B = \{\mathrm{P}_{j_1}, \ldots, \mathrm{P}_{j_l}\} \subseteq A$, arrange the value table of $F|_{s(A \setminus B) \times \overline{B}}$ as follows.
            (i) Let $k$ appear $n_l$ times, where
                $$n_l = (q-1)^{l-1} - \sum_{i=0}^{l-1} \binom{l}{i} n_i. \qquad (12)$$
            (ii) Let every element in $\mathbb{F}_q^* \setminus \{k\}$ appear $N_l$ times, where
                $$N_l = (q-1)^{l-1} - \sum_{i=0}^{l-1} \binom{l}{i} N_i. \qquad (13)$$
```

Lemma 1. *Construction I outputs an n-variable q-ary function F.*

Lemma 2. *Let F be constructed by Construction I. Then, for any subset of players $A \in \mathit{\Gamma}$ and any non-empty set $B \subseteq A$, the restriction function $F|_{s(A \setminus B) \times B}$ is balanced onto $\mathbb{F}_q^*$.*

Proof. Let $A \in \mathit{\Gamma}$ and $\emptyset \neq B \subseteq A$ with $|A| = m$ and $|B| = l \leqslant m$. According to Step 2 of Construction I, we have that for any subset $C \subseteq B$ with $|C| = s$, where $0 \leqslant s \leqslant l$, the secret key k appears $n_s = (q-1)^{s-1} - \sum_{i=0}^{s-1} \binom{s}{i} n_i$ times in the value table of $F|_{s(A \setminus C) \times \overline{C}}$, where $n_0 = 1$, and every element in $\mathbb{F}_q^* \setminus \{k\}$ appears $N_s = (q-1)^{s-1} - \sum_{i=0}^{s-1} \binom{s}{i} N_i$ times in the value table of $F|_{s(A \setminus C) \times \overline{C}}$, where $N_0 = 0$. Clearly, n_s and N_s depend only on s. Similar to Proposition 1, we can prove that

$$E_{s(A \setminus B) \times B} = \bigcup_{C \subseteq B} E_{s(A \setminus C) \times \overline{C}},$$

where for two distinct subsets $C_1, C_2 \subseteq B$, $E_{s(A \setminus C_1) \times \overline{C_1}} \bigcap E_{s(A \setminus C_2) \times \overline{C_2}} = \emptyset$. Therefore, $F|_{s(A \setminus B) \times B}$ is the concatenation function of $F|_{s(A \setminus C) \times \overline{C}}$, $C \subseteq B$. Note that the number of different $C \subseteq B$ with $|C| = s$ is $\binom{l}{s}$. Thus, in the value table of $F|_{s(A\setminus B)\times B}$, the secret key k appears $\sum_{i=0}^{l}\binom{l}{i}n_i$ times and every element in $\mathbb{F}_q^*\setminus\{k\}$ appears $\sum_{i=0}^{l}\binom{l}{i}N_i$ times. According to Eq.(12) and Eq.(13), we have $\sum_{i=0}^{l}\binom{l}{i}n_i = \sum_{i=0}^{l}\binom{l}{i}N_i = (q-1)^{l-1}$, which implies that $F|_{s(A\setminus B)\times B}$ is balanced onto $\mathbb{F}_q^*$. □

Theorem 2. *Let F be constructed by Construction I. Then, Secret Sharing Scheme I is perfect with information rate $\rho = 1$.*

Proof. It is clear that Secret Sharing Scheme I has $\rho = 1$. We now prove that if F is constructed by Construction I, then Secret Sharing Scheme I is perfect.

For any $A \in \Gamma$, the recovery algorithm f_A satisfies $f_A(s(A)) = F(\boldsymbol{s}(A)) = k$, thus the qualified group A can reconstruct the secret key.

For any forbidden group $A \in \Delta$, we assume that the players in A are collaborating to reconstruct the secret key by using some recovery algorithm, say f_B, where $B \in \Gamma$. As discussed in Section 3, we must have $B \not\subseteq A$, i.e., $C = A \bigcap B \subsetneq B$, where $C \subsetneq B$ means that C is a proper subset of B (i.e., $C \subseteq B$ but $C \neq B$). Since $C \subsetneq B$, then $B \setminus C \neq \emptyset$. Due to Lemma 2, the restriction function $F|_{s(C)\times(B\setminus C)}$ is balanced onto $\mathbb{F}_q^*$. Hence, the conditional probability determined by f_B satisfies

$$\Pr(K = \gamma \mid S(C) = s(C)) = \frac{1}{q-1} = \frac{1}{|\mathbf{K}|} = \Pr(K = \gamma), \tag{14}$$

where $\gamma \in \mathbb{F}_q^*$, which implies that for every $k \in \mathbf{K}$, the secret key k can be guessed correctly with probability $\Pr(K = k) = 1/|\mathbf{K}|$. Therefore, according to Definition 2, we get that Secret Sharing Scheme I is perfect. □

5 Secret Sharing Schemes with Distributed Shares

In Section 4, we have shown a construction of perfect democratic secret sharing schemes with information rate $\rho = 1$. Note that in Secret Sharing Scheme I, the shares are generated by the players themselves, but when the secret key that TC wants to share is changed, the function F published by TC should be updated accordingly. This may cause the problem of low efficiency if n is large, because TC has to recompute the ANF of the new function F, and this process needs approximately $\mathcal{O}(nq^n)$ operations over the finite field $\mathbb{F}_q$.

To avoid the drawback of updating the function F, we propose Secret Sharing Scheme II, where the shares of the players are computed and distributed secretly by TC. In Secret Sharing Scheme II, the public q-ary function F is fixed, and when the secret key is changed, the shares distributed to the players by TC will be updated accordingly. Comparing the two constructions, one can see that Secret Sharing Scheme I realizes the democracy, while Secret Sharing Scheme II is designed towards enhancing the efficiency.

