数理解析研究所講究録
第 853 巻 1993 年 80-87

Secret Sharing Schemes and Combinatorial Designs

Youjin SONG 宋 裕鎮   Shigeo TSUJII 辻井 重男

Department of Electrical and Electronic Engineering,
Tokyo Institute of Technology
2-12-1 O-okayama Meguro-ku Tokyo, 152, JAPAN

Abstract

If there are participants involved in a group wanting to recover a secret, then how can we share the secret? The purpose of this paper is to propose ideal threshold schemes in terms of combinatorial designs. We associate our scheme with threshold scheme expressed as a matrix and investigate the combinatorial properties of ideal schemes with threshold access structure. It is shown that their existence is equivalent to the existence of combinatorial designs. Also, assuming the existence of ideal schemes, we show the condition for the number of blocks of ideal schemes to be expressed by the cardinality of the divisible group.

keyword : threhold scheme, secret sharing, block design, matroid

1. Introduction and Terminology

Informally, a secret sharing scheme is a method of sharing a secret S among a finite set of participants in such a way that certain authorized subsets of participants can compute a secret S. The purpose of this paper is to propose ideal threshold schemes in terms of combinatorial designs. Also, assuming the existence of ideal scheme, we show the condition for the number of blocks of ideal schemes to be expressed by the cardinality of the divisible group.

Let $W \triangleq \{S, V_1, \cdots, V_n\}$. S is called a secret and V_i is called the share of the participant P_i.

Definition 1 *$(\mathcal{M}, S, V)$ is a secret sharing scheme (SS) if $\mathcal{M}$ is a mapping: $S \times R \longrightarrow V_1 \times V_2 \times \cdots \times V_n$, where R is a set of random inputs.*

Usually, access structures are defined as a subset of 2^P. For convenience, we define them as a subset of 2^V. We use P_i and V_i interchangeably. The set $\Gamma \subseteq 2^{\mathcal{P}}(2^{\mathcal{P}}$ is the collection of all subsets of $\mathcal{P})$ is a monotone access structure if whenever $A \in \Gamma$, for any set $A \subseteq B, A \neq B$ we have $B \in \Gamma$. If Γ consists of all subsets of $\mathcal{P}$ of at least some fixed size t, then we refer to Γ as the $(t, |P|)$-threshold access structure$(|P| \triangleq w)$. The set of minimal authorized subsets of Γ is denoted Γ_o. Γ_o uniquely determines Γ and conversely. Let $\mathcal{P}^c = \{p \in \mathcal{P} | \text{there exists} A \in \Gamma_o \text{ with } p \in A\}$. So $\mathcal{P}^c$ contains those participants p such that there exists $A \in \Gamma$ with $(A \backslash p) \notin \Gamma$. We say that Γ is connected if $\mathcal{P}^c = \mathcal{P}$. Let Γ be a montone access structure defined on participant set $\mathcal{P}$ and let q be a positive integer. A perfect secret sharing scheme is a matrix $\mathcal{M}[BD91][BS92]$ such that

(a) $|S(p_0)| = q$

(b) If $A \in \Gamma$ then $A \rightarrow p_0$

(c) If $A \notin \Gamma$ then $A \not\rightarrow p_0$

We say that $\mathcal{M}$ is connected if Γ is connected. If Γ is a threshold access structure then we refer to $\mathcal{M}$ as threshold scheme. Note that $|S(\mathcal{P} \cup p_0)| \geq q$ for all $p \in \mathcal{P}^c$. With this in mind we define the information rate,ρ, of $\mathcal{M}$ by

$$\rho = \frac{log_2 q}{\frac{1}{|\mathcal{P}^c|} \sum_{p \in \mathcal{P}^c} log_2 |S(p)|}.$$

We denote such a scheme by $PS(\Gamma, \rho, q)$. Note that $0 < \rho \leq 1$ and$\rho = 1$ if and only if $|S(\mathcal{P} \cup p_0)| = q$ for all $p \in \mathcal{P}^c$. It is known that $|V_i| \geq |S|$ in $PS(\Gamma, \rho, q)[BD91][BS92]$. where $|V_i|$ is the size of the share and $|S|$ is the size of the secret. A $PS(\Gamma, \rho, q)$ such that $|V_i| = |S|$ is called ideal. $[BD91]$ showed that every ideal scheme has a matroid structure on W by using a combinatorial argument. If $\rho = 1$ then secret sharing scheme $\mathcal{M}$ is said to be ideal.

