

Article

Some Secret Sharing Based on Hyperplanes

Guohui Wang ¹ and Yucheng Chen ^{2,*}¹ School of Mathematics and Physics, Qinghai University, Xining 810016, China; wanggh0039@126.com² School of Mathematics, Jiaying University, Meizhou 514015, China

* Correspondence: ycchen@jyu.edu.cn

Abstract

The secret sharing schemes (SSS) are widely used in secure multi-party computing and distributed computing, and the access structure is the key to constructing secret sharing schemes. In this paper, we propose a method for constructing access structures based on hyperplane combinatorial structures over finite fields. According to the given access structure, the corresponding secret sharing scheme that can identify cheaters is given. This scheme enables the secret to be correctly restored if the cheater does not exceed the threshold, and the cheating behavior can be detected and located.

Keywords: access structure; secret sharing schemes; difference sets; relative difference sets; hyperplanes

1. Introduction

The concept of secret sharing schemes (SSS) was introduced in 1979 by Shamir [1] and Blakley [2]. These schemes allow a secret to be divided into several parts, which are then distributed among participants. Only specific subsets of participants, known as qualified subsets, can reconstruct the original secret, while no information about the secret is accessible to unqualified subsets. The collection of all qualified subsets forms what is referred to as the access structure.

An SSS is considered perfect if no information about the secret is leaked to unqualified subsets. If any unqualified subset is able to obtain partial or full information about the secret, the scheme is deemed non-perfect. An SSS is classified as linear if the shares are generated through a linear transformation, and it is ideal if the size of each share is exactly equal to that of the secret.

The study of secret sharing schemes remains a vital area of modern cryptography, serving as a foundational element in the development of security protocols and encryption algorithms. The ideal linear SSS has promising applications in various cryptographic protocols, including secure multi-party computation [3–7], attribute-based encryption [8], digital signatures [9], and threshold cryptography [10]. Consequently, efficient methods for constructing an ideal linear SSS are a crucial area of research.

It has been established that there is a one-to-one correspondence between linear codes and SSS [11], with linear codes being a crucial tool for realizing linear secret sharing schemes. In theory, every linear code can be utilized to create an SSS, but identifying the corresponding access structure for a given scheme remains a challenging task. Conversely, it is equally difficult to find an ideal secret sharing scheme for any arbitrary access structure. Researchers have explored various access structures and derived conclusions about the ideal secret sharing schemes that correspond to them.



Academic Editor: Demos T. Tsahalidis

Received: 28 May 2025

Revised: 25 June 2025

Accepted: 6 July 2025

Published: 10 July 2025

Citation: Wang, G.; Chen, Y. Some Secret Sharing Based on Hyperplanes. *Computation* **2025**, *13*, 166.
<https://doi.org/10.3390/computation13070166>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

In 1981, McEliece and Sarwate [12] made significant contributions to the study of SSSs based on linear codes, constructing a threshold scheme using Reed-Solomon codes and highlighting the equivalence between Shamir's SSS and Reed-Solomon codes. Massey [13] noted that the primary challenge in using linear codes to construct SSSs is characterizing the types of access structures that can be achieved. Ito et al. [14] demonstrated that it is possible to construct linear secret sharing schemes for arbitrary access structures, although these schemes are inefficient, as the length of the key increases exponentially with the number of participants. In 2013, Tang et al. [15] showed that achieving an optimal linear code for a given access structure is equivalent to solving a quadratic system of equations formed by the access structure and its corresponding adversary structure. They also developed an algorithm to determine the optimal linear code. More recently, Harn et al. [16] introduced a general secret sharing scheme based on classical schemes and presented methods for using Karnaugh maps to identify minimal access structures and maximal adversary structures for a given access structure.

Despite these advancements, numerous challenges remain in relation to secret sharing schemes for given access structures. In this paper, we build on existing research and propose a method for constructing the corresponding access structure using difference sets and relative difference sets generated by hyperplanes. For these access structures, we employ polynomial codes to create ideal linear secret sharing schemes that can detect participants exhibiting deceptive behavior.

The structure of this paper is as follows. Section 2 presents a review of the notations and fundamental results related to difference sets. In Section 3, we introduce various families of access structures derived from the combinatorial properties of hyperplanes. Section 4 utilizes these access structures to design several secret sharing schemes. Finally, Section 5 provides a conclusion to the paper.

