2-threshold Ideal Secret Sharing Schemes Can Be Uniquely Modeled by Latin Squares*

Lintao Liu[1], Xuehu Yan[1]✉, Yuliang Lu[1], and Huaixi Wang[1]

National University of Defense Technology, Hefei 230027, P. R. China
liuta1989@163.com, publictiger@126.com, publicLuYL@126.com,
permutation@163.com

Abstract. In a secret sharing scheme, a secret value is encrypted into several shares, which are distributed among corresponding participants. It requires that only predefined subsets of participants can reconstruct the secret with their shares. The general model for secret sharing schemes is provided in different forms, in order to study the essential properties of secret sharing schemes. Considering that it is difficult to directly construct secret sharing schemes meeting the requirements of the general model, most of current theoretic researches always rely on other mathematical tools, such as matriod. However, these models can only handle with values in a finite field. In this paper, we firstly establish a one-to-one mapping relationship between Latin squares and 2-threshold secret sharing schemes. Afterwards, we utilize properties of Latin squares to further give an exact characterization for the general model of 2-threshold ideal secret sharing schemes. Furthermore, several interesting properties of 2-threshold ideal schemes are provided, which are not induced by any other means, especially nolinear schemes in an arbitrary integer domain.

Keywords: Ideal secret sharing · 2-threshold secret sharing · Latin square · Mutually orthogonal Latin squares.

1 Introduction

A secret sharing scheme consists of a dealer $\mathcal{D}$, a finite set of t participants P and a collection $\Gamma \in 2^P$ of subsets of these participants called the access structure. In a secret sharing scheme for Γ, $\mathcal{D}$ encrypts the secret taken from a finite domain $\mathcal{K}$, denoted by $\alpha \in \mathcal{K}$ into shares and distributes shares to the participants. In the meanwhile, these shares must satisfy two conditions: a) any subset in Γ can reconstruct α from its shares; b) any subset in $2^P - \Gamma$ cannot reveal any information of α in the information-theoretic sense. Schemes which strictly obey both conditions are further named as *perfect* secret sharing schemes, and all secret sharing schemes we talk in this paper are *perfect* by default. The first introduced access structure, proposed by Blakley [3] and Shamir [14] independently, is a special case, namely threshold access structure. Γ in k-threshold access structure

* Supported by the National Natural Science Foundation of China (Grant Number: 61602491).

is all the subsets whose cardinality is at least a certain threshold k, denoted by $\mathit{\Gamma} = \{C \in 2^P \mid |C| \geq k\}$. Specially, the k-threshold scheme with t participants is always referred as (k, t)-threshold scheme. Another significant aspect of secret sharing scheme is domains of the secret and shares [1, 4]. Obviously, shares with smaller size are more efficient for storage and transit. A secret sharing scheme is *ideal* in which the domain of each share is equal to that of the secret, both denoted by $\mathcal{K}$. Capocelli et al. [7] pointed out that the domain of each share is at least as large as that of the secret for all perfect secret sharing schemes.

The general model for secret sharing schemes is introduced by many researchers in different forms [5, 16, 1]. Stinson [16] represented a secret sharing scheme by a set $\mathcal{F}$ of distribution rules, each of which is a corresponding relationship between the secret and shares. The general model can be utilized to represent all secret sharing schemes, and makes it easier to give definitions and to present proofs. Since the set of distribution rules corresponding to a certain secret sharing scheme is difficult to directly construct, there exist few or even no theoretic researches or practical applications directly based on the general model. Considering that the biggest challenge is to create a set of distribution rules satisfying $\mathit{\Gamma}$ in the specified domain of the secret and shares, it is a good idea to look for mathematical tools equivalent to the general model.

Initially, Brickell and Davenport [5] introduced an abstract mathematical tool - matroid to give a characterization of ideal secret sharing schemes in a finite field. All monotone access structures of ideal secret sharing schemes can be represented by matroids, and further each matroid, which can be representable over a finite field, is corresponding to an ideal secret sharing scheme. However, researchers still cannot provide a sufficient and necessary condition to relate all ideal secret sharing schemes to matroids [2]. In the other hand, they only consider matriods which are representable in the finite field, that is, in the domain $|\mathcal{K}| = q^m$, where q^m is a power of a prime. Therefore, they cannot determine whether or not an ideal secret sharing scheme exists, if there is a connected matroid $\mathcal{F}$ corresponding to $\mathit{\Gamma}$ which is not representable over a given domain $\mathcal{K}$. Otherwise, this kind of ideal secret sharing schemes represented by matroids are linear schemes, so that the nolinear schemes are not involved. As a result, matroids are far from the general model.

In 1985, W. W. Wu [19] has shown in his book that all secret sharing schemes known at that time can be described in terms of Reed-Solomon codes, and that all of them are related to Latin squares. Since he only focused on discussing the relationship between $(2, 2)$-threshold ideal secret sharing schemes and Latin squares, Dénes and Keedwell [9] generalized his result to $(2, t)$-threshold schemes with the help of mutually orthogonal Latin squares (MOLS). However, the mentioned $(2, t)$-threshold schemes in their theorem are only based on Karnin et al.'s matrix-based linear threshold ideal schemes [12]. Afterwards, there exist few or even no essential researches on the relationship between Latin squares and threshold ideal secret sharing schemes. In recent years, secret sharing schemes based on Latin squares are quite another thing [8, 18]: considering that it is difficult to construct a complete Latin square from partial Latin squares, they distribute different partial Latin squares as shares to participants such that only the partial Latin square constructed by shares from subsets in Γ can determine the only complete Latin square. It is questionable whether this kind of schemes are really perfect.