Definition 2 *A (finite) incidence structure* $\mathbf{V}$ *is a triple* $(\mathbf{V}, \mathbf{B}, \mathbf{I})$ *which consists of two finite, nonempty and disjoint sets* $\mathbf{V}$ *and* $\mathbf{B}$ *and a subset* $\mathbf{I} \subseteq \mathbf{P} \times \mathbf{B}$. *The elements of* $\mathbf{I}$ *are called flags while those of* $\mathbf{V}$ *and* $\mathbf{B}$ *are referred to as points and lines respectively.* $\mathbf{I}$ *is called the incidence relation. We say that a point x and a line L are incident with each other and write $x \in L$ if and only if (x, L) is a flag.*

Definition 3 *A $t-(v, k, \lambda)$ design D (or, briefly a t-design) consists of a set of points and a set of blocks such that the following properties hold:*

(a) *D has v points.*

(b) *Every block of D consists of exactly k points.*

(c) *through any t points of D, there are exactly λ blocks.*

The five constants (v, b, r, k, λ) are called the parameters of the block design $(\mathbf{V}, \mathbf{B})$. In this paper, we will use the letters v, b, r, k and λ for the parameters unless stated otherwise.

For the definition of block design, see the Appendix and also for the theory of block design, see reference [$HP85$].

2. Basic Results on Ideal Scheme

In this section we briefly introduce basic results on ideal schemes[$BD91$][$BS92$][$SV87$].

Result 1 *Let $\mathcal{M}$ be a $PS(\Gamma, 1, q)$. Then every distinct row of $\mathcal{M}$ occurs precisely λ times, for some $\lambda \geq 1$.*

for some $\rho \leq 1$. Then the number of distinct rows of $\mathcal{N}$ is at least equal to the number of distinct rows of $\mathcal{M}$.

Result 2 *Let $\mathcal{D}$ be a $TD_1(t, w+1, q)$. Then there exists $\mathcal{M}$, a $PS(\Gamma, 1, q)$, where Γ is the (t, w)-threshold access structure.*

Result 3 *Let $\mathcal{M}$ be a $PS(\Gamma, 1, q)$, where Γ is the (t, w)-threshold access structure. Then there exists $\mathcal{D}$ a $TD_1(t, w+1, q)$.*

3. Ideal Threshold Schemes and Designs

In this section we look at the relationship between ideal threshold schemes and a class of block designs called GD, ARBIBD, and Steiner System.

3.1 Ideal scheme and design

Lemma 1 *A t-design can be constructed from finite geometry D.*

Proof: Consider the collection of subsets of B and the set of $\mathcal{P}$ on the d-dimensional vector space over the finite field $GF(q)$. Let G be a t-transitive multiply group on the set $\mathcal{P}$. We take t points $x_1, \cdots, x_t$ and a subset B of $\mathcal{P}$ including all that. That is, assume that there are λ blocks including distinct points $x_1, \cdots, x_t$ and let their blocks be $f_1(B) = B, f_2(B) = B, \cdots, f_\lambda(B) = B$. Now, If $y_1, \cdots, y_t$ are t points taken from set $\mathcal{P}$ arbitrarily, then there is a element g of G which moves $x_1, \cdots, x_t$ to $y_1, \cdots, y_t$ preserving their order. If we call the set $f_i(B)(f_i \in G)$ which is a mapping of B by using a element g of G as a block, then $gf_1(B), gf_2(B), \cdots, gf_\lambda(B)$ are blocks including $y_1, \cdots, y_t$. When the above is done while assuming that the number of elements of $\mathcal{P}$ is v and the number of elements of B is k, $(\mathcal{P}, \mathcal{B})$ is a $t-(v,k,\lambda)$ design consisting of the set $\mathcal{B} = \{gf_i(B) | gf_i \in G, i = 1, \cdots, \lambda\}$. Considering the elements of a set $\mathcal{B}$ as lines and elements of a set $\mathcal{P}$ as points, we can construct a $t-(v,k,\lambda)$ design from finite geometry D

Theorem 1 *If an element of a block occurs as the same numbers, then an ideal scheme $PS(\Gamma, 1, q)$ exists on the d-dimensional vector space over $GF(q)$.*

Proof: Let d be an integer and we assume the existence of $t-(v,k,\lambda)$design from Lemma1. An ideal condition for $\mathcal{M}$ is to have the same numbers q in each column. In terms of block design, this means that an element of a block in the corresponding design $\mathcal{D}$ occurs with the same frequency. (In such design, each element occurs in r blocks); As a result, an ideal scheme $PS(\Gamma, 1, q)$ exists.