5.1 A General Description

Recall that for an n-variable q-ary function F, $F|_A$ denotes the restriction of F to the set $E_A = \{x \in \mathbb{F}_q^n \mid \mathrm{supp}(x) = A\}$, where $A = \{i_1, \ldots, i_m\}$, and we use $A = \{\mathrm{P}_{i_1}, \ldots, \mathrm{P}_{i_m}\} \subseteq \mathcal{P}$ to denote a subset of players. In Table 3, we present Secret Sharing Scheme II, in which the shares of the players are computed and distributed secretly by TC. It can be seen that, different from Secret Sharing Scheme I, in Secret Sharing Scheme II, the q-ary function determined by TC does not depend on the choice of the secret key.

5.2 Perfect Secret Sharing Schemes from Orthogonal Arrays

An *orthogonal array*, denoted by $OA_\lambda(t, m, v)$, is a $\lambda v^t \times m$ array of v symbols, such that in any t columns of the array, every possible t-tuple of the symbols appears exactly λ times. An orthogonal array is called *simple* if and only if no two rows are identical. A large set of orthogonal arrays $LOA_\lambda(t, m, v)$ is a set of v^{m-t}/λ simple arrays $OA_\lambda(t, m, v)$ which satisfies that every possible m-tuple of the symbols appears in exactly one of the orthogonal arrays in the set. We refer to [34] for background on orthogonal arrays.

In Table 4, we propose a method to construct q-ary functions by using orthogonal arrays. By employing such functions in Secret Sharing Scheme II, we can get perfect secret sharing schemes.

Theorem 3. *Let F be constructed by Construction II. Then, Secret Sharing Scheme II is perfect.*

Proof. For any subset of players $A = \{\mathrm{P}_{i_1}, \ldots, \mathrm{P}_{i_m}\} \in \Gamma$, the recovery algorithm f_A satisfies $f_A\left(x_{i_1}^{(A)}, \ldots, x_{i_m}^{(A)}\right) = F|_A\left(x^{(A)}\right) = k$, where

$$x^{(A)} = \left(0, \ldots, 0, x_{i_1}^{(A)}, 0, \ldots, 0, x_{i_m}^{(A)}, 0, \ldots, 0\right),$$

thus the qualified group A can reconstruct the secret key.

For any forbidden group $A \in \Delta$, we assume that the players in A are collaborating to reconstruct the secret key by using some recovery algorithm, say f_B, where $B \in \Gamma$. As discussed in Section 3, we must have $B \nsubseteq A$, i.e., $C = A \bigcap B \subsetneq B$. Suppose that $|C| = t$, $|B| = m$, then $t < m$. From Step 2.1 of Construction II, we have that for $B \in \Gamma$, there exists $\left\{\mathcal{OA}_\gamma^{(B)} \mid \gamma \in \mathbb{F}_q^*\right\}$, which is a set of $q-1$ disjoint simple arrays $OA_1(m-1, m, q-1)$. Given $\gamma \in \mathbb{F}_q^*$, every possible $(m-1)$-tuple of $\mathbb{F}_q^*$ occurs exactly one time in $\mathcal{OA}_\gamma^{(B)}$, which implies that every possible t-tuple of $\mathbb{F}_q^*$ occurs exactly $(q-1)^{m-1-t}$ times in $\mathcal{OA}_\gamma^{(B)}$. Hence, from Step 2.2 of Construction II, we have that given $\gamma \in \mathbb{F}_q^*$, for any shares $s^{(B)}(C) \in (\mathbb{F}_q^*)^t$, the conditional probability determined by f_B satisfies

$$\begin{aligned} &\Pr\left(S^{(B)}(C) = s^{(B)}(C) \mid K = \gamma\right) \\ =&\frac{(q-1)^{m-1-t}}{(q-1)^{m-1}} = \frac{1}{(q-1)^t} = \Pr\left(S^{(B)}(C) = s^{(B)}(C)\right), \end{aligned}$$

Table 3. Secret Sharing Scheme II

Initialization Phase:

1. The set of all the players is $\mathcal{P} = \{\mathrm{P}_1, \ldots, \mathrm{P}_n\}$.
2. The access structure $(\varGamma, \varDelta)$ is public.

Sharing Phase:

1. The trusted center TC chooses a q-ary function $F : \mathbb{F}_q^n \to \mathbb{F}_q$ which satisfies
(i) For $A \in \varGamma$, $F|_A$ is balanced onto $\mathbb{F}_q^*$, which is carefully chosen.
(ii) For $A \in \varDelta$, $F|_A = 0$, i.e., $F|_A$ is a zero function.
Then, TC computes the algebraic normal form of F by using Eq.(2),
$$F(x) = \sum_{u=(u_1,\ldots,u_n)\in\mathbb{Z}_q^n} a_u x_1^{u_1} \cdots x_n^{u_n},$$
and the algebraic normal form of F is public.
2. Suppose TC wants to share a secret key $k \in \mathbb{F}_q^*$. Then, for every $A = \{\mathrm{P}_{i_1}, \ldots, \mathrm{P}_{i_m}\} \in \varGamma$, TC randomly chooses
$$\begin{aligned} x^{(A)} &= \left(0, \ldots, 0, x_{i_1}^{(A)}, 0, \ldots, 0, x_{i_m}^{(A)}, 0, \ldots, 0\right) \\ &\in (F|_A)^{-1}(k) = \{x \in \mathbb{F}_q^n \mid F|_A(x) = k\}, \end{aligned}$$
and TC transmits the values $x_{i_1}^{(A)}, \ldots, x_{i_m}^{(A)}$ secretly to $\mathrm{P}_{i_1}, \ldots, \mathrm{P}_{i_m}$ respectively. Finally, for $i = 1, \ldots, n$, the player P_i receives $s(\mathrm{P}_i) = \left\{s^{(A)}(\mathrm{P}_i) = x_i^{(A)} \;\middle|\; A \in \varGamma \text{ and } \mathrm{P}_i \in A\right\}$ as his share.

Reconstruction Phase:

For any $A = \{\mathrm{P}_{i_1}, \ldots, \mathrm{P}_{i_m}\} \in 2^{\mathcal{P}}$, the players in A do as follows.

