Discrete Mathematics and Theoretical Computer Science **6**, 2004, 471–482

Characterisations of Ideal Threshold Schemes

Josef Pieprzyk and Xian-Mo Zhang

Center for Advanced Computing – Algorithms and Cryptography
Department of Computing, Macquarie University
Sydney , NSW 2109, Australia
Email: josef,xianmo@ics.mq.edu.au

received May 18, 2004, accepted Nov 1, 2004.

We characterise ideal threshold schemes from different approaches. Since the characteristic properties are independent to particular descriptions of threshold schemes, all ideal threshold schemes can be examined by new points of view and new results on ideal threshold schemes can be discovered.

Keywords: Secret Sharing, Perfect Threshold Schemes, Ideal Threshold Schemes

1 Introduction

Since 1979 when threshold schemes were introduced by Blakley (Bla79) and Shamir (Sha79), many papers in this area have been published. These papers are mostly about particular designs and applications of threshold schemes.

In this work, we are interested in characterisations of ideal threshold schemes rather than particular constructions. Of course, these characteristic properties do not depend on any form of any ideal threshold scheme. This enables us to look at any ideal threshold scheme from new points of view, and further find new results on ideal threshold schemes.

This work is structured as follows. The basic concepts of threshold schemes, and more generally, secret sharing schemes are introduced in Section 2.

In Section 3, we describe (weakly and strongly) perfect secret sharing schemes using defining matrices. By the original definition (BS92), an ideal threshold scheme is a strongly perfect threshold scheme for which the set of secrets and the set of shares have the same cardinality.

In Sections 4 and 5, we derive a series of properties of weakly perfect threshold schemes that are helpful for us to characterise ideal threshold schemes in Section 6 from different points of view. Consequently "strongly perfect" in the original definition of ideal threshold schemes can be replaced by "weakly perfect".

We further obtain more results on ideal threshold schemes in Section 7 including an application in cheating prevention.

In Section 8, we work on the threshold schemes whose set of secrets and set of shares are identical, and derive more characteristic properties of ideal threshold schemes. In Section 9, we find some bounds on the parameters of ideal threshold schemes.

In Section 10, we compare this work with other results. Conclusions close the work.

2 Access Structures

Secret sharing is a method to share a secret among a set of participants $\mathbf{P} = \{P_1, \ldots, P_n\}$. Let $\mathbf{K}$ denote the set of *secrets* and $\mathbf{S}$ denote the set of *shares*. The secret sharing includes two algorithms: the distribution algorithm (dealer) and the recovery algorithm (combiner).

The dealer assigns shares $s_1, \ldots, s_n$, where the vector $(s_1, \ldots, s_n)$ is called a *share vector*, to all the participants $P_1, \ldots, P_n$, respectively.

Assume that the currently active participants are $P_{j_1}, \ldots, P_{j_\ell}$ and that they submit their shares to the combiner in order to recover the secret. Their shares $s_{j_1}, \ldots, s_{j_\ell}$ can determine a secret $K \in \mathbf{K}$ if and only if $\{P_{j_1}, \ldots, P_{j_\ell}\}$ is a qualified subset of $\mathbf{P}$, i.e., the set of currently active participants belongs to the *access structure* Γ.

Any access structure should be *monotone*, or more precisely, if $\mathcal{A} \in \Gamma$ and $\mathcal{A} \subseteq \mathcal{B} \subseteq \mathbf{P}$ then $\mathcal{B} \in \Gamma$.

As shown in (BD91) and (BS92), we can describe secret sharing with the access structure Γ by an $m \times (n+1)$ matrix M^* in which no two rows are identical. The matrix M^* has $n+1$ columns indexed by $0, 1 \ldots, n$. The number m of rows of M^* depends on a particular scheme. We index the m rows by $1, \ldots, m$. For a row of M^*, the entry in the 0th position holds a secret and the entry in the ith position ($i = 1, \ldots, n$) contains the corresponding share of P_i. Denote the entry on the ith row and the jth column of M^* by $M^*(i, j)$.

The matrix M^* is called a *defining matrix* of secret sharing with the access scheme Γ. The matrix M obtained from M^* by removing the 0th column is called the *associated matrix* of the scheme.

The dealer works in two stages. In the first stage, it creates the defining matrix M^* for secret sharing with the access structure Γ. The matrix is made public. In the second stage, the dealer randomly chooses a row of the matrix M^*. Let the row chosen be indexed by the integer i ($1 \le i \le m$). The secret is $K = M^*(i, 0)$ and shares are $s_j = M^*(i, j)$, $j = 1, \ldots, n$. The shares are distributed to the corresponding participants via secure channels.

Note that a defining matrix uniquely determines a secret sharing scheme but a secret sharing scheme has more defining matrices.

Permuting the rows of a defining matrix of secret sharing does not give a new scheme.

Permuting the columns of defining matrices of secret sharing is equivalent to changing the indices of participants.

It should be pointed out once again that a defining matrix of a secret sharing scheme is public.

The dealer chooses at random a single row of the matrix.

The shares are communicated to the corresponding participants via secure channels so the share s_i is known to the participant P_i only ($i = 1, \ldots, n$).

An access structure $\Gamma = \{\mathcal{A} \mid \#\mathcal{A} \ge t\}$ is called a (t, n)*-threshold access structure*, where $\#X$ denotes the cardinality of the set X (i.e. the number of elements in the set X) and the integer t is called the *threshold* of secret sharing, where $t \le n$.

Secret sharing schemes with the (t, n)-threshold access structure are called (t, n)-threshold schemes.

Threshold schemes were first introduced by Blakley (Bla79) and Shamir (Sha79). Ito *et al* (ISN87) generalised threshold schemes for arbitrary access structure.