3.2 Examples

Let us illustrate ideal schemes by some simple examples.

Example 1 *Let Γ be the $(2,2)$-threshold structure defined on participants set $\mathcal{P} = \{a, b\}$. Then $\mathcal{M}$ is a $PS(\Gamma, 1, 5)$ and $\mathcal{D}$ is the equivalent to GD(3,1,3;9).*

$$\mathcal{M} = \left(\begin{array}{ccc} p_0 & a & b \\ 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 3 & 3 \\ 1 & 2 & 3 \\ 1 & 1 & 4 \\ 2 & 2 & 2 \\ 2 & 3 & 4 \\ 3 & 2 & 1 \\ 4 & 4 & 4 \end{array}\right) \quad \mathcal{D} = \begin{array}{c} \{1\ 2\ 3\} \\ \{1\ 4\ 7\} \\ \{1\ 6\ 8\} \\ \{2\ 5\ 8\} \\ \{2\ 4\ 9\} \\ \{3\ 5\ 7\} \\ \{3\ 6\ 9\} \\ \{4\ 5\ 6\} \\ \{7\ 8\ 9\} \end{array} \tag{1}$$

Example 2 *Let Γ be the $(2,2)$-threshold structure defined on participants set $\mathcal{P} = \{a, b\}$. Then $\mathcal{M}$ is a $PS(\Gamma, 1, 3)$ and $\mathcal{D}$ is the equivalent to OA(3,1;3)*

$$\mathcal{M} = \left(\begin{array}{ccc} p_0 & a & b \\ 2 & 1 & 1 \\ 2 & 2 & 2 \\ 2 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 2 & 1 \\ 1 & 0 & 2 \end{array}\right) \quad \mathcal{D} = \begin{array}{lll} \{1 & 4 & 7\} \\ \{1 & 5 & 8\} \\ \{1 & 6 & 9\} \\ \{2 & 4 & 8\} \\ \{2 & 5 & 9\} \\ \{2 & 6 & 7\} \\ \{3 & 4 & 9\} \\ \{3 & 5 & 7\} \\ \{3 & 6 & 8\} \end{array} \tag{2}$$

Example 3 *Let* Γ *be the* $(2,3)$*-threshold structure defined on participants set* $\mathcal{P} = \{a, b, c\}$. *Then* $\mathcal{M}$ *is a* $PS(\Gamma, 1, 7)$ *and* $\mathcal{D}$ *is the equivalent to ARBIBD(4,4,1).*

$$\mathcal{M} = \left(\begin{array}{cccc} p_0 & a & b & c \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 3 & 6 \\ 0 & 3 & 4 & 4 \\ 1 & 2 & 2 & 4 \\ 1 & 1 & 4 & 5 \\ 1 & 4 & 3 & 3 \\ 2 & 1 & 2 & 6 \\ 2 & 3 & 3 & 5 \\ 2 & 4 & 1 & 4 \\ 3 & 2 & 1 & 5 \\ 3 & 3 & 2 & 3 \\ 3 & 4 & 4 & 6 \\ 4 & 2 & 5 & 1 \\ 5 & 5 & 3 & 2 \\ 6 & 6 & 6 & 6 \end{array}\right) \quad \mathcal{D} = \begin{array}{llll} \{1 & 2 & 3 & 4\} \\ \{1 & 5 & 9 & 13\} \\ \{1 & 6 & 11 & 16\} \\ \{1 & 7 & 12 & 14\} \\ \{2 & 6 & 10 & 14\} \\ \{2 & 5 & 12 & 15\} \\ \{2 & 8 & 11 & 13\} \\ \{3 & 5 & 10 & 16\} \\ \{3 & 7 & 11 & 15\} \\ \{3 & 8 & 9 & 14\} \\ \{4 & 6 & 9 & 15\} \\ \{4 & 7 & 10 & 13\} \\ \{4 & 8 & 12 & 16\} \\ \{5 & 6 & 7 & 8\} \\ \{9 & 10 & 11 & 12\} \\ \{13 & 14 & 15 & 16\} \end{array} \tag{3}$$

4. The Number of Blocks in Ideal Schemes

In this section we show the condition for the number of blocks of ideal schemes to be expressed by the cardinality of the divisible group.