1. **Determine the recovery algorithm.**
The players in A get
$$f_A(x_{i_1}, \ldots, x_{i_m}) = F(0, \ldots, 0, x_{i_1}, 0, \ldots, 0, x_{i_m}, 0, \ldots, 0) \tag{15}$$
as their recovery algorithm.
2. **Compute the secret key.**
The players in A pool their shares and compute $f_A\left(x_{i_1}^{(A)}, \ldots, x_{i_m}^{(A)}\right)$.

which implies from Bayes' theorem that

$$\begin{aligned} &\Pr\left(K = \gamma \;\middle|\; S^{(B)}(C) = s^{(B)}(C)\right) \\ =&\frac{\Pr\left(S^{(B)}(C) = s^{(B)}(C) \;\middle|\; K = \gamma\right) \Pr(K = \gamma)}{\Pr\left(S^{(B)}(C) = s^{(B)}(C)\right)} = \Pr(K = \gamma) = \frac{1}{|\mathbf{K}|}. \end{aligned} \tag{16}$$

Table 4. Construction II

Input:	A set of players $\mathcal{P} = \{\mathrm{P}_1, \dots, \mathrm{P}_n\}$ with access structure (Γ, Δ).
Output:	A function $F : \mathbb{F}_q^n \to \mathbb{F}_q$.
Step 1:	For every subset of players $A \in \Delta$, set $F\|_A = 0$, i.e., $F\|_A$ is a zero function.
Step 2:	For every subset of players $A = \{\mathrm{P}_{i_1}, \dots, \mathrm{P}_{i_m}\} \in \Gamma$, execute the following two steps. 1. Choose a large set of orthogonal arrays $LOA_1(m-1, m, q-1)$, i.e., a set of $q-1$ disjoint simple arrays $OA_1(m-1, m, q-1)$, which is denoted by $\{\mathcal{OA}_\gamma^{(A)} \mid \gamma \in \mathbb{F}_q^*\}$. 2. For $x \in E_A$, denote by $\tilde{x}$ the vector obtained by deleting all the zero coordinates of x. Then, set $F\|_A(x) = \gamma$ if and only if $\tilde{x}$ is a row vector of $\mathcal{OA}_\gamma^{(A)}$.

Due to Eq.(16), we have that for every $k \in \mathbf{K}$, the secret key k can be guessed correctly with probability $\Pr(K = k) = 1/|\mathbf{K}|$. Therefore, from Definition 2, Secret Sharing Scheme II is perfect. □

Remark 2. We can prove that by employing q-ary function F constructed in Construction II, Secret Sharing Scheme I is perfect. In fact, let k be the secret key and $\alpha_1, \dots, \alpha_n$ be the generated shares of $\mathrm{P}_1, \dots, \mathrm{P}_n$ respectively. When we add the constraint that $\tilde{x} = (\alpha_{i_1}, \dots, \alpha_{i_m})$ is a row vector of $\mathcal{OA}_k^{(A)}$ to Step 2.2 of Construction II, then the function F satisfies $F(\boldsymbol{s}(A)) = k$ for $A \in \Gamma$. Thus, it can be proved similarly as in Theorem 3 that Secret Sharing Scheme I is perfect. By adding this constraint, the output functions in Construction II form a proper subset of all the output functions in Construction I.

5.3 Perfect Secret Sharing Schemes from Resilient Functions

For two integers n and m, the function $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is called *t-resilient* if the output value of F satisfies for any $\{i_1, \dots, i_t\} \subseteq \{1, 2, \dots, n\}$, any $z_j \in \mathbb{F}_q$, $j = 1, \dots, t$, and any $\gamma \in \mathbb{F}_q$,

$$\Pr(F(x_1, \dots, x_n) = \gamma \mid x_{i_1} = z_1, \dots, x_{i_t} = z_t) = \Pr(F(x_1, \dots, x_n) = \gamma) = \frac{1}{q^m}. \tag{17}$$

In [23], t-resilient functions from $\mathbb{F}_q^n$ to $\mathbb{F}_q^m$ are characterized in terms of orthogonal arrays. Furthermore, Camion et al. [10] claimed that this characterization holds for t-resilient functions from $\mathcal{F}^n$ to $\mathcal{F}^m$, where $\mathcal{F}$ is a finite alphabet. Inspired by Construction II in Table 4 and the close relationship between orthogonal arrays and t-resilient functions, we find a way to construct

Table 5. Construction III

```
Input:  A set of players $\mathcal{P} = \{\mathrm{P}_1, \ldots, \mathrm{P}_n\}$ with access structure $(\Gamma, \Delta)$.
Output: A function $F : \mathbb{F}_q^n \to \mathbb{F}_q$, where $q - 1$ is a power of a prime.
Step 1: Choose a one-to-one mapping $\phi : \mathbb{F}_q^* \to \mathbb{F}_{q'}$, where $q' = q - 1$.
Step 2: For every subset of players $A \in \Delta$, set $F|_A = 0$, i.e., $F|_A$ is a zero function.
Step 3: For every subset of players $A = \{\mathrm{P}_{i_1}, \ldots, \mathrm{P}_{i_m}\} \in \Gamma$, execute the following two steps.