2. Preliminaries

2.1. Difference Sets

A k -element subset D of a group G is called a (v, k, λ) -difference set if the multiset

$$\Delta(D) = \{g_1 g_2^{-1} \mid g_1, g_2 \in D, g_1 \neq g_2\}$$

contains every nonidentity element of G exactly λ times, where G be a finite multiplicative group of order v . From a counting perspective, the parameters (v, k, λ) of a difference set satisfy the relation $k(k-1) = \lambda(v-1)$. We assume $k \leq v/2$ because if D is a (v, k, λ) -difference set, then its complement $G \setminus D$ forms a $(v, v-k, v-2k+\lambda)$ -difference set in G . Typically, the trivial cases $k=0$ and $k=1$ are excluded.

Difference sets are significant in both theoretical and practical applications. In design theory, the concept of a (v, k, λ) -difference set in G is equivalent to the symmetric (v, k, λ) -design in G [17].

2.2. Relative Difference Sets

A k -element subset R of a group G that includes a normal subgroup U of order u is called a (m, u, k, λ) relative difference set (RDS) in G relative to U if the multiset

$$\Delta(R) = \{g_1 g_2^{-1} \mid g_1, g_2 \in R, g_1 \neq g_2\}$$

contains every element of $G \setminus U$ exactly λ times, and does not include any element from U , where G be a finite multiplicative group of order mu . The subgroup U is referred to as the forbidden subgroup.

An (m, u, k, λ) RDS in G relative to a normal subgroup U is equivalent to a square-divisible (m, u, k, λ) -design, where the group G acts regularly on both points and blocks [18].

From a counting perspective, the parameters (m, u, k, λ) of an RDS satisfy the relation $k(k-1) = u\lambda(m-1)$. If $k = u\lambda$, the RDS is termed semi-regular, and its parameters are $(u\lambda, u, u\lambda, \lambda)$. Unlike difference sets, the complement $G \setminus R$ of an RDS is generally not an RDS. The trivial cases where $k = 0$ and $k = 1$ are typically excluded. A difference set can be seen as an RDS where $u = 1$.

2.3. Group Ring

Difference sets are often analyzed within the framework of the group ring $\mathbb{Z}[G]$, which is the group ring of G over the integers $\mathbb{Z}$. The definition of a (v, k, λ) -difference set D in G can be expressed by the following equation in $\mathbb{Z}[G]$:

$$DD^{(-1)} = (k - \lambda) \cdot 1_G + \lambda G$$

Here, for convenience, we identify the sets D , $D^{(-1)}$, and G with the corresponding group ring elements:

$$D = \sum_{g \in D} g, \quad D^{(-1)} = \sum_{g \in D} g^{-1}, \quad G = \sum_{g \in G} g,$$

and 1_G denotes the identity element of G .

Similarly, the definition of a (m, u, k, λ) relative difference set (RDS) R in G relative to a normal subgroup U is equivalent to the equation:

$$RR^{(-1)} = k \cdot 1_G + \lambda(G - U)$$

in the group ring $\mathbb{Z}[G]$.

2.4. Characters

In the case of an abelian group, a character of G is a homomorphism from G to the multiplicative group of complex roots of unity. The set of all such characters, denoted by $\hat{G}$, forms a group under pointwise multiplication, and this group is isomorphic to G . The identity element in this group is the trivial character, which maps every element of G to 1. The character sum of a character χ over a group ring element D corresponding to a subset of G is given by:

$$\chi(D) = \sum_{g \in D} \chi(g).$$

It is a well-established result that the character sum $\chi(D)$ equals 0 for all nontrivial characters χ of G if and only if D is a multiple of G , when considered as a group ring element. Additionally, the sum

$$\sum_{\chi \in \hat{G}} \chi(g)$$

is nonzero if and only if $g = 1_G$.

If a character χ is nontrivial on G but trivial on a subgroup U , it induces a nontrivial character ψ on the quotient group G/U , defined by $\psi(gU) = \chi(g)$. This definition is well-defined because if $g_1U = g_2U$, then there exists an element $u \in U$ such that $g_1 = ug_2$, and since $\chi(u) = 1$ for all $u \in U$, the value of ψ does not depend on the choice of representative.

The application of character sums to investigate difference sets in abelian groups was first introduced by Turyn in his groundbreaking work [19], and later this approach was expanded to generalized difference sets (RDSs).