In this paper, we establish a one-to-one mapping between Latin squares and 2-threshold ideal secret sharing schemes, so Latin squares can be regarded as a corresponding 2-threshold ideal schemes. Furthermore, we obtain some interesting properties of the general model for 2-threshold ideal schemes.

In this paper, we aim to find a mathematical tool to analyze secret sharing schemes from the view of the general model, by which related researches are not limited to linear secret sharing schemes in the finite field. Our main contributions are shown as follows:

1. A new form of the general model for secret sharing schemes, namely the sharing map, is proposed in order to intuitively illustrate the characteristics of secret sharing schemes. In addition, the sharing map is beneficial to analyze the relationship of Latin squares and 2-threshold ideal secret sharing schemes.
2. According to the sharing map, we prove the one-to-one correspondence between the Latin square and $(2, 2)$-threshold ideal secret sharing scheme, and then generalize it to the equivalence between mutually orthogonal Latin squares and $(2, t)$-threshold ideal secret sharing schemes. Especially, Latin squares of order n can be utilized to study all 2-threshold ideal secret sharing schemes, including both linear and nolinear schemes, in an arbitrary integer domain,denoted by $\mathcal{K} = Z_n$.
3. We extend the properties of Latin squares to interesting characteristics of 2-threshold ideal secret sharing schemes, such as: a) the number of distinct $(2, 2)$-threshold ideal secret sharing schemes in Z_n, b) the maximum number of participants in 2-threshold ideal secret sharing schemes in Z_n. Especially, when n is any integer rather than a power of a prime, these properties are difficult to be studied by other means.

The rest of paper is organized as follows. In Section 2 we introduce the basic knowledge of Latin squares, while Section 3 proposes a new form of the general model for secret sharing schemes. The key problem, the equivalence between Latin squares and 2-threshold ideal secret sharing schemes, are proved in Section 4. Afterwards, we show some interesting extended properties of 2-threshold ideal secret sharing schemes in Section 5. Section 6 concludes this paper and provide our future work.

2 Latin Squares

Let n be a positive integer and let S be a set of n distinct elements. A formal definition of the Latin square is given as follows: a Latin square of order n, based on the set S, is an $n \times n$ array, each of whose entries is an element of S such that each of the n elements of S occurs once in each row and once in each column.

In other word, each of rows and columns of a Latin square is a permutation of n elements of S. The actual nature of the elements of S is unimportant, so we always take S to be $Z_n = \{0, 1, \cdots, n-1\}$. Three examples of Latin squares of order $2, 3, 4$ are listed in Eq. (1).

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{bmatrix}. \tag{1}$$

In *Introductory Combinatorics* [6], Brualdi provided another definition of the Latin square from another view. Initially, two $n \times n$ arrays based on Z_n, namely $\mathcal{R}_n$ and $\mathcal{C}_n$, are created as shown in Eq. (2).

$$\mathcal{R}_n = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \cdots & \vdots \\ n-1 & n-1 & \cdots & n-1 \end{bmatrix}, \mathcal{C}_n = \begin{bmatrix} 0 & 1 & \cdots & n-1 \\ 0 & 1 & \cdots & n-1 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 1 & \cdots & n-1 \end{bmatrix}. \tag{2}$$

$\mathcal{A}_n$ is also any $n \times n$ array based on Z_n. Then, $\mathcal{A}_n$ is a Latin square if and only if the following two conditions are satisfied:

(1) When the array $\mathcal{R}_n$ and $\mathcal{A}_n$ are juxtaposed to form an array $\mathcal{R}_n \times \mathcal{A}_n$, each of generated ordered pairs $(\mathcal{R}_n(i,j), \mathcal{A}_n(i,j))$ occurs exactly once.

(2) When the array $\mathcal{C}_n$ and $\mathcal{A}_n$ are juxtaposed to form an array $\mathcal{C}_n \times \mathcal{A}_n$, each of generated ordered pairs $(\mathcal{C}_n(i,j), \mathcal{A}_n(i,j))$ occurs exactly once.

Therefore, there always exist n^2 distinct ordered pairs in $\mathcal{R}_n \times \mathcal{A}_n$ and $\mathcal{C}_n \times \mathcal{A}_n$, respectively. An example is given in Example 1.