    1. Choose an $(m, m-1, q')$ resilient function $G_A$.
    2. For $x \in E_A$, denote by $\tilde{x} = (x_{i_1}, \ldots, x_{i_m})$ the vector obtained by deleting
       all the zero coordinates of $x$. By abuse of notation, we use $\phi(\tilde{x})$ to denote
       $(\phi(x_{i_1}), \ldots, \phi(x_{i_m}))$. Then, define
           $F|_A(x) = \phi^{-1} \circ G_A \circ \phi(\tilde{x}).$   (18)
```

perfect secret sharing schemes with general access structures by employing t-resilient functions. The idea of constructing perfect secret sharing schemes by using resilient functions can be found in simplified (n, n)-threshold scheme that all the n players pool their shares and compute the secret key $k \in \mathbb{Z}_m$ ($\mathbb{Z}_m$ is the residue class ring with m elements) by the formula

$$k = \sum_{i=1}^{n} x_i \mod m,$$

where for $i = 1, \ldots, n$, $x_i \in \mathbb{Z}_m$ is the share of player P_i (see [33, Chapter 13] for more details). Note that the recovery algorithm $F(x) = \sum_{i=1}^{n} x_i \mod m$, $x = (x_1, \ldots, x_n) \in \mathbb{Z}_m^n$ is indeed an $(n-1)$-resilient function from $\mathbb{Z}_m^n$ to $\mathbb{Z}_m$. When $m = 2$, this idea appears in [21, Chapter 7] for the construction of binary (n, n)-threshold schemes. Resilient functions can also be employed as building blocks of perfect monotone secret sharing schemes from the description of monotone circuit, see [3,4].

For convenience, we denote t-resilient functions from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ by (n, t, q) resilient functions. Clearly, an (n, t, q) resilient function must be (n, t', q) resilient when $t' \leqslant t$. In Table 5, we use (n, t, q) resilient functions to construct q-ary functions. By employing such functions in Secret Sharing Scheme II, we can get perfect secret sharing schemes.

Remark 3. In Construction III, the finite field $\mathbb{F}_q$ should satisfy that $q - 1$ is a power of a prime, i.e., $q = p^s + 1$ for some prime p and positive integer s. If $q = 2^t$ for some $t \geqslant 2$, then p is odd and $p^s = 2^t - 1$. If q is odd, then p is even and $q = 2^t + 1$ for some $t \geqslant 1$. In Table 6, we give some examples of q such that $q - 1$ is a power of a prime.

Table 6. All numbers $2 < q < 2^{64}$ satisfying q is a power of a prime and $q-1$ is a power of a prime

q	$q-1$	q	$q-1$
$3 = 3^1$	$2 = 2^1$	$257 = 257^1$	$256 = 2^8$
$4 = 2^2$	$3 = 3^1$	$8192 = 2^{13}$	$8191 = 8191^1$
$5 = 5^1$	$4 = 2^2$	$65537 = 65537^1$	$65536 = 2^{16}$
$8 = 2^3$	$7 = 7^1$	$131072 = 2^{17}$	$131071 = 131071^1$
$9 = 3^2$	$8 = 2^3$	$524288 = 2^{19}$	$524287 = 524287^1$
$17 = 17^1$	$16 = 2^4$	$2147483648 = 2^{31}$	$2147483647 = 2147483647^1$
$32 = 2^5$	$31 = 31^1$	$2305843009213693952 = 2^{61}$	2305843009213693951
$128 = 2^7$	$127 = 127^1$		$= 2305843009213693951^1$

Note: a^1 means that a is a prime.

Theorem 4. *Let F be constructed by Construction III. Then, Secret Sharing Scheme II is perfect.*

Proof. For any subset of players $A = \{\mathrm{P}_{i_1}, \ldots, \mathrm{P}_{i_m}\} \in \mathit{\Gamma}$, the recovery algorithm f_A satisfies $f_A\left(x_{i_1}^{(A)}, \ldots, x_{i_m}^{(A)}\right) = F|_A\left(x^{(A)}\right) = k$, where

$$x^{(A)} = \left(0, \ldots, 0, x_{i_1}^{(A)}, 0, \ldots, 0, x_{i_m}^{(A)}, 0, \ldots, 0\right),$$

thus the qualified group A can reconstruct the secret key.

For any forbidden group $A \in \mathit{\Delta}$, we assume that the players in A are collaborating to reconstruct the secret key by using some recovery algorithm, say f_B, where $B \in \mathit{\Gamma}$. As discussed in Section 3, we must have $B \nsubseteq A$, i.e., $C = A \bigcap B \subsetneq B$. Suppose that $|C| = t$, $|B| = m$, then $t < m$. Let $x \in E_B$ with $\tilde{x} = (x_{i_1}, \ldots, x_{i_m}) \in (\mathbb{F}_q^*)^m$, where $\tilde{x}$ is the vector obtained by deleting all the zero coordinates of x. From Step 3.1 of Construction III, we have that G_B is an $(m, m-1, q')$ resilient function, where $q' = q-1$. Let $\{j_1, \ldots, j_t\} \subseteq \{i_1, \ldots, i_m\}$, then from Eq.(17), we have that for any $z_s \in \mathbb{F}_{q'}$, $s = 1, \ldots, t$, and any $\beta \in \mathbb{F}_{q'}$,

$$\begin{aligned} &\Pr(G_B \circ \phi(\tilde{x}) = \beta \mid \phi(x_{j_1}) = z_1, \ldots, \phi(x_{j_t}) = z_t) \\ =&\Pr(G_B \circ \phi(\tilde{x}) = \beta) = \frac{1}{q'} = \frac{1}{q-1}. \end{aligned} \tag{19}$$

According to Eq.(18), we get that Eq.(19) is equivalent to

$$\begin{aligned} &\Pr(F|_B(x) = \phi^{-1}(\beta) \mid x_{j_1} = \phi^{-1}(z_1), \ldots, x_{j_t} = \phi^{-1}(z_t)) \\ =&\Pr(F|_B(x) = \phi^{-1}(\beta)) = \frac{1}{q-1}. \end{aligned} \tag{20}$$

Since ϕ is a one-to-one mapping from $\mathbb{F}_q^*$ to $\mathbb{F}_{q'}$, then given the shares $s^{(B)}(C) \in (\mathbb{F}_q^*)^t$, for any $\gamma \in \mathbb{F}_q^*$, the conditional probability determined by f_B satisfies

$$\Pr\left(K = \gamma \mid S^{(B)}(C) = s^{(B)}(C)\right) = \Pr(K = \gamma) = \frac{1}{q-1} = \frac{1}{|\mathbf{K}|}, \tag{21}$$

which implies that for every $k \in \mathbf{K}$, the secret key k can be guessed correctly with probability $\Pr(K = k) = 1/|\mathbf{K}|$. Therefore, from Definition 2, we have that Secret Sharing Scheme II is perfect. □

Remark 4. It is proved in [23] that an (m, t, q) resilient function is equivalent to a large set of orthogonal arrays $LOA_{q^{m-1-t}}(t, m, q)$. In fact, in Step 3.2 of Construction III, the sets $\{\tilde{x} \in (\mathbb{F}_q^*)^m \mid F|_A(x) = \gamma, x \in E_A\}$, $\gamma \in \mathbb{F}_q^*$, consist of a large set of orthogonal arrays $LOA_1(m-1, m, q-1)$. Hence, Construction III can be seen as a special case of Construction II.