Lemma 1 ([19]). (i) A subset D of size k in an abelian group G of order v is a (v, k, λ) -difference set in G if and only if for every nontrivial character χ of G , we have $|\chi(D)| = \sqrt{k - \lambda}$.

(ii) A subset R of size k in an abelian group G of order μ , which contains a subgroup U of order u , is a (m, u, k, λ) -RDS in G relative to U if and only if for every nontrivial character χ of G , the following conditions hold:

$$|\chi(R)| = \begin{cases} \sqrt{k} & \text{if } \chi \text{ is nontrivial on } U, \\ \sqrt{k - u\lambda} & \text{if } \chi \text{ is trivial on } U. \end{cases}$$

The character properties specified in Lemma 1 for a subset D or R necessitate that the parameters $k - \lambda$ and λ (which are implicitly defined) must be integers.

3. Access Structures

3.1. Access Structures from Difference Sets

Let $\mathbb{F}_q$ be a finite field of order q , where q is a prime power.

Lemma 2. Let $\mathbb{F}_q^{s+1}$ be a vector space of dimension $s + 1$ over $\mathbb{F}_q$, where s be a positive integer. There are

$$h = \begin{bmatrix} s+1 \\ s \end{bmatrix}_q = \begin{bmatrix} s+1 \\ 1 \end{bmatrix}_q = \frac{q^{s+1} - 1}{q - 1}$$

subspaces

$$H_0, H_1, \dots, H_{h-1}$$

of $\mathbb{F}_q^{s+1}$ of dimension s , called hyperplanes. Let $\mathbb{F}_{q^{s+1}}$ be the additive group of $\mathbb{F}_q^{s+1}$ and consider $H_0, H_1, \dots, H_{h-1}$ as subgroups of $\mathbb{F}_{q^{s+1}}$. Let G be an arbitrary abelian group containing $\mathbb{F}_{q^{s+1}}$ as a central subgroup of index $h + 1$, and let

$$\{g_0, g_1, \dots, g_{h-1}\}$$

be coset representatives of $\mathbb{F}_{q^{s+1}}$ in G . Then

$$D = \sum_{i=0}^{h-1} g_i H_i$$

is a McFarland difference set [20] in G , i.e.,

$$(v, k, \lambda) = (q^{s+1}(\frac{q^{s+1} - 1}{q - 1} + 1), q^s(\frac{q^{s+1} - 1}{q - 1}), q^s(\frac{q^s - 1}{q - 1})).$$

Proof. The difference set is comprised of $h + 1$ subsets of $\mathbb{F}_{q^{s+1}}$, namely the hyperplanes together with the empty set.

$$\begin{aligned}
 DD^{(-1)} &= \sum_{i,j=0}^{h-1} g_i H_i H_j g_j^{-1}, \\
 &= q^s \sum_{i=0}^{h-1} g_i H_i g_i^{-1} + q^{s-1} \sum_{i,j=0}^{h-1} g_i g_j^{-1} \cdot \mathbb{F}_{q^{s+1}}. \\
 &= q^s \sum_{i=0}^{h-1} g_i H_i g_i^{-1} + (h-1)(G - \mathbb{F}_{q^{s+1}}) \\
 &= q^s (h \cdot 1_{\mathbb{F}_{q^{s+1}}} + \frac{q^s - 1}{q - 1} \cdot \mathbb{F}_{q^{s+1}}^*) + (h-1)(G - \mathbb{F}_{q^{s+1}})
 \end{aligned}$$

Let χ be a nontrivial character of G and consider the character sum

$$\begin{aligned}
 \chi(D) &= \sum_{i=0}^{h-1} \chi(g_i) \chi(H_i), \\
 \chi(DD^{(-1)}) &= |\chi(D)|^2.
 \end{aligned}$$

(1) χ is nontrivial on $\mathbb{F}_{q^{s+1}}$ and nontrivial on G ;

$$|\chi(D)| = \sqrt{\chi(DD^{(-1)})} = \sqrt{k - \lambda} = q^s.$$

(2) χ is trivial on $\mathbb{F}_{q^{s+1}}$ and nontrivial on G ;

$$|\chi(D)| = q^s.$$

From the above description, it is easy to judge from lemma 1(i) that such a construction produces a difference set.