3 Perfect Secret Sharing And Ideal Secret Sharing

We say that secret sharing with the access structure Γ is perfect if the following two conditions are satisfied:

(1) If $\mathcal{A} \in \Gamma$ then the participants in $\mathcal{A}$ can uniquely determine the secret by pooling their shares together.

(2) If $\mathcal{A} \notin \Gamma$ then the participants from $\mathcal{A}$ can determine nothing about the secret (in an information theoretic sense).

As mentioned in (BS92), Conditions (1) and (2) can be translated into conditions that need to be satisfied in the context of the defining matrix. We list the translations as follows.

(a) Let $\mathcal{A} \in \Gamma$. If $M^*(i,j) = M^*(i',j)$ for every $P_j \in \mathcal{A}$ then $M^*(i,0) = M^*(i',0)$.

(b) Let $\mathcal{A} \notin \Gamma$. For any $1 \le i_0 \le m$ and any $K \in \mathbf{K}$, there exists some i with $1 \le i \le m$ such that $M^*(i,j) = M^*(i_0,j)$ for all $P_j \in \mathcal{A}$ and $M^*(i,0) = K$.

(b') Let $\mathcal{A} = \{P_{j_1}, \ldots, P_{j_\ell}\} \notin \Gamma$. For any $s_{j_1}, \ldots, s_{j_\ell} \in \mathbf{S}$ and any $K \in \mathbf{K}$,

$$\#\{i \mid M^*(i,j_u) = s_{j_u} \text{ for all } P_{j_u} \in \mathcal{A} \text{ and } M^*(i,0) = K\}$$

is independent to the choice of K.

Condition (1) is corresponding to Condition a. Condition (2) has two translations: Condition (b) and Condition (b'). It is easy to verify that (b') implies (b).

For the case of a (t,n)-threshold scheme, Conditions (a), (b), and (b') can be rewritten as follows:

(c) Let $\#\mathcal{A} \ge t$. If $M^*(i,j) = M^*(i',j)$ for every $P_j \in \mathcal{A}$ then $M^*(i,0) = M^*(i',0)$.

(d) Let $\#\mathcal{A} < t$. For any $1 \le i_0 \le m$ and any $K \in \mathbf{K}$, there exists some i with $1 \le i \le m$ such that $M^*(i,j) = M^*(i_0,j)$ for all $P_j \in \mathcal{A}$ and $M^*(i,0) = K$.

(d') Let $\mathcal{A} = \{P_{j_1}, \ldots, P_{j_\ell}\}$ with $\ell < t$. For any $s_{j_1}, \ldots, s_{j_\ell} \in \mathbf{S}$ and any $K \in \mathbf{K}$,

$$\#\{i \mid M^*(i,j_u) = s_{j_u} \text{ for all } P_{j_u} \in \mathcal{A} \text{ and } M^*(i,0) = K\}$$

is independent to the choice of K.

Similarly, (d') implies (d).

The following definition is due to (BS92).

Definition 1 *A secret sharing scheme satisfying (a) and (b) is called* weakly perfect*. Alternatively, a* (t,n)*-threshold scheme satisfying (c) and (d) is called* weakly perfect.

In (BS92) the following definition is given.

Definition 2 *A secret sharing scheme satisfying (a) and (b') is called* strongly perfect*, or more briefly* perfect *if no confusion occurs. Alternatively, a (t,n)-threshold scheme satisfying (c) and (d') is called* strongly perfect*, or more briefly* perfect *if no confusion occurs.*

As mentioned in (BS92), for any strongly perfect secret sharing scheme, we have $\#\mathbf{K} \le \#\mathbf{S}$. In particular, if $\#\mathbf{K} = \#\mathbf{S}$ holds for a strongly secret sharing scheme, from (BS92), we have the following definition.

Definition 3 *An ideal secret sharing scheme is a strongly perfect secret sharing scheme satisfying $\#\mathbf{K} = \#\mathbf{S}$. Alternatively, an ideal threshold scheme is a strongly perfect threshold scheme satisfying $\#\mathbf{K} = \#\mathbf{S}$.*

In this work we pay our attention to ideal threshold schemes. New results on weakly perfect threshold schemes in this work are helpful for characterising ideal threshold schemes.

4 Properties of Weakly Perfect Threshold Schemes (I)

It should be noted that the inequality $\#\mathbf{K} \le \#\mathbf{S}$ also holds for any weakly perfect secret sharing scheme. The proof can be found from (PZ02). Then we state as follows.

Lemma 1 $\#\mathbf{K} \le \#\mathbf{S}$ *holds for any weakly perfect secret sharing scheme.*

Lemma 2 *Let a (t,n)-threshold scheme be weakly perfect. If $\#\mathbf{K} = \#\mathbf{S}$ then its defining matrix M^* has the following property. For any given $t-1$ integers, $1 \le j_1 < \cdots < j_{t-1} \le n$, if $M^*(i_0,0) = M^*(i',0)$, $M^*(i_0,j_1) = M^*(i',j_1)$, …, $M^*(i_0,j_{t-1}) = M^*(i',j_{t-1})$ then $M^*(i_0,j) = M^*(i',j)$, $j = 0,1,\ldots,n$.*

Proof Set

$$\begin{aligned} &M^*(i_0,0) = M^*(i',0) = K,\ M^*(i_0,j_1) = M^*(i',j_1) = s_{j_1},\ldots, \\ &M^*(i_0,j_{t-1}) = M^*(i',j_{t-1}) = s_{j_{t-1}} \end{aligned} \tag{1}$$

Let $\#\mathbf{K} = \#\mathbf{S} = b$. Write $\mathbf{K} = \{K_1,\ldots,K_b\}$ and $\mathbf{S} = \{\varepsilon_1,\ldots,\varepsilon_b\}$. Let M^* contain precisely m rows. Thus M^* be an $m \times (n+1)$ matrix. We index the rows of M^* by $1,\ldots,m$, and index the columns by $0,1,\ldots,n$. Consider the $m \times t$ matrix M_0, consisting of the t columns of M^* indexed by 0, $j_1,\ldots,j_{t-1}$.