There exist a large amount of constructions of resilient functions over finite fields, e.g. see [11,12,24,37]. We remark that, generally, given the value table of a q-ary function F, it needs approximately $\mathcal{O}(nq^n)$ operations over the finite field $\mathbb{F}_q$ to compute the ANF of F. However, it will be much easier for us to derive the ANF of F by using the known ANFs of resilient functions. We illustrate this process by a simple example in Appendix B, which provides a perfect secret sharing scheme realizing a non-monotone access structure.

For Secret Sharing Scheme II, it is clear that the information rate is

$$\rho = \min \left\{ \rho_i = \frac{1}{|\{A \in \Gamma \mid \mathrm{P}_i \in A\}|} \;\middle|\; 1 \leqslant i \leqslant n \right\}, \tag{22}$$

which depends on the access structure. In the worst case, there may exist a player who joins in 2^{n-1} qualified groups, then according to Eq.(22), the information rate is $\mathcal{O}(2^{-n})$ which is much lower than the upper bound.

We emphasize that in the sharing phase of Secret Sharing Scheme I and Secret Sharing Scheme II, the computational complexity depends on the access structure, which is often exponential in the number of players for practical applications. In general, for non-monotone secret sharing schemes, it is hard to decrease the complexity of the sharing phase (excepting some special access structures).

6 Conclusion

In this paper, we discuss secret sharing schemes realizing general (not necessarily monotone) access structures. For secret sharing schemes with general access structures, the attack model and the definition of unconditional security (called perfect) given in this paper are generalizations of the monotone access structure case. Secret Sharing Scheme I presented in Table 1 is a democratic scheme such that the shares are generated by the players. We prove that if the value table of the q-ary function F is well arranged, Secret Sharing Scheme I is perfect with information rate $\rho = 1$. We propose Secret Sharing Scheme II for the sake of efficiency, which requires the trusted center TC to distribute the shares. By employing orthogonal arrays as well as resilient functions in the construction of q-ary function F, we prove that Secret Sharing Scheme II is perfect.

For any access structure, the information rate of Secret Sharing Scheme I achieves the upper bound. However, for Secret Sharing Scheme II, the information rate depends on the access structure, which will be much lower than the upper bound in the worst case. For some access structures, the size of the shares in Secret Sharing Scheme II is exponential in the number of players. As a further work, it would be very interesting to design efficient perfect secret sharing schemes with general access structures which have high information rate.

References

1. Anderson, R., Ding, C., Helleseth, T., Klve, T.: How to build robust shared control systems. *Designs, Codes Cryptography*, vol. 15, no. 2, pages 111-124, 1998.
2. Beimel, A.: Secret-sharing schemes: a survey. In: Chee, Y.M. et al. (eds.) IWCC 2011. LNCS, vol. 6639, pp. 11–46. Springer, Heidelberg (2011)
3. Benaloh, J., Leichter, J.: Generalized secret sharing and monotone functions. In: Goldwasser, S. (ed.) CRYPTO'88. LNCS, vol. 403, pp. 27–35. Springer, Heidelberg (1990)
4. Benaloh, J.: General linear secret sharing (extended abstract), `http://research.microsoft.com/pubs/68477/glss.ps`
5. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: Proceedings of the 20th annual ACM symposium on Theory of computing, pp. 1–10. ACM Press, New York (1988)
6. Blakley, G.R.: Safeguarding cryptographic keys. In: Proceedings of the National Computer Conference, pp. 313–317. AFIPS Press, New York (1979)
7. Blakley, G.R., Kabatianskii, G.A.: Linear algebra aproach to secret sharing schemes. In: Chmora, A., Wicker, S.B. (eds.) Workshop on Information Protection. LNCS, vol. 829, pp. 33–40. Springer, Heidelberg (1994)
8. Brickell, E.F.: Some ideal secret sharing schemes. In: Quisquater, J.-J., Vandewalle, J. (eds.) EUROCRYPT'89. LNCS, vol. 434, pp. 468–475. Springer, Heidelberg (1990)
9. Brickell, E.F., Stinson, D.R.: Some improved bounds on the information rate of perfect secret sharing schemes. J. Cryptol. 5(3), 153–166 (1992)
10. Camion, P., Canteaut, A.: Construction of t-resilient functions over a finite alphabet. In: Maurer, U. (ed.) EUROCRYPT'96. LNCS, vol. 1070, pp. 283–293. Springer, Heidelberg (1996)
11. Camion, P., Canteaut, A.: Correlation-immune and resilient functions over a finite alphabet and their applications in cryptography. Des. Codes Crypt. 16(2), 121–149 (1995)
12. Carlet, C.: More correlation-immune and resilient functions over Galois fields and Galois rings. In: Fumy, W. (ed.) EUROCRYPT'97. LNCS, vol. 1233, pp. 422–433. Springer, Heidelberg (1997)
13. Carlet, C., Ding, C., Yuan, J.: Linear codes from perfect nonlinear mappings and their secret sharing schemes. *IEEE Trans. Inform. Theory*, vol. 51, no.6, pages 2089-2102, 2005.