Theorem 2 *The number of blocks of ideal scheme* $PS(\Gamma, 1, q)$ *expressed by the cardinality of the divisible group is*

$$b = n^2\lambda$$

Proof: From the relations of GD parameters

- $vr = bk$
- $r(k-1) = n(v/n-1)\lambda$,

we obtain the simple equation $b = \frac{v(v-n)\lambda}{k(k-1)} = \frac{kn^2(k-1)\lambda}{k(k-1)} = n^2\lambda$

Theorem 3 *The existence of ideal threshold scheme is equivalent to the existence of combinatorial design satisfying the condition for the number of blocks expressed by the cardinality of the divisible group. In other words, the following two statements are equivalent.*

- $D = (\mathcal{P}, \mathcal{B})$ is a t design with parameter v, b, r, k, λ satisfying the condition for the number of blocks expressed by the cardinality of the divisible group.
- $PS(\Gamma, 1, q)$ is an ideal scheme with (t, w)-threshold access structure Γ.

Proof: Immediate from theorems 1 and 2.

5. Conclusion

We have addressed the problems associated with a threshold scheme expressed as a matrix and investigated the combinatorial properties of ideal schemes with threshold access structure. We showed that their existence is equivalent to the existence of combinatorial designs. Also, we presented the condition for the number of blocks in ideal schemes.

Reference

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

[BS92] E.F.Brickell, D.R.Stinson, " *Some improved bounds on the information rate of perfect secret secret sharing schemes,*" J. Cryptology, 5,153-166,1992.

[Bl79] G.R.Blakley, " *Safeguarding cryptographic keys,*" Proc. of AFIPS 1979 Nat. Computer Conference 48, pp313-317, 1979.

[HP85] D.R.Hughes, F.C.Piper, " *Design theory,*" Cambridge Univ. Press, Cambridge, 1985.

[Sh79] A.Shamir, " *How to share secret,*" Commun. of the ACM,22, pp612-613, 1979.

[SV87] D.R.Stinson, S.A.Vanstone, "*A Combinatorial approach to threshold schemes,*" Advances in Cryptography - Proc. of Crypto'87, Notes Comp. Science, pp330-339, 1987.

Appendix 1 : *The Definition of Designs*

A group-divisible design $GD(k, \lambda, n; v)$ is a triple (X, G, A), which satisfies the following four properties:

(1) X is a set of v elements called points.

(2) G is a partition of X into v/n subsets of n points, called groups.

(3) A is a set of subsets of X (called blocks), each of size k, such that a group and a block contain at most one common point.

(4) every pair of points from distinct groups occurs in exactly λ blocks.

The relations between GD parameters is as follows (if $n = 1$, then this relation gives the relation of $BIBD$).

- $vr = bk$
- $r(k-1) = n(v/n-1)\lambda = (v-n)\lambda$

A Transversal Design $TD(k, \lambda; n)$ is a triple (X, G, A), which satisfies the following four properties:

(1) X is a set of kn elements called points.

(2) G is a partition of X into v/n subsets of n points, called groups.

(3) A is a set of λn^2 subsets of X (called blocks)such that a group and a block contain at most one common point.

(4) every pair of points from distinct groups occurs in exactly λ blocks.

An Affine Resolvable BIBD is a $2-(v, k, \lambda)$design $D = (P, B, I)$ which has a partition $\mathcal{B} = B_1 \cup B_2 \cup \cdots \cup B_r$ of the block set B such that any point occurs exactly once in the blocks of each set B_i, $1 \leq i \leq r$(i.e., each B_i is a parallel class of D), and two blocks of distinct classes intersect exactly in μ, $\mu \geq 0$, points. It holds that $|B| = rn$, $|P| = kn$, $n \geq 2$, and $\lambda = \frac{r(k-1)}{nk-1}$, $k = \mu n$.

An Orthogonal Array $OA(k, n)$ is an $n^2 \times k$ array, with entries chosen from a symbol set of n elements, such that any pair of columns contains every ordered pair of symbols exactly once.

A Steiner System $S(t, k, w)$ is a pair (X, A), where X is a set of w elements(called points) and A is a set of k-subsets of X(called blocks), such that every t-subset of points occurs in exactly one block. A $S(t, k, w)$ is said to be non-trivial if $t < k < w$.