Example 1 *A Latin square of order* 3 *is provided to illustrate the foregoing definition. Two groups are corresponding to $\mathcal{R}_n \times \mathcal{A}_n$ and $\mathcal{C}_n \times \mathcal{A}_n$, respectively.*

$$\begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} (0,0) & (0,1) & (0,2) \\ (1,1) & (1,2) & (1,0) \\ (2,2) & (2,0) & (2,1) \end{bmatrix}.$$

$$\begin{bmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} (0,0) & (1,1) & (2,2) \\ (0,1) & (1,2) & (2,0) \\ (0,2) & (1,0) & (2,1) \end{bmatrix}.$$

The preceding idea can also apply to two Latin squares. Let $\mathcal{A}$ and $\mathcal{B}$ be $n \times n$ Latin squares based on the integers in Z_n. Then $\mathcal{A}$ and $\mathcal{B}$ are named orthogonal, if in the juxtaposed $\mathcal{A} \times \mathcal{B}$, each of ordered pairs $(\mathcal{A}(i,j), \mathcal{B}(i,j))$ occurs exactly once. In other word, n^2 possible ordered pairs of integers in Z_n exist in $\mathcal{A} \times \mathcal{B}$. For example, two Latin squares of order 3 are orthogonal in Example 2.

Example 2 *Two orthogonal Latin squares of order* 3.

$$\begin{bmatrix} 2 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} (2,1) & (1,2) & (0,0) \\ (1,0) & (0,1) & (2,2) \\ (0,2) & (2,0) & (1,1) \end{bmatrix}.$$

Furthermore, the notion of orthogonality from two Latin squares is easily extended to any number of Latin squares. Let $\mathcal{A}_1, \mathcal{A}_2, ..., \mathcal{A}_m$ be Latin squares of order n. Then $\mathcal{A}_1, \mathcal{A}_2, ..., \mathcal{A}_m$ are mutually orthogonal, provided that each pair $\mathcal{A}_i, \mathcal{A}_j, (i \neq j)$ of them is orthogonal. We refer to mutually orthogonal Latin squares as MOLS.

3 The New Form of the General Model for Secret Sharing Schemes

Instead of restricting researches in some specific secret sharing scheme, the general model is beneficial to study the natural characteristics of secret sharing system. Brickell and Davenport [5] firstly defined a secret sharing scheme to be a finite matrix, and then proposed the tight relationship between ideal secret sharing schemes and matriods. Afterwards, Stinson [16] regarded the general model for secret sharing scheme as a collection of distribution rules and further provided a formal definition of a perfect secret sharing scheme realizing the access structure Γ. Unfortunately, the general model is only utilized as a formal tool to give definitions and to present proofs, since it is difficult to construct, store and transmit the collection of distribution rules according to the general model.

In order to make definitions clearly, we redefine a new form of the general model for secret sharing schemes as a sharing map, denoted by $\mathcal{M}$, in which each row consists of a secret and all corresponding ordered arrays of shares. Since we talk about ideal secret sharing schemes, the set of secret elements is equivalent to that of share elements, denoted by $\mathcal{K}$.

Let P be the set of participants, each of which is marked with a serial number, denoted by $P = \{p_1, \cdots, p_{|P|}\}$. We use an ordered array of $|P|$ shares to represent shares of participants, denoted by $g = (\beta_1, \cdots, \beta_{|P|}), \beta_i \in \mathcal{K}$. Let $A \subseteq P$. Then the ordered array $g(A)$ is the set of shares of participants in A, e.g., assuming that $A = \{p_{a_1}, \cdots, p_{a_{|A|}}\}$ and $a_1 < \cdots < a_{|A|}$, then $g(A) = (\beta_{a_1}, \cdots, \beta_{a_{|A|}})$. We put the secret, $\alpha \in \mathcal{K}$, and the corresponding set of all possible ordered arrays of shares, denoted by G^α in the same row of $\mathcal{M}$.

For sharing a secret $\alpha \in \mathcal{K}$, the dealer just needs to locate the row r indexed by α in $\mathcal{M}$, to choose an ordered array of shares $g^\alpha \in G^\alpha$ using the uniform distribution, and to assign each share β_i to the corresponding participant p_i. We assume that $\mathcal{M}$ is public knowledge, but the dealer's choice for g^α is private.

Let $A \subseteq P$. After distribution above, each participant $p_{a_i} \in A$ receives a share β_{a_i}. For recovery, they pool their shares together to create an ordered array by their serial numbers, denoted as $d(A) = (\beta_{a_1}, \cdots, \beta_{a_{|A|}})$. Let $G^\alpha(A) = \{g(A) | g \in G^\alpha\}$, that is, $G^\alpha(A)$ is the set of distinct ordered array of shares restricted to participants of A. It is now easy to define the access structure Γ. A subset $A \subseteq P$ is in Γ, if and only if there exists only one secret α such that $d(A) \in G^\alpha(A)$. That is, the secret is determined with shares of participants in A.

Let $H(G^\alpha, d(A)) = \{g \in G^\alpha | g(A) = d(A)\}$. We define that $A \subseteq 2^P - \Gamma$, if for all secrets $\alpha \in \mathcal{K}$, there is an integer γ such that $|H(G^\alpha, d(A))| = \gamma$. That is, there are the same number of order arrays in G^α for all $\alpha \in \mathcal{K}$, each of which satisfies the constraint from $d(A)$. Therefore, no secret information will be revealed with shares of participants in A.

For example, the sharing map of $(2, 2)$-threshold secret sharing scheme in Z_3 is shown as follows.