14. Carpentieri, M.: A perfect threshold secret sharing scheme to identify cheaters. Des. Codes Crypt. 5(3), 183–186 (1995)

15. Cramer, R., Damgård, I., Maurer, U.: General secure multi-party computation from any linear secret-sharing scheme. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 316–334. Springer, Heidelberg (2000)
16. Cramer, R., Damgård, I., Nielsen, J.B.: Secure Multiparty Computation and Secret Sharing: An Information Theoretic Approach. `https://users-cs.au.dk/jbn/mpc-book.pdf`
17. Cohen, G., Mesnager, S., Patey, A.: On Minimal and quasi-minimal linear codes. *Proceedings of Fourteenth International Conference on Cryptography and Coding*, Oxford, United Kingdom, IMACC 2013, LNCS 8308, pages 85-98. Springer, Heidelberg, 2013.
18. Cohen, G., Mesnager, S.: On Minimal and Almost-Minimal Linear Codes. *Proceedings of the 21st International Symposium on Mathematical Theory of Networks and Systems* (MTNS 2014), Session ”Coding theory”, pages 928-931, Groningen, Netherlands, 2014.
19. Cohen, G., Mesnager, S.: Variations on Minimal Linear Codes. *Proceedings of the 4th International Castle Meeting on coding theory and Application*Series: CIM Series in Mathematical Sciences, Vol. 3, Springer-Verlag, pages 125-131, 2015.
20. Cohen, G., Mesnager, S., Randriambololona, H.: Yet another variation on minimal linear codes. *Journal Advances in Mathematics of Communications* (AMC). To appear.
21. Ding, C., Pei, D., Salomaa, A.: Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography. World Scientific Publishing Co. Pte. Ltd., Singapore (1996)
22. Ding, K., Ding, C.: A Class of two-weight and three-weight codes and their applications in secret sharing. *IEEE Transactions on Information Theory* 61(11), pages 5835-5842, 2015.
23. Gopalakrishnan, K., Stinson, D.R.: Three characterizations of non-binary correlation-immune and resilient functions. Des. Codes Crypt. 5(3), 241–251 (1995)
24. Gupta, K.C., Sarkar, P.: Improved construction of nonlinear resilient S-boxes. IEEE Trans. Inf. Theory 51(1), 339–348 (2005)
25. Ito, M., Saito, A., Nishizeki,T.: Secret sharing schemes realizing general access structure. Electron. Comm. Jpn. Pt. III, 72(9), 56–64 (1989)
26. Karchmer, M., Wigderson, A.: On span programs. In: Proceedings of the 8th IEEE Structure in Complexity Theory, pp. 102–111. IEEE (1993)
27. Lee, C.-Y., Wang, Z.-H., Harn, L., Chang, C.-C.: Secure key transfer protocol based on secret sharing for group communications. IEICE Trans. Inf. and Syst. E94-D(11), 2069–2076 (2011)
28. Massey, J.: Minimal codewords and secret sharing. In: Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory, pp. 276–279. (1993)
29. McEliece, R.J., Sarwate, D.V.: On sharing secrets and Reed-Solomon codes. Commun. ACM 24(9), 583–584 (1981)
30. Pieprzyk, J., Zhang, X.-M.: Ideal threshold schemes from MDS codes. In: Lee, P.J., Lim, C.H. (eds.) ICISC 2002. LNCS, vol. 2587, pp. 253–263. Springer, Heidelberg (2003)
31. Pless, V., Brualdi, R.A., Huffman, W.C.: Handbook of Coding Theory. Elsevier Science Inc., New York (1998)
32. Shamir, A.: How to share a secret. Commun. ACM 22(11), 612–613 (1979)
33. Stinson, D.R.: Cryptography: Theory and Practice (third edition). CRC Press, Boca Raton (2006)

34. Stinson, D.R.: Combinatorial Designs: Construction and Analysis. Springer, New York (2004)
35. Yao, A.C.: Protocols for secure computations. In: Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, pp. 160–164. IEEE (1982)
36. Zhang, J., Li, X., Fu, F.-W.: Multi-receiver authentication scheme for multiple messages based on linear codes. In: Huang, X., Zhou, J. (eds.) ISPEC 2014. LNCS, vol. 8434, pp. 287–301. Springer, Heidelberg (2014)
37. Zhang, X.-M., Zheng, Y.: Cryptographically resilient functions. IEEE Trans. Inf. Theory 43(5), 1740–1747 (1997)

Appendix A: The Proof of Lemma 1

In this appendix, we give a full proof of Lemma 1. First we introduce a simple lemma.

Lemma 3. *For $l \geqslant 1$, the numbers n_l and N_l defined in (12) and (13) satisfy respectively,*

$$n_l = (q-2)\left(n_{l-1} + (-1)^l\right), \tag{23}$$

$$N_l = (q-2)N_{l-1} + (-1)^{l+1}. \tag{24}$$

Moreover, for $l \geqslant 1$, we have $n_l \geqslant 0$ and $N_l \geqslant 0$.

Proof. We only prove that for $l \geqslant 1$, $n_l = (q-2)\left(n_{l-1} + (-1)^l\right)$ and $n_l \geqslant 0$. The results that for $l \geqslant 1$, $N_l = (q-2)N_{l-1} + (-1)^{l+1}$ and $N_l \geqslant 0$ can be proved similarly.