Let j_t be an integer satisfying $1 \le j_t \le n$ and $j_t \notin \{j_1,\ldots,j_{t-1}\}$. Without loss of generality, we assume that $j_t > j_{t-1}$. Let M_1 denote a $m \times (t+1)$ matrix consisting of the $t+1$ columns of M^* indexed by 0, $j_1,\ldots,j_{t-1},j_t$.

Let $\Re_i$, $i = 1,\ldots,b$, denote the subset of $\mathbf{S}$ such that $\varepsilon \in \Re_i$ if and only if $(K_i,s_{j_1},\ldots,s_{j_{t-1}},\varepsilon)$ is a row of M_1.

Since $(K,s_{j_1},\ldots,s_{j_{t-1}})$ is a row of M_0, due to Condition (d), we know that $(K_i,s_{j_1},\ldots,s_{j_{t-1}})$ is a row of M_0, $i = 1,\ldots,b$, and thus $\#\Re_i > 0$, $i = 1,\ldots,b$. Due to Condition (c), we have $\Re_i \cap \Re_j = \emptyset$, if $j \ne i$ where $\emptyset$ denotes the empty set. Thus we have $\#(\Re_1 \cup \cdots \cup \Re_b) = \#\Re_1 + \cdots + \#\Re_b \ge b$. On the other hand $\Re_1 \cup \cdots \cup \Re_b \subseteq \mathbf{S}$ and then $\#(\Re_1 \cup \cdots \cup \Re_b) \le \#\mathbf{S} = b$. Therefore we know that $b = \#\mathbf{S} = \#\Re_1 + \cdots + \#\Re_b$. Recall that $\#\Re_i > 0$, $i = 1,\ldots,b$. Then we have

$$\#\Re_i = 1,\ i = 1,\ldots,b \tag{2}$$

From (2) and (1), we know that $M^*(i_0,j_t) = M^*(i',j_t)$. Since j_t is an arbitrary integer with $1 \le j_t \le n$ and $j_t \notin \{0,j_1,\ldots,j_{t-1}\}$, we have proved that $M^*(i_0,j) = M^*(i',j)$, $j = 0,1,\ldots,n$. □

Lemma 3 *Let a (t,n)-threshold scheme be weakly perfect. If* $\#\mathbf{K} = \#\mathbf{S}$ *then its defining matrix* M^* *has the following property. For any given t integers* $1 \le j_1 < \cdots < j_t \le n$, *if* $M^*(i_0, j_1) = M^*(i', j_1)$, ..., $M^*(i_0, j_t) = M^*(i', j_t)$ *then* $M^*(i_0, j) = M^*(i', j)$, $j = 0, 1, \ldots, n$.

Proof Due to the equalities in the lemma, by using Condition (c), we know that $M^*(i_0,0) = M^*(i',0)$. According to Lemma 2, the equalities in the lemma and $M^*(i_0,0) = M^*(i',0)$ together imply that $M^*(i_0, j) = M^*(i', j)$, $j = 0, 1, \ldots, n$. □

Summarising Lemmas 2 and 3, we conclude as follows.

Corollary 1 *Let a (t,n)-threshold scheme be weakly perfect. If* $\#\mathbf{K} = \#\mathbf{S}$ *then its defining matrix* M^* *has the following property. For any t given integers,* $0 \le j_1 < \cdots < j_t \le n$, *the submatrix* M' *of* M^*, *consisting of t columns indexed by* $j_1, \ldots, j_t$, *does not contain two identical rows.*

Proof We prove the corollary by contradiction. Assume that M' contains two identical rows then there exist integers i_0 and i' such that $i_0 \ne i'$ and $M^*(i_0, j_1) = M^*(i', j_1), \ldots, M^*(i_0, j_t) = M^*(i', j_t)$. According to Lemmas 2 and 3, $M^*(i_0, j) = M^*(i', j)$, $j = 0, 1, \ldots, n$. On the other hand, M^*, as a defining matrix of a secret sharing, does not contain two identical rows. The contradiction proves that all the rows of M' are mutually distinct. □

5 Properties of Weakly Perfect Threshold Schemes (II)

Weakly perfect threshold schemes have further properties.

Lemma 4 *Let a (t,n)-threshold scheme be weakly perfect. If* $\#\mathbf{K} = \#\mathbf{S}$ *then its defining matrix* M^* *has the following property. For any t given integers,* $1 \le j_1 < \cdots < j_t \le n$, *the submatrix* M' *of* M^*, *consisting of t columns indexed by* $j_1, \ldots, j_t$, *contains any given row vector* $(s_{j_1}, \ldots, s_{j_t})$ *where each* $s_j \in \mathbf{S}$.

Proof Let $\#\mathbf{K} = \#\mathbf{S} = b$. Write $\mathbf{K} = \{K_1, \ldots, K_b\}$ and $\mathbf{S} = \{\varepsilon_1, \ldots, \varepsilon_b\}$. Let M^* contain precisely m rows. Thus M^* be an $m \times (n+1)$ matrix. We index the rows of M^* by $1, \ldots, m$, and index the columns by $0, 1, \ldots, n$.

Consider the 1st row of M^*. Write $M^*(1,0) = K$, $M^*(1, j_1) = a_{j_1}$, ..., $M^*(1, j_{t-1}) = a_{j_{t-1}}$. Let M'' be the submatrix of M^*, consisting of $t+1$ columns indexed by $0, j_1, \ldots, j_t$. Let $\mathfrak{R}_i$, $i = 1, \ldots, b$, denote the subset of $\mathbf{S}$ such that $\varepsilon \in \mathfrak{R}_i$ if and only if $(K_i, a_{j_1}, \ldots, a_{j_{t-1}}, \varepsilon)$ is a row of M''.