Example 3 *A sharing map of a $(2, 2)$-threshold secret sharing scheme in $\mathcal{K} = Z_3$ is given as follows.*

α	G^α
0	$(0, 0), (1, 1), (2, 2)$
1	$(0, 1), (1, 2), (2, 0)$
2	$(0, 2), (1, 0), (2, 1)$

In Example 3, when we collect any one of share, such as β_1 or β_2, there always exists an ordered pair in each row. Therefore, nothing secret is deduced with single one share. With the ordered array of two shares, we can exactly locate it in the map and determine the secret.

As mentioned in Section 2, it is noticeable that the sharing map of $(2, 2)$-threshold ideal secret sharing scheme seems quite similar to the juxtaposed matrix by $\mathcal{C}_3$ and a Latin square $\mathcal{A}_3$, denoted by $\mathcal{C}_3 \times \mathcal{A}_3$. Based on the proposed general model, we can easily relate Latin squares with $(2, 2)$-threshold ideal secret sharing schemes. Firstly, we provide a theorem about the sufficient and necessary condition of $(2, 2)$-threshold ideal secret sharing schemes based on the new model.

Theorem 1. *A sharing map for a $(2, 2)$-threshold ideal secret sharing scheme satisfies the following two conditions:*

(C1) *The share of each participant corresponding to each secret, denoted by β_i^α, follows a uniform distribution in $\mathcal{K}$.*

(C2) *All ordered pairs of shares in $\mathcal{M}$ are distinct.*

Proof. Denote the probability of the event A be $\Pr[A]$. The condition **(C1)** means that, for all $\beta \in \mathcal{K}$, $\Pr[\beta_i^\alpha = \beta] = \frac{1}{|\mathcal{K}|}, i \in \{1, 2\}$. That is, the probability that the recovered integer is any integer in $\mathcal{K}$ with single one share is the same, denoted by $\Pr[\alpha' = \alpha \mid \beta] = \Pr[\beta_i^\alpha = \beta] = \frac{1}{|\mathcal{K}|}, (\alpha \in \mathcal{K})$. The attacker cannot deduce any secret information from only one share. In addition, the condition **(C1)** implies that the number of ordered arrays corresponding to each secret value is the integer multiple of $|\mathcal{K}|$, symbolically, $|G^{\alpha}(P)| = |\mathcal{K}| \times i$ ($\alpha \in \mathcal{K}, i \in Z^{+}$).

The condition **(C2)** is relatively straightforward: the original secret can be located accurately by any ordered pair. In this condition, we do not consider the possible duplicates of ordered arrays in the same row due to no essential influence on schemes. Combining **(C2)** with **(C1)**, it is deduced that each of $|\mathcal{K}|^2$ ordered pairs occurs exactly once in $\mathcal{M}$, and furthermore there exist total $|\mathcal{K}|$ ordered pairs of shares in each row. Symbolically, for $\alpha \in \mathcal{K}$, $|G^{\alpha}(P)| = |\mathcal{K}|$ and $|\bigcup_{\alpha \in \mathcal{K}} G^{\alpha}(P)| = |\mathcal{K}|^2$.

In summary, two conditions above are necessary and sufficient for a sharing map of a $(2,2)$-threshold ideal secret sharing scheme.

4 The One-to-one Mapping between Latin Squares and 2-threshold Ideal Secret Sharing Schemes

According to Theorem 1, we prove the equivalence between Latin squares and $(2,2)$-threshold ideal secret sharing schemes. Furthermore, the one-to-one relationship between mutually orthogonal Latin squares and 2-threshold ideal secret sharing scheme is also proved.

4.1 Latin Squares and $(2,2)$-threshold Ideal Secret Sharing Schemes

Considering the sharing map is equivalent to an implementation of a $(2,2)$-threshold ideal secret sharing scheme, our primary goal is equivalent to prove the equivalence between Latin squares and sharing maps.

Lemma 1. *Given a Latin square of ordered n, denoted by $\mathcal{A}_n$, there exists a $(2,2)$-threshold ideal secret sharing scheme for $\mathcal{K} = Z_n$.*

Proof. Based on $\mathcal{A}_n$, we can easily construct the sharing map of a $(2,2)$-threshold ideal secret sharing scheme by the following steps:

1. Create a $n \times n$ array $\mathcal{C}_n$ with the same integer in each column, just as shown in Section 2.
2. Juxtapose $\mathcal{C}_n$ and $\mathcal{A}_n$ to form $\mathcal{C}_n \times \mathcal{A}_n$.
3. Use the row number r as the secret α, and use the set of n ordered pairs in row r as the corresponding set of shares G^{α}. As a result, a sharing map $\mathcal{M}_n$ is generated.

Obviously, $\mathcal{M}$ satisfies two conditions in Theorem 1, so it is regarded as an implementation of a $(2,2)$-threshold ideal secret sharing. Therefore, it is concluded that a Latin square is sufficient to construct a corresponding $(2,2)$-threshold ideal secret sharing scheme.