Let

$$\mathcal{B} = \{B_a = D + a \mid a \in G\},$$

it is easy to know that the number of blocks in $\mathcal{B}$ is $|G| = v$, and $|B_a| = |D| = k$. In fact,

$$\begin{aligned}
 &\sharp\{a \in G : g'_1 \in D + a, g'_2 \in D + a\} \\
 &= \sharp\{a \in G : g'_1 - a \in D, g'_2 - a \in D\} \\
 &= \sharp\{(x, y) : x, y \in D, x - y = g'_1 - g'_2 (\neq 0)\} (\text{take } x = g'_1 - a, y = g'_2 - a) \\
 &= \lambda.
 \end{aligned}$$

It follows that $\mathcal{B}$ is a symmetric 2 -(v, k, λ) design on G . $\square$

3.2. Access Structures from Semi-Regular Relative Difference Sets

Based on the properties of the above difference set, there is the following construction of semi-regular RDSs.

Lemma 3. Let $\mathbb{F}_q^{s+1}$ be a vector space of dimension $s + 1$ over $\mathbb{F}_q$, where s be a positive integer. There are

$$h = \frac{q^{s+1} - 1}{q - 1}$$

subspaces

$$H_0, H_1, \dots, H_{h-1}$$

of $\mathbb{F}_q^{s+1}$ of dimension s , called hyperplanes. Let G be an arbitrary abelian group containing $\mathbb{F}_{q^{s+1}}$ as a central subgroup of index $h - 1$, and let

$$\{g_1, g_2, \dots, g_{h-1}\}$$

be coset representatives of $\mathbb{F}_{q^{s+1}}$ in G . Then

$$R = \sum_{i=1}^{h-1} g_i H_i$$

is a semi-regular RDS in G relative to H_0 , i.e.,

$$\begin{aligned} & (u\lambda, u, u\lambda, \lambda) \\ &= ((\frac{q^{s+1}-1}{q-1} - 1)^2, \frac{q^{s+1}-1}{q-1} - 1, (\frac{q^{s+1}-1}{q-1} - 1)^2, \frac{q^{s+1}-1}{q-1} - 1). \end{aligned}$$

Proof. The RDS is comprised of $h - 1$ subsets of $\mathbb{F}_{q^{s+1}}$, namely $h - 1$ of the h hyperplanes.

(1) If a nontrivial character χ of $\mathbb{F}_{q^{s+1}}$ is trivial on H_0 then each subset provides a contribution to the character sum modulus of 0,

(2) If a nontrivial character χ of $\mathbb{F}_{q^{s+1}}$ is nontrivial on H_0 then one subset contributes $\sqrt{k}$ and the rest contribute 0.

This gives the required character sum modulus for characters of G which are nontrivial on $\mathbb{F}_{q^{s+1}}$. For nontrivial characters of G which are trivial on $\mathbb{F}_{q^{s+1}}$, the required character sum modulus of 0 is again a consequence of the subset sizes.

From the above description, it is easy to judge from lemma 1(ii) that such a construction produces a RDS.

Let

$$\mathcal{B} = \{B_a = R + a \mid a \in G\}.$$

it is easy to know that the number of blocks in $\mathcal{B}$ is $|G| = u^2\lambda$, and $|B_a| = |R| = k = u\lambda$.

It follows that $\mathcal{B}$ is a symmetric $2-(u^2\lambda, k, \lambda)$ design on G . $\square$

4. Secret Sharing Scheme

4.1. Shamir Threshold Secret Sharing Scheme

Shamir threshold secret sharing scheme is mainly constructed by interpolation polynomial, and has one-to-one correspondence with RS code. (k, n) threshold scheme is simple and satisfies linearity, so it is widely used.

Next, let's briefly review the Shamir threshold secret sharing scheme

Shamir (k, n) -threshold scheme

Let $s \in \mathbb{F}_q$ be the main key, and there is a set $\{p_1, p_2, \dots, p_n\}$ of n participants, where $n \leq q$.

(1) Key distribution:

i. The key management center D secretly selects (uniformly and randomly) $k - 1$ elements $\{a_1, a_2, \dots, a_{k-1}\}$ in $\mathbb{F}_q$ and takes a polynomial in x as a variable

$$f(x) = s + a_1x + \dots + a_{k-1}x^{k-1}.$$

ii. D selects n different non-zero elements $x_1, x_2, \dots, x_n$ in $\mathbb{F}_q$ and calculates the following

$$y_i = f(x_i).$$

iii. D secretly distributes (x_i, y_i) to participant p_i .