From the proof of Lemma 2, we know that $\#\mathfrak{R}_i = 1$, $i = 1, \ldots, b$, and then it is easy to find that $\mathfrak{R}_1 \cup \cdots \cup \mathfrak{R}_b = \mathbf{S}$. Thus there exists some i_t with $1 \le i_t \le b$ such that $\mathfrak{R}_{i_t} = \{s_{j_t}\}$. By the definition of $\mathfrak{R}_{i_t}$, we know that $(K_{i_t}, a_{j_1}, \ldots, a_{j_{t-1}}, s_{j_t})$ is a row of M''.

Using the same arguments as above, we can prove that there exists some i_{t-1} with $1 \le i_{t-1} \le b$ such that $(K_{i_{t-1}}, a_{j_1}, \ldots, a_{j_{t-2}}, s_{j_{t-1}}, s_{j_t})$ is a row of M''.

Repeatedly, we can prove that there exists some i_1 with $1 \le i_1 \le b$ such that $(K_{i_1}, s_{j_1}, \ldots, s_{j_{t-2}}, s_{j_{t-1}}, s_{j_t})$ is a row of M''. Therefore we have proved that $(s_{j_1}, \ldots, s_{j_t})$ is a row of M'. □

Lemma 5 *Let a (t,n)-threshold scheme be weakly perfect. If* $\#\mathbf{K} = \#\mathbf{S}$ *then its defining matrix* M^* *has the following property. For any given* $t-1$ *integers,* $1 \le j_2 < \cdots < j_t \le n$, *the submatrix* M' *of* M^*, *consisting of t columns indexed by* $0, j_2, \ldots, j_t$, *contains any given row vector* $(K, s_{j_2}, \ldots, s_{j_t})$ *where* $K \in \mathbf{K}$ *and each* $s_j \in \mathbf{S}$.

Proof Let M_1 denote the $m \times (t-1)$ matrix, consisting of the $t-1$ columns of M^* indexed by $j_2,\dots,j_t$. According to Lemma 4, M_1 contains the row $(s_{j_2},\dots,s_{j_t})$. Due to Condition (d), M' contains a row $(K,s_{j_2},\dots,s_{j_t})$. □

Combining Lemmas 4 and 5, we get the following corollary.

Corollary 2 *Let a (t,n)-threshold scheme be weakly perfect. If $\#\mathbf{K} = \#\mathbf{S}$ then its defining matrix has the following property. For any given t integers, $0 \le j_1 < \cdots < j_t \le n$, the submatrix of M^*, consisting of t columns indexed by $j_1,\dots,j_t$, contains any given row vector $(s_{j_1},\dots,s_{j_t})$ (when $j_1 > 0$) and any given row vector $(K,s_{j_2},\dots,s_{j_t})$ (when $j_1 = 0$), where each $s_j \in \mathbf{S}$ and $K \in \mathbf{K}$.*

6 Characteristic Properties of Ideal Threshold Schemes

Combing Corollaries 1 and 2, we formulate the following statement.

Theorem 1 *Let a (t,n)-threshold scheme be weakly perfect. If $\#\mathbf{K} = \#\mathbf{S}$ then its defining matrix M^* has the following property. For any given t integers, $0 \le j_1 < \cdots < j_t \le n$, the submatrix of M^*, consisting of t columns indexed by $j_1,\dots,j_t$, contains any given row vector $(s_{j_1},\dots,s_{j_t})$ (when $j_1 > 0$) and any given row vector $(K,s_{j_2},\dots,s_{j_t})$ (when $j_1 = 0$), where each $s_j \in \mathbf{S}$ and $K \in \mathbf{K}$, precisely once.*

We can prove the converse of Theorem 1. However we have a stronger statement as follows.

Theorem 2 *Let a defining matrix M^* of a (t,n)-threshold scheme satisfy the following property. For any given t integers, $0 \le j_1 < \cdots < j_t \le n$, the submatrix of M^*, consisting of t columns indexed by $j_1,\dots,j_t$, contains any given row vector $(s_{j_1},\dots,s_{j_t})$ (when $j_1 > 0$) and any given row vector $(K,s_{j_2},\dots,s_{j_t})$ (when $j_1 = 0$), where each $s_j \in \mathbf{S}$ and $K \in \mathbf{K}$, precisely once. Then (i) the scheme is strongly perfect, (ii) $\#\mathbf{K} = \#\mathbf{S}$, and then the scheme is ideal.*

Proof

(i) Let $\{P_{j_1},\dots,P_{j_\ell}\}$ be the set of currently active participants. We first verify Condition (c). Let $\ell \ge t$. If $M^*(i,j_1) = M^*(i',j_1),\dots,M^*(i,j_\ell) = M^*(i',j_\ell)$, due to the property of M^*, it follows that $i = i'$. Clearly (c) is satisfied.