Lemma 2. *Given a $(2,2)$-threshold ideal secret sharing scheme for $\mathcal{K} = Z_n$, there exists a corresponding Latin square of order n $\mathcal{A}_n$.*

Proof. Based on a $(2,2)$-threshold ideal secret sharing scheme for $\mathcal{K} = Z_n$, we can create a corresponding sharing map $\mathcal{M}_n$. Furthermore, we can easily obtain a Latin square $\mathcal{A}_n$ in the following steps:

1. We extract all $G^\alpha, \alpha \in \mathcal{K}$ from $\mathcal{M}_n$, to construct a $n \times n$ array, denoted by $\mathcal{A}_M$.
2. For each row in $\mathcal{A}_M$, sort the ordered arrays by the first share β_1 from 0 to $n-1$, then we obtain a sorted sharing map, denoted by $\overline{\mathcal{A}_M}$.

   Remark 1. In a secret sharing scheme, the order of ordered pairs in G^α is arbitrary, so $\overline{\mathcal{A}_M}$ is equivalent to $\mathcal{A}_M$ in essence.
3. Pick shares of the second participant p_2 from each ordered pair, and put each of them to the same position in a new $n \times n$ array, namely $\mathcal{A}_n^{p_2}$. As a result, a square is generated.

Since all ordered pairs are distinct and the first share in the same column of $\overline{\mathcal{A}_M}$ is the same, the second share in the same column of $\overline{\mathcal{A}_M}$ must be distinct. According to Theorem 1, the second share in each row of $\overline{\mathcal{A}_M}$ also follows a uniform distribution. It is concluded that the square $\mathcal{A}_n^{p_2}$ is a Latin square.

As a result, example 4 is provided to illustrate the corresponding relation of a Latin square and a $(2,2)$-threshold ideal secret sharing scheme.

Example 4 *Given a sharing map of $(2,2)$-threshold ideal secret sharing scheme in Z_4 as shown in Table 1.*

Table 1. The sharing map of a $(2,2)$-threshold ideal secret sharing scheme in Z_4.

α	G^α
0	$(1,1), (3,3), (0,0), (2,2)$
1	$(3,0), (1,2), (2,3), (0,1)$
2	$(1,3), (0,2), (2,0), (3,1)$
3	$(0,3), (1,0), (3,2), (2,1)$

It is converted into a Latin square as shown in Eq. (3). Firstly, we extract all $G^\alpha, \alpha \in \mathcal{K}$ from $\mathcal{M}_n$ to construct $\mathcal{A}_M$, then sort $\mathcal{A}_M$ by β_1 in order to generate $\overline{\mathcal{A}_M}$, and finally pick out β_2 to construct the $n \times n$ array as the Latin square $\mathcal{A}_n^{p_2}$. In turn, the given sharing map also can be constructed from the Latin square $\mathcal{A}_n^{p_2}$.

$$\begin{bmatrix} (1,1) & (3,3) & (0,0) & (2,2) \\ (3,0) & (1,2) & (2,3) & (0,1) \\ (1,3) & (0,2) & (2,0) & (3,1) \\ (0,3) & (1,0) & (3,2) & (2,1) \end{bmatrix} \Leftrightarrow \begin{bmatrix} (0,0) & (1,1) & (2,2) & (3,3) \\ (0,1) & (1,2) & (2,3) & (3,0) \\ (0,2) & (1,3) & (2,0) & (3,1) \\ (0,3) & (1,0) & (2,1) & (3,2) \end{bmatrix} \Leftrightarrow \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{bmatrix}. \qquad (3)$$

According to two lemmas above, we can easily assert that a Latin square is equivalent to an implementation of a $(2,2)$-threshold ideal secret sharing scheme, that is Theorem 2. However, we give the essential proof of Theorem 2, to prove their necessary and sufficient conditions are equivalent.

Theorem 2. *There is a one-to-one mapping between a Latin square of order n and a $(2,2)$-threshold secret sharing scheme for $\mathcal{K} = Z_n$.*

Proof. A Latin square of order n $\mathcal{A}_n$ is a $n \times n$ array, which satisfies that:

(L1) Each element in Z_n occurs exactly once in each row of $\mathcal{A}_n$.
(L2) Each element in Z_n occurs exactly once in each column of $\mathcal{A}_n$.

Reviewing Theorem 1, the condition **(C1)** means that, for the second share, each element in Z_n occurs exactly once for all secrets $\alpha \in \mathcal{K}$. That is, **(L1)** can be deduced from **(C1)**.

In the other hand, considering the $n \times n$ array $\overline{\mathcal{M}_G}$ after sorted by β_1, for the second share, each element in Z_n also occurs exactly once in each column. Considering that **(C2)** requires that each ordered pair are distinct, so all the items corresponding to β_2 in the same column must be different due to the same item corresponding to β_1.

It is concluded that two essential conditions of a Latin square are equivalent to those of a $(2,2)$-threshold ideal secret sharing scheme. Theorem 2 now follows.

4.2 Mutually Orthogonal Latin Squares and 2-threshold Ideal Secret Sharing Schemes

Based on Theorem 2, the following equivalence between MOLS and 2-threshold ideal secret sharing scheme is easier to prove. However, the maximum number of Latin squares in MOLS is limited by order n, denoted by $L(n)$. Similarly, the maximum number of participants in 2-threshold ideal scheme, denoted by m, is also limited by n, and it is proved in this section that $m = L(n) + 1$.