(2) main key reconstruction:

Without losing generality, suppose that the participant set $\{p_1, p_2, \dots, p_k\}$ wants to reconstruct the main key s . Thus, they have a total of k point pairs:

$$(x_1, y_1), (x_2, y_2), \dots, (x_k, y_k).$$

Then, using the Lagrange interpolation formula,

$$f(x) = \sum_{j=1}^k y_j \prod_{1 \leq l \leq k, l \neq j} \frac{x - x_l}{x_j - x_l}.$$

This allows them to calculate the main key:

$$s = f(0) = \sum_{j=1}^k y_j \prod_{1 \leq l \leq k, l \neq j} \frac{x_l}{x_j - x_l}.$$

Therefore, any k or more participants together can reconstruct the main key s , while less than k participants can get no information about s .

This is a method to recover the main key based on linear equations. For any k subkey, without loss of generality, denoted (x_i, y_i) , where $y_i = f(x_i)$, $i = 1, \dots, k$. These k participants are able to obtain the following equations based on their mastery of the subkey set $\{(x_1, y_1), \dots, (x_k, y_k)\}$:

$$\begin{aligned} y_1 &= f(x_1) = s + a_1 x_1 + \dots + a_{k-1} x_1^{k-1}, \\ y_2 &= f(x_2) = s + a_1 x_2 + \dots + a_{k-1} x_2^{k-1}, \\ y_3 &= f(x_3) = s + a_1 x_3 + \dots + a_{k-1} x_3^{k-1}, \\ &\dots \\ y_k &= f(x_k) = s + a_1 x_k + \dots + a_{k-1} x_k^{k-1}, \end{aligned}$$

which is equivalent to

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{k-1} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & x_{k-1} & x_{k-1}^2 & \dots & x_{k-1}^{k-1} \\ 1 & x_k & x_k^2 & \dots & x_k^{k-1} \end{pmatrix} \cdot \begin{pmatrix} s \\ a_1 \\ \vdots \\ a_{k-2} \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{k-1} \\ y_k \end{pmatrix}.$$

The above coefficient matrix has rank k , and its corresponding transpose matrix is a Vandermonde matrix,

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_k \\ \vdots & \vdots & \dots & \vdots \\ x_1^{k-2} & x_2^{k-2} & \dots & x_k^{k-2} \\ x_1^{k-1} & x_2^{k-1} & \dots & x_k^{k-1} \end{pmatrix}.$$

Therefore, the unique solution $s, a_1, \dots, a_{k-1}$ of the equations containing k unknowns and k equations can be solved, so that the main key s can be recovered.

4.2. Construction of Secret Sharing Scheme Based on Given Access Structure

Let $\alpha_1, \dots, \alpha_n$ be n distinct elements of $\mathbb{F}_q$, where $1 < n \leq q$. For $1 \leq k \leq n$, the RS codes for vector $\alpha = (\alpha_1, \dots, \alpha_n) \in (\mathbb{F}_q)^n$ is

$$RS_k(\alpha) := \{(f(\alpha_1), \dots, f(\alpha_n)) \mid f(x) \in \mathbb{F}_q[x], \deg f(x) \leq k-1\}.$$

It is easy to know that $RS_k(\alpha)$ is a $[n, k, n-k+1]_q$ -linear MDS code, and its corresponding dual code is also an MDS code.

In fact, the generator matrix for $RS_k(\alpha)$ is

$$G_k(\alpha) = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \dots & \vdots \\ \alpha_1^{k-2} & \alpha_2^{k-2} & \dots & \alpha_n^{k-2} \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_n^{k-1} \end{pmatrix}.$$

In fact, the coefficient matrix of the threshold secret sharing scheme (after transposing) and the generator matrix of RS codes (the matrix composed of any k columns) are one-to-one corresponding.

Now, based on RS codes, we consider how to prevent some participants from cheating in the Shamir secret sharing scheme given the access structure.

Imagine l participants join forces, and m of them come up with forged subkeys. Can l participants find that any participant is cheating after joining forces? Furthermore, can they find out all m cheaters, point out the true subkeys of these cheaters, and work out the main keys?

Based on the access structure given in Section 3, the following results solve the above problems.

Theorem 1. Consider a Shamir secret sharing scheme with a threshold of $k = q^s(\frac{q^{s+1}-1}{q-1})$ on G , where there are n participants, $2 < k < n < |G| = q^{s+1}(\frac{q^{s+1}-1}{q-1} + 1)$.