We next verify Condition (d'). Let $\ell < t$ and M_1 denote the submatrix of M^*, consisting of the $\ell+1$ columns of M^* indexed by 0, j_1, …, j_ℓ. Let $K \in \mathbf{K}$ and $s_{j_1},\dots,s_{j_\ell} \in \mathbf{S}$. Since $\ell < t$, we know that $1+\ell \le t$. There are two cases to be considered: $1+\ell < t$ and $1+\ell = t$

Case 1: $1+\ell < t$.
Then $t-\ell \ge 2$ and then there are $t-\ell-1 (>0)$ integers, $1 \le j_{\ell+1} < \cdots < j_{t-1} \le n$, such that $\{j_{\ell+1},\dots,j_{t-1}\} \cap \{j_1,\dots,j_\ell\} = \emptyset$. Without loss of generality, we assume that $j_\ell < j_{\ell+1} < \cdots < j_{t-1}$. Let M_2 denote the submatrix of M^*, consisting of t columns of M^* indexed by 0, j_1, …, j_ℓ, $j_{\ell+1}$, …, j_{t-1}. According to the property of M^*, for any given $a_{j_{\ell+1}},\dots,a_{j_{t-1}} \in \mathbf{S}$, M_2 contains $(K,s_{j_1},\dots,s_{j_\ell},a_{j_{\ell+1}},\dots,a_{j_{t-1}})$ precisely once. Since $(a_{j_{\ell+1}},\dots,a_{j_{t-1}})$ has precisely $b^{t-\ell-1}$ different choices, we know that M_1, as a submatrix of M_2, contains the row $(K,s_{j_1},\dots,s_{j_\ell})$ precisely $b^{t-\ell-1}$ times. Clearly the value of $b^{t-\ell-1}$ is independent to the choice of K. We have verified condition (d') in Case i1.

Case 2: $1+\ell=t$.
According to the property of M^*, M_1 contains the row $(K, s_{j_1}, \ldots, s_{j_\ell})$, where $\ell = t-1$, precisely once. Thus condition (d') is satisfied in Case i2.

Summarising cases i1 and i2, we conclude that the scheme is strongly perfect. (i) has been proved.

(ii) Let M' be the submatrix of M^*, consisting of t columns indexed by $1, \ldots, t$, M_0 be the submatrix of M^*, consisting of t columns indexed by $0, 1, \ldots, t-1$, and M'_0 be the submatrix of M^*, consisting of $t-1$ columns indexed by $1, \ldots, t-1$. We fix $a_1, \ldots, a_{t-1} \in \mathbf{S}$. Due to the property of M^*, for each $s \in \mathbf{S}$, M' contains the row $(a_1, \ldots, a_{t-1}, s)$ precisely once. Thus M'_0 contains the row $(a_1, \ldots, a_{t-1})$ precisely $\#\mathbf{S}$ times. On the other hand, due to the property of M^*, for each $K \in \mathbf{K}$, M_0 contains the row $(K, a_1, \ldots, a_{t-1})$ precisely once. Thus M'_0 contains the row $(a_1, \ldots, a_{t-1})$ precisely $\#\mathbf{K}$ times. It follows that $\#\mathbf{K} = \#\mathbf{S}$. We have proved (ii).

By definition, (i) and (ii) together imply that the scheme is ideal. □

Theorem 3 *For a (t,n)-threshold scheme, the following statements are equivalent:*

(i) the scheme is ideal,

(ii) the scheme is weakly perfect and $\#\mathbf{K} = \#\mathbf{S}$,

(iii) the scheme is strongly perfect and $\#\mathbf{K} = \#\mathbf{S}$,

(iv) its defining matrix M^* has the following property. For any given t integers, $0 \le j_1 < \cdots < j_t \le n$, the submatrix of M^*, consisting of t columns indexed by $j_1, \ldots, j_t$, contains any given row vector $(s_{j_1}, \ldots, s_{j_t})$ (when $j_1 > 0$) and any given row vector $(K, s_{j_2}, \ldots, s_{j_t})$ (when $j_1 = 0$), where each $s_j \in \mathbf{S}$ and $K \in \mathbf{K}$, precisely once.

Proof According to Theorem 1, (ii) implies (iv). Due to Theorem 2, (iv) implies (i). By definition, (i) implies (iii). It is obvious that (iii) implies (ii). The proof is completed. □

From Lemma 1, $\#\mathbf{K} \le \#\mathbf{S}$ holds for any weakly perfect threshold scheme. Thus due to Theorem 3, ideal threshold schemes are a critical case of weakly perfect threshold schemes when $\#\mathbf{K} = \#\mathbf{S}$. Therefore it is interesting that "strongly perfect" in Definition 3 can be replaced by "weakly perfect".

From (iv) of Theorem 3, we formulate the following conclusion:

Corollary 3 *A defining matrix of any ideal (t,n)-threshold scheme has the size $b^t \times (n+1)$ where $b = \#\mathbf{K} = \#\mathbf{S}$. In other words, any ideal (t,n)-threshold scheme has precisely b^t possible shares vectors.*

7 Other Properties with Applications

From the proof of Theorem 2, we know

Corollary 4 *If a (t,n)-threshold scheme is ideal then its defining matrix M^* has the following property. For any ℓ $(0 < \ell \le t)$ integers, $0 \le j_1 < \cdots < j_\ell \le n$, the submatrix of M^*, consisting of ℓ columns indexed by $j_1, \ldots, j_\ell$, contains all b^ℓ possible rows each precisely $b^{t-\ell}$ times, where $\#\mathbf{K} = \#\mathbf{S} = b$. In particular, the jth ($j = 1, \ldots, n$) column of M^* contains all elements in $\mathbf{S}$ each precisely b^{t-1} times, and the 0th column of M^* contains all elements in $\mathbf{K}$ each precisely b^{t-1} times.*

Corollary 5 *If a (t,n)-threshold scheme is ideal then its defining matrix M^* has the following property. Any two row vectors of M^* are the same in at most $t-1$ corresponding coordinates, or equivalently, any two row vectors of M^* differ in at least $n-t+2$ corresponding coordinates.*

Proof Due to Theorem 3, M^* is a $b^t \times (n+1)$ matrix, where $\#\mathbf{K} = \#\mathbf{S} = b$. Let i' and i_0 be two integers with $1 \le i_0 < i' \le b^t$. Then the i_0th row vector of M^* is $(M^*(i_0,0), M^*(i_0,1), \ldots, M^*(i_0,n))$, and the i'th row vector of M^* is $(M^*(i',0), M^*(i',1), \ldots, M^*(i',n))$. According to (iv) of Theorem 3, there exist at most $t-1$ integers, $0 \le j_1 < \cdots < j_{t-1} \le n$, $M^*(i_0,j_1) = M^*(i',j_1), \ldots, M^*(i_0,j_{t-1}) = M^*(i',j_{t-1})$. In other words, the i_0th row vector and the i'th row vector differ in at least $n-t+2$ coordinates. □

The next corollary immediately follows Corollary 5.