Lemma 3. *Let $MOLS_n^m$ be mutually orthogonal Latin squares of order n, which consist of m Latin squares, $m \leq L(n)$. Then there exists a $(2, m+1)$-threshold ideal secret sharing scheme corresponding to $MOLS_n^m$.*

Proof. Obviously, the definition of MOLS means that a distinct $(2,2)$-threshold ideal secret sharing scheme is constructed based on each pair of Latin squares in MOLS, denoted by $\mathcal{A}_n^i$ and $\mathcal{A}_n^j, i \neq j$: juxtapose $\mathcal{A}_n^i$ and $\mathcal{A}_n^j$ to form an array $\mathcal{A}_n^i \times \mathcal{A}_n^j$, and pick up the ordered pairs in each row $\alpha \in Z_n$ of $\mathcal{A}_n^i \times \mathcal{A}_n^j$ as the corresponding set G^α in the sharing map $\mathcal{M}_n$. $\mathcal{M}_n$ is an implementation of a $(2,2)$-threshold ideal secret sharing scheme. We can deduce no secret information from one share, but the original secret is exactly determined by the ordered pair of two shares. Therefore, the MOLS with $m \leq L(n)$ Latin squares is equivalent to a $(2,m)$-threshold secret sharing scheme.

Reviewing Theorem 2, $\mathcal{C}_n$ and any Latin square $\mathcal{A}_n$ can be used to create a sharing map $\mathcal{M}_n$. Therefore, a $(2, m+1)$-threshold ideal secret sharing scheme can be created based on $\mathcal{C}_n$ and $m \leq L(n)$ mutually orthogonal Latin squares.

Lemma 4. *If $m > L(n)$, there does not exist any $(2, m+1)$-threshold ideal secret sharing scheme.*

Proof. Assuming there exists a $(2, m+1)$-threshold ideal secret sharing scheme for $\mathcal{K} = Z_n$, when $m > L(n)$. The $(2, m+1)$-threshold ideal secret sharing scheme consists of $\binom{m+1}{2}$ $(2,2)$-threshold ideal secret sharing schemes, and each participant $p_i \in P$ participates m $(2,2)$-threshold ideal secret sharing schemes. We choose m $(2,2)$-threshold ideal secret sharing schemes with p_1, and sort the sharing map of each schemes by β_1. As a result, we obtain m distinct Latin squares. Since m distinct Latin squares is sufficient to create a $(2, m)$-threshold ideal secret sharing scheme, they must be mutually orthogonal. Therefore, there must be m mutually orthogonal Latin squares, $m > L(n)$. It contradicts that the maximum number of MOLS is $L(n)$. Therefore, Lemma 4 now follows.

Based on Lemma 3 and Lemma 4, the equivalence between $MOLS_n^m$ and $(2, m+1)$-threshold ideal secret sharing scheme is obvious, so Theorem 3 is provided as follows.

Theorem 3. *There is a one-to-one mapping between $MOLS_n^m$ of order n with m Latin squares and a $(2, m+1)$-threshold secret sharing scheme in $\mathcal{K}$, where $|\mathcal{K}| = n$ for any integer n.*

According to Theorem 3, every 2-threshold ideal secret sharing schemes in any finite integer domain can be uniquely represented by MOLS. In comparison with previous ideal schemes restricted in the finite field, future researches based on Latin squares of order n will produce more interesting properties of 2-threshold ideal schemes.

5 Novel Properties of 2-threshold Ideal Schemes

After proofs of equivalences, we can utilize related researches on Latin squares to extend the characteristics of 2-threshold ideal secret sharing schemes. In this section, we focus on providing some properties of 2-threshold ideal schemes for $\mathcal{K} = Z_n$ is any finite integer domain, rather than only a finite field. Finally, some extensions are provided to illustrate the possible generalization to k-threshold ideal scheme, and some open questions of 2-threshold ideal schemes are also given.

5.1 How Many Distinct $(2,2)$-threshold Ideal Schemes in Z_n?

The number of Latin squares of order n is related with n, denoted as $\mathcal{N}(n)$. One classic result of $\mathcal{N}$ is that [15]:

$$\prod_{i=1}^{n} (i!)^{n/i} \geq \mathcal{N}(n) \geq \frac{(n!)^{2n}}{n^{n^2}}.$$

In Table 2 (from the sequence $A002860$ in the OEIS), it can be seen that $\mathcal{N}(n)$ grows extremely quickly with n increasing. Furthermore, the accurate number of $\mathcal{N}(n)$ is not easily provided when $n \geq 12$.

Table 2. The number of Latin squares of order n ($n \in [1, 12]$)

n	$\mathcal{N}(n)$
1	1
2	2
3	12
4	576
5	161,280
6	812,851,200
7	61,479,419,904,000
8	108,776,032,459,082,956,800
9	5,524,751,496,156,892,842,531,225,600
10	9,982,437,658,213,039,871,725,064,756,920,320,000
11	776,966,836,171,770,144,107,444,346,734,230,682,311,065,600,000
12	$\cdots$

Because the equivalence between a Latin square and a $(2, 2)$-threshold ideal secret sharing scheme, we make a conclusion about the number of $(2, 2)$-threshold ideal secret sharing schemes in Z_n in Theorem 4.