When $l > k$, any l participants join forces, and if there are no more than $l-k$ cheaters, the l participants can detect someone cheating. If there are no more than $\frac{l-k}{2}$ cheaters, the l participants can identify all the cheaters, indicate the true subkeys of these cheaters, and calculate the main key.

Proof. Let the l participants joining forces be $A_{i_1}, A_{i_2}, \dots, A_{i_l}$, where $1 \leq i_1 < i_2 < \dots < i_l \leq n$. Consider the RS codes

$$\mathcal{C} = \{c_f = (f(x_{i_1}), \dots, f(x_{i_l})) \mid f(x) \in \mathbb{F}_{q^{s+1}}[x], \deg f(x) \leq k-1\}.$$

Since linear code $\mathcal{C}$ is an MDS code with code length l and dimension k , the minimum distance of $\mathcal{C}$ is $d = l - k + 1$.

The key control center makes G and x_i ($1 \leq i \leq n$) public, so after players $A_{i_1}, A_{i_2}, \dots, A_{i_l}$ joins forces, their $x_{i_1}, x_{i_2}, \dots, x_{i_l}$ is known. In addition, the code $\mathcal{C}$ is known to l participants after l participants join forces.

Now let the control center adopt polynomial $h(x) \in \mathbb{F}_{q^{s+1}}[x]$ ($\deg h(x) \leq k - 1$), then the main key is $h(0)$, and $c = (h(x_{i_1}), \dots, h(x_{i_l}))$ is the codeword in $\mathcal{C}$, where $h(x_{i_j})$ is the subkey of players $h(x_{i_j})$ ($1 \leq j \leq l$).

If the l players join forces, $A_{i_1}, A_{i_2}, \dots, A_{i_l}$ each shows that their subkey is $b_1, b_2, \dots, b_l$, but m or less of them are forged. In other words, the Hamming distance between code word c and vector $b = (b_1, b_2, \dots, b_l)$ is less than or equal to m . According to error-correcting code theory, when $m \leq d - 1 = l - k$, it can be determined by the vector b whether there is a participant cheating. When vector b is a codeword in $\mathcal{C}$, there is no cheating, otherwise someone will be found cheating. Furthermore, if $m \leq \frac{d-1}{2} = \frac{l-k}{2}$, code $\mathcal{C}$ can correct the error of $\leq \frac{l-k}{2}$, so the codeword c can be recovered from vector b , all participants A_{i_j} of $b_j \neq h(x_{i_j})$ are cheaters, and the true subkey of A_{i_j} should be $h(x_{i_j})$. Since $l > t$, the main key $h(0)$ can be calculated by randomly taking t of these l players together with their real subkeys. $\square$

Example 1. Let $q = 3$, $s = 1$, then we can know that $|G| = q^{s+1}(\frac{q^{s+1}-1}{q-1} + 1) = 45$, $k = q^s(\frac{q^{s+1}-1}{q-1}) = 12$. Let $n = 18$, take $\{x_1, x_2, \dots, x_{18}\} = \{1, 2, \dots, 18\}$.

The key control center exposes $q = 3$ and $\{x_1, x_2, \dots, x_{18}\}$ of 18 participants $A_1, A_2, \dots, A_{18}$, and takes $h(x) \in \mathbb{F}_9[x]$ ($\deg h(x) \leq 11$) to calculate

$$(h(1), \dots, h(18))$$

The control center sends the subkey $(h(1), \dots, h(18))$ to participants $A_1, A_2, \dots, A_{18}$ respectively, and the main key is $h(0)$. But the polynomial $h(x)$ is kept secret from any participants.

Now let $l = 15$ players

$$A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8, A_9, A_{10}, A_{11}, A_{12}, A_{13}, A_{14}, A_{15}$$

join forces, they each show their own key, A_2 forged the fake sub-key. Since $m = 1 \leq \frac{l-k}{2}$, the deceiver can be identified based on the 15 players. The method is to consider RS code

$$\mathcal{C} = \{c_f = (f(1), f(2), f(3), f(4), f(5), f(6), f(7), f(8), f(9), f(10), f(11), f(12), f(13), f(14), f(15)) \mid f(x) \in \mathbb{F}_9[x], \deg f(x) \leq 11\}.$$

The code length of the RS is $l = 15$, the dimension is $k = 12$, and the minimum distance is $d = l - k + 1 = 4$, which can correct 1 error. The subkey presented by 15 players together gives vector b , which is 1 position different from the codeword c in the code $\mathcal{C}$, so the codeword c can be recovered from b by the RS code $\mathcal{C}$. After the subkey of the deceiver is recovered, the main key can be calculated according to the formula.