Corollary 6 *Let M^* be a defining matrix of an ideal (t,n)-threshold scheme, ℓ be any integer with $t \le \ell \le n$ and M_1 be any $b^t \times \ell$ submatrix of matrix M^* where $b = \#\mathbf{K} = \#\mathbf{S}$. Then any two row vectors of M_1 are the same in at most $t-1$ corresponding coordinates, or equivalently, any two row vectors of M_1 differ in at least $\ell - t + 1$ corresponding coordinates.*

In this section we show an application of Corollary 6. Consider an ideal (t,n)-threshold scheme with its defining matrix M^* and associated matrix M. Assume that the dealer chooses the i_0th row vector $(s_1,\ldots,s_n)$ of M and assigns $s_1,\ldots,s_n$ to participants $P_1,\ldots,P_n$, respectively. Let $\{P_{j_1},\ldots,P_{j_\ell}\}$ with $t \le \ell \le n$ be a subset of active participants. Let M_1 be the $b^t \times \ell$ submatrix of M, consisting of ℓ columns indexed by $j_1,\ldots,j_\ell$.

Denote the ith row vector of M_1 by L_i. Clearly, the row i_0 of M_1 is $L_{i_0} = (s_{j_1},\ldots,s_{j_\ell})$. Let there exist u cheaters, among the active participants $P_{j_1}, \ldots, P_{j_\ell}$, who submit modified shares to the combiner while the honest active participants submit correct shares to the combiner. Assume that the combiner receives the shares $s'_{j_1},\ldots,s'_{j_\ell}$ sent by $P_{j_1},\ldots,P_{j_\ell}$, where $s'_{j_i} = s_{j_i}$ if and only if P_{j_i} is honest. Write $L' = (s'_{j_1},\ldots,s'_{j_\ell})$. Clearly, $dist(L',L_{i_0}) = u$, where $dist(X,Y)$ denotes the number of coordinates in which vectors X and Y differ. We call $dist(X,Y)$ the *Hamming distance* between vectors X and Y.

Let $u \le \ell - t$. Set $d_m = \min\{dist(L',L_i) \mid 1 \le i \le b^t\}$. We first prove that $u = 0$ if and only if $d_m = 0$. The necessity is obvious. We next prove the sufficiency. Let $d_m = 0$. We now prove that $u = 0$ by contradiction. Assume that $u \ne 0$. Clearly $d_m = 0$ implies that L' must be identical with a row of M_1. Thus $L' = L_{i_1}$ for some i_1. Since $u \ne 0$, $i_1 \ne i_0$. According to Corollary 6, $dist(L',L_{i_0}) = dist(L_{i_1},L_{i_0}) \ge \ell - t + 1$. This contradicts the fact that $dist(L',L_{i_0}) = u \le \ell - t$. The contradiction proves that $u = 0$. Therefore, in the case of $u \le \ell - t$, the combiner (recovery algorithm) calculates d_m, then it can conclude that $L' = (s'_{j_1},\ldots,s'_{j_\ell})$ is correct or incorrect (i.e. $u = 0$ or $u \ne 0$) according to $d_m = 0$ or $d_m \ne 0$.

We further indicate that the correct shares can be found and the cheaters can be identified when $1 \le u \le \lfloor \frac{1}{2}(\ell - t) \rfloor$, where $\lfloor \frac{1}{2}(\ell - t) \rfloor$ denotes the greatest integer not larger than $\frac{1}{2}(\ell - t)$. The combiner can find a row L_{i_2} of M_1 such that $dist(L',L_{i_2}) = d_m$ where d_m has been defined in this section. We now prove that L_{i_2} is identical with $L_{i_0} = (s_{j_1},\ldots,s_{j_\ell})$. Assume otherwise, then $L_{i_2} \ne L_{i_0}$. Since both L_{i_0} and L_{i_2} are rows of M_1, due to Corollary 6, $dist(L_{i_2},L_{i_0}) \ge \ell - t + 1$. On the other hand, $dist(L_{i_2},L_{i_0}) \le dist(L_{i_2},L') + dist(L',L_{i_0}) \le d_m + u \le 2u \le \ell - t$. This contradicts the fact that $dist(L_{i_2},L_{i_0}) \ge \ell - t + 1$. The contradiction proves that $L_{i_2} = L_{i_0}$. Thus the correct vector $L_{i_2} = L_{i_0} = (s_{j_1},\ldots,s_{j_\ell})$ has been found. Comparing L' with L_{i_0} (i.e. L_{i_2}), the combiner (recovery algorithm) can determine who are cheaters.

It should be noted that such ability of ideal threshold schemes in cheating prevention is not based on particular constructions or particular descriptions.

8 More Characteristic Properties

If we simplify the condition $\#\mathbf{S} = \#\mathbf{K}$ by $\mathbf{S} = \mathbf{K}$, the properties of ideal threshold schemes will be more interesting.

Orthogonal arrays were introduced more than fifty years ago as a combinatorial problem (Bus52).

Definition 4 *An $m \times n$ matrix O with entries from b-set $\mathbf{B}$ is called an* orthogonal array*, denoted by (m,n,b,t), if any $m \times t$ submatrix of O contains all b^t possible row vectors each precisely λ times.*

Clearly $m = \lambda b^t$. The parameters m, t and λ are called the *size*, the *strength* and the *index* of the orthogonal array, respectively, while n is called the number of *constraints* and b is called the number of *levels*.