Theorem 4. *The number of* $(2, 2)$*-threshold ideal secret sharing schemes in* Z_n *is equal to the number of Latin squares of order* n*, denoted by* $\mathcal{N}(n)$*.*

Proof. In Theorem 2, it is proved that each of Latin squares of order n has a corresponding $(2, 2)$-threshold ideal secret sharing schemes in Z_n. Therefore, the number of them is equal.

Theorem 4 can be utilized to judge whether a so-called general construction of $(2, 2)$-threshold ideal schemes is just a special subset of all schemes representable by the proposed general model. In the other hand, the sharing map of a secret sharing scheme is always public in classic applications. Since there exist innumerable schemes when n is large, sharing maps of $(2, 2)$-threshold ideal schemes also can be kept private as the key for the dealer or the leader. Without the private sharing map, the secret is difficult to crack even if two shares are intercepted by attacker.

5.2 The Maximum Number of Participants in 2-threshold Ideal Schemes?

In 1983, Karnin et al. [12] provided a theorem for the maximum number of participants in k-threshold ideal secret sharing schemes for Z_n, denoted by $\mathcal{S}(n, k)$, as shown in Theorem 5.

Theorem 5. *[12] Given the number of all elements is a power of a prime, denoted by* $\mathcal{K} = Z_{q^m}$*. The maximum number of participants of* k*-threshold ideal secret sharing scheme is:*

$$q^m \leq \mathcal{S}(q^m, k) \leq q^m + k - 2, \quad q^m > k, \tag{4}$$

However, Theorem 5 is only restricted in threshold schemes in a Galois field GF(q^m), q^m is a power of a prime. In the more general situation, let n be a positive integer rather than q^m, and $\mathcal{K} = Z_n$. $\mathcal{S}(n, k)$ can not be solved by Karnin et al.'s theorem. Since there are some results about the maximum number of MOLS of order n, denoted by $\mathcal{W}(n)$, we can easily induce that $\mathcal{S}(n, 2) = \mathcal{W}(n) + 1$, as proved in Theorem 3.

Let $n \geq 2$ and $n = q^m$. It is known that $\mathcal{W}(n) = q^m - 1$ [6]. Therefore, we obtain the same result as Theorem 5.

Theorem 6. *Let $n \geq 2$ and $n = q^m$. The maximum number of participants of 2-threshold ideal secret sharing schemes is q^m, denoted as*

$$\mathcal{S}(q^m, 2) = q^m.$$

It is known that $\mathcal{W}(n) \leq n - 1$ for all $n \in Z^+$ [6]. Therefore, Theorem 7 is provided to give the upper bound of $\mathcal{S}(n, 2)$.

Theorem 7. *Let $\mathcal{K} = Z_n$. The number of participants in 2-threshold ideal secret sharing schemes is less than n, denoted as*

$$\mathcal{S}(n, 2) \leq n.$$

Let $n \geq 2$ be an integer and let $n = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_k^{e_k}$ be the factorization of n into distinct prime numbers $p_1, p_2, \cdots, p_k$. Then, $\mathcal{W}(n) \geq min\{p_i^{e_i} - 1 : i = 1, 2, \cdots, k\}$ [6]. Based on this conclusion, Theorem 8 is given as follows.

Theorem 8. *Let $n \geq 2$ and $n = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_k^{e_k}$ be the factorization of n into distinct prime numbers $p_1, p_2, \cdots, p_k$. Then, the maximum number of participants in 2-threshold ideal secret sharing schemes is greater than $min\{p_i^{e_i} : i = 1, 2, \cdots, k\}$, denoted as*

$$\mathcal{S}(n, 2) \geq min\{p_i^{e_i} : i = 1, 2, \cdots, k\}.$$

Although it is quite difficult to compute the accurate value of $\mathcal{W}(n)$ when n is not a power of a prime, there exists at least a pair of MOLS when $n \neq 2$ *and* 6. When $n = 2$ *or* 6, it is proved that there does not exist any MOLS [6]. Therefore, Theorem 9 is provided to describe the existence of $(2, 3)$-threshold ideal secret sharing scheme.

Theorem 9. *Let $n \in Z^+$ and $n \neq 2$ and 6. There exist $(2, 3)$-threshold ideal secret sharing schemes for Z_n.*

In 1994, Beimel and Chor introduced an interesting concept, named universally ideal access structure, which relates the access structure Γ with the finite domain $\mathcal{K}$. An access structure is universally ideal if there exists an ideal secret sharing scheme for it over any finite domain of secrets. A sufficient and necessary condition of an universally ideal access structure is to be ideal over the binary and ternary domains of secrets. According to Theorem 9, we can easily come to Corollary 1.

Corollary 1. *Only* $(2, 2)$*-threshold out of* 2*-threshold access structure is universally ideal.*

In this paper, we just collect a little part of properties of Latin squares and MOLS, and convert them into the corresponding theorems of 2-threshold ideal schemes. With the help of the proven equivalence, we are able to induce more valuable properties from existing researches of Latin squares.