Based on the access structure given by semi-regular RDSs in Section 3, the following secret sharing scheme is given.

Theorem 2. Consider a Shamir secret sharing scheme with a threshold of $k = (\frac{q^{s+1}-1}{q-1} - 1)^2$ on G , where there are n participants, $2 < k < n < |G| = (\frac{q^{s+1}-1}{q-1} - 1)^3$.

When $l > k$, any l participants join forces, and if there are no more than $l - k$ cheaters, the l participants can detect someone cheating. If there are no more than $\frac{l-k}{2}$ cheaters, the l participants can identify all the cheaters, indicate the true subkeys of these cheaters, and calculate the main key.

Proof. The proof is similar to the proof of Theorem 1, which is omitted here. $\square$

Remark 1. For reference, we list some known constructions of perfect ideal linear schemes and our new constructions in Table 1. It should be emphasized that we mainly use difference sets to construct the corresponding access structures, which is different from other literature in Table 1 using codes to construct the access structures. In addition, it is easy to see from Table 1 that for a given access structure with field size, we give two effective explicit constructs of perfect ideal linear secret sharing schemes. Under some conditions, the scope of our field size is larger, which can make the secret sharing schemes with more participants exist, therefore, our schemes have greater potential practical value. In addition, the scheme we constructed involves fewer application levels, which is also our next research task.

Table 1. Some known classes of perfect ideal linear secret sharing schemes with field size.

Field Size	Explicit Constructions	References
$\eta_1 \binom{n+1}{k}$	No	[21]
$\binom{n+1}{k}$	No	[22]
$n_0^{ r +1}$	Yes	[23]
$(\max\{n_0, r + 1\})^{T_1+1}$	Yes	[24]
$\binom{n}{k}$	No	[25]
$(1 + n_0)^{ r - t +1}$	Yes	[23]
$(1 + \max\{n_0, r - t \})^{T_2}$	Yes	[24]
$q^{s+1}(\frac{q^{s+1}-1}{q-1} + 1)$.	Yes	[Theorem 1]
$(\frac{q^{s+1}-1}{q-1} - 1)^3$.	Yes	[Theorem 2]

5. Conclusions

In this paper, we introduce a method for constructing access structures derived from hyperplane combinatorial structures over finite fields. For a given access structure, we present a corresponding secret sharing scheme designed to detect and identify cheaters. This scheme ensures that the secret can be accurately reconstructed as long as the number of cheaters does not surpass a predefined threshold, while also allowing for the detection and localization of any cheating activity.

Author Contributions: The idea of the manuscript was proposed by G.W. The main body of the manuscript was jointly written by G.W. and Y.C.; and Y.C. was also responsible for verifying the conclusion. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by The Talented Research Start-up Project of Jiaying University (No. 2022RC02) (Yucheng Chen); The 2024 Qinghai Province “Kunlun Talent-High-End Innovative and Entrepreneurial Talent” Cultivation Category Top-notch Talent Project (No. QHKLYC-GDCXCX-2024-216) (Guohui Wang).

Data Availability Statement: We did not cite any other data. All the data used are in the manuscript.

Acknowledgments: We are grateful to the anonymous referees for useful comments and suggestions that improved the presentation and quality of this paper.

Conflicts of Interest: The authors declare no conflicts of interest.