Lemma 6 *An orthogonal array (m,n,b,t) with an index λ is an orthogonal array (m,n,b,ℓ) with an index $\lambda b^{t-\ell}$ where ℓ is any integer with $1 \leq \ell \leq t$.*

In particular, we can formulate the following corollary.

Corollary 7 *Each column of an orthogonal array (m,n,b,t) with entries from a b-set $\mathbf{B}$ contains each element of $\mathbf{B}$ precisely λb^{t-1} times, where λ is the index of the orthogonal array.*

Lemma 7 *Let O_1 be an $m \times n_1$ submatrix of an orthogonal array (m,n,b,t) with an index λ. If $n_1 \geq t$ then O_1 is an orthogonal array (m,n_1,b,t) with an index λ.*

In particular, orthogonal arrays with index $\lambda = 1$ are used in this work.

Definition 5 *An orthogonal array with index $\lambda = 1$, i.e, an orthogonal array (b^t,n,b,t) is called an orthogonal array (b^t,n,b,t) of* index unity.

Orthogonal arrays (b^t,n,b,t) of index unity have many interesting properties. The following bounds on the number of constraints for orthogonal arrays (b^t,n,b,t) were proved by Bush (Bus52):

Lemma 8 *For an orthogonal array (b^t,n,b,t) of index unity, we have*

(i) if $t \leq b$ and b is even then $n \leq b+t-1$,

(ii) if $t \leq b$, b is odd and $t \geq 3$ then $n \leq b+t-2$,

(iii) if $t \geq b$, then $n \leq t+1$.

According to (iv) of Theorem 3, a defining matrix of an ideal (t,n)-threshold scheme with $\mathbf{K} = \mathbf{S}$, is an orthogonal array $(b^t,n+1,b,t)$ of index unity.

We next briefly recall the concept of codes. Let $\mathbf{B} = \{\varepsilon_1,\ldots,\varepsilon_b\}$ be a finite set and $\mathbf{B}^n$ be the set of all strings of length n over $\mathbf{B}$. Any nonempty subset $\Im$ of $\mathbf{B}^n$ is called a b-ary *block code*. Each string in $\Im$ is called a *codeword*. The parameter n is called the *length*. If $\min\{dist(\xi,\eta) \mid \xi,\eta \in \Im, \xi \neq \eta\} = d$, where $dist(\xi,\eta)$ denotes the Hamming distance between ξ and η, and $\#\Im = R$, then the code $\Im$ is called an $(n,R,d)_b$ *code*.

Definition 6 *Let $N_b(n,d)$ be the largest number R such that there exists an $(n,R,d)_b$ code. An $(n,R,d)_b$ code satisfying $R = N_b(n,d)$ is called* optimal *(Rom92).*

For any $(n,R,d)_b$ code, the following inequality holds and it is known as the *Singleton bound* (MS78), (PH98), (Rom92),

$$N_b(n,d) \le b^{n-d+1} \tag{3}$$

Lemma 9 *A $b^t \times n$ matrix O with entries from b-set* **B** *is an orthogonal array (b^t,n,b,t) of index unity if and only if all the b^t row vectors of O form an $(n,b^t,n-t+1)_b$ (optimal) code.*

Proof We first indicate that an $(n,b^t,n-t+1)_b$ code $\mathfrak{I}$ must be optimal. In fact, $\#\mathfrak{I} = b^t$ and $d = n-t+1$. Thus $\#\mathfrak{I} = b^{n-d+1}$. According to (3), we have $b^{n-d+1} = \#\mathfrak{I} \le N_b(n,d) \le b^{n-d+1}$. Thus $\#\mathfrak{I} = N_b(n,d)$ and thus we have proved that $(n,b^t,n-t+1)_b$ code is optimal.

We now prove the necessity of the lemma. Assume that O is an orthogonal array (b^t,n,b,t) of index unity. It is easy to verify that any two rows of O are the same in at most $t-1$ corresponding coordinates. In other words, any two rows of O differ in at least $n-t+1$ corresponding coordinates. Thus all the b^t row vectors of O form an $(n,b^t,d)_b$ code $\mho$ where $d \ge n-t+1$. On the other hand, from (3), we have $b^t = \#\mho \le N_b(n,d) \le b^{n-d+1}$ and then $t \le n-d+1$. From $t \le n-d+1$ and $d \ge n-t+1$, we conclude that $d = n-t+1$. This proves that $\mho$ is an $(n,b^t,n-t+1)_b$ code. We next prove the sufficiency of the lemma. Assume that all the b^t rows of matrix O form an $(n,b^t,n-t+1)_b$ code. Then the Hamming distance between any two distinct row vectors is at least $n-t+1$, in other words, any two distinct row vectors are the same in at most $t-1$ coordinates. Therefore, all the b^t row vectors of any $b^t \times t$ submatrix O_1 of O are mutually distinct, in other words, O_1 contains all b^t possible row vectors each precisely once. This proves that O is an orthogonal array (b^t,n,b,t) of index unity. □

Theorem 12 in Chapter 11 of (MS78) is a special case of Lemma 9 when both orthogonal array and code are linear. This implies that the entries in both array and code should be certain algebraic elements. Also the proof is based on coding theory. In contrast, Lemma 9 is more general and its proof does not require the set **B** to have any algebraic properties.

There exist many known optimal codes, for instance, cyclic codes of prime length, (some) global quadratic residue codes, Reed-Solomon codes, and more generally, MDS codes. The detailed description of such codes can be found from (MS78), (PH98), (Rom92). It should be noted that an optimal code is not necessarily an MDS code, as an MDS code is a special optimal code when all its codewords form a linear space. This requires the elements in the set **B** to have certain algebraic properties.