5.3 Extensions and Open Questions

There are a few generalization of the concept of a Latin square to the multidimensional case. Similarly, a k-dimensional Latin square of order n, denoted by $\mathcal{A}_n^k = ||a_{i_1 \cdots i_k}||$, is a k-dimensional matrix of order n including the first n natural numbers, which is such that for any j the set of n items is the permutation of the first n natural numbers, denoted by

$$a_{i_1 \cdots i_{j-1} 1 i_{j+1} \cdots i_k},\ a_{i_1 \cdots i_{j-1} 2 i_{j+1} \cdots i_k}, \cdots, a_{i_1 \cdots i_{j-1} n i_{j+1} \cdots i_k}.$$

If $\mathcal{A}_n^k$ exists, can we relate $\mathcal{A}_n^k$ to a (k, k)-threshold secret sharing scheme in Z_n. That is, the equivalence between m-dimensional Latin square of order n and (k, k)-threshold secret sharing scheme in Z_n needs to be proven. Furthermore, it is a question whether the concept of k-dimensional MOLS of order n still exists. If it exists, how about the one-to-one mapping relationship between k-dimensional MOLS of order n and k-threshold ideal schemes in Z_n. External direct products may be utilized to realize the extension to k-threshold ideal schemes [10].

In spite of many valuable researches on Latin squares [15, 13, 17, 11], there are still many open questions, especially with large order n, including: *a*) the exact number of Latin squares of order n; *b*) the exact maximum number of Latin squares in MOLS of order n. Since there do not exist deterministic computational formulas for them, it is difficult to further find exact solutions of the corresponding problems in 2-threshold ideal schemes, especially for any $\mathcal{K} = Z_n$, which is not a finite field.

6 Conclusion

In this paper, the essential equivalence between Latin squares and 2-threshold ideal secret sharing schemes is introduced and proved. With the help of related researches on Latin squares, we can better understand the general model for 2-threshold ideal secret sharing schemes, and further deduce two categories of properties of 2-threshold ideal secret sharing schemes in any finite integer domain, such as *a*) the number of distinct $(2, 2)$-threshold ideal schemes, *b*) the maximum number of participants in 2-threshold ideal schemes. In the meanwhile, we realize that it is difficult to solve some problems of the general model for secret sharing schemes, because there still exist many open questions about Latin squares. Our future work is to further extend properties of threshold ideal secret sharing schemes based on the existing knowledge of Latin squares.

References

1. Beimel, A., Chor, B.: Universally ideal secret-sharing schemes. IEEE Transactions on Information Theory **40**(3), 786–794 (1994)
2. Beimel, A., Livne, N., Padró, C.: Matroids can be far from ideal secret sharing. In: Theory of Cryptography Conference. pp. 194–212. Springer (2008)
3. Blakley, G.R.: Safeguarding cryptographic keys. In: Afips Conference Proceedings. vol. 48, pp. 313–317 (1979)
4. Bogdanov, A., Guo, S., Komargodski, I.: Threshold secret sharing requires a linear size alphabet. In: Theory of Cryptography Conference. pp. 471–484. Springer (2016)
5. Brickell, E.F., Davenport, D.M.: On the classification of ideal secret sharing schemes. Journal of Cryptology **4**(2), 123–134 (1991)
6. Brualdi, R.A.: Introductory combinatorics. Fifth Edition. China Machine Press, Beijing (2009)
7. Capocelli, R.M., De Santis, A., Gargano, L., Vaccaro, U.: On the size of shares for secret sharing schemes. Journal of Cryptology **6**(3), 157–167 (1993)
8. Chum, C.S., Zhang, X.: The latin squares and the secret sharing schemes. Groups–Complexity–Cryptology **2**(2), 175–202 (2010)
9. Dénes, J., Keedwell, A.D.: On golomb-posner codes and a remark of ww wu about secret-sharing systems. IEEE transactions on communications **38**(3), 261–262 (1990)
10. Gallian, J.: Contemporary abstract algebra. Nelson Education (2012)
11. Hedayat, A.S., Sloane, N.J.A., Stufken, J.: Orthogonal arrays: theory and applications. Springer Science & Business Media (2012)
12. Karnin, E., Greene, J., Hellman, M.: On secret sharing systems. IEEE Transactions on Information Theory **29**(1), 35–41 (1983)
13. McKay, B.D., Wanless, I.M.: On the number of latin squares. Annals of combinatorics **9**(3), 335–344 (2005)
14. Shamir, A.: How to share a secret. Communications of the ACM **22**(11), 612–613 (1979)
15. Shao, J.y., et al.: A formula for the number of latin squares. Discrete mathematics **110**(1-3), 293–296 (1992)
16. Stinson, D.R.: An explication of secret sharing schemes. Designs, Codes and Cryptography **2**(4), 357–390 (1992)
17. Stones, D.S.: The many formulae for the number of latin rectangles. the electronic journal of combinatorics **17**(1), 1 (2010)
18. Stones, R.J., Su, M., Liu, X., Wang, G., Lin, S.: A latin square autotopism secret sharing scheme. Designs, Codes and Cryptography **80**(3), 635–650 (2016)
19. Wu, W.W.: Elements of digital satellite communication, vol. 2. Computer Science Press (1985)