Since $n_0 = 1$, then according to Eq.(12), we can compute that $n_1 = 0$, which satisfies Eq.(23). Assume that for all $1 \leqslant l \leqslant L$, Eq.(23) holds, then for $l = L+1$, we have

$$\begin{aligned} n_{L+1} = (q-1)^L - \sum_{i=0}^{L} \binom{L+1}{i} n_i &= (q-1)^L - \sum_{i=1}^{L} \left(\binom{L}{i} + \binom{L}{i-1} \right) n_i - 1 \\ &= (q-1)^L - \sum_{i=1}^{L} \binom{L}{i} n_i - 1 - \sum_{i=1}^{L} \binom{L}{i-1} n_i \\ &= (q-1)^L - \sum_{i=0}^{L} \binom{L}{i} n_i - \sum_{i=1}^{L} \binom{L}{i-1} n_i. \end{aligned} \tag{25}$$

From Eq.(12), we obtain that for $l \geqslant 1$,

$$\sum_{i=0}^{l} \binom{l}{i} n_i = (q-1)^{l-1}. \tag{26}$$

Put (26) into (25) and apply the inductive assumption, then we have

$$
\begin{aligned}
n_{L+1} &= (q-1)^L - (q-1)^{L-1} - \sum_{i=1}^{L} \binom{L}{i-1} \Big((q-2)\Big(n_{i-1} + (-1)^i\Big)\Big) \\
&= (q-2)(q-1)^{L-1} - (q-2)\sum_{i=1}^{L} \binom{L}{i-1} n_{i-1} - (q-2)\sum_{i=1}^{L} \binom{L}{i-1} (-1)^i \\
&= (q-2)\Big((q-1)^{L-1} - (q-1)^{L-1} + n_L - (-1)^L \Big) \qquad (27) \\
&= (q-2)\left(n_L + (-1)^{L+1}\right),
\end{aligned}
$$

where Eq.(27) is from Eq.(12) in the case that $l = L$. Hence, for $l = L+1$, Eq.(23) holds, which implies that for any $l \geqslant 1$, $n_l = (q-2)\left(n_{l-1} + (-1)^l\right)$.

Suppose that for any $1 \leqslant l \leqslant L$, we have $n_l \geqslant 0$, which is already true for $L = 1$. Then, since $n_{L+1} = (q-2)\left(n_L + (-1)^{L+1}\right)$, we have $n_{L+1} \geqslant 0$ if $n_L \geqslant 1$, and $n_{L+1} = (-1)^{L+1}(q-2)$ if $n_L = 0$. If $n_L = (q-2)\left(n_{L-1} + (-1)^L\right) = 0$, then since $q > 2$, we have $n_{L-1} + (-1)^L = 0$, which implies that L is odd because $n_{L-1} \geqslant 0$. Hence, if $n_L = 0$, then $n_{L+1} = (-1)^{L+1}(q-2) = q-2 \geqslant 1$. Therefore, for any $l \geqslant 1$, we have $n_l \geqslant 0$.

The proof of Lemma 1. We only need to prove that for every $x \in \mathbb{F}_q^n$, $F(x)$ can be uniquely determined. Firstly, if $x = \mathbf{0}$, then $F(x) = 0$. Suppose that $\mathrm{supp}(x) = \{i_1, \ldots, i_m\}$, where $1 \leqslant m \leqslant n$, and $1 \leqslant i_j \leqslant n$ for $j = 1, \ldots, m$. Let $A = \{\mathrm{P}_{i_1}, \ldots, \mathrm{P}_{i_m}\}$. If $A \in \varDelta$, then $F(x) = 0$. If $A \in \varGamma$ and $x = \sum_{j=1}^{m} s(\mathrm{P}_{i_j}) e_{i_j}$, then $F(x) = k$. Thanks to Proposition 1, the remaining case we need to consider is that there exists a non-empty set $B \subseteq A$ with $|B| = l$ such that $x \in E_{s(A \setminus B) \times \overline{B}}$. In the following, we will show that the value table of $F|_{s(A \setminus B) \times \overline{B}}$ can be arranged in Step 2.2 of Construction I. That is to say, we will prove that $n_l \geqslant 0$, $N_l \geqslant 0$, and

$$
n_l + (q-2)N_l = \left|E_{s(A \setminus B) \times \overline{B}}\right| = (q-2)^l. \qquad (28)
$$

The results $n_l \geqslant 0$ and $N_l \geqslant 0$ are shown in Lemma 3, so we prove Eq.(28) below.

Since $n_0 = 1$ and $N_0 = 0$, which implies that $n_1 = 0$ and $N_1 = 1$, then it can be seen that Eq.(28) holds for $l = 0$ and $l = 1$. Assume that Eq.(28) holds for all $l \leqslant L$, then for $l = L+1$,

$$\begin{aligned}
&n_{L+1} + (q-2)N_{L+1} \\
=&(q-1)^L - \sum_{i=0}^{L} \binom{L+1}{i} n_i + (q-2)\left((q-1)^L - \sum_{i=0}^{L} \binom{L+1}{i} N_i\right) \\
=&(q-1)^{L+1} - \sum_{i=0}^{L} \binom{L+1}{i} (n_i + (q-2)N_i) \\
=&(q-1)^{L+1} - \sum_{i=0}^{L} \binom{L+1}{i} (q-2)^i \qquad (29) \\
=&(q-1)^{L+1} - \left((q-1)^{L+1} - (q-2)^{L+1}\right) \\
=&(q-2)^{L+1},
\end{aligned}$$

where Eq.(29) is due to the inductive assumption. Hence, for every $l = 1, \ldots, m$, Eq.(28) holds. Therefore, for $x \in E_{s(A \setminus B) \times \overline{B}}$, the value $F|_{s(A \setminus B) \times \overline{B}}(x)$ can be uniquely determined, and we have the desired result. □

Appendix B: An Example of Secret Sharing Scheme II

We illustrate Secret Sharing Scheme II by the following example, where the q-ary function F is constructed by Construction III in Table 5.