Lemma 10 *There exists an ideal (t,n)-threshold scheme if and only if there exists an orthogonal array $(b^t,n+1,b,t)$ of index unity where $b = \#\mathbf{K} = \#\mathbf{S}$.*

Proof Due to (iv) of Theorem 3, the sufficiency is obvious. We only need to prove the necessity. Assume that there exists an ideal (t,n)-threshold scheme. Since $\#\mathbf{S} = \#\mathbf{K}$, there exists a mapping χ from **K** to **S** such that $\chi(\mathbf{K}) = \mathbf{S}$, and $\chi(k') \ne \chi(k'')$ if $k' \ne k''$. Thus we obtain a new ideal threshold scheme from the given one by changing each k to $\chi(k)$. We note that in the new ideal threshold scheme the set of secrets is identical with the set of shares. According to (iv) of Theorem 3, any defining matrix M^* of the new scheme is an orthogonal array $(b^t,n+1,b,t)$. □

According to Theorem 3, Lemma 9 and Lemma 10, we can state as follows.

Theorem 4 *The following statements are equivalent:*

(i) there exists an ideal (t,n)-threshold scheme,

(ii) there exists a weakly perfect threshold scheme with $\#\mathbf{K} = \#\mathbf{S}$*,*

(iii) there exists a strongly perfect threshold scheme with $\#\mathbf{K} = \#\mathbf{S}$*,*

(iv) there exists an orthogonal array $(b^t, n+1, b, t)$ *of index unity where* $b = \#\mathbf{K} = \#\mathbf{S}$*,*

(v) there exists an $(n+1, b^t, n-t+2)_b$ *(optimal) code.*

According to Theorem 4, the existence of orthogonal arrays and the existence of optimal codes ensure the existence of ideal threshold schemes. Theorem 4 is helpful for us to examine ideal threshold schemes from different points of view.

9 On Parameters of Ideal Threshold Schemes

According to Lemma 8 and Theorem 4, there are some bounds on the parameters of ideal threshold schemes.

Theorem 5 *Ideal* (t, n)*-threshold schemes exist only when*

(i) $n \le b + t - 2$ *where* $\#\mathbf{S} = \#\mathbf{K} = b \ge t$ *is even, or*

(ii) $n \le b + t - 3$ *where* $b \ge t$ *is odd and* $t \ge 3$*, or*

(iii) $n = t$ *where* $b \le t$*.*

Proof Assume that there exists an ideal (t, n)-threshold scheme. From Theorem 4, there exists an orthogonal array $(b^t, n+1, b, t)$ of index unity where $b = \#\mathbf{K} = \#\mathbf{S}$. By using Lemma 8, it is easy to verify (i) and (ii). For the case of $b \le t$, by using Lemma 8, we know that $n + 1 \le t + 1$ i.e. $n \le t$. On the other hand, for a (t, n)-threshold scheme, we always have $t \le n$. Therefore we conclude that $n = t$ and then (iii) is true. □

We note that $n \ge t$ always holds. However we usually need (t, n)-threshold schemes with $n > t$. According to Theorem 5, for clarity, we state as follows.

Corollary 8 *Ideal* (t, n)*-threshold schemes with* $n > t$ *exist only when* $b > t$ *where* $\#\mathbf{S} = \#\mathbf{K} = b$*.*

10 Remarks

We now compare this work with other previous results.

A characterisation of perfect threshold schemes can be found from (SV88). More precisely, (SV88) proved that there exists a perfect (t, w)-threshold scheme with v shares and m secrets if and only if there exist m mutually t-compatible w-uniform hypergraphs on v points. It is not hard to verify that the "perfect" defined in (SV88) is equivalent to the "strongly perfect", or more briefly the "perfect", defined in (BS92). A basic difference between this work and (SV88) is that in this paper we work on characterisations of *ideal* threshold schemes.

All the results on ideal threshold schemes discussed in (PZ02) depend on a particular description of schemes by orthogonal arrays. However this does not automatically mean that these results are available for all ideal threshold schemes. To do so, it should be proved that the existence of orthogonal arrays is necessary for the existence of ideal threshold schemes. This needs much more work as done in this paper.

11 Conclusions

We have found a series of properties of weakly perfect threshold schemes. Based on this, we have derived a number of necessary and sufficient conditions for ideal threshold schemes from different approaches. Therefore we have examined ideal threshold schemes from new points of view and obtained new results on ideal threshold schemes.

References

[BD91] E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology*, 4:123–134, 1991.

[Bla79] G. R. Blakley. Safeguarding cryptographic keys. In *Proceedings of AFIPS 1979 National Computer Conference*, pages 313–317, 1979.

[BS92] E. F. Brickell and D.R. Stinson. Some improved bounds on information rate of perfect sharing schemes. *Journal of Cryptology*, 5:153–166, 1992.

[Bus52] K. A. Bush. Orthogonal arrays of index unity. Annals of Mathematical Statistics, 23:426–434, 1952.

[ISN87] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. In *Proceedings IEEE Globecom '87*, pages 99–102, 1987.

[MS78] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, New York, Oxford, 1978.

[PH98] V. C. Pless and W. C. Huffman. *Handbook of Coding Theory*. Elsevier Science B. V., 1998.

[PZ02] J. Pieprzyk and X. M. Zhang. Ideal threshold schemes from orthogonal arrays. In *4th International Conference on Information and Communication Security (ICICS 2002)*, volume 2513 of *Lecture Notes in Computer Science*, pages 469–479. Springer-Verlag, Berlin, Heidelberg, New York, 2002.

[Rom92] S. Roman. *Coding and information theory*. Springer-Verlag, Berlin, Heidelberg, New York, 1992.

[Sha79] A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.

[SV88] D. Stinson and S. A. Vanstone. A combinatorial approach to threshold schemes. *SIAM Journal on Discrete Mathematics*, 1:230–236, 1988.