References

- Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [\[CrossRef\]](#)
- Blakley, G.R. Safeguarding cryptographic keys. In Proceedings of the International Workshop on Managing Requirements Knowledge, New York, NY, USA, 4–7 June 1979; p. 313.
- Ben-Or, M.; Goldwasser, S.; Wigderson, A. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*; Association for Computing Machinery: New York, NY, USA, 2019; pp. 351–371.
- Chaum, D.; Crépeau, C.; Damgård, I. Multiparty unconditionally secure protocols. In Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, Chicago, IL, USA, 2–4 May 1988; pp. 11–19.
- Cramer, R.; Damgård, I.; Maurer, U. General secure multi-party computation from any linear secret-sharing scheme. In *Advances in Cryptology—EUROCRYPT 2000, Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Bruges, Belgium, 14–18 May 2000*; Springer: Berlin/Heidelberg, Germany, 2000; pp. 316–334.
- Cramer, R.; Daza, V.; Gracia, I.; Urroz, J.J.; Leander, G.; Martí-Farré, J.; Padró, C. On codes, matroids, and secure multiparty computation from linear secret-sharing schemes. *IEEE Trans. Inf. Theory* **2008**, *54*, 2644–2657. [\[CrossRef\]](#)
- Wang, Z.; Cheung, S.C.; Luo, Y. Information-theoretic secure multi-party computation with collusion deterrence. *IEEE Trans. Inf. Forensics Secur.* **2016**, *12*, 980–995. [\[CrossRef\]](#)
- Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 30 October–3 November 2006; pp. 89–98.
- Naor, M.; Wool, A. Access control and signatures via quorum secret sharing. In Proceedings of the 3rd ACM Conference on Computer and Communications Security, New Delhi, India, 14–15 March 1996; pp. 157–168.
- Desmedt, Y. Threshold cryptosystems. In *Advances in Cryptology—AUSCRYPT’92, Proceedings of the International Workshop on the Theory and Application of Cryptographic Techniques, Gold Coast, QLD, Australia, 13–16 December 1992*; Springer: Berlin/Heidelberg, Germany, 1993; pp. 1–14.
- Karchmer, M.; Wigderson, A. On span programs. In Proceedings of the Eighth Annual Structure in Complexity Theory Conference, San Diego, CA, USA, 18–21 May 1993; pp. 102–111.
- McEliece, R.J.; Sarwate, D.V. On sharing secrets and Reed-Solomon codes. *Commun. ACM* **1981**, *24*, 583–584. [\[CrossRef\]](#)
- Massey, J.L. Minimal codewords and secret sharing. In Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory, Mölle, Sweden, 22–27 August 1993; pp. 276–279.
- Ito, M.; Saito, A.; Nishizeki, T. Secret sharing scheme realizing general access structure. *Electron. Commun. Jpn. (Part III Fundam. Electron. Sci.)* **1989**, *72*, 56–64. [\[CrossRef\]](#)
- Tang, C.; Gao, S.; Zhang, C. The optimal linear secret sharing scheme for any given access structure. *J. Syst. Sci. Complex.* **2013**, *26*, 634–649. [\[CrossRef\]](#)
- Harn, L.; Hsu, C.; Zhang, M.; He, T.; Zhang, M. Realizing secret sharing with general access structure. *Inf. Sci.* **2016**, *367*, 209–220. [\[CrossRef\]](#)
- Ma, S.L.; Schmidt, B. Difference sets corresponding to a class of symmetric designs. *Des. Codes Cryptogr.* **1997**, *10*, 223–236. [\[CrossRef\]](#)
- Jungnickel, D. On automorphism groups of divisible designs. *Can. J. Math.* **1982**, *34*, 257–297. [\[CrossRef\]](#)
- Turyn, R. Character sums and difference sets. *Pac. J. Math.* **1965**, *15*, 319–346. [\[CrossRef\]](#)
- McFarl, R.L. A family of difference sets in non-cyclic groups. *J. Comb. Theory Ser. A* **1973**, *15*, 1–10. [\[CrossRef\]](#)
- Tassa, T.; Dyn, N. Multipartite secret sharing by bivariate interpolation. *J. Cryptol.* **2009**, *22*, 227–258. [\[CrossRef\]](#)
- Farras, O.; Padró, C.; Xing, C.; Yang, A. Natural generalizations of threshold secret sharing. *IEEE Trans. Inf. Theory* **2014**, *60*, 1652–1664. [\[CrossRef\]](#)
- Chen, Q.; Tang, C.; Lin, Z. Efficient explicit constructions of compartmented secret sharing schemes. *Des. Codes Cryptogr.* **2019**, *87*, 2913–2940. [\[CrossRef\]](#)
- Chen, Q.; Tang, C.; Lin, Z. Efficient explicit constructions of multipartite secret sharing schemes. *IEEE Trans. Inf. Theory* **2021**, *68*, 601–631. [\[CrossRef\]](#)
- Brickell, E.F. Some ideal secret sharing schemes. In *Advances in Cryptology—EUROCRYPT’89, Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Houthalen, Belgium, 10–13 April 1989*; Springer: Berlin/Heidelberg, Germany, 1990; pp. 468–475.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.