Example 1. Let $\mathcal{P} = \{\mathrm{P}_1, \mathrm{P}_2, \mathrm{P}_3, \mathrm{P}_4\}$ and $\Gamma = \{A_1 = \{\mathrm{P}_1, \mathrm{P}_2, \mathrm{P}_3\}, A_2 = \{\mathrm{P}_1, \mathrm{P}_2, \mathrm{P}_4\}, A_3 = \{\mathrm{P}_3, \mathrm{P}_4\}, A_4 = \{\mathrm{P}_1, \mathrm{P}_2, \mathrm{P}_3, \mathrm{P}_4\}\}$. The set of secret keys is $\mathbf{K} = \mathbb{F}_8^* = \{1, \alpha, \alpha^2, \ldots, \alpha^6\}$, where α is a primitive element of $\mathbb{F}_8$. Suppose that TC wants to share $k = \alpha^5$ as the secret key. Following Construction III, TC defines $\phi : \mathbb{F}_8^* \to \mathbb{F}_7$ as $\phi(\gamma) = \log_\alpha \gamma$, which means that if $\gamma = \alpha^a \in \mathbb{F}_8^*$ for some integer a, then $\log_\alpha \gamma = a$. For the access structure Γ, TC chooses

$$\begin{cases} G_{A_1}(z_1, z_2, z_3) = 2z_1 + 3z_2 + z_3, \\ G_{A_2}(z_1, z_2, z_4) = z_1 + 2z_2 + 3z_4, \\ G_{A_3}(z_3, z_4) = 2z_3 + 4z_4, \\ G_{A_4}(z_1, z_2, z_3, z_4) = z_1 + z_2 + z_3 + z_4 + 1 \end{cases} \qquad (30)$$

as the 7-ary linear resilient functions (see [10] for more details). After that, TC computes and secretly transmits the shares

$$\begin{aligned}
s(\mathrm{P}_1) &= \{s_1^{(A_1)} = \alpha, s_1^{(A_2)} = \alpha^2, s_1^{(A_4)} = \alpha\}, \\
s(\mathrm{P}_2) &= \{s_2^{(A_1)} = \alpha^2, s_2^{(A_2)} = \alpha^3, s_2^{(A_4)} = \alpha\}, \\
s(\mathrm{P}_3) &= \{s_3^{(A_1)} = \alpha^4, s_3^{(A_3)} = \alpha, s_3^{(A_4)} = \alpha\}, \\
s(\mathrm{P}_4) &= \{s_4^{(A_2)} = \alpha^6, s_4^{(A_3)} = \alpha^6, s_1^{(A_4)} = \alpha\},
\end{aligned}$$

to P_1, P_2, P_3, P_4 respectively. From (30), the 8-ary function F is defined as

$$\begin{aligned}
F|_{A_1}(x) &= \phi^{-1} \circ G_{A_1} \circ \phi(\tilde{x}) = x_1^2 x_2^3 x_3, \\
F|_{A_2}(x) &= \phi^{-1} \circ G_{A_2} \circ \phi(\tilde{x}) = x_1 x_2^2 x_4^3, \\
F|_{A_3}(x) &= \phi^{-1} \circ G_{A_3} \circ \phi(\tilde{x}) = x_3^2 x_4^4, \\
F|_{A_4}(x) &= \phi^{-1} \circ G_{A_4} \circ \phi(\tilde{x}) = \alpha x_1 x_2 x_3 x_4,
\end{aligned}$$

where $x \in \mathbb{F}_8^4$, $\tilde{x}$ denotes the vector obtained by deleting all the zero coordinates of x, and for every forbidden group $A \in \Delta = 2^{\mathcal{P}} \setminus \Gamma$, $F|_A = 0$. Finally, TC publishes

$$\begin{aligned}
F(x) &= (1 - x_4^7) x_1^2 x_2^3 x_3 + (1 - x_3^7) x_1 x_2^2 x_4^3 + (1 - x_1^7)(1 - x_2^7) x_3^2 x_4^4 + \alpha x_1 x_2 x_3 x_4 \\
&= x_3^2 x_4^4 + x_1^2 x_2^3 x_3 + x_1 x_2^2 x_4^3 - x_1^7 x_3^2 x_4^4 - x_2^7 x_3^2 x_4^4 + \alpha x_1 x_2 x_3 x_4 - x_1^2 x_2^3 x_3 x_4^7 \\
&\quad - x_1 x_2^2 x_3^7 x_4^3 + x_1^7 x_2^7 x_3^2 x_4^4.
\end{aligned}$$

Due to Theorem 4, this secret sharing scheme is perfect. In fact, assume that the players in the forbidden group $B = \{\mathrm{P}_1, \mathrm{P}_3, \mathrm{P}_4\} \in \Delta$ are collaborating to reconstruct the secret key. Their recovery algorithm defined in (15) is $f_B(x_1, x_3, x_4) = (1 - x_1^7) x_3^2 x_4^4$, which equals 0 for any $(x_1, x_3, x_4) \in (\mathbb{F}_8^*)^3$. Suppose that they try to use the recovery algorithms

$$\begin{aligned}
f_{A_1}(x_1, x_2, x_3) = F(x_1, x_2, x_3, 0) = {} & x_1^2 x_2^3 x_3, \\
f_{A_2}(x_1, x_2, x_4) = F(x_1, x_2, 0, x_4) = {} & x_1 x_2^2 x_4^3, \\
f_{A_4}(x_1, x_2, x_3, x_4) = F(x_1, x_2, x_3, x_4) = {} & x_3^2 x_4^4 + x_1^2 x_2^3 x_3 + x_1 x_2^2 x_4^3 - x_1^7 x_3^2 x_4^4 \\
& - x_2^7 x_3^2 x_4^4 + \alpha x_1 x_2 x_3 x_4 - x_1^2 x_2^3 x_3 x_4^7 \\
& - x_1 x_2^2 x_3^7 x_4^3 + x_1^7 x_2^7 x_3^2 x_4^4,
\end{aligned}$$

which are functions defined on $(\mathbb{F}_8^*)^3$, $(\mathbb{F}_8^*)^3$, and $(\mathbb{F}_8^*)^4$ respectively. For the players P_1, P_3, and P_4, the values of $s_2^{(A_1)}$, $s_2^{(A_2)}$, and $s_2^{(A_4)}$ are unknown random values, thus according to (21), the secret key can be guessed correctly with probability $1/|\mathbf{K}|$, i.e., the players in B can learn nothing about the secret key. Similar discussion holds for other forbidden groups.

Moreover, it is clear that the information rate of this scheme is

$$\rho = \min \left\{ \frac{\log_2 |\mathbf{K}|}{\log_2 |\mathbf{S}(\mathrm{P}_i)|} \;\middle|\; 1 \leqslant i \leqslant 4 \right\} = \frac{1}{3}.$$